**INE5680 – SEGURANÇA DE REDES, SISTEMAS E APLICAÇÕES**

**Laboratório Virtual para INE5680-2013.2

VIRTUALBOX**

**Instalação do Virtualbox (pode ser no seu Windows, Linux, MAC OS).**

<https://www.virtualbox.org/wiki/Downloads>

**VirtualBox platform packages**. The binaries are released under the terms of the GPL version 2.

* **VirtualBox 4.3 for Windows hosts** [x86/amd64](http://download.virtualbox.org/virtualbox/4.2.18/VirtualBox-4.2.18-88781-Win.exe)
* **VirtualBox 4.3 for OS X hosts** [x86/amd64](http://download.virtualbox.org/virtualbox/4.3.0/VirtualBox-4.3.0-89960-OSX.dmg)
* [**VirtualBox 4.3 for Linux** **hosts**](https://www.virtualbox.org/wiki/Linux_Downloads)

**VirtualBox 4.3 Oracle VM VirtualBox Extension Pack**
Convém instalar para se ter VMs mais completas:

 Oracle\_VM\_VirtualBox\_Extension\_Pack-4.2.18-88780 (a última versão)

**User Manual**

* [User Manual](http://download.virtualbox.org/virtualbox/4.3.0/UserManual.pdf) ([HTML version](https://www.virtualbox.org/manual/UserManual.html))
* [Frequently asked questions list](https://www.virtualbox.org/wiki/User_FAQ).

**------------------------------------------------------------------------------------------------------------------------------**

**CRIAÇÃO DAS VMs NO VIRTUALBOX**

**Entre no Gerenciador de VMs do Virtualbox instalado em sua máquina.
Para criar máquinas virtuais, clique em NOVO. Siga as instruções do gerenciador.

A) Dê nome para sua VM. Use os nomes para este lab:
 Backtrack 5 R3, Metasploitable Linux, Windows Server 2008.

B) Escolha o SO (nome, tipo e versão)

C) Indique o tamanho da memória (você pode seguir a sugestão do Virtualbox)

D) No Virtualbox, devem ser gerados arquivos:**

* **CRIAR UM DISCO RÍGIDO VIRTUAL AGORA (se escolher este, na próxima tela escolha o tipo de arquivo: VDI (Virtualbox Disk Image)**
* **UTILIZAR UM DISCO RÍGIDO VIRTUAL EXISTENTE (escolha este se você já tem a VM e pode utilizar o arquivo VMDK (Virtual Machine Disk), usado no ambiente de virtualização Vmware.**

**E) Use ARMAZENAMENTO EM DISCO RÍGIDO FÍSICO : Dinamicamente Alocado**

**F) LOCALIZAÇÃO E TAMANHO DO ARQUIVO:
Indique a sugestão do Virtualbox. Mas e, situações de VM Windows Server 2012, por exemplo, você pode alocar mais, do que o sugerido, por exemplo, 40Mb, ao invés de 25 Mb usual no Windows Server 2008.**

**G) Selecione o Disco Rígido de: DRIVER DO HOSPEDEIRO D:

 GA) Entre com um CD ou DVD no seu drive de disco, que contenha o arquivo .ISO de seu
 OS ou ferramenta virtualizado.

 GB) Ou escolha um arquivo .VMDK que você obteve, contendo seu SO ou ferramenta
 (neste caso você pode ter, por exemplo, um firewall funcionando em um apropriado
 SO, como o exemplo do FreeBSD-pfSense., uma VM que é um firewall.**

**Praticamente, sua VM já estará criada e você precisa, agora, é executá-la para vê-la rodando e testá-la. Procure ver a senha de administrador. Normalmente, em algumas VMs Linux, estas já vem pré-configuradas. Você pode usar essas senhas, como é visto a seguir.**

 **CONFIGURAÇÃO DE CADA VM**

**Com a VM criada, selecione a VM, clicando com o botão esquerdo de seu mouse. vá em Configurações e selecione Rede.

Você verá os quatro adaptadores de rede existentes no Virtualbox: Adaptador 1, Adaptador 2, ... Use Adaptador 1 com NAT e Adaptador 2 com Rede Interna. Neste caso, indique o nome sua rede virtual, aqui chamada de VLAN1. Esta rede virtual VLAN1 tem nela, para o nosso lab virtual, as seguintes VMs, como mostradas abaixo com suas respectivas senhas.**

**CONFIGURAÇÕES DAS MÁQUINAS VIRTUAIS (VMs)**

**Para o laboratório de INE5680-Segurança de Redes, Sistemas e Aplicações, precisamos de, no mínimo, as seguintes máquinas configuradas:**

1. **VM 1 – Backtrack 5 R3 (contém várias ferramentas instaladas, usadas na área de segurança, mas pode-se instalar outras, caso necessário. Backtrack é um Linux apropriado para ferramentas de segurança).**

**User: root**

**Pass: toor**

1. **VM 2 – Metasploitable Linux (Este é um SO vulnerável intencionalmente.)

User: msfadmin
Pass: msfadmin**
2. **VM3 – Windows Server 2008
Pressione CRTL + ALT + DELETE (teclas pelo lado direito do teclado). Caso não consiga logo chegar na tela de logon e aparecer tela azul com várias opções iniciais, clique em CANCELAR. Insista até que apareça:

Administrador
Pass: toor**

**CONFIGURAÇÃO DAS INTERFACES DE REDE EM LINUX**

**Para as VMs Backtrack 5 R3, Ubuntu 11.10 ou 12.04 e Metasploitable Linux)

Em Linux, a partir do diretório raiz ( / ), entrar no sub-diretório ( /etc/network/ ).
Verifique a existência do arquivo “interfaces”. Abra este com o editor “nano”. Aparecerá:

# This file describes the network interfaces available in your system
# and how to activate them. For more information, see interfaces (5).**

**# The loopback network interface
auto lo
iface lo inet loopback**

**# The primary network interface**

**auto eth0**

**iface eth0 inet dhcp**

**# The secondary network interface**

**auto eth1**

**iface eth1 inet static**

**address 192.168.1.xxx**

**network 192.168.1.0**

**netmask 255.255.255.0**

**broadcast 192.168.1.255**

**Onde xxx = 113 (Backtrack 5 R3)
 xxx = 114 (Metasploitable Linux)
 xxx = 115 (Ubuntu 11.10 ou Ubuntu 12.04)**

**----------------------------------------------------------

 CONFIGURAÇÃO DAS INTERFACES DE REDE EM WINDOWS**

 **Para VMs Windows Server (2003, 2008, 2012)

Windows Server 2003, era vulnerável e um exemplo de ataque possível, você pode encontrar em “Auditoria com Teste de Invasão**

 **Configurar Windows Server 2008 (Caso apareça tela para ativar, ignore, pois esta cópia. Este Windows foi obtido da Microsoftware, através do INE).

Painel de Controle -> Central de Rede e Compartilhamento
-> Gerenciar Conexões de Rede ->

Aparece:
-----------------------------------------
Intel® Pro/1000 RT Desktop Adapter (1)
Conexão Local
Rede
Intel® Pro/1000 RT Des ...**

**Clicar 2 vezes em Conexão Local para Ativar.**

**-----------------------------------------
Intel® Pro/1000 RT Desktop Adapter #2 (1)**

**Conexão Local 2
Rede não identificada
Intel® Pro/1000 RT Des ...**

**Clicar 2 cliques em Conexão Local 2 -> Clicar Propriedades (à esquerda) -> Configurar Protocolo TCP/IP Versão 4 (TCP/IP v4)-> Clicar Propriedades (à direita) ->

Configurar:
 Usar o seguinte endereço IP:
 Endereço IP: 192.168.1.116
 Máscara de sub-rede: 255.255.255.0

significando que os três primeiros bytes 192.168.1 é endereço de rede e 116 é endereço da máquina na rede VLAN1.**

 **Gateway padrão: 192.168.1.254
(pode ser definida uma VM que controla entrada-saída da Internet para a rede virtual VLAN1 (nome da rede virtual no Virtualbox Adapter 2) -> OK**

----------------------------------------

 **Caso exista na VLAN1, Windows Server 2012**

 **Configurar Windows Server 2012**

 **Fazer a mesma configuração que na VM Windows Server 2008,
 mas supondo, agora, que:**

 **Endereço IP: 192.168.1.118
 Máscara de sub-rede: 255.255.255.0
 Gateway padrão: 192.168.1.254**

**--------------------------------------------------------------------------------------------------------------------------------**

**ROTEIRO PAR AUDITORIA COM TESTE DE PENETRAÇÃO**

**Utilização de Ferramentas e VMs SOs**

1. **Nmap (Scanner de Rede) (Linux)**
2. **OpenVAS (Análise de Vulnerabilidades) (Linux)**
3. **Metasploit (via Backtrack 5 R3)
(Framework para exploração de vulnerabilidades no
 Metasploitable Linux e no Windows Server 2008)**

**----------------------------------------------------------------
----------------------------------------------------------------**

**CONFIGURANDO OUTRAS VMs**

**VIRTUALBOX

Livro: Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide, Editora PACKT, 2012.**

1. **VM pfSense (Um firewall que pode proteger sua rede virtual)

VM Kioptrix (Uma virtualização do sistema OS FreeBSD, vulnerável intencionalmente para vulnerabilidades** [**OWASP**](http://www.owasp.org/index.php/Main_Page) **– Top 10, que são as 10 vulnerabilidades mais ocorridas em ambientes Web). OWASP porpõe correções ...

As VMs aqui configuradas podem ser usadas para aprendizado sobre auditoria com Teste de Penetração em sistemas Web.**
2. **VM Kioptrix Level 1**
3. **VM Kioptrix Level 2**
4. **VM Kioptrix Level 3**
5. **Clone VM Kioptrix Level 3**
6. **VM kioptrix Level 4**

 **As VMs escritas em azul podem ser inicialmente utilizadas em testes de penetração em sistemas web.**

**----------------------------------------------------------------
----------------------------------------------------------------**