

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/fallback
DHCPREQUEST of 192.168.68.130 on eth0 to 255.255.255.255 port 67
DHCPACK of 192.168.68.130 from 192.168.68.1
bound to 192.168.68.130 -- renewal in 3568 seconds.
```

```
root@metasploitable:/home/msfadmin# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e1:a6:d4
          inet addr:192.168.68.130  Bcast:192.168.68.255  Mask:255.255.255
          inet6 addr: fe80::a00:27ff:fe01:a6d4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:257 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20575 (20.0 KB)  TX bytes:11627 (11.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)
```

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.
Escape character is '^]'.
220 (vsFTPD 2.3.4)
```

Exercício 1.1.c:

Comandos utilizados:

- `nmap -O <IP_alvo>`

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

```
(root@kali)-[/home/kali]
# nmap -O 192.168.68.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-07 18:44 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.68.130
Host is up (0.00085s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rairegistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:EI:A6:D6 (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 2.6.9 - 2.6.33
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 2.06 seconds
```

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://github.com/rapid7/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
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
|_http-malware-host: Host appears to be clean
111/tcp   open  rpcbind
139/tcp   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 (vulnerabilidade 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:

Vulnerabilidade de CVE-ID: CVE-2009-2446, que consiste em explorar 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.

```
(root@kali)-[/home/kali]
# nmap -sV --script vuln -p 3306 192.168.50.65
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-10 08:34 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.50.65
Host is up (0.00091s latency).

PORT      STATE SERVICE VERSION
3306/tcp  open  mysql   MySQL 5.0.51a-3ubuntu5
|_ ssl-ccs-injection: No reply from server (TIMEOUT)
|_ vulners:
|   cpe:/a:mysql:mysql:5.0.51a-3ubuntu5:
|   SSV:19118      8.5   https://vulners.com/seebug/SSV:19118 *EXPLOIT*
|   CVE-2009-2446  8.5   https://vulners.com/cve/CVE-2009-2446
```

Porta 5432:

Vulnerabilidade 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.

```
(root@kali)-[/home/kali]
# nmap -sV --script vuln -p 5432 192.168.50.65
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-10 08:31 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.50.65
Host is up (0.00084s latency).

PORT      STATE SERVICE VERSION
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ ssl-poodle:
|   VULNERABLE:
|     SSL POODLE information leak
|     State: VULNERABLE
|     IDS: BID:70574 CVE:2014-3566
|     The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|     products, uses nondeterministic CBC padding, which makes it easier
|     for man-in-the-middle attackers to obtain cleartext data via a
|     padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.securityfocus.com/bid/70574
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|_ ssl-ccs-injection:
|   VULNERABLE:
|     SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|     OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|     does not properly restrict processing of ChangeCipherSpec messages,
|     which allows man-in-the-middle attackers to trigger use of a zero
|     length master key in certain OpenSSL-to-OpenSSL communications, and
|     consequently hijack sessions or obtain sensitive information, via
|     a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|     References:
|       http://www.cvedetails.com/cve/2014-0224
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|       http://www.openssl.org/news/secadv_20140605.txt
|_ ssl-ohp-patama:
|   VULNERABLE:
```

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: cloudflare

```
(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)
+ Server: cloudflare
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://www.ietf.org/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 3 item(s) reported on remote host
+ End Time: 2022-03-10 09:30:51 (GMT-5) (434 seconds)

1 host(s) tested
```

c. Existe algum servidor de e-mail associado ao domínio `ietf.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)

Website Nameservers: ⓘ

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 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.mafaiol.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?


Hosting History				
Netblock owner	IP address	OS	Web server	Last seen
Google LLC 1600 Amphitheatre Parkway Mountain View CA US 94043	216.58.212.238	unknown	ESF	10-Mar-2022
Google LLC 1600 Amphitheatre Parkway Mountain View CA US 94043	142.250.178.14	unknown	ESF	3-Mar-2022
Google LLC 1600 Amphitheatre Parkway Mountain View CA US 94043	172.217.169.14	unknown	ESF	16-Feb-2022
Google LLC 1600 Amphitheatre Parkway Mountain View CA US 94043	142.250.180.14	unknown	ESF	8-Feb-2022
Google LLC 1600 Amphitheatre Parkway Mountain View CA US 94043	172.217.169.78	unknown	ESF	1-Feb-2022
Google LLC 1600 Amphitheatre Parkway Mountain View CA US 94043	142.250.200.14	unknown	ESF	25-Jan-2022
Google LLC 1600 Amphitheatre Parkway Mountain View CA US 94043	142.250.200.46	unknown	ESF	11-Jan-2022
Google LLC 1600 Amphitheatre Parkway Mountain View CA US 94043	142.250.187.206	unknown	ESF	3-Jan-2022
Google LLC 1600 Amphitheatre Parkway Mountain View CA US 94043	216.58.212.238	unknown	ESF	27-Dec-2021
Google LLC 1600 Amphitheatre Parkway Mountain View CA US 94043	142.250.187.206	unknown	ESF	20-Dec-2021


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

 **Wappalyzer**   

TECHNOLOGIESMORE INFOExport

Framework JavaScript
 [Polymer](#) 3.4.1

Biblioteca JavaScript
 [Hammer.js](#) 2.0.2

Script de Fonte
 [Google Font API](#)

Generate sales leads ^
Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.
[Create a lead list](#) →

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

Não existe, pois no Wappalyzer não existe nenhum WAF.

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

```
Servidores MX:
www.youtube.com.      86400    IN      CNAME  youtube-ui.l.google.com.
```

Exercício 1.1.j:

Ao rodar o código no IP 172.217.162.174, que corresponde ao da URL www.youtube.com, não se encontraram portas abertas.

Referências:

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