UNIVERSIDAD DE CUENCA

1.1_Descubrimiento en NMAP

Hosts activos

Dirección IP: 192.168.56.104 - Direccion MAC: 08:00:27:F2:C3:90

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

Dirección IP:

### 192.168.56.104

Port	State	Service
1099/tcp	open	rmiregistry
111/tcp	open	rpcbind
139/tcp	open	netbios-ssn
1524/tcp	open	ingreslock
2049/tcp	open	nfs
21/tcp	open	ftp
2121/tcp	open	ccproxy-ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
3306/tcp	open	mysql
445/tcp	open	microsoft-ds
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
53/tcp	open	domain
5432/tcp	open	postgresql
5900/tcp	open	vnc
6000/tcp	open	X11
6667/tcp	open	irc
80/tcp	open	http
8009/tcp	open	ajp13
8180/tcp	open	unknown

(end of excerpt)

1.2_Obtención-de-puertos-TCP-abiertos

Direcciones:

IP: 192.168.56.104 - ipv4
Fisica: mac - 08:00:27:F2:C3:90

Puertos:

Los 977 puertos escaneados pero no presentados, estan en estado: closed
Los 977 puertos respondieron con: reset

### 192.168.56.104

Port	State	Service
1099/tcp	open	rmiregistry
111/tcp	open	rpcbind
139/tcp	open	netbios-ssn
1524/tcp	open	ingreslock
2049/tcp	open	nfs
21/tcp	open	ftp
2121/tcp	open	ccproxy-ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
3306/tcp	open	mysql
445/tcp	open	microsoft-ds
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
53/tcp	open	domain
5432/tcp	open	postgresql
5900/tcp	open	vnc
6000/tcp	open	X11
6667/tcp	open	irc
80/tcp	open	http
8009/tcp	open	ajp13
8180/tcp	open	unknown

(end of excerpt)

1.3_Vulnerabilidades-mediante-puertos-TCP

Dirección IP:

```
# Nmap 7.93 scan initiated Tue Jan 31 02:00:16 2023 as: nmap -v -sS --script=vuln --stylesheet=https://svn.nmap.org/nmap/docs/nmap.xsl -oA /src/archivos/hosts/fase_3/192.168.56.104vunlnmaptcp 192.168.56.104
```

(end of excerpt)

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

Dirección IP:

```
# Nmap 7.93 scan initiated Tue Jan 31 02:03:17 2023 as: nmap -sV --script=vulners --script-args mincvss=7.5
--stylesheet=https://svn.nmap.org/nmap/docs/nmap.xsl                                                -oA
/src/archivos/hosts/fase_3/192.168.56.104vulners_nmap_serv 192.168.56.104
Nmap scan report for 192.168.56.104
Host is up (0.00022s 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)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      38100/tcp   mountd
|   100005  1,2,3      40615/udp   mountd
|   100021  1,3,4      44943/udp   nlockmgr
|   100021  1,3,4      56517/tcp   nlockmgr
|   100024  1          43932/tcp   status
|_  100024  1          44439/udp   status
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       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
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
|_http-server-header: Apache-Coyote/1.1
```

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

```
MAC Address: 08:00:27:F2:C3:90 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jan 31 02:03:29 2023 -- 1 IP address (1 host up) scanned in 11.89 seconds
```

(end of excerpt)
