Roteiro 2 Segurança em Sistemas Operacionais

Matheus Freitas Sant'Ana

Exercício 1.1.a: Descubra qual ip do seu alvo.

Comandos utilizados:

- dhclient eth0 para alocar o IP à máquina.
- Ifconfig para descobrir o IP.

IP do alvo: 192.168.68.130

```
root@metasploitable:/home/msfadmin# dhclient eth0

There is already a pid file /var/run/dhclient.pid with pid 4736

killed old client process, removed PID file

Internet Systems Consortium DHCP Client V3.0.6

Copyright 2004-2007 Internet Systems Consortium.

All rights reserved.

For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth0/08:00:27:e1:a6:d4

Sending on LPF/eth0/08:00:27:e1:a6:d4

Sending on Socket follows:

DHCPREQUEST of 192.168.68.130 on eth0 to 255.255.255.255 port 67

DHCPACK of 192.100.00.13v irom 192.168.68.1

bound to 192.168.68.130 -- renewal in 3568 seconds.
```

Exercício 1.1.b: reconhecendo serviços e portas abertas do alvo.

Comandos utilizados:

telnet <IP_alvo> <porta>

Nome do Processo: FTP

Versão: vsFTPd 2.3.4

```
root@kali)-[/home/kali]
telnet 192.168.68.130 21
Trying 192.168.68.130 ...
Connected to 192.168.68.130.
```

Exercício 1.1.c:

Comandos utilizados:

nmap -O <IP_alvo>

Versão, Distribuição e Arquitetura do S.O.: Linux 2.6.9 – 2.6.33

```
")-[/home/kali]
-0 192.168.68.130
Nmap 7.92 (https://nmap.org ) at 2022-03-07 18:44 EST
warning: Unable to determine any DNS servers. Reverse DNS is disables in a system of the system 
                                                                                                      n ajp13
n unknown
08:00:27:51:A6:D4 (Oracle VirtualBox virtual NIC)
general purpose
ux 2.6.X
/oslinux, kernel:2.6
Linux 2.6.9 - 2.6.33
ance: 1 hop
detection performed. Please report any incorrect results at https://nmap.o
```

Exercício 1.1.d : Criação de Escaneamento de Portas com Python

Link Github: https://github.com/MatFreitas/PortScanner.git

Exercício 1.1.e : Listar as vulnerabilidades das portas 21 e 445

Comandos utilizados:

nmap -v -script malware <IP_alvo>

```
PORT STATE SERVICE
21/tcp open ftp
| ftp-vsftpd-backdoor:
| VULNERABLE:
| vsFTPd version 2.3.4 backdoor
| State: VULNERABLE (Exploitable)
| IDs: BID:48539 CVE:CVE-2011-2523
| vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
| Disclosure date: 2011-07-03
| Exploit results:
| Shell command: id
| Results: uid=0(root) gid=0(root)
| References:
| https://www.securityfocus.com/bid/48539
| https://cve.mitre.org/cgi-bin/cvename.cgi?name-CVE-2011-2523
| https://cve.mitre.org/cgi-bin/cvename.cgi?name-CVE-2011-2523
| https://github.com/rapid//metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
| http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
22/tcp open ssh
22/tcp open smtp
53/tcp open domain
80/tcp open http
|_http-malware-host: Host appears to be clean
111/tcp open rpcbind
139/tco open netbios-ssn
445/tcp open microsoft-ds
```

Exercício 1.1.f: Encontrar um exploit para uma vulnerabilidade nos serviços testados no exercício anterior.

A vulnerabilidade da porta 21 do alvo, cuja aplicação é o TCP, é que essa versão da aplicação possui uma backdoor pela qual é possível abrir um shell na porta 6200/tcp (vunerabilidade CVE de ID CVE-2011-2523).

Exercício 1.1.g : Encontrar uma CVE classificada como alta para os serviços das portas 3306 e 5432.

Uma CVE classificada como alta é aquela cuja nota é 7.0-8.9

Comandos utilizados:

nmap -sV –script vuln -p <porta> <IP_alvo>

Vulnerabilidade alta Porta 3306:

Vulnerabiliade de CVE-ID: CVE-2009-2446, que consiste em exploitar o a aplicação com múltiplas formatações de string dentro da função do dispatch_command dentro do mysql, o que permite um crash no servidor, por exemplo.

Porta 5432:

Vulnerabiliade de CCS injection, que consiste basicamente em um ataque "man-in-the-middle", em que é possível utilizar uma chave master de tamanho zero e invadir as sessões do alvo.

Exercício 1.1.h : Realize uma consulta ao nome www.ietf.org, e responda:

Comandos utilizados:

- nikto -h <URL>
- a. Qual é o endereço IP associado?

IP: 104.16.44.99

```
(root⊗ kali)-[/home/kali]

# nikto -h www.ietf.org

- Nikto v2.1.6

+ Target IP: 104.16.44.99

+ Target Hostname: www.ietf.org

+ Target Port: 80

+ Message: Multiple IP addresses found: 104.16.44.99, 104.16.45.99

+ Start Time: 2022-03-10 09:23:37 (GMT-5)
```

b. Quais são seus servidores DNS ?

Servidor DNS: cloudfare

c. Existe algum servidor de e-mail associado ao domínio etf.org? Qual o seu nome e IP?

Comandos utilizados:

host <URL>

Nome: mail.ietf.org

IP: 4.31.198.44

```
(root@kali)-[/home/kali]
  host ietf.org
ietf.org has address 4.31.198.44
ietf.org has IPv6 address 2001:1900:3001:11::2c
ietf.org mail is handled by 0 mail.ietf.org.
```

Exercício 1.1.i : Escolha um site na Internet e responda as seguintes perguntas:

a) Quais servidores DNS são responsáveis por este domínio? (print a sua consulta)

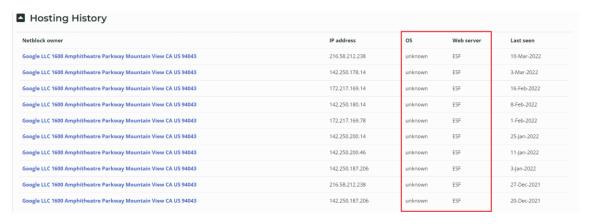
```
www.youtube.com using 4 DNS:
ns1.google.com (216.239.32.10)
ns2.google.com (216.239.34.10)
ns3.google.com (216.239.36.10)
ns4.google.com (216.239.38.10)

More Information »
```

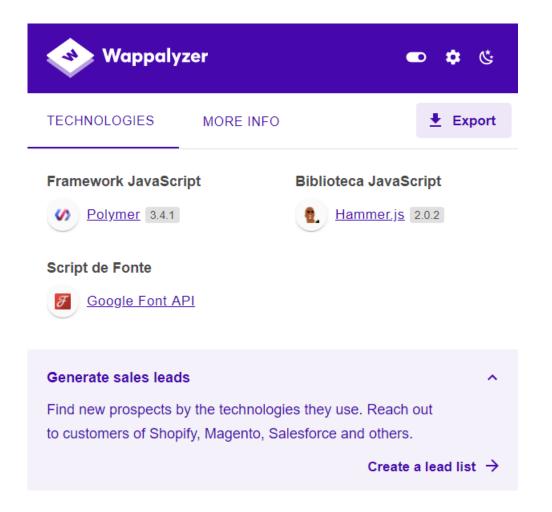
b) Existem outros domínios ou serviços hospedados no mesmo host (IP)? Quais são?

No	Web Site	Website IP Address \$	Web Hosting Company / IP Owner	Web Hosting / Server IP Location	Record Update Time \$	World Site Popular A Rating
1 🖽	google.com	142.250.74.238	Google Inc	■ USA	08 Mar 2022, 02:58	# 1
2 ±	youtube.com	142.250.74.238	Google Inc	USA	08 Mar 2022, 03:37	# 2
3 🖶	google.cn	142.250.74.227	Google Inc	■ USA	07 Mar 2022, 00:39	# 69
4 🖶	blogger.com	142.250.74.233	Google Inc	USA	07 Mar 2022, 00:39	# 128
5 ±	google.com.sg	142.250.74.227	Google Inc	■ USA	07 Mar 2022, 00:39	# 230
6 ±	google.co.id	142.250.74.227	Google Inc	■ USA	07 Mar 2022, 00:39	# 498
7 ₺	withgoogle.com	142.250.74.238	Google Inc	USA	07 Mar 2022, 00:39	# 2,604
8 #	google.co.ma	142.250.74.228	Google Inc	■ USA	07 Mar 2022, 00:39	# 4,597
9 #	google-analytics.com	142.250.74.228	Google Inc	■ USA	07 Mar 2022, 00:39	# 11,609
10 🖶	google.am	142.250.74.228	Google Inc	USA	07 Mar 2022, 00:39	# 30,313
11 🖶	www.mafiaol.com	142.250.74.243	Google Inc	■ USA	07 Mar 2022, 00:39	# 44,514
12 🖶	google.al	142.250.74.228	Google Inc	USA	07 Mar 2022, 00:39	# 74,601
13 🖶	www.brandiconimage.com	142.250.74.243	Google Inc	■ USA	07 Mar 2022, 00:39	# 114,651
14 🖶	lordfilm7.com	142.250.74.238	Google Inc	■ USA	07 Mar 2022, 00:39	# 122,921
15 🖶	google.ng	142.250.74.227	Google Inc	USA	07 Mar 2022, 00:39	# 126,116

c) Qual o Servidor WEB e Sistema Operacional que hospedam este site? Quais foram as últimas alterações?



d) Quais tecnologias (jquery, utilizadas por este site)?



e) Existe algum WAF protegendo este site? (Print a saída do comando)

Não existe, pois no Wappalyzer não existe nenhum WAF.

f) O Domínio possuí um servidor de e-mail configurado? Qual (is) Ip (s)?



Exercício 1.1.j:

```
Please enter the IP address to scan: 172.20.10.10
Do you wish to scan:
  A single port (1)
 A range of ports (2)
Please input option '1' or '2': 2
Please enter the port range to scan (example: '1-50'): 0-1024
Application METASPLOITABLE
Port 21 open
220 (vsFTPd 2.3.4)
Application METASPLOITABLE
Port 22 open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Application METASPLOITABLE
Port 25 open
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
Application METASPLOITABLE
Port 512 open
Where are you?
Application METASPLOITABLE
Port 514 open
```

Referências:	
https://repo.zenk-security.com/Programmation/Violent%20Python% %20A%20Cookbook%20for%20Hackers,%20Forensic%20Analyst 20Penetration%20Testers%20and%20Security%20Enginners.pdf	