Tarefa Prática 1 - Nmap, Web, Shodan, Metasploit

Nomes:

Bruno Aurélio Rôzza de Moura Campos (14104255)
Caio Cargnin Cardoso (09138003)

Matéria:

- Segurança da informação e sistemas - INE5680

Arquivo de Configuração:

- configurar_kali_e_OWASP_broken_no_virtualbox_e_Instalar_muti

Arquivo de Descrição do trabalho:

- INE5680-tarefa_pratica_metasploit_v14.pdf

PARTE 1.NMAP

Questão 1.

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

```
root@kali:~# nmap -sV -O 10.1.2.8
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-04 09:32 EDT
Nmap scan report for 10.1.2.8
Host is up (0.00045s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_py
thon/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL...)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap        Courier Imapd (released 2008)
443/tcp  open  ssl/https?
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp open  java-rmi    Java RMI
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
8081/tcp open  http        Jetty 6.1.25
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.
org/cgi-bin/submit.cgi?new-service :
SF-Port5001-TCP:V=7.70%I=7%D=4/4%Time=5CA60757%P=x86_64-pc-linux-gnu%r(NUL
SF:L,4,"\xac\xed\0\x05");
MAC Address: 08:00:27:F3:4A:C2 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.17 - 2.6.36
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.32 seconds
```

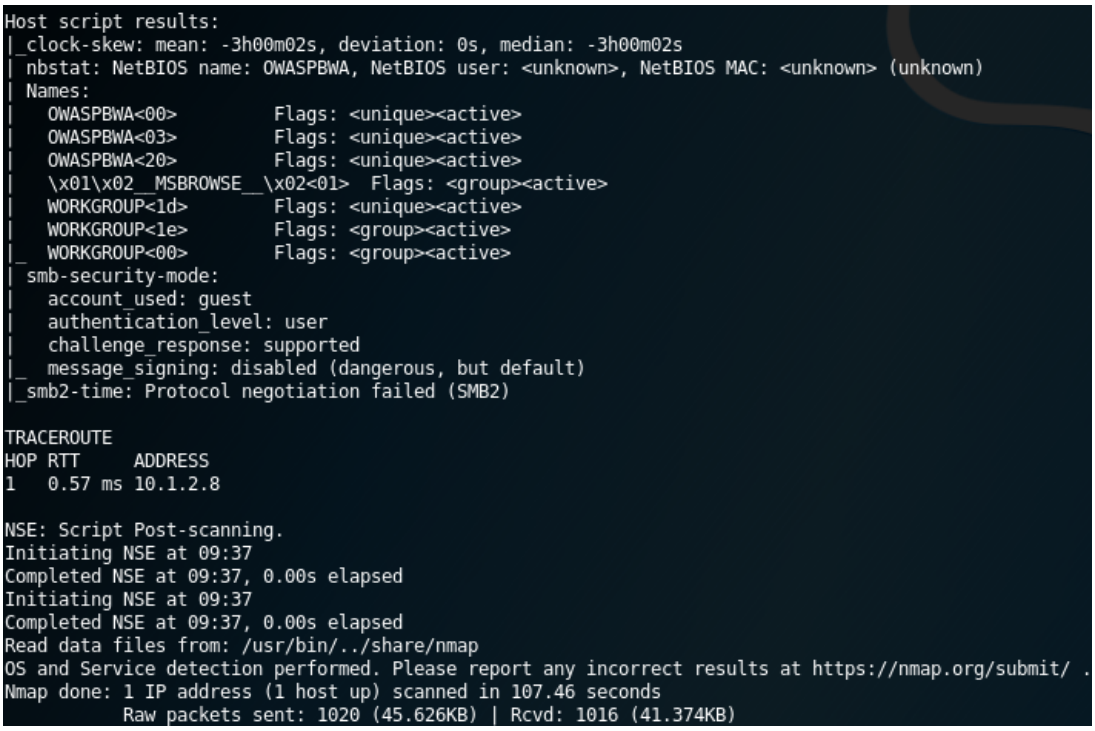
- Os parâmetros `-sV` servem para: detectar portas abertas para determinar informações de serviço / versão. Neste caso foi encontrado 9 portas abertas executando serviços do tipo ssh, http, imap, netbios-ssn, java-rmi e ssl.
- O parâmetro `-O` serve para detectar o sistema operacional.

Questão 2.

`nmap -v –A 10.1.2.6` (IP da máquina Owasp Broken)

```
root@kali:~# nmap -v -A 10.1.2.8
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-04 09:35 EDT
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 09:35
Completed NSE at 09:35, 0.00s elapsed
Initiating NSE at 09:35
Completed NSE at 09:35, 0.00s elapsed
Initiating ARP Ping Scan at 09:35
Scanning 10.1.2.8 [1 port]
Completed ARP Ping Scan at 09:35, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:35
Completed Parallel DNS resolution of 1 host. at 09:35, 0.16s elapsed
Initiating SYN Stealth Scan at 09:35
Scanning 10.1.2.8 [1000 ports]
Discovered open port 8080/tcp on 10.1.2.8
Discovered open port 80/tcp on 10.1.2.8
Discovered open port 143/tcp on 10.1.2.8
Discovered open port 445/tcp on 10.1.2.8
Discovered open port 22/tcp on 10.1.2.8
Discovered open port 139/tcp on 10.1.2.8
Discovered open port 443/tcp on 10.1.2.8
Discovered open port 5001/tcp on 10.1.2.8
Discovered open port 8081/tcp on 10.1.2.8
Completed SYN Stealth Scan at 09:35, 0.10s elapsed (1000 total ports)
Initiating Service scan at 09:35
Scanning 9 services on 10.1.2.8
Completed Service scan at 09:35, 14.03s elapsed (9 services on 1 host)
Initiating OS detection (try #1) against 10.1.2.8
NSE: Script scanning 10.1.2.8.
Initiating NSE at 09:35
Completed NSE at 09:37, 91.02s elapsed
Initiating NSE at 09:37
Completed NSE at 09:37, 0.01s elapsed
Nmap scan report for 10.1.2.8
Host is up (0.00057s latency).
Not shown: 991 closed ports
```

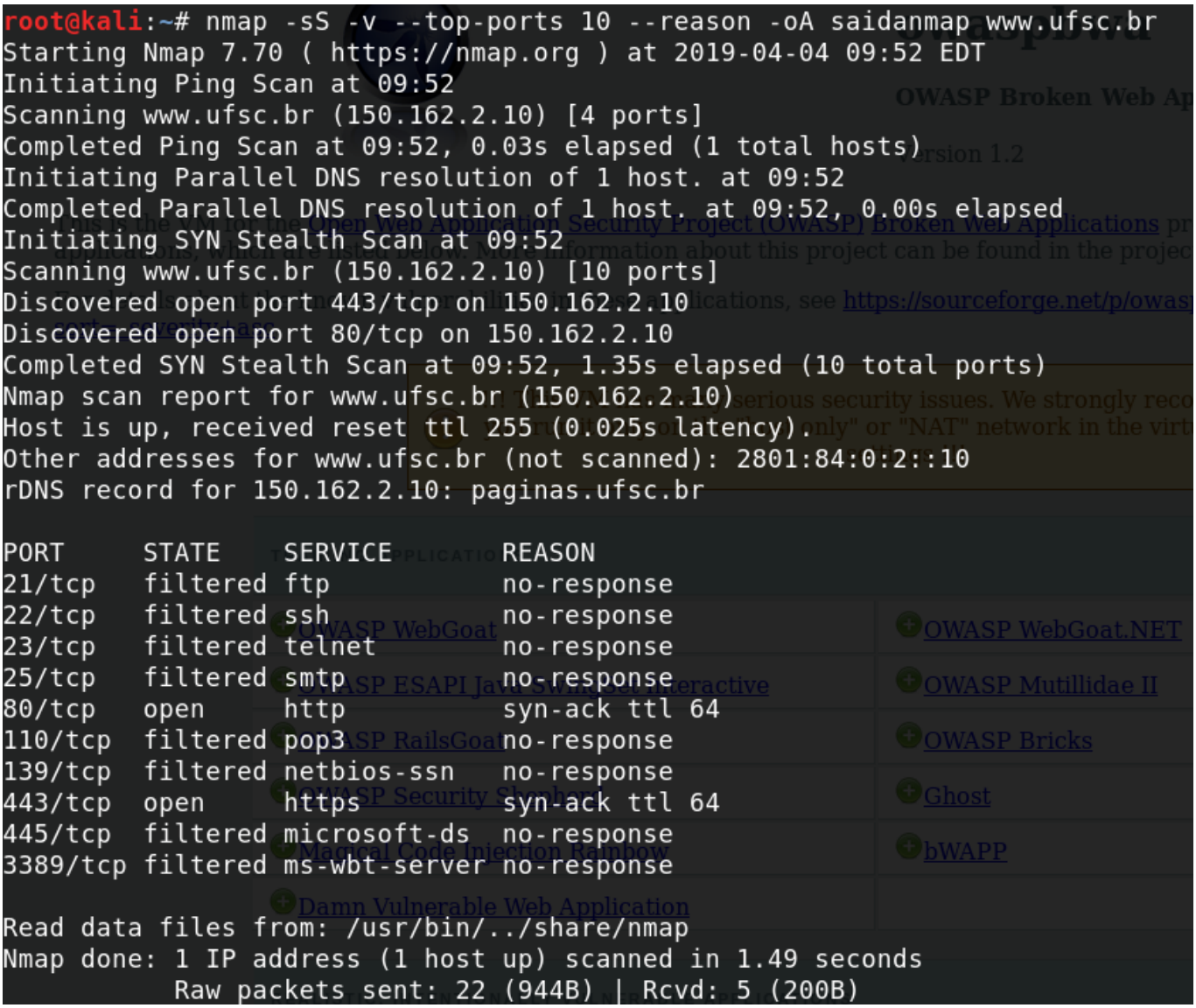
```
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ea:83:1e:45:5a:a6:8c:43:1c:3c:e3:18:dd:fc:88:a5 (DSA)
|_  2048 3a:94:d8:3f:e0:a2:7a:b8:c3:94:d7:5e:00:55:0c:a7 (RSA)
80/tcp   open  http        Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 O
penSSL...)
|_http-favicon: Unknown favicon MD5: 1F8C0B08FB6B556A6587517A8D5F290B
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8
k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
|_http-title: owaspbwa OWASP Broken Web Applications
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap        Courier Imapd (released 2008)
|_imap-capabilities: QUOTA THREAD=ORDEREDSUBJECT IMAP4rev1 completed CHILDREN CAPABILITY THREAD=REFERENCES OK SORT IDLE ACL2=UNIONA0001 ACL NAMESPACE UIDPLUS
443/tcp  open  ssl/https?
|_ssl-date: 2019-04-04T10:35:39+00:00; -3h00m02s from scanner time.
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp open  java-rmi    Java RMI
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Site doesn't have a title.
8081/tcp open  http        Jetty 6.1.25
| http-methods:
|   Supported Methods: GET HEAD POST TRACE OPTIONS
|_  Potentially risky methods: TRACE
|_http-server-header: Jetty(6.1.25)
|_http-title: Choose Your Path
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5001-TCP:V=7.70%I=7%D=4/4%Time=5CA6081F%P=x86_64-pc-linux-gnu%r(NUL
SF:L,4,"\xac\xed\0\x05");
MAC Address: 08:00:27:F3:4A:C2 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.17 - 2.6.36
Uptime guess: 0.029 days (since Thu Apr  4 08:56:04 2019)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=205 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



- O parâmetro `-v` serve para retornar as ações do nmap de modo verboso.
- O parâmetro `-A` serve para detectar alem da sistema operacional do host atacado, as portas abertas, o estado das portas, o serviço que roda em cada porta e qual a versão que esta sendo executado. Com este parâmetro é rodado um script scanning, e traceroute, conforme figura 4.

Questão 3.

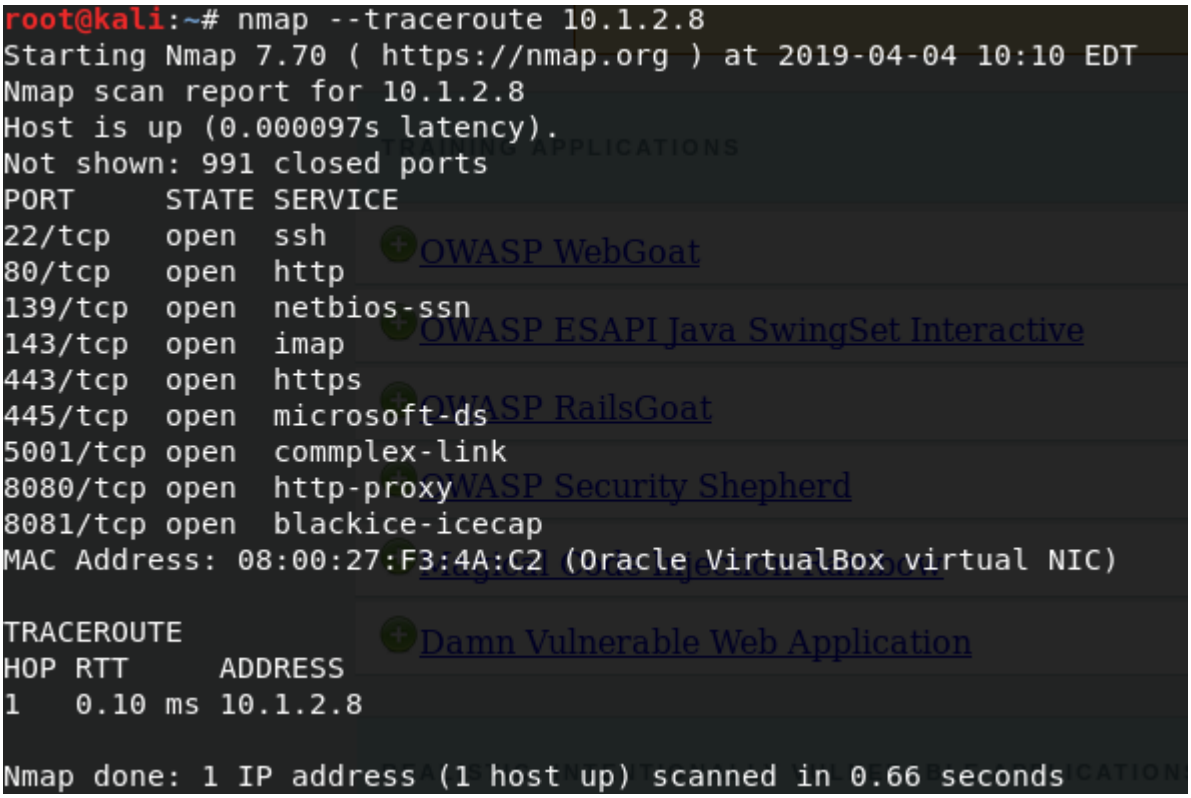
```
nmap –sS –v --top-ports 10 --reason -oA saidanmap www.ufsc.br
```



- O parâmetro `-sS` serve para retornar os pacotes TCP SYN. Na imagem 5, na coluna REASON é mostrado quais portas com os seus respectivos serviços retornaram algum resposta.
- O parâmetro `-v` serve para retornar as ações do nmap de modo verboso.
- O parâmetro `--top-ports 10` retorna as portas mais comuns.
- O parâmetro `--reason` mostra o motivo pelo qual uma porta está em um estado específico.
- O parâmetro `-oA` mostra os três principais formatos de uma só vez.
  Alem disso foi gerado 3 arquivos, `saidanmap.gnmap`, `saidanmap.nmap` e `saidanmap.xml` contendo uma tabela com a porta, estado, serviço e motivo do estado da porta, alem dos parâmetros, verbose, debugging, host, address, hostnames e scaninfo.

Questão 4.

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



- O parâmetro `--traceroute` mostra todos os saltos e hosts passados até o alvo.

Questão 5.

a. Qual a diferença entre um scan de conexão TCP e um SYN scan ?

- O scan TCP SYN é relativamente não-obstrusivo e camuflado, uma vez que ele nunca completa uma conexão TCP. Ele também permite uma diferenciação limpa e confiável entre os estados aberto (open), fechado (closed), e filtrado (filtered).
- O scan TCP é o scan padrão do TCP. Esse é o caso quando o usuário não tem privilégios para criar pacotes em estado bruto.

b. Qual questão anterior usa scan de conexão TCP e qual questão usa SYN scan?

- A questão 3 usa `-sS (scan TCP SYN)` e segundo o site do nmap por default o Nmap executa um scan SYN, então as questão 1 tambem utilizam um `scan TCP SYN`. Já a questão 2 usa `scan TCP`.

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

- Na questão 3 foi lista na porta TCP 445 uma serviço microsoft-ds. Este serviço apresenta uma vulnerabiliade que pode permite ataques remotos para causar DOS (denial of service).
  Esta vulnerabilidade foi catalogada na CVE com as sequintes informações:

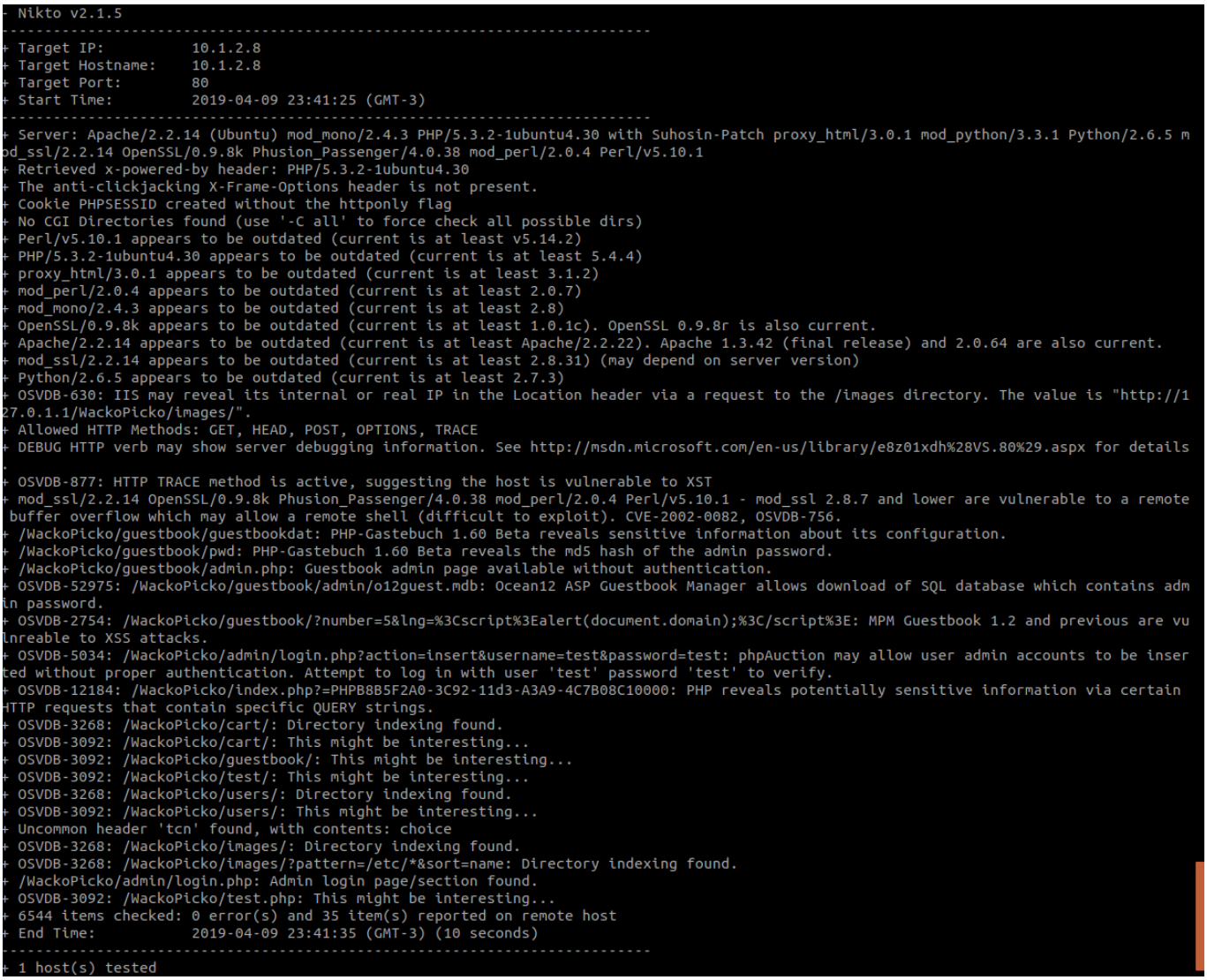
CVE-ID: CVE-2002-0597
Description: LANMAN service on Microsoft Windows 2000 allows remote attackers to cause a denial of service (CPU/memory exhaustion) via a stream of malformed data to microsoft-ds port 445.
Date Entry Created: 20030402

PARTE 2.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.



```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.1.2.8
+ Target Hostname:    10.1.2.8
+ Target Port:        80
+ Start Time:         2019-04-09 23:41:25 (GMT-3)
---------------------------------------------------------------------------
+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 m
od_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
+ Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.30
+ The anti-clickjacking X-Frame-Options header is not present.
+ Cookie PHPSESSID created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Perl/v5.10.1 appears to be outdated (current is at least v5.14.2)
+ PHP/5.3.2-1ubuntu4.30 appears to be outdated (current is at least 5.4.4)
+ proxy_html/3.0.1 appears to be outdated (current is at least 3.1.2)
+ mod_perl/2.0.4 appears to be outdated (current is at least 2.0.7)
+ mod_mono/2.4.3 appears to be outdated (current is at least 2.8)
+ OpenSSL/0.9.8k appears to be outdated (current is at least 1.0.1c). OpenSSL 0.9.8r is also current.
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.2.22). Apache 1.3.42 (final release) and 2.0.64 are also current.
+ mod_ssl/2.2.14 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ Python/2.6.5 appears to be outdated (current is at least 2.7.3)
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images directory. The value is "http://1
27.0.1.1/WackoPicko/images/".
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details
.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1 - mod_ssl 2.8.7 and lower are vulnerable to a remote
 buffer overflow which may allow a remote shell (difficult to exploit). CVE-2002-0082, OSVDB-756.
+ /WackoPicko/guestbook/guestbookdat: PHP-Gastebuch 1.60 Beta reveals sensitive information about its configuration.
+ /WackoPicko/guestbook/pwd: PHP-Gastebuch 1.60 Beta reveals the md5 hash of the admin password.
+ /WackoPicko/guestbook/admin.php: Guestbook admin page available without authentication.
+ OSVDB-52975: /WackoPicko/guestbook/admin/o12guest.mdb: Ocean12 ASP Guestbook Manager allows download of SQL database which contains adm
in password.
+ OSVDB-2754: /WackoPicko/guestbook/?number=5&lng=%3Cscript%3Ealert(document.domain);%3C/script%3E: MPM Guestbook 1.2 and previous are vu
lnreable to XSS attacks.
+ OSVDB-5034: /WackoPicko/admin/login.php?action=insert&username=test&password=test: phpAuction may allow user admin accounts to be inser
ted without proper authentication. Attempt to log in with user 'test' password 'test' to verify.
+ OSVDB-12184: /WackoPicko/index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain
HTTP requests that contain specific QUERY strings.
+ OSVDB-3268: /WackoPicko/cart/: Directory indexing found.
+ OSVDB-3092: /WackoPicko/cart/: This might be interesting...
+ OSVDB-3092: /WackoPicko/guestbook/: This might be interesting...
+ OSVDB-3092: /WackoPicko/test/: This might be interesting...
+ OSVDB-3268: /WackoPicko/users/: Directory indexing found.
+ OSVDB-3092: /WackoPicko/users/: This might be interesting...
+ Uncommon header 'tcn' found, with contents: choice
+ OSVDB-3268: /WackoPicko/images/: Directory indexing found.
+ OSVDB-3268: /WackoPicko/images/?pattern=/etc/*&sort=name: Directory indexing found.
+ /WackoPicko/admin/login.php: Admin login page/section found.
+ OSVDB-3092: /WackoPicko/test.php: This might be interesting...
+ 6544 items checked: 0 error(s) and 35 item(s) reported on remote host
+ End Time:           2019-04-09 23:41:35 (GMT-3) (10 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

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.

O que mais nos chamou a atenção foram 2 pontos:

- Não há autenticação para ser admin do servidor: `+ /WackoPicko/guestbook/admin.php: Guestbook admin page available without authentication.`
- É possível baixar todo o banco de dados: `+ OSVDB-52975: /WackoPicko/guestbook/admin/o12guest.mdb: Ocean12 ASP Guestbook Manager allows download of SQL database which contains admin password.`

Sobre as vulnerabilidades, o nikto retornou o arquivo `nikto.html` contendo todas as vulnerabilidades encontrada:

URI	/WackoPicko/WackoPicko/guestbook/admin.php
HTTP Method	GET
Description	/WackoPicko/guestbook/admin.php: Guestbook admin page available without authentication.
Test Links	http://10.1.2.8:80/WackoPicko/WackoPicko/guestbook/admin.php http://10.1.2.8:80/WackoPicko/WackoPicko/guestbook/admin.php
OSVDB Entries	OSVDB-0

Nesta vulnerabilidade da imagem acima é notável observar que através de uma requisição HTTP GET é possível ter acesso privilegiado na página sem necessitar de autenticação.

PARTE 3.OWASP –Vulnerabilidades em Aplicações Web

Questão 7.

Explique as vulnerabilidades A1, A2, A3 e A7 do documento TOP TEN2017:

- A1: injection - É uma falha na codificação de uma aplicação qualquer (seja web ou local) que permite ao atancate inserir uma consulta SQL
- A2: Broken Authentication - É uma vulnerabilidade nas sessões nas aplicações que utilizam autenticação que permite aos invasores comprometerem senhas, tokens de sessão ou explorem outras falhas de implementação para assumir as identidades de outros usuários.
- A3: Sensitive Data Exposure - Refere-se a proteção incorreta dos dados críticos tais como, por exemplo, números de cartão de crédito, senhas, entre outros.
- A7: Cross-Site Scripting (XSS) - Os ataques XSS típicos incluem roubo de sessão, controle de conta, desvio de MFA, substituição ou desfiguração de nó DOM (como painéis de login de trojan), ataques contra o navegador do usuário, como downloads de software mal-intencionado, registro de chaves e outros ataques do lado do cliente.
  Os alvos desta vulnerabilidade são os browsers dos usuários.
  Outro ponto importante sobre esta vulnerabilidade é que o problema de XSS é o segundo problema mais recorrente, registrado pelo OWASP Top 10.

Questão 8.

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 ‘or1=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).

O SQL INJECTION é o top 1 no relatório da OWASP 2017. Ao analisar o reltório é possível concluir que ao inserir o script `´'or 1=1 --` no campo de login é realizado um sql injection dá a possíbilidade de realizar o login, onde o script indica resultado verdadeiro, ignorando o restante da expressão.

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

A melhor forma de resolver o problema -e inserir uma validação dos dados de entrada tanto no campo de texto (front-end), quanto no back-end.

d. Clique em Logout.

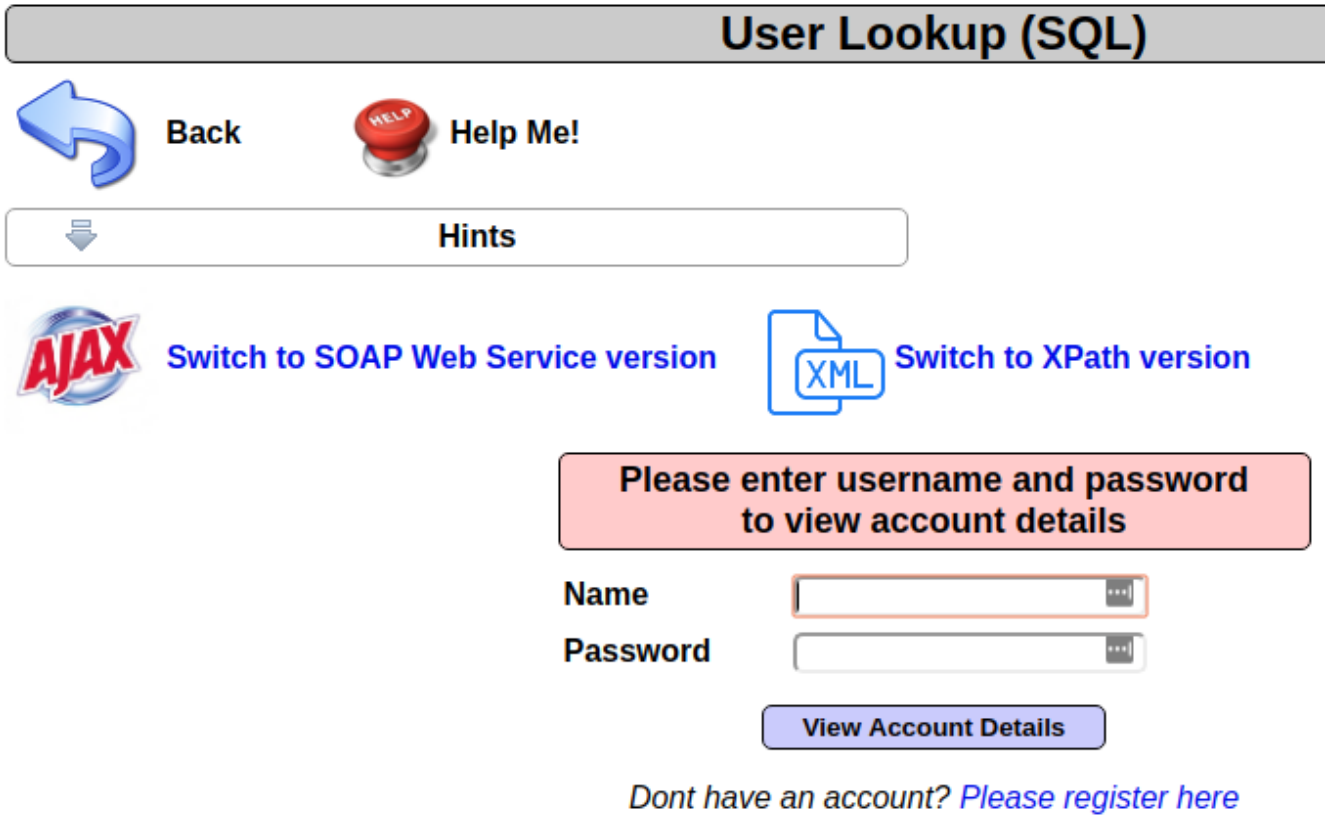
Questão 9.

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

a. Explique a vulnerabilidade explorada no experimento (pesquise no documento do TOP 10 da OWASP).

Esta falha de segurança ocorreu tambem por sql injection onde foi possível fazer a consulta de usuários com seus respectivos login e senha.
Sobre a query executada, o 1=1 faz retornar `true` e com o comentário (--) ignora a validação da senha.
Segundo o documento do TOP 10 da OWASP, o sql injection pode resultar em perda de dados, corrupção ou divulgação para partes não autorizadas, perda de responsabilidade ou negação de acesso. Alem disso, pode levar a uma aquisição completa do host.

b. Copie e cole um screenshot da execução de um experimento.



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

A melhor opção é usar uma API segura para realizar a autenticação.

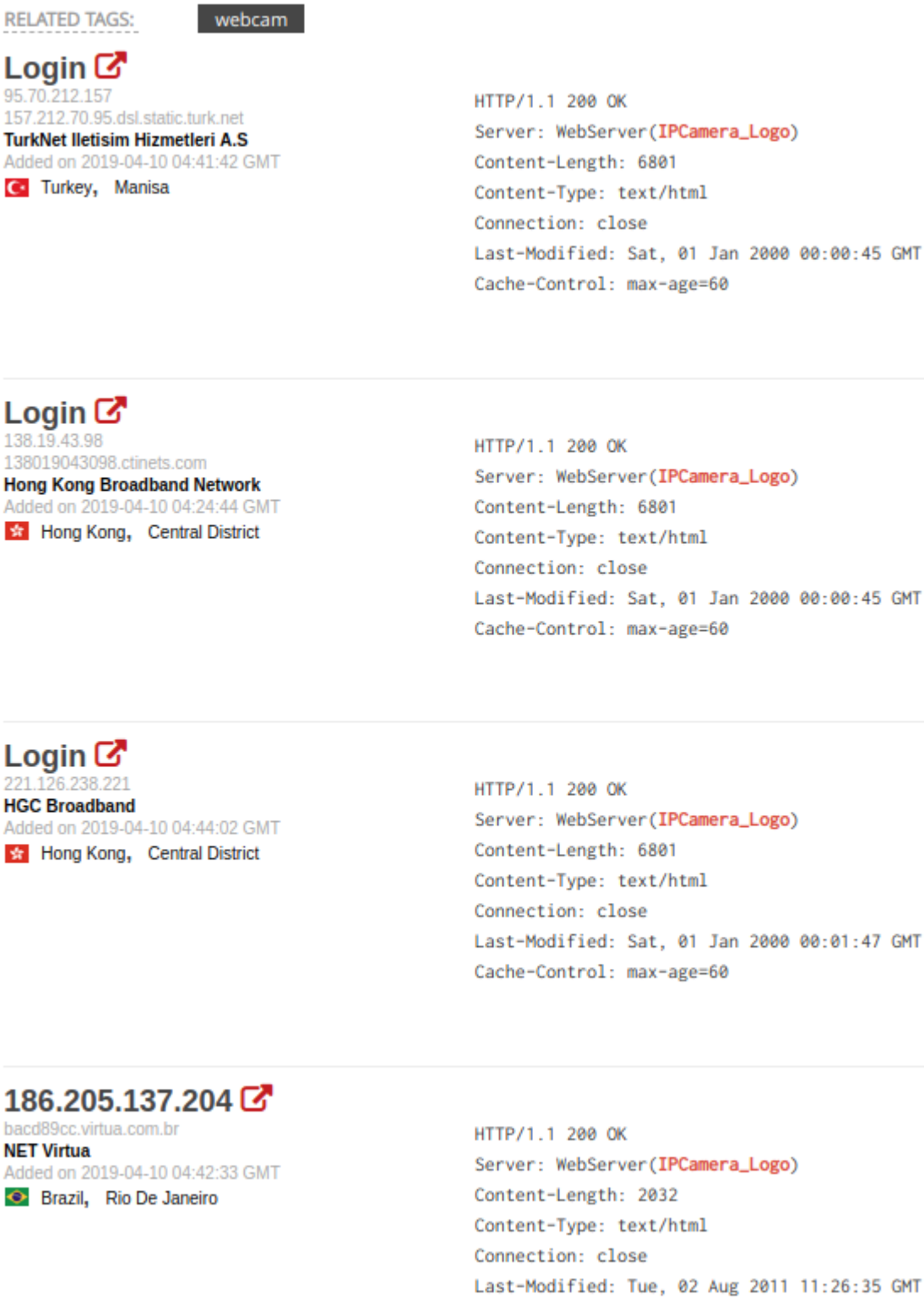
PARTE 4.Vulnerabilidades em IoT

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 Shodane o que é possível fazer com este site?
O Shodan é um scanner que encontra dispositivos conectados pela internet. O Shodan pode encontrar dispositivos como semáforos, câmeras de segurança, dispositivos de aquecimento doméstico e monitores de bebês. Este scanner da web também pode encontrar o sistema SCADA como estações de gás, usinas nucleares. Shodan informa a localização física dos dispositivos conectados pela internet.

b. (Apresentação) Faça o registro no site, pesquise e liste algum dispositivo IoT que você encontrou.
Na figura abaixo, segue uma list com 4 cameras IP com acesso livre



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?**
É possível ter acesso a todas as configurações das câmeras.

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

Um ataque poderia ser o desligamento da câmera num período propício ou senão, as cameras podem ser utilizadas para realizar um ataque DDos.

PARTE 5.Metasploit

Questão 14.

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

```
RHOSTS => 10.1.2.8
msf5 auxiliary(scanner/http/tomcat_mgr_login) > set RPORTS 8080
RPORTS => 8080
msf5 auxiliary(scanner/http/tomcat_mgr_login) > exploit

[-] 10.1.2.8:8080 - LOGIN FAILED: admin:admin (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: admin:manager (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: admin:role1 (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: admin:root (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: admin:s3cret (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: admin:vagrant (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: manager:admin (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: manager:manager (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: manager:role1 (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: manager:root (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: manager:tomcat (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: manager:s3cret (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: manager:vagrant (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: role1:admin (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: role1:manager (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: role1:role1 (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: role1:root (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: role1:tomcat (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: role1:s3cret (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: role1:vagrant (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: root:admin (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: root:manager (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: root:role1 (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: root:root (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: root:tomcat (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: root:s3cret (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: root:vagrant (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: tomcat:root (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: tomcat:tomcat (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: tomcat:s3cret (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: tomcat:vagrant (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: both:admin (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: both:manager (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: both:role1 (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: both:root (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: both:s3cret (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: both:vagrant (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: j2deployer:j2deployer (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: ovwebusr:OvW*busr1 (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: cxsdk:kdsxc (Incorrect)
[+] 10.1.2.8:8080 - Login Successful: root:owaspbwa
[-] 10.1.2.8:8080 - LOGIN FAILED: ADMIN:ADMIN (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: xampp:xampp (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: tomcat:s3cret (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: QCC:QLogic66 (Incorrect)
[-] 10.1.2.8:8080 - LOGIN FAILED: admin:vagrant (Incorrect)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/tomcat_mgr_login) >
```

a. O que é o ataque do dicionário?
É um ataque que utiliza um banco de dados com logins e senhas para tentar descobrir os dados da vítima através da força bruta.

b. O que foi encontrado?
Foi possível encontrar o login e senha da vítima.

c. Qual foi a vulnerabilidade usada para obter esse resultado?
Vulnerabilidade: CVE-2009-4189
A vítima usa uma senha padrão, o que permite que o atacante possa executar um ataque arbitrário utilizando força bruta e tenha acesso ao terminal da máquina dela através do Tomcat.

d. Como pode ser explorado esse resultado?
Com o login e senha, é possível fazer um acesso remoto na máquina da vítima e ter controle sobre ela.

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?
Backdoor.

b. O que faz o exploit para explorar a vulnerabilidade?
O exploit concede a um usuário não autorizado acesso no sistema da vítima de forma remota e assim executar comandos.

c. O que é o meterpreter?
Meterpreter é um payload do Metasploit que oferece ferramentas que auxiliam o invasor em um ataque, fornecendo informações sobre a vítima.

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.

- Comando `getsystem`: torna possível obter informações do sistema da vítima.
- Comando `clearev`: faz o wipe das informações de acessos (rastros)

Referências:

- https://nmap.org/ acesso 08/04/2019
- https://www.owasp.org/images/7/72/OWASP_Top_10-2017_(en).pdf.pdf acesso 08/04/2019