Report Scansione Nmap

IP Target: 192.168.50.101

IP Source: 192.168.50.100

Sistema Operativo Rilevato:

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

Porte Aperte e Servizi Corrispondenti:

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 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 unknown

Differenze Riscontrate tra le Scansioni TCP Connect e SYN:

Entrambe hanno identificato lo stesso set di porte aperte. In entrambi i casi, le porte come 21 (ftp), 22 (ssh), 23 (telnet), 25 (smtp), 80 (http), 3306 (mysql), e molte altre risultano aperte.

Descrizione dei Servizi:

1. **21/tcp ftp vsftpd 2.3.4**: Servizio File Transfer Protocol (FTP) utilizzando il demone **vsftpd**. Questa versione è nota per essere vulnerabile e spesso sfruttata in Metasploitable.

2. **22/tcp ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)**: OpenSSH fornisce comunicazioni sicure tramite la shell remota utilizzando il protocollo SSH. La versione specifica potrebbe avere vulnerabilità note.

3. **23/tcp telnet Linux telnetd**: Servizio Telnet per l'accesso remoto non crittografato. Notoriamente insicuro poiché trasmette le credenziali in chiaro.

4. **25/tcp smtp Postfix smtpd**: Il demone SMTP **Postfix** gestisce l'invio e la ricezione delle email.

5. **53/tcp domain ISC BIND 9.4.2**: Il servizio DNS utilizza BIND, che è un server DNS ampiamente utilizzato su sistemi Unix.

6. **80/tcp http Apache httpd 2.2.8 ((Ubuntu) DAV/2)**: Il server web Apache gestisce il traffico HTTP. Questa versione specifica potrebbe contenere vulnerabilità.

7. **111/tcp rpcbind 2 (RPC #100000)**: Il servizio **rpcbind** mappa i servizi RPC ai numeri di porta. È un punto di ingresso per varie vulnerabilità legate ai servizi RPC.

8. **139/tcp e 445/tcp netbios-ssn Samba smbd 3.X - 4.X**: Questi porti sono associati al servizio **Samba** per la condivisione di file e stampanti in reti Windows.

9. **512/tcp exec netkit-rsh rexecd**, **513/tcp login**, **514/tcp shell Netkit rshd**: Servizi legati a **rsh** e **rexec** per l'esecuzione remota di comandi, noti per vulnerabilità.

10. **1099/tcp java-rmi GNU Classpath grmiregistry**: Registrazione dei servizi Java RMI (Remote Method Invocation).

11. **1524/tcp bindshell Metasploitable root shell**: Una shell di bind su questa porta consente un accesso remoto non autorizzato alla shell root.

12. **2049/tcp nfs 2-4 (RPC #100003)**: Servizio Network File System (NFS) per la condivisione di file su reti.

13. **2121/tcp ftp ProFTPD 1.3.1**: Un altro servizio FTP utilizzando **ProFTPD**, una popolare alternativa a **vsftpd**.

14. **3306/tcp mysql MySQL 5.0.51a-3ubuntu5**: Il servizio di database MySQL. Versioni precedenti come questa possono avere vulnerabilità note.

15. **5432/tcp postgresql PostgreSQL DB 8.3.0 - 8.3.7**: Servizio di database **PostgreSQL**. Anche qui, le versioni meno recenti potrebbero essere vulnerabili.

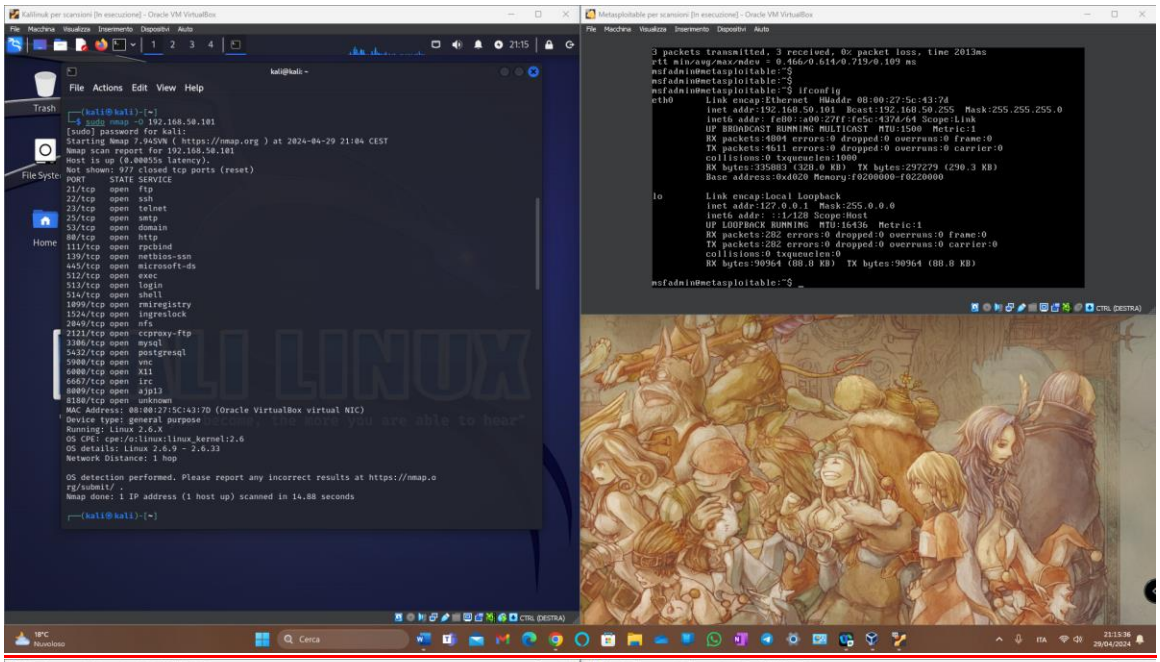
16. **5900/tcp vnc VNC (protocol 3.3)**: Servizio di desktop remoto VNC che può essere vulnerabile se non configurato correttamente.

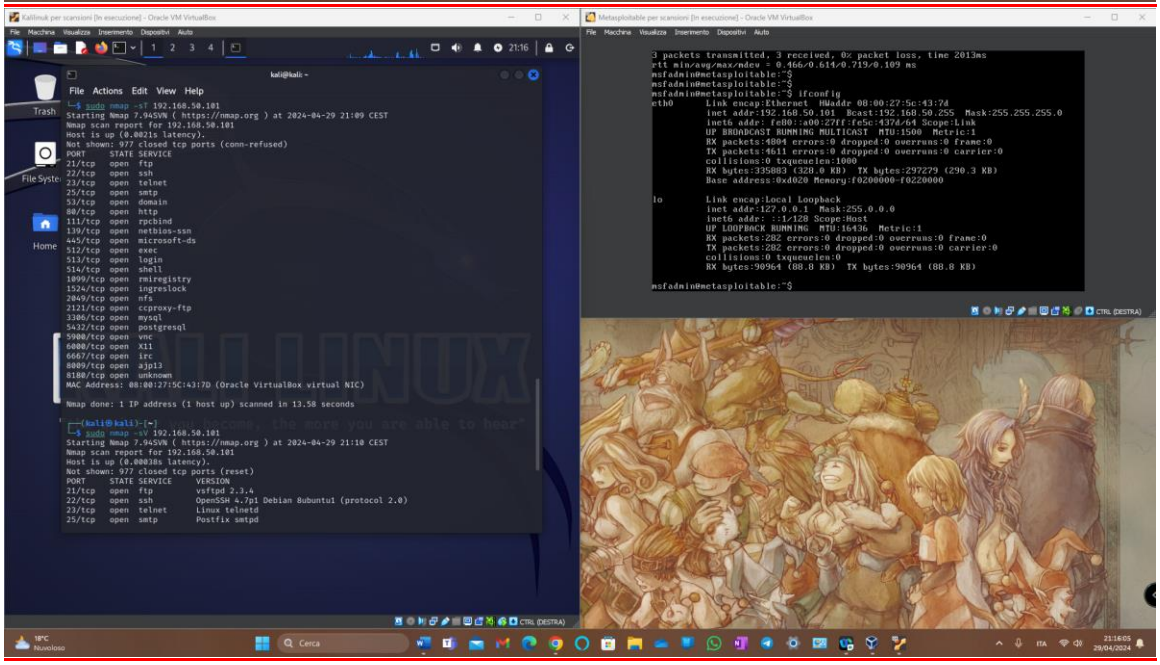
17. **6000/tcp X11 (access denied)**: Il servizio di display remoto X11, che se esposto, può essere sfruttato per attacchi.

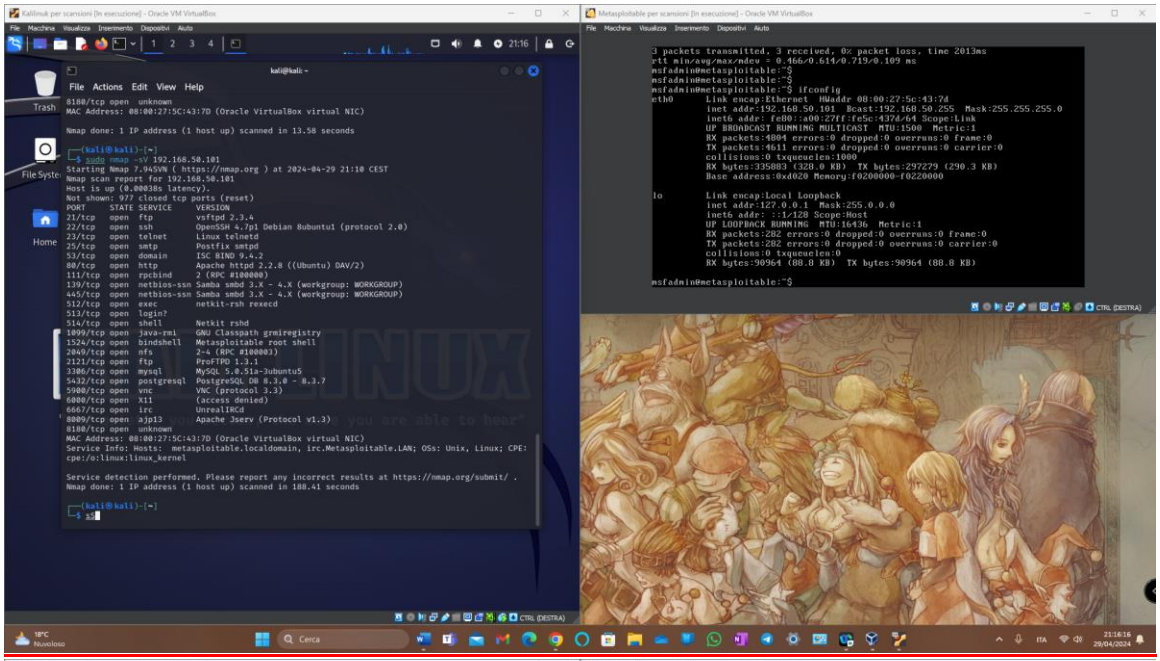
18. **6667/tcp irc UnrealIRCd**: Server IRC che può essere configurato per reti di chat.

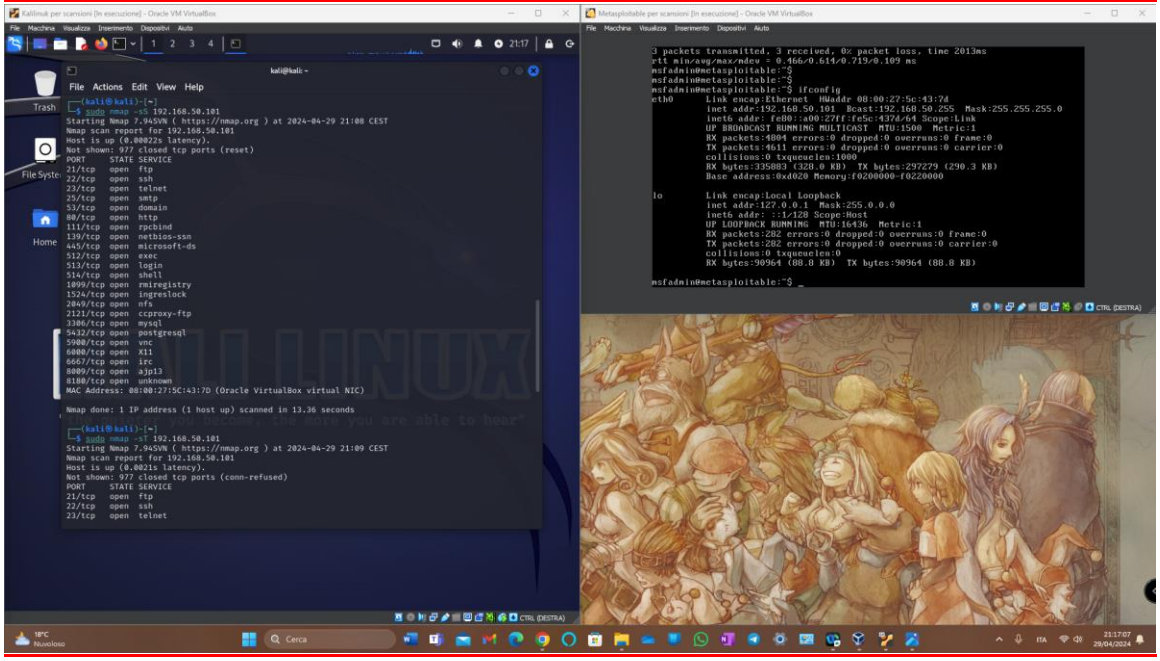
19. **8009/tcp ajp13 Apache Jserv (Protocol v1.3)** e **8180/tcp unknown**: Il protocollo AJP consente la comunicazione tra un server web e un contenitore di applicazioni.

Screen riassuntivi






Kalilinux per scansioni [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
8180/tcp open unknown
MAC Address: 08:00:27:5C:43:7D (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.58 seconds
(kali@kali)-[~]
$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.945VN (https://nmap.org) at 2024-04-29 21:10 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00038s 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 netkit-rsh rexecd
513/tcp open login?
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 unknown
MAC Address: 08:00:27:5C:43:7D (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: 1 IP address (1 host up) scanned in 188.41 seconds
(kali@kali)-[~]
$ ss
Metasploitable per scansioni [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
3 packets transmitted, 3 received, 0% packet loss, time 2013ms
rtt min/avg/max/mdev = 0.466/0.614/0.719/0.109 ms
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:5c:43:7d
inet addr:192.168.50.101 Bcast:192.168.50.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe5c:437d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:4804 errors:0 dropped:0 overruns:0 frame:0
TX packets:4611 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:335883 (328.0 KB) TX bytes:297279 (290.3 KB)
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:282 errors:0 dropped:0 overruns:0 frame:0
TX packets:282 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:90964 (88.8 KB) TX bytes:90964 (88.8 KB)
msfadmin@metasploitable:~$
CTRL (DESTRA)
18°C Nuvoloso
Cerca
ITA
21:16:16
29/04/2024


Kalilinux per scansioni [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.945VN (https://nmap.org) at 2024-04-29 21:08 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00022s 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: 08:00:27:5C:43:7D (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.36 seconds
(kali@kali)-[~]
$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.945VN (https://nmap.org) at 2024-04-29 21:09 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
Metasploitable per scansioni [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
3 packets transmitted, 3 received, 0% packet loss, time 2013ms
rtt min/avg/max/mdev = 0.466/0.614/0.719/0.109 ms
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:5c:43:7d
inet addr:192.168.50.101 Bcast:192.168.50.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe5c:437d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:4804 errors:0 dropped:0 overruns:0 frame:0
TX packets:4611 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:335883 (328.0 KB) TX bytes:297279 (290.3 KB)
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:282 errors:0 dropped:0 overruns:0 frame:0
TX packets:282 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:90964 (88.8 KB) TX bytes:90964 (88.8 KB)
msfadmin@metasploitable:~$
CTRL (DESTRA)
18°C Nuvoloso
Cerca
ITA
21:17:07
29/04/2024

1. **OS Fingerprinting**:

   Comando: sudo nmap -O 192.168.50.101

   - Scoperto: Basato sull'immagine fornita, il sistema operativo non è stato identificato in modo specifico, il che potrebbe essere dovuto alle impostazioni di sicurezza del target o a limitazioni nelle autorizzazioni di scansione di Nmap.

2. **SYN Scan**:

   Comando: sudo nmap -sS 192.168.50.101

   - Porte Aperte: Una serie di porte sono state identificate come aperte, inclusa la porta 22 (SSH), la porta 80 (HTTP), e altre porte per servizi specifici come PostgreSQL e MySQL.

3. **TCP Connect**:

   Comando: sudo nmap -sT 192.168.50.101

   - Risultati: La scansione TCP Connect ha prodotto risultati simili alla SYN Scan, confermando la disponibilità delle porte rilevate dalla SYN Scan.

4. **Version Detection**:

   Comando: sudo nmap -sV 192.168.50.101

   - Servizi e Versioni: Sono state rilevate versioni specifiche di vari servizi, come Apache web server e versioni di servizi legati al database.