

Testes de Invasão

Uma introdução prática ao hacking

Georgia Weidman

Copyright © 2014 by Georgia Weidman. Title of English-language original: *Penetration Testing: A Hands-On Introduction to Hacking*, ISBN 978-1-59327-564-8, published by No Starch Press. Portuguese-language edition copyright © 2014 by Novatec Editora Ltda. All rights reserved.

Copyright © 2014 por Georgia Weidman. Título original em inglês: *Penetration Testing: A Hands-On Introduction to Hacking*, ISBN 978-1-59327-564-8, publicado pela No Starch Press. Edição em português copyright © 2014 pela Novatec Editora Ltda. Todos os direitos reservados.

© Novatec Editora Ltda. 2014.

Todos os direitos reservados e protegidos pela Lei 9610 de 19/02/1998.

É proibida a reprodução desta obra, mesmo parcial, por qualquer processo, sem prévia autorização, por escrito, do autor e da Editora.

Editor: Rubens Prates

Tradução: Lúcia A. Kinoshita

Revisão gramatical: Marta Almeida de Sá

Editoração eletrônica: Carolina Kuwabata

ISBN: 978-85-7522-407-6

Histórico de impressões:

Outubro/2014 Primeira edição

Novatec Editora Ltda.

Rua Luís Antônio dos Santos 110

02460-000 – São Paulo, SP – Brasil

Tel.: +55 11 2959-6529

E-mail: novatec@novatec.com.br

Site: novatec.com.br

Twitter: twitter.com/novateceditora

Facebook: facebook.com/novatec

LinkedIn: linkedin.com/in/novatec

CAPÍTULO 1

Configurando o seu laboratório virtual

À medida que trabalhar neste livro, você irá adquirir uma experiência prática por meio do uso de diferentes ferramentas e técnicas usadas em testes de invasão ao trabalhar em um laboratório virtual executado no software de virtualização VMware. Descreverei o processo de configuração de seu laboratório, que executará vários sistemas operacionais dentro de seu sistema operacional de base, de modo a simular uma rede inteira usando somente um computador físico. Utilizaremos o nosso laboratório para atacar sistemas-alvo ao longo deste livro.

Instalando o VMware

Como primeiro passo da configuração de seu laboratório virtual, faça o download e instale um produto VMware para desktop. O VMware Player está disponível gratuitamente para uso pessoal para os sistemas operacionais Microsoft Windows e Linux (<http://www.vmware.com/products/player/>). O VMware também oferece o VMware Workstation (<http://www.vmware.com/products/workstation/>) para Windows e Linux, que inclui recursos adicionais como a capacidade de salvar imagens (snapshots) da máquina virtual para as quais é possível retroceder em caso de haver alguma falha. O VMware Workstation está disponível gratuitamente por 30 dias, porém, depois disso, será necessário comprá-lo ou voltar a usar o VMware Player.

Usuários de Mac podem executar uma versão trial do VMware Fusion (<http://www.vmware.com/products/fusion/>) gratuitamente durante 30 dias, e seu custo, depois disso, é de apenas 50 dólares. Como usuário de Mac, usarei o VMware Fusion ao longo do livro, mas as instruções para efetuar a configuração estão disponíveis também para o VMware Player.

Faça o download da versão do VMware que seja compatível com o seu sistema operacional e a sua arquitetura (32 bits ou 64 bits). Se houver algum problema na instalação do VMware, você encontrará suporte suficiente no site da VMware.

Instalando o Kali Linux

O Kali Linux é uma distribuição de Linux baseada em Debian, que vem com uma ampla variedade de ferramentas de segurança pré-instalada; ele será usado ao longo desta obra. Este livro foi escrito para o Kali 1.0.6, que era a versão atual na época desta publicação. Você encontrará um link para um torrent contendo uma cópia do Kali 1.0.6 no site deste livro (<http://nostarch.com/pentesting/>). À medida que o tempo passar, versões mais novas do Kali serão disponibilizadas. Se quiser, sintase à vontade para fazer o download da versão mais recente do Kali Linux a partir de <http://www.kali.org/>. Entretanto tenha em mente que muitas das ferramentas que usaremos neste livro estão em desenvolvimento no momento, portanto, se você usar uma versão mais recente do Kali, alguns dos exercícios poderão apresentar diferenças em relação às descrições contidas neste livro. Se preferir que tudo funcione conforme descrito, recomendo usar a versão 1.0.6 do Kali, disponibilizada no torrent (um arquivo chamado *kali-linux-1.0.6-vm-i486.7z*), que corresponde a uma imagem do VMware, pronta e compactada com o 7-Zip.

NOTA Você pode encontrar programas 7-Zip para as plataformas Windows e Linux em <http://www.7-zip.org/download.html>. Para usuários de Mac, recomendo o Ez7z, que se encontra em <http://ez7z.en.softonic.com/mac/>.

1. Depois que o arquivo 7-Zip for descompactado, acesse **File ▶ Open** (Arquivo ▶ Abrir) no VMware e direcione-o para o arquivo *Kali Linux 1.0.6 32 bit.vmx* na pasta *Kali Linux 1.0.6 32 bit* descompactada.
2. Depois que a máquina virtual for aberta, clique no botão **Play** (Executar) e, quando solicitado, conforme mostrado na figura 1.1, selecione **I copied it** (Eu a copiei).
3. À medida que o Kali Linux iniciar, você verá um prompt, conforme mostrado na figura 1.2. Selecione a opção destacada mais acima (default).
4. Depois que o Kali Linux iniciar, uma tela de login será apresentada, como a que está sendo mostrada na figura 1.3.

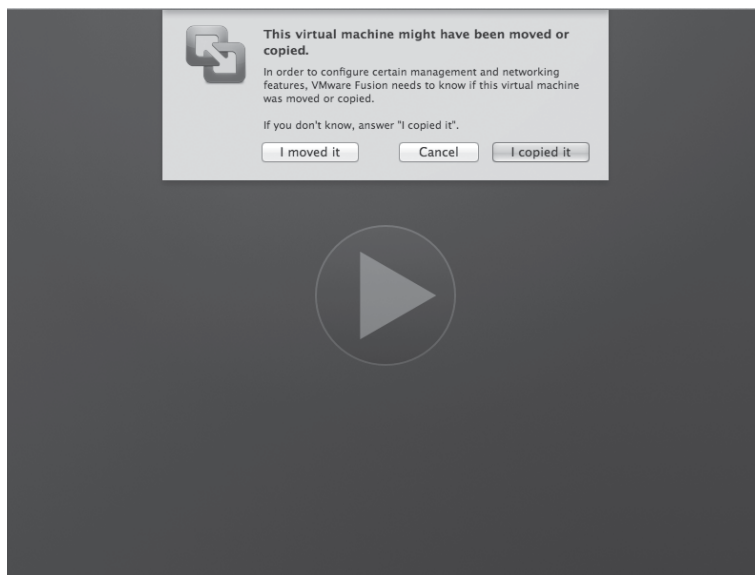


Figura 1.1 – Abrindo a máquina virtual Kali Linux.

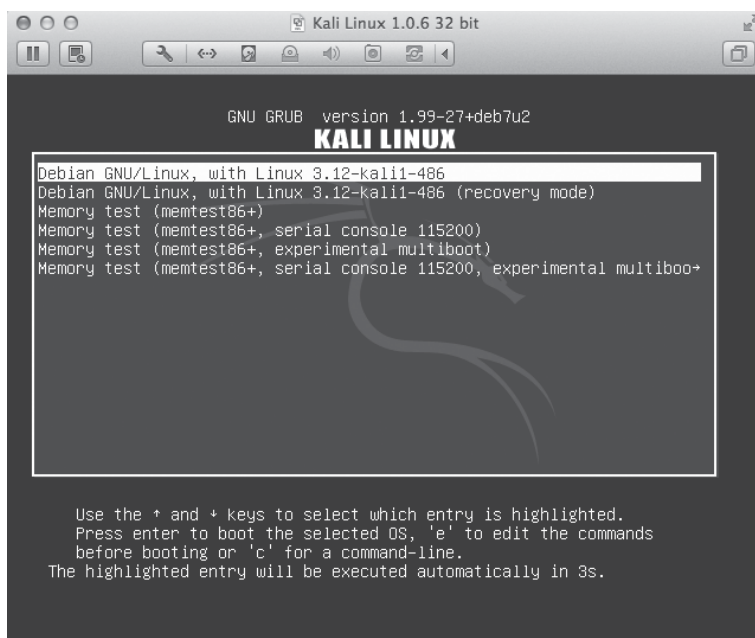


Figura 1.2 – Iniciando o Kali Linux.

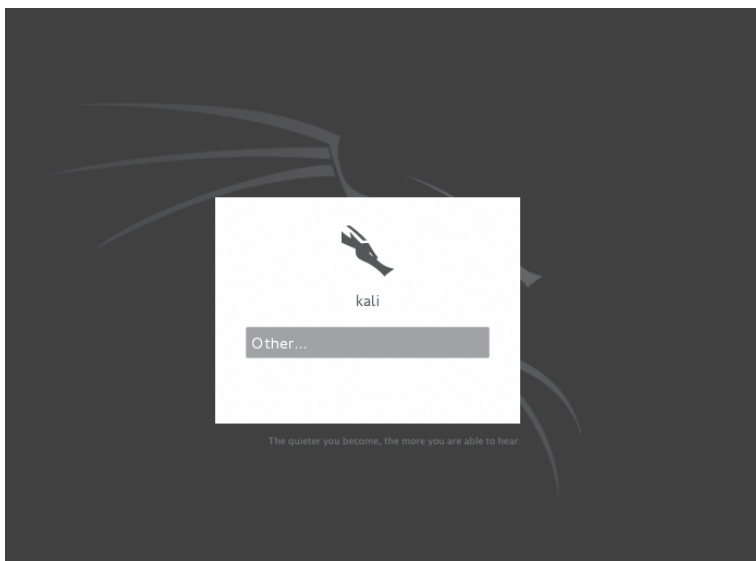


Figura 1.3 – Tela de login do Kali.

5. Clique em **Other** (Outro) e forneça as credenciais default do Kali Linux, ou seja, *root:toor*, como mostrado na figura 1.4. Em seguida, clique no botão **Log In**.

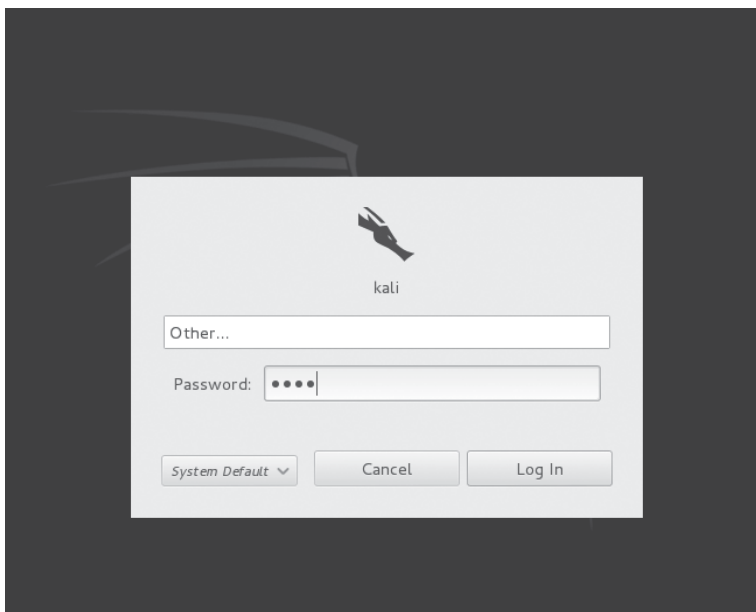


Figura 1.4 – Fazendo login no Kali.

6. Uma tela como a que está sendo mostrada na figura 1.5 será apresentada.



Figura 1.5 – A GUI do Kali Linux.

Configurando a rede de sua máquina virtual

Como usaremos o Kali Linux para atacar nossos sistemas-alvo por meio de uma rede, devemos colocar todas as nossas máquinas virtuais na mesma rede virtual (veremos um exemplo de movimentação entre redes no capítulo 13, que discute a pós-exploração de falhas). O VMware oferece três opções para conexões de redes virtuais: bridged (com bridge), NAT e host only (somente hosts). Você deverá escolher a opção bridged (com bridge), mas aqui estão algumas informações a respeito de cada uma delas:

- A *rede com bridge* (bridged network) conecta a máquina virtual diretamente à rede local usando a mesma conexão usada pelo sistema host. No que concerne à rede local, nossa máquina virtual será somente outro nó da rede, com seu próprio endereço IP.
- A *NAT*, sigla para *Network Address Translation* (Tradução de endereço de rede) define uma rede privada no computador host. A rede privada faz a tradução do tráfego de saída da máquina virtual para a rede local. Na rede local, o tráfego da máquina virtual parecerá vir do endereço IP do computador host.

- A rede *somente hosts* (host-only) limita a máquina virtual a uma rede privada local no host. A máquina virtual será capaz de se comunicar com outras máquinas virtuais na rede somente de hosts, bem como com o próprio computador host, porém não poderá enviar nem receber qualquer tráfego da rede local ou da Internet.

NOTA Como nossas máquinas virtuais-alvo terão diversas vulnerabilidades de segurança conhecidas, tome cuidado ao conectá-las à sua rede local, pois qualquer pessoa nessa rede também poderá atacar esses computadores. Por esse motivo, não recomento trabalhar, neste livro, em uma rede pública, em que você não possa confiar nos demais usuários.

Por padrão, o adaptador de rede da máquina virtual Kali Linux é definido com NAT. Aqui está o modo de alterar essa opção tanto no Windows quanto no Mac OS.

VMware Player no Microsoft Windows

Para alterar a rede virtual no VMware Player para Windows, inicie o VMware Player e, em seguida, clique em sua máquina virtual Kali Linux. Selecione **Edit virtual machine settings** (Alterar configurações da máquina virtual), conforme mostrado na figura 1.6. [Se você ainda estiver executando o Kali Linux no VMware Player, selecione **Player ▶ Manage ▶ Virtual machine settings** (Player ▶ Administração ▶ Configurações da máquina virtual).]

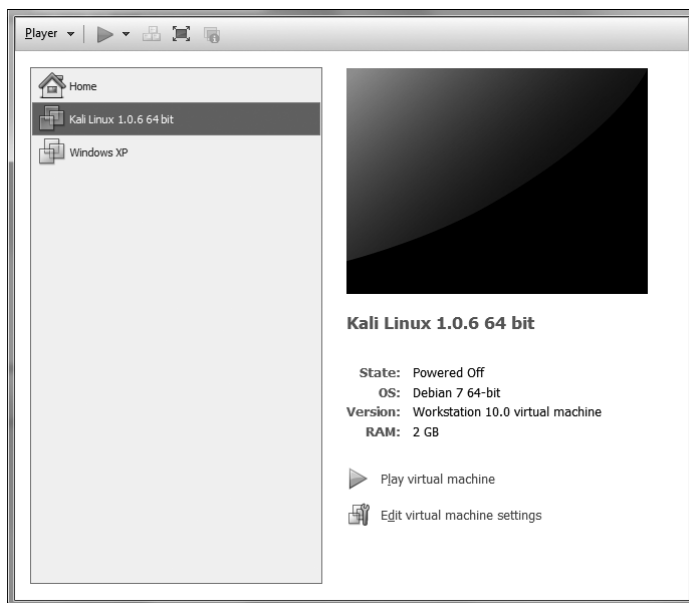


Figura 1.6 – Alterando o adaptador de rede do VMware.

Na tela seguinte, selecione **Network Adapter** (Adaptador de rede) na aba **Hardware** e selecione a opção **Bridged** (Com bridge) na seção **Network connection** (Conexão de rede), como mostrado na figura 1.7.

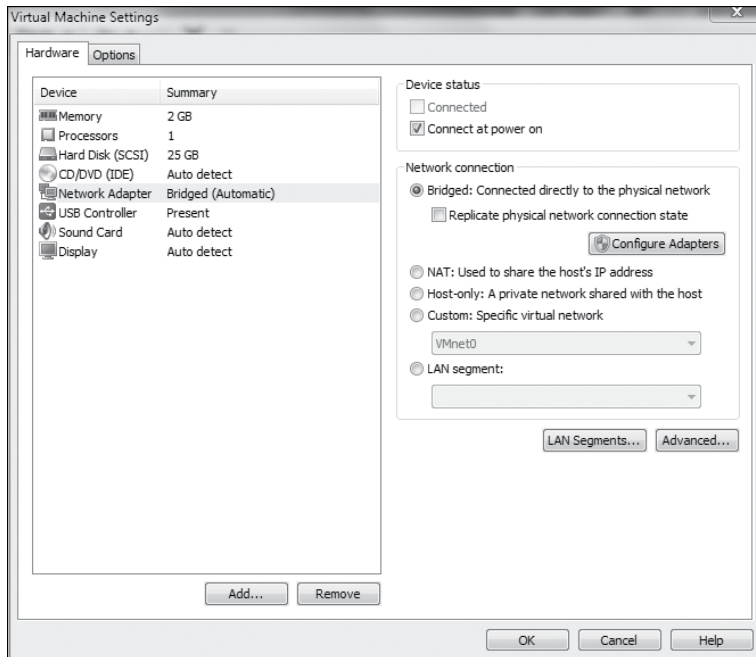


Figura 1.7 – Alterando as configurações do adaptador de rede.

Agora clique no botão **Configure Adapters** (Configurar adaptadores) e verifique o adaptador de rede que você está usando em seu sistema operacional host. Como você pode ver na figura 1.8, selecionei somente o adaptador Realtek wireless. Após ter efetuado a sua seleção, clique em **OK**.

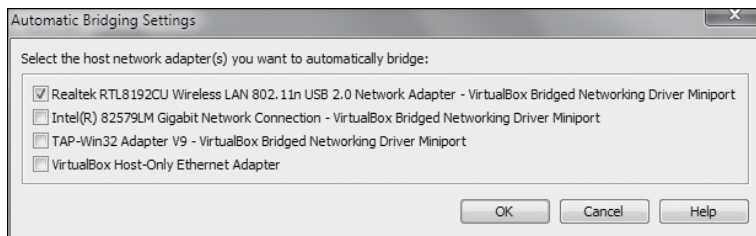


Figura 1.8 – Selecionando um adaptador de rede.

VMware Fusion no Mac OS

Para mudar a conexão da rede virtual no VMware Fusion, acesse **Virtual Machine ▶ Network Adapter** (Máquina Virtual ▶ Adaptador de rede) e altere de NAT para Bridged, conforme mostrado na figura 1.9.

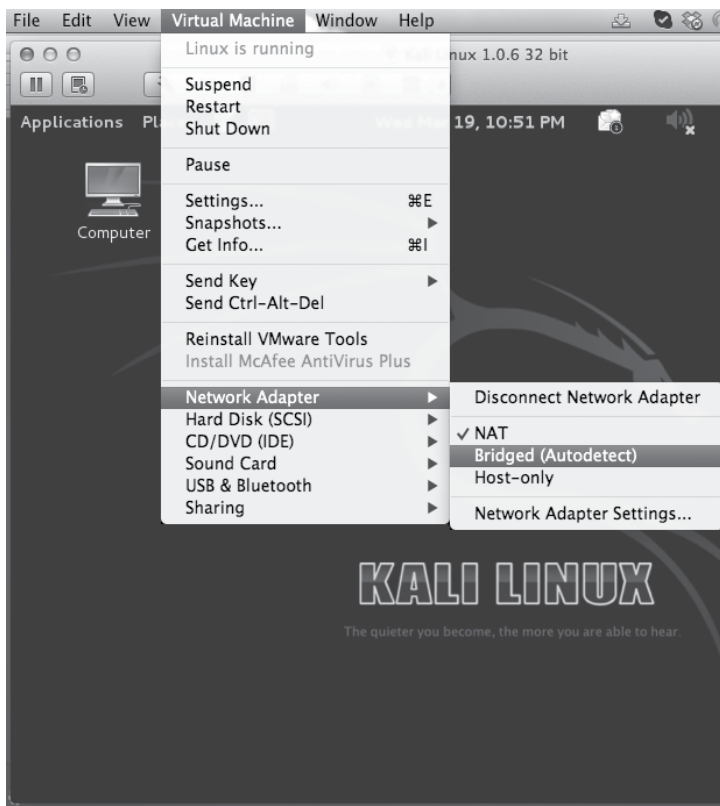


Figura 1.9 – Alterando o adaptador de rede.

Conectando a máquina virtual à rede

O Kali Linux deverá obter automaticamente um endereço IP da rede Bridged depois que a alteração for feita. Para conferir o seu endereço IP, abra um terminal Linux ao clicar no ícone do terminal (um retângulo preto com os símbolos >_) na parte superior à esquerda da tela do Kali [ou selecione **Applications ▶ Accessories ▶ Terminal** (Aplicativos ▶ Acessórios ▶ Terminal)]. Em seguida, execute o comando `ifconfig` para ver as informações de sua rede, conforme mostrado na listagem 1.1.

Listagem 1.1 – Informações de rede

```
root@kali:~# ifconfig
eth0    Link encap:Ethernet  HWaddr 00:0c:29:df:7e:4d
        inet addr:192.168.20.9  Bcast:192.168.20.255  Mask:255.255.255.0
        inet6 addr: fe80::20c:29ff:fedf:7e4d/64 Scope:Link
--trecho omitido--
```

NOTA root@kali:~# corresponde ao prompt do superusuário (root). Aprenderemos mais sobre esse e os demais comandos do Linux utilizados na instalação no capítulo 2.

O endereço IPv4 dessa máquina virtual é 192.168.20.9, como destacado em negrito na listagem 1.1. (O endereço IP de seu computador provavelmente será diferente.)

Testando o seu acesso à Internet

Agora vamos garantir que o Kali Linux possa se conectar à Internet. Usaremos o utilitário de rede ping para ver se podemos acessar o Google. Certifique-se de que o seu computador esteja conectado à Internet, abra um terminal Linux e digite o seguinte:

```
root@kali:~# ping www.google.com
```

Se vir algo parecido com a resposta a seguir, você estará online. (Aprenderemos mais sobre o comando ping no capítulo 3.)

```
PING www.google.com (50.0.2.221) 56(84) bytes of data.
64 bytes from cache.google.com (50.0.2.221): icmp_req=1 ttl=60 time=28.7 ms
64 bytes from cache.google.com (50.0.2.221): icmp_req=2 ttl=60 time=28.1 ms
64 bytes from cache.google.com (50.0.2.221): icmp_req=3 ttl=60 time=27.4 ms
64 bytes from cache.google.com (50.0.2.221): icmp_req=4 ttl=60 time=29.4 ms
64 bytes from cache.google.com (50.0.2.221): icmp_req=5 ttl=60 time=28.7 ms
64 bytes from cache.google.com (50.0.2.221): icmp_req=6 ttl=60 time=28.0 ms
--trecho omitido--
```

Se você não receber uma resposta, certifique-se de ter configurado o seu adaptador de rede para Bridged, que o Kali Linux tenha um endereço IP e, é claro, que o seu sistema host tenha acesso à Internet no momento.

Instalando o Nessus

Embora o Kali Linux tenha praticamente todas as ferramentas de que precisaremos, será necessário instalar alguns programas adicionais. Em primeiro lugar, iremos instalar o scanner de vulnerabilidades Nessus Home da Tenable Security. Esse scanner é gratuito somente para usos domésticos (você verá uma descrição das limitações no site do Nessus). Observe que o Nessus tem um desenvolvimento bastante ativo, portanto a versão atual, bem como a sua GUI, podem ter sido um pouco alteradas desde a publicação deste livro.

Utilize os passos a seguir para instalar o Nessus Home a partir do Kali:

1. Abra **Applications ► Internet ► Iceweasel Web Browser** (Aplicativos ► Internet ► Navegador web Iceweasel) e digite `http://www.tenable.com/products/nessus-home/` na barra de endereço. Preencha as informações de Register for an Activation Code (Registrar para obter um código de ativação) e clique em **Register** (Registrar). (Use um endereço real de email – você precisará do código de ativação mais tarde.)
2. Após ter acessado a página de Downloads, selecione a versão mais recente do Nessus para a plataforma Linux Debian 32 bits (*Nessus-5.2.5-debian6_i386.deb*, na época em que este livro foi publicado) e faça o download dessa versão em seu diretório root (o local default para download).
3. Abra um terminal Linux (clique no ícone do terminal na parte superior da tela do Kali) para abrir um prompt de root.
4. Digite **ls** para ver uma lista dos arquivos em seu diretório root. Você deverá ver o arquivo do Nessus que acabou de ser baixado.
5. Digite **dpkg -i** seguido do nome do arquivo que foi baixado (você pode digitar a primeira letra do nome do arquivo e teclar **tab** para utilizar o recurso de preenchimento com tab) e tecla **enter** para iniciar o processo de instalação. A instalação pode demorar um pouco, pois o Nessus processa diversos plugins. O progresso é mostrado por meio de uma linha contendo símbolos de sustenido (#).

```

Selecting previously unselected package nessus.
(Reading database ... 355024 files and directories currently installed.)
Unpacking nessus (from Nessus-5.2.5-debian6_amd64.deb) ...
Setting up nessus (5.2.5) ...
nessusd (Nessus) 5.2.5 [build N25109] for Linux
Copyright (C) 1998 - 2014 Tenable Network Security, Inc
Processing the Nessus plugins...
[#####
  
```

]

6. Depois de retornar ao prompt de root sem que tenha havido erros, o Nessus deverá estar instalado, e você verá uma mensagem como esta:

```
All plugins loaded
Fetching the newest plugins from nessus.org...
Fetching the newest updates from nessus.org...
Done. The Nessus server will start processing these plugins within a minute
nessusd (Nessus) 5.2.5 [build N25109] for Linux
Copyright (C) 1998 - 2014 Tenable Network Security, Inc
Processing the Nessus plugins...
[#####]
All plugins loaded

- You can start nessusd by typing /etc/init.d/nessusd start
- Then go to https://kali:8834/ to configure your scanner
```

7. Agora digite o comando a seguir para iniciar o Nessus:

```
root@kali:~# /etc/init.d/nessusd start
```

8. Abra o URL <https://kali:8834/> no navegador web Iceweasel. Você deverá ver um aviso de certificado SSL semelhante ao que está sendo mostrado na figura 1.10.

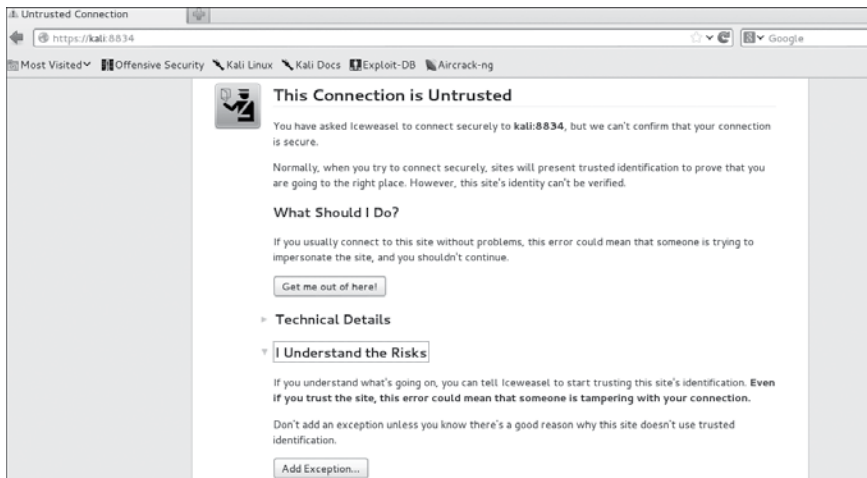


Figura 1.10 – Aviso de certificado SSL inválido.

NOTA Se você acessar o Nessus de fora do navegador Iceweasel no Kali, será necessário usar <https://<endereço IP do Kali>:8834> no lugar do endereço anterior.

9. Expanda **I Understand the Risks** (Entendo os riscos) e clique em **Add Exception** (Adicionar exceção). Em seguida, clique em **Confirm Security Exception** (Confirmar exceção de segurança), como mostrado na figura 1.11.



Figura 1.11 – Confirmando a exceção de segurança.

10. Clique em **Get Started** (Iniciar) na parte inferior à esquerda da página de abertura do Nessus e digite um nome de usuário e uma senha na página seguinte. Em meu exemplo, escolhi *georgia:password*. Se preferir algo diferente, lembre-se desses dados porque usaremos o Nessus no capítulo 6. (Observe que uso senhas fracas ao longo deste livro, como ocorrerá com vários clientes que você conhecerá. Em ambiente de produção, utilize senhas bem melhores do que *password*.)
11. Na página seguinte, insira o código de ativação recebido da Tenable Security por email.
12. Após ter se registrado junto à Tenable Security, selecione a opção para fazer download dos plugins (o download consumirá um pouco de tempo). Depois que o Nessus processar os plugins, ele será inicializado.

Quando o Nessus terminar de efetuar o download dos plugins e de configurar o software, você deverá ver a tela de login do Nessus, conforme mostrado na figura 1.12. Você poderá usar as credenciais da conta criada durante o processo de instalação para efetuar o login.

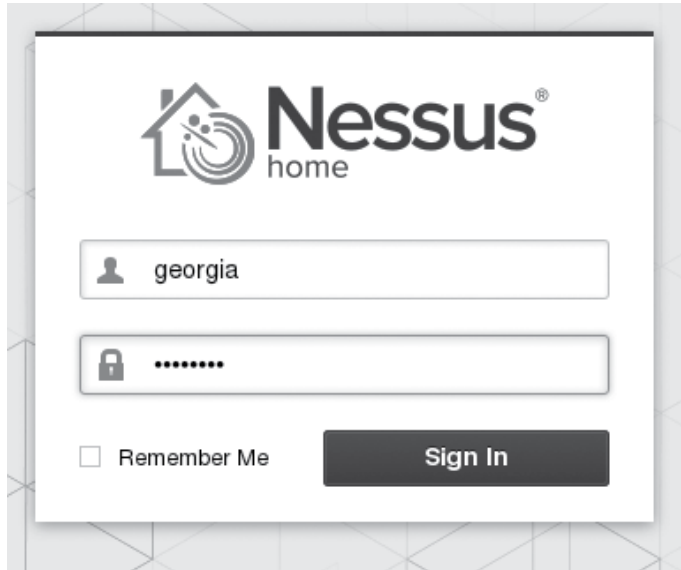


Figura 1.12 – Tela de login da interface web do Nessus.

Para encerrar o Nessus, basta fechar a sua aba no navegador. Retornaremos ao Nessus no capítulo 6.

Instalando softwares adicionais

Ainda não terminamos. Siga estas instruções para completar a sua instalação do Kali Linux.

Compilador Ming C

Precisamos instalar um cross-compilador (cross compiler) para que possamos compilar código C, de modo a executá-lo em sistemas Microsoft Windows. O compilador Ming está incluído nos repositórios do Kali Linux, porém não é instalado por default. Instale-o por meio deste comando:

```
root@kali:~# apt-get install mingw32
```

Hyperion

Usaremos o programa de criptografia Hyperion para evitar os softwares anti-vírus. O Hyperion atualmente não está incluído nos repositórios do Kali. Faça o download do Hyperion usando `wget`, descompacte-o e compile-o com o cross-compilador Ming instalado no passo anterior, conforme mostrado na listagem 1.2.

Listagem 1.2 – Instalando o Hyperion

```
root@kali:~# wget http://nullsecurity.net/tools/binary/Hyperion-1.0.zip
root@kali:~# unzip Hyperion-1.0.zip
Archive: Hyperion-1.0.zip
  creating: Hyperion-1.0/
  creating: Hyperion-1.0/FasmAES-1.0/
root@kali:~# i586-mingw32msvc-c++ Hyperion-1.0/Src/Crypter/*.cpp -o hyperion.exe
--trecho omitido--
```

Veil-Evasion

O Veil-Evasion é uma ferramenta que gera executáveis de payloads que podem ser usados para evitar soluções comuns de antivírus. Instale o Veil-Evasion Kali (veja a listagem 1.3) inicialmente efetuando o seu download por meio do comando `wget`. Em seguida, descompacte o arquivo `master.zip` baixado e vá para o diretório `Veil-master/setup`. Por fim, digite `./setup.sh` e siga os prompts default.

Listagem 1.3 – Instalando o Veil-Evasion

```
root@kali:~# wget https://github.com/ChrisTruncer/Veil/archive/master.zip
--2015-11-26 09:54:10-- https://github.com/ChrisTruncer/Veil/archive/master.zip
--trecho omitido--
2015-11-26 09:54:14 (880 KB/s) - 'master.zip' saved [665425]

root@kali:~# unzip master.zip
Archive: master.zip
948984fa75899dc45a1939ffbf4fc0e2ede0c4c4
  creating: Veil-Evasion-master/
--trecho omitido--
  inflating: Veil-Evasion-master/tools/pyherion.py
root@kali:~# cd Veil-Evasion-master/setup
root@kali:~/Veil-Evasion-master/setup# ./setup.sh

=====
[Web]: https://www.veil-evasion.com | [Twitter]: @veilevasion
```



```
=====
[*] Initializing Apt Dependencies Installation
--trecho omitido--
Do you want to continue? [Y/n]? Y
--trecho omitido--
root@kali:~#
```

Ettercap

O Ettercap é uma ferramenta para realizar ataques do tipo man-in-the-middle (homem-no-meio). Antes de executá-lo pela primeira vez, é necessário fazer algumas alterações em seu arquivo de configuração em `/etc/ettercap/etter.conf`. Abra esse arquivo de configuração a partir de um prompt de root no Kali usando o editor nano.

```
root@kali:~# nano /etc/ettercap/etter.conf
```

Inicialmente, altere os valores de `userid` e de `groupid` para `0` para que o Ettercap possa ser executado com privilégios de root. Faça rolagens até ver as linhas a seguir no arquivo. Substitua qualquer valor que estiver após os sinais de igual (=) por um `0`.

```
[privs]
ec_uid = 0      # ninguém é o default
ec_gid = 0      # ninguém é o default
```

Agora faça rolagens até à seção Linux do arquivo e remova o comentário (apague o caractere # na frente) das duas linhas mostradas em ❶ e em ❷ na listagem 1.4 para definir as regras de firewall de Iptables, de modo a redirecionar o tráfego.

Listagem 1.4 – O arquivo de configuração do Ettercap

```
#-----
#   Linux
#-----

# se ipchains for usado:
#redir_command_on = "ipchains -A input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"
#redir_command_off = "ipchains -D input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"

# se iptables for usado:
❶redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j
    REDIRECT --to-port %rport"
❷redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j
    REDIRECT --to-port %rport"
```

Salve o arquivo e saia ao teclar **Ctrl-X** e, em seguida, **Y** para salvar as alterações.

Configurando emuladores de Android

Agora iremos instalar três emuladores de Android no Kali, que serão usados nos testes de dispositivos móveis no capítulo 20. Inicialmente, devemos fazer o download do Android SDK.

1. Abra o navegador web Iceweasel a partir do Kali e acesse <https://developer.android.com/sdk/index.html>.
2. Faça o download da versão atual do ADT bundle para Linux 32 bits e salve-a em seu diretório root.
3. Abra um terminal, liste os arquivos ali presentes (ls) e descompacte o arquivo que acabou de ser baixado usando o unzip (os x's representam o nome de seu arquivo, pois as versões podem ter mudado desde que este livro foi publicado).

```
root@kali:~# unzip adt-bundle-Linux-x86-xxxxxxxxxxx.zip
```

4. Agora use cd para acessar o novo diretório (com o mesmo nome que o arquivo, sem a extensão .zip).

```
# cd sdk/tools
```

```
# ./android
```

5. O Android SDK Manager deverá ser aberto, como mostrado na figura 1.13.

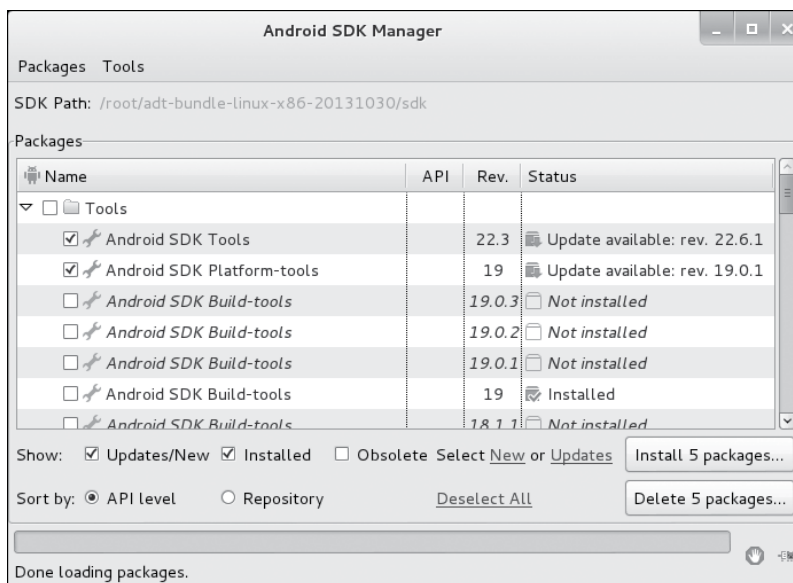


Figura 1.13 – O Android SDK Manager.

Faremos o download de quaisquer atualizações do Android SDK tools e do Android SDK platform tools (selecionados por default), bem como do Android 4.3 e de duas versões mais antigas do Android contendo vulnerabilidades específicas: o Android 2.2 e o Android 2.1. Marque as caixas à esquerda de cada versão de Android. Em seguida, [com Updates/New (Atualizações/Novos) e Installed (Instalado) selecionados], clique em **Install packages** (Instalar pacotes), conforme mostrado na figura 1.14. Aceite o acordo de licença, e o Android SDK deverá baixar e instalar os pacotes selecionados. É provável que a instalação demore alguns minutos.

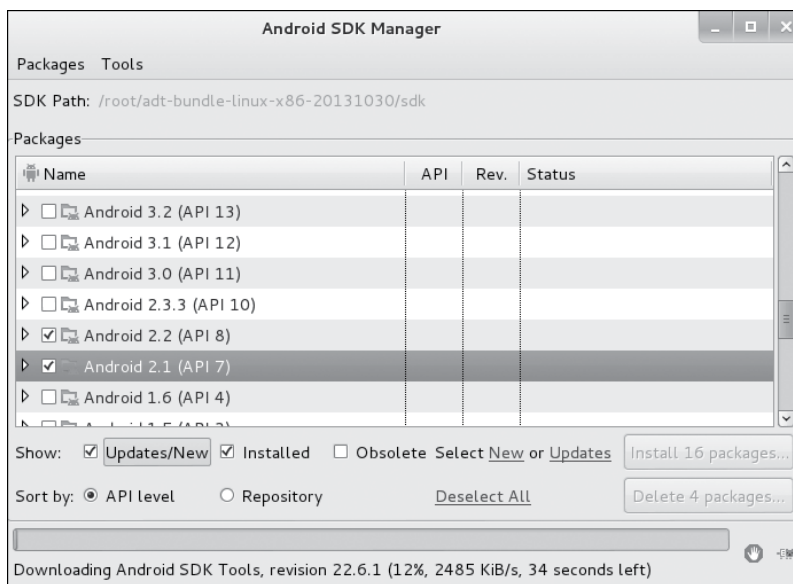


Figura 1.14 – Instalando o software do Android.

Agora é hora de configurar nossos dispositivos Android virtuais. Abra o Android SDK Manager e selecione **Tools ► Manage AVDs** (Ferramentas ► Gerenciar AVDs). Você deverá ver a janela mostrada na figura 1.15.

Criaremos três emuladores de Android baseados no Android 4.3, 2.2 e 2.1, como mostrado na figura 1.16. Utilize os valores apresentados na figura em cada emulador, porém configure o valor de Target (Alvo) com a versão de Android do emulador que você quer criar [as versões do Google API do Android 4.3 (Google APIs versão 18), 2.2 (Google APIs versão 8) e 2.1 (Google APIs versão 7)]. Preencha o campo **AVD Name** (Nome do AVD) com um valor descritivo. Adicione um valor baixo para SD Card (100 MB deve ser mais do que suficiente) para que você possa fazer download de arquivos em seus emuladores de Android. Configure Device para **Nexus 4** e Skin para **Skin with dynamic hardware controls** (Skin com controles dinâmicos de hardware). Deixe o restante das opções com seus valores default.

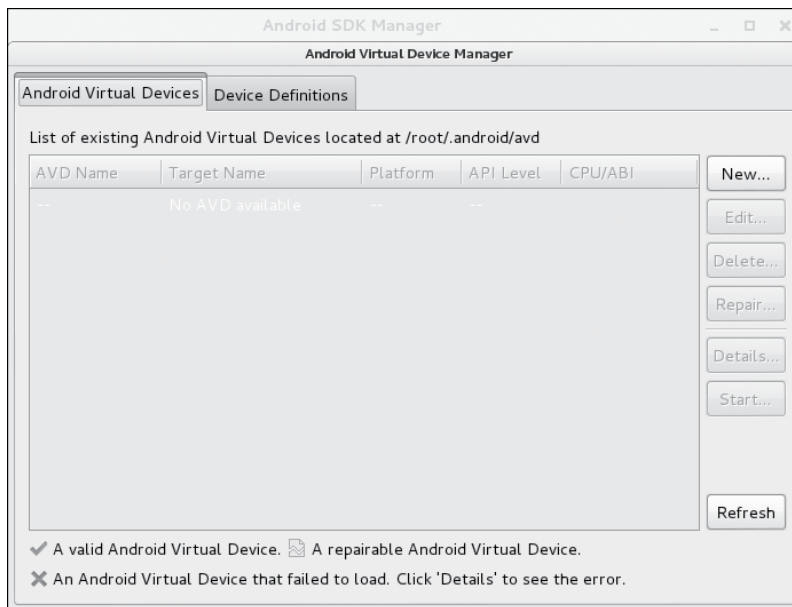


Figura 1.15 – Android Virtual Device Manager (Gerenciador de dispositivos Android virtuais).

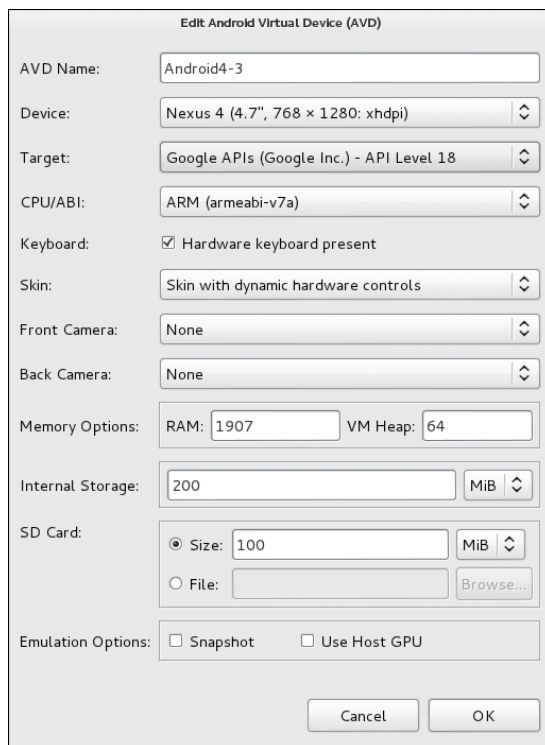


Figura 1.16 – Criando um emulador de Android.

Depois de ter criado todos os três emuladores, o seu AVD Manager deverá ter a aparência mostrada na figura 1.17 (os nomes dos dispositivos poderão ser diferentes, é claro).

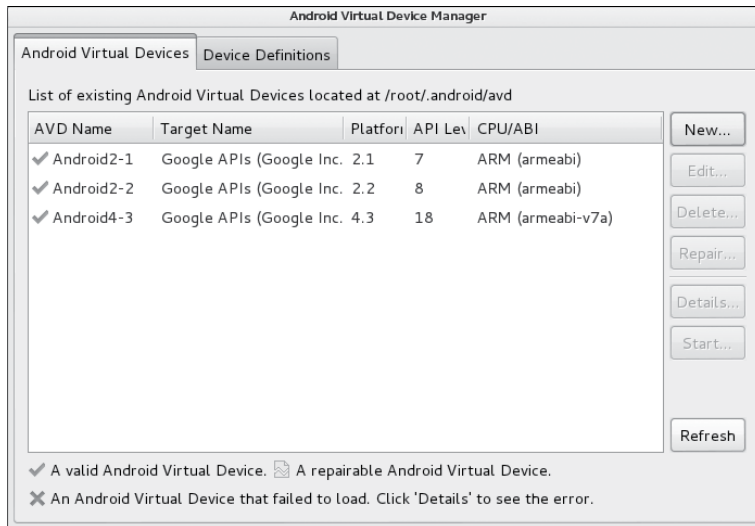


Figura 1.17 – Emuladores de Android criados no Android Virtual Device Manager.

Para iniciar um emulador, selecione-o e clique em **Start** (Iniciar). Em seguida, clique em **Launch** (Disparar) no diálogo pop-up, como mostrado na figura 1.18.

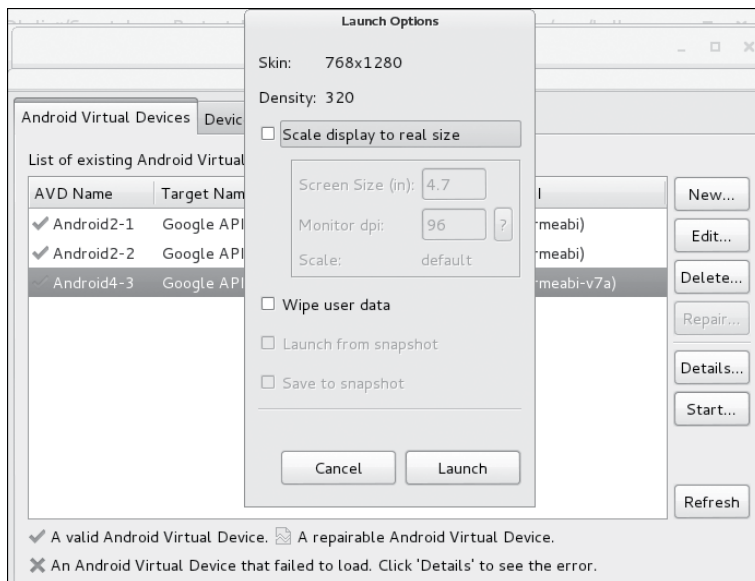


Figura 1.18 – Iniciando um emulador de Android.

Pode ser que sejam necessários alguns minutos para que o emulador seja iniciado da primeira vez, mas, uma vez que isso seja feito, você deverá ter algo que se parece muito com um dispositivo Android de verdade. O emulador do Android 4.3 está sendo mostrado na figura 1.19.



Figura 1.19 – Emulador do Android 4.3.

NOTA Para executar os emuladores de Android no Kali, é provável que seja necessário aumentar o desempenho de sua máquina virtual aumentando a sua RAM e os (núcleos *core*) de CPU. Posso executar todos os três emuladores com 3 GB de RAM e dois cores de CPU alocados no Kali. Essas alterações podem ser feitas nas configurações da máquina virtual em seu produto VMware. O nível de eficiência proporcionado ao Kali dependerá, é claro, dos recursos disponíveis em seu computador host. Como alternativa, em vez de executar os emuladores de Android no Kali Linux, você pode instalar o Android e os emuladores em seu sistema host ou até mesmo em outro sistema na rede local. Os exercícios do capítulo 20 funcionarão, desde que os emuladores possam se comunicar com o Kali.

Smartphone Pentest Framework

A seguir, faça o download e instale o Smartphone Pentest Framework (SPF), que usaremos para atacar dispositivos móveis. Utilize o comando `git` para fazer o download do código-fonte. Vá para o diretório *Smartphone-Pentest-Framework* baixado, como mostrado aqui:

```
root@kali:~# git clone -b SPFBook https://github.com/georgiaw/Smartphone-Pentest-Framework.git
root@kali:~# cd Smartphone-Pentest-Framework
```

Agora abra o arquivo *kaliinstall* no editor de texto nano. As primeiras linhas estão sendo mostradas na listagem 1.5. Observe as linhas que se referem a */root/adt-bundle-linux-x86-20131030/sdk/tools/android*. Se o nome da pasta de seu ADT bundle for diferente (por causa da disponibilização de uma versão mais recente), altere esse valor para que corresponda ao local correto em que você instalou o Android ADT na seção anterior.

Listagem 1.5 – Instalando o Smartphone Pentest Framework

```
root@kali:~/Smartphone-Pentest-Framework# nano kaliinstall
#!/bin/sh
## Instala os pacotes necessários
echo -e "$(tput setaf 1)\nInstallin serialport, dbdpg, and expect for perl\n"; echo "$(tput sgr0)"
echo -e "$(tput setaf 1)#####\n"; echo "$(tput sgr0)"
echo $cwd;
#apt-get -y install libexpect-perl libdbd-pg-perl libdevice-serialport-perl;
apt-get install ant
/root/adt-bundle-linux-x86-20131030/sdk/tools/android update sdk --no-ui --filter android-4 -a
/root/adt-bundle-linux-x86-20131030/sdk/tools/android update sdk --no-ui --filter addon-google_
apis-google-4 -a
/root/adt-bundle-linux-x86-20131030/sdk/tools/android update sdk --no-ui --filter android-14 -a
/root/adt-bundle-linux-x86-20131030/sdk/tools/android update sdk --no-ui --filter addon-google_
apis-google-14 -a
--trecho omitido--
```

Agora execute o script *kaliinstall*, como mostrado aqui:

```
root@kali:~/Smartphone-Pentest-Framework# ./kaliinstall
```

Isso fará o SPF ser instalado, o qual será usado no capítulo 20.

Por fim, devemos fazer mais uma alteração no arquivo de configuração do SPF. Vá para o diretório *Smartphone-Pentest-Framework/frameworkconsole* e abra o arquivo *config* no nano. Procure a opção *#LOCATION OF ANDROID SDK*. Se o nome da pasta de seu ADT bundle mudar em relação à versão corrente na época desta publicação, altere-o de acordo com essa mudança na linha que começa com *ANDROIDSDK=*.

```
root@kali:~/Smartphone-Pentest-Framework# cd frameworkconsole/
root@kali:~/Smartphone-Pentest-Framework/frameworkconsole# nano config
--trecho omitido--
#LOCATION OF ANDROID SDK
ANDROIDSDK = /root/adt-bundle-linux-x86-20131030/sdk
--trecho omitido--
```

Máquinas virtuais-alvo

Usaremos três computadores-alvo criados de forma personalizada para simular vulnerabilidades frequentemente encontradas em ambientes de cliente; usaremos o Ubuntu 8.10, o Windows XP SP3 e o Windows 7 SP1.

Você encontrará um link para um torrent que contém a máquina virtual Ubuntu em <http://www.nostarch.com/pentesting/>. O sistema-alvo está compactado por meio da compressão 7-Zip e *1stPentestBook?!* é a senha do arquivo. Você pode usar programas 7-Zip para abrir os arquivos compactados em todas as plataformas. Para os pacotes Windows e Linux, utilize <http://www.7-zip.org/download.html>; para o Mac OS, use Ez7z, disponível em <http://ez7z.en.softonic.com/mac/>. O arquivo compactado estará pronto para ser usado assim que for descompactado.

Para instalar as máquinas virtuais Windows, será preciso instalar e configurar o Windows XP SP3 e o Windows 7 SP1 para 32 bits. As fontes para a mídia de instalação incluem o TechNet e o MSDN (o Microsoft Developer Network), entre outras. (Você poderá usar suas máquinas virtuais Windows como trial durante 30 dias, sem uma chave de licença.)

Criando o alvo Windows XP

O seu alvo Windows XP deve ser constituído de uma instalação básica do Windows XP SP3, sem nenhuma atualização adicional de segurança. (Acesse o meu site em <http://www.bulbsecurity.com/> para obter mais informações sobre como encontrar uma cópia do Windows XP.) Depois que você tiver uma cópia do Windows XP SP3, aqui está o modo de instalá-lo no Microsoft Windows ou no Mac OS.

VMware Player no Microsoft Windows

Para instalar o Windows XP no VMware Player para Windows:

1. Selecione **Create A New Virtual Machine** (Criar uma nova máquina virtual) no VMware Player e aponte o New Virtual Machine Wizard (Assistente para nova máquina virtual) para o disco de instalação ou a imagem ISO do Windows XP. De acordo com o seu disco fonte ou a imagem, você terá a opção de usar o Easy Install (se você estiver instalando uma versão com uma chave de licença), ou poderá ver um aviso em um triângulo amarelo que diz: "Could not detect which operating system is in this disc image."

You will need to specify which operating system will be installed.” (Não foi possível detectar o sistema operacional que está nessa imagem de disco. Será necessário especificar o sistema operacional que será instalado). Nesse último caso, basta clicar em **Next** (Próximo).

2. No diálogo **Select a Guest Operating System** (Selecionar um sistema operacional guest), selecione **Microsoft Windows** na seção **Guest operating system** (Sistema operacional Guest) e a sua versão do Windows XP na caixa suspensa, como mostrado na figura 1.20, e clique em **Next** (Próximo).

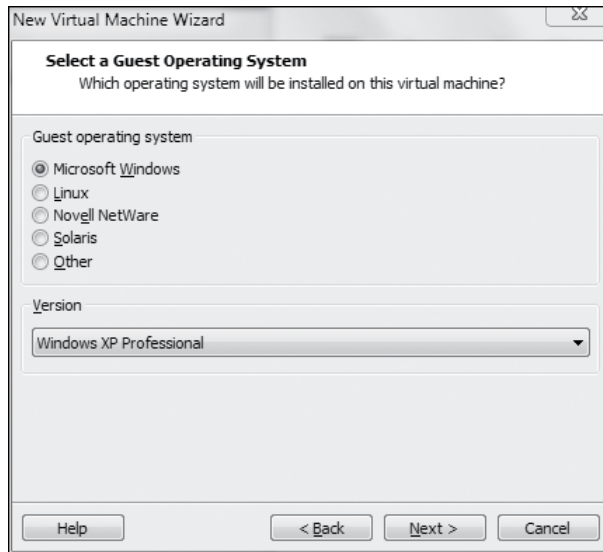


Figura 1.20 – Selecionando a sua versão de Windows XP.

3. No próximo diálogo, digite **Bookxp XP SP3** para o nome de sua máquina virtual e clique em **Next**.
4. No diálogo **Specify Disk Capacity** (Especificar a capacidade do disco), aceite o tamanho recomendado para o disco rígido de sua máquina virtual, que é de 40 GB, e selecione a opção **Store virtual disk as a single file** (Armazenar o disco virtual como um único arquivo), conforme mostrado na figura 1.21, e clique em **Next**.

NOTA A máquina virtual não ocupará todos os 40 GB; ela ocupará somente o espaço em seu disco rígido à medida que for necessário. Esse é somente um valor máximo.

5. No diálogo **Ready to Create Virtual Machine** (Pronto para criar a máquina virtual), mostrado na figura 1.22, clique em **Customize Hardware** (Personalizar o hardware).

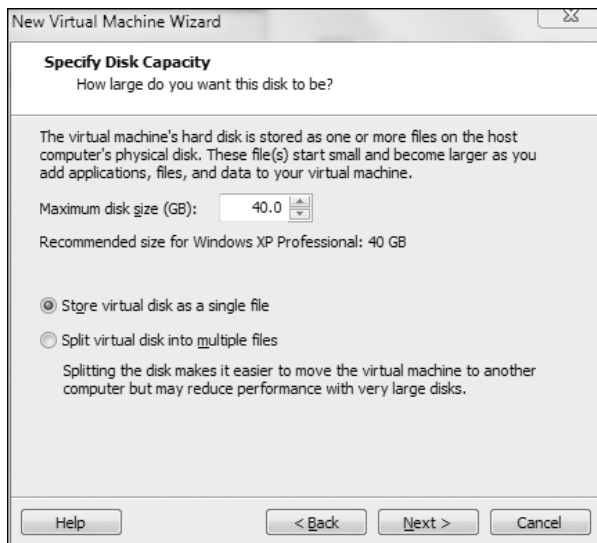


Figura 1.21 – Especificando a capacidade do disco.

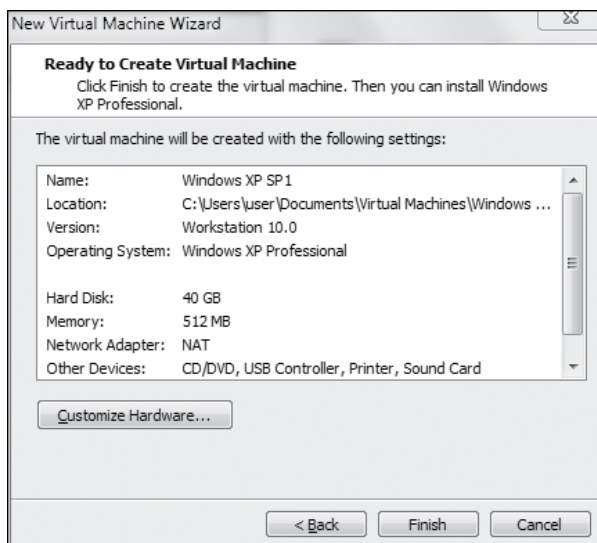


Figura 1.22 – Personalizando o seu hardware.

6. No diálogo **Hardware**, selecione **Network Adapter** (Adaptador de rede), e no campo **Network Connection** (Conexão de rede) que for apresentado, selecione **Bridged: Connected directly to the physical network** (Com bridge: conectado diretamente à rede física). Em seguida, clique em **Configure Adapters** (Configurar adaptadores) e selecione o adaptador que você estiver usando para se conectar com a Internet, como mostrado na figura 1.23. Então clique em **OK**, em **Close** (Fechar) e em **Finish** (Finalizar).

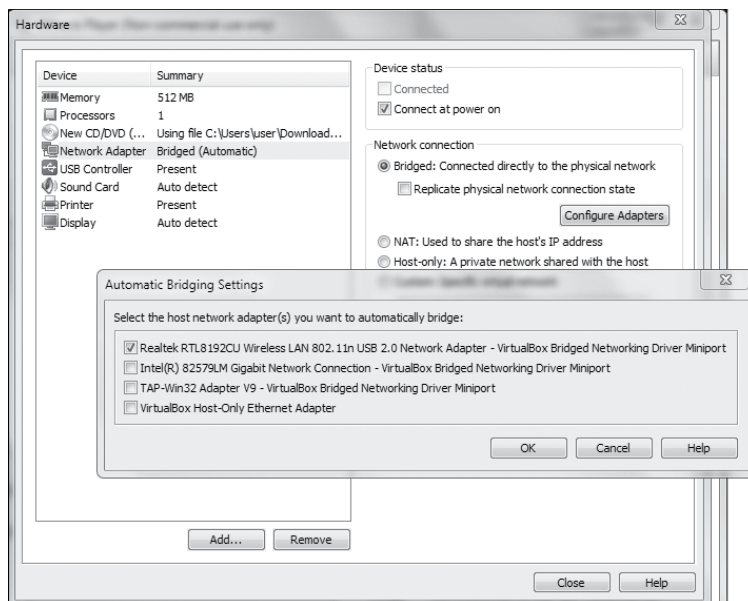


Figura 1.23 – Configurando o seu adaptador de rede como bridged (com bridge).

Agora você deverá ser capaz de executar a sua máquina virtual Windows XP. Continue com as instruções para a instalação e a ativação do Windows XP em “Instalando e ativando o Windows” na página 63.

VMware Fusion no Mac OS

No VMware Fusion, acesse **File ► New ► Import from disk or image** (Arquivo ► Novo ► Importar de disco ou de imagem) e aponte-o para o disco de instalação ou para a imagem do Windows XP, conforme mostrado na figura 1.24.

Siga os prompts para criar uma nova instalação do Windows XP SP3.

Instalando e ativando o Windows

Como parte do processo de instalação, você será solicitado a fornecer uma chave de licença do Windows. Se tiver uma, digite-a aqui. Caso contrário, você poderá usar a máquina virtual como trial durante 30 dias. Para prosseguir sem fornecer uma chave de licença, clique em **Next** (Próximo) quando uma chave for solicitada. Uma janela pop-up avisará que o fornecimento de uma chave de licença é recomendado e perguntará se você gostaria de fornecer uma agora, como mostrado na figura 1.25. Basta clicar em **No** (Não).

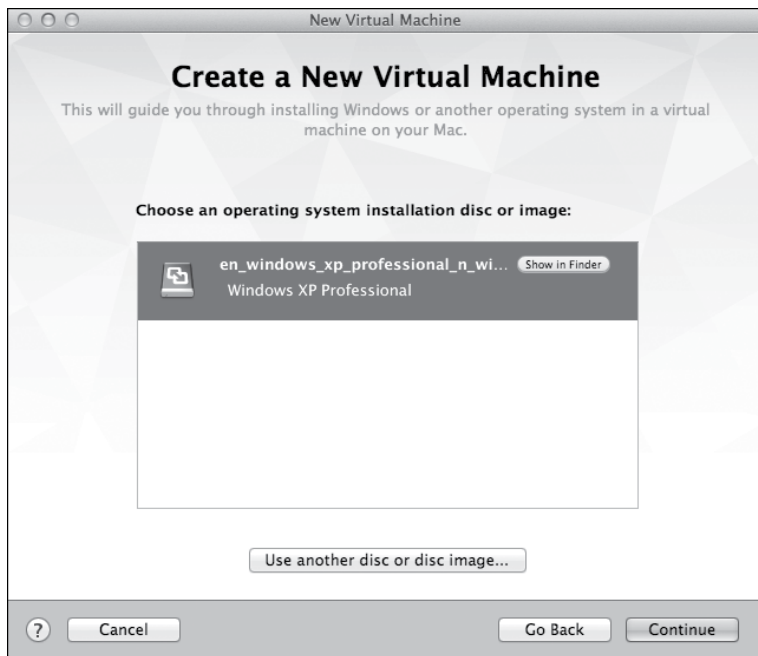


Figura 1.24 – Criando uma nova máquina virtual.

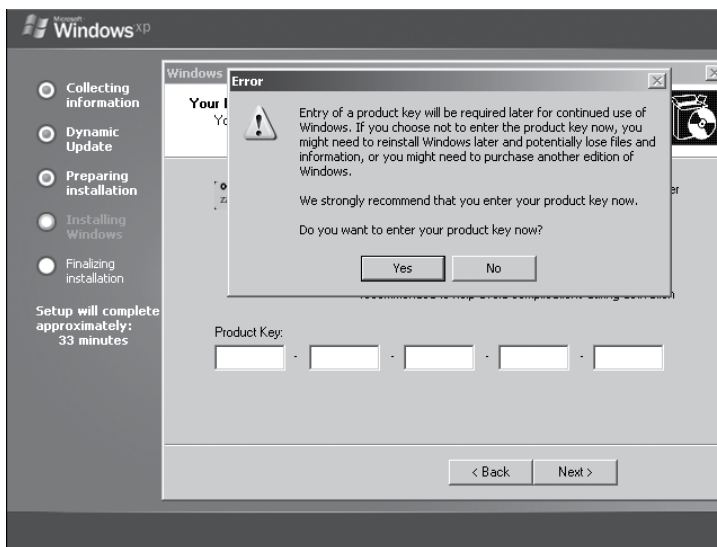


Figura 1.25 – Diálogo para a chave de licença.

Como mostrado na figura 1.26, quando solicitado, defina **Computer name** (Nome do computador) para **Bookxp**. Configure **Administrator password** (Senha do administrador) com **password**.



Figura 1.26 – Definindo o nome do computador e a senha de administrador.

Você pode deixar as configurações de data/hora e de TCP/IP com seus valores defaults, quando solicitado a fornecê-las. De modo semelhante, deixe o alvo Windows XP como parte do grupo de trabalho WORKGROUP, em vez de associá-lo a um domínio, conforme mostrado na figura 1.27.

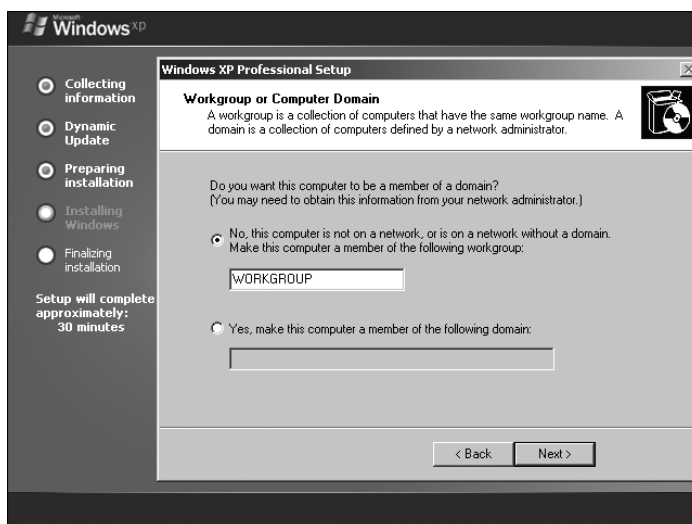


Figura 1.27 – Configurações do grupo de trabalho.

Informe ao Windows para não instalar automaticamente as atualizações de segurança, conforme mostrado na figura 1.28. Esse passo é importante, pois alguns dos exploits que executaremos dependem da ausência de patches no Windows.



Figura 1.28 – Desativando as atualizações automáticas de segurança.

Então você será solicitado a ativar o Windows. Se uma chave de licença foi fornecida, vá em frente e ative-o. Do contrário, você poderá selecionar **No, remind me every few days** (Não, lembrar mais tarde), como mostrado na figura 1.29.



Figura 1.29 – Ativando o Windows.

Agora crie as contas de usuário *georgia* e *secret*, conforme mostrado na figura 1.30. Criaremos senhas para esses usuários depois que a instalação estiver concluída.



Figura 1.30 – Adicionando usuários.

Quando o Windows iniciar, faça login como o usuário *georgia*, sem fornecer uma senha.

Instalando o VMware Tools

Agora instale o VMware Tools, que facilitará o uso de sua máquina virtual, por exemplo, ao permitir que você copie/cole e arraste programas para a máquina virtual a partir do sistema host.

VMware Player no Microsoft Windows

No VMware Player, instale o VMware Tools a partir de **Player ► Manage ► Install VMware Tools** (Player ► Administração ► Instalar o VMware Tools), conforme mostrado na figura 1.31. O instalador do VMware Tools deverá ser executado automaticamente no Windows XP.

VMware Fusion no Mac OS

Instale o VMware Tools a partir de **Virtual Machines ► Install VMware Tools** (Máquinas virtuais ► Instalar o VMware Tools), conforme mostrado na figura 1.32. O instalador do VMware Tools deverá ser executado automaticamente no Windows XP.



Figura 1.31 – Instalando o VMware Tools no VMware Player.



Figura 1.32 – Instalando o VMware Tools no VMware Fusion.

Desativando o Windows Firewall

Agora abra o Control Panel (Painel de controle) a partir no menu **Start** (Iniciar) do Windows. Clique em **Security Center** ► **Windows Firewall** (Central de segurança ► Firewall do Windows) para desativar o firewall do Windows, como mostrado na figura 1.33.



Figura 1.33 – Desativando o firewall do Windows.

Configurando as senhas dos usuários

Novamente no **Control Panel** (Painel de controle), acesse **User Accounts** (Contas de usuário). Clique no usuário **georgia** e selecione **Create a password** (Criar uma senha). Configure a senha de **georgia** para **password**, como mostrado na figura 1.34. Faça o mesmo para o usuário **secret**, porém defina a senha desse usuário como **Password123**.

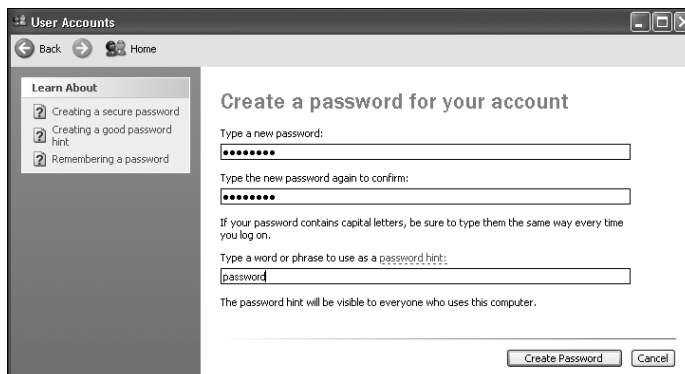


Figura 1.34 – Configurando a senha de um usuário.

Configurando um endereço IP estático

A seguir, defina um endereço IP estático para que suas informações de rede não se alterem à medida que você trabalhar neste livro. Entretanto, inicialmente, devemos descobrir o endereço de nosso gateway default.

Certifique-se de que o seu sistema Windows XP esteja configurado para usar uma rede com bridge no VMware. Por padrão, sua máquina virtual irá obter automaticamente um endereço IP usando o DHCP.

Para descobrir o gateway default, abra um prompt de comandos do Windows acessando **Start ▶ Run** (Iniciar ▶ Executar), digite **cmd** e clique em **OK**. No prompt de comandos, digite **ipconfig**. Isso fará as informações de rede serem apresentadas, incluindo o gateway default.

```
C:\Documents and Settings\georgia>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : XXXXXXXX
    IP Address. . . . . : 192.168.20.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.20.1

C:\Documents and Settings\georgia>
```

No meu caso, o endereço IP é 192.168.20.10, a máscara de sub-rede é 255.255.255.0 e o gateway default é 192.168.20.1.

1. No Control Panel (Painel de controle), acesse **Network and Internet Connections** (Conexões de rede e de Internet) e clique em **Network Connections** (Conexões de rede) na parte inferior da tela.
2. Clique com o botão direito do mouse em **Local Area Connection** (Conexão local) e selecione **Properties** (Propriedades).
3. Selecione **Internet Protocol (TCP/IP)** e selecione **Properties** (Propriedades). Agora digite um endereço IP estático e defina a máscara de sub-rede e o gateway default para que estejam de acordo com os dados descobertos por meio do comando **ipconfig**, como mostrado na figura 1.35. Defina Preferred DNS server (Servidor DNS de preferência) com o seu gateway default também.

Agora é hora de verificar se nossas máquinas virtuais podem se comunicar. Depois que você tiver certeza de que as configurações estão corretas, retorne à máquina virtual Kali (inicie-a, caso você a tenha desligado) e digite **ping <endereço IP estático de sua máquina virtual Windows XP>**, como mostrado aqui.

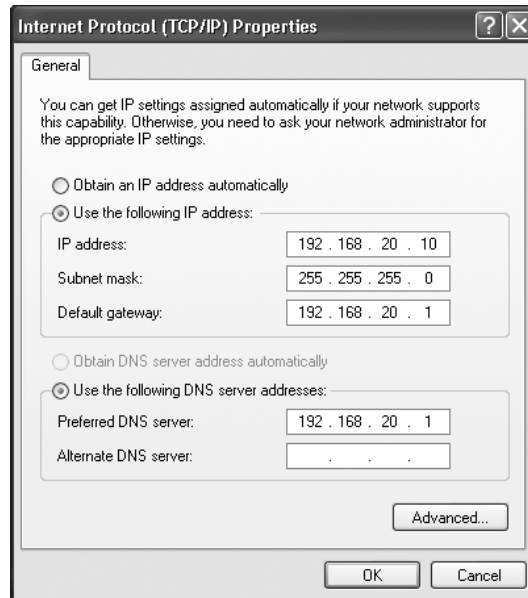


Figura 1.35 – Configurando um endereço IP estático.

NOTA O meu endereço IP é 192.168.20.10. Ao longo do livro, você deverá substituir esse valor pelo endereço IP de seus sistemas.

```
root@kali:~# ping 192.168.20.10
PING 192.168.20.10 (192.168.20.10) 56(84) bytes of data.
64 bytes from 192.168.20.10: icmp_req=1 ttl=128 time=3.06 ms
^C
```

Tecla **Ctrl-C** para interromper o comando ping. Se você vir uma saída que comece com 64 bytes from <endereço ip do XP>, como mostrado anteriormente, suas máquinas virtuais poderão se comunicar. Parabéns! Você configurou uma rede de máquinas virtuais.

Se, em vez disso, você vir uma mensagem que inclua o texto *Destination Host Unreachable* (Host destino inacessível), verifique se há problemas em sua rede: certifique-se de que suas máquinas virtuais estão na mesma rede virtual com bridge, verifique se o seu gateway default está correto e assim por diante.

Fazendo o XP atuar como se fosse membro de um domínio Windows

Por fim, devemos modificar uma configuração do Windows XP para que ele se comporte como se fosse membro de um domínio Windows, como ocorrerá com muitos de seus clientes. Não farei você configurar todo um domínio Windows aqui, porém, durante a fase de pós-exploração de falhas, alguns exercícios simularão um ambiente de domínio. Volte para a sua máquina virtual XP e siga os passos a seguir:

1. Selecione **Start ▶ Run** (Iniciar ▶ Executar) e digite **secpol.msc** para abrir o painel **Local Security Settings** (Configurações locais de segurança).
2. Expanda **Local Policies** (Políticas locais) à esquerda e dê um clique duplo em **Security Options** (Opções de segurança) à direita.
3. Na lista **Policy** (Políticas) no painel à direita, dê um clique duplo em **Network access: Sharing and security model for local accounts** (Acesso à rede: modelo de compartilhamento e de segurança para contas locais) e selecione **Classic – local users authenticate as themselves** (Clássico – usuários locais se autenticam como eles mesmos) na lista suspensa, como mostrado na figura 1.36.

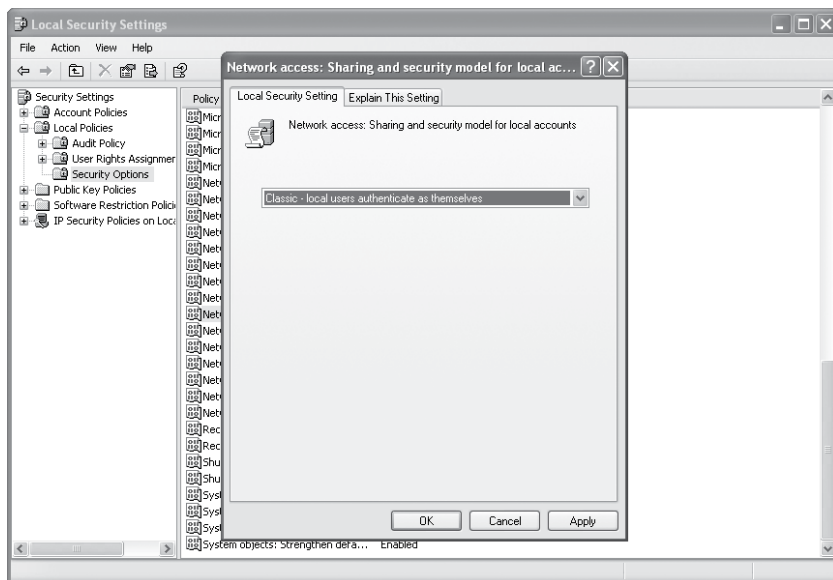


Figura 1.36 – Alterando uma configuração local de segurança para que seu alvo atue como membro de um domínio Windows.

4. Clique em **Apply** (Aplicar) e, em seguida, em **OK**.
5. Feche qualquer janela que estiver aberta em sua máquina virtual.

Instalando softwares vulneráveis

Nesta seção, instalaremos alguns softwares vulneráveis em sua máquina virtual Windows XP. Atacaremos esses softwares em capítulos posteriores. Abra a sua máquina virtual Windows XP e, enquanto continua logado com o usuário *georgia*, siga as instruções para instalar cada um dos pacotes listados aqui:

Zervit 0.4

Faça download do Zervit versão 0.4 a partir de <http://www.exploit-db.com/exploits/12582/>. (Clique na opção Vulnerable App para fazer o download dos arquivos.) Descompacte o arquivo baixado e dê um clique duplo no programa Zervit para abri-lo e executá-lo. Em seguida, digite o número de porta 3232 no console quando o software iniciar. Responda **Y** para permitir a listagem de diretórios, como mostrado na figura 1.37. O Zervit não será reiniciado automaticamente quando você fizer o boot do Windows XP novamente, portanto será necessário reiniciá-lo caso isso ocorra.

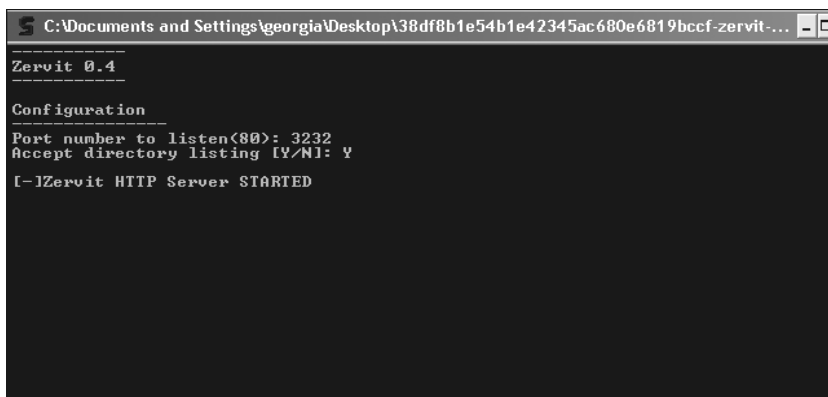


Figura 1.37 – Iniciando o Zervit 0.4.

SLMail 5.5

Faça o download e execute o SLMail versão 5.5 a partir de <http://www.exploit-db.com/exploits/638/>, usando as opções default quando solicitado. Basta clicar em **Next** (Próximo) para todas as opções, sem alterar nada. Se você vir um aviso sobre um nome de domínio, basta ignorá-lo e clicar em **OK**. Não precisamos realmente enviar nenhum email nesse caso.

Depois que o SLMail estiver instalado, reinicie a sua máquina virtual. Em seguida, abra **Start ▶ All Programs ▶ SL Products ▶ SLMail ▶ SLMail Configuration** (Iniciar ▶ Todos os programas ▶ Produtos SL ▶ SLMail ▶ Configurações do SLMail). Na aba **Users** (Usuários) default, clique com o botão direito do mouse na janela **SLMail Configuration** (Configurações do SLMail) e selecione **New ▶ User** (Novo ▶ Usuário), como mostrado na figura 1.38.

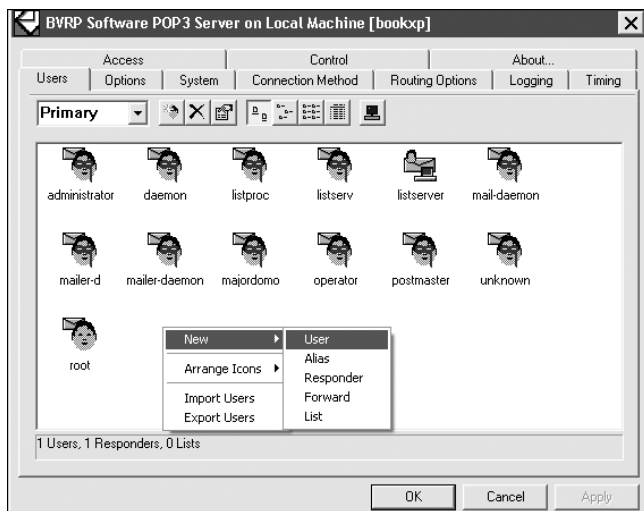


Figura 1.38 – Adicionando um usuário ao SLMail.

Clique no ícone do usuário que acabou de ser criado, insira o nome do usuário **georgia** e preencha as informações para esse usuário, como mostrado na figura 1.39. O nome do mailbox deve ser *georgia*, com senha igual a *password*. Mantenha os valores default e clique em **OK** após terminar.

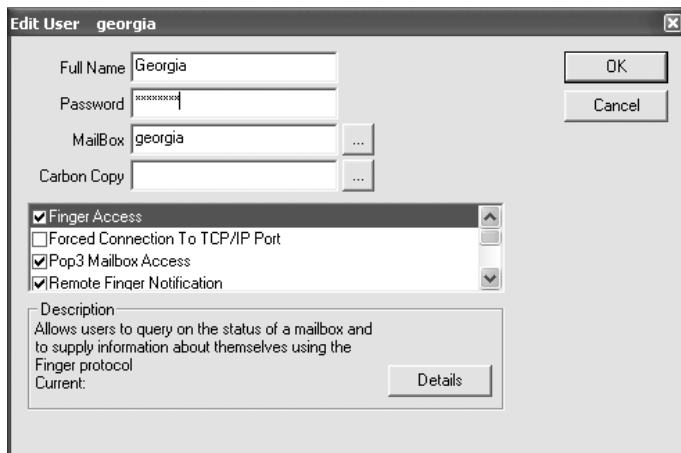


Figura 1.39 – Configurando as informações do usuário no SLMail.

3Com TFTP 2.0.1

Em seguida, faça o download de 3Com TFTP versão 2.0.1, que está na forma de um arquivo compactado, a partir de <http://www.exploit-db.com/exploits/3388/>. Extraia os arquivos e copie *3CTftpSvcCtrl* e *3CTftpSvc* para o diretório *C:\Windows*, como mostrado na figura 140.

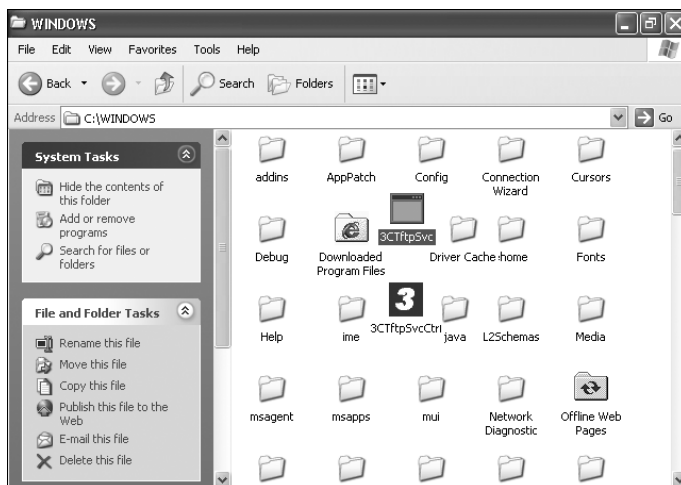


Figura 140 – Copiando o 3Com TFTP para C:\Windows.

Em seguida, abra *3CTftpSvcCtrl* (o ícone 3 azul) e clique em **Install Service** (Instalar o serviço), conforme mostrado na figura 141.

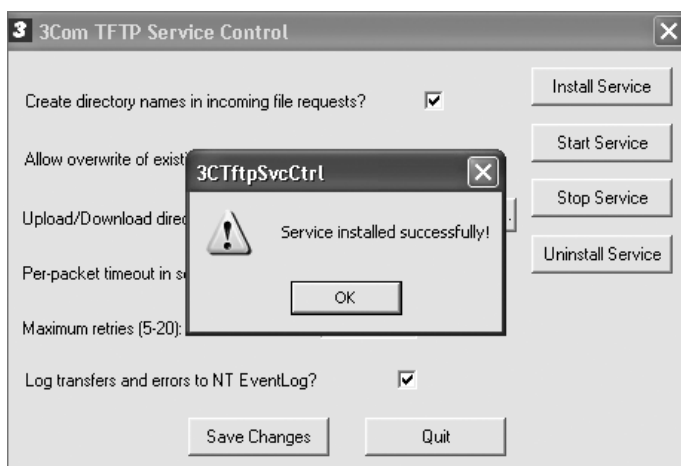


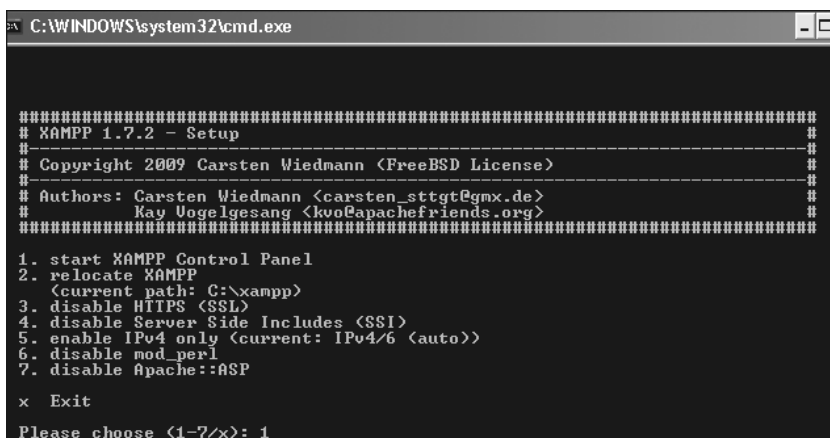
Figura 141 – Instalando o 3Com TFTP.

Clique em **Start Service** (Iniciar o serviço) para iniciar o 3Com TFTP pela primeira vez. A partir de agora, ele será iniciado automaticamente quando você fizer o boot do computador. Clique em **Quit** para sair.

XAMPP 1.7.2

Agora iremos instalar uma versão mais antiga do software XAMPP, a versão 1.7.2, a partir de http://www.oldapps.com/xampp.php?old_xampp=45/. (A versão mais antiga do Internet Explorer no Windows XP parece ter alguns problemas para abrir essa página.) Se você tiver problemas, faça o download do software a partir de seu sistema host e copie-o para o desktop do Windows XP.

1. Execute o instalador e aceite as opções default conforme elas forem apresentadas a você. Quando a instalação estiver concluída, selecione a opção **1. start XAMPP Control Panel** (1. iniciar o Painel de controle do XAMPP), como mostrado na figura 1.42.



```
C:\WINDOWS\system32\cmd.exe

#####
# XAMPP 1.7.2 - Setup
# -----
# Copyright 2009 Carsten Wiedmann <FreeBSD License>
# -----
# Authors: Carsten Wiedmann <carsten_stt@tgm.de>
#          Kay Vogelgesang <kvo@apache-friends.org>
# -----
1. start XAMPP Control Panel
2. relocate XAMPP
   <current path: C:\xampp>
3. disable HTTPS (SSL)
4. disable Server Side Includes (SSI)
5. enable IPv4 only <current: IPv4/6 <auto>>
6. disable mod_perl
7. disable Apache::ASP
x Exit
Please choose (1-7/x): 1
```

Figura 1.42 – Iniciando o XAMPP Control Panel (Painel de controle do XAMPP).

2. No XAMPP Control Panel, instale os serviços Apache, MySQL e FileZilla (marque a caixa de seleção **Svc** à esquerda do nome do serviço). Em seguida, clique no botão **Start** (Iniciar) de cada serviço. Sua tela deverá ter a aparência mostrada na figura 1.43.
3. Clique no botão **Admin** para o FileZilla no XAMPP Control Panel. O painel Admin está sendo mostrado na figura 1.44.
4. Acesse **Edit ► Users** (Editar ► Usuários) para abrir o diálogo **Users** (Usuários), mostrado na figura 1.45.

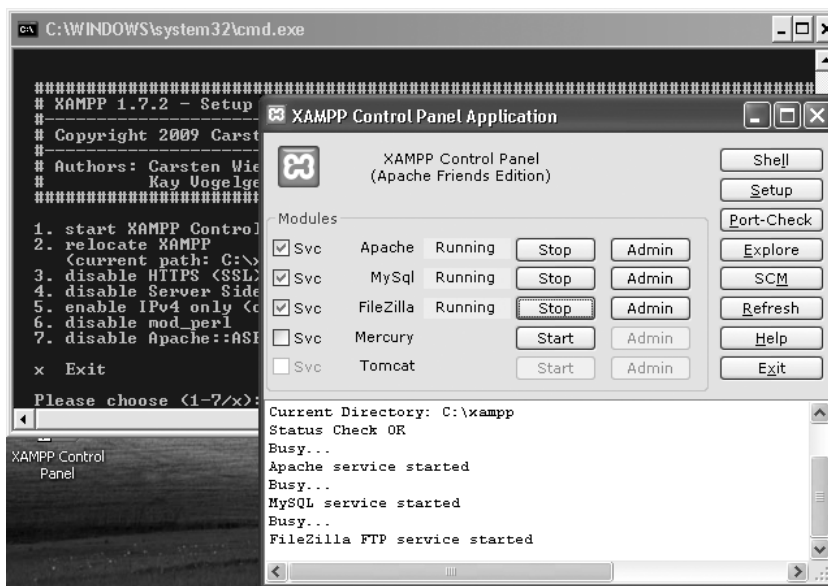


Figura 143 – Instalando e iniciando os serviços XAMPP.

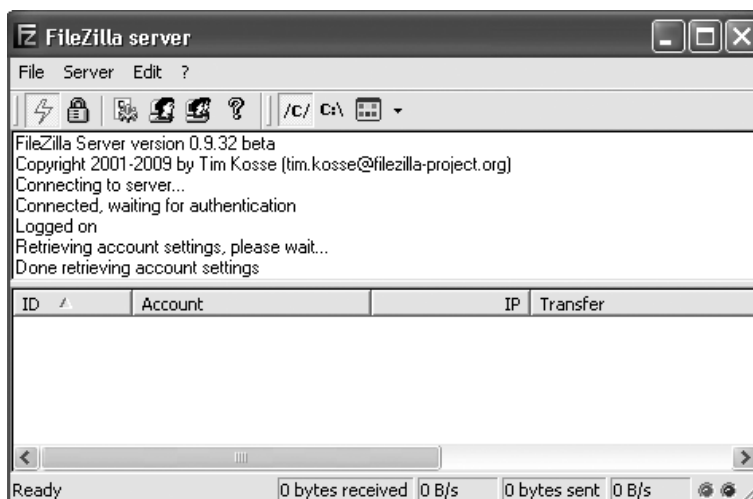


Figura 144 – O painel Admin do FileZilla.

5. Clique no botão **Add** (Adicionar) à direita da caixa de diálogo.
6. Na caixa de diálogo Add User Account (Adicionar conta de usuário), digite **georgia** e clique em **OK**.
7. Com **georgia** selecionado, marque a caixa **Password** (Senha) em **Account Settings** (Configurações da conta) e digite **password**.

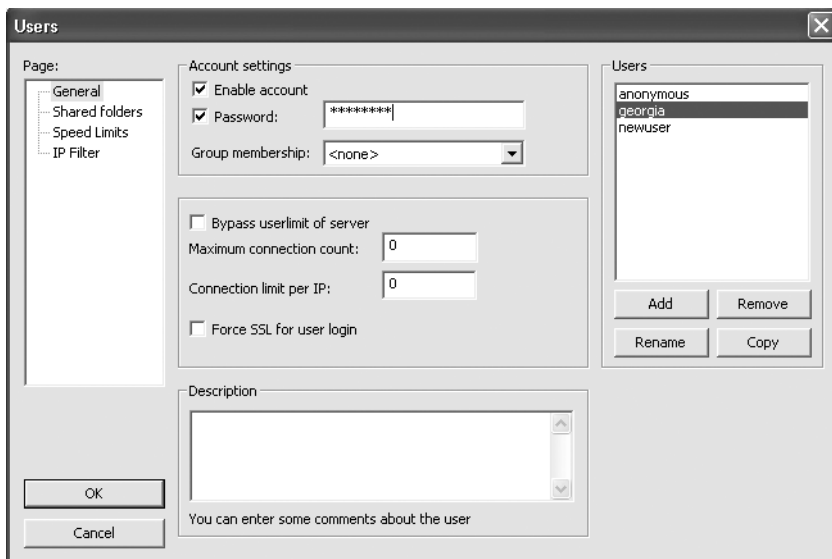


Figura 1.45 – Adicionando um usuário de FTP.

Clique em **OK**. Quando solicitado a compartilhar uma pasta, vá até a pasta *Documents* de *georgia* no Windows e selecione-a para compartilhá-la, conforme mostrado na figura 1.46. Deixe os valores default para todas as demais caixas de seleção, como mostrado na figura. Clique em **OK** após ter terminado e saia das várias janelas abertas.

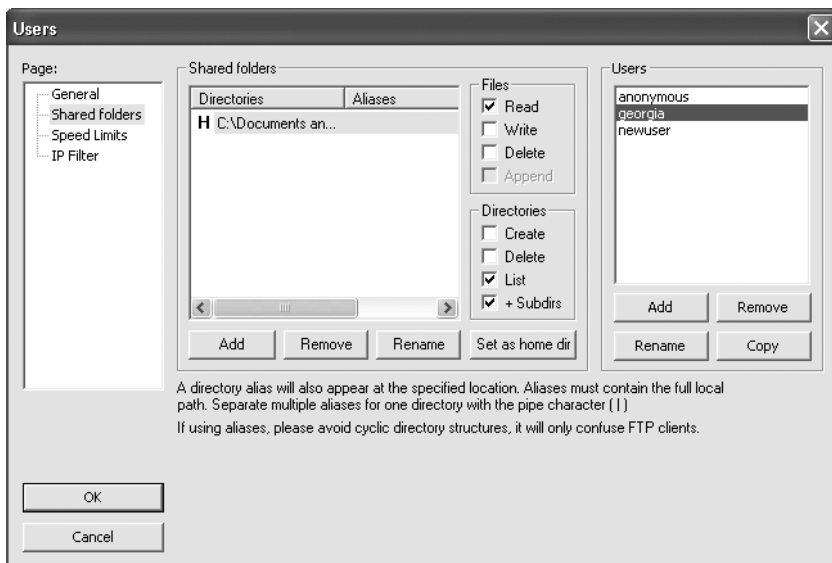


Figura 1.46 – Compartilhando uma pasta por meio de FTP.

Adobe Acrobat Reader

Agora instalaremos a versão 8.1.2 do Adobe Acrobat Reader a partir de http://www.oldapps.com/adobe_reader.php?old_adobe=17/. Siga os prompts default para instalá-lo. Após ter concluído, clique em **Finish** (Finalizar). (Nesse caso, novamente, pode ser que seja necessário fazer o download do arquivo em seu sistema host e copiá-lo para o desktop do Windows XP.)

War-FTP

A seguir, faça o download e instale a versão 1.65 do War-FTP a partir de <http://www.exploit-db.com/exploits/3570/>. Faça o download do executável de [exploit-db.com](http://www.exploit-db.com) para o desktop de *georgia* e execute o arquivo baixado para efetuar a instalação. Não é necessário iniciar o serviço FTP; iremos ativá-lo quando discutirmos o desenvolvimento de exploits nos capítulos de 16 a 19.

WinSCP

Faça o download e instale a versão mais recente do WinSCP a partir de <http://winscp.net/>. Selecione a opção **Typical Installation** (Instalação típica). Você pode desmarcar a seleção dos add-ons adicionais. Após ter concluído, clique em **Finish** (Finalizar).

Instalando o Immunity Debugger e o Mona

Agora iremos concluir a configuração da máquina virtual Windows XP ao instalar um depurador, que é uma ferramenta para ajudar a detectar erros em programas de computador. Usaremos o depurador nos capítulos referentes ao desenvolvimento de exploits. Acesse a página de registro do Immunity Debugger em http://debugger.immunityinc.com/ID_register.py. Preencha a página de registro e, em seguida, clique no botão **Download**. Execute o instalador.

Ao ser interrogado se você deseja instalar o Python, clique em **Yes** (Sim). Aceite o acordo de licença e siga os prompts default de instalação. Ao fechar o instalador, a instalação do Python será executada automaticamente. Utilize os valores default na instalação.

Depois que o Immunity Debugger e o Python estiverem instalados, faça o download do *mona.py* a partir de <http://redmine.corelanc.be/projects/mona/repository/raw/mona.py/>. Copie *mona.py* para *C:\Program Files\Immunity Inc\Immunity Debugger\PyCommands*, como mostrado na figura 1.47.

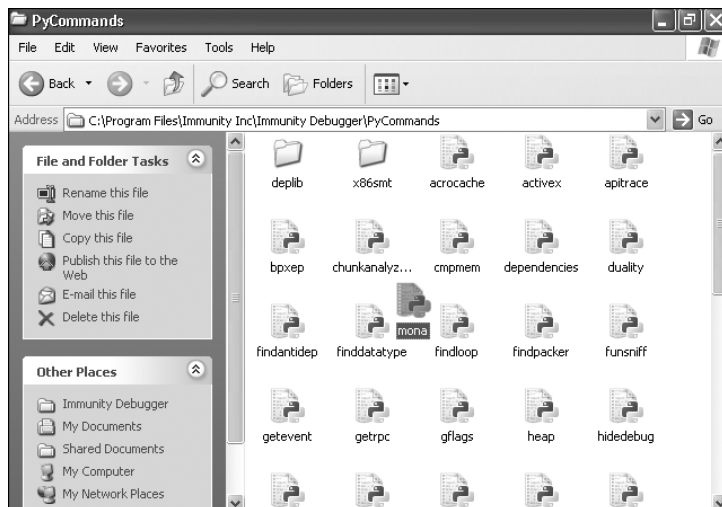


Figura 147 – Instalando o Mona.

Abra o Immunity Debugger e, no prompt de comandos na parte inferior da janela, digite **!mona config -set workingfolder c:\logs\%p**, como mostrado na figura 148. Esse comando diz ao mona para efetuar o log de sua saída em *C:\logs\<nome do programa>*, em que *<nome do programa>* corresponde ao programa que o Immunity Debugger estiver depurando no momento.

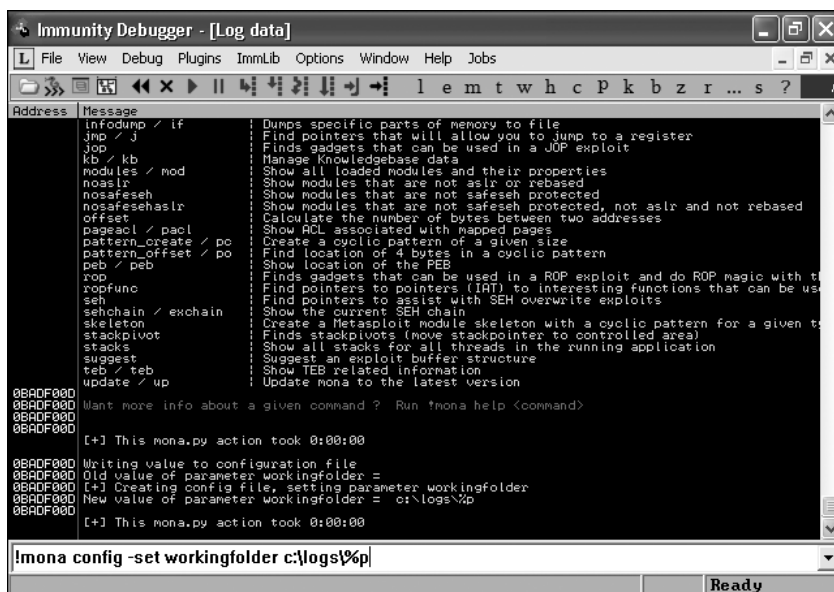


Figura 148 – Configurando os logs do Mona.

Agora o nosso alvo Windows XP está configurado e pronto para executar.

Instalando o alvo Ubuntu 8.10

Como o Linux tem código aberto, você pode simplesmente fazer o download da máquina virtual Linux como parte do torrent deste livro. Descompacte o arquivo *7-Zip BookUbuntu.7zip* e utilize a senha *1stPentestBook?!* para abrir o arquivo. Abra o arquivo *.vmx* no VMware. Se você vir uma mensagem que informe que a máquina virtual parece estar em uso, clique em **Take Ownership** (Assumir a propriedade) e, como ocorreu no Kali, selecione **I copied it** (Eu a copiei). O nome do usuário e a senha da máquina virtual propriamente dita são *georgia:password*.

Depois que tiver a máquina virtual Ubuntu carregada, certifique-se de que a interface de rede esteja definida com Bridged no VMware e clique no ícone de rede (os dois computadores) na parte superior à direita da tela para conectar a máquina virtual à rede. Não instale nenhuma atualização, se você for solicitado a fazê-lo. Como ocorre no Windows XP, iremos explorar softwares desatualizados nesse sistema. Agora essa máquina virtual está totalmente instalada. (Mostrarei como definir um endereço IP estático no Linux no capítulo 2.)

Criando o alvo Windows 7

Como ocorreu no Windows XP, será necessário instalar uma cópia do Windows 7 SP1 no VMware ao carregar a sua imagem ou o DVD. Uma versão trial de 30 dias do Windows 7 Professional SP1 32 bits funcionará bem, porém será necessário ativá-la após 30 dias se quiser continuar a usá-la. Para encontrar uma versão oficial do Windows 7 SP1, tente uma das opções a seguir:

- Acesse <http://www.softpedia.com/get/System/OS-Enhancements/Windows-7.shtml>.
- Acesse <http://technet.microsoft.com/en-us/evalcenter/dn407368>.

NOTA Sua escola ou o seu local de trabalho podem ter acesso a programas como o DreamSpark ou o BizSpark que dão acesso aos sistemas operacionais Windows. Você também pode dar uma olhada em meu site (<http://www.bulbsecurity.com/>) para obter mais recursos.

Criando uma conta de usuário

Após ter instalado o Windows 7 Professional SP1, desative a opção para efetuar atualizações de segurança e crie o usuário *Georgia Weidman* como administrador, com uma senha igual a *password*, conforme mostrado nas figuras 1.49 e 1.50.

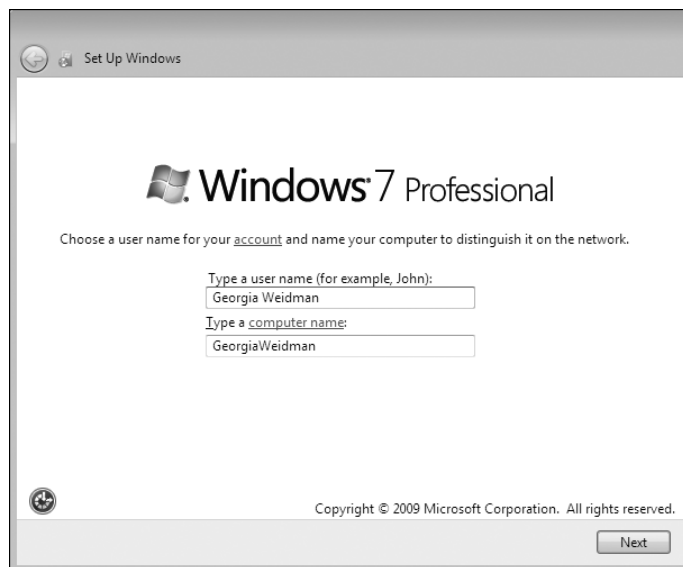


Figura 1.49 – Definindo um nome de usuário.

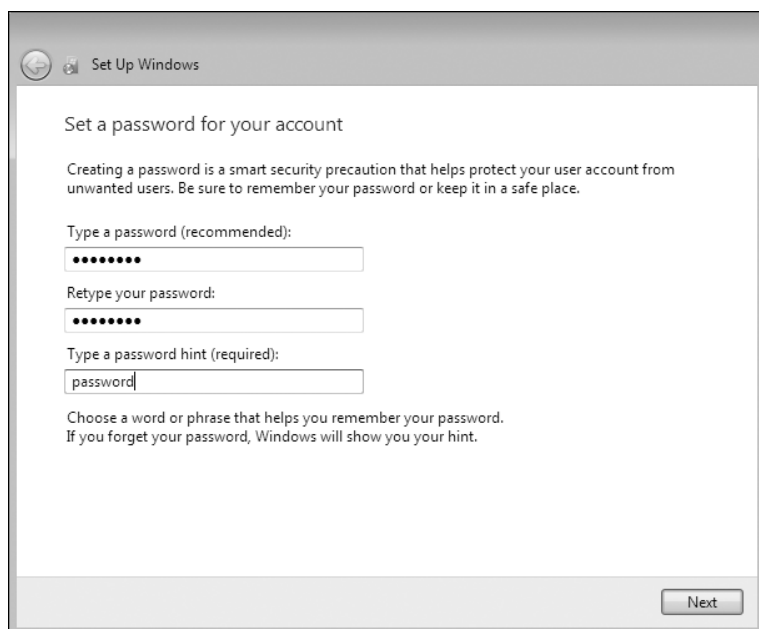


Figura 1.50 – Definindo uma senha para o usuário Georgia Weidman.

Novamente, desative as atualizações automáticas. Quando solicitado, defina o local corrente do computador para uma rede de trabalho. Após a instalação ter sido concluída, faça login com a conta *Georgia Weidman*. Deixe o **Windows Firewall** habilitado. O VMware fará a reinicialização do Windows 7 algumas vezes à medida que estiver instalando tudo.

Agora diga ao VMware para instalar o VMware Tools, como foi feito na seção sobre o Windows XP. Depois de ter instruído o VMware a instalar o VMware Tools na máquina virtual, se o instalador não for executado automaticamente, acesse **My Computer** (Meu computador) e execute o instalador do VMware Tools a partir do drive de DVD da máquina virtual, como mostrado na figura 1.51.

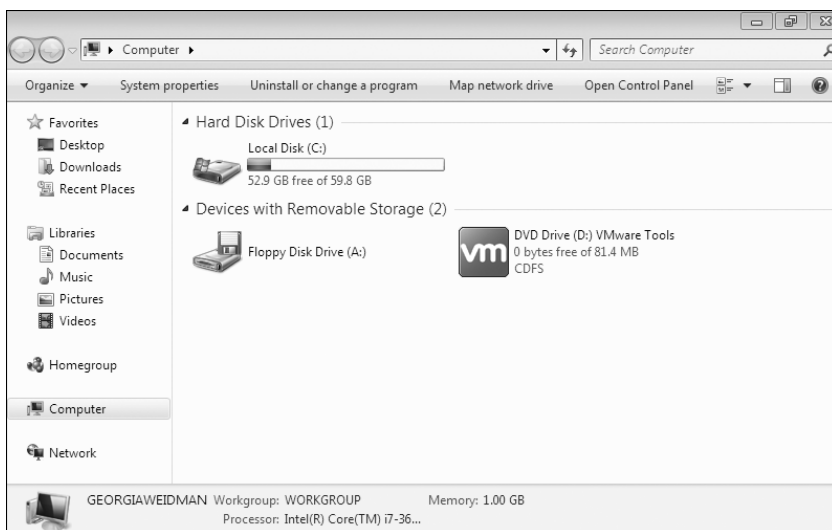


Figura 1.51 – Instalando o VMware Tools.

Desativando as atualizações automáticas

Apesar de nossos ataques ao Windows 7 contarem amplamente com falhas em softwares de terceiros, em vez de basear-se na ausência de patches do Windows, vamos, novamente, desativar as atualizações do Windows nessa máquina virtual. Para isso, acesse **Start ► Control Panel ► System and Security** (Iniciar ► Painel de Controle ► Sistema e Segurança). Em seguida, em Windows Update, clique em **Turn Automatic Updating On or Off** (Ativar ou desativar a atualização automática). Defina **Important updates** (Atualizações importantes) com **Never check for updates (not recommended)** [Nunca verificar se há atualização (não recomendado)], como mostrado na figura 1.52. Clique em **OK**.

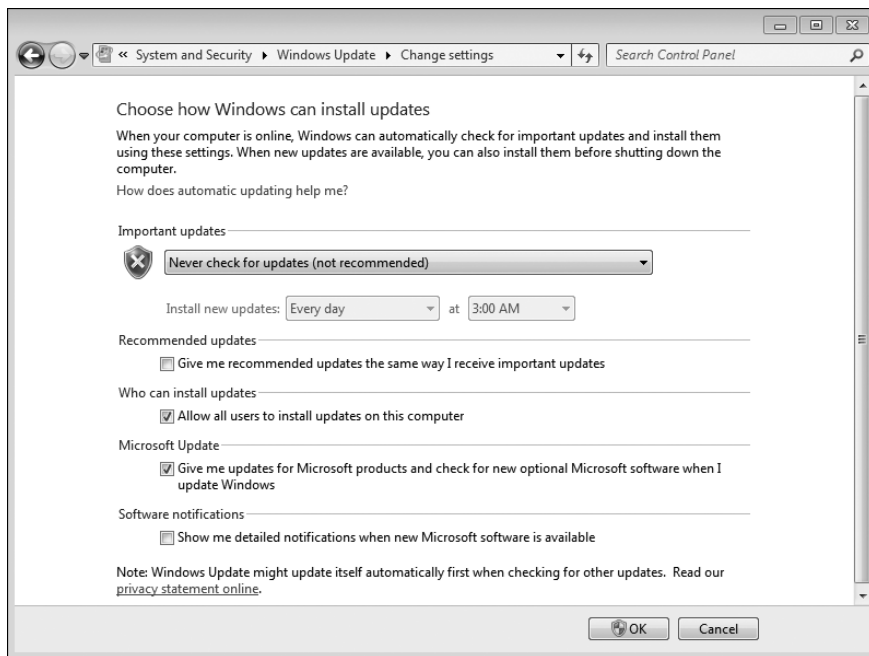


Figura 1.52– Desativando as atualizações automáticas.

Configurando um endereço IP estático

Configure um endereço IP estático ao selecionar **Start > Control Panel > Network and Internet > Network and Sharing Center > Change Adapter Settings > Local Area Network** (Iniciar > Painel de Controle > Rede e Internet > Central de rede e compartilhamento > Alterar as configurações do adaptador > Conexão local). Agora clique com o botão direito do mouse e selecione **Properties > Internet Protocol Version 4 (TCP/IPv4) > Properties** (Propriedades > Protocolo de Internet versão 4 (TCP/IPv4) > Propriedades). Configure esses valores conforme foi feito para o Windows XP (discutido em “Configurando um endereço IP estático” na página 70), porém utilize um valor diferente para o endereço IP do Windows 7, como mostrado na figura 1.53. Se você for solicitado a informar se deseja configurar essa rede como Home (Doméstica), Work (Trabalho) ou Public (Pública), selecione **Work**. (Certifique-se de que a configuração de rede de sua máquina virtual esteja definida para usar um adaptador com bridge.)

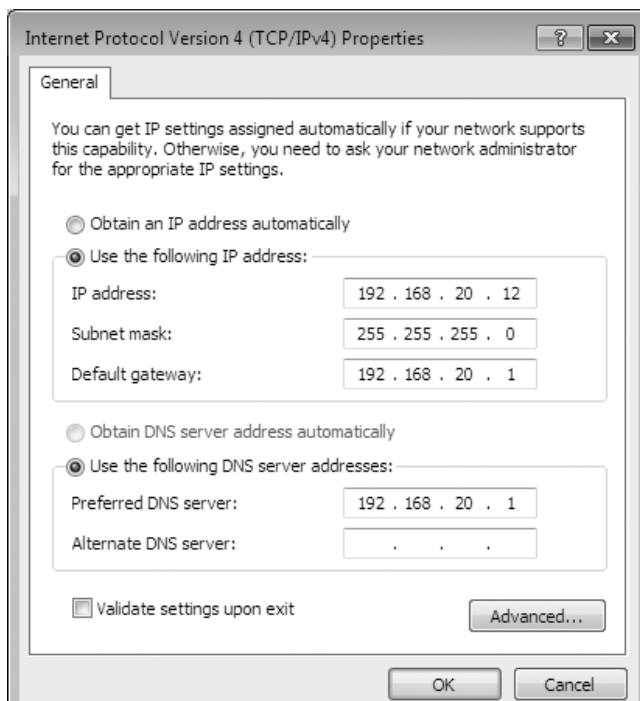


Figura 1.53– Configurando um endereço IP estático.

Pelo fato de o firewall do Windows estar ativado, o Windows 7 não responderá a um ping efetuado a partir do sistema Kali. Sendo assim, faremos o ping de nosso sistema Kali a partir do Windows 7. Inicie a sua máquina virtual Kali Linux e, a partir de sua máquina virtual Windows 7, clique no botão **Start** (Iniciar). Em seguida, digite **cmd** no diálogo **Run** (Executar) para abrir um prompt de comandos do Windows. No prompt, digite o seguinte:

```
ping <Endereço IP do Kali>
```

Se tudo estiver funcionando, você deverá ver respostas à solicitação ping, como descrito na seção “Configurando um endereço IP estático” na página 70.

Adicionando uma segunda interface de rede

Agora desligue a sua máquina virtual Windows 7. Iremos adicionar uma segunda interface de rede nessa máquina virtual, o que permitirá que o sistema Windows 7 faça parte de duas redes. Utilizaremos essa configuração durante a fase de pós-exploração de falhas para simular o ataque a sistemas adicionais em uma segunda rede.

No VMware Player do Microsoft Windows, selecione **Player ► Manage ► Virtual Machine Settings ► Add** (Player ► Administração ► Configurações da máquina virtual ► Adicionar), selecione **Network Adapter** (Adaptador de rede) e clique em **Next** (Próximo). Esse adaptador será o Network Adapter 2. No VMware Fusion no Mac OS, acesse **Virtual Machine Settings** (Configurações da máquina virtual), selecione **Add a Device** (Adicione um dispositivo) e selecione um adaptador de rede. Configure esse novo adaptador para a rede Host Only (Somente host). Clique em **OK**, e a máquina virtual deverá ser reiniciada. (Não é necessário configurar um endereço IP estático para o Network Adapter 2.) Quando a máquina virtual for iniciada, abra **Virtual Machine Settings** (Configurações da máquina virtual) novamente e você deverá ver os dois adaptadores de rede listados. Ambos deverão estar conectados quando o seu computador for ligado.

Instalando softwares adicionais

Agora instale os softwares a seguir em sua máquina virtual Windows 7 usando as configurações default ao longo do processo:

- O Java 7 Update 6, que é uma versão desatualizada do Java, a partir de http://www.oldapps.com/java.php?old_java=8120/.
- A versão 5.55 do Winamp a partir de http://www.oldapps.com/winamp.php?old_winamp=247/. (Remova a seleção para alterar a sua ferramenta de pesquisa e assim por diante.)
- A versão mais recente do Mozilla Firefox a partir de <http://www.mozilla.org/>.
- O Microsoft Security Essentials a partir de <http://windows.microsoft.com/en-us/windows/security-essentials-download/>. (Faça o download das assinaturas mais recentes de antivírus, garantindo que a versão correta será baixada para a sua instalação de 32 bits do Windows. Não ative a submissão automática de amostras nem o scan na instalação. Além disso, desative a proteção em tempo real, por enquanto. Ativaremos esse recurso quando estudarmos a maneira de evitar os softwares antivírus no capítulo 12. Essa configuração pode ser encontrada na aba **Settings** (Configurações) em **Real-time Protection** (Proteção em tempo real). Desmarque a seleção de **Turn on real-time protection (recommended)** [Ativar proteção em tempo real (recomendado)], conforme mostrado na figura 1.54. Clique em **Save changes** (Salvar alterações).

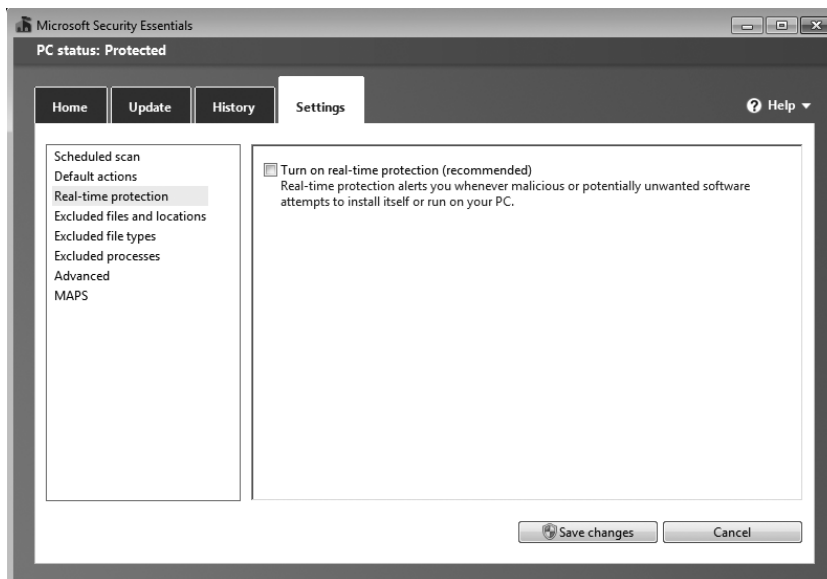


Figura 1.54 – Desativando a proteção em tempo real.

Por fim, instale a aplicação web *BookApp* personalizada, que se encontra no torrent deste livro. (*1stPentestBook?!* é a senha do arquivo.) Arrase e solte a pasta *BookApp* na máquina virtual Windows 7. Em seguida, siga as instruções contidas em *InstallApp.pdf*, que detalham a instalação do BookApp. Aqui está uma visão geral das instruções:

1. Execute *Step1-install-iis.bat* como administrador ao clicar com o botão direito do mouse no arquivo *.bat* e selecione **Run as administrator** (Executar como administrador). (Depois que a instalação estiver concluída, você poderá fechar qualquer janela DOS que permaneça aberta.)
2. Vá até a pasta *SQL* e execute *SQLEXPRWT_x86_ENU.EXE*. Instruções detalhadas, com imagens de telas capturadas, estão incluídas no PDF *InstallApp*.
3. Instale o Service Pack 3 ao executar *SQLServer2008SP3-KB2546951-x86-ENU.exe*. Ao ser avisado de que esse programa contém problemas conhecidos de compatibilidade, clique em **OK** para executá-lo e concluir a instalação. Opte por aceitar qualquer alteração.
4. Habilite **Named Pipes** (Pipes nomeados) usando o SQL Server Configuration Manager.
5. Retorne à pasta principal da aplicação e execute *Step2-Modify-FW.bat* como administrador.

6. Instale o suporte ao XML para o MS SQL por meio de *sqlxml_x86-v4.exe* na pasta SQL.
7. Execute *Step3-Install-App.bat* como administrador a partir da pasta principal da aplicação.
8. Utilize o MS SQL Management Studio para executar o *db.sql* a partir da pasta SQL, conforme descrito em detalhes no PDF *InstallApp*.
9. Por fim, altere as permissões do usuário no arquivo *AuthInfo.xml* na pasta da aplicação do livro para conceder todas as permissões a IIS_USERS.

Resumo

Configuramos o nosso ambiente virtual, fizemos o download do Kali Linux e o personalizamos para os ataques, configuramos nossa rede virtual e nossos sistemas operacionais-alvo – o Windows XP, o Windows 7 e o Ubuntu.

No próximo capítulo, iremos nos familiarizar com a linha de comando do Linux e estaremos no caminho certo para aprender a usar as diversas ferramentas e técnicas associadas aos testes de invasão, presentes neste livro.