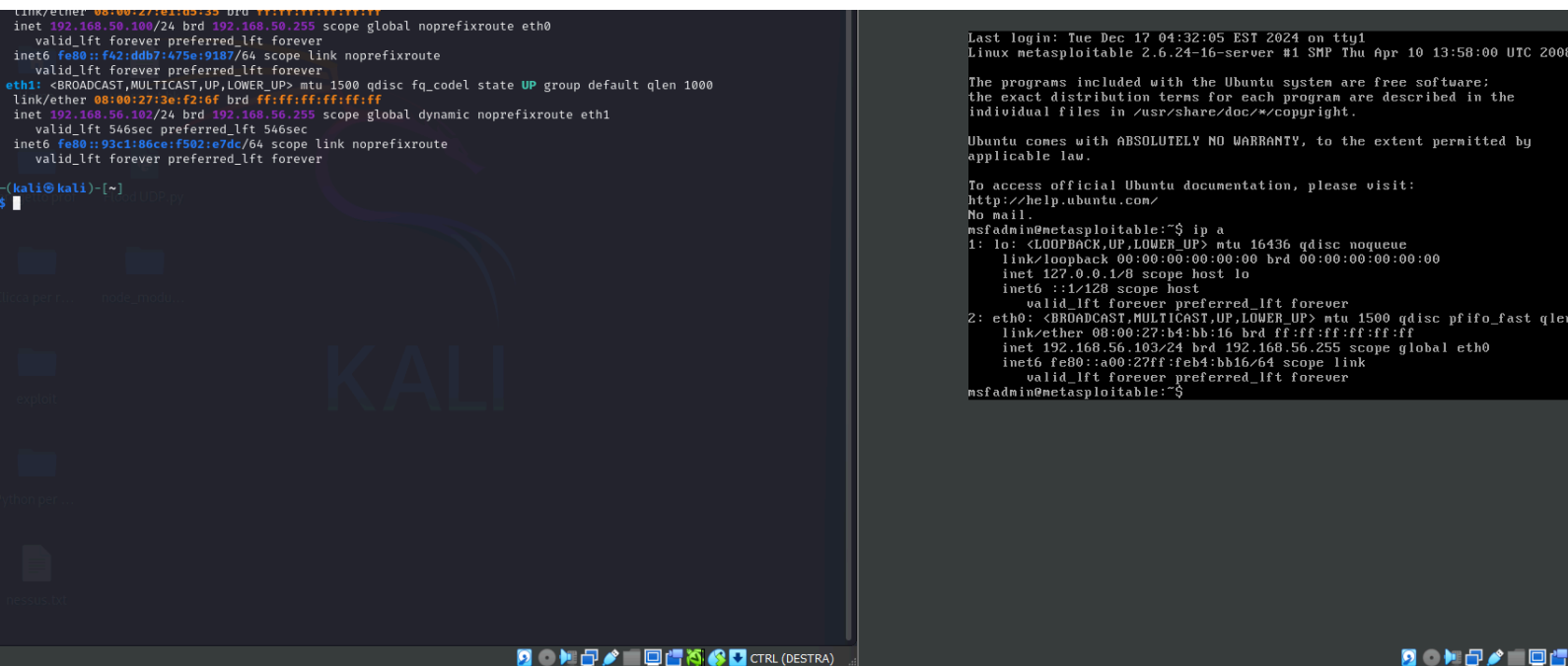
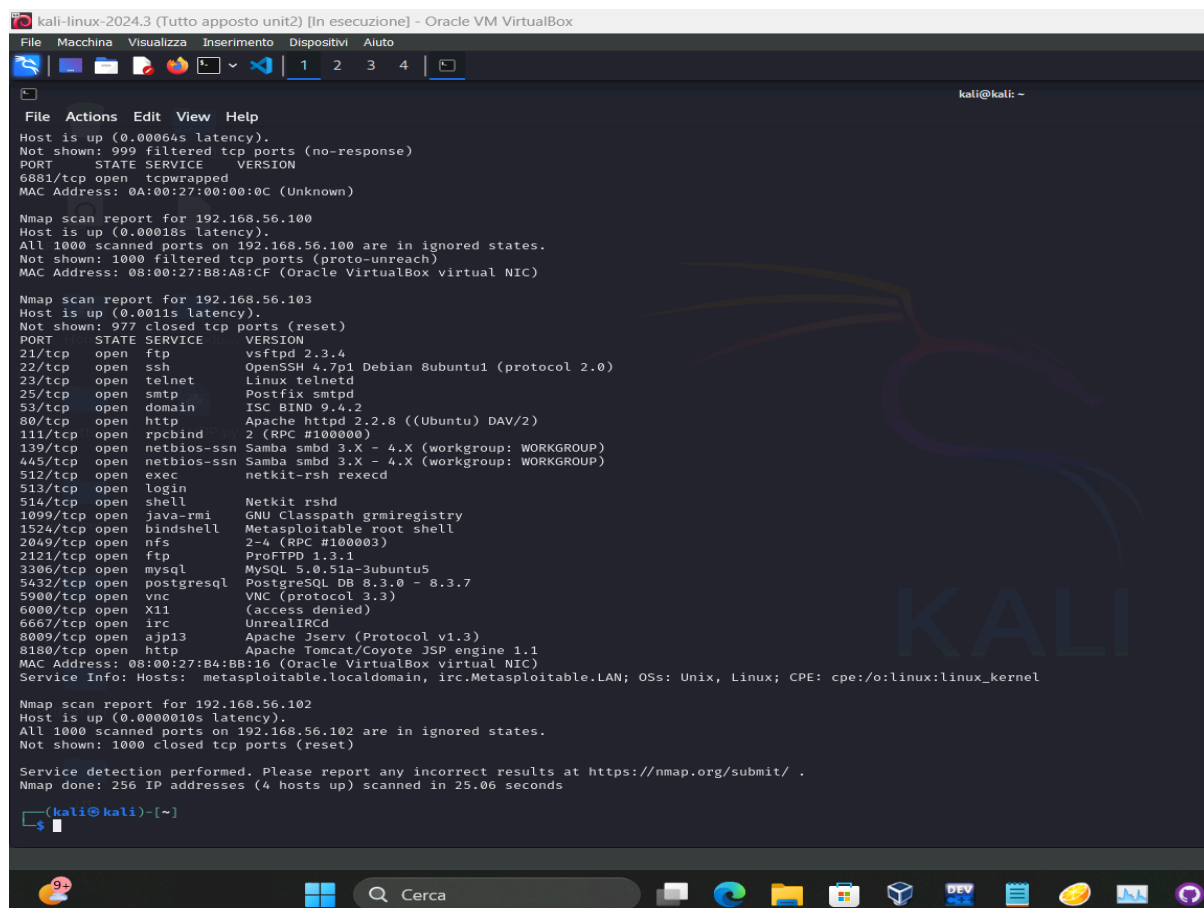


Vuln Telnet Scanner.

Inizialmente ho messo le mie 2 macchine sotto dhcp per bypassare la mia rete di casa.



Poi ho eseguito un **nmap -Sv** su tutti gli ip attivi nella rete per sgombrare l'ip della metasploitable e di tutti i suoi servizi aperti con corrispondente versione.



A seguire ho aperto `msfconsole` per ricercare la vulnerabilità di telnet.

The image shows a Kali Linux VM interface with a terminal window. The terminal output includes:

kali-linux-2024.3 [In esecuzione unità] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
[Icons]
File Actions Edit View Help
Host is up (0.00064s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
6881/tcp open tcpwrapped
MAC Address: 0A:00:27:00:00:0C (Unknown)

Nmap scan report for 192.168.56.100
Host is up (0.00018s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:B8:AB:CF (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.102
Host is up (0.0011s 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-Jubuntus
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:B4:BB:16 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: Unix, Linux; CPE: cpe:/o:linux:linux_

Nmap scan report for 192.168.56.102
Host is up (0.0000010s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 256 IP addresses (4 hosts up) scanned in 25.06 seconds

kali@kali: ~\$
kali@kali:~\$ msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

#k000kdk: #cdh000k:
.x000000000000c c000000000000x
:00000000000000k .k000000000000000:
'000000000kkk00000: :0000000000000000'
00000000.. 0000000000l .000000000
00000000.. c00000c. ,00000000x
l0000000.. d;. ,00000000l
.00000000. +. i .000000000.
c0000000. ,00c. '000. ,0000000c
00000000. ,0000. :0000. ,0000000
l00000. ,0000. :0000. ,000000l
,0000. ,0000. :0000. ,0000;
,0000 ,0000cccc0000. x000,
,kdll .00000000000000. ,d0k,
:kk;.0000000000000.c0k;
:k000000000000000k:
,x000000000000x,
,l00000000l.
,ddl.

--=[metasploit v6.4.38-dev]
+ --=[2469 exploits - 1273 auxiliary - 431 post]
+ --=[1478 payloads - 49 encoders - 13 nops]
+ --=[9 evasion]

Metasploit Documentation: https://docs.metasploit.com/
msf6 > search telnet_version

Matching Modules

Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/scanner/telnet/lantronix_telnet_version . normal No Lantronix Telnet Service Ba
nner Detection
1 auxiliary/scanner/telnet/telnet_version . normal No Telnet Service Banner Detec
tion

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version
msf6 >

In seguito ho selezionato la vulnerabilità corretta ed ho settato il mio target col comando `set RHOST <ip target>` ed ho dato un `run` per dare il via all'exploit e farmi droppe le credenziali di accesso.

[illegible]