Le venti vulnerabilità più critiche per la Sicurezza in Internet

CON IL PATROCINIO

Prefazione

La pubblicazione e la divulgazione in Italia de “Le venti vulnerabilità più critiche per la sicurezza in Internet” è stata possibile grazie alla condivisione da parte del SANS Institute e di Data Security di una filosofia comune sulla sicurezza informatica.
L’idea fondamentale che ha portato a questa collaborazione è la convinzione che, per ridurre il rischio di attacchi informatici, sia necessario un continuo impegno nella ricerca delle vulnerabilità e nello sviluppo di contromisure adeguate e, contemporaneamente, un’opera di sensibilizzazione verso gli utenti e le aziende affinché non si trovino impreparati di fronte a questo tipo di minacce.

Ricerca, aggiornamento continuo e formazione devono essere gli ingredienti sempre presenti nell’attività di un’azienda che si occupi di sicurezza informatica.
In questo modo si è in grado di proporre soluzione tecnologiche all’avanguardia e, allo stesso tempo, appropriate alla specificità del cliente e al livello di maturità tecnologica ed informatica degli utenti.

La diffusione in Italia delle ricerche sulle vulnerabilità più comuni nei sistemi informatici in questa seconda edizione aggiornata è il risultato del nostro costante impegno nel settore della ricerca e della formazione.
Crediamo che, solo attraverso un’alleanza forte tra tutti coloro che nel mondo si occupano di sicurezza informatica, sia possibile fronteggiare quanti, ogni giorno, si organizzano e si preparano ad usare le tecnologie informatiche per azioni criminali.

Stephen Northcutt
Director of Training and Certification
The SANS Institute

Romano Favero
Direttore Data Security

Le venti vulnerabilità più critiche per la sicurezza in Internet

Versione 3.2 – Febbraio 2003- Localizzata da Data Security

Introduzione

La maggior parte degli attacchi riusciti ai danni dei sistemi operativi deriva da un numero estremamente limitato di vulnerabilità software. Ciò si deve al fatto che coloro che effettuano gli attacchi agiscono in modo opportunistico, ovvero scelgono la strada più semplice e comoda, sfruttando le vulnerabilità più conosciute e impiegando gli strumenti di aggressione più efficaci e diffusi. Contano sul fatto che le aziende spesso non pongono rimedio ai problemi e quindi spesso conducono attacchi indiscriminati, scegliendo gli obiettivi dai risultati di una serie di scansioni in Internet per rilevare i sistemi vulnerabili. La compromissione dei sistemi del Pentagono a seguito dell'episodio di hacking Solar Sunrise e la facile e rapida diffusione dei worm Code Red e NIMDA, per fornire solo alcuni esempi, possono essere facilmente collegate allo sfruttamento di alcune vulnerabilità per le quali non sono state tempestivamente applicate le opportune correzioni.

Due anni fa, Il SANS Institute e il National Infrastructure Protection Center (NIPC) pubblicarono un documento che elencava le dieci vulnerabilità più critiche per la sicurezza in Internet. Da allora migliaia di organizzazioni hanno utilizzato quella lista, e la sua evoluzione a venti vulnerabilità diffusa un anno dopo, come guida per risolvere rapidamente i buchi di sicurezza più pericolosi. Le vulnerabilità che hanno favorito i tre esempi riportati sopra – l'episodio Solar Sunrise del Pentagon e i worm Code Red e NIMDA – sono riportate su quella lista.

Questa nuova versione delle "Venti Vulnerabilità più critiche" è in effetti costituita da due liste di dieci: i dieci servizi di Windows le cui vulnerabilità sono più frequentemente sfruttate e i dieci servizi di Unix le cui vulnerabilità sono utilizzate più spesso per condurre un attacco.
Sebbene vi siano migliaia di episodi di violazione della sicurezza che ogni anno colpiscono questi sistemi operativi, la stragrande maggioranza degli attacchi portati a termine sono diretti verso uno o più di questi servizi.

Per quanto anche gli amministratori di sicurezza più esperti troveranno nelle Venti Vulnerabilità più critiche un valido strumento di lavoro, la lista è diretta in particolare a quelle organizzazioni nelle quali scarseggiano le risorse la formare o dove mancano amministratori della sicurezza con una preparazione tecnica particolarmente avanzata. Coloro che hanno la responsabilità della gestione della rete in queste organizzazioni spesso raccontano di non aver corretto molte di queste vulnerabilità semplicemente perché non sapevano quali fossero le vulnerabilità più pericolose, ed erano troppo occupati per poterle eliminare tutte o non sapevano come correggere in modo sicuro. Tradizionalmente gli auditor e i security manager hanno sempre usato strumenti per la rilevazione delle vulnerabilità per cercare cinquecento, mille o anche duemila vulnerabilità molto specifiche, distogliendo gli amministratori dall'obiettivo di proteggere efficacemente tutti i loro sistemi dagli attacchi più comuni. Quando un amministratore di sistema riceve un report che elenca migliaia di vulnerabilità su centinaia di macchine, spesso rimane paralizzato.

Le Venti vulnerabilità più critiche è una lista delle vulnerabilità che richiedono un intervento immediato. L'elenco è ordinato per servizi perché in molti casi un singolo rimedio – disabilitare il servizio, aggiornare alla versione più recente, applicare una patch cumulativa – può risolvere dozzine di vulnerabilità specifiche del software che possono essere evidenziate da una scansione. Questa lista è stata progettata per mitigare questi problemi raggruppando le conoscenze di decine tra i più importanti esperti

di sicurezza. Essi provengono dalle agenzie federali statunitensi più sensibili a problemi della sicurezza, dai più importanti produttori di software, dalle più importanti società di consulenza, dai migliori progetti universitari per la sicurezza, dal CERT/CC e dal SANS Institute. L'elenco dei partecipanti è disponibile alla fine del presente documento.

L'elenco SANS/FBI delle venti vulnerabilità più critiche è un documento in continuo aggiornamento. Contiene istruzioni dettagliate e riferimenti a informazioni supplementari utili per correggere i problemi di sicurezza. Nel momento in cui si scoprono minacce più critiche di quelle elencate o metodi di intrusione più diffusi o più comodi, vengono aggiornati l'elenco delle vulnerabilità e le istruzioni per rimediare; in questo processo il vostro contributo è sempre gradito. Questo documento si basa sul consenso di un'intera comunità: la vostra esperienza nel combattere le intrusioni e nell'eliminare le vulnerabilità può aiutare quelli che verranno dopo di voi. Inviate i vostri suggerimenti a info@sans.org, specificando "Top Twenty Comments" nell'oggetto dell'e-mail.

Note per i lettori:

Codici CVE

Ogni vulnerabilità menzionata è accompagnata dai codici della catalogazione CVE (Common Vulnerabilities and Exposures). Spesso sono riportati anche i numeri CAN, ovvero i codici delle vulnerabilità che sono candidate ad essere incluse nella lista CVE, ma non sono state ancora completamente verificate. Per ulteriori informazioni relative al progetto CVE, oggetto di numerosi riconoscimenti ufficiali, consultate l'indirizzo http://cve.mitre.org.

I codici CVE e CAN corrispondono alle vulnerabilità più importanti che devono essere verificate per ciascuna voce. Ogni vulnerabilità CVE è collegata all'elemento corrispondente del servizio ICAT di indicizzazione delle vulnerabilità del National Institute of Standards (http://icat.nist.gov). Per ciascuna vulnerabilità ICAT fornisce una breve descrizione, un elenco delle caratteristiche (ad esempio ambito dell'attacco e danno potenziale), un elenco dei nomi e delle versioni dei software vulnerabili e i collegamenti ai bollettini sulle vulnerabilità e alle informazioni sulle patch.

Porte da bloccare a livello di firewall

Alla fine del documento troverete una sezione aggiuntiva che presenta l'elenco delle porte utilizzate dai servizi che vengono comunemente esplorati e attaccati. Bloccando il traffico che passa attraverso le porte di firewall o di altri dispositivi di protezione del perimetro della rete, potete ottenere un livello di difesa aggiuntivo che aiuta a tutelarvi da eventuali errori di configurazione. Tenete comunque presente che, anche se utilizzate un firewall per bloccare il traffico di rete diretto a una porta, essa non è protetta da possibili azioni causate da soggetti che si trovano già all'interno del perimetro, né dall'azione di hacker penetrati utilizzando altri metodi.

Le principali vulnerabilità per i sistemi Windows

Le principali vulnerabilità per i sistemi Unix

W1 Internet Information Services (IIS)

W1.1 Descrizione:

IIS è passibile di vulnerabilità in tre grandi categorie: problemi di gestione di richieste inattese, problemi di "buffer overflow" e vulnerabilità legate alle applicazioni di esempio. Ognuna di queste categorie verrà qui brevemente trattata.

1. *Problemi di gestione di richieste inattese.* Molte vulnerabilità di IIS sono dovute a problemi di gestione delle richieste HTTP non corrette o volutamente composte in modo anomalo. Un ben noto esempio è la vulnerabilità Unicode sfruttata dal worm Code Blue. Costruendo una richiesta che sfrutti una di queste vulnerabilità, un aggressore può da remoto:

    - Visualizzare il codice sorgente di programmi non compilati.
    - Visualizzare file che si trovano oltre la radice del Web server.
    - Visualizzare file che il Web server non dovrebbe rendere accessibili.
    - Eseguire comandi arbitrari sul server (che possono avere come conseguenza, per esempio, la cancellazione di file di importanza critica o l'istallazione di una backdoor).

2. *Problemi di buffer overflow.* Molte estensioni ISAPI (incluse le estensioni ASP, HTR, IDQ, PRINTER, e SSI) sono vulnerabili ai buffer overflow. Un ben noto esempio è la vulnerabilità dell'estensione ISAPI .idq, che viene sfruttata dai worm Code Red e Code Red II. Una richiesta costruita in modo particolare da un aggressore remoto può portare a:

    - Interruzione del servizio.
    - Esecuzione di codice arbitrario e/o di comandi da parte degli account predefiniti del Web server (es. gli account IUSR_nomeserver or IWAM_nomeserver).

3. *Problemi legati alle applicazioni di esempio.* Le applicazioni di esempio sono di solito progettate per esemplificare le funzionalità di un ambiente server e non per resistere ad attacchi, e non sono nate per essere applicazioni da utilizzare se non in fase di test. Se a ciò si aggiunge il fatto che è noto a tutti il loro indirizzo di default e che il loro codice sorgente è disponibile per scopo di analisi, si capisce come esse siano gli obiettivi preferiti degli exploit. Le conseguenze di tali exploit possono essere gravi; ad esempio:

    - Una applicazione di esempio, newdsn.exe, permette a un aggressore remoto di creare o sovrascrivere dei file sul server.
    - Alcune di queste applicazioni permettono di vedere da remoto qualsiasi file, e questo fatto può essere sfruttato per raccogliere informazioni come gli user id e le password dei database.
    - Una applicazione iisadmin, ism.dll, permette l'accesso remoto a informazioni riservate del server, tra le quali la password di amministratore.

W1.2 Sistemi operativi interessati

- Windows NT 4 (qualsiasi versione) con IIS 4
- Windows 2000 Server con IIS 5
- Windows XP Professional con IIS 5.1

W1.3 Riferimenti CVE

CVE-2001-0241, CVE-2001-0333, CVE-2001-0500, CAN-2002-0079, CVE-2000-0884, CVE-2000-0886, CAN-2002-0071, CAN-2002-0147, CAN-2002-0150, CAN-2002-0364, CAN-2002-0149, CVE-1999-0191, CAN-1999-0509, CVE-1999-0237, CVE-1999-0264, CVE-2001-0151, CAN-1999-0736, CVE-1999-0278,

CAN-2002-0073, CVE-2000-0778, CVE-1999-0874, CVE-2000-0226, CAN-1999-1376, CVE-2000-0770, CVE-2001-0507

W1.4 Come determinare se siete vulnerabili

Dato l'alto numero di vulnerabilità, e poiché alcune di queste sono corrette solo da pacchetti cumulativi diffusi da Microsoft, è facile prevedere che chiunque non abbia applicato la patch cumulativa sia vulnerabile. Per determinare se sul vostro server sono è stata applicato un certo pacchetto cumulativo, verificate nel registro la voci che corrisponde alla vostra piattaforma nell'elenco seguente.

Windows NT 4:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Hotfix\Q319733`

Windows NT 4 Terminal Server Edition:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Hotfix\Q317636`

Windows 2000:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000\SP3\Q319733`

Windows XP:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows XP\SP1\Q319733`

In alternativa potete utilizzare HFNetChk (consultate la voce "*Rimanete aggiornati* " al paragrafo W1.5) per verificare la presenza della patch corrispondente:

- NT 4: Q319733
- NT 4 Terminal Server Edition: Q317636
- 2000 or XP: Q319733

Siete probabilmente vulnerabili agli exploit che colpiscono le applicazioni di esempio se qualcuno dei file seguenti è presente nella vostra directory %wwwroot%/scripts (es: C:\inetpub\wwwroot\scripts or D:\web\scripts) o in una sua qualsiasi subdirectory:

- code.asp
- codebrws.asp
- ism.dll
- newdsn.exe
- viewcode.asp
- winmsdp.exe

W1.5 Come proteggersi

1. *Applicate le patch più recenti*. Nel caso di IIS 4 su NT 4 con Service Pack 6a, ciò significa applicare una patch cumulativa e una hotfix. Nel caso di IIS 5 su Windows 2000 o di IIS 5.1 su XP, la patch cumulativa e la hotfix sono incluse nei service pack. Gli URL relativi sono riportati qui sotto.

   IIS 4 su NT 4:

- Service Pack 6a: http://www.microsoft.com/ntserver/nts/downloads/recommended/SP6/allSP6.asp
- Security Rollup: http://www.microsoft.com/ntserver/nts/downloads/security/q319733/
- Hotfix: http://www.microsoft.com/ntserver/nts/downloads/security/q321599/

IIS 4 su NT 4 Terminal Server Edition:

- Service Pack 6: http://www.microsoft.com/ntserver/terminalserver/downloads/recommended/tsesp6/
- Security Rollup: http://www.microsoft.com/ntserver/terminalserver/downloads/critical/q317636/
- Hotfix: http://www.microsoft.com/ntserver/nts/downloads/security/q321599/

IIS 5 su Windows 2000:

- Service Pack 3: http://www.microsoft.com/windows2000/downloads/servicepacks/sp3/

IIS 5.1 su Windows XP:

- Service Pack 1: http://www.microsoft.com/WindowsXP/pro/downloads/servicepacks/sp1/

2. *Rimanete aggiornati.* Questi service pack, patch cumulative e hotfix pongono rimedio solo alle vulnerabilità che sono gia note. Non appena vengono scoperte nuove vulnerabilità di IIS, dovrete correggerle di conseguenza. HFNetChk (Network Security Hotfix Checker) è uno strumento che aiuta gli amministratori di sistema ad analizzare i sistemi locali e remoti per verificare che siano state installate le patch più recenti. Questo strumento funziona su Windows NT 4, Windows 2000 e Windows XP. La versione più recente più essere scaricata da Microsoft all'indirizzo http://www.microsoft.com/technet/security/tools/hfnetchk.asp.

3. *Eliminate le applicazioni di esempio. Le applicazioni di esempio*, inclusa iisadmin, dovrebbero essere utilizzate solo per verificare che l'istallazione sia corretta e che il server funzioni nel modo atteso, ma una volta compiute queste verifiche dovrebbero essere immediatamente rimosse. Le applicazioni in questione si trovano nella directory %wwwroot%/scripts. L'ideale sarebbe che l'amministratore scegliesse di non installare mai le applicazioni di esempio e gli strumenti di amministrazione Web-based.

4. *Disabilitate le estensioni ISAPI non necessarie.* La maggior parte dei sistemi IIS non hanno bisogno di molte delle estensioni ISAPI che sono mappate per default, in particolare di .htr, .idq, .ism, e .printer. Tutte le estensioni ISAPI che non vengono utilizzate dovrebbero essere disabilitate. Ciò può essere compiuto manualmente tramite l'Internet Services Manager oppure automaticamente utilizzando IIS Lockdown Wizard di Microsoft. La versione più recente di quest'ultimo strumento può essere scaricata da Microsoft all'indirizzo http://www.microsoft.com/technet/security/tools/locktool.asp.

5. *Filtrate le richieste HTTP.* Molti exploit di IIS, incluse le famiglie di Code Blue e Code Red, utilizzano richieste HTTP composte in modo particolare per operare attacchi Unicode o buffer overflow. Si può configurare il filtro URLScan per respingere tali richieste prima che il server tenti di processarle. La versione più recente di URLScan è integrata nel IIS Lockdown Wizard, ma può essere anche scaricata separatamente da Microsoft all'indirizzo http://www.microsoft.com/technet/security/tools/urlscan.asp.

W2 Microsoft Data Access Components (MDAC) -- Remote Data Services

W2.1 Descrizione

Il componente Remote Data Services (RDS) nelle versioni meno recenti dei Microsoft Data Access Components (MDAC) presenta un baco che permette agli utenti remoti di eseguire comandi locali con privilegi da amministratore. Sfruttando il baco assieme a una vulnerabilità nel Microsoft Jet database engine 3.5 (componente di MS Access), un exploit può anche stabilire un accesso anonimo dall'esterno ai database interni. Queste vulnerabilità sono ben documentate e i rimedi sono disponibili da più di due anni, ma i sistemi non aggiornati o mal configurati ne sono ancora esposti e sono ancora soggetti ad attacchi di questo tipo.

W2.2 Sistemi operativi interessati

La maggior parte dei sistemi Microsoft Windows NT 4.0 con IIS 3.0 o 4.0, Remote Data Services 1.5, o Visual Studio 6.0.

W2.3 Riferimenti CVE

CVE-1999-1011

W2.4 Come determinare se siete vulnerabili

Se utilizzate Microsoft Windows NT 4.0 con IIS 3.0 o 4.0, verificate l'esistenza di "msadcs.dll" (di solito questa dll è istallata in "C:\Program Files\Common Files\System\Msadc\msadcs.dll", ma il percorso può cambiare a seconda dei sistemi).

W2.5 Come proteggersi

Una eccellente guida alle caratteristiche delle vulnerabilità RDS e Jet che illustra come correggerle è disponibile all'indirizzo http://www.wiretrip.net/rfp/p/doc.asp?id=29&iface=2.

Anche Microsoft ha emesso diversi avvisi di sicurezza che descrivono l'exploit e i metodi per proteggersi attraverso alcune modifiche nella configurazione:

- http://support.microsoft.com/support/kb/articles/q184/3/75.asp
- http://www.microsoft.com/technet/security/bulletin/ms98-004.asp
- http://www.microsoft.com/technet/security/bulletin/ms99-025.asp

In alternativa si può prevenire il problema aggiornando i MDAC alle versioni 2.1 o successive (per quanto talvolta questo aggiornamento possa comportare alcuni problemi di compatibilità). L'ultima versione dei MDAC è disponibile all'indirizzo http://www.microsoft.com/data/download.htm

W3 Microsoft SQL Server

W3.1 Descrizione

Microsoft SQL Server (MSSQL) contiene numerose vulnerabilità gravi che permettono ad aggressori remoti di ottenere informazioni riservate, di alterare il contenuto del database, di compromettere i server SQL e, in alcune configurazioni, anche gli host.
Le vulnerabilità di MSSQL sono molto pubblicizzate e ancora sotto attacco. Un recente worm MSSQL, diffusosi nel Maggio 2002, sfruttava numerose vulnerabilità note di MSSQL. Gli host compromessi da questo worm generano un traffico di rete dannoso quando analizzano la rete alla ricerca di altri host vulnerabili. Ulteriori informazioni possono essere reperite agli indirizzi

- http://www.incidents.org/diary/diary.php?id=157
- http://www.eeye.com/html/Research/Advisories/AL20020522.html

La porta 1433 (la porta di default di MSSQL) è risultata regolarmente una delle porte più sondate secondo le analisi dell'Internet Storm Center. Maggiori informazioni sulle vulnerabilità di MSSQL scoperte più di recente possono essere reperite nel CERT Advisory 2002-22.

W3.2 Sistemi operativi interessati

Qualsiasi sistema Microsoft Windows con installato Microsoft SQL Server 7.0, Microsoft SQL Server 2000 o Microsoft SQL Server Desktop Engine 2000.

W3.3 Riferimenti CVE

CAN-2002-1138, CAN-2002-1137, CAN-2002-0056, CAN-2002-0649, CAN-2001-0542, CAN-2000-1081, CVE-1999-0999, CAN-2002-0624, CAN-2002-0154, CAN-2000-1209, CAN-2002-1123, CAN-2002-0186, CVE-2000-0202, CVE-2000-0402, CVE-2000-0485, CVE-2000-0603, CVE-2001-0344, CVE-2001-0879, CAN-2000-0199, CAN-2000-1082, CAN-2000-1083, CAN-2000-1084, CAN-2000-1085, CAN-2000-1086, CAN-2000-1087, CAN-2000-1088, CAN-2001-0509, CAN-2002-0187, CAN-2002-0224, CAN-2002-0641, CAN-2002-0642, CAN-2002-0643, CAN-2002-0644, CAN-2002-0645, CAN-2002-0650, CAN-2002-0695, CAN-2002-0721, CAN-2002-0729, CAN-2002-0859, CAN-2002-0982

W3.4 Come determinare se siete vulnerabili

Se la chiave del registro `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\`MSSQLServer è definita, significa che sul sistema è installato SQL Server o SQL Server Desktop Engine. Se il vostro sistema non è mai stato corretto o se non lo avete aggiornato con le patch più recenti, molto probabilmente è vulnerabile.
Microsoft ha sviluppato il Microsoft Baseline Security Analyzer (MBSA), che permette di verificare in SQL Server 7.0 e 2000 la mancanza di hotfix o la presenza di vulnerabilità note. MBSA è disponibile all'indirizzo http://www.microsoft.com/technet/security/tools/Tools/MBSAhome.asp.

Microsoft fornisce anche una guida per aiutare a verificare la versione di SQL: HOW TO: Identify Your SQL Server Service Pack Version and Edition.

Per accertarvi che le correzioni siano installate correttamente, verificate i singoli file analizzando la data e l'ora dei file riportate nel bollettino corrispondente della Microsoft Knowledge Base, agli indirizzi:

- Microsoft SQL Server 7.0
- Microsoft SQL Server 2000

W3.5 Come proteggersi

Sommario:

1. Applicate il più recente service pack per Microsoft SQL server.
2. Applicate le patch cumulative più recenti rilasciate dopo l'ultimo service pack.
3. Applicate ciascuna singola patch rilasciata dopo la più recente patch cumulativa.
4. Rendete più sicuro il server a livello di sistema e a livello di rete.

In dettaglio:

1. *Applicate il più recente service pack per Microsoft SQL server.* Le versioni più recenti dei service pack per Microsoft SQL Server sono:
   - SQL Server 7.0 Service Pack 4
   - SQL Server 2000 Service Pack 2

   Per accertarvi di essere informati sui prossimi aggiornamenti, controllate regolarmente il documento di Microsoft Technet Make Your SQL Servers Less Vulnerable.

2. *Applicate le patch cumulative più recenti rilasciate dopo l'ultimo service pack.* La patch cumulativa più recente per tutte le versioni di SQL Server è disponibile all'indirizzo MS02-061 Elevation of Privilege in SQL Server Web Tasks (Q316333/Q327068).

   Per accertarvi di essere informati sui prossimi aggiornamenti, verificate le patch cumulative più recenti per Microsoft SQL Server agli indirizzi:
   - Microsoft SQL Server 7.0
   - Microsoft SQL Server 2000
   - Microsoft SQL Server Desktop Engine 2000

3. *Applicate ciascuna singola patch rilasciata dopo la più recente patch cumulativa*. Attualmente non vi sono patch singole rilasciate dopo la MS02-061 Elevation of Privilege in SQL Server Web Tasks (Q316333/Q327068). Per accertarvi di essere informati sui prossimi aggiornamenti, verificate il rilascio di nuove patch singole agli indirizzi:
   - Microsoft SQL Server 7.0
   - Microsoft SQL Server 2000
   - Microsoft SQL Server Desktop Engine 2000

4. *Rendete più sicuro il server a livello di sistema e a livello di rete.*

   1. Una delle vulnerabilità MSSQL più frequentemente attaccate riguarda il fatto che l'account di amministrazione di default (noto come "sa") viene installato con password vuota. Se il vostro account "sa" non è protetto da password, non potete ritenervi sicuri e potete cadere vittima di worm o di altri exploit. Perciò seguite le raccomandazioni raccolte alla voce "System Administrator (SA) Login" in SQL Server Books Online per assicurarvi che l'account "sa" installato abbia una password sufficientemente robusta, e ciò anche se il vostro SQL server non usa tale account.

      Sulla Microsoft Developer's Network è presente la documentazione su come cambiare il login da amministratore (Changing the SQL Server Administrator Login) e su come verificare e cambiare la password di amministratore usando MSDE (Verify and Change the System Administrator Password by Using MSDE).

   2. Eseguite il servizio MSSQLServer e l'SQL Server Agent sotto un account valido di dominio con privilegi minimi, non come amministratore del dominio o con l'account SYSTEM (su NT) o LocalSystem (su 2000 or XP). Se il servizio compromesso viene eseguito con privilegi locali o di dominio permette all'aggressore di ottenere il controllo completo della vostra macchina e/o della vostra rete.
   3. Abilitate l'Autenticazione Windows NT, abilitate la verifica dei login effettuati e falliti e quindi fermate e riavviate il servizio MSSQLServer. Configurate i client in modo che usino l'Autenticazione NT.
   4. Si raccomanda un'azione di packet filtering effettuata a livello perimetrale in modo da bloccare le connessioni che provengono dall'esterno ai servizi non autorizzati all'interno della rete. Il filtering per l'ingresso dalle porte TCP 1433 e 1434 può prevenire l'azione di aggressori esterni che attraverso queste porte possono effettuare scansioni o infettare eventuali server Microsoft SQL vulnerabili residenti nella rete locale che non sono esplicitamente autorizzati a fornire servizi SQL pubblici.
   5. Se i vostri servizi richiedono che le porte TCP 1433 e 1434 debbano rimanere aperte, abilitate e personalizzate il filtering in ingresso e in uscita in modo da prevenire l'uso non corretto di queste porte.

Ulteriori informazioni su come rendere più sicuro Microsoft SQL Server possono essere reperite agli indirizzi

- Microsoft SQL Server 7.0 Security

- Microsoft SQL Server 2000 Security

W4 NETBIOS – Condivisioni di rete non protette in Windows

W4.1 Descrizione:

Microsoft Windows fornisce alle macchine host la possibilità di condividere con file o cartelle gli altri host tramite le condivisioni di rete. I meccanismi che permettono questa funzione sono il protocollo Server Message Block (SMB) o il Common Internet File System (CIFS). Questi protocolli permettono agli host di operare su file remoti come se risiedessero in locale.

Per quanto questa funzione di Windows sia utile e valida, la configurazione impropria delle condivisioni di rete può mettere in pericolo i file di sistema o può favorire processi che portino utenti o programmi ostili ad ottenere il pieno controllo dell'host. Uno dei metodi tramite i quali il virus Sircam (vedi il CERT Advisory 2001-22) e il worm Nimda (vedi il CERT Advisory 2001-26) si sono diffusi così rapidamente nell'estate del 2001 era proprio quello di scoprire le condivisioni di rete non protette e di replicarsi in queste. Molti possessori di computer aprono inconsciamente i loro sistemi agli hacker quando vogliono favorire i colleghi o i collaboratori esterni condividendo i loro dischi in lettura e in scrittura per gli utenti della rete. Facendo attenzione quando si configura le condivisione di rete, i rischi possono essere adeguatamente mitigati.

W4.2 Sistemi operativi interessati

Windows 95, Windows 98, Windows NT, Windows Me, Windows 2000 e Windows XP sono tutti vulnerabili.

W4.3 Riferimenti CVE

CAN-1999-0519, CVE-2000-0979, CAN-2000-1079, CVE-2000-0044, CAN-1999-0621, CAN-1999-0520, CAN-1999-0518

W4.4 Come determinare se siete vulnerabili

Per Windows NT (SP4), Windows 2000 o Windows XP, il Microsoft Baseline Security Advisor aiuta a verificare se l'host è vulnerabile e indica come risolvere il problema. Il test di verifica può essere seguito in locale o su un host remoto.

La maggior parte degli scanner di rete disponibili in commercio rilevano le condivisioni aperte. Un rapido e sicuro test gratuito per rilevare la presenza di condivisioni di file SMB e le relative vulnerabilità, valido per macchine che montano qualsiasi versione di Windows, è disponibile al sito Web della Gibson Research Corporation all'indirizzo http://grc.com/. Cliccate su "ShieldsUP" per ricevere una valutazione in tempo reale sulla vulnerabilità SMB per qualsiasi sistema e istruzioni dettagliate per aiutare gli utenti Microsoft Windows ad affrontare le vulnerabilità SMB. Fate attenzione che se siete connessi a una rete nella quale alcuni dispositivi intermedi bloccano, il risultato prodotto da ShieldsUP sarà che non siete vulnerabili mentre, in realtà, lo potete essere. È il caso, ad esempio, di utenti collegati tramite un provider che blocca SMB all'interno della propria rete: in questo caso ShieldsUP riporterà che non siete vulnerabili, mentre in realtà siete esposti ad eventuali attacchi da parte di tutti gli utenti che utilizzano lo stesso provider.

W4.5 Come proteggersi

Per limitare il rischio determinato dalle vulnerabilità sfruttabili attraverso le Condivisioni di rete di Windows si possono intraprendere diverse azioni:

- Disabilitare le condivisioni quando non sono necessarie. Se l'host non ha bisogno di condividere file, disabilitate le condivisioni di rete nel pannello di controllo della rete di Windows. Se dovete chiudere una specifica condivisione, potete disabilitarla attraverso il menu delle proprietà di Explorer relative alla directory condivisa, attraverso il Server Manager o attraverso il Group Policy Editor.

- Non permettete condivisioni operate tramite Internet. Controllate tramite il Pannello di Controllo di rete di Windows che tutti gli host connessi a Internet abbiano le condivisioni di rete disabilitate. Lo scambio di file con gli host connessi ad Internet deve essere permesso solo tramite FTP o HTTP.
- Non permettete le condivisioni senza autenticazione. Se è necessaria la condivisione, configuratela in modo che sia necessaria una password per accedere alla condivisione.
- Limitate la condivisione solo alle directory strettamente necessarie. Di norma è necessario condividere solo una cartella e, al limite, le relative sottocartelle.
- Restringete il più possibile i permessi di accesso alle cartelle condivise. Ponete attenzione in particolare a consentire la scrittura solo quando strettamente necessario.
- Per una maggiore sicurezza, permettete la condivisione solo ad indirizzi IP specifici, poiché i nomi DNS possono essere aggirati.
- Bloccate le porte utilizzate dalle condivisioni di Windows al perimetro della vostra rete. Bloccate le porte NetBIOS comunemente utilizzate dalle condivisioni di Windows al perimetro della vostra rete usando il vostro router esterno o il vostro firewall per la protezione perimetrale. Le porte che devono essere bloccate sono le TCP dalla 137 alla 139 TCP, le UDP dalla 137 alla 139, la 445 TCP e la 445 UDP.

W5 Accesso anonimo – Null session

W5.1 Descrizione:

Una connessione tramite Null session, nota anche come Accesso anonimo, è un meccanismo che consente ad un utente anonimo di ottenere informazioni attraverso la rete (come ad esempio nomi utente e condivisioni) o di connettersi senza autenticazione. Viene utilizzato da applicazioni come explorer.exe per enumerare le condivisioni sui server remoti. Nei sistemi Windows NT, 2000 e XP, molti servizi locali sono eseguiti con l'account SYSTEM, noto su Windows 2000 e XP come *LocalSystem.* L'account SYSTEM viene utilizzato per varie operazioni critiche di sistema. Quando una macchina ha bisogno di recuperare dati di sistema da un'altra, l'account SYSTEM apre una sessione nulla su questa seconda macchina.

L' account SYSTEM possiede privilegi virtualmente illimitati e non richiede alcuna password, in modo che non ci si possa connettere normalmente come SYSTEM. A volte l'account SYSTEM ha bisogno di accedere ad informazioni presenti su altre macchine come ad esempio condivisioni disponibili, nomi utente e altre funzionalità tipiche delle Risorse di Rete. Poiché non può connettersi agli altri sistemi con UserID e password, utilizza per accedere una Sessione Nulla. Sfortunatamente anche gli aggressori possono connettersi utilizzando una Sessione Nulla.

W5.2 Sistemi operativi interessati

Tutte le versioni di Windows NT, 2000 e XP.

W5.3 Riferimenti CVE

CAN-2000-1200

W5.4 Come determinare se siete vulnerabili

Provate a connettervi al vostro sistema con una Sessione Nulla utilizzando il seguente comando:

```
net use \\a.b.c.d\ipc$ "" /user:""
```

(dove a.b.c.d rappresenta l'indirizzo IP del sistema remoto).

Se ricevete una risposta di "connessione non riuscita", il vostro sistema non è vulnerabile. Se non ricevete alcuna risposta significa che il comando è stato eseguito con successo e il vostro sistema è vulnerabile.

Potete anche utilizzare lo strumento "*Hunt for NT*". Si tratta di un componente dell'NT Forensic Toolkit reperibile presso http://www.foundstone.com/.

W5.5 Come proteggersi

I controller di dominio richiedono sessioni nulle per comunicare. Perciò, se state lavorando in un dominio di rete, potete limitare la quantità di informazioni che può cadere in mano agli aggressori, ma non potete fermarne del tutto la disponibilità. Per limitare la quantità di informazioni disponibili agli aggressori, modificate la seguente chiave di registro:

```
HKLM/System/CurrentControlSet/Control/LSA/RestrictAnonymous=1
```

Ricordate che qualsiasi modifica al registro potrebbe provocare un malfunzionamento del vostro sistema. Effettuate quindi le opportune verifiche prima di renderle la modifica definitiva. Per semplificare il ripristino del registro, vi raccomandiamo di effettuarne sempre il backup.

L'impostazione di RestrictAnonymous su 1 permette ugualmente la disponibilità di alcune informazioni per gli utenti anonimi, ma la riduce al minimo. Questa è l'impostazione più restrittiva possibile in Windows NT. In Windows 2000 e XP potete invece impostare il valore a 2. Questa azione bloccherà l'accesso degli utenti anonimi a tutte le informazioni con permessi di accesso non esplicitamente assegnati all'utente anonimo o al gruppo Tutti, il quale include anche gli utenti della sessione nulla.

Se non avete bisogno della condivisione di file e stampa, svincolate il NetBIOS dal TCP/IP.

Fate attenzione al fatto che la configurazione di RestricAnonymous sui controller di dominio e su altri server specifici può compromettere molte operazioni normali di rete. Per questa ragione si raccomanda di configurare questo valore solo per le macchine visibili da Internet. Tutte le altre macchine dovrebbero essere protette da un firewall configurato per bloccare NetBIOS e CIFS.

L'accesso ai controller di dominio o ad altri computer non specificamente configurati per l'accesso esterno non dovrebbe essere mai consentito agli utenti Internet. Per fermare tale accesso, bloccate sul router esterno o sul firewall le porte TCP e UDP dalla 135 alla 139 e le porte 445 TCP e UDP.

W6 Autenticazione LAN Manager -- Hashing LM debole

W6.1 Descrizione:

Per quanto la maggior parte degli ambienti Windows attuali non necessitino del supporto LAN Manager (LM), Microsoft memorizza per default in locale gli hash delle password legati al LM (noti anche come hash LANMAN) nei sistemi Windows NT, 2000 e XP. Siccome LAN Manager usa uno schema di codifica molto più debole di quelli, più aggiornati, attualmente utilizzati da Microsoft (NTLM and NTLMv2), le password del LAN Manager possono essere violate in brevissimo tempo. Anche le password che in un altro ambiente sarebbero considerate "forti" possono essere violate con sistemi "brute-force" in meno di una settimana.

La debolezza degli hash del Lan Manager deriva dal fatto che:

- le password sono troncate a 14 caratteri;
- le password utilizzano lo spazio come carattere di riempimento per raggiungere i 14 caratteri;
- i caratteri usati nelle password vengono convertiti tutti in caratteri maiuscoli;
- le password vengono divise in due blocchi di sette caratteri.

Questo processo di hashing comporta che, per ottenere un accesso autenticato al vostro sistema, un eventuale aggressore ha bisogno solo di determinare due semplici password da sette caratteri, che per di più contengono solo caratteri maiuscoli. Siccome la difficoltà nel violare gli hash aumenta con progressione geometrica in proporzione alla lunghezza dell'hash, ciascuna stringa di sette caratteri è almeno di un ordine di grandezza più semplice da attaccare con sistemi "brute-force" rispetto a una stringa di quattordici caratteri. Dal momento che le stringhe sono tutte esattamente di sette caratteri (spazi inclusi) e tutte in caratteri maiuscoli, anche un attacco da dizionario risulta molto semplificato. IL metodo di hashing del Lan Manager rende quindi inefficace qualsiasi buona policy sull'uso delle password.

In aggiunta al rischio dettato dal fatto di avere gli hash collegati a LM memorizzati nel SAM, il processo di autenticazione del LAN Manager è spesso abilitato per default sui client e accettato dai server. La conseguenza è che macchine Windows, in grado di utilizzare hash più robusti, inviano hash LM deboli attraverso la rete, rendendo l'autenticazione di Windows vulnerabile all'intercettazione attraverso packet sniffing e facilitando il compito degli aggressori di recuperare e violare le password degli utenti.

W6.2 Sistemi operativi interessati

Tutti i sistemi operativi Microsoft Windows.

W6.3 Riferimenti CVE

Non disponibili.

W6.4 Come determinare se siete vulnerabili

Se utilizzate un'installazione predefinita di NT, 2000 o XP, siete vulnerabili, perché l'impostazione predefinita prevede il salvataggio in locale degli hash del LAN Manager.

Se nel vostro ambiente avete sistemi operativi che richiedono l'autenticazione LM per comunicare con in server, allora siete vulnerabili perché tali macchine inviano gli hash del Lan Manager attraverso la rete, e questi corrono il rischio di essere intercettati.

I più sofisticati strumenti per la determinazione delle password in ambiente Windows come LC4 (l0phtcrack versione 4, disponibile all'indirizzo http://www.atstake.com/research/lc/download.html) vi mostreranno tutti gli hash trovati nel database SAM (LM, NTLM o NTLMv2), e metteranno in evidenza la possibilità di violare ciascun hash. *ATTENZIONE: Non utilizzate mai un password scanner, neanche sui sistemi per i quali avete un accesso da amministratore, senza autorizzazione esplicita e preferibilmente scritta da parte del vostro datore di lavoro. È già accaduto che amministratori di sistema con le migliori intenzioni siano stati licenziati per aver utilizzato strumenti per la determinazione delle password senza autorizzazione.*

W6.5 Come proteggersi

1. *Disabilitare l'autenticazione LM attraverso la rete.* Il modo migliore per sostituire l'autenticazione LAN Manager in Windows è quello di utilizzare NT Lan Manager versione 2 (NTLMv2). I metodi di verifica/risposta di NTLMv2 eliminano la maggior parte dei difetti del Lan Manager utilizzando crittografia più avanzata e meccanismi di autenticazione e per la sicurezza delle sessioni decisamente migliori. La chiave del registro che controlla questa proprietà per Windows NT e 2000 è:

   Hive: HKEY_LOCAL_MACHINE
   Key: System\CurrentControlSet\Control\LSA
   Value: LMCompatibilityLevel
   Value Type: REG_DWORD - Number
   Valid Range: 0-5
   Default: 0

   Descrizione: questi parametri specificano il tipo di autenticazione che sarà utilizzato.
   0 – Spedisce le risposte LM e le risposte NTLM; non usa mai il meccanismo di sicurezza delle sessioni NTLMv2
   1 – Usa meccanismo di sicurezza delle sessioni NTLMv2 se richiesto
   2 – Invia solo l'autenticazione NTLM
   3 – Invia solo l'autenticazione NTLMv2
   4 – DC rifiuta l'autenticazione LM
   5 – DC rifiuta l'autenticazione LM e NTLM (accetta solo NTLMv2)

   Se tutti i vostri sistemi sono Windows NT SP4 o successivi, potete impostare il valore a 3 su tutti i

client e a 5 su tutti i controller di dominio, in modo da evitare qualsiasi trasmissione di hash LM in rete. I sistemi di vecchio tipo (come Windows 95/98) non usano NTLMv2 con il Client di rete Microsoft predefinito. Per implementare le funzionalità NTLMv2, installate il Directory Services Client. Una volta installato, la chiave del registro corrispondente è "LMCompatibility," e i valori consentiti sono 0 o 3.

Se non potete obbligare i vostri client più vecchi ad usare NTLMv2, potete ottenere comunque un certo miglioramento nel sistema di hashing LM forzando NTLM (NT Lan Manager, versione 1) sul controller di dominio (impostate "LMCompatibilityLevel" a 4). Ma l'opzione più sicura riguardo a questi sistemi è quella di passare a sistemi più recenti, dal momento che i sistemi operativi più vecchi non permettono neanche questo minimo livello di sicurezza.

2. *Evitare la memorizzazione degli Hash LM.* Un altro problema che si presenta anche qualora si eviti che gli hash LM vengano inviati attraverso la rete è che gli hash vengono comunque creati e memorizzati nella SAM o Active Directory. Microsoft rende disponibile un meccanismo per evitare la creazione degli hash LM, ma solo in Windows 2000 e XP.
   Sui sistemi Windows 2000, la funzione è controllata da questa chiave del registro:

   Hive: HKEY_LOCAL_MACHINE
   Key: System\CurentControlSet\Control\LSA\NoLMHash

   Se questa chiave viene creata in un Controller di Dominio di Windows 2000, gli hash LanMan non saranno più creati e memorizzati nella Active Directory.
   Su Windows XP, la stessa funzionalità può essere implementata impostando questo valore del registro:

   Hive: HKEY_LOCAL_MACHINE
   Key: System\CurrentControlSet\Control\Lsa
   Value: NoLMHash
   Type: REG_DWORD - Number
   Data: 1

   Dopo aver effettuato queste modifiche al registro, è necessario riavviare il sistema in modo che le nuove impostazioni abbiano effetto. NOTA IMPORTANTE: Questa operazione evita solo che vengano generati nuovi hash LM. Gli hash LM esistenti vengono rimossi singolarmente solo quando l'utente modifica la propria password.

I seguenti articoli di Microsoft forniscono alcune utili indicazioni:

- How to Disable LM Authentication on Windows NT [Q147706] specifica le modifiche al registro richieste per Windows 9x e Windows NT/2000.
- LMCompatibilityLevel and Its Effects [Q175641] spiega i problemi di interoperabilità relativi a questo parametro.
- How to Enable NTLMv2 Authentication for Windows 95/98/2000/NT [Q239869] illustra come utilizzare il Directory Services Client di Windows 2000 in Windows 95/98 per superare i limiti di compatibilità con NTLMv2.
- New Registry Key to Remove LM Hashes from Active Directory and Security Account Manager

W7 Autenticazione generica di Windows - Account senza password o con password deboli

W7.1 Descrizione:

In quasi tutte le interazioni tra gli utenti e i sistemi informativi vengono utilizzate password, frasi identificative o codici di sicurezza. La maggior parte delle forme di autenticazione, come la maggior parte

delle protezioni per file e dati, si basa su password fornite dall'utente. Dal momento che gli accessi correttamente autenticati spesso non vengono registrati, o anche se vengono registrati non lo sono in modo da fornire alcun segnale di allarme, una password compromessa rappresenta un'opportunità di esplorare un sistema dall'interno potenzialmente senza essere identificati. Un aggressore avrebbe accesso completo a qualsiasi risorsa disponibile per quell'utente e sarebbe molto vicino ad essere in grado di accedere ad altri account, a macchine vicine e forse anche ad ottenere privilegi di amministrazione. Nonostante questi pericoli, gli account con password deboli o addirittura senza password rimangono estremamente diffusi e le società con una buona policy sull'utilizzo delle password ancora troppo rare.

Le più comuni vulnerabilità delle password sono dovute (a) ad account senza password o con password deboli, (b) al fatto che, a prescindere dalla robustezza delle password, spesso gli utenti non le proteggono, (c) al fatto che il sistema operativo o il software applicativo creano account di amministrazione con password deboli o privi di password (d) al fatto che gli algoritmi di hashing delle password sono noti e spesso gli hash vengono memorizzati in modo da essere accessibili a chiunque. La difesa migliore e la più corretta contro queste vulnerabilità è una solida policy che includa le istruzioni per creare delle buone password e che riassuma i comportamenti corretti per conservarne la riservatezza, unita a una verifica proattiva dell'integrità delle password.

W7.2 Sistemi operativi interessati

Qualsiasi sistema operativo e applicazione per accedere alla quale gli utenti si autentichino tramite user ID e password.

W7.3 Riferimenti CVE

CAN-1999-0506, CAN-1999-0504, CVE-2000-0222, CAN-1999-0505

W7.4 Come determinare se siete vulnerabili

Per quanto vi siano alcuni sintomi osservabili di una generale debolezza delle password, come la presenza di account attivi appartenenti a utenti che non operano più all'interno dell'organizzazione o a servizi non più attivi, l'unico modo per accertarsi che ogni singola password sia sufficientemente robusta è quello di verificare tutte le password con gli stessi strumenti per la determinazione delle password utilizzati dagli aggressori. *ATTENZIONE: Non utilizzate mai un password scanner, neanche sui sistemi per i quali avete un accesso da amministratore, senza autorizzazione esplicita e preferibilmente scritta da parte del vostro datore di lavoro. È già accaduto che amministratori di sistema con le migliori intenzioni siano stati licenziati per aver utilizzato strumenti per la determinazione delle password senza autorizzazione.*

I migliori strumenti per la determinazione delle password sono:

- LC4 (l0phtcrack versione 4)
- John the Ripper
- Symantec NetRecon

W7.5 Come proteggersi

La difesa migliore e la più corretta contro la debolezza delle password è una solida policy che includa le istruzioni su come generare buone password e descriva i comportamenti corretti per mantenerne la sicurezza, assieme ad una verifica proattiva dell'integrità delle password.

1. *Assicuratevi che le vostre password siano sufficientemente robuste*. Disponendo di tempi e risorse hardware adeguate, qualsiasi password può essere violata utilizzando il sistema "brute force". Ma ci sono metodi più semplici e molto più efficaci per venire a conoscenza delle password con uno sforzo minore. I password cracker utilizzano metodi conosciuti come "attacchi da dizionario". Dal momento che i metodi crittografici sono noti, gli strumenti per l'individuazione delle password non fanno altro che confrontare le password in forma crittata con le forme crittate di parole del dizionario (in diverse

lingue), di nomi propri, e con le permutazioni di entrambi. Di conseguenza una password la cui radice assomigli in qualche modo a una parola è estremamente suscettibile di essere violata da un attacco da dizionario. Molte organizzazioni insegnano ai propri utenti a generare password che includano combinazioni di caratteri alfanumerici e caratteri speciali, e gli utenti la maggior parte delle volte prendono una parola (ad esempio "password") e convertono le lettere in numeri o caratteri speciali ("pa$$w0rd"). Queste permutazioni non proteggono, però, dagli attacchi da dizionario: "pa$$w0rd" ha la stessa possibilità di essere violata di "password."

Una buona password, quindi, non deve avere come radice una parola o un nome proprio. Una solida policy sulle password dovrebbe indirizzare gli utenti verso la creazione di password derivate da qualcosa di più casuale, come una frase o il titolo di un libro o di una canzone. Concatenando una stringa più lunga (prendendo la prima lettera di ogni parola o associando alle parole un carattere speciale o togliendo le vocali, ecc.), gli utenti possono generare stringhe sufficientemente lunghe che combinano caratteri alfanumerici e caratteri speciali in modo tale da creare una grande difficoltà ai tentativi di attacco con metodi da dizionario. E in più se la frase è facile da ricordare, lo sarà anche la password.

Una volta fornite agli utenti le corrette indicazioni su come generare buone password, possono essere messe in opera le procedure per controllare che queste indicazioni vengano seguite. Il modo migliore per farlo è quello di convalidare le password ogni volta che l'utente le cambia, impiegando Passfilt.

Gli strumenti per la determinazione delle password devono essere utilizzati in modalità stand-alone come parte di un esame sistematico. FATE ANCORA ATTENZIONE*: Non utilizzate mai un password scanner, neanche sui sistemi per i quali avete un accesso da amministratore, senza autorizzazione esplicita e preferibilmente scritta da parte del vostro datore di lavoro. È già accaduto che amministratori di sistema con le migliori intenzioni siano stati licenziati per aver utilizzato strumenti per la determinazione delle password senza autorizzazione.* Una volta ricevuta l'autorizzazione ad utilizzare strumenti per la determinazione delle password sul vostro sistema, attivateli regolarmente su una macchina protetta. Gli utenti le cui password vengono violate devono essere avvisati in modo confidenziale e devono essere fornite loro le istruzioni su come scegliere una buona password. Gli amministratori di sistema e il management dovrebbero sviluppare assieme questo tipo di procedure, in modo tale che il management possa provvedere quando gli utenti non rispondono alle notifiche.

Un altro modo per proteggersi da password deboli o assenti è quello di utilizzare forme alternative di autenticazione come token generatori di password o sistemi di autenticazione biometrica. Se avete problemi derivati da password deboli, usate quindi metodi diversi per l'autenticazione degli utenti.

2. *Proteggete le password robuste.* Anche se le password sono robuste, gli account possono essere ugualmente compromessi se gli utenti non proteggono adeguatamente la propria password. Una buona policy include sempre istruzioni che specificano come gli utenti non devono mai riferire la propria password a nessun'altro, non devono mai trascrivere la password in supporti che possano essere letti da altri e devono rendere adeguatamente sicuro qualsiasi file nel quale sia conservata una password per l'autenticazione automatica (le password sono più facili da proteggere quando questa pratica è utilizzata solo quando assolutamente necessario).

   La modifica periodica della password deve essere fatta rispettare in modo che quelle password che non rispettano queste regole siano vulnerabili solo in una finestra temporale limitata, e deve essere tassativamente vietato che le vecchie password possano essere riutilizzate. Controllate che agli utenti giungano gli avvisi e sia data loro le possibilità di modificare la propria password prima della scadenza. Quando si trovano di fronte a frasi come: "la vostra password è scaduta e deve essere cambiata," gli utenti tendono a scegliere una cattiva password.

3. *Controllate rigorosamente gli account.*
   - Qualsiasi account per l'accesso a un servizio e qualsiasi account di amministrazione che non sia più in uso deve essere disabilitato o eliminato. Qualsiasi account per l'accesso a un

servizio e qualsiasi account di amministrazione che siano in uso deve essere forniti di una password solida e recente.
   - Verificate gli account presenti sul vostro sistema e create una master list. Non dimenticate di verificare le password su dispositivi come router e stampanti digitali, fotocopiatrici e controller connessi a Internet.
   - Sviluppate procedure per aggiungere account autorizzati alla lista e per rimuove dalla lista gli account che non sono più in uso.
   - Verificate periodicamente la lista per controllare che non siano stati aggiunti nuovi account e che gli account non più in uso siano stati rimossi.
   - Adottate rigide procedure per la rimozione degli account quando i dipendenti o i collaboratori della società non lavorano più lì o quando gli account non sono più necessari.

4. *Implementate una solida policy per le password in azienda.* In aggiunta ai controlli a livello di sistema operativo o a livello di rete, esistono degli strumenti completi che aiutano a gestire una buona policy per le password. L'Enterprise Security Manager (ESM) di Symantec è uno strumento di monitoraggio che risiede sull'host che evidenzia qualsiasi cambiamento nella policy, la creazione di nuovi account e verifica la robustezza delle password. ESM inoltre può eseguire tentativi per verificare la violabilità delle password in accordo con la policy attiva nella vostra rete. ESM utilizza un ambiente client-manager: l'agente è posto sui server o sulle workstation e invia le segnalazioni a un gestore centralizzato. Utilizzando una console remota, è possibile vedere i log e possono essere generati dei report sullo stato attuale della situazione. ESM verificherà i log e segnalerà qualsiasi modifica che sia stata fatta dalla situazione di partenza.

W8 Internet Explorer

W8.1 Descrizione:

Microsoft Internet Explorer (IE) è il web browser installato di serie sulle piattaforme Microsoft Windows. Tutte le versioni esistenti di Internet Explorer presentano vulnerabilità critiche. È possibile progettare pagine Web che sfruttino queste vulnerabilità sull'Internet Explorer dell'utente che visualizza tali pagine.

Le vulnerabilità possono essere classificate in diverse categorie che comprendono lo spoofing di pagine Web, le vulnerabilità dei controlli ActiveX, le vulnerabilità da Active scripting, l'interpretazione non corretta di MIME-type e di content-type e i buffer overflow. Le conseguenze possono riguardare la rivelazione del contenuto di cookye, file o dati in locale, l'esecuzione di programmi in locale, il download e l'esecuzione di codice arbitrario, fino al controllo completo del sistema vulnerabile.

W8.2 Sistemi operativi interessati

Queste vulnerabilità sono presenti sui sistemi Microsoft Windows con qualsiasi versione di Microsoft Internet Explorer. È importante notare che IE viene installato da una grande varietà di software Microsoft e che quindi è spesso presente su tutti i sistemi Windows, anche sui server per i quali un sistema di navigazione del Web è raramente necessario.

W8.3 Riferimenti CVE

CAN-2002-0193, CAN-2002-0190, CVE-2002-0027, CVE-2002-0022, CVE-2001-0875, CVE-2001-0727, CVE-2001-0339, CVE-2001-0154, CVE-2001-0002

W8.4 Come determinare se siete vulnerabili

Se utilizzate Internet Explorer sul vostro sistema e non avete installato la più recente patch cumulativa, molto probabilmente siete vulnerabili. Se sulla vostra rete è abilitato l'Aggiornamento di Windows, potete verificare sia se IE è effettivamente installato, sia quali patch di Internet Explorer siano presente sul vostro sistema visitando l'indirizzo http://windowsupdate.microsoft.com. Se sul vostro sistema non è disponibile l'Aggiornamento di Windows, potete utilizzare per la verifica HFNetChk (Network Security Hotfix Checker) o il Microsoft Baseline Security Analyzer (MBSA).

Potete anche andare all'indirizzo http://browsercheck.qualys.com per valutare l'effetto di queste vulnerabilità sul vostro sistema.

W8.5 Come proteggersi

Sono disponibili le patch per queste vulnerabilità per le versioni 5.01, 5.5, 6.0 di Internet Explorer. Anche le versioni precedenti di Internet Explorer sono vulnerabili, ma non sono disponibili per queste versioni le patch di alcune vulnerabilità. Se sul vostro sistema è attiva una versione precedente di IE, dovreste prendere in considerazione un aggiornamento.

Se utilizzate IE 5.01 o successivo, iniziate installando il service pack per Internet Explorer più recente. Potete trovare le versioni più aggiornate agli indirizzi:

- Internet Explorer 6, service pack 1
- Internet Explorer 5.5, service pack 2
- Internet Explorer 5.01, service pack 2

Dopo aver installato il service pack 2 per IE 5.5 o IE 5.01, dovete anche aggiungere la più recente cumulative security patch (Q323759), che rimedia ad ulteriori vulnerabilità. (Questa patch è già inclusa nel service pack 1per IE 6.) Per maggiori informazioni riguardo le vulnerabilità a cui rimedia questa patch e le modifiche appropriate da apportare alla vostra configurazione per mitigare i rischi, verificare il relativo Security Bulletin e il corrispondente Knowledge Base article.

Ciascuno di questi articoli discute una variante della vulnerabilità cross-site scripting, della quale qualche aspetto non viene completamente risolto dalla patch. Per ulteriori informazioni, andate all'indirizzo http://sec.greymagic.com/adv/gm010-ie/. Di solito è buona prassi disabilitare gli script quando non sono necessari.

Per mantenere protetto il vostro sistema, seguite costantemente le uscite di nuovi aggiornamenti di IE utilizzando Windows Update, HFNetChk, o il Microsoft Baseline Security Analyzer (MBSA). Potete anche ottenere informazioni generali sugli aggiornamenti di IE dalla Internet Explorer Home.

W9 Accesso remoto al Registro

W9.1 Descrizione:

Microsoft Windows 9x, Windows CE, Windows NT, Windows 2000 e Windows XP impiegano un database gerarchico centralizzato, meglio conosciuto come Registro, per gestire il software, la configurazione dei dispositivi e le impostazioni degli utenti.
Permessi o impostazioni di sicurezza non corretti possono permettere un accesso remoto al Registro. È possibile sfruttare questo fatto per compromettere il sistema o porre le basi per adattare l'associazione dei file e i permessi in modo da consentire l'esecuzione di codice dannoso.

W9.2 Sistemi operativi interessati

Tutte le versioni di Microsoft Windows 9x, Windows CE, Windows NT, Windows 2000 e Windows XP.

W9.3 Riferimenti CVE

CAN-1999-0562, CVE-2000-0377, CVE-2000-0663, CVE-2002-0049, CAN-2001-0045, CAN-2002-0642

W9.4 Come determinare se siete vulnerabili

L'NT Resource Kit (NTRK) disponibile presso Microsoft contiene un file eseguibile denominato "regdump.exe" che verifica passivamente i permessi per l'accesso remoto al Registro da un host Windows NT verso altri host Windows NT/Windows 2000 o Windows XP attraverso Internet o la rete interna.

Oltre a ciò, è possibile scaricare una raccolta di shell script a linea di comando che verificano i permessi di accesso al vostro Registro, oltre a una serie di altre caratteristiche che riguardano la sicurezza. È disponibile all'indirizzo http://www.afentis.com/top20.

W9.5 Come proteggersi

Per far fronte a questa minaccia, l'accesso al Registro di sistema deve essere limitato e devono essere rivisti i permessi impostati per le chiavi del Registro più critiche. Prima di ottimizzare il Registro, gli utenti di Microsoft Windows NT 4.0 devono anche assicurarsi che sul loro sistema sia già installato il Service Pack 3 (SP3). *ATTENZIONE: Le modifiche al Registro di sistema possono comportare seri effetti sulle performance e sull'operatività del computer e, in casi estremi, possono causare danni irreparabili e richiedere la reinstallazione del sistema operativo.*

- *Limitate l'accesso dalla rete.* Per limitare l'accesso al Registro dalla rete, seguite i passi elencati qui sotto per creare la seguente chiave di Registro:
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
  - Descrizione: REG_SZ
  - Valore: Registry Server

  I permessi di sicurezza impostati in questa chiave definiscono gli Utenti o i Gruppi ai quali è permesso l'accesso remoto al Registro. L'istallazione preimpostata di Windows definisce questa chiave e imposta l'Access Control List per fornire pieni privilegi all'Amministratore del sistema e al Gruppo degli Amministratori (e ai Backup Operators in Windows 2000).
  Le modifiche al Registro di sistema richiedono un riavvio per avere effetto. Per creare la chiave di Registro che limita l'accesso al registro:

  1. Avviate l'Editor di Registro ("regedt32.exe" or "regedit.exe") e andate alla seguente sottochiave:

     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

  2. Dal menu "Modifica", selezionate "Nuova Chiave".
  3. Inserite i seguenti valori:

     Nome chiave: SecurePipeServers
     Tipo: REG_SZ

  4. Andate alla seguente sottochiave:

     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers

  5. Dal menu "Modifica", selezionate "Nuova Chiave".
  6. Inserite i seguenti valori:

     Nome chiave: winreg
     Tipo: REG_SZ

  7. Andate alla seguente sottochiave:

     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

  8. Dal menu "Modifica", selezionate "Nuova Chiave".
  9. Inserite i seguenti valori:

     Nome valore: Description

Tipo: REG_SZ
Valore: Registry Server

10. Andate alla seguente sottochiave:

    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

11. Selezionate "winreg." Cliccate "Security" e quindi "Permissions." Aggiungete gli Utenti o i Gruppi ai quali volete fornire l'accesso.
12. Uscite dall'Editor di Registro e riavviate Microsoft Windows.
13. Se in un momento successivo volete cambiare la lista degli utenti che possono accedere al registro, ripetete i passi 10-12.

- *Limitate gli accessi remoti autorizzati.* Applicare limitazioni troppo ristrette sul registro può avere effetti secondari su servizi dipendenti quali il Directory Replicator e il servizio di spooling per le stampanti di rete.

  È possibile aggiungere un grado di granularità ai permessi, aggiungendo il nome di account per il quale il servizio funziona all'access list della chiave "winreg", oppure configurando Windows in modo che ignori le restrizioni di accesso per certe chiavi elencandole nei valori Machine o User sotto la chiave 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: (Un percorso valido a un indirizzo del registro)
  Description: Allow machines access to listed locations in the registry provided
  that no explicit access restrictions exist for that location.
  Value: Users
  Value Type: REG_MULTI_SZ - Multi string
  Default Data: (none)
  Valid Range: (Un percorso valido a un indirizzo del registro)
  Description: Allow users access to listed locations in the registry provided
  that no explicit access restrictions exist for that location.

  Nel Registro di Microsoft Windows 2000 e Windows XP:

  Value: Machine
  Value Type: REG_MULTI_SZ - Multi string
  Default Data: System\CurrentControlSet\Control\ProductOptionsSystem\
  CurrentControlSet\Control\Print\PrintersSystem\CurrentControlSet\
  control\Server ApplicationSystm\CurrentControlSet\Services\Eventlog\
  Software\Microsoft\Windows NT\CurrentVersion
  Value: Users (non esiste per default)

Per maggiori informazioni, leggete il Microsoft Knowledge Base Article Q153183, How to Restrict Access to NT Registry from a Remote Computer.

W10 Windows Scripting Host

W10.1 Descrizione:

Nella primavera del 2000, uno script di Visual Basic (VBScript), il worm "Love Bug" (conosciuto anche come virus "ILOVEYOU"),ha causato danni per milioni di dollari. Questo worm, come gli altri che sono arrivati dopo, sfruttano il Windows Scripting Host (WSH), che permette a qualsiasi file di testo con estensione ".vbs" di essere eseguito come uno script di Visual Basic. Se WSH è abilitato, un tipico worm si propaga includendo un VBScript come contenuto di un altro file che si esegue quando tale file viene visto, in qualche caso anche solo in anteprima.

Anche se gli amministratori devono sempre controllare che applicativi come browser, client di posta o le suite che li contengono siano sempre aggiornati alle versioni più recenti e siano loro applicate le ultime patch, aggiornare queste applicazioni per eliminare la possibilità che siano colpite da un particolare worm è una soluzione non definitiva (non migliore di una semplice reazione) ai rischi derivati dallo scripting. Windows Scripting Host può essere disabilitato senza problemi, compiendo così una mossa preventiva per impedire la proliferazione dei worm.

W10.2 Sistemi operativi interessati

Windows Scripting Host può essere installato manualmente o con Internet Explorer 5 (o successivi) su Windows 95 o NT. È invece installato per default sulle macchine con Windows 98, ME, 2000 e XP.

W10.3 Riferimenti CVE

CAN-2001-1325, CVE-2001-0149

W10.4 Come determinare se siete vulnerabili

Se utilizzate Windows 95 o NT con IE 5 o successivi, o utilizzate Windows 98, ME, 2000 o XP e non avete disabilitato WSH, allora siete vulnerabili.

W10.5 Come proteggersi

- Disabilitate o rimuovete del tutto Windows Scripting Host, come sottolineato anche nelle istruzioni fornite da Symantec e Sophos.
- Aggiornate sempre il vostro software Anti-Virus e le relative definizioni. Alcuni Anti-Virus presentano anche un'opzione che blocca gli script.

U1 Remote Procedure Call (RPC)

U1.1 Descrizione

Le Remote Procedure Call (RPC) consentono ai programmi di un computer di eseguire programmi presenti su un altro computer passando loro i dati e recuperando i risultati. Le RPC vengono quindi largamente utilizzate in diversi servizi di rete come l'amministrazione da remoto, la condivisione dei file NFS e NIS. Nelle RPC vi sono però diverse imperfezioni che possono essere sfruttate. In molti casi i servizi RPC vengono eseguiti con privilegi di root, facendo di conseguenza correre gravi rischi ai sistemi che presentano vulnerabilità nei servizi RPC che possono portare un aggressore ad ottenere un accesso root non autorizzato da remoto. Ci sono prove convincenti che la maggior parte degli attacchi del tipo "distributed denial of service" verificatisi durante il 1999 ed i primi mesi del 2000 siano stati eseguiti da sistemi vittime delle vulnerabilità RPC. Anche il massiccio attacco riuscito ai danni dei sistemi delle forze armate americane durante l'incidente Solar Sunrise ha sfruttato vulnerabilità dell' RPC riscontrate su centinaia di sistemi del Dipartimento della Difesa.

U1.2 Sistemi interessati:

Quasi tutte le versioni di Unix e Linux istallano automaticamente, e spesso attivano, servizi RPC.

U1.3 Lista CVE:

CVE-1999-0166, CVE-1999-0167, CVE-1999-0168, CVE-1999-0170, CVE-1999-0211, CVE-1999-0977, CVE-1999-0018, CVE-2000-0666, CVE-1999-0002, CVE-2001-0803, CVE-1999-0493, CAN-2002-0573, CVE-2001-0717, CVE-1999-0003, CVE-1999-0019, CVE-1999-0208, CVE-1999-0696, CVE-1999-0693, CVE-1999-0008, CVE-2001-0779, CAN-2002-0033, CAN-2002-0391, CAN-2002-0677, CAN-2002-0679,

U1.4 Come stabilire se siete vulnerabili:

Utilizzate un vulnerability scanner o il comando 'rpcinfo' per verificare se state utilizzando uno dei servizi RPC più comunemente sfruttati:

Servizio RPC	*Numero programma RPC*
rpc.ttdbserverd	100083
rpc.cmsd	100068
rpc.statd	100024
rpc.mountd	100005
sadmind	100232
cachefsd	100235
snmpXdmid	100249

I servizi RPC vengono generalmente sfruttati per attacchi del tipo "buffer overflow", che hanno successo perché i programmi RPC non eseguono un controllo appropriato degli errori o una adeguata convalida degli input. Le vulnerabilità del tipo "buffer overflow" consentono agli aggressori di inviare dati che il programma non si aspetta (spesso in forma di codice dannoso) nello spazio di memoria del programma. A causa dello scarso controllo errori e dell'insufficiente convalida degli input, i dati sovrascrivono le parti di memoria che sono pronte ad essere eseguite dal processore. In un attacco overflow riuscito, questo codice dannoso viene quindi eseguito dal sistemo operativo. Dal momento che molti servizi RPC vengono eseguiti con privilegi di root, sfruttando un di questi servizi è possibile ottenere da remoto un accesso root al sistema non autorizzato.

U1.5 Come proteggersi:

1. Disattivate o rimuovete tutti i servizi RPC che non sono strettamente necessari all'operatività della vostra rete.
2. Installate le patch più recenti per tutti i servizi che non potete rimuovere:

   Patch per Sotware Solaris:
   http://sunsolve.sun.com

   Patch per Software IBM AIX:
   http://www.ibm.com/support/us
   http://techsupport.services.ibm.com/server/fixes

   Patch per Software SGI:
   http://support.sgi.com

   Patch per Software Compaq (Digital Unix):
   http://www.compaq.com/support

   Patch per Software Linux:
   http://www.redhat.com/apps/support/errata
   http://www.debian.org./security

3. Verificate regolarmente se il produttore distribuisce nuove patch e installatele immediatamente.
4. Bloccate la porta RPC (porta 111) a livello di router o firewall perimetrale.
5. Bloccate le porte RPC di "loopback" 32770-32789 (TCP e UDP).
6. Nei sistemi operativi che lo permettono, abilitate uno stack non-eseguibile. Anche se uno stack non-eseguibile non protegge da tutti i buffer overflow, può ostacolare lo sfruttamento di alcuni buffer overflow standard pubblicamente disponibili in Internet.
7. Per i file system esportati in NFS, si può prevedere i seguenti accorgimenti:
   1. Usate una export list basata su host/IP.
   2. Se possibile, impostate il file system esportato come no-suid o per sola lettura.
   3. Utlizzate 'nfsbug' per rintracciare le vulnerabilità.

Potete trovare un documento di sintesi che riporta indicazioni specifiche sulle tre principali vulnerabilità RPC - Tooltalk, Calendar Manager e Statd - all'indirizzo: http://www.cert.org/incident_notes/IN-99-04.html

Si possono reperire documenti che riguardano le specifiche vulnerabilità RPC agli indirizzi:

- Statd: http://www.cert.org/advisories/CA-2000-17.html
  http://www.cert.org/advisories/CA-1999-05.html
  http://www.cert.org/advisories/CA-1997-26.html
- Tooltalk: http://www.cert.org/advisories/CA-2002-26.html
  http://www.cert.org/advisories/CA-2002-20.html
  http://www.cert.org/advisories/CA-2001-27.html
- Calendar Manager: http://www.cert.org/advisories/CA-2002-25.html
  http://www.cert.org/advisories/CA-1999-08.html
- Cachefsd: http://www.cert.org/advisories/CA-2002-11.html
- Sadmind: http://www.cert.org/advisories/CA-1999-16.html
  http://www.cert.org/advisories/CA-2001-11.html
- Mountd: http://www.cert.org/advisories/CA-1998-12.html
- SnmpXdmid: http://www.cert.org/advisories/CA-2001-05.html

U2 Web Server Apache

U2.1 Descrizione

Gli amministratori di server Web troppo spesso concludono che poichè l'Internet Information Server (IIS) di Microsoft è particolarmente soggetto ad essere violato (vedi W1. Internet Information Server), il web server open-source Apache è completamente sicuro. Per quanto possa essere condivisibile il confronto con IIS, e nonostante Apache goda di una meritata reputazione di sicurezza, ad una attenta analisi anche questo web server non è invulnerabile.

I metodi per violare Apache o i suoi moduli nel recente passato sono state pochi, ma molto ben documentati e velocemente utilizzati in attacchi concreti. Tra i più recenti vi sono:

- Apache/mod_ssl Worm (CERT Advisory CA-2002-27)
- Apache Chunk Handling Exploit (CERT Advisory CA-2002-17)

In definitiva, nessun web server può essere considerato sicuro finché non viene analizzato nel contesto della sua interazione con le diverse applicazioni web, in particolare con i programmi CGI e con i database. Anche una configurazione particolarmente sicura di Apache può permettere l'accesso non autorizzato ai dati se gli script non sono attentamente verificati o i controlli d'accesso ai database non sono correttamente configurati. Gli script CGI vengono eseguiti con gli stessi permessi del web server, e così uno script CGI fatto ad arte o semplicemente scritto non correttamente può essere altrettanto pericoloso di una vulnerabilità nel software di Apache. Sfortunatamente queste debolezze nel back end del web server rimangono problemi di stretta attualità.

È anche necessario rafforzare la sicurezza del sistema operativo per impedire che i contenuti web vengano sottratti o modificati. Per quanto ciò valga per tutti i servizi attivi, il fatto che i servizi web tendano ad avere una esposizione verso l'esterno si presta alla falsa idea che essi ed i dati che proteggono siano in qualche modo indipendenti dal resto del sistema. Quanto l'omissione di questa attività possa rendere vulnerabile un sistema è spiegato su http://www.wired.com/news/technology/0,1282,43234,00.html.

U2.2 Sistemi interessati:

Quasi tutti i sistemi Linux e molti altri sistemi Unix si presentano con Apache pre-installato e abilitato. Tutti i sistemi Unix sono in grado di far girare Apache. (Gli amministratori di Windows devono fare altrettanta attenzione perché la versione di Apache per Windows è ugualmente soggetta alle stesse vulnerabilità o comunque a vulnerabilità simili.)

U2.3 Lista CVE:

CAN-2002-0392, CAN-2002-0061, CVE-1999-0021, CVE-1999-0172, CVE-1999-0266, CVE-1999-0067, CVE-1999-0260, CVE-1999-0262, CVE-2000-0010, CVE-1999-0174, CVE-1999-0066, CVE-1999-0146, CAN-2002-0513, CAN-2002-0682, CAN-2002-0257, CVE-2000-0208, CVE-2000-0287, CVE-2000-0941, CAN-2000-0832, CVE-1999-0070, CVE-2002-0082, CAN-2002-0656, CAN-2002-0655, CVE-2001-1141, CAN-2002-0657, CAN-1999-0509, CVE-1999-0237, CVE-1999-0264

U2.4 Come stabilire se siete vulnerabili:

Controllate quale sia la versione più recente e il più recente livello di patch sul sito di Apache: http://httpd.apache.org. Se la vostra versione non è la più recente, il vostro server è probabilmente vulnerabile. Su questo sito troverete anche una lista aggiornata delle vulnerabilità più recenti e la documentazione su come determinare se siete affetti da tali vulnerabilità.

U2.5 Come proteggersi:

Le seguenti istruzioni possono aiutarvi a proteggere un web server Apache:

1. Recuperate da Apache le patch più recenti all'indirizzo http://www.apache.org/dist/httpd/patches/. Se possibile, aggiornate alla versione più recente.
2. Modificate l'HTTP Response token di default di Apache. Ciò farà in modo che il vostro server Apache restituisca false informazioni nel suo header di risposta, aiutando a nascondere il software del web server. Anche se questa tecnica non impedisce a un determinato aggressore di scoprire quale sia il vostro software, può fare molto per proteggere il vostro web server Apache da worm che innescano il loro codice di attacco basandosi sulle informazioni ricevute in risposta dagli header. Seguite la discussione di Security Focus su come ciò possa proteggere dall' Apache/mod_ssl Worm descritto nel CERT Advisory CA-2002-27.
3. Compilate solo i moduli di Apache necessari per il corretto funzionamento del vostro server. Come per un sistema operativo sul quale girano servizi inutili, lo stesso Apache dovrebbe essere ridotto al minimo per diminuire l'esposizione a futuri problemi di sicurezza.
4. Considerate la possibilità di eseguire Apache in un ambiente chroot(). Per evitare che vengano eseguite con successo le richieste HTTP dannose, un web server dovrebbe essere configurato per inizializzarsi con la funzione chroot() di Unix. Quando un web server parte in chroot, è posto in un ambiente che si potrebbe definire una "Botte di ferro". Da questa configurazione il web server non può accedere ad alcuna parte della struttura delle directory del sistema operativo al di fuori dell'area chroot() definita. Ciascun web server implementa chroot() in modo diverso, e quindi è necessario consultare la documentazione del software specifico per qualsiasi istruzione. Potete comunque trovare ulteriori informazioni nelle WWW Security FAQ.
5. Non eseguite Apache come root. Create un nuovo utente con privilegi minimi sulla vostra rete e nel database offerto dai vostri servizi web ed eseguite Apache con tale utente. NON usate l'account nobody, perché questo account è utilizzato per mappare l'account di root account su NFS.
6. Eliminate i contenuti html di default, inclusi i due script CGI test-cgi e printenv. Le vulnerabilità presenti nei contenuti di default sono molto ben conosciute e frequentemente sfruttate negli attacchi.
7. Da tenere presente nella gestione degli script CGI:
    - Non configurate il supporto CGI sui Web Server che non ne hanno bisogno.
    - Rimuovete tutti i programmi CGI di esempio dai vostri web server operativi.
    - Analizzate gli script CGI che rimangono ed eliminate dai web server qualsiasi CGI non sicuro.
    - Assicuratevi che tutti i programmatori di CGI aderiscano a una rigida policy che prescriva il controllo della lunghezza del buffer di input nei programmi CGI.
    - Controllate che la vostra directory CGI bin non contenga alcun compilatore o interprete.
    - Eliminate lo script "view-source" dalla directory cgi-bin.
    - Configurate il vostro server Apache perché usi il sistema di avvisi che segnala gli errori degli script CGI. Gli amministratori web hanno bisogno di tenere delle tabelle su tutte queste problematiche di sicurezza collegate ai loro web server. Per aiutare in questo monitoraggio, il web server dovrebbe essere configurato per utilizzare pagine per la risposta agli errori CGI che siano personalizzate, in particolare per i codici di errore 401, 403, 413 e 500. Le pagine di errore sono script CGI in PERL che vengono attivati ogni volta che il server riscontra uno di questi codici di errore. Questi script Questi script sovrintendono a molte importanti funzioni come quella di pubblicare un messaggio di avviso per il client e di spedire immediatamente una notifica via e-mail all'Amministratore. Il messaggio e-mail rende automatico il processo di raccolta dal web server delle informazione di sessione correlate alla sicurezza e degli error log.
    - Non permettete l'indexing delle directory. La visualizzazione del contenuto delle directory può fornire ad un aggressore troppe informazioni riguardo alla struttura delle directory del vostro sito e sulle convenzioni che utilizzate nella denominazione dei file.
    - Non usate Server Side Include (SSI). SSI può potenzialmente portare ad usi non autorizzati e fare in modo che il web server esegua codice del sistema operativo che non era stato previsto dallo sviluppatore.
    - Allo scopo di limitare le directory che possono essere servite ai client, non permettete al server Apache di seguire collegamenti simbolici.
    - Create degli script CGI di avviso per l'identificazione di CGI Scanner. Utilizzate uno script CGI di avviso e rinominatelo chiamandolo come uno dei CGI più vulnerabili come: test-cgi,

phf, php.cgi, ecc. Quando un CGI Vulnerability scanner viene eseguito contro il vostro web server, esegue questi script che avvisano via e-mail l'amministratore.

8. Il suggerimento forse più importante di tutti è quello di controllare che il sistema operativo e i servizi che stanno sotto il vostro web server siano rafforzati, o tutti i provvedimenti suggeriti fin qui risulteranno inutili. Seguite ciò che è descritto negli altri punti di questo documento, nelle SANS Consensus Security Guides, e nei Center for Internet Security's Benchmarks.

Per ulteriori informazioni di sicurezza su Apache, consultate http://www.sans.org/Gold/apache.php e http://www.infosecuritymag.com/articles/april01/features1_web_server_sec.shtml.

U3 Secure Shell (SSH)

U3.1 Descrizione

Secure shell (ssh) è un popolare servizio per rendere sicuri i login, l'esecuzione di comandi e il trasferimento di file attraverso una rete. La maggior parte dei sistemi utilizza il pacchetto open-source OpenSSH o la versione commerciale di SSH Communication Security. Per quanto ssh sia largamente più sicuro dei programmi di telnet, ftp, e R-command per sostituire i quali è stato progettato, sono state riscontrate diverse falle in entrambi i pacchetti citati. Si tratta per la maggior parte di bachi di minore importanza, ma alcuni costituiscono dei problemi di sicurezza che devono essere riparati immediatamente. Il più pericoloso di questi buchi di sicurezza attivamente sfruttati permette agli aggressori di ottenere da remoto un accesso root alla macchina.

È stato dimostrato che lo stesso protocollo SSH1 è potenzialmente vulnerabile e in certe configurazioni può permettere la decifratura di una sessione in transito. Per questo invitiamo gli amministratori ad utilizzare, quando possibile, il più solido protocollo SSH2.

Oltre a ciò, gli utenti di OpenSSH devono stare attenti al fatto che le librerie OpenSSL sulle quali di solito OpenSSH è installato presentano a loro volta delle vulnerabilità. Leggete i CERT Advisory 2002-23 per maggiori dettagli. Devono stare anche attenti al fatto che, anche se per un breve periodo di tempo, nell'estate 2002 è stata distribuita una versione di OpenSSH che conteneva un trojano. Leggete http://www.openssh.org/txt/trojan.adv per i dettagli e per controllare che non si tratti della versione che state utilizzando.

U3.2 Sistemi interessati:

Qualsiasi sistema Unix o Linux che esegua OpenSSH 3.3 o precedenti, oppure SSH 3.0.0 o precedenti di SSH Communication Security.

U3.3 Lista CVE:

Per ssh di SSH Communication Security: CVE-2000-0575, CVE-2000-0992, CVE-2001-0144, CVE-2001-0361, CAN-2001-0471, CVE-2001-0553, CVE-2001-0259

Per OpenSSH: CVE-2000-1169, CVE-2001-0144, CVE-2001-0361, CVE-2001-0872, CVE-2000-0525, CAN-2001-0060, CAN-2002-0002, CAN-2002-0575, CAN-2002-0639, CAN-2002-0083, CAN-2002-0640, CAN-2002-0656, CAN-2002-0655, CVE-2001-1141, CAN-2002-0657

U3.4 Come stabilire se siete vulnerabili:

Utilizzate un vulnerability scanner per controllare se state utilizzando una versione vulnerabile o verificate la versione del software riportata eseguendo il comando 'ssh -V'.

U3.5 Come proteggersi:

1. Passate alla versione più recente di OpenSSH o SSH. Oppure, se SSH o OpenSSH sono preistallati nel vostro sistema operativo, recuperate le patch più recenti presso il produttore del vostro sistema operativo. Se usate OpenSSL, controllate che usi le librerie nella versione più recente.

2. Se possibile, evitate di utilizzare il protocollo SSH1, che presenta alcune note debolezze già corrette nel protocollo SSH2.
3. Entrambe le implementazioni di ssh comprendono una varietà di opzioni di configurazione per limitare le macchine che possono connettersi e per indicare quali utenti possano autenticarsi per definire attraverso quali meccanismi debbano avvenire queste operazioni. Gli amministratori dovrebbero scegliere quali di queste opzioni può risultare più appropriata per il loro ambiente.

U4 Simple Network Management Protocol (SNMP)

U4.1 Descrizione

Il Simple Network Management Protocol (SNMP) è largamente utilizzato per controllare e configurare da remoto quasi tutti i tipi di dispositivi TCP/IP moderni. Anche se SNMP è supportato nelle sue varie distribuzioni da quasi tutte le piattaforme di rete, è usato più di frequente come metodo per configurare e gestire dispositivi quali stampanti, router e switch e per inviare input a servizi di monitoraggio della rete.

La comunicazione Simple Network Management consiste in diversi tipi di messaggi scambiati tra le stazioni di gestione SNMP e i dispositivi di rete che eseguono quello che comunemente è definito come agent software. Sia metodologia con la quale questi messaggi sono trattati, sia il meccanismo di autenticazione che sottende a tale trattamento, presentano significative vulnerabilità.

Le vulnerabilità che stanno dietro il metodo attraverso il quale la versione 1 di SNMP tratta e cattura i messaggi è descritta in dettaglio nel CERT Advisory CA-2002-03. Esistono una serie di vulnerabilità nel modo in cui i messaggi di richiesta e cattura sono gestiti e decodificati dalle stazioni di gestione e dagli agenti. Queste vulnerabilità non sono limitate a una specifica implementazione di SNMP, ma affliggono una varietà di distribuzioni di SNMP di diversi produttori. Sfruttando queste vulnerabilità gli aggressori possono arrivare a risultati che variano dal denial of service alla modifica della configurazione e del sistema di gestione delle macchine abilitate all'SNMP.

Il meccanismo interno di autenticazione dei protocolli SNMP meno recenti presenta anche un'altra importante vulnerabilità. Le versioni 1 e 2 di SNMP utilizzano un meccanismo di autenticazione "community string" non crittata. La mancanza di crittografia è già abbastanza grave, ma in più la community string usata per default nella grande maggioranza dei dispositivi SNMP è "public," e solo pochi produttori più accorti di apparati di rete la modificano in "privata" per il trattamento delle informazioni più sensibili. Gli aggressori possono sfruttare la vulnerabilità di SNMP per riconfigurare o per spegnere i dispositivi da remoto. Lo sniffing del traffico SNMP può rivelare molti dettagli relativi alla struttura della vostra rete e ai dispositivi ad essa collegati Gli intrusi utilizzano queste informazioni per scegliere gli obiettivi e per pianificare gli attacchi.

A dispetto del fatto che queste vulnerabilità sono presenti solo nelle prime versioni dei protocolli SNMP, molti produttori abilitano per default la versione 1 di SNMP. Molti non offrono prodotti in grado di utilizzare SNMP versione 3, che non presenta nessuna di queste vulnerabilità congenite. In ogni caso esistono dei sostituti gratuiti che provvedono a fornire il supporto SNMPv3 con licenza GPL o BSD.

SNMP non è un'esclusiva di Unix e viene usato diffusamente anche in Windows per apparati di rete, stampanti e altri dispositivi. La maggior parte degli attacchi che si appoggiano a SNMP finora riscontrati si è presentata però su sistemi UNIX con configurazioni non corrette.

U4.2 Sistemi interessati:

Quasi tutti i sistemi Unix e Linux sono distribuiti con l'SNMP installato e spesso abilitato per default. Anche la maggior parte degli altri sistemi operativi e dispositivi compatibili con SNMP sono vulnerabili.

U4.3 Lista CVE:

CAN-2002-0013, CAN-2002-0797, CAN-2002-0012, CAN-2002-0796, CAN-1999-0516, CAN-1999-0517, CAN-1999-0254, CAN-1999-0186, CAN-1999-0615, CVE-2001-0236,

U4.4 Come stabilire se siete vulnerabili:

Potete verificare se SNMP è attivo sui dispositivi connessi alla vostra rete adoperando uno scanner o effettuando un controllo manuale.

SNMPing – Potete richiedere lo strumento di scanning gratuito SNMPing al SANS Institute inviando un messaggio vuoto a snmptool@sans.org. Riceverete un messaggio di risposta con l'URL dal quale potrete scaricare lo strumento.

SNScan – Foundstone ha creato un altro strumento per lo scanning SNMP di semplice uso chiamato SNScan, che può essere scaricato da http://www.foundstone.com/knowledge/free_tools.html.

Se non potete utilizzare uno degli strumenti sopra citati, avete la possibilità di verificare manualmente se SNMP è attivo sui vostro sistemi. Consultate la documentazione del vostro sistema operativo per le indicazioni su come identificare l'implementazione specifica di SNMP, il daemon di base può di solito essere identificato trovando "snmp" nella process list o cercando tra i servizi che girano sulle porte 161 o 162. Consultate il CERT Advisory CA-2002-03 per ulteriori informazioni.

Se SNMP è attivo e riscontrate una delle seguenti variabili, potreste soffrire di una vulnerabilità legata a una stringa di default o comunque troppo facile da indovinare:

1. Community name SNMP vuoti o di default.
2. Community name SNMP facili da indovinare.
3. Community string SNMP nascoste.

Leggete http://www.sans.org/newlook/resources/IDFAQ/SNMP.htm per informazioni su come identificare la presenza di queste condizioni..

U4.5 Come proteggersi:

- *Vulnerabilità di cattura e gestione della richiesta:*
    1. Se non avete necessità assoluta di utilizzare l'SNMP, disabilitatelo.
    2. Quando possibile, utilizzate SNMP versione 3.
    3. Se dovete usare SNMPv1 o v2, controllate di aver installato la patch più recente rilasciata dal vostro produttore. Un buon punto di partenza per ottenere le informazioni specifiche per ciascun produttore è consultare l'Appendice A del CERT Advisory CA-2002-03.
    4. Filtrate SNMP (porte 161 TCP/UDP e 162 TCP/UDP) ai punti di ingresso delle vostre reti, a meno che non sia assolutamente necessario effettuare il polling o gestire i dispositivi dall'esterno della rete locale.
    5. Sui sistemi con gli agenti SNMP effettuate un controllo degli accessi basato sugli host. Anche se questa possibilità dipende dalle funzionalità del sistema che ospita gli agenti SNMP, è possibile effettuare comunque un controllo per verificare da quali sistemi i vostri agenti accettano richieste. Sulla maggior parte dei sistemi Unix è possibile effettuare questo controllo configurando TCP-Wrappers o Xinetd. Potete anche usare un firewall che effettui il packet filtering sugli agenti per bloccare le richieste SNMP indesiderate.

- *Vulnerabilità correlate alle stringhe di default o troppo semplici da indovinare:*
    1. Se non avete necessità assoluta di utilizzare l'SNMP, disabilitatelo.
    2. Quando possibile, utilizzate SNMP versione 3.
    3. Se dovete usare SNMPv1 o v2, utilizzate per i community name la stessa policy che usate per le password. Assicuratevi che siano difficili da indovinare o da violare e che siamo periodicamente modificati.
    4. Controllate e convalidate i community name utilizzando snmpwalk. Potete trovare maggiori informazioni su http://www.zend.com/manual/function.snmpwalk.php. Una buona guida per questo strumento è reperibile all'indirizzo http://www.sans.org/newlook/resources/IDFAQ/SNMP.htm.

5. Filtrate SNMP (porte 161 TCP/UDP e 162 TCP/UDP) ai punti di ingresso delle vostre reti, a meno che non sia assolutamente necessario effettuare il polling o gestire i dispositivi dall'esterno della rete locale.
6. Dove possibile, impostate le MIB in sola lettura. Potete trovare maggiori informazioni sull'argomento all'indirizzo http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#xtocid210315.

U5 File Transfer Protocol (FTP)

U5.1 Descrizione

Il daemon FTP viene utilizzato per distribuire file ad utenti anonimi o autenticati con username e password. I servizi FTP anonimi non richiedono una password univoca (vale per tutti) e tutti gli utenti usano lo stesso nome di login ("anonymous" o "ftp"), così da permettere a chiunque l'accesso al servizio.

Il servizio FTP autenticato richiede invece un username e una password, ma entrambi vengono trasmessi in chiaro attraverso la rete, consentendo a un terzo di intercettarli durante lo scambio di credenziali. Per sottrarre le informazioni di login FTP, un aggressore ha bisogno di piazzare un network sniffer da qualche parte lungo il percorso di connessione come, ad esempio, sul server FTP della LAN o sul client LAN. Questi sniffer sono stati utilizzati in molti episodi recenti che hanno riguardato la sicurezza.

Oltre a questa insita insicurezza nella trasmissione, sono state rilevate diverse vulnerabilità gravi in molte versioni dei software FTP server, sia in quelle fornite da produttori di sistemi operativi (Sun, HP-UX, ecc), sia in quelle sviluppate dalla comunità open source (WU-FTPD, ProFTPD, ecc). Molti degli attacchi che sfruttano queste vulnerabilità permettono all'aggressore di ottenere un accesso root alla macchina che ospita il server FTP, mentre altri permettono semplicemente l'esecuzione di comandi a livello di utente. La recente vulnerabilità di WU-FTPD, ad esempio, permette agli aggressori di ottenere un accesso root e di caricare sul sistema strumenti come i "rootkits", ed utilizzare quindi il sistema per i loro intenti. La maggior parte dei sistemi di attacco a queste vulnerabilità richiede che sia abilitato l'accesso anonimo, ma qualcuno funziona anche quando l'accesso anonimo viene negato a condizione che il server FTP ascolti la porta della rete. È da notare che anche se il server FTP usa una chiamata chroot() al sistema per confinare l'utente anonimo in una specifica directory, può essere ugualmente attaccato se presenta dei bachi importanti nell'implementazione.

U5.2 Sistemi interessati:

Quasi tutti i sistemi Unix e Linux sono distribuiti con almeno un FTP server installato e spesso abilitato per default.

U5.3 Lista CVE:

CVE-1999-0368, CVE-2001-0550, CVE-1999-0080, CVE-1999-0878, CVE-1999-0879, CVE-1999-0950, CAN-2001-0249, CAN-1999-0527, CAN-1999-0911, CVE-1999-0955, CVE-2000-0573, CVE-2001-0187, CAN-2001-0935, CVE-1999-0880, CAN-2000-0574, CAN-2001-0247, CVE-2001-0053, CVE-2001-0318, CAN-2001-0248, CVE-1999-0082, CVE-1999-0083, CVE-2000-0856, CAN-2001-0065, CAN-2001-0283, CVE-2001-0456

U5.4 Come stabilire se siete vulnerabili:

Diverse versioni di daemon FTP UNIX presentano un grande numero di vulnerabilità e devono essere regolarmente aggiornate e corrette. Controllate quale sia la versione più recente e l'ultimo livello di patch del vostro specifico FTP server software consultando il sito del produttore del vostro sistema operativo o del software FTP. Le la vostra versione non è la più recente, vi sono delle possibilità che sia vulnerabile e che i metodi per sfruttare le sue vulnerabilità siano pubblicamente disponibili nella comunità underground.

Si può anche utilizzare lo scanner gratuito Nessus (http://www.nessus.org) per evidenziare le vulnerabilità FTP.

U5.5 Come proteggersi:

Per proteggere il servizio FTP si dovrebbero adottare i seguenti accorgimenti:

1. Passate alla versione più recente del vostro FTP. I più conosciuti server FTP gratuiti sono WU-FTPD e ProFTPD. Se la vostra versione di FTP era compresa nel sistema operativo, rivolgetevi al produttore del vostro sistema operativo per le informazioni sull'aggiornamento.
2. Disabilitate l'accesso anonimo ai servizi FTP se non è necessario. Seguite le istruzioni contenute nel manuale del software della vostra specifica versione. Per WU-FTPD e ProFTPD, create o modificate il file /etc/ftpusers e aggiungete gli username "anonymous" e "ftp" (su righe diverse). Questo file definisce quali utenti **non** sono abilitati a connettersi al server FTP. Per aggiungere un ulteriore livello di sicurezza, togliete anche l'utente "ftp" dal file delle password.
3. Nel caso in cui fosse necessario la funzionalità dell'FTP anonimo, controllate almeno che sia disabilitata la possibilità di un caricamento anonimo, in modo che gli utenti abbiano bisogno di un username valido e di una password per inserire file sul vostro server. Il caricamento anonimo è disabilitato per default sulla maggior parte dei daemon FTP. Per verificare che sia davvero disabilitato, collegatevi al vostro server FTP e provate ad eseguire un comando "put qualche.file". Se l'istruzione non ha successo, il messaggio di errore vi indicherà che il caricamento non è abilitato.
4. Limitate l'accesso al server FTP a determinati indirizzi IP o domini utilizzando TCP wrappers. TCP wrappers è già preinstallato sulle più recenti distribuzioni di Unix e Linux. Se non lo avete, potete installarlo dai sorgenti che potete trovare all'indirizzo ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.tar.gz.
   Inserendo una riga del tipo "in.ftpd: 10.164.168.15" o "in.ftpd: .dominio_fidato.com" nel vostro file /etc/hosts.allow, permetterete l'accesso solo da uno specifico dominio o indirizzo IP. Potreste quindi inserire "in.ftpd: ALL" in /etc/hosts.deny per bloccare l'accesso a tutti gli altri e confermare l'avvio del daemon FTP via "tcpd" in /etc/inetd.conf. Alcune distribuzioni di Linux (come ad esempio RedHat) utilizzano una versione migliorata di inetd chiamata xinetd, che contiene il codice TCP wrapper e controlla di default i file sopra descritti. Consultate il manuale per suggerimenti sulla configurazione di xinetd.
5. Implementate delle restrizioni ai permessi dei file sull'FTP server in modo che gli utenti possano accedere solo ai file di cui hanno bisogno. La maggior parte dei server FTP offrono la possibilità di imporre un controllo granulare degli accessi per gli utenti FTP che si somma ai permessi UNIX dei file.
6. Aggiungete tutti gli account di amministrazione (come root, daemon, sys, ecc.) al file /etc/ftpusers in modo che tali account non possano essere accessibili in FTP.
7. Considerate la possibilità di sostituire FTP con soluzioni software più sicure come SFTP o SCP (componenti del pacchetto Secure Shell) e utilizzate un web server per distribuire file a un pubblico vasto.
8. Disattivate i server FTP inutilizzati e disinstallate il software dal sistema. Chiudete con il firewall la porta 21 sui dispositivi perimetrali se essa non viene utilizzata.

U6 Servizi R – Relazioni di Trust

U6.1 Descrizione

Remote shell (rsh), remote copy (rcp), remote login (rlogin), e remote execution (rexec) – conosciuti tutti assieme come "R-commands" – sono molto usati nel mondo Unix. Le organizzazioni con molti server Unix spesso configurano i corrispondenti "R-services" (in.rshd, in.rlogind, in.rexecd) in modo che gli utenti possano spostarsi da una macchina all'altra senza inserire ogni volta uno user ID e una password. Anche nelle reti dove le risorse di un dato utente sono contenute da un singolo sistema, gli amministratori sono spesso responsabili di dozzine o anche centinaia di sistemi, e quindi configurano i servizi R in modo da facilitare i propri movimenti da una macchina all'altra. Un singolo utente può effettuare comandi rsh, rcp, rlogin o rexec dalla macchina A alla macchina B senza dover ri-autenticarsi

inserendo il nome o l'indirizzo della macchina A nel suo file ~/.rhosts file sulla macchina B. Tutti gli utenti possono eseguire comandi rsh, rcp, rlogin o rexec dalla macchina A alla macchina B senza dover ri-autenticarsi se il nome o l'indirizzo della macchina A è presente nel file /etc/hosts.equiv della macchina B.

I servizi R soffrono di due grandi fondamentali debolezze nelle connessioni di rete: mancanza di crittografia e autenticazione dell'host piuttosto scarsa. La trasmissione dell'informazione tra i client R-command e i servizi R in testo piano fa in modo che i dati o ciò che viene digitato sulla tastiera possano essere intercettati. Il fatto che i servizi R accettino semplicemente il nome o l'indirizzo presentato da un client che si connette consente che queste informazioni siano catturate. Se non sono state stabilite relazioni di trust, gli utenti sono obbligati a inviare in rete le password in chiaro. Con le relazioni di trust, un aggressore può assumere l'identità di un utente valido su un host valido e utilizzarla per ottenere l'accesso a tutte le altre macchine che hanno impostato la relazione con la macchina violata.

U6.2 Sistemi interessati:

Quasi tutti i sistemi Unix e Linux sono distribuiti con i servizi R installati e spesso abilitati per default.

U6.3 Lista CVE:

CVE-1999-0113, CVE-1999-0627, CVE-1999-0180, CAN-1999-0651, CAN-1999-0515

U6.4 Come stabilire se siete vulnerabili:

I servizi R girano su un meta-server chiamato "inetd" o , su alcuni sistemi, "xinetd." Inetd permette le connessioni rsh o rcp se vi è una voce per "in.rshd" (il nome specifico può variare lievemente a seconda della vostra distribuzione) in /etc/inetd.conf o in /etc/inet/inetd.conf. Allo stesso modo, rexec richiede una voce per "in.rexecd," e rlogin una voce per "in.rlogind." Xinetd funziona in modo simile, aspettando che nella directory /etc/xinetd.d appaia un file nominato dopo che ciascun servizio è partito.

Le relazioni di Trust sono stabilite su una macchina se vi sono delle voci nel file /etc/hosts.equiv o nel file ~/.rhosts di ciascun utente valido.

U6.5 Come proteggersi:

Disabilitate i servizi R su qualsiasi sistema nel quale non siano assolutamente necessari. Le funzionalità dei servizi R possono essere svolte in modo molto più sicuro da Secure shell (ssh, disponibile presso OpenSSH o presso SSH Communications Security) e i sui complementi di scp e sftp. Se i servizi R sono assolutamente necessari, disabilitate le relazioni di trust e utilizzata TCP Wrappers per registrare tutti i tentativi di connessione, limitate l'accesso a specifici host ed effettuale la verifica degli host. La funzionalità di TCP Wrappers è già contenuta in xinetd.

Per disabilitare le relazioni di trust, eliminate il file /etc/hosts.equiv e il file ~/.rhosts di ciascun utente. Se dovete proprio utilizzare le relazioni di trust, non usate mai il carattere "+" (carattere jolly), perché può essere utilizzato da qualsiasi utente o da qualsiasi macchina (o, peggio, da qualsiasi utente da qualsiasi macchina) per connettersi con credenziali corrette, e assicuratevi di usare TCP Wrappers. Non utilizzate mai ~/.rhosts per permettere l'autenticazione senza password.

U7 Line Printer Daemon (LPD)

U7.1 Descrizione

Il Berkeley line printer daemon (LPD) è storicamente il servizio che permette agli utenti di connettersi a una stampante locale da una macchina locale o da una macchina remota attraverso la porta TCP 515. Anche se sono disponibili server alternativi, LPD rimane il più utilizzato server di stampa tra le diverse distribuzioni di Unix e Linux. Molte implementazioni di LPD, però, contengono delle falle di programmazione che hanno portato a buffer overflow, permettendo agli aggressori di eseguire codice arbitrario con privilegi di root. Così tanti sistemi operativi Unix contengono daemon LPD vulnerabili che il

CERT ha emesso un avviso generale (http://www.cert.org/advisories/CA-2001-30.html) alla fine del 2001 per fornire informazioni specifiche sui problemi e sui rimedi per dozzine di diversi sistemi Unix.

U7.2 Sistemi interessati:

Quasi tutti i sistemi Unix e Linux sono distribuiti con una versione di LPD installata e spesso abilitata per default.

U7.3 Lista CVE:

CVE-2001-0353, CVE-1999-0299, CVE-2000-0534, CVE-2001-0670, CAN-1999-0061, CAN-2000-1208, CAN-2001-0671

U7.4 Come stabilire se siete vulnerabili:

Siccome tutti i sistemi Unix e Linux sono distribuiti con un qualche server di stampa installato, e dal momento che anche quelli che utilizzano un qualche sostituto di LPD (come LPRng) chiamano il loro servizio "lpd" o "in.lpd," dovreste controllare presso il vostro distributore per verificare se quella che utilizzate è la versione più recente o comunque se la versione è corretta con la patch più recente, e se non è così considerate vulnerabile il vostro sistema.

U7.5 Come proteggersi:

Consultate il CERT Advisory 2001-30 per le informazioni su come risolvere il problema sul vostro specifico sistema operativo. Gli utenti Solaris possono consultare anche CERT Advisory 2001-15 e Sun Security Bulletin #00206.

Se la vostra macchina non ha bisogno di fungere da server di stampa per richieste da remoto, avete la possibilità di ridurre al minimo il rischio di future vulnerabilità in LPD disabilitando il servizio "in.lpd" in inetd o in xinetd. Per inetd, commentate la voce "in.lpd" in /etc/inetd.conf o in /etc/inet/inetd.conf e riavviate inetd. Per xinetd, aggiungete la riga "disable = yes" al file "in.lpd" e riavviate xinetd. Se proprio avete bisogno si soddisfare richieste di stampa da remoto, restringere gli host abilitati a connettersi a in.lpd con TCP Wrappers.

Potete garantirvi una certa protezione dai buffer overflow abilitando uno stack non eseguibile sui sistemi operativi che supportano questa funzione. Anche se uno stack non eseguibile non protegge da tutti i buffer overflow, può ostacolare lo sfruttamento di alcuni buffer overflow standard pubblicamente disponibili su Internet.

U8 Sendmail

U8.1 Descrizione

Sendmail è il programma che invia, riceve e inoltra la maggior parte della posta elettronica elaborata su computer UNIX e Linux. La grande diffusione dell'uso di Sendmail in Internet lo rende uno degli obiettivi di attacco principali, concretizzatisi in numerosi exploit nel corso degli anni.

La maggior parte di questi exploit hanno successo solo con le versioni meno recenti del software. Sendmail, infatti, non ha presentato vulnerabilità gravi negli ultimi due anni. Nonostante questi problemi ormai vecchi siano stati ben documentati e siano stati risolti nelle versioni più recenti, sono ancora oggi in circolazione un tale numero di versioni non aggiornate o mal configurate che Sendmail rimane uno dei servizi più spesso presi di mira.

I rischi che si presentano nell'utilizzo di Sendmail possono essere raggruppati in due categorie principali: l'acquisizione di privilegi causata da buffer overflow e la non corretta configurazione che fa diventare la vostra macchina un tramite per la posta elettronica inviata da un'altra macchina. Il primo è un problema che riguarda qualsiasi sistema che utilizzi ancora le vecchie versioni del codice. Il secondo è il risultato dell'uso dei file di configurazione non corretti o di quelli di default e rappresenta uno degli ostacoli maggiori nella lotta alla diffusione dello spam.

U8.2 Sistemi interessati:

Quasi tutti i sistemi Unix e Linux sono distribuiti con una versione di Sendmail installata e spesso abilitata per default.

U8.3 Lista CVE:

CVE-1999-0206, CVE-1999-0203, CVE-1999-0204, CVE-1999-0047, CAN-1999-0512, CVE-1999-0130, CVE-1999-0131, CVE-1999-0393, CVE-1999-1309, CVE-2001-0653, CVE-2000-0319, CVE-1999-1109, CVE-1999-0129, CVE-1999-0095

U8.4 Come stabilire se siete vulnerabili:

Sendmail ha presentato in passato un grande numero di vulnerabilità. Non fidatevi sempre della stringa di versione restituita dal daemon, perché questi non fa altro che leggerla da un file di testo presente sul sistema che può non essere correttamente aggiornato.

Verificate quale sia la versione più recente di Sendmail (se dovete istallarlo da zero) o quale sia il livello di patch raggiunto (se Sendmail è già inserito nel vostro sistema operativo); se non state utilizzando l'ultima versione o l'ultimo livello di patch, probabilmente siete vulnerabili.

U8.5 Come proteggersi:

Per proteggere Sendmail dovrebbero essere adottate le seguenti precauzioni:

1. Passate alla versione più recente e/o installate la più recente patch. Il codice sorgente è reperibile all'indirizzo http://www.sendmail.org/. Se la vostra versione di Sendmail è inserita nel sistema operativo, le patch dovrebbero essere disponibili presso il sito web del produttore del vostro sistema operativo (all'indirizzo http://www.sendmail.org/ potrete trovare anche diverse informazioni specifiche che riguardano i diversi produttori, che comprendono le indicazioni sulla configurazione e sui tempi di compilazione).
2. Sendmail è di solito abilitato per default sulla maggior parte dei sistemi Unix e Linux, anche in quelle che non sono utilizzate come mail server o mail relay. Non eseguite Sendmail in modalità daemon (disabilitate l'opzione "-bd") su tali macchine. Potrete comunque spedire messaggi dal vostro sistema richiamando periodicamente "sendmail -q" per far partire la posta in uscita.
3. Se dovete utilizzare Sendmail in modalità daemon, assicuratevi che la vostra configurazione sia progettata per inviare correttamente la posta e solo per i vostri sistemi. Consultate http://www.sendmail.org/tips/relaying.html e http://www.sendmail.org/m4/anti-spam.html per i consigli su come effettuare una corretta configurazione del vostro server. A partire dalla versione 8.9.0 di Sendmail, la funzione di open relay è disabilitata per default. Molti produttori di sistemi operativi, però, la ri-abilitano nelle loro configurazioni di default. Se state utilizzando la versione di Sendmail che vi è arrivata con il vostro sistema operativo, controllate con molta attenzione che il vostro server non sia utilizzabile come relay.
4. Quando aggiornate il codice binario di Sendmail, controllate di aggiornare o di verificare anche il file di configurazione, poiché le vecchie configurazioni possono ancora permettere il relaying anche con il codice aggiornato.

U9 BIND/DNS

U9.1 Descrizione

Il pacchetto software *Berkeley Internet Name Domain* (BIND) è l'implementazione di gran lunga più utilizzata del Domain Name Service (DNS), il sistema che permette di localizzare un server su Internet (o in una rete locale) utilizzando un nome (ad esempio www.sans.org) senza dover conoscere il suo specifico indirizzo IP. La diffusione di BIND lo ha reso bersaglio di frequenti attacchi. Anche se gli sviluppatori di BIND sono storicamente molto rapidi nel correggerne le vulnerabilità, un numero eccessivo di server non aggiornati o mal configurati rimane esposto agli attacchi.

A questa categoria contribuiscono un certo numero di fattori. I più importanti di questi sono costituiti da amministratori che non sono informati degli aggiornamenti di sicurezza, da sistemi che utilizzano il daemon BIND (chiamato "named") senza averne bisogno e da file di configurazione non appropriati. Ciascuno di questi sistemi può subire un denial of service, un buffer overflow o un DNS cache poisoning. Tra le più recenti debolezze scoperte in BIND, vi è quella discussa nel CERT Advisory CA-2002-15 che può portare a un denial of service. In questo caso un aggressore invia particolari pacchetti DNS per forzare il controllo interno che è in sé vulnerabile e fare in modo che il daemon BIND si disattivi. Un'altra vulnerabilità scoperta permette un attacco buffer overflow, trattato nel CERT Advisory CA-2002-19, nel quale gli aggressori utilizzano le versioni vulnerabili delle librerie del DNS resolver. Inviando risposte DNS confezionate ad arte, l'aggressore può sfruttare questa vulnerabilità ed eseguire codice arbitrario o anche causare un'interruzione del servizio.

Oltre ai rischi che un BIND vulnerabile pone al server che lo ospita, è da aggiungere una singola macchina compromessa può costituire una piattaforma per attività dannose che hanno come obiettivo altre macchine su Internet, o può essere utilizzata come deposito di materiale illecito senza che l'amministratore lo sappia.

U9.2 Sistemi interessati:

Quasi tutti i sistemi Unix e Linux sono distribuiti con una versione di BIND installata e spesso abilitata per default. Esistono versioni binarie di BIND anche per Windows

U9.3 Lista CVE:

CVE-1999-0009, CVE-1999-0833, CVE-2001-0010, CVE-2001-0011, CVE-2001-0013, CVE-1999-0024, CVE-2001-0012, CVE-1999-0837, CVE-1999-0848, CVE-1999-0849, CAN-2002-0400

U9.4 Come stabilire se siete vulnerabili:

Se utilizzate una versione di BIND arrivata con il vostro sistema operativo, verificate di essere aggiornati con le patch più recenti rilasciate dal vostro produttore. Se utilizzate BIND installato dal sorgente dell'Internet Software Consortium (ISC), controllate che quella che state usando sia la versione più recente di BIND. Qualsiasi versione non aggiornata o non corretta del software è passibile di vulnerabilità.

Nella maggior parte dei sistemi, il comando "named -v" mostrerà la versione di BIND installata, numerata come X.Y.Z, dove X è la versione principale, Y è la versione secondaria e Z è il livello di patch. Vi sono attualmente tre versioni principali di BIND: 4, 8 e 9. Se utilizzate BIND installato dal codice sorgente, dovreste sostituire la versione 4 con le versioni più recenti 8 o, meglio ancora, 9. Potete recuperare il codice aggiornato dal sito ISC.

Un approccio ancora più corretto sarebbe quello di utilizzare un vulnerability scanner aggiornato per verificare periodicamente il vostro sistema DNS per controllare che non presenti nuove vulnerabilità.

U9.5 Come proteggersi:

- *Per proteggervi dalle vulnerabilità di BIND in generale:*
    1. Disabilitate il daemon BIND (chiamato "named") su tutti i sistemi che non sono specificatamente demandati e autorizzati ad essere server DNS. Per prevenire il fatto che questa modifica possa essere invertita, è buona norma rimuovere anche il software di BIND.
    2. Applicate tutte le patch del vostro produttore o aggiornate i vostri DNS Server alla versione più recente. Per maggiori informazioni su come rafforzare la vostra istallazione di BIND, consultate gli articoli su come rendere sicuri i servizi di naming riportati nella Unix Security Checklist del CERT
    3. Per rendere più difficili gli attacchi o le scansioni automatiche al vostro sistema, nascondete il banner "Version String" di BIND sostituendo la reale versione di BIND con un numero falso nel file "named.conf".

4. Permettete i trasferimenti di zona solo verso DNS server secondari nel vostro dominio. Disabilitata i trasferimenti di zona verso domini padri o figli, utilizzando al suo posto delegation e forwarding.
5. Per evitare che "named" compromessi mettano a rischio il vostro intero sistema, fate in modo che BIND venga eseguito come utente senza privilegi in una directory chroot(). Per BIND 9, consultate http://www.losurs.org/docs/howto/Chroot-BIND.html
6. Disabilitate la *recursion* e il *glue fetching*, per difendervi dalla contaminazione della cache del DNS

- *Per proteggervi dalle vulnerabilità di BIND scoperte recentemente:*
  1. Per la vulnerabilità Denial of Service su ISC BIND 9: http//www.cert.org/advisories/CA-2002-15.html
  2. Per i Buffer Overflow nelle librerie del Resolver DNS: http//www.cert.org/advisories/CA-2002-19.html

Per delle eccellenti guide su come rafforzare BIND sui sistemi Solaris e per maggiori indicazioni sulla documentazione per BIND, consultate Hardening the BIND v8 DNS Server e Running the BIND9 DNS Server Securely.

U10 Autenticazione generica di Unix - Account senza password o con password deboli

U10.1 Descrizione

In quasi tutte le interazioni tra gli utenti e i sistemi informativi vengono utilizzate password, frasi identificative o codici di sicurezza. La maggior parte delle forme di autenticazione, come la maggior parte delle protezioni per file e dati, si basa su password fornite dall'utente. Dal momento che gli accessi correttamente autenticati spesso non vengono registrati, o anche se vengono registrati non lo sono in modo da fornire alcun segnale di allarme, una password compromessa rappresenta un'opportunità di esplorare un sistema dall'interno senza essere identificati. Un aggressore avrebbe accesso completo a qualsiasi risorsa disponibile per quell'utente e sarebbe molto vicino ad essere in grado di accedere ad altri account, a macchine vicine e forse anche ad ottenere privilegi di amministrazione. Nonostante questi pericoli, gli account con password deboli o addirittura senza password rimangono estremamente diffusi e le società con una buona policy sull'utilizzo delle password ancora troppo rare.

Le più comuni vulnerabilità delle password sono dovute (a) ad account senza password o con password deboli, (b) al fatto che, a prescindere dalla robustezza delle password, spesso gli utenti non le proteggono, (c) al fatto che il sistema operativo o il software applicativo creano account di amministrazione con password deboli o privi di password (d) al fatto che gli algoritmi di hashing delle password sono noti e spesso gli hash vengono memorizzati in modo da essere accessibili a chiunque. La difesa migliore e la più corretta contro queste vulnerabilità è una solida policy che includa le istruzioni per creare delle buone password e che riassuma i comportamenti corretti per conservarne la riservatezza, unita a una verifica proattiva dell'integrità delle password.

U10.2 Sistemi interessati:

Qualsiasi sistema operativo e applicazione per accedere alla quale gli utenti si autentichino tramite user ID e password.

U10.3 Lista CVE:

CAN-1999-0502

U10.4 Come stabilire se siete vulnerabili:

Sul sistema locale, le password vengono salvate in either /etc/passwd o in /etc/shadow. /etc/passwd ha bisogno di essere leggibile da tutti gli utenti della rete per poter permettere il processo di

autenticazione. Se tale file include anche gli hash delle password, allora ogni utente con accesso al sistema può leggere gli hash e provare a violarli con un password cracker.
Per custodire gli hash si può utilizzare in alternativa /etc/shadow, che deve essere leggibile solo da root. Se i vostri account locali non sono protetti da /etc/shadow, allora il rischio per le vostre password diventa molto alto.

Se utilizzate NIS, gli hash delle password sono leggibili da tutti gli utenti e si viene a costituire come nel caso precedente un rischio molto elevato. Ciò può essere il caso di alcune implementazioni di LDAP come servizio di autenticazione di rete.

Ma anche se gli hash delle password sono protetti, le password possono essere indovinate in altri modi. Per quanto vi siano alcuni sintomi osservabili di una generale debolezza delle password, come la presenza di account attivi appartenenti a utenti che non operano più all'interno dell'organizzazione o a servizi non più attivi, l'unico modo per accertarsi che ogni singola password sia sufficientemente robusta è quello di verificare tutte le password con gli stessi strumenti per la determinazione delle password utilizzati dagli aggressori. *ATTENZIONE: Non utilizzate mai un password scanner, neanche sui sistemi per i quali avete un accesso da amministratore, senza autorizzazione esplicita e preferibilmente scritta da parte del vostro datore di lavoro. È già accaduto che amministratori di sistema con le migliori intenzioni siano stati licenziati per aver utilizzato strumenti per la determinazione delle password senza autorizzazione.*

I migliori strumenti per la determinazione delle password sono:

- Crack
- John the Ripper
- Symantec NetRecon

U10.5 Come proteggersi:

La difesa migliore e la più corretta contro la debolezza delle password è una solida policy che includa le istruzioni su come generare buone password e descriva i comportamenti corretti per mantenerne la sicurezza, assieme ad una verifica proattiva dell'integrità delle password.

1. *Assicuratevi che le vostre password siano sufficientemente robuste*. Disponendo di tempi e risorse hardware adeguate, qualsiasi password può essere violata utilizzando il sistema "brute force". Ma ci sono metodi più semplici e molto più efficaci per venire a conoscenza delle password con uno sforzo minore. I password cracker utilizzano metodi conosciuti come "attacchi da dizionario". Dal momento che i metodi crittografici sono noti, gli strumenti per l'individuazione delle password non fanno altro che confrontare le password in forma crittata con le forme crittate di parole del dizionario (in diverse lingue), di nomi propri, e con le permutazioni di entrambi. Di conseguenza una password la cui radice assomigli in qualche modo a una parola è estremamente suscettibile di essere violata da un attacco da dizionario. Molte organizzazioni insegnano ai propri utenti a generare password che includano combinazioni di caratteri alfanumerici e caratteri speciali, e gli utenti la maggior parte delle volte prendono una parola (ad esempio "password") e convertono le lettere in numeri o caratteri speciali ("pa$$w0rd"). Queste permutazioni non proteggono, però, dagli attacchi da dizionario: "pa$$w0rd" ha la stessa possibilità di essere violata di "password."

   Una buona password, quindi, non deve avere come radice una parola o un nome proprio. Una solida policy sulle password dovrebbe indirizzare gli utenti verso la creazione di password derivate da qualcosa di più casuale, come una frase o il titolo di un libro o di una canzone. Concatenando una stringa più lunga (prendendo la prima lettera di ogni parola o associando alle parole un carattere speciale o togliendo le vocali, ecc.), gli utenti possono generare stringhe sufficientemente lunghe che combinano caratteri alfanumerici e caratteri speciali in modo tale da creare una grande difficoltà ai tentativi di attacco con metodi da dizionario. E in più se la frase è facile da ricordare, lo sarà anche la password.

   Una volta fornite agli utenti le corrette indicazioni su come generare buone password, possono essere messe in opera le procedure per controllare che queste indicazioni vengano seguite. Il modo

migliore per farlo è quello di convalidare le password ogni volta che l'utente le cambia. La maggior parte dei tipi di Unix può usare Npasswd come front-end per verificare le password inserite alla luce della vostra policy. I sistemi abilitati PAM possono anche includere cracklib (le librerie del tool "Crack").

Gli strumenti per la determinazione delle password devono essere utilizzati in modalità stand-alone come parte di un esame sistematico. FATE ANCORA ATTENZIONE*: Non utilizzate mai un password scanner, neanche sui sistemi per i quali avete un accesso da amministratore, senza autorizzazione esplicita e preferibilmente scritta da parte del vostro datore di lavoro. È già accaduto che amministratori di sistema con le migliori intenzioni siano stati licenziati per aver utilizzato strumenti per la determinazione delle password senza autorizzazione.* Una volta ricevuta l'autorizzazione ad utilizzare strumenti per la determinazione delle password sul vostro sistema, attivateli regolarmente su una macchina protetta. Gli utenti le cui password vengono violate devono essere avvisati in modo confidenziale e devono essere fornite loro le istruzioni su come scegliere una buona password. Gli amministratori di sistema e il management dovrebbero sviluppare assieme questo tipo di procedure, in modo tale che il management possa provvedere quando gli utenti non rispondono alle notifiche.

Un altro modo per proteggersi da password deboli o assenti è quello di utilizzare forme alternative di autenticazione come token generatori di password o sistemi di autenticazione biometrica. Se avete problemi derivati da password deboli, usate quindi metodi diversi per l'autenticazione degli utenti.

2. *Proteggete le password robuste.* Se custodite gli hash delle password in /etc/passwd, aggiornate i vostri sistemi per usare /etc/shadow. Se sul vostro sistema utilizzate NIS or LDAP in un modo per cui gli hash non sono protetti, chiunque (anche un utente non autenticati) può leggere gli hash delle vostre password e tentare di violarli. Dovreste quindi rendere sicuri i permessi e compiere regolarmente delle verifiche di violabilità.

   Anche se le password sono robuste, gli account possono essere ugualmente compromessi se gli utenti non proteggono adeguatamente la propria password. Una buona policy include sempre istruzioni che specificano come gli utenti non devono mai riferire la propria password a nessun'altro, non devono mai trascrivere la password in supporti che possano essere letti da altri e devono rendere adeguatamente sicuro qualsiasi file nel quale sia conservata una password per l'autenticazione automatica (le password sono più facili da proteggere quando questa pratica è utilizzata solo quando assolutamente necessario).
   La modifica periodica della password deve essere fatta rispettare in modo che quelle password che non rispettano queste regole siano vulnerabili solo in una finestra temporale limitata, e deve essere tassativamente vietato che le vecchie password possano essere riutilizzate. Controllate che agli utenti giungano gli avvisi e sia data loro le possibilità di modificare la propria password prima della scadenza. Quando si trovano di fronte a frasi come: "la vostra password è scaduta e deve essere cambiata," gli utenti tendono a scegliere una cattiva password.

3. *Controllate rigorosamente gli account.*

   - Qualsiasi account per l'accesso a un servizio e qualsiasi account di amministrazione che non sia più in uso deve essere disabilitato o eliminato. Qualsiasi account per l'accesso a un servizio e qualsiasi account di amministrazione che siano in uso deve essere forniti di una password solida e recente.
   - Verificate gli account presenti sul vostro sistema e create una master list. Non dimenticate di verificare le password su dispositivi come router e stampanti digitali, fotocopiatrici e controller connessi a Internet.
   - Sviluppate procedure per aggiungere account autorizzati alla lista e per rimuove dalla lista gli account che non sono più in uso.
   - Verificate periodicamente la lista per controllare che non siano stati aggiunti nuovi account e che gli account non più in uso siano stati rimossi.
   - Adottate rigide procedure per la rimozione degli account quando i dipendenti o i collaboratori della società non lavorano più lì o quando gli account non sono più necessari.

4. *Implementate una solida policy per le password in azienda*. In aggiunta ai controlli a livello di sistema operativo o a livello di rete, esistono degli strumenti completi che aiutano a gestire una buona policy per le password. L'Enterprise Security Manager (ESM) di Symantec è uno strumento di monitoraggio che risiede sull'host che evidenzia qualsiasi cambiamento nella policy, la creazione di nuovi account e verifica la robustezza delle password. ESM inoltre può eseguire tentativi per verificare la violabilità delle password in accordo con la policy attiva nella vostra rete. ESM utilizza un ambiente client-manager: l'agente è posto sui server o sulle workstation e invia le segnalazioni a un gestore centralizzato. Utilizzando una console remota, è possibile vedere i log e possono essere generati dei report sullo stato attuale della situazione. ESM verificherà i log e segnalerà qualsiasi modifica che sia stata fatta dalla situazione di partenza.

Appendice A – Porte generalmente vulnerabili

In questa sezione, abbiamo elencato le porte che sono generalmente esaminate e attaccate. Il blocco di queste porte rappresenta il requisito minimo per la sicurezza perimetrale, non una lista esaustiva delle specifiche per il firewall. Una regola di gran lunga migliore sarebbe quella di bloccare tutte le porte inutilizzate. Comunque, anche se ritenete che queste porte siano bloccate, dovete sempre controllarle attivamente per scoprire eventuali tentativi d'intrusione. Un ultimo avvertimento è doveroso: il blocco di alcune delle porte elencate può disabilitare servizi necessari. Prima di implementare queste raccomandazioni, consideratene i potenziali effetti.

Tenete presente che il blocco di queste porte non rappresenta un sostituto alle soluzioni di sicurezza globali. Se le porte non sono state rese sicure in maniera adeguata su ogni sistema host della vostra organizzazione, un aggressore che ha ottenuto l'accesso alla vostra rete con altri mezzi (un modem telefonico, un trojan allegato ad un'e-mail o un complice interno all'organizzazione, per esempio) può sfruttare dette porte anche se sono bloccate.

1. Servizi di login-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin e altri (da 512/tcp a 514/tcp);
2. RPC e NFS-- Portmap/rpcbind (111/tcp e 111/udp), NFS (2049/tcp e 2049/udp), lockd (4045/tcp e 4045/udp);
3. NetBIOS in Windows NT -- 135 (tcp e udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 – le prime porte più la 445(tcp e udp);
4. X Windows -- da 6000/tcp a 6255/tcp;
5. Naming Services-- DNS (53/udp) per tutte le macchine che non sono server DNS, trasferimenti di zona DNS (53/tcp) eccezion fatta per le external secondaries, LDAP (389/tcp e 389/udp);
6. Mail-- SMTP (25/tcp) per tutte le macchine che non siano relay di posta esterni, POP (109/tcp e 110/tcp), IMAP (143/tcp);
7. Web-- HTTP (80/tcp) e SSL (443/tcp) eccezion fatta per i server Web esterni, e potreste anche bloccare le comuni porte HTTP più significative (8000/tcp, 8080/tcp, 8888/tcp, ecc.);
8. "Small Services"-- porte al di sotto di 20/tcp e 20/udp, time (37/tcp e 37/udp);
9. Varie-- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/udp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp e 161/udp, 162/tcp e 162/udp), BGP (179/tcp), SOCKS (1080/tcp);
10. ICMP -- bloccate le eco request in entrata (ping e traceroute di Windows), blocco delle echo reply in uscita, time exceeded e messaggi destination unreachable **eccezion fatta per** i messaggi "packet too big" (type 3, code 4). (Questo suggerimento suppone che vogliate rinunciare all'uso classico dell'echo request ICMP al fine di bloccarne alcuni noti utilizzi illeciti).

In aggiunta a queste porte, bloccate gli indirizzi "spoofed" -- pacchetti in arrivo dall'esterno della vostra azienda che hanno come sorgente indirizzi interni, indirizzi privati (RFC1918 e rete 127) e riservati IANA. Bloccate anche i pacchetti instradati alla sorgente o i pacchetti con il campo delle opzioni IP impostato.

Appendice B – Gli esperti che hanno collaborato a creare la lista dei venti servizi più vulnerabili

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
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
Chris Rouland, Internet Security Systems
Bruce Schneier, Counterpane Internet Security Inc.
Greg Shipley, Neohapsis
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

Le persone che hanno contribuito ad assegnare le priorità alle singole voci CVE per definire i test da utilizzare negli scanner Top 20. Per i dettagli sul sistema utilizzato, consultate 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
André Mariën, 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 Justiça, Brasilia Brazil

Altri esperti di sicurezza che hanno collaborato alla redazione della Top 20 del 2001 e della Top 10 del 2000, fornendo le basi sulle quali è stata costruita la Top 20 del 2002.

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

Appendice C – Versione italiana

La versione italiana de "Le venti vulnerabilità più critiche per la sicurezza in Internet" è stata curata dal Centro Ricerche Data Security.

Data Security
Sede e Centro Ricerche
Corso Vittorio Emanuele 20 - Palazzo Concordia
33170 Pordenone
Telefono +39 043429400 - Fax +39 0434 26840
http://www.datasecurity.it

Ufficio di Milano
Viale Corsica 7, 20133 Milano

SANS Institute

Il SANS Institute (System Administration, Networking and Security) è stato fondato nel 1989 come gruppo di ricerca e organizzazione educativa. Con la sua attività permette a più di 156.000 professionisti della sicurezza informatica quali analisti, amministratori di sistema e amministratori di rete, di condividere le proprie esperienze e di trovare le soluzioni ai problemi che, giorno dopo giorno, vengono riscontrati.

Alla base del SANS vi sono molti professionisti di agenzie governative, aziende e istituti universitari di tutto il mondo che investono ogni anno centinaia di ore nella ricerca e nella formazione per aiutare la comunità internazionale a risolvere i problemi della sicurezza informatica.

Molte risorse del SANS, come le raccolte di notizie, la diffusione dei risultati delle ricerche, i bollettini sulla sicurezza e documenti vincitori di diversi premi, sono disponibili a chiunque voglia essere aggiornato sulle problematiche di sicurezza. I ricavi provenienti dalle pubblicazioni e dalle attività di formazione vengono investiti in programmi universitari di ricerca.

Il SANS supporta diversi programmi di ricerca, tra i quali:

SANS Computer & Information Security Training - (www.sans.org)
Il SANS fornisce una serie di corsi focalizzati sulle pratiche di difesa dei sistemi e delle reti dai pericoli che li minacciano. I corsi, sviluppati da una comunità di centinaia di amministratori, security manager e professionisti della sicurezza informatica, coprono sia i temi fondamentali della sicurezza, sia aspetti tecnici che analizzano in profondità i temi dell'information security.

The GIAC Certification Program - (www.giac.org)
Fondato nel 1999, il Global Information Assurance Certification program è un programma di certificazione che si occupa di diversi aspetti della sicurezza informatica, dall'intrusion detection ai firewall e alla protezione perimetrale, dalla sicurezza dei sistemi alle politiche di intervento e di risoluzione dei problemi. GIAC si caratterizza nel campo delle certificazioni della sicurezza perché, non solo valuta le conoscenze dei candidati, ma verifica anche la capacità di mettere in pratica queste conoscenze in casi reali.

SANS Resources - (www.sans.org/newlook/resources/)
Molte risorse del SANS, come raccolte di notizie, resoconti delle ricerche, bollettini di sicurezza e documenti di approfondimento, sono gratuite. La SANS Information Security Reading Room (http://rr.sans.org) conta oltre 1300 articoli suddivisi in 63 diverse categorie.

Oltre a questi, il SANS offre gratuitamente:

- SANS NewsBites (www.sans.org/newlook/digests/newsbites.htm), una raccolta degli articoli più importanti sulla sicurezza informatica pubblicati ogni settimana.
- SANS Security Alert Consensus, la raccolta settimanale dei bollettini di sicurezza con gli avvisi di SANS, CERT, Global Incident Analysis Center, National Infrastructure Protection Center, Department of Defense, Security Portal, Ntbugtraq, Sun e molti altri.
- SANS Windows Security Newsletter, che fornisce mensilmente gli aggiornamenti per la sicurezza in ambiente NT.

Incidents.org and the Internet Storm Center - (www.incidents.org)
Nel 2001 SANS ha creato Incidents.org, che riunisce in tutto il mondo i maggiori analisti nel settore dell'intrusion detection, esperti di questioni legali e professionisti della sicurezza.

Center for Internet Security and SCORE - (www.cisecurity.org/www.sans.org/SCORE)
Il SANS Institute è un membro fondatore del Center for Internet Security, una iniziativa congiunta di industrie, governo americano e società di ricerca nata per facilitare il miglioramento degli standard nel settore della sicurezza informatica.

CLUSIT
Associazione Italiana per la Sicurezza Informatica

Il CLUSIT - Associazione Italiana per la Sicurezza Informatica, è una associazione "no profit" con sede presso l'Università degli studi di Milano, Dipartimento di Scienze dell'Informazione.

Gli obiettivi principali che l'Associazione persegue sono la creazione e la diffusione di una cultura della sicurezza informatica presso le aziende private, gli enti della pubblica amministrazione e le organizzazioni economiche del nostro paese.

Il CLUSIT intende:

- Promuovere e favorire iniziative per la diffusione di tutti gli aspetti della sicurezza informatica.
- Contribuire sia a livello comunitario che italiano alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica.
- Concorrere alla definizione di percorsi di formazione per la preparazione delle diverse figure professionali operanti nel settore della sicurezza informatica.
- Promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

I soci del Clusit

L'associazione, che è stata fondata il 4 luglio 2000, conta ad oggi oltre 250 soci, appartenenti al mondo della ricerca, dell' industria, del commercio, del settore bancario ed assicurativo, della Pubblica Amministrazione, della telefonia e di Internet.

Le manifestazioni del Clusit

- MASTER Universitario in Sicurezza Informatica: Università degli Studi di Milano
- INFOSECURITY (Fiera di Milano).
- WEBSecurity (Milano) - Convegno annuale realizzato in collaborazione con NetBusiness.
- Antikrimen Expo e Antikrimen Conference (Firenze).
- SMAU (Roma - Milano).
- SEMINARI CLUSIT, gratuiti per i soci.

Le commissioni di studio del Clusit

- I nuovi rischi informatici e le soluzioni proposte dalle Compagnie specializzate: un misto di assicurazione e di consulenza in sicurezza informatica.
- Certificazioni in materia di sicurezza informatica.
- Firma elettronica - Carta d'identità elettronica.
- Sanità e sicurezza informatica.
- Tutela dei minori su Internet.
- Applicazione della Legge sulla Privacy 675/1996.
- OpenSource e Sicurezza.
- L'analisi della sicurezza informatica in ambito economico aziendale.

ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA
Dipartimento di Informatica e Comunicazione Università degli Studi di Milano
Via Comelico 39 - 20135 MILANO - Tel. 347.2319285
http://www.clusit.it
e-mail: info@clusit.it

Data Security

Data Security è una società formata da un team di esperti di e-Security e di problematiche organizzative e tecnologiche che si occupa di gestione della sicurezza a 360 gradi, a partire dall'analisi del rischio fino all'implementazione di sofisticate soluzioni tecnologiche.

Ciò che distingue in maniera significativa Data Security è la capacità di padroneggiare e integrare le componenti organizzative, normative, tecnologiche e di processo per realizzare soluzioni realmente efficaci e in sintonia con l'organizzazione e i sistemi aziendali.

Una corretta gestione del rischio informativo richiede infatti una serie di analisi approfondite e lo studio di soluzioni il cui effetto può essere garantito solo da consulenti esperti. Queste analisi, correlate a progetti di ambito prettamente informatico, consentono di adottare le soluzioni più adeguate alle esigenze del cliente e di mitigare l'impatto sui processi produttivi già in atto.

- Analisi del rischio informatico e studio delle priorità di intervento.
- Test e Certificazione dei Sistemi e delle procedure di Sicurezza.
- Consulenza legale, tecnica e organizzativa su Sicurezza, Privacy, Autenticazione, Firma Digitale e Business Continuity.
- Formazione qualificata e sensibilizzazione sulle problematiche della sicurezza di personale e dirigenti.
- Audit e Assessment di Sicurezza.
- Test di vulnerabilità dei sistemi informatici dall'esterno e dall'interno della rete.
- Definizione delle politiche per la Sicurezza delle informazioni.
- Consulenza dedicata alla Pubblica Amministrazione per la redazione e l'aggiornamento del Documento Programmatico sulla Sicurezza (DPR 318/99), per lo sviluppo del sistema di gestione della sicurezza (Direttiva Interministeriale del 16/01/02) e per l'implementazione di Firma Digitale, Carta del Cittadino e Carta di identità elettronica
- Progettazione di sistemi di Storage, Disaster Recovery e Business Continuity

Oltre a ciò Data Security è in grado di fornire, attraverso i suoi partner, le migliori soluzioni tecnologiche per la Sicurezza informatica e di integrarle con i sistemi esistenti.

- **Soluzioni per l'Autenticazione e Controllo degli Accessi**, per ottimizzare e rendere sicuri i permessi e le procedure di accesso alle diverse risorse da parte degli utenti con tecnologie di Single Sign-on, utilizzo di smart card e soluzioni basate sull'impiego di telefoni cellulari GSM;
- **Soluzioni per la Sicurezza nelle comunicazioni**, grazie a tecnologie basate su crittografia e Firma Digitale, per garantire l'autenticità e l'integrità delle informazioni conservando un'estrema semplicità di utilizzo;
- **Soluzioni per la Protezione delle applicazioni Web**, utilizzando le ultime tecnologie anti-intrusione, per ridurre al minimo il rischio di violazione del proprio sito Internet con i conseguenti danni di immagine, di perdita di dati e di frodi finanziarie;
- **Soluzioni per la Protezione dei dati** e delle applicazioni tramite l'integrazione di sistemi **Storage** intrinsecamente sicuri e sistemi di **Backup/Restore** completamente automatici e centralizzati. L'utilizzo di entrambi i sistemi garantisce una altissima protezione dei dati e delle applicazioni ed aumentano la SLA (Service Level Availability) delle applicazioni/server.
- **Soluzioni di Content Monitoring e Security Monitoring in ASP**, per garantire 24 ore su 24 e 7 giorni su 7 il controllo e l'aggiornamento continuo dei sistemi di difesa della rete aziendale, per migliorare la sicurezza delle connessioni ad Internet e difendere la posta elettronica aziiendale da virus e spam.

Data Security, inoltre, promuove e sponsorizza assieme ai suoi partner tecnologici Gemplus, nCipher, Ubizen, Network Associates, Qualys, HiperCheck e Verisign-Trust Italia, diversi progetti di ricerca ed iniziative culturali nel campo della sicurezza informatica.

DATA SECURITY
Sede e Centro Ricerche: Corso V. Emanuele 20, 33170 Pordenone – Tel. 0434 29400 - Fax 0434 26840
Ufficio di Milano: Viale Corsica 7, 20133 Milano
http://www.datasecurity.it