

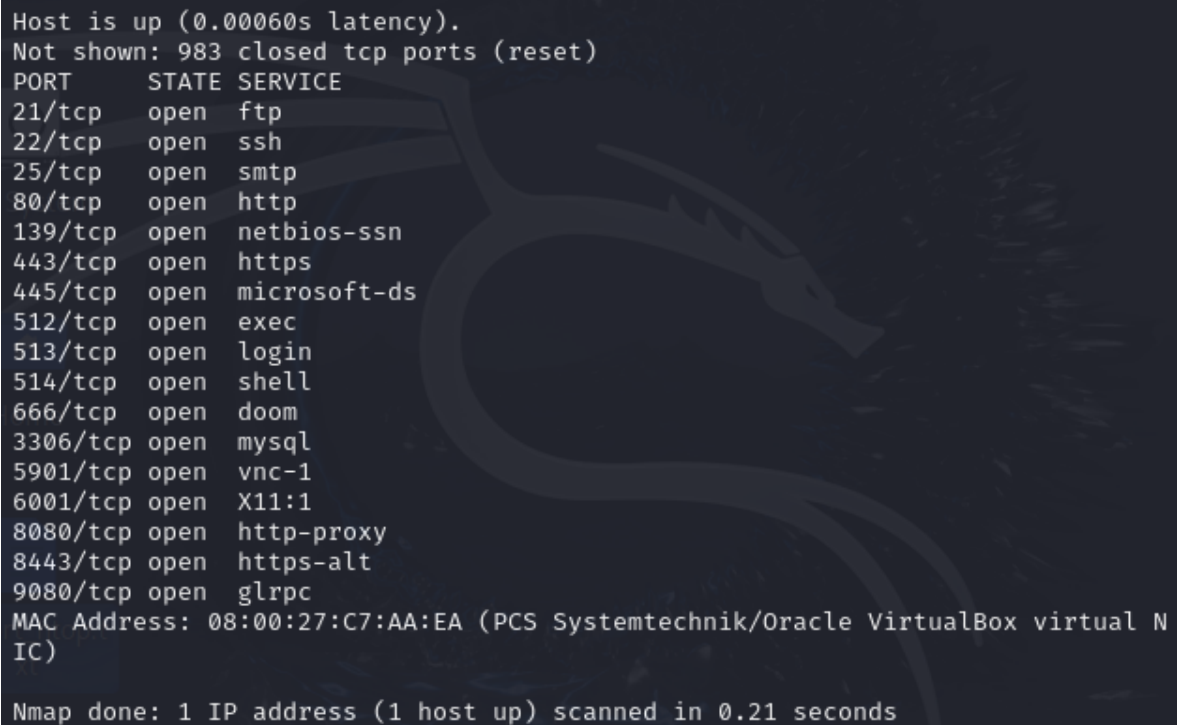
Contacto: Emmanuel Izaguirre Ruiz

Versión del informe: Vulnerabilidades con nmap.

1.2 Escaneo Básico de un Objetivo

Para escanear un dispositivo o máquina en la red (por ejemplo, una máquina Debian con la IP <IP_debian>), puedes utilizar el siguiente comando básico:

nmap <IP_debian>



```
Host is up (0.00060s latency).
Not shown: 983 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
666/tcp   open  doom
3306/tcp  open  mysql
5901/tcp  open  vnc-1
6001/tcp  open  X11:1
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
9080/tcp  open  glrpc
MAC Address: 08:00:27:C7:AA:EA (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

Comando nmap, nos muestra todos los puertos abiertos de la máquina Debian.

Paso 2: Enumerar Puertos y Verificar Servicios

2.1 Escaneo de Puertos y Servicios

nmap -sV --script=vuln

```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-18 16:35 EST
Nmap scan report for 192.168.100.78
Host is up (0.00022s latency).
Not shown: 983 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp?
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp    open  smtp         Postfix smtpd
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4
.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
443/tcp   open  ssl/http     Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4
.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
512/tcp   open  exec         netkit-rsh rshd
513/tcp   open  login?
514/tcp   open  shell?
666/tcp   open  doom?
3306/tcp  open  mysql        MySQL 5.0.96-0ubuntu3
5901/tcp  open  vnc          VNC (protocol 3.8)
6001/tcp  open  X11          (access denied)
8080/tcp  open  http         nginx 1.4.0
8443/tcp  open  ssl/http     nginx 1.4.0
9080/tcp  open  http         lighttpd 1.4.19
2 services unrecognized despite returning data. If you know the service/versi

```

Con este comando encontramos de forma detallada las vulnerabilidades que presentan los servicios detectados en el dispositivo oibjetivo.

2.2 Escaneo Detallado y Búsqueda de Vulnerabilidades

Para realizar un escaneo más detallado que busque vulnerabilidades conocidas, utiliza el siguiente comando con el script --script=vuln:

Documentar Vulnerabilidades Asociadas a los Servicios

3.1 Anotar los Servicios y sus Versiones

En el resultado del escaneo, toma nota de los servicios y sus versiones. Ejemplo de salida:

Apache 2.2.8, apache httpd, suhosin-pach mod, samba smbd 3.x, mysql 5.0.96, nginx 1.4.0, lighthttpd 1.4.19 así como 10 puertos abiertos vulnerables.

3.2 Buscar Vulnerabilidades en Bases de Datos Públicas

Apache 2.4.7, NVD

Tiene una vulnerabilidad que permite una ejecución remota de código debido a un error en SSL.