# Roteiro 2 - Segurança em Sistemas Operacionais
# Marcelo Cesário Miguel

## 1. Reconhecimento o alvo

### a. Descubra qual ip do seu alvo.

Primeiro, realizei um netdiscover para ver os ips conectados na rede

```
Currently scanning: 192.168.43.0/16   |   Screen View: Unique Hosts

9 Captured ARP Req/Rep packets, from 7 hosts.   Total size: 540
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________

192.168.15.1    10:72:23:14:84:fd      3     180  TELLESCOM INDUSTRIA E COM
192.168.15.5    0c:54:15:39:67:b4      1      60  Intel Corporate
192.168.15.10   18:c0:4d:30:51:6b      1      60  GIGA-BYTE TECHNOLOGY CO.,
192.168.15.31   d4:a6:51:1d:b8:9c      1      60  Tuya Smart Inc.
192.168.15.48   00:05:16:62:e7:e3      1      60  SMART Modular Technologie
192.168.15.50   08:00:27:1d:77:8e      1      60  PCS Systemtechnik GmbH
192.168.15.51   0c:54:15:39:67:b4      1      60  Intel Corporate
```

Depois, realizei nmap no range de 192.168.15.1-254 com a flag -sV para identificar meu o metasploit

```
Nmap scan report for marcelo (192.168.15.50)
Host is up (0.000071s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service detection performed. Please report any incorrect results at https://nmap.
```

### b. reconhecendo serviços e portas abertas do alvo.

```
┌──(root㉿kali)-[/home/kali]
└─# telnet 192.168.15.50 21
Trying 192.168.15.50 ...
Connected to 192.168.15.50.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
421 Timeout.
Connection closed by foreign host.
```

## c. Fingerprint

Para descobrir o sistema operacional, realizei um nmap com a flag -O, tendo o mesmo resultado que o exercício anterior, porém com os dados do sistema operacional de cada ip.

```
Nmap scan report for 192.168.15.50
Host is up (0.0011s 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  rmiregistry
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: 08:00:27:1D:77:8E (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
```

## d. Criação de Escaneamento de Portas com Python.

Criei uma aplicação port.py que recebe como argumento o ip alvo, start port e end port, sendo as duas últimas o intervalo de portas tcp a serem analisadas.

**O arquivo pode ser encontrado aqui:**
**https://github.com/MarceloCMiguel/tec-hack/blob/master/h2/port.py**

```python
import socket
import sys

if len(sys.argv) == 4:
    ip = sys.argv[1]
    start = sys.argv[2]
    end = sys.argv[3]
    print(f"Checking open ports from ip {ip} in range {start}-{end}")
else:
    print("Number of args wrong, must have ip, start e end")
def find_open_ports(ip,start,end):
        max_ports = 65535
        for i in range(int(start),int(end)):
                a_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
                location = (ip, i)
                result_of_check = a_socket.connect_ex(location)
                if result_of_check == 0:
                        try:
                                service = socket.getservbyport(i, "tcp")
                                print(f"Service {service} running in port {i}")

                        except:
                                print(f"Error to check service in port {i}, but it`s open")
                a_socket.close()
find_open_ports(ip, start, end)

```

```
└─$ python port.py 192.168.15.50 1 65330
Checking open ports from ip 192.168.15.50 in range 1-653
Service ftp running in port 21
Service ssh running in port 22
Service telnet running in port 23
Service smtp running in port 25
Service domain running in port 53
Service http running in port 80
Service sunrpc running in port 111
Service netbios-ssn running in port 139
Service microsoft-ds running in port 445
Service exec running in port 512
Service login running in port 513
Service shell running in port 514
Service rmiregistry running in port 1099
Service ingreslock running in port 1524
Service nfs running in port 2049
Service iprop running in port 2121
Service mysql running in port 3306
Service distcc running in port 3632
Service postgresql running in port 5432
Error to check service in port 5900, but it`s open
Service x11 running in port 6000
Service ircd running in port 6667
Service ircs-u running in port 6697
Error to check service in port 8009, but it`s open
Error to check service in port 8180, but it`s open
Error to check service in port 8787, but it`s open
Error to check service in port 43870, but it`s open
Error to check service in port 52852, but it`s open
Error to check service in port 55344, but it`s open
```

## e. Listar as vulnerabilidades das portas 21 e 445

nmap -sV --script vuln -p 21,445 192.168.15.50

```
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
| 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_backdoo
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 08:00:27:1D:77:8E (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix
```

**f. encontrar um exploit para uma vulnerabilidade nos serviços testados no exercício anterior.**

nmap -Pn -sS -sC --script exploit -p 445,21 192.168.0.38

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -sS -sC --script exploit -p 445,21 192.168.0.38
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-06 13:32 EST
Nmap scan report for 192.168.0.38
Host is up (0.00079s latency).

PORT    STATE SERVICE
21/tcp  open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       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
445/tcp open  microsoft-ds
MAC Address: 08:00:27:1D:77:8E (Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 6.04 seconds
```

Size: 122 x 34

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

Sendo um CVE de nivel alto um valor entre 7-8.9.

Para a porta 3306:

```
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
|       SAINT:D505D53863BE216621FDAECA22896071  7.5     https://vulners.com/saint/SAINT:D505D53863BE216621FDAEC
|       SAINT:A9E0BE0CEF71F1F98D3CB3E95173B3D0  7.5     https://vulners.com/saint/SAINT:A9E0BE0CEF71F1F98D3CB3E
|       SAINT:79BA92A57C28E796ADD04A6A8AE158CE  7.5     https://vulners.com/saint/SAINT:79BA92A57C28E796ADD04A6
|       SAINT:3101D21E4D8017EA5B14AF668DC39CAD  7.5     https://vulners.com/saint/SAINT:3101D21E4D8017EA5B14AF6
|       PACKETSTORM:85678       7.5     https://vulners.com/packetstorm/PACKETSTORM:85678       *EXPLOIT*
|       PACKETSTORM:82247       7.5     https://vulners.com/packetstorm/PACKETSTORM:82247       *EXPLOIT*
|       MSF:EXPLOIT/WINDOWS/MYSQL/MYSQL_YASSL_HELLO      7.5     https://vulners.com/metasploit/MSF:EXPLOIT/WIND
|       MSF:EXPLOIT/LINUX/MYSQL/MYSQL_YASSL_HELLO       7.5     https://vulners.com/metasploit/MSF:EXPLOIT/LINU
|       CVE-2008-0226   7.5     https://vulners.com/cve/CVE-2008-0226
```

Size: 111 x 34

Para a porta 5432

```
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| vulners:
|   cpe:/a:postgresql:postgresql:8.3:
|       SSV:60718       10.0    https://vulners.com/seebug/SSV:60718    *EXPLOIT*
|       CVE-2013-1903   10.0    https://vulners.com/cve/CVE-2013-1903
|       CVE-2013-1902   10.0    https://vulners.com/cve/CVE-2013-1902
|       SSV:30015       8.5     https://vulners.com/seebug/SSV:30015    *EXPLOIT*
|       SSV:19652       8.5     https://vulners.com/seebug/SSV:19652    *EXPLOIT*
|       POSTGRESQL:CVE-2013-1900        8.5     https://vulners.com/postgresql/POSTGRESQL:CVE-2013-1900
|       POSTGRESQL:CVE-2010-1169        8.5     https://vulners.com/postgresql/POSTGRESQL:CVE-2010-1169
|       CVE-2010-1447   8.5     https://vulners.com/cve/CVE-2010-1447
|       CVE-2010-1169   8.5     https://vulners.com/cve/CVE-2010-1169
|       MSF:ILITIES/LINUXRPM-RHSA-2012-1047/    7.5     https://vulners.com/metasploit/MSF:ILITIES/LINUXRPM-RHS
|       MSF:ILITIES/LINUXRPM-RHSA-2012-1046/    7.5     https://vulners.com/metasploit/MSF:ILITIES/LINUXRPM-RHS
```

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

**i. Qual é o endereço IP associado?**

```
┌──(root㉿kali)-[/home/kali]
└─# nikto -h www.ietf.org
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          104.16.45.99
+ Target Hostname:    www.ietf.org
+ Target Port:        80
+ Message:            Multiple IP addresses found: 104.16.45.99, 104.16.44.99
+ Start Time:         2022-03-07 12:51:47 (GMT-5)
---------------------------------------------------------------------------
```

IP: 104.16.45.99

**ii. Quais são seus servidores DNS?**

```
┌──(root㉿kali)-[/home/kali]
└─# host -t ns www.ietf.org
www.ietf.org is an alias for www.ietf.org.cdn.cloudflare.net.

┌──(root㉿kali)-[/home/kali]
└─# dig ns www.ietf.org

; <<>> DiG 9.18.0-2-Debian <<>> ns www.ietf.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6214
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.ietf.org.                  IN      NS

;; ANSWER SECTION:
www.ietf.org.           866     IN      CNAME   www.ietf.org.cdn.cloudflare.net.

;; AUTHORITY SECTION:
cloudflare.net.         1778    IN      SOA     ns1.cloudflare.net. dns.cloudflare.com. 22717066

;; Query time: 592 msec
;; SERVER: 192.168.50.1#53(192.168.50.1) (UDP)
;; WHEN: Mon Mar 07 13:00:36 EST 2022
;; MSG SIZE  rcvd: 144
```

www.ietf.org.cdn.cloudflare.net.

**iii. Existe algum servidor de e-mail associado ao domínio ietf.org? Qual o seu nome e IP?**

```
Servidores MX:
ietf.org.       1800    IN      MX 0    mail.ietf.org.
```

mail.ietf.org

```
└─# nikto -h mail.ietf.org
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          4.31.198.44
+ Target Hostname:    mail.ietf.org
+ Target Port:        80
+ Start Time:         2022-03-10 08:01:02 (GMT-5)
---------------------------------------------------------------------------
```

IP = 4.31.198.44

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

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

```
└─# host -t ns youtube.com
youtube.com name server ns1.google.com.
youtube.com name server ns2.google.com.
youtube.com name server ns3.google.com.
youtube.com name server ns4.google.com.
```

   ii. **Existem outros domínios ou serviços hospedados no mesmo host (IP)? Quais são?**

```
┌──(root㉿kali)-[/home/kali]
└─# nikto -h youtube.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          142.251.129.206
+ Target Hostname:    youtube.com
+ Target Port:        80
+ Start Time:         2022-03-10 09:05:34 (GMT-5)
---------------------------------------------------------------------------
+ Server: ESF
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good
+ Root page / redirects to: https://youtube.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'ESF' to 'sffe' which may suggest a WAF, load balancer or proxy
 is in place
+ Uncommon header 'cross-origin-resource-policy' found, with contents: cross-origin
^C
```

```
└─# nmap -sn 142.250.219.206
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-10 09:08 EST
Nmap scan report for gru06s64-in-f14.1e100.net (142.250.219.206)
Host is up (0.0063s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

   iii. **Qual o Servidor WEB e Sistema Operacional que hospedam este site? Quais foram as últimas alterações?**

```
Running: Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.
OS details: Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22),
```

| | |
|---|---|
| Site | https://www.youtube.com |
| Netblock Owner | Google LLC |
| Hosting company | Google |

iv. **Quais tecnologias (jquery, utilizadas por este site)?**

**Server-Side**

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| SSL | A cryptographic protocol providing communication security over the Internet | |

**Client-Side**

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

| Technology | Description | Popular sites using this technology |
|---|---|---|
| JavaScript | Widely-supported programming language commonly used to power client-side dynamic content on websites | |

v. **Existe algum WAF protegendo este site? (Print a saída do comando)**

```
└─# wafw00f www.youtube.com

                ( W00f! )
                404 Hack Not Found
                405 Not Allowe
                403 Forbidden
                502 Bad Gateway
                500 Internal E

                ~ WAFW00F : v2.1.0 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.youtube.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

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

```
Servidores MX:
youtube.com.    300     IN      MX 0    smtp.google.com.
```

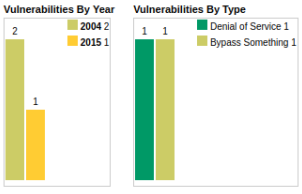
## j. portas TCP e UDP do alvo

```
└─$ python port.py 192.168.15.50 1 65330
Checking open ports from ip 192.168.15.50 in range 1-653
Service ftp running in port 21
Service ssh running in port 22
Service telnet running in port 23
Service smtp running in port 25
Service domain running in port 53
Service http running in port 80
Service sunrpc running in port 111
Service netbios-ssn running in port 139
Service microsoft-ds running in port 445
Service exec running in port 512
Service login running in port 513
Service shell running in port 514
Service rmiregistry running in port 1099
Service ingreslock running in port 1524
Service nfs running in port 2049
Service iprop running in port 2121
Service mysql running in port 3306
Service distcc running in port 3632
Service postgresql running in port 5432
Error to check service in port 5900, but it`s open
Service x11 running in port 6000
Service ircd running in port 6667
Service ircs-u running in port 6697
Error to check service in port 8009, but it`s open
Error to check service in port 8180, but it`s open
Error to check service in port 8787, but it`s open
Error to check service in port 43870, but it`s open
Error to check service in port 52852, but it`s open
Error to check service in port 55344, but it`s open
```

**Vulnerability Trends Over Time**

| Year | # of Vulnerabilities | DoS | Code Execution | Overflow | Memory Corruption | Sql Injection | XSS | Directory Traversal | Http Response Splitting | Bypass something | Gain Information | Gain Privileges | CSRF | File Inclusion | # of exploits |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2004 | 2 | 1 | | | | | | | | | | | | | |
| 2015 | 1 | | | | | | | | | 1 | | | | | |
| Total | 3 | 1 | | | | | | | | 1 | | | | | |
| % Of All | | 33.3 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 33.3 | 0.0 | 0.0 | 0.0 | 0.0 | |

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those y




Denial of Service 1
Bypass Something 1