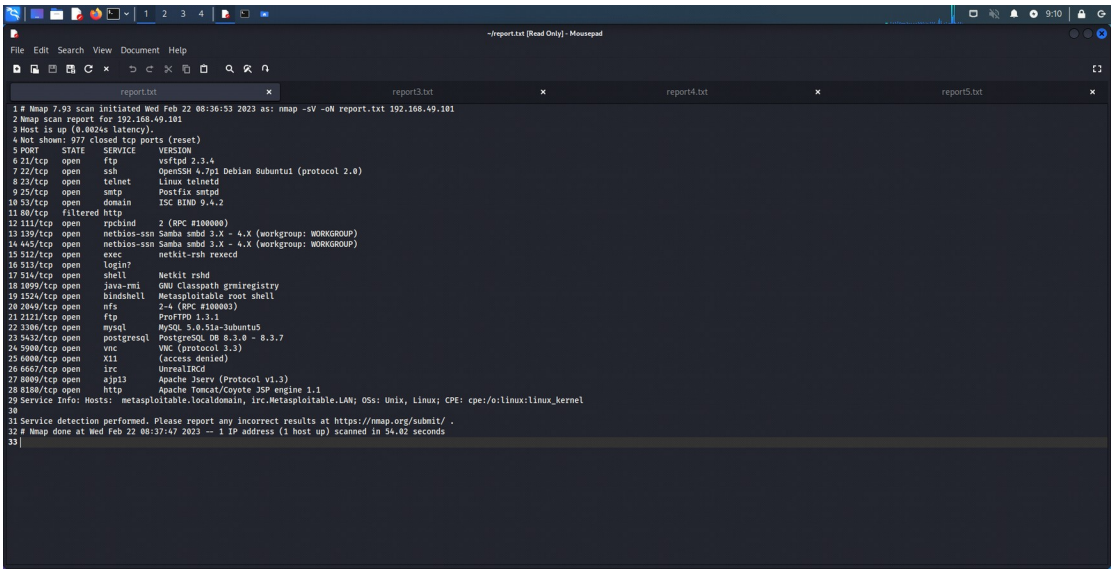
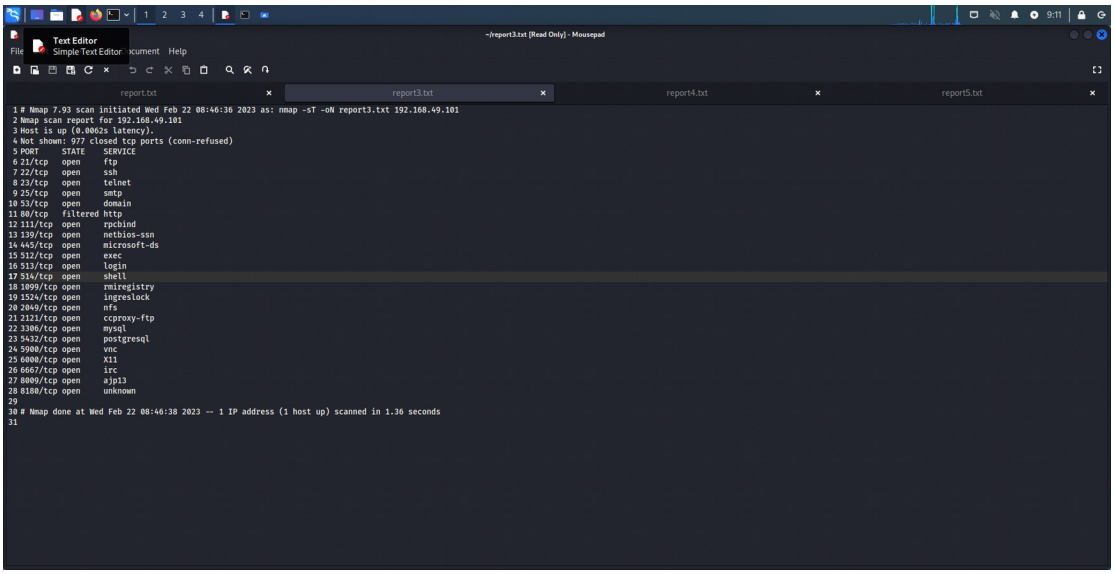
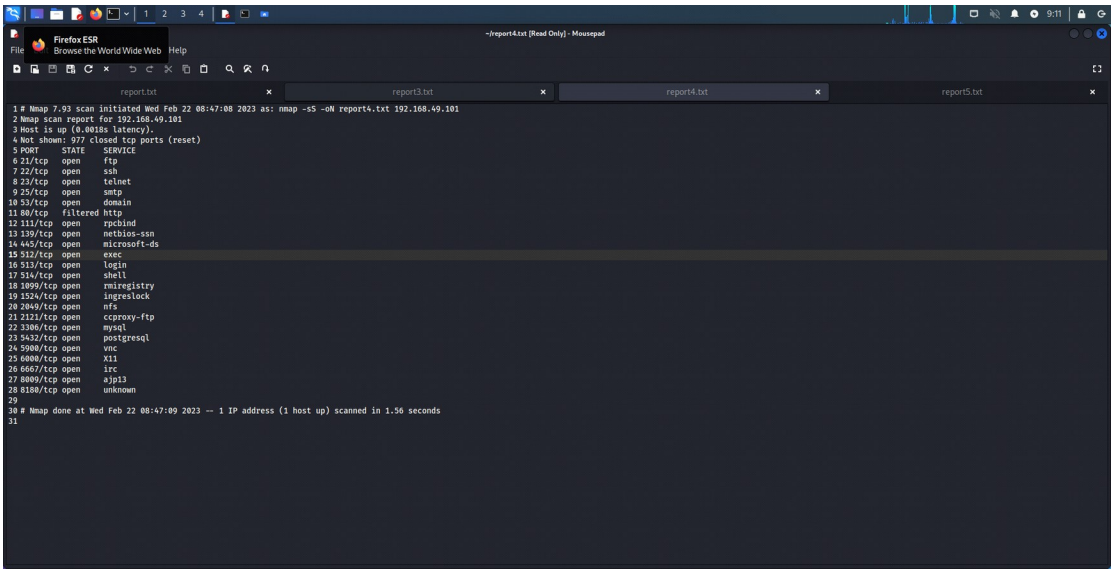
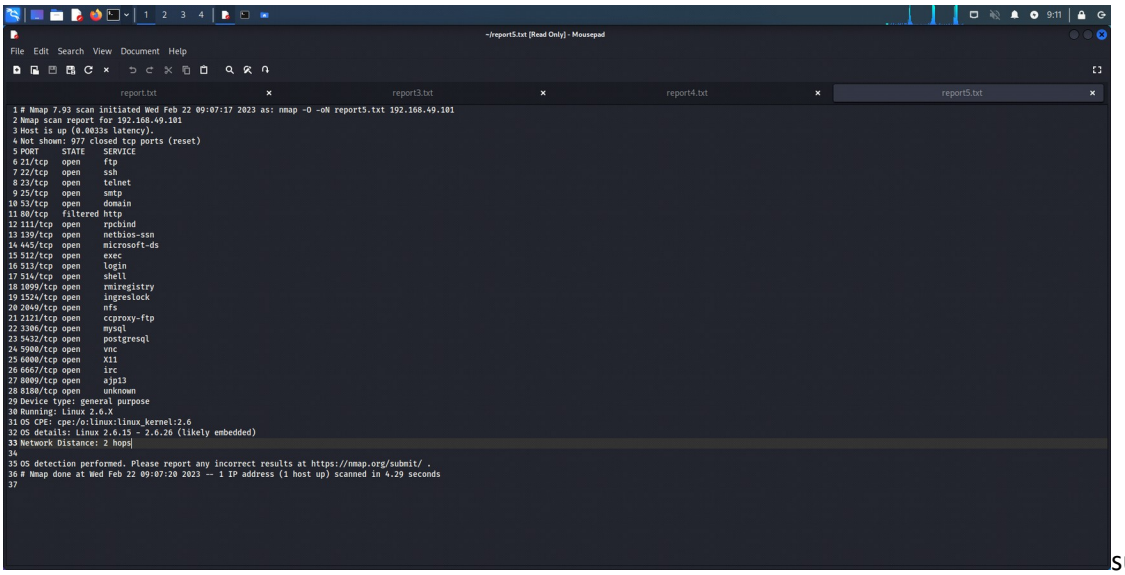

~/report.txt [Read Only] - Mousepad
File Edit Search View Document Help
report.txt
report3.txt
report4.txt
report5.txt
1 # Nmap 7.93 scan initiated Wed Feb 22 08:36:53 2023 as: nmap -sV -oN report.txt 192.168.49.101
2 Nmap scan report for 192.168.49.101
3 Host is up (0.0024s latency).
4 Not shown: 977 closed tcp ports (reset)
5 PORT STATE SERVICE VERSION
6 21/tcp open ftp vsftpd 2.3.4
7 22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
8 23/tcp open telnet Linux telnetd
9 25/tcp open smtp Postfix smtpd
10 53/tcp open domain ISC BIND 9.4.2
11 80/tcp filtered http
12 111/tcp open rpcbind 2 (RPC #100000)
13 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
14 445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
15 512/tcp open exec netkit-rsh rexecd
16 513/tcp open login?
17 514/tcp open shell Netkit rshd
18 1099/tcp open java-rmi GNU Classpath grmiregistry
19 1524/tcp open bindshell Metasploitable root shell
20 2049/tcp open nfs 2-4 (RPC #100003)
21 2121/tcp open ftp ProFTPD 1.3.1
22 3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
23 5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
24 5900/tcp open vnc VNC (protocol 3.3)
25 6000/tcp open X11 (access denied)
26 6667/tcp open irc UnrealIRCd
27 8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
28 8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
29 Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
30
31 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
32 # Nmap done at Wed Feb 22 08:37:47 2023 -- 1 IP address (1 host up) scanned in 54.02 seconds
33

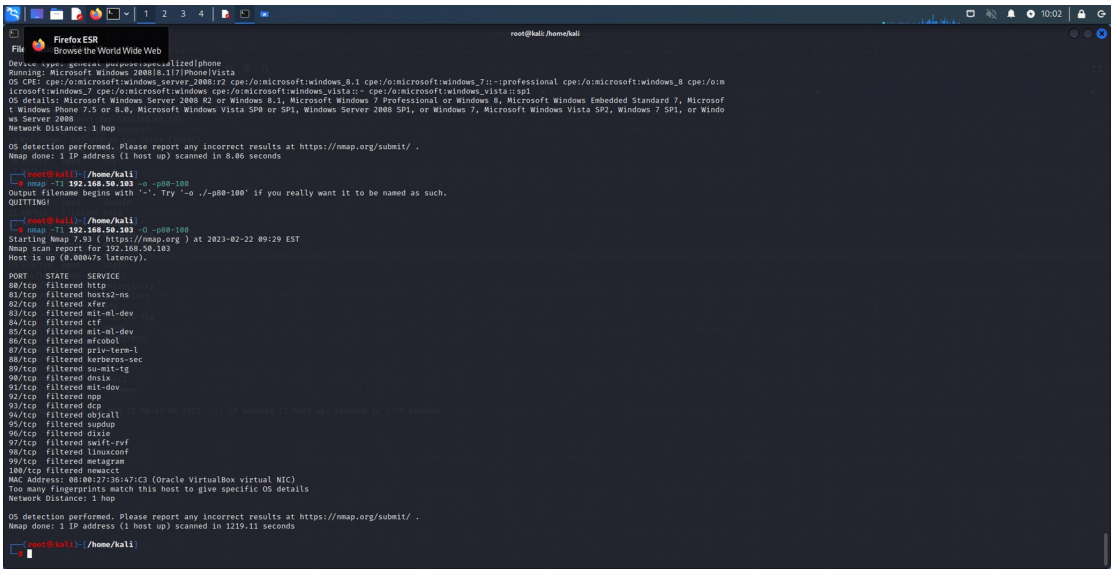

Text Editor
Simple Text Editor
~/report3.txt [Read Only] - Mousepad
report.txt
report3.txt
report4.txt
report5.txt
1 # Nmap 7.93 scan initiated Wed Feb 22 08:46:36 2023 as: nmap -sT -oN report3.txt 192.168.49.101
2 Nmap scan report for 192.168.49.101
3 Host is up (0.0002s latency).
4 Not shown: 977 closed tcp ports (conn-refused)
5 PORT STATE SERVICE
6 21/tcp open ftp
7 22/tcp open ssh
8 23/tcp open telnet
9 25/tcp open smtp
10 53/tcp open domain
11 80/tcp filtered http
12 111/tcp open rpcbind
13 139/tcp open netbios-ssn
14 445/tcp open microsoft-ds
15 512/tcp open exec
16 513/tcp open login
17 514/tcp open shell
18 1099/tcp open rmiregistry
19 1524/tcp open ingreslock
20 2049/tcp open nfs
21 2121/tcp open ccproxy-ftp
22 3306/tcp open mysql
23 5432/tcp open postgresql
24 5900/tcp open vnc
25 6000/tcp open X11
26 6667/tcp open irc
27 8009/tcp open ajp13
28 8180/tcp open unknown
29
30 # Nmap done at Wed Feb 22 08:46:38 2023 -- 1 IP address (1 host up) scanned in 1.36 seconds
31





su windows non si riesce a trovare le porte aperte perchè il firewall blocca lo scan

la soluzione è impostare il timing a t1 e la scansione avviene con successo


Firefox ESR
Browse the World Wide Web
root@kali: /home/kali
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
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 8.06 seconds
root@kali: /home/kali
nmap -T1 192.168.50.103 -o -p80-100
Output filename begins with '-'. Try '-o ./-p80-100' if you really want it to be named as such.
QUITTING!
root@kali: /home/kali
nmap -T1 192.168.50.103 -O -p80-100
Starting Nmap 7.93 (https://nmap.org) at 2023-02-22 09:29 EST
Nmap scan report for 192.168.50.103
Host is up (0.00047s latency).
PORT STATE SERVICE
80/tcp filtered http
81/tcp filtered hosts2-ns
82/tcp filtered xfer
83/tcp filtered mit-ml-dev
84/tcp filtered ctf
85/tcp filtered mit-ml-dev
86/tcp filtered mfcobol
87/tcp filtered priv-term-l
88/tcp filtered kerberos-sec
89/tcp filtered su-mit-tg
90/tcp filtered dnsix
91/tcp filtered mit-dov
92/tcp filtered npp
93/tcp filtered dcp
94/tcp filtered objcall
95/tcp filtered supdup
96/tcp filtered dixie
97/tcp filtered swift-rvf
98/tcp filtered linuxconf
99/tcp filtered metagram
100/tcp filtered newacct
MAC Address: 08:00:27:36:47:C3 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
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 1219.11 seconds
root@kali: /home/kali
#