

Sílvia César Roxo Giavaroto
Gerson Raimundo dos Santos

BACKTRACK LINUX AUDITORIA E TESTE DE INVASÃO EM REDES DE COMPUTADORES

 EDITORA
CIÊNCIA MODERNA

Backtrack Linux - Auditoria e Teste de Invasão em Redes de Computadores
Copyright© Editora Ciência Moderna Ltda., 2013

Todos os direitos para a língua portuguesa reservados pela EDITORA CIÊNCIA MODERNA LTDA.

De acordo com a Lei 9.610, de 19/2/1998, nenhuma parte deste livro poderá ser reproduzida, transmitida e gravada, por qualquer meio eletrônico, mecânico, por fotocópia e outros, sem a prévia autorização, por escrito, da Editora.

Editor: Paulo André P. Marques

Produção Editorial: Aline Vieira Marques

Assistente Editorial: Lorena Fernandes

Capa: Carlos Candal

Diagramação: Lúcia Quaresma

Copidesque: Lorena Fernandes

Várias **Marcas Registradas** aparecem no decorrer deste livro. Mais do que simplesmente listar esses nomes e informar quem possui seus direitos de exploração, ou ainda imprimir os logotipos das mesmas, o editor declara estar utilizando tais nomes apenas para fins editoriais, em benefício exclusivo do dono da Marca Registrada, sem intenção de infringir as regras de sua utilização. Qualquer semelhança em nomes próprios e acontecimentos será mera coincidência.

FICHA CATALOGRÁFICA

GIAVAROTO, Sílvia César Roxo. SANTOS, Gerson Raimundo dos.

Backtrack Linux - Auditoria e Teste de Invasão em Redes de Computadores

Rio de Janeiro: Editora Ciência Moderna Ltda., 2013.

1. Programação de Computador – Programas e Dados 2. Ciência da Computação

I — Título

ISBN: 978-85-399-0383-2

CDD 005
004

Editora Ciência Moderna Ltda.

R. Alice Figueiredo, 46 – Riachuelo

Rio de Janeiro, RJ – Brasil CEP: 20.950-150

Tel: (21) 2201-6662/ Fax: (21) 2201-6896

E-MAIL: LCM@LCM.COM.BR

WWW.LCM.COM.BR

Agradecimentos

Sílvio César Roxo Giavaroto

Gostaria primeiramente de agradecer a DEUS, por ter, em todos os dias de minha vida, me abençoado, me guardado e ter permitido que eu chegasse até aqui. À minha esposa e companheira Adriana Giavaroto pela paciência e incentivo, à minha princesa e filha querida Priscila, saiba que todos os dias peço a DEUS para que seu caminho seja sempre iluminado, me orgulho de você. Aos meus pais maravilhosos, Antoninho e Inajá, que sempre acreditaram em mim e me apoiaram nas batalhas que a vida tem me reservado, amo vocês. Às minhas irmãs Gisele e Ana Paula.

Um agradecimento especial ao coautor do livro, meu amigo Gerson Raimundo dos Santos, foi um prazer ter trabalhado com você nesta obra e espero que seja a primeira de muitas.

Quero também agradecer aos companheiros de trabalho, Alexandre Antônio Barelli, sempre me proporcionando novos desafios e que me fazem crescer profissionalmente, Ciro Faustino de Azevedo Bastos, Alexandre Daniel Ventura Nitão, Caio de Moura Navas, que já algum tempo me acompanham na batalha.

Gerson Raimundo dos Santos

Na realização deste trabalho, agradeço primeiramente a DEUS, pelo vigor e força de vontade sempre a mim concedida.

Agradeço à minha querida esposa Andrea, que, às vezes, se pergunta o que uma pessoa faz tanto tempo diante de um computador, claro que você está certa, pois a vontade de fazer algo compromete boa parte do tempo e, sem controle, prejudicamos a todos.

Aos meus queridos filhos Thiago e David, razão de toda a minha força e inspiração, sempre queremos deixar uma pequena marca, para que seja posteriormente usada como um grande exemplo.

Agradeço de forma especial aos meus queridos pais, Adeli e Efigênia, que me incentivaram, com muito amor, desde criança a ser um grande homem através dos estudos. À minha irmã Erci, persistente em seus ideais, mas sempre com amor e paciência e ao meu irmão Jefferson, que sempre apoiou meus projetos simpatizando com o software livre e hoje é capaz de fazer coisas interessantes com o Linux.

Ao meu grande amigo Silvio Giavaroto, idealista que trabalha arduamente com grande espírito de equipe. Nada melhor que fazermos grandes amigos na tempestade, diante de grandes obstáculos, pela qual o comprometimento e força de união, devem ser amplamente aplicados.

Agradeço ao Diretor de Telemática, Alexandre Antônio Barelli, pelas oportunidades e empurrões, é fato que necessitamos sair sempre da zona de conforto e sermos incumbidos de missões e desafios, a fim de produzirmos algo relevante, como bons frutos. Estendo o agradecimento aos programadores: Caio de Moura Navas, Ciro Faustino de Azevedo Bastos e Alexandre Daniel Ventura Nitão, que diante das adversidades e desafios constantes, sempre aplicam soluções com altíssima criatividade e sem perder o bom humor, sobremaneira resolvendo de forma exemplar as tarefas confinadas.

A todos os meus inimigos e desanimadores, que, de alguma forma, lançaram alguma negatividade. Creio que vocês são o melhor combustível

para prosseguirmos, quando conseguimos nos relacionar com todos, como se fôssemos realmente irmãos, é indicativo que crescemos e estamos alcançando o cume da montanha.

No mais, ficarei imensamente feliz se, de uma forma ou de outra, este livro contribuir com a formação de alguém, de forma que toda a ideia seja utilizada e aplicada fortalecendo o bem e potencializando os profissionais da área de Segurança da Informação no incansável combate, muitas das vezes ao desconhecido e submundo dos bits.

Finalizando, externo a maior riqueza que adquiri ao longo dos anos: boas amizades, bons livros, boas dicas e meu laboratório, sempre caseiro que, constantemente, indica que preciso melhorar sempre, extraindo um dos maiores e sublimes sumos com gosto inigualáveis que somente alguns podem saborear e que todos não podem tirar: um pouco de conhecimento.

Sumário

Sobre os Autores	XVIII
-------------------------------	--------------

Prefácio	xv
-----------------------	-----------

Público-Alvo.....	xv
-------------------	----

Algumas Considerações.....	xv
----------------------------	----

Importante.....	xvi
-----------------	-----

Convenções Usadas Neste Livro.....	xvi
------------------------------------	-----

INTRODUÇÃO	1
-------------------------	----------

CAPÍTULO I	3
-------------------------	----------

Conhecendo o BackTrack.....	5
-----------------------------	---

O Que é BackTrack.....	5
------------------------	---

Instalando o BackTrack 5 em uma Virtualbox.....	7
---	---

Iniciando o BackTrack 5 em Modo Gráfico.....	12
--	----

Configurando a Rede.....	13
--------------------------	----

Iniciando, Parando e Reiniciando Serviços de Rede.....	14
--	----

Checando número de IP.....	15
----------------------------	----

Atribuição de IP via DHCP.....	15
--------------------------------	----

Configurando IP Manualmente e Atribuindo Rota Default.....	16
--	----

Atualizando o BackTrack.....	16
------------------------------	----

Iniciando e Parando Serviços Apache e SSH.....	17
Metodologia do Teste de Penetração (Penetration Testing).....	19

Capítulo II 29

Reconhecimento.....	31
Um Pouco de Segurança da Informação.....	31
Reconhecimento (Footprinting).....	33
Engenharia Social.....	34
Detectando Sistemas Ativos (ping).....	36
Genlist.....	40
Informações sobre DNS (Domain Name System).....	40
Consulta Simples com NSLOOKUP.....	42
DNSENUM.....	42
DNSMAP.....	43
DNSRECON.....	45
FIERCE.....	45
Utilizando o NMAP e NETCAT para Fingerprint.....	48
Mais Informações com o NETIFERA.....	53
xprobe2.....	58

Capítulo III 61

Varreduras.....	63
Técnicas de Ataques por Rastreamento de Portas (Scanning).....	63

Um Pouco Sobre Conexões TCP.....	64
Técnicas de Varreduras com o NMAP.....	67
Varreduras Furtivas TCP Syn.....	71
Detectando Firewalls e IDS.....	73
Utilizando Táticas de Despistes.....	74
Ferramenta de Varredura Automatizada (AutoScan).....	75
Zenmap.....	79
Varreduras com o Canivete Suíço NETCAT.....	81

Capítulo IV 85

Enumeração.....	87
Princípios de Enumeração.....	87
Enumeração Netbios com Nbtscan.....	88
Enumeração SNMP com Snpcheck.....	90
Deteccção de Versões.....	97
Detectando Servidores Web com Httprint.....	99
A Ferramenta AMAP.....	101
Enumerando SMTP.....	103
A Ferramenta SMTPScan.....	105

Capítulo V 109

Invasão do Sistema.....	111
Ganho de Acesso.....	111

Utilizando a Ferramenta xHydra.....	112
Utilizando Medusa.....	121
Utilizando Metasploit.....	126
Exploit, Payload e Shellcode.....	127
Interfaces do Metasploit.....	127
Explorando RPC.....	129
Explorando Conficker com Meterpreter.....	132
Dumping de Hashes de Senhas.....	136
Utilizando hashdump do Metasploit.....	137
Roubando Tokens com Incognito Meterpreter.....	137

Capítulo VI 141

Manutenção.....	143
Garantindo o Retorno.....	143
Plantando um Backdoor.....	143
Escondendo Arquivos com Alternate Data Stream (ADS).....	145
Garantindo Acesso Físico como Administrador.....	149
Apagando Rastros.....	153
LOGS de Máquinas Windows.....	153
LOGS de Máquinas Linux.....	157
LOGS do Apache em máquinas Windows.....	158
LOGS do Servidor IIS Internet Information Server.....	159

Capítulo VII	161
Ataques VOIP	163
Ataques Envolvendo VOIP	163
Ataque SIP Bombing	164
Ataque Eavesdroppin	165
Ataque Man in the Middle	165
Ataque Call Hijacking	166
Ataque SPIT (Spam over IP Telephony)	166
Ataque Caller ID Spoofing	167
Camada de Segurança para VOIP	172
Capítulo VIII	177
Miscelânea	179
Quebrando Senhas com John The Ripper	179
Interceptando Dados com Wireshark	182
Levantando Informações com Maltego	187
Scapy	196
Saint	206
Apache Tomcat Brute Force	211
MySQL Brute Force	216
Hydra	217
Joomla Vulnerability Scanner Project	219
WhatWeb	221
Nessus	223
Epílogo	231

Sobre os Autores

Sílvio César Roxo Giavaroto. Atualmente, exerce as funções de analista de segurança e administrador de redes Linux no Palácio dos Bandeirantes do Governo do estado de São Paulo, possui graduação no Curso Superior de Tecnologia em Redes de Computadores, Pós-Graduação MBA Especialista em Segurança da Informação, também é professor universitário e ministra aulas em segurança de redes na graduação e infraestrutura de redes locais na pós-graduação. Possui sólidos conhecimentos na área de defesa com ênfase em tecnologia da informação. Detém ainda certificação internacional reconhecida pelo Departamento de Defesa dos Estados Unidos, que identifica profissionais capazes de encontrar vulnerabilidades em sistemas, a C|EH Certified Ethical Hacker. Mantém o site <http://www.backtrackbrasil.com.br>.

Gerson Raimundo dos Santos. Atualmente exerce as funções de Analista de Segurança e Administrador de Redes Linux no Palácio dos Bandeirantes do Governo do estado de São Paulo. Sempre que possível, contribui com a Comunidade Viva o Linux artigos e dicas usando o codinome "Gerson Raymond". Leitor assíduo do portal Viva O Linux, pela qual encontra-se parte da sua Monografia - Projeto Squid. Bacharel em Ciências da Computação, Técnico em Telecomunicações e Técnico em Eletrônica com amplos conhecimentos em centrais de grande porte na área de telefonia(Ericsson, Alcatel, Siemens), microeletrônica, robótica, inteligência artificial, linguagens de programação C e C++, Expressões Regulares (Sed, Sort, Egrep, AWK, etc.), Mikrotik, Asterisk, Elastix, Virtualização XEN e KVM. Aficionado por segurança em redes e ferramentas de Pentest. Desde 2000, vem aplicando os seus conhecimentos utilizando distribuições Linux (Slackware, OpenBSD, CentOS, Puias, Opensuse, Debian), sistemas de monitoramento com ZABBIX, bem como implementações de sistemas de segurança utilizando Iptables, Snort, Honeypot e Denyhost. Ultimamente utilizando a distribuição BACKTRACK um aglomerado de ferramentas de pentest, pela qual possibilita, através de testes e critérios rigorosos de segurança melhores mecanismos de proteção. Mantém o site <http://www.backtrackbrasil.com.br>.

Prefácio

Derivado do WHAX, Whoppix e Auditor, BackTrack é uma distribuição voltada para testes de penetração em redes de computadores. Utilizado em grande escala por auditores de segurança, administradores de redes e hackers éticos, atualmente encontra-se na versão 5 e possui mais de 300 ferramentas que podem ser utilizadas na execução de testes de penetração.

A última versão pode ser baixada no site <http://www.backtrack-linux.org/downloads>.

Público-Alvo

Este livro é destinado a todos os profissionais que atuam na área de segurança da informação, estudantes que estão iniciando seus estudos na área de segurança de sistemas computacionais, administradores de redes, assim como profissionais que já possuam alguma experiência na área e queiram aperfeiçoar seus conhecimentos.

Algumas Considerações

Este livro pressupõe que você possua experiência com comandos básicos do sistema operacional LINUX e conhecimento básico sobre redes TCP/IP. Como enfatizado anteriormente, o BackTrack possui mais de 300 ferramentas, porém neste livro não serão abordadas todas elas, mas somente as que julgamos mais potentes e eficazes em testes de penetração.

Importante

As informações contidas neste livro são de finalidade única e exclusivamente educativa e profissional. Os autores não se responsabilizam pelo uso indevido do conteúdo apresentado, use o conhecimento para o bem.

Convenções Usadas Neste Livro



Este ícone indica contramedida / correção.

INTRODUÇÃO

“Se você conhece o inimigo e a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece, mas não o inimigo, para cada vitória sofrerá uma derrota. Se você não conhece o inimigo nem a você mesmo, perderá todas as batalhas.”

Sun Tzu

Não é novidade que o acesso à tecnologia da informação e à inclusão digital aumentam a cada dia que passa, nos dias atuais, em uma era globalizada, onde quase tudo é movido através das novas tendências tecnológicas, hoje é possível que uma pessoa, utilizando-se de um computador e possuindo acesso à rede mundial de computadores “internet”, possa usufruir de serviços de sistemas financeiro online como “netbank”, trocar e-mails, adquirir vários tipos de produtos através do comércio eletrônico etc.

Paralelamente com as facilidades do mundo digital, a fim de se manter seguro e proteger os dados que ali estão inseridos e comuns, na maioria das empresas, a utilização de tecnologias avançadas para proteção de seus ativos, sejam eles tangíveis ou intangíveis. Soluções que vão desde um simples antivírus a complexos sistemas de criptografia, aliados às potentes regras de um sistema de firewall ou implementação de sistemas de detecção de intrusos IDS.

Contudo, neste meio, um inimigo caminha silenciosamente, o invasor intitulado como “blackhat”, pela mídia é conhecido como Hacker. Este indivíduo é dotado de conhecimentos avançados sobre sistemas e redes de computadores, habilidades que permitem ao mesmo sucesso na interceptação e subtração

indevida da informação, é muito difícil e, às vezes, até impossível mensurar os danos causados por um blackhat.

Diante de novas tendências, táticas de invasões e da rapidez com que se move o mundo digital, é de suma importância que administradores de redes ou sistemas tenham em mente que “blackhats” estão em constante evolução e são inúmeros os métodos utilizados nas práticas de invasões. Conhecer tal ameaça, é fundamental que os profissionais envolvidos neste meio estejam treinados e preparados para lidar com situações que envolvam a segurança da informação a fim de manter um ambiente seguro e proteger os dados que ali estão inseridos.

Abordaremos neste livro algumas das inúmeras técnicas utilizadas pelos invasores e, com isto, apresentaremos a você, leitor, um entendimento básico sobre vulnerabilidades que possam afetar seu ambiente computacional. Ao final você estará apto a detectar falhas e vulnerabilidades e, então, aplicar correções diminuindo possíveis ataques a seu ambiente.

CAPÍTULO I

- ✔ O Que é BackTrack—5
- ✔ Instalando o BackTrack 5 em uma Virtualbox—7
- ✔ Iniciando o BackTrack 5 em Modo Gráfico—12
- ✔ Configurando a Rede—13
- ✔ Iniciando, Parando e Reiniciando Serviços de Rede—14
- ✔ Checando número de IP:—15
- ✔ Atribuição de IP via DHCP:—15
- ✔ Configurando IP Manualmente e Atribuindo Rota Default:—16
- ✔ Atualizando o BackTrack—16
- ✔ Iniciando e Parando Serviços Apache e SSH—17
- ✔ Metodologia do Teste de Penetração (Penetration Testing)—19

Conhecendo o BackTrack

"Nenhum de nós é tão inteligente quanto todos nós juntos."

Warren Bennis

O Que é BackTrack

Baseado no WHAX, Whoppix e Auditor, BackTrack é uma ferramenta voltada para testes de penetração muito utilizada por auditores, analistas de segurança de redes e sistemas, hackers éticos etc. Sua primeira versão é de 26 de maio de 2006, seguida pelas versões [2] de 6 de março de 2007, [3] de 19 de Junho de 2008, [4] de 22 de Novembro de 2010 e [5] de 2011.

Atualmente, possui mais de 300 ferramentas voltadas para testes de penetração, existem ainda algumas certificações que utilizam o BackTrack como ferramenta principal, OSCP Offensive Security Certified Professional, OSCE Offensive Security Certified Expert e OSWP Offensive Security Wireless Professional, certificações oferecidas pela Offensive Security que mantém o BackTrack.



Figura 1. Interface KDE BackTrack5

Instalação do BackTrack

A instalação do BackTrack é relativamente fácil e você poderá instalá-lo diretamente em sua máquina, em uma máquina virtual, rodar diretamente de um live cd ou até mesmo em um dispositivo pen drive. Neste livro, abordaremos a instalação do BackTrack em uma virtualbox.

Você poderá fazer o download da virtualbox para Linux, Mac, Solaris ou Windows no site <https://www.virtualbox.org/wiki/Downloads>. Para instalação do BackTrack 5, utilizaremos a máquina virtualbox versão 4.1.4 para Windows.

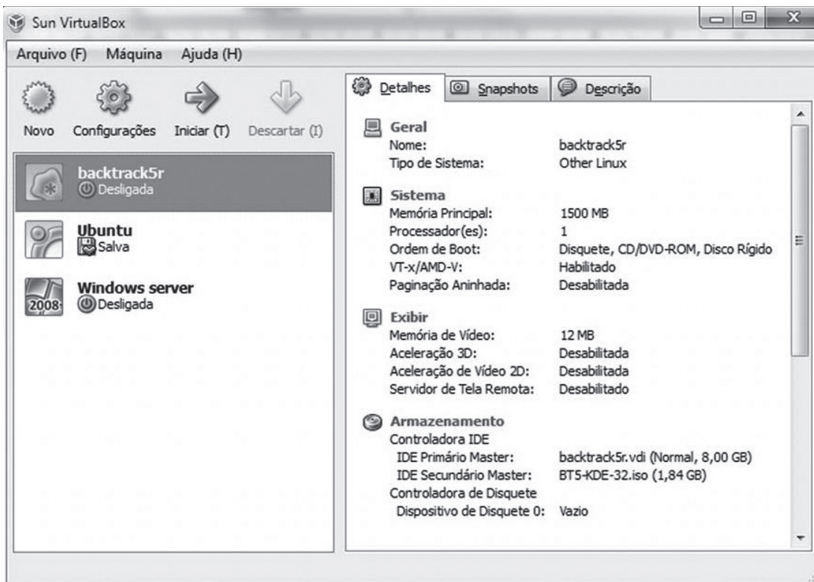


Figura 2. VirtualBox para Windows.

O download do BackTrack 5 poderá ser feito no site <http://www.BackTrack-linux.org/downloads/>, neste livro trabalharemos com a imagem BT5-KDE-32.iso.

Instalando o BackTrack 5 em uma Virtualbox

Para nossos testes instalaremos o BackTrack em uma virtualbox. Deste modo, você não precisará se preocupar com particionamentos de discos que são necessários para instalação em modo dual-boot, porém se ainda você optar por este modo de instalação, um tutorial está disponível em <http://www.BackTrack-linux.org/tutorials/dual-boot-install>.

A única desvantagem em executar o BackTrack em uma máquina virtual é que o sistema fica mais lento em relação à instalação direta no computador. Outro

fator é a utilização de placas de redes wireless que deverão ser do tipo USB, isto devido às próprias limitações da máquina virtual.

A seguir serão descritos os passos para instalar a imagem ISO do BackTrack 5.

A partir da inicialização da VirtualBox, siga as seguintes etapas:

1. Inicie o assistente de criação dando um clique no botão novo.
2. Será aberta a janela de bem-vindo ao assistente, clique em próximo.
3. Na próxima janela, escolha um nome para sua máquina, o sistema operacional Linux e a versão.
4. Na tela a seguir, selecione a quantidade de memória a ser utilizada, aconselhável 1 GB.
5. Na próxima tela, habilite a opção disco de boot e criar novo disco rígido.
6. Na tela a seguir habilite a opção VDI (Virtual Disk Image).
7. Na próxima janela, selecione a opção dinamicamente alocado.
8. Na janela a seguir, ajuste o tamanho do disco virtual para 8GB.
9. Será mostrado o sumário de configurações.
10. Na janela inicial, clique na máquina que você criou a mesma estará no modo desligada.

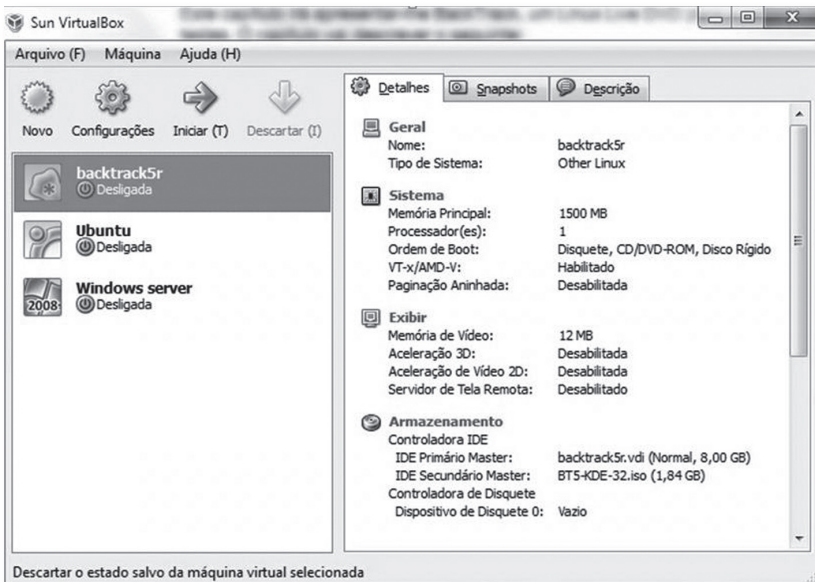


Figura 3. Tela VirtualBox apresentando sistemas desligados.

11. A próxima janela a surgir será o assistente de primeira execução, dê um clique em próximo.
12. Na próxima janela, selecione a mídia de instalação, no caso a imagem baixada BT5-KDE-32. iso.
13. A próxima tela exibirá o sumário de configurações, clique em iniciar.
14. Se até agora você seguiu todos os passos, a tela de subida do sistema será exibida, selecione o modo Default Boot text Mode conforme mostrado na figura 3.1,

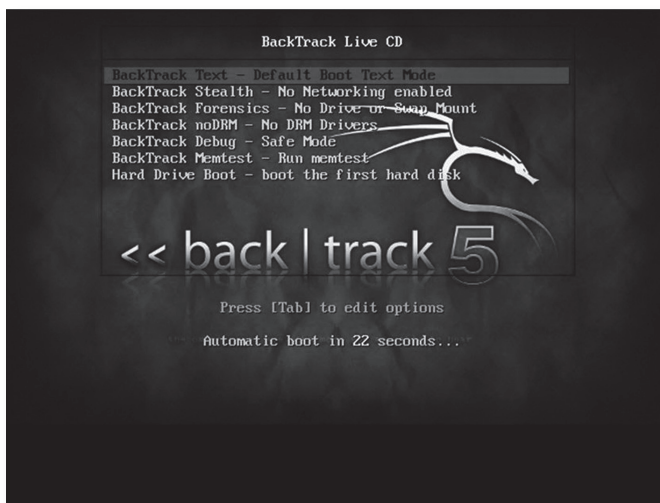


Figura 3.1. Tela inicial BackTrack Live CD.

15. O próximo passo será entrar no modo gráfico, para tal, digite startx conforme mostrado na figura 3.2 e o modo gráfico será carregado.

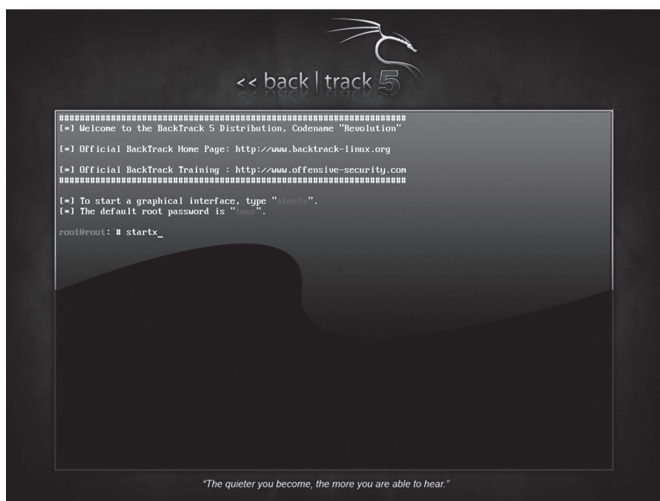


Figura 3.2. Tela para carregamento de ambiente gráfico.

16. Já no BackTrack, dê um clique sobre o ícone Install BackTrack existente na área de trabalho, após isto, a janela de seleção de idioma surgirá, selecione o idioma português do Brasil e clique em avançar.
17. Será exibida a tela para seleção da região e horário, ajuste conforme sua região e hora.
18. Em seguida a tela de configuração de teclado será mostrada, basta selecionar o layout do seu teclado e dar um clique em avançar.
19. A próxima janela exibida será a de particionamento, selecione apagar e usar disco inteiro conforme mostrado na figura 3.3.

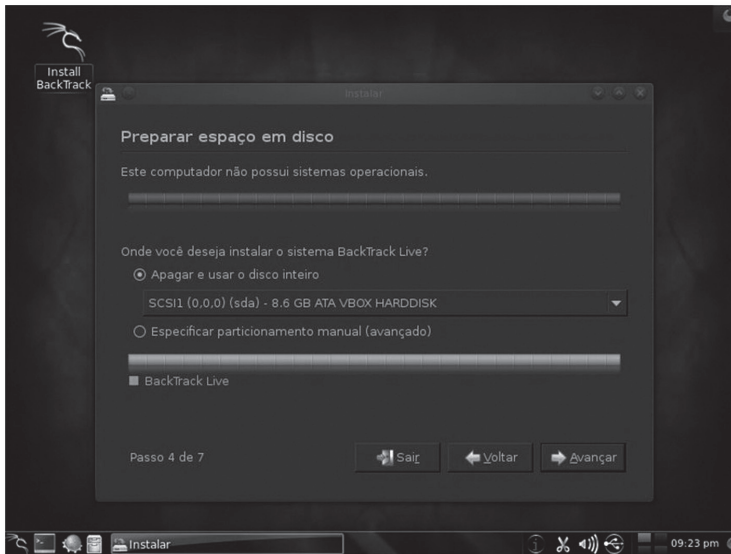


Figura 3.3. Tela particionamento de disco.

20. A próxima janela mostrará o status de instalação.



Figura 3.4. Tela de status de instalação do sistema.

Caso você tenha seguido os vinte passos anteriores, seu BackTrack estará instalado e pronto para ser utilizado nos testes que estarão por vir.

Iniciando o BackTrack 5 em Modo Gráfico

Ao iniciar o BackTrack 5, surgirá uma tela solicitando seu login e sua password, para login digite root e na senha digite toor e uma nova tela será exibida agora bastará digitar startx para subir o modo gráfico.

Configurando a Rede

Ao criar sua máquina virtual, você poderá optar pelos três tipos de conectividade, NAT, Bridge e Host-only.

➤ **Modo NAT**

Quando estamos utilizando uma máquina virtual, NAT (Network Address Translation) é a maneira mais simples de acessar a rede externa e geralmente não requer qualquer tipo de configuração é o padrão utilizado pela VirtualBox. Com a função NAT habilitada, a máquina utilizará a interface física do computador e atribuirá um IP do servidor DHCP contido no software da VirtualBox, vale ressaltar que, neste modo, a máquina não se conectará a rede interna, porém poderá se conectar à internet.

➤ **Modo Bridge**

No modo Bridge, será criada uma ponte entre a interface virtual e a interface real, caso sua rede trabalhe com um servidor DHCP um endereço dinâmico será atribuído à interface virtual, no caso de não haver o servidor DHCP, você poderá atribuir manualmente o endereço de IP da sua rede e, nesse caso, as redes poderão se comunicar.

➤ **Modo Host-only**

No modo host-only ou somente host, a placa de rede só se comunicará com a máquina que está hospedando a máquina virtual. Poderá ainda se comunicar com outras máquinas hospedadas na mesma máquina virtual.

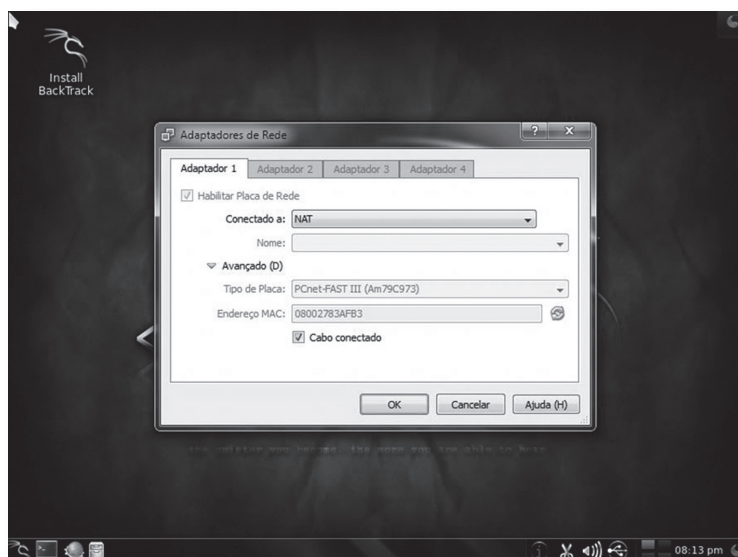


Figura 4. Placa de Rede Trabalhando em Modo NAT.

Iniciando, Parando e Reiniciando Serviços de Rede

No BackTrack 5, para iniciar o serviço de rede, você poderá abrir o Shell e digitar o seguinte comando:

```
root@bt:~# /etc/init.d/networking start
```

Para interromper o serviço de rede, abra a Shell e digite o seguinte comando:

```
root@bt:~# /etc/init.d/networking stop
```

Para reiniciar o serviço de rede, abra o Shell e digite o seguinte comando:

```
root@bt:~# /etc/init.d/networking restart
```

Checando número de IP:

```
root@bt:~# ifconfig eth0
```

```
eth0  Link encap:EthernetHWaddr 08:00:29:fd:8d:79
inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
inet6addr: fe80::a00:29ff:fed:8d79/64  Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:8 errors:0 dropped:0 overruns:0 frame:0
        TX packets:19 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:1444 (1.4 KB)  TX bytes:1712 (1.7 KB)
        Interrupt:10  Base address:0xd020
```

Atribuição de IP via DHCP:

```
root@bt:~# dhclient eth0
```

```
Internet Systems Consortium DHCP Client V3.1.1
Copyright 2004-2008 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth0/08:00:27:8d:76:21
Sending on  LPF/eth0/08:00:27:8d:76:21
Sending on  Socket/fallback
DHCPREQUEST of 10.0.2.15 on eth0 to 255.255.255.255 port 67
DHCPACK of 10.0.2.15 from 10.0.2.2
bound to 10.0.2.15 -- renewal in 37988 seconds.
```

Configurando IP Manualmente e Atribuindo Rota Default:

```
root@bt:~# ifconfig eth0 192.168.0.10/24
root@bt:~# route add default gw 192.168.0.1
root@bt:~# echo nameserver 192.168.0.254 >> /etc/resolv.conf
```

Atualizando o BackTrack

Após a instalação do BackTrack, você poderá fazer a atualização do sistema e para isto basta que você siga os seguintes passos:

1. Você pode utilizar os repositórios do Ubuntu ou Debian, a primeira coisa a fazer é verificar o arquivo `/etc/apt/sources.list`, veja abaixo o padrão `source.list` do BackTrack 5:

```
debhttp://all.repository.BackTrack-linux.org revolution main microverse non-free testing
debhttp://32.repository.BackTrack-linux.org revolution main microverse non-free testing
debhttp://source.repository.BackTrack-linux.org revolution main microverse non-free testing
```

2. O próximo passo para que você possa realizar a atualização é realizar a sincronização dos arquivos a partir de um repositório. Para isto, execute o seguinte comando:

```
root@bt:~# apt-get update
```

3. Feita a sincronização, agora você poderá prosseguir com a atualização, execute o seguinte comando:

```
root@bt:~# apt-get upgrade
```

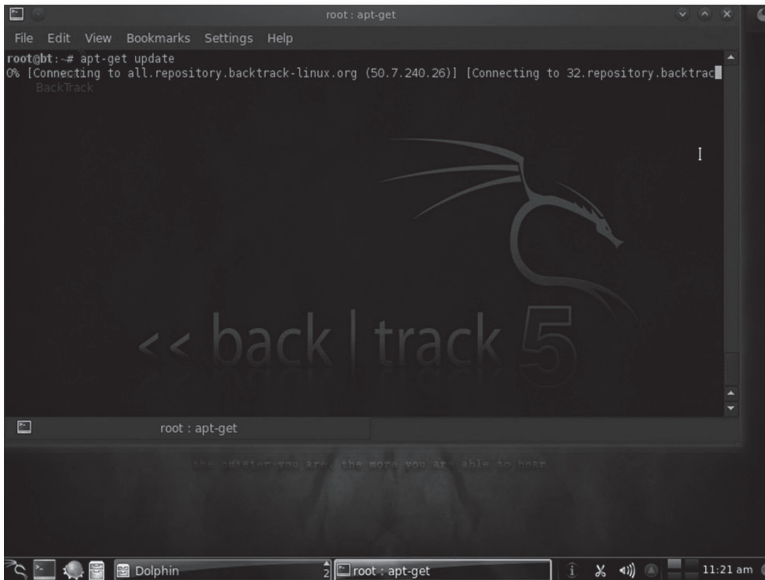


Figura 5. Tela apt-get update.

Iniciando e Parando Serviços Apache e SSH

A seguir mostraremos como iniciar os serviços Apache e SSH no BackTrack 5.

Iniciando o Apache:

```
root@bt:~# /etc/init.d/apache2 start
```

Você pode checar se o serviço foi ativado abrindo o navegador e digitando o endereço de loopback conforme a figura 6.

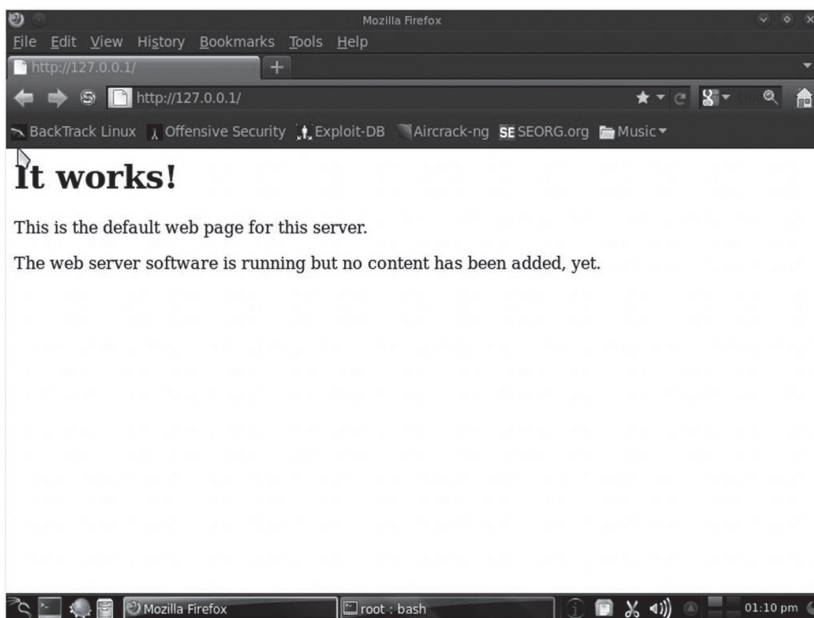


Figura 6. Navegador mostrando serviço apache ativo.

Se preferir, você ainda pode verificar se porta 80 está ativa através do comando `netstat`, conforme mostrado abaixo:

```
root@bt:~# netstat -an | grep 80

tcp instal0 0 0.0.0.0:80  0.0.0.0:*    LISTEN
```

Para finalizar o serviço apache, basta executarmos o seguinte comando:

```
root@bt:~# /etc/init.d/apache2 stop
```

A seguir, mostraremos como gerar chave e iniciar o serviço SSH.

Para isto você deverá executar o seguinte comando:

```
root@bt:~# sshd-generate

root@bt:~# sudo /etc/init.d/ssh start
```

Para finalizar o serviço, bastará digitar o comando abaixo:

```

root@bt:~# /etc/init.d/ssh stop
Session Edit View Bookmarks Settings Help
#####
[*] Welcome to the BackTrack 5 Distribution, Codename "Revolution"

[*] Official BackTrack Home Page: http://www.backtrack-linux.org

[*] Official BackTrack Training : http://www.offensive-security.com
#####

[*] To start a graphical interface, type "startx".
[*] The default root password is "toor".

Last login: Fri Nov  4 14:28:37 2011 from 192.168.56.101
root@bt:~#

```

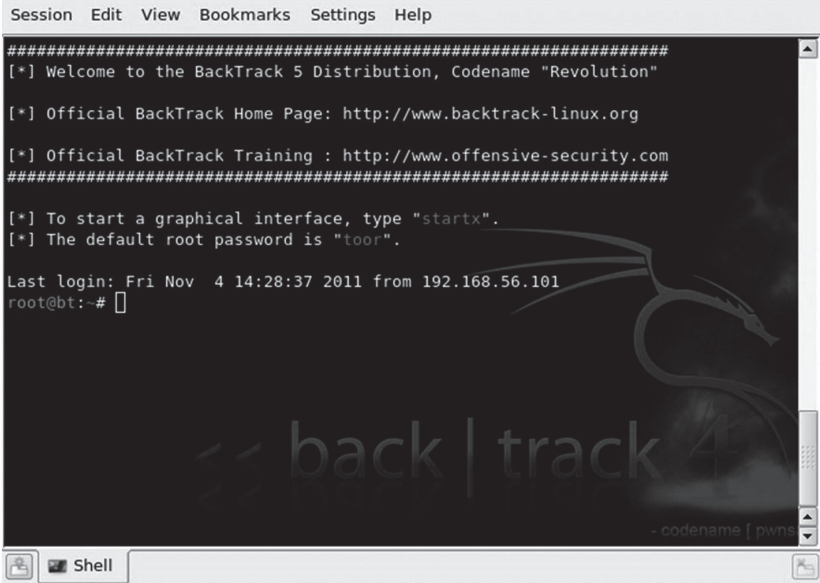


Figura 7. Linux BackTrack 4 acessando BackTrack 5 através do SSH.

Metodologia do Teste de Penetração (Penetration Testing)

Definido como Penetration testing, trata-se de um método para testar e descobrir vulnerabilidades em uma rede ou sistemas operacionais. Nesta etapa, são analisadas e exploradas todas as possibilidades de vulnerabilidades. Pentest insere métodos de avaliação de segurança em um sistema de computador ou rede, aplicando simulações de ataques como se fosse um estranho mal intencionado no intuito de invadir um sistema. Tais Pentest possibilitam verificar a real estrutura do sistema, que é vasculhado em todas as áreas inerentes à estrutura de segurança. São de suma importância os

testes aplicados, pois através deles poderemos verificar falhas em hardware e software utilizados e criar mecanismos de defesas ou ajustes adequados.

Com o intuito de proteção e hardenização, os testes de penetração são de extrema importância para uma empresa ou organização. Com a constante e radical mudança de hábitos propiciada pelo avanço da tecnologia, aliada à disseminação das informações pelos mecanismos de buscas (Google, Yahoo, etc.) e a latente busca por um retorno de valores monetários, muitas empresas ou instituições cada vez mais instalam sistemas (servidores, aplicativos, software) sem critérios específicos relacionados à segurança. O importante é funcionar e ter o retorno esperado. Desta forma, inúmeros problemas de segurança são implantados em sistemas, com o intuito de roubar informações, práticas de crimes e outros adjacentes.

Outro problema relacionado às deficiências citadas se enquadram na falta de especialistas da área de segurança da informação com bagagem aos sistemas legados, bem como na falta de interesse ou desconsideração das empresas ou instituições no investimento destes profissionais. Um profissional da área de segurança envolvido com pentest precisa pensar como um Blackhat, Cracker ou Hacker e possuir os mesmos costumes (mecanismos) de raciocínio relacionados a descobrir as vulnerabilidades do sistema-alvo.

Todas as informações levantadas durante o processo do pentest resultarão em relatórios técnicos pormenorizados, incluindo soluções pertinentes ao sistema legado (hardware e software) avaliado. Pentest, no entanto, caracteriza-se como uma completa auditoria de segurança, pela qual explora de forma abrangente todos os aspectos que envolvem a segurança de um sistema. Uma sequência de processos é aplicada constituindo várias fases do processo de investigações, ou seja, um levantamento maciço de informações contribuirá com um resultado positivo em cima do alvo. Considerando que todas as informações adquiridas pelo pentest serão aplicadas em benefício do sistema investigado e analisado.

Pentest é o oposto do “hacking”; apesar de usar as mesmas ferramentas de análises e raciocínios aplicados. A meta do pentest é puramente aplicar as melhores técnicas de segurança, a fim de proteger o maior patrimônio que existe - a informação - e estas técnicas poderão ser aplicadas da melhor forma

possível, seja reparando hardwares com bugs presentes, aplicando patches de segurança, otimizando softwares, políticas de senhas, entre outros, logo após o reconhecimento total do alvo analisado.

Estes procedimentos de pentest, como citado, são similares aos aplicados pelos Blackhats e eles são divididos em cinco fases, pelas quais se constituem os processos de um ataque.

1. Informações do Alvo.

Nesta etapa, nada pode ser descartado. Devemos aplicar de 90% de nosso trabalho. Quanto mais informações relacionadas com o nosso objetivo, maior probabilidade de acesso ao nosso sistema auditado.

Todas as informações relacionadas ao segmento da empresa: servidores, roteadores, firewalls, costumes dos funcionários e sua capacitação, amigos, pessoas relacionadas à empresa, empresas terceirizadas, e-mails, MSN, telefones, tipo de informação que chega ao lixo, etc.

Podemos aplicar a engenharia social, pela qual contribuirá de forma significativa com as informações necessárias, muitas das vezes apenas um telefonema recebido por um funcionário não qualificado ou treinado já consome o sucesso da penetração do sistema desejado.

Através das informações do Google, Yahoo e outros mecanismos de busca, em poucas horas conseguimos uma gama de informações potencializando nosso pentest. A disseminação de informações importantes nos sites de relacionamento como Facebook, Orkut, etc, facilita sobre maneira a obtenção dos dados desejados. Diretores, gerentes e administradores de redes, de uma forma geral, chegam a publicar informações desnecessárias que comprometem toda uma estrutura organizacional e, muitas das vezes, isto é feito apenas pelo ego e prazer pessoal, não levando em conta o sigilo necessário e a preservação dos dados de uma empresa.

Podemos ainda citar a falta de treinamento e aperfeiçoamento de diretores, gerentes e administradores, etc, envolvidos em várias camadas críticas de informações sem a menor estrutura requerida. O processo de informatização

chegou de repente e envolveu muitas pessoas de forma inesperada e, com isso, deficiências humanas estão enraizadas em vários segmentos do processo.

Tudo isso é um grande facilitador e, com certeza, os Blackhats sabem disso e cada vez mais exploram estas deficiências. No entanto, o analista de segurança, utilizando os mesmos conhecimentos deve cumprir a sua missão utilizando técnicas de prevenção e reajustes do sistema debilitado, a fim de conter as intrusões maliciosas.

2. Varreduras de Sistema

Depois de obter todas as informações necessárias, como softwares utilizados, tipos de firewall, serviços ativos, etc, e conhecendo as deficiências apresentadas poderemos utilizar a ferramenta de pentest adequada e explorar o nosso objetivo.

Hardwares utilizados, servidores, firewalls, tipo de serviços utilizando portas específicas são considerados nesta etapa. A verificação de IDS/IPS presente na rede deve ser analisada com um critério maior, a fim de aplicarmos mecanismos engenhosos relacionado à dificuldade imposta pelo sistema-alvo. Sabemos que várias regras devem ser bem aplicadas a um sistema de firewall, IDS/IPS e falta de configuração adequada de uma delas pode comprometer todo o sistema e garantir a intrusão desejada.

3. Ganhando o Acesso do Sistema

Nesta fase, o sistema é violado, devido à descoberta de vulnerabilidade, a invasão é consolidada e, através dela, podemos explorar as camadas internas do sistema, a fim de descobrir outros meios, pelos quais possa potencializar nosso ataque. Podemos verificar as estruturas de diretórios, políticas de senhas, enfim, várias alternativas podem ser aplicadas extraindo o máximo de informações. O reconhecimento do sistema pode ser ampliado conforme a necessidade específica relacionada aos posteriores pentest que serão aplicados. Uma análise geral do sistema ou mapeamento geral e detalhado será caracterizado pela personalidade de cada individuo invasor. A vivência e

experiência do invasor permitem diferentes ações não específicas que podem levar a várias situações inesperadas. Claro que, no início da ação, todos seguirão o mesmo caminho de acesso, mas, uma vez dentro do sistema, as diversidades de situações que podem ser aplicadas poderão dificultar o seu rastreamento de forma significativa e comprometedora.

4. Mantendo o Acesso no Sistema

Uma vez dentro do sistema, através de várias técnicas, poderemos verificar as possibilidades de instalação de rootkits, backdoor, etc, bem como outros métodos que possam contribuir com as facilidades que necessitamos, como portas abertas e organização de arquivos e estruturas ao nosso favor verificando se o sistema realmente está apto a dificultar determinadas ações. É necessária a inserção de uma estrutura maliciosa, com a qual possa contribuir a ratificação de um pentest real. Desta forma, teremos uma situação consolidada, que contribuirá com a aplicação de mecanismos de defesas e bloqueios inerentes ao sistema trabalhado. Devemos entender que tais invasões ao sistema nem sempre influenciam na ruptura do sistema operacional e em arquivos, pois, na maioria das intrusões consolidadas, os invasores estão atrás de informações que poderão contribuir quase sempre em ações que possibilitem lucros ou situações relacionadas a crimes. Pode ser que o próprio invasor corrija deficiências encontradas pelo caminho, mas é quase certo que ele poderá deixar uma alternativa exclusiva de acesso que contribua a ele um retorno inesperado e munido de várias situações complicativas.

5. Retirando as Evidências

A maioria dos invasores profissionais aplicam regras criteriosas, a fim de limpar o caminho traçado. Sabem que tais ações cometidas tratam-se de crimes, portanto utilizam planejamentos adequados eliminando rastros que comprometam sua identidade ou localização específica. O pentest utilizará os mesmos conceitos, embora esteja autorizado a executar as mesmas ações dos invasores. Tais procedimentos contribuem com a implementação de mecanismos que possam rastrear os invasores de forma eficiente possibilitando estudos posteriores ou configurações que não estavam presentes, desta

forma aumentando o potencial do sistema verificado, aplicando uma maior eficiência através de técnicas existentes. O Analista de Segurança deverá se atualizar constantemente e sempre verificar as suas ferramentas de testes, através de várias simulações. É necessário pensar como os invasores: entender seus métodos de operação e possuir conhecimentos das tecnologias envolvidas, pela qual contribuirá na investigação precisa dos procedimentos aplicados pelo invasor. Com a informação adquirida e configurações específicas, poderão ser aplicadas de forma a monitorar a integralidade do sistema, possibilitando informar qualquer alteração na sua estrutura.

Definição dos Tipos de Pentest para Varreduras

Blind: é um dos mais utilizados. Neste procedimento, o auditor não possui nenhuma informação do sistema-alvo que irá atacar. Ele deverá criar os meios mais eficazes possibilitando resultados positivos da ação aplicada. No entanto o sistema alvo sabe que será atacado e possui conhecimentos específicos das ações adotadas pelo pentest. O sistema alvo tem inteira consciência do que será aplicado no teste.

Double Blind: neste procedimento, o auditor também não possui nenhuma informação do sistema-alvo que irá atacar. O sistema-alvo também não sabe que será atacado, bem como os pentest que serão aplicados pelo auditor na estrutura do sistema alvo analisado.

Gray Box: neste procedimento, o auditor tem um conhecimento parcial do sistema-alvo, que possui informações de que será atacado, bem como os testes que serão aplicados pelo auditor responsável, a fim de obter informações específicas do sistema-alvo.

Double Gray Box: neste procedimento, o auditor tem conhecimento parcial do sistema-alvo, e possui informações que será atacado, porém não tem conhecimento dos testes que serão aplicados na varredura, a fim de obter informações específicas.

Tandem: neste procedimento, o auditor tem total conhecimento sobre o sistema-alvo que será analisado e ele tem consciência que será atacado e quais os procedimentos que serão adotados durante a realização destes ataques.

Reversal: neste procedimento, o auditor tem total conhecimento sobre o sistema-alvo que será analisado, porém ele não tem consciência que será atacado, bem como os procedimentos que serão adotados durante a realização dos ataques.

Como podemos observar, toda a explanação dos tipos de definição dos pen-test utilizados vão a encontro de um único objetivo, caracterizar os testes de penetração e explorar todas as vias possíveis, possibilitando a viabilidade e consumação de um ataque. Através de vários métodos, podemos dimensionar de forma criteriosa os impactos dos testes no sistema-alvo, caso tenhamos sucesso na invasão pretendida. Não obstante, podemos consolidar estes procedimentos como uma excelente auditoria de segurança crucial para qualquer tipo de situação disponível que utiliza os serviços legados na área de TI, utilizando como base os protocolos TCP/IP.

Através dos métodos utilizados nos testes de penetração, podemos definir dois tipos de situações comumente utilizados na área de varredura pelo analista de segurança, denominadas de Black Box e White Box. A seguir, veremos as definições de cada uma e como se resume a sua aplicabilidade nos testes do sistema-alvo a ser verificado.

Black Box (Teste da Caixa Preta)

Definição no português de caixa preta caracteriza a falta de conhecimento prévio de toda a infraestrutura do sistema-alvo que será testado. Portanto, é necessária a pormenorização de todos os dados analisados, a fim de determinarmos a sua localização e dimensão dos sistemas e aplicativos envolvidos, antes de podermos aplicar as técnicas de análises pretendidas ao sistema-alvo.

O Black Box, ou caixa preta, simulam varreduras de ataques em cima de conhecimentos específicos do sistema-alvo, possibilitando auditar de forma

significativa a estrutura do sistema. Isto possibilita estratégias de aperfeiçoamentos que contribuirão com um sistema mais eficiente.

WHITE BOX (Teste da Caixa Branca)

Definido como teste de caixa branca caracteriza que quem vai aplicar os testes no sistema possui total conhecimento da estrutura do sistema-alvo, incluindo toda a sua magnitude de informações, como diagrama de rede, tipos de endereçamentos IP de redes utilizados, bem como qualquer informação adquirida, seja por engenharia social ou técnicas adjacentes com propósitos peculiares ao objetivo.

White Box executa simulações reais em um ambiente de produção durante o expediente de uma empresa ou quando pode ocorrer a disseminação de informações não autorizadas - termo conhecido como "vazamento de informações" -, comumente utilizados em espionagens industriais. Nesta situação o invasor pode ter acesso ao código fonte do sistema, algo altamente comprometedor, bem como conhecimento de toda estrutura física da rede, como esquemas, endereços, routers, etc, ampliando a possibilidade de deter ainda informações mais preciosas, como senhas de administradores ou usuários-chaves do sistema-alvo.

Resumo do Capítulo

Neste capítulo, mostramos como instalar o BackTrack e como preparar nosso ambiente para testes utilizando máquina virtual. Foram apresentadas as configurações básicas do LinuxBackTrack, como configurações de rede e serviços. Você também pode acompanhar os princípios e metodologias que envolvem um teste de penetração.