SEGREDOS DE HACKING REVELADOS

Informação e Guia Instrucional

SEGREDOS DE HACKING REVELADOS

Produção de ⌈ S&C Enterprises

Índice

AVISO LEGAL

Os autores deste manual gostariam de expressar nossas preocupações sobre o uso indevido
das informações contidas neste manual. Ao adquirir este manual, você
concordar com as seguintes estipulações. Quaisquer ações e / ou atividades relacionadas ao
o material contido neste manual é exclusivamente de sua responsabilidade.
O uso indevido das informações neste manual pode resultar em
acusações criminais contra as pessoas em questão. o
os autores não serão responsabilizados no caso de qualquer crime
acusações contra quaisquer indivíduos que usem indevidamente o
informações neste manual para infringir a lei.
(Nota: este manual foi criado apenas para fins informativos.)

3

Introdução

ELE internet está sempre crescendo e você e eu somos realmente pedregulhos em um vasto oceano de informações. Eles dizem o que você não saber que não pode te machucar. Quando se trata da Internet acredito exatamente o oposto. Na Internet existem milhões e milhões de usuários de computador fazendo logon e logoff diariamente. As informações são transferidas de um ponto a outro em um batimento cardiaco. Entre aqueles milhões e milhões de usuários, há tu.

Por mais humilde que você seja um usuário da Internet, você está condenado contra os tubarões da super rodovia da informação diariamente.

O problema com isso é a furtividade com que acontece. Atualmente cerca de 30-40% de todos os usuários estão cientes dos acontecimentos em seus computador. Os outros simplesmente não se importam ou não têm o "saber como" adequado para reconhecer se o seu sistema está sob ataque e ou sendo usado.

Você comprou este manual porque está preocupado com o seu privacidade na Internet. Como você deveria estar. Na internet nada é exatamente o que parece ser. O desinformado vai conseguir machucar de muitas maneiras.

T

4

Ao se interessar pela sua privacidade e segurança, você provou para estar acima do resto. Você nunca pode ter o bastante em formação. Informação é poder e quanto mais informado você, um usuário torna-se menos provável que você seja vítima de tubarões de a Internet.

Neste manual, abordarei com você coisas que podem assustá-lo. Algumas coisas podem até deixá-lo paranóico sobre ter um computador. Não desanime, pois também vou te dizer como se proteger. As razões para dizer a você a "sujeira" se você vai é que eu acho importante que você saiba o que está em risco.

Escrevi este manual como um guia. Para mostrar como os hackers ganham acesso ao seu sistema usando falhas e programas de segurança. o a teoria diz que se você estiver ciente do que eles estão fazendo e como eles estão fazendo isso, você estará em uma posição muito melhor para proteger você mesmo desses ataques.

(Ao longo deste manual, você verá referência ao termo "Hacker." Este é um termo que uso de forma muito vaga para esses indivíduos.)

Estes são apenas alguns dos tópicos que serão abordados:

□□Como "hackers" entram em seu sistema

□□Quais ferramentas eles usam
□□Como um hacker pode efetivamente “desinsetar” sua casa por meio de seu computador. (Não acredite em mim, continue lendo, você será muito surpreso)
□ A□quais informações eles têm acesso. E por que você deve tentar se proteger. (Você pode se surpreender em descobrir o que eles sabem.)
□□Dicas e truques que os hackers usam
□□Como o seu software antivírus sozinho não é suficiente
□□O que procurar se você suspeitar que está sendo hackeado
□□Qual é a maior falha em todos os computadores
□□E mais ...

5

De maneira nenhuma vou fazer uma afirmação ridícula de que este manual irá protegê-lo de tudo. O que direi é que lendo este manual, espero que você esteja em uma situação melhor para se proteger de ter suas informações comprometidas.
Você sabia que não importa se você está conectado à rede 24 horas por dia ou 15 minutos por dia seu sistema está vulnerável. Não só é vulnerável em 15 minutos, você pode perder todos seus dados são bloqueados de seu próprio sistema e têm todos os seus informações confidenciais, como “Números de contas bancárias”, “Seus Orçamento ”,“ Seu endereço residencial ”comprometido.
Não me venha com mal, não estou tentando colocá-lo em um estado de paranóia também. O que estou dizendo é que se você não tomar cuidado você se deixa vulnerável a uma ampla gama de ataques.
Talvez você esteja cético e dizendo a si mesmo "Oh, eu não faço qualquer coisa na net exceto verificar meu e-mail etc. esse tipo de coisa não pode acontecer comigo. ”
Ok eu gosto de um desafio vamos fazer um teste!

6

INTRUSÃO DO SISTEMA EM 15 SEGUNDOS

Intrusão no sistema em 15 segundos, isso mesmo, pode ser feito. Se você possui certas falhas de segurança, seu sistema pode ser quebrado em menos de 15 segundos.
Para começar este capítulo, gostaria que você fizesse o seguinte. Conectar a a Internet usando sua conta dial up se você estiver em dial up. Se você está em um serviço dedicado, como conexões de alta velocidade (ou seja, Cabo e DSL) e prossiga com as etapas abaixo.
□□Clique em **Iniciar**
□□Vá para **Executar**
□□Clique em **Executar** (é um manual passo a passo) :-)
□□Digite **Winipcfg**
□□Pressione a tecla **Enter**

Capítulo

Página 9

7
Isso deve abrir uma janela semelhante à seguinte
* Por motivos editoriais, as informações acima foram omitidas *
O que você deve ver no endereço IP é um número que parece
algo assim.
207.175.1.1 (O número será diferente.)
Se você usar o acesso discado à Internet, encontrará o seu IP
endereço sob o adaptador PPP. Se você tem acesso dedicado, você
irá encontrar o seu endereço IP com outro nome de adaptador como (PCI
Busmaster, Adaptador SMC, etc.) Você pode ver uma lista clicando em
na seta para baixo.

Página 10

8
Assim que tiver o endereço IP, anote-o e feche-o
janela clicando em (OK) e faça o seguinte.
□□Clique em **Iniciar**
□□Vá para **Executar** (clique em **Executar**)
□□Digite o comando e clique em **OK**
Neste ponto, você deve ver uma tela semelhante a esta.
Digite o seguinte no prompt do Dos
□□**Nbtstat - um endereço IP**
Por exemplo: nbtstat –A 207.175.1.1
(Observe que você deve digitar A em letras maiúsculas.)

Página 11

9
Isso lhe dará uma leitura parecida com esta
Tabela de nomes de máquinas remotas NetBIOS

_____
Nome
Status do tipo

J-1
<00> ÚNICO registrado
TRABALHAR
<00> GRUPO

Registrado
J-1
<03> Registrado UNIQUE
J-1
<20> Registrado UNIQUE
TRABALHAR
<1E> GRUPO registrado
TRABALHAR
<1D> ÚNICO registrado
__MSBROWSE__. <01> GRUPO registrado
(Mais uma vez, as informações foram omitidas por motivos de privacidade)
Os números entre <> são valores de código hexadecimal. O que somos
interessado em é o número "Código Hex" de <20>. Se você não
veja um código hexadecimal de <20> na lista, isso é uma coisa boa. Se você fizer
tem um código hexadecimal <20>, então você pode estar preocupado.
Agora você provavelmente está confuso sobre isso, então vou explicar.
Um código hexadecimal <20> significa que você possui compartilhamento de arquivos e impressoras
ligadas. É assim que um "hacker" verificaria se você
ter o "compartilhamento de arquivo e impressora" ativado. Se ele / ela se torna
ciente do fato de que você tem "compartilhamento de arquivos e impressoras"
ligado, então eles continuariam a tentar obter acesso a
Seu sistema.
**(Observação: para sair da janela do prompt do DOS, digite Exit
e pressione Enter)**

10
Vou mostrar agora como essa informação pode ser usada para obter
acesso ao seu sistema.
Um potencial hacker faria uma varredura em um intervalo de endereços IP para
sistemas com "Compartilhamento de arquivos e impressoras" ativado. Uma vez que eles
encontraram um sistema com compartilhamento ativado na próxima etapa
seria descobrir o que está sendo compartilhado.
É assim:
Visualização da rede \\ <insira ip_address aqui>
Nosso hacker em potencial obteria uma resposta que pareceria
algo assim.
Recursos compartilhados em \\ ip_address
Sharename
Comentário de tipo
MEUS DOCUMENTOS
Disco
TEMP
Disco
O comando foi concluído com sucesso.
Isso mostra ao hacker que sua vítima em potencial tem seu
Pasta de documentos compartilhada e seu diretório temporário compartilhado. Para
o hacker para, então, obter acesso a essas pastas, seu próximo comando
vai ser.

Net use x: \\ <insira o endereço IP aqui> \ temp
Se tudo correr bem para o hacker, ele receberá uma resposta de
(O comando foi concluído com sucesso.)
Neste ponto, o hacker agora tem acesso ao diretório TEMP do
sua vítima.
P. O tempo aproximado que o hacker médio leva para fazer
este ataque?
R.
15 segundos ou menos.

Página 13

11
Não dá muito tempo para acessar sua máquina, não é? Quantos
de vocês tinha o "Compartilhamento de arquivos e impressoras" ativado?
Senhoras e senhores: Isso é chamado de ataque Netbios. Se você é
executando uma rede doméstica, então as chances são de você ter arquivo e
compartilhamento de impressora ativado. Este pode não ser o caso de todos vocês
mas tenho certeza de que muitos de vocês provavelmente o fazem. Se
você está compartilhando recursos, por favor, proteja com senha o
diretórios.
Qualquer diretório compartilhado que você tem em seu sistema dentro de seu
rede terá uma mão segurando a pasta. Que parece
isto.
Você pode verificar quais pastas são compartilhadas pelo Windows
Explorador.
□□Clique em Iniciar
□□Role para cima para programas
Neste ponto, você verá uma lista de todos os diferentes programas em
Seu sistema
Encontre o Windows Explorer e procure por pastas que se pareçam com o
imagem acima.
Depois de encontrar essas pastas, proteja-as com senha. Não
se preocupe, vou lhe mostrar como fazer isso no Capítulo 8 em um
formato de instrução visual passo a passo.

Página 14

12
Netbios é uma das formas mais antigas de ataques ao sistema que ocorrem. Isto
geralmente é esquecido porque a maioria dos sistemas são protegidos
contra isso. Recentemente, houve um aumento de Netbios
Ataques.
Mais adiante neste manual, cobriremos algumas medidas de prevenção
métodos. Por enquanto, desejo apenas mostrar a você o potencial de segurança
imperfeições.

Página 15

13
O "CAVALO" DE TROJAN
Achei necessário dedicar um capítulo aos cavalos de Tróia. Trojan's são

provavelmente o mais comprometedor de todos os tipos de ataques. Trojans estão sendo lançados às centenas todas as semanas, cada vez mais habilmente projetado que o outro. Todos nós conhecemos a história do Cavalo de Tróia provavelmente o maior movimento estratégico já feito.
Em meus estudos, descobri que os cavalos de Tróia são os principais responsáveis para quase todas as máquinas baseadas no Windows sendo comprometidas.
Para aqueles de vocês que não sabem o que são Trojans, irei brevemente explique. Trojans são pequenos programas que efetivamente fornecem Controle remoto de "hackers" sobre todo o seu computador.

Capítulo

Alguns recursos comuns com cavalos de Tróia são os seguintes:

□□Abra sua unidade de CD-Rom

□ Φα| α□uma captura de tela do seu computador

□□Grave seus pressionamentos de tecla e envie-os para o "Hacker"

□□Acesso total a todas as suas unidades e arquivos

□□Capacidade de usar seu computador como uma ponte para fazer outras atividades relacionadas a hackers.

□□Desative o seu teclado

□□Desative o mouse ... e muito mais!

Vamos examinar mais de perto alguns dos mais populares Trojans:

□□Netbus

□□SubSeven

O Netbus Trojan tem duas partes, como quase todos os Trojans. Existe um cliente e um servidor. O servidor é o arquivo que teria que ser instalado em seu sistema para ter seu sistema comprometido. Veja como o hack seria.

O hack

Objetivo: fazer com que a vítima potencial instale o servidor em seu sistema.

Método 1

Envie o arquivo do servidor (para fins de explicação, chamaremos o arquivo netbusserver.exe) para você via e-mail. Era assim que era feito originalmente.

O hacker alegaria que o arquivo era algum tipo de jogo.
Quando você clica duas vezes no arquivo, o resultado não é nada.
Você não vê nada. **(Muito suspeito)**
Nota: (Quantas vezes você clicou duas vezes em um arquivo que alguém lhe enviou e aparentemente enviou nada)
Neste ponto, o que aconteceu é que o servidor agora foi instalado em seu sistema. Tudo o que o "hacker" precisa fazer é usar o Cliente Netbus para conectar ao seu sistema e tudo que você tem em seu sistema agora está acessível para este “hacker”.

16
Com o aumento da conscientização sobre o uso de Trojans, “hackers” tornou-se mais inteligente, daí o método 2.
Método 2
Objetivo: fazer com que você instale o servidor em seu sistema.
Vamos ver, quantos de vocês recebem jogos de amigos?
Jogos como acertar um portão na cara com uma torta. Talvez o jogo atirar em Saddam? Existem muitos arquivos pequenos engraçados como esse.
Agora vou mostrar como alguém pretende obter acesso a seu computador pode usar isso contra você.
Existem programas utilitários disponíveis que podem combinar o (“Servidor” (também conhecido como Trojan)) arquivo com um “executável” legítimo Arquivo." (Um arquivo executável é qualquer arquivo terminado em .exe). Será em seguida, produza outro arquivo (.exe) de algum tipo. Pense nisso processo como misturar veneno em uma bebida.
Por exemplo:
Suco de tomate + veneno = algo
Agora, o resultado não é mais o suco de tomate, mas você pode chame do que você quiser. O mesmo procedimento vale para combinando o Trojan com outro arquivo.
Por exemplo:
O “Hacker” em questão faria o seguinte: (para demonstração para fins, usaremos um jogo de xadrez)
Nome: chess.exe (nome do arquivo que inicia o xadrez jogos)
Trojan: netbusserver.exe (o Trojan)
(Novamente, para fins de explicação, vamos chamá-lo assim)

17
O utilitário joiner combinará os dois arquivos e produzirá 1 arquivo executável chamado:
<insira o nome aqui> .exe
Esse arquivo pode então ser renomeado de volta para chess.exe. Não é exatamente o mesmo jogo de xadrez. É como o suco de tomate, é apenas ligeiramente diferente.
A diferença nesses arquivos será notada em seu tamanho.
O arquivo original:

tamanho do chess.exe: 50.000 bytes
O novo arquivo (com Trojan): tamanho chess.exe: 65.000 bytes
(Nota: Esses números e figuras são apenas para explicação
apenas para fins)
O processo de juntar os dois arquivos leva cerca de 10 segundos para
seja feito. Agora o "hacker" tem um novo arquivo de xadrez para enviar
com o Trojan nele.
P. O que acontece quando você clica no novo arquivo chess.exe?
Resposta: O programa de xadrez começa normalmente. Não mais
suspeita porque o arquivo fez alguma coisa. A única diferença
enquanto o programa de xadrez é iniciado, o Trojan também é instalado
em seu sistema.
Agora você recebe um e-mail com o anexo, exceto no
formato de chess.exe.
O desavisado executará o arquivo e verá um jogo de xadrez.
Enquanto isso, em segundo plano, o "Trojan" fica silenciosamente
instalado no seu computador.

Se isso não for assustador o suficiente, depois que o Trojan se instalar em
seu computador, ele enviará uma mensagem de seu
computador para o hacker, informando-lhe as seguintes informações.
Nome de usuário: (um nome pelo qual o chamam)
Endereço IP: (Seu endereço IP)
Online: (sua vítima está online)
Portanto, não importa se você está em discagem. O potencial
o hacker será notificado automaticamente quando você fizer logon no seu
computador.
Você provavelmente está se perguntando "qual é a probabilidade de isso ter
aconteceu comigo?" Bem, pense sobre isso. Levar em
considere o segundo capítulo deste manual. Usado em
conjunção com os métodos mencionados acima pode fazer para
uma combinação mortal.
Esses métodos são apenas algumas maneiras que os "hackers" podem
obtenha acesso à sua máquina.
Listadas abaixo estão algumas outras maneiras pelas quais eles podem infectar
arquivo para você.
Grupos de notícias:
Ao postar artigos em grupos de notícias com anexos de arquivo como
(mypic.exe) em grupos de notícias adultos é quase garantido que
ter alguém sendo vítima.
Não se deixe enganar, pois essas pessoas irão postar esses arquivos em
quaisquer grupos de notícias.
Boatos:
Infelizmente, não há como controlar esse efeito. Vocês
receber o arquivo de um amigo que o recebeu de um amigo etc.
etc.

19

O email:

O método de entrega mais amplamente utilizado. Pode ser enviado como um anexo em um e-mail endereçado a você.

Sites inseguros:

Sites que não estão “acima da mesa”, por assim dizer. arquivos baixado de tais lugares deve sempre ser aceito com alta suspeita.

IRC:

Em servidores IRC, às vezes, quando você entra em um canal, você receber automaticamente um arquivo como “mypic.exe” ou “sexy.exe” ou sexy.jpg.vbs algo nesse sentido. Normalmente você encontrará os aspirantes são os culpados por isso.

Sites de bate-papo:

Os sites de bate-papo são provavelmente um dos principais lugares onde esse tipo de de atividade ocorre. A parte triste disso é que 80% não são ciente disso.

Como você pode ver, existem muitas maneiras diferentes de entregar isso arquivo para você como um usuário. Ao informá-lo desses métodos, eu espero ter deixado você mais ciente dos perigos potenciais em torno de você. No Capítulo 3, discutiremos quais arquivos devem ser considerado aceitável.

20

ARQUIVOS ACEITÁVEIS

Do último capítulo, você provavelmente está se perguntando o que exatamente é seguro aceitar como arquivo de qualquer pessoa. Espero que eu responda à maioria, senão a todas as suas perguntas sobre quais tipos de arquivos pode ser considerado seguro ou mais normal.

Vou mostrar o que as extensões normais devem ser para diferentes tipos de arquivos e que tipo de arquivo nunca deve vir em formatos .exe.

Começaremos com algo que tenho certeza de que a maioria, senão todas as pessoas já tiveram acontecer com eles pelo menos uma vez.

AS FOTOS

Alguém já mandou uma foto sua para você? Se você ficar em um site de bate-papo de qualquer tipo, então as chances são você conheceu alguém ou um grupo de pessoas que talvez tenham queria enviar a foto deles. Se eles fizeram, então espero que não estava na forma de **(mypic.exe)** . Se fosse você pode querer para executar uma verificação de vírus nesses arquivos em particular.

Capítulo

21

Para todos os propósitos intensivos, as imagens devem realmente vir apenas no formatos listados abaixo.

□□Jpg (jpeg)
Por exemplo (steve.jpg)
□□Bmp (bitmap) Por exemplo (steve.bmp)
□□TIFF
(Marcação
Imagem
Arquivo
Formato)
Por exemplo (steve.tiff)
□□Gif
(Gráficos
Intercâmbio
Formato)
Por exemplo (steve.gif)

Tudo isso é legítimo!

Seu navegador pode visualizar quase todos esses arquivos, exceto o tiff formato. Outros programas que podem ser usados para visualizar esses arquivos são Photoshop, Paintshop, Netscape, Internet Explorer e Imaging apenas para citar alguns.

AVISO!

Esses são os tipos de arquivo pelos quais as imagens devem vir. Qualquer outra coisa deve ser inaceitável. não há razão para ter uma imagem de qualquer tipo em um arquivo .exe. Nunca aceite a desculpa de que é um arquivo de imagem de extração automática!

LEIA-ME E ARQUIVOS DE TEXTO

Quase todos os documentos de informações do programa na rede vêm em um desses formatos. Esses arquivos são simplesmente informações documentos digitados em algum programa de processamento de texto ou texto editor.

22

Alguns exemplos de suas extensões são:

□□DOC
Formato de documento para Microsoft Word, Word.
Exemplo: (readme.doc)

□□TXT
O arquivo de formato de texto pode ser aberto por Notepad, Word,
Microsoft
Palavra.
Exemplo: (readme.txt)
□□RTF
(Formato de texto rico)
Todos esses são formatos legítimos aceitáveis. A verdade é que um
os arquivos de texto podem vir em quase todos os formatos. No entanto existem
formatos que eles realmente nunca deveriam usar.
Por exemplo:
□□<qualquercoisa> .com
□□<qualquer coisa> .exe
□□<qualquercoisa> .txt.vbs
Não há razão para que nenhum arquivo seja enviado a você em qualquer um dos
formatos acima se forem documentos de texto. Eu também posso te assegurar
não há razão para que um arquivo tenha uma extensão dupla. Tal
arquivos, caso você venha a recebê-los, devem ser tratados com
suspeita.
**De forma alguma você deve abrir um arquivo se você não
saber que tipo de arquivo é.**

Se você não tiver certeza sobre o tipo de arquivo, aqui é um método por
que você pode verificar. Vá para o seu mecanismo de pesquisa favorito para
exemplo:
Altavista: http://www.altavista.com
Ou
Metacrawler: http://www.metacrawler.com
□□Clique no campo de pesquisa
(Em seguida, digite o tipo de arquivo sobre o qual está perguntando, por exemplo)
□□Tipo de arquivo Doc
□□Tipo de arquivo Exe
□□Tipo de arquivo Rtf
Isso exibirá sites que darão uma explicação mais detalhada sobre
exatamente que tipo de arquivo é.
Você pode usar as informações acima para entender melhor o que
tipo de arquivos que você recebe de indivíduos. Sem arriscar
instalar qualquer coisa em sua máquina.
Abordamos métodos pelos quais seu computador pode ser acessado
por um Ataque Netbios, como os arquivos podem ser infectados e como eles podem
ser entregue. No Capítulo 4, discutiremos quem é responsável por
esses ataques. Veremos o tipo de indivíduos por trás do
teclado responsável por esses ataques.

Acho necessário esclarecer o termo hacker. Talvez o seu
a definição de um hacker foi influenciada e contaminada pelo
anos. Tem havido várias atividades relacionadas ao computador
atribuídos ao termo “hacker”, mas foram muito mal interpretados.
Infelizmente para as pessoas que são verdadeiramente definidas dentro do
mundo da tecnologia underground como um “hacker”, isso é um insulto para eles.
Existem vários tipos de “hackers”, cada um com o seu
agenda. Meu objetivo é ajudar a protegê-lo do pior deles.

Hackers anarquistas

Estas são as pessoas de quem você deveria estar cansado. O único deles
a intenção de infiltração no sistema é causar danos ou usar
informações para criar confusão. Eles são principalmente os indivíduos
que são responsáveis pela maioria dos ataques ao sistema contra
usuários domésticos. Eles são mais propensos a se interessar pelo que está
máquina de outra pessoa, por exemplo a sua.
Geralmente, você descobrirá que esses indivíduos têm um pouco acima
nível de habilidade do computador e se consideram hackers. Elas
glorificar-se nas realizações dos outros. Ideia deles

Capítulo

de se classificar como um hacker é o de adquirir programas
e utilitários disponíveis na rede, use esses programas com
nenhum conhecimento real de como esses aplicativos funcionam e se eles
conseguem "invadir" a classe do sistema de alguém como um
hacker. Esses indivíduos são chamados de “Kiddie Hackers”.
Eles usam esses programas fornecidos a eles de forma maliciosa em
qualquer um que eles possam infectar. Eles não têm um propósito real para o que eles
estão fazendo, exceto o fato de dizer “Sim! Eu invadi <inserir
nome aqui> computador! ” Isso lhes dá o direito de se gabar de seus
amigos.
Se houver qualquer dano a ocorrer em um sistema sendo invadido
esses indivíduos irão realizá-lo.
Esses indivíduos geralmente são alunos do ensino médio. Eles se gabam
sobre suas realizações para seus amigos e tentar construir um
imagem de ser hackers.

Hackers

Um hacker, por definição, acredita no acesso a informações gratuitas.
Geralmente são pessoas muito inteligentes que pouco se importam
sobre o que você tem em seu sistema. A emoção deles vem de

infiltração de sistema por motivos de informação. Hackers ao contrário
“Crackers e anarquistas” sabem ser capazes de quebrar o sistema
a segurança não faz de você um hacker mais do que adicionar 2 + 2
faz de você um matemático. Infelizmente, muitos jornalistas
e os escritores foram enganados ao usar a palavra 'hacker ”. Elas
atribuíram quaisquer atividades ilegais relacionadas ao computador ao termo
“Hacker.”
Hackers reais visam principalmente instituições governamentais. Eles acreditam
informações importantes podem ser encontradas no governo
instituições. Para eles, o risco vale a pena. Quanto maior a segurança
melhor será o desafio. Quanto melhor o desafio, melhor eles
precisa ser. Quem é o melhor cowboy do teclado? Por assim dizer!
Esses indivíduos vêm em uma variedade de classes de idade. Eles variam
de alunos do ensino médio a graduados universitários. São bastante

---

adeptos da programação e inteligentes o suficiente para ficar de fora do
Holofote.
Eles não se importam particularmente em se gabar de seus
realizações, pois os expõe à suspeita. Eles preferem
trabalhar nos bastidores e preservar seu anonimato.
Nem todos os hackers são solitários, muitas vezes você descobrirá que eles têm uma
círculo de associados, mas ainda há um nível de anonimato entre
eles. Um colega meu uma vez me disse "se eles disserem que são
um hacker, então eles não são! ”

Biscoitos

Para fins de definição, incluí este termo. Isto é
principalmente o termo dado a indivíduos versados na técnica
de contornar a proteção de direitos autorais de software. Geralmente são
altamente qualificado em linguagens de programação.
Eles costumam ser confundidos com Hackers. Como você pode ver, eles são
semelhantes em sua agenda. Ambos lutam contra a segurança de algum tipo,
mas eles são "animais" completamente diferentes.
Ser capaz de atribuir seus ataques ao tipo certo de atacante é
muito importante. Identificando seu invasor como um
Hacker Anarquista ou Hacker você tem uma ideia melhor do que você é
contra.
“Conheça o seu inimigo e conheça a si mesmo e você sempre será
vitorioso..."

FERRAMENTAS DO COMÉRCIO

O que é um carpinteiro sem martelo? “Hackers” requerem ferramentas
a fim de tentar comprometer a segurança de um sistema. Algum
ferramentas estão prontamente disponíveis e algumas são escritas por outros
hackers, com a única intenção de serem usados para invasões de sistema.
Alguns “hackers usam um pouco de engenhosidade com seus ataques e não

dependem necessariamente de qualquer ferramenta específica. No final, porém, resume-se a que eles precisam infectar seu sistema, a fim de comprometê-lo.
Para entender melhor os meios pelos quais os "hackers" se comprometem segurança do sistema, acho importante entender quais ferramentas eles usar. Isso lhe dará uma visão do usuário sobre o que exatamente eles procuram e como obtêm esta informação. Nesta seção, eu também explica como essas ferramentas são usadas em conjunto com cada de outros.

Capítulo

28

Scanners de porta

O que é um scanner de porta?
Um scanner de porta é uma ferramenta útil que verifica um computador procurando para portas ativas. Com este utilitário, um potencial “hacker” pode descobrir quais serviços estão disponíveis em um computador de destino das respostas que o scanner de porta recebe. Dê uma olhada em a lista abaixo para referência.
Iniciando a varredura.
Host de destino: www.suaempresa.com
TCP
Porta
: 7
(eco)
TCP
Porta
: 9
(descartar)
TCP
Porta
: 13
(dia)
TCP
Porta
: 19
(chargen)
TCP
Porta
: 21

(ftp)
TCP
Porta
: 23
(telnet)
TCP
Porta
: 25
(smtp)
TCP
Porta
: 37
(Tempo)
TCP
Porta
: 53
(domínio)
TCP
Porta
: 79
(dedo)
TCP
Porta
: 80
(www)
TCP
Porta
: 110
(pop)
TCP
Porta
: 111
(sunrpc)
Finalizado.
A varredura de portas abertas é feita de duas maneiras. O primeiro é para
escaneie um único endereço IP para portas abertas. A segunda é fazer a varredura
um intervalo de endereços IP para encontrar portas abertas.
Tente pensar nisso como ligar para um único número de telefone de
diga 555-4321 e pergunte por cada ramal disponível. No
em relação à digitalização, o número de telefone é equivalente ao IP
endereço e as extensões para abrir portas.

29
Verificar um intervalo de endereços IP é como ligar para todos os números
entre 555-0000 a 555-9999 e pedindo a cada
ramal disponível em todos os números.
P. Qual é a aparência de um scanner de porta?

Trojans

Os Trojans são definitivamente uma das ferramentas que os “hackers” usam.

Existem centenas de Trojans. Listá-los todos faria
este manual é extremamente longo. Para fins de definição, vamos nos concentrar
em um casal.

Sub Seven

O cavalo de Troia Sub Seven possui muitos recursos e capacidades. Isto
é, na minha opinião, de longe, o Trojan mais avançado que já vi.
Dê uma olhada em alguns dos recursos do Sub Seven.

□□livro de endereços
□□WWP Pager Retriever
□□UIN2IP
□□scanner de IP remoto
□□pesquisa de host
□□obter a chave do CD do Windows
□□atualizar a vítima a partir do URL
□□Aquisição do ICQ
□□pasta raiz do FTP
□□recuperar senhas dial-up junto com números de telefone
e nomes de usuário
□□redirecionamento de porta
□□IRC bot. para uma lista de comandos
□□Marcadores do gerenciador de arquivos
□□criar pasta, excluir pasta [vazia ou cheia]
□□gerente de processo
□□texto 2 discurso
□□Reinicie o servidor
□□Aol Instant Messenger Spy
□□Yahoo Messenger Spy
□□Microsoft Messenger Spy
□□Recuperar lista de uins e senhas de ICQ
□□Recuperar lista de usuários e senhas do AIM
□□Redirecionamento de aplicativo
□□Editar arquivo
□□Execute cliques na área de trabalho da vítima
□□Definir / alterar as configurações do protetor de tela [Scrolling Marquee]
□□Reinicie o Windows [veja abaixo]
□□Servidor de ping
□□Compactar / descompactar arquivos antes e depois das transferências
□□The Matrix
□□Scanner Ultra Fast IP
□□Ferramenta IP [Resolve nomes de host / endereços IP de ping]

Contínuo…

□□Obtenha as informações da casa da vítima [não é possível em todos os servidores]:

- Endereço
- Nome do negócio
- Cidade
- Empresa
- País
- Tipo de Cliente
- O email
- Nome real
- Estado
- Código da cidade
- Código do país
- Telefone Local
- Código postal

E mais…
Acho que você entendeu exatamente o que esse cavalo de Tróia
é capaz de. Aqui está uma foto da aparência do SubSeven
gostar.

32

Netbus:

O NetBus é um Trojan mais antigo, mas ainda assim é usado.
Consiste em um servidor e uma parte cliente. O servidor-
parte é o programa que deve estar rodando em seu
computador. Isso deve dar uma ideia do que é Netbus
capaz de.
Recursos do Netbus:

□□Abra / feche o CD-ROM uma vez ou em intervalos (especificado em
segundos).

□□Mostrar imagem opcional. Se nenhum caminho completo da imagem for fornecido,
irá procurá-lo no diretório Patch. A imagem suportada-
formatos são BMP e JPG .

□□Trocar botões do mouse - o botão direito do mouse fica com o esquerdo
funções do botão do mouse e vice-versa.

□□Inicie o aplicativo opcional.

□□Jogue arquivo de som opcional. Se nenhum caminho completo do arquivo de som for
dado, ele irá procurá-lo no diretório Patch. O apoiado
o formato de som é WAV .

□□Aponte o mouse para coordenadas opcionais. Você também pode
navegue com o mouse no computador de destino com o seu próprio.

□□Mostrar uma caixa de diálogo de mensagem na tela. A resposta é sempre
enviado de volta para você.

□□Desligue o sistema, faça logoff do usuário, etc.

□□Vá para um URL opcional no navegador da web padrão.

□□Enviar pressionamentos de tecla para o aplicativo ativo no alvo
computador. O texto no campo "Mensagem / texto" será
inserido no aplicativo que tem o foco. (”|” Representa
digitar).

□□Ouça os pressionamentos de tecla e envie-os de volta para você.

□□Obtenha um screendump (não deve ser usado muito lentamente
conexões).
□□Retorne informações sobre o computador de destino.
□□Carregue qualquer arquivo seu para o computador de destino. Com isso
recurso, será possível atualizar remotamente Patch com um
nova versão.

Página 35

33
□□Aumente e diminua o volume do som.
□□Grave sons captados pelo microfone. O som é enviado
de volta para você.
□□Faça sons de clique sempre que uma tecla for pressionada.
□□Baixe e exclua qualquer arquivo do destino. Vocês
escolha o arquivo que deseja baixar / excluir em uma visualização que
representa os discos rígidos no destino.
□ Aσ□teclas (letras) do teclado podem ser desativadas.
□□Gerenciamento de proteção por senha.
□□Mostrar, eliminar e focalizar janelas no sistema.
□□Redirecionar dados em uma porta TCP especificada para outro host e
porta.
□□Redirecionar E / S de aplicativos de console para uma porta TCP especificada
(telnet o host na porta especificada para interagir com o
aplicativo).
□□Configure o exe do servidor com opções como porta TCP e e-mail
notificação.
É assim que o cliente Netbus se parece.

Página 36

34
Marceneiros
Anteriormente, você me viu fazer referências a utilitários que
combine dois arquivos executáveis em um. Isso é o que estes
programas são. Esses programas tornam possível ocultar o
Trojans em arquivos legítimos.
ICQ
Embora não seja um utilitário para hackear, existem
arquivos de programa escritos por programadores não nomeados para ele.
Quanto mais Trojans avançados têm a capacidade de notificar o
“Hacker” via ICQ se você está online ou não. Dado
que você está infectado com um Trojan.
Se você não estiver infectado, o ICQ pode servir como um utilitário para
forneça seu endereço IP. Atualmente existem
arquivos / programas disponíveis na rede que permitem que você
“Corrigir” o ICQ para que revele os números de IP de qualquer pessoa no
Lista de “hackers”. Também existem arquivos que permitem adicionar usuários
no ICQ sem sua autorização ou notificação.

Página 37

35
Para fins de demonstração, vamos ver como seria um hack
se um hacker com os utilitários mencionados acima fosse para
tentativa de hackear a máquina de um usuário.
Hack 1:
Objetivo: Obter acesso à máquina do usuário.
Passo 1: Obtenha o ICQ # do usuário
Passo 2: Adicionar usuário à lista ICQ
Etapa 3: usar obter informações sobre o usuário
Passo 4: Registre o endereço IP do usuário
Etapa 5: iniciar um prompt do DOS
Etapa 6: nbtstat –A <endereço IP>
Etapa 7: procure o código hexadecimal <20>
Etapa 8: (assumindo que existe um hexágono de <20>) visão da rede
\\endereço de IP.
Passo 9: Veja quais compartilhamentos estão disponíveis, diremos que "C" está sendo
compartilhado.
Etapa 10: net use x: \\ ip_address \ c
O acesso à máquina do usuário foi alcançado.
No cenário acima, nosso “hacker em potencial” usou o patch
programas disponíveis para o ICQ obter o endereço IP do
“Vítima” e então lançar seu ataque.
Com a compreensão de como um "indivíduo" pode obter acesso
para sua máquina, vamos passar para o Capítulo 6. Vamos
discuta o que está em risco depois que seu computador estiver
comprometido.

36
ACESSO CONCEDIDO
Muitas vezes eu ouço comentários como "e daí se eles invadirem meu
sistema não há nada no meu sistema de interesse. ” Eu não posso te dizer
quão mais errado você pode estar. A única coisa que posso pensar quando
Eu ouço alguém dizer que essa pessoa não está ciente do que
tipo de informação a que têm acesso.
Vou mostrar exatamente que tipo de informação um “hacker” tem
acesso a uma vez que seu sistema foi invadido. Tente
lembre-se de que não é para assustar você, é para informar
tu. Lembre-se de que você está lendo este manual para obter uma melhor
compreensão de como se proteger.
Capítulo

37

Informações de conta bancária

Tenho certeza que se você for como a maioria das pessoas, você tem banco na web de alguns
Gentil. Provavelmente, você paga suas contas online através do site do seu banco.
A maioria dos bancos exige que você use navegadores de criptografia de 128 bits para fazer
seu banco online. Esta forma de banco on-line criptografa
suas informações e protegê-las de olhares indiscretos dos
mundo que deseja obter acesso a essas informações vitais.
Isso deve ilustrar ainda mais o quão poderoso é o método de criptografia é:

□□criptografia de 40 bits, significa que há **2^{40} chaves possíveis** que pode caber no **cadeado** que mantém sua conta em formação. Isso significa que há muitos bilhões (a 1 seguido por 12 zeros) de chaves possíveis.

□□criptografia de 128 bits, significa que há **2^{88}** (um três seguido por 26 zeros) vezes mais combinações de teclas do que há para criptografia de 40 bits. Isso significa um computador exigiria exponencialmente mais processamento poder do que para a criptografia de 40 bits para encontrar a chave correta.

Esse é um método muito poderoso de criptografar dados enviados de seu máquina para a máquina de bancos. Infelizmente é inútil para você uma vez que seu computador foi comprometido.

Pergunta: como?

Uma das características de um “Trojan” é um key logger. O princípio por trás disso, todas as teclas pressionadas serão gravadas e enviadas de volta ao “hacker”.

Que tipo de informação você insere quando faz transações bancárias conectados?

A maioria dos bancos tem algum tipo de tela de login, onde você digita seu nome de usuário e senha. É aqui que fica interessante.

Isso significa que, uma vez que você digite seu login e senha para o seu conta bancária online o “hacker” agora tem acesso a ela.

38

Você provavelmente está se perguntando bem "Como eles sabem o que banco em que estou? "

Essas informações são facilmente obtidas fazendo o que é chamado de captura de tela. Isso dá ao “hacker” uma imagem de sua área de trabalho e todas as janelas abertas no momento. A captura de tela ficaria assim.

A partir dessa captura de tela, eles podem dizer em qual site você está (em qual caso seja o seu banco). A partir daí é só uma questão de entrando em sua conta bancária e fazendo o que quiserem.

Como você pode ver, embora esteja em um site seguro, ele ainda não protege suas informações, uma vez que seu computador está comprometido.

Talvez existam alguns de vocês que não usam serviços bancários online. Talvez você use outro programa para gerenciar suas finanças. Há uma variedade de programas disponíveis para fins financeiros finalidades.

O problema é que, uma vez que um "hacker" tenha acesso ao seu sistema, ele tem acesso a esses arquivos. Eles podem copiar os arquivos de seu computador para o deles e navegue por eles em seu lazer.

O email

Basta colocar todos os e-mails enviados para você estão acessíveis a um “hacker” uma vez que seu sistema foi comprometido. Eles podem lê-los e possivelmente verifique seu e-mail antes de fazer isso.

Fotos

Se você tem fotos suas ou de membros da família em seu sistema, eles também estão disponíveis para o "hacker". Eu não acho que eu precisa explicar o perigo aqui. Não apenas o indivíduo comprometeu o seu sistema de computador, eles também sabem o que você parece.

Retomar

Isso pode não soar como um arquivo prioritário para um "hacker", mas fique com mim por um segundo. Quantos de vocês têm currículos digitados em seus computadores? Tenho certeza que muitos de vocês fazem. Se um “hacker” fosse baixe seu currículo agora eles têm acesso a:

Nome:
Endereço:
Telefone:
Local de trabalho:

Adicione a isso o que está acima e vamos dar uma olhada no que eles sabem.

□□Endereço de e-mail de amigos, familiares, associados.
□□Seu endereço residencial.
□□Número de telefone
□□Qual a sua aparência
□□Onde você trabalha (e trabalhou)
□□Conta bancária (incluindo quanto dinheiro você tem)

Ele não para por aí também. Essas são apenas algumas das coisas

isso pode acontecer quando seu sistema está comprometido. Este não é ficção científica - essas são possibilidades da vida real. A extensão disso as informações foram coletadas apenas de arquivos em seu sistema. Leva em consideração o seguinte.

SURVELLANCE VIA CONEXÃO DE INTERNET

Não se engane, isso é muito real. Dependendo de quanto você ler e quanto você sabe sobre Trojans você provavelmente é ciente do que estou falando.

Se você não está ciente, estou me referindo à capacidade de efetivamente transformar seu computador em um survellance de áudio / vídeo unidade sem você saber.

Pergunta: como?

Resposta: Quantos de vocês têm webcams? Quantos de voce tem microfones?

Nem todos os cavalos de Tróia têm a capacidade de acessar sua webcam e Microfone. Aqueles que o fazem, têm a capacidade de transformar seu computador em uma câmera de vídeo / áudio survellance.

O Trojan grava os sons em uma sala através do seu microfone e então envia o arquivo de volta para o "hacker". O hacker então reproduz o arquivo e pode ouvir qualquer som gravado no sala. Adicione a isso, uma vez que a gravação é um arquivo, eles podem reproduzi-lo voltar sempre que quiserem para quem eles quiserem.

Pelo mesmo método, eles acessam sua webcam de forma eficaz obter um feed de vídeo e áudio de sua casa do que é atualmente acontecendo naquela sala.

Parece loucura, mas posso garantir que não é. Eu não acho que eu preciso dizer que tipo de risco à segurança isso representa para você e sua família.

41

Agora você provavelmente está preocupado / com medo do possível vulnerabilidades do seu computador. Não sinta. No Capítulo 7, iremos discuta métodos para se proteger desses indivíduos.

42

COMO SE PROTEGER

Há um ditado que diz "É melhor prevenir do que remediar".

Depois de ler este manual, espero que você esteja procurando maneiras de proteja sua privacidade. Retire-o de quem pode invadir.

Os indivíduos responsáveis por esses ataques sempre serão presa daqueles que não têm interesse em defender seus privacidade.

"Dê um peixe a um homem e ele comerá durante o dia. Ensine um homem como pescar e ele nunca morrerá de fome. "

Ao mostrar as etapas e procedimentos que você pode usar para proteger seu sistema seja hackeado, você rapidamente recuperará o seu sentido de segurança.

Capítulo

43

FIREWALLS

Um firewall em termos leigos é essencialmente um programa que filtra dados da rede para decidir se deve ou não encaminhá-los para seus destino ou negá-lo.

Esses programas geralmente protegem você da rede de entrada ataques. ” Isso significa solicitação de rede não autorizada de estrangeiros os computadores serão bloqueados.

Eu não posso enfatizar o quão importante é nos dias de hoje ter um firewall de algum tipo instalado e “rodando” em seu computador.

Eu pessoalmente recomendo que você use um dos seguintes ou ambos se você puder.

Black Ice Defender

Este é um programa de firewall abrangente e muito amigável. eu altamente recomendável para usuários avançados e novatos. Tem um interface gráfica simples que é fácil de entender e agradável para o olho.

Ele detecta o seu invasor, interrompe o ataque e / ou analisa e dá você o máximo de informações disponíveis sobre o “atacante”.

Você pode baixar Black Ice Defender em:

http://www.networkice.com

44

Lockdown 2000

Também recomendo o Lockdown 2000 como medida de segurança. Lockdown2000 tem uma interface gráfica muito boa e é amigo do usuário. Ele faz a mesma coisa que o Black Ice Defender, mas também executa verificações em seu sistema em busca de cavalos de Tróia. Ele monitora o seu arquivos de registro e de sistema para as alterações que ocorrem. Então dá a você a opção de desfazer todas as alterações ou de permitir.

Você pode obter uma cópia do Lockdown2000 em:

http://www.lockdown2000.com

Acho que usar os dois firewalls em conjunto funciona muito bem. Como ambos compensam as deficiências do de outros.

Software antivírus
Este também é outro software que você deve por todos os meios
tem em seu sistema. Todos nós sabemos que é uma necessidade, mas nós
são todos culpados de não usá-los.
Existem vários softwares antivírus por aí. Norton
Antivírus e Mcafee são dois dos mais comuns. Elas
são todos bons e fazem o seu trabalho.
Você pode encontrar cada um desses programas em:
http://www.norton.com
http://www.mcafee.com

45
Eu pessoalmente recomendo usar 1 antivírus e ambos os firewalls.
O motivo é que eu acho que o Black Ice Defender bloqueia os ataques de entrada
e quaisquer alterações de sistema que ocorram em seu sistema Lockdown
capturas.
DICAS E TRUQUES
Eu sinto que é necessário que você preste atenção especial a este
seção. Os programas acima funcionarão e farão seu trabalho, mas
isso é apenas metade da batalha.
Existem certas precauções que você precisa tomar como usuário para
certifique-se de que seu sistema permaneça uma "fortaleza".
Dica nº 1:
Para usuários dial-up: se você for um usuário dial-up, use um
modem interno ou externo para ficar online. Se você tem
um modem externo então essa dica é fácil. Se você olhar para o
modem você verá luzes na frente dele.
Quando você estiver fazendo qualquer coisa na rede, você notará luzes
piscando que indica que você está enviando dados e recebendo
Dados. Dependendo da frequência com que as luzes piscam e da velocidade com que
piscar dá uma ideia aproximada de quanta atividade está acontecendo entre
seu computador e a rede.
É aqui que um pouco de percepção entra em jogo. Se você é
conectados à internet e estão apenas sentados ao lado do seu sistema
fazendo absolutamente nada, essas luzes não têm que ser
piscando rapidamente. Eles piscarão periodicamente, indicando que é
verificando sua conectividade, no entanto, não deve haver dados pesados
transferência de qualquer tipo se você não estiver fazendo nada na net.
Por exemplo: Se você tem seu programa de e-mail aberto e você está
apenas sentado lendo seu e-mail, você pode notar que a cada 15
às vezes 20 minutos que as luzes piscarão para frente e para trás

---

46
indicando que está enviando e recebendo dados. Isso é normal porque
é provável que você tenha seu programa de e-mail configurado para verificar
seu e-mail a cada 20 minutos.
Se por acaso você notar que as luzes do seu modem estão piscando

consistentemente, digamos que um período de 2 minutos ininterruptos seja extremamente
suspeito.
Se você tiver um modem interno, não será capaz de ver o
luzes no seu modem, em vez disso, você pode contar com as duas tvs
ícones no canto inferior direito da tela perto do relógio.
Eles serão parecidos com isto.
Quaisquer dados sendo enviados e recebidos serão notados pelo piscar
das luzes rapidamente.
Se você estiver usando cabo ou dsl, o mesmo se aplica. Nunca deveria
ser qualquer forma de transferência de dados pesados de qualquer tipo de seu sistema
a qualquer coisa, a menos que você esteja autorizando. Alguns exemplos de
atividades que podem justificar a transferência de dados pesados são as seguintes:
□□Programas legítimos em execução que podem precisar acessar o
rede ocasionalmente. (ou seja, programas de e-mail)
□□Se você estiver executando um servidor FTP onde as pessoas propositalmente
faça login em sua máquina para baixar os arquivos que você forneceu
eles têm acesso.
□□Se você estiver baixando arquivos da Internet
Coisas dessa natureza vão gerar muita transferência de dados.

Página 49

47
Permita-me aproveitar esta oportunidade para explicar a você outra “ferramenta”
você deve estar ciente. Vamos supor que você perceba que existe um
muitos dados sendo enviados e recebidos de sua máquina e você
nem mesmo sentando nele.
Como você sabe o que está acontecendo?
Vamos fazer um pequeno exercício.
□□Clique em **Iniciar**
□□Vá para **Executar (clique em Executar)**
□□Digite **Comando**
□□Clique em **OK**
Novamente, você deve obter uma tela semelhante a esta.

Página 50

48
Depois de ter essa tela, digite o seguinte:
□□**Netstat –a**
Este comando lhe dará uma lista de todos os seus
computador está se comunicando online atualmente.
A lista que você obterá será semelhante a esta:
Conexões Ativas
Protocolo
Endereço Local Endereço Estrangeiro
Estado
TCP
COMP: 0000 10.0.0.1: 0000
ESTABELECIDO
TCP

COMP: 2020
10.0.0.5: 1010 ESTABELECIDO
TCP
COMP: 9090
10.0.0.3: 1918 ESTABELECIDO
Você verá uma variedade de listagens como a acima. Isso vai te dar o
Protocal sendo usado, o endereço local (seu computador) e o que
porta do seu computador, o "Endereço Estrangeiro" está sendo conectado
para e o (Estado) do qual o (endereço estrangeiro) é. Para
exemplo, se for (estabelecido), então isso significa qualquer que seja o
endereço estrangeiro diz que está conectado à sua máquina.
Existe software disponível que irá mostrar-lhe esta informação
sem digitar todos esses comandos.
O nome do software é Xnetstat, você pode obter um
cópia dele daqui:
http://www.arez.com/fs/xns/
Se por algum motivo você acredita que está enviando e recebendo
muitos dados, então é aconselhável fazer um netstat –a para ver o que é
conectado ao seu computador e em quais portas.

Protegendo recursos compartilhados

Para aqueles de vocês que têm redes internas entre dois
os computadores provavelmente têm algum tipo de recurso compartilhado. Mais cedo
neste manual, mostrei como encontrar o que está sendo compartilhado.
Vamos dar uma olhada em como proteger esses recursos compartilhados.

□□Clique em **Iniciar**

□□Vá até **Programas**

□□Vá para o **Windows Explorer** (clique nele)

Depois de fazer isso, você deve ver uma janela que aparece
com um monte de pastas listadas à esquerda e mais pastas listadas
à direita.
Percorra a lista e procure os arquivos compartilhados que você
tenho. Para uma atualização, a pasta terá esta aparência.

Depois de encontrar essas pastas, você deve protegê-las.

□□Clique na pasta (uma vez) para que seja destacada

□□Use o botão direito do mouse, (o mais próximo do seu dedo mínimo
dedo) e clique na pasta.
Você receberá um menu:
Seu menu pode parecer diferente do meu, mas o que você está procurando
pois é a palavra "compartilhar".

Ao clicar em Compartilhamento, você verá outra janela que parece
como o seguinte.

Página 54

52
É aqui que você pode compartilhar esta pasta ou desligá-la. Se você deseja desativar o compartilhamento que você selecionaria (Não compartilhado).

Página 55

53
Se você precisar compartilhar uma pasta, siga estas etapas. Isso vai tornar a pasta somente leitura. Isso significa que ninguém pode deletar qualquer coisa dessas pastas se elas invadirem seu sistema usando um ataque “Netbios”.

Página 56

54
A próxima etapa é proteger o diretório com senha.
Depois de digitar a senha, clique em (OK) e pronto.
Minha sugestão pessoal é definir qualquer diretório que você está compartilhando para (Somente leitura) e senha para protegê-lo. Isso é apenas se você precisar compartilhar recursos.

Página 57

55
Desativando o compartilhamento de arquivos e impressoras
Para aqueles de vocês que não têm uma rede doméstica disponível deve desativar o compartilhamento de arquivos e impressoras. Não há razão para ter este recurso está ativado. Siga as etapas a seguir para desativá-lo.
(Você precisará do CD do Windows 95/98 para isso)
□□Clique em **Iniciar**
□□Role para cima até **Configurações**
□□Clique em **Painel de Controle**
Isso o levará ao seu Painel de Controle. Você verá uma variedade de ícones, o que você está procurando será o ícone que diz (Rede) e é assim.

Página 58

56
Depois de encontrar o ícone, clique duas vezes nele. Então você vai receber uma tela parecida com esta.

Página 59

57
Para desligar o compartilhamento de arquivos e impressoras, você precisará clicar em o botão que diz (Compartilhamento de arquivos e impressoras).
Depois de clicar nele, uma caixa será aberta:

Página 60

58
Desmarque ambos e clique em ok.
Você deve clicar em (OK) novamente e isso o levará de volta ao

Painel de controle.
Neste ponto, será solicitado o seu CD do Windows. Basta inserir
e clique em OK.
Às vezes, você receberá uma mensagem que diz
"O arquivo que está sendo copiado é mais antigo que o arquivo existente ..etc.etc. Fazer
deseja manter seu arquivo existente? "
Você deve clicar em NÃO.
Quando o processo estiver completamente concluído, o seu sistema perguntará se
você deseja reiniciar. Clique em Sim. Assim que seu sistema tiver
reiniciado, você pode voltar à tela de rede e verificar
certifique-se de que o "Compartilhamento de arquivos e impressoras" esteja desativado.
Em termos de software, até este ponto, falamos sobre como
proteja seu sistema. Eu gostaria de discutir o processo envolvido para se
seu sistema está infectado.

59

OH NÃO! MEU SISTEMA ESTÁ INFECTADO

Espero que este não seja o caso da maioria de vocês, mas eu sei
algumas pessoas serão infectadas. O único
maneira que você realmente vai saber se está infectado é diagnosticar
seu computador corretamente.
Eu recomendo obter o **Lockdown 2000** para isso. Instale-o no seu
sistema e execute uma verificação completa do sistema em sua máquina. (Consulte o
documentação para Lockdown 2000)
Depois de executar o **Lockdown 2000** , execute seu antivírus apenas
no caso de **Lockdown ter** perdido alguma coisa. Você pode se perguntar por que eu
sugere tal redundância? Os computadores são construídos com base no princípio
de redundância. Um programa sempre compensará o
deficiências do outro.
Isso deve revelar a maioria, senão todos os Trojans que residem atualmente em
sua máquina. Até que você esteja absolutamente certo de não possuir
quaisquer Trojans em sua máquina, sugiro estar alerta sobre o
acontecimentos no seu computador.
1. Observe as luzes de transmissão e recepção no modem, como
nós discutimos.
2. Execute os programas de firewall que sugeri bloquear
intrusos.
3. Monitore seu sistema em busca de acontecimentos incomuns (CD Rom
abrindo sem motivo)
4. Use o comando Netstat para ver quais portas estão sendo usadas
se você ficar desconfiado.
O objetivo final é não ser paranóico sobre o uso de seu
computador. É sobre ser inteligente sobre como você usa seu
computador.

60

CADA MAIOR FLAW SISTEMAS

Para todo sistema de computador, sempre existe essa falha de sistema.

Não importa o quão poderoso seja o sistema que você tem, quantos diferentes programas de firewall que você executa ou quantos scanners de vírus você tem. No final, você é o pior inimigo de seu sistema.
Todos os “hackers” sabem disso, não se engane quanto a isso. agradecidamente poucos têm a resistência necessária para uma forma de hackear chamado de “Engenharia Social”.
Engenharia Social: este é um termo usado entre "hackers" para técnicas que dependem das fraquezas das pessoas ao invés de Programas; o objetivo é enganar as pessoas para que revelem senhas ou outras informações que comprometem um sistema individual segurança.
É muito mais fácil falar do que fazer, mas pode ser feito. Maioria golpes de telemarketing que roubam dinheiro das pessoas são formas de "Engenharia social." A maioria desses golpes ocorre devido ao indivíduos que se fazem passar por empresas de cartão de crédito e / ou empresas de investimento. Esses ataques de engenharia social são focados em fazer com que você dê a eles seu dinheiro, o resultado final.

Capítulo

Transforme esse processo em uma indústria de tecnologia onde muitas pessoas não são tão conhecedores de computador e você tem o "lobo em pele de cordeiro!
Algumas das formas mais comuns de engenharia social com foco em qualquer usuário em particular é ligar para uma "marca / vítima" que tem as informações necessárias e se passando por um técnico de serviço de campo ou um colega de trabalho com um problema de acesso urgente. Esse tipo de O ataque acontece principalmente em cenas de negócios.
A engenharia social direcionada a um ambiente de negócios geralmente ocorre como um golpe de telefone. O golpe se resume a quão verossímil o “Hacker” soa no telefone. Eles testam seu conhecimento e inteligência contra outro humano. Essa técnica é usada para muitas coisas, como obter senhas e informações básicas sobre um sistema ou organização. Saiba que não é o único tipo de “social engenharia ”que é usada.
Esses mesmos princípios são aplicados quando se trata de sua computador. As linhas de bate-papo tornam as pessoas altamente suscetíveis a tais caos social.

EXEMPLO DE CHATLINE

Em uma linha de bate-papo, uma pessoa não é avaliada por sua aparência. Elas

tornam-se tão verossímeis quanto sua capacidade de escrever e expressar
eles mesmos.
Em uma linha de bate-papo, sua percepção e intuição é tudo que você precisa
dependem. A pessoa do outro lado do teclado pode ser
nada como eles se descrevem. O mesmo vale para e-mail
ou qualquer forma de comunicação sem reconhecimento visual.
Você lê o que eles enviam / dizem para você e sua própria imaginação é
o que preenche os espaços em branco. Essa pessoa pode soar romântica, engraçada
e com os pés no chão. Existe um valor de confiança que é construído e
dependendo de quanto tempo você está na Internet, esta inicial
base de confiança é formada muito rapidamente.

Página 64

Neste ponto, depois que o gelo foi quebrado, por assim dizer, o
“Hacker” pode perguntar se você deseja ver sua foto. Isto é o
ponto de viragem da sua conversa. A maioria das pessoas responderia com certeza
e, em seguida, receba a foto do “hacker”.
É aqui que a situação fica interessante. O “hacker” em
pergunta tem a janela de oportunidade para qualquer tentativa de enviar
você uma imagem real ou um Trojan.
Se o "hacker" lhe enviar uma imagem legítima, isso ajuda a
construir confiança entre eles e você. Se eles vão para a greve certo
do morcego, então eles correm o risco de se expor. Em ambos os casos
o objetivo deles foi alcançado, que é fazer com que você aceite
o arquivo deles.
Ganhando sua confiança e fazendo com que você, como usuário, abandone seu
guarda que você comprometeu a segurança de seus sistemas.
Dado que requer um certo nível de sutileza e graça para realizar
este tipo de ataque. Exige que o "hacker" seja socialmente hábil,
perspicaz e muito confiante. Normalmente não são as características de
a definição estereotipada de “hacker”.
Para se proteger neste nível, você deve estar ciente do
"jogos." A verdade é que tudo isso é um jogo para “hackers”.
Os hackers valorizam seu anonimato para vencê-los, o truque é
para reverter a situação. Faça com que eles se exponham e
sua intenção.
Vejamos uma situação da vida real que você pode encontrar.
Para simplificar, diremos que você encontrou um “potencial
hacker ”em uma linha de bate-papo. A pessoa parece charmosa, engraçada até
normal em todos os sentidos da palavra. A conversa se torna um
pouco pessoal em algum momento e embora não dê a ele sua vida
história, você compartilha algumas informações bastante confidenciais com este
pessoa.
A conversa esquenta e se transforma em um possível
comércio de imagens. O “hacker em potencial” deseja trocar fotos
com você. Você diz a ele / ela que não tem uma foto e a

Página 65

observação é algo no sentido de "bem, você gostaria de ver
minha foto mesmo assim? " Então você concorda que ele / ela lhe envie seus
foto.
Ao receber a foto, você percebe que o arquivo se chama:
□□John.exe ou susan.exe
(Relembrando o que você leu neste manual, você sabe que seus
a imagem nunca deve estar neste formato. Então você não clica duas vezes
nele)
É aqui que sua consciência e intuição entram em ação.
duas opções.
A) Enfrente o “hacker em potencial” sobre o tipo de arquivo.
B) Participe do jogo e veja se consegue pegar essa pessoa
fazendo-os se exporem.
Se você confrontar a pessoa, talvez receba explicações como
“É uma imagem autoextraível.” Nesse ponto, você pode dizer a eles
eles estão mentindo. Você provavelmente vai assustar o "hacker em potencial"
sendo tão direto com eles. É mais do que provável que eles registrem
offline muito rapidamente. Se você entrar no jogo, terá o
chance de talvez pegá-los, ou pelo menos descobrir quem eles são.

EXEMPLO IRC

IRC é um campo de caça para “hackers”. Não requer muita habilidade
ou muito know-how, para infectar o computador de um indivíduo no IRC.
Algumas das táticas mais comuns é assumir a identidade de um
garota e ir a canais onde as imagens são comumente
trocado. Canais como “adultos com mais de 30 anos” ou “chat para adultos”.
Hackers sabem que hackear é 60% guerra psicológica 40%
conhecimento de informática.
Um dos métodos mais populares de enviar um Trojan a uma pessoa
no IRC é enviar automaticamente o arquivo quando você entrar em um
canal. A razão é que algumas pessoas têm um
recurso ativado em seus programas de IRC que automaticamente
aceita transferências de arquivos de entrada.
(Consulte a documentação do programa IRC)
Ao entrar no canal, você aceita o arquivo automaticamente. Se
você está ciente do arquivo, pode ver que ele se chama algo como
tiffany.jpg.exe. Por pura curiosidade, algumas pessoas vão abrir
o arquivo para ver o que é, especialmente aqueles que não estão cientes de
os perigos potenciais de tais arquivos. O resultado é (MISSÃO
REALIZADO).
Como você pode ver claramente, os "hackers" são bastante adeptos da arte de
subterfúgio. Eles são espertos, astutos e não discriminam
contra quem está no computador, eles tentarão obter acesso também.
Eles vão atacar quem for vítima de qualquer armadilha que preparem.
IRC continua sendo uma das principais fontes de vítimas para “crianças
hackers. ”
A receita para se proteger exige que você esteja alerta, desconfiado
e um pouco de paranóia ajuda. Encare isso, todo mundo está paranóico sobre

algo ou o outro. No próximo capítulo, discutiremos como
continue relatando “hackers”.

Página 67

COMO DENUNCIAR HACKERS

Parar os hackers pode ser muito difícil, às vezes, aparentemente
impossível. Eu acredito, no entanto, se você usar os tipos certos de
programas combinados com autoeducação sobre como os hackers pensam,
você pode tornar seu computador muito mais seguro.
Reportar hackers às vezes pode ser um pouco complicado. Um monte de
os usuários nunca relatam tentativas de hack. Simplesmente porque eles apenas
não se importe ou acredite que o "hacker" sabe que não pode entrar
seu sistema. Há também a razão de os usuários simplesmente não saberem
quais etapas tomar quando perceberem que seu sistema está sendo
atacado.
Depois que seu sistema estiver conectado à Internet, alguma forma de
ataque de sistema eventualmente atingirá seu computador. A maioria dos
vezes esses ataques serão completamente aleatórios. Embora não seja todo
ataque único já feito deve ser relatado, ataques repetitivos
deve. Ataques repetidos da mesma pessoa / endereço IP
sempre deve ser relatado. Esta é uma indicação clara de que
alguém está tentando obter acesso ao seu computador.
Se você estiver usando Black Ice Defender e / ou Lockdown 2000, você
será capaz de ver o endereço IP da pessoa que está tentando
invadir seu sistema.

Capítulo

Página 68

O que você faz agora que sabe que alguém está tentando
hackear seu computador?
Antes de fazer qualquer coisa, você precisará de alguns utilitários. eu
recomendo obter o seguinte programa.
□□NetLab
Netlab tem uma variedade de utilitários combinados em um fácil de usar
aplicativo.
Você pode obter uma cópia do Netlab em:
http://www.filedudes.lvdi.net/win95/dns/netlab95.html
Depois de obter uma cópia do NetLab e instalá-lo, você estará pronto.

Acho que o melhor procedimento para isso é começar identificando como
muitas vezes esse "indivíduo" tentou invadir seu
sistema e em que horários.
(Consulte a documentação do programa de firewall para obter instruções sobre
onde localizar o número de ataques originados de um IP
Morada.)
Depois de identificar quantas vezes a pessoa
tentou obter acesso e a que horas o mais recente
ataque foi, é uma boa idéia verificar se eles realmente conseguiram passar.
Para verificar o que está conectado atualmente ao seu computador, faça o
Segue:
□□Anote o endereço IP que você recebeu da Black Ice e
ou Lockdown 2000
□□Clique em **Iniciar**
□□Vá para **Executar**
□□Digite **Command** e pressione **Enter**

Isso o levará ao prompt do DOS novamente.
Digite o seguinte no prompt do DOS.
□□**Netstat**
Isso lhe dará uma lista de todas as conexões ativas para o seu
computador e será algo parecido com isto.
Conexões Ativas
Protocolo
Endereço Local Endereço Estrangeiro
Estado
TCP
COMP: 0000 10.0.0.1: 0000
ESTABELECIDO
TCP
COMP: 2020
10.0.0.5: 1010 ESTABELECIDO
TCP
COMP: 9090
10.0.0.3: 1918 ESTABELECIDO
Suas informações terão números diferentes. Usei o IP
endereço 10.0.0.x apenas para fins de demonstração.

Se o seu invasor estiver conectado ao seu computador, você verá o IP dele
endereço nesta lista. Compare esta lista com o endereço IP que você
escreveu.
Na tabela acima, você verá os números após (:)
Por exemplo:
COMP: 2020
O 2020 representa o número da porta que o computador estrangeiro
está conectado no seu computador.

Usando nosso exemplo, vamos dar uma olhada na segunda linha. Esse nos mostra que alguém está conectado ao nosso computador na porta (2020) do endereço IP 10.0.0.5.
Depois de avaliar que o "hacker" não teve sucesso em suas tentativas de hackear seu computador, você pode prosseguir para reúna informações para relatar o ataque.
Inicie o NetLab
□□Digite o endereço IP na seguinte área

Página 71

69
□□Digite o endereço IP na área indicada abaixo

Página 72

70
□□Após digitar o endereço IP clique no **ping** indicado abaixo

---

Página 73

71
Neste ponto, você verá um de dois resultados. Você verá um resposta indicando que a pessoa está online ou você não verá resposta indicando que eles estão offline. Fazemos isso para verificar se o a pessoa ainda está conectada.
1: Este é o endereço IP para o qual você está executando o ping
2: o tempo que leva para fazer o ping do endereço.

Página 74

72
A próxima etapa é verificar a quem pertence o endereço IP. Você pode faça isso usando **whois.arin.net** no endereço IP da pessoa.
Depois de digitar o endereço IP na **string de consulta,** clique no Botão **Whois** . Você verá então a quem pertence o endereço IP.
Isso revelará quem é o provedor de serviços de Internet “hackers”.
Isso é muito importante, se você puder descobrir onde o invasor está vindo de você pode encaminhar as informações apropriadas para as pessoas certas.

Página 75

73
Vamos recapitular nosso procedimento em um formato passo a passo.
A) Vá para o prompt do DOS
B) Execute netstat para verificar se eles conseguiram
C) Inicie o Netlab e faça um teste de ping para verificar se eles ainda estão conectado
D) Faça uma pesquisa Whois (usando whois.arin.net)
Depois de realizar as etapas acima, você precisará enviar o informações ao seu ISP e ao ISP do invasor. O objetivo é forneça a eles o máximo de informações possível sobre o invasor.
Ambos os programas de firewall (Black Ice Defender) e (Lockdown

2000) criar arquivos de log de cada ataque. Copie as informações junto
com seu próprio teste e inclua os tempos de cada ataque em um
e-mail e envie-o ao seu provedor de ISP. Envie uma cópia desse e-mail
ao provedor de ISP do invasor também.
(Observação: você pode precisar ligar para o provedor de Internet do invasor para
obtenha o endereço de e-mail correto. Se a chamada envolverá longa distância
cobranças envie a mensagem para support@thehackersisp.com)
Todos os provedores de ISP possuem um departamento de Abuso. Eles são
responsável por lidar com tais questões. Se você enviar o e-mail para
o departamento de suporte do ISP “hackers” eles irão encaminhá-lo
para a divisão correta.
É sua responsabilidade relatar quaisquer ataques feitos contra
seu computador. Eu encorajo você a tomar parte ativa em
relatando ataques repetidos do mesmo endereço IP contra
seu computador, pois são indicações claras de alguém
visando você.
Pode ser que você tenha algo em que estejam interessados, ou
talvez seu sistema tenha sido comprometido antes de seu
realização, e com a instalação do programa de firewall você
agora estão bloqueando seus ataques. Seja qual for o motivo, agora que
você está ciente de que seu objetivo é proteger sua privacidade.

74

PALAVRAS FINAIS

Parabéns! Você chegou ao final do manual.
Isso provavelmente não é uma conquista para livros do mesmo
comprimento. Mas este manual é diferente. Você sempre pode fazer
consulte este manual sempre que tiver dúvidas. Isso é
como um manual e um curso em um. Aprendendo as lacunas do sistema
e truques que os “hackers” usam é apenas metade do processo. Protegendo
sua privacidade depende de você 90%, o resto pode ser tratado por
Programas.
Você tem os meios e a capacidade de se proteger. Pela leitura
este manual sozinho você provou isso. Você pode pensar em
você mesmo que está fora de combate na Internet, não. Nós todos
tem que começar a aprender de algum lugar. Até mesmo hackers e outros
chamados de “hackers” tiveram que começar a aprender em algum lugar. Ninguém
estava
nasceu com o conhecimento de como funciona um computador.
A Internet é uma ferramenta pela qual muitos desses "hackers" educam
eles mesmos. Você pode fazer o mesmo. Continua sendo o mais poderoso
ferramenta de informação e desenvolvimento que existe.
Mais e mais empresas e serviços estão migrando para o
mundo online. Você pode sentar e assistir ou pular
no movimento e cavalgá-lo. Está tudo nas tuas mãos.
Tenha cuidado ao lidar com pessoas online, mas não seja
muito paranóico. Aproveite o poder da Internet, pode ser um ótimo
ativo para você ou sua empresa.

Capítulo

A população online está crescendo exponencialmente. Com o recente crescimento do acesso dedicado, seu computador está conectado ao Internet 24 horas por dia. O acesso de alta velocidade dá a você o oportunidade de baixar arquivos em taxas extremamente rápidas. É um longo caminho do antigo dial up BBS. Conforme a tecnologia aumenta, também deve sua consciência.

Realisticamente, a maioria de nós não se preocupa com o funcionamento interno do Internet. Talvez tenhamos uma mera curiosidade sobre o que acontece nos bastidores, mas nenhum de nós realmente acredita que faz muito diferença para nós sabermos dessa informação. Nós nos preocupamos principalmente sobre como realizar nossas atividades diárias e aproveitar o poder de a Internet. Queremos ser capazes de registrar uma conversa online com nossos amigos e família e usar a Internet como ferramenta em nosso benefício.

A Internet conecta você ao mundo onde se um amigo de A Austrália deseja falar com você ao vivo, eles podem ligar suas webcams ligam seus microfones e fazem uma videoconferência. É um corte acima de um telefonema por uma fração do preço. Não deixe “Hackers” transformam avanços futuros em pesadelos indesejados. Você, como usuário, pode evitar isso tomando cuidado. Pegue o extra passos necessários para se proteger. Quando comparado com o benefícios que você pode ter definitivamente vale um extra de 1 hora a 2 horas de seu tempo.

Não pare de aprender, leia tudo o que puder. Por que não? Você tem o mundo ao seu alcance e informações em cada turno. Mas a maioria importante, quando tudo estiver dito e feito, recupere sua privacidade daqueles que podem tentar comprometê-lo.

Com grande respeito

S&C Enterprises
Grupo de Consulta