

Segurança

Tecnologias Anti-Hacker



1. Apresentação do Curso

O Objetivo do curso é levar aos alunos o conhecimento sobre invasões de computadores, desde o motivo até a solução, passando por vulnerabilidades e como torná-las sem efeito. Inclui também conceitos básicos de rede e de comunicação de dados.

O Curso

Durante o curso será apresentado material 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 e o que lhes aconteceram, 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 redes, conhecimento de programação (geralmente em linguagens como C, C++, Java e Assembler). Contudo, existem diversos tipos de "hackers", dos que possuem mais experiência para os que apenas "copiam" furos de segurança explorados por outros hackers.

Temos:

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.

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.

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 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 ser detectado (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 Tsutomu Shimomura estavam chegando a um nome, ele conseguia enganar as investigações através do controle que tinha da rede de telefonia da GTE (consessionária telefônica dos 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", ou "xforce.iss.net". 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, desassemblaram o código do sistema operacional de um celular da OKI. 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 uma 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. Enquanto isso, aproveitou seu acesso "invisível" através do "The Well" para invadir um outro provedor, chamado NetCom, de onde roubou milhares de cartões de crédito. Após isso, invadiu uma máquina em toad.com. De lá, iniciou o ataque à rede de Tsutomu Shimomura. Através de um 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), 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.

Tsutomu conseguiu chegar a Kevin devido a um rastro deixado em Ariel. Nela, algumas informações apontavam para a máquina em quem confiava, contudo, como isso poderia ocorrer, uma vez que a mesma estava fora do ar? 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.

2. 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 camandas falhar, provavelmente não haverá comunicação.

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 entendida foram atendidas. Imagine que, 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 4 cadeias decimais separadas por pontos (esta representação é apenas para tornar nossas vidas mais fáceis). Ele entende como 4 octetos, ou 4 campos de 8 bits:

11001000.11110001.11101100.01011110

Algumas conclusões e fatos 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 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.

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 para ir a 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.

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 (e 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.invasao.com.br". Este caso é uma referência ao servidor www, dentro do domínio invasao.com.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.

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 transporta 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 em qualquer sentido. Portanto, ao tentar ler seu correio eletrônico, 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.

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 3 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 reposta 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.

...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 pode haver 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 backbone da Embratel. 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).

3. Entendendo a Invasão

"Na Internet Brasileira, a quantidade de vítimas, sejam corporativas ou o usuário final, só não é maior pela falta de conhecimento que nossos "hackers wannabe" possuem, 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. 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.

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:

NTBugtraq

A lista NTBugtraq é uma lista moderada por um canadense chamado 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 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>

NT Security

A lista NT Security é uma lista NÃO 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 no seguinte endereço:

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

Os white-hats (os black-hats e crackers também) se mantêm muito bem atualizados. Ser inscrito em diversas lista 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://www.hackers.com.br>

Ponto de Vista do Black-Hat

O black-hat possui tanta habilidade quanto o white-hat. Porém, ao descobrir uma nova vulnerabilidade, não publicará esta 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 no anexo 6). 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.

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.

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). Um resumo sobre ele pode ser encontrado em:

http://www.zdnet.com/zdtv/thesite/0797w4/iview/iview747_072497.html

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.

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 a falhas. Por consequência, também estão sujeitos à falhas.

A grande maioria dos furos de segurança surgem 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 este 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) = verdadeiro.

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.

Plataforma Windows: Windows 9x

O Windows 9x (95 ou 98) 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 pela Internet, 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.

A principal medida que deve ser adotada é a remoção do compartilhamento de arquivos e impressoras para redes Microsoft, no painel de controle. Caso seu computador participe de uma rede, dentro de uma empresa por exemplo, consulte o administrador da rede ANTES de realizar qualquer alteração. As empresas geralmente possuem políticas internas para tais configurações.

Veja:

Através do ícone "Rede" no painel de controle, se tem acesso à caixa de diálogo ao lado. Lá, você poderá encontrar o componente "Compartilhamento de arquivos e impressoras para redes Microsoft". Este componente transforma o Windows 9x em uma espécie de servidor de rede que, se configurado de forma incorreta, poderá abrir seu computador para qualquer invasor. Se não for

possível remover o componente, peça propriedades do adaptador dial-up (como na imagem acima), vá em "Ligações" e desmarque a opção "Compartilhamento de arquivos e impressoras para redes Microsoft". Isso fará com que o componente servidor do Windows 9x não esteja ativo através de sua conexão via modem / dial-up.

Além da configuração de rede de um computador Windows 9x, existem outros aspectos que devem ser observados. O primeiro deles é em relação à atualizações. O Windows 9x possui um serviço bastante interessante, chamado Windows Update. Através dele, quando conectado na Internet, você poderá atualizar seu sistema automaticamente. Basta clicar o ícone "Windows Update" no menu iniciar. Manter o seu sistema sempre atualizado é primordial para manter a segurança.

O segundo aspecto é em relação a que serviços seu computador está iniciando automaticamente ao ser ligado / inicializado. Olhe dentro do grupo "Iniciar" por programas estranhos, e nas seguintes chaves no registro:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
Por padrão, apenas o sysstray e algum programa anti-virus devem estar listados. Se em algumas destas linhas está aparecendo algum programa que você tenha pego da

Internet recentemente, é aconselhável instalar um anti-virus atualizado o mais rápido possível. Provavelmente é um cavalo-de-tróia.

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:

```
Microsoft(R) Windows 98  
(C)Copyright Microsoft Corp 1981-1999.
```

```
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

O Windows NT/2000 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, pois isso forçaria a escrita de um material inteiramente novo. Porém, existem alguns tópicos que podem e devem ser abordados, que contém 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 à 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, 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 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 (O Linux pode enxergar partições NTFS para leitura).

Em segundo lugar, logo após a instalação, o último "service pack" deve ser instalado. Service packs são atualizações do Windows NT, disponíveis no site da Microsoft. Estas atualizações são acumulativas, portanto, caso o último service pack seja o 7, não será necessário instalar os anteriores. Apenas a última versão. Observação: no Windows 2000, o método de atualizações foi alterado. Ele está muito parecido com o do Windows 9x (através do Windows Update). Portanto, para atualizar um sistema Windows 2000, basta escolher a opção "Windows Update" no menu iniciar. Caso deseje baixar manualmente as atualizações, poderá proceder pelo seguinte endereço:

<http://www.microsoft.com/windows2000/downloads/>

Uma vez instalado e atualizado, precisamos então realizar algumas alterações no sistema para torná-lo mais seguro. Existem 4 alterações essenciais: auditoria, remover serviços desnecessários, alterar as permissões padrão do sistema de arquivos, e alterar as configurações de rede.

1. 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, 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.

2. Removendo 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

Clipbook Server

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

SNMP Service / SNMP Trap Service

São dois serviços que permitem a utilização do Simple Network Management Protocol. Se não possuem uma intenção específica (como instalado pelo administrador para monitoração do computador) ou se não estiver corretamente configurado, pode revelar muitas informações sobre o computador em si, como interfaces de rede, rotas padrão, entre outros dados. É recomendado ter cautela com tais serviços

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 a praticamente qualquer informação. 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 (no Windows 2000, o serviço se chama "Task Scheduler")

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.

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, 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.

FTP Voyager / FTP Explorer / WS_FTP

Estes 3 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.

Microsoft SQL Enterprise Manager

O Microsoft SQL Enterprise Manager é uma console de gerência de servidores Microsoft SQL 7.0, 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.

4. 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.

Desta forma, os seguintes passos podem ser adotados:

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.

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 infra-estrutura, **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).

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 são leigos e não saberão a diferença entre um 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.

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. Alguns deles são:

CA Unicenter TNG FrameWork

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

Este é um programa extramamente caro, da Computer Associates, que tem por objetivo a gerência completa da uma infra-estrutura de TI, desde módulos de anti-virus até backup. Porém, o módulo básico, chamado "Framework", é gratuito, e pode ser baixado do site da CA para avaliação. Porém, apesar de gratuito, o módulo básico possui o mapeamento de rede via SNMP (Simple Network Management Protocol) incluído. Com esta aplicação, usando o protocolo SNMP, que a grande maioria dos roteadores, switches, e outros equipamentos de conectividade suportam, inclusive servidores, é possível construir o mapa de uma rede com detalhes impressionantes. Portanto, é primordial numa rede, que o firewall filtre tráfego SNMP (portas 161 e 162).

Existem outros 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.

Essential Net Tools

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 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)

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.

WhatsUp Gold

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

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 invasao.com.br 25
```

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

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

Trojan Horses e Back Doors

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

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

Veja no anexo 7, 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://www.antivirus.com>

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).

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.

No anexo 8, temos um exemplo de buffer overflow no Windows NT.

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 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).

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

Internet Security Systems Xforce

PacketStorm Library

CIAC (Computer Incident Advisory Capability)

CERT (Computer Emergency Response Team)

5. 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, erveço 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 vezes 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 de rede inválidos também são possíveis. A cerca de 2 anos atrás, foi lançado 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 são 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).

DDoS (Distributed Denial of Service)

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. Daí surgiu a ideia do DDoS: várias máquinas espalhadas por toda a Internet, enviando tráfego simultaneamente, para um mesmo servidor, estação ou rede.

Os ataques do tipo DDoS ficaram conhecidos a partir dos ataques recentes realizados contra sites na Internet populares, 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 tem 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 2 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, atacarem uma determinada rede ou máquina.

Trin00, TFN (Tribe Flood Network, Schaft)

Estes são 3 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 endereço na Internet.

A regra básica é impedir tráfego não autorizado, não só "entrando" na rede, mas também, a partir dela.

No anexo 9, existem 2 documentos bastante interessantes sobre ataques DDoS.

IP Spoofing

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. No anexo 10, a técnica é descrita em detalhes em um ótimo whitepaper.

6. 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 wannabe 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 anti-virus e executá-lo fazendo uma varredura em todo o sistema. Isso eliminará a possibilidade de cavalos-de-tróia. Caso não ache nada, então é muito provável que, se o seu computador é 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.

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 partem 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 fácil volatilidade. 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.

Firewall (Incluindo Personal Firewall)

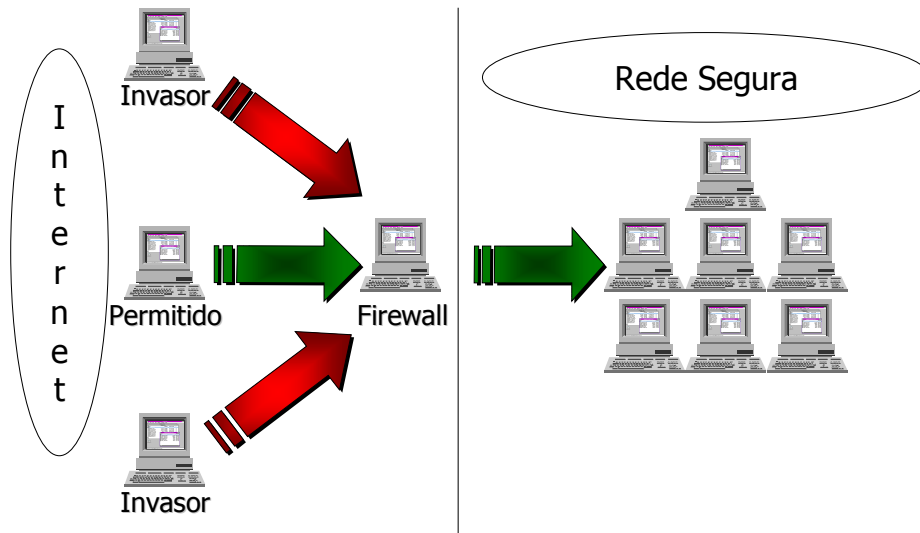
Como o nome sugere (do inglês, “parede ou porta corta fogo”), os firewalls são esquemas de hardware, software, ou os dois juntos, capazes de, baseados em características do tráfego, permitir ou não a passagem deste tráfego. Basicamente, o firewall analisa informações como endereço de origem, endereço 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 que um esquema de firewall seja eficiente, algumas regras devem ser observadas:

1. todo tráfego entre as redes PRECISA passar pelo firewall ou filtragem
2. deve existir alguma forma de reporting ou log, para se ter uma idéia de que tipo de tráfego está sendo rejeitado
3. O firewall em si deve ser imune à penetração / invasão (deve rodar o código mais simples possível, e a menor quantidade de código possível)

A seguir, vemos um esquema simples de firewall:

Firewalls: Filtragem



Existem outros modelos 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:

Existem alguns produtos, ou soluções de software bastante interessantes, que tentam implementar o mesmo princípio de um firewall em seu computador. Estes programas são chamados de Personal Firewalls, e são bem baratos, ou de graça. Alguns deles:

ZoneAlarm

Muito bom produto, um dos melhores, e gratuito. Ainda está em beta, mas é bem estável. Não recomendo a sua instalação em um computador Windows 2000 com mais de um processador.

Norton Internet Security 2000

<http://www.symantec.com/sabu/nis/>

Fantástico produto da Symantec, aclamado por diversas revistas e publicações especializadas. O núcleo do componente de filtragem veio de outro produto, o atGuard, da WRQ, que era vendido até o final do ano passado. A Symantec licenciou o produto e construiu essa suite de proteção. Inclui até anti-virus.

Para quem usa Linux, por padrão, o núcleo do sistema possui filtragem de pacotes. Atualmente, a ferramenta usada (no caso do RedHat) o IPChains.

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:

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

-- X --

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



(81) 3221-9116 / 3221-9124

www.invasao.com.br

www.futura.com.br