



As 20 Vulnerabilidades de Segurança Mais Críticas na Internet (Versão em Português)

Versão 2.501 Em Português 30 de Janeiro, 2002
Copyright 2001, The SANS Institute

Há pouco mais de um ano, o instituto SANS (System Administration, Networking and Security) e o NIPC/FBI (National Infrastructure Protection Center, FBI) divulgaram um documento que resumia as dez vulnerabilidades mais críticas de segurança na Internet ("The Top Ten Most Critical Internet Security Vulnerabilities", ou simplesmente, "Top 10"). Milhares de organizações usaram esta lista para priorizar esforços de modo que fosse possível sanar a priori as vulnerabilidades consideradas mais perigosas. Uma nova lista, divulgada em 1o de Outubro de 2001, atualiza e expande a lista Top 10. Com este novo lançamento, nos aumentamos a lista para conter as vinte vulnerabilidades mais críticas ("Top 20"), dividida em três categorias: vulnerabilidades gerais, vulnerabilidades no Windows, e vulnerabilidades no UNIX.

A lista Top 20 do SANS/FBI é valiosa porque a maioria dos ataques bem sucedidos direcionados a sistemas de computadores através da Internet pode ser atribuída à exploração de falhas de segurança incluídas nesta lista. Por exemplo, o comprometimento do sistema no incidente 'Solar Sunrise' ocorrido no Pentágono, bem como a fácil e rápida propagação do Code Red e NIMDA podem ser atribuídos à exploração de vulnerabilidades contidas na lista.

Estas poucas vulnerabilidades de software contabilizam a maioria dos ataques bem sucedidos, simplesmente pelo fato dos atacantes serem oportunistas, isto é, escolherem o caminho mais fácil e conveniente. Eles exploram as falhas mais comuns usando as mais efetivas e difundidas ferramentas de ataque. Os atacantes partem do princípio que as organizações não corrigem seus sistemas e saem vasculhando sistemas vulneráveis na Internet.

No passado, os administradores de sistemas relataram

Registro de Atualizações

- v. 2.501 - 30/01/02
Versão em Português
[Apêndice C](#) adicionado
- v. 2.501 - 15/11/01
Erro na seção [G5.1](#) corrigido no item #7 de regras de filtragem
- v. 2.500 - 10/10/01
Os números CVE foram tornados links ativos
Quinta nota adicionada em [Notas para Leitores](#)
- v. 2.400 - 8/10/01
Seção [G2.5](#) atualizada
Seção [U1.5](#) atualizada
Seção [U5.5](#) atualizada
Seção [U6.1](#) atualizada
Seção [U7.1](#) atualizada
- v. 2.300 - 7/10/01
[Apêndice B](#) atualizado
Seção [U5.5](#) atualizada
- v. 2.200 - 6/10/01
URL de download do adicionado à seção [G4.5](#)
Regra de filtragem adicionada à seção [G5.1](#)
Correção feita no [Apêndice A](#)
- v. 2.100 - 2/10/01
Atualização se refere a [vulnerabilidades Windows](#) e inclui uma feature do Windows importante, recém-lançada, que protege os sistemas contra LM hashes e uma correção para os sistemas afetados pelo bug RDS.
- v. 2.008 - 1/10/01
Lista é atualizada e expandida para incluir 20 vulnerabilidades organizadas em 3 categorias: vulnerabilidades que afetam [todos os sistemas](#), aquelas que afetam [sistemas Windows](#) e aquelas que afetam [sistemas Unix](#).

que não teriam corrigido muitas destas falhas, primeiro, porque simplesmente não sabiam quais delas eram as mais perigosas, e segundo, porque estavam muito ocupados para corrigi-las. Algumas das ferramentas de scan de vulnerabilidades procuram por 300, 500 ou até mesmo 800 vulnerabilidades, diminuindo assim o foco principal dos administradores de sistemas, que precisam garantir que todos os seus sistemas encontram-se protegidos dos ataques mais comuns. A lista Top 20 foi criada justamente para aliviar estas dificuldades, combinando o conhecimento de dezenas de especialistas em segurança das agências federais mais reconhecidas na área, principais firmas de consultoria e fabricantes de software de segurança, melhores programas na área de segurança mantidos nas universidades, o CERT/CC e o instituto SANS. Uma lista de participantes pode ser encontrada no final deste documento.

O seu retorno e comentários são bem-vindos.

Instituto SANS

Cinco Notas Para Leitores:

Nota 1. Atualizações

A lista Top 20 do SANS/FBI é um documento dinâmico. Ele inclui instruções passo a passo e referências a informações úteis que permitem corrigir as falhas. Nós atualizaremos a lista e as instruções, à medida que forem identificadas ameaças mais críticas e métodos mais recentes e convenientes de contorná-las. Neste processo, sua participação é sempre muito bem-vinda. Este é um documento produzido através do consenso da comunidade, portanto a sua experiência combatendo atacantes e eliminando vulnerabilidades de segurança pode ajudar outras pessoas. Envie as suas sugestões via e-mail para info@sans.org indicando no campo Assunto[Subject] "Top Twenty Comments".

Nota 2. Números CVE

Para cada vulnerabilidade, você encontrará referência ao respectivo número CVE (Common Vulnerabilities and Exposures). Você pode também encontrar referências a números CAN, que nada mais são do que candidatos a números CVE, ou seja, ainda não foram completamente verificados. Maiores detalhes sobre o renomado projeto CVE veja em <http://cve.mitre.org/>

Na seção de Vulnerabilidades Gerais, os números CVE correspondem a exemplos de algumas das vulnerabilidades tratadas em cada um dos itens listados. No entanto, nas seções sobre Vulnerabilidades Windows e Unix, os números CVE correspondem às mais importantes vulnerabilidades que devem ser verificadas para cada um dos itens listados.

Nota 3. Portas a bloquear no firewall

No final do documento, você encontrará uma seção extra que inclui uma lista das portas associadas aos serviços verificados e atacados com maior frequência.

Ao bloquear o tráfego a estas portas, seja no firewall ou em qualquer outro dispositivo de proteção na rede de perímetro, estará adicionando-se um nível de defesa maior, que o resguardará melhor de eventuais erros de configuração. Repare, no entanto, que usar um firewall para bloquear tráfego direcionado a uma porta específica não o protege de ataques de usuários internos ou de hackers que tenham penetrado na sua rede através de outros meios.

Nota 4. Varredura automática a procura das vulnerabilidades "Top 20"

Este documento apresenta métodos manuais para verificar se um sistema possui ou não as vulnerabilidades incluídas na lista "Top 20". Uma das formas mais eficazes de identificar as vulnerabilidades Windows e Unix - principalmente se você tem o cuidado de auditar o sistema antes dele entrar em produção e também de auditá-lo regularmente - é usar uma ferramenta de scan automática. Bob Todd, autor da ferramenta de scan SARA, criou uma versão especial da mesma projetada especificamente para identificar a presença das vulnerabilidades da lista "Top 20" do SANS/FBI. A ferramenta pode ser obtida através do site do CIS (Center for Internet Security), em <http://www.cisecurity.org/> Algumas outras ferramentas de scan também podem ser utilizadas. O instituto SANS manterá uma lista das ferramentas que incluam, dentre as suas

funcionalidades, a identificação das vulnerabilidades contidas na lista "Top 20" (<http://www.sans.org/>).

Nota 5. Referências ao Serviço de Indexação de Vulnerabilidades ICAT

Cada referência a uma vulnerabilidade CVE está associada a uma entrada no serviço de indexação de vulnerabilidades ICAT, mantido pelo NIST (National Institute of Standards and Technology's) em <http://icat.nist.gov/>. O ICAT oferece uma breve descrição de cada vulnerabilidade, uma lista das características de cada vulnerabilidade (por exemplo, a dimensão do ataque e os danos potenciais associados), uma lista dos nomes dos software vulneráveis incluindo suas respectivas versões, referências a alertas de segurança sobre uma determinada vulnerabilidade e informações sobre como corrigi-la.

[Back to Top ^](#)

Vulnerabilidades Que Afetam todos os Sistemas (G)

G1 - Instalações default de sistemas operacionais e aplicativos

G1.1: Descrição

A maioria dos softwares, incluindo sistemas operacionais e aplicativos, vem com scripts ou programas que têm por objetivo instalar os sistemas tão rapidamente quanto possível, com a máxima funcionalidade e com o mínimo de esforço por parte do administrador. Para atingir este objetivo, os programas normalmente instalam mais componentes do que a maioria dos usuários necessita. A filosofia do fabricante é que é melhor habilitar funções que não são necessárias, do que o usuário ter que instalar funções adicionais na medida em que for preciso. Esta visão, embora seja conveniente para o usuário, origina a existência de muitas das mais críticas vulnerabilidades de segurança, pois os usuários não mantêm, nem corrigem componentes de software não usados. Além disso, muitos usuários desconhecem o que realmente é instalado, deixando programas perigosos no sistema, simplesmente porque eles não sabem que estão lá.

Estes serviços vulneráveis fornecem meios para os atacantes invadirem seus sistemas.

No que diz respeito aos sistemas operacionais, as instalações default comumente incluem serviços adicionais, abrindo conseqüentemente as portas associadas a eles. É justamente por estas portas que os atacantes costumam invadir. Quanto menos portas abertas, menor a probabilidade de o sistema ser invadido.

No que diz respeito aos aplicativos, normalmente, as instalações default incluem scripts ou programas de exemplos, e que em princípio são desnecessários. Uma das vulnerabilidades mais sérias relacionada com servidores web diz respeito aos scripts de exemplo, os atacantes os usam para invadir o sistema ou obter informação sobre ele. Na maioria dos casos, o administrador de algum sistema comprometido ignora a instalação de tais scripts. Os scripts de exemplo constituem um grave problema, pois normalmente não passam por um processo de controle de qualidade tão apurado quanto outros software. Aliás, na maioria das vezes, eles são escritos sem nenhuma preocupação de segurança. A verificação de erros é freqüentemente esquecida, o que faz com que estes scripts de exemplo se constituam em um terreno fértil para ataques do tipo buffer overflow.

G1.2 Sistemas Afetados:

A maioria dos sistemas operacionais e aplicativos.

Lembre-se que praticamente todas as extensões de terceiros que acompanham os servidores web incluem arquivos usados como exemplo, muitos dos quais são potencialmente perigosos.

G1.3 Entradas CVE:

(Nota: Esta lista não é completa. É apenas uma amostra de algumas das vulnerabilidades englobadas nesta

categoria).

[CVE-1999-0415](#), [CVE-1999-0678](#), [CVE-1999-0707](#), [CVE-1999-0722](#), [CVE-1999-0746](#),
[CVE-1999-0954](#), [CVE-2000-0112](#), [CVE-2000-0192](#), [CVE-2000-0193](#), [CVE-2000-0217](#),
[CVE-2000-0234](#), [CVE-2000-0283](#), [CVE-2000-0611](#), [CVE-2000-0639](#), [CVE-2000-0672](#),
[CVE-2000-0762](#), [CVE-2000-0868](#), [CVE-2000-0869](#), [CVE-2000-1059](#)

G1.4 Como determinar se você está vulnerável:

Se você já utilizou um programa para instalar um sistema ou serviço (como a maioria das companhias já o fez), e não removeu os serviços desnecessários nem instalou todos os patches de segurança, então seu sistema é passível de ataques.

Mesmo que você tenha seguido procedimentos adicionais de configuração, você ainda estará vulnerável. É preciso que seja executada uma ferramenta de scan de portas e de vulnerabilidades contra qualquer sistema que irá ser conectado na Internet. Ao analisar os resultados, tenha em mente o princípio que seus sistemas devem funcionar com o menor número de serviços e de pacotes de software necessários para executar as tarefas requeridas pelo seu sistema. Qualquer programa ou serviço adicional constitui-se em uma ferramenta para o atacante - especialmente, porque a maioria dos administradores de sistemas não corrige os programas e serviços que efetivamente não estão sendo usados.

G1.5 Como se proteger:

Remova o software desnecessário, desabilite serviços desnecessários e feche portas não usadas. Devido ao fato que esta pode ser uma tarefa longa e árdua, muitas das grandes organizações desenvolveram, para cada sistema operacional e conjunto de aplicativos usados, diretrizes de instalação padronizadas. Estas diretrizes incluem a instalação das funcionalidades mínimas necessárias para que o sistema funcione de maneira eficaz. O CIS (Center for Internet Security) desenvolveu um benchmark para avaliar a configuração mínima de segurança em sistemas Solaris e Windows 2000, fruto da experiência e conhecimento de mais de 170 organizações de diversos países (veja <http://www.cisecurity.org/>). As ferramentas de teste e de benchmarking para outros sistemas estão sendo desenvolvidas. As ferramentas do CIS podem ser usadas para testar o nível de segurança e comparar a segurança de sistemas entre as várias divisões de uma empresa. As diretrizes do CIS podem ser usadas para melhorar a segurança da maioria dos sistemas operacionais.

[Back to Top ^](#)

G2 - Contas sem senhas ou com senhas fracas

G2.1: Descrição:

A maioria dos sistemas é configurada para usar senhas como a primeira, e única, linha de defesa. A identidade do usuário (User ID) é razoavelmente fácil de obter, e a maioria das companhias oferece acesso dial-up que comumente dribla o firewall. Conseqüentemente, se um atacante puder determinar um nome e uma senha de cliente, poderá também ter acesso à rede. Senhas fáceis de adivinhar e senhas default constituem um problema grave, pior ainda são as contas sem senha. Na prática, todas essas contas (com senhas fracas, senhas default, ou pior, sem senhas) devem ser removidas do seu sistema.

Adicionalmente, muitos sistemas têm contas de usuário que fazem parte da instalação padrão, as quais geralmente mantêm a mesma senha em todas as instalações do software. Os atacantes procuram geralmente por este tipo de contas, amplamente conhecidas pela comunidade 'blackhat'. Conseqüentemente, é preciso que estas contas sejam identificadas e removidas do sistema.

G2.2 Sistemas Afetados:

Qualquer sistema operacional ou aplicativo onde os usuários sejam autenticados através de um ID e senha.

G2.3 Entradas CVE:

(Nota: Esta lista não é completa. É apenas uma amostra de algumas das vulnerabilidades englobadas nesta categoria).

[CVE-1999-0291](#), [CAN-1999-0501](#), [CAN-1999-0502](#), [CAN-1999-0503](#), [CAN-1999-0505](#),
[CAN-1999-0506](#), [CAN-1999-0507](#), [CAN-1999-0508](#), [CAN-1999-0516](#), [CAN-1999-0517](#),
[CAN-1999-0518](#), [CAN-1999-0519](#)

G2.4 Como determinar se você está vulnerável:

Para determinar se você está vulnerável ou não, é preciso identificar quais as contas presentes no seu sistema. Para tal, deve ser seguido o seguinte procedimento:

1. Examine as contas nos seus sistemas e crie uma lista mestre. Não esqueça de verificar senhas de sistemas como roteadores e impressoras, copiadoras e controladores de impressora conectados à Internet.
2. Desenvolva procedimentos para adicionar contas pré-autorizadas à lista, e para remover contas quando elas não estão mais em uso.
3. Verifique a lista regularmente para certificar-se que nenhuma conta nova tenha sido adicionada sem permissão e as contas não utilizadas tenham sido removidas.
4. Utilize uma ferramenta de quebra de senhas para identificar contas com senhas fracas ou sem senha. (Antes de usar este tipo de ferramentas, verifique se você tem permissão oficial por escrito).
 - a. LC3 - Microsoft Windows NT e Windows 2000 <http://atstake.com>
 - b. Microsoft Personal Security Advisor - Microsoft Windows NT e Microsoft Windows 2000, <http://www.microsoft.com/security/mpsaA>
 - c. John the Ripper - Unix, <http://www.openwall.com/john>
 - d. Pandora - Novell, <http://www.nmrc.org/pandoraA>
5. Mantenha procedimentos rígidos para remoção de contas de empregados ou contratados quando saem, ou quando as contas não são mais necessárias.

G2.5 Como se proteger:

Para eliminar estes problemas de senha, duas etapas precisam ser executadas. Na primeira, todas as contas sem senhas recebem uma ou são definitivamente removidas e as senhas fracas são fortalecidas. Infelizmente, quando é solicitado aos usuários fortalecerem as suas senhas, freqüentemente eles escolhem outra igualmente fácil de se adivinhar. Isto nos leva à segunda etapa: as novas senhas, quando alteradas, também precisam ser verificadas. Existem programas específicos que não permitem alterações de senha que não estão de acordo com a sua política de segurança, os mais populares são:

1a. Para Unix: Npasswd (SunOS 4/5, Digital Unix, HP/UX, e AIX)
<http://www.utexas.edu/cc/unix/software/npasswd>

1b. Para Unix: Cracklib e módulos associados do PAM (Linux)

2. Para Windows NT: Passfilt

<http://support.microsoft.com/support/kb/articles/Q161/9/90.asp>

Estes programas garantem que as senhas sejam de comprimento e composição tal que sejam difíceis de serem quebradas ou descobertas. Repare que muitos fabricantes de sistemas Unix incluem algum mecanismo de suporte interno para a construção de senhas confiáveis, mas existem também outros pacotes disponíveis.

Muitas organizações adicionam programas de controle de senha, mecanismos que garantem que as senhas sejam mudadas regularmente, e que senhas antigas não sejam reutilizadas. Se a expiração de senhas for implementada, certifique-se que os usuários sejam alertados a trocar a sua senha antes dela expirar. Diante de uma mensagem do tipo: "sua senha expirou, ela deve ser mudada", a maioria dos usuários tende a escolher uma senha fraca.

O sistema Windows 2000 da Microsoft inclui opções de restrição de senha no Group Policy. Um administrador pode configurar a rede de forma tal que as senhas de usuários requeiram comprimento mínimo, idade mínima e máxima, e outros parâmetros. A idade mínima é importante pois sem ela os usuários tendem a mudar sua senha quando requerido, mas tornam a usá-la logo em seguida. Requerendo-se idades mínimas em senhas se força aos usuários a lembrá-las e torna menos provável a chance deles voltarem a usar as senhas anteriores.

Outro ponto importante é a conscientização dos usuários para entender como e por quê escolher senhas fortes. A recomendação mais comum dada durante o processo de escolha de senhas é escolher uma frase ou parte de uma canção que inclua um número, e construir a senha da primeira ou segunda letra de cada palavra que compõe a frase, além de dígitos de quaisquer números. Adicionando pontuação torna a senha ainda mais difícil de ser quebrada.

Uma outra maneira de se proteger contra senhas fracas ou mesmo contas sem senhas, é utilizar uma forma alternativa de autenticação de usuários, tal como sistemas de geração de senhas ou biometria. Se você estiver tendo problemas com senhas fracas, use meios alternativos de autenticar usuários.

[Back to Top ^](#)

G3. Backups incompletos ou inexistentes

G3.1: Descrição:

Quando um incidente ocorrer (e ocorrerá em quase todas organizações), a recuperação do incidente requer backups atualizados e métodos de recuperação dos dados previamente testados. Algumas organizações fazem backups diários, mas nunca verificam se eles estão realmente funcionando. Outras criam políticas e procedimentos de backup, mas não de restauração. Frequentemente, tais erros são descobertos somente depois que um hacker invade os sistemas e os dados são destruídos, ou arruinados de alguma outra maneira.

Um segundo problema que envolve backups é a falta de proteção física das mídias. Os backups contêm a mesma informação sensível que reside no servidor, portanto devem ser protegidos da mesma maneira.

G3.2 Sistemas Afetados:

Qualquer sistema crítico.

G3.3 Entradas CVE:

N/D

G3.4 Como determinar se você está vulnerável:

Um inventário deve ser feito identificando todos os sistemas críticos e, para cada um deles, deve ser

executada uma análise identificando o risco e a ameaça correspondente. As políticas e os procedimentos de backup devem claramente remeter a estes sistemas. Uma vez identificados os sistemas críticos, deve ser validado o seguinte:

1. Existem procedimentos de backup para tais sistemas?
2. O intervalo dos backups é adequado?
3. Os backups estão sendo realizados de acordo com os procedimentos?
4. É verificada a mídia usada nos backup para certificar-se que os dados estão sendo armazenados corretamente?
5. A mídia de backup está corretamente protegida, seja ela mantida dentro ou fora da empresa?
6. Existem cópias do sistema operacional e de aplicativos de restauração que sejam armazenadas fora da empresa?
7. Os procedimentos de restauração foram validados e testados?

G3.5 Como se proteger:

No mínimo, os backups devem ser feitos diariamente. Na maioria das organizações, o requisito mínimo é que sejam executados backups completos semanalmente e backups incrementais diariamente. Ao menos uma vez por mês, a mídia deve ser verificada restaurando-se os dados em um servidor de teste para comprovar se os mesmos estão sendo corretamente restaurados. Esta é a exigência mínima. Algumas companhias executam backups completos uma ou várias vezes por dia. No que diz respeito a backups, a mais recente solução consiste em ter uma rede inteiramente redundante que implemente tolerância a falhas- solução usada em sistemas de tempo real críticos (financeiros e de comércio eletrônico), sistemas que controlam infra-estruturas críticas, e alguns sistemas do Departamento de Defesa dos EUA (DoD).

[Back to Top ^](#)

G4 - Grande número de portas abertas

G4.1: Descrição:

Ambos, tanto os usuários legítimos quanto os atacantes, se conectam aos sistemas através de portas abertas. Quanto maior o número de portas abertas, maior a possibilidade de alguém se conectar ao seu sistema. Consequentemente, é importante manter o menor número de portas abertas necessárias para o correto funcionamento do sistema, o restante deve ser fechado.

G4.2 Sistemas Afetados:

A maioria dos sistemas operacionais.

G4.3 Entradas CVE:

(Nota: Esta lista não é completa. É apenas uma amostra de algumas das vulnerabilidades englobadas nesta categoria).

[CVE-1999-0189](#), [CVE-1999-0288](#), [CVE-1999-0351](#), [CVE-1999-0416](#), [CVE-1999-0675](#),
[CVE-1999-0772](#), [CVE-1999-0903](#), [CVE-2000-0070](#), [CVE-2000-0179](#), [CVE-2000-0339](#),
[CVE-2000-0453](#), [CVE-2000-0532](#), [CVE-2000-0558](#), [CVE-2000-0783](#), [CVE-2000-0983](#)

G4.4- Como determinar se você está vulnerável:

O comando netstat pode ser executado localmente a fim de identificar quais portas estão abertas, no entanto a forma mais confiável de fazer isto é utilizando uma ferramenta de scan de portas contra seus sistemas. O resultado é uma lista de todas as portas que estão realmente ativas. Caso os resultados obtidos através do netstat difiram dos obtidos usando a ferramenta de scan, é preciso que se investigue o por quê. Uma vez que ambas listas coincidam, procure saber por quê cada uma das portas indicadas está aberta, e o que está sendo executado em cada uma delas. Toda porta que não puder ser justificada deve ser fechada. A lista de portas final deve ser gravada e usada para fazer auditorias regularmente, garantindo assim que não apareça nela nenhuma porta adicional.

Dentre as muitas ferramentas de scan de portas, a mais popular é o Nmap. A versão Unix desta ferramenta pode ser encontrada em: <http://www.insecure.org/nmap/>, enquanto que a versão para sistemas NT pode ser encontrada em: <http://www.eeye.com/html/Research/Tools/nmapnt.html>. Existem algumas outras ferramentas de scan de portas que também funcionam bem. Qualquer ferramenta que for usada, ela DEVE ser configurada para varrer todas as portas UDP e TCP no range 1-65535.

Antes de executar algum tipo de varredura de portas nos sistemas dentro da sua organização, você deve ter sempre permissão por escrito. Alguns sistemas operacionais, em particular dispositivos que implementem TCP/IP nativo, quando examinados, podem apresentar um comportamento imprevisível. Esta varredura pode também acionar firewalls ou sistemas de detecção de intrusão internos, podendo ser interpretada como um ataque interno, caso não for reportado o alerta de maneira apropriada.

G4.5 Como se proteger:

Uma vez identificadas as portas abertas, sua tarefa consiste em identificar o conjunto mínimo de portas que devem permanecer abertas para o bom funcionamento do sistema - feche todas as portas restantes. Para fechar uma porta desabilite ou remova o serviço associado a ela.

Em sistemas Unix, muitos dos serviços são controlados pelo super daemon inetd e seu correspondente arquivo de configuração, inetd.conf. O arquivo inetd.conf lista os serviços associados a uma determinada porta, e freqüentemente é usado para fechar portas. Ao remover um determinado serviço do arquivo inetd.conf, reinicializando-o em seguida, se faz com que a porta associada a tal serviço seja fechada. Outros serviços são inicializados através de scripts, os quais são executados durante o processo de inicialização do sistema (tais como: /etc/rc, /etc/rc.local, ou scripts encontrados nos diretórios /etc/rc*). Consulte a documentação do sistema para saber como desabilitar estes scripts, uma vez que o procedimento varia para cada versão Unix. Além disso, existe um programa chamado lsof que pode ser usado para auditar portas abertas. Este programa pode ser obtido em: <ftp://vic.cc.purdue.edu/pub/tools/UNIX/lsof/lsof.tar.gz>

Em sistemas Windows NT e 2000, para determinar que serviço/programa está escutando em uma determinada porta, pode ser usada a ferramenta fport, da <http://www.foundstone.com/>. No Windows XP, pode ser utilizado o comando netstat com a opção `-o`. Esta informação lhe permitirá desabilitar o serviço e fechar a porta associada a ele.

[Back to Top ^](#)

G5 - Ausência de filtro de pacotes de entrada e saída que garantam o uso de endereços válidos

G5.1: Descrição:

O Spoofing de endereços IP é um método comumente usado por atacantes para esconder evidências. Por o exemplo, o tão popular ataque 'smurf' faz uso de uma funcionalidade dos roteadores para enviar pacotes a milhares de máquinas. Cada pacote contém o endereço forjado de uma vítima. Os computadores que recebem este tipo de pacote, em resposta, inundam à vítima com outros pacotes, chegando a retirá-la da rede em

alguns casos. Filtrando o tráfego que entra na sua rede (ingress filtering) e que sai (egress filtering) pode ajudar a elevar o nível de proteção. As regras básicas de filtragem são como segue:

1. Nenhum pacote que entra em sua rede pode ter como endereço de origem qualquer IP da sua rede interna.
2. Todo pacote que entra em sua rede deve ter como endereço de destino algum endereço pertencente à sua rede interna
3. Qualquer pacote que sai da sua rede deve ter como endereço de origem algum IP que pertença à sua rede interna.
4. Nenhum pacote que sai da sua rede deve ter como endereço de destino algum IP de sua rede interna.
5. Nenhum pacote que entra ou sai de sua rede deve conter como endereço de origem ou destino qualquer endereço privado ou endereço reservado segundo descrito na RFC 1918. Estão incluídos neste espaço de endereçamento as redes 10.x.x.x/8, 172.16.x.x/12 ou 192.168.x.x/16, e a rede 127.0.0.0/8, correspondente a loopback.
6. Bloqueie qualquer pacote que tenha a opção 'source routing' ativada ou o campo 'IP Options' ativado.
7. Endereços reservados de auto-configuração DHCP e Multicast também devem ser bloqueados:

- 0.0.0.0/8
- 169.254.0.0/16
- 192.0.2.0/24
- 224.0.0.0/4
- 240.0.0.0/4

G5.2 Sistemas Afetados:

A maioria dos sistemas operacionais.

G5.3 Entradas CVE:

(Nota: Esta lista não é completa. É apenas uma amostra de algumas das vulnerabilidades englobadas nesta categoria).

[CAN-1999-0528](#), [CAN-1999-0529](#), [CAN-1999-0240](#), [CAN-1999-0588](#)

G5.4 Como determinar se você está vulnerável:

Tente enviar um pacote forjado e observe se seu firewall ou roteador externo o bloqueia. O dispositivo não somente deve bloquear o tráfego, mas deve também gerar um registro do evento (log), que indique que os pacotes forjados foram bloqueados. Repare, no entanto, que isto abre as portas para um ataque novo: flood no arquivo de logs. Certifique-se que seu sistema de logging suporta uma carga pesada, caso contrário ele será vulnerável a um ataque do tipo DoS (Denial of Service). Programas como o nmap podem ser usados para enviar pacotes criados ou pacotes com endereços forjados, para testar este tipo de filtros. Uma vez que os filtros foram adequadamente implementados, não assuma que eles estão funcionando de maneira efetiva, teste-os freqüentemente.

G5.5 Como se proteger:

Para defender-se deste tipo de ataque, você deve implementar regras de filtragem no seu firewall e roteador de borda. Os seguintes exemplos correspondem a regras em um roteador Cisco:

1. Filtros de entrada:

```
interface Serial 0
  ip address 10.80.71.1 255.255.255.0
  ip access-group 11 in
access-list 11 deny 192.168.0.0 0.0.255.255
access-list 11 deny 172.16.0.0 0.15.255.255
access-list 11 deny 10.0.0.0 0.255.255.255
access-list 11 deny <your internal network>
access-list 11 permit any
```

2. Filtros de saída:

```
interface Ethernet 0
  ip address 10.80.71.1 255.255.255.0
  ip access-group 11 in
access-list 11 permit <your internal network>
```

[Back to Top ^](#)

G6 - Sistema de logs inexistente ou incompleto

G6.1: Descrição

Uma das premissas de segurança é: "A prevenção é ideal, mas a detecção é imprescindível". Enquanto você permitir tráfego entre a sua rede e a Internet, existe a oportunidade de um atacante invadir a sua rede. Novas vulnerabilidades surgem a cada semana, e poucas são as maneiras de defender-se de um atacante que use uma vulnerabilidade nova. Uma vez que você tenha sido atacado, sem registros (logs), a possibilidade de você descobrir o que eles fizeram no seu sistema é mínima. Sem esta informação, sua organização deve escolher entre fazer uma restauração completa do sistema operacional a partir da mídia original, torcendo para que os dados armazenados estejam corretos; ou correr o risco de possuir um sistema ainda controlado pelo hacker.

Você não pode detectar um ataque se não sabe o que está ocorrendo na sua rede. Os logs provêm detalhes sobre o que está acontecendo, os sistemas que estão sendo atacados e os que foram efetivamente invadidos.

O registro de eventos deve ser feito de maneira regular em todos os sistemas críticos, e os logs devem ser devidamente armazenados e arquivados, pois você nunca sabe quando eles serão necessários. A maioria dos especialistas recomenda o envio de todos os logs a um servidor central que grave os dados em uma mídia que não possa ser apagada, de forma que o atacante não possa adulterar os logs e evitar assim a sua detecção.

G6.2 Sistemas Afetados:

Todos os sistemas operacionais e dispositivos de rede.

G6.3 Entradas CVE:

[CAN-1999-0575](#), [CAN-1999-0576](#), [CAN-1999-0578](#)

G6.4 Como determinar se você está vulnerável:

Audite os logs dos sistemas mais críticos. Se você não tiver logs, ou se eles não estiverem armazenados em um servidor central e copiados em mídia segura, você está vulnerável.

G6.5 Como se proteger:

Configure todos os seus sistemas de logs para registrar as informações localmente e para enviar os logs a um sistema remoto. Isto provê redundância e adiciona uma camada extra de segurança. Além disso, ambos sistemas de registro podem ser comparados, onde qualquer discrepância pode indicar atividade suspeita. Adicionalmente, este esquema permite o cruzamento de informações: uma entrada isolada no arquivo de logs de um único servidor pode não ser suspeita, mas a mesma entrada em 50 servidores de uma organização diferindo em apenas um minuto entre uma e outra, pode ser sinal de um problema maior.

Quando possível, envie os logs a um dispositivo que use mídia que não possa ser apagada.

[Back to Top ^](#)

G7 - Programas CGI vulneráveis

G7.1 Descrição

A maioria dos servidores, incluindo IIS da Microsoft e Apache, suportam programas CGI (Common Gateway Interface) para proporcionar interatividade em páginas web, permitindo algumas funções como o levantamento e a verificação de dados. De fato, a maioria dos servidores web são distribuídos com programas CGI de exemplo. Infelizmente, muitos programadores de CGI não consideram que seus programas oferecem, para qualquer usuário de qualquer lugar na Internet, uma ligação direta com o sistema operacional da máquina que abriga o servidor web. Os programas CGI vulneráveis representam para os atacantes um alvo particularmente atraente porque são relativamente fáceis de serem localizados e operam com os privilégios do próprio servidor web.

Os atacantes costumam utilizar os programas CGI vulneráveis para desfigurar websites, roubar números de cartão de crédito, ou instalar 'backdoors' para permitir futuras invasões. Quando o website do Departamento de Justiça foi desfigurado, uma investigação concluiu que muito provavelmente uma brecha de segurança em um programa CGI tinha sido o caminho usado pelos atacantes. Da mesma forma, os aplicativos do servidor web são igualmente vulneráveis às ameaças criadas por programadores descuidados. Como regra geral, os programas de exemplos que acompanham as distribuições dos servidores web sempre devem ser retirados dos sistemas de produção.

G7.2 Sistemas Afetados:

Todos os servidores Web.

G7.3 Entradas CVE:

(Nota: Esta lista não é completa. É apenas uma amostra de algumas das vulnerabilidades englobadas nesta categoria).

[CVE-1999-0067](#), [CVE-1999-0346](#), [CVE-2000-0207](#), [CVE-1999-0467](#), [CAN-1999-0509](#),
[CVE-1999-0021](#), [CVE-1999-0039](#), [CVE-1999-0058](#), [CVE-2000-0012](#), [CVE-2000-0039](#),
[CVE-2000-0208](#), [CAN-1999-0455](#), [CAN-1999-0477](#)

G7.4 Como determinar se você está vulnerável:

Se você tiver qualquer programa de exemplo no seu servidor web, você está vulnerável. Se você tiver programas CGI legítimos, certifique-se de estar usando a versão mais recente, e execute contra o seu site

uma ferramenta de scan de vulnerabilidades. Simulando o comportamento de um atacante, você estará preparado para proteger seus sistemas. Para encontrar scripts CGI vulneráveis, você pode usar a ferramenta Whisker, que pode ser encontrada em:

<http://www.wiretrip.net/rfp/>

G7.5 Como se proteger:

A seguir, são listadas as diretrizes básicas que devem ser seguidas para proteger seu site das vulnerabilidades nos programas CGI:

1. Remova do seu servidor web de produção todos os programas CGI de exemplo.
2. Examine os programas CGI restantes e remova os que são considerados inseguros.
3. Assegure-se que todos os programadores de CGI sigam uma estrita política de verificação de tamanho nos buffers de entrada.
4. Aplique patches para as vulnerabilidades que não podem ser removidas.
5. Certifique-se que seu diretório /cgi não inclua nenhum compilador ou interpretador.
6. Remova o script 'view-source' do diretório cgi-bin.
7. Não rode seu servidor web com privilégios de administrador. A maioria dos servidores web pode ser configurada para rodar como processos de algum usuário menos privilegiado, tal como o usuário "nobody".
8. Não habilite suporte a CGI em servidores web que não o necessitem.

[Back to Top ^](#)

Vulnerabilidades no Windows (W)

W1 - Falha no Unicode conhecida como "Web server folder traversal"

W1.1 Description:

O Unicode é um padrão para representar caracteres, onde cada símbolo utiliza dois bytes, o que permite um total de 65.536 combinações, com as quais é possível representar o alfabeto da maioria das línguas do mundo. O padrão Unicode foi adotado pela maioria dos fabricantes de software, incluindo a Microsoft. O envio de uma URL que contém uma seqüência inválida de Unicode UTF-8 a um servidor IIS por um atacante, pode forçar o servidor a executar comandos arbitrários. Este tipo de ataque é conhecido também como o ataque "directory transversal".

Os caracteres equivalentes em Unicode de / e \ são %2f e %5c, respectivamente.

Entretanto, você pode também representar estes caracteres usando seqüências denominadas "overlong". As seqüências "overlong" são as representações inválidas de Unicode que são mais longas do que o requerido realmente para representar o caracter. Tanto / como \ podem ser representados com um único byte. Uma representação "overlong", tal como %c0%af representa o caracter / usando dois bytes. O IIS não foi escrito para verificar a segurança em seqüências do tipo "overlong". Assim, ao enviar uma seqüência de Unicode overlong em uma URL, as verificações de segurança da Microsoft serão contornadas. Se o pedido for feito a um diretório marcado como "executável", o atacante poderá fazer com que os arquivos sejam executados no servidor. Informação adicional sobre a ameaça do ataque Unicode pode ser encontrada em:

<http://www.wiretrip.net/rfp/p/doc.asp?id=57&face=2>

W1.2 Sistemas Afetados:

Windows NT 4.0 da Microsoft com IIS 4.0 e Windows 2000 Server com IIS 5.0, que não possuem o "Service Pack 2" instalado.

W1.3 Entradas CVE:

[CVE-2000-0884](#)

W1.4 Como determinar se você está vulnerável:

Se você estiver usando uma versão de IIS sem patches, você provavelmente está vulnerável. A melhor maneira de determinar se você está vulnerável é utilizar a ferramenta hfnetchk. Tal ferramenta é indicada para verificar o estado de instalação de patches em um ou vários sistemas, podendo ser utilizada através da rede. A vulnerabilidade Unicode "Web server folder traversal" foi sanada usando as seguintes correções:

- Q269862 - MS00-057
- Q269862 - MS00-078
- Q277873 - MS00-086
- Q293826 - MS01-026
- Q301625 - MS01-044
- Windows 2000 Service Pack 2

Se nenhuma destas correções estiver instalada, o sistema está vulnerável.

Para uma verificação mais específica, execute o ataque em seu próprio sistema para ver se é bem sucedido. Tente executar o seguinte comando em seu browser contra seu servidor IIS:

<http://vitima/winnt/system32/cmd.exe?/c%2Bdir%2Bc:%5C%20>

Esta URL pode necessitar de modificações para testar um determinado sistema. Se o diretório 'scripts' foi removido (o que é recomendado), este comando falhará. Você pode testar um sistema temporariamente criando um diretório que tenha permissões para executar comandos, ou usando um outro diretório (diferente do diretório "scripts" usado no exploit) que possua estas permissões. Por exemplo, você pode ter removido o diretório "scripts", mas tem um diretório chamado cgi-bin, logo, teste seu sistema usando este último.

Se você estiver vulnerável, esta URL transmitirá ao navegador uma lista do diretório C: do servidor vulnerável. Você está realizando o ataque da mesma forma que um atacante. A única diferença é você está emitindo um comando não destrutivo (como o dir), quando um atacante poderia fazer danos significativos ou criar um "backdoor" em seu sistema.

W1.5 Como se proteger:

Para defender os seus sistemas contra este ataque, você deve instalar os patches mais recentes da Microsoft. Para mais informações sobre como obtê-los, veja o boletim de segurança da Microsoft em:

<http://www.microsoft.com/technet/security/bulletin/MS00-078.asp>

As ferramentas 'IIS Lockdown' e 'URL Scan' também protegerão seus sistemas contra esta vulnerabilidade. A ferramenta IIS Lockdown ajuda os administradores a proteger um servidor IIS, e está disponível em:

<http://www.microsoft.com/technet/security/tools/locktool.asp>

A ferramenta URLScan funciona como um filtro para as requisições HTTP. Por exemplo, ele pode ser usado

para filtrar pedidos que contenham caracteres codificados com UTF8. A ferramenta URLScan está disponível em:

<http://www.microsoft.com/technet/security/URLScan.asp>

[Back to Top ^](#)

W2 - Buffer Overflow nas Extensões ISAPI

W2.1 Descrição

O servidor Internet Information Server (IIS), da Microsoft, é o software de servidor Web encontrado na maioria dos web sites operando nas plataformas Windows NT e Windows 2000. Quando o IIS é instalado, diversas extensões de ISAPI são instaladas automaticamente. O ISAPI (Internet Services Application Programming Interface), permite aos programadores estender as potencialidades de um servidor IIS utilizando bibliotecas DLLs. Várias DLLs, como idq.dll, contém erros de programação que resultam na realização imprópria da checagem de erros. Em particular, não bloqueiam strings de entrada longos (long input strings). Os atacantes podem enviar dados a estas DLLs, no que é conhecido como buffer overflow, resultando no controle completo do servidor IIS por parte do atacante.

W2.2 Sistemas Afetados:

O buffer overflow do idq.dll afeta o Microsoft Indexing Server 2.0 e o Indexing Service no Windows 2000. O buffer overflow do .printer afeta o servidor Windows 2000 Server, Advanced Server, e Server Data Center Edition com IIS 5.0 instalado. A DLL vulnerável também acompanha a versão profissional do Windows 2000 mas não é mapeada na instalação padrão. Por precaução, você deve usar o Group Policy, se possível, para desabilitar a impressão via Web (Computer Configuration:Administrative Templates:Printers) nas estações de trabalho.

W2.3 Entradas CVE:

[CVE-1999-0412](#), [CVE-2001-0241](#), [CAN-2000-1147](#), [CAN-2001-0500](#)

W2.4 Como determinar se você está vulnerável:

Se o seu web server não tiver ao menos o Service Pack 2 instalado, você provavelmente está vulnerável. Se você não tiver certeza quais patches estão instalados, utilize a ferramenta Hfnetchk:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/hfnetchk.asp>

Os seguintes patches incluem as correções para o buffer overflow do .printer:

- Q296576 - MS01-023
- Q300972 - MS01-033
- Q301625 - MS01-044
- Windows 2000 SP2
- Q299444 - The Windows NT 4.0 Security Roll-up Package

Os seguintes patches incluem as correções para o buffer overflow do idq.dll:

- Q300972 - MS01-033
- Q301625 - MS01-044

- The Windows NT 4.0 Security Roll-up Package

W2.5 Como se proteger:

Instale os patches mais recentes da Microsoft. Estes podem ser encontrados em:

- Windows NT 4.0:
<http://www.microsoft.com/ntserver/nts/downloads/critical/q299444/default.asp>
- Windows 2000 Professional, Server and Advanced Server:
<http://www.microsoft.com/technet/security/bulletin/MS01-044.asp>
- Windows 2000 Datacenter Server: Patches para Windows 2000 Datacenter Server são específicos para o hardware utilizado e podem ser obtidos diretamente do fabricante.
- Windows XP: Estas vulnerabilidades não afetam o Windows XP.

O administrador deve retirar o mapeamento de todas as extensões de ISAPI que não forem necessárias. Verifique regularmente quais extensões foram novamente mapeadas.

Lembre-se do princípio do menor privilégio, seus sistemas devem funcionar com o menor número de serviços necessários para que funcionem corretamente.

As ferramentas "IIS Lockdown" e "URL Scan" também protegerão seu sistema contra esta vulnerabilidade. A ferramenta IIS Lockdown ajuda os administradores a proteger um servidor IIS, e está disponível em:

<http://www.microsoft.com/technet/security/tools/locktool.asp>

A ferramenta URLScan funciona como um filtro para as requisições HTTP. Exemplo: pode ser usado para filtrar os pedidos que contêm caracteres codificados com UTF8. A ferramenta URLScan está disponível em:

<http://www.microsoft.com/technet/security/URLScan.asp>

[Back to Top ^](#)

W3 - Brecha nos Serviços de Dados Remotos (RDS) do IIS

W3.1 Descrição

O servidor IIS da Microsoft (IIS) é o software de servidor Web encontrado na maioria dos web sites operando na plataforma Microsoft Windows NT e Windows 2000. Para executar comandos remotos com privilégios de administrador, os usuários maliciosos exploram falhas de programação nos serviços RDS (Remote Data Services), Serviços de Dados Remotos do IIS.

W3.2 Sistemas Afetados:

Sistemas Microsoft Windows NT 4.0 que utilizam o servidor IIS e têm o diretório virtual /msadc estão provavelmente vulneráveis.

W3.3 Entradas CVE:

[CVE-1999-1011](#)

W3.4 Como determinar se você está vulnerável:

Se você estiver com um sistema sem patches, você está vulnerável. Um guia excelente em relação à fragilidade do RDS e como corrigi-la pode ser encontrado em:

<http://www.wiretrip.net/rfp/p/doc.asp?id=29&iface=2>

W3.5 Como se proteger:

Não é possível corrigir esta falha através de um patch. Para se proteger contra esta vulnerabilidade, siga os passos encontrados nos seguintes boletins de segurança:

- <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>

Alternativamente, você pode se prevenir fazendo a respectiva atualização para uma versão de MDAC mais recente que 2.1. As versões mais recentes de MDAC estão disponíveis em:

<http://www.microsoft.com/data/download.htm>

[Back to Top ^](#)

W4 - NETBIOS: Falta de proteção nos compartilhamentos em redes Windows

W4.1: Descrição

O protocolo Server Message Block (SMB), conhecido também como Common Internet File System (CIFS), permite compartilhar arquivos através de redes. A configuração incorreta do SMB pode expor arquivos críticos do sistema ou permitir acesso completo do sistema a qualquer usuário hostil conectado à Internet.

Muitos usuários de forma ingênua, abrem seus sistemas aos hackers quando tentam facilitar a conveniência para colegas de trabalho, e alguns usuários externos quando abrem o acesso de leitura e escrita nos compartilhamentos realizados pela rede. Administradores de um site do governo utilizado para o desenvolvimento de software voltado para o planejamento de missão, permitiram acesso irrestrito aos seus arquivos, de modo que pessoas em um outro departamento do governo pudessem ter fácil acesso aos arquivos. No período de dois dias, os atacantes descobriram os compartilhamentos de rede abertos e roubaram o software de planejamento de missão.

Abrir o acesso para o compartilhamento de arquivos em máquinas Windows os faz vulneráveis ao roubo de informação e determinados tipos de vírus. Os sistemas operacionais Macintosh e Unix também são vulneráveis, se habilitarem o compartilhamento de arquivos.

Os mecanismos de SMB que permitem compartilhar arquivos também podem ser utilizados por atacantes para obter informações sensíveis dos sistemas Windows. A informação do usuário e do grupo (usernames, últimas datas de login, política de senha, informação de RAS), informações do sistema, e determinadas chaves do registro podem ser obtidas através de uma conexão "null session" ao serviço de sessão do NetBIOS. Esta informação é útil aos hackers porque lhes ajuda a adivinhar uma senha ou descobrir uma senha por via de um ataque de força bruta.

W4.2 Sistemas Afetados:

Sistemas Microsoft Windows NT e Windows 2000.

W4.3 Entradas CVE:

[CVE-1999-0366](#), [CVE-2000-0222](#), [CVE-2000-0979](#), [CAN-1999-0518](#), [CAN-1999-0519](#),
[CAN-1999-0520](#), [CAN-1999-0621](#), [CAN-2000-1079](#)

W4.4 Como determinar se você está vulnerável:

Um teste rápido, seguro e grátis, para identificar a presença de compartilhamento de arquivos SMB e as vulnerabilidades associadas, e que funciona em qualquer sistema Windows, está disponível no site da empresa Gibson Research Corporation na seguinte url: <http://grc.com/>. Deve-se clicar no ícone "ShieldsUP" e você receberá uma avaliação em tempo real se o sistema tem algum arquivo exposto através do SMB. As instruções detalhadas estão disponíveis para ajudar usuários do Microsoft Windows a lidar com as vulnerabilidades no SMB.

Repare que se você está conectado através de uma rede onde existe algum dispositivo intermediário que bloqueie SMB (firewall, por exemplo), a ferramenta "ShieldsUP" pode relatar que você não está vulnerável quando, de fato, você está. Este é o caso, por exemplo, dos usuários de cable modem onde o provedor está bloqueando SMB. A ferramenta "ShieldsUP" irá reportar que você não está aparentemente vulnerável, no entanto, os 4000 ou mais usuários do mesmo sistema de cabo poderão explorar esta vulnerabilidade.

O conselheiro pessoal de segurança da Microsoft (Microsoft Personal Security Advisor) relatará se você é vulnerável a ataques de SMB, e pode também corrigir o problema. Como seu funcionamento é local, seus resultados são confiáveis. Está disponível em:

<http://www.microsoft.com/technet/security/tools/mpsa.asp>

W4.5 Como se proteger:

Utilize os próximos passos para se defender contra compartilhamentos desprotegidos:

1. Ao compartilhar arquivos, assegure que somente diretórios necessários estão compartilhados.
2. Para segurança adicional, permita o compartilhamento somente a endereços IP específicos, porque os nomes DNS podem ser forjados (spoofed).
3. Em sistemas Windows (NT e 2000), utilize o sistema de permissão de acesso a arquivos para permitir o compartilhamento somente com as pessoas que requerem acesso.
4. Para sistemas Windows, impeça a enumeração anônima dos usuários, grupos, configuração do sistema e das chaves de registro, através da conexão "null session". Veja o item W5 para mais informações.
5. Bloqueie conexões entrantes na sua rede (inbound) ao serviço de sessão de NetBIOS (porta 139 tcp) e ao Microsoft CIFS (porta 445 TCP/UDP) no roteador ou no próprio sistema operacional.
6. Considere a implementação da chave de registro "RestrictAnonymous" para sistemas conectados à Internet de forma isolada ou em domínios não confiáveis. Para mais informações, acesse as seguintes páginas:

Windows NT 4.0:

<http://support.microsoft.com/support/kb/articles/Q143/4/74.asp>

Windows 2000:

<http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP>

[Back to Top ^](#)

W5 - Vazamento de informações através de sessão anônima "null session"

W5.1 Descrição:

Uma conexão de sessão nula, também conhecida como o início de uma sessão anônima, é um mecanismo que permite que um usuário anônimo recupere informação (tal como nomes de usuários e arquivos compartilhados) sobre a rede, ou para conectar sem autenticação. É usada por aplicativos como explorer.exe para listar arquivos compartilhados em servidores remotos. Em sistemas Windows NT e Windows 2000, muitos dos serviços funcionam sob a conta SYSTEM, conhecido como LocalSystem no Windows 2000. A conta SYSTEM é usada para várias operações críticas do sistema. Quando uma máquina precisa recuperar dados de outro sistema, a conta SYSTEM abre uma sessão nula com a outra máquina.

A conta SYSTEM tem privilégios virtualmente ilimitados e não possui senha, o que impede que seja realizado o login com a conta SYSTEM. SYSTEM às vezes precisa acessar informações em outras máquinas como compartilhamentos, nomes de usuários, etc. -- funcionalidade do tipo Network Neighborhood. Como não é possível logar nos outros sistemas utilizando um identificador de usuário (UserID) e senha, é utilizada a sessão nula para se conseguir o acesso. Infelizmente, hackers também podem realizar o login utilizando-se do mesmo mecanismo.

W5.2: Sistemas Afetados:

Sistemas Windows NT 4.0 e Windows 2000

W5.3 Entradas CVE:

[CAN-2000-1200](#)

W5.4 Como determinar se você está vulnerável:

Tente conectar-se ao seu sistema através de uma sessão nula, usando o seguinte comando:

```
net use \\a.b.c.d\ipc$ "" /user:""
(onde a.b.c.d é o endereço IP do sistema remoto.)
```

Se você receber uma resposta "connection failed", então seu sistema não é vulnerável. Se não receber nenhuma resposta, o comando foi bem sucedido, e o seu sistema é vulnerável.

O programa "Hunt for NT" também pode ser usado. Ele é um componente do NT Forensic Toolkit disponibilizado em <http://www.foundstone.com/>.

W5.5 Como se proteger:

Os controladores de domínio requerem sessões nulas para se comunicar. Conseqüentemente, se você estiver trabalhando em um ambiente de domínio, você pode minimizar as informações que os atacantes podem obter, mas não poderá evitar completamente o vazamento das mesmas. Para limitar a informação disponível aos atacantes, em uma máquina de Windows NT 4.0, pode-se modificar a seguinte chave do registro:

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

Ajustando a chave de registro RestrictAnonymous para 1, ainda deixará alguma informação disponível aos usuários anônimos. No Windows 2000 você pode ajustar o valor para 2. Isto bloqueia o acesso de usuários anônimos a toda informação onde o acesso explícito não foi concedido a eles ou ao grupo Everyone (Todos), que inclui usuários anônimos.

Sempre que você modificar o registro, existe a chance de seu sistema parar de funcionar corretamente. Conseqüentemente, todas as mudanças devem ser testadas. Deve-se fazer um backup para garantir uma futura restauração.

Se você não precisar compartilhar arquivos e impressoras, pode-se desabilitar o serviço de NetBIOS do TCP/IP.

Nota: Configurando o RestricAnonymous em controladores de domínio e determinados outros servidores pode comprometer muitas operações normais da rede. Por esta razão, recomenda-se que somente aquelas máquinas que são visíveis à Internet tenham este valor configurado. Todas as outras máquinas devem ser protegidas por um firewall configurado para bloquear NetBIOS e CIFS.

Os usuários de Internet nunca devem ter permissão de acesso a qualquer controlador interno de domínio ou a outro computador não configurado especificamente para o acesso externo. Para evitar tal acesso, deve-se bloquear as seguintes portas no roteador ou no firewall externo:

TCP e UDP 135 até 139 e 445

[Back to Top ^](#)

W6 - Codificação fraca de senhas no SAM (LAN Manager hash):

W6.1 Descrição:

Embora a maioria dos usuários de Windows não necessite do suporte do gerente de LAN (Lan Manager), a Microsoft armazena hashes de senhas do Lan Manager na configuração padrão de sistemas Windows NT e em Windows 2000. O Lan Manager usa um esquema (scheme) muito fraco de criptografia para as senhas, mais antigo do que o utilizado em aplicativos mais recentes da Microsoft, com isso as senhas do Lan Manager podem ser quebradas em um curto período de tempo. Mesmo os hashes de senha fortes podem ser quebrados em menos de um mês. As principais fragilidades dos hash de senha Lan Manager são:

- Senha de tamanho fixo de, no máximo, 14 caracteres.
- Senhas curtas são preenchidas com "espaços" para conter 14 caracteres.
- Senha convertida para letras maiúsculas.
- Senha é dividida em dois blocos de sete letras.

Isto quer dizer que um programa para quebrar senhas somente precisa quebrar duas senhas de sete letras, sem mesmo necessitar testar as letras minúsculas. Além disso, o LAN Manager é vulnerável à interceptação da senha. A interceptação dos hashes da senha pode fornecer aos atacantes as senhas do usuário.

W6.2 Sistemas Afetados:

Sistemas Windows NT de Microsoft e 2000

W6.3 Entradas CVE:

N/D

W6.4 Como determinar se você está vulnerável:

Se você possuir uma instalação padrão do Windows NT ou 2000, você está vulnerável já que os hashes do LAN Manager são criados por default. Você pode (caso tenha a permissão por escrito de seu empregador) testar a facilidade de quebrar sua senha em seu próprio sistema, usando uma ferramenta de quebra de senhas, como o LC3 (versão 3 do l0phtcrack) por exemplo:

<http://www.atstake.com/research/lc3/download.html>

W6.5 Como se proteger:

A proteção de seus sistemas contra as senhas fracas geradas pelo LMHash pode ser feita de duas maneiras. A primeira consiste em desabilitar a autenticação usando LAN Manager através da rede e usar o método de autenticação NTLMv2. NTLMv2 (NT LanManager versão 2), os métodos de desafio/resposta do NT LanManager, superam a maioria das fragilidades no Lan Manager(LM) utilizando criptografia mais forte e melhorando os mecanismos de segurança e autenticação de sessão.

Com o Windows NT 4.0 SP4 e sistemas mais novos, incluindo o Windows 2000, a Microsoft possibilitou usar somente o NTLMv2 em sua rede. A chave do registro que controla esta opção no Windows NT e 2000 é: HKLM\System\CurrentControlSet\Control\LSA\LMCompatibilityLevel. Se você ajustar o valor para 3, a estação de trabalho ou o servidor apresentarão somente as credenciais NTLMv2 para autenticação. Se você ajustar o valor para 5, todos os controladores de domínio recusarão a autenticação do LM e do NTLM e aceitarão somente o NTLMv2.

É necessário planejar as mudanças com cuidado se você ainda tiver sistemas mais antigos, tais como Windows 95, em sua rede. Os sistemas mais antigos não usam NTLMv2 com o Microsoft Network Client. Em Windows 9x, o parâmetro é HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\LMCompatibility, e os valores permitidos são 0 ou 3 (com o Directory Services Client). A opção mais segura é começar se livrando daqueles sistemas mais velhos, já que não permitem que você forneça o nível mínimo da segurança que uma organização requer.

O artigo da Microsoft Technet "How to Disable LM Authentication on Windows NT [Q147706]" detalha as mudanças necessárias no registro de sistemas Windows 9x e os Windows NT/2000. O artigo "LMCompatibilityLevel and Its Effects [Q175641]" explica os problemas com este parâmetro. Um outro artigo muito útil da Technet é "How to Enable NTLMv2 Authentication for Windows 95/98/2000/NT [Q239869]". Este artigo explica o uso do Directory Services Client do Windows 2000 para conseguir que os sistemas Windows 95/98 superem a limitação de incompatibilidade com o NTLMv2.

O problema de simplesmente remover os hashes de LanMan na rede é que os hashes ainda são criados e armazenados no SAM ou Active Directory. A Microsoft recentemente desenvolveu um novo mecanismo para desligar a criação dos hashes de LanMan. Em sistemas Windows 2000, vá à seguinte chave do registro: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

No menu de edição do RegEdt32 ou do RegEdit, clique Add Key e adicione uma chave chamada NoLMHash. Após ter feito isto, feche o editor de registro e reinicialize o computador. A próxima vez que um usuário mudar a senha, o computador não criará um hash LanMan. Se esta chave for criada em um controlador de domínio Windows 2000, os hashes de LanMan não serão criados, nem armazenados no Active Directory.

Nos Windows XP, a mesma funcionalidade pode ser implementada ajustando-se o valor do registro para:

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

Isto terá o mesmo efeito da criação da chave NoLMHash nos sistemas Windows 2000. Para mais informações sobre estas mudanças, consulte o artigo Q299656 do Microsoft KnowledgeBase em:

<http://support.microsoft.com/support/kb/articles/q299/6/56.asp>

Vulnerabilidades no Unix(U)

U1 - Buffer Overflow nos serviços de Remote Procedure Call (RPC):

U1.1 Descrição:

As chamadas RPC (Remote Procedure Call) permitem que programas de um computador executem programas num outro computador. Este recurso é extensamente usado no acesso a alguns serviços de rede, tais como arquivos compartilhados via NFS, ou ainda no NIS. Muitas vulnerabilidades têm sido causadas por falhas no RPC e estão sendo ativamente exploradas. Há evidências de que a maioria dos sistemas que participaram dos ataques DDoS ocorridos durante 1999 e 2000, foi comprometida através de vulnerabilidades no serviço de RPC.

O ataque muito bem sucedido contra sistemas militares dos E.U.A. durante o incidente conhecido como 'Solar Sunrise', também explorou uma falha do RPC encontrada em centenas de sistemas no Departamento de Defesa dos EUA.

U1.2 Sistemas Afetados:

A maioria das versões Unix.

U1.3 Entradas CVE:

[CVE-1999-0003](#), [CVE-1999-0693](#), [CVE-1999-0696](#), [CVE-1999-0018](#), [CVE-1999-0019](#),
[CVE-1999-0704](#), [CAN-2001-0236](#), [CVE-2000-0666](#)

U1.4 Como determinar se você está vulnerável:

Verifique se você está usando um dos três serviços de RPC mais freqüentemente explorados, a saber:

- rpc.ttdbserverd
- rpc.cmsd
- rpc.statd

Estes serviços geralmente são explorados pelos ataques de buffer overflow, que são bem sucedidos, pois os programas que implementam as RPCs não fazem a devida verificação de erro. Uma vulnerabilidade do tipo buffer overflow permite que um atacante envie dados pelos quais o programa não está esperando, e como o programa não faz a devida verificação de erro, termina por passar estes dados para o processamento.

U1.5 Como se proteger:

Siga os passos abaixo para proteger seus sistemas de ataques de RPC:

1. Onde for possível, desligue e/ou elimine estes serviços das máquinas diretamente acessíveis via Internet.
2. Onde seja de fato necessário utilizar RPC, instale os patches mais recentes.

Para patches de Solaris:

<http://sunsolve.sun.com/>

Para o IBM AIX:

<http://techsupport.services.ibm.com/support/rs6000.support/downloads>
<http://techsupport.services.ibm.com/rs6k/fixes.html>

Para patches SGI:

<http://support.sgi.com/>

Para patches Compaq (Digital Unix):

<http://www.compaq.com/support>

Para Linux:

<http://www.redhat.com/support/errata/RHSA-2000-039-02.html>

<http://www.debian.org/security/2000/20000719aA>

<http://www.cert.org/advisories/CA-2000-17.html>

3. Consulte regularmente a base de dados de patches do fabricante, buscando por novos patches e instalando-os imediatamente.
4. Bloqueie a porta de RPC (porta 111) no roteador de borda ou no firewall.
5. Bloqueie as portas de "loopback" do RPC: 32770-32789 (TCP e UDP).

Um documento contendo detalhes específicos sobre cada uma das três principais vulnerabilidades no RPC pode ser encontrado em: http://www.cert.org/incident_notes/IN-99-04.html

Os seguintes documentos fornecem informações sobre alguns serviços RPC vulneráveis:

statd: <http://www.cert.org/advisories/CA-99-05-statd-automountd.html>

ToolTalk: <http://www.cert.org/advisories/CA-98.11.tooltalk.html>

Calendar Manager: <http://www.cert.org/advisories/CA-99-08-cmsd.html>

[Back to Top ^](#)

U2 - Vulnerabilidades no Sendmail

U2.1 Descrição:

O Sendmail é o programa que envia, recebe e encaminha a maioria do correio eletrônico processado em computadores UNIX e Linux. O fato de ser amplamente usado na Internet faz com que o Sendmail seja um alvo em potencial para os atacantes. Foram encontradas diversas falhas ao longo dos anos, sendo que o primeiro alerta emitido pelo CERT/CC, em 1988, fez referência justamente a uma falha de segurança no Sendmail.

Um dos ataques mais comuns acontece quando o atacante cria e envia uma mensagem de correio eletrônico, especialmente formatada, para a máquina que está usando Sendmail e este a interpreta como instrução para enviar o arquivo de senhas para a máquina do atacante (ou ainda para outra vítima), onde então as senhas podem ser quebradas.

U2.2 Sistemas Afetados:

A maioria das versões de Unix e Linux.

U2.3 Entradas CVE:

[CVE-1999-0047](#), [CVE-1999-0130](#), [CVE-1999-0131](#), [CVE-1999-0203](#), [CVE-1999-0204](#),
[CVE-1999-0206](#)

U2.4 Como determinar se você está vulnerável:

O Sendmail tem um grande número de vulnerabilidades e deve ser freqüentemente atualizado de acordo com as versões e correções mais recentes. Verifique qual a última versão disponível do Sendmail e quais os patches mais recentes; se o Sendmail que você está utilizando não seguir estes requisitos, então você provavelmente está vulnerável.

U2.5 Como se proteger:

Os passos abaixo devem ser seguidos para proteger o Sendmail:

1. Faça o upgrade para a versão mais recente do Sendmail e/ou aplique os patches recomendados:
<http://www.cert.org/advisories/CA-97.05.sendmail.html>
2. Não execute o Sendmail em modo daemon (desligue o switch -bd) em máquinas que não atuam como servidoras ou relays de correio eletrônico.

[Back to Top ^](#)

U3 - Bind Weaknesses

U3.1 Descrição:

O pacote BIND, Berkeley Internet Name Domain, é a implementação mais usada do Domain Name Service (DNS) - a maneira que nos permite localizar sistemas na Internet através do nome (por exemplo, www.sans.org) sem ter que saber endereços IP específicos -- e isto faz com que ele seja um alvo favorito para ataques. Infelizmente, de acordo com um estudo realizado em meados de 1999, cerca de 50% do total de servidores de DNS conectados à Internet estão executando versões vulneráveis do BIND. O típico exemplo de ataque ao BIND é o caso em que os atacantes apagam os logs do sistema e instalam ferramentas para obter acesso com privilégios de administrador. Feito isto, eles então compilam e instalam programas de IRC e ferramentas para varrer a Internet em busca de redes vulneráveis (network scanners), que foram usadas para varrer mais de uma dúzia de redes classe-B, a procura de outros sistemas com versões vulneráveis do BIND.

Em questão de minutos, estavam usando o sistema comprometido para atacar centenas de sistemas remotos, resultando em várias outras invasões bem sucedidas. Este exemplo ilustra o caos que pode ser gerado por uma única vulnerabilidade de um software como o DNS. Versões velhas do BIND incluem também vulnerabilidades do tipo buffer overflow, que os atacantes podem explorar para obter acesso não autorizado.

U3.2 Sistemas Afetados:

Vários sistemas UNIX e Linux.

U3.3 Entradas CVE:

[CVE-1999-0024](#), [CVE-1999-0184](#), [CVE-1999-0833](#), [CVE-1999-0009](#), [CVE-1999-0835](#),
[CVE-1999-0848](#), [CVE-1999-0849](#), [CVE-1999-0851](#), [CVE-2001-0010](#), [CVE-2001-0011](#),
[CVE-2001-0013](#)

U3.4 Como determinar se você está vulnerável:

Execute uma ferramenta automática de scan de vulnerabilidades (vulnerability scanner) para identificar a versão do BIND ou verifique manualmente os arquivos para ver se estão vulneráveis. Se estiver na dúvida, seja precavido e faça uma atualização do serviço.

U3.5 Como se proteger:

As seguintes providências devem ser tomadas para se defender de ataques contra o BIND:

1. Desligue o daemon do BIND (chamado "named") em todos os sistemas que não são autorizados a atuar como servidores de DNS. Alguns especialistas recomendam remover também o software de DNS.
2. Nas máquinas que são servidores autorizados de DNS, atualize a versão e aplique os patches mais recentes. Siga as orientações contidas nos seguintes alertas:
Para a vulnerabilidades NXT: <http://www.cert.org/advisories/CA-99-14-bind.html>
Para o QINV (Inverse Query) e vulnerabilidades do NAMED: http://www.cert.org/advisories/CA-98.05.bind_problems.html
<http://www.cert.org/summaries/CS-98.04.html>
3. Execute o BIND como um usuário sem privilégios, protegendo assim de eventuais ataques remotos. (No entanto, somente os processos executados como root podem ser configurados para usar portas abaixo de 1024 - um requisito do DNS. Conseqüentemente, você deve configurar o BIND para mudar o user-id após fazer a associação à porta.)
4. Execute o BIND numa estrutura de diretórios chroot() para se proteger de eventuais ataques remotos.
5. Bloqueie a transferência de zonas, exceto de máquinas autorizadas.
6. Desabilite as opções de 'recursion e glue fetching', para se defender de ataques de contaminação do cache do DNS.
7. Configure seu servidor de modo que se esconda a versão do BIND utilizada.

[Back to Top ^](#)

U4 - Comandos remotos (r)

U4.1 Descrição:

As relações de confiança são muito usadas em ambientes UNIX, principalmente na administração de sistemas. Muitas companhias nomeiam um único administrador como responsável por dezenas ou até centenas de sistemas. Os administradores usam freqüentemente as relações de confiança e os comandos UNIX r para trabalhar, acessando vários sistemas, mais confortavelmente. Os comandos r permitem ao usuário acessar um sistema remoto sem a exigência da senha.

Em vez de exigir uma combinação de nome de usuário/senha, a máquina remota autentica qualquer usuário que tente acessá-la através de endereços IP confiáveis. Se um atacante conseguir controlar qualquer máquina de uma rede confiável, poderá assim ter acesso as demais máquinas que confiam na máquina comprometida. Os seguintes comandos r são usados com freqüência:

1. rlogin - remote login
2. rsh - remote shell
3. rcp - remote copy

U4.2 Sistemas Afetados:

A maioria dos sistemas Unix, inclusive o Linux.

U4.3 Entradas CVE:

[CVE-1999-0046](#), [CVE-1999-0113](#), [CVE-1999-0185](#), [CAN-1999-0651](#)

U4.4 Como determinar se você está vulnerável:

As relações de confiança são estabelecidas através da configuração de dois arquivos: /etc/hosts.equiv ou ~/.rhosts. Verifique estes arquivos em seus sistemas Unix, para determinar se existem relações de confiança configuradas.

U4.5 Como se proteger:

Não permita relações de confiança baseadas em endereços IP e não use os comandos r. A autenticação baseada em endereços IP é muito fácil de ser burlada. A autenticação deve ser baseada em mecanismos mais seguros, tais como o 'token' ou pelo menos, em senhas. Se os comandos r forem necessários, limite o acesso e controle o perímetro da rede com muito cuidado. Nunca permita o arquivo "rhosts" na conta do usuário "root". Você pode usar o comando "find" do Unix para frequentemente procurar por arquivos "rhosts" que possam ter sido criados nas contas dos usuários.

[Back to Top ^](#)

U5 - LPD (daemon do serviço de impressão remota)

U5.1 Descrição:

Em ambientes Unix, o in.lpd permite aos usuários interagir com a impressora local. O LPD aguarda requisições através da porta 515 TCP. Os programadores que desenvolveram o código responsável por transferir trabalhos para impressão de uma máquina para outra, cometeram um erro que originou uma vulnerabilidade de buffer overflow. Se o daemon receber muitos trabalhos para impressão dentro de um curto intervalo de tempo, ele deixará de funcionar ou processará código arbitrário com privilégios elevados.

U5.2 Sistemas Afetados:

The following systems are impacted:

- Solaris 2.6 para SPARC
- Solaris 2.6 x86
- Solaris 7 para SPARC
- Solaris 7 x86
- Solaris 8 para SPARC
- Solaris 8 x86
- A maioria dos sistemas Linux

U5.3 Entradas CVE:

[CVE-1999-0032](#), [CVE-1999-0299](#), [CVE-2000-0917](#), [CAN-2001-0670](#), [CAN-2001-0668](#), [CAN-2001-0353](#), [CAN-1999-0061](#)

U5.4 Como determinar se você está vulnerável:

Utilize uma ferramenta de scan de vulnerabilidades (vulnerability scanner) no seu sistema ou ainda verifique-o manualmente. A maneira mais fácil de fazer a checagem manual é ver se seu sistema está executando o LPD e verificar qual versão está sendo usada. Se você estiver executando uma das versões vulneráveis do

software, sem aplicar os patches recomendados, então você está vulnerável.

U5.5 Como se proteger:

A Sun Microsystems divulgou um boletim de segurança, o Sun Security Bulletin #00206, tratando desta vulnerabilidade, no dia 30 de Agosto de 2001. Tal boletim contém as informações sobre os patches necessários e está disponível em: <http://sunsolve.sun.com/security>

O alerta do CERT correspondente a esta vulnerabilidade pode ser encontrado em: <http://www.cert.org/advisories/CA-2001-15.html>

O patch para Linux pode ser obtido em: <http://redhat.com/support/errata/RHSA-2001-077.html>

Outras opções para se defender dos ataques que exploram esta vulnerabilidade incluem:

1. Desabilitar o serviço de impressão remota no arquivo /etc/inetd.conf, caso seja desnecessário o uso deste serviço.
2. Habilite o 'noexec_user_stack', que é ajustado através da inclusão das seguintes linhas no arquivo /etc/system e reiniciando a máquina (reboot):
 - set noexec_user_stack = 1
 - set noexec_user_stack_log = 1
3. Bloqueie o acesso à porta 515/tcp
4. Utilize o [tcpwrappers](#), que faz parte do pacote tcpd-7.6 e está disponível em: <http://www.sun.com/solaris/freeware.html#cd>

[Back to Top ^](#)

U6 - Serviços sadmind e mountd

U6.1 Descrição:

O Sadmin permite a administração remota de sistemas Solaris, através de uma interface gráfica que disponibiliza funções de administração do sistema. O Mountd controla o acesso aos arquivos mapeados pelo NFS em hosts UNIX. As falhas de buffer overflows existentes nestes aplicativos, originados por erros de programação, podem ser explorados, permitindo aos atacantes obter o controle do sistema com privilégios de "root".

Nota: Esta vulnerabilidade é um caso especial de buffer overflow, tratado no item U.1. Buffer Overflows em serviços RPC. Os colaboradores desta lista detectaram a ocorrência tão freqüente deste caso especial, que decidiram criar um segundo item dedicado exclusivamente a ele.

U6.2 Sistemas Afetados:

Várias versões Unix.

U6.3 Entradas CVE:

[CVE-1999-0977](#), [CVE-1999-0002](#), [CVE-1999-0493](#), [CVE-1999-0210](#)

U6.4 Como determinar se você está vulnerável:

Use um scan de vulnerabilidades (vulnerability scanner) para verificar se estes serviços estão sendo executados e se estão vulneráveis ao ataque.

U6.5 Como se proteger:

As seguintes ações protegem seus sistemas das vulnerabilidades do NFS, incluindo do sadmind e do mountd:

1. Onde for possível, desligue e/ou remova o sadmind e o mountd das máquinas diretamente acessíveis via Internet.

2. Instale os patches mais recentes:

Para patches de Solaris, consulte:

Para patches de Solaris, consulte:

<http://sunsolve.sun.com/>

Para o IBM AIX, consulte:

<http://techsupport.services.ibm.com/support/rs6000.support/downloads>

<http://techsupport.services.ibm.com/rs6k/fixes.html>

Para patches do Software SGI:

<http://support.sgi.com/>

Para patches de Compaq (Digital Unix):

<http://www.compaq.com/support>

3. Configure listas de exportação baseadas no host/ip.

4. Configure seus sistemas de arquivo exportados como "read-only", e se possível sem acesso a suid.

5. Use o nfsbug para fazer a varredura em busca de vulnerabilidades de NFS.

Informações adicionais podem ser encontradas em:

<http://www.cert.org/advisories/CA-99-16-sadmind.html>

<http://www.cert.org/advisories/CA-98.12.mountd.html>

[Back to Top ^](#)

U7 - Mensagens-padrão do SNMP - Simple Network Management Protocol

U7.1 Descrição:

O protocolo SNMP (Simple Network Management Protocol) é muito usado pelos administradores de rede para monitorar e administrar todos os tipos de equipamentos conectados à rede, desde roteadores e impressoras, até servidores e estações de trabalho. O SNMP usa uma "community string" sem criptografia, como seu único mecanismo de autenticação. A falta de criptografia por si só já é um fato ruim, além disto, a community string definida como padrão e usada por grande parte dos equipamentos SNMP é "public", sendo que somente alguns dos fabricantes de equipamentos de rede "mais espertos" alteram a community para "private", quando se trata de informações mais sensíveis. Os atacantes podem usar esta vulnerabilidade no SNMP para

reconfigurar ou desligar remotamente os equipamentos. O tráfego SNMP, quando interceptado ("sniffed"), pode revelar muitas informações sobre a estrutura de sua rede, bem como dos sistemas e os equipamentos conectados a ela. Os invasores usam tais informações para escolher alvos e planejar os ataques.

Nota: O SNMP não é parte integrante apenas dos sistemas Unix. No entanto, ele está listado junto com as vulnerabilidades Unix, pois os colaboradores desta lista notaram um grande número de ataques a sistemas Unix, explorando a configuração imprópria do SNMP, enquanto que este não parece ser um problema muito explorado em ambientes Windows.

U7.2 Sistemas Afetados:

Todos os sistemas UNIX e equipamentos de rede.

U7.3 Entradas CVE:

[CAN-1999-0517](#), [CAN-1999-0516](#), [CAN-1999-0254](#), [CAN-1999-0186](#)

U7.4 Como determinar se você está vulnerável:

Verifique se você está executando o SNMP em seus equipamentos de rede e computadores. Se estiver, verifique os arquivos de configuração, em busca das vulnerabilidades mais comuns:

- Community name SNMP padrão ou não definida.
- Community name SNMP triviais.

U7.5 Como se proteger:

Os seguintes passos o ajudarão a se defender contra os ataques ao SNMP:

1. Se você não precisar de fato do SNMP, desligue o serviço.
2. Se você realmente precisar usar o SNMP, então use para as community names a mesma política definida para senhas. Certifique-se que as communities não sejam triviais ou fáceis de quebrar, e que são modificadas periodicamente.
3. Valide e verifique as community names usando a ferramenta snmpwalk. Informações adicionais podem ser encontradas em: <http://www.zend.com/manual/function.snmpwalk.php>
4. Bloqueie o SNMP (porta 161/UDP) no roteador de borda ou no firewall, a menos que seja absolutamente necessário gerenciar equipamentos de fora da rede local.
5. Sempre que possível, defina as MIBs como "read only".
Informações adicionais podem ser encontradas em:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#xtocid210315

[Back to Top ^](#)

Apêndice A: Portas Vulneráveis Mais Comuns

Nesta seção, listamos as portas que são freqüentemente sondadas e atacadas. Bloquear tais portas é uma exigência mínima para a segurança do perímetro de sua rede, não sendo uma lista detalhada para a configuração de um firewall. A regra mais adequada seria bloquear todas as portas que não estão sendo usadas. E mesmo que você saiba que estas portas estejam bloqueadas, ainda assim você deve monitorá-las ativamente para detectar tentativas de invasão. Em tempo, um aviso importante: bloquear algumas das portas da lista a seguir, pode desabilitar serviços necessários. Por favor, considere os efeitos colaterais destas recomendações antes de implementá-las.

Tenha em mente que bloquear estas portas não substitui uma solução detalhada de segurança. Ainda que as portas tenham sido bloqueadas, um atacante que já obteve acesso à sua rede através de outro meio (por exemplo, por um modem, um Trojan embutido em uma mensagem de E-mail, ou uma pessoa que é funcionário da organização) pode explorar tais portas, caso elas não tenham sido devidamente configuradas em todas as máquinas de sua organização.

1. Serviços de login -- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin etc (512/tcp até 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 em Windows NT -- 135 (tcp e udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 - as mesmas portas do NT e a 445(tcp and udp)
4. X Windows -- 6000/tcp até 6255/tcp
5. Serviços de nomes -- DNS (53/udp) para todas as máquinas que não são servidoras de DNS, DNS zone transfers (53/tcp) exceto de fontes secundarias externas, LDAP (389/tcp e 389/udp).
6. Correio (Mail)-- SMTP (25/tcp) para todas as máquinas que não são relay de correio externos, POP (109/tcp e 110/tcp), e IMAP (143/tcp)
7. Web -- HTTP (80/tcp) e SSL (443/tcp) exceto para servidores Web externos, e talvez bloquear o acesso a portas altas que também são usadas pelo HTTP (8000/tcp, 8080/tcp, 8888/tcp, etc.).
8. "Small Services" -- portas abaixo de 20/tcp e 20/udp, e horário (time) (37/tcp and 37/udp)
9. Miscelânea -- 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 - bloquear o recebimento de 'echo request'(ping e traceroute Windows) vindo de fontes externas, bloquer 'echo replies' saindo de sua rede (outbound), as mensagens de 'time exceeded' e 'destination unreachable' exceto mensagens de "packet too big" (type 3, code 4). (Este item assume que você está disposto a sacrificar o uso legítimo do ICMP echo request ('ping') para poder bloquear algumas formas maliciosas de uso do protocolo).

Além destas portas, bloqueie pacotes com endereços forjados ("spoofed") - basicamente, pacotes que chegam de fora de sua companhia e tem como endereço de origem aparente algum endereço de sua rede local, endereços reservados (RFC1918 e rede 127.) ou endereços reservados pelo IANA. Também bloqueie pacotes nos quais as opções 'source routing' ou 'IP options' estejam ativadas

Apêndice B. Os Especialistas que Ajudaram a Criar as Listas das Dez e Vinte Vulnerabilidades Mais Comuns na Internet (conhecidas respectivamente como "Top 10" e "Top 20").

Phil Benchoff, Virginia Tech CIRT
Tina Bird, Counterpane Internet Security Inc.
Matt Bishop, University of California Davis
Chris Brenton, Dartmouth Inst. for Security Studies
Lee Brotzman, NASIRC Allied Technology Group Inc.
Steve Christey, MITRE
Rob Clyde, Symantec
Eric Cole, SANS Institute
Scott Conti, University of Massachusetts
Kelly Cooper, Genuity
Igor Gashinsky, NetSec Inc.
Bill Hancock, Exodus Communications
Shawn Hernan, CERT Coordination Center
Bill Hill, MITRE
Ron Jarrell, Virginia Tech CIRT
Christopher Klaus, Internet Security Systems

Ron Nguyen, Ernst & Young
David Nolan, Arch Paging
Stephen Northcutt, SANS Institute
Alan Paller, SANS Institute
Ross Patel, ViaCode Ltd and Afentis Security Team
Hal Pomeranz, Deer Run Associates
Chris Prorise, 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
Bruce Schneier, Counterpane Internet Security Inc.

Valdis Kletnieks, Virginia Tech CIRT
Clint Kreitner, Center for Internet Security
Jimmy Kuo, Network Associates Inc.
Scott Lawler, Veridian
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

Gene Schultz, Lawrence Berkeley Laboratory
Greg Shipley, Neohapsis
Derek Simmel, Carnegie Mellon University
Ed Skoudis, Predictive Systems
Gene Spafford, Purdue University CERIAS
Lance Spitzner, Sun Microsystems, GESS Team
Wayne Stenson, Honeywell
Jeff Stutzman
Frank Swift
Bob Todd, Advanced Research Corporation
Jeff Tricoli, FBI NIPC
Viriya Upatising, Loxley Information Services Co.
Laurie Zirkle, Virginia Tech CIRT

[Back to Top ^](#)

Apêndice C. A tradução em Português foi feita por:

[Mike Poor](#) - Compugenx, LLC

CAIS - Centro de Atendimento a Incidentes de Segurança (ou Security Incidents Response Center)
RNP - Rede Nacional de Pesquisa (ou Brazilian Research Network)

[Alexandre da Costa Medeiros](mailto:alexcm@cais.rnp.br) <alexcm@cais.rnp.br>
[Jacomo Dimmit Boca Piccolini](mailto:jacomo@cais.rnp.br) <jacomo@cais.rnp.br>
[Liliana E. Velasquez Alegre Solha](mailto:nina@cais.rnp.br) <nina@cais.rnp.br>
[Renata Cicilini Teixeira](mailto:renata@cais.rnp.br) <renata@cais.rnp.br>

[Back to Top ^](#)