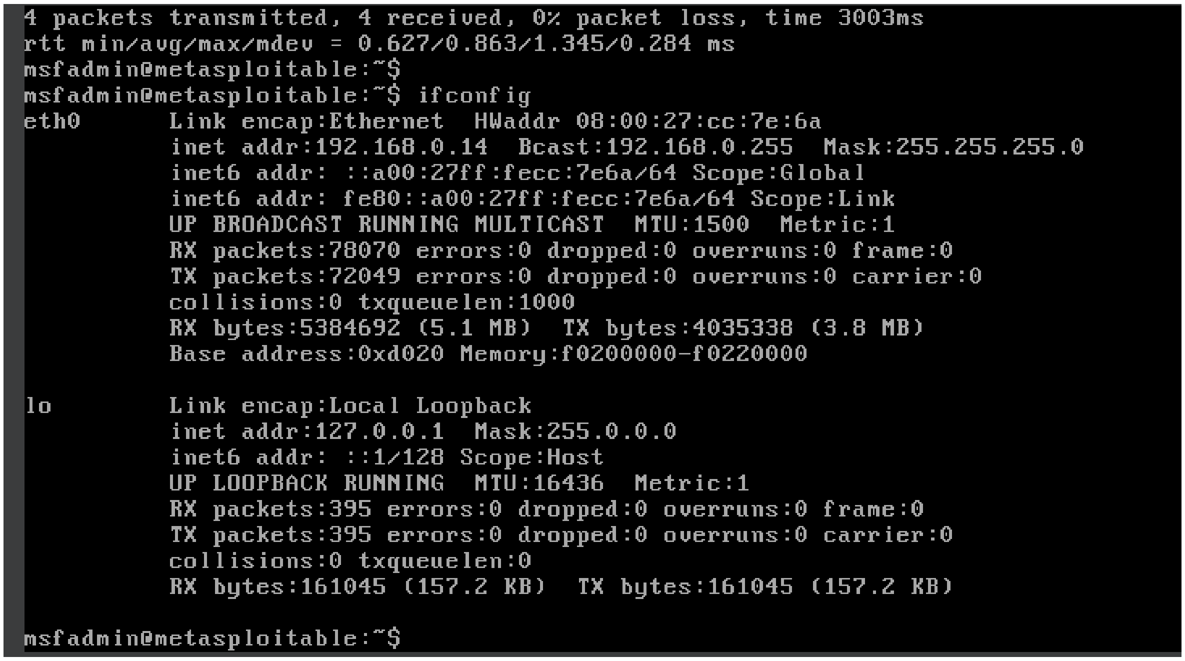
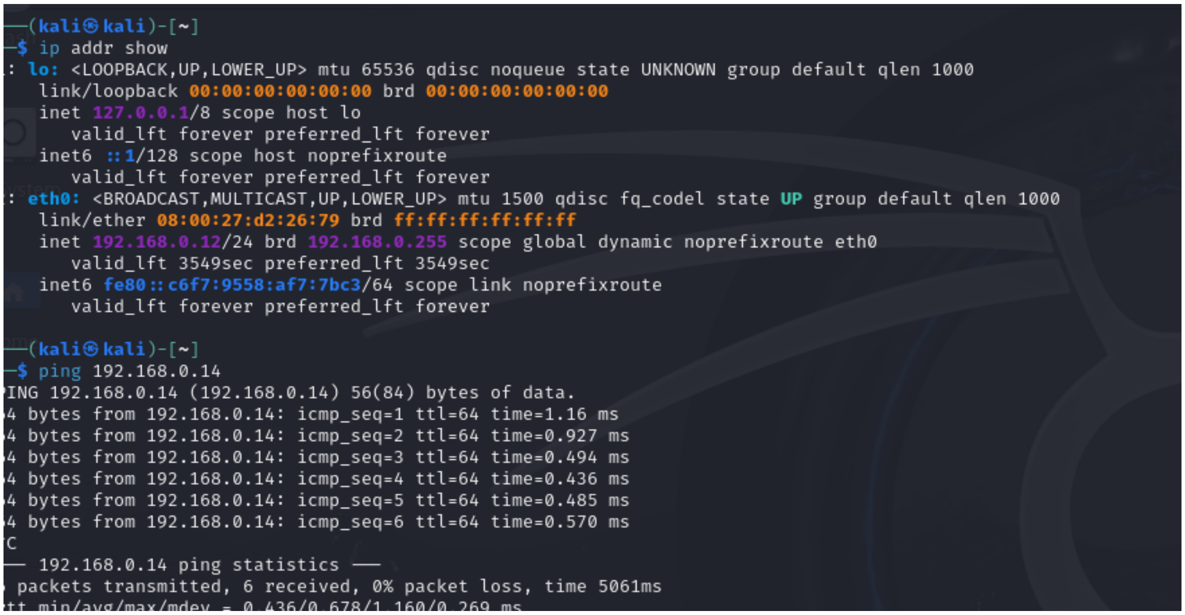
Proyecto de Reconocimiento en Pentesting en una Máquina Vulnerable.

Paso 1: Encuentra la dirección IP del target.



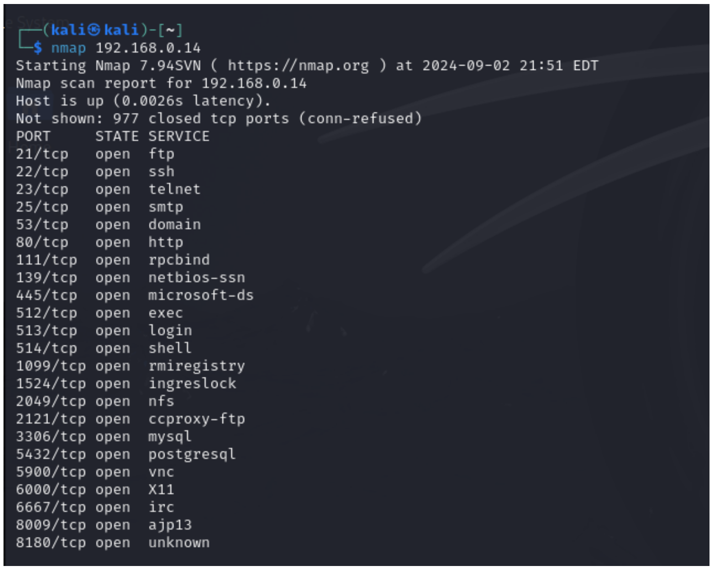
```
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.627/0.863/1.345/0.284 ms
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:cc:7e:6a
          inet addr:192.168.0.14  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: ::a00:27ff:fecc:7e6a/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fecc:7e6a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:78070 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72049 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5384692 (5.1 MB)  TX bytes:4035338 (3.8 MB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:395 errors:0 dropped:0 overruns:0 frame:0
          TX packets:395 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:161045 (157.2 KB)  TX bytes:161045 (157.2 KB)

msfadmin@metasploitable:~$
```



```
──(kali㉿kali)-[~]
─$ ip addr show
: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
      valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
      valid_lft forever preferred_lft forever
: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:d2:26:79 brd ff:ff:ff:ff:ff:ff
   inet 192.168.0.12/24 brd 192.168.0.255 scope global dynamic noprefixroute eth0
      valid_lft 3549sec preferred_lft 3549sec
   inet6 fe80::c6f7:9558:af7:7bc3/64 scope link noprefixroute
      valid_lft forever preferred_lft forever

──(kali㉿kali)-[~]
─$ ping 192.168.0.14
ING 192.168.0.14 (192.168.0.14) 56(84) bytes of data.
4 bytes from 192.168.0.14: icmp_seq=1 ttl=64 time=1.16 ms
4 bytes from 192.168.0.14: icmp_seq=2 ttl=64 time=0.927 ms
4 bytes from 192.168.0.14: icmp_seq=3 ttl=64 time=0.494 ms
4 bytes from 192.168.0.14: icmp_seq=4 ttl=64 time=0.436 ms
4 bytes from 192.168.0.14: icmp_seq=5 ttl=64 time=0.485 ms
4 bytes from 192.168.0.14: icmp_seq=6 ttl=64 time=0.570 ms
C
── 192.168.0.14 ping statistics ──
 packets transmitted, 6 received, 0% packet loss, time 5061ms
tt min/avg/max/mdev = 0.436/0.678/1.160/0.269 ms
```

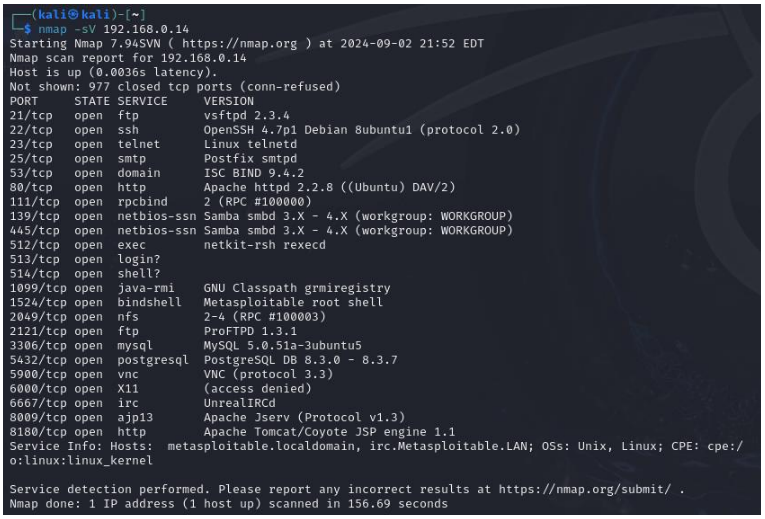
Paso 2: Encuentra información sobre el sistema operativo y versiones del target.

Escaneo Basico



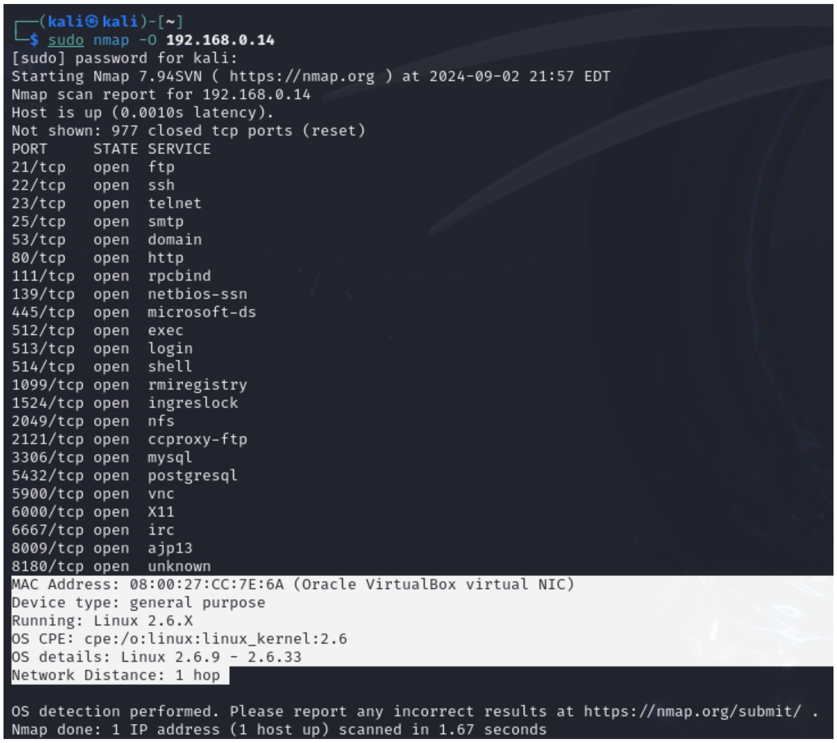
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.0.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-02 21:51 EDT
Nmap scan report for 192.168.0.14
Host is up (0.0026s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
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
```

Escaneo de servicios y versiones



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.0.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-02 21:52 EDT
Nmap scan report for 192.168.0.14
Host is up (0.0036s latency).
Not shown: 977 closed tcp ports (conn-refused)
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        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell?
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
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: 1 IP address (1 host up) scanned in 156.69 seconds
```

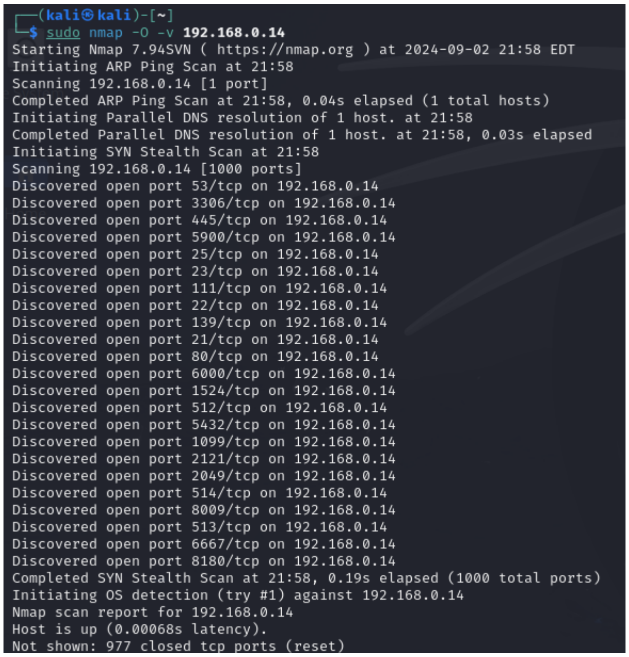
Detecta sistema operativo.



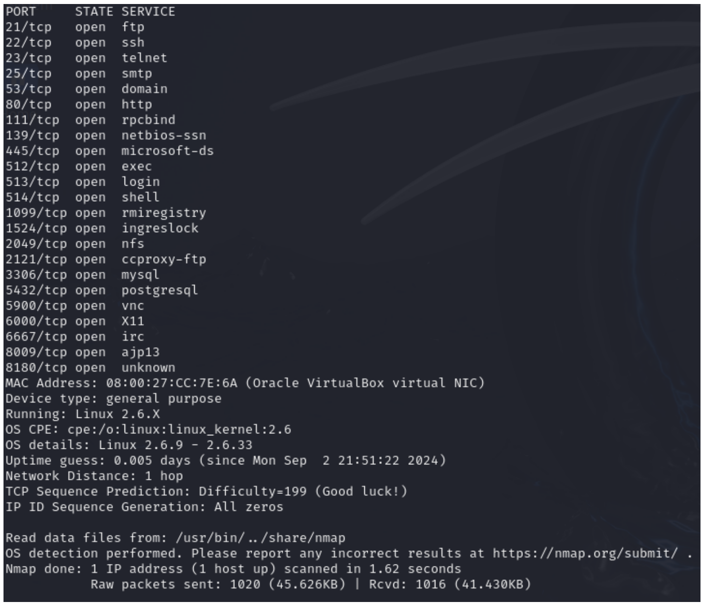
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.0.14
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-02 21:57 EDT
Nmap scan report for 192.168.0.14
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   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:CC:7E:6A (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.67 seconds
```

Paso 3: Enumera los puertos y servicios del target.

Escaneo completo de puertos:

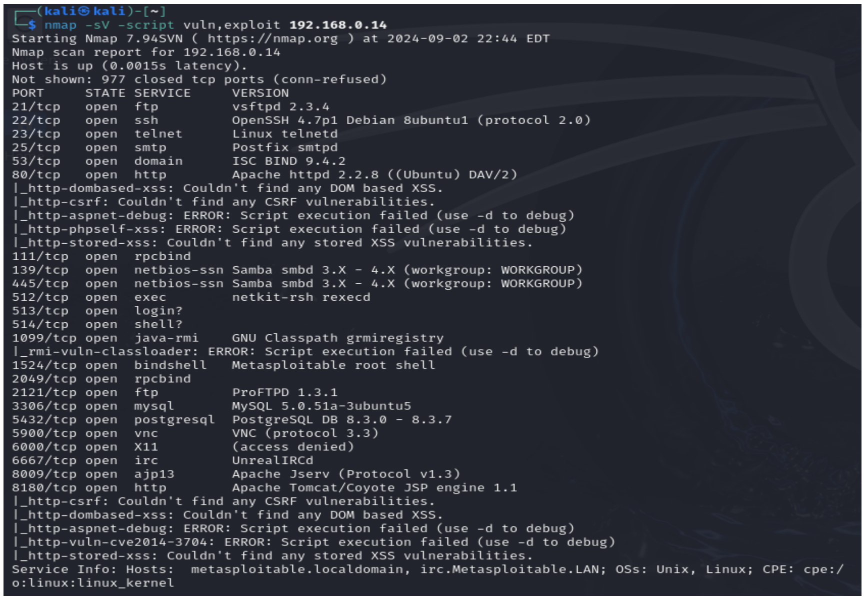


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O -v 192.168.0.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-02 21:58 EDT
Initiating ARP Ping Scan at 21:58
Scanning 192.168.0.14 [1 port]
Completed ARP Ping Scan at 21:58, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:58
Completed Parallel DNS resolution of 1 host. at 21:58, 0.03s elapsed
Initiating SYN Stealth Scan at 21:58
Scanning 192.168.0.14 [1000 ports]
Discovered open port 53/tcp on 192.168.0.14
Discovered open port 3306/tcp on 192.168.0.14
Discovered open port 445/tcp on 192.168.0.14
Discovered open port 5900/tcp on 192.168.0.14
Discovered open port 25/tcp on 192.168.0.14
Discovered open port 23/tcp on 192.168.0.14
Discovered open port 111/tcp on 192.168.0.14
Discovered open port 22/tcp on 192.168.0.14
Discovered open port 139/tcp on 192.168.0.14
Discovered open port 21/tcp on 192.168.0.14
Discovered open port 80/tcp on 192.168.0.14
Discovered open port 6000/tcp on 192.168.0.14
Discovered open port 1524/tcp on 192.168.0.14
Discovered open port 512/tcp on 192.168.0.14
Discovered open port 5432/tcp on 192.168.0.14
Discovered open port 1099/tcp on 192.168.0.14
Discovered open port 2121/tcp on 192.168.0.14
Discovered open port 2049/tcp on 192.168.0.14
Discovered open port 514/tcp on 192.168.0.14
Discovered open port 8009/tcp on 192.168.0.14
Discovered open port 513/tcp on 192.168.0.14
Discovered open port 6667/tcp on 192.168.0.14
Discovered open port 8180/tcp on 192.168.0.14
Completed SYN Stealth Scan at 21:58, 0.19s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.0.14
Nmap scan report for 192.168.0.14
Host is up (0.00068s latency).
Not shown: 977 closed tcp ports (reset)
```

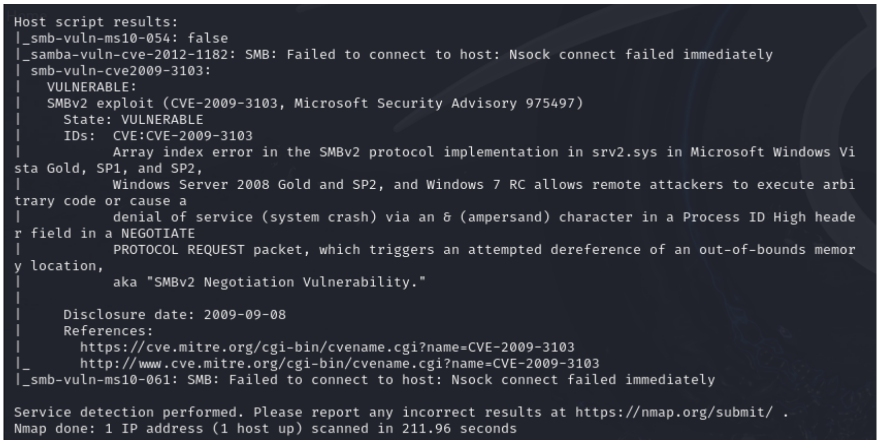


```
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  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:CC:7E:6A (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.005 days (since Mon Sep  2 21:51:22 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=199 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds
           Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.430KB)
```

Usa scripts:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -script vuln,exploit 192.168.0.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-02 22:44 EDT
Nmap scan report for 192.168.0.14
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (conn-refused)
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-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-phpself-xss: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
111/tcp  open  rpcbind
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?
514/tcp  open  shell?
1099/tcp open  java-rmi    GNU Classpath grmiregistry
|_rmi-vuln-classloader: ERROR: Script execution failed (use -d to debug)
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  rpcbind
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-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/
o:linux:linux_kernel
```



```
Host script results:
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: SMB: Failed to connect to host: Nsock connect failed immediately
| smb-vuln-cve2009-3103:
|   VULNERABLE:
|   SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2009-3103
|           Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vi
sta Gold, SP1, and SP2,
|           Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute arbi
trary code or cause a
|           denial of service (system crash) via an & (ampersand) character in a Process ID High heade
r field in a NEGOTIATE
|           PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memor
y location,
|           aka "SMBv2 Negotiation Vulnerability."
|
|     Disclosure date: 2009-09-08
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_      http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_smb-vuln-ms10-061: SMB: Failed to connect to host: Nsock connect failed immediately

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 211.96 seconds
```

Servicios Abiertos:

- **FTP (vsftpd 2.3.4)**: Este es un servidor FTP vulnerable que puede permitir una conexión de backdoor si se conecta en un puerto específico. Esto podría permitir a un atacante ejecutar comandos de manera remota.
- **SSH (OpenSSH 4.7p1)**: Aunque no muestra vulnerabilidades directamente, esta versión es bastante antigua, lo que sugiere que podría ser vulnerable a ciertos tipos de ataques, como vulnerabilidades de fuerza bruta o exploits conocidos.
- HTTP (Apache httpd 2.2.8): Esta versión del servidor Apache es susceptible a múltiples vulnerabilidades, incluidas aquellas que permiten la ejecución de código remoto y ataques XSS (Cross-Site Scripting).
- **Samba (smbd 3.X - 4.X)**: La presencia de SMB abierto puede ser vulnerable, y se mencionan específicamente varias vulnerabilidades de SMB.
- **SMBv2 (CVE-2009-3103)**: Es vulnerable a un exploit que permite la ejecución de código arbitrario o denegación de servicio debido a un error en la implementación del protocolo SMBv2. Esta es una vulnerabilidad crítica que permite a un atacante causar un bloqueo o ejecutar código arbitrario de forma remota.
- **MySQL 5.0.51a**: Las versiones antiguas de MySQL pueden tener varias vulnerabilidades que permiten la inyección de SQL o el escalamiento de privilegios.
- **PostgreSQL (8.3.0 - 8.3.7)**: Similar a MySQL, esta versión es antigua y puede tener múltiples vulnerabilidades de inyección de SQL, escalamiento de privilegios, o incluso la exposición de datos sensibles.
- **Apache Tomcat/Coyote JSP Engine 1.1**: Este motor JSP tiene varias vulnerabilidades, incluidas aquellas que permiten la ejecución de código arbitrario y ataques de inclusión de archivos.

2.- Vulnerabilidades Críticas Detectadas:

- **CVE-2009-3103 (SMBv2)**: Es una vulnerabilidad crítica en el protocolo SMBv2 que permite a un atacante ejecutar código arbitrario o causar una denegación de servicio enviando paquetes especialmente manipulados.

Posibles Brechas de Seguridad:

- **Backdoor en vsftpd**: Permite la ejecución de comandos remotos, lo cual es una brecha crítica.
- **Ejecución Remota en SMBv2**: Permite la ejecución de código arbitrario, lo cual es extremadamente peligroso en redes internas.
- **Servicios y versiones desactualizadas**: La presencia de versiones antiguas de Apache, MySQL, PostgreSQL, y SSH sugiere que el sistema no ha sido actualizado, lo que podría exponerlo a una amplia gama de exploits conocidos