Utilizando NMAP para escanear puertos en la maquina Metasploitable. No tengo Debian porque me crashea constantemente:

```
└─$ nmap 192.168.1.113
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-11 11:35 CST
Nmap scan report for 192.168.1.113
Host is up (0.00010s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:50:FD:80 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

Utilizo el siguiente comando que me pide el ejercicio que es nmap -sV 192.168.1.113

```
Nmap scan report for 192.168.1.113
Host is up (0.00015s 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)
111/tcp  open  rpcbind     2 (RPC #100000)
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?
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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
MAC Address: 08:00:27:50:FD:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Un
ix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Aquí hacemos un escaneo más exhaustivo donde los dice los puertos que están abiertos la versión de los mismos.

En el caso de la maquina metasploitable, cuando hacemos el escaneo con el siguiente comando en la terminal nmap -sV --script=vuln 192.168.1.113 nos da el siguiente resultado:

```
┌──(fede㉿Fede)-[~]
└─$ nmap -sV --script=vuln 192.168.1.113
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-11 11:48 CST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
```

Por lo que para obtener las vulnerabilidadesvulners 192.168.1.113

Pongo aquí una pequeña captura de los resultados obtenidos pero son muchos para adjuntarlos…..

```
|       POSTGRESQL:CVE-2009-0922        4.0     https://vulners.com/postgresql/PO
STGRESQL:CVE-2009-0922
|       CVE-2014-0066   4.0     https://vulners.com/cve/CVE-2014-0066
|       CVE-2014-0060   4.0     https://vulners.com/cve/CVE-2014-0060
|       CVE-2012-2655   4.0     https://vulners.com/cve/CVE-2012-2655
|       CVE-2009-3229   4.0     https://vulners.com/cve/CVE-2009-3229
|       POSTGRESQL:CVE-2022-41862       3.7     https://vulners.com/postgresql/PO
STGRESQL:CVE-2022-41862
|       CVE-2022-41862  3.7     https://vulners.com/cve/CVE-2022-41862
|       SSV:19322       3.5     https://vulners.com/seebug/SSV:19322    *EXPLOIT*
|       PACKETSTORM:127092      3.5     https://vulners.com/packetstorm/PACKETSTO
RM:127092       *EXPLOIT*
|       CVE-2010-0733   3.5     https://vulners.com/cve/CVE-2010-0733
|       POSTGRESQL:CVE-2024-4317        3.1     https://vulners.com/postgresql/PO
STGRESQL:CVE-2024-4317
|       POSTGRESQL:CVE-2024-10977       3.1     https://vulners.com/postgresql/PO
STGRESQL:CVE-2024-10977
|_      POSTGRESQL:CVE-2019-10209       2.2     https://vulners.com/postgresql/PO
STGRESQL:CVE-2019-10209
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
MAC Address: 08:00:27:50:FD:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Un
ix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 109.08 seconds
```

Viendo los puertos abiertos y las versiones y sin navegar en esta búsqueda anterior, paso a enumerar 6 ejemplos de vulnerabilidades:

Puerto,Servicio,Versión,Vulnerabilidad,Descripción,Referencia

21,FTP,vsftpd 2.3.4,CVE-2011-2523,Backdoor en vsftpd 2.3.4 que permite ejecución remota de código.,Link a CVE

22,SSH,OpenSSH 4.7p1,CVE-2008-5161,Debilidad en OpenSSH que permite ataques de canal lateral.,Link a CVE

23,Telnet,Linux telnetd,CVE-1999-0611,"Telnet transmite credenciales en texto plano, vulnerable a MITM.",Link a CVE

25,SMTP,Postfix smtpd,CVE-2010-5321,Postfix expone vulnerabilidades de retransmisión de correo.,Link a CVE

80,HTTP,Apache httpd 2.2.8,CVE-2017-9798,Apache vulnerable a inyección de scripts (OptionsBleed).,Link a CVE

3306,MySQL,MySQL 5.0.51a-3ubuntu5,CVE-2009-2446,MySQL vulnerable a ataques de autenticación remota.,Link a CVE