Двадесетте най-критични уязвимости в сигурността на Интернет
Общо мнение на експертите

Въпроси и коментари можете да отправяте на адрес top20@sans.org.

Въведение
Топ 20 на SANS за уязвимостите в сигурността на Интернет

Появата на огромно мнозинство от червеи и други успешни кибератаки става възможна поради уязвимостите в малък брой често използвани услуги на операционната система. Нападателите се възползват от възможностите. Те поемат по най-лесния и най-удобния път и използват известните пропуски чрез най-ефективните и широко разпространени средства за атака. Те залагат на организации, които не взимат мерки за отстраняване на проблемите и често атакуват безразборно, като сканират Интернет за всякакви уязвими системи. Лесното разпространение на червеи като Blaster, Slammer и Code Red, довело до разрушителни последици, може да бъде проследено директно до злонамереното използване на незакърпени уязвимости.

Преди четири години институтът SANS и Националният център за защита на инфраструктурата (National Infrastructure Protection Center - NIPC) към ФБР публикуваха документ, обобщаващ десетте най-критични уязвимости в сигурността на Интернет. Хиляди организации използваха този списък, както и разширените Топ 20 списъци, които бяха издадени след 1-2 години, за да създадат приоритети в своите усилия, така че да закърпят първо най-опасните дупки. Уязвимите услуги, които доведоха до разпространението на споменатите по-горе червеи Blaster, Slammer и Code Red, както и NIMDA са част от този списък.

Този актуализиран Топ 20 на SANS представлява всъщност два списъка Топ 10: десетте най-използвани уязвими услуги в Windows и десетте най-използвани уязвими услуги в UNIX и Linux. Макар че всяка година се случват хиляди инциденти със сигурността, които оказват влияние върху тези операционни системи, огромното мнозинство успешни атаки са насочени към една или повече от тези двадесет уязвими услуги.

Топ 20 е списък на уязвимостите, които изискват незабавно вземане на мерки, съставен след консенсус. Той е резултат от съвместната работата на десетки водещи експерти в областта на сигурността. Те идват от най-пряко свързаните със сигурността на информацията федерални агенции в САЩ, Великобритания и Сингапур; от водещите производители на софтуер и консултантски фирми в областта на сигурността; от най-добрите университетски програми, свързани със сигурността; от множество други потребителски организации и от института SANS. Списък на участниците можете да намерите в края на този документ.

Топ 20 на SANS е "жив" документ. Той включва подробни инструкции и препратки към допълнителна информация, полезна за отстраняване на пропуските в сигурността. Ние ще обновяваме този списък и инструкциите паралелно с идентифицирането на най-критичните заплахи и най-често срещаните или подходящи методи за справяне с тях и ще приветстваме вашето участие в този процес. Това е документ, отразяващ общото мнение на цялата общност – вашият опит в борбата с нападателите и в отстраняването на уязвимостите може да помогне на другите, които идват след вас. Моля изпращайте предложенията си по електронната поща на адрес top20@sans.org.

Бележки към читателите

Номера от списъка на CVE

В описанието на всяка уязвимост ще откриете препратки към номерата от списъка на CVE (Common Vulnerabilities and Exposures - често срещани уязвимости и излагания на опасност). Можете да видите и CAN номера. CAN номера получават кандидатите за влизане в списъка на CVE, които все още не са проверени изцяло. За повече информация относно отличения с награди проект CVE, посетете http://cve.mitre.org.

CVE и CAN номерата отразяват уязвимостите с най-висок приоритет, които трябва да бъдат проверени за всяка позиция. Всяка препратка към уязвимост от списъка на CVE има линк към свързаната с нея уязвимост в службата за индексиране на уязвимости (http://icat.nist.gov) на проекта ICAT на Националния институт по стандарти и технология (National Institute of Standards and Technology - N). ICAT предоставя кратко описание на всяка уязвимост, списък с нейните характеристики (например диапазон на свързаните с нея атаки и потенциални щети), списък с имената и номерата на версиите на уязвимия софтуер, както и линкове към страници със съвети и информация за кръпките за съответните уязвимости.

Портове, които трябва да бъдат блокирани от защитната стена

---- Преминете към индекса на портовете, които трябва да бъдат блокирани от защитната стена или шлюза ----

В края на този документ ще намерите един допълнителен раздел, който предлага списък от най-често проучваните и атакувани портове. Чрез блокиране на тези портове с помощта на защитна стена (firewall) или други устройства за защита на периметъра на мрежата, вие можете да добавите допълнителен слой за защита, който да ви помага да се предпазите от грешки и пропуски в конфигурацията. Забележете обаче, че използването на защитна стена или маршрутизатор за блокиране на мрежовия трафик, насочен към определен порт, не защитава този порт от враждебно настроени колеги, които вече са вътре във вашия периметър, нито от хакери, които може би са проникнали във вашия периметър чрез други средства. Освен това, много по-сигурно е в конфигурациите на защитната стена и маршрутизатора да се зададе отказ или блокиране на всичко по подразбиране, което не е изрично разрешено, отколкото да се блокират поотделно конкретни портове.

обратно в началото ^

Топ уязвимости на Windows системите

- W1 Уеб сървъри и услуги
- W2 Услуга Workstation (работни станции)
- W3 Услуги за отдалечен достъп до Windows
- W4 Microsoft SQL Server (MSSQL)
- W5 Автентификацията при Windows
- W6 Уеб браузъри
- W7 Приложения за споделяне на файлове
- W8 LSASS
- W9 Пощенски клиент
- W10 Съобщения в реално време

Топ уязвимости на UNIX системите

- U1 Системата за имена на домейни BIND
- U2 Уеб сървър
- U3 Автентификация
- U4 Системи за контрол на версиите
- U5 Обслужване на транспортирането на пощата
- U6 Simple Network Management Protocol (SNMP)
- U7 Open Secure Sockets Layer (SSL)
- U8 Лоша конфигурация на корпоративните услуги NIS/NFS
- U9 Бази данни
- U10 Kernel (ядро)

обратно в началото ^

Топ уязвимости на Windows системите (W)

W1 Уеб сървъри и услуги

W1.1 Описание

С течение на времето инсталациите по подразбиране на различните HTTP сървъри и допълнителните компоненти за обслужване на HTTP заявки, както и различните медии в Windows платформите, търсещи връзка с Интернет, се оказаха уязвими спрямо голям брой сериозни атаки. Влиянието на тези уязвимости може да включва:

- Отказ от обслужване
- Разгласяване или компрометиране на поверителни файлове или данни
- Изпълнение на произволни команди на сървъра
- Пълно компрометиране на сървъра

HTTP сървъри като IIS, Apache, и iPlanet (понастоящем SunOne) имаха многобройни проблеми, за които бяха създадени кръпки веднага след откриването им. Уверете се, че са инсталирани всички последни кръпки и, че е стартирана текущата версия на сървъра. При по-голямата част от софтуера за HTTP сървъри конфигурацията по подразбиране е доста отворена, като предоставя широки пътища за експлойтите. Отделете време за настройка на конфигурацията така, че тя да разрешава само минималния набор възможности, необходими за коректна работа на уеб сайта.

IIS използва програмна кука (hook), известна като ISAPI, за асоцииране на файлове с определени разширения към DLL-и (известни като ISAPI филтри).

Препроцесори като ColdFusion и PHP използват ISAPI, а IIS включва множество ISAPI филтри за работа с функции като Active Server Pages (ASP), Net уеб услуги и уеб базирано споделяне на принтери. Много ISAPI филтри, инсталирани по подразбиране с IIS, не са необходими при повечето инсталации и голяма част от тях могат да бъдат използвани злонамерено. Примери за злонамерени програми, които използват този механизъм за разпространение, са добре известните червеи Code Red и Code Red 2. Разрешете само ISAPI разширенията, които уеб сървърът ще трябва да разпознава. Препоръчва се да се ограничат HTTP опциите, които могат да бъдат използвани с всяко разрешено ISAPI разширение.

Много уеб сървъри включват примерни приложения или уеб сайтове, които са били проектирани да демонстрират функционалните им възможности. Тези приложения не са предназначени да осигуряват сигурна работа при нормални работни условия. Някои IIS примерни приложения позволяват отдалечено разглеждане или презаписване на произволни файлове, както и отдалечен достъп до друга поверителна информация за сървъра, включително администраторската парола. Премахнете тези приложения, преди да поставите сървъра в работно състояние.

Инсталация на IIS, която не се поддържа, също може да стане жертва на уязвимости, открити след датата на излизане на софтуера на пазара. Пример за това са уязвимостите в ntdll.dll на WebDAV в IIS 5.0, които позволяват атаки от тип отказ от обслужване и могат да разрешат на всеки посетител на даден уеб сайт да създава и стартира скриптове на сървъра, както и уязвимостта Unicode exploit, която позволява на всеки посетител на уеб сайт да изпълнява произволни команди на уеб сървъра само чрез заявка за достъп до умело създадени URL-та.

Инсталация на IIS, която не се поддържа редовно, също може да стане жертва на уязвимости, открити след датата на излизане на софтуера на пазара. Пример за това са PCT и SSL уязвимостите, третирани от кръпката MS04-011 на Microsoft, които могат да разрешат състояние тип отказ от обслужване или възможност за нападателя да поеме управлението на сървъра. Навременното инсталиране на кръпките на обществено достъпните сървъри е от критично значение.

Добавъчни модули от други производители, като ColdFusion и PHP, могат да внесат допълнителни уязвимости в една инсталация на IIS чрез неудачна промяна на конфигурацията или чрез уязвимости, вътрешноприсъщи на продукта.

W1.2 Засягани операционни системи

Всяка система с Microsoft Windows и инсталиран уеб сървър може да бъде засегната. Тук се включват, без списъкът да е изчерпателен:

- Microsoft IIS: Windows NT4.0 и по-високи версии, включително XP Professional
- HTTP сървър Apache: поддържат се Windows NT 4.0 SP3 и по-високи версии, макар да се смята, че върви на Win95 и Win98

- Sun Java System/Sun One/iPlanet Web Server: Windows NT 4.0 SP6 и по-високи версии

Моля отбележете: Windows 2000 Server се продава с инсталиран по подразбиране IIS, както откриха много администратори по време на нашествието на покритите с позорна слава Nimda и Code Red. Освен това, някои приложения, разработени от трети страни, се нуждаят от функционалните възможности, осигурявани от IIS, което може би кара администраторите несъзнателно да инсталират този софтуер. Никога не считайте, че една мрежа е имунизирана срещу атаки към уеб сървъра само, защото такъв сървър не е инсталиран умишлено; редовно проверявайте мрежите за присъствие на сървър-"мошеник". За повече информация прегледайте по-долу "Как да определите дали сте подложени на риск".

W1.3 Свързани с въпроса CVE номера

a. IIS

CVE entries for IIS 2.0
CVE entries for IIS 3.0
CVE entries for IIS 4.0
CVE entries for IIS 5.0

b. Apache

CAN-2001-0729, CAN-2002-0249, CAN-2002-0654, CAN-2002-0661, CAN-2002-0661, CAN-2003-0016, CAN-2003-0017, CAN-2003-0460, CAN-2003-0844, CAN-2004-0492, CAN-2004-0493

CVE-1999-0448, CVE-2000-0505, CVE-2001-1342, CVE-2001-1342

Apache модули: CAN-2003-0844, CAN-2004-0492

c. iPlanet/Sun

CAN-2002-0686, CAN-2002-1042, CAN-2002-1315, CAN-2002-1315, CAN-2002-1316, CAN-2003-0411, CAN-2003-0412, CAN-2003-0414, CAN-2003-0676, CAN-2003-0676

CVE-2000-1077, CVE-2000-1077, CVE-2001-0252, CVE-2001-0327, CVE-2001-0327, CVE-2002-0845, CVE-2002-0845

d. Добавъчни елементи

CAN-1999-0455, CAN-1999-0477, CAN-1999-1124, CAN-2001-0535, CAN-2001-1120, CAN-2002-1309, CAN-2003-0172

CVE-1999-0756, CVE-1999-0922, CVE-1999-0924, CVE-2000-0410, CVE-2000-0538

ColdFusion: CVE-1999-0756¸ CVE-1999-0760, CVE-1999-0922, CVE-1999-0924, CAN-2002-1309, CAN-2004-0407, CVE-2000-0189, CVE-2000-0382, CVE-2000-0410, CVE-2000-0538, CVE-2002-0576

PHP: CAN-2002-0249, CAN-2003-0172

e. **Други услуги**
CAN-1999-1369, CAN-2003-0227, CAN-2003-0349, CAN-2003-0725, CAN-2003-0905

CVE-1999-0896, CVE-1999-1045, CVE-2000-0211, CVE-2000-0272, CVE-2000-0474, CVE-2000-1181, CVE-2001-0083

eEye SecureIIS: CAN-2001-0524

Jakarta Tomcat: CAN-2003-0045

W1.4 Как да определите дали сте подложени на риск
Всички инсталации на уеб сървър по подразбиране и без инсталирани кръпки са уязвими по презумпция.

Повечето доставчици на уебсървъри и услуги осигуряват богата информация по отношение на текущите проблеми със сигурността. Ето някои примери:

- Apache HTTP сървър Main Page & Security Report
- Microsoft TechNet Security Centre
- Microsoft Internet Information Server (IIS) Security Centre
- Sun Web, Portal, & Directory Servers Download Centre
- Macromedia Security Zone
- Real Networks Security Issues
- PHP Home Page и Downloads

Проверявайте *редовно* също така нивата на кръпките и версиите на софтуера на уеб сървъра и свързаните с него услуги, включително и конфигурациите спрямо предоставената от производителя информация относно сигурността и базата данни на CVE*,* за да оцените потенциалната уязвимост. Важно е да се разбере, че нови проблеми се откриват непрекъснато и най-добрата практика е да се консултира текущата база данни на CVE с цел правилно оценяване на потенциалната уязвимост.

Съществуват някои отдалечени и локални средства за оценяване на уязвимостта, които помагат на администраторите на уеб сървъри да проверяват своите мрежи; те включват:

- Nessus (отворен код)
- SARA (отворен код)
- Nikto (отворен код)
- eEye Free Utilities & Commercial Scanners
- Microsoft Baseline Security Analyzer (специфичен за IIS)

Препоръчва се средствата за отдалечено оценяване на уязвимостта да се стартират на цялата мрежа, а не само на известните сървъри, с цел да се оцени потенциалната уязвимост на "мошеническите" инсталации на уеб сървъри.

W1.5 Как да се защитим срещу тези уязвимости

За повечето системи

1. Инсталирайте съответните кръпки за HTTP услугата, както и за операционната система и за всички приложения, заредени на същия хост. След като кръпките са актуализирани веднъж, поддържайте ги в това състояние.
2. Инсталирайте базиран на хоста антивирусен софтуер и софтуер за откриване на непозволени прониквания. Уверете се, че и двете са актуализирани по отношение на кръпките и преглеждайте често лог файловете.
3. Забранете скрипт интерпретаторите, които не се използват и премахнете изпълнимите им файлове. Например, perl, perlscript, vbscript, jscript, javascript и php.
4. Разрешете записването на логове, ако то е по избор, и ги преглеждайте често, за предпочитане чрез автоматизиран процес, който резюмира събитията и докладва за изключенията и подозрителните събития.
5. Използвайте подобна на syslog система за сигурно съхраняване на друга система на логовете на операционната система и HTTPd.
6. Отстранете или ограничете системните инструменти, които често се използват от нападателите като помощни средства при началното компрометиране и експанзията отвъд началния хост-жертва. Например: tftp(.exe), ftp(.exe), cmd.exe, bash, net.exe, remote.exe и telnet(.exe).
7. Ограничете приложенията, работещи на хоста, до HTTP услуга/демон и поддържащите ги услуги.
8. Там, където това се окаже практично, не стартирайте домейнови или други системи за автентификация на хоста.
9. Бъдете нащрек и сведете до минимум всички вектори във вътрешната мрежа, които влизат през публичен уеб сървър(и). Например, NetBIOS споделяния, доверени взаимоотношения и взаимодействие между бази данни.
10. Използвайте различни конвенции за имената на акаунтите и уникални пароли за публично отворените системи и за вътрешните системи. Не трябва всяко изтичане на информация от публично отворена система да подпомага атака към вътрешните системи.

а. IIS

Инсталирането на кръпките на сървъра при самото му инсталиране е необходимо, но не достатъчно. Инсталирайте кръпките паралелно с откриването на нови слабости в IIS. Ако имате инсталиран само един сървър, можете да използвате Windows Update и Automatic Update. Ако са няколко, инструментът HFNetChk (Network Security Hotfix Checker) помага на системния администратор при сканирането на локални или отдалечени системи за необходимостта от нови кръпки. Този инструмент работи на Windows NT 4, Windows 2000 и Windows XP. Текущата версия може да бъде свалена от сайта на Microsoft http://www.microsoft.com/technet/security/tools/hfnetchk.asp.

И нещо допълнително: в читалнята на SANS можете да намерите една много полезна статия, озаглавена Securing a Windows 2000 IIS Web Server – Lessons Learned от Harpal.

Използване на IIS Lockdown Wizard за обезопасяване на инсталацията

Microsoft пусна лесен за използване инструмент под името IIS Lockdown Wizard, който да подпомага обезопасяването на IIS инсталациите. Текущата версия може да бъде свалена от сайта на Microsoft
http://www.microsoft.com/technet/security/tools/locktool.asp

Стартирането на IIS Lockdown Wizard в режим "custom" или "expert" ще ви позволи да извършите следните препоръчителни промени в една IIS инсталация:

- Забрана на WebDAV (освен ако използването му за публикуване на информация в уеб пространството не е абсолютно наложително).
- Изключване на всички ненужни ISAPI разширения (включително .htr, .idq, .ism и особено на .printer).
- Отстраняване на приложения, инсталирани като образци (примери за използване).
- Налагане на забрана на уеб сървъра за стартиране на системни команди, които често се използват за компрометирането му (например cmd.exe и tftp.exe).

В читалнята на SANS можете да намерите статията Using Microsoft's IISlockdown tool to protect your IIS Web Server от Jeff Wichman, която е специално насочена към средството IISlockdown.

Използване на URLScan за филтриране на HTTP заявки
Много IIS експлойти, включително Code Blue и фамилията Code Red, използват злонамерено оформени HTTP заявки при атаки от тип обхождане на директория (directory traversal) или препълване на буфер. Филтърът URLScan може да бъде конфигуриран така, че да отхвърля такива заявки преди сървърът да се опита да ги обработи. Текущата версия е интегрирана в IIS Lockdown Wizard, но може да бъде свалена и отделно от сайта на Microsoft
http://www.microsoft.com/technet/security/tools/urlscan.mspx.

b. Apache

Проблемите на контрола на достъпа, ограничението чрез IP и модулите за сигурност на Apache, както много други проблеми, са дискутирани на страницата Apache Tutorials.

Освен това, в читалнята на SANS можете да намерите изключително полезната статия Securing Apache: Step-by-Step от Artur Maj, която разглежда подробно задачите по обезопасяването на един Apache сървър.

c. iPlanet/Sun One

Edmundo Farinas разглежда обезопасяването на iPlanet в своята статия Security Considerations for the iPlanet Enterprise Web Server on Solaris, която се намира в читалнята на SANS.

Освен това, Sun предлага и статията Sun ONE Application Server Security Goals, която разглежда подробно стъпките, препоръчвани за обезопасяване iPlanet/Sun One сървър.

d. Добавъчни модули

Ако използвате добавъчни модули, като ColdFusion, PerlIIS, или PHP, проверете на уеб сайтовете на производителите за кръпки и за съвети относно конфигурирането им. По очевидни причини, Microsoft не включва кръпки за софтуер на трети страни в Windows Update и съответните услуги за актуализиране.

За информация относно обезопасяването на ColdFusion прегледайте в читалнята на SANS статията Web Application Security, with a Focus on ColdFusion от Joseph Higgins

В читалнята на SANS се намира и статията Securing PHP: Step-by-step от Artur Maj, която илюстрира процеса на обезопасяване на PHP приложенията.

Един допълнителен полезен ресурс е PHP Manual, Chapter 16. Security, където подробно е разгледана сигурността на PHP.

e. Други услуги

Макар че съществуват общи стъпки, които са изброени по-горе, и които могат да бъдат изпълнени за обезопасяване на повечето уеб услуги, всяка от тях обикновено има свой собствен уникален набор от актуализации и кръпки, предоставяни от производителя, препоръчителни конфигурации и възможности за записване на логовете.

Прегледайте документацията, както и цялата информация, публикувана на уеб сайта на производителя и се уверете, че сте се абонирали за всички уведомителни услуги и писма с новини от производителя. Това ще ви помогне да бъдете непрекъснато информирани за съответните проблеми по сигурността и да се справяте с тях бързо и ефективно.

обратно в началото ^

W2 Услуга Workstation (работни станции)

W2.1 Описание

Услугата Windows Workstation отговаря за обработката на заявки от потребители за достъп до ресурси като файлове и принтери. Услугата определя дали ресурсите се намират в локалната система или в споделен мрежов обект и насочва по съответен подходящ начин потребителските заявки.

Функциите по управление на мрежата, осигурявани от услугата, могат да бъдат извикани чрез един от следните механизми:

- DCE/RPC повиквания по протокол SMB след свързване с услугата чрез именован канал \\pipe\wkssvc.
- DCE/RPC повиквания директно през UDP порт (> 1024)
- DCE/RPC повиквания директно през TCP порт (> 1024)

Отбележете, че услугата се свързва към първия наличен TCP и UDP порт над 1024.

Услугата Workstation съдържа стек-базирано препълване на буфер, което може да бъде задействано чрез специално създадено DCE/RPC повикване. Проблемът

възниква, тъй като параметрите се предават на функцията за влизане в системата без никакви проверки на ограниченията. Това препълване може да бъде злонамерено използвано от неавтентифициран отдалечен нападател за изпълняване на произволен код на уязвимата Windows машина със "SYSTEM" привилегии. Нападателят може да получи пълен контрол върху компрометираната машина. В Интернет беше публикуван код на експлойт, който използва тази уязвимост, и той беше използван при някои варианти на червея Phatbot/Gaobot, който зарази милиони системи по целия свят.

W2.2 Засягани операционни системи
Windows 2000 SP2, SP3 и SP4
Windows XP
Windows XP 64 Bit Edition

W2.3 CVE/CAN номера
CAN-2003-0812

W2.4 Как да определите дали сте уязвими
Системите, работещи под Windows 2000 без кръпката MS03-049 и под Windows XP без кръпката MS03-043, са уязвими.

Проверете за наличието на следните записи в регистъра:
KB828035: Under HKLM\Software\Microsoft\Updates\Windows XP (Windows XP)
KB828749: Under HKLM\Software\Microsoft\Updates\Windows 2000 (Windows 2000)
Ако тези записи липсват в регистъра, Windows системата е уязвима.

Друга възможност е използването на някакъв мрежов скенер като Microsoft Baseline Security Analyzer (MBSA), който да провери дали е инсталирано подходящото обновяване. MBSA може да бъде свален от
http://www.microsoft.com/technet/security/tools/mbsahome.mspx

W2.5 Как да се защитим

(a) Уверете се, че на Windows системите са инсталирани последните кръпки, свързани със сигурността. Специално проверете дали на системите с Windows 2000 е инсталирана кръпката MS03-049, а на системите Windows XP – кръпката MS03-043.
(b) Блокирайте портовете 139/tcp и 445/tcp на периметъра на мрежата. Това ще възпрепятства отдалечения нападател да използва препълването през SMB.
(c) Отворете на мрежовия периметър само необходимите TCP портове над 1024. Това ще възпрепятства отдалечения нападател да използва препълването през DCE/RPC повикванията. Отбележете, че е трудно при защитната стена да се блокират UDP портовете над 1024, тъй като портовете в този диапазон се използват като ефемеридни портове.
(d) Използвайте TCP/IP филтрирането, което се предлага при Windows 2000 и XP, или Internet Connection Firewall при системите с Windows XP, за да блокирате входящия достъп до съответните портове.

(e) Уверете се, че са инсталирани съответните кръпки от производителя за приложения от трети страни, работещи на индивидуализирани Windows 2000/XP платформи. Cisco, например, публикува документ, според който някои продукти на Cisco са уязвими спрямо това препълване. Cisco осигури и съответни кръпки.
(f) Ако системата е самостоятелна, т.е. не принадлежи към Windows мрежово обкръжение, услугата Workstation може да бъде изключена без никакви последствия.

Допълнителна информация:

Microsoft Advisory
http://www.microsoft.com/technet/security/bulletin/MS03-049.mspx

eEye Advisory
http://www.eeye.com/html/Research/Advisories/AD20031111.html

CERT Advisories
http://www.cert.org/advisories/CA-2003-28.html
http://www.kb.cert.org/vuls/id/567620

CORE Security Advisory
http://archives.neohapsis.com/archives/vulnwatch/2003-q4/0066.html

Cisco Advisory
http://www.cisco.com/warp/public/707/cisco-sa-20040129-ms03-049.shtml

Gaobot Worm
http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.gaobot.gen.html

обратно в началото ^

W3 Услуги за отдалечен достъп до Window

W3.1 Описание

Семейството операционни платформи на Windows поддържа множество различни методи и технологии за работа в мрежа. Те притежават вградена поддръжка за повечето стандартни мрежови протоколи и вградени функционални възможности за повечето специфични за Microsoft методи и техники за работа в мрежа. Сред специфичните за MS мрежови технологии съществуват печално известни или зле конфигурирани елементи като NETBIOS Network Shares, Anonymous Logon NULL сесии, отдалечен достъп до регистъра и отдалечено повикване на процедури. Тези елементи водят до споделяне в голям мащаб на най-често срещаните на мрежово ниво експлойти за Windows и са описани накратко в следния текст.

NETBIOS - Незащитени мрежови споделяния в Windows. Microsoft Windows осигурява на една хост машина възможността да споделя файлове или папки с други хостове през мрежата чрез незащитени мрежови споделяния в Windows. Механизмът, на който се основава тази възможност, е протоколът Server Message Block (SMB) или Common Internet File System (CIFS). Тези протоколи позволяват на един хост да обработва отдалечени файлове така, както обработва локалните.
Въпреки че това е мощно и полезно свойство на Windows, неправилната

конфигурация на мрежовите споделяния може да изложи на непозволено разкриване критични файлове от системата или да осигури на злонамерен потребител или програма механизъм за получаване на пълен контрол над хоста. Един от начините, по който червеят I-Worm.Klez.a-h (Klez Family), вирусът Sircam (вижте CERT Advisory 2001-22) и червеят Nimda (вижте CERT Advisory 2001-26) се разпространиха така бързо през 2001, беше откриването на незащитени мрежови споделяния и поставянето на техни копия в тях. Много собственици на компютри неволно отварят своите системи за хакери, когато се опитват да увеличат удобствата за свои колеги и външни сътрудници, разрешавайки четенето и записа на своите устройства от мрежови потребители. Но когато се положат грижи за осигуряване на правилно конфигуриране на мрежовите споделяния, рисковете от компрометиране могат да бъдат значително намалени.

Анонимно влизане в системата - Нулева сесия е сесия, която се стартира без автентифициране (т.е. с празно потребителско име и парола). Нулевите сесии могат да бъдат използвани за извеждане на информация за потребители, групи, споделяния и политика по отношение на паролите. При Microsoft Windows NT услугите, стартирани като Local System account на локалния компютър, комуникират с други услуги по мрежата чрез стартиране на нулеви сесии. Услугите при Windows 2000 и по-новите версии, стартирани като Local System account на локалния компютър, използват акаунта на локалния компютър, за да се автентифицират пред другите сървъри. Active Directory, работещ в естествения си режим, не приема заявки за нулеви сесии. При смесен режим, Active Directory позволява достъп, съвместим с версиите, по-стари от Windows 2000, чрез приемане на заявки за нулеви сесии, което на свой ред, наследява уязвимостите, внасяни от нулевите сесии при Windows NT.

Отдалечен достъп до регистъра - Microsoft Windows 9x, Windows CE, Windows NT, Windows 2000, Windows ME и Windows XP използват централизирана йерархична база данни, известна като регистър, за да управляват софтуера, конфигурацията на устройствата и потребителските настройки. Неподходящите разрешения или настройки на сигурността могат да позволят отдалечен достъп до регистъра. Нападателите могат да използват тази възможност, за да компрометират системата или да поставят основата за създаване на файлови асоциации и разрешения, които позволяват изпълнението на злонамерен код.

Отдалечено извикване на процедури - Много версии на операционните системи на Microsoft (Windows NT 4.0, 2000, XP и 2003) осигуряват механизъм за комуникация между процесите, който позволява на програми, стартирани на един хост, да изпълняват кодове на отдалечени хостове. Бяха публикувани три уязвимости, които позволяват на един нападател да стартира произволен код на податливите хостове чрез привилегиите на локалната система (Local System privileges). Една от тези уязвимости беше използвана от червеите Blaster/MSblast/LovSAN и Nachi/Welchia. Съществуват и други уязвимости, които позволяват на нападателите да осъществяват атаки от тип отказ от обслужване срещу RPC компоненти.

W3.2 Засягани операционни системи

Всички Windows 95, Windows 98, Windows NT Workstation и Server, Windows Me, Windows 2000 Workstation и Server, Windows XP Home и Professional и Windows 2003 са уязвими.

W3.3 CVE/CAN номера

NETBIOS
CVE-2000-0979

CAN-1999-0518, CAN-1999-0519, CAN-1999-0621, CAN-2000-1079

Анонимно влизане в системата
CVE-2000-1200

Отдалечен достъп до регистъра
CVE-2000-0377, CVE-2002-0049

CAN-1999-0562, CAN-2001-0045, CAN-2001-0046, CAN-2001-0047, CAN-2002-0642, CAN-2002-0649, CAN-2002-1117

Отдалечено извикване на процедури
CAN-2002-1561, CAN-2003-0003, CAN-2003-0352, CAN-2003-0528, CAN-2003-0605, CAN-2003-0715

W3.4 Как да определите дали сте уязвими

Как да определите дали сте уязвими по отношение на проблемите, свързани с NETBIOS.
Съществуват много средства, които могат да ви помогнат да определите дали на дадена система има уязвимости, свързани с NETBIOS.

NbtScan - NetBIOS Name Network изследва услугите за споделяне на файлове на NETBIOS, които се предлагат на съответните системи. NbtScan може да се намери на: http://www.inetcat.org/software/nbtscan.html.

NLtest – изключително мощен инструмент, включен в Windows 2000 and 2003 Support Tools (можете са го намерите на компакт диска с продукта) и Windows NT4 Resource Kit. NLtest може да осигури богата информация относно потенциалните уязвимости на конфигурацията.

Потребителите на Windows 95/98/Me могат да използват Legion v2.11, последната версия на скенера Legion File Share от Rhino9, за да сканират за мрежови споделяния под Windows.

Администраторите на Windows 2000 могат да използват Security Fridays Share Password Checker (SPC), за да сканират своите Windows 95/98/Me клиенти за споделяне на файлове и да проверят дали са уязвими по отношение на уязвимостта Share Level Password, чрез която един нападател може да научи паролите на споделянията.

При Windows NT (SP4), Windows 2000, Windows XP и Windows 2003, Microsoft Baseline Security Analyser ще докладва за хостове, които са уязвими за SMB експлойти, и може да бъде използван за решаване на проблема. Тестовете могат да бъдат стартирани локално или от отдалечени хостове.

Потребителите на Windows NT, Windows 2000, Windows XP и Windows 2003 могат просто да въведат командата *net share* от командния ред, за да проверят кои ресурси са споделени. За повече информация относно командата net share напишете *net share /?*.

ВАЖНА забележка: Тази материал съдържа информация относно извършването на промени в споделени ресурси. Преди да бъде променен някой споделен ресурс, убедете се, че знаете как да бъде възстановен ресурсът, ако възникне проблем. Препоръчва се всички промени да бъдат тествани цялостно, преди да бъдат реализирани в работни условия. За информация относно споделените ресурси щракнете върху номерата на следващите статии, за да видите съответната статия в Microsoft Knowledge Base:

125996 - Saving and Restoring Existing Windows Shares

308419 - HOW TO Set, View, Change, or Remove Special Permissions for Files and Folders in Windows XP

307874 - HOW TO Disable Simplified Sharing and Password-Protect a Shared Folder in Windows XP

174273 – How to Copy Files and Maintain NTFS and Share Permissions

Разрешения по подразбиране при нови споделяния:

Windows NT, Windows 2000, и Windows XP (по-стари от сервизен пакет 1)

- Всички – Пълен контрол

Windows XP SP1 • Всички – За четене

По подразбиране Windows XP има една споделена директория, наречена "SharedDocs." Физически тя се намира в:

"C:\Documents and Settings\All Users\Documents"

- Всички Пълен контрол

Повечето комерсиални мрежови скенери ще открият съществуващите споделяния. Един бърз, безплатен и сигурен тест за наличието на SMB споделяне на файлове и свързаните с него уязвимости, който е ефикасен за машини, работещи под операционната система Windows, можете да намерите на Gibson Research Corporation web site. Следвайте линковете до *ShieldsUP,* за да получите оценка в реално време на всички излагания на опасност на системата, свързани с SMB. Предлагат се и подробни инструкции, които да помогнат на потребителите на Microsoft Windows да се справят с SMB уязвимостите. Забележете, че ако системата е свързана в мрежа, в която има междинно устройство, блокиращо SMB, средството *ShieldsUP* ще докладва, че системата не е уязвима, но всъщност тя е. Такъв е случаят, например, при потребители с кабелен модем, при които доставчикът блокира SMB в мрежата с кабелен модем. *ShieldsUP* ще докладва, че системата не е уязвима. Но останалите около 4,000 души, които са потребители на същата кабелна мрежа все пак могат да използват тази уязвимост.

Ето няколко автоматизирани сканиращи средства, които могат да откриват уязвимости, свързани със споделянията:

- Nessus-- безплатно, мощно, съвременно и лесно за използване средство за отдалечено сканиране на сигурността
- Winfingerprint by vacuum --Win32 Host/Network Enumeration Scanner

Как да определите дали сте уязвими по отношение на проблемите, свързани с анонимното влизане в системата. Опитайте се да създадете нулева сесия на компютъра, като зададете от командния ред следната команда: (*Start --> Run -->* напишете *cmd*):

```
C:\>net use \\ipaddress\ipc$ "" /user:""
```

Този синтаксис осигурява връзка със скритите комуникации между процесите "share (*IPC$*) на ipaddress като вграден анонимен потребител (*/user:""*) с празна () парола.

Ако в отговор се получи съобщението: System error 5 has occurred. Access is denied., то системата не е уязвима.

Ако се получи съобщението "The command completed successfully", то системата е уязвима.

Описаните по-горе средства - Nessus и Winfingerprint – могат да бъдат използвани също така за откриване на уязвимости, свързани с нулевите сесии.

Как да определите дали сте уязвими по отношение на проблемите, свързани с отдалечения достъп до регистъра. NT Resource Kit (NTRK), който се предлага от Microsoft, съдържа изпълним файл, наречен *Regdump.exe,* който ще тества пасивно разрешенията за отдалечен достъп до регистъра от Windows NT хост до други Windows NT/Windows 2000 или Windows XP хостове по Интернет или вътрешна мрежа.

Освен това, можете да свалите колекция от shell скриптове от командния ред, които ще тестват разрешенията за достъп до регистъра, както и редица други средства, свързани със сигурността, от http://www.afentis.com/top20.

Как да определите дали сте уязвими по отношение на проблемите, свързани с отдалеченото извикване на процедури.
Microsoft са създали средство за бърза корекция (hotfix) и проверка на конфигурацията и кръпките, което може да бъде свалено безплатно; това вероятно е най-добрият начин да определите дали Windows хостовете са податливи на някоя от тези уязвимости. То се нарича Microsoft Baseline Security Analyzer (MBSA) и можете да го намерите на
http://www.microsoft.com/technet/security/tools/mbsahome.mspx

Съществува и самостоятелно средство за сканиране, което ще провери за липсващи кръпки, свързани със сигурността, само за CAN-2003-0352, CAN-2003-0528, CAN-2003-0605 и CAN-2003-0715; можете да го намерите на http://support.microsoft.com/?kbid=827363. Ние обаче препоръчваме да се използва MBSA, което има по-широко покритие. За домашните потребители и тези, които се грижат само за няколко компютъра, вероятно ще бъде по-лесно да

посетят сайта за Windows Update на http://windowsupdate.microsoft.com/ и да проверят за наличието на остарял софтуер на отделните машини.

W3.5 Как да се защитим

Сервизните пакети и средствата за бърза корекция на Microsoft са насочени съм уязвимостите в сигурността а операционните системи и приложните програми. Изключително важно е на всяка система да бъде инсталиран най-новия сервизен пакет.
Червеят *Sasser*, например, и неговите разновидности (използващи уязвимост на системата LSASS) заразиха много незакърпени системи по целия свят, а системите, на които беше инсталирано средството за бърза корекция MS04-011 бяха имунизирани срещу тази изключително опасна уязвимост. Microsoft пусна средството за бърза корекция MS04-011 няколко седмици преди появата на червея *Sasser*.

ЗАБЕЛЕЖКА: Microsoft вече не поддържа Windows 95 и Windows NT4 Workstation. Поддръжката за Windows NT4 Server приключва на 31 декември 2004.

За подробности относно жизнения цикъл на поддържаните операционни системи и продукти използвайте статията на Microsoft *Product Lifecycle Dates - Windows Product Family.*

За да намерите съответните средства за бърза корекция за дадена система, използвайте:

- Услугата Windows Update (*Start – Windows Update*). Тя автоматично открива всички необходими за системата средства за бърза корекция и ги инсталира след като потребителят избере (*одобри*) средствата за бърза корекция, които трябва да бъдат инсталирани.
- Он-лайн услугата Windows *Security Bulletin Search,* намираща се на: http://www.microsoft.com/technet/security/current.aspx

Въпреки че текущите сервизни пакети и средства за бърза корекция са насочени към решаването на много проблеми, свързани с проектирането на софтуера (като препълвания на буфери, грешки при проектирането на кода и т.н.), в операционната система Windows съществуват множество потенциално опасни възможности, които имат легитимна и документирана функционалност, но в много случаи могат да бъдат безопасно забранени или обезопасени с цел повишаване на сигурността на системата.

Как да се защитим срещу атаките, свързани с NETBIOS. Могат да бъдат предприети различни действия, които да намалят риска от използване на дадена уязвимост през мрежовите споделяния на Windows:

- Забранете услугите *Alerter* и *Messenger* (те са забранени по подразбиране при Windows 2003, но са настроени на автоматично стартиране (*Automatic* startup) при Windows 2000/XP/NT4). Забраняването на тези услуги значително намалява, предотвратява или снижава стойността на инвентаризацията на системата, която се провежда обикновено преди атака или заразяване.

За да забраните тези услуги:

- Изберете *Start – Programs – Administrative Tools – Services*;
- Изберете услугата *Alerter* – щракнете двукратно върху нея – задайте на *Startup type* стойност *Disabled* – натиснете бутона *Apply* – натиснете бутона *Stop* – натиснете бутона *OK.*
- Изберете услугата *Messenger* – щракнете двукратно върху нея – задайте на *Startup type стойност Disabled* – натиснете бутона *Apply* – натиснете бутона *Stop* – натиснете бутона *OK.*

Забранете споделянето навсякъде, където то не е необходимо.
Ако не е необходимо дадена система да осигурява услуги, свързани с файлове и печат (повечето типични офисни и домашни работни станции попадат в тази категория), *Server* може да бъде забранена при системи с Windows NT4/2000/2003/XP. За да забраните услугата *Server*:

Изберете *Start – Programs – Administrative Tools – Services* – изберете услугата *Server* – щракнете двукратно върху нея – задайте на *Startup type* стойност *Disabled* – натиснете бутона *Apply* – – натиснете бутона *Stop* – – натиснете бутона *OK.*
Ако системата не се нуждае от стартиране на услугата *Server*, могат да се изпълнят следните стъпки за обезопасяване на системите Windows NT4/2000/2003/XP:

1. Изведете списък на всички скрити споделяния по подразбиране (*C$, D$, E$* etc) като напишете командата:

```
Net share
```

от командния ред на системата. Запишете си съществуващите споделяния.

2. Изтрийте скритите споделяния по подразбиране като напишете командата:

```
Net share C$ /delete
```

от командния ред на системата. В повечето случаи всички споделяния, означени с *букви от азбуката* (*C$, D$, E$* и т.н.) и споделянето *ADMIN$* могат да бъдат безопасно изтрити. Изтриването на споделянето по подразбиране *IPC$* е препоръчително за всяка система.

3. За да се превърне изтриването на споделянията по подразбиране в окончателно (те ще се възстановят автоматично при рестартиране на системата или на услугата *Server*), е необходимо да се направят следните промени в регистъра:

- Отворете редактора на регистъра (Registry editor);
- Идете на ключа: *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ lanmanserver\parameters*
- Създайте в този ключ нова стойност:
- Име на стойността: *AutoShareWks*
- Тип на стойността: *DWord*
- Стойност: *00000000*

- Създайте в този ключ нова стойност:
- Име на стойността: *AutoShareServer*
- Тип на стойността: *DWord*
- Стойност: *00000000*

Прегледайте съществуващите на системата споделяния, които *не са по подразбиране* (създадени са допълнително). Това може да се осъществи чрез:

- Графичния интерфейс (*My Computer* – десен клик – *Manage – Shared Folders – Shares*). Изберете споделянията, които трябва да бъдат забранени – десен клик – Изберете *Stop Sharing.*
- Командния ред (от командния ред на системата или като част от някакъв скрипт):
    - Изведете списък на всички споделяния, като напишете командата:

      ```
      Net share
      ```

      от командния ред на системата. Запишете си съществуващите споделяния.
- Изтрийте ненужните споделяния, като напишете командата:

  ```
  Net share ShareName /delete
  ```

  от командния ред на системата.

По този начин ще изтриете окончателно само споделянията, които *не са по подразбиране* (създадени са допълнително). За окончателно изтриване на скритите споделяния по подразбиране *C$, D$, ADMIN$* вижте процедурата в предишния абзац.

- На Windows 95/98/Me клиентите, които са част от Windows NT домейн, се препоръчва настройването на контроли за достъп до споделените файлове на ниво потребител.
- Не разрешавайте споделяне с хостове по Интернет. Уверете се, че Windows мрежовите споделяния на всички свързани с Интернет хостове са забранени от мрежовия контролен панел на Windows. Споделянето на файлове с хостове по Интернет трябва да се извършва чрез SCP, FTP или HTTP.
- Не разрешавайте неавтентифицирани споделяния. Ако е необходимо споделяне на файлове, не разрешавайте неавтентифициран достъп до споделен ресурс. Конфигурирайте споделянето така, че свързването с него да се осъществява чрез парола.
- Ограничете споделянията до минималния необходим брой папки. В общия случай споделянията трябва да обхващат само една папка и може би нейните подпапки.
- Ограничете до необходимия минимум разрешенията за достъп до споделените папки. Бъдете особено внимателни относно достъпа за запис – разрешавайте го само, когато е абсолютно необходим.
- За да получите допълнителна сигурност, разрешете споделянето само от специфични IP адреси, тъй като DNS имената могат да бъдат фалшифицирани.

Как да се защитите срещу проблемите, свързани с анонимното влизане във вашите системи. ВАЖНА забележка: Тази материал съдържа информация относно извършването на промени в регистъра. Преди да бъде променен регистъра, убедете се, че му е направено резервно копие и че знаете как той да бъде възстановен, ако възникне проблем. Препоръчва се всички промени да бъдат тествани цялостно, преди да бъдат реализирани в работни условия. За информация относно изготвянето на резервно копие, възстановяването и редактирането на регистъра щракнете върху номерата на следващите статии, за да видите съответната статия в Microsoft Knowledge Base:

256986 - Description of the Microsoft Windows Registry
323170 - HOW TO Backup, Edit, and Restore the Registry in Windows NT 4.0
322755 - HOW TO Backup, Edit, and Restore the Registry in Windows 2000
322756 - HOW TO Backup, Edit, and Restore the Registry in Windows XP Windows Server 2003

Windows NT домейн контролерите изискват нулеви сесии, за да комуникират. Следователно, ако се работи в Windows NT домейн или Windows 2000/2003 Active Directory, работещ в смесен режим, който позволява съвместим достъп от машини с версии по-стари от Windows 2000, информацията, която нападателите могат да получат, може да се сведе до минимум, но изтичането й не може изцяло да се спре, като се зададе стойност 1 на регистъра RestrictAnonymous. Например, GetAcct на компанията Security Friday заобикаля RestrictAnonymous=1 и ще получи информация за SID и потребителския идентификатор. Идеалното решение при вътрешна (native) Windows 2000/2003 Active Directory, е да се зададе стойност 2 на регистъра RestrictAnonymous.

За да ограничите информацията, достъпна чрез нулевите сесии, щракнете върху следващите номера на статии, за да видите самите статии в Microsoft Knowledge Base:

143474 - Restricting Information Available to Anonymous Logon Users in Windows NT
246261 - How to Use the RestrictAnonymous Registry Value in Windows 2000

За да отстраните дефектите в стойността на регистъра RestrictAnonymous, щракнете върху следващия номер на статия, за да видите самата статия в Microsoft Knowledge Base:

296405 - The RestrictAnonymous Registry Value May Break the Trust to a Windows 2000 Domain

Как да се защитите от отдалечен достъп до регистъра на вашите системи. За да се справите с тази заплаха, трябва да ограничите достъпа до системния регистър и да преразгледате настройките на разрешенията за критичните ключове от регистъра. Преди настройването на регистъра потребителите на Microsoft Windows NT 4.0 трябва да се уверят също така, че е инсталиран сервизен пакет 4 (SP4) или по-нов.

Важна забележка: Тази материал съдържа информация относно извършването на промени в регистъра. Преди да бъде променен регистъра, убедете се, че му е направено резервно копие и че знаете как той да бъде възстановен, ако възникне проблем. Препоръчва се всички промени да бъдат тествани цялостно, преди да бъдат реализирани в работни условия. За информация относно изготвянето на резервно копие, възстановяването и редактирането на регистъра щракнете върху номерата на следващите статии, за да видите съответната статия в Microsoft Knowledge Base:

256986 - Description of the Microsoft Windows Registry
323170 - HOW TO Backup, Edit, and Restore the Registry in Windows NT 4.0
322755 - HOW TO Backup, Edit, and Restore the Registry in Windows 2000

322756 - HOW TO Backup, Edit, and Restore the Registry in Windows XP Windows Server 2003

Ограничете мрежовия достъп. За да ограничите мрежовия достъп до регистъра, изпълнете стъпките, изброени по-долу, за да създадете следния ключ в регистъра:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Control\ SecurePipeServers\winreg
- Описание: REG_SZ
- Стойност: Registry Server

Зададените на този ключ разрешения, свързани със сигурността, определят потребителя или групите, на които е разрешен отдалечен достъп до регистъра. Инсталациите на Windows по подразбиране дефинират този ключ и съдържанието на списъка за контрол на достъпа (Access Control List) така, че да осигурят пълни привилегии на системния администратор и на администраторската група (и на Backup операторите при Windows 2000).

За да влязат в сила, промените в системния регистър изискват рестартиране на машината. За да създадете ключ, който да ограничава достъпа до регистъра:

1. Стартирайте Registry Editor ("regedt32.exe" или "regedit.exe") и идете до следния подключ: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
2. В меню "Edit" щракнете върху "Add Key".
3. Въведете следните стойности: ○ Key Name: SecurePipeServers ○ Class: REG_SZ
4. Идете до следния подключ: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers
5. В меню "Edit" щракнете върху "Add Key".
6. Въведете следните стойности: ○ Key Name: winreg ○ Class: REG_SZ
7. Идете до следния подключ: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ SecurePipeServers\winreg
8. В меню "Edit" щракнете върху "Add Key".
9. Въведете следните стойности: ○ Value Name: Description ○ Data Type: REG_SZ ○ String: Registry Server
10. Идете до следния подключ: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ SecurePipeServers\winreg
11. Изберете "winreg". Щракнете върху "Security", а след това - върху "Permissions". Добавете потребителите и групите, на които трябва да се даде достъп.
12. Излезте от Registry Editor и рестартирайте Microsoft Windows.
13. Ако в по-късен момент пожелаете да се направят промени в списъка на потребителите, които могат да имат достъп до регистъра, повторете стъпки 10-12.

Ограничете разрешения отдалечен достъп. Налагането на строги ограничения по отношение на регистъра може да има неблагоприятни странични ефекти върху свързаните с него услуги като Directory Replicator и услугата за Spooler на мрежовия принтер.

Затова е възможно към разрешенията да се добави определена дефинираност чрез добавяне в списъка за достъп на ключа "winreg" на името на акаунта, под което се стартира услугата, или чрез конфигуриране на Windows така, че да заобикаля ограничението на достъпа до някои ключове чрез изброяването им в стойностите Machine или Users на ключа AllowedPaths:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
SecurePipeServers\winreg\AllowedPaths
Value: Machine
Value Type: REG_MULTI_SZ - Multi string
Default Data: System\CurrentControlSet\Control\ProductOptionsSystem\
CurrentControlSet\Control\Print\PrintersSystem\CurrentControlSet\
Services\EventlogSoftware\Microsoft\WindowsNT\CurrentVersionSystem\
CurrentControlSet\Services\Replicator
Valid Range: (валидна пътечка до място в регистъра)
Description: Разрешава на машините достъп до изброените места в регистъра, ако за съответното място не съществуват изрични ограничения на достъпа.
Value: Users
Value Type: REG_MULTI_SZ - Multi string
Default Data: (няма)
Valid Range: (валидна пътечка до място в регистъра)
Description: Разрешава на машините достъп до изброените места в регистъра, ако за съответното място не съществуват изрични ограничения на достъпа.

В регистъра на Microsoft Windows 2000 и Windows XP:
Value: Machine
Value Type: REG_MULTI_SZ - Multi string
Default Data: System\CurrentControlSet\Control\ProductOptionsSystem\
CurrentControlSet\Control\Print\PrintersSystem\CurrentControlSet\ control\Server
ApplicationSystem\CurrentControlSet\Services\Eventlog\
Software\Microsoft\Windows NT\CurrentVersion
Value: Users (не съществува по подразбиране)

Обикновено съществува интервал от време между момента, в който една уязвимост стане известна и момента, в който за нея започне да се предлага кръпка. Понякога по някакви съображения уязвимостта трябва да остане разрешена. За да намали риска, една организация може да ограничи достъпа чрез защитни стени или маршрутизатори. Допълнителна мярка е създаването на нови правила за IDS (Intrusion Detection System - система за откриване на непозволените прониквания), което ще предупреди организацията или ще задейства изпращането на отговор. Примерни правила за Snort можете да намерите тук.

Как да се защитите от проблеми, свързани с отдалеченото извикване на процедури на вашите системи.

Най-добрият начин, известен досега, е прилагането на съответните кръпки, посочени от MBSA или Windows Update: вижте "Как да определите дали сте уязвими по отношение на проблемите, свързани с отдалеченото извикване на процедури" по-горе. Ако нямате възможност да го направите, съществуват много други начини за забраняване или ограничаване на някои функционални възможности на отдалеченото извикване на процедури, като някои от тях можете да намерите в чудесния обзор на http://www.ntbugtraq.com/dcomrpc.asp.

ВНИМАВАЙТЕ: забраняването или ограничаването на някои функционални възможности на отдалеченото извикване на процедури може да прекрати работата на Windows услуги, които вие използвате, така че трябва винаги да тествате всички модификации първо в неработна среда.

Ако на вашите системи не могат да се поставят кръпки, ще трябва да блокирате портовете, свързани с отдалеченото извикване на процедури при Windows (TCP портове 135, 139, 445 и 593; UDP портове 135, 137, 138 и 445) от периметъра на мрежата. Разбира се най-добрата практика е винаги да се блокират по подразбиране *всички* услуги, които не са необходими, от периметъра на мрежата.

За повече информация:

Статия Q153183 от Microsoft Knowledge Base. How to Restrict Access to NT Registry from a Remote Computer.

Друг източник е Microsoft Security Bulletin Search.

MSDN Library (Потърсете Securing Registry)

Статия 310426 от Microsoft Knowledge Base: HOW TO: Use the Windows XP and Windows Server 2003 Registry Editor

Network access: Remotely accessible registry paths and subpaths

Windows Server 2003 Security Guide

обратно в началото ^

W4 Microsoft SQL Server (MSSQL)

W4.1 Описание

Microsoft SQL Server (MSSQL) съдържа някои сериозни уязвимости, които позволяват на отдалечените нападатели да получават поверителна информация, да променят съдържанието на базите данни, да компрометират SQL сървърите и при някои конфигурации да компрометират сървърните хостове.

MSSQL уязвимостите са добре известни и непрекъснато атакувани. Два появили се неотдавна MSSQL червея - от май 2002 и от януари 2003, използват различни известни пропуски при MSSQL. Хостовете, компрометирани от тези червеи, генерират опасно висок мрежов трафик, докато сканират за други уязвими хостове. Допълнителна информация относно тези червеи можете да намерите съответно

За червея SQLSnake/Spida Worm (май 2002)

- http://isc.incidents.org/analysis.html?id=157
- http://www.eeye.com/html/Research/Advisories/AL20020522.html
- http://www.cert.org/incident_notes/IN-2002-04.html

За червея SQL-Slammer/SQL-Hell/Sapphire Worm (януари 2003)

- http://isc.incidents.org/analysis.html?id=180
- http://www.nextgenss.com/advisories/mssql-udp.txt
- http://www.eeye.com/html/Research/Flash/AL20030125.html

- http://www.cert.org/advisories/CA-2003-04.html

Internet Storm Center редовно регистрира портове 1433 и 1434 (това са портовете по подразбиране на MSSQL сървъра и монитора) като два от най-често сканираните портове.

Програмата на експлойта SQLSnake използва администраторския акаунт по подразбиране, наричан "sa" акаунт, който няма парола. За правилното конфигуриране и защита на всяка система е важно да се гарантира, че всички акаунти в системата са защитени с парола или напълно деактивирани, ако не се използват. Можете да намерите повече информация относно настройването и управлението на паролите на "sa" акаунтите в документацията Microsoft Developer Network в раздел Changing the SQL Server Administrator Login, както и във Verify and Change the System Administrator Password by Using MSDE. Акаунтът "sa" трябва да има сложна, трудна за отгатване парола, дори ако не се използва за стартиране на вашата конкретна реализация на SQL/MSDE.

Програмата на експлойта SQL Slammer се основава на препълване на буфер в SQL Server Resolution Service. Това препълване на буфер се осъществява успешно и по този начин се компрометира сигурността на хоста, когато червеят изпраща умело създадени атакуващи пакети към UDP порта 1434 на уязвимите системи-мишени. Ако на една машина са стартирани SQL услуги, които са зависими от такова препълване на стековия буфер, и тя получи пакети от този вид, това обикновено води до пълно компрометиране на сигурността на сървъра и системата. Най-ефективните средства за защита от този червей са старателното инсталиране на кръпки, старателното прилагане на практики за проактивно конфигуриране на системата и сигурно входно/изходно филтриране на UDP порта 1434 на мрежовите шлюзове.

Microsoft Server 2000 Desktop Engine (MSDE 2000) може да се разглежда като "SQL Server Lite" (олекотен вариант на SQL Server). Много собственици на системи дори не разбират, че MSDE е стартиран на техните системи и че имат инсталирана версия на SQL Server. MSDE 2000 се инсталира като част от следните продукти на Microsoft:

- SQL/MSDE Server 2000 (издания Developer, Standard и Enterprise)
- Visual Studio .NET (издания Architect, Developer и Professional)
- ASP.NET Web Matrix Tool
- Office XP
- Access 2002
- Visual Fox Pro 7.0/8.0

Освен това, има и много други софтуерни пакети, които използват софтуера MSDE 2000. За да видите актуализирания им списък, моля посетете http://www.SQLsecurity.com/forum/applicationslistgridall.aspx. Тъй като този софтуер използва MSDE като главна машина за своята база данни, той страда от същите уязвимости като SQL/MSDE Server. MSDE 2000 може да бъде конфигуриран да подслушва за входящи връзки от клиенти по множество различни начини. Той може да бъде конфигуриран така, че клиентите да могат да използват именувани канали при NetBIOS сесия (TCP порт 139/445) или

сокети при клиенти, свързващи се към TCP порт 1433, или и двете. Независимо от използвания метод, SQL Server и MSDE винаги ще подслушват на UDP порт 1434. Този порт е проектиран като порт за наблюдение. Клиентите ще изпращат към този порт съобщения, за да открият в динамичен режим как да се свържат със сървъра.

Машината на MSDE 2000 връща информация за себе си винаги, когато получи пакета 0x02 с големина един байт на UDP порт 1434. Други пакети с дължина един байт причиняват препълване на буфера, без дори да е необходимо да се автентифицират пред самия сървър. Тези проблеми се изострят допълнително от факта, че атаката е отправена през UDP. Независимо от това дали MSDE 2000 процесът е стартиран в контекста на сигурността на потребител на домейн или от локалния SYSTEM акаунт, успешното използване на тези пробиви в сигурността може да означава тотално компрометиране на системата-мишена.

Тъй като SQL-Slammer използва препълване на буфер в системата-мишена, следването на най-добрите практики на своевременно инсталиране на кръпки и качествено конфигуриране на системата подпомага намаляването на опасността от тази заплаха. Чрез сваляне и използване на защитни средства като Microsoft SQL Critical Update Kit, можете да проверите дали локалните системи са уязвими спрямо този експлойт, да сканирате цели домейни или мрежи за съществуването на уязвими системи и автоматично да обновите засегнатите файлове със SQL Critical Update.

Моля прегледайте доклада и анализа, публикувани на сайта incidents.org, за повече подробности относно червея SQL/MSDE Slammer. Точно тази атака засегна гръбнака на Интернет (Internet Backbone) за няколко часа сутринта на 25 януари 2003.

W4.2 Засягани операционни системи

Всички Microsoft Windows системи с инсталирани Microsoft SQL/MSDE Server 7.0, Microsoft SQL/MSDE Server 2000 или Microsoft SQL/MSDE Server Desktop Engine 2000, както и всички системи, които използват отделно машината на MSDE.

W4.3 CVE/CAN номера

CVE-1999-0999, CVE-2000-0202, CVE-2000-0402, CVE-2000-0485, CVE-2000-0603,CVE-2001-0344, CVE-2001-0879

CAN-2000-0199, CAN-2000-1081, CAN-2000-1082, CAN-2000-1083, CAN-2000-1084,CAN-2000-1085, CAN-2000-1086, CAN-2000-1087, CAN-2000-1088, CAN-2000-1209,CAN-2001-0509, CAN-2001-0542, CAN-2002-0056, CAN-2002-0154, CAN-2002-0186,CAN-2002-0187, CAN-2002-0224, CAN-2002-0624, CAN-2002-0641, CAN-2002-0642,CAN-2002-0643, CAN-2002-0644, CAN-2002-0645, CAN-2002-0649, CAN-2002-0650,CAN-2002-0695, CAN-2002-0721, CAN-2002-0729, CAN-2002-0859, CAN-2002-0982,CAN-2002-1123, CAN-2002-1137, CAN-2002-1138, CAN-2002-1145, CAN-2003-0118

W4.4 Как да определите дали сте уязвими
Microsoft е публикувал серия средства за повишаване на сигурността на сайта http://www.microsoft.com/sql/downloads/securitytools.asp. Комплектът, наречен SQL Critical Update Kit, съдържа полезни инструменти като SQL Scan, SQL Check и SQL Critical Update.

Chip Andrews от sqlsecurity.com е създал инструмент, наречен SQLPingv2.2. Този инструмент изпраща UDP пакет с големина един байт (стойност 0x02) на порт 1434 на единичен хост или на цяла подмрежа. SQL Server-и, подслушващи UDP 1434, ще отговорят като разкрият подробности за системата, като номер на версията, брой на компютрите и т.н. SQLPing се смята за инструмент за сканиране и откриване на заплахи, много подобен на SQL Scan на Microsoft и няма да компрометира допълнително сигурността на вашата система и мрежа. Допълнителни инструменти за сигурност на SQL могат да се намерят на уеб сайта на Chip Andrew SQL/MSDE Security Web site.

W4.5 Как да се защитим
Накратко:

1. Забранете SQL/MSDE Monitor Service на UDP порт 1434.
2. Инсталирайте последния сервизен пакет (service pack) за Microsoft SQL/MSDE Server и/или MSDE 2000.
3. Инсталирайте последната кумулативна кръпка, която е публикувана след последния сервизен пакет.
4. Инсталирайте всички отделни кръпки, които са публикувани след последната кумулативна кръпка.
5. Разрешете влизането с автентификация на SQL Server.
6. Обезопасете сървъра на ниво система и на ниво мрежа.
7. Сведете до минимум привилегиите на услугата MSSQL/MSDEServer и на SQL/MSDE Server Agent.

Подробности:

1. Забранете SQL/MSDE Monitor Service на UDP порт 1434.

   Това може да бъде лесно изпълнено чрез инсталиране и използване на функционалните възможности на SQL Server 2000 Service Pack 3a. Машината на базата данни MSDE 2000 на Microsoft има две уязвимости от типа препълване на буфер, които могат да бъдат използвани от отдалечен нападател без дори да е необходимо той да се автентифицира пред сървъра. Тези проблеми се изострят допълнително от факта, че атаката е отправена през UDP. Независимо от това дали MSDE 2000 процесът е стартиран в контекста на сигурността на потребител на домейн или от акаунт на локалната СИСТЕМА, успешното използване на тези пробиви в сигурността може да означава тотално компрометиране на системата-мишена. MS-SQL/MSDE Slammer изпраща с много висока скорост UDP пакети с дължина 376 байта на порт 1434, като използва произволни мишени. Компрометираните системи незабавно ще започнат да изпращат идентични пакети с дължина 376 байта веднага след заразяването си. Червеят изпраща трафик на произволни IP адреси, включително IP адреси

с множествено разпръскване (multicast), като причинява отказ от обслужване (Denial of Service) на мрежата-мишена. Има сведения, че отделните заразени машини увеличават трафика си до 50 Mb/сек след заразяването си.

2. Приложете последния сервизен пакет за Microsoft SQL/MSDE Server и MSDE 2000.

   Текущата версия на сервизния пакет за Microsoft SQL/MSDE Server е:

   - SQL/MSDE Server 7.0 Service Pack 4
   - MSDE/SQL Server 2000 Service Pack 3a

   За да сте сигурни, че ще бъдете уведомени незабавно за всички бъдещи обновявания, следете Make Your SQL/MSDE Servers Less Vulnerable на Microsoft TechNet. .

3. Приложете последната кумулативна кръпка, която е публикувана след последния сервизен пакет.

   Последната кумулативна кръпка за всички версии на SQL/MSDE/MSDE Server можете да намерите на MS02-061 Elevation of Privilege in SQL/MSDE Server Web Tasks (Q316333/Q327068).

   За да сте сигурни, че ще бъдете уведомени незабавно за всички бъдещи обновявания, проверявайте коя е последната кумулативна кръпка за Microsoft SQL/MSDE Server на:

   - Microsoft SQL/MSDE Server 7.0
   - Microsoft SQL Server 2000
   - MSDE Server Desktop Engine 2000 (MSDE 2000)

4. Приложете всички отделни кръпки, които са публикувани след последната кумулативна кръпка.

   Засега няма отделна кръпка след публикуването на MS02-061 Elevation of Privilege in SQL/MSDE Server Web Tasks (Q316333/Q327068). Но за да сте сигурни, че ще бъдете уведомени незабавно за всички бъдещи обновявания, проверявайте за нови публикувани отделни кръпки на:

   - Microsoft SQL/MSDE Server 7.0
   - Microsoft SQL Server 2000
   - MSDE Server Desktop Engine 2000 (MSDE 2000)

5. Разрешете влизането с автентификация на SQL Server.

   Обикновено влизането с автентификация на SQL Server не е разрешено. Може да го разрешите от Enterprise Manager (Server properties; етикет Security).

6. Обезопасете сървъра на ниво система и на ниво мрежа.

Една от най-често атакуваните MSSQL/MSDE уязвимости е свързана с факта, че администраторският акаунт (известен като "sa") е инсталиран по подразбиране без парола. Ако вашия SQL/MSDE "sa" акаунт не е защитен с парола, вие в действителност не сте обезопасени и можете да бъдете засегнати от червеи и други експлойти. Следователно, трябва да следвате препоръките в раздела "System Administrator (SA) Login" на SQL/MSDE Server Books Online, за да си гарантирате, че вграденият "sa" акаунт има силна парола дори ако вашия SQL/MSDE сървър не използва този акаунт. В Microsoft Developer's Network има документация върху Changing the SQL Server Administrator Login и относно Verify and Change the System Administrator Password by Using MSDE.

7. Сведете до минимум привилегиите на услугата MSSQL/MSDEServer и на SQL/MSDE Server Agent.

   Стартирайте услугата MSSQL/MSDEServer и SQL/MSDE Server Agent от валиден акаунт на домейна с минимални привилегии, а не като администратор на домейна, нито от SYSTEM (за NT), нито от LocalSystem (за 2000 или XP) акаунт. Една компрометирана услуга, стартирана с локални или домейн привилегии, би предоставила на нападателя пълен контрол върху вашата машина и/или вашата мрежа.

   a. Разрешете Windows NT автентификацията, разрешете проследяването на успешните и неуспешни влизания в системата, а след това спрете и рестартирайте услугата MSSQL/MSDEServer. Ако е възможно конфигурирайте вашите клиенти така, че да използват NT автентификация.

   b. Филтрирането на пакетите трябва да бъде извършено на границите на мрежата така, че да се забранят именно неразрешените входящи или изходящи връзки към специфичните MSSQL услуги. Входното и изходното филтриране на TCP/UDP портове 1433 и 1434 може да предотврати сканирането или заразяването на уязвими Microsoft SQL/MSDE сървъри от страна на вътрешните и външни нападатели от вашата мрежа или други мрежи, на които не е изрично разрешено да осигуряват публични SQL/MSDE услуги.

   c. Ако TCP/UDP портове 1433 и 1434 трябва да бъдат разрешени на вашите Интернет шлюзове, разрешете и настройте входно/изходното филтриране, за да предотвратите злонамереното използване на тези портове.

Допълнителна информация за обезопасяването на Microsoft SQL/MSDE Server може да бъде намерена на

- Microsoft SQL/MSDE Server 7.0 Security
- Microsoft SQL/MSDE Server 2000 Security

обратно в началото ^

W5 Автентификацията при Windows

W5.1 Описание

Паролите, състоящи се от отделна дума или цяла фраза, и кодовете за сигурност се използват фактически при всяко взаимодействие между потребителите и информационните системи. Повечето форми на автентификация на потребителя както и на защита на файлове и данни се основават на въвеждани от потребителя пароли. Тъй като правилно автентифицираният достъп често не се

регистрира и дори, ако се регистрира, вероятно няма да предизвика съмнение, една компрометирана парола представлява възможност за изследване на съответната система отвътре, като това изследване ще остане практически неразкрито. Един нападател ще има пълен достъп до всички ресурси, които са на разположение на съответния потребител, и ще има значително по-добри възможности да получи достъп до други акаунти, до околните машини и дори може би администраторски привилегии. Въпреки тази опасност акаунтите със зле създадени или празни пароли все още са твърде разпространени, а организациите с правилна политика по отношение на паролите се срещат засега твърде рядко.

Най-често срещаните уязвимости по отношение на паролите са:

- Потребителски акаунти със слаби или несъществуващи пароли.
- Независимо от силата на паролата, потребителите не я пазят в тайна.
- Операционната система или допълнителният софтуер създават административни акаунти със слаби или несъществуващи пароли.
- Хеш алгоритмите за паролите са известни и често хешовете се съхраняват така, че всеки може да ги види. Най-добрата и най-подходящата защита срещу тези уязвимости е политиката на силни пароли, която включва цялостни инструкции за създаване на добри навици по отношение на паролите и проактивна проверка за целостта на паролите.

Microsoft Windows не съхранява и не предава паролите в явен текст, а използва хешване на паролите за автентификация. Хешът представлява резултат с фиксиран размер, получен след прилагане на математическа функция (хеш алгоритъм) към произволно количество данни (известни също като message digest). Съществуват три Windows алгоритми за автентификация: LM (по-малко сигурен, по-съвместим); NTLM и NTLMv2 (по-сигурни и по-малко съвместими). Въпреки че повечето Windows обкръжения в момента не се нуждаят от поддръжка на LAN Manager (LM), Microsoft Windows съхранява по подразбиране наследени хешове за LM пароли (известни също като LANMAN хешове) на Windows NT, 2000 и XP системи (но не и на Windows 2003). Тъй като LM използва много по-слаба кодираща схема, отколкото повечето използвани понастоящем от Microsoft алгоритми (NTLM и NTLMv2), LM паролите могат да бъдат разбити за много кратък период от време. Дори пароли, които другаде биха били считани за силни, могат да бъдат открити чрез груба сила (brute force) за около седмица при използвания понастоящем хардуер.

http://msdn.miscrosoft.com/library/default.asp?url=/library/en-us/security/Security/h_gly.asp

Слабостта на LM хешовете произтича от следното:

- Паролите се отрязват до дължина 14 символа.
- Паролите се допълват с интервали, за да получат дължина 14 символа.
- Паролите се конвертират до символи от горния регистър.
- Паролите се разделят на две части от по седем символа.

Този хеш процес означава, че нападателят трябва само да се справи с тривиалната задача за откриване на две пароли с дължина седем символа, написани на горния регистър, за да получи автентифициран достъп до вашата система. Тъй като трудността при кракване на хешове нараства геометрично с

увеличаване дължината на хеша, всеки низ с дължина седем символа е поне с един порядък по-лесен за атакуване чрез груба сила, отколкото един комбиниран низ с дължина 14 символа. Тъй като всички низове се състоят точно от седем символа (включително и интервалите) и са написани изцяло на горния регистър, една речникова атака също се улеснява. Следователно методът на LM хешовете изцяло подронва политиката на създаване на добри пароли.

Друга опасност, освен риска от наличието на наследени LM хешове, съхранявани в SAM, представлява фактът, че автентификационният процес чрез LAN Manager често е разрешен по подразбиране на клиентите и приеман от сървърите. Като резултат, Windows машините, способни да използват силни хеш алгоритми, изпращат вместо тях слаби LM хешове по мрежата, като по този начин правят Windows автентификацията уязвима за подслушване чрез подслушване на пакети, и следователно улеснява усилията на нападателя за придобиване и кракване на потребителски пароли.

W5.2 Засягани операционни системи
Всички Microsoft Windows операционни системи.

W5.3 CVE/CAN номера
CVE-2000-0222

CAN-1999-0504, CAN-1999-0505, CAN-1999-0506

W5.4 Как да определите дали сте уязвими
Макар че съществуват очевидни симптоми на общата слабост на паролите, като съществуването на активни акаунти за потребители, които са напуснали организацията или за услуги, които не се използват, единственият начин да се уверите, че всяка отделна парола е силна, е да проверите всички пароли чрез същите средства за кракване на пароли, които използват нападателите.

Моля отбележете: Никога не стартирайте скенер за пароли, дори на системи, на които имате административен достъп, без изрично и за предпочитане писмено разрешение от вашия началник. Администратори, които са имали най-добри намерения, бяха уволнени затова, че са стартирали средства за кракване на пароли без да имат пълномощия за това.

Някои от най-добрите средства за кракване са: LC4 (l0phtcrack version 4) и John the Ripper

В зависимост от локално съхранявания хеш на LAN Manager:

- Ако работите с инсталация по подразбиране на NT, 2000 или XP, вие сте уязвими, тъй като хешовете на LAN Manager се съхраняват локално по подразбиране.
- Ако във вашето обкръжение има стари операционни системи, които изискват LM автентификация, за да комуникират със сървърите, то вие сте уязвими,

W5.5 Как да се защитим
Най-добрата и най-подходящата защита срещу слаби пароли е силната политика, която включва цялостни инструкции за добиване на добри навици по отношение на паролите и проактивна проверка за целостта на паролите.

1. **Уверете се, че всички пароли са силни.** При наличие на достатъчно хардуерни средства и достатъчно време, всяка парола може да бъде кракната чрез груба сила. Но съществуват по-прости и по-успешни начини да откриете паролите без такива разходи. Кракерите на пароли използват методи, известни като речникови атаки. Тъй като методите за кодиране са известни, програмите за кракване просто сравняват кодираната форма на една парола с кодираната форма на думите в речника (на много езици), със собствените имена и с пермутации от двете. Следователно една парола, чиито корен по някакъв начин прилича на дума от речника, е силно податлива на речникова атака. Много организации инструктират потребителите да създават парола като включват в тях комбинации от буквено-цифрени и специални символи и потребителите много често спазват тези инструкции, като вземат една дума ("password") и преобразуват буквите в цифри или специални символи ("pa$$w0rd"). Такива пермутации не могат да осигурят защита срещу речникова атака: при кракване "pa$$w0rd" вероятно ще бъде разпозната като "password".
   Следователно една парола не може да се основава на дума или собствено име. Политиката на силни пароли трябва да подтиква потребителите да създават пароли на основата на нещо по-случайно, като фраза или заглавие на книга или песен. Чрез съставяне на по-дълъг низ (като се вземе първата буква от всяка дума или всяка дума се замени със специален символ, или се премахнат всички гласни и т.н.) потребителите могат да създадат достатъчно дълги низове, които комбинират буквено-цифрени и специални символи по начин, който силно ще затрудни кракването чрез речникови атаки. И ако низът е лесен за запомняне, то паролата също ще се помни лесно.
   След като на потребителите бъдат дадени подходящи инструкции за създаване на добри пароли, трябва да се създадат и процедури, които да гарантират спазването на тези инструкции. Най-добрият начин за изпълнение на тази задача е валидирането на паролите при смяната им от потребителя чрез използване на Passfilt (NT4).
   Windows 2000, XP, 2003 притежават мощни средства за налагане на спазването на политиката по отношение на паролите. За да видите използваната по настоящем политика по отношение на паролите при повечето Windows системи, следвайте следните стъпки (Start - Programs - Administrative Tools - Local Security Policy – изберете Account Policies - Password Policy). Local Security Policy има следните настройки: :

- **Паролата трябва да съответства на изискванията за сложност (Password must meet complexity requirements.)** Определя дали паролите трябва да съответстват на изискванията за сложност. Изискванията за сложност са задължителни при промяна или създаване на пароли. Ако тази политика се спазва, паролите трябва да съответстват на следните минимални изисквания:
  - Да не съдържат цялото име на потребителския акаунт или част от него
  - Да бъдат с дължина поне шест символа

- Дасъдържат символи, принадлежащи на три от следните четири категории:
    - Главни латински букви (A до Z)
    - Малки латински букви (a до z)
    - Основните 10 цифри (0 до 9)
    - Други символи, различни от буквено-цифрените (например, !, $, #, %)

- **Задължително съхраняване на историята на паролите (Enforce password history)** (диапазон: 0-24): Определя броя на уникалните нови пароли, които трябва да се асоциират с един потребителски акаунт преди да се разреши повторното използване на стара парола. Стойността трябва да бъде между 0 и 24 пароли. Даването на стойност "0 запомнени пароли" на този параметър позволява незабавното използване на стара парола; Стойност "24 запомнени пароли" изисква 24 смени на паролата преди да е възможно да се използва началната парола. Тази политика позволява на администраторите да повишат сигурността, като направят невъзможно непрекъснато използване на едни и същи стари пароли. За да поддържате ефективността на историята на паролите, не разрешавайте смяна на паролите веднага след като конфигурирате минималния срок на годност на паролите.

- **Максимален срок на годност на паролите (Maximum password age)** (обхват: 0-999 дни): Определя периода от време (в дни), през който една парола може да бъде използвана, преди системата да поиска от потребителя да я смени. Можете да настроите паролите да изтичат след определен брой дни между 1 и 999 или да направите паролите вечни като зададете за броя дни стойност, равна на 0.

- **Минимален срок на годност на паролите (Minimum password age)** (обхват: 0-999 дни): Определя периода от време (в дни), през който една парола може да бъде използвана, преди потребителят да може да я смени. Можете да посочите стойност между 1 и 999 дни или да позволите незабавни промени, като зададете за броя дни стойност равна на 0. Минималният срок на годност на паролите трябва да бъде по-малък от максималния. Задайте на минималния срок на годност на паролите стойност, по-голяма от 0, ако искате параметърът "Enforce password history" да бъде ефективен. Ако минималният срок на годност на паролите не е зададен, потребителите могат да променят непрекъснато паролите си, докато не стигнат до любимата си стара парола. Настройките по подразбиране не съвпадат с тази препоръка, така че администраторът може да зададе парола за даден потребител и след това да изисква от него да смени тази дефинирана от администратора парола при влизане в системата. Ако "password history" има стойност 0, на потребителя няма да му се наложи да избира нова парола. По тази причина "password history" има стойност 1 по подразбиране.

- **Минимална дължина на паролите (Minimum password length)** (диапазон: 0-14 символа): Определя най-малкия брой символи, който може да съдържа паролата за един потребителски акаунт. Можете да зададете стойност между 1 и 14 символа или да укажете, че не е необходима парола, като зададете стойност 0. Минималната дължина на паролите трябва да съответства на корпоративната политика за сигурност (иначе казано се препоръчва стойността да бъде 8 и повече символа; National Security Agency (NSA) препоръчва 12 символа).

- **Съхраняване на пароли чрез използване на обратимо кодиране за всички потребители в домейна (Store password using reversible encryption for all users in the domain)** Определя дали съхраняването на пароли при Windows 2000, 2003 и XP Professional използва обратимо кодиране. Тази политика осигурява поддръжка на приложения, използващи протоколи, които изискват познаване на паролата на потребителя с цел автентификация. Съхраняването на пароли чрез използване на обратимо кодиране е еквивалентно на съхраняване на версиите на паролите в явен текст. По тази причина тази настройка не бива да бъде разрешена, освен ако изискванията на приложението са по-важни от необходимостта от защита на информацията за паролите.

Един подход, който може да бъда използван за автоматично създаване и присвояване на сложни пароли на потребителските акаунти, е следният: стартирайте следната команда (от командния ред на Windows NT4, 2000, XP, 2003):

Net user username /random

Изпълнението на тази команда ще присвои произволни сложни (но винаги с дължина 8 символа) пароли на даден акаунт и ще изобрази тази парола на екрана на конзолата. Този метод е обикновено по-подходящ за присвояване на пароли на акаунти на услуги, а не на действителни потребители.

Най-добрият начин за проверка на качеството на паролите е стартирането на програми за кракване на пароли в самостоятелен режим като част от рутинното сканиране.

Важна забележка: Никога не стартирайте скенер за пароли, дори на системи, на които имате административен достъп, без изрично и за предпочитане писмено разрешение от вашия началник. Администратори, които са имали най-добри намерения, бяха уволнени затова, че са стартирали средства за кракване на пароли без да имат пълномощия за това.

След като сте получили пълномощия да стартирате програми за кракване на вашата система, го правете редовно от защитена машина. Потребители, чиито пароли са кракнати, трябва да бъдат уведомявани дискретно, като им се дават инструкции как да изберат добра парола. Администраторите и ръководството трябва да разработят тези процедури съвместно, така че ръководството да може да оказва помощ, когато потребителите не желаят да спазват тези инструкции.

Друг начин за защита срещу липса на пароли или слаби пароли е използването

на алтернативна форма за автентификация като маркери (tokens) за автоматично създаване на пароли или биометрия.

1. **Защитете силните пароли.** Дори ако паролите сами по себе си са силни, акаунтите могат да бъдат компрометирани, ако потребителите не пазят паролите си в тайна. Добрата политика трябва да включва инструкции, според които потребителят никога не бива да издава своята парола на друго лице, да не я записва там, където би могла да бъде прочетена от други, и да обезопасява по подходящ начин всички файлове, в които паролата се съхранява с цел автоматична автентификация (паролите се защитават по-лесно, ако този метод се използва само при абсолютна необходимост). Поставянето на срок на годност на паролите трябва да бъде задължително, така че всички пароли, които успеят да се промъкнат през тези правила, да бъдат уязвими само за кратък период от време, като не трябва да се използват повторно стари пароли. Убедете се, че потребителите са предупредени и имат възможност да променят своята парола, преди тя да изтече. Когато се сблъскат неочаквано със съобщението "Your password has expired and must be changed," потребителите проявяват склонност за избор на слаба парола.

2. **Контролирайте стриктно акаунтите.**
    - Всички акаунти на услуги или администраторски акаунти, които не се използват, трябва да бъдат забранени или премахнати. Всички акаунти на услуги или администраторски акаунти, които се използват, трябва да получат нови и силни пароли.
    - Проверете акаунтите на вашите системи и създайте главен списък (master list). Не забравяйте да проверявате паролите на системи като маршрутизатори и свързани към Интернет дигитални принтери, копиращи машини и контролери на принтерите.
    - Разработете процедури за добавяне на оторизирани акаунти към списъка и за премахване на акаунти, когато те не се използват повече.
    - Проверявайте редовно списъка, за да се убедите, че не са добавени нови акаунти, и че неизползваните акаунти са премахнати.
    - Използвайте строги процедури за изтриване на акаунти, при напускане на служители или партньори, или когато акаунтите не са необходими повече.

3. **Поддържайте корпоративна политика на силни пароли.** Освен контрола на ниво услуги в операционната система или мрежата, съществуват много други обширни възможности, които подпомагат провеждането на добра политика по отношение на паролите. На сайта SANS Security Policy Project можете да намерите много примерни начини за управление на паролите, насоки за разработка на политика, основни сведения за сигурността на паролите и линкове към много уеб сайтове, посветени на политиката, свързана със сигурността (която включва и информация по отношение на паролите)

4. **Забранете LM автентификацията през мрежата.** Най-добрият заместител при Windows на автентификацията чрез LAN Manager е NT LAN Manager

версия 2 (NTLMv2). Методите challenge/response при NTLMv2 преодоляват много слабости в LM, като използват силно кодиране и подобрени механизми за автентификация и сигурност на сесиите. Ключът от регистъра, който контролира тази възможност при Windows NT и 2000, е:

Раздел: HKEY_LOCAL_MACHINE
Ключ: System\CurrentControlSet\Control\LSA
Стойност: LMCompatibilityLevel
Тип на стойността: REG_DWORD - Number
Валиден диапазон: 0-5
Стойност по подразбиране: 0

Описание: Този параметър определя типа на използваната автентификация.

0 – Изпращане на LM и NTLM отговори; никога да не се използва NTLMv2 за сигурност на сесията
1 – Използване на NTLMv2 за сигурност на сесията, ако това е уговорено
2 – Изпращане само на NTLM автентификация
3 - Изпращане само на NTLMv2 автентификация
4 - DC отказва LM автентификация
5 - DC отказва LM и NTLM автентификация (приема само NTLMv2)

При Windows 2000, 2003 и XP същите функционални възможности могат да бъдат реализирани чрез конфигуриране на настройката на нивото на автентификация на LAN Manager (Windows 2000) или Network security: Ниво на автентификация на LAN Manager (Windows XP, 2003) (Start - Programs - Administrative Tools - Local Security Policy - Local Policies - Security Options).

Ако всичките ви системи са Windows NT SP4 или по-нови, можете да зададете стойност 3 за всички клиенти и 5 за всички контролери на домейни, за да предотвратите всяко предаване на LM хешове по мрежата. Но старите системи (като Windows 95/98) няма да използват NTLMv2 с Microsoft Network Client по подразбиране. За да използвате възможността NTLMv2, инсталирайте Directory Services Client. След това името на стойността в регистъра ще бъде "LMCompatibility," а разрешените стойности са 0 или 3.

Ако не можете да накарате вашите клиенти със стар софтуер да използват NTLMv2, можете да получите известно подобрение на LM хеша чрез използване на NTLM (NT Lan Manager, версия 1) на контролера на домейна (задайте на LMCompatibilityLevel стойност 4 или ако използвате средство за политика по отношение на локалната сигурност (Local Security Policy) задайте за нивото на автентификация чрез LAN Manager стойност: Send NTLMv2 Response only\Refuse LM). Но най-сигурната възможност по отношение на старите системи е да преминете към по-нови операционни платформи, тъй като старите операционни системи не позволяват поддържането на това минимално ниво на сигурност.

5. **Предотвратете съхраняването на LM хеша.** Голям проблем при обикновеното отстраняване на LM хешовете, които са преминали през мрежата, е че тези хешове са създадени и съхранявани в SAM или активната директория (Active Directory). Microsoft е създал механизъм за изключване на създаването на всички хешове, но само при Windows 2000, 2003 и XP. При Windows 2000 системи (SP2 или по-нови), тази функция се контролира от

следния ключ от регистъра:

Раздел: HKEY_LOCAL_MACHINE
Ключ: System\CurrentControlSet\Control\LSA\NoLMHash

Ако този ключ е създаден на контролера на домейна на Windows 2000, LanMan хешовете няма да се създават и съхраняват повече в активната директория (Active Directory).

При Windows XP и 2003 същите функционални възможности могат да бъдат реализирани чрез разрешаването на следната настройка в Network security: Do not store LAN Manager hash value on next password change (не съхранявайте стойността на LAN Manager хеша при следващата смяна на паролата) (Start - Programs - Administrative Tools - Local Security Policy - Local Policies - Security Options).

След като тези промени бъдат направени, системата трябва да бъде рестартирана, за да могат те да влязат в сила.

> **Важна забележка:** По този начин ние предотвратяваме само създаването на нови LM хешове. Съществуващите LM хешове се премахват поотделно следващия път, когато потребителят смени паролата си.

6. **Предотвратяване на копирането на хешовете на паролите и базата данни на SAM.** Средствата за кракване на пароли, упоменати в този раздел, получават достъп до хешовете на паролите чрез:
   - Подслушване на пароли по мрежата. Мерки за противодействие: 1. Използване на превключваеми (switched) мрежи; 2. Откриване и отстраняване на мрежови карти в случаен режим (те могат да бъдат открити чрез повечето платени средства за оценка, както и чрез безплатни средства като ethereal).
   - Копиране на SAM файла (намиращ се в папката %SystemRoot%\System32\Config\ обикновено на C:\Winnt\System32\Config\ - за Windows NT4 и 2000 или C:\Windows\System32\Config\ - за Windows XP и 2003). Този файл обикновено е заключен от Windows OS и може да бъде копиран само, когато на системата се зарежда алтернативна операционна система. SAM файлът може да бъде получен също така и при възстановяване на негово резервно копие или на System State (Windows 2000, 2003, XP). SAM файлът се намира също така и на NT4 Repair Disk.

   Мерки за противодействие: Ограничаване и наблюдаване на физическия достъп до компютърните системи (специално за контролерите на домейни), носителите с резервни копия и Repair Disk.

   Следните статии от Microsoft съдържат полезна информация:

   - How to Disable LM Authentication on Windows NT [Q147706] обяснява в подробности необходимите промени в регистъра на Windows 9x и Windows NT/2000.

- MS03-034 : Flaw in NetBIOS Could Lead to Information Disclosure (824105)
- LMCompatibilityLevel and Its Effects [Q175641] обяснява проблемите, свързани с този параметър при съвместна работа.
- How to Enable NTLMv2 Authentication for Windows 95/98/2000/NT [Q239869] обяснява как да използваме Directory Services Client на Windows 2000 за Windows 95/98 с цел да преодолеем ограничението на съвместимостта за NTLMv2.

New Registry Key to Remove LM Hashes from Active Directory and Security Account Manager

обратно в началото ^

W6 Уеб браузъри

W6.1 Описание

Браузърът е средството, чрез което компютърните потребители на системи с Microsoft Windows получават достъп до Интернет. Най-разпространеният уеб баузър е Microsoft Internet Explorer (IE), който е инсталиран по подразбиране на платформите Microsoft Windows. Други уеб браузъри са Mozilla, Firefox, Netscape и Opera. Последната версия на IE е 6, и именно нея ще обсъдим тук. Обсъжданите тук уязвимости важат също за Mozilla версии 1.4 - 1.7.1, Firefox версия 0.9.x, Netscape версия 7.x, и Opera версия 7.x.

Проблемите могат да се разделят на 6 категории:

1. Голям брой уязвимости през последните няколко години в сравнение с останалите браузъри – 153 уязвимости в IE от април 2001г. досега според Security Focus Archive.
2. По-дълго време за закърпване на известните уязвимости в IE – Потребителите чакат повече от 6 месеца от момента, в който е открита уязвимостта до пускането на кръпката от Microsoft.
3. Active X и Active Scripting на IE представляват уязвимости; особено използването на ActiveX даваше в миналото възможност за заобикаляне на ограниченията, свързани със сигурността на операционната система, и за компрометиране на хост машините.
4. Голям брой незакърпени уязвимости – 34, според http://umbrella.name/originalvuln/msie/
5. Spyware/Adware уязвимости – Те касаят всички браузъри, но IE е по-уязвим от останалите.
6. Интегриране на браузъра IE в кернела на операционната система, което я прави по-уязвима при експлоатация.

При другите браузъри също е имало проблеми, но никога до такава степен, както при IE. Един злонамерен уеб дизайнер може да създава уеб страници, които да използват злонамерено уязвимостите на Internet Explorer при обикновено прелистване на уеб страници. Отличен пример за това е уязвимостта "Download.Ject". Тя е известна от доста месеци и използва уязвимостите на Active X. Дори след като на 8 юни 2004 беше публикуван експлойт, кръпка за IE беше пусната чак през юли 2004 г. Поради комбинацията от ActiveX, работата със скриптове и интегрирането с операционната система Windows, Internet Explorer е по-уязвим към атаки от повечето други браузъри. Последствията могат да включват разкриване на бисквитки (cookies), локални файлове или данни,

изпълнение на локални програми, сваляне и изпълняване на произволен код или пълно превземане на уязвимата система.

W6.2 Засягани операционни системи

тези уязвимости съществуват при системи с Microsoft Windows, работещи с произволна версия на този браузър. Важно е да се отбележи, че IE се инсталира при инсталирането на голяма част от софтуера на Microsoft и следователно обикновено се намира на всички Windows системи, дори ако потребителят не е пожелал да го инсталира или използва. Всички останали браузъри се инсталират по лична преценка на потребителя и той решава дали браузърът да се използва от другите приложения.

W6.3 Уязвимости на браузърите, с благосклонното съгласие на Secunia

A. Internet Explorer:

2004 - 15 документа, свързани със сигурността (до 30юли 2004)

1. Microsoft Internet Explorer Multiple Vulnerabilities
2. Internet Explorer Frame Injection Vulnerability
3. Internet Explorer File Download Error Message Denial of Service Weakness
4. Internet Explorer Security Zone Bypass and Address Bar Spoofing Vulnerability
5. Internet Explorer Local Resource Access and Cross-Zone Scripting Vulnerabilities
6. Microsoft Internet Explorer and Outlook URL Obfuscation Issue
7. Windows Explorer / Internet Explorer Long Share Name Buffer Overflow
8. Microsoft Outlook Express MHTML URL Processing Vulnerability
9. Internet Explorer/Outlook Express Restricted Zone Status Bar Spoofing
10. Multiple Browser Cookie Path Directory Traversal Vulnerability
11. Internet Explorer Cross Frame Scripting Restriction Bypass
12. Internet Explorer File Identification Variant
13. Internet Explorer Travel Log Arbitrary Script Execution Vulnerability
14. Internet Explorer File Download Extension Spoofing
15. Internet Explorer showHelp() Restriction Bypass Vulnerability

B. Уязвимости на Mozilla

2004 - 7 документа на Secunia, свързани със сигурността

1. Mozilla Fails to Restrict Access to "shell:"
2. Mozilla XPInstall Dialog Box Security Issue
3. Multiple Browsers Frame Injection Vulnerability
4. Mozilla Browser Address Bar Spoofing Weakness
5. Mozilla / NSS S/MIME Implementation Vulnerability
6. Multiple Browser Cookie Path Directory Traversal Vulnerability
7. Mozilla Cross-Site Scripting Vulnerability

D. Уязвимости на Netscape

2004 - 2 документа на Secunia, свързани със сигурността

1. Mozilla Fails to Restrict Access to "shell:"
2. Multiple Browsers Frame Injection Vulnerability

E. Уязвимости на Opera

2004 - 8 документа на Secunia, свързани със сигурността

1. Opera Browser Address Bar Spoofing Vulnerability
2. Multiple Browsers Frame Injection Vulnerability
3. Opera Address Bar Spoofing Security Issue
4. Opera Browser Favicon Displaying Address Bar Spoofing Vulnerability
5. Multiple Browsers Telnet URI Handler File Manipulation Vulnerability
6. Opera Browser Address Bar Spoofing Vulnerability
7. Multiple Browser Cookie Path Directory Traversal Vulnerability
8. Opera Browser File Download Extension Spoofing

W6.4 Идентифициране на уязвимостите на браузърите и защита от тях

Ако използвате Internet Explorer на вашата система, в момента не съществува лесен начин да разберете дали сте уязвими, поради големия брой незакърпени уязвимости, които съществуват. Независимо от това, трябва да посещавате редовно сайта Windows Update, за да си гарантирате, че IE е защитен от уязвимости, за които има кръпки. Потребителите, които се интересуват от допълнителна защита срещу уязвимостите в браузъра, трябва да разгледат следните възможности:

a. Да помислят за използването на алтернативни браузъри, които не използват ActiveX. Тъй като уеб сайтът Windows Update, който използва ActiveX, ще бъде злополучно засегнат от този подход, опитайте се вместо него да използвате възможността "Automatic Updates". Другите възможности за обновяване включват използването на Shavlik's HFNetChkPro™ или Microsoft Baseline Security Analyzer (MBSA) за изпълнение на същата задача. Освен това, он-лайн средствата за анализ на Internet Explorer, като Qualys Browser Check могат да бъдат много ценни при оценка на състоянието на сигурността на IE на вашите системи.
b. Ако възможността, описана в подточка а. се окаже трудна за реализиране в корпоративни обкръжения поради използването на ActiveX в интранет, помислете за използването на Internet Explorer в интранет и на алтернативен браузър за Интернет достъп.
c. Ако използването на алтернативен браузър не може да се осъществи, помислете за цялостна забрана на ActiveX, с изключение на вътрешните ActiveX аплети, които може би са предварително инсталирани на машината. Microsoft предоставя начин за спиране работата на една ActiveX контрола в Internet Explorer.

Другите браузъри не притежават автоматизираните средства, с които разполага Internet Explorer. Ако използвате Mozilla/Firefox, Netscape или Opera, трябва да проверявате на съответните им уеб сайтове (http://www.mozilla.org, http://www.netscape.com, http://www.opera.com), или http://umbrella.name/index.html) за открити уязвимости и средства за поправката им (fixes).

W6.5 как да обезопасите Internet Explorer

За да конфигурирате настройките за сигурност на Internet Explorer:

1. Изберете Internet Options от меню Tools.
2. Изберете Security tab и след това щракнете върху Custom Level for the Internet zone.

Повечето от пропуските в IE се използват чрез Active Scripting или ActiveX контроли.

3. В Scripting изберете Disable за "Allow paste operations via script", за да предотвратите непозволен достъп до съдържанието чрез временната памет (clipboard).

   Забележка: Забраняването на Active Scripting може да причини проблеми при работата на някои уеб сайтове.

ActiveX контролите не са толкова популярни, но са потенциално по-опасни, тъй като позволяват по-голям достъп до системата.

4. Изберете Disable за "Download signed ActiveX Controls".
5. Изберете Disable за "Download unsigned ActiveX Controls".
6. Изберете също Disable за "Initialize and script ActiveX Controls not marked as safe".

Java аплетите обикновено имат повече възможности от скриптовете.

7. От Microsoft VM изберете "High safety for Java permissions" за да използвате подходящо сандъче с пясък (sandbox) за Java аплетите и да предотвратите достъп с използване на привилегии до вашата система.
8. От Miscellaneous изберете "Disable for Access to data sources across domains" за да избегнете атаки от типа Cross-site scripting.

Моля, уверете се, че няма непроверени сайтове в зоните Trusted sites или Local intranet, тъй като тези зони имат по-слаби настройки за сигурност в сравнение с останалите.

обратно в началото ^

W7 Приложения за споделяне на файлове

W7.1 Описание

програмите за споделяне на файлове от типа "равен с равен" (P2P) са широко използвани от бързо растящ кръг от потребители. Тези приложения често се използват за сваляне и разпространение на различни видове данни (да споменем няколко примера: музика, видео, графична информация, текст, сорсов код, и собствена информация). P2P приложенията се използват по множество легитимни начини, включително за разпространение на изпълними програми с отворен код/GPL, ISO имиджи на Linux дистрибуции за начално зареждане, творения на независими художници и дори комерсиални медии като трайлери на филми или представяния на игри. Но понякога данните често са съмнителни или защитени от авторското право. След юридическите неприятности, през които премина Napster, по-голямата част от тези P2P програми сега работят през разпределена мрежа от клиенти, като споделят директории с файлове или цели твърди дискове с данни. Потребителите могат да въвеждат параметри за претърсване на клиентския софтуер, след което се отварят един или повече канали за комуникация между участниците, тъй като клиентският софтуер установява контакт с другите потребители на мрежата, за да открие желания файл. Клиентите участват в комуникацията чрез сваляне на файлове от други потребители, чрез разрешаване на достъп до техните данни за останалите и при някои модели чрез функциониране като супервъзли (supernodes), които могат да

координират претърсването на множество потребители.

Комуникацията Peer to Peer се състои в получаване на заявки, отговори и прехвърляне на файлове. Един участник може едновременно да извършва няколко сваляния (downloads), като същевременно обслужва множество качвания (uploads). Претърсванията за определено съдържание могат да използват почти всеки текстов низ, който потребителят може да измисли. Повечето от тези програми използват понастоящем портове по подразбиране, но могат ръчно или автоматично да бъдат настроени така, че да използват други портове, ако това е необходимо за заобикалянето на детектиращи програми, защитни стени или изходни филтри. Изглежда тенденцията е към използването на http-обвивки (wrappers) за по-лесно заобикаляне на корпоративните ограничения. Многопосочната природа на търсенето и прехвърлянето на файлове могат да предизвикат значителен трафик при големите LAN и да задръстят напълно линковете на WAN.

При използването на P2P софтуер съществуват множество уязвимости. Те могат да бъдат разделени в три категории. Технически уязвимости са тези, които могат да бъдат използвани отдалечено. Социални уязвимости са тези, които се използват чрез промяна или маскиране на двоичното съдържание, което искат да свалят останалите потребители. И накрая, юридически уязвимости са тези, които могат да се получат поради нарушаване на авторското право или разпространение на осъдителни материали.

Както споменахме по-горе, технически уязвимости са тези, които могат да бъдат използвани отдалечено и могат да бъдат резултат от просто сваляне, инсталиране и стартиране на една от тези програми от страна на потребителите. Всички изброени по-долу CVE and CAN номера се отнасят до технически уязвимости. Те обхващат диапазона от отказ от обслужване до достъп до произволен файл и на тях трябва да се гледа много сериозно. Проблемите, свързани със защита на личната информация и конфиденциалността, не са отразени в базата данни на CVE, но те могат да бъдат причинени от P2P приложенията и да представляват източник на сериозни опасения. Много от тези приложения съдържат "spyware" или "adware" компоненти, които могат да заемат дори още по-голяма ширина на лентата, тъй като докладват на създателите си за навиците на потребителите при сърфиране из уеб пространството. Един зле конфигуриран P2P клиент може да осигури неавтентифициран достъп до цялата ви мрежа като сподели прикачени по мрежата устройства през P2P приложението. Ограничението относно типовете файлове, които могат да бъдат споделяни, е много малко или изобщо липсва. В резултат може да се стигне до компрометиране на конфиденциална информация, интелектуална собственост и други данни.

Социални уязвимости се появяват, когато злонамерен или вече заразен потребител създаде или промени файл, така че да прилича на информация, желана от друг потребител. Като резултат се създават вируси, троянски коне, червеи и друг злонамерен софтуер. Жертва на такива атаки обикновено става потребителят с по-ниска техническа грамотност, който ще щракне два пъти върху даден файл, без да забележи, че разширението или иконата му не съответстват на нормално асоциираните с този тип данни или който може да бъде подлъган да стартира изпълним файл. Независимо от същността на сваляното съдържание потребителите трябва да използват актуализиран антивирусен софтуер за сканиране на свалените файлове. Винаги, когато е

възможно трябва да се прави валидиране на контролните суми, за да се гарантира, че това, което е свалено, е именно желаното от потребителя и написаното от създателя му. P2P механизмите също могат да се използват за разпространение на злонамерен код; голям брой вируси се разпространяват като се маскират на търсено от потребителите P2P съдържание и се записват в папките със споделено съдържание на заразените клиенти. P2P трафикът може също така да тунелира и управлява трафика на компрометираните машини (зомбита).

Както корпоративните, така и домашните потребители трябва да обърнат сериозно внимание на юридическите уязвимости. Съдържанието, което може да бъде получено чрез P2P приложенията, включва защитени от авторското право музика, филми и програми. Различни организации, между които MPAA, RIAA и BSA работят активно, за да сложат край на нарушаването на авторското право, което се получава през P2P мрежите. Призовки към потребители, съдебни предписания и граждански искове са залели съдилищата. Успехът на тези усилия, или резултатът от липсата на такива, моралността или неморалността на свалянето на подобни материали трябва да отстъпи на второ място пред разходите, които прави една компания, за да отговаря или да се защитава срещу обвиненията в закононарушение. Порнографските материали също са широко достъпни през P2P мрежите. Дали такива материали са разрешени от вашите закони или не е без значение, ако срещу вашата компания започне съдебен процес за сексуален тормоз, тъй като един служител е свалил чрез компютър на компанията материали, които друг служител намира за обидни.

W7.2 Засягани операционни системи

Версии на P2P софтуера се предлагат за всички използвани понастоящем операционни системи Windows, както и за версиите на UNIX и Linux.

W7.3 CVE/CAN номера

CAN-2000-0412, CVE-2001-0368, CAN-2002-0314, CAN-2002-0315, CVE-2002-0967, CAN-2003-0397

W7.4 Как да определите дали сте уязвими

Детектирането на P2P дейност в мрежата може да се окаже предизвикателство. Можете да откриете P2P софтуер, стартиран на вашата мрежа, като наблюдавате трафика през общите портове, използвани от софтуера, или чрез претърсване на трафика за определени низове от приложния слой, често използвани от P2P софтуера. Моля погледнете в края на този документ списъка на портовете, които се използват често от P2P приложенията. Съществуват много приложни програми и услуги, които могат да подпомогнат детектирането или предпазването от P2P трафик. Известна част от базирания на хоста софтуер за предотвратяване на непозволени прониквания може да предотврати инсталирането или стартирането на P2P приложения. Network Based Application Recognition (NBAR) на Cisco и други мрежово базирани продукти могат да предотвратят влизането или излизането на P2P трафик от мрежата или да наблюдават P2P трафика. Наблюдаването на вашите WAN връзки чрез приложения като NTOP също може да открие P2P трафик. Можете да пожелаете също така да сканирате местата за мрежово съхранение за наличието на съдържание, което често се сваля от потребителите, включително *.mp3, *.wma, *.avi, *.mpg, *.mpeg, *.jpg, *.gif,

*.zip, и *.exe. Наблюдението на дисковете за внезапно намаляване на свободното дисково пространство може също да се окаже полезно. Nessus също предлага плъгин за детектиране на стартирани P2P приложения, а при машини с Microsoft Windows може да се използва SMS за сканиране за изпълними файлове, инсталирани на работните станции.

W7.5 Как да се защитим

Корпоративни политика:

1. Във вашата компания трябва да има приета и твърдо прилагана политика срещу свалянето на материали, защитени от закона за авторското право.
2. Във вашата компания трябва да има приета и твърдо прилагана политика за допустимото използване на корпоративната Интернет връзка.
3. Трябва да се извършва редовно сканиране на мрежовите устройства и на работните станции на корпорацията за съхраняване на непозволени материали.

Ограничения по отношение на мрежата:

1. Не трябва да се позволява на обикновените потребители да инсталират какъвто и да било софтуер, особено приложения "равен с равен"
2. Помислете за използването на прокси сървър за контролиране на достъпа през Интернет.
3. Изходното филтриране ще ограничи достъпа до всички портове, които не се използват за целите на бизнеса, макар че тази мярка ще е по-малко ефективна, тъй като повечето P2P приложения преминаха към http.
4. Наблюдавайте вашата мрежа за наличието на P2P трафик и сигнализирайте за нарушаването на възприетата политика по съответните канали.
5. Използвайте корпоративни версии на антивирусния софтуер и се уверете, че актуализирането му се извършва ежедневно.

Портове, които се използват често от приложенията "равен с равен"

Napster	eDonkey	Gnutella	KaZaa
tcp 8888	tcp 4661	tcp/udp 6345	tcp 80 (WWW)
tcp 8875	tcp 4662	tcp/udp 6346	tcp/udp 1214
tcp 6699	udp 4665	tcp/udp 6347	
		tcp/udp 6348	

Базата данни с подписи на Snort се намира на http://www.snort.org/cgi-bin/sigs-search.cgi?sid=p2p

549 P2P napster login
550 P2P napster new user login
551 P2P napster download attempt
552 P2P napster upload request
556 P2P Outbound GNUTella client request
557 P2P GNUTella client request
559 P2P Inbound GNUTella client request

561 P2P Napster Client Data
562 P2P Napster Client Data
563 P2P Napster Client Data
564 P2P Napster Client Data
565 P2P Napster Server Login
1383 P2P Fastrack (kazaa/morpheus) GET request
1432 P2P GNUTella GET
1699 P2P Fastrack (kazaa/morpheus) traffic
2180 P2P BitTorrent announce request
2181 P2P BitTorrent transfer

обратно в началото ^

W8 LSASS

W8.1 Описание

Услугата Local Security Authority Subsystem на Windows съдържа критично препълване на буфер, което при злонамерено използване може да доведе до пълно компрометиране на системата при Windows 2000, Server 2003 и издания Server 2003 64 Bit, XP и XP 64 бита. Това препълване е разгледано в бюлетина за сигурност на Microsoft Security MS04-011. Тази атака може да бъде извършена отдалечено и анонимно през RPC за Windows 2000 и XP системи, но изисква локални привилегии, за да бъде изпълнена на Server 2003 или 64 битовото издание на Windows XP.

Услугата Local Security Authority Subsystem Service (LSASS) играе важна роля в автентификацията пред системата и във функционалността Active Directory. Точно тук, при процеса на интерфейс с Active Directory функцията по записване в системата на LSASRV.dll може да бъде препълнена чрез необичайно дълъг низ. Тази уязвимост потенциално може да доведе до пълно компрометиране на системата.

Важното значение на факта, че тази уязвимост може да бъзе използвана отдалечено по злонамерен начин, се демонстрира от скорошното разпространение на Sasser и Korgo -червеи, чието действие се основава на LSASS. Те са известни също като W32.Sasser (http://www.cert.org/current/archive/2004/07/12/archive.html#sasser, http://www.microsoft.com/security/incident/sasser.mspx) и W32.Korgo (http://www.cert.org/current/archive/2004/07/12/archive.html#korgo). Много от последните злонамерени “bot” червеи също използват тази уязвимост, за да заразяват, и тяхната важност като нарастващ проблем на сигурността расте с всеки ден и често се пренебрегва.

На уязвимостта беше даден CVE номер CAN-2003-0533. Настоятелно препоръчваме на мрежовите администратори не само да закърпят своите системи срещу тази уязвимост, но и да инсталират всички необходими контроли на достъпа на входните точки на мрежата, за да възпрат Windows RPC базираните злонамерени агенти от навлизане в уязвимите обкръжения.

Засягани операционни системи

Windows 2000, Windows XP и Professional, 64-битовото издание на Windows XP, Windows 2003

W8.3 CVE/CAN номера

CVE-1999-0227
CAN-1999-1234, CAN-2001-1122, CAN-2003-0507, CAN-2003-0533, CAN-2003-0663, CAN-2003-0818

W8.4 как да определите дали сте уязвими:

Наличието на тази уязвимост може да бъде проверено или през мрежата или локално на самата система. Мрежовата проверка и мрежовите администратори, които трябва да открият уязвимите машини в една мрежа или в един диапазон от IP номера, са по-подходящи от гледна точка на сигурността. Локалната проверка е по-подходяща за крайни потребители, които трябва да открият дали тяхната система е уязвима.

Следните три безплатни средства могат да открият тази уязвимост при мрежово базирана проверка:

1. Nessus,мрежово базирано средства за оценка на уязвимостите, има smb_kb835732.nasl plug-in (id 12209) което проверява за съществуването на кръпка KB835732. Подробности и възможност за сваляне - http://cgi.nessus.org/plugins/dump.php3?id=12209

2. DSScan на Foundstone позволява преглеждане на цялата мрежа и осигурява възможност за изпращане на предупреждания към уязвимите системи. Подробности и възможност за сваляне - http://www.foundstone.com/resources/proddesc/dsscan.htm

3. Скенер за червея Sasser на eEye определя дали системата е уязвима за експлойта LSASS и червея Sasser. Подробности и възможност за сваляне - http://www.eeye.com/html/resources/downloads/audits/index.html

При локални проверки можете да разчитате на следните средства от Microsoft.

1. Microsoft Baseline Security Analyzer (MBSA) ви позволява да определите дали вашата машина е уязвима за този експлойт. Подробности и възможност за сваляне - http://www.microsoft.com/technet/security/tools/mbsahome.mspx

2. Windows Update сканира вашия компютър и ви предлага селекция от обновления, пригодени точно за вас. Ако MS04-011 (KB835732) е изброено като едно от обновленията, които още не са инсталирани на вашата машина, то тя е уязвима. На http://windowsupdate.microsoft.com можете да намерите инструкции стъпка по стъпка.

W8.5 Как да се защитим

Накратко:

1. Блокирайте всички портове при защитната стена
2. Инсталирайте последната кръпка от Microsoft

3. Разрешете усъвършенстваното TCP/IP филтриране на системата

Подробности:

1. Блокирайте всички портове при защитната стена.

   Ако имате защитна стена, можете да подпомогнете защитата на анклавните мрежи и системи от атаки, които идват отвън, чрез блокиране на следните портове:

   - UDP/135, UDP/137, UDP/138, UDP/445
   - TCP/135, TCP/139, TCP/445, TCP/593

   Препоръчваме ви да използвате персонална хост базирана защитна стена и след това да блокирате целия нежелан входящ трафик. Ако използвате възможността Internet Connection Firewall (ICF) на Windows XP или на Windows Server 2003, за да подпомогнете защитата на вашите хостове, свързани към Интернет, то тя по подразбиране блокира нежелания входящ трафик. За да разрешите възможността Internet Connection Firewall като използвате Network Setup Wizard, изпълнете следните стъпки:

   a. Щракнете върху **Start** и след това щракнете върху **Control Panel**

   b. В Category View, която се появява по подразбиране, щракнете върху **Network and Internet Connections** и след това щракнете върху **Setup or change your home or small office network.** Възможността Internet Connection Firewall е разрешена, когато в Network Setup Wizard изберете конфигурация, указваща, че вашата система е директно свързана към Интернет.

   За да конфигурирате ръчно Internet Connection Firewall, изпълнете следните стъпки:

   a. Щракнете върху **Start** и след това щракнете върху **Control Panel**
   b. В Category View, която се появява по подразбиране,, щракнете върху **Network and Internet Connections** и след това щракнете върху **Network Connections**.
   c. Щракнете с десния клавиш на мишката върху връзките, за които искате да разрешите Internet Connection Firewall, и след това щракнете върху **Properties**
   d. Щракнете върху страницата **Advanced**
   e. Щракнете върху кутийката с отметка, за да изберете **Protect my computer or networks by limiting or preventing access to this computer from the Internet**, и след това щракнете върху **OK**

Забележка: Ако искате да разрешите използването на някои програми и услуги през защитната стена, щракнете върху **Settings** на етикета **Advanced** и след това изберете необходимите програми, протоколи и услуги.

2. Инсталирайте последната кръпка за LSASS в зависимост от конкретната Windows операционна система.

   Кръпката за уязвимостта LSASS може да се вземе от следния сайт на Microsoft.
   http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

3.Разрешете усъвършенстваното TCP/IP филтриране, за да блокирате целия входящ трафик. За да конфигурирате TCP/IP филтрирането, изпълнете следните стъпки.

   A)Щракнете върху **Start**, посочете **Control Panel**, щракнете с десния бутон на мишката върху **Network Connections**, и след това щракнете върху **Open**.

   B)Щракнете с десния бутон на мишката върху връзката, за която искате да конфигурирате контрол на входящия достъп, и след това щракнете върху **Properties**

   C)В ***AdapterName*Connection Properties** което се намира на етикета **General**, щракнете върху **Internet Protocol (TCP/IP)**, и след това щракнете върху **Properties**.

   D)В диалоговата кутия **Internet Protocol (TCP/IP) Properties** щракнете върху **Advanced**.

   E)Щракнете върху етикета **Options**.

   F)Щракнете върху **TCP/IP Filtering** и след това щракнете върху **Properties**.

   G)Щракнете, за да изберете кутията с отметка **Enable TCP/IP Filtering (All adapters)**.

   H)В **TCP/IP Filtering** има три колони със следните етикети:

   - **TCP Ports**
   - **UDP Ports**
   - **IP Protocols**

   Във всяка колона трябва да изберете една от следните възможности:

   A)**Permit All**. Изберете тази опция, ако желаете да разрешите всички пакети за TCP или UDP трафик.

   B)**Permit Only.** Изберете тази опция, ако желаете да разрешите само избран TCP или UDP трафик. Щракнете върху **Add** и след това въведете съответния номер на порт или протокол в диалоговата кутия **Add Filter**. Не можете да блокирате UDP или TCP трафик

чрез избиране на **Permit Only** в колоната**IP Protocols** и след това чрез добавяне на IP протоколи 6 и 17.

Забележка: Когато конфигурирате TCP/IP филтрирането, моля припомнете си кои портове трябва да блокирате. За уязвимостта LSASS трябва да блокирате входящия TCP/445 порт.

обратно в началото ^

W9 Пощенски клиент

W9.1 Описание

Microsoft Outlook представлява програма за управление на личната информация и пощенски клиент за Microsoft Windows. Макар да е преди всичко програма за електронна поща, Microsoft Outlook предоставя също календар, както и възможност за управление на предстоящите задачи и контактите. Когато се използва съвместно с Microsoft Exchange Server, Microsoft Outlook може да предложи допълнителни функционални възможности за групуер като поддържане на няколко потребители, помощ при координирането на часовете за срещи и възможност за споделени календари и пощенски кутии.

Outlook Express (OE) е по-малко функционална, но безплатна версия на Outlook, която осигурява базисни услуги за електронна поща и управление на контактите. Тя върви заедно с Internet Explorer още от версия 1.0, който пък от своя страна представлява неразделна част от всички версии на Microsoft Windows, като се започне от Windows 95. Най-новата версия на Outlook Express, 6.0 с инсталиран SP1 може да се свали безплатно от http://www.microsoft.com/windows/oe/. Чрез интегриране на продукти като Internet Explorer и Outlook Express в други продуктови линии, включително в Office, BackOffice и операционната система Windows, Microsoft позволи използването на общи технологии и кодове в цялата платформа. За съжаление, тази практика въведе също и отделни уязвими точки и увеличи влиянието, което може да оказва всяка отделна уязвимост по отношение на сигурността.

Една от целите на Microsoft бе да разработи лесно за използване и интуитивно решение за електронна поща и управление на информацията. За съжаление, вградените възможности за автоматизация са в конфликт с вградените контроли за сигурност (често пренебрегвани от крайните потребители). Това обуслови възникването на пощенски вируси, червеи и злонамерени кодове, които компрометират локалната система, както и на много други форми на атака.

Потенциалните заплахи за сигурността на пощенските клиенти включват:

- Заразяване на компютъра с вирус или червей – злонамерен код, който се разпространява чрез прикрепени файлове или вградени скриптове в тялото на съобщението;
- Спам – нежелана комерсиална електронна поща;
- Уеб сигнализиране – валидиране на адреси на електронната поща, задействано чрез отваряне на съобщение от получателя му.

При подходящо конфигуриране текущите версии на Outlook и Outlook Express могат успешно да защитят потребителите от гореспоменатите заплахи.

W9.2 Засягани операционни системи

Всички версии на Microsoft Windows идват с Outlook Express, който е свързан с

Internet Explorer, и следователно е потенциално уязвим.

За да определите коя е текущата версия на OE, стартирайте Internet Explorer и след това изберете About Internet Explorer от менюто Help. Версиите, по-ниски от 6, трябва да бъдат незабавно заменени с по-нови и обновени с всички подходящи средства за бърза поправка, които имат отношение към сигурността.

Outlook се качва на една машина само, ако потребителят я инсталира съзнателно като самостоятелно приложение или като част от пакета Microsoft Office. Версиите на Outlook за Microsoft Windows включват::

- Outlook 95
- Outlook 97
- Outlook 98
- Outlook 2000, известен също като Outlook 9
- Outlook XP, известен също като Outlook 10 или Outlook 2002
- Outlook 2003, известен също като Outlook 11

Версиите преди Outlook 2000 не се поддържат повече от Microsoft Corp. и настоятелно се препоръчва те да бъдат заменени възможно най-скоро с по-високи и поддържани версии на продукта (Outlook 2003, 2002 или 2000).

На всички версии на Outlook трябва да се инсталират последните сервизни пакети за съответните продукти.

Текущи версии на сервизните пакети за Outlook:

- Outlook 2000 – сервизен пакет 3
- Outlook XP (Outlook 2002) – сервизен пакет 3
- Outlook 2003 понастоящем няма сервизни пакети.

За да определите коя е текущата версия на Outlook, стартирайте програмата и след това изберете About Outlook от менюто Help.

Литература:
Outlook Express http://www.microsoft.com/windows/oe/
Outlook http://www.microsoft.com/office/outlook/
Дати на жизнения цикъл на продуктите
http://support.microsoft.com/default.aspx?id=fh;[ln];lifeprodo
Обновления за Microsoft Office http://office.microsoft.com/OfficeUpdate

CVE-1999-0967, CVE-2000-0036, CVE-2000-0567, CVE-2000-0621, CVE-2000-0662,CVE-2000-0753, CVE-2000-0788, CVE-2001-0149, CVE-2001-0340, CVE-2001-0538,CVE-2001-0660, CVE-2001-0666, CVE-2001-0726, CVE-2001-1088, CVE-2002-0152,CVE-2002-0685, CVE-2002-1056

CAN-1999-0004, CAN-1999-0354, CAN-1999-1016, CAN-1999-1033, CAN-1999-1164,CAN-2000-0105, CAN-2000-0216, CAN-2000-0415, CAN-2000-0524, CAN-2000-0653,CAN-2000-0756, CAN-2001-0145, CAN-2001-0945, CAN-2001-0999, CAN-2001-1325,CAN-2002-0285, CAN-2002-0481, CAN-2002-0507, CAN-2002-0637, CAN-2002-1121,CAN-2002-1179, CAN-2002-1255, CAN-2003-0007, CAN-2003-0301, CAN-2004-0121, CAN-2004-0215, CAN-2004-0284, CAN-2004-0380,

CAN-2004-0501, CAN-2004-0502 , CAN-2004-0503, CAN-2004-0526

W9.3 Как да определите дали сте уязвими
Всички компютри, на които е инсталиран Internet Explorer, ще съдържат Outlook Express.. Ръчното инсталиране на приложенията от поредицата Microsoft Office може да включва програмата Outlook, заедно с най-често използваните пакети като Word, Excel, PowerPoint и Access.

Една система може да бъде уязвима, ако

a. не е изцяло актуализирана, което може да се провери, ако посетите MS update или

1. настройките, които имат отношение към сигурността, са неподходящо направени.

W9.4 Как да се защитим
Има няколко неща, които можете да направите, за да конфигурирате Outlook и/или Outlook Express, така че да сведете до минимум, рисковете за сигурността.

Обезопасяване на Outlook / Outlook Express
По подразбиране настройките на Outlook и Outlook Express, които са свързани със сигурността и конфигурирането, са доста слаби. От значение е контролът върху тях да бъде засилен и да се провери дали е актуализиран основният софтуер. Примерите за изпълняване на тази задача включват:

1. Посещавайте често сайта за обновяване на Microsoft Update http://windowsupdate.microsoft.com и инсталирайте всички критични кръпки.
2. Забранете прозореца за предварителен преглед на съобщенията (Message Preview Pane), като щракнете върху View > Layout и изтриете отметката върху опцията Show preview pane.
3. Затегнете настройките, имащи отношение към сигурността, които са свързани с входящата поща.
   Изберете Tools > Options и след това щракнете върху етикета Security. Щракнете върху радиобутона "Restricted sites zone (More secure)" и след това настройте ръчно стойността до висока (high). Щракнете върху Apply и OK, за да потвърдите избора си.

Защита от прикрепени файлове с потенциално злонамерен код

Във версиите на Oulook 2000 (SP3), Outlook 2002 (SP1 и по-високи) и Outlook 2003 (всички версии) е включена ефективна защита срещу прикрепени файлове, които потенциално съдържат злонамерен кад. По подразбиране всички прикрепени файлове с разширения като .exe, .com, .vbs и т.н. се блокират автоматично. Когато съществува легитимна необходимост от изпращането на изпълними файлове като прикрепени към съобщение, се препоръчва използването на някакво средство за архивиране като WinZip или различен метод за прехвърляне на файлове (FTP, SCP).

Пълен списък на разширенията, блокирани от Outlook, може да се намери в статията:

http://www.microsoft.com/office/ork/2003/three/ch12/OutG07.htm

За да разширите списъка по подразбиране на типовете файлове, които се блокират, е необходимо да редактирате регистъра по следния начин:

1. Щракнете върху Start, щракнете върху Run, напишете regedit, и след това щракнете върху OK.
2. Намерете и след това щракнете върху следния ключ от регистъра:

За Outlook 2003:

HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Outlook\Security

За Outlook XP/2002:

HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Outlook\Security

За Outlook 2000:

HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Outlook\Security

3. В менюто Edit посочете New и след това щракнете върху String Value.
4. Напишете Level1Add и след това натиснете ENTER.
5. В менюто Edit щракнете върху Modify.
6. Напишете <разширенията_на_файловите_имена> и след това щракнете върху OK.

Забележка: *разширенията_на_файловите_имена* е списък с разширенията на имената на прикрепените файлове. Всяко разширение на имената на прикрепените файлове се отделя с точка и запетая. Например, напишете .zip; .gif ако искате да блокирате едновременно .zip и .gif файловете, идващи като прикрепени към електронната поща.

Статията на Microsoft Technet KB837388 *How to configure Outlook to block additional attachment file name extensions* предлага подробно описание на този процес:

http://support.microsoft.com/?kbid=837388

Защита от SPAM (нежелана комерсиална електронна поща)

В Outlook 2003 е включена ефективна защита от спам. За да я конфигурирате, отворете Outlook – изберете *Actions – Junk E-mail – Junk E-mail Options.*
В етикета *Options* на тази диалогова кутия има 4 радиобутона, които контролират конфигурацията и прага на задействане на анти-спам машината:

- No Automatic Filtering – не се прави филтриране за спам ;
- Low (настройка по подразбиране) – много ефективна настройка; премества по-голямата част от непотребната поща в папката Junk E-mail и на практика дава много малко фалшиви разпознавания;
- High – агресивно филтриране на спама. Отстранява почти цялата непотребна поща (изпраща я в папката *Junk E-Mail*), но може потенциално да маркира някое легитимно писмо като спам. Ако се избере тази настройка, се препоръчва папката *Junk E-mail* да се проверява редовно за наличие на легитимни писма, погрешно идентифицирани като спам;
- Safe Lists Only – до потребителя ще достигат само писма от податели или домейни от *Safe Senders List* (списък на безопасните податели) или*Safe Recipients List* (списък на безопасните получатели). Това е най-ефективната настройка срещу спам, но тя изисква известно време и усилия за създаване на Safe Senders List и Safe Recepients List с всички легитимни адреси и домейни, които могат да комуникират с потребителя.

Outlook Express и по-старите версии на Outlook не притежават ефективни анти-спам възможности, но имат Blocked Senders List, който може да се индивидуализира от потребителя. За да го настроите в Outlook Express, идете на *Tools > Message Rules* и изберете *Blocked Senders List*.

Защита от злонамерен код, вграден в текста на съобщение

E-mail съобщенията във формат rich-text (HTML, RTF) могат да съдържат вграден в текста злонамерен код, за разлика от съобщенията с обикновен текст, които не могат да съдържат никакъв код. Най-простият и ефективен начин за защита от такъв злонамерен код е четенето на всички e-mail съобщения в обикновен текстов формат. За да конфигурирате това в Outlook 2003, идете на *Tools > Options,* и изберете етикета *Preferences,* след това бутона *E-mail Options* и поставете отметка на *Read all standard mail in plain text* и *Read all digitally signed mail in plain text*. Натиснете двукратно *OK*.

Защита от уеб сигнализиране

Уеб сигнализирането е метод за проверка дали едно e-mail съобщение е отворено, и следователно, дали получателят му е действителна цел за бъдещо изпращане на спам, чрез включване на малки изображения (обикновено 1x1 пиксела) в тялото на съобщение с HTML формат. Тази техника е широко използвана от изпращачите на спам и реклами. Освен даването на потвърждение, че даден потребител е отворил e-mail съобщението, уеб сигнализирането позволява да се получи определена информация (IP адрес, език, версия на браузъра) за потребителя и неговата система. За да предотвратите уеб сигнализирането при Outlook 2003, отворете Outlook – изберете *Tools > Options,* и идете на етикета *Security*. Идете на бутона *Change Automatic Download Settings…* и изберете кутиите с отметки *Don't download pictures or other content automatically in HTML e-mail* и *Warn me before downloading content when editing, forwarding, or replying to e-mail* – натиснете двукратно *OK.*

User Behavior

Тъй като най-често човешкият елемент е най-слабото звено в процеса на обезпечаване на сигурността, от значение е да се следват някои насоки за добра практика при работа с електронна поща.

Дори ако файлът идва от надежден източник, е важно със сигурност да бъде проверен за вируси и друг злонамерен софтуер, както е обяснено в подробности в следващия раздел, озаглавен "Антивирусен софтуер".

При получаване на прикрепен файл го запомнете в папка, различна от *My Documents*, тъй като много вируси използват именно нея като отправна точка. Изберете друга папка или дори друг дял от диска, за да отделите пристигащите прикрепени файлове от останалата си информация.

Не отваряйте прикрепени файлове, които не очаквате, дори ако са от приятели. Дори DOC и XLS файловете могат да съдържат вградени програми на Basic, които могат да причинят вреда на вашата система. Ако трябва да отворите документа с друг продукт на Microsoft, като Word, отидете непременно в Tools > Options > Security и изберете радиобутона, намиращ се до High, за да забраните

макросите, освен ако те не са подписани от автора им.

Винаги проверявайте всички налични цифрови подписи, асоциирани към изпълними файлове, за да се уверите в целостта на файла и да проверите, че той действително идва от надежден източник.

Антивирусен софтуер
Антивирусният софтуер може да подпомогне защитата на компютрите от повечето вируси, червеи, троянски коне и друг злонамерен код. Жизнено важно е сигнатурните бази данни на антивирусните програми да се обновяват поне веднъж седмично (в идеалния случай ежедневно и автоматично), за да подпомогнат предпазването дори от най-новите заплахи. Повечето съвременни антивирусни решения напълно автоматизират изпълнението на тази задача. Благоразумно е като предпазна мярка да осигурите сканиране на всички файлове независимо от типа на файла или произхода му.

Съвременните антивирусни решения притежават способността да сканират цялата входяща и изходяща поща, за да гарантират, че злонамерените файлови типове и скриптове се блокират преди да могат да нанесат вреда на локалната система.

Горещо ви препоръчваме преди използването на електронна поща и други Интернет услуги да инсталирате актуализирани средства за защита от вируси, тъй като много вируси се разпространяват през пощенските клиенти във вид на прикрепени файлове или злонамерен скрипт код, който се стартира при четене или предварителен преглед на съобщението..

Литература:
Microsoft Antivirus Reference
http://www.microsoft.com/security/protect/antivirus.asp

Обновяване на Outlook и Outlook Express
С течение на времето Outlook Express е била неколкократно актуализирана, така че да осигурява по-голяма вградена функционалност, стабилност и сигурност. Най-новата версия, може да бъде свалена безплатно от
http://www.microsoft.com/windows/oe/

За да се уверите, че Outlook и всички други ваши Office програми са изцяло актуализирани, посетете Office Product Updates page. Този сайт открива автоматично критичните и препоръчителни обновявания, които са необходими.

За подробна информация относно другите възможности, свързани със сигурността и настройките в Office 2003, прочетете Office 2003 Security white paper.
Забележка: Преди да правите промени в някой от свързани в мрежа компютри, трябва да се свържете със системния администратор. Администраторите могат да намерят подробна техническа информация относно обновяването във връзка със сигурността на Outlook E-Mail Security в Office Resource Kit.
Деинсталиране на Outlook и Outlook Express
Ако се използва отделен клиент за електронната поща или за управление на информацията, Outlook и/или Outlook Express могат да бъдат деинсталирани безопасно.

Outlook при всички версии на Windows
Outlook може да бъде премахнат чрез щракане върху Start > Settings > Control Panel и двойно щракане върху иконата Add/Remove Programs. Когато се отвори диалоговия прозорец на свойствата на Add/Remove Program, щракнете върху етикета *Outlook* и изберете бутона *Remove*.

Outlook Express при Windows 98/ME
Outlook Express може да бъде отстранен от системата като се щракне на Start > Settings > Control Panel и след това двукратно върху иконата Add/Remove Programs. Когато се отвори диалоговия прозорец на свойствата на Add/Remove Program, щракнете върху страницата Windows Setup, придвижете се надолу до Microsoft Outlook Express и изтрийте отметката в кутийката до него.

Щракнете върху бутоните Apply и OK, за да потвърдите избора си, и Windows ще деинсталира Outlook Express.

Outlook Express при Windows 2000/XP или обновени версии на Internet Explorer
Стъпките, необходими за отстраняване на Outlook Express при Windows 2000/XP или за потребители, които са актуализирали браузъра си до най-новата версия, са по-сложни. За пълни подробности потърсете следните ръководства на Microsoft:

За потребители на Windows 2000, които използват Microsoft Outlook Express версии 5.x/6.0
http://support.microsoft.com/default.aspx?scid=kb;EN-US;q263837

За потребители на Windows 98/Me, които са се обновили до Microsoft Outlook Express версии 5.x/6.00
http://support.microsoft.com/default.aspx?scid=kb;EN-US;q256219

Забележка: Outlook Express може да се инсталира без да забележите при инсталирането на сервизен пакет, на важна циклична поправка (roll-up) или при обновяване на операционната система.

обратно в началото ^

W10 Съобщения в реално време

W10.1 Описание

Технологията за съобщения в реално време се разви през последните няколко години от ново добавъчно приложение, което позволява на потребителите бързо да влизат във връзка с приятелите и семейството си, до същностна характеристика на операционната система Windows, често използвана за бизнес комуникации, сътрудничество и работна поддръжка. Макар че на разработените от трети страни приложения за съобщения в реално време (IM) все още се пада голяма част от реализациите на IM, съществува нарастваща тенденция за интегриране на функционалната възможност за съобщения в самата операционна система, което може потенциално да създаде директна заплаха и за сигурността за организации, които са приели политика или обезопасителни операционни рамки, не допускащи използването на тази технология. Откриването на уязвимости в тези програми създава значителен риск и за организации, които не предприемат технически контрамерки, нямат служители по сигурността, нито възможности за намаляване на тази непрекъснато нарастваща вградена в системата заплаха.

Уязвимости в тези програми, които могат да бъдат използвани отдалечено, или свързани с тях зависимости се превръщат в нарастваща заплаха за целостта и сигурността на мрежите, право пропорционална на бързото им интегриране и инсталиране в Windows системите. Сценариите на атаките, насочени към уязвимостите на съобщенията в реално време, варират в широки рамки и могат да приемат формата на отдалечено изпълнение на препълвания на буфери (RPC базирани, лошо формирани пакети), атаки, базирани на URI/злонамерена връзка, уязвимости при прехвърлянето на файлове и Active X експлойти.

Уязвимостите в тези програми обикновено попадат в следните категории:

- **Остарели ActiveX контроли** – например препълването на буфер "ResDLL"при MSN Messenger CAN-2002-0155, уязвимостта Yahoo! Voice Chat ActiveX Control Buffer Overflow (http://www.securityfocus.com/bid/7561), уязвимостта Yahoo! Webcam ActiveX Control Buffer Overrun (http://www.securityfocus.com/bid/8634).
- **Проблеми при реализацията на URI** – например изпълнението на злонамерен скрипт при Yahoo! Messenger CAN-2002-0032, препълването на буфер на URI манипулатор при Yahoo! Messenger CAN-2002-0031.
- **Различни препълвания на буфери, като тези, възникващи при прехвърляне на файлове.** – например, неуспешното валидиране на файлове при MSN Messenger CAN-2004-0122, препълванията на буфери на полета "Imvironment" и "message" при Yahoo! Messenger, съответно CAN-2002-0320 и CAN-2002-0320, препълването на буфер TLV 0x2711при разбор на пакетите при AOL Instant Messenger CAN-2002-0005, VU#912659, уязвимостта на Yahoo! Messenger YAuto.DLL Open Buffer Overflow (http://www.securityfocus.com/bid/9145), уязвимостта на AOL Instant Messenger Getfile Screenname Buffer Overrun (http://www.securityfocus.com/bid/8825)

Тези приложения не само вкарват мрежови уязвимости в системите, но създават също така риск от загуба на интелектуална собственост, опасност от загуба на конфиденциалност и заплаха от загуба на производителност на служителите. Макар че намаляването на влиянието на слабостите в тези програми, които могат да бъдат използвани отдалечено по злонамерен начин, е от най-голямо значение, необходимата приемлива политика на използване и поставянето в действие на входящия/изходящия трафик е също от първостепенно значение за гарантирано избягване на проблемите, които съобщенията в реално време могат да вкарат в една мрежа.

W10.2 Засягани операционни системи:
Microsoft Instant Messenger може да се стартира на Windows 98, Windows ME, Windows 2000 и Professional, Windows XP и Windows 2003. При всички версии на Microsoft Windows XP Instant Messenger пристига вмъкнат в операционната система.

W10.3 CVE/CAN номера:

CVE-2002-0005[NOMINATE], CVE-2002-0032, CVE-2002-0155[NOMINATE], CVE-2002-0785

CAN-2002-0031[NOMINATE], CAN-2002-0228, CAN-2002-0320, CAN-2002-0362[NOMINATE], CAN-2003-0717[NOMINATE], CAN-2004-0043, CAN-2002-1486[NOMINATE]

W10.4 Как да определите дали сте уязвими:
За да откриете коя е текущата версия на Microsoft Instant Messenger, стартирайте програмата и след това изберете About Instant Messenger от менюто Help. Версиите по-ниски от 6.2 трябва веднага да бъдат ъпгрейднати и обновени със съответните средства за бърза поправка (hotfixes).

W10.5 Как да се защитим:

(a) Уверете се, че целият инсталиран софтуер за съобщения като Yahoo, MSN, AOL, Trillian и т.н. е обновен с всички кръпки от производителите.

(b) Конфигурирайте системата за предотвратяване/откриване на непозволени прониквания, за да ви предупреждава при всички прехвърляния на файлове, които използват някоя от програмите за съобщения.

(c) Ато политиката на сигурността на съответния сайт го позволява, блокирайте чрез защитната стена следващите портове. Отбележете, че по този начин не получавате пълна защита, тъй като някои от тези приложения могат за заобикалят ограниченията на защитните стени.

- 1863/tcp: Microsoft .NET Messenger, MSN Messenger
- 5050/tcp: Yahoo Messenger
- 6891/tcp: MSN Messenger File Transfers
- 5190-5193/tcp: AOL Instant Messenger

(d) Блокирайте достъпа до уеб страници, съдържащи линкове с URL като "aim:" или "ymsgr:". По този начин можете да предотвратите използването на пропуските в URI манипулаторите. Друга възможност е внимателно да премахнете тези ключове в регистрите в "HKEY_CLASSES_ROOT".

(e) Блокирайте достъпа до уеб страници, извикващи ActiveX контроли, свързани с някакви проблеми на програмите за съобщения. По този начин можете да предотвратите използването на уязвимости в ActiveX контролите, свързани с програмите за съобщения.

обратно в началото ^

Топ уязвимостите на UNIX системите (U)

U1 Системата за имена на домейни BIND

U1.1 Описание
Пакетът Berkeley Internet Name Domain (BIND) се превърна в най-широко използваната в света реализация на Domain Name Service (DNS). DNS е критична система, която улеснява конвертирането на имена на хостове (hostnames) (например, www.sans.org) в съответния регистриран IP адрес. Поради повсеместното използване и важния характер на BIND, той се превръща в цел на често провеждани атаки. Атаките тип “отказ от обслужване” (DoS),

които обикновено довеждат до пълна загуба на услугите за наименоване на Интернет сайтове, отдавна тормозят BIND. Вътре в BIND бяха открити и възможности за различни други атаки, като препълвания на буфери и затрудняване работата на кешовете (cashe poisoning). Макар, че екипът, който разработва BIND е доказал, че е много бърз при реагиране и/или поправяне на уязвимостите, все още работят прекалено много остарели, зле конфигурирани и/или уязвими сървъри.

Голям брой фактори допринасят за това положение. Основна роля между тях играят администраторите, които не са уведомени за обновяванията, свързани със сигурността; системите, на които е стартиран BIND демон (наричан "named"), без това да е необходимо; и зле конфигурираните файлове. Всяка от тези причини може да предизвика отказ от обслужване, препълване на буфер или "cashe poisoning" на DNS кеша. Между откритите съвсем наскоро слабости на BIND е отказът от обслужване, разискван в CERT Advisory CA-2002-15. В този случай един нападател би могъл да изпраща специфични DNS пакети така, че да предизвика вътрешна проверка за съвместимост, която сама по себе си е уязвима и причинява изключване на BIND демона. Друг пример е атаката тип "препълване на буфер", обсъдена в CERT Advisory CA-2002-19, при която нападателят би могъл да използва уязвими реализации на библиотеките на DNS преобразувателя (resolver). Чрез изпращане на злонамерени DNS отговори нападателят може да използва тази уязвимост и да изпълнява произволни кодове, дори да предизвика отказ от обслужване.

Допълнителен риск внася и уязвимият BIND сървър, който може да бъде компрометиран и използван като склад за забранени материали без знанието на администратора, или при атаки от тип stepping-stone, които използват сървъра като платформа за по-нататъшна злонамерена дейност.

U1.2 Засягани операционни системи

На практика всяка UNIX и Linux система се разпространява с някаква версия на BIND. Инсталацията на BIND може да бъде съзнателна при работа като сървър или неумишлена, като част от обща инсталация. За Windows платформа се предлага и бинарна версия на BIND.

U1.3 CVE/CAN номера

CVE-1999-0009, CVE-1999-0024, CVE-1999-0184, CVE-1999-0833, CVE-1999-0837,
CVE-1999-0835, CVE-1999-0848, CVE-1999-0849, CVE-1999-0851, CVE-2000-0887, CVE-2000-0888, CVE-2001-0010, CVE-2001-0011, CVE-2001-0012, CVE-2001-0013,
CAN-2002-0029, CAN-2002-0400, CAN-2002-0651, CAN-2002-0684,
CAN-2002-1219, CAN-2002-1220, CAN-2002-1221, CAN-2003-0914

U1.4 Как да определите дали сте уязвими

Всеки DNS сървър, работещ с версия на BIND, която е свързана с операционната система, трябва да бъде сравнена с текущите кръпки, предлагани от съответния производител. Ако използваната версия на BIND е компилирана от сорс, идващ от Internet Software Consortium (ISC), трябва да се провери дали това е последна

версия. Остарелите или незакърпени версии на BIND най-вероятно са уязвими.

При повечето инсталации на системи командата "named -v" ще покаже версията на инсталирания BIND с номерация от вида X.Y.Z, където X е главната версия, Y е подверсията, а Z е нивото на кръпката. Понастоящем трите главни версии на BIND са 4, 8 и 9. Ако се използва версия на BIND, вградена от сорс, трябва да се избягва използването на версия 4 и вместо нея да се инсталира версия 9. Можете да се снабдите с последния сорс - версия 9.3.0rc2, от ISC.

Един подходящ подход за поддържане на сигурността на BIND е абонаментът за персонализираните предупреждаващи за уязвимости доклади, като предлаганите от SANS или четенето на съветите публикувани в OSVDB. Освен предупрежденията, свързани със сигурността, един актуализиран скенер за уязвимости може да бъде високоефективен при диагностицирането на всички потенциални уязвимости в DNS системите.

U1.5 Как да се защитим

- **За обща защита от BIND уязвимости:**
    1. Забранете BIND демона (наричан "named") на всяка система, която не е специално предназначена и оторизирана да работи като DNS сървър.
    2. Инсталирайте всички предлагани кръпки или направете обновяване на DNS сървърите до последната версия. За повече информация относно повишаването на сигурността на BIND инсталацията прегледайте статиите относно обезопасяването на “name services”, които са упоменати в UNIX Security Checklist.
    3. За да затрудните автоматизираните атаки или сканирания на една система, скрийте банера "Version String" в BIND, като замените в опциите на файла "named.conf" действително използваната версия на BIND с фалшив номер на версията.
    4. Разрешете прехвърлянията на зоните (zone transfers) само на вторичните DNS сървъри в домейни, на които може да се има доверие. Забранете прехвърлянията на зоните към родителски или дъщерни домейни, като вместо тях използвате делегиране и препращане.
    5. Ограничаване: За да предотвратите излагане на опасност на една цяла система от компрометирана BIND услуга, поставете ограничения на BIND, така че да се стартира като непривилегирован потребител в директория chroot()ed. За BIND 9, прегледайте http://www.losurs.org/docs/howto/Chroot-BIND.html.
    6. Забранете рекурсивните заявки и обработката от типа “glue fetching”, за да се защитите от DNS cashe poisoning.

- **За да се защитите от наскоро открити BIND уязвимости:**
    1. За уязвимостта Отказ от обслужване при ISC BIND 9: http//www.cert.org/advisories/CA-2002-15.html
    2. Няколко уязвимости Отказ от обслужване при ISC BIND 8: http://www.isc.org/products/BIND/bind-security.html

3. Cache poisoning чрез отрицателни отговори: http://www.kb.cert.org/vuls/id/734644

Съществуват множество прекрасни ръководства за повишаване на сигурността на BIND. Едно чудесно ръководство за повишаване на сигурността на BIND при системи Solaris, както и допълнителни препратки към документация за BIND, можете да намерите в Running the BIND9 DNS Server Securely и в архивите на статиите относно сигурността на BIND, предлагани от Afentis. Можете да прегледате също така документацията относно общите практики за сигурност на BIND на http://www.linuxsecurity.com/resource_files/server_security/securing_an_internet_name_server.pdf.
Администраторите могат също да се поинтересуват от алтернативи на BIND, като DJBDNS, който може да бъде намерен на http://cr.yp.to/djbdns.html.

обратно в началото ^

U2 Уеб сървър

U2.1 Описание

HTTP трафикът е определено най-често срещаният начин на използване на обществения Интернет. Unix уеб сървърите като Apache и Sun Java System Web Server (наричан по-рано iPlanet) обслужват по-голямата част от този трафик, и от такава гледна точка заслужават изключително внимателно изследване по отношение на проблемите, свързани със сигурността. Тези проблеми включват уязвимости в самия сървър, както и допълнителните модули, cgi скриптовете по подразбиране, примерните и тестовите cgi скриптове, PHP бъговете и различни други вектори на атака.

Макар че съществуват много такива вектори, всеобхватната и най-главна причина за компрометиране на един Unix уеб сървър се корени в самата система, която не е добре конфигурирана по време на инсталирането или не се поддържа редовно. Резултатът от такова компрометиране може да бъде всякакъв: от отказ от обслужване до обезобразяване на уеб сайт, пълен административен достъп на нападателя до сървъра и всякакви подобни щети.

Различните производители и проектите с отворен код предоставят за своите продукти конфигурация, съответстваща на най-добрата практика, и непрекъснати обновявания, свързани със сигурността; бдителността на всеки администратор на уеб сайт относно тяхното актуализиране е жизнено важна. Важно е да се разбере, че повечето уеб сървъри се компрометират чрез добре известни публични експлойти, които използват уязвимости, отдавна закърпени или обезопасени по друг начин от производителя.

U2.2 Засягани операционни системи

Всички UNIX системи могат да стартират HTTP сървър. Много Linux и UNIX варианти идват с инсталиран и разрешен по подразбиране Apache. Освен това, както Apache, така и iPlanet/Java System могат да се стартират на даден хост от други операционни системи, включително Windows, и изглежда са податливи на много от същите уязвимости.

U2.3 CVE/CAN номера

ЗАБЕЛЕЖКА: Както бе споменато, както Apache, така и iPlanet/Java System

могат да работят на различни платформи. Потребителите на такива сървъри трябва да прегледат съответния номер от следващия списък на CVE/CAN номерата, както и номер W1 от списъка за Windows, за да се уверят, че са взели предвид всички възможни уязвимости.

Apache
CVE-1999-0021, CVE-1999-0066, CVE-1999-0067, CVE-1999-0070, CVE-1999-0146,
CVE-1999-0172, CVE-1999-0174, CVE-1999-0237, CVE-1999-0260, CVE-1999-0262,
CVE-1999-0264, CVE-1999-0266, CAN-1999-0509, CVE-2000-0010, CVE-2000-0208, CVE-2000-0287, CAN-2000-0832, CVE-2000-0941, CVE-2002-0061, CVE-2002-0082, CVE-2002-0392, CAN-2002-0513, CAN-2002-0655, CAN-2002-0656, CAN-2002-0657, CAN-2002-0682, CAN-2003-0132, CAN-2003-0189, CAN-2003-0192, CAN-2003-0254 ,CAN-2004-0488,CAN-2004-0492

iPlanet/Sun Java System Web Server
CVE-2000-1077, CAN-2001-0419,CAN-2001-0746,CAN-2001-0747,CAN-2002-0686, CVE-2002-0845,CAN-2002-1315, CAN-2002-1316

OpenSSL
CAN-2003-0543, CAN-2003-0544, CAN-2003-0545

PHP
CVE-2002-0081, CAN-2003-0097, CAN-2004-0594

Други
CAN-2004-0529, CAN-2004-0734

U2.4 Как да определите дали сте уязвими
Всяка инсталация на уеб сървър по подразбиране или незакърпена такава трябва да се счита за уязвима по презумпция.

Най-добрият начин да бъдете винаги в течение относно проблемите, свързани със сигурността на даден продукт, е да преглеждате страницата с информация за сигурността на съответния производител. Примери за такива страници са:

- HTTP сървър Apache Main Page & Security Report (Включва връзки към ApacheWeek)
- Sun Web, Portal, & Directory Servers Download Center & BigAdmin Portal
- PHP Home Page и Downloads
- OpenSSL

За всяка изброена уязвимост трябва да бъдат взети мерки *възможно най-скоро*. Интервалът от време между момента на обявяване на уязвимостта и появата на публичен експлойт, и пускането в мрежата на червей, използващ този експлойт, става все по-малък.

За да подпомогнете процеса на оценяване на уязвимостите, можете да използвате всеки от няколкото предлагани скенери на уязвимости, включително Nessus и SARA (и двата са с отворен код), или някои от Free Utilities или Commercial Scanners, предлагани от eEYE. Такива сканирания трябва да бъдат стартирани в цялата мрежа, за да позволят на администратора да оцени риска от

известни и неизвестни сървъри.

U2.5 Как да се защитим

1. Уверете се, че на всички уебсървъри са стартирани последните кръпки; вижте връзките към съответните сайтове на производителите в "Как да определите дали сте уязвими"
2. Забранете всички функционални възможности на сървъра, които не са необходими. Обърнете особено внимание на CGI достъпа, поддръжката на php, mod_ssl и mod_proxy (за Apache). Забранете ги всичките по подразбиране, като ги разрешавате само тогава, когато обслужването ги изисква!
    - Ако са необходими PHP, CGI, SSI или други скрипт езици, обмислете използването на suEXEC. suEXEC позволява стартирането на скриптове под Apache с идентификация на потребителя различна от идентификацията на потребителя на Apache.
    - **ПРЕДУПРЕЖДЕНИЕ:** Задълбоченото вникване в suEXEC е строго задължително. Неправилното му използване може да създаде нови дупки в сигурността.
        1. За Apache 1.3.x вижте http://httpd.apache.org/docs/suexec.html
        2. за Apache 2.0.x вижте http://httpd.apache.org/docs-2.0/suexec.html
3. Обезопасете съдържанието на cgi-bin и другите директории със скриптове. Всички примерни скриптове и скриптове по подразбиране трябва да бъдат премахнати.
4. Обезопасете PHP:
   Това е широкообхватна цел сама по себе си и като част от цялото. Следващите редове дават някои стабилни начални точки за проверка на сигурността на вашата реализация на PHP.
    - Забранете параметрите, които ще накарат PHP да разкрива информация в HTTP заглавния блок (header).
    - Уверете се, че PHP е стартиран в safe mode.

      Подробна информация може да бъде намерена на: http://www.securityfocus.com/printable/infocus/1706
5. Обезопасяването на Apache може да бъде подпомогнато чрез допълнителни модули. Модулът mod_security (www.modsecurity.org) може да подпомогне защитата от Cross Site Scripting (XSS) и SQL инжекция. Подробни инструкции за използването му можете да намерите на техните уеб сайтове.
6. Проверката на скриптовете за уязвимости, включително XSS и SQL инжекция е също от значение. Съществуват няколко инструменти с отворен сорс, които могат да изпълнят такава проверка. Nikto (предлага се на http://www.cirt.net/code/nikto.shtml) е един от най-всестранните инструменти за CGI сканиране.

7. Трябва да помислите по въпроса за стартирането на HTTP сървър в среда chroot. Ако HTTP сървърът е стартиран като chroot, той няма достъп до никаква част от структурата на директориите на операционната система извън chroot. Това често може да помогне за предотвратяването на експлойтите. Един експлойт, например, може да извика обвивката (shell), но тъй като /bin/sh вероятно не е (и не трябва да бъде) в chroot, експлойтът ще бъде неефективен.
   ПРЕДУПРЕЖДЕНИЕ: Стартирането като chroot може да има неблагоприятен ефект върху CGI, PHP, бази данни и други модули или комуникации, които се нуждаят от достъп на обкръжението на уеб сървъра до външни библиотеки или изпълними програми.
8. Тъй като съществуват различни методи за "chrooting", за повече сведения трябва да прегледате документацията на софтуера. Допълнителна информация може да бъде намерена на:
   - http://www.w3.org/Security/Faq/wwwsf3.html#SVR-Q5
   - http://www.modsecurity.org/documentation/apache-internal-chroot.html
   - http://wwws.sun.com/software/whitepapers/webserver/wp_ws_security.pdf
9. Не стартирайте вашия уеб сървър като администратор. За стартирането му трябва да бъдат създадени единичен потребител и група с минимални привилегии, като през този потребител или група не трябва да се стартират други системни процеси (например, стартирайте Apache чрез потребител "apache" вместо потребител "nobody").
10. Ограничете разгласяваната информация за сървъра.
    Макар, че това предложение ще срещне несъгласие от страна на хора, които смятат, че намаляването на риска чрез "информационно затъмнение" не е правилния начин, общественият Интернет е подложен на голям брой опити за злонамерени атаки, извършвани пипнешком (blind sweeping) (това се доказва и от факта, че в много логове на Apache можете да видите множество поредни опити за злонамерено използване на IIS); има също така и няколко експлойта, които се задействат от информацията в заглавния блок (header).
    - За да промените маркера по подразбиране на HTTP отговора на Apache:
      1. За Apache 1.3.x вижте http://httpd.apache.org/docs/mod/core.html#servertokens http://httpd.apache.org/docs/mod/core.html#serversignature.
      2. За Apache 2.0.x вижте http://httpd.apache.org/docs-2.0/en/mod/core.html#servertokens.
    - Уверете се, че mod_info не е достъпен по Интенет.
    - Индексирането на директории трябва да бъде забранено.
11. Ефективното и щателно записване на логовете е важно за ефикасното проследяване на всички потенциални проблеми, свързани със сигурността или необяснимото поведение, което може да има даден сървър. Рутинното преглеждане на логовете и съхраняването на по-старите логове в архив е добра практика. Това ще направи размера на лога по-лесно управляем и ще улесни разбора на съдържанието му, ако това се окаже необходимо.

Разнообразна информация относно форматите на логовете и преглеждането им можете да намерите на:

- За Apache 1.3.x вижте: http://httpd.apache.org/docs/logs.html
- За Apache 2.0.x вижте: http://httpd.apache.org/docs-2.0/logs.html

В много случаи съдържанието на тези логове може да се окаже недостатъчно. Добре би било да записвате GET and POST полезните активности (payloads), особено когато използвате PHP, CGI или други скриптове. По този начин можете да получите важни данни и доказателства в случай на компрометиране на сигурността. Записването на GET и POST полезните активности може да се осъществи чрез mod_security. (за Apache).

- http://www.modsecurity.org
- http://www.securityfocus.com/infocus/1706

обратно в началото ^

U3 Автентификация

U3.1 Описание

Паролите от една или няколко думи и/или кодовете за сигурност се използват практически при всяко взаимодействие между потребителите и информационните системи. Повечето форми на автентификация на потребителите, както и на защита на файлове и данни разчитат основно на поставените от потребителя или продавача пароли. Освен това, тъй като правилно автентифицираният достъп често не се записва в логовете, или ако се записва вероятно няма да предизвика подозрения, една компрометирана парола дава възможност за практически неоткриваемо изследване на системата. Един нападател, който притежава валидна потребителска парола, ще има пълен достъп до всички ресурси, с които разполага съответния потребител, и ще има значително по-добри възможности да получи достъп до други акаунти, до околните машини и дори може би да получи достъп на ниво администратор до системата. Въпреки тази заплаха, потребителските и администраторските акаунти със зле измислени или без никакви пароли все още се срещат често. А организациите с добре разработени и строго прилагана политика все още се срещат рядко.
Най-често срещаните уязвимости, свързани с паролите, са: (a) потребителски акаунти със слаби или несъществуващи пароли; (b) потребителски акаунти с общоизвестни или записвани в явен вид пароли; (c) системата или софтуерът създават администраторски акаунти с широкоизвестни слаби или несъществуващи пароли; и (d) слаби или широкоизвестни алгоритми за хешване на паролите и/или хешовете за потребителските пароли се съхраняват при слаба сигурност и всеки може да ги види.

Най-добрата защита срещу всички тези уязвимости е добре разработената политика по отношение на паролите, която включва: подробни инструкции към потребителите за създаване на силни пароли; ясни правила за потребителите, гарантиращи сигурността на паролите им и редовното им сменяне; създаване на практика на IT екипа за бърза замяна на слаби/несигурни/по подразбиране или широкоизвестни пароли и временно забраняване на неактивните или затваряне на неизползваните акаунти; проактивен и редовно използван процес за проверка на силата и сложността на всички пароли; отстраняване на ненужните потребителски акаунти по подразбиране и административни акаунти; редовна проверка на лог файла за достъп до системата/автентификация. Общото

ръководство за конфигуриране на Unix може да се намери на:
http://www.cert.org/tech_tips/unix_configuration_guidelines.html

U3.2 Засягани операционни системи
Всяка операционна система или приложение на всяка платформа, при които автентификацията на потребителите се извършва чрез потребителски идентификатор и парола.

U3.3 CVE/CAN номера
CAN-1999-0501, CVE-1999-0502, CAN-1999-1029, CVE-2001-0259, CVE-2001-0553, CVE-2001-0978, CVE-2001-1017, CVE-2001-1147, CVE-2001-1175, CAN-2004-0243, CAN-2004-0653
U3.4 Как да определите дали сте уязвими

1. Проверете дали има общи акаунти

- Ако съществуват общоизвестни потребителски акаунти, използвани съвместно от няколко лица или временни служители и/или паролите се записват в явен вид на бележки върху бюрата или мониторите, то в дадената мрежа има явни благоприятни възможности за всеки, който има физически достъп до тези системи.

2. Проверете дали има слаби пароли или слаба стратегия при определянето на паролите

- Конфигурирането на нови потребителски акаунти с една и съща начална парола или начална парола, която лесно може да бъде отгатната (дори ако началната парола трябва да се смени след първото влизане в системата) може да даде на нападателите възможност да получат достъп до една система.

- Определете дали хешовете на паролите се съхраняват в /etc/passwd или в /etc/shadow на всяка локална система. Файлът /etc/passwd трябва да може да се чете от всички потребители на мрежата, за да се извършва автентификация на потребителите. Но ако този файл съдържа също хешове на паролите, то всеки потребител, който има достъп до системата може да чете тези хешове и да се опита да ги разбие с програма за кракване на пароли. Файлът /etc/shadow е проектиран така, че да може да се чете само от администратора и трябва да се използва за съхраняване на хешове на пароли там, където го има. Ако вашите локални акаунти не са защитени от /etc/shadow, то рискът за вашите пароли е изключително висок. Повечето нови операционни системи ще използват по подразбиране /etc/shadow за съхраняване на хешовете за паролите, освен ако това не е отменено при инсталирането. Може би ще успеете да използвате алгоритъма MD5, за да хешвате паролите си; той е доста по-сигурен от стария кодиращ алгоритъм.

3. NIS обкръжения

- NIS е набор услуги за бази данни, които осигуряват информация за местоположението, наречена Maps, на други мрежови услуги, като

Network File System (NFS). Файловете, конфигуриращи NIS, са проектирани така, че съдържат хешовете на NIS паролите; в резултат хешовете могат да бъдат прочетени от всички потребители и паролите са изложени на риск. Такъв ще бъде случаят и при някои реализации на LDAP като мрежова услуга за автентификация. По-новите реализации на NIS, като NIS+ или LDAP, са общо взето по-строги при защитата на хешовете за паролите, освен ако това не е отменено при инсталирането. Но тези по-нови реализации се настройват и конфигурират по-трудно, което може да ви обезкуражи да ги използвате.

4. Общи съображения

- Дори ако хешовете за паролите са защитени от /etc/shadow или други реализации, паролите могат да бъдат отгатнати по други начини. Съществуват други слабости на паролите, включващи съществуването на неизползвани акаунти за потребители, които са напуснали дадена организация. Организациите обикновено са немарливи при затварянето на стари потребителски акаунти, освен ако не са възприети съответни процедури или администраторът не е особено старателен.

- Инсталирането по подразбиране (от производителя или от администратора) на операционни системи или мрежови приложения може да въведе широка гама от ненужни и неизползвани услуги. В много случаи несигурността относно нуждите на операционната система или приложението кара много производители или администратори да инсталират целия софтуер в случай, че се окаже необходим в бъдеще. Това значително опростява процеса на инсталирането, но и въвежда широка гама от ненужни услуги и акаунти, чиито пароли са по подразбиране/слаби/известни.

- Освен това, за паролите, изпращани по мрежата в явен текст, например чрез telnet, FTP или HTTP, съществува риск да бъдат подслушани (sniffed) от злонамерени лица. Използването на кодирана връзка, например чрез OpenSSH или SSL, може да скрие дадена парола от всеки, който шпионира мрежовите връзки.

U3.5 Как да се защитим

Най-добрата и най-подходящата защита срещу слаби пароли е силната политика, която осигурява подробни инструкции за добиване на добри навици по отношение на потребителските пароли, а също и изисква редовна проактивна проверка за целостта на паролите от страна на системните администратори при пълната подкрепа на организацията. Като насоки за добра политика по отношение на паролите трябва да се използват следните стъпки:

1. **Уверете се, че паролите са достатъчно силни.** При наличие на достатъчно хардуерни ресурси и достатъчно време, всяка парола може да бъде кракната чрез отгатване с груба сила. Програмите за кракване на пароли, с които боравят нападателите, използват методи, известни като речникови атаки. Тъй като методите за кодиране са широко известни, програмите за кракване просто сравняват кодираната форма на една парола с кодираните форми на всички думи в речника (на много езици),

със собствените имена и с често използвани пермутации от двете. Следователно една парола, която по някакъв начин прилича на дума (или думи на почти всеки от известните езици) е силно податлива на речникова атака. Много организации инструктират потребителите да създават пароли като включват в тях комбинации от буквено-цифрени и специални символи и потребителите много често го правят като вземат една дума (например, password) и преобразуват буквите в цифри или специални символи (например, pa$$w0rd). Такива пермутации не могат да осигурят защита срещу речникова атака: pa$$w0rd е също толкова лесно да бъде кракната, както и password.

Следователно една добра парола не може да се основава на дума или собствено име. Една политика на силни пароли трябва да подтиква потребителите да създават пароли на основата на нещо по-случайно, като фраза или по-дълго заглавие на книга или песен. Чрез преобразуване на една по-дълга фраза в низ (например, чрез вземане на първата буква от всяка дума във фразата (за препоръчване със смесени малки и главни букви) или чрез замяна на дума от началната фраза със специален символ, и/или чрез замяна на всички гласни в преобразуваната фраза с различни специални символи и т.н.), потребителите могат да създадат достатъчно дълги пароли-низове, които комбинират буквеноцифрови и специални символи по начин, който да направи кракването чрез речникови атаки много по-трудно. И ако началната фраза е лесна за запомняне, то същото ще важи и за получената от нея парола-низ.

След като на потребителите се дадат подходящи инструкции за създаване на добри пароли, трябва да се създадат и подробни процедури, които да гарантират спазването на тези инструкции. Най-добрият начин за изпълнение на тази задача е валидирането на паролите при смяната им от потребителя. Повечето дистрибуции на UNIX/LINUX могат да използват Npasswd като предна линия на проверката на съответствието на въвежданите пароли с възприетата политика по отношение на паролите. Системите, използващи PAM, могат също да бъдат разширени така, че да включват cracklib (библиотеките, които придружават Crack) за проверка на паролите при създаването им. Повечето нови системи, използващи PAM, могат също да бъдат настроени, така че да отказват приемането на лоши пароли, които не съответстват на определени правила.

Ако обаче паролите не могат да бъдат проверявани чрез използване на речниковите библиотеки, тъй като са въведени чрез използването на инструменти като Npasswd или използващи PAM библиотеки, то програмите за кракване трябва да бъдат стартирани от системния администратор в самостоятелен режим като част от редовна проактивна процедура. Обикновено най-добрият избор са инструменти като тези, които използват потенциалните нападатели. При UNIX/LINUX-базирана платформа те би трябвало да включват Crack и John the Ripper.

Моля отбележете: Никога не стартирайте скенер за пароли, дори на системи, на които имате административен достъп, без изрично и за предпочитане писмено разрешение от вашия началник/организация. Администратори, които са имали най-добри намерения, бяха уволнени затова, че са стартирали средства за кракване на пароли без да имат пълномощия за това. Това упълномощаване трябва да бъде във формата

на писмо, което да представлява част от политиката на организациите по отношение на силните пароли и да позволява редовни планирани проверки на паролите.

След като сте получили пълномощия да стартирате програми за кракване на вашата система, го правете редовно от физически защитена и обезопасена машина. Инструментите, инсталирани на тази машина трябва да бъдат недостъпни за всички, освен за упълномощения системен администратор. Потребители, чиито пароли са кракнати, трябва да бъдат уведомявани дискретно, като им се дават инструкции как да изберат по-добра парола. Като част от политиката на организацията по отношение на паролите, администраторите и ръководството трябва да разработят тези процедури за уведомяване съвместно, така че ръководството да може да дава насоки и оказва помощ, когато потребителите не желаят да спазват инструкциите.

Други възможни начини за защита срещу липса на пароли или слаби пароли и/или за изпълнение на процедурите, залегнали в политиката по отношение на паролите са (a) използването на алтернативна форма за автентификация като маркери (tokens) за автоматично създаване на пароли или биометрия. Тези методи са ефективни, когато имате проблем със слабите пароли и могат да бъдат използвани като алтернативен начин за автентификация на потребителите. Трябва да се отбележи, че някои маркери за генериране на пароли изискват създаването на процедури, които да гарантират, че те не са общодостъпни за неоторизирани потребители и че дори ако бъдат откраднати, те бързо ще започнат да получават отказ от системата. Биометрията е бързо развиваща се област, която зависи от вида на автентификацията (например, отпечатъци от пръсти или разпознаване на лицеви белези), част от технологията все още не е усъвършенствана и често могат да се получат грешки при автентификацията. (b) Съществуват много цялостни инструменти, създадени от различни производители, (безплатни и платени), които могат да подпомогнат провеждането на политика на добри пароли.

2. **Защитете силните пароли.** Ако съхранявате хешовете за паролите в /etc/passwd, обновете системата си така, че да използва /etc/shadow. Ако системата ви използва NIS или LDAP по такъв начин, че хешовете не могат да бъдат защитени, всеки (дори неавтентифицираните потребители) може да чете вашите хешове за паролите и да се опитва да ги кракне. Трябва да потърсите по-сигурни алтернативи на версиите на NIS и LDAP, които използвате. Докато тези несигурни приложения бъдат обезопасени/заменени, вие трябва да сложите подходящи права на файловете от гледна точка на сигурността и да стартирате проактивно кракване като редовна процедура срещу подобни хипотези. Обмислете използването на алгоритъма MD5 при хешването на пароли вместо кодиране.

   Дори ако паролите сами по себе си са силни, акаунтите могат да бъдат компрометирани, ако потребителите не пазят паролите си в тайна. Добрата политика по отношение на паролите трябва да включва подробни инструкции за потребителя, които да изискват той никога да не издава своята парола на друго лице, да не я записва там, където би могла да бъде прочетена от други, да обезопасява по подходящ начин всички

файлове, в които паролата се съхранява с цел автоматична автентификация, и ако разбере, че паролата му е открадната или известна на други лица, да уведоми незабавно системния администратор. Поставянето на срок на годност на паролите трябва да бъде задължително, така че всички пароли, които успеят да се промъкнат през тези правила да бъдат уязвими само за кратък период от време, като не трябва да се използват повторно стари пароли. Администраторите трябва да се убедят, че потребителите са предупредени за предстоящата смяна на паролата и имат няколко възможности да я сменят, преди тя да изтече. Когато се сблъскат неочаквано със съобщението "Your password has expired and must be changed," потребителите проявяват тенденция за избор на лоша парола.

3. Контролирайте строго акаунтите

По-надолу са описани серия от мерки, които ще гарантират по-строг контрол на акаунтите:

- Всички акаунти на услуги, административни акаунти или акаунти по подразбиране, които не се използват, трябва да бъдат забранени или, ако е възможно, изцяло премахнати.
- Всички акаунти на услуги, административни акаунти или акаунти по подразбиране, които се използват, трябва да получат нови и силни пароли веднага щом услугата или акаунта се инсталира или активира.
- Конфигурирайте новите потребителски акаунти със случайно генерирани начални пароли и принудете потребителите да ги сменят при първото влизане в системата.
- Проверявайте акаунтите на вашите системи редовно и проактивно и поддържайте главен списък (master list) на всички акаунти с описание на изискваните от тях услуги и предполагаемо предназначение.
- Редовно проверявайте дали акаунтите са необходими все още.
- Разработете строги процедури за идеално добавяне/премахване на оторизирани акаунти към/от списъка
- Използвайте строги процедури за премахване на акаунти, при напускане на служители или партньори, или когато акаунтите не са необходими повече.
- Поддържайте връзка с отдел Кадри на вашата организация, за да бъдете уведомявани за напускащите.
- Проверявайте главния списък редовно и планомерно за да се убедите, че не са добавени нови акаунти, и че неизползваните акаунти са изтрити.

Освен това, не забравяйте да проверявате акаунтите и паролите на спомагателните системи като маршрутизатори, превключватели и свързани към интернет дигитални принтери, копиращи машини и контролери на принтерите. Ако управлението на паролите при тях е слабо и някои потребителя използват една и съща парола за тях и за Unix system, това може да даде зелена светлина на злонамерените потребители.

Можете да намерите списък с паролите по подразбиране на продукти на различни производители на адрес: http://www.cirt.net/cgi-bin/passwd.pl

4. Кодирани влизания в системата

Използването и на най-силните пароли може да бъде спорно, ако паролите се изпращат по мрежата в явен текст. Ако това се случи, всеки, който има достъп до мрежовия трафик, може да види паролата във вида, в който е изпратена. Пример за програми и протоколи, които изпращат пароли в явен текст, са telnet, FTP, HTTP и Berkeley r-services.

За да се предотврати това, трябва да се използват кодирани програми и протоколи. При използване на кодирани програми и протоколи паролата не се изпраща по мрежата в явен текст, което затруднява много повече откриването й чрез традиционно подслушване (sniffing).

Съществуват много алтернативи на използването на изброените по-горе програми. OpenSSH може да замени telnet, FTP и Berkely r-services, а SSL може да се използва за осигуряване на кодиране на протокола HTTP.

5. Суперпотребителски акаунти

Административният (root) акаунт е най-привилегирования акаунт в една Unix система. Той няма ограничения по отношение на сигурността, което означава, че вие можете да изпълните всяка задача на системата. Това е АКАУНТА, до който един злонамерен потребител иска да получи достъп!

- Не позволявайте отдалечено влизане в системата с администраторски права. Един потребител трябва да използва командата su, за да получи администраторски достъп. Su заменя действителната uid (идентификация на потребителя) на акаунта с тази на друг акаунт, в този случай администраторския акаунт.
- Ако потребителят се нуждае само от някои привилегировани команди, използвайте sudo. Sudo (superuser do) позволява на един системен администратор да дава на определени потребители (или групи потребители) възможността да стартират някои (или всички) команди като администратор при записване на всички команди и аргументи. В този случай не е необходимо потребителят да въвежда администраторската парола.
- Използването на администраторския акаунт трябва да бъде ограничено до настройване на дадена система, приложения за настройване, специфично конфигуриране или критични ситуации.
- Ограничете броя на хората, които имат достъп до администраторските пароли. Те трябва да бъдат известни само на лицата, ангажирани с администрирането на тази система.

Допълнителна информация за Sudo може да бъде намерена на http://www.courtesan.com/sudo/, а помощна информация за Su може да бъде получена чрез изписване на man su на командния ред.

6. Общи акаунти

Общите акаунти често се използват в етапа на разработка за разрешаване на едно приложение да комуникира с друго приложение или с база данни. Достъпът на производителя е друга ситуация, при която често се използват общи акаунти. От значение е при управлението на тези акаунти да се полагат надлежни грижи, за да се поддържа отчетност на извършените действия.

Общи положения

- Първо, използвайте общите акаунти в краен случай. Ако един потребител се нуждае от чест или продължителен достъп, на него трябва да му се създаде индивидуален акаунт.
- Ако е необходим общ акаунт (множество отделни лица се нуждаят от достъп още при производителя, приложенията се нуждаят от автентифициран достъп и т.н.), едно лице с нсеобходимия авторитет трябва да носи отговорност за всички действия, извършвани с този акаунт.

Акаунти на приложенията
Не кодирайте твърдо паролите в самите приложения.
Осигурете подходяща защита на информацията за акаунтите и паролите (кодирани файлове, разрешения за четене и т.н.)

Достъп на производителя
- Снабдете се със споразумение с подписано съгласие за поддръжка на акаунта, в което производителят поема отговорност за действията, извършени чрез акаунта.
- Определете пазител на паролата на производителя, който да отговаря за управлението на паролите на производителя.
- Съхранявайте паролите на акаунтите за поддръжка в пликове и осигурете достъп при поискване от страна на производителя.
- Когато е възможно, използвайте двуетапна автентификация.
- Когато е възможно или необходимо, карайте пазителят на паролите на производителя да сменя паролите на акаунтите за поддръжка след използването им. Тази фаза не е строго необходима, ако се използва двуетапна автентификация.
- Проверявайте дали пликовете, които съдържат паролите, не са били обработвани по някакъв начин.
- Извършвайте редовни проверки на дейността.

7. Проверки за проследяване

Извършването на проверка за проследяване на дейността на потребителите е важна част от обезопасяването на една система. Записването на всички опити за автентификация, независимо от това дали са успешни или не, ще ви помогне при определяне на това, което се е случило с вашите системи. Правилното записване на дейността на su и sudo също е важно, тъй като то ще ви покаже кой се е опитвал да изпълнява дейности чрез разрешения (permissions), които са различни от необходимите за тези дейности.

Честото преглеждане на проверките за проследяване може да ви помогне да откриете потенциална злоупотреба с привилегии или друг вид анормална дейност на вашите системи.

За повече информация относно всички аспекти на записването на извършваните дейности можете да погледнете на http://www.loganalysis.org/

обратно в началото ^

U4 Системи за контрол на версиите

U4.1 Описание

Системите за контрол на версиите осигуряват средства за управление на различните версии на документи или сорсови кодове и улесняват едновременната работа на много потребители върху един и същ набор файлове.

Подобни системи са от значение при управлението на всеки проект за разработка на софтуер, корпоративни или правни документи, тъй като те осигуряват не само решение за централно съхранение, но и позволяват намирането на различните версии.

Concurrent Versions System (CVS) е най-популярната система за контрол на сорсови кодове, която се използва понастоящем в Linux/Unix обкръженията. Много проекти с отворен код разрешават "анонимен" достъп до CVS хранилищата. Едно CVS хранилище може да бъде конфигурирано за отдалечен достъп чрез протокола "pserver", който по подразбиране се стартира на порт 2401/tcp. Сървър, конфигуриран по този начин, съдържа следните уязвимости:

A)Купообразно (heap-based) препълване на буфер, което може да бъде задействано чрез специално създадени "Entry-Lines". Един нападател може да използва препълването на буфер за изпълнение на произволен код на CVS сървъра. Код на експлойт за CVS сървъри, стартирани на Linux, FreeBSD и Solaris платформи, беше публикуван в пощенските списъци, имащи отношение към сигурността. Заслужава си да се отбележи, че всяко хранилище, конфигурирано за "анонимен достъп", е потенциално уязвимо.

B)Уязвимостите в реализацията на други команди и функции могат да бъдат използвани от автентифициран нападател с цел постигане на отказ от обслужване от страна на CVS сървъра, или изпълнение на произволен код на CVS сървъра. Някои от тези недостатъци могат да бъдат използвани от "анонимните" потребители.

Subversion е друга система за контрол на версиите за Linux, която печели популярност. Проектът бе стартиран с цел проектиране на по-добра система от CVS. Достъп до хранилището на Subversion може да бъде получен чрез протокола"svn", ако хранилището поддържа "svnserve". По подразбиране сървърът svn се стартира на порт 3690/tcp. Сървърът съдържа следните уязвимости:

- Купообразно (heap-based) препълване на буфер, което може да бъде използвано от неавтентифициран нападател за изпълнение на произволен код.
- Стеково (stack-based) препълване, което може да бъде задействано чрез специално създадена "get-dated-rev" svn команда. Ако сървърът е конфигуриран за анонимен достъп, един неавтентифициран нападател може да стартира на сървъра произволен код. В Интернет бяха публикувани множество експлойти за този недостатък.

Ако един нападател получи достъп, той не само може да "зарази" сорсовите файлове със задни вратички и бъгове, които след внедряването на софтуера в практиката ще доведат до голям брой компрометирани системи, но това може да му бъде полезно и за обвиняване на добросъвестен служител в противозаконни деяния чрез "Identity Spoofing" (подправяне на самоличност).

U4.2 Засягани операционни системи

Linux, FreeBSD, AIX, HP-UX, Solaris, SGI и потенциално всички останали, на които са стартирани CVS и/или Subversion.

U4.3 CVE/CAN номера
CAN-2004-0396
CAN-2004-0414
CAN-2004-0416
CAN-2004-0417
CAN-2004-0418
CAN-2004-0397
CAN-2004-0413

U4.4 Как да определите дали сте уязвими
Ако вашият CVS сървър е конфигуриран за отдалечен достъп чрез протокола "pserver" и вие работите с някоя от следните версии на софтуера CVS, то вашият CVS сървър е уязвим -
CVS стабилна версия (stable release) 1.11.16 и по-ниските
CVS характеристична версия (feature release) 1.12.8 и по-ниските.
Можете да разберете коя е версията на CVS като стартирате командата "cvs ver".

Ако вашият Subversion сървър е конфигуриран за отдалечен достъп чрез протокола "svn" и вие работите с версия, по-ниска от 1.0.5, вашият сървър е уязвим.

U4.5 Как да се защитим

За CVS сървър:
- Уверете се, че вашият софтуер CVS е обновен до последното ниво на кръпките. Сорсовият код за най-новия софтуер може да бъде свален от: https://www.cvshome.org/ .
- Конфигурирайте CVS сървъра да използва за отдалечен достъп протокола SSH вместо протокола pserver. Освен това, стартирайте CVS сървъра в "chroot" обкръжение. Подробни инструкции можете да намерите на: http://www.netsys.com/library/papers/chrooted-ssh-cvs-server.txt
- Ако достъп до CVS хранилището се получава в мрежата на компанията/корпорацията, блокирайте порт 2401/tcp на мрежовия периметър.
- Уверете се, че публикуваните експлойти са неефективни срещу вашия CVS сървър. Публикуваните експлойти можете да намерите на: http://www.k-otik.com/exploits/05212004.CVS_Linux.c.php http://www.k-otik.com/exploits/05212004.CVS_Solaris.c.php.
- Опитайте се да хоствате CVS сървъра за анонимен достъп само за четене на самостоятелна система. За предпочитане в демилитаризираната зона (DMZ).

За Subversion сървър:
- Уверете се, че вашият Subversion сървър е обновен до последната версия на софтуера. Последната версия можете да свалите от: http://subversion.tigris.org
- Конфигурирайте Subversion хранилищата така, че да бъдат достъпни чрез webDAV вместо да използвате протокола "svn".

- Ако достъп до Subversion хранилището се получава в мрежата на компанията/корпорацията, блокирайте порт 3690/tcp на мрежовия периметър.
- Уверете се, че публикуваните експлойти са неефективни срещу вашия Subversion сървър. Публикуваните експлойти можете да намерите на: http://www.metasploit.com/projects/Framework/modules/exploits/svnserve_date.pm
  http://www.k-otik.com/exploits/06112004.subexp.c.php.
- Опитайте се да хоствате Subversion сървъра за анонимен достъп само за четене на самостоятелна система. За предпочитане в демилитаризираната зона (DMZ).

U4.6 Препратки
CERT Advisory (съвети)
http://www.kb.cert.org/vuls/id/192038

SecurityFocus BIDs
http://www.securityfocus.com/bid/10384
http://www.securityfocus.com/bid/10499
http://www.securityfocus.com/bid/10386
http://www.securityfocus.com/bid/10519

Страница на CVS
http://www.cvshome.org

Страница на Subversion
http://subversion.tigris.org

Пощенски списъци, имащи отношение към сигурността
http://www.securityfocus.com/archive/1/363775/2004-05-17/2004-05-23/0
http://www.securityfocus.com/archive/1/365541/2004-06-07/2004-06-13/0
http://www.securityfocus.com/archive/1/363781/2004-05-17/2004-05-23/0
http://archives.neohapsis.com/archives/bugtraq/2004-06/0180.html

обратно в началото ^

U5 Обслужване на транспортирането на пощата

U5.1 Описание на уязвимостта
Електронната поща е едно от най-широко използваните приложения в Интернет, както и SMTP е един от най-старите протоколи. Агентите за транспортиране на пощата (MTA) са сървърите, отговарящи за пренасянето на пощата от изпращача до съответния получател(и) обикновено чрез протокола SMTP, който може да бъде кодиран с SSL на необезопасените портове с TLS, ако и двата края го поддържат. Sendmail е най-широко използваният MTA на основата на Unix, макар че с течение на времето проблемите, свързани със сигурността му, и сложното конфигуриране на този достопочтен софтуер предизвикаха появата на няколко популярни алтернативи, включващи Qmail, Courier-MTA, Postfix, и Exim.

Като се има предвид широкото използване на електронната поща, не е учудващо, че тази система е атакувана постоянно от вируси, червеи и по-персонифицирани нападатели с човешки облик. Макар че повечето такива атаки се фокусират върху най-често използваните пощенски клиенти, MTA са също много често срещан вектор на атака. Повечето от уязвимостите, използвани

понастоящем срещу тези сървъри, могат да бъдат разпределени на следните категории:

- Атаки срещу незакърпени системи, включително надхвърляне възможностите на буфери, heap препълвания и т.н.
- Злоупотреба с отворени възможности (relays) за препращане на писма, любимото средство на спамерите.
- Използване на друга нерелейна лоша конфигурация, като базата данни с потребителски акаунти за целите на спама или социалното инженерство (или дори атаки срещу пощенски клиенти).

Можете да бъдете сигурни, че ако в една мрежа е стартиран уязвим MTA, той ще бъде открит и използван почти незабавно. За щастие можем драстично да намалим риска за дадена система за електронна поща като предприемем някои прости стъпки по време на инсталирането и и продължим редовно да изпълняваме практитическите мерки за поддръжка. Тези MTA, които стриктно следват RFC, са най-подходящи, тъй като по-голямата част от софтуера за спам не следва RFC.

U5.2 Засягани операционни системи

Почти всички версии и дистрибуции на Unix пристигат с един от MTA, изброени по-горе. Макар че много производители на Unix през последните години подобриха значително отношението си към сигурността при инсталациите по подразбиране, трябва да се смята, че всяка система с MTA, която не е закърпена и не се поддържа и/или се стартира с конфигурация по подразбиране, е уязвима.

U5.3 CVE/CAN Номера

Sendmail

CVE-1999-0047, CVE-1999-0095, CVE-1999-0096, CVE-1999-0129, CVE-1999-0131,CVE-1999-0203, CVE-1999-0204, CVE-1999-0206, CVE-1999-1109, CVE-2000-0319,CVE-2001-0653, CVE-2001-1349, CVE-2002-0906

CAN-1999-0098, CAN-1999-0163, CAN-2001-0713, CAN-2001-0714, CAN-2001-0715,CAN-2002-1165, CAN-2002-1278, CAN-2002-1337, CAN-2003-0161, CAN-2003-0285,CAN-2003-0694

Qmail

CVE-2000-0990, CAN-2003-0654

Courier-MTA

CVE-2002-0914, CVE-2002-1311, CVE-2003-0040, CVE-2004-0224, CVE-2004-0777

Exim

CVE-2001-0889

CAN-2003-0743,CAN-2004-0399,CAN-2004-0400

Postfix

CAN-2003-0468

U5.4 Как да определите дали сте уязвими

Проверете нивото на кръпките
За да определите дали вашата система е уязвима, първата ви стъпка трябва да включва определяне на нивото на кръпките на вашия MTA и откриване дали за това ниво съществуват уязвимости или не. Като използвате CVE (http://cve.mitre.org/), вие ще можете да определите уязвимостите, свързани с вашия MTA.

Sendmail
Sendmail притежаваше в миналото голям брой уязвимости. Тези уязвимости често се дължаха на нейната сложност. Те превърнаха Sendmail в една от най-злонамерено използваните услуги в Интернет.

Всяка остаряла или незакърпена версия на софтуера вероятно е уязвима.

За да определите версията на Sendmail, използвайте следната команда:
echo \$Z | sendmail -bt -d

Не вярвайте сляпо на номера на версията, връщан от демона, защото той просто го чете от текстов файл в системата, който може да не е обновен правилно.

За да определите дали версията, която използвате е актуална, проверете кое е текущото издание на версията на Sendmail: http://www.sendmail.org/current-release.html

Exim
Exim е друг популярен MTA с пълни функционални възможности. В миналото той е имал някои уязвимости.

За да определите версията наExim, използвайте следната команда:
exim -bV

За да определите дали версията, с която работити, е текущата, проверете текущото издание (release) на версията на Exim на:
http://www.exim.org/version.html

Qmail
Qmail е сигурен MTA, който в миналото е имал някои уязвимости. Той е и един от най-популярните MTA след Sendmail.

Няма лесен и надежден начин за откриване на версията на Qmail освен проверка на версията в man страниците чрез използване на GNU grep:

```
grep -A1 version /var/qmail/man/man7/qmail.7
```

Qmail притежава множество усъвършенствания, разработени от потребителите, което силно усложнява идентифицирането на уязвимостите.

Можете да откриете кръпките, препоръчвани за Qmail на http://www.qmail.org/top.html#patches, и можете да намерите пакет (чието име е

netqmail), който съдържа qmail и препоръчваните кръпки на:
http://www.qmail.org/netqmail/

Courier-MTA
Courier-MTA е стриктна RFC система за пощенски сървър, която поддържа Maildir+, maildrop и MySQL, Postgresql и LDAP за съхраняване на акаунти на прякори (alias) и потребители.

За да откриете версията му, използвайте командата "showmodules".

Бележки по отношение на сигурността и последна версия има на
http://www.courier-mta.org

Postfix
Подобно на Qmail, Postfix е сигурен MTA и в миналото е имал още по-малко уязвимости. Последните версии притежават усъвършенствани възможности за контрол на достъпа, инспектиране на съдържанието и ограничаване на скоростта, така че преминаването към по-висока версия е добра идея, дори ако версията, която използвате, не е уязвима.

За да определите версията на Postfix, използвайте следната команда:
postconf -d mail_version

За да определите дали версията, с която работите, е текущата, проверете текущото издание (release) на версията на Postfix на:
ftp://ftp.porcupine.org/mirrors/postfix-release/index.html

- **Проверете състоянието на вашия relay (препредавател, възможност за препредаване на пощата)**

Какво представлява отворения relay
Препредаването на пощата е основната функция на един MTA, но погрешните конфигурации могат да превърнат вашия MTA в отворен relay. Това се случва, когато MTA препредава пощенско съобщение, при което нито подателят, нито получателят са локални потребители. С други думи, подателят и получателят не са част от домейна и MTA няма нищо общо с транзакцията. При нормални обстоятелства няма причина писмото да минава през MTA.

***Проверете дали вашитя MTA не е отворен* relay**
Проверката дали вашият MTA не е отворен relay е едно от най-важните неща, които трябва да се свършат след проверката на нивото на кръпките му. Тя ще ви позволи да проверите дали някой не изпраща нежелана комерсиална поща (SPAM) през вашия MTA. Следните средства ще ви помогнат да осъществите това:
http://www.abuse.net/relay.html
http://www.cymru.com/Documents/auditing-with-expect.html

*К**акво представлява списъка на черните дупки в реално време?***
Списъкът на черните дупки в реално време(RBL) е списък с IP адреси на сървъри, чиито собственици отказват да спрат разпространението на SPAM по Интернет. Тези списъци се използват от администраторите на пощата, за да отказват връзки към своите MTA, идващи от тези известни спамъри.

Как да откриете дали вашият пощенски сървър не е описан в RBL
Ако откриете, че вашият пощенски сървър е в един от тези списъци, има вероятност той да е отворен relay, освен ако не сте променили наскоро конфигурацията си. Възможно е и някой от вашите действителни потребители да злоупотребява с вашия сървър и да изпраща SPAM или "newsletters" (писма с новини). Това също може да доведе до появата ви в RBL. Можете да потърсите IP на вашия пощенски сървър тук, за да проверите дали не фигурира в списъците:
http://www.mail-abuse.com/support/lookup.html
http://www.ordb.org/

Имайте предвид, че съществуват много RBL и че тази справочна страница включва само най-популярните от тях.

- **Проверка на вашия пощенски сървър**

Проверяването на вашия пощенски сървър ще ви позволи да идентифицирате уязвимостите, които могат да бъдат използвани от злонамерени лица за извършване на непозволени действия на/чрез вашия пощенски сървър.

Nessus
Nessus е безплатен и мощен отдалечен скенер за уязвимости, който включва специфичен плъгин за SMTP сървъри. Той ще ви позволи да идентифицирате уязвимостите на MTA по бърз и ефикасен начин.

Можете да откриете Nessus и неговите плъгини на http://www.nessus.org

SARA
Sara е съкращение на Security Auditor's Research Assistant (помощник при проверки за изследване на сигурността). Той е средство за анализ на сигурността, като Топ 20 на уязвимостите на SANS са включени в списъка на сканираните уязвимости.

SARA може да се намери на http://www-arc.com/sara/

U5.5 Как да се защитим
За да защитите вашия пощенски сървър, трябва да предприемете следните стъпки, които са разделени на две части: Общи препоръки, които са независими от пощенския сървър, и Специфични препоръки, ориентирани към пощенските сървъри Sendmail, Qmail и Postfix:

2.Общи препоръки

- Вземете решение дали е необходимо да работите с MTA, и дали той трябва да бъде обществено достъпен.
- Забранете пощенския сървър на всяка система, която не е специално проектирана и оторизирана да бъде пощенски сървър. Трябва да се създадат процедури, които да предотвратят повторното разрешаване на тези възможности. За да усилите ефекта, приложете политика с използване на защитни стени.
- Инсталирайте всички кръпки от производителите или обновете вашия пощенски сървър до последната му версия.

- Използвайте отделен вътрешен MTA за обработка на вътрешния пощенски трафик.
- Ограничете нивото на привилегиите, с които работи MTA, или го стартирайте в chrooted ограничение, ако това е възможно.
- Прочетете цялата документация на пощенските сървъри, и се запишете в съответните пощенски списъци, ако има такива.

Защита срещу препредаване на пощата

За да предотвратите злоупотребата с вашия пощенски сървър от страна на спамери, той трябва да бъде конфигуриран така, че да не препредава поща, която не идва от проверени мрежи и домейни:

Sendmail
Ако трябва да стартирате Sendmail в режим демон, уверете се, че вашата конфигурация е направена така, че да препредава пощата правилно и само за системи от вашето обкръжение. Прегледайте http://www.sendmail.org/tips/relaying.html и http://www.sendmail.org/m4/anti_spam.html, които ще ви помогнат при правилното конфигуриране на вашия сървър. От Sendmail 8.9.0 нагоре, свободното препредаване на пощата беше забранено по подразбиране. Много производители на операционни системи, обаче, отново го разрешиха в конфигурациите по подразбиране. Ако използвате версия на Sendmail, закупена заедно с операционната система, вземете специални мерки, за да гарантирате, че вашият сървър не се използва за препредаване на пощата.

Qmail
Qmail предлага добра документация относно селективното препредаване на пощата и помощ за забраняване на препредаването на пощата от вашата система. Прегледайте http://www.lifewithqmail.org/lwq.html#relaying

Courier-MTA
Сам по себе си затворен relay, Courier предоставя помощ относно това, как да се разреши препредаването на пощата за някои мрежи или IP адреси. Освен това, за да осигури препредаване на пощата, той използва SMTP автентификация. Http://www.courier-mta.org – раздел FAQ.

Exim
Exim също е снабден с подробни инструкции за начините за предотвратяване на препредаването на пощата.
http://www.exim.org/howto/relay.html

Postfix
При Postfix има някои стъпки, които ще ви помогнат да ограничите достъпа и да контролирате препредаването на пощата. Препредаването на пощата ще бъде разрешено само за хостовете и мрежите, изброени в ,параметъра 'mynetworks'. Прегледайте http://www.postfix.org/SMTPD_ACCESS_README.html

3.Други подробности, специфични за отделните приложения

A)Допълнителна информация за това, как да конфигурирате и използвате Sendmail по по-сигурен начин, можете да получите на:
http://www.sendmail.org/secure-install.html
http://www.sendmail.org/m4/security_notes.html
http://www.sendmail.org/~gshapiro/security.pdf

B)За да предотвратите излагането на опасност на цялата ви система от един компрометиран Postfix, ограничете го така, че да работи като непривилегирован потребител в директорията chroot()ed. За конфигуриране на Postfix погледнете
http://www.linuxjournal.com/article.php?sid=4241

C)Следващата връзка е пример за това, как да конфигурирате вашия MTA да използва черните дупки
http://www.ordb.org/faq/#usage

D)Courier-MTA е направен така, че да поддържа RBL списъци и да осигурява първоначален списък на rbl-сървърите в конфигурационния файл esmtpd.

E)Postfix ссъдържа много възможности за ограничаване на UCE; информация за тях можете да намерите на:
http://www.securitysage.com/antispam/intro.html

обратно в началото ^

U6 Simple Network Management Protocol (SNMP)

U6.1 Описание

The Simple Network Management Protocol (SNMP) е широко използван за отдалечено наблюдение и конфигуриране на почти всички видове съвременни устройства, използващи TCP/IP. Макар че SNMP е “вездесъщ” при мрежовите платформи, той се използва най-често като метод за конфигуриране и управление на устройства като принтери, рутери, превключватели, точки за достъп и за осигуряване на вход на услуги за мониторинг на мрежата.

Комуникацията чрез Simple Network Management представлява обмен на различни видове съобщения между SNMP управляващи станции и мрежовите устройства, на които е стартирано това, което сме свикнали да наричаме програми-агенти (agent software). Методът, по който се обработват тези съобщения, и механизмът за автентификация, който стои зад тази обработка, имат значителни уязвимости, които могат да бъдат използвани злонамерено.

Уязвимостите, които произтичат от метода, по който SNMP версия 1 управлява и улавя съобщения, са описани подробно в CERT Advisory CA-2002-03. Съществуват редица уязвимости в начина, по който съобщенията от тип “trap and request” се обработват и декодират от управляващи станции и агенти.

Тези уязвимости не са характерни само за някоя специфична версия на SNMP, а засягат множество дистрибуции на SNMP, предлагани от различни продавачи. Резултатът от действията на нападателите, които използват тези уязвимости, може да бъде разположен навсякъде в диапазона между отказ от обслужване и нежелано конфигуриране и управление на вашите машини, работещи със SNMP.

Вътрешният механизъм за автентификация на по-старите версии на SNMP също представлява значителна уязвимост. SNMP версии 1 и 2 използват като единствен механизъм за автентификация един некодиран "community string". Липсата на кодиране сама по себе си е достатъчно неприятна, но използваният

по подразбиране от голямото множество SNMP устройства “community string” е "публичен", като само някои разумни продавачи на мрежово оборудване са променили низа на "частен" за по-конфиденциалната информация. Нападателите могат да използват тази уязвимост на SNMP, за да преконфигурират или изключват отдалечено устройствата. Подслушването на SNMP трафика може да разкрие много неща за структурата на вашата мрежа, както и за системите и устройствата, свързани към нея. Нападателите, които се опитват да проникнат в чужди компютри, използват тази информация за да набелязват цели и да планират атаки.

Повечето продавачи разрешават SNMP версия 1 по подразбиране, а мнозина не предлагат продукти, способни да използват моделите за сигурност на SNMP версия 3, които могат да бъдат конфигурирани да използват подобрени методи за автентификация. Въпреки това, съществуват безплатни заместители, които осигуряват поддръжка на SNMP версия 3 чрез GPL или BSD лицензи.

SNMP не е предназначен само за UNIX; той е широко използван при Windows за мрежово оборудване, безжични точки за достъп и мостове, принтери и вградени устройства. Но повечето от наблюдаваните досега атаки, свързани със SNMP, бяха осъществени на UNIX системи с лоши SNMP конфигурации. SNMP трафикът се предава в явен вид, така че използването му в случай, че трафикът може да бъде наблюдаван, трябва да бъде внимателно обмислено.

За да даде повече сведения за уязвимостите на SNMP, CERT CC е разработил обширен раздел Най-често задавани въпроси (FAQ) за SNMP, които можете да намерите на http://www.cert.org/tech_tips/snmp_faq.html.

U6.2 Засягани операционни системи

Почти всички UNIX и Linux системи идват с инсталиран SNMP, който често е разрешен по подразбиране. Повечето други използващи SNMP мрежови устройства и операционни системи също са уязвими.

U6.3 CVE/CAN номера

CVE-1999-0294	CVE-1999-0472	CVE-1999-0815	CVE-1999-1335	CVE-2000-0221
CVE-2000-0379	CVE-2000-0515	CVE-2000-1058	CVE-2001-0236	CVE-2001-0487
CVE-2001-0514	CVE-2001-0564	CVE-2001-0888	CVE-2002-0017	CVE-2002-0069
CVE-2002-0302	CAN-1999-0186	CAN-1999-0254	CAN-1999-0499	CAN-1999-0516
CAN-1999-0517	CAN-1999-0615	CAN-1999-0792	CAN-1999-1042	CAN-1999-1126
CAN-1999-1245	CAN-1999-1460	CAN-1999-1513	CAN-2000-0147	CAN-2000-0885
CAN-2000-0955	CAN-2000-1157	CAN-2000-1192	CAN-2001-0046	CAN-2001-0352
CAN-2001-0380	CAN-2001-0470	CAN-2001-0552	CAN-2001-0566	CAN-2001-0711
CAN-2001-0840	CAN-2001-1210	CAN-2001-1220	CAN-2001-1221	CAN-2001-1262
CAN-2002-0012	CAN-2002-0013	CAN-2002-0053	CAN-2002-0109	CAN-2002-0305
CAN-2002-0478	CAN-2002-0540	CAN-2002-0812	CAN-2002-1048	CAN-2002-1170
CAN-2002-1408	CAN-2002-1426	CAN-2002-1448	CAN-2002-1555	CAN-2003-0137
CAN-2003-0935	CAN-2003-1002	CAN-2004-0311	CAN-2004-0312	CAN-2004-0576
CAN-2004-0616	CAN-2004-0635	CAN-2004-0714		

U6.4 Как да определите дали сте уязвими
Можете да проверите дали SNMP е стартиран на свързаните към мрежата устройства като стартирате сканираща програма или като проверите ръчно.

- SNMPing – Вземете безплатния инструмент за сканиране SNMPing от института SANS на http://www.sans.org/alerts/snmp/.
- SNScan - Foundstone създаде друг лесен за използване инструмент за сканиране на SNMP, наречен SNScan, който можете да получите от http://www.foundstone.com/knowledge/free_tools.html.
- Nessus – Скенер за оценка на сигурността с отворен сорс можете да намерите на http://www.nessus.org

Ако не можете да използвате никой от гореописаните инструменти, вие трябва да проверите ръчно дали на вашите системи е стартиран SNMP. Прегледайте документацията на вашата операционна система, за да разберете точно как да определите коя е конкретната реализация на SNMP, но базовата услуга може обикновено да се определи чрез изпълнение на grep за "snmp" в списъка на процесите, или чрез претърсване на услугите, стартирани на портове 161 или 162. (Средството lsof tool може да се окаже полезно при присвояване (map) на портове на процесите).

Откриването на стартиран SNMP вероятно е достатъчно доказателство, че сте уязвим спрямо широкоразпространените грешки от типа "trap and request" обработка. За допълнителна информация моля прегледайте CERT Advisory CA-2002-03.

Ако SNMP е стартиран и някое от тези условия е налице, вие вероятно имате пропуск или уязвимост, свързана с низ по подразбиране или такъв, който лесно може да бъде отгатнат:
1. Празни SNMP "community" имена или такива по подразбиране.
2. SNMP "community", които лесно могат да бъдат отгатнати.
3. Скрити SNMP "community" низове.

Моля разгледайте http://www.sans.org/resources/idfaq/snmp.php за информация относно начина за определяне на наличието на тези условия.

U6.5 Как да се защитим
Уязвимости от типа "trap and request" обработка:
1. Забранете SNMP, ако той не ви е абсолютно необходим.
2. Използвайте навсякъде, където е възможно, потребителския модел на сигурност на SNMP версия 3 с автентификация на съобщенията и възможност за кодиране на данните на протокола.
3. Ако се налага да използвате SNMP версия 1 или версия 2, уверете се, че използвате най-новата закърпена версия, предлагана от вашия продавач. Добра отправна точка за получаване на информация, специфична за отделните продавачи, е Приложение А на CERT Advisory CA-2002-03.
4. Филтрирайте SNMP (порт 161 TCP/UDP и 162 TCP/UDP) във входните точки към вашите мрежи, освен ако не е абсолютно необходимо да отворите и управлявате устройствата външно.
5. Използвайте хост базиран контрол на достъпа до вашите системи с SNMP агенти. Макар че тази възможност може да бъде ограничена от способността на операционната система да използва SNMP агент, може да се осъществи контрол над системите, от които вашите агенти ще приемат заявки. При повечето UNIX

системи това може да се осъществи чрез TCP-Wrappers или конфигурация Xinetd. За блокиране на нежеланите SNMP заявки може да се използва защитна стена, изградена с помощта на агент за филтриране на пакети на хоста.

Уязвимости, свързани с низ по подразбиране, или такъв, който лесно може да бъде отгатнат:
1. Забранете SNMP, ако той не ви е абсолютно необходим.
2. Използвайте навсякъде, където е възможно, потребителския модел на сигурност на SNMPv3 с автентификация на съобщенията и възможност за кодиране на данните на протокола.
3. Ако се налага да използвате SNMP версия 1 или версия 2, за "community" имена използвайте същите правила както при паролите. Уверете се, че са трудни за отгатване или кракване и че се сменят периодично.
4. Валидирайте и проверявайте "community" имена като използвате snmpwalk. Допълнителна информация можете да намерите на http://www.zend.com/manual/function.snmpwalk.php. Добър материал, посветен на този инструмент можете да намерите на http://www.sans.org/resources/idfaq/snmp.php.
5. Филтрирайте SNMP (порт 161 TCP/UDP и 162 TCP/UDP) във входните точки на вашите мрежи, освен ако не е абсолютно необходимо да проверявате или управлявате външно устройствата. След това, ако е възможно, конфигурирайте входния филтър, така че да разрешава SNMP трафик само между доверени подмрежи.
6. Направете MIB разрешени само за четене там, където е възможно. Допълнителна информация можете да намерите на http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#xtocid210315

обратно в началото ^

U7 Open Secure Sockets Layer (SSL)

U7.1 Описание

Библиотеката OpenSSL с отворен сорс осигурява криптографска поддръжка на приложенията, които си комуникират по мрежата. Тя е много широко разпространена реализация на протокола SSL/TLS и се използва от голям брой производители. Най-известният пример за приложение, което използва тази библиотека, е уеб сървърът Apache (за поддържане на сигурни http връзки). Много от често използваните POP3, IMAP, SMTP и LDAP сървъри също имат баизрани на OpenSSL копия.

Тъй като библиотеката OpenSSL е интегрирана в голям брой приложения, всяка уязвимост в библиотеката може да бъде използвана чрез тези приложения. Например, публично са известни множество експлойти, които могат да компрометират Apache сървъри, компилирани с някои версии на библиотеката. Същите експлойти, обаче, могат лесно да бъдат модифицирани така, че да компрометират sendmail, openLDAP, CUPS, или други приложения, разрешаващи OpenSSL.

В библиотеката OpenSSL бяха открити множество уязвимости. Най-сериозни от тях са 5 уязвимости, описани в CAN-2002-0655, CAN-2002-0656, CAN-2002-0557, CAN-2002-0659 и CAN-2003-0545. Тези уязвимости могат да бъдат използвани отдалечено по злонамерен начин за изпълнение на произволен код с нивото на привилегии на приложенията, използващи библиотеката OpenSSL. В някои случаи, както при 'sendmail', успешното им злонамерено използване може да ги зарадва и с "root" привилегии.

U7.2 Засягани операционни системи

Всяка UNIX или LINUX система, работеща със следните версии на OpenSSL, е затегната (a) 0.9.7c или по-ниска (b) 0.9.6l или по-ниска. Това може да засяга дистрибуционни пакети на Linux като Apache, CUPS, Curl, OpenLDAP, Stunnel, Sendmail и всички други приложения, базирани на OpenSSL.

U7.3 CVE/CAN номера

CVE-1999-0428, CVE-2001-1141, CAN-2000-0535, CAN-2002-0655, CAN-2002-0656, CAN-2002-0557, CAN-2002-0659, CAN-2003-0078, CAN-2003-0131, CAN-2003-0147, CAN-2003-0543, CAN-2003-0544, CAN-2003-0545, CAN-2003-0851, CAN-2004-0079, CAN-2004-0081, CAN-2004-0112, CAN-2004-0607

U7.4 Как да определите дали сте уязвими

Проверете резултата от изпълнението на командата 'openssl version'. Ако версията не е 0.9.7d или 0.9.6m, системата е уязвима.

U7.5 Как да се защитим

1. Обновете се до най-новата версия на OpenSSL. Ако OpenSSL е инсталиран заедно с операционната система, инсталирайте последните кръпки, предоставяни от производителя. Отбележете, че в някои случаи за разрешаване на обновените библиотеки може да се наложи прекомпилиране и/или промяна на линковете на приложенията.

2. Ако е възможно, помислете за използването на ipfilter / netfilter или други инструменти, изпълняващи функциите на защитни стени, за да поставите ограничения за системите, които могат да се свързват със сървър с разрешена OpenSSL. Отбележете, че един от най-често срещаните примери за използване на OpenSSL, е за обезопасяване на HTTP трафика по обществения Интернет за електронна търговия, където ограничаването на хостовете вероятно е неприложимо.

обратно в началото ^

U8 Лоша конфигурация на корпоративните услуги NIS/NFS

U8.1 Описание

Network File System (NFS) и Network Information Service (NIS) представляват две важни услуги, често използвани при UNIX сървърите. NFS е услуга, създадена първоначално от Sun Microsystems и предназначена да споделя ("експортира") файлови системи/директории и файлове по мрежата между UNIX системи. От друга страна, NIS представлява набор услуги, които работят като обслужване на свободно разпределени бази данни, за осигуряване на информация за местоположението, наречена карти (Maps), на други мрежови услуги, като NFS. Най-често създаваните карти са свързани с passwd и груповите файлове, които се използват от там за централизиране на автентификацията на потребителите. Файлът hosts е друга често използвана цел за NIS.

С течение на времето бяха откривани различни проблеми, свързани със сигурността при двете услуги (препълвания на буфери, DoS и слаба автентификация), които ги превръщат в често използвани цели на атаките.

Освен услугите без инсталирани кръпки, които все още се срещат често, повишен риск представляват лошите конфигурации на NFS и NIS, които лесно позволяват злонамерено използване на дупките в сигурността, както и локален и отдалечен достъп на потребителите до тези дупки.

Немарливата автентификация, която предлага NIS при заявки за NIS "карти" (maps), позволява на потребителите да използват приложения като ypcat или getent, които могат да изведат на екрана стойностите на базата данни или "картата" (map) на NIS базата данни, или да намерят файла с паролите. Същият проблем се получава и при NFS, която се доверява абсолютно на UID (ID на потребителя) и на GID (ID-та на групата), които NFS клиентът представя пред сървъра, като в зависимост от конфигурацията на сървъра, това може да позволи на всеки потребител да монтира (mount) и изследва отдалечената файлова система. .

U8.2 Засягани операционни системи

Почти всички UNIX и Linux системи идват с инсталирани версии на NFS и NIS, които често са разрешени по подразбиране. В случай на NFS, въпреки че тя може да бъде разрешена по подразбиране, файлът exports е обикновено празен (файлът exports определя кои директории са споделени и как се споделят).

U8.3 CVE/CAN номера

NFS
CVE-1999-0002, CVE-1999-0166, CVE-1999-0167, CVE-1999-0170, CVE-1999-0211, CVE-1999-0832, CVE-1999-1021, CVE-2000-0344, CVE-2002-0830

CAN-1999-0165, CAN-1999-0169, CAN-2000-0800, CAN-2002-0830, CAN-2002-1228, CAN-2003-0252, CAN-2003-0379, CAN-2003-0576, CAN-2003-0680, CAN-2003-0683, CAN-2003-0976, CAN-2004-0154

NIS
CVE-1999-0008, CVE-1999-0208, CVE-1999-0245, CVE-2000-1040
CAN-1999-0795, CAN-2002-1232, CAN-2003-0176, CAN-2003-0251

U8.4 Как да определите дали сте уязвими

Следните стъпки се отнасят към уязвимостите в софтуера NIS/NFS:

1. Проверете дали сте инсталирали кръпките, които предлага вашият продавач. При повечето версии командата rpc.mountd – version за NFS и ypserv – version за NIS ще покажат съответните им версии. Всяка незакърпена или остаряла версия вероятно е уязвима.
2. Един по-завършен подход при софтуерните уязвимости се състои в използването на обновен скенер на неизправности, който да проверява периодично вашата система за наличието на нови пропуски.

Следните стъпки се отнасят към конфигурирането на NIS:

1. Уверете се, че паролата на root не се поддържа в NIS map.

2. Проверете дали паролите на потребителите са в съответствие със стабилните практики, свързани със сигурността. За целта можете да използвате програма за кракване на пароли.
3. Ако е възможно, за хешване на паролите използвайте Blowfish или MD5 вместо DES.

Важна забележка: Никога не стартирайте програма за кракване на пароли, дори на системи, на които имате административен достъп, без изрично и за предпочитане писмено разрешение от вашия началник. Администратори, които са имали най-добри намерения, бяха уволнени затова, че са стартирали средства за кракване на пароли без да имат пълномощия за това.

Следните стъпки се отнасят към конфигурирането на NFS:

1. Проверете дали хостовете, мрежовите групи и правата във файла /etc/exports са актуализирани.
2. Стартирайте командата showmount -e SERVER_IP, за да видите какво се експортира. Проверете дали вашите монтирания са в съответствие с вашата политика по отношение на сигурността.

U8.5 Как да се защитим

Следните стъпки се отнасят към конфигурирането на NIS:

1. Предотвратете възможността други системи да се маскират като NIS сървър при всеки клиент, на който можете изрично да укажете списък на NIS сървърите, разрешени за свързване.
2. Ако изготвяте DBM файлове, активирайте възможността YP_SECURE, за да бъдете сигурни, че сървърът ще отговаря само на заявки от клиент на привилегированите портове. Това може да се осъществи чрез използване на ключа "s" в командата makedbm.
3. Включете доверените хостове и мрежи във /var/yp/securenets, използван от процесите ypserv и ypxfrd и не забравяйте да рестартирате демоните, за да могат промените да влязат в сила.
4. Уверете се, че записът +:*:0:0::: фигурира във вашия файл с пароли за клиентите на NIS.
5. Помислете за използването на NIS по сигурен протокол като SSH. Добра отправна точка е http://www.math.ualberta.ca/imaging/snfs/.

Забележка: В някои конфигурации Lightweight Directory Access Protocol (LDAP) замества NIS и всички Linux дистрибуции поддържат LDAP като copc за различни елементи от обслужването на имената, като passwd, group, и hosts. Една добра книга за администриране на системата LDAP би била доста полезна. Освен това, LDAP сам по себе си поддържа SSL кодиране и репликация (повторение).

Следните стъпки се отнасят към конфигурирането на NFS:

1. При разрешаване на клиентите във файла /etc/exports използвайте цифрови IP адреси или пълните имена на домейните, а не съкратените (от файла hosts или от NIS картата на хостовете).
2. Използвайте файла /etc/exports, за да ограничите достъпа до файловата система NFS чрез добавяне на следните параметри:

- Забранете на обикновените потребители да монтират NFS файлова система чрез добавяне на параметъра за сигурност (secure) след IP адреса или името на домейна на вашия NFS клиент. (например: /home 10.20.1.25(secure))
- Експортирайте файловата система NFS със съответните права. Това може да се осъществи чрез добавяне на съответни параметри (ro за Read-only или rw за Read-Write) след IP адреса или името на домейна на вашия NFS клиент във файла /etc/exports. (например: /home 10.20.1.25(ro))
- Ако е възможно, използвайте параметъра root_squash след IP адреса или името на домейна на вашия NFS клиент. Ако този параметър е разрешен, root идентификацията на суперпотребителя на NFS клиента ще бъде заменена с nobody идентификацията на обикновен потребител и групово ID "nogroup" (то може да бъде променено, за да съответства на вашите нужди чрез параметрите "anonuid" и "anongid") в NFS сървъра. Това означава, че root потребителят на клиента няма да има достъп и няма да прави промени във файловете, за които само root на сървъра може да получава достъп и да прави промени, като по този начин root потребителя на клиента няма да може да получава привилегии на суперпотребител на сървъра. (например: /home 10.20.1.25(root_squash))
- Ако искате да експортирате директория с анонимни разрешения (permissions), използвайте параметъра "all_squash", който присвоява всяко id на потребител и id на група на ID-то на anonuid и anongid.
- Пълния набор параметри можете да намерите на etc/exports manpage. "man exports", или онлайн на http://www.netadmintools.com/html/5exports.man.html

3. За тестване на конфигурацията може да се използва средството NFSBug. Тестовете ще включват откриване на експортираните към света файлови системи, определяне дали действат ограниченията при експорт, определяне дали файловите системи могат да бъдат монтирани през средството за присвояване на портове (portmapper), опит за отгатване на манипулаторите (handles) на файлове и изпробване на различни бъгове за достъп до файловите системи. http://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/nfsbug/

4. При Solaris проверете дали сте активирали със сигурност възможността за наблюдение на портовете (Port Monitoring). Това може да се осъществи чрез добавяне на реда set nfssrv:nfs_porttmon = 1 във файла /etc/system. Linux системата по подразбиране отказва да работи съвместно с NFS клиенти, които използват непривилегирован порт (над 1024).

Общи съображения, свързани с NIS и NFS:

1. Прегледайте отново политиката си по отношение на защитните стени и се уверете, че сте блокирали всички портове, които не са необходими, както и порт 111/tcp/udp (Portmap) и порт 2049/tcp/udp (Rpc.nfsd). Разрешете достъпа до NIS и NFS сървърите само на оторизирани клиенти. Друга възможна мярка за ограничавене достъпа през tcp_wrappers, ще намерите

на http://sunsite.cnlab-switch.ch/ftp/software/security/security-porcupine.org/.

Във файла etc/hosts.allow трябва да запишете услугата и IP номера, на който е разрешено да получи достъп до услугата (например portmap: 10.20.0.0/16, за да разрешите на частната мрежа от Клас-B 10.20.0.0 да получава достъп до услугата portmap). Също така във файла /etc/hosts.deny трябва да включите услугите и IP номерата, на които НЕ Е разрешено да получават достъп до услугите (например, portmap: ALL ще откаже достъп на всички IP адреси, които не са включени в /etc/hosts.allow). Отказването на достъп до услугата portmap е важно, защото тя е единствената услуга, през която работи NFS.

2. Обмислете използването на NFS през протокол с висока степен на сигурност като SSH. Добра отправна точка е http://www.math.ualberta.ca/imaging/snfs/.

3. Инсталирайте всички кръпки от продавача или обновете вашите NIS и NFS сървъри до последната версия. За повече информация относно повишаване сигурността на вашата UNIX инсталация погледнете UNIX Security Checklist на CERT...

Забранете демоните на NFS и NIS на всички системи, които не са специално предназначени и оторизирани да служат като NFS и/или NIS сървър. С цел да направите тази промяна необратима, е разумно да изтриете и NFS и/или NIS софтуера от системата.

обратно в началото ^

U9 Бази данни

U9.1 Описание

Базите данни са елементи от електронния бизнес, финансите, банкирането, системата за планиране на корпоративните ресурси (ERP) и съдържат критична информация от партньорите, клиентите и служителите. Въпреки значението на целостта на данните и конфиденциалността им, за системите за управление на базите данни (DBMS) обикновено не се изисква същото ниво на сигурност както при операционните системи и мрежите. Системите за управление на базите данни представляват съвкупности от програми, които съхраняват, модифицират и извличат информация от базата данни.

Целостта и конфиденциалността на данните могат да бъдат компрометирани от много фактори, включително сложността на реализацията, използването на несигурни пароли, лошата конфигурация, зле написаните приложения, твърдокодираните пароли и неразкритите задни вратички към системата. Повечето бизнес и правителствени организации използват базите данни за лична информация, като например за възнагражденията на служителите и медицински сведения, за които те носят законова отговорност по отношение на неприкосновеността и конфиденциалността им. Базата данни съхранява поверителни финансови данни, минали и бъдещи, включително сведения за търговски сделки, бизнес транзакции и счетоводни данни. Базите данни съдържат също подробна информация за клиентите, включително банкови сметки, номера на кредитни карти и доверени данни за бизнес партньори.

Базите данни са изключително сложни приложения и често е трудно да бъдат конфигурирани и обезопасени. Приложенията за бази данни като MySQL,

PostgreSQL и ORACLE притежават много от следните възможности: потребителски акаунти и пароли, модел на привилегиите и специфични разрешения за контрол на обектите в базата данни, вградени команди, уникални скрипт и програмни езици, мрежови протоколи, кръпки и сервизни пакети, както и мощни програми за управление на базите данни и средства за разработката им. Мнозина администратори се занимават с управление на бази данни на непълен работен ден и често не проумяват сложността на тези приложения. Като резултат, сериозни уязвимости в сигурността и лоши конфигурации често остават непроверени или изцяло неоткрити. Традиционната общност на специалистите по сигурност общо взето игнорира проблема за сигурността на базите данни; повечето професионалисти по бази данни обикновено не разглеждат сигурността като една от своите отговорности. Повечето бази данни притежават широк набор от свойства и възможности, които могат да бъдат злонамерено използвани за компрометиране на конфиденциалността, разполагаемостта и целостта на данните.

Всички модерни системи за релационни бази данни са "адресируеми по порт," което означава, че всеки, който разполага с лесните за набавяне средства за търсене, може да се опита да се свърже директно с базата данни, като заобиколи механизмите за сигурност, използвани от операционната система. Например,достъп до Oracle може да се получи през TCP порт 1521, MySQL може да стане достъпен през TCP порт 3306, а PostgreSQL - през TCP порт 5432. Повечето приложения за бази данни имат също добре известни акаунти и пароли по подразбиране, които осигуряват различни нива на достъп до ресурсите и таблиците на базите данни. Понастоящем много бази данни са тясно свързани с крайни приложения, като най-често това са уеб базирани приложения. Ако приложението е лошо написано или конфигурирано, това може да позволи на нападателя да проведе атака с SQL инжекция или да използва някои от уязвимостите на базите данни.

CERT CC публикува документ със съвети CA-2003-05 за множество уязвимости на Oracle, които могат да компрометират съответната база данни. Още по-наскоро US-CERT издаде документ със съвети относно уязвимостите, свързани с SQL инжекция в Oracle E-Business Suite (TA04-160A), които могат да доведат до компрометиране на приложението на базата данни и целостта на данните.

По подобен начин MySQL също съдържа някои уязвимости. Кратко описание на някои от най-често срещаните атаки към MySQL можете да намерите в наскоро публикуваната от Next Generation Software статия
http://www.nextgenss.com/papers/HackproofingMySQL.pdf.

U9.2 Засягани операционни системи

Почти всички Linux системи се разпространяват с версия на DBMS с отворен код, като MySQL и PostgreSQL, както и с комерсиални решения на DBMS, като Oracle. Различни UNIX варианти като Solaris, AIX, HPUX поддържат ORACLE, DB2 и други известни комерсиални бази данни, както и много DBMS с отворен код.

U9.3 CVE/CAN номера

Oracle:
CVE-2002-0567, CVE-2002-0571

CAN-1999-0652, CAN-1999-1256, CAN-2002-0858, CAN-2002-1264, CAN-2003-0095, CAN-2003-0096, CAN-2003-0222, CAN-2003-0634, CAN-2003-0727, CAN-2003-0894

MySQL:
CVE-1999-1188, CVE-2000-0045, CVE-2000-0148, CVE-2000-0981, CVE-2001-0407

CAN-1999-0652, CAN-2001-1274, CAN-2001-1275, CAN-2002-0229, CAN-2002-0969, CAN-2002-1373, CAN-2002-1374, CAN-2002-1375, CAN-2002-1376, CAN-2003-0073, CAN-2003-0150, CAN-2003-0515, CAN-2003-0780, CAN-2004-0381, CAN-2004-0388, CAN-2004-0627, CAN-2004-0628

PostgreSQL:
CVE-2002-0802

CAN-1999-0862, CAN-2000-1199, CAN-2001-1379, CAN-2002-0972, CAN-2002-1397, CAN-2002-1398, CAN-2002-1399, CAN-2002-1400, CAN-2002-1401, CAN-2002-1402, CAN-2003-0040, CAN-2003-0500, CAN-2003-0515, CAN-2003-0901, CAN-2004-0366, CAN-2004-0547

U9.4 Как да определите дали сте уязвими
Уверете се, че всички DBMS, които идват с операционната система, работят с последните си версии. Незакърпените и остарелите версии на базите данни вероятно са уязвими.

Инсталацията по подразбиране на DBMS вероятно притежава уязвимости, които могат да бъдат използвани от нападател.

Сканирайте системите за уязвимости, за да определите дали софтуерът на DBMS е уязвим:

- MySQL Network Scanner: позволява сканирането на цялата мрежа за наличие на MySQL сървър с парола по подразбиране (празна), като може също и да идентифицира сървърите-"мошеници".
- Скенерът с отворен код за мрежови уязвимости Nessus (http://www.nessus.org) също прави проверки за често срещани пролуки в базите данни под UNIX.
- Комерсиалните скенери за уязвимости като Foundstone, Qualys, eEyE Retina също могат да бъдат използвани за откриване на уязвимости в базите данни.
- Освен това, съществуват и специални скенери на бази данни, като AppSecInc или ISS Database Scanner.

U9.5 Как да се защитим
На първо място, е важно да се уверим, че приложенията за бази данни са закърпени до последното налично ниво на кръпките. За информация относно кръпките, проверете на уеб сайтовете на съответните производители:

- Oracle (http://otn.oracle.com/software/index.html) MySQL (http://www.mysql.com/products/mysql/)

- PostgreSQL (ftp://ftp.postgresql.org/pub)

След това се уверете, че DBMS и приложенията са обезопасени:

- Използване на минимални привилегии.
- Премахване/промяна на паролите по подразбиране на привилегированите и системните акаунти на базите данни преди инсталирането на системата в мрежата.
- Използване на съхранявани процедури там, където това е възможно.
- Премахване/забраняване на ненужните съхранени процедури.
- Поставяне на ограничения за дължина на всички полета на формуляри.
- Валидиране на всички данни от страната на сървъра (дължина, формат, тип).

Съществуват множество полезни редурси, които подпомагат обезопасяването на DBMS:

- Oracle (http://otn.oracle.com/deploy/security/index.html)
- MySQL (http://dev.mysql.com/doc/mysql/en/Security.html)
- PostgreSQL (http://www.postgresql.org/docs/7/interactive/security.htm)

Осведомявайте се редовно за уязвимостите и предупрежданията, обявявани от производителите:

- Oracle Security Alerts (http://otn.oracle.com/deploy/security/alerts.htm)
- MySQL (http://lists.mysql.com/)
- PostgreSQL (http://www.postgresql.org/lists.html)

Институтът SANS публикува подробен документ за проверка на сигурността на Oracle, който е полезен при проверка на инсталацията на база данни Oracle: http://www.sans.org/score/oraclechecklist.php

Центърът за Интернет сигурност също е разработил Oracle Database Benchmark Tool, който е полезен при сравнителна проверка на сигурността на базите данни: http://www.cisecurity.org/bench_oracle.html

SANS Security Oracle Step-by-Step осигурява полезни и практични съвети за увеличаване на сигурността на Oracle (https://store.sans.org/store_item.php?item=80)

И накрая, допълнителна информация относно сигурността на базите данни можете да намерите тук:

- Читалня на SANS по сигурност на базите данни (http://www.sans.org/rr/catindex.php?cat_id=3)
- http://www.petefinnigan.com/orasec.htm

обратно в началото ^

U10 Кернел (ядро)

U10.1 Описание

Централният компонент на операционните системи е кернелът. Кернелът отговаря за голям брой взаимодействия на ниско ниво между операционната система и хардуера, паметта, планирането във времето, комуникациите между процесите, файловите системи и други. Тъй като кернелът има привилегирован достъп до всички аспекти на системата, едно компрометиране на ниво кернел може да бъде унищожително. Рисковете от уязвимости в кернела включват отказ от обслужване, изпълнение на произволен код със системни привилегии, неограничен достъп до файловата система или достъп на ниво администратор. Множество уязвимости могат да се използват злонамерено по отдалечен начин и са особено опасни, когато атаката се провежда чрез извършване на услуга, свързана с публикуване в Интернет. В някои случаи чрез изпращане на лошо образуван icmp пакет кернелът може да попадне в безкраен цикъл, консумирайки всички ресурси на процесора, правейки машината безполезна и причинявайки отказ от обслужване.
Подходящо настройване на кернела може да защити системите от атаки, както и да подобри функционалните характеристики на системата.

U10.2 Засягани операционни системи
Фактически всички варианти на Unix, включително Solaris и HP-UX, дистрибуции на Linux, версии на BSD и версии на Windows страдат от уязвимости на кернела, причинени или от вътрешно присъщи фактори или от недостатъци в приложенията, които засягат неблагоприятно кернела.

U10.3 CVE/CAN номера
CVE-1999-0295, CVE-1999-0367, CVE-1999-0482, CVE-1999-0727, CVE-1999-0804, CVE-1999-1214, CVE-1999-1339, CVE-1999-1341, CVE-2000-0274, CVE-2000-0375, CVE-2000-0456, CVE-2000-0506, CVE-2000-0867, CVE-2001-0062, CVE-2001-0268, CVE-2001-0316, CVE-2001-0317, CVE-2001-0859, CVE-2001-0993, CVE-2001-1166, CVE-2002-0046, CVE-2002-0766, CVE-2002-0831

CAN-1999-1166, CAN-2000-0227, CAN-2001-0907, CAN-2001-0914, CAN-2001-1133, CAN-2001-1181, CAN-2002-0279, CAN-2002-0973, CAN-2003-0127, CAN-2003-0247, CAN-2003-0248, CAN-2003-0418, CAN-2003-0465, CAN-2003-0955, CAN-2003-0984, CAN-2004-0003, CAN-2004-0010, CAN-2004-0177, CAN-2004-0482, CAN-2004-0495, CAN-2004-0496, CAN-2004-0497, CAN-2004-0554, CAN-2004-0602

U10.4 как да определите дали сте уязвими
Съществуват различни начини, които да ви помогнат да определите дали кернелът е уязвим.

- Ако производителят предлага тази възможност, когато регистрирате софтуера, регистрирайте се и за получаване на писма, уведомяващи за обновления, свързани със сигурността.
- Повечето пощенски списъци, свързани със сигурността, публикуват уязвимостите в кернела веднага след обявяването им.
- Проследяването на версията на кернела, с който работят системите, трябва да бъде част от стандартната процедура.
- За определяне на версията на кернела, с който работят системите, може да се използва софтуер за оценка на сигурността. Nessus има голям брой плъгини за тестване на системи за уязвимости на кернела. *Внимание:*

много от тези плъгини са способни да причинят условия за възникване на отказ от обслужване, затова при сканиране на вашите системи трябва да вземете мерки за предотвратяване на неочаквани престои.

U10.5 Как да се защитим

Има два класа параметри, които могат да бъдат конфигурирани в кернела, за да осуетят атаките. Единият е свързан с настройването на системните ресурси за ограничаване на атаките тип отказ от обслужване и тип препълване на буфер. Вторият клас се отнася до повишаване на сигурността на конфигурационните настройки на мрежата, насочено срещу мрежовите атаки. Командите и параметрите, които трябва да се конфигурират, зависят от платформата. За да разберете как да настроите подходящо кернела, трябва да прегледате документацията за съответната платформа.

Препоръчва се щателното тестване на всички модификации преди внедряването им в работната среда, както и изготвянето и поддържането в готовност на резервни копия в случай на възникване на проблемг.

Съществуват множество полезни ресурси, които да ви помогнат да обезопасите системите чрез съответна настройка на кернела.
Solaris Tunable Parameters Reference Manual (Solaris 8)
Solaris Tunable Parameters Reference Manual (Solaris 9)
Solaris Operating Environment Network Settings for Security
Solaris Kernel Tuning for Security или http://www.securityfocus.com/infocus/1385

Linux Kernel Hardening
The Linux Kernel Archives
Linux Kernel Hardening

AIX Kernel Tuning

HP-UX Kernel Tuning and Performance Guide

http://docs.hp.com/hpux/pdf/5185-6559.pdf
http://docs.hp.com/hpux/pdf/TKP-90203.pdf
http://docs.hp.com/cgi-bin/otsearch/hpsearch
http://docs.hp.com/

Наръчник за FreeBSD (съдържа информация за настройка на кернела):
http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/index.html

OpenBSD:
http://www.openbsd.org/faq/index.html
http://www.openbsd.org/docum.html (за повече информация)

NetBSD Tuning, Kernel Tuning

обратно в началото ^

Приложение А Най-често използвани портове

В този раздел ще опишем портовете, които често са обект на проучване и атаки. Блокирането на тези портове е минималното изискване за сигурност на

периметъра, а не подробна спецификация за конфигуриране на защитната стена. Много по-добър подход е блокирането на всички неизползвани портове, т.е отказване на целия трафик, а след това разрешаване на специфични протоколи (тези, които използвате при работата си) да влизат в периметъра на вашата мрежа. Дори ако сте сигурни, че тези портове са блокирани, вие пак трябва да ги наблюдавате активно, за да откриете евентуалните опити за непозволено проникване. Трябва да имате предвид и следното предупреждение: блокирането на някои от портовете от списъка по-надолу може да забрани услуги, които са ви необходими. Моля преди да изпълните тези препоръки преценете потенциалния ефект от тях.

> **Забележка:** Важно е да се илюстрира едно широко разпространеното убеждение, че извършването на отказ или блокиране по подразбиране, което не е изрично разрешена политика при конфигурирането на защитните стени, е много по-ефективна практика по отношение на сигурността от блокирането на определени портове. Този подход е по-удобен за администраторите на маршрутизатори или защитни стени, тъй като позволява техните конфигурационни и контролни списъци да бъдат по-кратки, по-логични и по-лесни за поддръжка.

Имайте предвид, че блокирането на тези портове не е заместител на цялостните правила и мерки за сигурност. Дори ако портовете са блокирани, един нападател, който е получил достъп до вашата мрежа по други методи (например, чрез dial-up модем, троянски кон, пристигащ като прикрепен файл към писмо по електронната поща, атака от потребител , намиращ се зад точката на филтриране, или компрометирана машина) може да използва тези портове по злонамерен начин, ако те не са подходящо обезопасени на всяка хост система във вашата организация.

Име	**Порт**	**Протокол**	**Описание**
Small services	<20	tcp/udp	Малки услуги
FTP	21	tcp	прехвърляне на файлове
SSH	22	tcp	услуги login
TELNET	23	tcp	услуги login
SMTP	25	tcp	mail
TIME	37	tcp/udp	синхронизация във времето
WINS	42	tcp/udp	WINS replication
DNS	53	udp	naming services
DNS zone transfers	53	tcp	naming services
DHCP server	67	tcp/udp	конфигуриране на хост
DHCP client	68	tcp/udp	конфигуриране на хост
TFTP	69	udp	разни
GOPHER	70	tcp	стара услуга, подобна на WWW
FINGER	79	tcp	разни
HTTP	80	tcp	уеб
alternate HTTP port	81	tcp	уеб
alternate HTTP port	88	tcp	уеб (понякога Kerberos)

LINUXCONF	98	tcp	конфигуриране на хост
POP2	109	tcp	mail
POP3	110	tcp	mail
PORTMAP/RPCBIND	111	tcp/udp	RPC portmapper
NNTP	119	tcp	network news service
NTP	123	udp	синхронизация във времето
NetBIOS	135	tcp/udp	DCE-RPC endpoint mapper
NetBIOS	137	udp	NetBIOS name service
NetBIOS	138	udp	NetBIOS datagram service
NetBIOS/SAMBA	139	tcp	споделяне на файлове & услуга login
IMAP	143	tcp	mail
SNMP	161	tcp/udp	разни
SNMP	162	tcp/udp	разни
XDMCP	177	udp	X display manager protocol
BGP	179	tcp	разни
FW1-secureremote	256	tcp	CheckPoint FireWall-1 mgmt
FW1-secureremote	264	tcp	CheckPoint FireWall-1 mgmt
LDAP	389	tcp/udp	naming services
HTTPS	443	tcp	уеб
Windows 2000 NetBIOS	445	tcp/udp	SMB по IP (Microsoft-DS)
ISAKMP	500	udp	IPSEC Internet Key Exchange
REXEC	512	tcp	} трите
RLOGIN	513	tcp	} Berkeley r-services
RSHELL	514	tcp	} (използва се за отдалечен login)
RWHO	513	udp	разни
SYSLOG	514	udp	разни
LPD	515	tcp	отдалечено отпечатване
TALK	517	udp	разни
RIP	520	udp	routing protocol
UUCP	540	tcp/udp	прехвърляне на файлове
HTTP RPC-EPMAP	593	tcp	HTTP DCE-RPC endpoint mapper
IPP	631	tcp	отдалечено отпечатване
LDAP over SSL	636	tcp	LDAP over SSL
Sun Mgmt Console	898	tcp	отдалечено администриране
SAMBA-SWAT	901	tcp	отдалечено администриране
Windows RPC programs	1025	tcp/udp	} често разпределяни
Windows RPC programs	to		} от DCE-RPC portmapper
Windows RPC programs	1039	tcp/udp	} на Windows хостовете

SOCKS	1080	tcp	разни
LotusNotes	1352	tcp	бази данни/groupware
MS-SQL-S	1433	tcp	бази данни
MS-SQL-M	1434	udp	бази данни
CITRIX	1494	tcp	отдалечено графично изображение
WINS replication	1512	tcp/udp	WINS replication
ORACLE	1521	tcp	бази данни
NFS	2049	tcp/udp	NFS споделяне на файлове
COMPAQDIAG	2301	tcp	Compaq отдалечено администриране
COMPAQDIAG	2381	tcp	Compaq отдалечено администриране
CVS	2401	tcp	споделяне на файлове между сътрудници
SQUID	3128	tcp	уеб кеш
Global catalog LDAP	3268	tcp	Глобален каталог LDAP
Global catalog LDAP SSL	3269	tcp	Глобален каталог LDAP SSL
MYSQL	3306	tcp	база данни
Microsoft Term. Svc.	3389	tcp	отдалечено графично изображение
LOCKD	4045	tcp/udp	NFS споделяне на файлове
Sun Mgmt Console	5987	tcp	отдалечено администриране
PCANYWHERE	5631	tcp	отдалечено администриране
PCANYWHERE	5632	tcp/udp	отдалечено администриране
VNC	5800	tcp	отдалечено администриране
VNC	5900	tcp	отдалечено администриране
X11	6000-6255	tcp	X Windows сървър
FONT-SERVICE	7100	tcp	X Windows font service
alternate HTTP port	8000	tcp	уеб
alternate HTTP port	8001	tcp	уеб
alternate HTTP port	8002	tcp	уеб
alternate HTTP port	8080	tcp	уеб
alternate HTTP port	8081	tcp	уеб
alternate HTTP port	8888	tcp	уеб
Unix RPC programs	32770	tcp/udp	} често разпределяни
Unix RPC programs	to		} от RPC portmapper
Unix RPC programs	32899	tcp/udp	} на Solaris хостове
COMPAQDIAG	49400	tcp	Compaq отдалечено администриране
COMPAQDIAG	49401	tcp	Compaq отдалечено администриране
PCANYWHERE	65301	tcp	отдалечено администриране

ICMP: блокирайте входящите заявки за echo (ping и traceroute при Windows), блокирайте изходящите отговори на echo, съобщения за превишаване на времето и “destination unreachable” с изключение на съобщенията "packet too big" (тип 3, код 4). (Този елемент предполага, че вие желаете да изпреварите легитимното използване на ICMP заявката за echo, за да блокирате някои известни злонамерени начини за използването му).

Освен тези портове, блокирайте фалшифицираните адреси: пакети, идващи уж отвън към вашата компания, но всъщност генерирани от вътрешни адреси, лични адреси (RFC1918) и адресите, резервирани за IANA (за подробности погледнете на http://www.iana.org/assignments/ipv4-address-space). Съветваме ви също така да блокирате пакетите, към broadcast или multicast адреси. Конкретното блокиране на “source routed” пакети, както и на пакети с IP опции също е във ваша полза.

Трябва също така да поставите изходни филтри на граничните маршрутизатори, за да блокирате генерирането на фалшифицираните пакети от вашата мрежа. Позволявайте излизането навън от вашата организация само на пакети, генерирани от действителни ваши адреси.

Признаване на запазените марки: Институтът SANS оценява значението на интелектуалната собственост, запазените марки, авторското право, марките на услугите и патентите и се е стремял да спазва съответните стандарти в този документ. Изброените по-надолу продукти, системи и приложения са признати за запазени марки. Ако смятате, че сме пропуснали някои продукти със запазени марки, моля изпратете на top20@sans.org вашите коментари и забележки и ние ще направим необходимите промени в този документ.

обратно в началото ^

Приложение B

Списък на експертите, които оказаха помощ при създаването на списъците на двадесетте най-критични услуги за 2003 г.

Adair Collins, US Department of Energy
Alan Paller, SANS Institute
Alex Lucas, United Kingdom National Infrastructure Security Co-ordination Center
Alexander Kotkov, CCH Legal Information Services
Anton Chuvakin, Ph.D., netForensics
BJ Bellamy, Kentucky Auditor of Public Accounts
Bradley Peterson, US Department of Energy
Cathy Booth, United Kingdom National Infrastructure Security Co-ordination Center - Incident Response CESG
Chris Benjes, National Security Agency
Christopher Misra, University of Massachusetts Amherst
Dave Dobrotka, Ernst & Young
Dominic Beecher, United Kingdom National Infrastructure Security Co-ordination
Ed Fisher, CableJiggler Consulting, LLC
Edward Skoudis, International Network Services
Edward W. Ray, MMICMAN LLC
Erik Kamerling, Pragmeta Networks/SANS Institute - Editor
Gerhard Eschelbeck, Qualys
Jeff Campione, Editor 2002
Jeff Ito, Indus Corporation
Jeni Li, Arizona State University
Kevin Thacker, United Kingdom National Infrastructure Security Co-ordination
Koon Yaw Tan, Infocomm Development Authority of Singapore (IDA)
Pedro Paulo Ferreira Bueno, MetroRED Telecom, Brazil
Pete Beck, United Kingdom National Infrastructure Security Co-ordination
Richard (Rick) Wanner, InfoSec Centre of Expertise (COE) CGI Information Systems & Management Consultants Inc.
Roland M Lascola, U.S. Dept. of Energy - Office of Independent Oversight and Performance Assurance
Ross Patel, Afentis Security
Russell Morrison, AXYS Environmental Consulting Ltd.
Scott A. Lawler, CISSP, Veridian Information Solutions
Stephen Northcutt, SANS Institute
Valdis Kletnieks, Virginia Tech
William Eckroade, U.S. Dept. of Energy

Благодарим също и на хората, които свършиха прекрасна работа при редактирането, форматирането и публикуването на списъка за 2003 г.

Audrey (Dalas) Bines, SANS Institute
Brian Corcoran, SANS Institute
Cara L. Mueller, SANS Institute

Екипът на Топ 20 би желал също да благодари на следните бивши кадри на SANS, които отделиха от времето си, за да прегледат и коментират проекта за 2003 г.

Paul Graham, CIT at the University at Buffalo (UB)
Jerry Berkman, UC Berkeley
Neil W Rickert, Northern Illinois University
Travis Hildebrand, US Department of Veteran Affairs
Christoph Gruber, WAVE Solutions

Mark Worthington, Affiliated Computer Services (ACS), Riverside Public Library
Matthew Nehawandian, CISSP

Това са експертите, които помогнаха за създаването на списъка на уязвимостите в Топ 20 за 2002 г.

Jeff Campione, Federal Reserve Board - Editor
Eric Cole, Editor, 2001 Edition
Ryan C. Barnett, Department of the Treasury/ATF
Chris Benjes, National Security Agency
Matt Bishop, University of California, Davis
Chris Brenton, SANS Institute
Pedro Paulo Ferreira Bueno, Open Communications Security, Brazil
Anton Chuvakin, Ph.D., netForensics
Rob Clyde, Symantec
Dr. Fred Cohen, Sandia National Laboratories
Gerhard Eschelbeck, Qualys
Dan Ingevaldson, Internet Security Systems
Erik Kamerling, Pragmeta Networks
Gary Kessler, Gary Kessler Associates
Valdis Kletnieks, Virginia Tech CIRT
Alexander Kotkov - CCH Legal Information Services
Jamie Lau, Internet Security Systems
Scott Lawler, Veridias Information Solutions
Jeni Li, Arizona State University
Nick Main, Cerberus IT, Australia
Jose Marquez, Alutiiq Security and Technology
Christopher Misra, University of Massachusetts
Stephen Northcutt, SANS Institute
Craig Ozancin, Symantec
Alan Paller, SANS Institute
Ross Patel, Afentis, UK
Marcus Ranum, ranum.com
Ed Ray - MMICMAN LLC
Chris Rouland, Internet Security Systems
Bruce Schneier, Counterpane Internet Security Inc.
Greg Shipley, Neohapsis
Ed Skoudis, Predictive Systems
Gene Spafford, Purdue University CERIAS
Koon Yaw Tan, Infocomm Development Authority of Singapore
Mike Torregrossa, University of Arizona
Viriya Upatising, Loxley Information Services, Thailand
Rick Wanner, CGI Information Systems and Management Consultants

Списък на хората, които подпомогнаха бързата обработка на CVE номерата, допринесла за определяне на тестовете, които бяха използвани в скенерите от Топ 20 за 2002 г. Подробности по използвания процес можете да намерите на www.sans.org/top20/testing.pdf

Charles Ajani, Standard Chartered Bank, London, UK
Steven Anderson, Computer Sciences Corporation, North Kingstown RI
John Benninghoff, RBC Dain Rauscher, Minneapolis MN
Layne Bro, BEA Systems, Denver CO

Thomas Buehlmann, Phoenix AZ
Ed Chan, NASA Ames Research Center, San Jose CA
Andrew Clarke, Computer Solutions, White Plains NY
Brian Coogan, ManageSoft, Melbourne Australia
Paul Docherty, Portcullis Computer Security Limited,UK
Arian Evans, U.S. Central Credit Union, Overland Park KS
Rich Fuchs, Research Libraries Group, Mountain View CA
Mark Gibbons, International Network Services, Minneapolis MN
Dan Goldberg, Rochester NY
Shan Hemphill, Sacramento CA
Michael Hensing, Charlotte, NC, Microsoft
Simon Horn, Brisbane Australia
Bruce Howard, Kanwal Computing Solutions, Jilliby NSW Australia
Tyler Hudak, Akron OH
Delbert Hundley, MPRI Division of L-3COM, Norfolk VA
Chyuan-Horng Jang, Oak Brook IL
Kim Kelly, The George Washington University, Washington DC
Martin Khoo, Singapore Computer Emergency Response Team (SingCERT), Singapore
Susan Koski, Pittsburgh PA
Kevin Liston, AT&T, Columbus OH
Andre Marien, Ubizen, Belgium
Fran McGowran, Deloitte & Touche, Dublin, Ireland, UK
Derek Milroy, Zurich North America, Chicago IL
Bruce Moore, Canadian Forces Network Operations Center, DND, Ottawa Canada
Castor Morales, Ft. Lauderdale FL
Luis Perez, Boston MA
Reg Quinton, University of Waterloo, Ontario Canada
Bartek Raszczyk, UWM Olsztyn, Olsztyn Poland
Teppo Rissanen, Plasec Oy, Helsinki Finland
Alan Rouse, N2 Broadband, Duluth GA
Denis Sanche, PWGSC ITSD/IPC, Hull, QC Canada
Felix Schallock, Ernst & Young, Vienna, Austria
Gaston Sloover, Fidelitas, Buenos Aires Argentina
Arthur Spencer, UMASS Medical School, Worcester MA
Rick Squires
Jeff Stehlin, HP
Koon Yaw TAN, Infocomm Development Authority of Singapore, Singapore
Steven Weil, Seitel Leeds & Associates, Seattle WA
Lance Wilson, Time Warner Cable/Broadband IS, Orlando FL
Andrew Wortman, Naval Research Laboratory, Washington DC
Carlos Zottman, Superior Tribunal de Justica, Brasilia Brazil

Още няколко експерти по сигурност, които оказаха помощ при съставянето на Топ 20 за 2001 г. и 2000 г., на основата на които бе съставен Топ 20 2002 г.

Billy Austin, Intrusion.com
Phil Benchoff, Virginia Tech CIRT
Tina Bird, Counterpane Internet Security Inc.
Lee Brotzman, NASIRC Allied Technology Group Inc.
Mary Chaddock
Steve Christey, MITRE
Scott Conti, University of Massachusetts

Kelly Cooper, Genuity
Scott Craig, KMart
Sten Drescher, Tivoli Systems
Kathy Fithen, CERT Coordination Center
Nick FitzGerald, Computer Virus Consulting Ltd.
Igor Gashinsky, NetSec Inc.
Bill Hancock, Exodus Communications
Robert Harris, EDS
Shawn Hernan, CERT Coordination Center
Bill Hill, MITRE
Ron Jarrell, Virginia Tech CIRT
Jesper Johansson, Boston University
Christopher Klaus, Internet Security Systems
Clint Kreitner, Center for Internet Security
Jimmy Kuo, Network Associates Inc.
Jim Magdych, Network Associates Inc.
Dave Mann, BindView
Randy Marchany, Virginia Tech
Mark Martinec "Jozef Stefan" Institute
William McConnell, Trend Consulting Services
Peter Mell, National Institutes of Standards and Technology
Larry Merritt, National Security Agency
Mudge, @stake
Tim Mullen, AnchorIS.com
Ron Nguyen, Ernst & Young
David Nolan, Arch Paging
Hal Pomeranz, Deer Run Associates
Chris Prosise, Foundstone Inc.
Jim Ransome
RAZOR Research - BindView Development
Martin Roesch, Snort
Vince Rowe, FBI, NIPC
Marcus Sachs, JTF-CNO US Department of Defense
Tony Sager, National Security Agency
Gene Schultz, Lawrence Berkeley Laboratory
Eric Schultze, Foundstone
Derek Simmel, Carnegie Mellon University
Ed Skoudis, Predictive Systems
Lance Spitzner, Sun Microsystems, GESS Team
Wayne Stenson, Honeywell
Jeff Stutzman
Frank Swift
Bob Todd, Advanced Research Corporation
Jeff Tricoli, FBI NIPC
Laurie Zirkle, Virginia Tech CIRT

Експерти, които допринесоха за превеждане на Топ 20 на български език

Евгений Николов, НЛКВ-БАН
Цецко Николов, НЛКВ-БАН
Jess Garcia, LAEFF-INTA

обратно в началото ^