

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Segurança em Redes

Conceitos Básicos

Romulo Moacyr Cholewa
S73417HN37@hotmail.com – <http://www.rmc.eti.br>

09/2001

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Conteúdo.

1. Distribuição / Cópia
2. Apresentação
 - 2.1. Filosofia
 - 2.2. Opinião
 - 2.3. Ponto de vista sobre Hackers
 - 2.3.1. White-hats
 - 2.3.2. Black-hats
 - 2.3.3. Defacers
 - 2.3.4. Crackers
 - 2.3.5. Phreakers
 - 2.3.6. Wannabes / Script Kiddies
 - 2.3.7. Exemplo: Estudo de Caso: “TakeDown”
 - 2.3.8. Exemplo: ISP, Portal, Instituição Financeira
 - 2.3.9. Exemplo: Operadora de Telefonia Celular
 - 2.4. Canais de Divulgação
3. Entendendo Redes e a Internet
 - Introdução a Redes
 - 3.1. Conceito de Redes
 - 3.1.1. Interfaces de Rede
 - 3.1.2. Transmissão de Dados – Camada Física
 - 3.1.3. Transmissão de Dados – Camada de Rede
 - 3.1.4. Transmissão de Dados – Camada de Transporte
 - 3.1.5. Transmissão de Dados – Camada de Aplicação
 - 3.2. A Conexão a uma Rede
 - 3.3. Interligando Redes
 - 3.4. TCP/IP
 - 3.4.1. ARP (Address Resolution Protocol)
 - 3.4.2. IP (Internet Protocol)
 - 3.4.3. ICMP (Internet Control Message Protocol)
 - 3.4.4. TCP (Transmission Control Protocol)
 - 3.4.5. UDP (User Datagram Protocol)
 - 3.5. Protocolos de Aplicação
 - 3.5.1 DNS (Domain Name System)
 - 3.6. Sockets (Soquetes de Comunicação)
 - 3.7. Gerenciando Erros de Comunicação
 - 3.7.1. PING (Packet Internet Grouper)
 - 3.7.2. TRACERT (traceroute)
 - 3.8. ... Então, O que é a Internet
4. Entendendo a Invasão
 - 4.1. O porque da Invasão
 - 4.1.1. Ponto de Vista do white-hat
 - 4.1.2. Ponto de Vista do Black-hat
 - 4.2. vulnerabilidades no meu sistema
 - 4.2.1. Que Componentes são Vulneráveis
 - 4.2.1.1. Sistema Operacional
 - 4.2.1.2. Instant Messaging
 - 4.2.1.3. Correio Eletrônico
 - 4.2.1.4. Gerência Remota
 - 4.2.1.5. Programas Diversos
5. Técnicas de Invasão
 - 5.1. Brechas de Configuração

- 5.2. Trojan Horses e Back Doors
- 5.3. Buffer Overflow
- 5.4. Password Crackers
- 5.5. Exploits
- 5.6. Man-in-the-Middle
- 6 Outros Tipos de Ataques
 - 6.1. DoS (Denial of Service Attack)
 - 6.2. DDoS (Distributed Denial of Service Attack)
 - 7.2.1. trin00, TFN, TFN2K, Schafit
 - 7.2.2. CodeRed 1, CodeRed 2, Nimda (Code Rainbow)
 - 6.3. IP Spoofing
 - 6.4. DNS (Name Server) Spoofing / Poisoning
- 7. Ferramentas
 - 7.1. Obtendo Informações
 - 7.1.1. Portscanning
 - 7.1.2. Services fingerprinting
 - 7.1.3. Sniffing
 - 7.2. Automatização do Estudo de vulnerabilidades Conhecidas
 - 7.3. Personal Firewalls
 - 7.3.1. Introdução ao Conceito de Filtragem de Pacotes
 - 7.3.2. ZoneAlarm
 - 7.3.3. TPF – Tiny Personal Firewall
 - 7.4. Antivírus
- 8 Seu computador foi invadido ?
 - 8.1. O que fazer?
 - 8.2. Precauções
 - 8.3. Análise Forense
 - 8.4. Onde obter mais informações
- 9. Comércio Eletrônico
 - 9.1. Análise de vulnerabilidades
 - 9.2. O Quê Pode dar Errado
- 10 Como Prevenir
 - 10.1. Como configurar Corretamente o meu Acesso
 - 10.2. Informação é o melhor Remédio ? (“Full Disclosure”)
 - 10.3. A Informação Moderada é o melhor Remédio ?
 - 10.4. Firewall (Incluindo Personal Firewalls)
 - 10.5. IDS (Intrusion Detection Systems)

1. Distribuição / Cópia

A partir da presente data (30/04/2002), o autor deste material, **Rômulo M. Cholewa**, torna-o público e notório, autorizando aos interessados a copiá-lo, imprimi-lo e distribuí-lo livremente, desde que todo o seu conteúdo seja necessariamente preservado, isto é, que o mesmo permaneça na íntegra e sem quaisquer alterações. Ressalte-se, ainda, que no ato da divulgação do mencionado material, independentemente da sua natureza ou intenção, este deverá ser referenciado e vinculado à autoria de **Rômulo M. Cholewa**.

Outrossim, o autor informa e adverte, sob o amparo legal da Lei dos Direitos Autorais (**LEI n.º 9.610/98**), que está terminantemente proibida a publicação e/ou utilização de seu material para fins de natureza lucrativa ou remunerada, quer esta seja direta quer mesmo indireta.

Este material é livre, e deve permanecer assim. O foco deste material não é o profissional de segurança da informação. A intenção é orientar de forma básica as pessoas que não possuem conhecimento específico no assunto, e que mais e mais procuram a Internet como meio de comunicação.

Todos os nomes registrados são propriedade de seus respectivos donos. As imagens de programas e processos registrados contidos neste material também são devidamente creditadas, como observado, e são usadas neste material apenas para fins ilustrativos e educacionais.

2. Apresentação

O Objetivo é levar a todos o conhecimento sobre invasões de computadores, desde o motivo até a sua solução, passando por vulnerabilidades e como torná-las sem efeito. Inclui também conceitos básicos de rede e de comunicação de dados, que são essenciais a completa compreensão do assunto, assim como outros conceitos, incluindo funcionamento básico de ferramentas usadas para obter informações de computadores em rede, bem como regras de filtragem de pacotes, usadas em firewalls.

O Material

Ao longo do material serão apresentadas informações sobre hackers, como agem e o que querem, como se proteger e como detectar um invasor. Serão mostrados alguns fatos acontecidos no mundo da segurança, algumas histórias de hackers famosos, bem como algumas histórias dos bastidores.

Opinião

Sobre os Hackers

"Conheça seu inimigo como a si próprio, e elabore sua estratégia de defesa e ataque baseadas em suas vulnerabilidades."

O perfil típico do hacker é: jovem entre 15 ~ 25 anos, com amplo conhecimento de programação (geralmente em linguagens como C, C++, Java e Assembler), e noções de redes e Internet. O mais interessante é que no Brasil, a grande maioria dos “hackers” começa cedo, algumas vezes com 12 anos, em conhecimentos de programação nas linguagens citadas acima. Muitos destes se esquecem da importância do funcionamento da Internet e de redes em si, o que, de certa forma, é algo bom. A atuação e força de tais “hackers” seriam bem mais poderosas caso aliassem o conhecimento em redes e Internet ao conhecimento em linguagens de programação.

As afirmações acima nos levam a uma conclusão: a grande maioria dos hackers entre 12 ~ 25 anos não desenvolve vulnerabilidades, apenas copiam vulnerabilidades publicadas em sites especializados, e fazem uso destas em massa, antes que qualquer tentativa de correção destas vulnerabilidades seja humanamente possível ou viável.

Notadamente, devemos deixar claro que muitos “hackers” trabalham verdadeiramente empenhados em descobrir falhas e ajudar os usuários de tecnologia a se protegerem. O termo “hacker” tem sido muito usado ultimamente, mas com uma conotação não muito acertada. Muitas vezes, o termo tem sido associado a reportagens e publicações que distorcem o seu verdadeiro sentido.

De qualquer forma, a maioria das empresas desenvolvedoras de software (principalmente sistemas operacionais ou software com aplicações específicas em redes ou segurança), publicam correções no período de 24 a 48 horas após a divulgação de uma vulnerabilidade na Internet (vide “Canais de Divulgação”, a seguir). Isto só ocorre hoje por causa da pressão natural do mercado em exigir uma resposta, diante da publicação de uma falha. Devemos então, agradecer, diretamente, aos especialistas em segurança, e aos verdadeiros “hackers” por permitir que tal processo funcione.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Existem diversos tipos de “hackers”, dos que possuem mais experiência para os que apenas “copiam” furos de segurança explorados por outros hackers. Podemos classificá-los quanto a sua experiência, conhecimento, e “ramo” de atuação, sendo este último parâmetro o mais usado.

White-Hats

Os white-hats são os hackers que exploram problemas de segurança para divulgá-los abertamente, de forma que toda a comunidade tenha acesso à informações sobre como se proteger. Desejam abolir a “segurança por obscuridade”, que nada mais é do que tentar proteger ou manter a segurança pelo segredo de informações sobre o funcionamento de uma rede, sistema operacional ou programa em geral. Seu lema é o “full disclosure”, ou conhecimento aberto, acessível a todos. Alguns adotam também a filosofia de “moderated disclosure”, ou conhecimento moderado, liberando informações sobre como funciona um bug ou vulnerabilidade, mas sem liberar, na maioria das vezes, o que chamamos de “exploit”, ou código que permite explorar a vulnerabilidade.

Black-Hats

Ao contrário dos white-hats, apesar de movidos também pela curiosidade, usam suas descobertas e habilidades em favor próprio, em esquemas de extorsão, chantagem de algum tipo, ou qualquer esquema que venha a trazer algum benefício, geralmente, e obviamente, ilícito. Estes são extremamente perigosos e difíceis de identificar, pois nunca tentarão chamar a atenção. Agem da forma mais furtiva possível.

Defacers

Os defacers, na grande maioria das vezes, são organizados em grupos. São, geralmente, muito jovens, algumas vezes começando com apenas 12 anos. Usam seus conhecimentos para invadir servidores que possuam páginas web, e tem por objetivo modificar estas páginas.

Obviamente, mudar a página principal de um site famoso ou não dá uma certa quantidade de “exposição”, tornando o “hacker”, ou o grupo, conhecido na comunidade. Muitos analistas sugerem que a grande motivação destes grupos seja justamente se tornarem conhecidos na comunidade, e de certa forma, “provarem” que são capazes. Muitas vezes ocorrem disputas entre grupos de defacers, para descobrirem quem consegue desfigurar o maior número de sites no menor tempo. Apesar da maioria esmagadora dos defacers negar, eles são, por amostragem, “pixadores” digitais.

Geralmente não criam ou descobrem novas vulnerabilidades. Apenas usam o que já foi descoberto recentemente, se aproveitando do atraso entre a publicação de uma falha e a publicação / aplicação de correções.

Existem inúmeros grupos de defacers Brasileiros, e muitos deles são considerados os “mais eficazes e rápidos” do mundo. Frequentemente, utilizam o IRC (Internet Relay Chat – ou bate-papo online).

Estatísticas de sites como o Alldas.org demonstram que o Brasil, hoje, resguardando as devidas proporções, é um dos Países do mundo que mais sofre com defacements. Isso está diretamente relacionado com a “qualidade” e nível técnico dos “hackers” em nosso País.

Crackers

As denominações para os crackers são muitas. Alguns classificam de crackers, aqueles que tem por objetivo invadir sistemas em rede ou computadores apenas pelo desafio. Contudo, historicamente, o nome “cracker” tem uma relação com a modificação de código, para obter funcionalidades que não existem, ou de certa forma, limitadas. Um exemplo clássico são os diversos grupos existentes na Internet que tem por

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

finalidade criar “patches” ou mesmo “cracks” que modificam programas comerciais (limitados por mecanismos de tempo por exemplo, como shareware), permitindo seu uso irrestrito, sem limitação alguma.

Phreakers

Apesar de muitos considerarem um cientista russo chamado Nicola Tesla (que na virada do século realizava experiências assustadoras – até para os dias de hoje – com eletricidade) como o primeiro hacker da história, os primeiros hackers da era digital (ou seria analógica?) lidavam com telefonia. Sua especialidade é interferir com o curso normal de funcionamento das centrais telefônicas, mudar rotas, números, realizar chamadas sem tarifação, bem como realizar chamadas sem serem detectados (origem). Com a informatização das centrais telefônicas, ficou inclusive mais fácil e acessível o comprometimento de tais informações. Kevin Mitnick, considerado o maior hacker de todos os tempos (veremos que nem tanto – a mídia exerceu uma influência decisiva), era um ótimo phreaker. Na fase final de sua captura, quando os agentes de governo ajudados pelo Sr. Tsutomu Shimomura, especialista de segurança do SDSC – San Diego Supercomputing Center, estavam chegando a um nome, ele conseguia enganar as investigações através do controle que tinha da rede de telefonia da GTE (uma das concessionárias telefônicas nos EUA).

Wannabes

Os wannabes ou script-kiddies são aqueles que acham que sabem, dizem para todos que sabem, se anunciam, ou divulgam abertamente suas “façanhas”, e usam em 99% dos casos scripts ou exploits conhecidos, já divulgados, denominados “receitas de bolo”, facilmente encontradas em sites como “www.rootshell.com”, “xforce.iss.net” ou “securiteam.com”. Estes possuem relação direta com a maioria dos usuários da Internet Brasileira. São facilmente encontrados em fóruns de discussão sobre o tema, e principalmente no IRC. A maioria não possui escrúpulo algum, portanto, tomar medidas de cautela é aconselhável. Os wannabes geralmente atacam sem uma razão ou objetivo, apenas para testar ou treinar suas descobertas, o que nos torna, usuários Internet, potenciais alvos.

Exemplo / Estudo de Caso: “TakeDown”

Para entender melhor o que pensa um típico black-hat, um phreaker, e um white-hat, analisemos o caso de Kevin Mitnick e Tsutomu Shimomura.

Kevin Mitnick a um bom tempo (meados dos anos 80) já havia sido investigado pela polícia, por atividades ilícitas ligadas a segurança de computadores, sempre relacionadas a sua atuação como hacker. Por volta de 1992 ~ 1994, Tsutomu Shimomura, e outro hacker conhecido, chamado Mark Lotto, desmontaram o código do sistema operacional de um celular da OKI, através de engenharia reversa. Tsutomu em si trabalhava como consultor para a Motorola. Ninguém sabe ao certo o que fez o Kevin tentar invadir as máquinas de Tsutomu, contudo, a comunidade tem uma certeza: não foi um ataque simples, foi algo planejado. Tudo indica que o objetivo de Kevin era conseguir obter os códigos fonte dos celulares que Tsutomu possuía, para posteriormente vendê-los.

Tudo começou quando ele conseguiu controlar as centrais telefônicas da GTE. Kevin discava de um celular, e raramente de casa, de uma cidade chamada Raleigh, na Carolina do Norte, USA. Assim, invadiu as máquinas de um provedor chamado The Well, que usava para ter acesso a Internet. Ele usou como ponto de partida os servidores do “The Well” para o ataque. Também comprometeu estações e servidores no provedor “Toad.com”. Perceba que, tanto o “The Well” como o “Toad.com” são considerados os pilares da comunidade da Internet que conhecemos hoje.

Enquanto isso aproveitou seu acesso “invisível” através do “The Well” para invadir um outro provedor, chamado NetCom, de onde roubou milhares de números de cartões de crédito. Após o roubo dos números, invadiu uma máquina em toad.com. De lá, iniciou o ataque à rede de Tsutomu Shimomura. Através de um

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

antigo exploit do finger, e usando um pouco de port scanning, ele conseguiu descobrir que uma máquina de Tsutomu, chamada Ariel, tinha uma relação de confiança com outra máquina na rede de Tsutomu. Ele tirou esta máquina do ar (através de um ataque do tipo DoS), e utilizou uma técnica chamada IP Spoofing, para a máquina Ariel “pensar” que estava sendo acessada pela máquina na qual confiava. Daí pra frente, ficou fácil. Observe que Kevin usou de uma série de artifícios para não ser detectado, desde a sua ligação telefônica até seu acesso aos computadores de Tsutomu, e que sua motivação também era financeira. Inclusive, muitos dos métodos usados por ele são amplamente divulgados hoje em dia.

Tsutomu conseguiu chegar a Kevin devido a um rastro deixado em Ariel. Descobriu então, que as conexões tinham partido de toad.com. Assim, iniciou uma caçada, que vários meses depois, chegou em Raleigh, e culminou com a captura do Kevin (com ajuda do FBI) em fevereiro de 1995, através do sinal de seu celular, que usava para se conectar.

O mais interessante de tudo é que Kevin não era especialista em UNIX (sistema usado por Tsutomu, pelo toad.com, pela Well). Ele era na verdade especialista em VMS / VAX, um sistema da Digital. Ele parecia ter profundos conhecimentos sobre sistemas da Digital. Tudo indica que Kevin seguiu várias dicas de alguém em Israel, que até hoje, ninguém conseguiu identificar. Kevin forneceu várias informações sobre como invadir sistemas VMS / VAX, e recebeu as dicas de como usar o IP spoofing, que, na época, era uma técnica recente, nunca testada, apenas discutida academicamente.

Existe um site na Internet que possui um log demonstrando até a sessão de telnet que Kevin usou, algumas chamadas que ele teria realizado para o Mark Lotto, demonstrando seu interesse pelo código fonte dos celulares, e algumas gravações da secretária telefônica do Tsutomu, que supostamente, teriam sido feitas pelo Kevin. O site pode ser acessado em: <http://www.takedown.com>

Existem também dois livros que contam a história. Um, com a visão de Kevin, escrito pelo Jonattan Littman, e outro, com a visão de Tsutomu, escrito pelo John Markoff em conjunto com ele. Este último possui uma edição nacional, pela Companhia das Letras. Chama-se “Contra-Ataque”. O livro escrito pelo Littman chama-se “The Fugitive Game: online with Kevin Mitnick”. Ambos os livros podem ser encontrados online, em livrarias como Amazon.com, por menos de 20 dólares cada.

Kevin Mitnick foi solto em 21 de janeiro de 2000, e está sobre condicional. Boatos dizem que o governo Americano está usando Kevin Mitnick como consultor de segurança.

Ninguém sabe o paradeiro de Tsutomu Shimomura.

Exemplo: ISP, Portal, Instituição Financeira

Em meados de 1998, um provedor de acesso a Internet no Nordeste, um dos maiores do Brasil, é hackeado 2 vezes.

Apesar das portas de entrada usadas não terem sido 100% identificadas, ambas invasões foram usadas para, de certa forma, prejudicar sua imagem perante seus usuários.

No primeiro ataque, a página principal foi modificada (deface), e substituída por uma “brincadeira” com a mascote do provedor, que incluía até uma pequena música que tratava dos preços praticados pelo mesmo, e de sua segurança falha.

No segundo ataque, a coisa se tornou um pouco mais séria. Os hackers colocaram na página principal do provedor informações de cadastro, como número de cartões de crédito de usuários. Apesar dos hackers apenas conseguirem acesso a poucas informações (cadastro de novos usuários realizados no período de 24 horas), colocaram no texto da nova página que, supostamente, teriam acesso a todo o banco de dados de todos os usuários. O impacto na mídia local foi devastador.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Em ambos os casos, os hackers que tiveram sucesso em invadir um dos servidores do provedor modificaram as páginas principais do mesmo, fazendo com que, qualquer usuário ou pessoa com acesso a Internet, pudesse visualizar o resultado do ataque.

Este tipo de ação é mais conhecido na Internet como “deface”, ou ataque de desfiguração de site. O objetivo é alterar de alguma forma a página principal da empresa, por se tratar de uma invasão relativamente simples (o comprometimento de apenas um servidor), mas com resultados sérios.

Dependendo do ramo de atuação da empresa que tem seu site desfigurado, as implicações podem ser profundas. No caso de provedores de acesso a Internet, entidades financeiras (como bancos, por exemplo), portais e empresas de segurança, a página principal modificada indica à comunidade em geral que a instituição é falha em manter a integridade de seus dados, e, obviamente, a segurança dos mesmos. O impacto é direto no produto que estas empresas comercializam.

Provedores de acesso a Internet terão sua credibilidade afetada, de forma que novos clientes optarão por outros provedores justamente por não confiarem na segurança de seus dados.

Entidades financeiras talvez sejam as empresas mais afetadas. A segurança da informação nestas entidades é primordial, e o comprometimento da sua segurança demonstrará a comunidade que tal instituição não possui capacidade para manter seus dados seguros. No caso do provedor de acesso a Internet, a perda de clientes significará uma perda direta de faturamento, mas na ordem de poucas dezenas de dólares por cliente. No caso de uma instituição financeira, a perda poderá significar potencialmente a descapitalização da instituição, ou uma perda da ordem de milhares de dólares por cliente.

No caso de empresas de segurança, a perda na prática será a descrença em seus serviços, diretamente. O mais interessante é que uma empresa de segurança provavelmente terceiriza serviços como hospedagem de páginas, o que lhe isenta da responsabilidade em um caso desses. Contudo, o efeito causado geralmente não consegue ser justificado. Quando isso ocorre, e, se realmente a empresa terceiriza seus serviços de web hosting, deve colocar em seu site um aviso para seus clientes e usuários sobre onde ocorreram as falhas, e um resumo de responsabilidades.

Exemplo: Operadora de Telefonia Celular

No final do primeiro semestre de 2001, uma operadora de telefonia celular, no Brasil, teve um de seus servidores Windows NT hackeados.

O servidor em questão era responsável pelo envio de mensagens do tipo SMS (Short Messaging System). Ao acessar a página, o usuário recebia uma página relatando o ocorrido, escrito pelo hacker. Mais um caso de defacement.

Em resumo, uma constante em casos de “defacements” é a quebra da credibilidade da empresa afetada.

Canais de Divulgação

A Internet em si é a melhor forma de se manter atualizado sobre novas vulnerabilidades, ferramentas, bugs, patches e atualizações, bem como sites hackeados, ou “defacements”.

Perceba que muitos destes canais de comunicação são os mesmos usados pelos maiores especialistas de segurança da atualidade. Portanto, não é difícil ver uma nova vulnerabilidade ser anunciada, e o próprio fabricante ou desenvolvedor do software tomar conhecimento da mesma pelo mesmo canal. Em listas como a bugtraq, e a ntbugtraq, é comum isto ocorrer.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Isso é considerado uma grande vantagem, pois quanto mais cedo ou mais rápido se toma providências contra uma falha de segurança, menor são as chances de ter problemas com hackers. A desvantagem é, na maioria das vezes, não ter correções disponíveis quando a vulnerabilidade é publicada.

Contudo, prepare-se para receber em média 400 mensagens diárias sobre o tema. Tal fluxo de mensagens somente é “aceitável” para aquele profissional que lida com segurança da informação em sua empresa, ou tem responsabilidades desta natureza.

Microsoft Security Site & Bulletins

A Microsoft mantém um site dedicado a questões de segurança em todos os seus produtos. Lá, você poderá fazer o download de correções / patches para qualquer software que a Microsoft produza e possua uma falha corrigida.

O site pode ser acessado em:

<http://www.microsoft.com/security>

A estrutura do site é organizada em boletins. Cada falha de segurança é publicada oficialmente através de um boletim, enviado a uma lista de assinantes, e publicado no site. Cada boletim possui todas as informações pertinentes à falha, bem como instruções sobre como se proteger.

Para fazer parte da lista de assinantes, basta visitar a página:

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

...E seguir suas instruções.

Bugtraq e demais listas em securityfocus.com

Moderada pelo Elias Levy, a.k.a. Aleph One, é uma das maiores e melhores listas de discussão (com tráfego de dezenas de mensagens diariamente), principalmente de segurança, em ambientes UNIX. Para se inscrever, basta enviar um email em branco para:

bugtraq-subscribe@securityfocus.com

O site securityfocus mantém vários fóruns de discussão sobre segurança, que abrangem os mais diversos temas. Para visualizar uma relação de fóruns, visite o site:

<http://www.securityfocus.com/cgi-bin/forums.pl>

Pra visualizar instruções sobre como participar de cada lista, visite:

<http://www.securityfocus.com/cgi-bin/subscribe.pl>

O site possui, entre os que mantêm, fóruns com fabricantes específicos, como Microsoft, Sun, e Linux. Para aqueles que dão suporte a produtos destes fabricantes, vale a pena dar uma olhada.

NTBugtraq

A lista NTBUGTRAQ é uma lista moderada pelo canadense Russ Cooper. Ela discute segurança em ambiente Windows NT e 2000. O nível de “barulho” ou de informações que não dizem respeito ao assunto é

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

muito baixo (Russ é bem rigoroso na moderação do grupo), portanto, a grande maioria das informações é de nível alto. Para assiná-la, basta enviar uma mensagem para:

listserv@listserv.ntbugtraq.com

e no corpo da mensagem:

subscribe ntbugtraq Primeiro_nome Sobrenome

Contudo, antes de assinar esta lista, é aconselhável ler a FAQ da mesma em:

<http://ntbugtraq.ntadvice.com/default.asp?pid=31&sid=1>

Windows 2000 Mag. Security Administrator

O site www.ntsecurity.net já foi referência sobre segurança em ambientes Microsoft. Contudo, a cerca de 2 anos, foi deixado de lado, e assumido pela Windows 2000 Magazine, revista de renome mundial para tudo que envolve Windows 2000 (se chamava antes Windows NT Magazine).

O site oferece diversas listas de discussão sobre segurança.

Ao acessar:

<http://www.ntsecurity.net>

Você poderá se inscrever nos fóruns de discussão. Instruções podem ser encontradas diretamente na página principal.

SecuriTeam

O pessoal da securiteam.com reúne, em uma única lista de divulgação, as principais falhas de segurança encontradas em qualquer software. Além disso, divulga o lançamento de ferramentas de segurança importantes.

Esta lista é de máxima importância para aqueles que levam segurança a sério. Para assiná-la, envie uma mensagem em branco para:

List-subscribe@securiteam.com

Para acessar o site:

<http://www.securiteam.com>

Alldas.org Defaced Archive

Os responsáveis pelo site da Alldas.org assumiram a lista de sites desfigurados. Esta lista antes era mantida pelo pessoal da attrition.org, que desistiu de manter o banco de dados pela quantidade de trabalho que o mesmo necessitava.

Aparentemente, o alldas.org também está passando por problemas. O site está instável, e não se sabe a razão. Contudo, a lista está funcionando, na maioria das vezes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Para assinar a lista, basta enviar uma mensagem para:

ml-manager@defaced.alldas.org

Com o corpo em branco, e

Subscribe alldas-defaced

No campo de assunto.

O serviço também oferece diversas estatísticas sobre sites hackeados. Estes dados são muito interessantes, pois você poderá listar as invasões por sistema operacional, domínio, e até pelo nome do hacker ou grupo que realizou o deface.

<http://alldas.org>

Destas páginas, podemos encontrar algumas informações alarmantes:

- O Brasil está em segundo lugar em domínios hackeados. Perde apenas para os .com;
- Os grupos de defacers do Brasil estão no topo da lista com maior número de sites;
- O sistema operacional mais invadido foi Microsoft; em segundo lugar, Linux;
- Dezenas de sites são desfigurados diariamente.

Existe também uma espécie de search engine, onde é possível pesquisar por sites desfigurados. Você poderá visualizar o site original, a página desfigurada, entre outras informações.

ISS – Internet Security Systems Forums

A lista NT Security é uma lista moderada (espere por dezenas de mensagens diariamente), mantida por uma empresa chamada ISS (Internet Security Systems). Para assiná-la, a forma mais fácil é ir ao seguinte endereço:

<http://xforce.iss.net/maillists/>

Lá, você encontrará diversas listas sobre segurança, tanto mantidas pela ISS, como também listas de terceiros.

3. Entendendo Redes e a Internet

Introdução em Redes

Conceito de Redes

As redes de computadores foram criadas a partir da necessidade de se compartilhar dados e dispositivos. Com a distribuição do dado, valioso ou não, tal ambiente passou a ser alvo de um estudo de vulnerabilidades, tanto por parte dos administradores conscientes, quanto por potenciais ameaças (sabotagem ou espionagem industrial, por exemplo).

Contudo, para que a comunicação de dados ocorra entre computadores, é necessário que uma série de etapas e requisitos sejam cumpridos. Podemos dividir a comunicação em rede, didaticamente, em 4 camadas: a parte física (meio de transmissão placas de rede, cabeamento...), a camada de endereçamento / roteamento (responsável pelo endereçamento e pela escolha do melhor caminho para entrega dos dados), a parte de transporte (protocolo de comunicação responsável pelo transporte com integridade dos dados), e a camada de aplicação (que faz interface com o usuário). Se algum elemento de alguma destas camadas falhar, não haverá comunicação.

Interfaces de Rede

O principal contato que temos com uma rede, ou algo palpável que a represente, provavelmente, é através de uma interface, ou placa de rede. Este equipamento, que pode vir na forma de uma placa para ser instalada internamente (dentro do seu computador), ou na forma de um modem (para comunicação dos dados via linhas analógicas), possui diversos padrões, tipos, modelos, e fabricantes. Contudo, de forma resumida, este componente é responsável por ligar o meio de transmissão (geralmente um cabo de rede, ou uma linha telefônica) ao computador. Um dado importante: a grande maioria das placas de rede possui um endereço único, que determina seu fabricante, e sua “impressão digital”. Teoricamente, não existe nenhuma outra interface de rede com o mesmo endereço físico. Contudo, existem técnicas para modificá-lo. Este endereço físico é parte essencial na transmissão dos dados.

Transmissão dos Dados – Camada Física

O principal conceito de transmissão de dados é o da divisão em pacotes, ou frames de rede, dependendo da camada analisada. De forma genérica, os dados trafegam dentro do meio (cabeamento, por exemplo) organizados em lotes, chamados “pacotes”.

Cada pacote possui uma série de controles para a transmissão dos dados, como delimitadores de início e fim, e uma checagem de erros (para quem receber o pacote, poder avaliar se ele chegou corretamente ou se houve alguma perda durante a transmissão), e uma forma de endereçamento (para identificação e escolha da rota). Como a maioria dos meios de transmissão só permite um acesso por vez, a divisão em pacotes resolve o problema de forma inteligente. Se cada ponto que deseja transmitir, o fizer em pedaços, com intervalos de tempo entre as transmissões, para o usuário, parecerá que a comunicação é simultânea. Contudo, em alguns tipos de rede, como no Ethernet, dois ou mais computadores podem tentar transmitir no mesmo momento. Isso causará uma “colisão”: os pacotes serão corrompidos, e os computadores terão de retransmitir os pacotes, observando desta vez, um certo tempo de espera, diferente, para que a colisão não ocorra novamente. Essa forma de utilizar o meio de transmissão se chama CSMA/CD (Carrier Sense, Multiple Access with Collision Detection).

Existem outras formas de transmissão mais eficientes, porém, bem mais caras. Uma delas se chama Token Passing, ou passagem de token. Neste método de acesso ao meio, cada computador transmite em uma ordem pré-determinada, de forma que todos tenham o mesmo tempo de acesso ao meio, geralmente em uma configuração lógica em anel. Outra forma seria o Frame Switching, ou Cell Switching, usado em redes ATM ou Frame Relay (de altíssima velocidade).

Transmissão dos Dados – Camada de Rede

A camada de rede é responsável primariamente pelo endereçamento lógico dos pacotes. Assim, é possível determinar a origem, o destino, e escolher o melhor caminho para um pacote. Por exemplo, numa rede complexa como a Internet, frequentemente, existem diversos caminhos entre seu computador e um servidor, por exemplo, no Japão. Através do seu endereço de origem, alguns roteadores (equipamentos que conectam redes distintas) decidirão qual o melhor caminho, baseado em tráfego, distância e etc., entre você e o servidor no Japão. Outra função é a quebra dos pacotes, caso a rede seguinte não suporte pacotes do mesmo tamanho (também chamado de fragmentação de pacotes).

Transmissão dos Dados – Camada de Transporte

Na camada de transporte, são desempenhadas tarefas de controle de tráfego. Nesta camada, existem mecanismos que determinarão se o pacote foi ou não transmitido corretamente, se o mesmo chegou em sequência (em caso negativo, alguma informação deve existir para que a ordenação seja possível), bem como adequação a velocidade de transmissão (mais rápido ou não, dependendo da capacidade da rede e número de pacotes recebidos com erro).

Transmissão de Dados – Camada de Aplicação

Nesta camada, estão presentes os protocolos que fazem direta interface com o usuário, ou que tratam as informações da rede, nos apresentando de uma forma compreensível. Um exemplo típico de camada de aplicação: o Ambiente de Rede, presente em máquinas Windows 9x e Windows NT / 2000. Para que o usuário consiga visualizar a rede, existe neste caso um protocolo, chamado NetBIOS, que torna possível aquele tipo de representação. Um outro exemplo seria o FTP (File Transfer Protocol), um protocolo da pilha TCP/IP, usado para transferência de arquivos. Através dele, o usuário ganha um prompt de comando, de onde pode enviar ou receber arquivos, depois de adequadamente autenticado.

A Conexão a uma Rede

A comunicação de um computador a uma rede se dá atendendo as necessidades de todas as camadas apresentadas. Primeiro, precisamos de uma interface física, que permita ao computador enxergar o meio de comunicação da rede. Isso é feito geralmente através de uma placa de rede, ou de um modem. No caso das placas de rede, as formas mais comuns de conexão são através de cabeamento par trançado (inicialmente projetado para telefonia, mas modificado para comportar o tráfego de dados) ou através de cabeamento coaxial (parecido com um cabo de antena externa de TV). A maioria das redes locais usa uma destas tecnologias, ou, caso uma maior velocidade ou maior distância seja necessária, alguma tecnologia baseada em fibra ótica ou transmissão sem fio (via rádio, microondas, satélite, laser, etc.).

O interessante das redes locais com cabeamento par trançado ou coaxial é sua facilidade de instalação. No caso do cabo par trançado, serão usados conectores do tipo RJ-45 (parecidos com conectores de telefone), e um hub ou switch (uma espécie de concentrador), que interligará os diversos segmentos de cabo (em redes par-trançado, cada segmento é único do computador ao concentrador). No caso do cabo coaxial, não é necessário o hub, pois o cabo “passa” em todos computadores. Porém, se o cabo for rompido, toda a rede será comprometida.

Interligando Redes

Dada a abrangência de algumas redes como a Internet, determinadas pilhas de protocolo (linguagem de comunicação entre computadores) foram projetadas para suportar a divisão dos endereços em “regiões”, similares aos “bairros” em nossas cidades. Estas divisões permitem uma melhor configuração da rede, como a organização das máquinas e a transmissão dos dados de forma hierárquica. Além disso, permitem uma melhor utilização do endereçamento.

Contudo, para que diversas redes se comuniquem, faz-se necessária a presença de um determinado tipo de componente: o roteador. Ele é responsável pela comunicação de dados entre redes distintas. Ele desempenha esta tarefa analisando os campos de endereço origem e endereço destino, uma tabela de rotas, e enviando o pacote pelo caminho presente na tabela (rota) ou pelo melhor caminho (caso existam várias rotas para um mesmo destino, e caso o roteador seja dinâmico).

Em conjunto com o endereço físico das placas de rede, também chamado de endereço de hardware, o endereçamento lógico fecha o conceito de endereçamento. Repare que o endereço lógico, ou de protocolo, usado pelos roteadores, geralmente pode ser determinado manualmente. Já o endereço físico não: é registrado pelo fabricante da interface de rede.

Então, temos um problema: se um computador tiver sua placa de rede trocada, não conseguirá mais se comunicar na rede. Isto seria verdade se não existisse o endereçamento lógico, pois ao se trocar uma interface de rede, todas as tabelas de roteamento teriam de ser trocadas, pois o endereço mudou, e porque o endereço físico não possui nenhuma característica hierárquica.

Para resolver o problema, as pilhas e protocolo criam uma associação entre o endereço físico e o lógico. Tomemos como exemplo a pilha de protocolos TCP/IP. Nela, existe um protocolo chamado ARP (Address Resolution Protocol) responsável por descobrir endereços físicos e associá-los a endereços lógicos.

Funciona da seguinte forma:

1º caso: dois computadores numa mesma rede

1. Computador A deseja se comunicar com computador B
2. Computador A envia uma chamada ARP na rede, para todos os computadores, perguntando “Qual o endereço físico do computador que possui endereço lógico ABCD?”
3. Computador ABCD ouve, e responde: “meu endereço físico é: XYZW”
4. A partir deste momento, o computador A poderá enviar os pacotes diretamente para o computador B, pois todas as informações de endereçamento estão presentes (endereço físico e lógico dele próprio, e do destino).

2º caso: computadores em redes diferentes

1. Computador A deseja se comunicar com computador B
2. Computador A verifica o endereço lógico de computador B, e constata que o mesmo NÃO está na mesma subrede que ele próprio
3. Computador A então, tenta enviar pacote para seu roteador
4. Computador A estabelece comunicação com roteador, da mesma forma que exemplificado no 1º caso
5. Roteador estabelece comunicação com computador B, da mesma forma que exemplificado no 1º caso

Perceba a diferença. Os endereços físicos somente são importantes dentro de uma mesma rede, justamente porque não existe hierarquia em seu formato. Contudo, através do endereço lógico, computador A pode determinar que computador B não pertencia a sua rede, e enviou o pacote para o componente responsável pela interligação de redes: o roteador, que, por sua vez, sabia para onde enviar o pacote, de

forma que o mesmo chegasse ao computador B. Caso o roteador não possuísse esta informação, retornaria uma mensagem para o computador A, dizendo: “rede destino inalcançável”.

TCP/IP

O TCP/IP (Transmission Control Protocol / Internet Protocol), é uma pilha de protocolos que vem sendo modelada a décadas, desde a criação de uma rede chamada ARPANET, em meados dos anos 60, nos EUA. Ao contrário do que muitos acham, não é apenas um protocolo de comunicação, mas uma pilha deles. Essa pilha de linguagens de comunicação permite que todas as camadas de comunicação em rede sejam atendidas e a comunicação seja possível. Todas as pilhas de protocolo, de uma forma ou de outra, tem de atender a todas as camadas, para permitir que os computadores consigam trocar informações.

Podemos fazer uma analogia de uma pilha de protocolos com a comunicação verbal. Se alguém fala com outra pessoa, e esta o entende, é porque todas as camadas para que a “fala” seja interpretada foram atendidas. Imagine, para que duas pessoas se comuniquem verbalmente, será necessário:

1. Que ambas saibam o mesmo idioma
2. Que ambas tenham toda a estrutura fisiológica para que emitam som (voz – cordas vocais, língua, garganta, pulmões, etc.)
3. Que ambas possuam toda a estrutura fisiológica para que ouçam o som (orelha, ouvido interno, tímpanos, etc.)

Nesta pilha de protocolos, temos como mais importantes:

ARP (Address Resolution Protocol)

O ARP é o protocolo responsável pelo mapeamento ou associação do endereço físico ao endereço lógico, de computadores numa mesma rede. Ele faz isso através do processo exemplificado no tópico anterior.

IP

O Internet protocol é o responsável pelo endereçamento lógico de pacotes TCP/IP. Além disso, é responsável pelo roteamento destes pacotes, e sua fragmentação, caso a rede seguinte não possa interpretar pacotes do mesmo tamanho. O mais importante para entendermos o funcionamento do IP é entender como é feito seu endereçamento lógico.

Um endereço IP é algo parecido com isto:

200.241.236.94

Apesar de aparentemente não ter muita lógica, este endereço contém uma série de informações. A primeira delas é que, neste número estão presentes a identificação da rede na qual o computador está ligado, e o seu número, em relação a esta rede. Detalhe: o computador NÃO interpreta este número acima como quatro cadeias decimais separadas por pontos (esta representação é apenas para tornar nossas vidas mais fáceis). Ele entende como quatro octetos, ou quatro campos de 8 bits:

11001000.11110001.11101100.01011110

Para facilitar a organização das redes inicialmente, o endereçamento foi dividido em 5 classes:

Endereço de classe A;
Endereço de classe B;
Endereço de classe C;
Endereço de classe D;
Endereço de classe E.

Para identificar cada classe, é necessário observar o primeiro octeto.

Classe A

Se o primeiro octeto, no formato binário, se iniciar com 0, então o endereço é de classe A. Para descobrirmos seus equivalentes em decimal, basta converter o número mínimo e o máximo, de 8 bits, com o primeiro bit igual a 0:

| Binário | Decimal |
|---------------------|---------|
| 00000000 a 01111111 | 0 a 127 |

Portanto, qualquer endereço IP que tenha o primeiro octeto compreendido entre 0 e 127, é um endereço de classe A.

Classe B

Os endereços de classe B possuem o primeiro octeto, em binário, iniciado por 10:

| Binário | Decimal |
|---------------------|-----------|
| 10000000 a 10111111 | 128 a 191 |

Assim sendo, endereços IP iniciados com números compreendidos entre 128 a 191, são endereços de classe B.

Classe C

Endereços de classe C possuem o primeiro octeto, em binário, iniciado por 110:

| Binário | Decimal |
|---------------------|-----------|
| 11000000 a 11011111 | 192 a 223 |

Desta forma, endereços IP iniciados com números compreendidos entre 192 e 223, são endereços de classe C.

Os endereços de classe D e E não são usados para endereçamento de computadores. A classe D é reservada para um serviço chamado Multicast, enquanto a classe E, para experimentos (ambas são reservadas).

Algumas conclusões, fatos e padrões sobre endereços IP:

1. QUALQUER endereço iniciado por 127, é considerado endereço de diagnóstico, e representa sua própria interface (também chamado de loopback);
2. O endereçamento IP usado hoje é chamado de IP versão 4. O número de endereços IP em uso preocupa vários especialistas. Um dos projetistas da pilha, Vincent Cerf, previu que até 2008, todos os endereços estarão em uso. Para isso, já existe em funcionamento uma nova versão, chamada de IP versão 6, que terá como endereçamento 128 bits, ao invés dos 32 bits do IP versão 4;

3. Para entender as vulnerabilidades e como funciona a maioria dos mecanismos de ataque e defesa, é necessário entender o conceito básico do endereçamento IP;
4. A pilha TCP/IP vem sendo modificada desde a década de 60. Como seu design / conceito é bastante antigo, existem diversas vulnerabilidades inerentes ao protocolo, que são bastante usadas por hackers;
5. Cada octeto não pode ter um valor decimal acima de 255 afinal, 8 bits somente conseguem assumir 256 combinações diferentes, o que dá, em decimal, a contagem de 0 a 255.

Máscara

Ao contrário do que muitos pensam, a classe do endereço NÃO determina ou fixa que porções do endereço representam a rede, e que porções do endereço representam a máquina dentro da rede. Isto é feito pela máscara de subrede. O conceito da máscara é bastante simples: ela possui o mesmo formato de um endereço IP (4 octetos). Ela é comparada posicionalmente ao endereço IP e, onde houver o bit 1, aquele bit correspondente no endereço IP será parte da identificação da rede. Onde houver o bit 0, será parte da identificação do endereço da máquina **dentro** daquela rede. Pensando estritamente desta forma, podemos claramente perceber que a coisa pode ficar bem complicada. Contudo, existe um padrão que regula a utilização destes bits, para que sua configuração não fuja ao controle. Esse padrão obedece as seguintes regras:

1. A porção de rede se inicia da esquerda para a direita, enquanto a porção host, da direita para a esquerda;
2. Endereços de classe A, tem, por padrão, a máscara 255.0.0.0
3. Endereços de classe B, tem, por padrão, a máscara 255.255.0.0
4. Endereços de classe C, tem, por padrão, a máscara 255.255.255.0

Alguns exemplos:

Exemplo 1:

O endereço 200.241.35.46 é um endereço de classe C. Possui, por padrão, máscara 255.255.255.0, o que significa que, a máquina que possuir este endereço, está na rede 200.241.35, e possui, dentro desta rede, o endereço 46.

| Octeto | 1º octeto | 2º octeto | 3º octeto | 4º octeto |
|--------------|-----------|-----------|-----------|-----------|
| End. IP dec. | 200 | 241 | 35 | 46 |
| Máscara dec. | 255 | 255 | 255 | 0 |
| End IP bin. | 11001000 | 11110001 | 00100011 | 01011110 |
| Máscara bin. | 11111111 | 11111111 | 11111111 | 00000000 |
| Separação | End. Rede | | | End. Host |

Exemplo 2:

O endereço 10.126.46.99 é um endereço de classe A. Possui, por padrão, máscara 255.0.0.0, o que significa que, a máquina que possuir este endereço, está na rede 10, e possui, dentro desta rede, o endereço 126.46.99.

| Octeto | 1º octeto | 2º octeto | 3º octeto | 4º octeto |
|--------------|-----------|-----------|-----------|-----------|
| End. IP dec. | 10 | 126 | 46 | 99 |
| Máscara dec. | 255 | 0 | 0 | 0 |
| End IP bin. | 00001010 | 01111110 | 01011110 | 01100011 |
| Máscara bin. | 11111111 | 00000000 | 00000000 | 00000000 |
| Separação | End. Rede | | End. host | |

Exemplo 3:

O endereço 190.23.56.89 é um endereço de classe B. Possui, por padrão, máscara 255.255.0.0, o que significa que, a máquina que possuir este endereço, está na rede 190.23, e possui, dentro desta rede, o endereço 56.89.

| Octeto | 1º octeto | 2º octeto | 3º octeto | 4º octeto |
|--------------|-----------|-----------|-----------|-----------|
| End. IP dec. | 190 | 23 | 56 | 89 |
| Máscara dec. | 255 | 255 | 0 | 0 |
| End IP bin. | 10111110 | 00010111 | 00111000 | 01011001 |
| Máscara bin. | 11111111 | 11111111 | 00000000 | 00000000 |
| Separação | End. Rede | | End. Host | |

Algumas conclusões e fatos sobre a máscara:

1. O que define qual porção do endereço representa a rede e qual porção representa o host é a máscara, e não a classe do endereço IP (apesar de existir um padrão que associa determinadas máscaras às classes);
2. A máscara pode ser mudada, alterando a representação das porções rede/host do endereço IP;
3. Computadores com a porção rede do endereço diferentes SOMENTE se comunicarão se existir um roteador entre eles (neste caso, o computador origem irá automaticamente enviar o pacote para o roteador resolver o caminho até a rede destino);
4. Computadores com a porção rede do endereço iguais SOMENTE se comunicarão se NÃO existir um roteador entre eles (estiverem na mesma rede física. Neste caso, o computador NÃO tentará enviar o pacote para o roteador, pois o endereço destino está na mesma rede que a sua).

Problemas comuns de configuração IP:

1. Máscara errada;
2. Endereço do gateway (roteador) errado;
3. Porção rede errada, ou endereço IP duplicado.

ICMP (Internet Control Message Protocol)

A função do ICMP é basicamente de diagnóstico e tratamento de mensagens. Através dele, é possível determinar, por exemplo, quanto tempo um pacote está demorando em ir para uma máquina remota e voltar (**round trip**), bem como determinar se houve perda de pacotes durante a transmissão. Com ele, também é possível determinar qual o caminho que um pacote está seguindo a partir de uma máquina. O ICMP também possui outras funções como o SOURCE_SQUENCH. Esta função permite ao protocolo IP saber se a taxa de transmissão está muito rápida entre redes. Quando um roteador recebe um pacote ICMP SOURCE_SQUENCH, ele sabe que terá de diminuir a velocidade para não saturar o próximo roteador. Existem outros tipos de pacotes ICMP, como o perigoso SOURCE_ROUTING, que possibilita a troca temporária de uma rota.

TCP (Transmission Control Protocol)

O protocolo TCP é um protocolo de transporte, responsável pela entrega correta dos pacotes. Sua principal característica é a confiabilidade. Para cada pacote ou conjunto de pacotes que envia, espera do destinatário uma confirmação da chegada dos mesmos. Caso isso não ocorra, ou o pacote chegue corrompido, ele tratará de efetuar a retransmissão. Ele também coloca nos pacotes um número de sequência, para que o destino possa remontar o dado original, caso os pacotes sigam por caminhos diferentes ou cheguem atrasados (fora de ordem). Este número de sequência também é usado como recurso de segurança.

UDP (User Datagram Protocol)

O UDP assim como o TCP, também é um protocolo de transporte. Contudo, não possui nenhuma checagem de erros, confirmação de entrega ou sequenciamento. Ele é muito utilizado em aplicações que necessitem de tráfego urgente, e não sejam tão sensíveis a algumas perdas de pacotes. Exemplos de aplicações que usam UDP como transporte: transmissão de áudio e vídeo pela rede (RealPlayer, Realvideo ou Media Player), jogos online (como Quake, Half-Life). Pela falta do número de sequência ou confirmação de conexão, tráfego UDP é muito mais vulnerável em termos de segurança.

Protocolos de Aplicação

Em cima da infra-estrutura fornecida pelos protocolos descritos até agora, funcionam os protocolos de aplicação. Estes fazem a interface com o usuário, ou com a aplicação do usuário. Exemplos de protocolos de aplicação: HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), SNMP (Simple Network Management Protocol), POP3 (Post Office Protocol v.3), TELNET, e assim por diante. Cada protocolo de aplicação se comunica com a camada de transporte através de portas de comunicação. Existem 65536 portas possíveis, e por convenção, as portas de 1 a 1023 são conhecidas como “Well Known Port Numbers”, portas privilegiadas ou portas baixas, que possuem serviços mais comuns previamente associados.

Cada protocolo de aplicação precisa de uma porta, TCP ou UDP, para funcionar. Os mais antigos possuem suas portas padrão já determinadas. Exemplo:

| Protocolo / Aplicação | Porta Padrão | Transporte |
|-----------------------|--------------|------------|
| FTP | 21 | TCP |
| TELNET | 23 | TCP |
| SMTP | 25 | TCP |
| WINS NameServer | 42 | UDP |
| HTTP | 80 | TCP |
| POP3 | 110 | TCP |
| SNMP | 161 | UDP |
| SNMP trap | 162 | UDP |

As portas acima de 1023 são denominadas portas altas, e são usadas como end points, ou pontos de “devolução” de uma conexão. Imagine uma conexão como um cano de água conectando duas casas. A diferença é que neste cano, a água pode ir a qualquer sentido. Portanto, ao tentar ler seu correio eletrônico, você provavelmente usará um protocolo chamado POP3, que funciona na porta 110. Seu computador estabelecerá uma conexão com o servidor de correio, na porta 110 remota, e 1026 (por exemplo) localmente. A porta local é na maioria dos protocolos, uma porta acima de 1023, desde que não esteja sendo usada.

DNS (Domain Name System)

No final da década de 70, começaram a pensar numa forma mais fácil de tratar computadores ligados a uma rede TCPIP. Imagine que, para estabelecer uma conexão, você deve fornecer o endereço IP do destino, e o serviço que deseja usar (no caso, a porta), e o transporte. Decorar dezenas de endereços IP não é uma tarefa fácil, tão pouco prática. O DNS foi concebido para evitar este transtorno. Através dele, cada host recebe um nome, mais fácil de aprender, dentro de uma hierarquia, o que ajuda ainda mais na hora de identificá-lo. Um exemplo seria “www.rmc.eti.br”. Este caso é uma referência ao servidor www, dentro do domínio rmc.eti.br. No Brasil, a entidade que controla o registro de nomes (de forma a impedir fraudes e utilização indevida / registro indevido) é a FAPESP – Fundação de Fomento a Pesquisa do Estado de São Paulo – <http://registro.br>.

Sockets (soquetes de comunicação)

Os sockets são a base para o estabelecimento da comunicação numa rede TCP/IP. Através dele é que a transferência de dados se torna possível. Cada conexão é montada por um socket, que é composto de três informações:

1. endereçamento (origem e destino)
2. porta origem / destino
3. transporte

Portanto, no caso acima, ao tentar ler seu correio, um socket será estabelecido entre sua máquina e o servidor de correio. Para montá-lo, precisamos:

1. do seu endereço IP e do endereço IP destino
2. porta origem / destino (neste caso, porta destino 110, origem 1026)
3. transporte (TCP)

Gerenciando Erros de Comunicação

Por padrão, existem alguns utilitários presentes na pilha TCPIP que possibilitam ao usuário diagnosticar problemas. Alguns dos utilitários mais usados são:

PING (Packet INternet Grouper)

Este utilitário utiliza o protocolo ICMP para diagnosticar o tempo de resposta entre dois computadores ligados numa rede TCP/IP. A partir daí, pode-se ter uma estimativa do tráfego (se o canal de comunicação está ou não saturado) bem como o tempo de latência do canal. Ao contrário do que muitos pensam, a latência de um link está também diretamente ligada a velocidade do roteador (em termos de processamento) e não somente a velocidade do canal de comunicação.

TRACERT (traceroute)

O tracert também utiliza pacotes ICMP (em máquinas Windows) para realizar diagnósticos. Porém, desta vez, você poderá determinar qual o caminho que os pacotes farão até um host destino. A função do tracert ou traceroute é justamente essa: traçar a rota entre uma origem e um destino. Ele mostrará todos os nós (roteadores) entre a origem e o destino, com o tempo médio que o pacote levou para atingir o determinado nó. Com este utilitário também é possível determinar se existe um loop em algum roteador entre a origem e o destino. Alguns roteadores entram em loop quando perdem um de seus links, ou simplesmente quando não estão configurados corretamente. Vale citar que todo pacote possui um tempo de vida, que representa a quantidade em segundos que ele pode passar sendo processado pelos roteadores. Suponha que o tempo de vida (TTL – Time To Live) de um pacote é 127. Cada roteador por onde o pacote passar, diminuirá deste valor, o tempo que o pacote passou para ser processado internamente. Na grande maioria dos casos, os roteadores processam o pacote em muito menos de 1 segundo, porém, mesmo assim, diminuirão pelo menos uma unidade do TTL. Este valor evita que tráfego “morto” seja mantido em circulação, tipicamente em loops que potencialmente podem ser criados por configurações de rotas erradas.

...Então, O que é a Internet

Uma vez explicados os conceitos da pilha de protocolos usada na Internet, e seu funcionamento, fica mais fácil entendê-la. A Internet nada mais é do que uma rede enorme, a nível mundial, que usa como linguagem de comunicação, a pilha de protocolos TCP/IP. Como tal herda uma série de vulnerabilidades inerentes à própria pilha TCP/IP, além de problemas e bugs que possam existir nas aplicações que usam esta infra-estrutura de rede.

Muitos perguntam naturalmente como a Internet pode funcionar. Seu conceito é bastante simples. Na década de 60, criou-se na Universidade de Berkeley, em Chicago, uma rede experimental, para utilização militar. Esta rede cresceu muito, dada a necessidade das próprias universidades de trocarem informações. Ela se chamava ARPANET. No início da década de 80, esta rede passou a utilizar apenas uma pilha de protocolos padrão, que na época passou a se chamar TCP/IP. Pouco tempo depois, ocorreu a abertura desta rede para fins comerciais, o que, ao longo de pouco mais de 10 anos, a transformou no que conhecemos hoje.

A comunicação na Internet é provida através de backbones, ou espinhas dorsais de comunicação (link de altíssima velocidade) mantidos por provedores, pontos de presença, governos, entidades de ensino, e empresas privadas. Contudo, para participar dela, uma série de requisitos precisam ser obedecidos. O primeiro deles é relativo ao endereçamento.

Vimos que o endereço IP, numa rede, precisa ser distinto. Portanto, em toda a Internet, não podem existir dois endereços IP iguais. Assim sendo, para uma máquina se comunicar com outras na Internet, ela deve possuir um endereço válido. Cada provedor de backbone possui um lote, ou intervalo de endereços IP que pode fornecer aos seus clientes. Aqui no Brasil, podemos citar a Embratel como provedora de backbone. Ao requisitar um link com a Internet à Embratel, receberá juntamente com o link, um intervalo de endereços para ser usado por seus computadores, ligados ao seu backbone. A nível mundial, o órgão que gerencia os endereços IP válidos chama-se IANA (Internet Assigned Numbers Authority).

Para que a comunicação seja possível a nível mundial, cada detentor de uma rede (ou espaço de endereçamento) é responsável por estabelecer a comunicação com seu provedor de backbone, bem como configurar seu roteador ou roteadores com as rotas necessárias ao funcionamento de sua sub rede. Se levarmos isso a uma escala mundial, cada detentor de uma sub rede fazendo com que ela seja acessível através de um roteador corretamente configurado, entendemos como funciona a Internet a nível administrativo (por mais incrível que pareça).

4. Entendendo a Invasão

"Na Internet Brasileira, a quantidade de vítimas, sejam corporativas ou o usuário final, só não é maior pela falta de divulgação, não pela quantidade de investimentos ou medidas de contra-ataque adotadas, que são desprezíveis."

O Porquê da Invasão

Os motivos são diversos. Variam desde a pura curiosidade pela curiosidade, passando pela curiosidade em aprender, pelo teste de capacidade ("vamos ver se eu sou capaz"), até o extremo, relativo a ganhos financeiros, extorsão, chantagem de algum tipo, espionagem industrial, venda de informações confidenciais e, o que está muito na moda, ferir a imagem de uma determinada empresa ou serviço (geralmente, a notícia de que uma empresa foi invadida é proporcional a sua fama – e normalmente um desastre em termos de RP).

As empresas hoje em dia investem quantias fantásticas em segurança, mas não no Brasil. O retrato do descaso à segurança de informações no Brasil é claramente traduzido na falta de leis neste sentido. Além disso, existe um fator agravante: quando existir o interesse em elaborar tais leis, serão por indivíduos que não tem por objetivo principal a segurança em si. O resultado serão leis absurdas, que irão atrapalhar mais do que ajudar. Um exemplo disso é o que vem ocorrendo em alguns estados nos EUA. Nestes estados, a lei chega a ser tão restritiva que até testes de vulnerabilidade são considerados ilegais, mesmo com o consentimento da empresa contratante do serviço.

Isto no aspecto empresarial.

No caso do usuário final, esse está entregue à sorte. Não existe nenhum serviço de segurança gratuito, que possa ser utilizado pelo usuário: os provedores de acesso não garantem a segurança do usuário conectado à sua rede (assim como uma companhia telefônica não poderia ser responsabilizada por um trote).

De qualquer forma, existem diversas ferramentas e procedimentos que podem ser usados para aumentar o nível de segurança de seu computador, digamos, em casa, que acessa a Internet por um link discado. É justamente neste nicho de mercado em que estão as principais vítimas, que inclusive, não são notícia no dia seguinte a uma invasão. A quantidade de "wannabes" é enorme, e a tendência é aumentar. Os wannabes estão sempre à procura de um novo desafio, e o usuário final na maioria das vezes é a vítima preferida, JUSTAMENTE pela taxa de sucesso que os Wannabes tem em relação ao número de ataques realizados.

"A grande maioria das empresas no Brasil tratam o seu setor de informática como um custo, ou despesa, e não como um investimento. Portanto, se assim o é em termos genéricos, podemos concluir que os recursos destinados a medidas de segurança são desprezíveis."

Ponto de Vista do White-hat

O white-hat geralmente é um programador bem sucedido, que, na grande maioria das vezes, é contratado como consultor de segurança. Nestes casos, ele também recebe o nome de **"Samurai"**. Ao descobrir uma falha ou vulnerabilidade, envia um **"how-to"**, ou procedimento para que o problema seja recriado, para amigos ou pessoas de convívio próximo, que também estejam envolvidas com segurança ou desenvolvimento. Uma vez confirmada a falha, ela é reportada em listas de discussão que debatem o tema, onde os maiores especialistas se encontram. Exemplos de listas:

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Os white-hats (os black-hats e crackers também) se mantêm muito bem atualizados. Ser inscrito em diversas listas de discussão, ler muito sobre o tema e visitar sites de segurança é essencial. Alguns sites muito bons sobre o tema:

<http://www.securityfocus.com/>
<http://packetstorm.securify.com>
<http://www.securiteam.com>
<http://www.hackers.com.br>

Ponto de Vista do Black-Hat

"Os usuários finais bem como as empresas não tratam a segurança das informações como algo importante, ou de sua responsabilidade. Podemos fazer uma analogia com nossa segurança na sociedade moderna. Se qualquer pessoa for a um estacionamento público, visado por ladrões de carro, com toda certeza não deixará seu carro aberto com a chave em cima do banco, assim como também não deixará seu rádio à mostra. Da mesma forma, foram-se os tempos onde a maioria de nós dormia com nossas casas abertas, com as portas destrancadas."

O black-hat possui tanta habilidade quanto o white-hat. Porém, ao descobrir uma nova vulnerabilidade, não a publicará na Internet: usará para fins geralmente ilegais, em proveito próprio. Possui também profundos conhecimentos de programação, e geralmente está empregado em alguma empresa de desenvolvimento de sistemas, ou como programador-analista, ou como responsável pelo suporte. Hoje em dia, podemos encontrar black-hats em empresas de comunicação, assim como em provedores de acesso à Internet (ISPs).

Contudo, ao contrário do white-hat, wannabe ou cracker, o black-hat fará de tudo para manter sua identidade secreta, bem como suas atividades ilegais. A própria natureza ilegal de suas realizações o mantém afastado de qualquer publicidade. A maioria dos black-hats possui algum tipo de identidade “digital”, ou pseudônimo na Internet, que afasta qualquer possibilidade de identificação, como um email free (contas free de correio eletrônico, com cadastro errado), e acessa a Internet por servidores de Proxy alheios (uma lista de servidores proxy pode ser encontrada nos anexos). Possui contas de acesso a Internet em diversos provedores, de preferência em provedores muito pequenos ou do interior, que não possuem um sistema exato para identificação de chamadas ou conexões. Hoje em dia, provedores gratuitos fornecem este acesso de forma bastante satisfatória, principalmente em grandes cidades.

Provedores gratuitos que não possuem senhas individualizadas, só podem identificar um usuário pelo número da chamada. É aí onde entra o Phreaker. Contudo, no Brasil, em grandes cidades, as companhias telefônicas NÃO utilizam o sistema BINA (“B” Identifica Número de “A”), por motivos de carga imposta às centrais telefônicas. A troca das informações de “caller ID” necessárias à identificação do número origem de uma chamada gera uma utilização maior das centrais. Muitas centrais que já estão em sua capacidade máxima não conseguiriam operar com as informações de “Caller ID” habilitadas. Assim sendo, se torna praticamente impossível identificar a origem de uma chamada, por parte de um provedor de acesso.

Mesmo assim, teríamos o sistema de tarifação da companhia telefônica, que, judicialmente, poderia comprovar a origem de uma ligação. Contudo, existem várias formas de se “burlar” a tarifação. Uma delas é discar de um telefone público isolado, em um horário de nenhum movimento (madrugada). Outra opção é “roubar” uma linha telefônica diretamente em um quadro de conexões de um quarteirão, ou até mesmo no próprio poste de iluminação pública, ou em quadros de telefonia de um condomínio, por exemplo. A terceira opção seria usar conhecimentos de “phreaking” para evitar que a companhia telefônica consiga obter a identificação da chamada.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Independente do método utilizado, o esforço empregado na identificação será proporcional ao efeito das ações de um hacker. Um black-hat pode perfeitamente usar os métodos descritos acima, de conexão através de um provedor gratuito, apenas para identificar ou obter informações necessárias ao seu trabalho. Uma vez determinada uma abordagem ou traçada uma metodologia para se realizar uma invasão, aí sim, métodos mais avançados podem ser usados, como roubo de linha (conhecido no Brasil como “papagaio”) ou até phreaking, impedindo sua identificação.

Além do black-hat, temos os crackers e os wannabes, que de certa forma, poderiam ser enquadrados como black-hats, mesmo não tendo conhecimento para tal.

"As empresas muitas vezes sequer oferecem a infra-estrutura necessária a um administrador de redes e segurança competente. Analisam apenas a questão de custo/benefício imediata, sem levar em consideração o impacto que uma invasão poderá ter na imagem da empresa, e na perda direta de clientes a longo prazo."

Os crackers farão ou tentarão fazer uma invasão apenas pelo desafio, ou para enaltecer seu ego, junto ao espelho, ou junto à comunidade da qual participa. Neste aspecto, o wannabe possui mais ou menos o mesmo ponto de vista. Contudo, o wannabe usa mais suas “histórias” para se afirmar dentro do seu grupo social do que o cracker. Um exemplo clássico do comportamento de um cracker foi o demonstrado pelo Kevin Poulsen, hacker bastante conhecido, que foi preso nos EUA por ter invadido a rede de defesa (ARPANET), entre outras coisas, como forjar ligações para uma emissora de rádio para vencer um concurso, que tinha como prêmio... um Porsche.

Hoje, é consultor de segurança, e escreve artigos para diversos sites especializados sobre o tema. É colunista chefe em <http://www.securityfocus.com/>.

Como demonstrado, esta é uma diferença básica: o cracker possui algum conhecimento e é mais objetivo em suas realizações. O wannabe geralmente não é organizado, e tenta testar em tudo e em todos as novidades que conseguir obter. Este é mais perigoso, pois pelo fato de atirar em todas as direções, pode atingir qualquer um, eu, você, ou alguém conhecido / famoso. É também o mais fácil de cair nas mãos da justiça, pela enorme trilha de pistas que deixa no caminho por onde passa.

O mais interessante disso tudo é que a grande maioria dos black-hats do passado, hoje são White-hats (até onde sabemos), e são bem sucedidos como colunistas e palestrantes. Contudo, poucos conseguiram emplacar como consultores de segurança.

Alguns do hackers mais famosos podem ser encontrados em:

<http://tlc.discovery.com/convergence/hackers/hackers.html>

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

4. Vulnerabilidades em Meu Sistema

Todo e qualquer sistema, código, script ou programa, é vulnerável a bugs. Todos estes são escritos por mãos (dedos) humanas, e concebidos por mentes humanas, sujeitas à falhas. Por consequência, também estão sujeitos à falhas.

A grande maioria dos furos de segurança surge de bugs no código original. Contudo, nem todos os bugs são furos de segurança. Obviamente, se um bug surge em uma aplicação de editoração de imagens ou texto, não necessariamente estará relacionada a segurança. Porém, se este bug é descoberto e existe no software do firewall que sua empresa usa, ou você possui instalado em seu computador, aí sim, estará relacionado diretamente com segurança. É inclusive importante observar que muitos destes bugs surgem pela interação de programas. Digamos, que o programa original, instalado em um contexto onde realiza suas tarefas sozinho, não apresente falhas. Mas, a partir do momento que é posto para trabalhar em conjunto com outro programa, expõe algum bug ou falha operacional. Estas por sinal são as mais difíceis de diagnosticar, pois geralmente apresentam características intermitentes.

Que Componentes São Vulneráveis

Qualquer um.

Principalmente se está ligado diretamente a algum serviço de rede.

Existem diversos tratados, estudos e documentos discutindo estatísticas de produção de bugs. Contudo, uma regra básica que sempre trará um bom aproveitamento com relação à segurança é a seguinte: menos código no ar, menos bugs, menos problemas de segurança.

Axioma 1 (Murphy) *Todos os programas têm bugs.*

Teorema 1 (Lei dos Programas Grandes) *Programas grandes possuem ainda mais bugs do que o seu tamanho pode indicar.*

Prova: por inspeção

Corolário 1.1 *Um programa relativo a segurança possui bugs de segurança.*

Teorema 2 *Se você não executar um programa, não importará se ele possui ou não bugs.*

Prova: como em todos os sistemas lógicos, (falso → verdadeiro) = falso.

Corolário 2.1 *Se você não executar um programa, não importará se ele possui ou não bugs de segurança.*

Teorema 3 *Máquinas expostas devem rodar tão poucos programas quanto possível; os que rodarem, devem ser tão pequenos quanto o possível.*

Prova: corolários 1.1 e 2.1

Corolário 3.1 (Teorema Fundamental dos Firewalls) *A maioria dos hosts não consegue atender às nossas necessidades: eles rodam programas demais que são grandes demais. Desta forma, a única solução é isolar atrás de um firewall se você deseja rodar qualquer programa que seja.*

(Firewalls and Internet Security: Repelling the Wily Hacker
William Cheswick / Steven Bellovin)

Conclusão: quanto menos serviços no ar, menor a possibilidade do computador apresentar uma falha de segurança.

Sistema Operacional

"Não existe sistema operacional seguro. O que existe é um administrador consciente e capaz, que, a partir das ferramentas disponibilizadas com o sistema operacional, terá como tarefa usá-las para garantir a segurança desejada."

Um dos maiores mitos que existem hoje na Internet e no meio de segurança é relativo a sistemas operacionais. O mito existe em torno da rivalidade entre Windows NT / 2000 contra soluções baseadas em UNIX. Qualquer programa está sujeito a falhas, inclusive programas da Microsoft, **E** programas feitos pela comunidade, para uso em alguma das diversas plataformas UNIX, como o Linux.

Tradicionalmente, os profissionais de segurança que hoje existem vieram do ambiente de programação, ou foram um dia, hackers (sejam white-hats ou black-hats). Cada um destes profissionais possui suas preferências de uso, e tenderão a recomendar aquele sistema que dominam, ou que se sentem mais confortáveis em operar / configurar. Porém, alguns destes profissionais, por não conhecerem bem outras soluções, de uma forma ou de outra têm a tendência a não recomendá-la (seja por uma preferência pessoal ou até comercial, pois deixará de “vender” uma consultoria caso seu cliente escolha outra solução que não domine).

Outro problema bastante comum, mas que poucos tem a coragem de admitir, é que a grande maioria dos administradores de sistemas UNIX possui conhecimentos básicos sobre redes, segurança e administração destes ambientes. Contudo, a maioria dos administradores para a plataforma Microsoft não possui estes conhecimentos básicos, o que torna as instalações desta plataforma mais susceptíveis a ataques bem sucedidos. Neste caso, a “facilidade” em operar o sistema prejudica de forma indireta a sua segurança, a longo prazo.

Regra básica número 1 de segurança em sistemas operacionais:

"Mantenha todo o sistema, e, principalmente os serviços de rede que nele são executados, atualizados ao máximo – principalmente se a atualização for relativa a algum problema de segurança".

Regra básica número 2 de segurança em sistemas operacionais:

(seguindo o “Teorema Fundamental dos Firewalls”)

"Execute somente serviços necessários. Qualquer programa, serviço, código de algum tipo que não seja necessário, deve ser tirado do ar, e, se possível, removido da instalação, ou impossibilitado de ser executado".

Regra básica número 3 de segurança em sistemas operacionais:

"Senhas ou contas de administrador ou equivalente NÃO devem ser usadas (ou apenas em algum caso onde a tarefa EXIJA tal privilégio), bem como não devem ser de conhecimento público".

Regra básica número 4 de segurança em sistemas operacionais:

"Segurança física é tudo. Somente permita ter acesso à console do servidor, aqueles que detenham acesso de administração. A grande maioria dos exploits de segurança somente funcionarão se o hacker possuir acesso físico / local à console do computador. Evite ao máximo compartilhar um computador e, se for impossível evitar, nunca digite, use ou acesse nada confidencial neste computador / servidor".

Regra básica número 5 de segurança em sistemas operacionais:

"Se um servidor for invadido, e uma conta de administrador ou equivalente for comprometida, não há forma de medir o estrago causado. Um invasor com poderes de administração poderá realizar qualquer tarefa no ambiente. Portanto, o tempo que se levará para apurar os danos será muito maior que o suportável. Colete todos os dados que achar pertinente, para apurar posteriormente a invasão, e comece do zero: reinstale o servidor".

Plataforma Windows: Windows 9x / ME

O Windows 9x / ME (95, 98 ou ME) não foi concebido com segurança em mente. Contudo, a Microsoft esqueceu que, com o advento da Internet, alguma segurança deveria existir por padrão no sistema para evitar ataques, para usuários deste sistema. De qualquer forma, existem alguns procedimentos que qualquer um pode adotar para tornar seu computador Windows 9x mais seguro. Obviamente, é praticamente impossível ter uma funcionalidade de servidor de algum tipo, exposto à Internet, aliada à segurança, com este sistema operacional.

Existem várias vulnerabilidades documentadas e bastante exploradas nesta família de sistemas operacionais. Tentar manter um computador Windows 9x/ME seguro, é relativamente possível, desde que:

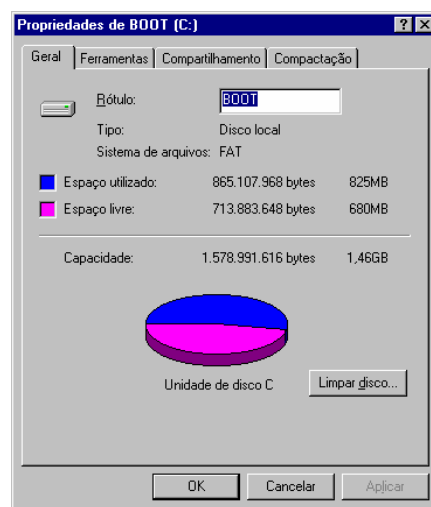
1. Não existam programas “servidores” rodando no mesmo, principalmente se forem “Microsoft”, incluindo o compartilhamento de arquivos e impressoras para redes Microsoft, ou Novell;
2. Não seja possível obter acesso a console do computador. Caso o computador seja compartilhado, esqueça qualquer tipo de segurança. Caso o computador esteja em um quiosque, cybercafé ou semelhante, devemos partir do princípio de que ele já está comprometido;
3. Caso o computador não esteja compartilhado, que possua um personal firewall instalado;
4. Caso o computador não esteja compartilhado, que possua um antivírus instalado.

Programas “servidores”

Por padrão, uma instalação default do Windows 9X não possui nenhum programa “servidor” de rede instalado. É necessária a intervenção do usuário para efetuar a instalação de algum. Neste caso, este sistema operacional não possui nenhuma segurança local, ou através de sistema de arquivos, o que torna impossível manter uma configuração segura, caso algum programa seja usado para acessar os arquivos do computador.

Como podemos ver ao lado, os sistemas de arquivos que o Windows 9x suporta são o FAT12, FAT16 e FAT32, além do CDFS (presente apenas em CDs). Nenhum destes sistemas de arquivos suporta definir permissões de acesso. Isto é uma limitação dos sistemas de arquivos, o que torna impossível definir uma “ACL” (Access Control List – lista de controle de acessos) baseada em uma lista de usuários válidos ou não.

Aliado a este fato, o Windows 9x não possui contextos de segurança associados a usuários. A funcionalidade de definição de usuários que o Windows 9x possui é apenas para diferenciar as configurações individuais de cada um, como cores, papel de parede, Menu Iniciar, etc. Baseado nisto, podemos concluir que, para o Windows 9x, a regra básica no. 5 sempre se aplica: qualquer um que tenha acesso ao sistema localmente é considerado um administrador.

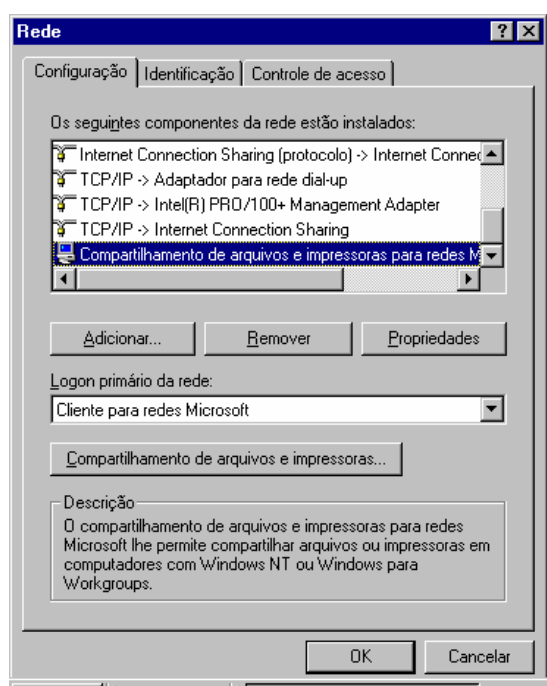


Muitos usuários deste sistema instalam componentes “servidores”, como Web Server (A Microsoft possui um para esta plataforma: chama-se Personal Web Server), servidor FTP (como o SERV-U), e o próprio Compartilhamento de arquivos e Impressoras para Redes Microsoft.

Se formos definir graus de periculosidade para estes componentes, diria que o Personal Web Server ganha disparado. Além de ser um componente que exige um conhecimento diferenciado para operar, possui diversas vulnerabilidades que tornam o computador susceptível a ataques.

Em segundo lugar, temos o Compartilhamento. Este componente de rede não é instalado por padrão, mas é muito comum usuários com pequenas redes domésticas, ou na empresa, instalá-lo para permitir a troca de arquivos na rede local.

Para instalá-lo, existem dois métodos, que resultam no mesmo efeito.

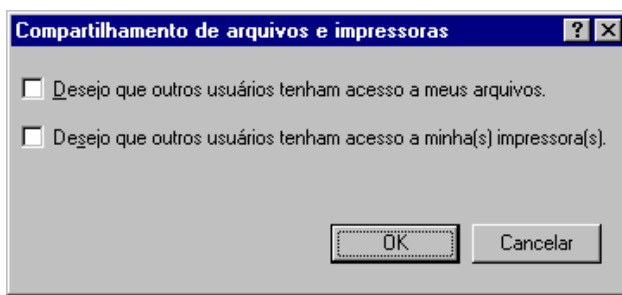


O primeiro deles, é indo às propriedades do ambiente de rede, e adicionando o serviço “Compartilhamento de Arquivos e Impressoras para redes Microsoft”, como podemos ver ao lado, através do botão “Adicionar”, opção “Serviço” / “Microsoft”, onde o componente pode ser encontrado.

O segundo método é clicando no botão “Compartilhamento de arquivos e impressoras”, que pode ser visto na imagem acima...

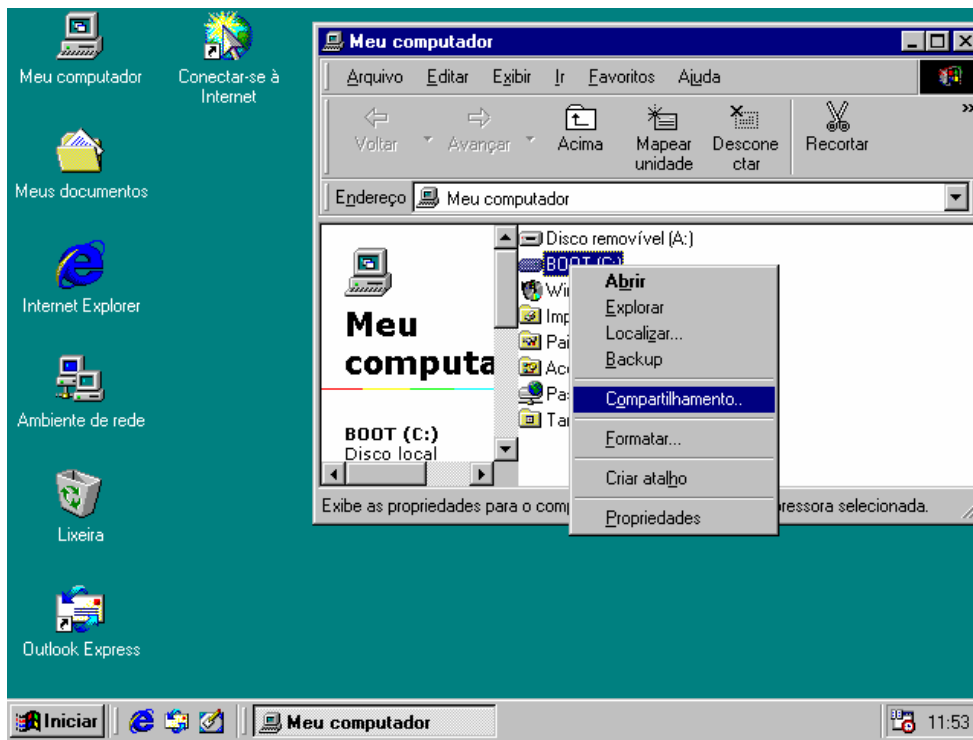
... e selecionando algumas das opções ao lado.

Em qualquer um dos casos, o componente será instalado. Porém, a instalação deste componente NÃO torna o computador vulnerável em uma rede, pelo menos não a uma invasão; apenas a ataques do tipo DoS (vide secção “Outros Tipos de Ataques” / DoS (Denial of Service Attack), pois este componente tem se provado susceptível a este tipo de ataque.



Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

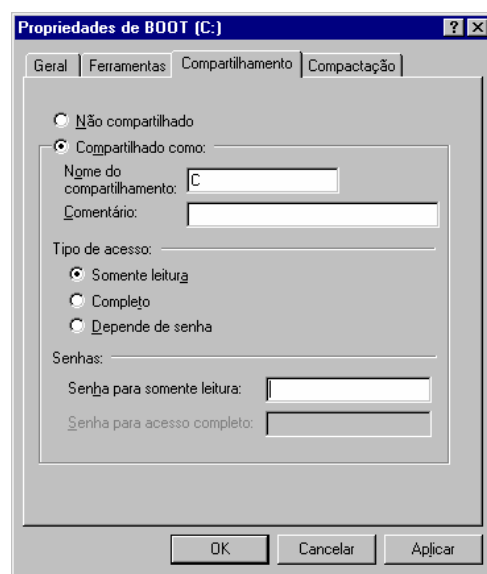
Uma vez instalado esse componente fará com que o sistema operacional torne disponível, no menu de click secundário do mouse, sobre qualquer pasta ou unidade de disco, a opção “Compartilhamento”, que pode ser vista abaixo:



Através desta opção, o usuário poderá acessar o menu ao lado...

... Que permite que o usuário compartilhe a pasta ou disco em questão para a rede.

Contudo, ao clicar em “OK”, a pasta será compartilhada para toda a rede, sem distinção de usuário ou senha. Desta forma, potencialmente qualquer outro computador que tenha contato através de qualquer tipo de rede a este computador, e que possua funcionalidades de rede Microsoft, poderá acessar a pasta.



Neste caso, a única forma de proteger este serviço, é definindo o “Tipo de acesso” como “Depende de senha”, e definindo uma senha para leitura ou escrita. Porém, apesar de definir uma senha tornar a pasta relativamente segura, nada impede que um potencial invasor tente técnicas de ataque por “força bruta”, ou seja, tentando várias combinações de senha até descobrir a mesma. E, descobrindo a senha, mesmo que seja somente a de escrita, o estrago já será imenso, como podemos ver a seguir.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

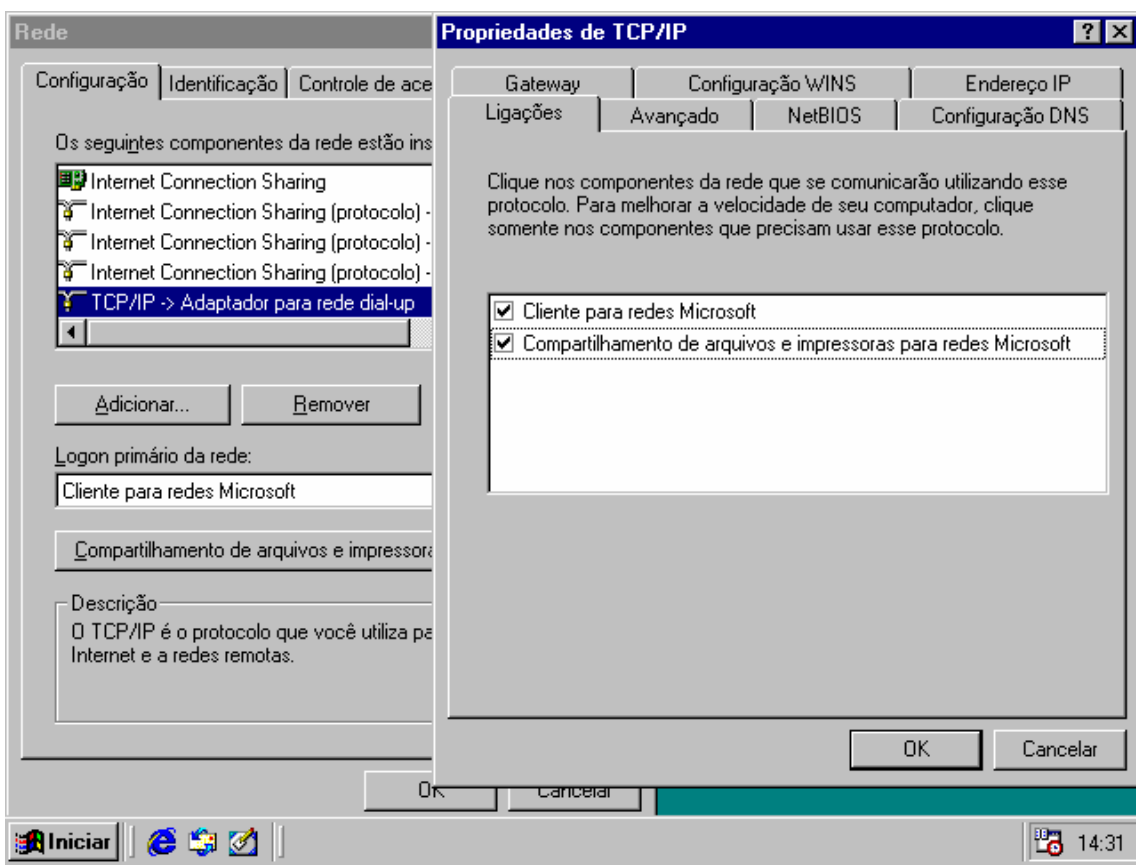
Compartilhamento através de dial-up

Se já existe o risco de um compartilhamento mal configurado ser acessado em uma rede local, imagine através da Internet. As possibilidades são as mesmas, porém, o risco é elevado em ordens de grandeza.

Qualquer componente (serviço) de rede instalado no Painel de Controle \ Redes, ou através das propriedades do Ambiente de Rede pode ou não estar associado às interfaces de rede a qual irá funcionar.

Neste caso, se um serviço estiver associado a uma interface de rede local, então a rede local terá acesso ao mesmo. Caso o serviço esteja associado ao adaptador de rede dial-up, então, a rede a qual se conectar via adaptador dial-up terá acesso também ao serviço.

Estas associações, ou “ligações”, podem ser checadas na opção de propriedades dos componentes de rede:



Ao pedir propriedades do protocolo TCP/IP, associado ao adaptador de rede dial-up, conseguimos chegar à janela de configuração que possui a ligação.

Repare que, por padrão, pelo fato do computador possuir um adaptador dial-up, e de ter instalado o compartilhamento de arquivos e impressoras para redes Microsoft, os dois estarão “ligados”. Portanto, o compartilhamento estará funcionando através da Internet, caso o adaptador dial-up (um modem, por exemplo) esteja conectado à grande rede.

Caso o computador em questão faça parte de uma rede corporativa ou doméstica, por exemplo, a check Box que associa o adaptador dial-up ao "Compartilhamento de arquivos e impressoras para redes Microsoft" DEVE ser desmarcado.

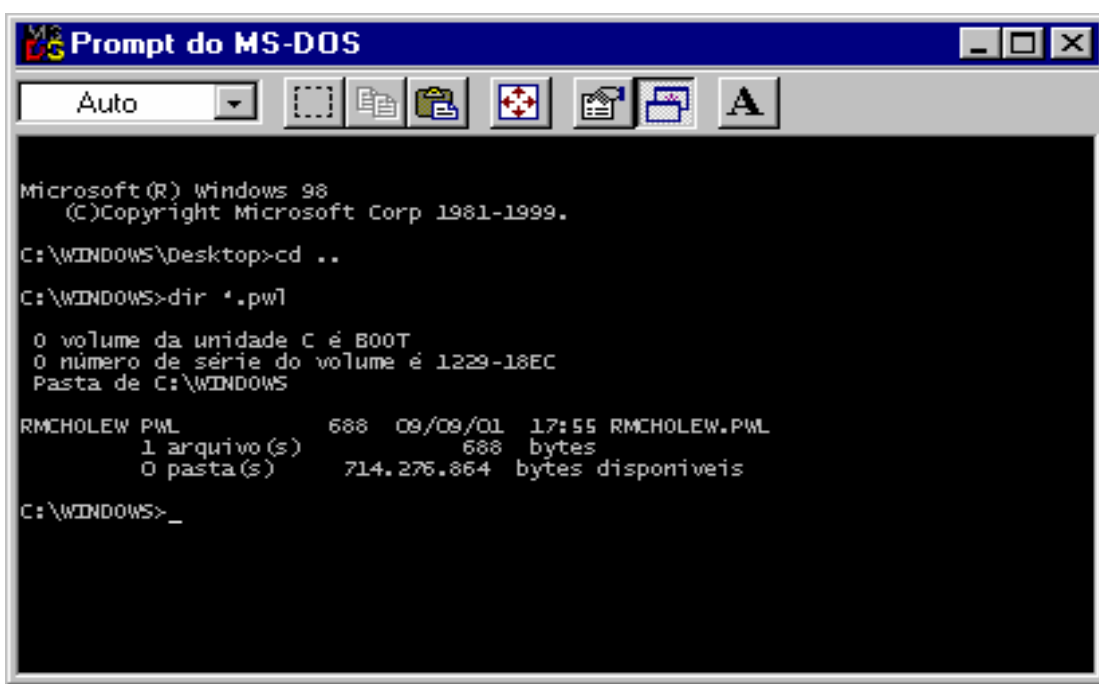
Acesso a console

É considerado “acesso a console” quando qualquer usuário pode manipular o computador a partir do próprio teclado e mouse, localmente. Em um ambiente como Windows 9x, como vimos anteriormente, por não existir definição de usuários em um contexto de segurança, bem como não existir a definição de permissões, qualquer acesso local é considerado também como acesso de administração.

Neste caso, a primeira coisa que um potencial invasor tentará é instalar um cavalo de tróia, ou “Trojan Horse”, que permitirá que o mesmo acesse este computador posteriormente, através da rede. Existem diversos cavalos de tróia disponíveis na Internet, como o Back Orifice e o Netbus, que veremos mais adiante.

Em segundo lugar, o acesso local permite que o invasor copie os arquivos .pwl. O Windows 9x, por padrão, se possuir os componentes de rede instalados, salva a lista de senhas de cada usuário, em arquivos “nomedous.pwl”, onde “nomedous” é o nome do usuário que efetuou logon, truncado em 8 caracteres, da esquerda para a direita, dentro do diretório do Windows.

Veja:



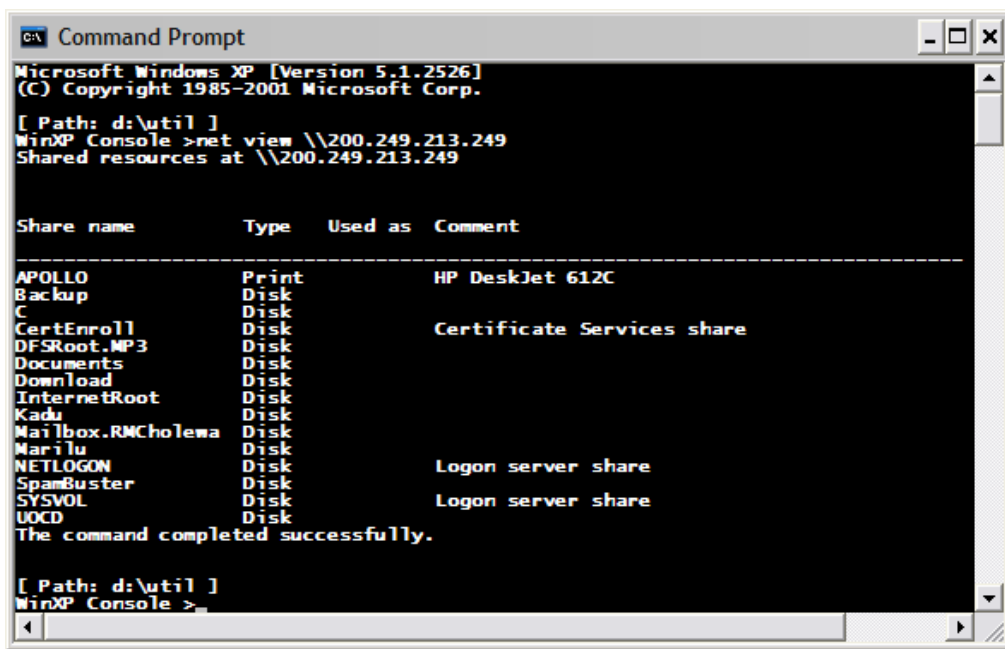
Apesar deste arquivo guardar as senhas criptografadas, a criptografia usada é muito fraca, facilmente quebrada por diversos programas que existem na Internet, justamente para este fim.

Portanto, se um invasor tiver acesso a estes arquivos, seja através de um compartilhamento, ou através da console, potencialmente terá acesso a uma lista de senhas. Aliado ao fato de que raramente usamos senhas diferentes para os diversos serviços que usamos hoje em dia, imagine o que pode ocorrer.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Voltando à questão do compartilhamento, a metodologia que provavelmente será usada para acessar uma configuração realizada de forma incorreta, poderá ser a seguinte:

Visualização dos compartilhamentos de um computador:



```
C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2526]
(C) Copyright 1985-2001 Microsoft Corp.

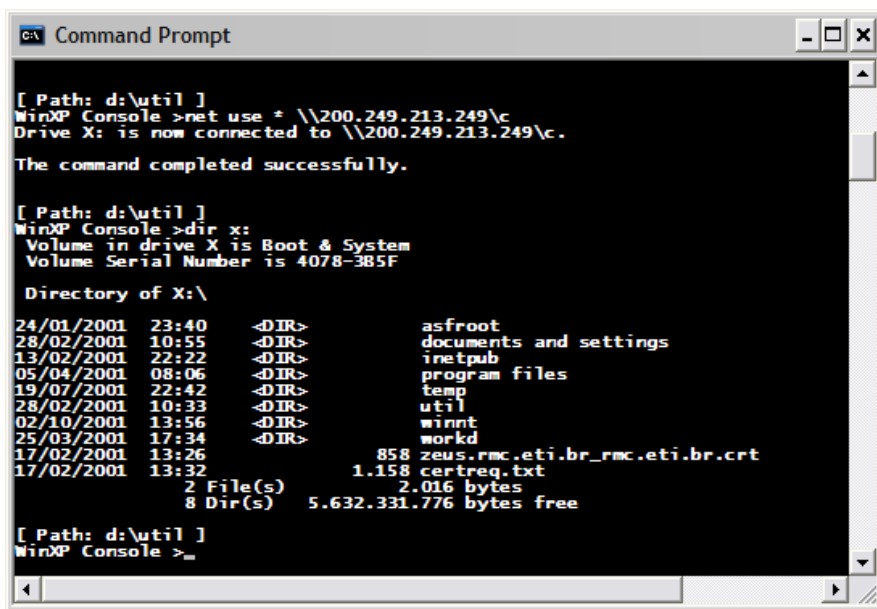
[ Path: d:\util ]
WinXP Console >net view \\200.249.213.249
Shared resources at \\200.249.213.249

Share name      Type    Used as  Comment
-----
APOLLO          Print
Backup          Disk
C               Disk
CertEnroll      Disk    Certificate Services share
DFSRoot.MP3     Disk
Documents       Disk
Download        Disk
InternetRoot    Disk
Kadu            Disk
Mailbox.RMCholewa Disk
Marilu          Disk
NETLOGON        Disk    Logon server share
SpamBuster      Disk
SYSVOL          Disk    Logon server share
UOCD            Disk
The command completed successfully.

[ Path: d:\util ]
WinXP Console >
```

Uma vez visualizados os compartilhamentos, o invasor pode simplesmente acessar todos aqueles que não possuem senha, das seguintes formas:

...Por mapeamento:



```
C:\ Command Prompt

[ Path: d:\util ]
WinXP Console >net use * \\200.249.213.249\c
Drive X: is now connected to \\200.249.213.249\c.
The command completed successfully.

[ Path: d:\util ]
WinXP Console >dir x:
Volume in drive X is Boot & System
Volume Serial Number is 4078-3B5F

Directory of X:\

24/01/2001  23:40    <DIR>      asfroot
28/02/2001  10:55    <DIR>      documents and settings
13/02/2001  22:22    <DIR>      inetpub
05/04/2001  08:06    <DIR>      program files
19/07/2001  22:42    <DIR>      temp
28/02/2001  10:33    <DIR>      util
02/10/2001  13:56    <DIR>      winnt
25/03/2001  17:34    <DIR>      workd
17/02/2001  13:26      858 zeus.rmc.eti.br_rmc.eti.br.crt
17/02/2001  13:32      1.158 certreq.txt
                2 File(s)          2.016 bytes
                8 Dir(s)      5.632.331.776 bytes free

[ Path: d:\util ]
WinXP Console >
```

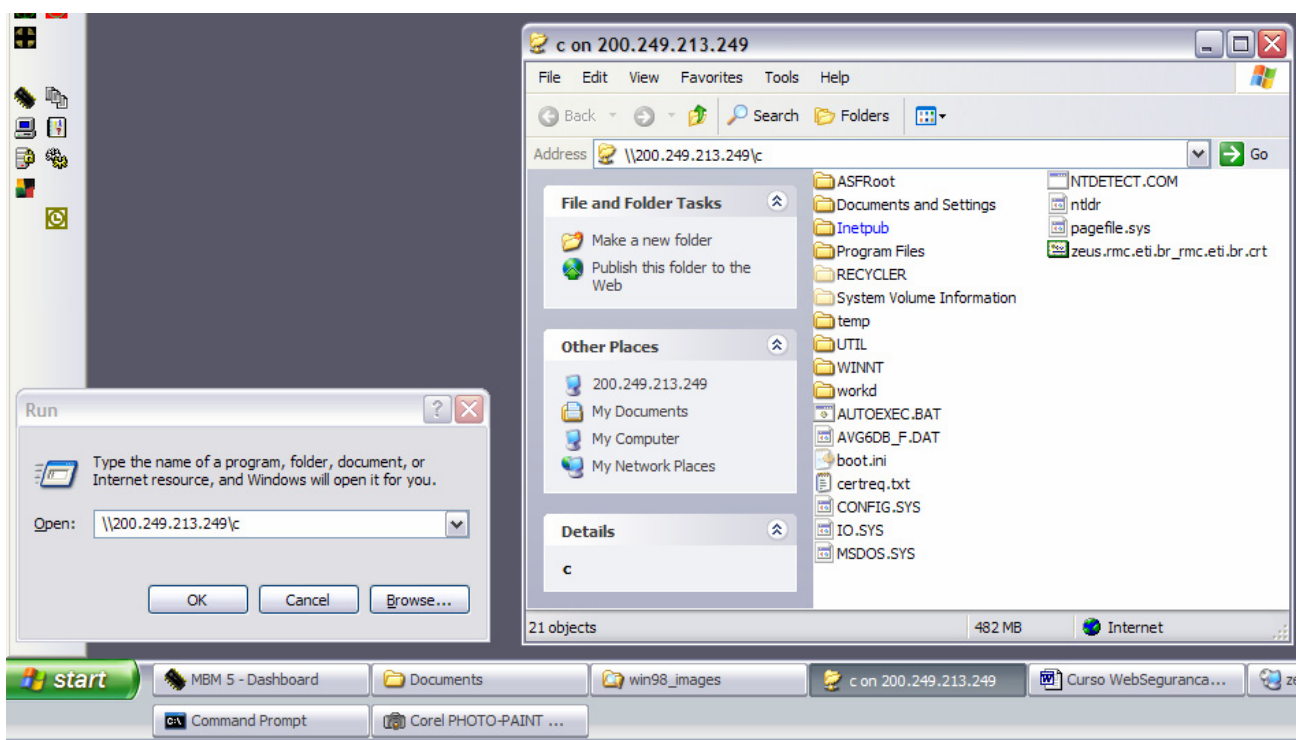
Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

A partir daí, o compartilhamento remoto do drive C: (C) foi associado ao drive local X:. Repare que todos os arquivos remotos estão acessíveis. Existem também outras informações que podem ser acessadas através do serviço de compartilhamento, descritas mais adiante em “Ferramentas” / Services Fingerprinting.

...Por interface gráfica

Através da interface gráfica se torna ainda mais fácil acessar o compartilhamento. Veja:



Botão iniciar, executar, [\\ip_remoto\compartilhamento](#) [enter] e o suficiente. Substitua “ip_remoto” pelo endereço IP do computador remoto que possui o compartilhamento a ser acessado, e “compartilhamento” pelo nome do compartilhamento.

Personal Firewall / Antivírus

Estes dois temas serão abordados em outra secção (Ferramentas) mais adiante. Contudo, são de primordial importância. Estudos comprovam que, hoje em dia, cerca de 80 a 90% das infecções por vírus ou cavalos de tróia se dão através de correio eletrônico. Portanto, um bom antivírus poderá detectar, corrigir ou eliminar uma mensagem que contenha um vírus ou cavalo de tróia, assim como um personal firewall poderá potencialmente evitar que, uma vez instalado, o vírus ou cavalo de tróia funcione através da rede (apesar de não impedir o efeito destrutivo que um vírus pode potencialmente carregar localmente, como deleção ou corrupção de dados).

Programas e aplicativos iniciados automaticamente

Finalmente, um aspecto que deve ser checado é em relação a que serviços seu computador está iniciando automaticamente ao ser ligado / inicializado. Olhe dentro do grupo “Iniciar” por programas estranhos. Também verifique se existe, dentro da pasta/diretório do Windows, um arquivo chamado

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

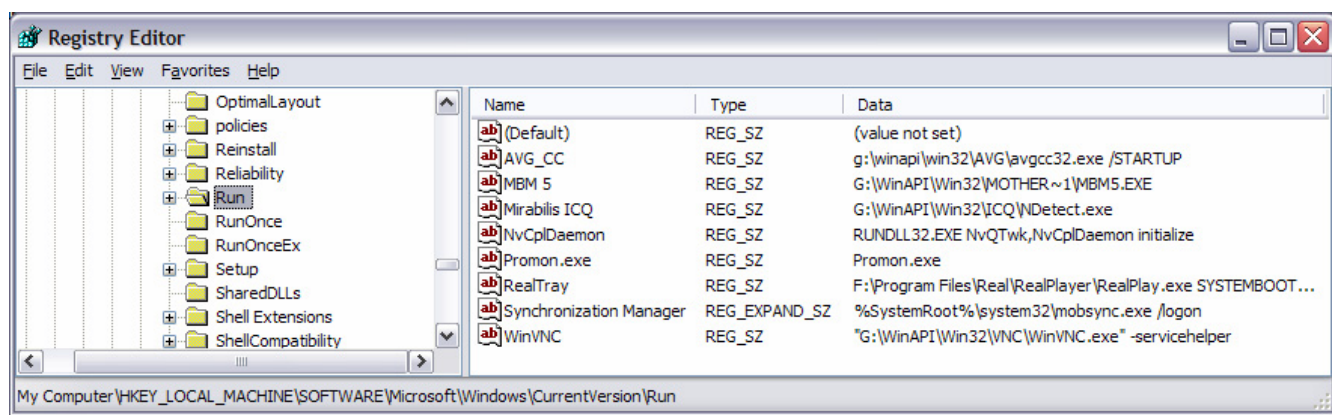
“winrun.bat”. Qualquer “ícone” ou programa dentro do grupo Iniciar (StartUp), bem como qualquer linha de comando dentro do arquivo “winrun.bat”, será executado quando o sistema carregar (o winrun.bat é executado quando o sistema carrega a interface gráfica – herança do Windows 3.x. O grupo “Iniciar” é executado quando o usuário efetua logon, ou se identifica. Caso o Computador não esteja configurado para múltiplos usuários, ou não participe de uma rede local, ele é executado como parte da carga da interface personalizada do computador.

Também é possível iniciar programas e aplicativos direto do registro. As chaves:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run ... Especificam que programas serão executados quando o Windows carregar.

Por padrão, apenas o systray e algum programa anti-virus devem estar listados. Se em algumas destas linhas está aparecendo algum programa que você tenha baixado da Internet recentemente, é aconselhável instalar um anti-virus atualizado o mais rápido possível. Provavelmente é um cavalo-de-tróia.

Veja:



Neste caso, estão listados:

AVG_CC: Antivírus
MBM 5: Programa de monitoração da CPU (temperatura, voltagem, etc.)
Mirabilis ICQ: Programa de mensagens instantâneas – ICQ
NvCplDaemon: Programa de controle da placa de vídeo
Promon.exe: Programa de controle da placa de rede
RealTray: RealPlayer
Synchroni...: Componente do Windows XP
WinVNC: Programa para acesso remoto à console do computador

Perceba que nenhum dos programas acima é um cavalo de tróia. Contudo, se verificar a existência de alguma linha que aponte para um arquivo recuperado da Internet recentemente, deve executar um antivírus urgente.

Indo um pouco mais além, você pode executar o comando “netstat -an” para verificar se seu computador está configurado para “escutar” em alguma porta suspeita. Isto também pode indicar algum cavalo-de-tróia.

Ao digitar o “netstat -an” você terá como resposta algo assim:

```
C:\WINDOWS\Desktop>netstat -an
```

Conexões ativas

| Proto | Endereço local | Endereço externo | Estado |
|-------|---------------------|------------------|-----------|
| TCP | 200.249.213.241:137 | 0.0.0.0:0 | LISTENING |
| TCP | 200.249.213.241:138 | 0.0.0.0:0 | LISTENING |
| TCP | 200.249.213.241:139 | 0.0.0.0:0 | LISTENING |
| UDP | 200.249.213.241:137 | *:* | |
| UDP | 200.249.213.241:138 | *:* | |

```
C:\WINDOWS\Desktop>
```

Essa é a típica resposta de um computador com uma placa de rede, que não está conectado à Internet, e que acabou de ser iniciado. Note que ele está escutando nas portas 137, 138 e 139. Para um computador Windows 9x, isso é normal. Contudo, se você não realizou a instalação de nenhum programa de rede em seu computador que o transforme em algum tipo de servidor, e ainda assim portas estranhas aparecerem listadas, isto quer dizer que algo está errado. Uma lista de portas que indicam cavalos-de-tróia pode ser encontrada no anexo 3. Porém, alguns destes cavalos-de-tróia usam portas que por padrão, são usadas por serviços conhecidos, como FTP – File Transfer Protocol (porta 20 e 21), HTTP – Hypertext Transfer Protocol (porta 80) e assim por diante. Portanto, antes de imaginar que está infectado, certifique-se de que tais serviços não estejam rodando em seu computador. Uma lista com as portas privilegiadas (conhecidas como “Well known port numbers”) pode ser encontrada no anexo 4, bem como uma lista de portas não privilegiadas, acima de 1024, podem ser encontradas no anexo 5. Caso o material não esteja à mão e uma consulta seja necessária, dentro da pasta “\WINDOWS\” (Windows 9x) ou “\WINNT\SYSTEM32\DRIVERS\ETC” (Windows NT/2000) existe um arquivo chamado “services” que contém as principais portas.

Plataforma Windows NT / 2000 / XP

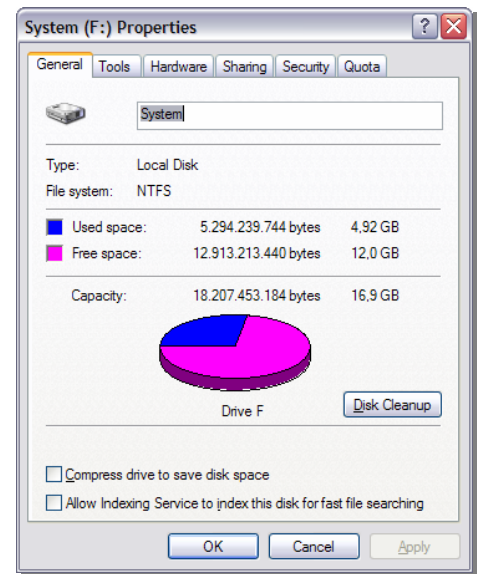
O Windows NT/2000/XP foi concebido para suportar e operar sobre padrões de segurança, ao contrário do Windows 9x. A intenção deste material não é escrever um tutorial de segurança no Windows NT/2000/XP, pois isso forçaria a escrita de um material inteiramente novo. Porém, existem alguns tópicos que podem e devem ser abordados, que contêm conceitos básicos de proteção usando este sistema operacional.

A principal diferença em termos de segurança do Windows NT/2000 para o 9x, nós podemos reconhecer logo no início: apenas um usuário válido pode usar o computador localmente, bem como via rede, de acordo com as permissões configuradas. Você precisa ser autenticado para ter acesso a console. Portanto, manter um cadastro de usuários é necessário. Este cadastro deve forçar os usuários a trocar de senha periodicamente, bem como exigir que senhas de um determinado tamanho mínimo sejam usadas (em sistemas seguros, é recomendado usar o máximo de caracteres suportados pelo NT: 14. No caso do 2000/XP, também podemos usar 14, pois é um bom valor. Contudo, o Windows 2000 permite senhas de até 256 caracteres).

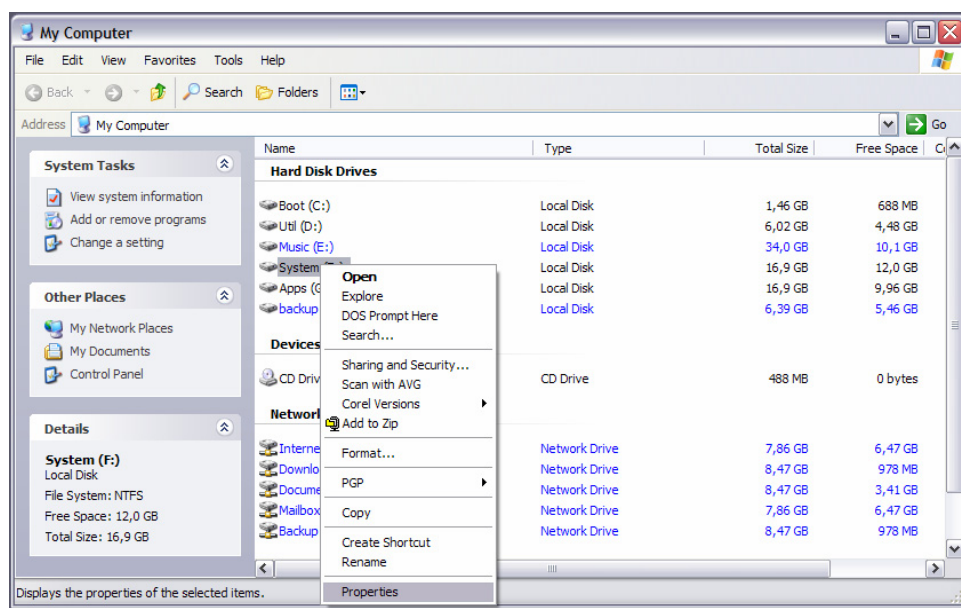
A primeira coisa que se deve fazer ao usar NT/2000/XP é escolher que sistemas de arquivos você usará. Se segurança é um requisito, o sistema NTFS deve ser usado. Contudo, o sistema NTFS não será visível por outro sistema operacional, apenas pelo NT/2000/XP (O Linux pode enxergar partições NTFS para leitura).

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Este sistema de arquivos nativo do NT/2000/XP permite a definição de uma “ACL”, ou lista de controle de acesso, baseada nos usuários que existem cadastrados no computador, ou servidor de rede. Assim, você poderá especificar quem pode acessar que arquivo, com que nível de permissão, mesmo localmente.



As permissões podem ser definidas através da janela de propriedades de qualquer disco, diretório/pasta ou arquivo que esteja em um sistema NTFS...

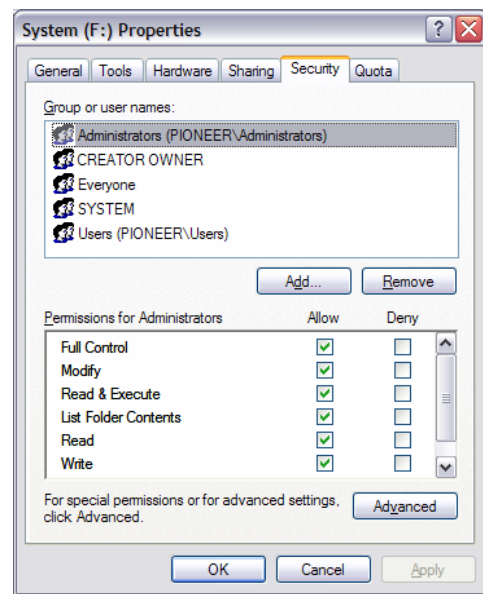


Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

... e escolhendo a tab “Security” ou “Segurança”.

Nesta tab, você pode definir todas as permissões que cada usuário ou grupo de usuários terá sobre o objeto. Poderá também escolher se este objeto receberá suas permissões por herança, a partir do objeto acima na hierarquia, como também, se deseja que as permissões sejam diferentes deste ponto em diante.

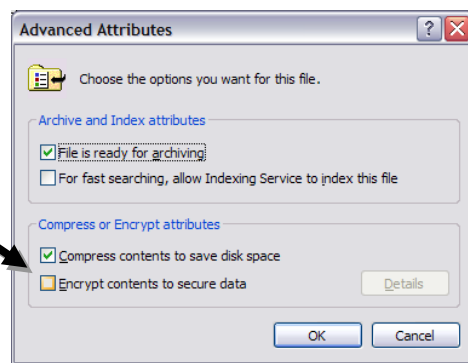
Além disso, cada usuário pode ter permissões individuais, e com características diferentes.



Outra possibilidade que o Windows 2000 / XP traz é a criptografia de um arquivo ou diretórios, bastando ir à mesma janela de propriedades, botão avançado, e marcando a opção correspondente.

Ao clicar nesta opção, o Windows irá criptografar o arquivo ou pasta, com a chave de criptografia do usuário atualmente “logado”. Isto tornará o arquivo ou pasta virtualmente impossível* de ser acessado por outro usuário, MESMO que a unidade de disco seja removida e colocada em outro computador.

* desde que a opção de recuperação de emergência esteja desabilitada.



Porém, deve se ter bastante cuidado com mudanças de permissões em arquivos do sistema, assim como criptografia. Alterar as permissões de um arquivo usado pelo NT / 2000 / XP pode tornar o computador inutilizável, pois o próprio sistema não terá permissão para acessar os arquivos. Em caso de dúvida, devem-se sempre adicionar permissões de leitura e escrita também para o item “SYSTEM”, que representa o próprio sistema operacional.

Quanto ao recurso de criptografia, deve ser usado apenas em arquivos de dados.

Outro ponto que deve ser observado é: caso seja usuário de um sistema Windows NT 4.0. Ao se converter uma partição para NTFS, as permissões estarão “em branco”. A seguinte tabela demonstra as permissões que podem ser aplicadas, segundo recomendação da própria Microsoft:

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

| Pasta | Permissão |
|--------------------------------|---|
| \\WINNT e todas as sub-pastas. | Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control |

Uma vez aplicadas as permissões acima, as seguintes permissões devem ser feitas:

| Pasta | Permissão |
|---|--|
| \\WINNT\\REPAIR | Administrators: Full Control |
| \\WINNT\\SYSTEM32\\CONFIG | Administrators: Full Control CREATOR OWNER: Full Control Everyone: List SYSTEM: Full Control |
| \\WINNT\\SYSTEM32\\SPOOL | Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read Power Users: Change SYSTEM: Full Control |
| \\WINNT\\COOKIES \\WINNT\\FORMS \\WINNT\\HISTORY \\WINNT\\OCCACHE \\WINNT\\PROFILES \\WINNT\\SENDTO \\WINNT\\Temporary Internet Files | Administrators: Full Control CREATOR OWNER: Full Control Everyone: Add System : Full Control |

Observação: as permissões acima só necessitam ser aplicadas caso o computador em questão possua o Service Pack 5 ou anterior.

Caso deseje rever as permissões de um ambiente Windows 2000, a tabela acima pode servir de guia, apenas alterando o diretório “\\WINNT\\PROFILES” para “\\Documents and Setings” na mesma partição em que o sistema está instalado.

Também é recomendado que, caso deseje testar permissões em arquivos de sistema, que seja feito em um computador para esta finalidade, pois como visto anteriormente, a aplicação de uma ACL incorreta em arquivos usados pelo sistema operacional pode deixar o computador bloqueado. Neste caso, o disco com o sistema deve ser colocado em outro computador com o mesmo sistema operacional, e ter suas permissões revogadas para “Everyone – full Control”

Auditoria

Em um sistema seguro, é primordial que exista algum tipo de auditoria, onde certos erros de permissão sejam armazenados para análise. É recomendado que no NT/2000/XP, todos os objetos sejam auditados quanto à falha de acesso. No caso do objeto “Logon/Logoff”, é também recomendado que o sucesso seja auditado, para que uma análise de quem efetuou ou não logon no computador, localmente ou via rede, seja possível. Não acione a auditoria em processos ou em arquivos, a não ser que seja para depuração de um problema de segurança eminente. Estes dois objetos causam muita atividade de log, deixando o computador / servidor mais lento.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Parando / desabilitando serviços desnecessários

Alguns serviços que são instalados por padrão são considerados ou vulneráveis a ataque, ou serviços que podem divulgar informações reservadas do sistema, via rede. É recomendado parar tais serviços para impedir que isto ocorra.

Os seguintes serviços precisam ser parados, e configurados para inicialização Manual:

Alerter

Permite que um suposto “hacker” envie mensagens de alerta para a console

Messenger

Permite que um suposto “hacker” via rede visualize o nome do usuário atualmente logado na console, através do comando nbtstat. Isso dá ao “hacker” um nome de usuário válido para um ataque de força bruta em sua senha.

Clipbook Server

Permite que um usuário via rede visualize o conteúdo da área de trabalho

Index Server

É um serviço geralmente instalado juntamente com o pacote de serviços de Internet (Option Pack no caso do Windows NT 4.0), ou por padrão, no Windows 2000/XP. Permite a pesquisa via string de texto em qualquer arquivo indexado. É recomendado não usar tal serviço (no Windows 2000/XP, se chama “Indexing Service”). Vulnerabilidades conhecidas, como o caso do CodeRed I e II, worm que assolou a Internet em Julho de 2001, são baseadas em falhas deste componente.

Spooler / Print spooler

É o serviço de impressão. Em servidores que ficam expostos à Internet diariamente, e não possuam nenhum serviço de impressão ativo, é recomendado que seja desabilitado (no Windows 2000/XP, se chama “Print Spooler”). Existem ataques do tipo DoS contra este serviço.

SNMP Service / SNMP Trap Service

São dois serviços que permitem a utilização do Simple Network Management Protocol. Se não possuírem uma intenção específica (como instalado pelo administrador para monitoração do computador) ou se não estiver corretamente configurado, podem revelar muitas informações sobre o computador em si, como interfaces de rede, rotas padrão, entre outros dados. É recomendado ter cautela com tais serviços. Mesmo que exista a necessidade de monitorar, por exemplo, o tráfego nas interfaces de rede, neste caso, é recomendado que o tráfego seja monitorado a partir do switch ou roteador.

Perceba que não existem falhas correntes publicadas para este serviço, mas o seu uso em si pode divulgar informações sobre o computador. Maiores detalhes em “Ferramentas” / Services Fingerprinting.

Scheduler

É um serviço que permite o agendamento de tarefas no sistema. Você pode programar para que tarefas sejam executadas numa determinada hora. Cuidado: por padrão, qualquer programa iniciado pelo sistema de agendamento, possuirá o contexto de segurança do próprio sistema, tendo acesso à praticamente qualquer informação (no caso do Windows NT 4.0). Caso seja realmente necessário, crie um usuário sem direitos (com direito apenas de executar a tarefa desejada) e programe este serviço para ser iniciado no contexto de segurança deste usuário criado. Em relação ao Windows 2000 e ao XP, não existe esta preocupação. Contudo, não é recomendado dar ao grupo “Server Administrators” o poder de agendar tarefas. Apenas o administrador deve possuir este direito. (no Windows 2000, o serviço se chama “Task Scheduler”).

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

No Windows XP, parar este serviço pode prejudicar a performance do sistema. Diversas tarefas internas de otimização de performance, como desfragmentação das unidades de disco são agendadas através deste serviço. Portanto, no caso específico do Windows XP, não é recomendado pará-lo.

Em computadores que são usados exclusivamente em casa, e que não participam de nenhuma rede, apenas acessam a Internet através de um modem, é recomendado também parar os seguintes serviços:

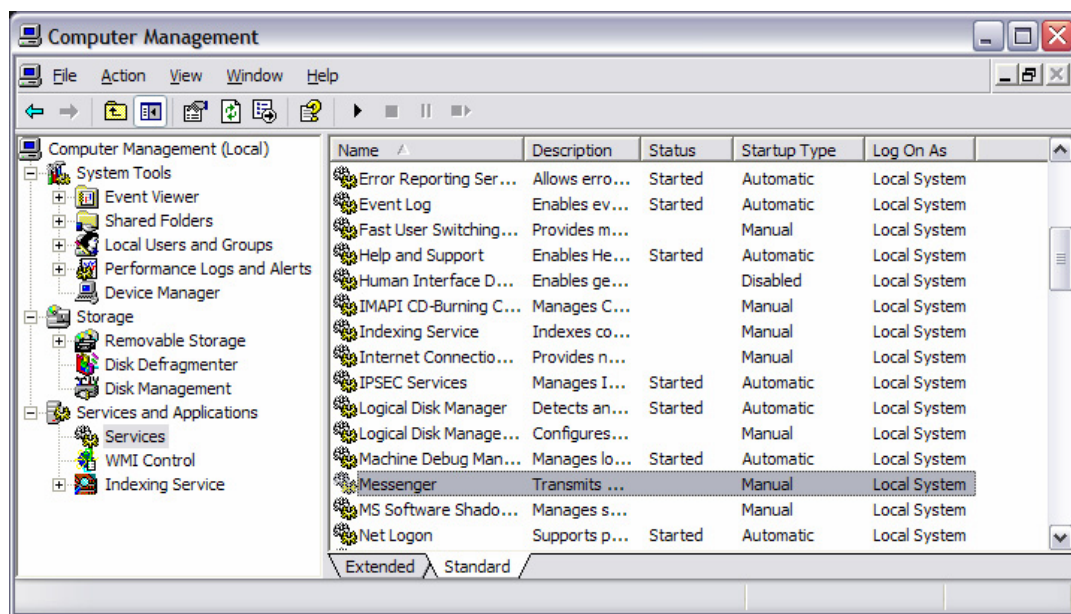
Computer Browser

Serviço essencial a uma rede Microsoft. Permite que este computador seja eleito um “Browser Master”, ou controlador de lista de recursos de um grupo de trabalho ou domínio. Numa configuração de apenas uma máquina, não é necessário estar no ar.

Server

O “Server Service” é o equivalente no Windows NT/2000, ao “Compartilhamento de arquivos e impressoras para redes Microsoft”, do Windows 9x. Da mesma forma, se seu computador não participa de nenhuma rede, e apenas acessa a Internet via modem, este serviço pode ser parado, e configurado para não iniciar automaticamente, assim como os demais.

Para interromper os serviços, no Windows NT 4.0, basta ir ao painel de controle, “Serviços”. No caso do Windows 2000 / XP, clique com o botão direito no “Meu Computador”, escolha “Gerenciar”. Depois, expanda a opção “Serviços e aplicativos”. Veja:



Alteração das configurações de rede

Caso você se enquadre no tipo de usuário que possui um computador Windows NT, sem estar conectado a nenhuma rede, e apenas acessa a Internet via modem, este passo não é necessário. Contudo, caso seu computador faça parte de uma rede, os serviços “Computer Browser” e “Server” não deverão ser parados (consulte o administrador da rede antes de realizar tais alterações, caso o computador esteja no trabalho). Mesmo assim, é possível se proteger contra suas vulnerabilidades.

No painel de controle, escolha a opção “Redes” (Network). Na última opção, em “Ligações” (Bindings), escolha no campo “Mostrar as ligações para” (Show bindings for), a opção “Todos os adaptadores” (All adapters).

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Se seu acesso à Internet estiver corretamente configurado, pelo menos duas das opções deverão ser “Remote Access WAN Wrapper”. Expanda as duas (clcando no sinal de +). Na opção que possuir “Cliente WINS (TCP/IP)” (WINS Client (TCP/IP)), clique em cima, e depois, no botão “Desabilitar” (Disable).

Os serviços “SNMP” e “Simple TCPIP Services” podem ser facilmente removidos, caso tenham sido instalados e não estejam em uso. Para isso, no caso do Windows NT 4.0, basta ir ao ícone “Rede” no painel de controle, ir às configurações de serviços, e removê-los.

No caso do Windows 2000 ou XP, deve-se ir ao painel de controle, “adicionar e remover programas”, “instalação do Windows”, e removê-los.

Além destas configurações básicas de segurança, é bom manter em mente o fato de que o Windows NT / 2000 / XP é vulnerável a ação de alguns vírus e cavalos-de-tróia, assim como qualquer sistema operacional. Usar por padrão um bom software antivírus é uma boa medida, caso tenha o hábito de usar o computador “logado” como administrador ou equivalente.

O Windows XP possui incorporado ao sistema funcionalidades de firewall. Veja a seção “Ferramentas” / Personal Firewalls para maiores detalhes.

Instant Messaging

Existem diversos programas desta categoria na Internet. A maioria deles possui a função básica de permitir a troca rápida de mensagens entre dois computadores ou mais. Muitos também possuem funções que permitem troca de arquivos e imagens, e até voz pela Internet. Vejamos os três mais usados: ICQ (I Seek You), AIM (Aol Instant Messenger) e o MSN Explorer.

ICQ (I Seek You)

O ICQ é o programa mais usado da Internet, depois do browser, com dezenas de milhões de usuários no mundo inteiro. Foi criado por uma empresa de Israel, chamada Mirabilis que, posteriormente, foi comprada pela AOL (Amer Online). É um programa de mensagens instantâneas: permite que você envie mensagens em tempo real para qualquer um em sua lista de contatos. Além de mensagens, você pode realizar um bate-papo (chat) ou enviar e receber arquivos. Contudo, o programa tenta deixar bem claro para seu usuário que ele não possui nenhuma pretensão de ser seguro. Ao realizar uma instalação padrão do ICQ, várias telas de aviso serão mostradas ao usuário, deixando claro que o programa não é seguro. De qualquer forma, continua sendo usado por todos, principalmente por ser gratuito.

<http://www.icq.com>

Infelizmente, todos os avisos que o programa nos mostra relativos à segurança são verdadeiros, e algumas medidas de precaução são interessantes ao se fazer uso deste programa. A principal medida deve ser com relação a que informações pessoais colocar na configuração do sistema, pois a maioria das informações estará disponível para outros usuários do ICQ. Evite colocar informações pessoais como endereço residencial, telefone, ou mesmo endereço de correio eletrônico principal (é sempre uma boa medida ter uma conta em algum serviço de correio free, como hotmail.com, para estas ocasiões). Muitas pessoas na Internet usam aquelas informações, principalmente o endereço de correio eletrônico, para envio de SPAM.

Em seguida, configure seu ICQ para NÃO mostrar seu endereço IP. Isso torna muito mais fácil para um suposto “hacker” tentar invadir seu computador (tudo começa pela obtenção de um endereço IP). Mesmo assim, existem formas de se descobrir o endereço IP de alguém, mesmo que ela tenha configurado seu ICQ para não mostrá-lo. Ao enviar ou receber uma mensagem, seu computador terá uma conexão estabelecida

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

com o computador do outro usuário. Assim, um simples comando `netstat -an` revelará o endereço IP. Para testar:

- Abra uma sessão DOS, e digite no prompt: `netstat -an`
- Envie uma mensagem para quem você deseja descobrir o endereço IP
- Novamente, digite no prompt: `netstat -an`

(você pode até usar um programa que seja mais prático do que o `netstat` na linha de comando, como o Netmon – discutido na seção “Ferramentas” / Services Fingerprinting)

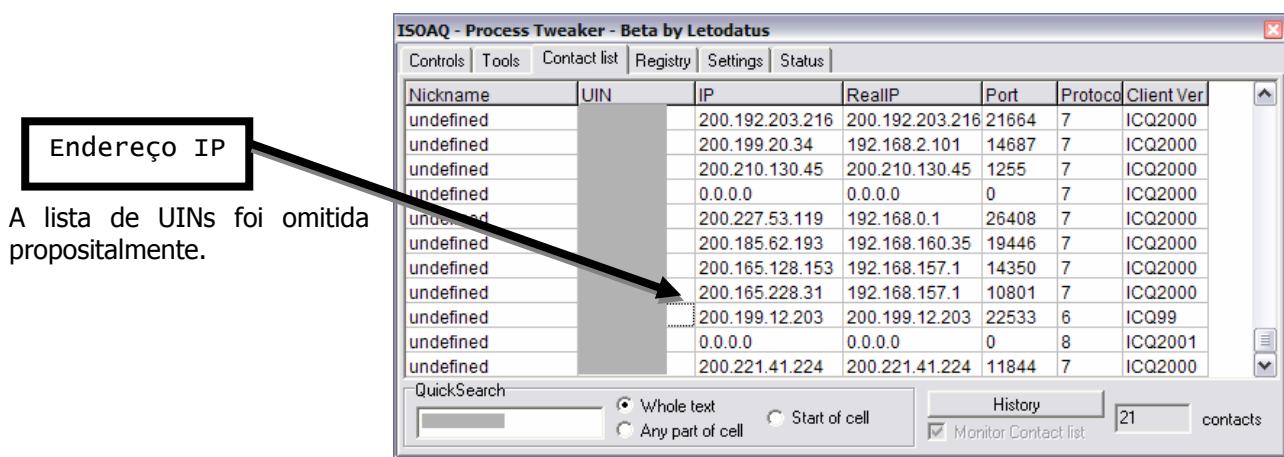
O novo endereço que aparecer, será o endereço IP do outro usuário, para quem enviou a mensagem.

Outra forma, mais prática, é usar uma ferramenta como o ISOAQ. Feito para versões antigas do ICQ, ainda funciona muito bem para esta finalidade, como podemos ver:



No. ICQ

O nome e o UIN foram omitidos propositalmente.



Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

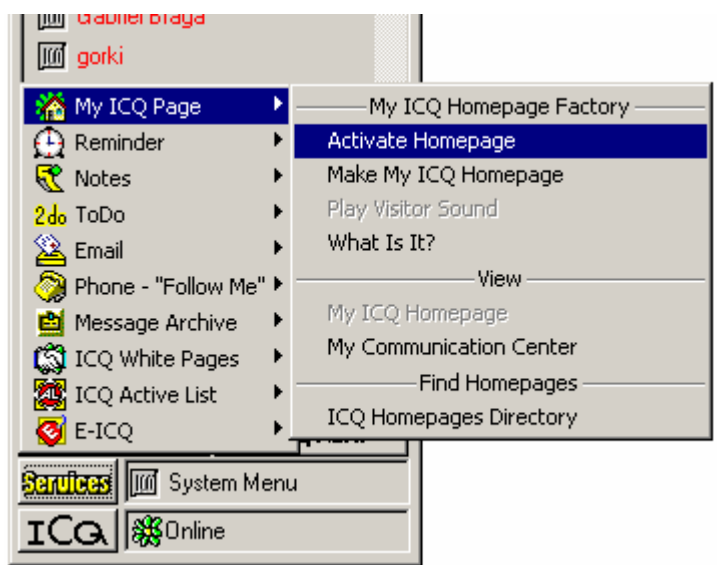
Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Perceba que este programa fornece todos os endereços de todos em sua contact list, desde que estejam conectados. Também fornece a versão do ICQ que cada um usa, obviamente, os endereços IP, entre outras coisas.

Ele pode ser baixado de: <http://isoaq.hosted.ru/index.html>

Existem ainda outras configurações de segurança dentro do ICQ, que dificultam o trabalho de alguém que tente lhe prejudicar. Existem algumas falhas no ICQ e alguns serviços que NÃO devem ser usados. A principal falha é o servidor Web que o ICQ possui incorporado. Este servidor web permite que pessoas se conectem a seu computador, e JAMAIS deve ser usado...

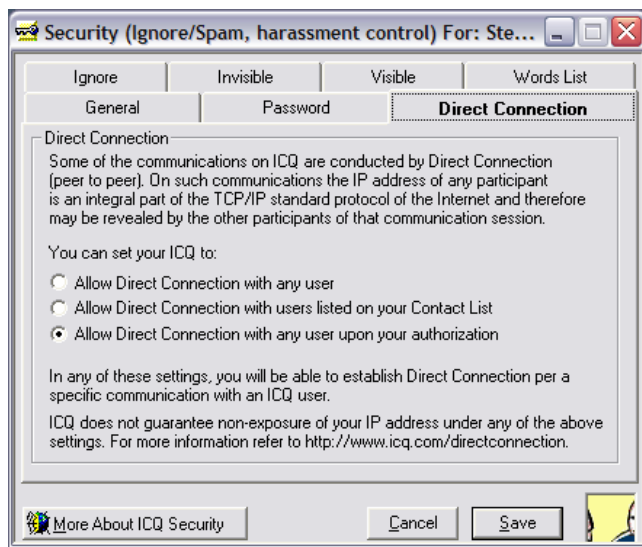
...Uma falha no programa permite que alguém acesse qualquer conteúdo do seu disco, onde o ICQ estiver instalado. Portanto, deixe esta opção abaixo sempre desligada (Services, My ICQ Page, Activate Homepage – ela está presente em versões antigas do programa):



Esta opção apenas está disponível em versões antigas. Na versão mais recente, a opção chama-se “My ICQ Web Front”.

Existem algumas outras opções rudimentares de segurança no ICQ, que devem ser usadas, como, por exemplo, ignorar um usuário (qualquer contato que seja indesejado será ignorado caso seja configurado nesta lista).

Nesta opção ao lado, o usuário pode escolher o nível de segurança, se sua autorização é requerida para adição na lista de alguém, se permite uma conexão direta com outros usuários, e se o seu status será publicado na Web, em cada uma das tabs de opções.



Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

AIM (Aol Instant Messenger)

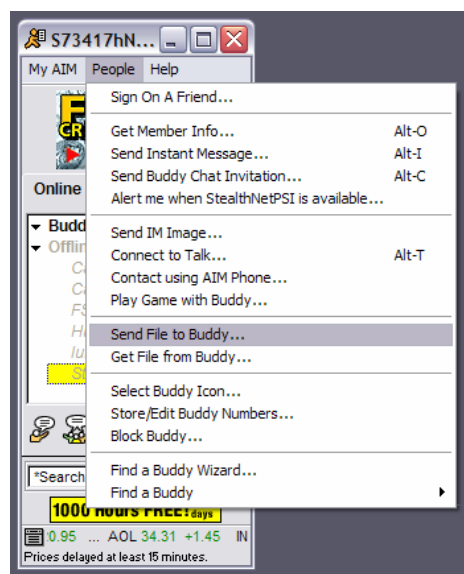
Por design, o AIM é mais seguro que o ICQ. Obviamente, se todas as medidas forem tomadas, o ICQ pode ser tão seguro quanto qualquer outro software de mensagens instantâneas. Contudo, o AIM não permite conexões diretas entre usuários.

Cada cliente AIM se conecta aos servidores da América Online, e envia mensagens através dele. Assim, fica mais difícil de descobrir o endereço IP de alguém.

Porém, o AIM possui uma função para envio de arquivos, e imagens na própria janela do programa. Ao escolher esta opção, o programa fechará uma conexão diretamente com a pessoa na qual está conversando, e deseja enviar/receber o arquivo ou imagem.

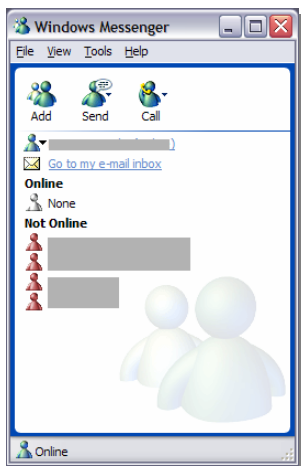
Esta opção habilita a conexão direta. De qualquer forma, se o usuário desejar enviar um arquivo, seja através do menu ao lado, ou arrastando uma imagem para a tela de Chat, o programa irá adverti-lo que, para continuar, uma conexão será estabelecida diretamente entre os dois computadores.

Pelos motivos explicados anteriormente, este tipo de função deve ser evitado.



Windows Messenger

A Microsoft obviamente descobriu o mercado para os programas de mensagens instantâneas, e embarcou nele. O software da Microsoft chama-se Windows Messenger, e usa como protocolo de comunicação apenas http (o mesmo usado para o serviço web – de páginas).



O Windows Messenger, por ser o mais simples, trazendo menos recursos, é um dos menos susceptíveis a falhas. Ele também usa o princípio do AIM, onde a mensagem circula através do servidor que provém a infra-estrutura. Vantagem de ambos, pois a lista de contatos fica guardada lá, e não se perde.

Porém, ele possui uma função de conversação, onde é possível estabelecer contato com alguém de sua lista via voz, como em um telefone, usando os recursos multimídia do computador. Ele também permite enviar e receber arquivos. Nestes casos, uma conexão direta entre os dois computadores será estabelecida, e será possível descobrir o seu endereço IP. Devem ser evitados.

Em todos os casos, a principal preocupação com os serviços de mensagens instantâneas é a divulgação de seu endereço IP. No caso do AIM e do MSN Explorer, isto pode ser ainda evitado, com algumas medidas simples, como vimos. Já o ICQ, por ser o mais usado em todo o mundo, e o mais complexo, é o que reúne o maior potencial para insegurança.

Contudo, deve ficar claro que todos eles, corretamente configurados, podem ser usados. Lembre-se que, qualquer um que receba um arquivo que seja um cavalo de tróia, e o execute, não poderá colocar a culpa no método usado para compartilhá-lo. Neste caso, é apenas uma questão de educação e hábito.

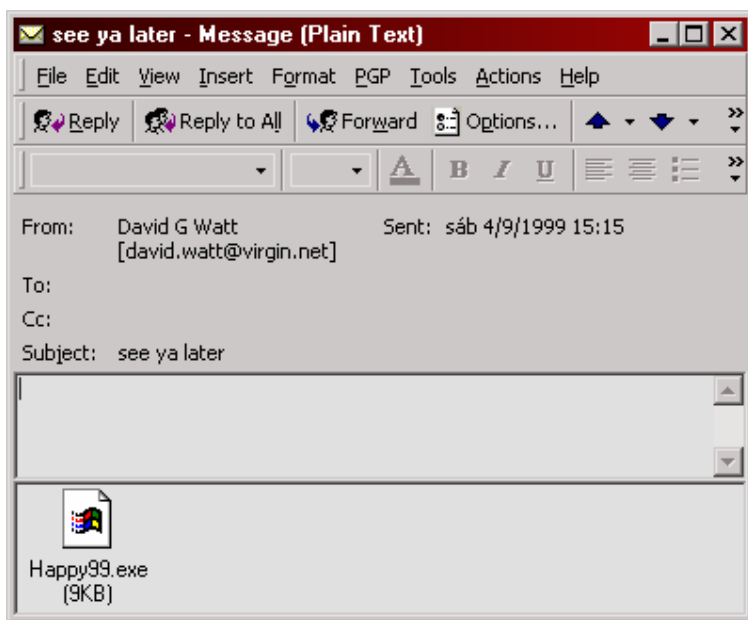
Correio Eletrônico

O correio eletrônico, hoje em dia, é claramente o meio mais usado para disseminação de vírus e cavalos-de-tróia. O email de certa forma é uma aplicação bastante invasiva hoje em dia, e, por este motivo, todo cuidado é pouco ao receber qualquer mensagem que seja, com um arquivo anexo. A maioria dos usuários de rede e Internet hoje no mundo todo, acessam suas contas de correio através de um protocolo de recepção de mensagens chamado POP3 (Post Office Protocol v. 3). Este protocolo, aliado à configuração padrão da maioria dos programas clientes de correio, faz com que, ao checar sua caixa postal, todas as mensagens sejam baixadas de forma não interativa. Caso algum dos correios esteja infectado com um script ou cavalo-de-tróia, o usuário somente saberá quando o correio já estiver dentro de sua caixa postal local.

Assim sendo, é muito comum o usuário, movido pela curiosidade, tentar abrir qualquer documento anexo à mensagem. Boa parte dos cavalos-de-tróia são programinhas gráficos apelativos, com mensagens que alimentam a curiosidade do usuário, como pequenas animações, desenhos, ou coisas do gênero. Ao executar algum programa destes, o usuário tem a impressão de que nada ocorreu. Contudo, o cavalo-de-tróia tem uma segunda função, que geralmente abre o computador para um ataque via Internet. Os cavalos-de-tróia serão discutidos mais a frente.

Exemplo de uma mensagem de correio com o happy99.exe anexo. Este trojan/worm foi lançado no final de 1998, e ainda hoje, circula em grande quantidade na Internet.

Foi o primeiro vírus a realmente “popularizar” a onda que vemos hoje de disseminação pelo correio. Isto forçou os fabricantes e desenvolvedores de programas antivírus a adatar seus softwares, de forma que eles chequem “no vôo” as mensagens que são depositadas na caixa postal local.

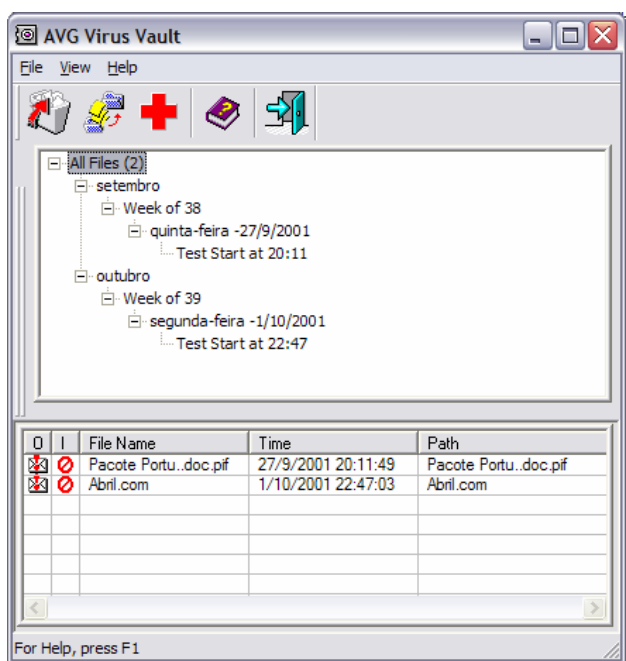


O grande problema que tira o sono da maioria dos administradores de rede de empresas é a queda do conceito que se tinha de que, “se não executar um anexo, nunca será infectado”. Esta frase perdeu a validade, uma vez que existem scripts e programas que exploram falhas nos software de correio, e se “auto-executam”.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Obviamente, este definitivamente não é o comportamento padrão que um programa de correio deve ter. Estes scripts ou programas maliciosos usam falhas para se executarem automaticamente, e isso só é possível por causa delas. Para ficar protegido contra este tipo de ameaça, a melhor saída é sempre manter o seu sistema atualizado. Estas falhas são corrigidas antes que algum script seja difundido o suficiente (infelizmente, a maioria das pessoas não costuma manter seus sistemas atualizados).

Contudo, o risco maior neste caso passa a ser dos administradores de grandes ambientes, que terão de efetuar atualizações praticamente durante à noite, para poder concluir o trabalho antes que as falhas se tornem perdas reais, no dia seguinte. Todo administrador de rede já possui trabalho o suficiente, pois por mais que instrua os usuários de uma rede a não executarem arquivos anexos, os avisos não funcionam. Agora, imaginemos este ambiente, com vírus e worms que sequer precisem ser executados.



Apesar dos antivírus hoje em dia detectarem estes vermes que usam falhas de segurança, pela característica de alguns, quando o arquivo ou o email chega ao antivírus, pode já ter sido interpretado pelo núcleo do programa. Isto acontece com o browser, ao visitar uma página que possua o “JS.Exception” ou o “Happytime”. O js.exception.exploit basicamente explora uma falha de javascript, e o Happytime, de VB Script.

Para maiores informações sobre o “js.exception.exploit” e o Happytime:

<http://www.symantec.com/avcenter/venc/data/js.exception.exploit.html>
<http://www.symantec.com/avcenter/venc/data/vbs.haptime.a@mm.html>

Como o email é a forma mais usada para disseminação de vírus e programas maliciosos, alguns programas já incorporam funcionalidades que impeçam o usuário de executar ou abrir arquivos anexos a mensagens, com extensões suspeitas.

O Personal Firewall “ZoneAlarm” possui o recurso de renomear automaticamente arquivos anexos em mensagens com extensões perigosas, como .exe, .com, .pif, .vbs, entre outras (falaremos dele na secção “Personal Firewalls”). Programas de correio, como o Outlook XP (que faz parte do Office XP) por padrão, não aceitarão arquivos com estas extensões, automaticamente ignorando-os. Isso infelizmente não os torna mais seguros, diante da avalanche de falhas que estes programas têm apresentado.

Gerência Remota

Hoje em dia, existem diversos programas para gerência remota disponíveis. Com o aumento da velocidade dos meios de comunicação de dados, vemos que as facilidades para gerência remota têm melhorado, principalmente, em qualidade. Hoje, apenas com uma linha discada, analógica, a 33.6 Kbps, Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

conseguimos capturar a console de um computador ou servidor, ou até abrir uma sessão gráfica remotamente, isto tudo com um nível de usabilidade impressionante.

Contudo, quando estamos falando destas facilidades, devemos lembrar também que o acesso a um computador através de um método destes é praticamente a mesma coisa que estar na console do computador. Muitas vezes, não lembramos deste detalhe e não tomamos as devidas precauções.

Podemos classificar estes programas / serviços em dois tipos:

1. Captura de console
2. Sessão remota

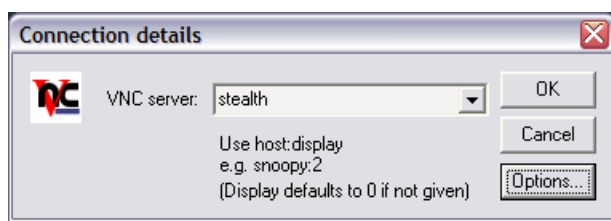
Captura de console

Os programas que permitem capturar a console fazem exatamente isso. Permitem que, remotamente, se consiga ver e usar o ambiente gráfico (GUI) presente na console do computador, desde que devidamente autenticado. Geralmente, este tipo tem a pior performance, devido ao alto tráfego causado pelas imagens da interface gráfica (a imagem geralmente é passada como uma matriz de pontos).

VNC (Virtual Network Computing)

(<http://www.uk.research.att.com/vnc/>)

O VNC tem se tornado uma febre recentemente em empresas. É um utilitário gratuito, que pode ser baixado diretamente do site da AT&T acima.



O VNC é simplesmente um utilitário que permite a captura da tela de um computador, seja ele um Linux, Windows ou Macintosh. Isso por sinal é o que faz dele um sucesso.

Outra grande vantagem do VNC é o cliente Java. O VNC possui um componente servidor (instalado no computador que se deseja gerenciar) e um componente cliente (instalado no computador que se deseja usar para acessar o servidor). Contudo, o próprio componente servidor possui um servidor Web incorporado, o que dispensa ter o cliente. Em resumo, é possível capturar a tela de um computador remotamente, apenas através de um browser.

O VNC possui duas falhas de segurança em potencial.

A autenticação inicial do VNC é criptografada. Porém, todo o tráfego a partir daí é “clear text” (sem criptografia de nenhum tipo). Portanto, sua utilização é recomendada apenas em redes confiáveis (trusted networks), ou que façam uso de canais privados de comunicação criptografados, como VPNs (Virtual Private Networks).

Como abre inicialmente duas portas TCP, é fácil detectar que um computador possui o VNC instalado. Um método bastante simples é apontar um browser com suporte a Java para o endereço IP que se deseja testar, especificando a porta, como por exemplo:

http://servidor_a_ser_testado:5800

... Substituindo o “servidor_a_ser_testado” pelo nome ou IP do computador. Caso este computador possua o VNC instalado, e não exista nenhum filtro ou firewall que bloqueie estas portas, receberá no browser uma janela assim:

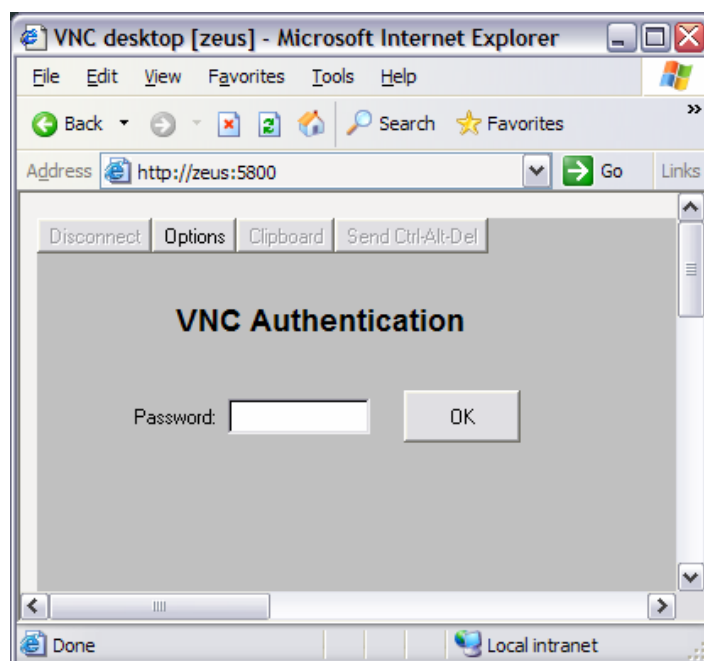
Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

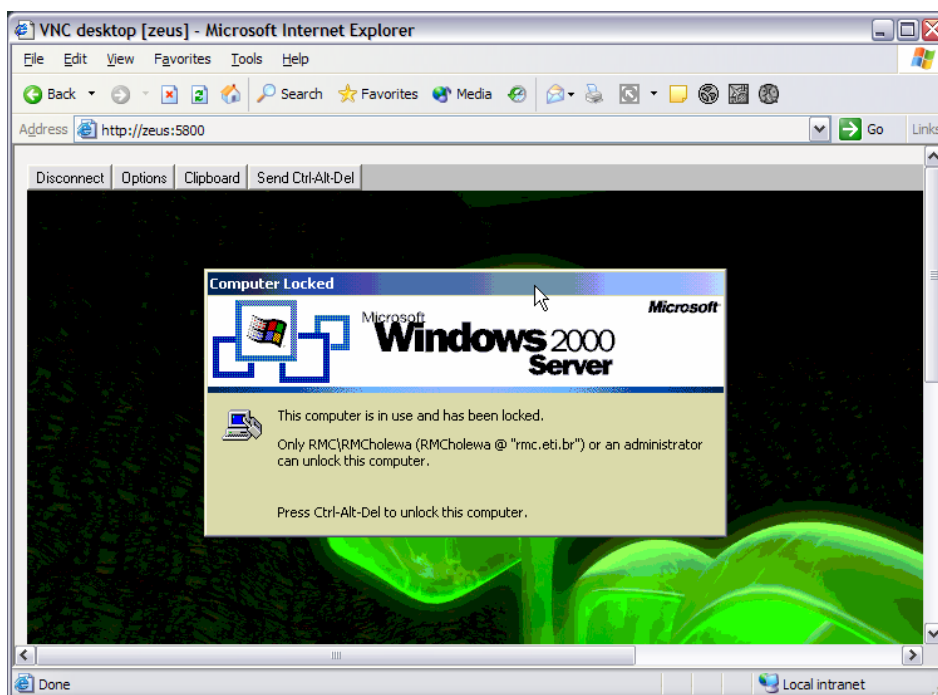
A tela ao lado comprova que o computador “Zeus” possui o VNC instalado. Caso saiba a senha e a digite corretamente, a console do computador remoto se abrirá.

Um pequeno detalhe: com o Windows NT / 2000 / XP, a console pode ficar bloqueada, através das teclas CTRL+ALT+DEL [ENTER]. Neste caso, apesar de capturar a console remota, o cliente não poderá prosseguir, a não ser que possua a senha para desbloqueá-la.

Portanto, uma recomendação básica para quem usa o VNC com o NT/2000/XP é manter o hábito de sempre deixar a console travada.



Veja:



Uma vez de posse da informação de que um determinado computador em rede possui o VNC instalado, um potencial hacker poderá usar uma ferramenta de ataque por força bruta, e tentar quebrar a senha de acesso do VNC, como o VNCrack:

<http://www.phenoelit.de/vncrack/>

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Este utilitário terá maior eficiência contra a versão 3.3.3r7 e anteriores. Como administradores instalam o VNC e nunca atualizam, é muito comum encontrar versões até bem mais antigas.

"É difícil admitir, mas os invasores geralmente conhecem tudo sobre você e seu sistema. Por outro lado, nós não conhecemos quem são, e o que pretendem. Além disso, o tempo está a seu favor, e absolutamente contra nós".

PCAnywhere

(<http://www.symantec.com/pcanywhere/index.html>)

O PCAnywhere é um dos produtos de acesso remoto mais conhecidos e difundidos. Ele é fabricado pela Symantec, a mesma empresa que fabrica o Norton Antivirus. O PCAnywhere fornece o controle total de um computador remotamente, seja através de uma rede, seja através de uma linha discada (modem).

A maioria dos usuários desta ferramenta, quando a configuram para acesso via modem, acham que não é necessário colocar uma senha de acesso, e confiam completamente no número de telefone como barreira segurança ("quem vai adivinhar que no fone 2225522 existe um modem para gerência via PCAnywhere?"). Infelizmente, existe uma técnica chamada "war dialing", usada para descobrir, dentro de um intervalo de números telefônicos, quais respondem "voz" e quais respondem "dados". Basicamente, é um programa que usa um computador para tentar, um a um, vários números telefônicos e emitir um relatório sobre quais destes responderam com sinal de modem. A maioria das grandes empresas possui suas próprias centrais telefônicas, e contratam um serviço da companhia telefônica chamado DDR (Discagem Direta Ramal). Assim, os números telefônicos desta empresa são sequenciais, facilitando ainda mais a técnica de war dialing. Quando isto não ocorre, o "hacker" tem por prazer configurar o programa de war dialing para discagem randômica, e deixá-lo trabalhando por semanas (às vezes até meses). Mais cedo ou mais tarde, ele achará algum número telefônico com um modem na ponta. Apesar de parecer uma técnica tipo "loteria", sua eficácia é bastante alta, principalmente em empresas que usem serviços telefônicos de DDR.

Além disso, o próprio PCAnywhere possui bugs, como qualquer outro programa. De acordo com o teorema fundamental dos firewalls, qualquer programa possui bugs. Um programa relativo à segurança terá bugs relativos a segurança. A última vulnerabilidade detectada no PCAnywhere permitia um ataque do tipo DoS, que impedia o programa de ser acessado remotamente depois de um ataque (versão 10.0). Porém, observe que a má configuração de um programa relativo a segurança pode ser desastrosa, muitas vezes pior e mais abundante do que qualquer problema relativo a bugs.

Veja mais informações sobre problemas com o PCAnywhere em:

<http://www.securiteam.com/windowsntfocus/5FP0C1F55G.html>

<http://www.securiteam.com/exploits/5BP0G201FO.html>

<http://www.securiteam.com/windowsntfocus/5YP0C0K3FI.html>

Sessão remota

Os programas de sessão remota permitem abrir uma nova sessão para um usuário, onde um novo ambiente é carregado, independente da console. Imagine um terminal remoto, com uma diferença: gráfico.

Estas aplicações possuem a melhor performance, porque, apesar de tratarem partes da tela como uma matriz de pontos, mostram alguns itens na tela com comandos pré-definidos. Assim, como a utilização da rede é menor, há um ganho em velocidade.

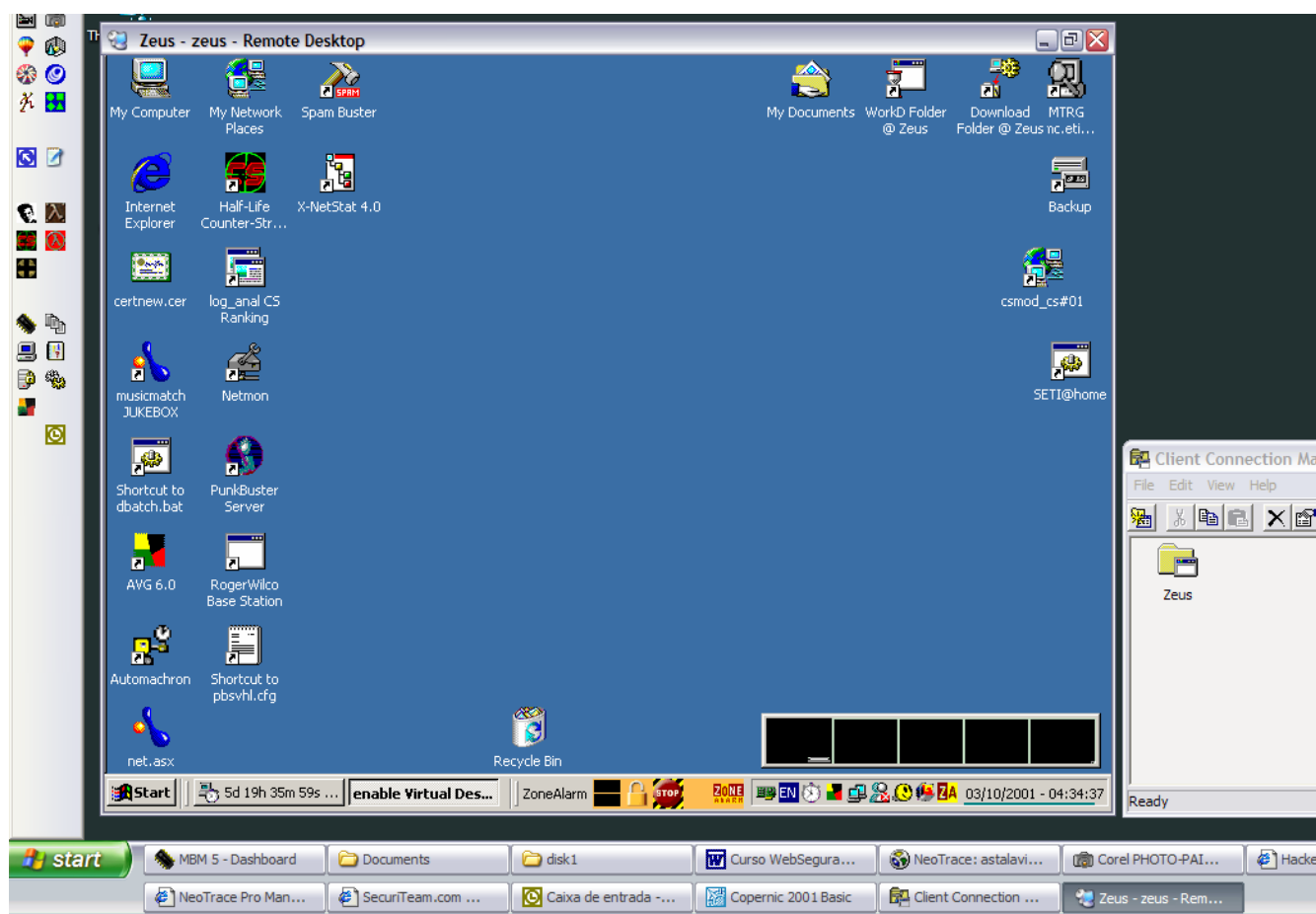
Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

TSC (Terminal Services)

O terminal services faz parte de qualquer instalação de Windows 2000 / XP. No Windows NT 4.0, era um sistema operacional à parte, chamado “Microsoft Windows NT 4.0 Terminal Server Edition”. Foi projetado por uma empresa chamada “Cytrix”, como um produto de nome “Winframe”. A Microsoft adquiriu a licença de uso do mesmo, e agora faz parte do núcleo do sistema.

O TSC permite que uma console remota seja aberta para um usuário, de forma que o ambiente do mesmo será totalmente carregado, independente da console. Com um desempenho fantástico mesmo em redes de baixa velocidade (modem), foi projetado originalmente para permitir o uso dos “Thin clients”, ou computadores simples que executariam suas tarefas remotamente. Foi a época da volta à centralização.

Contudo, esta onda não durou muito, e hoje, é difícil justificar uma licença de terminal service, para aplicações (o produto é tarifado baseado em quantas sessões simultâneas permite). Porém, todo Windows 2000 / XP permite até duas conexões simultâneas, para fins de gerência remota.



O serviço usa a porta 3389/tcp. Não existem vulnerabilidades detectadas até hoje nele, e todo o tráfego entre o programa cliente e o servidor é criptografado. Contudo, Já foi descoberto um problema que permite um ataque do tipo DoS no servidor como um todo. Maiores informações em:

<http://www.microsoft.com/technet/security/bulletin/MS01-040.asp>

<http://www.securiteam.com/windowsntfocus/5QP0M2A4UI.html>

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Um detalhe: O serviço de terminal só está disponível no Windows NT 4.0 Terminal Server Edition ou no Windows 2000 Server em diante. Com o Windows XP, ele também está disponível na versão Professional, e permitirá conexões com console remota da mesma forma.

Repare que a captura das informações digitadas no lado cliente também é possível. Assim sendo, é recomendada sua utilização apenas em computadores que não sejam compartilhados, e que sejam confiáveis.

Estes são três dos programas de gerência remota mais usados hoje pela comunidade. Cada um deles requer uma certa experiência em sua manipulação, pois se feita de forma errada, derá a um invasor, a possibilidade de controlar o computador ou servidor remotamente, de qualquer lugar.

Poucos administradores tomam cuidado ao usar uma destas ferramentas, ou qualquer outra, de gerência remota. O maior erro é fazer uso delas em computadores compartilhados, ou que estejam conectados à redes não confiáveis (untrusted networks). Existem diversos programas disponíveis livremente na Internet que armazenam em um arquivo, para posterior análise por parte de um “hacker”, todas as teclas digitadas em uma máquina comprometida. A conclusão óbvia: se algum utilitário de gerência remota for usado a partir de uma destas máquinas, estarão no arquivo armazenadas informações sobre host, usuário e senha usados para ativá-la.

Portanto, não adianta garantir apenas a segurança do componente de controle (servidor) da aplicação. A utilização do cliente de gerência deve ser feita de um computador confiável, restrito, e que não seja compartilhado, preferencialmente, conectado a uma rede confiável (afinal, o tráfego da rede pode também estar sendo monitorado por um suposto “hacker”).

Programas Diversos

Vários programas usados amplamente possuem problemas de segurança. Como regra padrão, nunca salve a senha em nenhum programa que permita esta opção. Nosso comodismo sempre forçará para que deixemos as senhas salvas nos programas (e podem ser facilmente retiradas do registro do computador, ou de arquivos especiais no disco). Alguns exemplos clássicos são:

FTP Voyager / FTP Explorer / WS_FTP

Estes três programas de FTP são bastante usados como clientes FTP. As senhas de acesso a sites FTP são salvas ou no registro ou em arquivos dentro da pasta do programa, e são criptografadas com um esquema bem fraco. Existem também programas na Internet que podem ser usados para retirar destes arquivos as senhas dos sites FTP. Recomendação: caso use um destes programas para efetuar acesso FTP a algum site que tenha acesso diferente de anonymous, NÃO escolha a opção de salvar a senha, ou lembrá-la. Esta é uma recomendação válida para qualquer programa que seja.

Microsoft SQL Enterprise Manager

O Microsoft SQL Enterprise Manager é uma console de gerência de servidores Microsoft SQL, que utilizam como base o MMC (Microsoft Management Console). Foi descoberta uma vulnerabilidade quando o usuário registra um banco de dados para gerência, e opta por salvar a senha para uso posterior. A senha é armazenada no registro do sistema com criptografia fraca, sendo possível descobrir qual a senha. É recomendado NÃO salvar a senha, e, ao registrar um novo banco de dados, marcar a opção de não salvar a senha e perguntar pela informação de autenticação todas as vezes que entrar no Enterprise Manager. Esta vulnerabilidade está presente na versão 7.0 do banco de dados, e não na versão 2000.

Microsoft Option Pack / Internet Information Server 4.0 ou posterior

O servidor web da Microsoft, o IIS (Internet Information Server) tem a má fama de ser inseguro. Contudo, isso se deve à configuração padrão do mesmo, logo após a instalação. Também seguindo o Teorema Fundamental dos Firewalls, quanto menos software existir, menor a quantidade de bugs, e por consequência, menor a quantidade de problemas relativos à segurança. A instalação padrão do IIS / Option Pack trás uma série de exemplos e a documentação do software. Alguns destes componentes possuem diversos problemas de segurança (pelo próprio fato de serem exemplos). No processo de instalação, desmarque qualquer opção relativa a exemplos, e documentação. Além disso, desmarque quaisquer componentes que não serão usados. Após a instalação, PARE os sites web, FTP, SMTP ou NNTP instalados por padrão, e NÃO os use em um ambiente de produção. Deixe-os desativados. Crie o seu site web, por exemplo, do nada. Com isso, você terá absoluta certeza de que nenhum arquivo alheio ao seu site estará acessível.

Também considere não usar o RAD, componente usado para desenvolvimento, e o WebDAV, em ambientes de produção. Lembre-se, servidores de desenvolvimento JAMAIS devem ser usados como servidores de produção. A maioria dos ataques é possível justamente porque o mesmo servidor é usado para o desenvolvimento de programas e páginas, assim como servi-las para a Internet.

Extensões de FrontPage

O FrontPage é um programa que permite a edição de páginas web com recursos WYSIWYG (What You See Is What You Get), mesmo que a pessoa não saiba uma linha sequer de HTML.

Contudo, o FrontPage é dividido em duas partes: o programa cliente, e a porção servidora (chamada de extensões do programa).

É possível criar um site com FrontPage localmente, e depois, transferi-lo para o servidor web, através do componente servidor. Caso o servidor remoto não suporte as extensões de FrontPage, as páginas poderão ser transferidas através de FTP.

Entretanto, as extensões também são usadas por outros programas para editoração e publicação de páginas, como o Visual Interdev, que permite a edição de páginas web de conteúdo dinâmico, suportando ASP, VBScript, e etc.

As primeiras versões destas extensões possuíam dezenas de vulnerabilidades, entre elas, a possibilidade de se escrever em qualquer arquivo do servidor, sem senha. Elas também permitiam que a senha do site fosse recuperada, porque eram guardadas em um arquivo texto (Access.cnf) dentro do diretório /_vti_pvt do servidor.

Dentro deste mesmo diretório, embaixo da raiz, é possível ver arquivos que contém a configuração do servidor. Exemplos:

- **Access.cnf**
config de segurança
- **Linkinfo.cnf**
informações sobre links no site principal
- **Service.cnf**
várias informações sobre a configuração do servidor, como também que extensões executáveis estão associadas
- **Services.cnf**
webs que o servidor possui

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Como se não bastasse, diversos componentes das extensões, que permitem a utilização de recursos chamados “bots”, possuem vulnerabilidades de buffer overflow, o que permite usá-los para executar comandos remotamente.

Uma documentação detalhada sobre as falhas das Extensões do FrontPage pode ser encontrada em:

<http://www.insecure.org/sploits/Microsoft.frontpage.insecurities.html>

Perceba que estas vulnerabilidades são antigas. Hoje em dia, as novas versões não exibem mais estas vulnerabilidades. É recomendado que qualquer site / servidor que use extensões de FrontPage, seja atualizado.

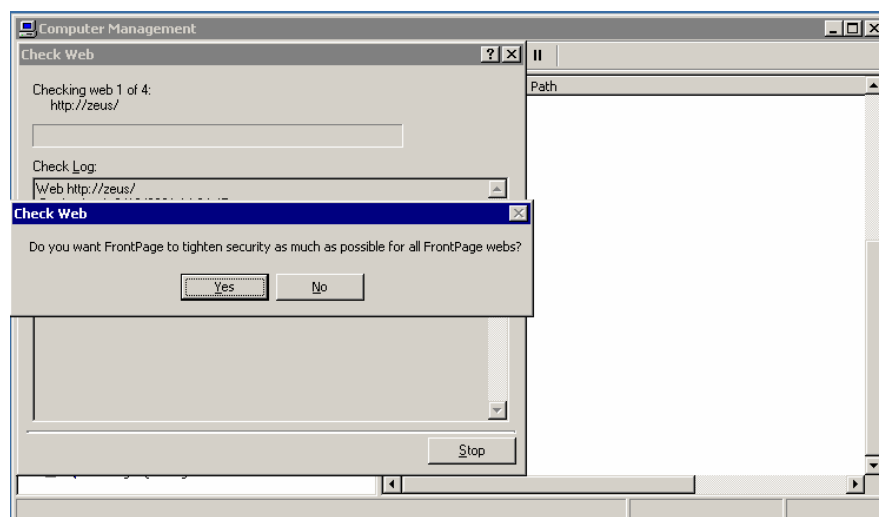
Para tal: <http://msdn.microsoft.com/library/en-us/dnservext/html/fpovrw.asp>

... ou vá no site do produto (<http://www.microsoft.com/frontpage>) e clique nos downloads ao lado.

Ao proceder com a instalação das extensões, o produto irá perguntar se deseja reforçar a segurança dos sites que as usem. Responda que “sim”.

Você também pode acessar a mesma função, clicando com o botão direito no site, indo em “All Tasks”, escolhendo “Check Server Extensions”. Qualquer inconsistência será corrigida, e a opção ao lado apresentada.

Contudo, lembre-se de atualizar as extensões.



Browsers / Navegadores

Hoje em dia, existem quatro browsers usados normalmente na Web. O Internet Explorer, o Netscape, O Mozilla, e o Opera.

Todos eles possuem falhas de segurança. Portanto, é primordial mantê-los atualizados. Sempre use a última versão, mesmo que isso implique em um download considerável.

Além disso, devem-se instalar as correções publicadas.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Internet Explorer

Para instalar as correções do Internet Explorer, basta realizar o Windows Update, que existe nos sistemas da Microsoft desde o Windows 98. Caso seja usuário do Windows 95, deve visitar a página do browser, e baixar as atualizações, que podem ser encontradas em:

<http://www.microsoft.com/windows/ie/downloads/archive/default.asp>

Para baixar a versão atual:

<http://www.microsoft.com/windows/ie/downloads/ie6/default.asp>

Para visualizar a versão do Internet Explorer que possui, clique no menu Ajuda, “Sobre o Internet Explorer”.



Netscape

O Netscape possui uma ferramenta de atualização que pode ser acessada também através do menu de ajuda (Centro de Segurança, ou Security Center).

Mozilla

De todos os browsers, talvez o Mozilla seja considerado o mais seguro, devido a sua política de atualizações frequentes, e suas opções bastante avançadas para depuração de erros, assim como tão um roteiro para detectar, analisar e sanar problemas. Para acessar uma página com uma lista de bugs encontrados, e atualizações, basta ir ao menu “QA”, e clicar em “Known Bugs”.



Opera

O Opera aparentemente não possui nenhum esquema de atualizações automáticas, ou de distribuição de patches. É recomendado que o usuário cheque com frequência a página do produto para avaliar se está executando uma versão atualizada.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

<http://www.opera.com/download/>

Contudo, o Opera utiliza as bibliotecas Java da Sun, caso deseje suporte a Java. Neste caso, é interessante manter o runtime Java atualizado.

<http://java.sun.com/j2se/>

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

5. Técnicas de Invasão

Várias técnicas básicas de invasão ou de DoS exploram problemas gerados pela má configuração de computadores e servidores em rede, que são os alvos primários caso algum hacker se interesse em invadir uma determinada rede.

Existem diversas técnicas de invasão, que poderíamos tratar melhor se chamássemos de abordagens. Existem diferentes abordagens para diferentes ambientes de rede. A abordagem usada na invasão de uma rede corporativa será completamente diferente da abordagem usada em uma pequena rede que talvez nem esteja conectada diretamente à Internet, como também será diferente da abordagem usada para invadir um usuário apenas.

Em termos de “facilidade”, uma rede pequena, corporativa, que não tem contato com a Internet, em escritórios de pequeno a médio porte, é a mais vulnerável, numa abordagem “de dentro para fora”. Contudo, tentar invadir uma rede destas de “fora para dentro” é muito difícil, pois não existem conexões permanentes com a Internet. Nestes casos, um potencial hacker tentará comprometer qualquer computador que esteja localmente conectado a rede, mas que possua um modem, ou algum outro método de acesso a Internet. Nestes casos, técnicas de engenharia social são muito usadas, pois a falta de conexão permanente limita muito a gama de ferramentas que podem ser usadas para extrair informações.

Uma rede conectada 24 x 7 à Internet já possui pelo menos um canal permanente. Caso a rede não tenha nenhum servidor para a Internet, e use alguma técnica de acesso como Proxy ou NAT, estará relativamente segura.

Por último, ambientes que acessam a Internet através de canais permanentes, e que possuem servidores também conectados nesta estrutura, com endereços reais, disponibilizando serviços, são os mais vulneráveis.

Desta forma, os seguintes passos podem ser detectados:

Probing

Hackers tentarão investigar sua rede para determinar: que **serviços rodam em quê servidores**; quais são as **versões destes serviços**; quais são os servidores, e onde estão **localizados na rede**; um esboço ou um **mapa da rede**; relações de **confiança entre os servidores**; **sistemas operacionais** utilizados; possíveis estações de **gerência na rede**; **filtragem de pacotes** (se existir); sistema de detecção à intrusão – **IDS** (se existir); **honeypots** ou potes de mel (se existirem); **portscanning** (passivo e com spoofing se possível). Se for justificável, utilização de **war dialing**. Descobrir qual **a relação da rede interna da empresa, com a rede de gerência** (entenda-se por rede interna, aquela usada pelos funcionários).

Observação importante: dependendo da “inteligência” do suposto hacker, a fase de probing será realizada através de algum método que impossibilite sua identificação, como através de provedores gratuitos ou através de linhas telefônicas roubadas. O probing em si poderá ser detectado, mas sua origem não será.

Hoje em dia, com o advento dos provedores de acesso a Internet gratuita, se torna muito fácil esconder a natureza de um ataque. A grande maioria dos provedores gratuitos não exige cadastro, nem monitoram os acessos através de contas usuário / senha individuais. Assim, qualquer um se conectar através de um provedor gratuito terá seu vínculo de identificação ligado apenas ao seu endereço de rede IP, e o telefone de origem.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Entretanto, em várias cidades, as companhias telefônicas desabilitam as funções de rastreamento de telefones, mais conhecido como BINA (“B” Identifica Número de “A”), devido à sobrecarga nas centrais telefônicas em horários de pico.

Devemos também lembrar que o horário de pico de utilização do sistema telefônico (horário comercial) difere do horário de pico de utilização da Internet no Brasil (das 20 a 01 hora). Quando isto ocorre, o provedor perde a única informação que pode associar uma conexão / endereço de rede IP a um telefone de origem.

Nestes casos, a única forma de rastrear a origem da chamada é através da própria companhia telefônica. Todas elas possuem restrições quanto a isto, e não podem divulgar informações sobre ligações, a não ser perante decisão judicial.

Se passarmos a pensar como um potencial hacker, veremos que, dependendo do nível do ataque, e de seu risco, o fato de o seu número de telefone apenas poder ser rastreado e conhecido através de decisão judicial é uma barreira de proteção à privacidade que não ameaça o ataque em si.

Caso o potencial invasor sinta que, dada a gravidade dos atos e conseqüências que poderão se desenvolver, ele poderá ser alvo de um processo judicial, então valerá apenas, para ele, utilizar uma técnica alternativa, como o roubo de uma linha telefônica ou a utilização de um telefone público.

Por mais incrível que pareça, esta última alternativa não está muito longe da realidade. A linha telefônica que alimenta um “orelhão”, ou telefone público, é praticamente a mesma linha telefônica que alimenta uma empresa ou residência. Assim sendo, e com pouco conhecimento de eletrônica, se consegue grampear esta linha, e usá-la para um ataque.

Engenharia Social (Social Engineering)

O próximo passo, ou realizado em paralelo, será a utilização de técnicas de **engenharia social**. Através destas técnicas, **informações valiosas** poderão ser obtidas. Descobrir **informações pessoais** sobre o(s) administrador(es) da rede; informações sobre **fornecedores de suprimentos e manutenção**; descobrir quem tem **acesso privilegiado** a qualquer servidor ou estação; avaliar o grau de conhecimento desta pessoa (**quanto menor, melhor, se possuir acesso privilegiado**); descobrir **números de telefone importantes** (o número de telefone do administrador, das pessoas envolvidas com a administração da infraestrutura, **telefones de departamentos** como comercial); tentar também obter uma **lista de endereços de correio eletrônico** importantes. Tentar obter informações do **suporte telefônico** da empresa, caso possua. Obter **acesso ao lixo** da vítima, se possível (sim, os filmes que falam de hackers o fazem geralmente de forma bastante errada: contudo, nisso eles acertaram: uma das maiores fontes de informação sobre a vítima será seu lixo).

Quem trabalha em uma empresa que possua servidores de dados e uma rede, sabe que a maioria dos cargos do alto escalão são ocupados por empresários que não possuem muito conhecimento técnico, e facilmente caem vítimas de cavalos de tróia. Aliado a este fato, também sabe que estes mesmos empresários, apesar de não terem a real necessidade, e dependendo do tamanho da empresa, conhecem as senhas de acesso aos servidores, com direito de administração, isso quando suas próprias contas de acesso à rede não são equivalentes a administradores.

A partir daí, o próximo passo será tentar relacionar as informações coletadas até agora. Baseado nas informações levantadas no primeiro passo, o hacker irá pesquisar na Internet e na sua comunidade sobre vulnerabilidades existentes nas versões dos programas, serviços e sistemas operacionais usados pela rede.

Além disso, caso a relação da rede interna com a rede de gerência seja direta, uma abordagem baseada em cavalos-de-tróia será interessante. O objetivo passará a ser conseguir ter acesso ao tráfego da rede interna. Isto pode ser feito enviando trojans para departamentos administrativos, comerciais, e financeiros. A maioria dos funcionários destes departamentos é leiga e não saberá a diferença entre um

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

documento do Word e um executável anexo ao seu correio eletrônico. É bem provável que, com alguns dias de investigação do tráfego da rede interna, você consiga alguma senha com direitos de administração. Como administradores de rede tem o hábito de usar a mesma senha para diversas ferramentas, se na primeira fase alguma ferramenta de gerência remota foi achada, então, é mais do que provável que as senhas serão idênticas.

Muitos “hackers” consideram a utilização de cavalos-de-troia algo condenável, tecendo duras críticas. Contudo, estatísticas comprovam que a utilização desse método é bastante difundida.

Independente da abordagem adotada, o hacker terá duas coisas em mente: objetividade, e máxima dissimulação. Tudo será feito sem pressa, para não levantar suspeitas. Ele poderá até tentar fazer amizade com alguém que trabalhe na empresa (isso é mais fácil do que parece: basta visitar os mesmos lugares que essa pessoa visita, principalmente se estes lugares forem escolas, universidades ou clubes, pois nestes lugares existe um sentido maior de união). Obviamente, tudo isso dependerá da informação que se deseja obter: o hacker avaliará se todo o esforço vale a pena. Contudo, lembre-se que muitos fazem pelo desafio, e superarão enormes dificuldades somente para provar a si mesmos que são capazes.

Programas Usados para Obter Informações

Diversos programas podem ser usados para obter informações sobre a rede ou computadores / servidores remotos. Todos eles serão vistos em detalhes na seção “Ferramentas”. Alguns deles são:

SNMP

O SNMP (Simple Network Management Protocol) é um protocolo de rede usado para gerência de equipamentos em rede.

Através dele, é possível consultar informações de computadores e equipamentos que possuam o serviço. Ele tem uma abordagem bastante simples, e consiste em ter, no equipamento ou computador, um “agente” SNMP, que coletará dados sobre o mesmo. O formato e as informações que cada equipamento possui é conhecido como MIB (Management Information Base). Possuindo a MIB de um equipamento ou computador, pode-se então consultar estas informações, e, algumas vezes, alterá-las.

Contudo, este protocolo / serviço é bastante inseguro. Para acessá-lo, não é necessário usuário ou senha, apenas conhecer a “comunidade” na qual o agente está configurado.

Com essa informação, e com qualquer programa que interprete a saída de dados do agente, pode-se literalmente montar o mapa de uma rede, e consultar informações como utilização de disco, CPU e rede de computadores e equipamentos, bem como tabela de rotas.

Existem programas que usam o SNMP para construir o mapa de uma rede. Podemos citar o Tivoli, o Lucent NavisAccess, e o SNMPc. Porém, qualquer ferramenta SNMP pode ser usada.

Por exemplo, qualquer computador UNIX que possua as funcionalidades SNMP instaladas possui um utilitário chamado “Snmwalk” para consultar um agente. Existe uma ferramenta similar para Windows, presente no Resource Kit do Windows NT/2000/XP, chamada SNMPUTIL, com a mesma função. As portas 161 e 162/udp sempre devem estar sendo filtradas e monitoradas.

Essential Net Tools

(<http://www.tamos.com/>)

Programa fantástico que explora a má configuração de computadores Windows conectados a Internet. Através dele, é possível, dado um intervalo de endereços IP, visualizar quais destes estão com o compartilhamento de

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

arquivos e impressoras ativado, e com algo compartilhado. Você ficaria surpreso com a quantidade de computadores que possuem a raiz do drive C: compartilhada, permitindo acesso a qualquer arquivo dentro do disco, inclusive o .pwl, arquivo que possui a senha salva dos usuários deste computador. Para evitar que o EssNetTools seja efetivo, é necessário filtrar no firewall as portas usadas pelo NetBIOS (135, 136, 137, 139 e 445, tcp/udp).

CIS (Cerberus Internet Scanner / Typhon)

(<http://www.cerberus-infosec.co.uk/cis.shtml>)

(<http://www.nextgenss.com/>)

O CIS é um pequeno programa de análise de vulnerabilidades. Apesar de pequeno, é impressionante. Ele roda sob Windows NT 4 / 2000 e, dado um endereço IP, ele produzirá uma página HTML com todos os testes realizados. O CIS testa por vulnerabilidades conhecidas, como finger, VRFY (SMTP), DNS, Web, entre outras. O mais impressionante é quando ele consegue acessar as informações de contas de usuários de uma máquina Windows NT, má configurada. Para evitar a efetividade do CIS, é aconselhável usar ele próprio, analisar quais vulnerabilidades foram encontradas, e saná-las uma a uma.

O projeto do CIS parece não estar sendo atualizado. Contudo, o pessoal da Next Generation Security Software criou o Typhon, em cima do CIS, atualizado. O Typhon estende as ferramentas do CIS, com novos recursos e uma nova interface. Fantástico.

Nmap

(<http://www.insecure.org/nmap>)

*"If your goal is to understand your network from a 40,000-foot view, then Windows port scanning tools will suffice. But if you're serious about your security and looking for the holes that crackers will find, then take the time to install a Linux box and use nmap." --
[Info World](#)*

nmap é a ferramenta de portscanning mais fantástica conhecida. Com ele, é possível realizar desde um scan ativo de um único endereço, até scans passivos de uma rede inteira, de forma automatizada, revelando inclusive o sistema operacional da vítima, através da assinatura da conexão TCP. Possui inclusive a opção de realizar o scan com o endereço de origem “spoofado”, ou mudado (no caso de scan passivo). Ele roda sobre Linux. É uma das ferramentas mais usadas. No site acima, existe até uma versão gráfica dele. Evitar a ação do nmap é praticamente impossível. De qualquer forma, é primordial configurar um firewall para apenas permitir tráfego entrando na rede, para as portas / serviços que tem de ser acessíveis de fora.

WhatsUp Gold

(<http://www.ipswitch.com>)

O WhatsUp é um programa desenvolvido pela empresa IPswitch, com a intenção de ser uma ferramenta de monitoração de rede. Porém, ele possui internamente uma função usada para “descobrir”, dado um intervalo de endereços, quais estão ou não ativos, bem como outras informações, como o nome das máquinas. Bastante eficiente em redes Microsoft, com ele você poderá ter uma idéia de quantas máquinas estão ativas numa determinada classe, por exemplo. Para barrar o WhatsUp, basta filtrar as portas do NetBIOS e tráfego ICMP.

TELNET

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

O próprio telnet do Windows pode ser usado para descobrir que versão um determinado servidor está rodando, por exemplo, de sendmail, servidor web, POP3 ou FTP. Para isso, basta disparar um TELNET para a porta do serviço desejado. Vejamos:

```
telnet xyzwabcd.com.br 25
```

```
220 dominus.elogica.com.br ESMTP Sendmail 8.9.3/8.9.3; wed, 29 Mar 2000 20:38:40 -0300
```

Agora, sabemos que o servidor é um sendmail, versão 8.9.3. Aliado ao nmap, descobrimos qual o sistema operacional.

Trojan Horses e Back Doors

Trojan Horses / Cavalos de Tróia

Os trojan horses são programas que demonstram um determinado tipo de comportamento, ou se propõem a uma determinada tarefa, geralmente a realizam, proém, sem que o usuário saiba, executam alguma outra tarefa. Esta segunda função na maioria das vezes abre o computador para invasões ou acesso remotos.

Hoje em dia, existem inúmeros programas do tipo trojan horse, ou cavalo-de-tróia, mas o conceito aplicado a informática existe a décadas. O primeiro programa usado como trojan horse que ganhou a comunidade foi o NetBus. Após o NetBus (que é tido como um software de gerência remota, e não como um trojan horse), surgiram diversos outros, sendo o mais famoso deles, o Back Orifice. Este, foi criado por um grupo de hackers que se intitulam “The Cult of the Dead Cow”, ou cDc (<http://www.cultdeadcow.com/>)

Vejamos nos anexos, uma coletânea de telas de trojans conhecidos. Cada um destes programas pode ser removido através de um bom programa de anti-virus, como o Norton anti-virus, o AVP, ou o TrendMicro. Todos estes anti-virus possuem download para avaliação (30 dias) e poderão salvar sua pele, mesmo que você não compre o programa (desinstale em seguida).

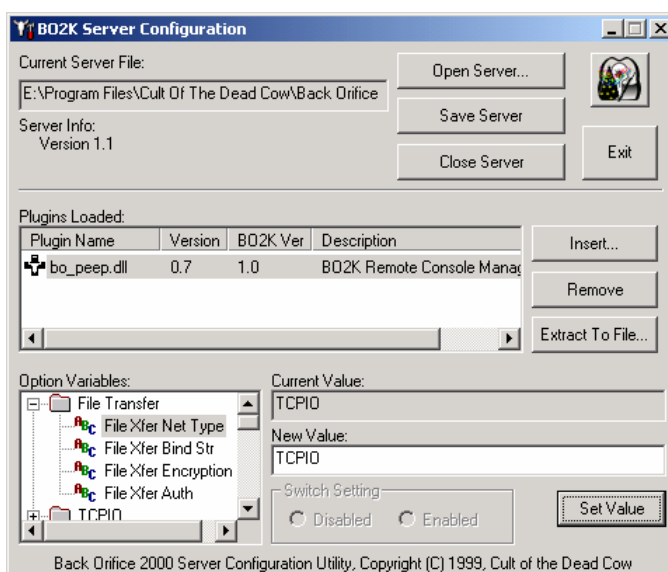
<http://symantec.com/avcenter> e <http://www.avp.com>

AVG é gratuito:

<http://www.grisoft.com>

O mais famoso de todos os trojans é o Back Orifice. Ele é capaz de tomar o controle COMPLETO de um computador com qualquer versão do Windows. Através dele, podemos até visualizar remotamente a tela do computador. Enviar mensagens, dar boot, travar, copiar arquivos, capturar todas as teclas pressionadas, entre outras funções.

Apesar de ter sido lançado a mais de um ano, ele ainda assola a Internet, principalmente aqueles usuários que não tomam precauções básicas, como receber arquivos de desconhecidos, executáveis, e abri-los.

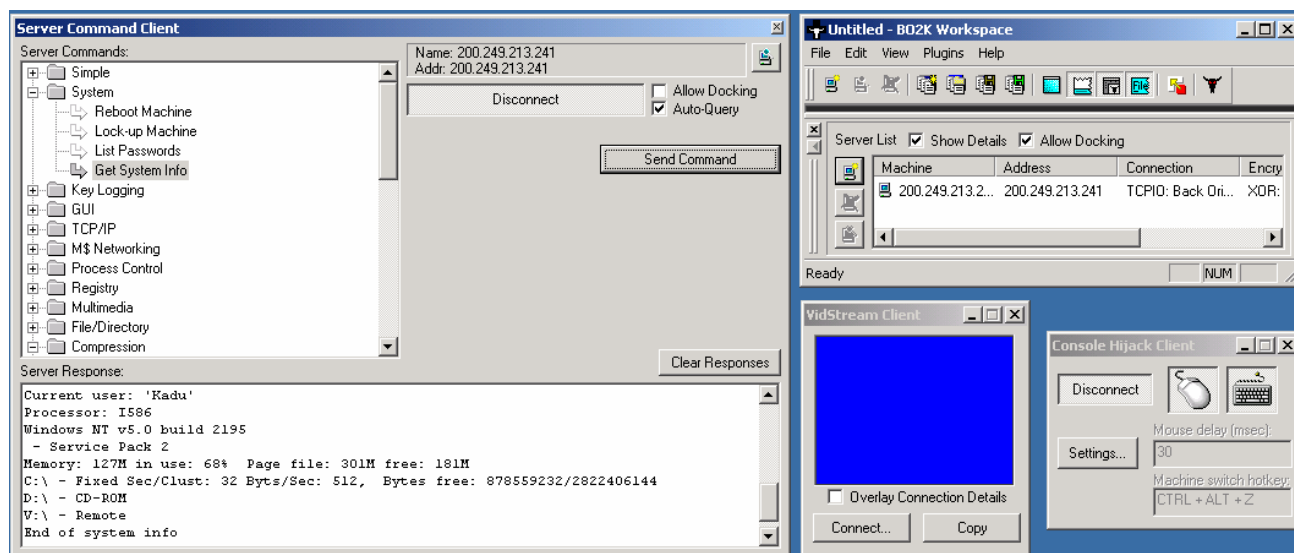


Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Ele possui requintes como suporte a plugins. Vem em dois componentes: a parte “Server” ou servidor, e a parte “Client” ou cliente. A parte servidora é a enviada para a vítima, e a parte cliente, usada para controlar o componente servidor.

Conjunto de telas de controle (cliente):



Backdoors

Já os backdoors podem ter mais ou menos a mesma funcionalidade de um trojan, mas possuem outras intenções. Quando um hacker consegue acesso a um sistema, uma de suas primeiras atitudes será instalar backdoors no sistema. Estas backdoors lhe permitirão voltar a ter acesso a este sistema se por acaso o dono / usuário ou administrador descobrir que sua segurança foi violada. Uma backdoor pode ser na forma de um programa (assim como os trojans), como um script (principalmente em ambiente UNIX), ou até como uma série de procedimentos (criar uma conta com direitos de administração, com um nome comum). Esta é a principal diferença para um trojan, que geralmente é um arquivo executável.

Buffer Overflow

Buffer overflows são consequência direta de péssimos hábitos de programação. Consiste em enviar para um programa que espera por uma entrada de dados qualquer, informações inconsistentes ou que não estão de acordo com o padrão de entrada de dados. De forma resumida, seria mais ou menos tentar encaixar uma bola de basquete em um buraco de golf.

Em programas que não tratam a consistência dos dados de entrada, pode haver uma desestruturação do código em execução, permitindo que código estranho seja enviado e executado. Imagine um buffer de entrada de dados configurado para receber 32 bytes. Imagine agora que este mesmo buffer não possui uma checagem da consistência dos dados. Agora, tente enviar mais do que 32 bytes. Isso normalmente estourará o buffer (buffer overflow), e normalmente, o que passar de 32 bytes, invadirá outras áreas de memória do sistema. Dependendo de que áreas sejam estas, é possível fazer com que esta “carga extra” também seja executada. É exatamente aí onde mora o perigo.

As formas mais comuns de buffer overflow são encontradas em servidores web e de FTP. Ao se submeter uma URL muito grande (geralmente acima de 150 caracteres) o servidor para de responder. Vários softwares servidores Web e FTP famosos já foram vítimas de tais vulnerabilidades, como o Apache Web

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Server, o Internet Information Server, o Serv-U FTP Server, War FTP d, entre outros. No ambiente UNIX, existem ou existiram diversas vulnerabilidades deste tipo nos servidores de SMTP (envio de correio) e POP3 (recebimento de correio).

A critério de exemplo, uma pesquisa sobre “buffer overflow” em um site de segurança como o <http://www.securiteam.com> retorna em média 1300 páginas, APENAS relativas à segurança.

Password Crackers

Os password crackers são em sua grande maioria programas de ataque de força bruta, que tentarão, dada uma combinação possível, cada combinação até descobrir qual é a senha. Os algoritmos de criptografia empregados geralmente são conhecidos publicamente. Sua segurança reside em sua chave. Contudo, esta chave é secreta. Assim sendo, o password cracker aplicará o algoritmo em cada combinação possível de letras até achar aquela que seja igual a senha criptografada original.

Geralmente os password crackers são lentos, e sua eficiência depende inteiramente da qualidade das senhas. Senhas difíceis para um password cracker são aquelas que possuem letras, números, e caracteres de pontuação, como “! @#\$%&*()[]{}-_=+<,>./”. Contudo, a melhor senha sempre será aquela sem sentido, randômica, e que use tais caracteres.

Um típico password cracker levará algo em torno de 2 a 3 anos de trabalho para quebrar uma senha de 7 caracteres, com estas características. Para cada novo caractere adicionado ao tamanho da senha, a dificuldade e o tempo sobem em ordem exponencial. Uma senha com 14 caracteres com tais características levaria milhares de anos. Com isso, chegamos a conclusão de que a senha ideal hoje possui pelo menos 12 a 14 caracteres, e as características descritas acima.

Além dos password crackers típicos, que usam a força bruta, existem aqueles que se baseiam em vulnerabilidades dos algoritmos de criptografia empregados. Estes não atacam por força bruta, mas revertendo o processo de criptografia, geralmente baseado em algoritmo, ou quanto se tem o conhecimento das chaves.

Alguns dos password crackers mais famosos:

L0pht Heavy Industries / @Stake “L0phtCrack” ou LC3 (Windows NT/2000)

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

Crack 4.1 / 5.0 (UNIX)

<http://www.crypto.dircon.co.uk/download/c50-faq.html>

http://www.deter.com/unix/software/crack_4.1.tar.gz

Winzip / RAR / ARJ Password Crackers

<http://www.password-crackers.com/crack.html>

NAT (NetBIOS Auditing Tool)

<http://bbs.ee.ntu.edu.tw/boards/Security/6/16.html>

<http://nmrc.org/faqs/hackfaq/hackfaq-14.html#ss14.6>

<http://www.fastlane.net/~thegnome/files/snt/index.html>

Diversos

<http://www.lostpassword.com/>

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Para acelerar o processo de quebra / descoberta das senhas, a maioria dos password crackers podem ser alimentados com um dicionário de palavras construído pelo usuário. Assim, você pode alimentar o dicionário com palavras mais objetivas, aumentando a possibilidade de acerto.

Exploits

Exploits são pequenos scripts ou programas que exploram uma vulnerabilidade de segurança. Seria mais ou menos como encontrar um furo numa cortina, enfiar os dois dedos, e arrebentar o furo. Geralmente são códigos locais (precisam ser executados no computador que se deseja comprometer), apesar de existirem exploits remotos (via rede). O nome “exploit” também é atribuído as vulnerabilidades descobertas em softwares (sistemas operacionais, servidores, programas em geral). Existem diversos sites de segurança que falam sobre exploits mais recentes. Os mais famosos são:

RootShell

<http://www.rootshell.com>

Internet Security Systems Xforce

<http://xforce.iss.net>

SecuriTeam

<http://www.securiteam.com>

CIAC (Computer Incident Advisory Capability)

<http://ciac.llnl.gov/>

CERT (Computer Emergency Response Team)

<http://www.cert.org>

Man-in-the-Middle

Os ataques do tipo man-in-the-middle são usados em sistemas de segurança baseados em token. Consiste em interceptar o tráfego entre dois computadores, e, para ambos, continuar parecendo que a comunicação é direta. Contudo, a entidade que intercepta o tráfego também o altera, de forma que a requisição de rede pareça original e autêntica. São ataques bastante difíceis de ocorrer, pois geralmente requerem grande conhecimento de programação e da rede que se deseja comprometer. Normalmente, ataques MITM (Man-in-the-Middle) requerem que um dos pontos de conexão já tenha sido comprometido (como o provedor a qual você está conectado, ou o fornecedor da rede onde se encontra o servidor que se deseja acessar). A maioria dos ataques MITM é usada contra sistemas criptográficos. Para maiores informações:

How to brake RSA

<http://gaia.cs.umass.edu/cs653-1998/notes/ch9-1/sld001.htm>

6. Outros Tipos de Ataques

Existem outros tipos de ataque que, se não permitem uma quebra de segurança direta, como o comprometimento das informações armazenadas em um servidor, ajudam nos ataques de invasão, muitas vezes até tornando-os possíveis.

DoS (Denial of Service)

Como o próprio nome sugere, ataques deste tipo geralmente não comprometem a privacidade dos dados. A finalidade de um ataque DoS é tirar um serviço, servidor, computador ou até mesmo uma rede do ar. Os ataques do tipo DoS são usados muitas vezes em conjunto com invasões, ou porque alguns tipos de invasões exigem que determinados computadores não estejam funcionando (como no caso do spoofing) ou para despistar / desviar a atenção da invasão em si. Ataques DoS também são usados simplesmente para “atrapalhar” ou desacreditar um serviço.

Os ataques DoS na sua grande maioria usam buffer overflows para conseguir obter sucesso. Contudo, qualquer forma de tirar um computador, serviço ou rede do ar é considerado um ataque DoS. Por exemplo, a maioria dos servidores que possuem alguma segurança possuem também logs de acesso (arquivos de sistema onde são armazenadas informações críticas, como acesso, autenticação e etc). Imagine que o administrador coloque os logs no mesmo espaço em disco do sistema. Assim, se gerarmos milhares (talvez milhões) de entradas no log, o arquivo irá crescer até ocupar todo o disco. Outro tipo de ataque DoS comum: várias redes possuem programadas uma ação, caso um login tente por diversas efetuar login e erre suas credenciais. Esta ação geralmente é o bloqueio indeterminado da conta (login), que apenas pode ser restaurado com a intervenção do administrador. Forçar o travamento de uma conta destas é considerado um ataque DoS, principalmente quando esta conta é a usada por algum serviço (se a conta for bloqueada, o serviço sairá do ar).

Já ataques que visam tirar do ar uma rede, ou um servidor através de tráfego excessivo, ou enviando pacotes inválidos também são possíveis. Em meados de 1997, foi lançada na Internet uma vulnerabilidade em pilhas TCP/IP de computadores Windows. Consistia em enviar para um determinado serviço, pacotes TCP com uma sinalização de “urgência”. Contudo, o conteúdo do pacote era composto de caracteres inválidos. Este ataque DoS ficou conhecido como OOB (Out Of Band data). Hoje em dia, a grande maioria das pilhas TCP/IP é protegida contra este tipo de ataque, e variações. Porém, como no velho ditado “água mole em pedra dura tanto bate até que fura”, se a quantidade de informação inválida for realmente muito grande, ainda existe a possibilidade de tirar do ar o computador. Para se obter a quantidade suficiente de pacotes, o ataque do tipo DoS foi estendido, para o que conhecemos hoje como DDoS (Distributed Denial of Service).

Entretanto, devemos observar o fato de que o ataque DoS OOB, apesar de ter sido descoberto originalmente para a plataforma Windows (serviços NetBIOS / SMB), provou-se eficaz contra uma gama de protocolos e plataformas, incluindo diversos UNIX, e até equipamentos de rede.

DDoS (Distributed Denial of Service)

<http://staff.washington.edu/dittrich/misc/ddos/>

<http://www.research.att.com/~smb/talks/nanoq-dos/index.htm>

Os ataques do tipo DDoS consistem geralmente em enviar para uma única máquina ou rede, milhões de pacotes de rede ou requisições de serviço, em um dado momento. Obviamente, não existe maneira de gerar este tráfego todo de um único ponto.



Imagine que um computador, que chamaremos de "atacker", deseje derrubar o computador "vítima", com tráfego. Agora, de forma simples, imagine que nosso "atacker" está conectado via modem (50 Kbps) enquanto a "vítima" está conectada via ISDN (64 Kbps).

Neste Exemplo típico, podemos entender de forma fácil a dificuldade: por mais pacotes de rede que "atacker" envie para a "vítima", o canal de comunicação da vítima nunca ficará saturado.

Por sua vez, se os pacotes enviados utilizarem como transporte TCP, "atacker" corre o risco de "se derrubar", visto que para todo tráfego que ele gerar, a vítima tentará estabelecer uma conexão TCP (three way handshake). Daí, concluímos que praticamente todos os ataques do tipo DDoS utilizam UDP como transporte (se forem ataques direcionados).

Concluímos então como surgiu a idéia do DDoS: várias máquinas espalhadas por toda a Internet, enviando tráfego simultaneamente, para um mesmo servidor, estação ou rede. Assim, não importa o tamanho da conexão do servidor, estação ou rede, ela ficará potencialmente saturada.

O DDoS ficou conhecido a partir dos ataques realizados contra sites populares na Internet, como yahoo.com, amazon.com, zdnet.com, entre outros. Contudo, utilitários que exploram ou criam ataques DDoS, apesar de difíceis de obter, já existiam desde meados de 1999.

A lógica de um ataque DDoS é bem simples. Imagine um servidor de páginas web, que normalmente recebe 100.000 acessos por dia. Agora, imagine que 200 ou 300 computadores espalhados pela Internet, ao mesmo tempo, e continuamente, enviem requisições de acesso à página. Dependendo do número de requisições, o servidor poderá deixar de responder simplesmente porque chegou ao seu limite de conexões.

Existem outros tipos de pacotes ou requisições de conexão que têm uma eficácia muito maior do que uma simples requisição de acesso web. Contudo, o segredo está em como gerar este tráfego ou requisições, de várias máquinas espalhadas pela Internet. Isto é feito através de dois componentes de software: o agente ou server (software, programa ou "daemon" que é executado nas máquinas espalhadas pela Internet), e o cliente (componente que "controla" a ação dos agentes).

Os agentes ou servers são colocados para rodar em servidores espalhados pela Internet por hackers, que invadem os sistemas. Existe uma ferramenta de ataque DDoS chamada trin00 onde o agente é um vírus para a plataforma Windows (é colocado em execução em computadores como um trojan ou cavalo-de-tróia). Uma vez disseminados os agentes, o "hacker" através do cliente, envia um comando de ataque para os agentes, ao mesmo tempo, atacam uma determinada rede ou máquina.

Trin00, TFN (Tribe Flood Network, Schaft)

Estes são três exemplos clássicos de ferramentas de ataque DDoS. O trin00 já foi portado para a plataforma Windows, enquanto o TFN é o mais usado. Já o Schaft, apesar de relativamente antigo, é bem mais raro de ser achado. Atualmente, existe uma forma do agente do trin00 que infecta computadores como um cavalo-de-tróia. Já o TFN possui uma versão chamada TFN2K, com várias melhorias, incluindo até criptografia da conversação entre o cliente e os agentes, de forma a burlar a detecção destas ferramentas.

Em ambientes corporativos ligados à Internet, a forma mais comum de detecção é através da quantidade de tráfego. Na maioria das redes que possuem monitoração de tráfego, a característica será uma série de tentativas de conexão, ou tráfego, gerado de diversas máquinas da rede interna, para um único

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

endereço na Internet. Tráfego abundante utilizando como transporte o UDP também é sinal de um ataque DDoS, caso os pacotes tenham o mesmo destino, sejam saindo de sua rede, ou tentando entrar nela.

Contra estes tipos de ataques, existem poucas medidas, principalmente se o objetivo do “hacker” for realizar um ataque DDoS por ocupação de banda. Contudo, um bom firewall pode dificultar bastante a eficácia de um ataque destes. Algumas regras básicas de filtragem em firewalls para evitar ataques DDoS:

1. Filtrar qualquer tráfego ICMP entrando ou saindo da rede
2. Filtrar qualquer tráfego entrando na rede, em portas (serviços) que não estão em uso
3. Filtrar qualquer tráfego saindo da rede, a partir de computadores que fiquem 24 horas no ar, e que NÃO precisem emitir tal tráfego
4. No firewall, configurá-lo de forma a impedir conexões a partir do localhost (127.0.0.0)
5. De qualquer máquina que possua filtragem de pacotes (Windows 2000, Linux, etc.) impedir conexões a partir de interfaces internas e / ou localhost (127.0.0.0)

A regra básica é impedir tráfego não autorizado, não só “entrando” na rede, mas também, a partir dela, de forma que computadores em sua rede interna não possam ser usados como agentes. Veja o capítulo a seguir, “Ferramentas” / Personal Firewalls. Lá, filtragem de pacotes será tratada com maiores detalhes.

O que é mais importante percebermos no DDoS é a dificuldade de se proteger. Imagine que um ataque seja iniciado contra um host dentro da rede interna de sua empresa. Imagine também que o firewall da empresa não permita que o tráfego entre na rede interna, descartando todos os pacotes (UDP). Neste cenário, entenda que os pacotes chegaram até a porta do roteador, portanto, mesmo que o firewall descarte os mesmos, já ocuparam a banda do link de WAN. Neste caso, apesar do ataque não ter sido eficiente contra especificamente o servidor ou host em questão, irá tirar toda a rede do ar.

CodeRed I, CodeRed II, Nimda e afins

Apesar de serem considerados worms, ou vermes, uma espécie de vírus, eles possuem funções internas que se assemelham bastante a um ataque do tipo DDoS, apesar de não ser possível direcionar tais ataques.

Em 1988, a Internet foi assolada por um verme, ou prova de conceito criado por um estudante de graduação de Ciência da Computação, da Universidade de Cornell, nos Estados Unidos. O então desconhecido Sr. Robert Morris, não tinha a mínima idéia dos efeitos do código que tinha acabado de construir, e inicialmente, não pensava que sequer funcionasse.

O programa escrito por ele visava explorar uma falha no sendmail, software usado para troca de mensagens eletrônicas (email). Contudo, algo não saiu como planejado: o verme que acabara de construir entrou em colapso (loop infinito) ao infectar os servidores, e, como efeito disso, passou a utilizar todos os recursos dos servidores, como CPU e memória.

O caos se instalou nas principais instituições de ensino (universidades) e algumas instituições controladas pelo governo americano. Mais de 6000 hosts foram infectados pelo verme, e todos eles se transformaram em “zumbis”, ou agentes, na tentativa de propagar-se.

Em julho de 2001, a história se repetiu.

Code Red

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide "Distribuição / Cópia" neste material para maiores detalhes.

A Internet foi atacada novamente por um verme com as mesmas características. O Code Red, ou "Código Vermelho", utiliza uma falha no servidor web da Microsoft, o IIS - Internet Information Server, e, através desta falha, uma vez infectado, o servidor passa a se comportar como zumbi, ou agente, tentando de forma randômica, descobrir novos servidores que usem o IIS, vulnerável, para infectá-los.

<http://www.cert.org/advisories/CA-2001-19.html>

O mais interessante disso tudo, é que, 13 anos após o Internet Worm original, de Robert Morris, o mesmo princípio ainda obteve sucesso. Pior, um patch, ou atualização, que corrige a falha explorada pelo Code Red, tinha sido publicado um mês antes.

<http://www.microsoft.com/technet/security/bulletin/MS01-033.asp>

Entretanto, o primeiro Code Red, ou Code Red I, não possui uma carga que podemos classificar como realmente prejudicial ao servidor infectado. Não nos termos que incluem roubo ou comprometimento das informações. Seria mais adequado classificarmos o mesmo como uma prova de conceito, ou "proof of concept", apesar do aumento de tráfego que acarreta. Além disso, o seu código possui um bug. Ele gera randomicamente, endereços de rede (IP) que irá tentar infectar. O bug fez com que estes endereços não fossem realmente randômicos, fazendo com que o Code Red I atacasse uma faixa limitada de endereços, diminuindo seu raio de ação.

Uma análise COMPLETA do Code Red pode se encontrada em:

<http://www.eeye.com/html/advisories/codered.zip>

Code Red II

Como se não bastasse, pelo fato do Code Red I não possuir uma carga diretamente prejudicial, foi lançado na Internet uma nova versão, chamada Code Red II. Esta versão possui o bug corrigido, de forma que seu algoritmo usado para gerar endereços de rede funcione corretamente.

Além de gerar endereços de rede com maior eficiência, desta vez, trouxe uma carga extremamente prejudicial.

Ao ser infectado pelo verme em sua mais nova versão, o servidor terá a raiz de cada partição (unidades de disco) válidas adicionadas à estrutura de diretórios do servidor web. Isso faz com que qualquer arquivo em todo o servidor se torne disponível a Internet, através de um browser.

O verme também copia, para dentro do diretório /scripts do servidor web, uma cópia do arquivo cmd.exe. Este arquivo, no Windows NT 4.0 / 2000, é o prompt de comando. Com o comando certo enviado através de uma URL, para o servidor infectado, e com a ajuda do cmd.exe, é possível executar QUALQUER comando no mesmo, até mesmo criar um usuário, e adicioná-lo ao grupo de administradores.

Ele também cria um novo explorer.exe, na raiz do drive C:, que é executado quando alguém efetua login na console do servidor. Através dele que o Code Red II realiza a maioria de suas tarefas, como descrito acima.

Nimda / Code Rainbow

<http://www.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html>

O Nimda só não é considerado o worm mais perigoso de todos os tempos porque utiliza uma vulnerabilidade encontrada a quase um ano, e corrigida em 17 de outubro de 2000 (unicode traversal

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide "Distribuição / Cópia" neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide "Distribuição / Cópia" neste material para maiores detalhes.

vulnerability - Microsoft Bulletin MS00-078 - <http://www.microsoft.com/technet/security/bulletin/ms00-078.asp>).

O Nimda é tão perigoso porque alia às funções de um worm, três formas de contágio, uma delas normalmente encontrada em vírus hoje em dia: contaminação através de mensagens de correio eletrônico.

Para os três modos que o nimda pode infectar o sistema, em todas as três, ele usa falhas de segurança encontradas e consertadas a bastante tempo. De qualquer forma, é muito comum encontrarmos usuários e administradores de sistema que simplesmente não fazem seu dever de casa, atualizando seus computadores e servidores.

Ele infecta sistemas de forma quase idêntica ao Code Red - através de uma falha do servidor web IIS - Internet Information Server - apesar de não ser exatamente a mesma. Ele compartilha a partição que contém os arquivos de dados do servidor web, habilita a conta de "guest", e a coloca dentro do grupo de administradores (isso no Windows NT 4.0 / 2000).

Da mesma forma que o Code Red II, sistemas servidores infectados com o Nimda devem ser formatados e reinstalados, devido ao comprometimento de uma conta de administrador ou equivalente. O que mais impressiona neste worm é o fato de que ele também infecta através de mensagens de correio, e na visita de páginas infectadas (servidores web infectados pelo Nimda exibirão páginas que também contaminarão computadores que as visualizar - desde que não estejam atualizados).

Conclusões

Apesar do Internet Worm original, que aparentemente não foi colocado na Internet com a intenção de prejudicar computadores conectados à rede, os worms de hoje em dia são bem mais perigosos. Perceba que estes exploram falhas de segurança presentes em sistemas operacionais, já corrigidas a pelo menos um mês do início do contágio, o que levanta uma questão alarmante: administradores de sistema não estão cumprindo com suas tarefas básicas, como atualização / instalação de patches.

Também podemos concluir que daqui pra frente, com o aumento do poder computacional, iremos presenciar uma onda de worms e vírus cada vez mais sofisticados. Quase 100% dos vírus hoje em dia utilizam alguma funcionalidade de rede, seja para sua propagação, ou como sua funcionalidade principal.

E pensar que tudo isso poderia ter sido evitado apenas se os sistemas estivessem atualizados. Estudos comprovam que o Code Red I infectou cerca de 250.000 servidores pelo mundo, em apenas 9 horas, no dia 19 de julho de 2001. O Code Red II, que utiliza a mesma falha do Code Red I, ainda conseguiu atingir mais de 100.000 servidores. A análise dos worms indica que o Code Red II infectou TODOS os sistemas vulneráveis em menos de 48 horas. Além das falhas de segurança já explicadas, o Code Red foi responsável pelo aumento de cerca de 300% do tráfego na Internet, deixando toda a rede cerca de 3 vezes mais lenta; ou seja, afetando a todos, mesmo aqueles que não estavam vulneráveis ao ataque direto.

Outra lição que pode ser tirada destes acontecimentos recentes: como eles infectam servidores web, e realizam esta tarefa enviado comandos diretamente para qualquer servidor que encontrarem randomicamente, também foram responsáveis por tirar do ar equipamentos de rede que possuem servidores web embutidos, de diversos fabricantes, simplesmente porque estes componentes não possuíam uma checagem correta de buffers de entrada. Com isso, até equipamentos de rede como switches e roteadores foram afetados.

Para se proteger de worms e vírus no futuro, a melhor forma é manter o sistema atualizado, e com um bom antivírus instalado. Estas medidas teriam transformado estes worms em absolutamente... nada.

Apesar destes worms terem cargas potencialmente nocivas, e terem como seu objetivo principal explorar uma vulnerabilidade em um software servidor, causaram o efeito colateral de elevar em até 300% o tráfego na Internet. Vários computadores e equipamentos de rede foram tirados do ar devido ao tráfego

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide "Distribuição / Cópia" neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

causado pelos worms. Mesmo não tendo sido considerados ataques DDoS com uma natureza direcionada, acarretaram este efeito indiretamente. Este, por sinal, é o saldo mais perigoso e comentado sobre a ação dos mesmos.

IP Spoofing

<http://www.fc.net/phrack/files/p48/p48-14.html>

http://www.pcwebopedia.com/TERM/I/IP_spoofing.html

A técnica de spoofing possui uma lógica bastante simples. Muitos serviços antigos que são executados em hosts UNIX dependem de uma relação de confiança, baseada no endereço de rede de um determinado host. Digamos que um serviço determinado, só aceite comandos ou conexões de um computador que esteja em um determinado endereço IP pré-configurado. A técnica de spoofing consiste em “personificar” este computador na qual a vítima confia. Basicamente, precisa-se ter o endereço IP da vítima, o endereço IP do computador “confiado”, ter algum modo de tirar o computador “confiado” do ar, saber como quebrar o número de sequência TCP da vítima. Teoricamente, qualquer serviço que tenha sua segurança dependente apenas da confirmação de um endereço origem de rede, é vulnerável a este tipo de ataque. É uma técnica bastante apurada, e que requer geralmente uma certa dedicação. Nos anexos, a técnica é descrita em detalhes em um ótimo whitepaper.

Para maiores detalhes sobre como proteger uma rede de IP Spoofing, veja o capítulo “Ferramentas” / Personal Firewalls, que possui maiores detalhes sobre como implementar segurança com filtragem de pacotes.

DNS (Name Server) Spoofing / Poisoning

Como vimos anteriormente, o serviço de DNS adiciona uma nova camada de identificação para rede. As conexões são feitas através de endereços IP, que fecham “sockets”, descritos anteriormente. Contudo, fica praticamente impossível hoje em dia “decorar” centenas de endereços IP para tentar estabelecer uma conexão. Assim sendo, existe o serviço de DNS, que de certa forma elimina esta dificuldade. Ao invés de decorar endereços de rede, estes são associados a nomes, que obedecem a uma regra de nomenclatura bem específica. De acordo com esta regra, podemos identificar rapidamente um servidor ou serviço.

Contudo, a maioria das pessoas digita em seus programas de acesso endereços DNS ou FQDN (Fully Qualified Domain Name). Se você deseja acessar o site da Receita Federal, para tentar ler informações sobre sua declaração de imposto de renda, dificilmente digitará no browser:

<http://161.148.231.100>

É provável que digite:

<http://www.receita.fazenda.gov.br>

Ao digitar este endereço no seu browser, ele consultará o servidor DNS configurado em seu computador e perguntará: “qual o endereço IP do servidor www.receita.fazenda.gov.br ?” A resposta será: “161.148.231.100”. A partir daí, a conexão será estabelecida com o endereço IP destino.

O DNS Spoofing consiste em modificar as informações do servidor DNS de forma que a resposta seja diferente. Assim, seu computador acessará OUTRO servidor, sem seu conhecimento.

Além do spoofing, existe o poisoning. Todas as “perguntas” feitas a um servidor de DNS são guardadas, e aquelas perguntas mais frequentes são armazenadas, e reutilizadas, evitando gerar tráfego para cada requisição (se eu já sei a resposta de uma pergunta, não preciso fazê-la). O poisoning significa alterar

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

estas informações de “cache”, ou “mudar” a resposta para uma determinada pergunta que o servidor DNS já possui. Em resumo, ao perguntar para o servidor DNS “qual o endereço IP do servidor www.receita.fazenda.gov.br?”, ao invés de responder “161.148.231.100”, ele responderá outro endereço de rede, provavelmente de uma máquina previamente preparada por um hacker para tal fim.

Portanto, temos dois cenários:

1. Quando o servidor DNS é a autoridade de um domínio
2. Quando o servidor DNS não é a autoridade de um domínio, e resolve o IP pelo seu cache.

Nestes dois casos, o resultado é o mesmo. Contudo, esta técnica de ataque requer acesso ao servidor DNS, de forma a modificar o arquivo que contém as informações do domínio, ou modificar o cache do servidor.

7. Ferramentas

Existem diversas ferramentas prontas para testar vulnerabilidades em hosts, ou redes. Estas ferramentas podem ser classificadas basicamente em:

- Portscanners
- Service Fingerprinter
- Sniffer

Estas ferramentas são usadas para recuperar informações do computador remoto, ou da rede na qual ele está. Finalmente, estas informações são usadas para dar a vantagem ao invasor, que, numa segunda parte de um possível ataque, irá listar quais falhas de segurança cada componente descoberto possui.

Estas ferramentas não têm muita utilidade sozinhas, se não forem aliadas a algumas técnicas. Estas técnicas é que permitem explorar as falhas que as ferramentas podem potencialmente apresentar.

Portscanners

Portscanners são a base de qualquer tentativa de invasão. Da mesma forma, são a base para qualquer teste de vulnerabilidade que possa ser feito.

O portscan basicamente consiste em tentar estabelecer, com um determinado host, conexões TCP em todas as portas, da 0 a 65535. Devido ao princípio de negociação de conexão do TCP, o three-way handshake, para cada tentativa de conexão em uma porta aberta, o host que está sendo testado irá responder. Quando isto ocorre, sabemos então que a determinada porta está aberta.

Na maioria das implementações de pilhas TCP, mesmo que uma determinada porta não esteja aberta, geralmente o host responderá com uma recusa de conexão. Neste caso, sabemos que o host existe, está online, que a porta não está no ar, mas que provavelmente, não existe um firewall entre você e o host.

Chegamos a esta conclusão porque existe uma **diferença** entre “**connection refused**”, e “**connection time out**”. Quando uma conexão é recusada, o host envia um pacote de volta, determinando o estado da porta (fechada). Quando existe um firewall corretamente configurado, ele simplesmente descarta o pacote de requisição de conexão do portscanner, e o mesmo assumirá que a porta está fechada por time out (o pacote foi enviado, mas nenhuma resposta foi recebida, seja qual for).

Portanto, quando um hacker usa um portscanner e recebe “connection refused” como resposta, ele sabe que potencialmente, nenhum firewall existe. Quando um firewall está presente, e corretamente configurado, nenhum pacote de resposta será enviado, não importa de que tipo.

Isto implica em 2 resultados: se o firewall estiver presente, o portscan demorará minutos, às vezes, dezenas de minutos. Quando o host sendo testado responde com “connection refused”, o portscan demora poucos segundos.

Mais à frente, em “Introdução ao Conceito de Filtragem de Pacotes”, veremos que um firewall pode simular a rejeição de um pacote, ou o descarte do mesmo.

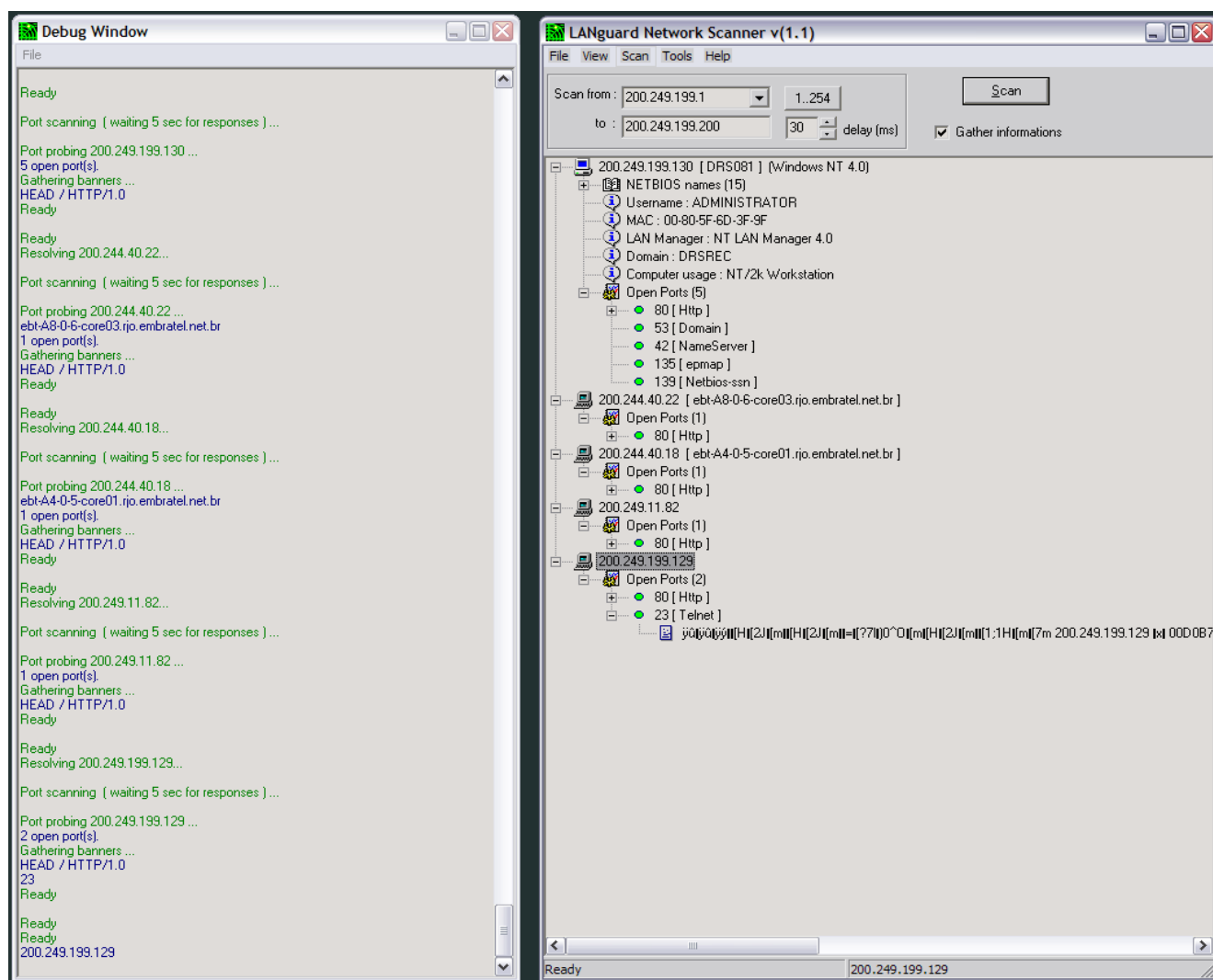
Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Existem diversos portscanners disponíveis na Internet. A maioria dos bons portscanners está disponível para a plataforma UNIX. Entretanto, existem opções interessantes para Windows, apesar de não tão poderosas (vide “nmap”, em “Técnicas de Invasão”).

Entretanto, devido à natureza de uma transferência de dados UDP, a maioria dos scanners usam TCP. Os que possuem a opção UDP não obtêm resultado confiável, pois uma porta UDP pode estar aberta, mas não enviar resposta caso a requisição não seja exata.

LANGuard Network Scanner

<http://www.gfi.com/lanselm/lanselmdownloads.htm>



O LANGuard Network Scanner é uma ferramenta poderosa para Windows. Ele reúne em um único utilitário um service fingerprinter, e um portscanner eficiente. Basta entrar com o endereço IP inicial, e o endereço IP final. Ele irá consultar cada um dos endereços no intervalo, e listar os serviços existentes. Além disso, captura as informações de cada porta.

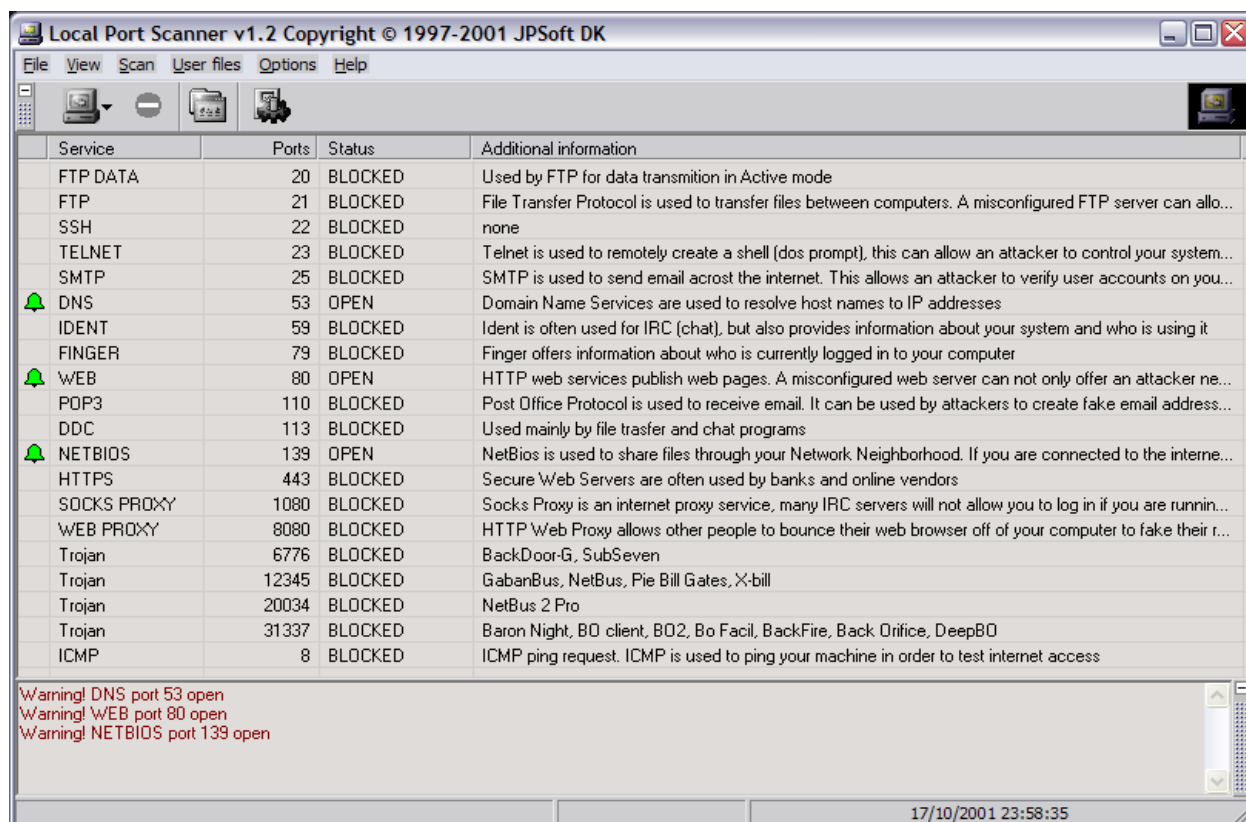
Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

LPS – Local Port Scanner

<http://www.jpsoft.dk/products.php>

Apesar de ser direcionado para scanear a máquina localmente, nada impede que seja informado qualquer endereço IP válido. É bem eficiente, e permite diversos modos de scan, como stealth, quick e full. Enquanto não sai uma compilação decente do NMAP para Windows, o LPS faz seu trabalho, mas costuma ser lento.



Services Fingerprinting

O service fingerprinting é uma técnica que consiste em determinar que serviço está rodando em uma determinada porta. Uma vez descoberto o serviço, determinar sua versão e revisão, se possível, e listar também vulnerabilidades.

O portscanner só faz parte do trabalho. É por isso que o service fingerprinting é considerado uma técnica, e não um programa ou utilitário (apesar de existirem programas que automatizam o processo, deixando a coisa mais fácil).

Se formos analisar de forma prática, veremos que o portscanner apenas detecta a presença de uma porta aberta, mas não identifica que serviço está rodando naquela porta. Um exemplo clássico disso são servidores Web (http) ou FTP rodando em portas diferentes do padrão, o que é perfeitamente possível e fácil de se fazer, e desejável quando se quer esconder este serviço. É muito comum vermos na Internet servidores Web rodando em portas como 8000, 8080, ou 8888, diferentes da porta padrão (80), ou servidores FTP rodando em portas como 2020, 2121 ou 2021 (diferentes do padrão 21).

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

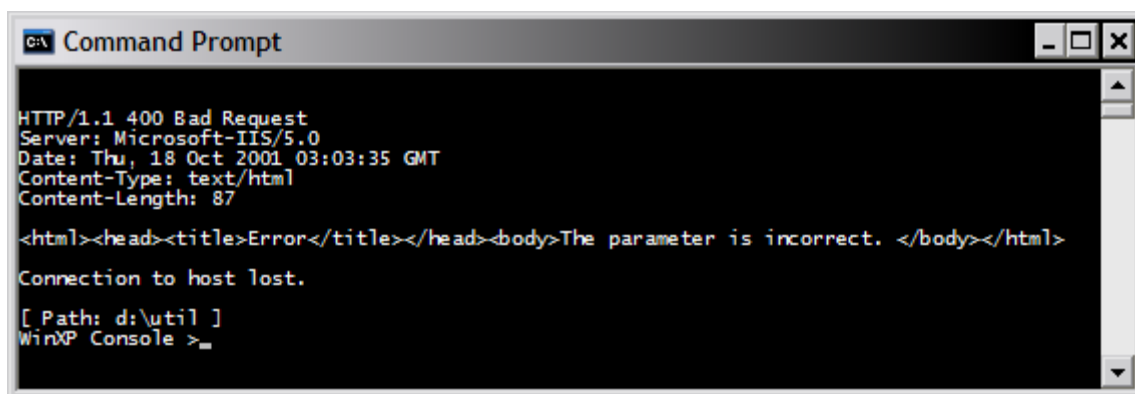
Além de tentar determinar o tipo de serviço presente em uma determinada porta, a técnica consiste em identificar qual o desenvolvedor / produtor do programa que disponibiliza serviço. Imagine que existem diversos servidores Web disponíveis no mercado, como Apache, Internet Information Server, Netscape Enterprise Server, entre outros, assim como dezenas de servidores FTP, como Internet Information Server, Serv-U, WFTPD, e etc.

Alguns dos programas usados para desenvolver esta técnica, além de classificarem o que está rodando em uma determinada porta, analisam sua versão e já classificam quais são as vulnerabilidades conhecidas do mesmo.

Todos os programas que ajudam nesta técnica utilizam padrões de resposta enviados durante uma conexão para tentar “adivinhar” qual o serviço que está em execução em uma determinada porta. Portanto, são sujeitos a falhas, e a melhor forma de analisar e utilizar a técnica é através de experiência, e manualmente.

Imagine que uma das formas mais eficientes de service fingerprinting é usar o telnet. Você estabelece uma conexão TCP com um determinado host, especificando uma porta, digita alguns comandos e descobre, na maioria dos casos, qual o programa que está rodando.

Exemplo 1: Servidor Web.



```
C:\ Command Prompt

HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Thu, 18 Oct 2001 03:03:35 GMT
Content-Type: text/html
Content-Length: 87

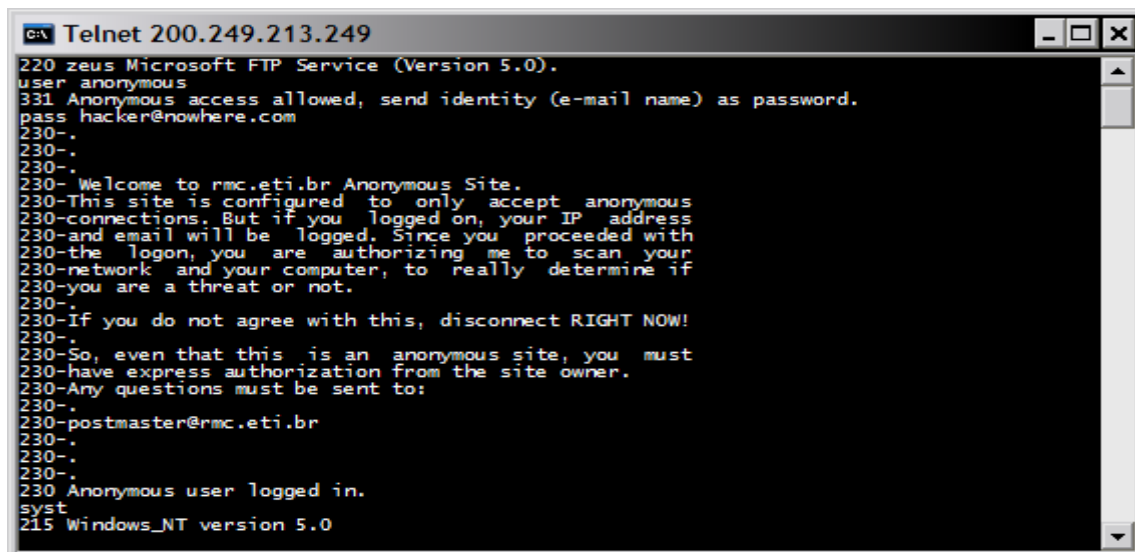
<html><head><title>Error</title></head><body>The parameter is incorrect. </body></html>

Connection to host lost.

[ Path: d:\util ]
WinXP Console >_
```

Um simples comando como “telnet endereço_ip 80”, e depois, “get ../..” (requisição inválida) nos revelou MUITA coisa. Sabemos agora que o servidor roda o Internet Information Server versão 5.0 (presente apenas em computadores Windows 2000). Descobriu-se com um comando simples, 2 informações primordiais.

Exemplo 2: Servidor FTP.



```
C:\ Telnet 200.249.213.249

220 zeus Microsoft FTP Service (Version 5.0).
user anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
pass hacker@nowhere.com
230-.
230-.
230-.
230- Welcome to rmc.eti.br Anonymous Site.
230-This site is configured to only accept anonymous
230-connections. But if you logged on, your IP address
230-and email will be logged. Since you proceeded with
230-the logon, you are authorizing me to scan your
230-network and your computer, to really determine if
230-you are a threat or not.
230-
230-If you do not agree with this, disconnect RIGHT NOW!
230-
230-So, even that this is an anonymous site, you must
230-have express authorization from the site owner.
230-Any questions must be sent to:
230-.
230-postmaster@rmc.eti.br
230-.
230-.
230-.
230- Anonymous user logged in.
syst
215 Windows_NT version 5.0
```

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

O comando “telnet endereço_ip 21” estabeleceu uma conexão com a porta 21 do servidor. Como podemos ver na imagem, ele já se identificou como um Windows NT 5.0 (Windows 2000). Através dos comandos “user” e “pass” foi efetuado login como usuário anônimo. Após o login, o comando “SYST” nos devolveu novamente a versão do sistema.

E toda ferramenta que foi necessária: o telnet do Windows.

No tópico “Automatização do Estudo de vulnerabilidades Conhecidas” ainda neste capítulo, veremos algumas das ferramentas básicas para service fingerprinting.

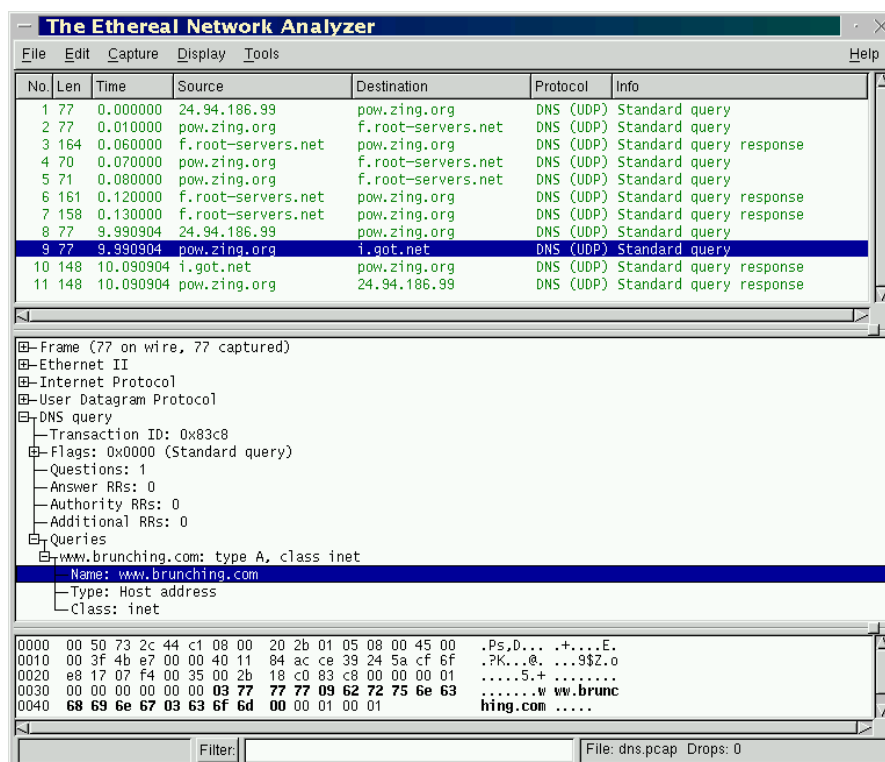
Sniffing

O sniffing é uma técnica bastante antiga, que explora uma vulnerabilidade de qualquer rede que possua tráfego compartilhado. Mais comum e simples de realizar em redes Ethernet, consiste em programar a interface de rede do computador para escutar todo e qualquer pacote de rede que por ela trafegue, independente do destinatário. Por padrão, as placas de rede somente retiram da rede aqueles pacotes endereçados fisicamente para si. Porém, você pode colocar a placa em modo “promíscuo”, que fará com que ela recupere da rede qualquer pacote que passar por ela. Assim, você poderá observar qualquer pacote que trafegue na rede.

Muitos serviços TCPIP antigos não utilizam criptografia para trocar senhas, transmitindo na rede informações de autenticação em modo texto, simples. Através de um software de sniffing, você pode observar todo o tráfego e eventualmente capturar usuários e senhas válidas para determinados serviços, como HTTP (Web), FTP (transferência de arquivos), TELNET (emulação de terminal, ou terminal remoto) e POP3 (leitura de correio eletrônico).

Alguns sistemas operacionais já vem equipados com sniffers. É o caso do Windows NT Server / Windows 2000 Server, e do Linux.

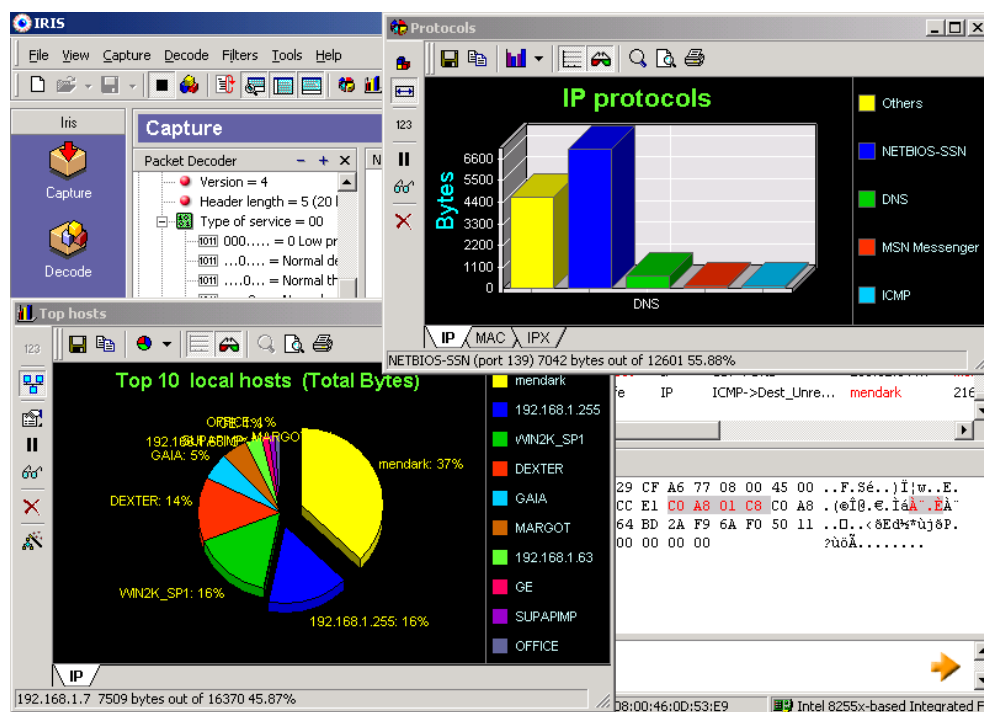
Entretanto, existem ótimos sniffers para Linux (os melhores são para sistemas UNIX, além de serem “free” ou open-source), como o Ethereal (<http://www.ethereal.com/>).



Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Para Windows, temos o Iris, da Eletronic Eye, que é pago, mas possui download de teste limitado por tempo (<http://www.eeye.com/html/Products/Iris/index.html>).



Automatização do Estudo de Vulnerabilidades Conhecidas

Como já foi explorado anteriormente, existem diversas ferramentas que automatizam a busca por vulnerabilidades. Estas ferramentas procedem da seguinte forma:

1. Realizam um portscan no host;
2. Identificam o sistema operacional;
3. Internamente, em seu banco de dados próprio, listam quais as vulnerabilidades conhecidas deste sistema operacional, e dos serviços detectados;
4. Testam as vulnerabilidades conhecidas, e listam as que obtiveram sucesso.

Os melhores programas com tais características geralmente são pagos, e custam caro. Eles incorporam as funcionalidades acima, e, além disso, fazem a atualização do banco de dados de vulnerabilidades frequentemente, através da Internet. Assim, sempre estarão testando por falhas que são atuais.

eEye Retina

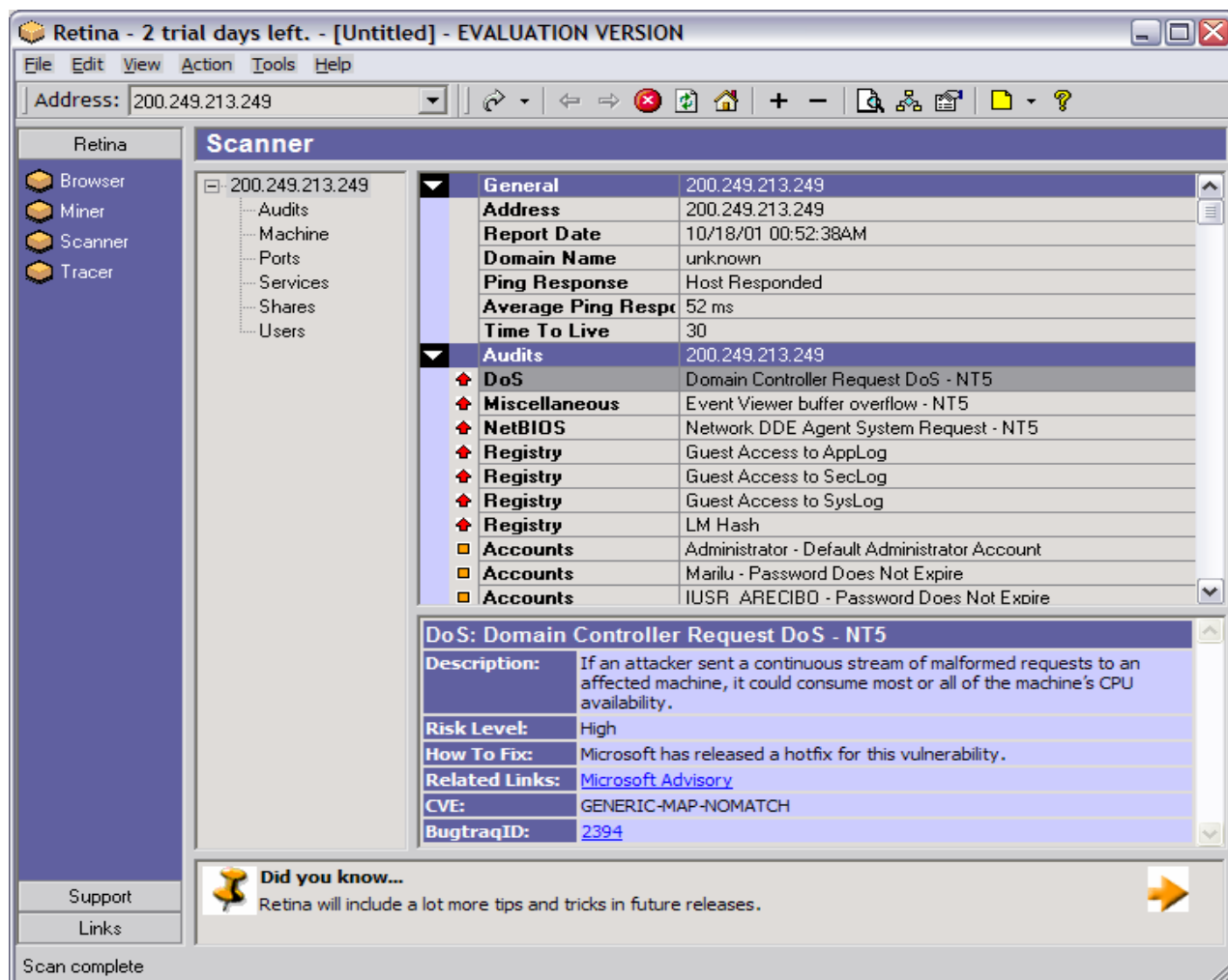
<http://www.eeye.com/html/Products/Retina/index.html>

O Retina é uma das ferramentas mais fantásticas disponíveis, para análise automatizada de segurança. Além de realizar os passos descritos acima, mostra, para cada vulnerabilidade encontrada, caso seja problema de bug ou furo no programa, o link para o site do fornecedor, contendo a correção. Caso seja um problema de configuração, mostrará onde obter a solução.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Infelizmente, a política comercial da eEye é bastante agressiva. Além dos preços serem bastante altos, é cobrado até o serviço de atualização. Entretanto, o site dispõe de versões de demonstração para download, com timebomb de 15 dias, o que já é mais do que o suficiente para se ter uma idéia de como o programa funciona.



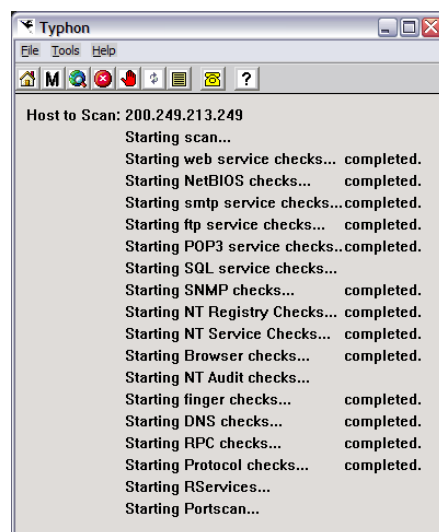
Typhon CIS (Cerberus Internet Scanner)

(<http://www.nextgenss.com/>)

(<http://www.cerberus-infosec.co.uk/cis.shtml>)

O Typhon já foi abordado em “técnicas de invasão”. Contudo, podemos dar uma olhada no que ele é capaz.

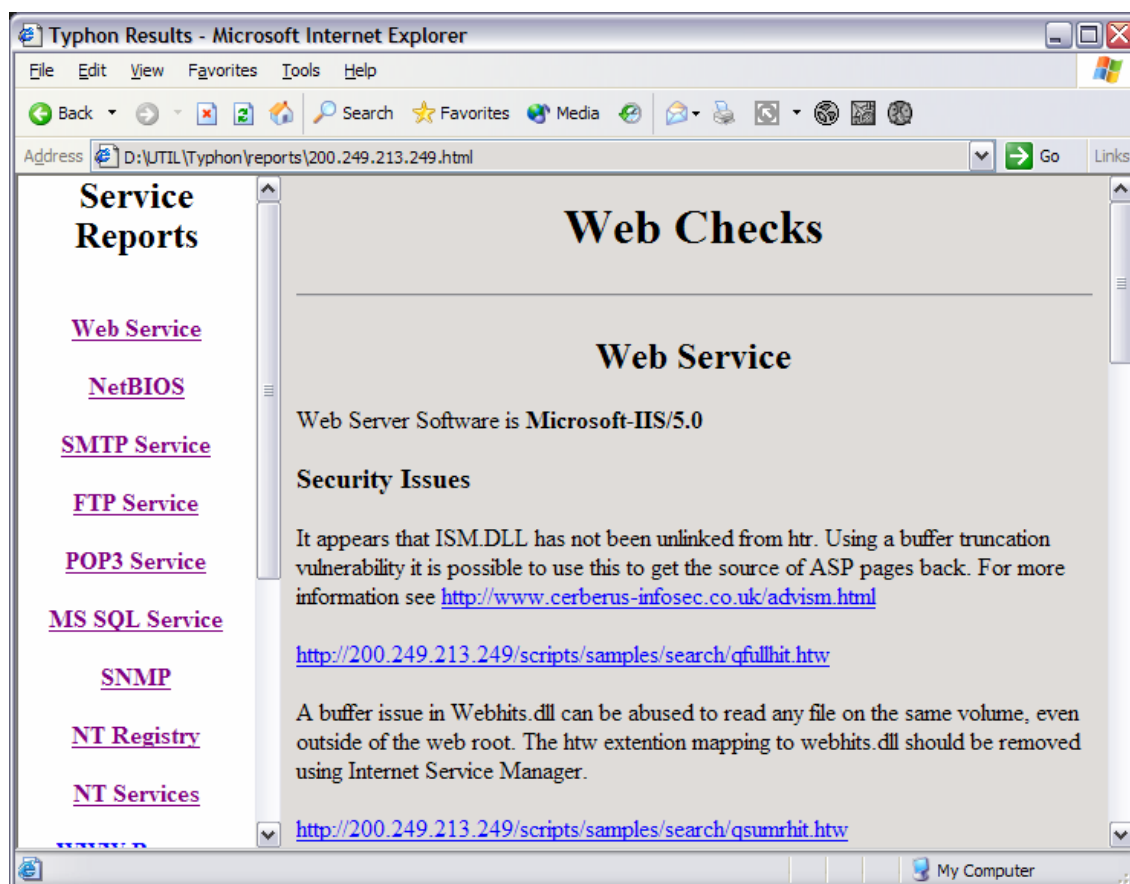
Ele possui módulos para testar cada um dos serviços ao lado. O mais interessante é que ele também funciona contra hosts UNIX, pois possui módulos para esta plataforma, tornando-o uma ferramenta valiosa, e sem custo algum.



Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Depois de realizar o teste no endereço de rede selecionado, o programa montará uma página com todos os detalhes do teste, e o que foi encontrado, como segue:



O Typhon é um programa pequeno e de grande ajuda na hora de realizar testes de vulnerabilidade. Contudo, é importante notar que, para um teste ter informações reais, e úteis, deve ser realizado de uma rede externa, e a partir de um computador que não possua nenhuma relação de confiança com o host a ser examinado, como usuário, senha, ou permissão no firewall. Caso esta observação não seja atendida, o teste não terá validade.

Essential Net Tools

(<http://www.tamos.com/>)

Talvez o programa mais difundido entre os “hackers wannabe”, pois torna a pesquisa de hosts vulneráveis, e o acesso a esses hosts, MUITO fácil. Entretanto, é voltado para apenas uma funcionalidade de rede, o NetBIOS / SMB (Server Message Block), que é a base de uma rede Microsoft, o que inclui todo e qualquer programa que seja compatível, como Samba (para UNIX).

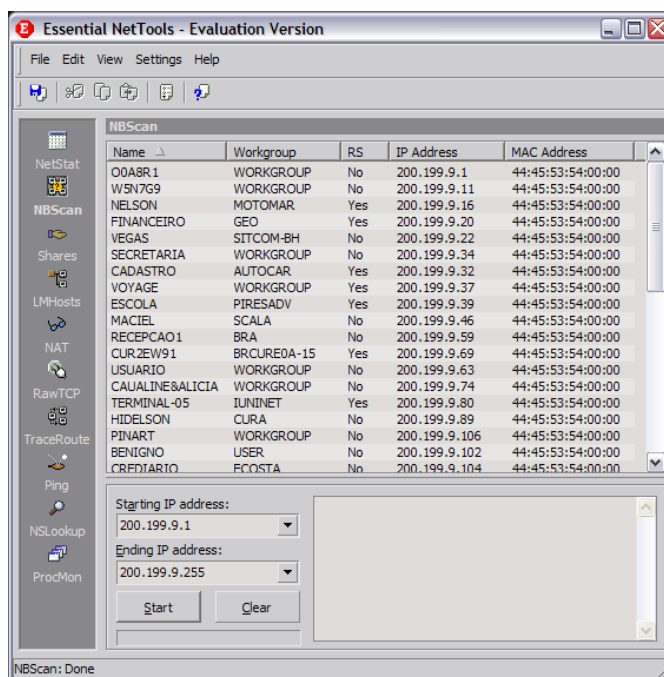
Essa ferramenta, como outras do gênero (como o rhino9 legion - <http://www.dsinet.org/tools/mirrors/rhino9/>), não explora uma falha de segurança no software da Microsoft, ou no Samba. Por sua vez, ela tenta achar falhas de configuração. Quanto a isto, é impressionante a quantidade de computadores conectados à Internet que demonstram tais falhas de configuração.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

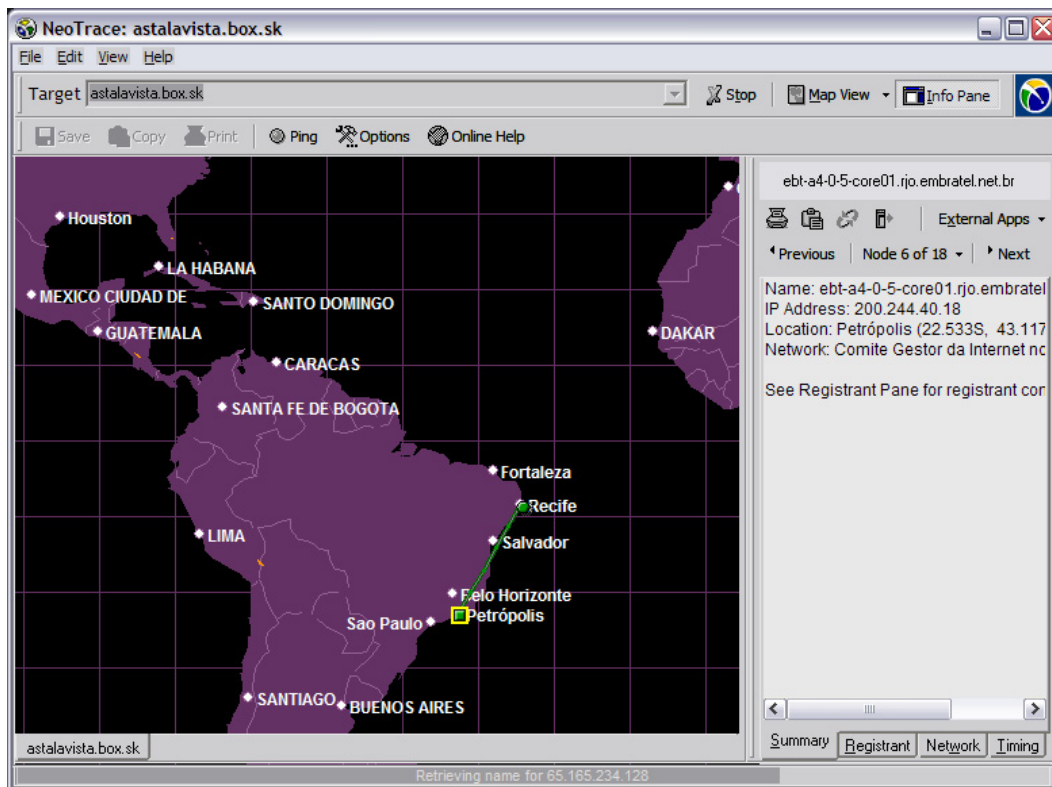
O Essential NetTools, em sua mais nova versão, traz uma série de utilitários interessantes. Ele agora incorpora um netstat em tempo real, um NAT (Netbios Auditing Tool), ou brute force para NetBIOS, traceroute, ping, nslookup e lista de processos.

Apesar de ser uma ferramenta bastante simples, ele demonstra claramente como existem computadores configurados de forma errada conectados à Internet. Isto, aliado ao fato de que tais ferramentas são fáceis de achar e usar, estabelecem um quadro bastante inseguro.



Neotrace

<http://www.neotrace.com>



Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

O Neotrace é um ótimo programa que permite, dado um endereço IP, traçar em um mapa mundi a rota que o pacote de dados percorre de seu computador até o destino. É um excelente recurso para descobrir a localização geográfica de potencial invasor, por exemplo.

Além de traçar a rota, ele identifica todas as redes as quais os endereços dos roteadores no meio do caminho pertencem.

Finalmente, é importante observar que nenhuma dessas ferramentas substitui a real experiência de um profissional qualificado.

Personal Firewalls

Introdução ao Conceito de Filtragem de Pacotes

Ao contrário do que muitos acham, um firewall não é um componente de software ou hardware (ou os dois). Um firewall é um conceito, uma série de regras, que devem ser implementadas, para que ao final, se consiga obter o “efeito” de firewalling.

Estas regras são bastante simples, contudo, imutáveis.

- “Todo o tráfego (em qualquer sentido que seja) deve passar pelo firewall
- Apenas tráfego autorizado, a partir da ACL (Access Control List) deverá passar pelo firewall, em qualquer dos sentidos
- O firewall em si deve ser imune à invasão.”

(Firewalls and Internet Security: Repelling the Wily Hacker
William Cheswick / Steven Bellovin)

Apesar destes conceitos, a idéia do firewall, ultimamente, tem sido bastante deturpada, infelizmente. Hoje em dia, temos no mercado diversos produtos denominados Personal Firewalls, ou firewalls pessoais, com a intenção de proteger o computador de ataques. Eles resumem as 3 premissas de um sistema firewall em um único produto, ou programa / software, que você pode instalar em seu computador.

Estes programas funcionam de forma bastante simples. Eles utilizam a forma universal de filtragem de pacotes para determinar se um determinado pacote de dados pode ou não passar. A nível lógico, eles ficam entre a interface de rede e o sistema operacional, atuando antes que o mesmo possa processar o dado.

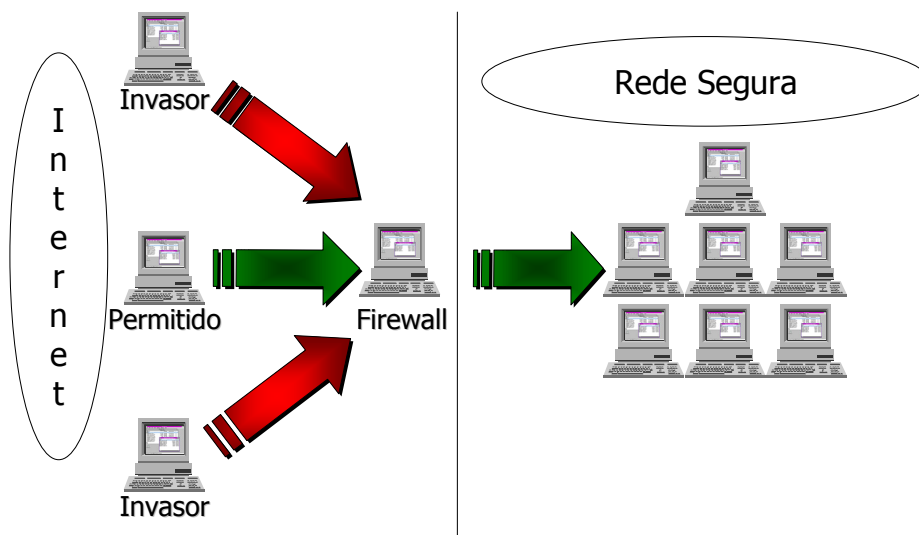
Padrão universal de filtragem de pacotes

Todo e qualquer componente de filtragem de pacotes, em qualquer esquema de firewall, seja via software ou hardware, utiliza o seguinte padrão:

| Função | Valor |
|------------------|--|
| Número | Número da regra ou identificador |
| Pol. | Aceitar (accept), Rejeitar (reject), Descartar (deny) pacote |
| Função / Sentido | Entrada (inbound), Saída (outbound), Repassagem (forward) |
| Interface | Designação da interface, A qual a regra será aplicada |
| Proto | TCP, UDP, ICMP |
| Origem | IP Origem |
| Destino | IP Destino |
| Opções | Opções de filtragem, como SYN, ACK, regra reversa, regra de exclusão |
| Logging | Habilitar ou não opções de logging |

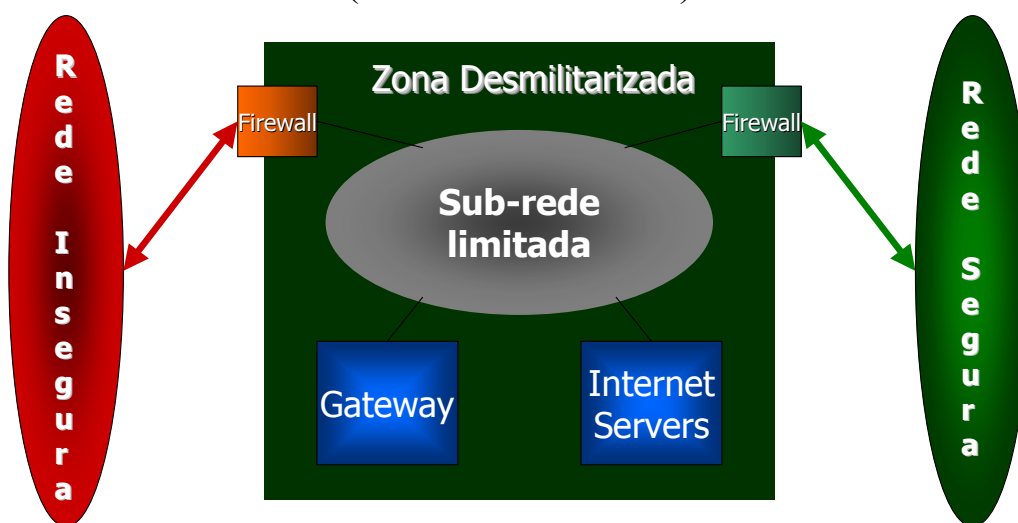
A seguir, vemos um esquema simples de firewall:

Firewalls: Filtragem



Existem outros modelos lógicos para uso com firewalls. O modelo mais eficiente é o de “zona desmilitarizada”. Nele, servidores e computadores críticos são protegidos tanto da rede interna quanto da rede externa. Veja:

Screened Zone / DMZ (Demilitarized Zone)



Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Componentes de filtragem de um firewall sempre usarão as funções acima. Entretanto, os personal firewalls associam tais funções à aplicação que está tentando acessar a rede, ou que está tentando colocar algum componente servidor no ar.

Portanto, os personal firewalls exibirão alertas baseados na utilização dos programas. Digamos por exemplo, que você acabou de instalar um personal firewall e, pela primeira vez, irá usar o correio eletrônico. Ao abrir o programa de correio, quando ele tentar acessar os servidores remotos para enviar ou receber mensagens, você receberá um alerta do personal firewall, identificando o programa, e qual a função que ele deseja realizar.

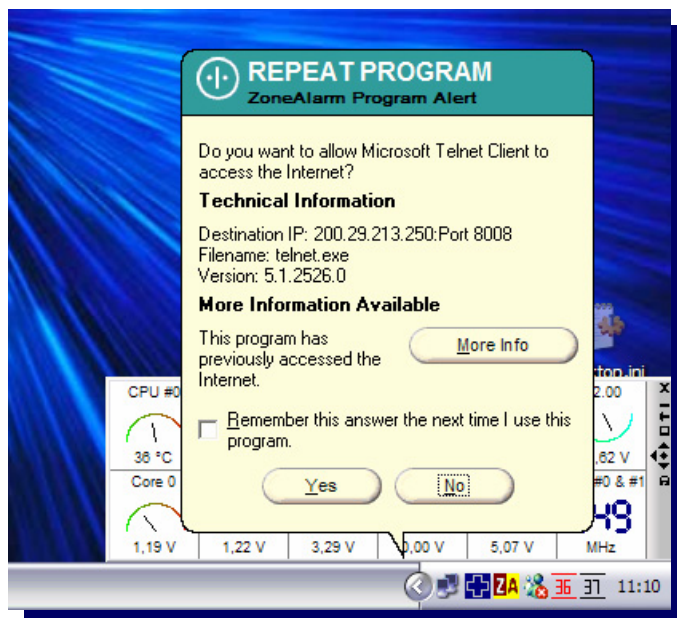
Esta é a parte mais importante para a correta configuração do mesmo.

Devemos sempre ficar alerta para programas que não conhecemos, que tentem acessar a rede. Nestes casos, podemos de forma fácil identificar um cavalo de tróia, por exemplo.

Veja:

No caso ao lado, o personal firewall detectou que a aplicação “Microsoft Telnet Client” está tentando acessar a Internet. Ele está tentando acesar o endereço IP 200.29.213.250, porta destino 8008.

Podemos também perceber ao lado que temos a opção de permitir ou não o acesso, bem como gravar nossa decisão para o futuro.



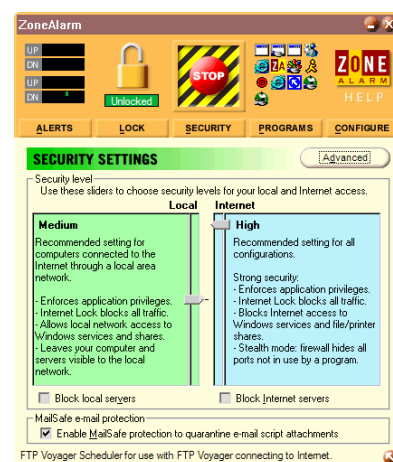
ZoneLabs ZoneAlarm

<http://www.zonealarm.com>

Definitivamente, o ZoneAlarm é o personal firewall para a plataforma Windows mais usado hoje em dia. Seu sucesso é devido ao fato de que ele torna um tipo de configuração potencialmente complicado, em algo relativamente fácil.

Ele separa a rede em duas áreas. As redes internas, tratadas como “local”, e a Internet, que é qualquer endereço que não esteja na área local. Assim, você pode ter duas configurações distintas, uma para cada área.

Infelizmente, o ZoneAlarm não permite a definição de regras complexas.



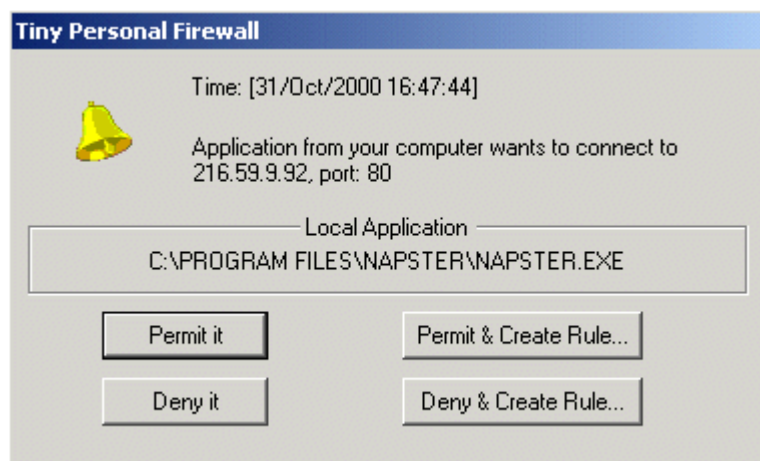
Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Tiny Pesonal Firewall

<http://www.tinysoftware.com/home/tiny?s=3782371648935103301A3&pg=download>

O TPF é tão eficiente quando o ZoneAlarm. Contudo, possui alguns recursos bem mais avançados. Ele permite a definição de regras, baseadas nas definições padrão (vide tabela). Além disso, permite também gerência remota.

O TPF é uma ótima opção para quem se sente já confortável com regras e filtragem de pacotes. Entretanto, é bem mais fácil cometer um engano com ele do que com o zonealarm.



Antivírus

Existem inúmeros antivírus no mercado. Entretanto, a grande maioria é paga, para a plataforma Windows. É difícil achar algum que seja gratuito. Um exemplo é o AVG, da Grisoft, que pode ser baixado de <http://www.grisoft.com>.

Basicamente, hoje em dia todos os programas antivírus permitem três tipos de funcionalidades. Proteção em tempo real (impede a armazenagem ou execução de arquivo infectado), proteção via email (cheça automaticamente todas as mensagens e limpa ou apaga vírus anexos) e a pesquisa de arquivos. Como atualmente a grande maioria dos vírus são espalhados via email, um bom antivírus que tenha integração com seu programa de emails é essencial.

8. Seu Computador Foi Invadido ?

A primeira reação natural é desligar o computador imediatamente. Contudo, apesar de parecer ser algo lógico para um usuário final, em uma empresa definitivamente não é a melhor abordagem.

O Que Fazer ?

Usuário final

O usuário terá muita dificuldade de detectar que foi invadido. A não ser que o hacker deixe sua “assinatura” dentro do computador, o típico usuário na grande maioria das vezes sequer saberá que alguém mexeu em seus arquivos, a não ser que possua algum utilitário para detectar uma invasão. Em todo caso, se isto for verdade, o usuário acabou de provar que o programa não funciona (...).

A primeira coisa que deve ser feita é instalar um bom antivírus e executá-lo fazendo uma varredura em todo o sistema. Isso eliminará a possibilidade de cavalos-de-troia. Caso não ache nada, então é muito provável que, se o seu computador for Windows, ele foi invadido pelo compartilhamento de arquivos e impressoras para redes Microsoft, ou por algum serviço que esteja sendo executado, como FTP ou HTTP.

Usuário Corporativo

Neste caso, o administrador da rede deve ser notificado **IMEDIATAMENTE**. **NÃO DESLIGUE**, ou desconecte o computador! Parte da análise que será feita depende inteiramente do fato de que o hacker ainda não sabe que foi descoberto. Simplesmente chame o administrador. Ele tomará alguma abordagem. Perceba que, do ponto de vista de um invasor, desconectar o computador da rede é praticamente a mesma coisa do que desligá-lo.

Precauções

"Jamais fale com estranhos na rua, ou aceite qualquer coisa de um estranho".

Mais uma vez, lembre-se que segurança é um hábito. Se seguir os procedimentos relacionados aqui, dificilmente alguém invadirá seu computador. Contudo, mesmo que você siga estes procedimentos, lembre-se também da segurança local. Não adianta tomar nenhuma precaução e deixar alguém mexer no seu computador inadvertidamente, ou sem acompanhamento. Da mesma forma, jamais use um computador compartilhado para digitar senhas ou informações sensíveis, **MESMO QUE** lhe dêem todas as seguranças possíveis e imagináveis.

Análise Forense

Assim como em qualquer estudo criminalístico, o estudo sério da criminalidade envolvendo informática também tem seu ramo de análise forense. Contudo, pela própria informalidade do ambiente de informática nas empresas, e pela ausência de um corpo de estudo criminalístico na polícia, o assunto é tratado como conto de fadas.

Grandes empresas que possuam uma infra-estrutura de TI proporcional terão provavelmente sua própria equipe de TI de segurança, e, conseqüentemente, de análise forense. Estudos mostram que a maioria dos ataques parte de dentro da empresa. Levando isso em consideração, faz-se necessária a presença de uma equipe que estude casos como por exemplo, proliferação de vírus. Porém, o objetivo principal da análise é a investigação de uma falha, com a intenção de colher evidências, que ajudem no processo de responsabilização, bem como no reparo dos danos e da própria falha.

O trabalho do investigador forense é baseado em provas digitais, dados armazenados em sistemas de informática. A característica destes dados é sua volatibilidade. Dados podem ser alterados com muita facilidade, estragando uma prova crucial, ou incriminando quem não tem nada a ver com a história.

O especialista em segurança deve:

- Colocar na mesma rede do computador / sistema comprometido um outro computador, geralmente um notebook, e analisar o tráfego
- Desconectar o computador da rede
- Analisar cada processo que o computador possui no ar
- Tentar recuperar cada log possível, retirá-lo do computador e guardá-lo em um local seguro

Só então o computador poderá ser desligado.

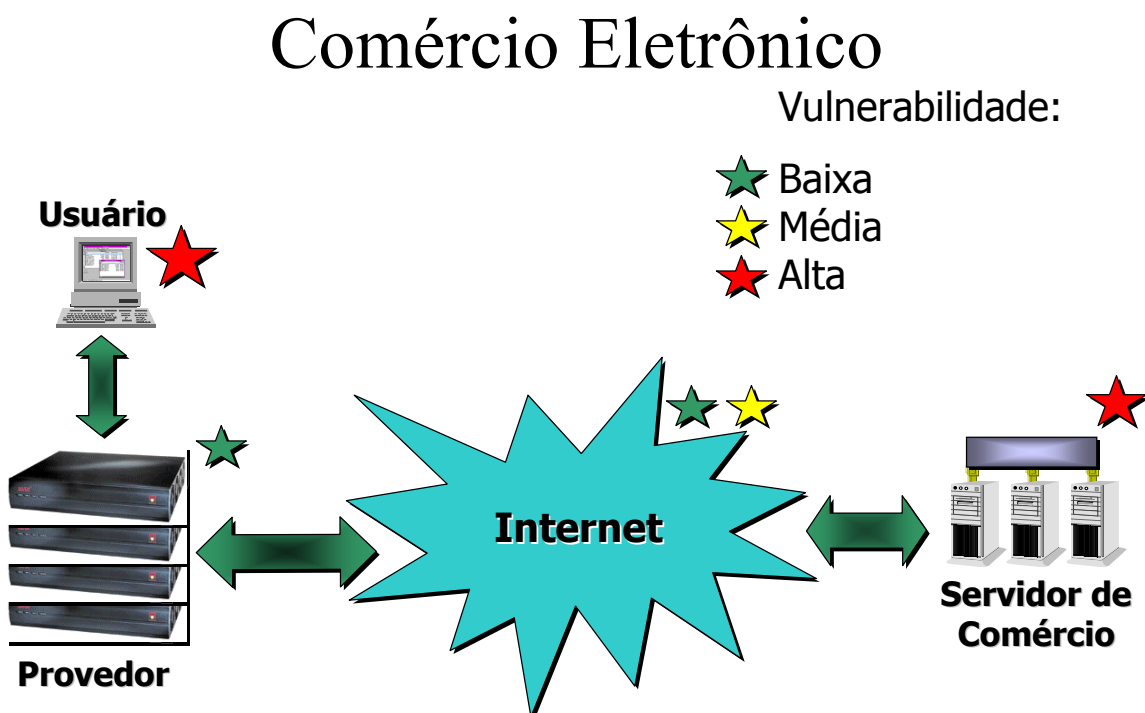
8. Comércio Eletrônico

Tecnicamente falando, a tecnologia envolvida com comércio eletrônico é relativamente segura. Contudo, a segurança ao se realizar uma transação bancária, por exemplo, depende de diversos fatores, não só da tecnologia ou da segurança que a instituição financeira possui.

Análise de Vulnerabilidades

Existem diversos pontos que são vulneráveis no comércio eletrônico. A típica conexão do usuário, até seu banco, no caso de home banking pela Internet, se parece com o seguinte diagrama:

<http://home.netscape.com/eng/ssl3/3-SPEC.HTM>
<http://www.setco.org/>



No diagrama acima, vemos claramente que o maior risco de segurança está no computador do próprio usuário. Se este estiver infectado com um cavalo-de-troia como o BO, todas as suas senhas, transações financeiras, enfim, tudo que estiver sendo digitado no teclado pode ser capturado para um arquivo e acessado por um suposto "hacker".

Muitos autores de segurança irão discutir o quão seguras são as soluções para comércio eletrônico. Realmente, a grande maioria das soluções **técnicas** é excelente. Contudo, o usuário leigo não possui o conceito ou conhecimento para separar até onde vai a tecnologia de seu computador, e onde se inicia a tecnologia da companhia telefônica ou do provedor de acesso, ou até mesmo da instituição financeira ou loja virtual que se está acessando. O usuário leigo enxerga todos estes elementos como um único serviço. Assim

sendo, ele não tomará as precauções necessárias com a segurança de seu computador, muitas vezes porque o serviço de comércio eletrônico lhe “disse” que o sistema era tão seguro que chegava a ser à prova de falhas. Hackers que desejem obter tais informações SEMPRE explorarão as FALHAS dos sistemas. Nunca irão de encontro com uma barreira praticamente intransponível: atacarão sempre o ponto mais frágil, mais vulnerável, aquele elo que pode ser “corrompido”. Neste caso, fácil até demais: o computador do usuário.

A grande maioria dos sites de comércio eletrônico usam três tecnologias (separadas ou em conjunto, na maioria das vezes). São elas:

- 1. SSL (Secure Sockets Layer)**
- 2. SET (Secure Eletronic Transactions)**
- 3. Shopping Carts**

O SSL é um padrão de criptografia desenvolvido pela Netscape, para criar um túnel seguro, onde todas as informações entre o browser do usuário e o site da loja ou instituição financeira são trocadas de forma criptografada. Acessar e quebrar as informações durante o tráfego é praticamente impossível. Contudo, estudos comprovam ser possível realizar tal façanha.

<http://developer.netscape.com/docs/manuals/security/sslin/contents.htm>

O padrão SET (Secure Eletronic Transactions) foi criado por administradoras de cartão de crédito, com a intenção de instituir um método capaz de impedir fraudes relativas a transações financeiras (geralmente compras através da Internet). A filosofia do sistema é bem simples: ao se comprar um produto numa loja virtual, você seleciona o(s) produto(s), e, na hora de efetuar o pagamento, através do SET, a cobrança é enviada diretamente do seu computador para a instituição financeira (digamos, a administradora do seu cartão de crédito). Assim, suas informações pessoais como o número do seu cartão NÃO são enviadas para a loja, e sim para administradora. A loja apenas recebe a confirmação do débito. Desta forma, mesmo que o site da loja seja atacado e suas informações sejam expostas, elas não conteriam em tese seu cadastro. Recentemente tivemos a invasão de uma grande loja de venda de CDs pela Internet, a CD Universe. Milhares de números de cartões de crédito foram comprometidos, o que forçou a empresa a entrar em um acordo com a administradora e emitir novos cartões para todos aqueles expostos. Um gasto de milhares de dólares, sem contar com o dano causado a imagem da empresa.

Os shopping carts são pequenos programas usados nos sites de comércio eletrônico que acompanham as páginas que você visitou recentemente no site, assim como que itens escolheu ultimamente, e que itens estão na sua relação de compra. A grande maioria deles utiliza “cookies”, pequenos textos que são trocados entre o seu browser e o site, para armazenar tais informações. Em sites que não possuem SET, ou que trabalham com programas de shopping carts de baixa qualidade / vulneráveis, eles podem gravar em cookies suas informações pessoais, sem criptografia, ou com criptografia fraca. Assim, qualquer um que tenha acesso ao seu computador localmente terá potencialmente acesso a tais arquivos. Algumas vezes, até senhas e números de cartões de crédito podem ser gravados em cookies. Como regra básica, não efetue transações de comércio eletrônico em computadores compartilhados. Mesmo assim, certifique-se que sua máquina está livre de cavalos-de-tróia antes de prosseguir.

O Quê Pode dar Errado

Alguns pontos podem dar errado em uma transação de comércio eletrônico. O primeiro deles é o computador do usuário possuir um cavalo-de-tróia instalado. O segundo ponto é o site em que se está realizando a transação não possuir criptografia SSL (a chave ou cadeado no canto inferior direito do browser, ou a URL não ser iniciada por https://). O terceiro ponto é o site comercial não fazer uso da tecnologia SET e armazenar números de cartões de crédito, assim como seu cadastro. Caso o site seja invadido, o será provavelmente porque os hackers buscavam tais informações.

9. Como Prevenir

Assim como a segurança é boa parte uma questão de hábito, a prevenção também. Existem várias formas de prevenir o comprometimento das informações, com pequenas alterações em programas, sem nenhum custo. Além disso, existem na Internet diversos utilitários que nos ajudam a manter seguros nossos sistemas, muitos deles sem custo algum.

Senhas

A primeira instância de segurança em qualquer sistema é sua senha. Escolha senhas difíceis. Uma senha difícil é aquela com no mínimo 12 caracteres, sem sentido, incluindo letras, números e caracteres especiais, como !, @, #, \$, e etc.

Correio Eletrônico

Como diz o ditado: “a curiosidade para o mal geralmente possui consequências maléficas”, tenha por hábito não abrir documentos ou programas anexos em mensagens de correio eletrônico. De forma análoga, evite baixar programas ou recebê-los através do ICQ por exemplo, sem saber sua procedência.

Antivírus

Tenha um antivírus instalado, mantenha-o sempre atualizado (pelo menos a cada 15 dias). Os antivírus atuais detectam cavalos-de-troia, o que quase que elimina a possibilidade de alguém tentar invadir seu computador através de um, desde que devidamente atualizado

Como Configurar Corretamente o Meu Acesso

Como discutido anteriormente, a maioria dos usuários da Internet não configura corretamente seus computadores. Além disso, o sistema operacional na maioria das vezes é o Windows 9x, que não possui nenhuma pretensão de ser seguro. Contudo, vimos que mesmo em sistemas operacionais que provém ferramentas para torná-lo seguro, algumas medidas são necessárias, como discutido no módulo “Sistema Operacional”.

A principal checagem é ver se o componente “Compartilhamento de arquivos e impressoras para redes Microsoft” está instalado. Se for um computador com APENAS acesso a Internet, que não participe de nenhuma rede, este componente pode ser removido. No caso do Windows NT / 2000, da mesma forma, o “Server Service” pode ser parado caso o computador não participe de nenhuma rede.

Informação é o Melhor Remédio (“Full Disclosure”)

Muitos programas, sistemas operacionais e até sistemas de informação baseiam sua segurança na ausência de informações. Seria mais ou menos como dizer que sua casa está segura porque não existe nenhum ladrão que “conheça” seu endereço, e não porque a fechadura da porta da frente é eficaz. No mundo da informática, seria o equivalente a alegar que um produto, software ou sistema operacional é seguro porque ninguém sabe como ele funciona, e não porque ele realmente possui qualidades de segurança. Boa parte da comunidade de especialistas hoje em dia segue pelo caminho do “full disclosure”, ou conhecimento aberto para todos. Isso implica em um aumento da segurança em ordens de grandeza, mas também, no número de ameaças, afinal, da mesma forma que os especialistas em segurança terão acesso às informações, os hackers também terão. Contudo, agindo assim a comunidade terá muito mais recursos para resolver qualquer

problema no menor tempo possível. Além disso, a comunidade exercerá maior pressão nas empresas para que consertem os problemas em tempo recorde.

Informação Moderada é o Melhor Remédio ? ("Responsible Disclosure")

Hoje em dia, é comum ver o comportamento de “informação moderada” nas principais listas de discussão sobre segurança. Ao contrário da filosofia de liberar qualquer informação, potencialmente danosa, ou não, apenas avisos de vulnerabilidades são publicados, mas NÃO os exploits, ou código que permita explorar uma falha.

Querendo ou não, este tipo de abordagem diminui ou retarda a disseminação de ataques. Contudo, não previne. A única forma ainda continua sendo a informação: se manter atualizado, informado diretamente dos canais de divulgação, sobre vulnerabilidades e suas correções.

Firewall (Incluindo Personal Firewall)

Como o nome sugere (do inglês, “parede ou porta corta fogo”), os firewalls são esquemas de hardware, software, ou os dois juntos, capazes de, baseados em características do tráfego, permitir ou não a passagem deste tráfego. Basicamente, o firewall analisa informações como endereço de origem, endereço de destino, transporte, protocolo, e serviço ou porta. Para cada pacote que passar pelo firewall, ele consultará uma ACL (Access Control List, ou lista de controle de acessos), que é uma espécie de tabela de regras, que contém informações sobre que tipo de pacote pode ou não passar. Baseado nesta informação rejeita ou repassa o dado. Contudo, ao contrário do que muitos pensam, um firewall não é apenas UM produto, seja hardware ou software. O firewall é um CONJUNTO de componentes, geralmente compostos por hardware e software.

Para maiores detalhes sobre firewalls, veja o capítulo sobre “Personal Firewalls”.

IDS (Intrusion Detection Systems)

Os IDS são sistemas avançados capazes de detectar, em tempo real, quando um ataque está sendo realizado e, baseado nas características do ataque, alterar sua configuração ou remodelá-la de acordo com as necessidades, e até avisar o administrador do ambiente sobre o ataque. Sistemas de IDS são geralmente caros, e exigem certas modificações na rede. Na maioria das vezes está acoplado a um sistema de firewall, ou possui este embutido.

Os IDS são sistemas descentralizados, com a filosofia de agentes e servidores. Componentes instalados nos equipamentos, estações de trabalho e / ou servidores, monitoram as atividades da rede, e reportam a um servidor. Este servidor, obedecendo a uma série de regras de comportamento, toma a atitude designada para cada tipo de ocorrência.

Existem também computadores ou agentes autônomos, que possuem a única função de analisar todo o tráfego da rede e submeter os resultados para o servidor central. Estes agentes funcionam porque numa rede ethernet (apdrão usado em 98% das redes locais) todo o tráfego é compartilhado. Portanto, este agente terá sua interface de rede em modo promíscuo, apenas para capturar todo o tráfego, ou “sniffar” a rede, a procura de algum padrão suspeito.

Para maiores informações, existe um ótimo documento sobre IDS que pode ser acessado em:

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm

-- x --

Trust no one. Be afraid, be very afraid”.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Anexos

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Lista de Portas TCP/UDP Usadas Por Cavalos-de-Tróia e Programas Afins

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide "Distribuição / Cópia" neste material para maiores detalhes.

Lista atualizada em 17/03/2000. Listas atualizadas podem ser encontradas em:
<http://www.simovits.com/nyheter9902.html>

--

port 2 - Death
port 21 - Back Construction, Blade Runner, Doly Trojan, Fore, FTP trojan, Invisible FTP, Larva, Net Administrator, Senna Spy FTP Server, WebEx, WinCrash
port 23 - Tiny Telnet Server, Truva At1
port 25 - Ajan, Antigen, Email Password Sender, Haebu Coceda (Naebi), Happy 99, Kuang2, NewApt, ProMail trojan, Shtrilitz, Stealth, Tapiras, Terminator, WinPC, WinSpy
port 31 - Agent 31, Hackers Paradise, Masters Paradise
port 41 - DeepThroat
port 48 - DRAT
port 50 - DRAT
port 59 - DMSetup
port 79 - Firehotcker
port 80 - Executor, Hooker, RingZero
port 99 - Hidden Port
port 110 - ProMail trojan
port 113 - Kazimas
port 119 - Happy 99
port 121 - JammerKillah
port 123 - Net Controller
port 146 - Infector
port 146 (UDP) - Infector
port 421 - TCP Wrappers
port 456 - Hackers Paradise
port 531 - Rasmin
port 555 - Ini-Killer, NeTAdministrator, Phase Zero, Stealth Spy
port 605 - Secret Service
port 666 - Attack FTP, Back Construction, Satanz Backdoor, ServeU,
port 777 - Aim Spy
port 911 - Dark Shadow
port 999 - DeepThroat, winSatan
port 1000 - Der Spacher 3
port 1001 - Der Spacher 3, Silencer, WebEx
port 1010 - Doly Trojan
port 1011 - Doly Trojan
port 1012 - Doly Trojan
port 1015 - Doly Trojan
port 1020 - Vampire
port 1024 - NetSpy
port 1042 - Bla
port 1045 - Rasmin
port 1050 - MiniCommand
port 1080 - WinHole
port 1090 - Xtreme
port 1095 - RAT
port 1097 - RAT
port 1098 - RAT
port 1099 - RAT
port 1170 - Psyber Stream Server, Streaming Audio trojan, Voice
port 1200 (UDP - NoBackO
port 1201 (UDP - NoBackO
port 1207 - SoftWAR
port 1234 - Ultors Trojan
port 1243 - BackDoor-G, SubSeven, SubSeven Apocalypse
port 1245 - Voodoo Doll
port 1269 - Mavericks Matrix
port 1313 - NETrojan
port 1349 (UDP) - BO DLL
port 1492 - FTP99CMP
port 1509 - Psyber Streaming Server
port 1600 - Shivka-Burka
port 1807 - SpySender
port 1969 - OpC BO
port 1981 - Shockrave
port 1999 - BackDoor, TransScout
port 2000 - Der Spaeher 3, Insane Network, TransScout
port 2001 - Der Spaeher 3, TransScout, Trojan Cow
port 2002 - TransScout
port 2003 - TransScout
port 2004 - TransScout
port 2005 - TransScout
port 2023 - Ripper
port 2115 - Bugs

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide "Distribuição / Cópia" neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

port 2140 - Deep Throat, The Invasor
port 2155 - Illusion Mailer
port 2283 - HVL Rat5
port 2300 - Xplorer
port 2565 - Striker
port 2583 - WinCrash
port 2600 - Digital RootBeer
port 2716 - The Prayer
port 2773 - SubSeven
port 2801 - Phineas Phucker
port 3024 - WinCrash
port 3128 - RingZero
port 3129 - Masters Paradise
port 3150 - Deep Throat, The Invasor
port 3456 - Terror Trojan
port 3459 - Eclipse 2000
port 3700 - Portal of Doom
port 3791 - Eclipse
port 3801 (UDP) - Eclipse
port 4092 - WinCrash
port 4242 - Virtual Hacking Machine
port 4321 - BoBo
port 4567 - File Nail
port 4590 - ICQTrojan
port 5000 - Bubbel, Back Door Setup, Sockets de Troie
port 5001 - Back Door Setup, Sockets de Troie
port 5011 - One of the Last Trojans (OOTLT)
port 5031 - NetMetropolitan
port 5031 - NetMetropolitan
port 5321 - Firehotcker
port 5400 - Blade Runner, Back Construction
port 5401 - Blade Runner, Back Construction
port 5402 - Blade Runner, Back Construction
port 5550 - Xtcp
port 5512 - Illusion Mailer
port 5555 - ServeMe
port 5556 - BO Facil
port 5557 - BO Facil
port 5569 - Robo-Hack
port 5637 - PC Crasher
port 5638 - PC Crasher
port 5742 - WinCrash
port 6000 - The Thing
port 6272 - Secret Service
port 6400 - The Thing
port 6667 - ScheduleAgent
port 6669 - Host Control, Vampire
port 6670 - DeepThroat
port 6711 - SubSeven
port 6712 - SubSeven
port 6713 - SubSeven
port 6771 - DeepThroat
port 6776 - 2000 Cracks, BackDoor-G, SubSeven
port 6912 - Shit Heep (not port 69123!)
port 6939 - Indoctrination
port 6969 - GateCrasher, Priority, IRC 3
port 6970 - GateCrasher
port 7000 - Remote Grab, Kazimas, SubSeven
port 7215 - SubSeven
port 7300 - NetMonitor
port 7301 - NetMonitor
port 7306 - NetMonitor
port 7307 - NetMonitor
port 7308 - NetMonitor
port 7789 - Back Door Setup, ICKiller
port 8080 - RingZero
port 8787 - Back Orifice 2000
port 8897 - HackOffice
port 8989 - Rcon
port 9400 - InCommand
port 9872 - Portal of Doom
port 9873 - Portal of Doom
port 9874 - Portal of Doom
port 9875 - Portal of Doom
port 9876 - Cyber Attacker
port 9878 - TransScout
port 9989 - iNi-Killer
port 9999 - The Prayer
port 10067 (UDP) - Portal of Doom
port 10086 - Syphillis
port 10101 - BrainSpy
port 10167 (UDP) - Portal of Doom
port 10520 - Acid Shivers

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

port 10607 - Coma
port 10666 (UDP) - Ambush
port 11000 - Senna Spy
port 11050 - Host Control
port 11223 - Progenic trojan, Secret Agent
port 12076 - Gjamer
port 12223 - Hack'99 KeyLogger
port 12345 - GabanBus, NetBus, Pie Bill Gates, X-bill
port 12346 - GabanBus, NetBus, X-bill
port 12349 - BioNet
port 12361 - Whack-a-mole
port 12362 - Whack-a-mole
port 12623 (UDP) - DUN Control
port 12631 - WhackJob
port 13000 - Senna Spy
port 16484 - Mosucker
port 16772 - ICQ Revenge
port 16969 - Priority
port 17300 - Kuang2 The Virus
port 17777 - Nephron
port 19864 - ICQ Revenge
port 20001 - Millennium
port 20034 - NetBus 2 Pro
port 20203 - Chupacabra, Logged
port 20331 - B!a
port 21544 - GirlFriend
port 22222 - Prosiak
port 23456 - Evil FTP, Ugly FTP, Whack Job
port 23476 - Donald Dick
port 23477 - Donald Dick
port 26274 (UDP) - Delta Source
port 27374 - SubSeven
port 27573 - SubSeven
port 29891 (UDP) - The Unexplained
port 30029 - AOL Trojan
port 30100 - NetSphere
port 30101 - NetSphere
port 30102 - NetSphere
port 30303 - Sockets de Troie
port 30999 - Kuang2
port 31336 - Bo Whack
port 31337 - Baron Night, BO client, BO2, Bo Facil
port 31337 (UDP) - BackFire, Back Orifice, DeepBO
port 31338 - NetSpy DK
port 31338 (UDP) - Back Orifice, DeepBO
port 31339 - NetSpy DK
port 31666 - BOWhack
port 31785 - Hack'a'Tack
port 31787 - Hack'a'Tack
port 31788 - Hack'a'Tack
port 31789 (UDP) - Hack'a'Tack
port 31791 (UDP) - Hack'a'Tack
port 31792 - Hack'a'Tack
port 32418 - Acid Battery
port 33333 - Prosiak
port 33911 - Spirit 2001a
port 34324 - BigGluck, TN
port 34555 (UDP) - Trinoo
port 35555 (UDP) - Trinoo
port 37651 - YAT
port 40412 - The Spy
port 40421 - Agent 40421, Masters Paradise
port 40422 - Masters Paradise
port 40423 - Masters Paradise
port 40426 - Masters Paradise
port 47262 (UDP) - Delta Source
port 50505 - Sockets de Troie
port 50766 - Fore, Schwindler
port 52317 - Acid Battery 2000
port 53001 - Remote Windows Shutdown
port 54283 - SubSeven
port 54320 - Back Orifice 2000
port 54321 - School Bus
port 54321 (UDP) - Back orifice 2000
port 57341 - NetRaider
port 60000 - Deep Throat
port 61348 - Bunker-Hill
port 61466 - Telecommando
port 61603 - Bunker-Hill
port 63485 - Bunker-Hill
port 65000 - Devil
port 65432 - The Traitor

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

port 65432 (UDP) - The Traitor
port 65535 - RC

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Portas TCP/UDP Privilegiadas: 0 à 1024 (Well Known Port Numbers)

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

| Keyword | Decimal | Description | References |
|-------------|---------|------------------------------|------------|
| | 0/tcp | Reserved | |
| | 0/udp | Reserved | |
| # | | Jon Postel | |
| tcpmux | 1/tcp | TCP Port Service Multiplexer | |
| tcpmux | 1/udp | TCP Port Service Multiplexer | |
| # | | Mark Lottor | |
| compressnet | 2/tcp | Management Utility | |
| compressnet | 2/udp | Management Utility | |
| compressnet | 3/tcp | Compression Process | |
| compressnet | 3/udp | Compression Process | |
| # | | Bernie Volz | |
| # | 4/tcp | Unassigned | |
| # | 4/udp | Unassigned | |
| rje | 5/tcp | Remote Job Entry | |
| rje | 5/udp | Remote Job Entry | |
| # | | Jon Postel | |
| # | 6/tcp | Unassigned | |
| # | 6/udp | Unassigned | |
| echo | 7/tcp | Echo | |
| echo | 7/udp | Echo | |
| # | | Jon Postel | |
| # | 8/tcp | Unassigned | |
| # | 8/udp | Unassigned | |
| discard | 9/tcp | Discard | |
| discard | 9/udp | Discard | |
| # | | Jon Postel | |
| # | 10/tcp | Unassigned | |
| # | 10/udp | Unassigned | |
| systat | 11/tcp | Active Users | |
| systat | 11/udp | Active Users | |
| # | | Jon Postel | |
| # | 12/tcp | Unassigned | |
| # | 12/udp | Unassigned | |
| daytime | 13/tcp | Daytime | |
| daytime | 13/udp | Daytime | |
| # | | Jon Postel | |
| # | 14/tcp | Unassigned | |
| # | 14/udp | Unassigned | |
| # | 15/tcp | Unassigned [was netstat] | |
| # | 15/udp | Unassigned | |
| # | 16/tcp | Unassigned | |
| # | 16/udp | Unassigned | |
| qotd | 17/tcp | Quote of the Day | |
| qotd | 17/udp | Quote of the Day | |
| # | | Jon Postel | |
| msp | 18/tcp | Message Send Protocol | |
| msp | 18/udp | Message Send Protocol | |
| # | | Rina Nathaniel <---none---> | |
| chargen | 19/tcp | Character Generator | |
| chargen | 19/udp | Character Generator | |
| ftp-data | 20/tcp | File Transfer [Default Data] | |
| ftp-data | 20/udp | File Transfer [Default Data] | |
| ftp | 21/tcp | File Transfer [Control] | |
| ftp | 21/udp | File Transfer [Control] | |
| # | | Jon Postel | |
| # | 22/tcp | Unassigned | |
| # | 22/udp | Unassigned | |
| telnet | 23/tcp | Telnet | |
| telnet | 23/udp | Telnet | |
| # | | Jon Postel | |
| | 24/tcp | any private mail system | |
| | 24/udp | any private mail system | |
| # | | Rick Adam | |
| smtp | 25/tcp | Simple Mail Transfer | |
| smtp | 25/udp | Simple Mail Transfer | |
| # | | Jon Postel | |
| # | 26/tcp | Unassigned | |
| # | 26/udp | Unassigned | |
| nsw-fe | 27/tcp | NSW User System FE | |
| nsw-fe | 27/udp | NSW User System FE | |
| # | | Robert Thomas | |
| # | 28/tcp | Unassigned | |
| # | 28/udp | Unassigned | |
| msg-icp | 29/tcp | MSG ICP | |
| msg-icp | 29/udp | MSG ICP | |
| # | | Robert Thomas | |
| # | 30/tcp | Unassigned | |
| # | 30/udp | Unassigned | |
| msg-auth | 31/tcp | MSG Authentication | |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

| | | |
|------------|--------|----------------------------------|
| msg-auth | 31/udp | MSG Authentication |
| # | | Robert Thomas |
| # | 32/tcp | Unassigned |
| # | 32/udp | Unassigned |
| dsp | 33/tcp | Display Support Protocol |
| dsp | 33/udp | Display Support Protocol |
| # | | Ed Cain |
| # | 34/tcp | Unassigned |
| # | 34/udp | Unassigned |
| | 35/tcp | any private printer server |
| | 35/udp | any private printer server |
| # | | Jon Postel |
| # | 36/tcp | Unassigned |
| # | 36/udp | Unassigned |
| time | 37/tcp | Time |
| time | 37/udp | Time |
| # | | Jon Postel |
| rap | 38/tcp | Route Access Protocol |
| rap | 38/udp | Route Access Protocol |
| # | | Robert Ullmann |
| rlp | 39/tcp | Resource Location Protocol |
| rlp | 39/udp | Resource Location Protocol |
| # | | Mike Accetta |
| # | 40/tcp | Unassigned |
| # | 40/udp | Unassigned |
| graphics | 41/tcp | Graphics |
| graphics | 41/udp | Graphics |
| nameserver | 42/tcp | Host Name Server |
| nameserver | 42/udp | Host Name Server |
| nickname | 43/tcp | who Is |
| nickname | 43/udp | who Is |
| mpm-flags | 44/tcp | MPM FLAGS Protocol |
| mpm-flags | 44/udp | MPM FLAGS Protocol |
| mpm | 45/tcp | Message Processing Module [recv] |
| mpm | 45/udp | Message Processing Module [recv] |
| mpm-snd | 46/tcp | MPM [default send] |
| mpm-snd | 46/udp | MPM [default send] |
| # | | Jon Postel |
| ni-ftp | 47/tcp | NI FTP |
| ni-ftp | 47/udp | NI FTP |
| # | | Steve Kille |
| auditd | 48/tcp | Digital Audit Daemon |
| auditd | 48/udp | Digital Audit Daemon |
| # | | Larry Scott |
| login | 49/tcp | Login Host Protocol |
| login | 49/udp | Login Host Protocol |
| # | | Pieter Ditmars |
| re-mail-ck | 50/tcp | Remote Mail Checking Protocol |
| re-mail-ck | 50/udp | Remote Mail Checking Protocol |
| # | | Steve Dorner |
| la-maint | 51/tcp | IMP Logical Address Maintenance |
| la-maint | 51/udp | IMP Logical Address Maintenance |
| # | | Andy Malis |
| xns-time | 52/tcp | XNS Time Protocol |
| xns-time | 52/udp | XNS Time Protocol |
| # | | Susie Armstrong |
| domain | 53/tcp | Domain Name Server |
| domain | 53/udp | Domain Name Server |
| # | | Paul Mockapetris |
| xns-ch | 54/tcp | XNS Clearinghouse |
| xns-ch | 54/udp | XNS Clearinghouse |
| # | | Susie Armstrong |
| isi-gl | 55/tcp | ISI Graphics Language |
| isi-gl | 55/udp | ISI Graphics Language |
| xns-auth | 56/tcp | XNS Authentication |
| xns-auth | 56/udp | XNS Authentication |
| # | | Susie Armstrong |
| | 57/tcp | any private terminal access |
| | 57/udp | any private terminal access |
| # | | Jon Postel |
| xns-mail | 58/tcp | XNS Mail |
| xns-mail | 58/udp | XNS Mail |
| # | | Susie Armstrong |
| | 59/tcp | any private file service |
| | 59/udp | any private file service |
| # | | Jon Postel |
| | 60/tcp | Unassigned |
| | 60/udp | Unassigned |
| ni-mail | 61/tcp | NI MAIL |
| ni-mail | 61/udp | NI MAIL |
| # | | Steve Kille |
| acas | 62/tcp | ACA Services |
| acas | 62/udp | ACA Services |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide "Distribuição / Cópia" neste material para maiores detalhes.

| | | |
|------------|--------|-----------------------------------|
| # | | E. Wald |
| # | 63/tcp | Unassigned |
| # | 63/udp | Unassigned |
| covia | 64/tcp | Communications Integrator (CI) |
| covia | 64/udp | Communications Integrator (CI) |
| # | | "Tundra" Tim Daneliuk |
| # | | |
| tacacs-ds | 65/tcp | TACACS-Database Service |
| tacacs-ds | 65/udp | TACACS-Database Service |
| # | | Kathy Huber |
| sql*net | 66/tcp | Oracle SQL*NET |
| sql*net | 66/udp | Oracle SQL*NET |
| # | | Jack Haverty |
| bootps | 67/tcp | Bootstrap Protocol Server |
| bootps | 67/udp | Bootstrap Protocol Server |
| bootpc | 68/tcp | Bootstrap Protocol Client |
| bootpc | 68/udp | Bootstrap Protocol Client |
| # | | Bill Croft |
| tftp | 69/tcp | Trivial File Transfer |
| tftp | 69/udp | Trivial File Transfer |
| # | | David Clark |
| gopher | 70/tcp | Gopher |
| gopher | 70/udp | Gopher |
| # | | Mark McCahill |
| netrjs-1 | 71/tcp | Remote Job Service |
| netrjs-1 | 71/udp | Remote Job Service |
| netrjs-2 | 72/tcp | Remote Job Service |
| netrjs-2 | 72/udp | Remote Job Service |
| netrjs-3 | 73/tcp | Remote Job Service |
| netrjs-3 | 73/udp | Remote Job Service |
| netrjs-4 | 74/tcp | Remote Job Service |
| netrjs-4 | 74/udp | Remote Job Service |
| # | | Bob Braden |
| | 75/tcp | any private dial out service |
| | 75/udp | any private dial out service |
| # | | Jon Postel |
| deos | 76/tcp | Distributed External Object Store |
| deos | 76/udp | Distributed External Object Store |
| # | | Robert Ullmann |
| | 77/tcp | any private RJE service |
| | 77/udp | any private RJE service |
| # | | Jon Postel |
| vettcp | 78/tcp | vettcp |
| vettcp | 78/udp | vettcp |
| # | | Christopher Leong |
| finger | 79/tcp | Finger |
| finger | 79/udp | Finger |
| # | | David Zimmerman |
| www-http | 80/tcp | World Wide Web HTTP |
| www-http | 80/udp | World Wide Web HTTP |
| # | | Tim Berners-Lee |
| hosts2-ns | 81/tcp | HOSTS2 Name Server |
| hosts2-ns | 81/udp | HOSTS2 Name Server |
| # | | Earl Killian |
| xfer | 82/tcp | XFER Utility |
| xfer | 82/udp | XFER Utility |
| # | | Thomas M. Smith |
| mit-ml-dev | 83/tcp | MIT ML Device |
| mit-ml-dev | 83/udp | MIT ML Device |
| # | | David Reed <--none--> |
| ctf | 84/tcp | Common Trace Facility |
| ctf | 84/udp | Common Trace Facility |
| # | | Hugh Thomas |
| mit-ml-dev | 85/tcp | MIT ML Device |
| mit-ml-dev | 85/udp | MIT ML Device |
| # | | David Reed <--none--> |
| mfcobol | 86/tcp | Micro Focus Cobol |
| mfcobol | 86/udp | Micro Focus Cobol |
| # | | Simon Edwards <--none--> |
| | 87/tcp | any private terminal link |
| | 87/udp | any private terminal link |
| # | | Jon Postel |
| kerberos | 88/tcp | Kerberos |
| kerberos | 88/udp | Kerberos |
| # | | B. Clifford Neuman |
| su-mit-tg | 89/tcp | SU/MIT Telnet Gateway |
| su-mit-tg | 89/udp | SU/MIT Telnet Gateway |
| # | | Mark Crispin |
| dnsix | 90/tcp | DNSIX Securit Attribute Token Map |
| dnsix | 90/udp | DNSIX Securit Attribute Token Map |
| # | | Charles Watt |
| mit-dov | 91/tcp | MIT Dover Spooler |
| mit-dov | 91/udp | MIT Dover Spooler |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide "Distribuição / Cópia" neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

| | | |
|------------|---------|------------------------------------|
| # | | Eliot Moss |
| npp | 92/tcp | Network Printing Protocol |
| npp | 92/udp | Network Printing Protocol |
| # | | Louis Mamakos |
| dcp | 93/tcp | Device Control Protocol |
| dcp | 93/udp | Device Control Protocol |
| # | | Daniel Tappan |
| objcall | 94/tcp | Tivoli Object Dispatcher |
| objcall | 94/udp | Tivoli Object Dispatcher |
| # | | Tom Bereiter <--none--> |
| supdup | 95/tcp | SUPDUP |
| supdup | 95/udp | SUPDUP |
| # | | Mark Crispin |
| dixie | 96/tcp | DIXIE Protocol Specification |
| dixie | 96/udp | DIXIE Protocol Specification |
| # | | Tim Howes |
| swift-rvf | 97/tcp | Swift Remote Vitural File Protocol |
| swift-rvf | 97/udp | Swift Remote Vitural File Protocol |
| # | | Maurice R. Turcotte |
| # | | |
| tacnews | 98/tcp | TAC News |
| tacnews | 98/udp | TAC News |
| # | | Jon Postel |
| metagram | 99/tcp | Metagram Relay |
| metagram | 99/udp | Metagram Relay |
| # | | Geoff Goodfellow |
| newacct | 100/tcp | [unauthorized use] |
| hostname | 101/tcp | NIC Host Name Server |
| hostname | 101/udp | NIC Host Name Server |
| # | | Jon Postel |
| iso-tsap | 102/tcp | ISO-TSAP |
| iso-tsap | 102/udp | ISO-TSAP |
| # | | Marshall Rose |
| gppitnp | 103/tcp | Genesis Point-to-Point Trans Net |
| gppitnp | 103/udp | Genesis Point-to-Point Trans Net |
| acr-nema | 104/tcp | ACR-NEMA Digital Imag. & Comm. 300 |
| acr-nema | 104/udp | ACR-NEMA Digital Imag. & Comm. 300 |
| # | | Patrick McNamee <--none--> |
| csnet-ns | 105/tcp | Mailbox Name Nameserver |
| csnet-ns | 105/udp | Mailbox Name Nameserver |
| # | | Marvin Solomon |
| 3com-tsmux | 106/tcp | 3COM-TSMUX |
| 3com-tsmux | 106/udp | 3COM-TSMUX |
| # | | Jeremy Siegel |
| rtelnet | 107/tcp | Remote Telnet Service |
| rtelnet | 107/udp | Remote Telnet Service |
| # | | Jon Postel |
| snagas | 108/tcp | SNA Gateway Access Server |
| snagas | 108/udp | SNA Gateway Access Server |
| # | | Kevin Murphy |
| pop2 | 109/tcp | Post Office Protocol - Version 2 |
| pop2 | 109/udp | Post Office Protocol - Version 2 |
| # | | Joyce K. Reynolds |
| pop3 | 110/tcp | Post Office Protocol - Version 3 |
| pop3 | 110/udp | Post Office Protocol - Version 3 |
| # | | Marshall Rose |
| sunrpc | 111/tcp | SUN Remote Procedure Call |
| sunrpc | 111/udp | SUN Remote Procedure Call |
| # | | Chuck McManis |
| mcidas | 112/tcp | MCIDAS Data Transmission Protocol |
| mcidas | 112/udp | MCIDAS Data Transmission Protocol |
| # | | Glenn Davis |
| auth | 113/tcp | Authentication Service |
| auth | 113/udp | Authentication Service |
| # | | Mike St. Johns |
| audionews | 114/tcp | Audio News Multicast |
| audionews | 114/udp | Audio News Multicast |
| # | | Martin Forssen |
| sftp | 115/tcp | Simple File Transfer Protocol |
| sftp | 115/udp | Simple File Transfer Protocol |
| # | | Mark Lottor |
| ansanotify | 116/tcp | ANSA REX Notify |
| ansanotify | 116/udp | ANSA REX Notify |
| # | | Nicola J. Howarth |
| uucp-path | 117/tcp | UUCP Path Service |
| uucp-path | 117/udp | UUCP Path Service |
| sqlserv | 118/tcp | SQL Services |
| sqlserv | 118/udp | SQL Services |
| # | | Larry Barnes |
| nntp | 119/tcp | Network News Transfer Protocol |
| nntp | 119/udp | Network News Transfer Protocol |
| # | | Phil Lapsley |
| cfdpkt | 120/tcp | CFDPKT |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

| | | |
|-------------|---------|------------------------------------|
| cfdpkt | 120/udp | CFDPTKT |
| # | | John Ioannidis |
| erpc | 121/tcp | Encore Expedited Remote Pro.Call |
| erpc | 121/udp | Encore Expedited Remote Pro.Call |
| # | | Jack O'Neil <---none--- ></td |
| smakynet | 122/tcp | SMAYNET |
| smakynet | 122/udp | SMAYNET |
| # | | Mike O'Dowd |
| ntp | 123/tcp | Network Time Protocol |
| ntp | 123/udp | Network Time Protocol |
| # | | Dave Mills |
| ansatrader | 124/tcp | ANSA REX Trader |
| ansatrader | 124/udp | ANSA REX Trader |
| # | | Nicola J. Howarth |
| locus-map | 125/tcp | Locus PC-Interface Net Map Ser |
| locus-map | 125/udp | Locus PC-Interface Net Map Ser |
| # | | Eric Peterson |
| unitary | 126/tcp | Unisys Unitary Login |
| unitary | 126/udp | Unisys Unitary Login |
| # | | |
| locus-con | 127/tcp | Locus PC-Interface Conn Server |
| locus-con | 127/udp | Locus PC-Interface Conn Server |
| # | | Eric Peterson |
| gss-xlicen | 128/tcp | GSS X License Verification |
| gss-xlicen | 128/udp | GSS X License Verification |
| # | | John Light |
| pwdgen | 129/tcp | Password Generator Protocol |
| pwdgen | 129/udp | Password Generator Protocol |
| # | | Frank J. Wacho |
| cisco-fna | 130/tcp | cisco FNATIVE |
| cisco-fna | 130/udp | cisco FNATIVE |
| cisco-tna | 131/tcp | cisco TNATIVE |
| cisco-tna | 131/udp | cisco TNATIVE |
| cisco-sys | 132/tcp | cisco SYSMAINT |
| cisco-sys | 132/udp | cisco SYSMAINT |
| statsrv | 133/tcp | Statistics Service |
| statsrv | 133/udp | Statistics Service |
| # | | Dave Mills |
| ingres-net | 134/tcp | INGRES-NET Service |
| ingres-net | 134/udp | INGRES-NET Service |
| # | | Mike Berrow <---none--- ></td |
| loc-srv | 135/tcp | Location Service |
| loc-srv | 135/udp | Location Service |
| # | | Joe Pato |
| profile | 136/tcp | PROFILE Naming System |
| profile | 136/udp | PROFILE Naming System |
| # | | Larry Peterson |
| netbios-ns | 137/tcp | NETBIOS Name Service |
| netbios-ns | 137/udp | NETBIOS Name Service |
| netbios-dgm | 138/tcp | NETBIOS Datagram Service |
| netbios-dgm | 138/udp | NETBIOS Datagram Service |
| netbios-ssn | 139/tcp | NETBIOS Session Service |
| netbios-ssn | 139/udp | NETBIOS Session Service |
| # | | Jon Postel |
| emfis-data | 140/tcp | EMFIS Data Service |
| emfis-data | 140/udp | EMFIS Data Service |
| emfis-cntl | 141/tcp | EMFIS Control Service |
| emfis-cntl | 141/udp | EMFIS Control Service |
| # | | Gerd Beling |
| bl-idm | 142/tcp | Britton-Lee IDM |
| bl-idm | 142/udp | Britton-Lee IDM |
| # | | Susie Snitzer <---none--- ></td |
| imap2 | 143/tcp | Interim Mail Access Protocol v2 |
| imap2 | 143/udp | Interim Mail Access Protocol v2 |
| # | | Mark Crispin |
| news | 144/tcp | News |
| news | 144/udp | News |
| # | | James Gosling |
| uaac | 145/tcp | UAAC Protocol |
| uaac | 145/udp | UAAC Protocol |
| # | | David A. Gomberg |
| iso-tp0 | 146/tcp | ISO-IP0 |
| iso-tp0 | 146/udp | ISO-IP0 |
| iso-ip | 147/tcp | ISO-IP |
| iso-ip | 147/udp | ISO-IP |
| # | | Marshall Rose |
| cronus | 148/tcp | CRONUS-SUPPORT |
| cronus | 148/udp | CRONUS-SUPPORT |
| # | | Jeffrey Buffon |
| aed-512 | 149/tcp | AED 512 Emulation Service |
| aed-512 | 149/udp | AED 512 Emulation Service |
| # | | Albert G. Broscius |
| sql-net | 150/tcp | SQL-NET |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide "Distribuição / Cópia" neste material para maiores detalhes.

| | | |
|-------------|---------|------------------------------------|
| sql-net | 150/udp | SQL-NET |
| # | | Martin Picard <---none---> |
| hems | 151/tcp | HEMS |
| hems | 151/udp | HEMS |
| # | | Christopher Tengi |
| bftp | 152/tcp | Background File Transfer Program |
| bftp | 152/udp | Background File Transfer Program |
| # | | Annette DeSchon |
| sgmp | 153/tcp | SGMP |
| sgmp | 153/udp | SGMP |
| # | | Marty Schoffstahl |
| netsec-prod | 154/tcp | NETSC |
| netsec-prod | 154/udp | NETSC |
| netsec-dev | 155/tcp | NETSC |
| netsec-dev | 155/udp | NETSC |
| # | | Sergio Heker |
| sqlsrv | 156/tcp | SQL Service |
| sqlsrv | 156/udp | SQL Service |
| # | | Craig Rogers |
| knet-cmp | 157/tcp | KNET/VM Command/Message Protocol |
| knet-cmp | 157/udp | KNET/VM Command/Message Protocol |
| # | | Gary S. Malkin |
| pcmail-srv | 158/tcp | PCMail Server |
| pcmail-srv | 158/udp | PCMail Server |
| # | | Mark L. Lambert |
| nss-routing | 159/tcp | NSS-Routing |
| nss-routing | 159/udp | NSS-Routing |
| # | | Yakov Rekhter |
| sgmp-traps | 160/tcp | SGMP-TRAPS |
| sgmp-traps | 160/udp | SGMP-TRAPS |
| # | | Marty Schoffstahl |
| snmp | 161/tcp | SNMP |
| snmp | 161/udp | SNMP |
| snmptrap | 162/tcp | SNMPTRAP |
| snmptrap | 162/udp | SNMPTRAP |
| # | | Marshall Rose |
| cmip-man | 163/tcp | CMIP/TCP Manager |
| cmip-man | 163/udp | CMIP/TCP Manager |
| cmip-agent | 164/tcp | CMIP/TCP Agent |
| smip-agent | 164/udp | CMIP/TCP Agent |
| # | | Amatzia Ben-Artzi <---none---> |
| xns-courier | 165/tcp | Xerox |
| xns-courier | 165/udp | Xerox |
| # | | Susie Armstrong |
| s-net | 166/tcp | Sirius Systems |
| s-net | 166/udp | Sirius Systems |
| # | | Brian Lloyd <---none---> |
| namp | 167/tcp | NAMP |
| namp | 167/udp | NAMP |
| # | | Marty Schoffstahl |
| rsvd | 168/tcp | RSVD |
| rsvd | 168/udp | RSVD |
| # | | Neil Todd |
| send | 169/tcp | SEND |
| send | 169/udp | SEND |
| # | | William D. Wisner |
| print-srv | 170/tcp | Network PostScript |
| print-srv | 170/udp | Network PostScript |
| # | | Brian Reid |
| multiplex | 171/tcp | Network Innovations Multiplex |
| multiplex | 171/udp | Network Innovations Multiplex |
| cl/1 | 172/tcp | Network Innovations CL/1 |
| cl/1 | 172/udp | Network Innovations CL/1 |
| # | | Kevin DeVault <---none---> |
| xyplex-mux | 173/tcp | Xyplex |
| xyplex-mux | 173/udp | Xyplex |
| # | | Bob Stewart |
| mailq | 174/tcp | MAILQ |
| mailq | 174/udp | MAILQ |
| # | | Rayan Zachariassen |
| vmnet | 175/tcp | VMNET |
| vmnet | 175/udp | VMNET |
| # | | Christopher Tengi |
| genrad-mux | 176/tcp | GENRAD-MUX |
| genrad-mux | 176/udp | GENRAD-MUX |
| # | | Ron Thornton |
| xdmcp | 177/tcp | X Display Manager Control Protocol |
| xdmcp | 177/udp | X Display Manager Control Protocol |
| # | | Robert W. Scheifler |
| nextstep | 178/tcp | NextStep Window Server |
| NextStep | 178/udp | NextStep Window Server |
| # | | Leo Hourvitz |
| bgp | 179/tcp | Border Gateway Protocol |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide "Distribuição / Cópia" neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide "Distribuição / Cópia" neste material para maiores detalhes.

| | | |
|-------------|---------|--------------------------------------|
| bgp | 179/udp | Border Gateway Protocol |
| # | | Kirk Loughheed |
| ris | 180/tcp | Intergraph |
| ris | 180/udp | Intergraph |
| # | | Dave Buehmann |
| unify | 181/tcp | Unify |
| unify | 181/udp | Unify |
| # | | Vinod Singh <---none---> |
| audit | 182/tcp | Unisys Audit SITP |
| audit | 182/udp | Unisys Audit SITP |
| # | | Gil Greenbaum |
| ocbinder | 183/tcp | OCBinder |
| ocbinder | 183/udp | OCBinder |
| ocserver | 184/tcp | OCServer |
| ocserver | 184/udp | OCServer |
| # | | Jerrilynn Okamura <---none---> |
| remote-kis | 185/tcp | Remote-KIS |
| remote-kis | 185/udp | Remote-KIS |
| kis | 186/tcp | KIS Protocol |
| kis | 186/udp | KIS Protocol |
| # | | Ralph Droms |
| aci | 187/tcp | Application Communication Interface |
| aci | 187/udp | Application Communication Interface |
| # | | Rick Carlos |
| mumps | 188/tcp | Plus Five's MUMPS |
| mumps | 188/udp | Plus Five's MUMPS |
| # | | Hokey Stenn |
| qft | 189/tcp | Queued File Transport |
| qft | 189/udp | Queued File Transport |
| # | | Wayne Schroeder |
| gacp | 190/tcp | Gateway Access Control Protocol |
| cacp | 190/udp | Gateway Access Control Protocol |
| # | | C. Philip Wood |
| prospero | 191/tcp | Prospero Directory Service |
| prospero | 191/udp | Prospero Directory Service |
| # | | B. Clifford Neuman |
| osu-nms | 192/tcp | OSU Network Monitoring System |
| osu-nms | 192/udp | OSU Network Monitoring System |
| # | | Doug Karl |
| srmp | 193/tcp | Spider Remote Monitoring Protocol |
| srmp | 193/udp | Spider Remote Monitoring Protocol |
| # | | Ted J. Socolofsky |
| irc | 194/tcp | Internet Relay Chat Protocol |
| irc | 194/udp | Internet Relay Chat Protocol |
| # | | Jarkko Oikarinen |
| dn6-nlm-aud | 195/tcp | DNSIX Network Level Module Audit |
| dn6-nlm-aud | 195/udp | DNSIX Network Level Module Audit |
| dn6-smm-red | 196/tcp | DNSIX Session Mgt Module Audit Redir |
| dn6-smm-red | 196/udp | DNSIX Session Mgt Module Audit Redir |
| # | | Lawrence Lebahn |
| dls | 197/tcp | Directory Location Service |
| dls | 197/udp | Directory Location Service |
| dls-mon | 198/tcp | Directory Location Service Monitor |
| dls-mon | 198/udp | Directory Location Service Monitor |
| # | | Scott Bellew |
| smux | 199/tcp | SMUX |
| smux | 199/udp | SMUX |
| # | | Marshall Rose |
| src | 200/tcp | IBM System Resource Controller |
| src | 200/udp | IBM System Resource Controller |
| # | | Gerald MCBrearty <---none---> |
| at-rtmp | 201/tcp | AppleTalk Routing Maintenance |
| at-rtmp | 201/udp | AppleTalk Routing Maintenance |
| at-nbp | 202/tcp | AppleTalk Name Binding |
| at-nbp | 202/udp | AppleTalk Name Binding |
| at-3 | 203/tcp | AppleTalk Unused |
| at-3 | 203/udp | AppleTalk Unused |
| at-echo | 204/tcp | AppleTalk Echo |
| at-echo | 204/udp | AppleTalk Echo |
| at-5 | 205/tcp | AppleTalk Unused |
| at-5 | 205/udp | AppleTalk Unused |
| at-zis | 206/tcp | AppleTalk Zone Information |
| at-zis | 206/udp | AppleTalk Zone Information |
| at-7 | 207/tcp | AppleTalk Unused |
| at-7 | 207/udp | AppleTalk Unused |
| at-8 | 208/tcp | AppleTalk Unused |
| at-8 | 208/udp | AppleTalk Unused |
| # | | Rob Chandhok |
| tam | 209/tcp | Trivial Authenticated Mail Protocol |
| tam | 209/udp | Trivial Authenticated Mail Protocol |
| # | | Dan Bernstein |
| z39.50 | 210/tcp | ANSI Z39.50 |
| z39.50 | 210/udp | ANSI Z39.50 |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide "Distribuição / Cópia" neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

| | | |
|-----------|---------|-------------------------------------|
| # | | Mark Needleman |
| # | | |
| 914c/g | 211/tcp | Texas Instruments 914C/G Terminal |
| 914c/g | 211/udp | Texas Instruments 914C/G Terminal |
| # | | Bill Harrell <---none---> |
| anet | 212/tcp | ATEXSSTR |
| anet | 212/udp | ATEXSSTR |
| # | | Jim Taylor |
| ipx | 213/tcp | IPX |
| ipx | 213/udp | IPX |
| # | | Don Provan |
| vmpwscs | 214/tcp | VM PWSCS |
| vmpwscs | 214/udp | VM PWSCS |
| # | | Dan Shia |
| softpc | 215/tcp | Insignia Solutions |
| softpc | 215/udp | Insignia Solutions |
| # | | Martyn Thomas <---none---> |
| atls | 216/tcp | Access Technology License Server |
| atls | 216/udp | Access Technology License Server |
| # | | Larry DeLuca |
| dbase | 217/tcp | dBASE Unix |
| dbase | 217/udp | dBASE Unix |
| # | | Don Gibson |
| # | | |
| mpp | 218/tcp | Netix Message Posting Protocol |
| mpp | 218/udp | Netix Message Posting Protocol |
| # | | Shannon Yeh |
| uarps | 219/tcp | Unisys ARPs |
| uarps | 219/udp | Unisys ARPs |
| # | | Ashok Marwaha <---none---> |
| imap3 | 220/tcp | Interactive Mail Access Protocol v3 |
| imap3 | 220/udp | Interactive Mail Access Protocol v3 |
| # | | James Rice |
| fln-spx | 221/tcp | Berkeley rlogind with SPX auth |
| fln-spx | 221/udp | Berkeley rlogind with SPX auth |
| rsh-spx | 222/tcp | Berkeley rshd with SPX auth |
| rsh-spx | 222/udp | Berkeley rshd with SPX auth |
| cdc | 223/tcp | Certificate Distribution Center |
| cdc | 223/udp | Certificate Distribution Center |
| # | | Kannan Alagappan |
| # | 224-241 | Reserved |
| # | | Jon Postel |
| # | | Unassigned |
| # | 242/tcp | Unassigned |
| # | 242/udp | Unassigned |
| sur-meas | 243/tcp | Survey Measurement |
| sur-meas | 243/udp | Survey Measurement |
| # | | Dave Clark |
| # | 244/tcp | Unassigned |
| # | 244/udp | Unassigned |
| link | 245/tcp | LINK |
| link | 245/udp | LINK |
| dsp3270 | 246/tcp | Display Systems Protocol |
| dsp3270 | 246/udp | Display Systems Protocol |
| # | | weldon J. Showalter |
| # | 247-255 | Reserved |
| # | | Jon Postel |
| # | 256-343 | Unassigned |
| pdap | 344/tcp | Prospero Data Access Protocol |
| pdap | 344/udp | Prospero Data Access Protocol |
| # | | B. Clifford Neuman |
| pawserv | 345/tcp | Perf Analysis Workbench |
| pawserv | 345/udp | Perf Analysis Workbench |
| zserv | 346/tcp | Zebra server |
| zserv | 346/udp | Zebra server |
| faterv | 347/tcp | Fatmen Server |
| faterv | 347/udp | Fatmen Server |
| csi-sgwp | 348/tcp | Cabletron Management Protocol |
| csi-sgwp | 348/udp | Cabletron Management Protocol |
| # | 349-370 | Unassigned |
| clearcase | 371/tcp | Clearcase |
| clearcase | 371/udp | Clearcase |
| # | | Dave LeBlang |
| ulistserv | 372/tcp | Unix Listserv |
| ulistserv | 372/udp | Unix Listserv |
| # | | Anastasios Kotsikonas |
| legent-1 | 373/tcp | Legent Corporation |
| legent-1 | 373/udp | Legent Corporation |
| legent-2 | 374/tcp | Legent Corporation |
| legent-2 | 374/udp | Legent Corporation |
| # | | Keith Boyce <---none---> |
| hassle | 375/tcp | Hassle |
| hassle | 375/udp | Hassle |
| # | | Reinhard Doelz |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

| | | |
|-----------------|---------|---------------------------------------|
| nip | 376/tcp | Amiga Envoy Network Inquiry Proto |
| nip | 376/udp | Amiga Envoy Network Inquiry Proto |
| # | | Kenneth Dyke |
| tnETOS | 377/tcp | NEC Corporation |
| tnETOS | 377/udp | NEC Corporation |
| dsETOS | 378/tcp | NEC Corporation |
| dsETOS | 378/udp | NEC Corporation |
| # | | Tomoo Fujita |
| is99c | 379/tcp | TIA/EIA/IS-99 modem client |
| is99c | 379/udp | TIA/EIA/IS-99 modem client |
| is99s | 380/tcp | TIA/EIA/IS-99 modem server |
| is99s | 380/udp | TIA/EIA/IS-99 modem server |
| # | | Frank Quick |
| hp-collector | 381/tcp | hp performance data collector |
| hp-collector | 381/udp | hp performance data collector |
| hp-managed-node | 382/tcp | hp performance data managed node |
| hp-managed-node | 382/udp | hp performance data managed node |
| hp-alarm-mgr | 383/tcp | hp performance data alarm manager |
| hp-alarm-mgr | 383/udp | hp performance data alarm manager |
| # | | Frank Blakely |
| arns | 384/tcp | A Remote Network Server System |
| arns | 384/udp | A Remote Network Server System |
| # | | David Hornsby |
| ibm-app | 385/tcp | IBM Application |
| ibm-app | 385/udp | IBM Application |
| # | | Lisa Tomita <---none---> |
| asa | 386/tcp | ASA Message Router Object Def. |
| asa | 386/udp | ASA Message Router Object Def. |
| # | | Steve Laitinen |
| aurp | 387/tcp | Appletalk Update-Based Routing Pro. |
| aurp | 387/udp | Appletalk Update-Based Routing Pro. |
| # | | Chris Ranch |
| unidata-ldm | 388/tcp | Unidata LDM Version 4 |
| unidata-ldm | 388/udp | Unidata LDM Version 4 |
| # | | Glenn Davis |
| ldap | 389/tcp | Lightweight Directory Access Protocol |
| ldap | 389/udp | Lightweight Directory Access Protocol |
| # | | Tim Howes |
| uis | 390/tcp | UIS |
| uis | 390/udp | UIS |
| # | | Ed Barron <---none---> |
| synotics-relay | 391/tcp | SynOptics SNMP Relay Port |
| synotics-relay | 391/udp | SynOptics SNMP Relay Port |
| synotics-broker | 392/tcp | SynOptics Port Broker Port |
| synotics-broker | 392/udp | SynOptics Port Broker Port |
| # | | Illan Raab |
| dis | 393/tcp | Data Interpretation System |
| dis | 393/udp | Data Interpretation System |
| # | | Paul Stevens |
| embl-ndt | 394/tcp | EMBL Nucleic Data Transfer |
| embl-ndt | 394/udp | EMBL Nucleic Data Transfer |
| # | | Peter Gad |
| netcp | 395/tcp | NETScout Control Protocol |
| netcp | 395/udp | NETScout Control Protocol |
| # | | Anil Singhal <---none---> |
| netware-ip | 396/tcp | Novell Netware over IP |
| netware-ip | 396/udp | Novell Netware over IP |
| mpn | 397/tcp | Multi Protocol Trans. Net. |
| mpn | 397/udp | Multi Protocol Trans. Net. |
| # | | Soumitra Sarkar |
| kryptolan | 398/tcp | Kryptolan |
| kryptolan | 398/udp | Kryptolan |
| # | | Peter de Laval |
| # | 399/tcp | Unassigned |
| # | 399/udp | Unassigned |
| work-sol | 400/tcp | Workstation Solutions |
| work-sol | 400/udp | Workstation Solutions |
| # | | Jim Ward |
| ups | 401/tcp | Uninterruptible Power Supply |
| ups | 401/udp | Uninterruptible Power Supply |
| # | | Guenther Seybold |
| genie | 402/tcp | Genie Protocol |
| genie | 402/udp | Genie Protocol |
| # | | Mark Hankin <---none---> |
| decap | 403/tcp | decap |
| decap | 403/udp | decap |
| nced | 404/tcp | nced |
| nced | 404/udp | nced |
| ncld | 405/tcp | ncld |
| ncld | 405/udp | ncld |
| # | | Richard Jones <---none---> |
| imsp | 406/tcp | Interactive Mail Support Protocol |
| imsp | 406/udp | Interactive Mail Support Protocol |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

| | | |
|----------------|---------|---|
| # | | John Myers |
| timbuktu | 407/tcp | Timbuktu |
| timbuktu | 407/udp | Timbuktu |
| # | | Marc Epard |
| prm-sm | 408/tcp | Prospero Resource Manager Sys. Man. |
| prm-sm | 408/udp | Prospero Resource Manager Sys. Man. |
| prm-nm | 409/tcp | Prospero Resource Manager Node Man. |
| prm-nm | 409/udp | Prospero Resource Manager Node Man. |
| # | | B. Clifford Neuman |
| decladebug | 410/tcp | DECLadebug Remote Debug Protocol |
| decladebug | 410/udp | DECLadebug Remote Debug Protocol |
| # | | Anthony Berent |
| rmt | 411/tcp | Remote MT Protocol |
| rmt | 411/udp | Remote MT Protocol |
| # | | Peter Eriksson |
| synoptics-trap | 412/tcp | Trap Convention Port |
| synoptics-trap | 412/udp | Trap Convention Port |
| # | | Illan Raab |
| smsp | 413/tcp | SMSP |
| smsp | 413/udp | SMSP |
| infoseek | 414/tcp | InfoSeek |
| infoseek | 414/udp | InfoSeek |
| # | | Steve Kirsch |
| bnet | 415/tcp | BNet |
| bnet | 415/udp | BNet |
| # | | Jim Mertz |
| silverplatter | 416/tcp | Silverplatter |
| silverplatter | 416/udp | Silverplatter |
| # | | Peter Ciuffetti |
| onmux | 417/tcp | Onmux |
| onmux | 417/udp | Onmux |
| # | | Stephen Hanna |
| hyper-g | 418/tcp | Hyper-G |
| hyper-g | 418/udp | Hyper-G |
| # | | Frank Kappe |
| ariel1 | 419/tcp | Ariel |
| ariel1 | 419/udp | Ariel |
| # | | Jonathan Lavigne |
| smpte | 420/tcp | SMPTE |
| smpte | 420/udp | SMPTE |
| # | | Si Becker <71362.22@CompuServe.COM> |
| ariel2 | 421/tcp | Ariel |
| ariel2 | 421/udp | Ariel |
| ariel3 | 422/tcp | Ariel |
| ariel3 | 422/udp | Ariel |
| # | | Jonathan Lavigne |
| opc-job-start | 423/tcp | IBM Operations Planning and Control Start |
| opc-job-start | 423/udp | IBM Operations Planning and Control Start |
| opc-job-track | 424/tcp | IBM Operations Planning and Control Track |
| opc-job-track | 424/udp | IBM Operations Planning and Control Track |
| # | | Conny Larsson |
| icad-el | 425/tcp | ICAD |
| icad-el | 425/udp | ICAD |
| # | | Larry Stone |
| smartsdp | 426/tcp | smartsdp |
| smartsdp | 426/udp | smartsdp |
| # | | Alexander Dupuy |
| svrloc | 427/tcp | Server Location |
| svrloc | 427/udp | Server Location |
| # | | |
| ocs_cmu | 428/tcp | OCS_CMU |
| ocs_cmu | 428/udp | OCS_CMU |
| ocs_amu | 429/tcp | OCS_AMU |
| ocs_amu | 429/udp | OCS_AMU |
| # | | Florence Wyman |
| utmpsdp | 430/tcp | UTMPSPD |
| utmpsdp | 430/udp | UTMPSPD |
| utmpcd | 431/tcp | UTMPCD |
| utmpcd | 431/udp | UTMPCD |
| iasd | 432/tcp | IASD |
| iasd | 432/udp | IASD |
| # | | Nir Baroz |
| nnsdp | 433/tcp | NNSP |
| nnsdp | 433/udp | NNSP |
| # | | Rob Robertson |
| mobileip-agent | 434/tcp | MobileIP-Agent |
| mobileip-agent | 434/udp | MobileIP-Agent |
| mobileip-mn | 435/tcp | MobileIP-MN |
| mobileip-mn | 435/udp | MobileIP-MN |
| # | | Kannan Alagappan |
| dna-cml | 436/tcp | DNA-CML |
| dna-cml | 436/udp | DNA-CML |
| # | | Dan Flowers |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide "Distribuição / Cópia" neste material para maiores detalhes.

| | | |
|---------------|---------|-------------------------------------|
| comscm | 437/tcp | comscm |
| comscm | 437/udp | comscm |
| # | | Jim Teague |
| dsfgw | 438/tcp | dsfgw |
| dsfgw | 438/udp | dsfgw |
| # | | Andy McKeen |
| dasp | 439/tcp | dasp |
| dasp | 439/udp | dasp |
| # | | Thomas Obermair |
| sgcp | 440/tcp | sgcp |
| sgcp | 440/udp | sgcp |
| # | | Marshall Rose |
| decvms-sysmgt | 441/tcp | decvms-sysmgt |
| decvms-sysmgt | 441/udp | decvms-sysmgt |
| # | | Lee Barton |
| cvc_hostd | 442/tcp | cvc_hostd |
| cvc_hostd | 442/udp | cvc_hostd |
| # | | Bill Davidson |
| https | 443/tcp | https |
| https | 443/udp | https |
| # | | MCom |
| snpp | 444/tcp | snpp |
| snpp | 444/udp | snpp |
| # | | Kipp E.B. Hickman |
| microsoft-ds | 445/tcp | Simple Network Paging Protocol |
| microsoft-ds | 445/udp | Simple Network Paging Protocol |
| # | | [RFC1568] |
| ddm-rdb | 446/tcp | Microsoft-DS |
| ddm-rdb | 446/udp | Microsoft-DS |
| ddm-dfm | 447/tcp | Arnold Miller |
| ddm-dfm | 447/udp | DDM-RDB |
| ddm-byte | 448/tcp | DDM-RDB |
| ddm-byte | 448/udp | DDM-RFM |
| # | | DDM-RFM |
| as-servermap | 449/tcp | DDM-BYTE |
| as-servermap | 449/udp | DDM-BYTE |
| # | | DDM-BYTE |
| tserver | 450/tcp | Jan David Fisher |
| tserver | 450/udp | AS Server Mapper |
| # | | AS Server Mapper |
| # | | Barbara Foss |
| exec | 451-511 | TServer |
| # | 512/tcp | TServer |
| # | | Harvey S. Schultz |
| biff | 512/udp | Unassigned |
| # | | remote process execution; |
| # | | authentication performed using |
| # | | passwords and UNIX loppgin names |
| # | | used by mail system to notify users |
| # | | of new mail received; currently |
| # | | receives messages only from |
| # | | processes on the same machine |
| login | 513/tcp | remote login a la telnet; |
| # | | automatic authentication performed |
| # | | based on privileged port numbers |
| # | | and distributed data bases which |
| # | | identify "authentication domains" |
| who | 513/udp | maintains data bases showing who's |
| # | | logged in to machines on a local |
| # | | net and the load average of the |
| # | | machine |
| cmd | 514/tcp | like exec, but automatic |
| # | | authentication is performed as for |
| # | | login server |
| syslog | 514/udp | |
| printer | 515/tcp | spooler |
| printer | 515/udp | spooler |
| # | | Unassigned |
| # | | Unassigned |
| talk | 516/tcp | like tenex link, but across |
| # | | machine - unfortunately, doesn't |
| # | | use link protocol (this is actually |
| # | | just a rendezvous port from which a |
| # | | tcp connection is established) |
| talk | 517/udp | like tenex link, but across |
| # | | machine - unfortunately, doesn't |
| # | | use link protocol (this is actually |
| # | | just a rendezvous port from which a |
| # | | tcp connection is established) |
| ntalk | 518/tcp | |
| ntalk | 518/udp | |
| utime | 519/tcp | unixtime |
| utime | 519/udp | unixtime |
| efs | 520/tcp | extended file name server |
| router | 520/udp | local routing process (on site); |
| # | | uses variant of Xerox NS routing |
| # | | information protocol |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide "Distribuição / Cópia" neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

| | | |
|----------------|---------|--|
| # | 521-524 | Unassigned |
| timed | 525/tcp | timeserver |
| timed | 525/udp | timeserver |
| tempo | 526/tcp | newdate |
| tempo | 526/udp | newdate |
| # | 527-529 | Unassigned |
| courier | 530/tcp | rpc |
| courier | 530/udp | rpc |
| conference | 531/tcp | chat |
| conference | 531/udp | chat |
| netnews | 532/tcp | readnews |
| netnews | 532/udp | readnews |
| netwall | 533/tcp | for emergency broadcasts |
| netwall | 533/udp | for emergency broadcasts |
| # | 534-538 | Unassigned |
| apertus-ldp | 539/tcp | Apertus Technologies Load Determination |
| apertus-ldp | 539/udp | Apertus Technologies Load Determination |
| uucp | 540/tcp | uucpd |
| uucp | 540/udp | uucpd |
| uucp-rlogin | 541/tcp | uucp-rlogin Stuart Lynne |
| uucp-rlogin | 541/udp | uucp-rlogin sl@wimsey.com |
| # | 542/tcp | Unassigned |
| # | 542/udp | Unassigned |
| klogin | 543/tcp | |
| klogin | 543/udp | |
| kshell | 544/tcp | krcmd |
| kshell | 544/udp | krcmd |
| # | 545-549 | Unassigned |
| new-rwho | 550/tcp | new-who |
| new-rwho | 550/udp | new-who |
| # | 551-555 | Unassigned |
| dsf | 555/tcp | |
| dsf | 555/udp | |
| remotefs | 556/tcp | rfs server |
| remotefs | 556/udp | rfs server |
| # | 557-559 | Unassigned |
| rmonitor | 560/tcp | rmonitord |
| rmonitor | 560/udp | rmonitord |
| monitor | 561/tcp | |
| monitor | 561/udp | |
| chshell | 562/tcp | chcmd |
| chshell | 562/udp | chcmd |
| # | 563/tcp | Unassigned |
| # | 563/udp | Unassigned |
| 9pfs | 564/tcp | plan 9 file service |
| 9pfs | 564/udp | plan 9 file service |
| whoami | 565/tcp | whoami |
| whoami | 565/udp | whoami |
| # | 566-569 | Unassigned |
| meter | 570/tcp | demon |
| meter | 570/udp | demon |
| meter | 571/tcp | udemon |
| meter | 571/udp | udemon |
| # | 572-599 | Unassigned |
| ipcserver | 600/tcp | Sun IPC server |
| ipcserver | 600/udp | Sun IPC server |
| nqs | 607/tcp | nqs |
| nqs | 607/udp | nqs |
| urm | 606/tcp | Cray Unified Resource Manager |
| urm | 606/udp | Cray Unified Resource Manager |
| # | | Bill Schiefelbein |
| sift-uft | 608/tcp | Sender-Initiated/Unsolicited File Transfer |
| sift-uft | 608/udp | Sender-Initiated/Unsolicited File Transfer |
| # | | Rick Troth |
| npmp-trap | 609/tcp | npmp-trap |
| npmp-trap | 609/udp | npmp-trap |
| npmp-local | 610/tcp | npmp-local |
| npmp-local | 610/udp | npmp-local |
| npmp-gui | 611/tcp | npmp-gui |
| npmp-gui | 611/udp | npmp-gui |
| # | | John Barnes |
| ginad | 634/tcp | ginad |
| ginad | 634/udp | ginad |
| # | | Mark Crother |
| mdqs | 666/tcp | |
| mdqs | 666/udp | |
| doom | 666/tcp | doom Id Software |
| doom | 666/udp | doom Id Software |
| # | | |
| elcsd | 704/tcp | errlog copy/server daemon |
| elcsd | 704/udp | errlog copy/server daemon |
| entrustmanager | 709/tcp | EntrustManager |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

| | | |
|----------------|---------|---------------------------------------|
| entrustmanager | 709/udp | EntrustManager |
| # | | Peter Whittaker |
| netviewdm1 | 729/tcp | IBM NetView DM/6000 Server/Client |
| netviewdm1 | 729/udp | IBM NetView DM/6000 Server/Client |
| netviewdm2 | 730/tcp | IBM NetView DM/6000 send/tcp |
| netviewdm2 | 730/udp | IBM NetView DM/6000 send/tcp |
| netviewdm3 | 731/tcp | IBM NetView DM/6000 receive/tcp |
| netviewdm3 | 731/udp | IBM NetView DM/6000 receive/tcp |
| # | | Philippe Binet (phbinet@vnet.IBM.COM) |
| netgw | 741/tcp | netGW |
| netgw | 741/udp | netGW |
| netrcs | 742/tcp | Network based Rev. Cont. Sys. |
| netrcs | 742/udp | Network based Rev. Cont. Sys. |
| # | | Gordon C. Galligher |
| flexlm | 744/tcp | Flexible License Manager |
| flexlm | 744/udp | Flexible License Manager |
| # | | Matt Christiano |
| # | | |
| fujitsu-dev | 747/tcp | Fujitsu Device Control |
| fujitsu-dev | 747/udp | Fujitsu Device Control |
| ris-cm | 748/tcp | Russell Info Sci Calendar Manager |
| ris-cm | 748/udp | Russell Info Sci Calendar Manager |
| kerberos-adm | 749/tcp | kerberos administration |
| kerberos-adm | 749/udp | kerberos administration |
| rfile | 750/tcp | |
| loadav | 750/udp | |
| pump | 751/tcp | |
| pump | 751/udp | |
| qrh | 752/tcp | |
| qrh | 752/udp | |
| rrh | 753/tcp | |
| rrh | 753/udp | |
| tell | 754/tcp | send |
| tell | 754/udp | send |
| nlogin | 758/tcp | |
| nlogin | 758/udp | |
| con | 759/tcp | |
| con | 759/udp | |
| ns | 760/tcp | |
| ns | 760/udp | |
| rxex | 761/tcp | |
| rxex | 761/udp | |
| quotad | 762/tcp | |
| quotad | 762/udp | |
| cycleserv | 763/tcp | |
| cycleserv | 763/udp | |
| omserv | 764/tcp | |
| omserv | 764/udp | |
| webster | 765/tcp | |
| webster | 765/udp | |
| phonebook | 767/tcp | phone |
| phonebook | 767/udp | phone |
| vid | 769/tcp | |
| vid | 769/udp | |
| cadlock | 770/tcp | |
| cadlock | 770/udp | |
| rtip | 771/tcp | |
| rtip | 771/udp | |
| cycleserv2 | 772/tcp | |
| cycleserv2 | 772/udp | |
| submit | 773/tcp | |
| notify | 773/udp | |
| rpasswd | 774/tcp | |
| acmaint_dbd | 774/udp | |
| entomb | 775/tcp | |
| acmaint_transd | 775/udp | |
| wpages | 776/tcp | |
| wpages | 776/udp | |
| wpgs | 780/tcp | |
| wpgs | 780/udp | |
| concert | 786/tcp | Concert |
| concert | 786/udp | Concert |
| # | | Josyula R. Rao |
| mdbs_daemon | 800/tcp | |
| mdbs_daemon | 800/udp | |
| device | 801/tcp | |
| device | 801/udp | |
| xtreelic | 996/tcp | Central Point Software |
| xtreelic | 996/udp | Central Point Software |
| # | | Dale Cabell |
| maitrd | 997/tcp | |
| maitrd | 997/udp | |
| busboy | 998/tcp | |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

| | | |
|-----------|----------|-----------|
| puparp | 998/udp | |
| garcon | 999/tcp | |
| applix | 999/udp | Applix ac |
| puprouter | 999/tcp | |
| puprouter | 999/udp | |
| cadlock | 1000/tcp | |
| ock | 1000/udp | |
| | 1023/tcp | Reserved |
| | 1024/udp | Reserved |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Portas TCP/UDP Não Privilegiadas (Registered Port Numbers)

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

| Keyword | Decimal | Description | References |
|-----------------|----------|-------------------------------------|------------|
| | ----- | ----- | ----- |
| | 1024/tcp | Reserved | |
| | 1024/udp | Reserved | |
| # | | IANA | |
| blackjack | 1025/tcp | network blackjack | |
| blackjack | 1025/udp | network blackjack | |
| iad1 | 1030/tcp | BBN IAD | |
| iad1 | 1030/udp | BBN IAD | |
| iad2 | 1031/tcp | BBN IAD | |
| iad2 | 1031/udp | BBN IAD | |
| iad3 | 1032/tcp | BBN IAD | |
| iad3 | 1032/udp | BBN IAD | |
| # | | Andy Malis | |
| instl_boots | 1067/tcp | Installation Bootstrap Proto. Serv. | |
| instl_boots | 1067/udp | Installation Bootstrap Proto. Serv. | |
| instl_bootc | 1068/tcp | Installation Bootstrap Proto. Cli. | |
| instl_bootc | 1068/udp | Installation Bootstrap Proto. Cli. | |
| # | | David Arko < | |
| socks | 1080/tcp | Socks | |
| socks | 1080/udp | Socks | |
| # | | Ying-Da Lee | |
| nerv | 1222/tcp | SNI R&D network | |
| nerv | 1222/udp | SNI R&D network | |
| # | | Martin Freiss | |
| hermes | 1248/tcp | | |
| hermes | 1248/udp | | |
| alta-ana-lm | 1346/tcp | Alta Analytics License Manager | |
| alta-ana-lm | 1346/udp | Alta Analytics License Manager | |
| bbn-mmc | 1347/tcp | multi media conferencing | |
| bbn-mmc | 1347/udp | multi media conferencing | |
| bbn-mmx | 1348/tcp | multi media conferencing | |
| bbn-mmx | 1348/udp | multi media conferencing | |
| sbook | 1349/tcp | Registration Network Protocol | |
| sbook | 1349/udp | Registration Network Protocol | |
| editbench | 1350/tcp | Registration Network Protocol | |
| editbench | 1350/udp | Registration Network Protocol | |
| # | | Simson L. Garfinkel | |
| equationbuilder | 1351/tcp | Digital Tool Works (MIT) | |
| equationbuilder | 1351/udp | Digital Tool Works (MIT) | |
| # | | Terrence J. Talbot | |
| lotusnote | 1352/tcp | Lotus Note | |
| lotusnote | 1352/udp | Lotus Note | |
| # | | Greg Pflaum | |
| relief | 1353/tcp | Relief Consulting | |
| relief | 1353/udp | Relief Consulting | |
| # | | John Feiler | |
| rightbrain | 1354/tcp | RightBrain Software | |
| rightbrain | 1354/udp | RightBrain Software | |
| # | | Glenn Reid | |
| intuitive edge | 1355/tcp | Intuitive Edge | |
| intuitive edge | 1355/udp | Intuitive Edge | |
| # | | Montgomery Zukowski | |
| # | | | |
| cuillamartin | 1356/tcp | CuillaMartin Company | |
| cuillamartin | 1356/udp | CuillaMartin Company | |
| pegboard | 1357/tcp | Electronic PegBoard | |
| pegboard | 1357/udp | Electronic PegBoard | |
| # | | Chris Cuilla | |
| # | | | |
| connlcli | 1358/tcp | CONNLCI | |
| connlcli | 1358/udp | CONNLCI | |
| ftsrv | 1359/tcp | FTSRV | |
| ftsrv | 1359/udp | FTSRV | |
| # | | Ines Homem de Melo | |
| mimer | 1360/tcp | MIMER | |
| mimer | 1360/udp | MIMER | |
| # | | Per Schroeder | |
| linx | 1361/tcp | LinX | |
| linx | 1361/udp | LinX | |
| # | | Steffen Schilke <---none---> | |
| timeflies | 1362/tcp | TimeFlies | |
| timeflies | 1362/udp | TimeFlies | |
| # | | Doug Kent | |
| ndm-requester | 1363/tcp | Network DataMover Requester | |
| ndm-requester | 1363/udp | Network DataMover Requester | |
| ndm-server | 1364/tcp | Network DataMover Server | |
| ndm-server | 1364/udp | Network DataMover Server | |
| # | | Toshio Watanabe | |
| # | | | |
| adapt-sna | 1365/tcp | Network Software Associates | |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

| | | |
|----------------|----------|---------------------------------------|
| adapt-sna | 1365/udp | Network Software Associates |
| # | | Jeffery Chiao <714-768-401> |
| netware-csp | 1366/tcp | Novell Netware Comm Service Platform |
| netware-csp | 1366/udp | Novell Netware Comm Service Platform |
| # | | Laurie Lindsey |
| dcs | 1367/tcp | DCS |
| dcs | 1367/udp | DCS |
| # | | Stefan Siebert |
| screencast | 1368/tcp | ScreenCast |
| screencast | 1368/udp | ScreenCast |
| # | | Bill Tschumy |
| gv-us | 1369/tcp | GlobalView to Unix Shell |
| gv-us | 1369/udp | GlobalView to Unix Shell |
| us-gv | 1370/tcp | Unix Shell to GlobalView |
| us-gv | 1370/udp | Unix Shell to GlobalView |
| # | | Makoto Mita |
| fc-cli | 1371/tcp | Fujitsu Config Protocol |
| fc-cli | 1371/udp | Fujitsu Config Protocol |
| fc-ser | 1372/tcp | Fujitsu Config Protocol |
| fc-ser | 1372/udp | Fujitsu Config Protocol |
| # | | Ryuichi Horie |
| chromagrafx | 1373/tcp | Chromagrafx |
| chromagrafx | 1373/udp | Chromagrafx |
| # | | Mike Barthelemy |
| molly | 1374/tcp | EPI Software Systems |
| molly | 1374/udp | EPI Software Systems |
| # | | Jim Vlcek |
| bytex | 1375/tcp | Bytex |
| bytex | 1375/udp | Bytex |
| # | | Mary Ann Burt |
| ibm-pps | 1376/tcp | IBM Person to Person Software |
| ibm-pps | 1376/udp | IBM Person to Person Software |
| # | | Simon Phipps |
| cichlid | 1377/tcp | Cichlid License Manager |
| cichlid | 1377/udp | Cichlid License Manager |
| # | | Andy Burgess |
| elan | 1378/tcp | Elan License Manager |
| elan | 1378/udp | Elan License Manager |
| # | | Ken Greer |
| dbreporter | 1379/tcp | Integrity Solutions |
| dbreporter | 1379/udp | Integrity Solutions |
| # | | Tim Dawson |
| telesis-licman | 1380/tcp | Telesis Network License Manager |
| telesis-licman | 1380/udp | Telesis Network License Manager |
| # | | Karl Schendel, Jr. |
| apple-licman | 1381/tcp | Apple Network License Manager |
| apple-licman | 1381/udp | Apple Network License Manager |
| # | | Earl wallace |
| udt_os | 1382/tcp | |
| udt_os | 1382/udp | |
| gwha | 1383/tcp | GW Hannaway Network License Manager |
| gwha | 1383/udp | GW Hannaway Network License Manager |
| # | | J. Gabriel Foster |
| os-licman | 1384/tcp | Objective Solutions License Manager |
| os-licman | 1384/udp | Objective Solutions License Manager |
| # | | Donald Cornwell |
| atex_elmd | 1385/tcp | Atex Publishing License Manager |
| atex_elmd | 1385/udp | Atex Publishing License Manager |
| # | | Brett Sorenson |
| checksum | 1386/tcp | Checksum License Manager |
| checksum | 1386/udp | Checksum License Manager |
| # | | Andreas Glocker |
| cadsi-lm | 1387/tcp | Computer Aided Design Software Inc LM |
| cadsi-lm | 1387/udp | Computer Aided Design Software Inc LM |
| # | | Sulistio Muljadi |
| objective-dbc | 1388/tcp | Objective Solutions DataBase Cache |
| objective-dbc | 1388/udp | Objective Solutions DataBase Cache |
| # | | Donald Cornwell |
| iclpv-dm | 1389/tcp | Document Manager |
| iclpv-dm | 1389/udp | Document Manager |
| iclpv-sc | 1390/tcp | Storage Controller |
| iclpv-sc | 1390/udp | Storage Controller |
| iclpv-sas | 1391/tcp | Storage Access Server |
| iclpv-sas | 1391/udp | Storage Access Server |
| iclpv-pm | 1392/tcp | Print Manager |
| iclpv-pm | 1392/udp | Print Manager |
| iclpv-nls | 1393/tcp | Network Log Server |
| iclpv-nls | 1393/udp | Network Log Server |
| iclpv-nlc | 1394/tcp | Network Log Client |
| iclpv-nlc | 1394/udp | Network Log Client |
| iclpv-wsm | 1395/tcp | PC Workstation Manager software |
| iclpv-wsm | 1395/udp | PC Workstation Manager software |
| # | | A.P. Hobson |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

| | | |
|-----------------|----------|-------------------------------------|
| dvl-activemail | 1396/tcp | DVL Active Mail |
| dvl-activemail | 1396/udp | DVL Active Mail |
| audio-activmail | 1397/tcp | Audio Active Mail |
| audio-activmail | 1397/udp | Audio Active Mail |
| video-activmail | 1398/tcp | Video Active Mail |
| video-activmail | 1398/udp | Video Active Mail |
| # | | Ehud Shapiro |
| cadkey-licman | 1399/tcp | Cadkey License Manager |
| cadkey-licman | 1399/udp | Cadkey License Manager |
| cadkey-tablet | 1400/tcp | Cadkey Tablet Daemon |
| cadkey-tablet | 1400/udp | Cadkey Tablet Daemon |
| # | | Joe McCollough |
| goldleaf-licman | 1401/tcp | Goldleaf License Manager |
| goldleaf-licman | 1401/udp | Goldleaf License Manager |
| # | | John Fox <---none---> |
| prm-sm-np | 1402/tcp | Prospero Resource Manager |
| prm-sm-np | 1402/udp | Prospero Resource Manager |
| prm-nm-np | 1403/tcp | Prospero Resource Manager |
| prm-nm-np | 1403/udp | Prospero Resource Manager |
| # | | B. Clifford Neuman |
| igi-lm | 1404/tcp | Infinite Graphics License Manager |
| igi-lm | 1404/udp | Infinite Graphics License Manager |
| ibm-res | 1405/tcp | IBM Remote Execution Starter |
| ibm-res | 1405/udp | IBM Remote Execution Starter |
| netlabs-lm | 1406/tcp | NetLabs License Manager |
| netlabs-lm | 1406/udp | NetLabs License Manager |
| dbsa-lm | 1407/tcp | DBSA License Manager |
| dbsa-lm | 1407/udp | DBSA License Manager |
| # | | Scott Shattuck |
| sophia-lm | 1408/tcp | Sophia License Manager |
| sophia-lm | 1408/udp | Sophia License Manager |
| # | | Eric Brown |
| here-lm | 1409/tcp | Here License Manager |
| here-lm | 1409/udp | Here License Manager |
| # | | David Ison |
| hiq | 1410/tcp | HiQ License Manager |
| hiq | 1410/udp | HiQ License Manager |
| af | 1411/tcp | AudioFile |
| af | 1411/udp | AudioFile |
| # | | Jim Gettys |
| innosys | 1412/tcp | InnoSys |
| innosys | 1412/udp | InnoSys |
| innosys-ac1 | 1413/tcp | Innosys-ACL |
| innosys-ac1 | 1413/udp | Innosys-ACL |
| # | | Eric Welch <--none---> |
| ibm-mqseries | 1414/tcp | IBM MQSeries |
| ibm-mqseries | 1414/udp | IBM MQSeries |
| # | | Roger Meli |
| dbstar | 1415/tcp | DBStar |
| dbstar | 1415/udp | DBStar |
| # | | Jeffrey Millman |
| novell-lu6.2 | 1416/tcp | Novell LU6.2 |
| novell-lu6.2 | 1416/udp | Novell LU6.2 |
| # | | Peter Liu <--none---> |
| timbuktu-srv1 | 1417/tcp | Timbuktu Service 1 Port |
| timbuktu-srv1 | 1417/udp | Timbuktu Service 1 Port |
| timbuktu-srv2 | 1418/tcp | Timbuktu Service 2 Port |
| timbuktu-srv2 | 1418/udp | Timbuktu Service 2 Port |
| timbuktu-srv3 | 1419/tcp | Timbuktu Service 3 Port |
| timbuktu-srv3 | 1419/udp | Timbuktu Service 3 Port |
| timbuktu-srv4 | 1420/tcp | Timbuktu Service 4 Port |
| timbuktu-srv4 | 1420/udp | Timbuktu Service 4 Port |
| # | | Marc Epard |
| gandalf-lm | 1421/tcp | Gandalf License Manager |
| gandalf-lm | 1421/udp | Gandalf License Manager |
| # | | gilmer@gandalf.ca |
| autodesk-lm | 1422/tcp | Autodesk License Manager |
| autodesk-lm | 1422/udp | Autodesk License Manager |
| # | | David Ko |
| essbase | 1423/tcp | Essbase Arbor Software |
| essbase | 1423/udp | Essbase Arbor Software |
| hybrid | 1424/tcp | Hybrid Encryption Protocol |
| hybrid | 1424/udp | Hybrid Encryption Protocol |
| # | | Howard Hart |
| zion-lm | 1425/tcp | Zion Software License Manager |
| zion-lm | 1425/udp | Zion Software License Manager |
| # | | David Ferrero |
| sas-1 | 1426/tcp | Satellite-data Acquisition System 1 |
| sas-1 | 1426/udp | Satellite-data Acquisition System 1 |
| # | | Bill Taylor |
| mload | 1427/tcp | mload monitoring tool |
| mload | 1427/udp | mload monitoring tool |
| # | | Bob Braden |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

| | | |
|---------------|----------|---|
| informatik-lm | 1428/tcp | Informatik License Manager |
| informatik-lm | 1428/udp | Informatik License Manager |
| # | | Harald Schlangmann |
| # | | |
| nms | 1429/tcp | Hypercom NMS |
| nms | 1429/udp | Hypercom NMS |
| tpdu | 1430/tcp | Hypercom TPDU |
| tpdu | 1430/udp | Hypercom TPDU |
| # | | Noor Chowdhury |
| rgtp | 1431/tcp | Reverse Gosip Transport |
| rgtp | 1431/udp | Reverse Gosip Transport |
| # | | |
| blueberry-lm | 1432/tcp | Blueberry Software License Manager |
| blueberry-lm | 1432/udp | Blueberry Software License Manager |
| # | | Steve Beigel |
| ms-sql-s | 1433/tcp | Microsoft-SQL-Server |
| ms-sql-s | 1433/udp | Microsoft-SQL-Server |
| ms-sql-m | 1434/tcp | Microsoft-SQL-Monitor |
| ms-sql-m | 1434/udp | Microsoft-SQL-Monitor |
| # | | Peter Hussey |
| ibm-cics | 1435/tcp | IBM CISC |
| ibm-cics | 1435/udp | IBM CISC |
| # | | Geoff Meacock |
| sas-2 | 1436/tcp | Satellite-data Acquisition System 2 |
| sas-2 | 1436/udp | Satellite-data Acquisition System 2 |
| # | | Bill Taylor |
| tabula | 1437/tcp | Tabula |
| tabula | 1437/udp | Tabula |
| # | | Marcelo Einhorn |
| # | | |
| eicon-server | 1438/tcp | Eicon Security Agent/Server |
| eicon-server | 1438/udp | Eicon Security Agent/Server |
| eicon-x25 | 1439/tcp | Eicon X25/SNA Gateway |
| eicon-x25 | 1439/udp | Eicon X25/SNA Gateway |
| eicon-slp | 1440/tcp | Eicon Service Location Protocol |
| eicon-slp | 1440/udp | Eicon Service Location Protocol |
| # | | Pat Calhoun |
| cadis-1 | 1441/tcp | Cadis License Management |
| cadis-1 | 1441/udp | Cadis License Management |
| cadis-2 | 1442/tcp | Cadis License Management |
| cadis-2 | 1442/udp | Cadis License Management |
| # | | Todd Wichers |
| ies-lm | 1443/tcp | Integrated Engineering Software |
| ies-lm | 1443/udp | Integrated Engineering Software |
| # | | David Tong |
| marcam-lm | 1444/tcp | Marcam License Management |
| marcam-lm | 1444/udp | Marcam License Management |
| # | | Therese Hunt |
| proxima-lm | 1445/tcp | Proxima License Manager |
| proxima-lm | 1445/udp | Proxima License Manager |
| ora-lm | 1446/tcp | Optical Research Associates License Manager |
| ora-lm | 1446/udp | Optical Research Associates License Manager |
| apri-lm | 1447/tcp | Applied Parallel Research LM |
| apri-lm | 1447/udp | Applied Parallel Research LM |
| # | | Jim Dillon |
| oc-lm | 1448/tcp | OpenConnect License Manager |
| oc-lm | 1448/udp | OpenConnect License Manager |
| # | | Sue Barnhill |
| peport | 1449/tcp | PEport |
| peport | 1449/udp | PEport |
| # | | Qentin Neill |
| dwf | 1450/tcp | Tandem Distributed workbench Facility |
| dwf | 1450/udp | Tandem Distributed workbench Facility |
| # | | Mike Bert |
| infoman | 1451/tcp | IBM Information Management |
| infoman | 1451/udp | IBM Information Management |
| # | | Karen Burns <---none--- ></td |
| gtegsc-lm | 1452/tcp | GTE Government Systems License Man |
| gtegsc-lm | 1452/udp | GTE Government Systems License Man |
| # | | Mike Gregory |
| genie-lm | 1453/tcp | Genie License Manager |
| genie-lm | 1453/udp | Genie License Manager |
| # | | Paul Applegate |
| interhdl_elmd | 1454/tcp | interHDL License Manager |
| interhdl_elmd | 1454/udp | interHDL License Manager |
| # | | Eli Sternheim eli@interhdl.com |
| esl-lm | 1455/tcp | ESL License Manager |
| esl-lm | 1455/udp | ESL License Manager |
| # | | Abel Chou |
| dca | 1456/tcp | DCA |
| dca | 1456/udp | DCA |
| # | | Jeff Garbers |
| valisys-lm | 1457/tcp | Valisys License Manager |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

| | | |
|----------------|----------|---|
| valisys-lm | 1457/udp | Valisys License Manager |
| # | | Leslie Lincoln |
| nrcabq-lm | 1458/tcp | Nichols Research Corp. |
| nrcabq-lm | 1458/udp | Nichols Research Corp. |
| # | | Howard Cole |
| proshare1 | 1459/tcp | Proshare Notebook Application |
| proshare1 | 1459/udp | Proshare Notebook Application |
| proshare2 | 1460/tcp | Proshare Notebook Application |
| proshare2 | 1460/udp | Proshare Notebook Application |
| # | | Robin Kar |
| ibm_wrless_lan | 1461/tcp | IBM Wireless LAN |
| ibm_wrless_lan | 1461/udp | IBM Wireless LAN |
| # | | |
| world-lm | 1462/tcp | World License Manager |
| world-lm | 1462/udp | World License Manager |
| # | | Michael S Amirault |
| nucleus | 1463/tcp | Nucleus |
| nucleus | 1463/udp | Nucleus |
| # | | Venky Nagar |
| msl_lmd | 1464/tcp | MSL License Manager |
| msl_lmd | 1464/udp | MSL License Manager |
| # | | Matt Timmermans |
| pipes | 1465/tcp | Pipes Platform |
| pipes | 1465/udp | Pipes Platform mfarlin@peerlogic.com |
| # | | Mark Farlin |
| oceansoft-lm | 1466/tcp | Ocean Software License Manager |
| oceansoft-lm | 1466/udp | Ocean Software License Manager |
| # | | Randy Leonard |
| csdmbase | 1467/tcp | CSDMBASE |
| csdmbase | 1467/udp | CSDMBASE |
| csdm | 1468/tcp | CSDM |
| csdm | 1468/udp | CSDM |
| # | | Robert Stabl |
| aal-lm | 1469/tcp | Active Analysis Limited License Manager |
| aal-lm | 1469/udp | Active Analysis Limited License Manager |
| # | | David Snocken +44 (71)437-7009 |
| uaiact | 1470/tcp | Universal Analytics |
| uaiact | 1470/udp | Universal Analytics |
| # | | Mark R. Ludwig |
| csdmbase | 1471/tcp | csdmbase |
| csdmbase | 1471/udp | csdmbase |
| csdm | 1472/tcp | csdm |
| csdm | 1472/udp | csdm |
| # | | Robert Stabl |
| openmath | 1473/tcp | OpenMath |
| openmath | 1473/udp | OpenMath |
| # | | Garth Mayville |
| telefinder | 1474/tcp | Telefinder |
| telefinder | 1474/udp | Telefinder |
| # | | Jim White |
| taligent-lm | 1475/tcp | Taligent License Manager |
| taligent-lm | 1475/udp | Taligent License Manager |
| # | | Mark Sapsford |
| clvm-cfg | 1476/tcp | clvm-cfg |
| clvm-cfg | 1476/udp | clvm-cfg |
| # | | Eric Soderberg |
| ms-sna-server | 1477/tcp | ms-sna-server |
| ms-sna-server | 1477/udp | ms-sna-server |
| ms-sna-base | 1478/tcp | ms-sna-base |
| ms-sna-base | 1478/udp | ms-sna-base |
| # | | Gordon Mangione |
| dberegister | 1479/tcp | dberegister |
| dberegister | 1479/udp | dberegister |
| # | | Brian Griswold |
| pacerforum | 1480/tcp | PacerForum |
| pacerforum | 1480/udp | PacerForum |
| # | | Peter Caswell |
| airs | 1481/tcp | AIRS |
| airs | 1481/udp | AIRS |
| # | | Bruce Wilson, 905-771-6161 |
| miteksys-lm | 1482/tcp | Miteksys License Manager |
| miteksys-lm | 1482/udp | Miteksys License Manager |
| # | | Shane McRoberts |
| afs | 1483/tcp | AFS License Manager |
| afs | 1483/udp | AFS License Manager |
| # | | Michael R. Pizolato |
| confluent | 1484/tcp | Confluent License Manager |
| confluent | 1484/udp | Confluent License Manager |
| # | | James Greenfiel |
| lansource | 1485/tcp | LANSOURCE |
| lansource | 1485/udp | LANSOURCE |
| # | | Doug Scott |
| nms_topo_serv | 1486/tcp | nms_topo_serv |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

| | | |
|----------------|-----------|--|
| nms_topo_serv | 1486/udp | nms_topo_serv |
| # | | Sylvia Siu |
| localinfosrvr | 1487/tcp | LocalInfoSrvr |
| localinfosrvr | 1487/udp | LocalInfoSrvr |
| # | | Brian Matthews |
| docstor | 1488/tcp | DocStor |
| docstor | 1488/udp | DocStor |
| # | | Brian Spears |
| dmdocbroker | 1489/tcp | dmdocbroker |
| dmdocbroker | 1489/udp | dmdocbroker |
| # | | Razmik Abnous |
| insitu-conf | 1490/tcp | insitu-conf |
| insitu-conf | 1490/udp | insitu-conf |
| # | | Paul Blacknell |
| anynetgateway | 1491/tcp | anynetgateway |
| anynetgateway | 1491/udp | anynetgateway |
| # | | Dan Poirier |
| stone-design-1 | 1492/tcp | stone-design-1 |
| stone-design-1 | 1492/udp | stone-design-1 |
| # | | Andrew Stone |
| netmap_lm | 1493/tcp | netmap_lm |
| netmap_lm | 1493/udp | netmap_lm |
| # | | Phillip Magson |
| ica | 1494/tcp | ica |
| ica | 1494/udp | ica |
| # | | John Richardson, Citrix Systems |
| cvc | 1495/tcp | cvc |
| cvc | 1495/udp | cvc |
| # | | Bill Davidson |
| liberty-lm | 1496/tcp | liberty-lm |
| liberty-lm | 1496/udp | liberty-lm |
| # | | Jim Rogers |
| rfx-lm | 1497/tcp | rfx-lm |
| rfx-lm | 1497/udp | rfx-lm |
| # | | Bill Bishop |
| watcom-sql | 1498/tcp | Watcom-SQL |
| watcom-sql | 1498/udp | Watcom-SQL |
| # | | Rog Skubowius |
| fhc | 1499/tcp | Federico Heinz Consultora |
| fhc | 1499/udp | Federico Heinz Consultora |
| # | | Federico Heinz |
| vlsi-lm | 1500/tcp | VLSI License Manager |
| vlsi-lm | 1500/udp | VLSI License Manager |
| # | | Shue-Lin Kuo |
| sas-3 | 1501/tcp | Satellite-data Acquisition System 3 |
| sas-3 | 1501/udp | Satellite-data Acquisition System 3 |
| # | | Bill Taylor |
| shivadiscovery | 1502/tcp | Shiva |
| shivadiscovery | 1502/udp | Shiva |
| # | | Jonathan Wenocur |
| imtc-mcs | 1503/tcp | Databeam |
| imtc-mcs | 1503/udp | Databeam |
| # | | Jim Johnstone |
| evb-el | 1504/tcp | EVb Software Engineering License Manager |
| evb-el | 1504/udp | EVb Software Engineering License Manager |
| # | | B.G. Mahesh < mahesh@sett.com> |
| funkproxy | 1505/tcp | Funk Software, Inc. |
| funkproxy | 1505/udp | Funk Software, Inc. |
| # | | Robert D. Vincent |
| # | 1506-1523 | Unassigned |
| ingreslock | 1524/tcp | ingres |
| ingreslock | 1524/udp | ingres |
| orasrv | 1525/tcp | oracle |
| orasrv | 1525/udp | oracle |
| prospero-np | 1525/tcp | Prospero Directory Service non-priv |
| prospero-np | 1525/udp | Prospero Directory Service non-priv |
| pdap-np | 1526/tcp | Prospero Data Access Prot non-priv |
| pdap-np | 1526/udp | Prospero Data Access Prot non-priv |
| # | | B. Clifford Neuman |
| tlisrv | 1527/tcp | oracle |
| tlisrv | 1527/udp | oracle |
| coauthor | 1529/tcp | oracle |
| coauthor | 1529/udp | oracle |
| issd | 1600/tcp | |
| issd | 1600/udp | |
| nkd | 1650/tcp | |
| nkd | 1650/udp | |
| proshareaudio | 1651/tcp | proshare conf audio |
| proshareaudio | 1651/udp | proshare conf audio |
| prosharevideo | 1652/tcp | proshare conf video |
| prosharevideo | 1652/udp | proshare conf video |
| prosharedata | 1653/tcp | proshare conf data |
| prosharedata | 1653/udp | proshare conf data |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

```

prosharerequest 1654/tcp    proshare conf request
prosharerequest 1654/udp    proshare conf request
prosharenotify  1655/tcp    proshare conf notify
prosharenotify  1655/udp    proshare conf notify
#
netview-aix-1   1661/tcp    netview-aix-1
netview-aix-1   1661/udp    netview-aix-1
netview-aix-2   1662/tcp    netview-aix-2
netview-aix-2   1662/udp    netview-aix-2
netview-aix-3   1663/tcp    netview-aix-3
netview-aix-3   1663/udp    netview-aix-3
netview-aix-4   1664/tcp    netview-aix-4
netview-aix-4   1664/udp    netview-aix-4
netview-aix-5   1665/tcp    netview-aix-5
netview-aix-5   1665/udp    netview-aix-5
netview-aix-6   1666/tcp    netview-aix-6
netview-aix-6   1666/udp    netview-aix-6
#
licensedaemon   1986/tcp    cisco license management
licensedaemon   1986/udp    cisco license management
tr-rsrb-p1      1987/tcp    cisco RSRB Priority 1 port
tr-rsrb-p1      1987/udp    cisco RSRB Priority 1 port
tr-rsrb-p2      1988/tcp    cisco RSRB Priority 2 port
tr-rsrb-p2      1988/udp    cisco RSRB Priority 2 port
tr-rsrb-p3      1989/tcp    cisco RSRB Priority 3 port
tr-rsrb-p3      1989/udp    cisco RSRB Priority 3 port
#PROBLEMS!=====
mshnet          1989/tcp    MHSnet system
mshnet          1989/udp    MHSnet system
#
Bob Kummerfeld
#PROBLEMS!=====
stun-p1         1990/tcp    cisco STUN Priority 1 port
stun-p1         1990/udp    cisco STUN Priority 1 port
stun-p2         1991/tcp    cisco STUN Priority 2 port
stun-p2         1991/udp    cisco STUN Priority 2 port
stun-p3         1992/tcp    cisco STUN Priority 3 port
stun-p3         1992/udp    cisco STUN Priority 3 port
#PROBLEMS!=====
ipsendmsg       1992/tcp    IPsendmsg
ipsendmsg       1992/udp    IPsendmsg
#
Bob Kummerfeld
#PROBLEMS!=====
snmp-tcp-port   1993/tcp    cisco SNMP TCP port
snmp-tcp-port   1993/udp    cisco SNMP TCP port
stun-port       1994/tcp    cisco serial tunnel port
stun-port       1994/udp    cisco serial tunnel port
perf-port       1995/tcp    cisco perf port
perf-port       1995/udp    cisco perf port
tr-rsrb-port    1996/tcp    cisco Remote SRB port
tr-rsrb-port    1996/udp    cisco Remote SRB port
gdp-port        1997/tcp    cisco Gateway Discovery Protocol
gdp-port        1997/udp    cisco Gateway Discovery Protocol
x25-svc-port    1998/tcp    cisco X.25 service (XOT)
x25-svc-port    1998/udp    cisco X.25 service (XOT)
tcp-id-port     1999/tcp    cisco identification port
tcp-id-port     1999/udp    cisco identification port
callbook       2000/tcp
callbook       2000/udp
dc              2001/tcp
wizard         2001/udp    curry
globe          2002/tcp
globe          2002/udp
mailbox        2004/tcp
emce           2004/udp    CCWS mm conf
berknet        2005/tcp
oracle         2005/udp
invokator      2006/tcp
raid-cc        2006/udp    raid
dectalk        2007/tcp
raid-am        2007/udp
conf           2008/tcp
terminaldb     2008/udp
news           2009/tcp
whosockami     2009/udp
search         2010/tcp
pipe_server    2010/udp
raid-cc        2011/tcp    raid
servserv       2011/udp
ttyinfo        2012/tcp
raid-ac        2012/udp
raid-am        2013/tcp
raid-cd        2013/udp
troff          2014/tcp

```

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

| | | |
|----------------|----------|------------------------------------|
| raid-sf | 2014/udp | |
| cypress | 2015/tcp | |
| raid-cs | 2015/udp | |
| bootserver | 2016/tcp | |
| bootserver | 2016/udp | |
| cypress-stat | 2017/tcp | |
| bootclient | 2017/udp | |
| terminaldb | 2018/tcp | |
| rellpack | 2018/udp | |
| whosockami | 2019/tcp | |
| about | 2019/udp | |
| xinupageserver | 2020/tcp | |
| xinupageserver | 2020/udp | |
| servexec | 2021/tcp | |
| xinuexpansion1 | 2021/udp | |
| down | 2022/tcp | |
| xinuexpansion2 | 2022/udp | |
| xinuexpansion3 | 2023/tcp | |
| xinuexpansion3 | 2023/udp | |
| xinuexpansion4 | 2024/tcp | |
| xinuexpansion4 | 2024/udp | |
| ellpack | 2025/tcp | |
| xribs | 2025/udp | |
| scrabble | 2026/tcp | |
| scrabble | 2026/udp | |
| shadowserver | 2027/tcp | |
| shadowserver | 2027/udp | |
| submitserver | 2028/tcp | |
| submitserver | 2028/udp | |
| device2 | 2030/tcp | |
| device2 | 2030/udp | |
| blackboard | 2032/tcp | |
| blackboard | 2032/udp | |
| glogger | 2033/tcp | |
| glogger | 2033/udp | |
| scoremgr | 2034/tcp | |
| scoremgr | 2034/udp | |
| imsl doc | 2035/tcp | |
| imsl doc | 2035/udp | |
| objectmanager | 2038/tcp | |
| objectmanager | 2038/udp | |
| isis | 2042/tcp | |
| isis | 2042/udp | |
| isis-bcast | 2043/tcp | |
| isis-bcast | 2043/udp | |
| rims1 | 2044/tcp | |
| rims1 | 2044/udp | |
| cdfunc | 2045/tcp | |
| cdfunc | 2045/udp | |
| sdfunc | 2046/tcp | |
| sdfunc | 2046/udp | |
| dls | 2047/tcp | |
| dls | 2047/udp | |
| dls-monitor | 2048/tcp | |
| dls-monitor | 2048/udp | |
| shilp | 2049/tcp | |
| shilp | 2049/udp | |
| dlsrpn | 2065/tcp | Data Link Switch Read Port Number |
| dlsrpn | 2065/udp | Data Link Switch Read Port Number |
| dlswpn | 2067/tcp | Data Link Switch Write Port Number |
| dlswpn | 2067/udp | Data Link Switch Write Port Number |
| ats | 2201/tcp | Advanced Training System Program |
| ats | 2201/udp | Advanced Training System Program |
| rtsserv | 2500/tcp | Resource Tracking system server |
| rtsserv | 2500/udp | Resource Tracking system server |
| rtscclient | 2501/tcp | Resource Tracking system client |
| rtscclient | 2501/udp | Resource Tracking system client |
| # | | Aubrey Turner |
| # | | |
| hp-3000-telnet | 2564/tcp | HP 3000 NS/VT block mode telnet |
| www-dev | 2784/tcp | world wide web - development |
| www-dev | 2784/udp | world wide web - development |
| NSWS | 3049/tcp | |
| NSWS | 3049/udp | |
| ccmail | 3264/tcp | cc:mail/lotus |
| ccmail | 3264/udp | cc:mail/lotus |
| dec-notes | 3333/tcp | DEC Notes |
| dec-notes | 3333/udp | DEC Notes |
| # | | Kim Moraros |
| mapper-nodemgr | 3984/tcp | MAPPER network node manager |
| mapper-nodemgr | 3984/udp | MAPPER network node manager |
| mapper-mapethd | 3985/tcp | MAPPER TCP/IP server |
| mapper-mapethd | 3985/udp | MAPPER TCP/IP server |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

| | | |
|-----------------|---------------|------------------------------------|
| mapper-ws_ethd | 3986/tcp | MAPPER workstation server |
| mapper-ws_ethd | 3986/udp | MAPPER workstation server |
| # | | John C. Horton |
| bmap | 3421/tcp | Bull Apprise portmapper |
| bmap | 3421/udp | Bull Apprise portmapper |
| # | | Jeremy Gilbert |
| udt_os | 3900/tcp | Unidata UDT OS |
| udt_os | 3900/udp | Unidata UDT OS |
| # | | James Powell |
| nuts_dem | 4132/tcp | NUTS Daemon |
| nuts_dem | 4132/udp | NUTS Daemon |
| nuts_bootp | 4133/tcp | NUTS Bootp Server |
| nuts_bootp | 4133/udp | NUTS Bootp Server |
| # | | Martin Freiss |
| unicall | 4343/tcp | UNICALL |
| unicall | 4343/udp | UNICALL |
| # | | James Powell |
| krb524 | 4444/tcp | KRB524 |
| krb524 | 4444/udp | KRB524 |
| # | | B. Clifford Neuman |
| rfa | 4672/tcp | remote file access server |
| rfa | 4672/udp | remote file access server |
| complex-main | 5000/tcp | |
| complex-main | 5000/udp | |
| complex-link | 5001/tcp | |
| complex-link | 5001/udp | |
| rfe | 5002/tcp | radio free ethernet |
| rfe | 5002/udp | radio free ethernet |
| telepathstart | 5010/tcp | TelepathStart |
| telepathstart | 5010/udp | TelepathStart |
| telepathattack | 5011/tcp | TelepathAttack |
| telepathattack | 5011/udp | TelepathAttack |
| # | | Helmuth Breitenfellner |
| mmcc | 5050/tcp | multimedia conference control tool |
| mmcc | 5050/udp | multimedia conference control tool |
| rmonitor_secure | 5145/tcp | |
| rmonitor_secure | 5145/udp | |
| aol | 5190/tcp | America-Online |
| aol | 5190/udp | America-Online |
| # | | Marty Lyons |
| padl2sim | 5236/tcp | |
| padl2sim | 5236/udp | |
| hac1-hb | 5300/tcp | # HA cluster heartbeat |
| hac1-hb | 5300/udp | # HA cluster heartbeat |
| hac1-gs | 5301/tcp | # HA cluster general services |
| hac1-gs | 5301/udp | # HA cluster general services |
| hac1-cfg | 5302/tcp | # HA cluster configuration |
| hac1-cfg | 5302/udp | # HA cluster configuration |
| hac1-probe | 5303/tcp | # HA cluster probing |
| hac1-probe | 5303/udp | # HA cluster probing |
| hac1-local | 5304/tcp | |
| hac1-local | 5304/udp | |
| hac1-test | 5305/tcp | |
| hac1-test | 5305/udp | |
| # | | Eric Soderberg |
| x11 | 6000-6063/tcp | X Window System |
| x11 | 6000-6063/udp | X Window System |
| # | | Stephen Gildea |
| sub-process | 6111/tcp | HP SoftBench Sub-Process Control |
| sub-process | 6111/udp | HP SoftBench Sub-Process Control |
| meta-corp | 6141/tcp | Meta Corporation License Manager |
| meta-corp | 6141/udp | Meta Corporation License Manager |
| # | | Osamu Masuda <--none--> |
| aspentec-lm | 6142/tcp | Aspen Technology License Manager |
| aspentec-lm | 6142/udp | Aspen Technology License Manager |
| # | | Kevin Massey |
| watershed-lm | 6143/tcp | Watershed License Manager |
| watershed-lm | 6143/udp | Watershed License Manager |
| # | | David Ferrero |
| statsci1-lm | 6144/tcp | StatSci License Manager - 1 |
| statsci1-lm | 6144/udp | StatSci License Manager - 1 |
| statsci2-lm | 6145/tcp | StatSci License Manager - 2 |
| statsci2-lm | 6145/udp | StatSci License Manager - 2 |
| # | | Scott Blachowicz |
| lonewolf-lm | 6146/tcp | Lone Wolf Systems License Manager |
| lonewolf-lm | 6146/udp | Lone Wolf Systems License Manager |
| # | | Dan Klein |
| montage-lm | 6147/tcp | Montage License Manager |
| montage-lm | 6147/udp | Montage License Manager |
| # | | Michael Ubell |
| xdsxdm | 6558/udp | |
| xdsxdm | 6558/tcp | |
| afs3-fileserver | 7000/tcp | file server itself |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

| | | |
|-----------------|-----------|--|
| afs3-fileserver | 7000/udp | file server itself |
| afs3-callback | 7001/tcp | callbacks to cache managers |
| afs3-callback | 7001/udp | callbacks to cache managers |
| afs3-prserver | 7002/tcp | users & groups database |
| afs3-prserver | 7002/udp | users & groups database |
| afs3-vlserver | 7003/tcp | volume location database |
| afs3-vlserver | 7003/udp | volume location database |
| afs3-kaserver | 7004/tcp | AFS/Kerberos authentication service |
| afs3-kaserver | 7004/udp | AFS/Kerberos authentication service |
| afs3-volser | 7005/tcp | volume managment server |
| afs3-volser | 7005/udp | volume managment server |
| afs3-errors | 7006/tcp | error interpretation service |
| afs3-errors | 7006/udp | error interpretation service |
| afs3-bos | 7007/tcp | basic overseer process |
| afs3-bos | 7007/udp | basic overseer process |
| afs3-update | 7008/tcp | server-to-server updater |
| afs3-update | 7008/udp | server-to-server updater |
| afs3-rmtsys | 7009/tcp | remote cache manager service |
| afs3-rmtsys | 7009/udp | remote cache manager service |
| ups-onlinet | 7010/tcp | onlinet uninterruptable power supplies |
| ups-onlinet | 7010/udp | onlinet uninterruptable power supplies |
| # | | Brian Hammill |
| font-service | 7100/tcp | X Font Service |
| font-service | 7100/udp | X Font Service |
| # | | Stephen Gildea |
| fodms | 7200/tcp | FODMS FLIP |
| fodms | 7200/udp | FODMS FLIP |
| # | | David Anthony |
| man | 9535/tcp | |
| man | 9535/udp | |
| isode-dua | 17007/tcp | |
| isode-dua | 17007/udp | |

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

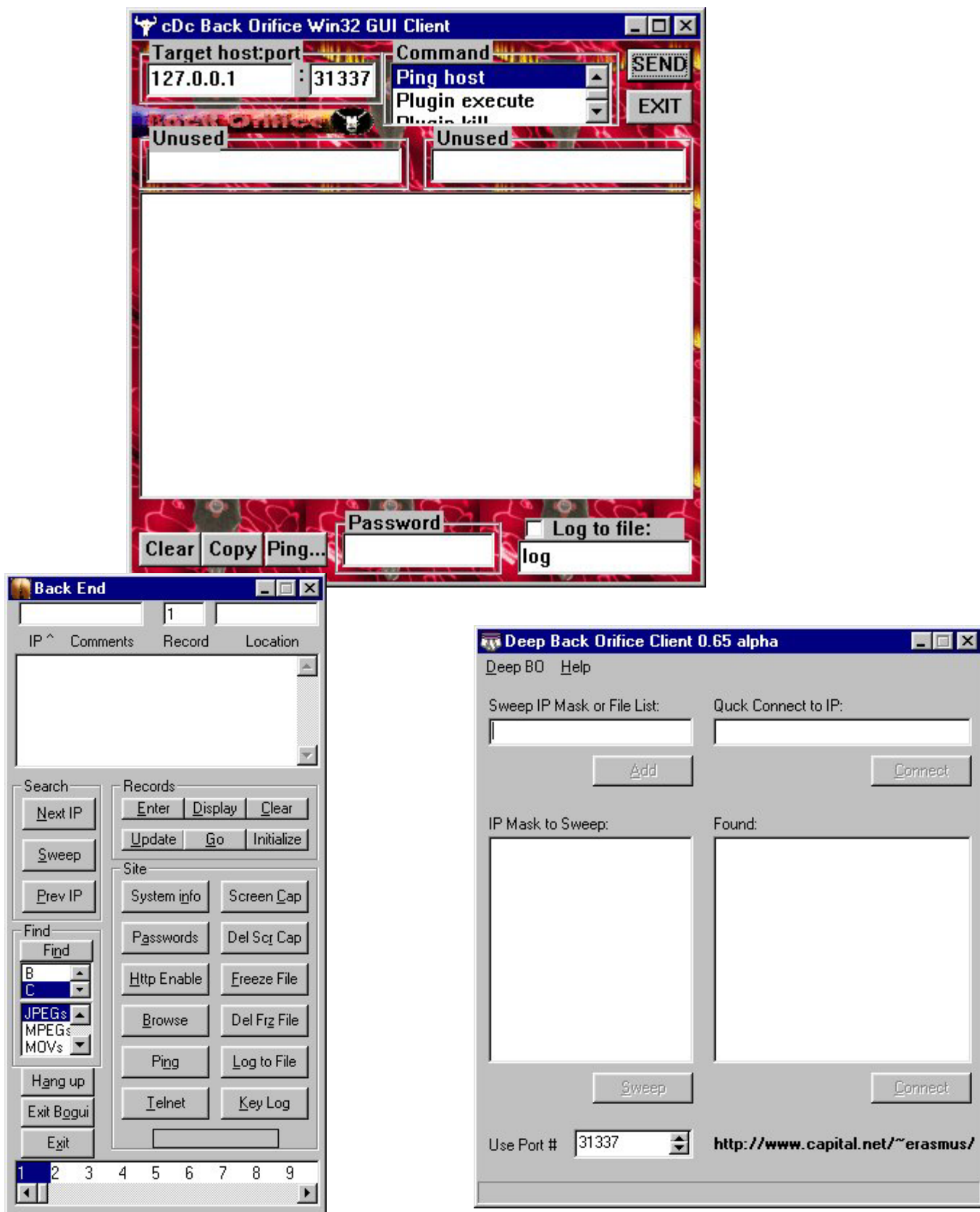
Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Telas de Trojans Mais Conhecidos

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Back Orifice FrontEnds (Clients)

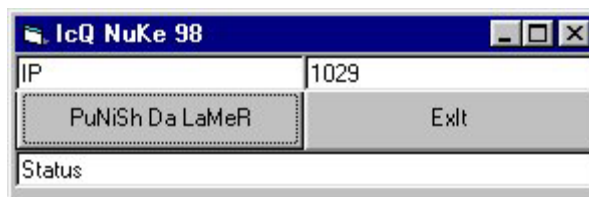


Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

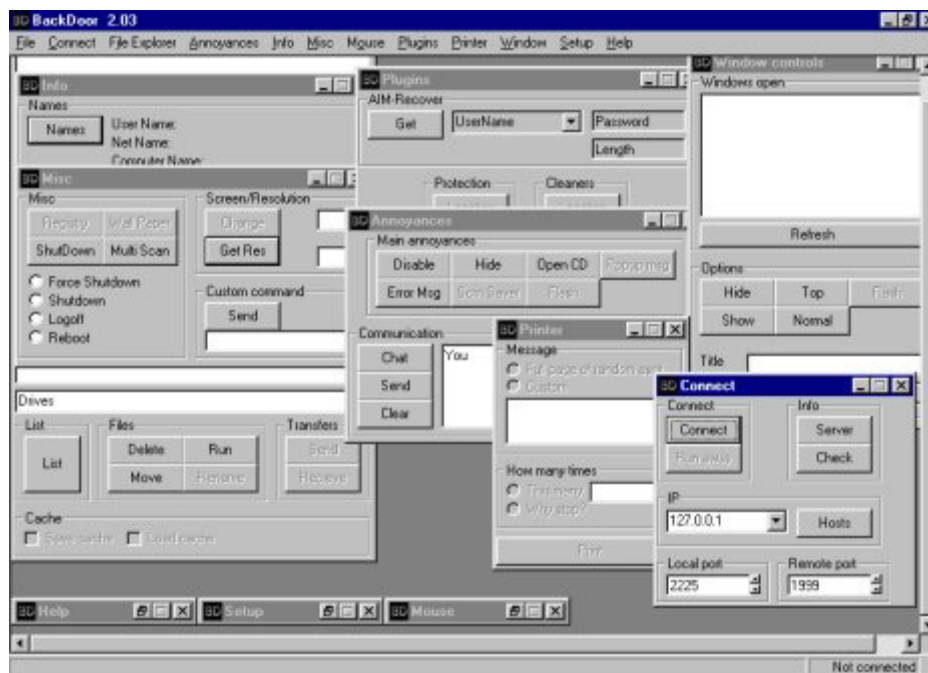
Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Backdoor

Tela do trojan:



Tela do Backdoor



ICKiller ou ICQKiller



Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

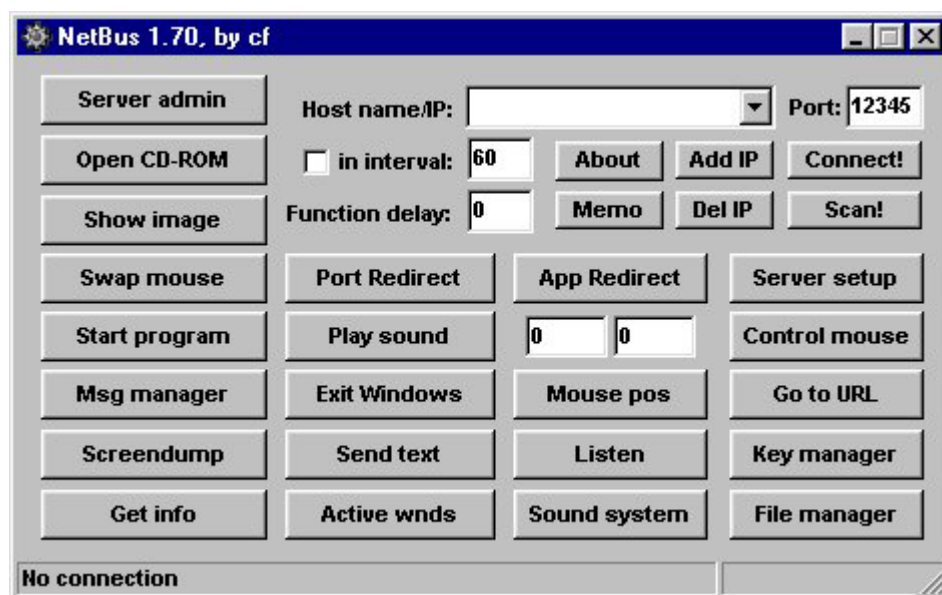
Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

NetBus

Tela de um trojan conhecido como “Whack-A-Mole”



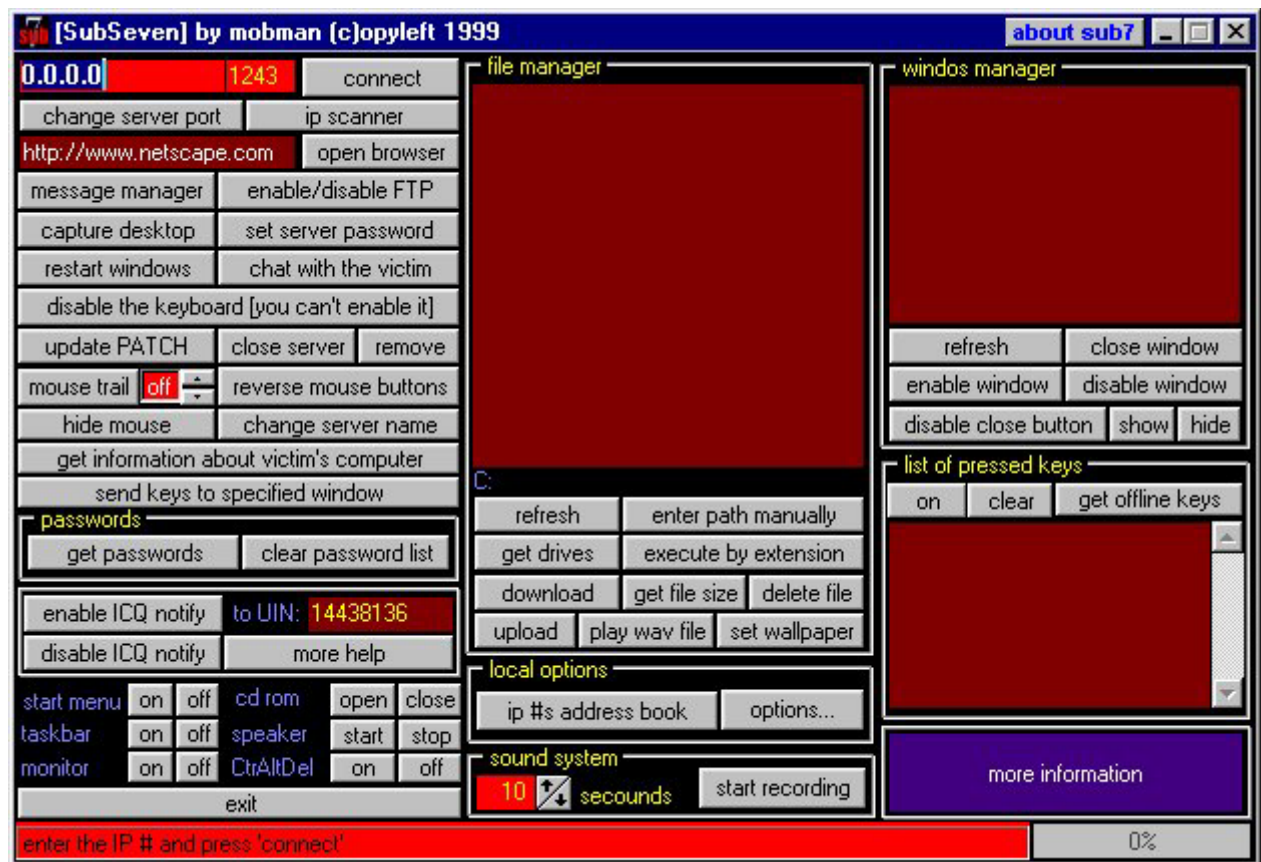
Tela de Controle



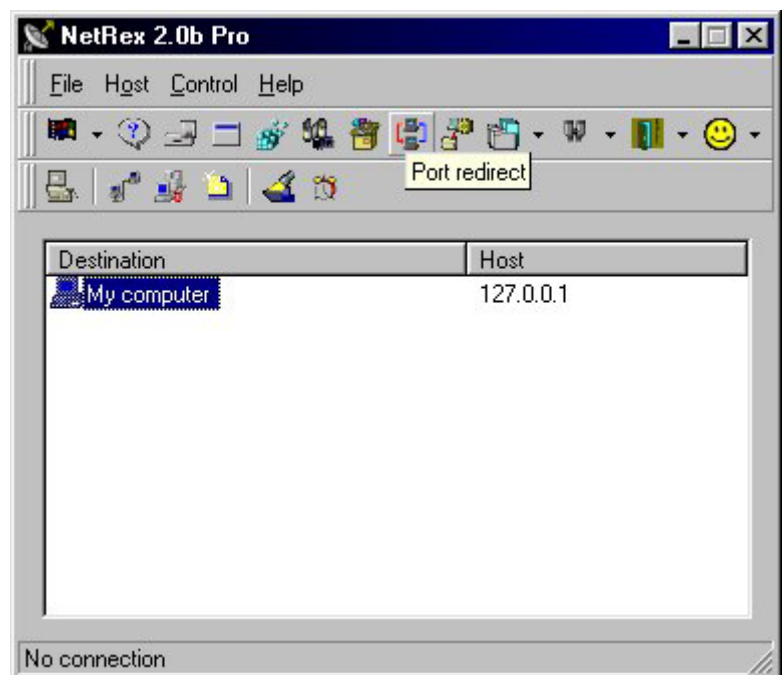
Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

SubSeven



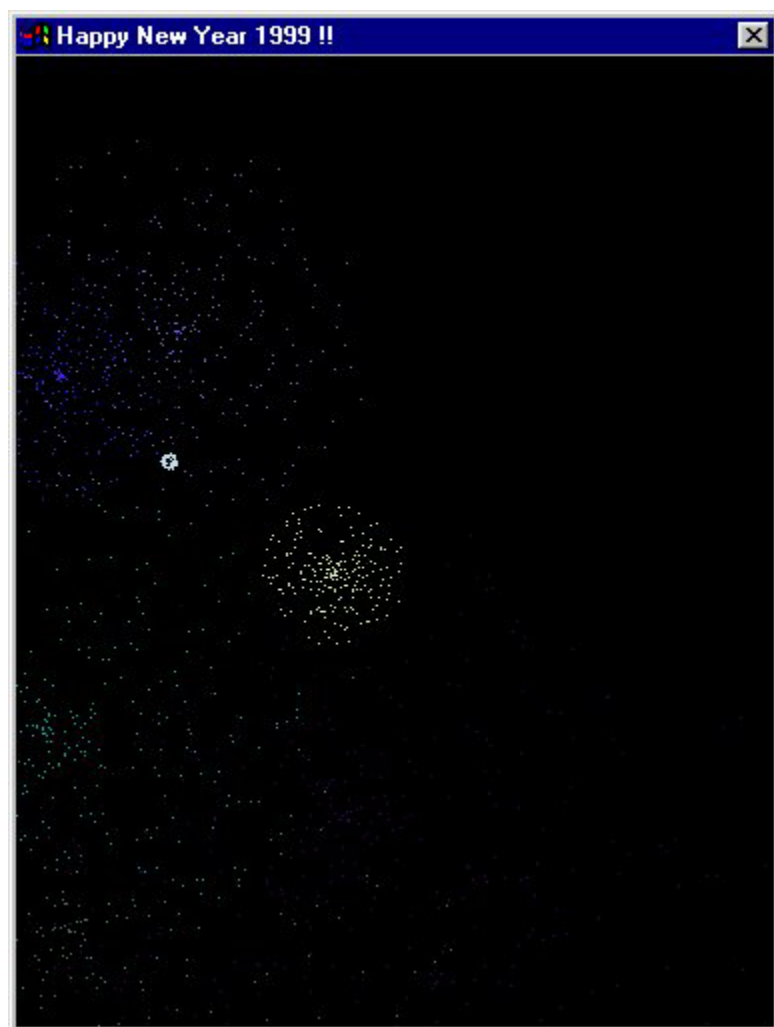
NetRex (Clone do NetBus 2.0)



Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Happy99



Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.

Deep Throat



Romulo Moacyr Cholewa – <http://www.rmc.eti.br>, agosto de 2001. Vide “Distribuição / Cópia” neste material para maiores detalhes.