UNIVERSIDAD DE CUENCA

1.1_Descubrimiento en NMAP

Hosts activos

Dirección IP: 192.168.56.106   -   Direccion MAC:

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

Dirección IP:

### 192.168.56.106

Port	*State*	*Service*
135/tcp	*open*	*msrpc*
139/tcp	*open*	*netbios-ssn*
445/tcp	*open*	*microsoft-ds*

(end of excerpt)

1.2_Obtención-de-puertos-TCP-abiertos

Direcciones:

IP: 192.168.56.106 - ipv4
Fisica: no se pudo obtener - no se pudo obtener

Puertos:

Los 997 puertos escaneados pero no presentados, estan en estado: filtered
Los 997 puertos respondieron con: no-response

### 192.168.56.106

Port	State	Service
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds

(end of excerpt)

1.2_Obtención-de-puertos-UDP-abiertos

Direcciones:

IP: 192.168.56.106 - ipv4
Fisica: no se pudo obtener - no se pudo obtener

Puertos:

Los 998 puertos escaneados pero no presentados, estan en estado: open|filtered
Los 998 puertos respondieron con: no-response

### 192.168.56.106

Port	State	Service
123/udp	open	ntp
137/udp	open	netbios-ns

(end of excerpt)

1.3_Vulnerabilidades-mediante-puertos-TCP

Dirección IP:

```
# Nmap 7.93 scan initiated Tue Jan 31 08:51:17 2023 as: nmap -v -sS --script=vuln
--stylesheet=https://svn.nmap.org/nmap/docs/nmap.xsl -oA /src/archivos/hosts/fase_3/192.168.56.106vunlnmaptcp
192.168.56.106
Nmap scan report for 192.168.56.106
Host is up (0.0016s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)

Read data files from: /usr/bin/../share/nmap
# Nmap done at Tue Jan 31 08:52:02 2023 -- 1 IP address (1 host up) scanned in 44.45 seconds

(end of excerpt)
--------------------------------------------------------------------------------------------------------------------------------------------------
```

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

Dirección IP:

```
# Nmap 7.93 scan initiated Tue Jan 31 08:52:44 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_3/192.168.56.106vulners_nmap_serv 192.168.56.106
Nmap scan report for 192.168.56.106
Host is up (0.0015s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jan 31 08:52:56 2023 -- 1 IP address (1 host up) scanned in 11.74 seconds

(end of excerpt)
------------------------------------------------------------------------------------------------------------------------------------------------------
```