Lab #2:

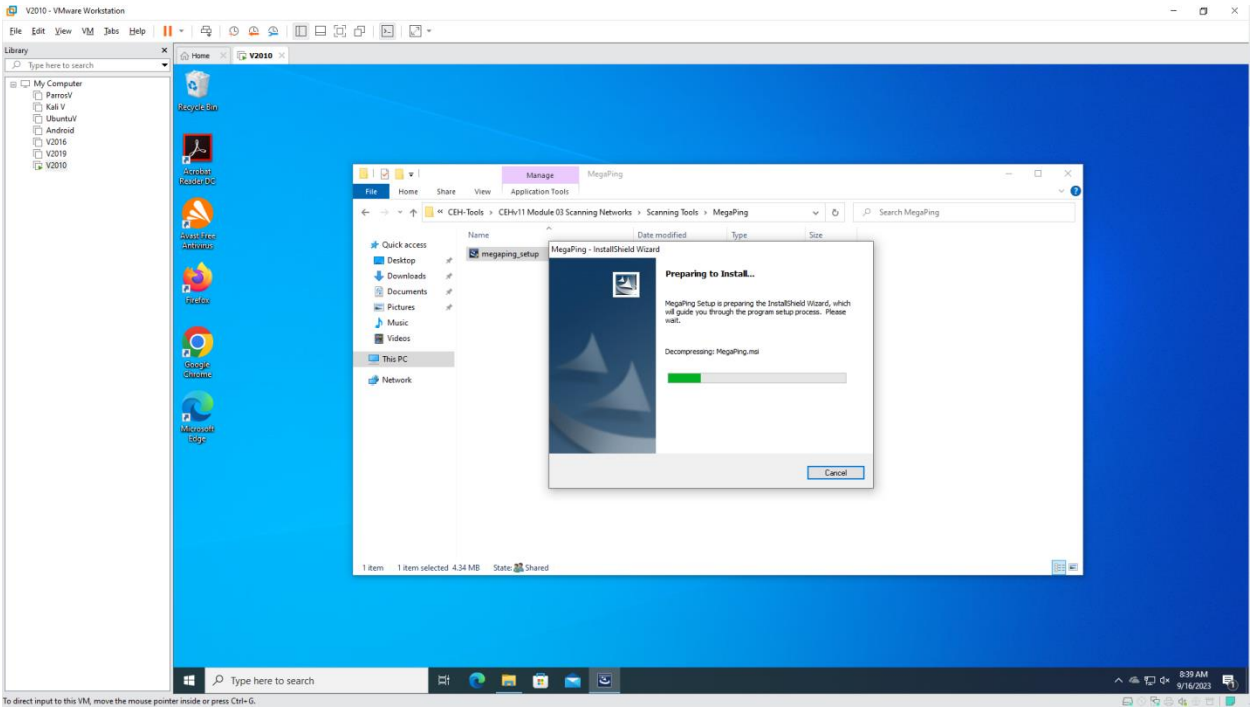
Course Name: Ethical Hacking and Offensive Security (HOD401)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 16/09/2023

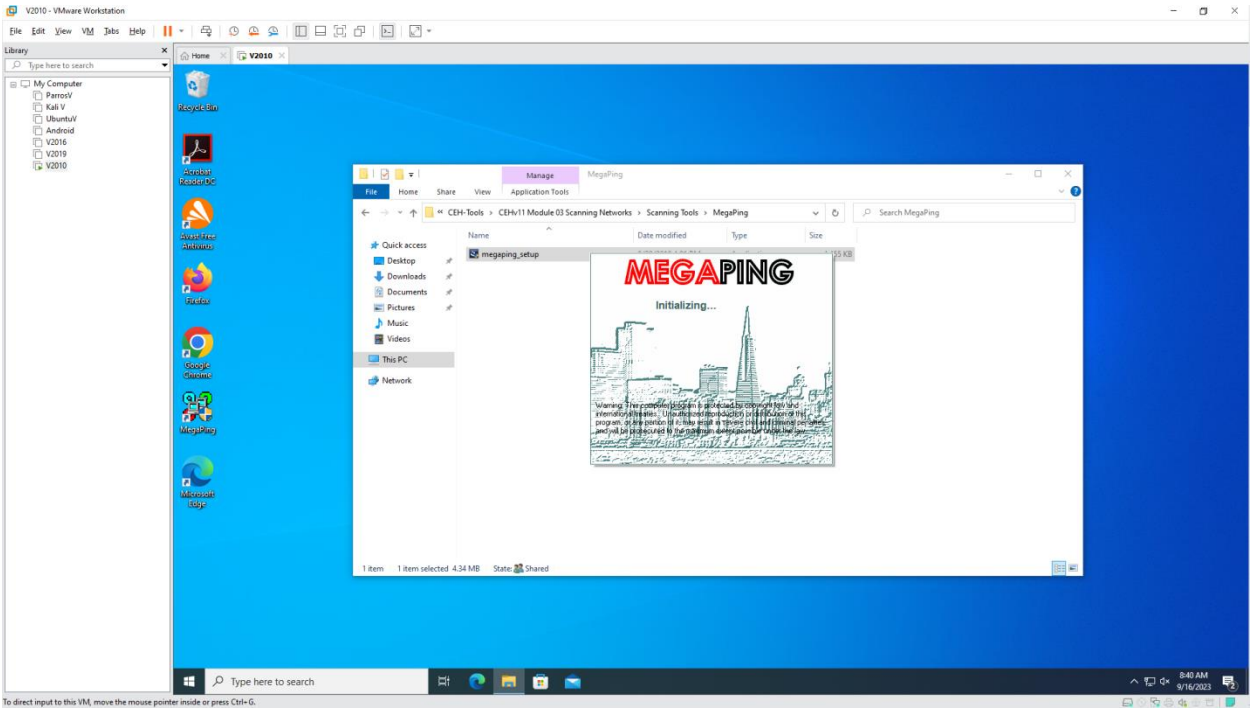
Lab tasks

2. Perform Port and Service Discovery

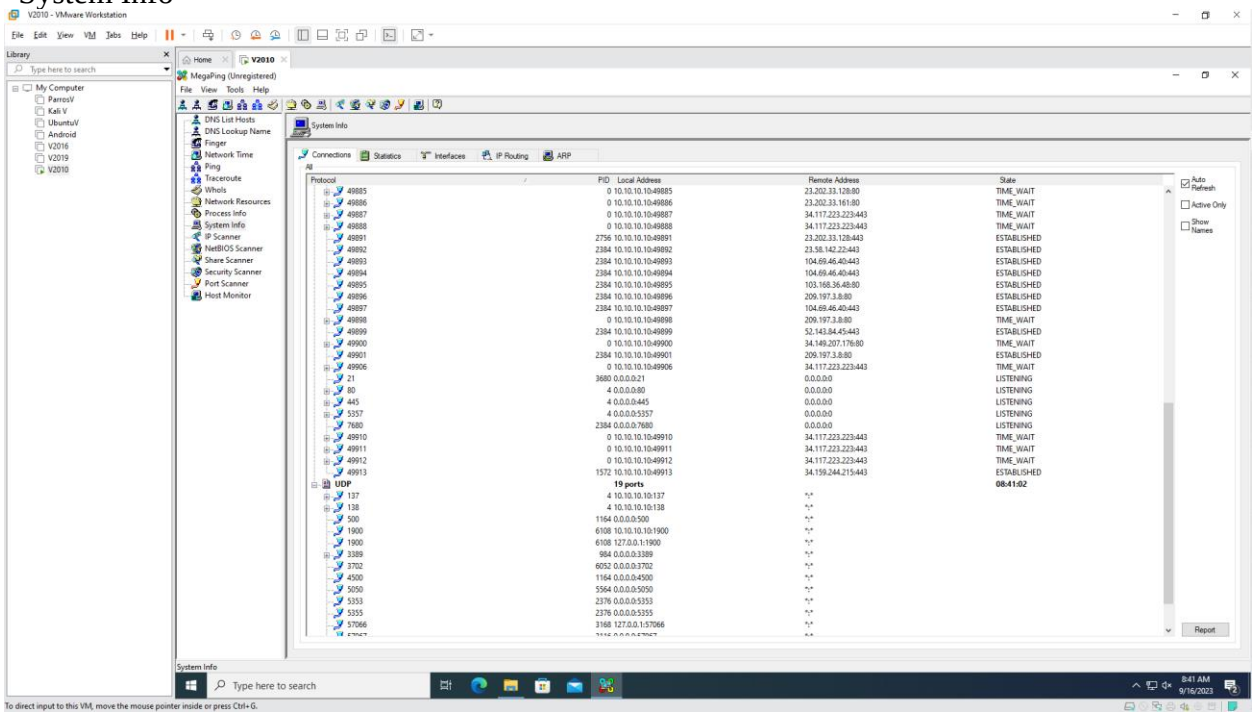
2.1 Perform Port and Service Discovery using MegaPing

- Open Windows 10, Windows Server 2016, Parrot and Ubuntu machine
- Install MegaPing

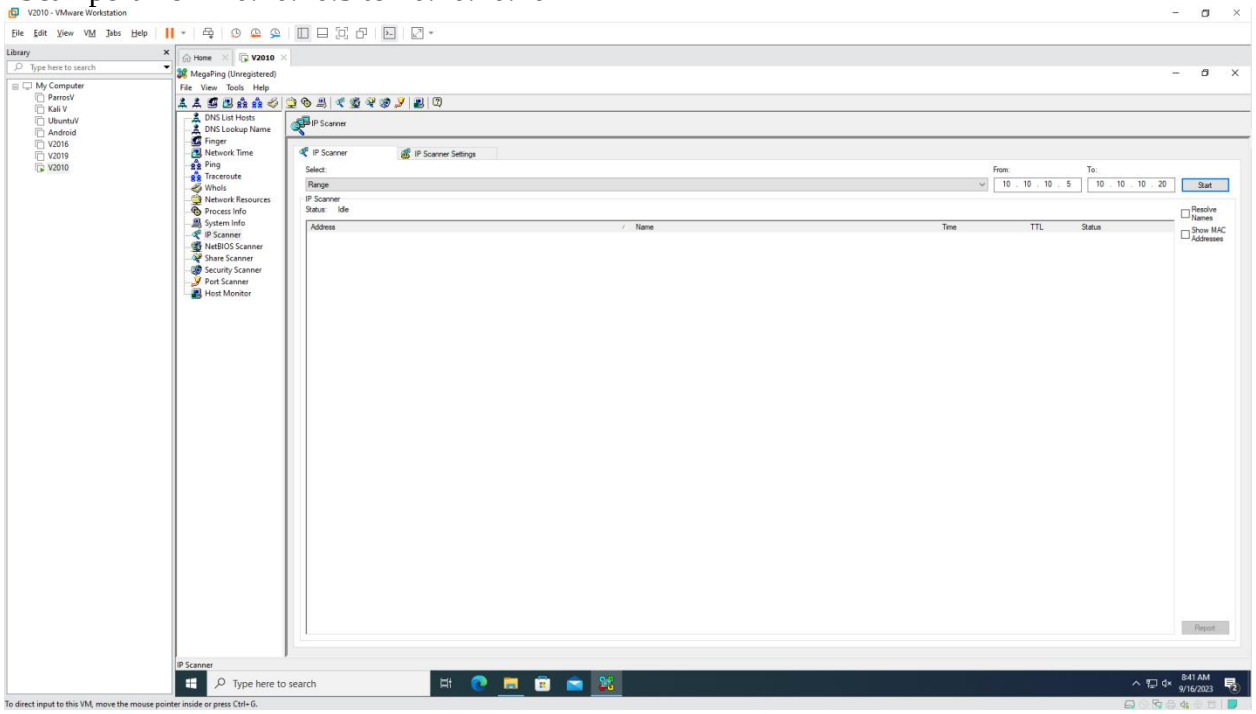

V2010 - VMware Workstation
MegaPing - InstallShield Wizard
Preparing to Install...
MegaPing Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.
Decompressing: MegaPing.msi
Cancel
megaping_setup
Type here to search
8:39 AM
9/16/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


V2010 - VMware Workstation
MEGAPING
Initializing...
megaping_setup
Type here to search
8:40 AM
9/16/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

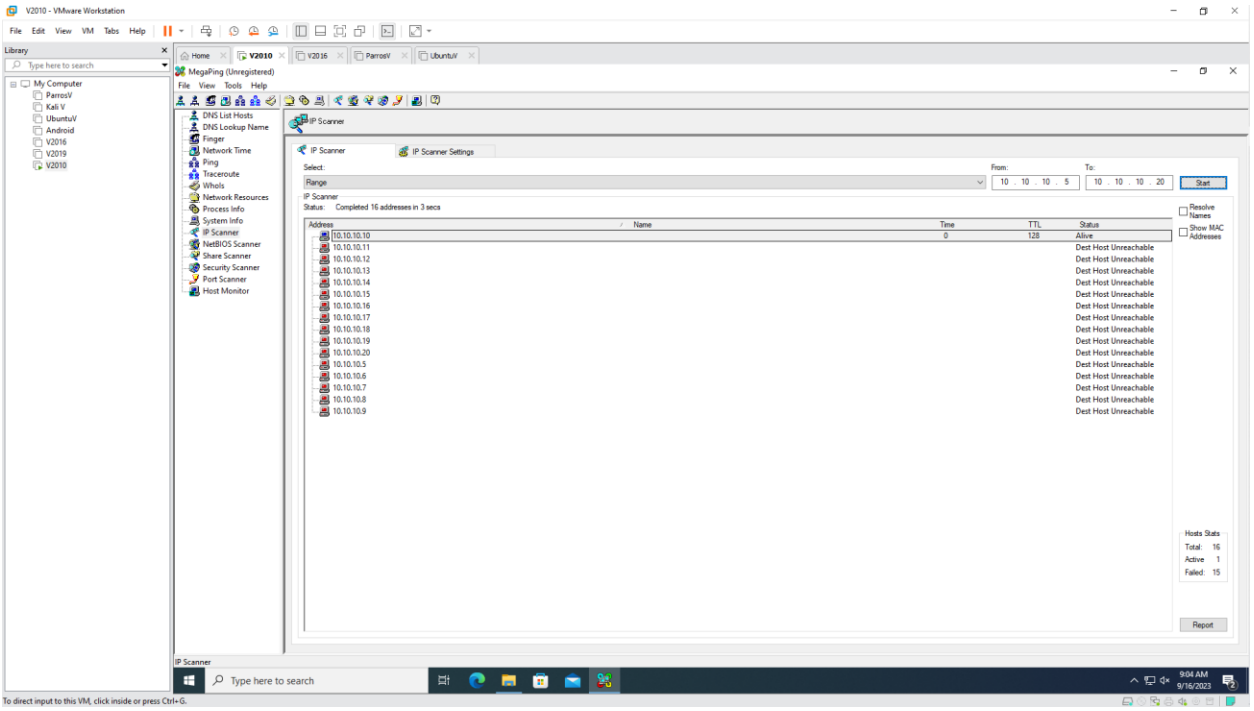
- System Info



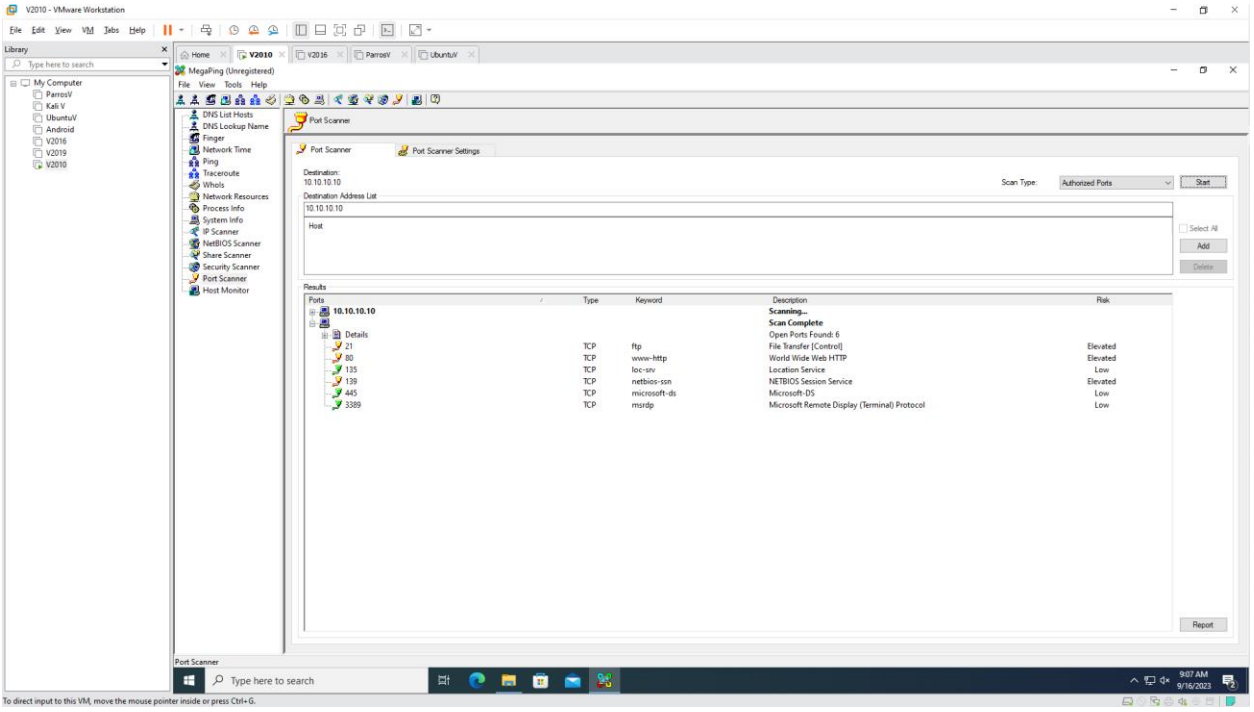
- Scan port from 10.10.10.5 to 10.10.10.20



- Result

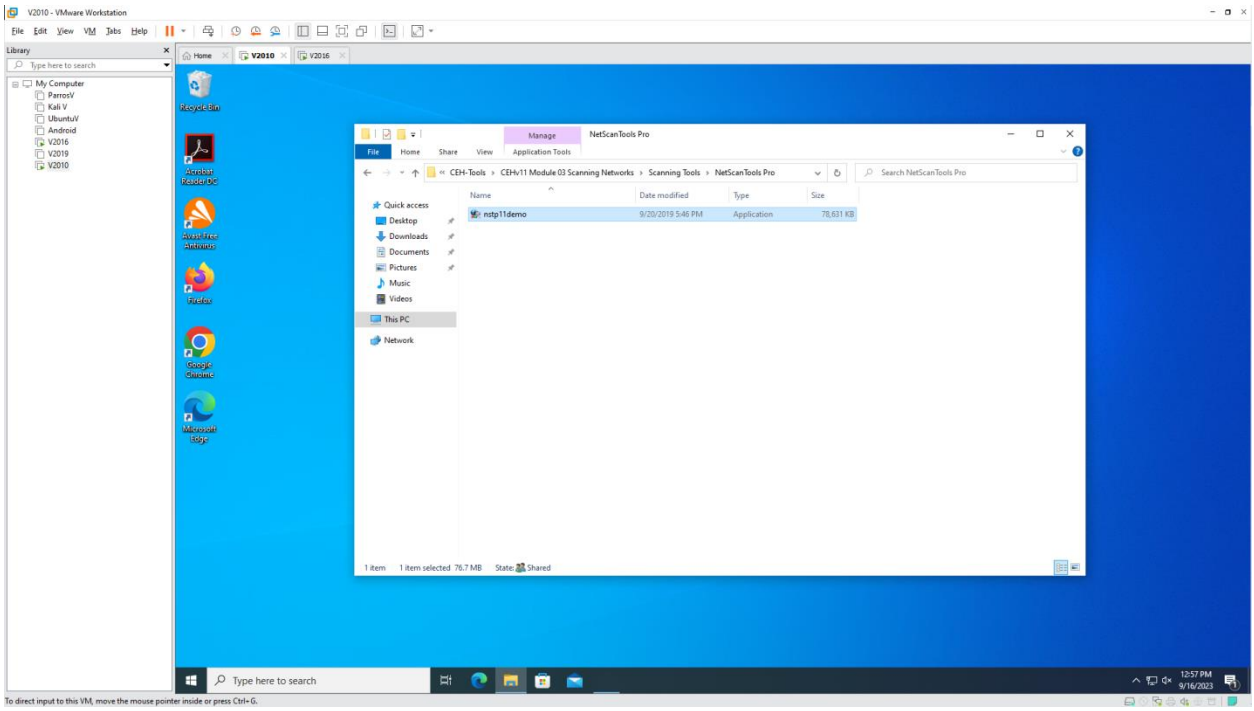


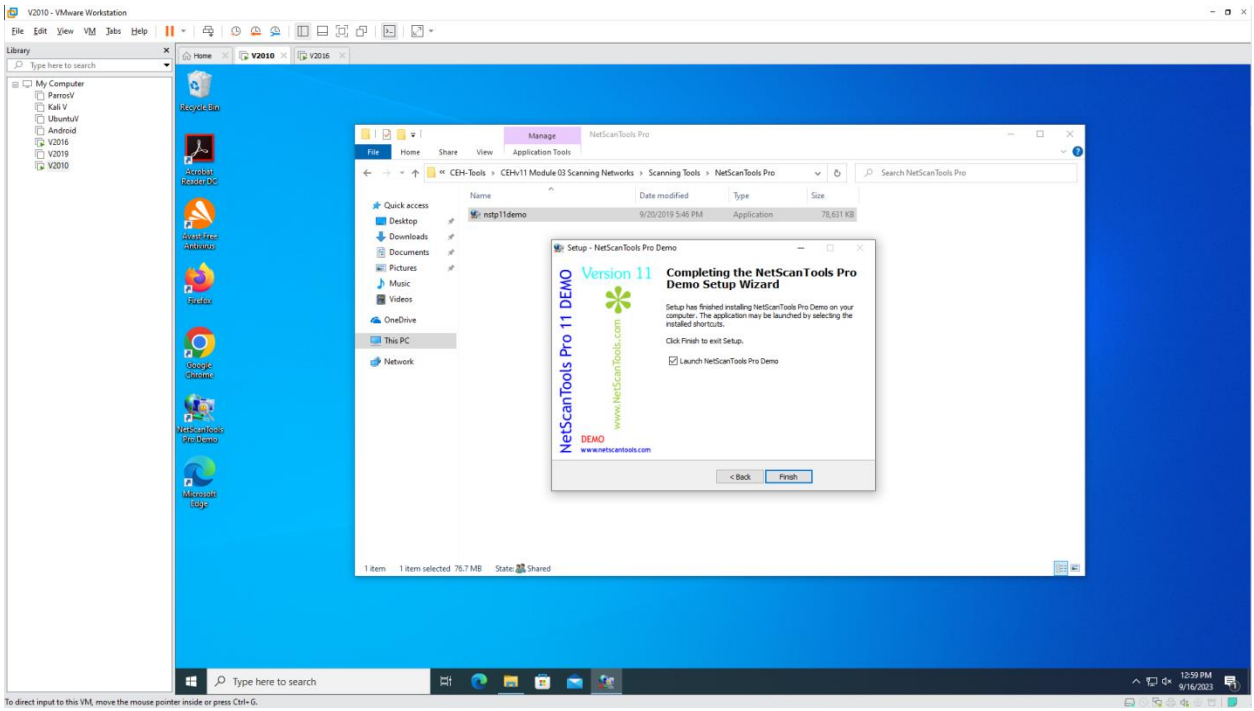
- Port scanner

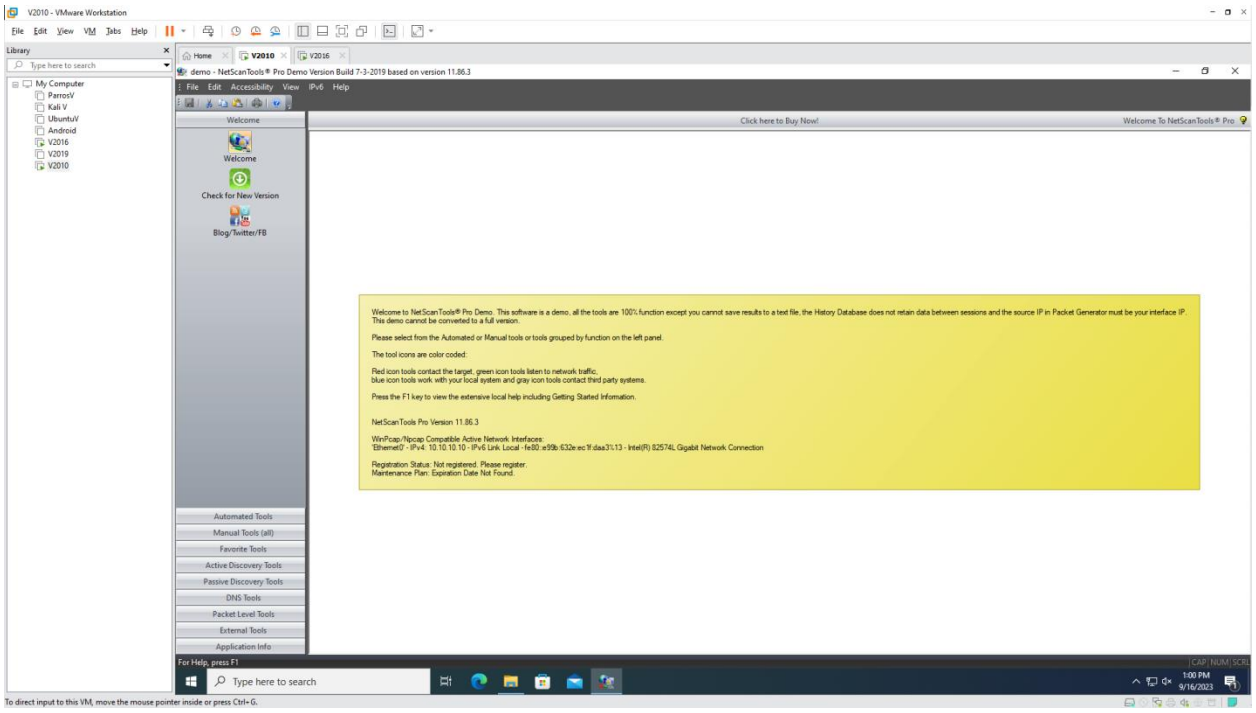


2.2 Perform Port and Service Discovery using NetScanTools Pro

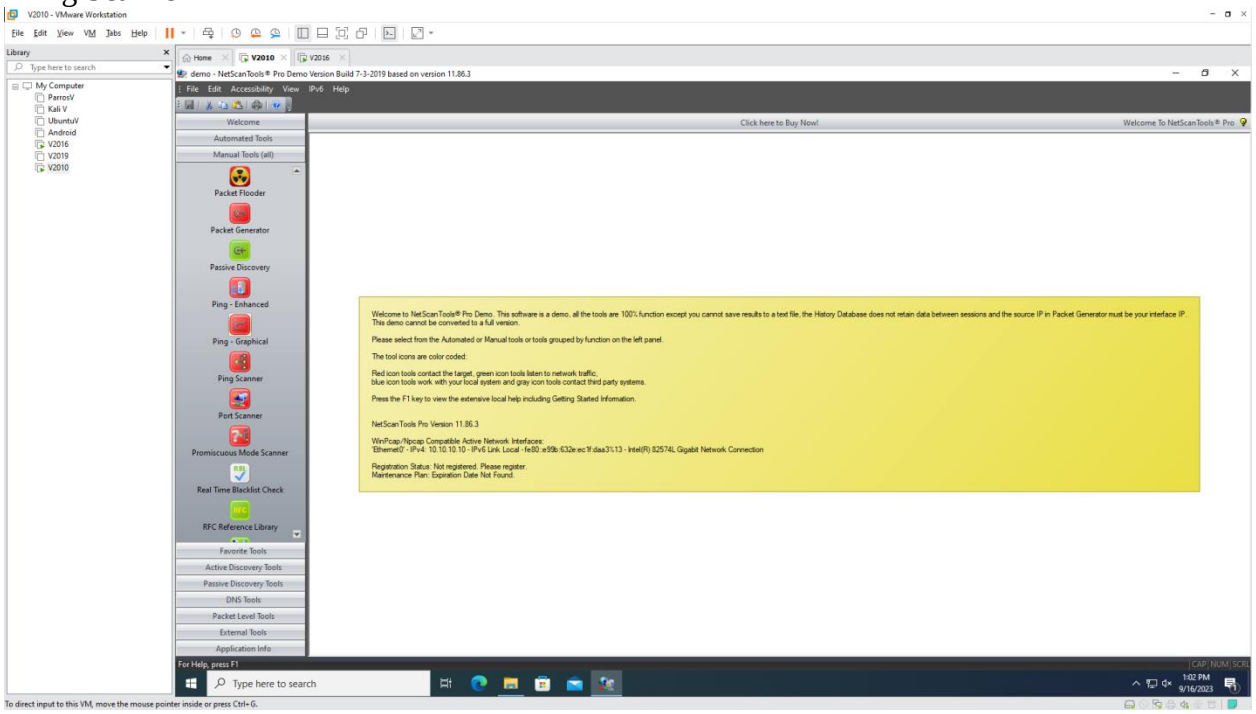
- Install NetScanTools Pro

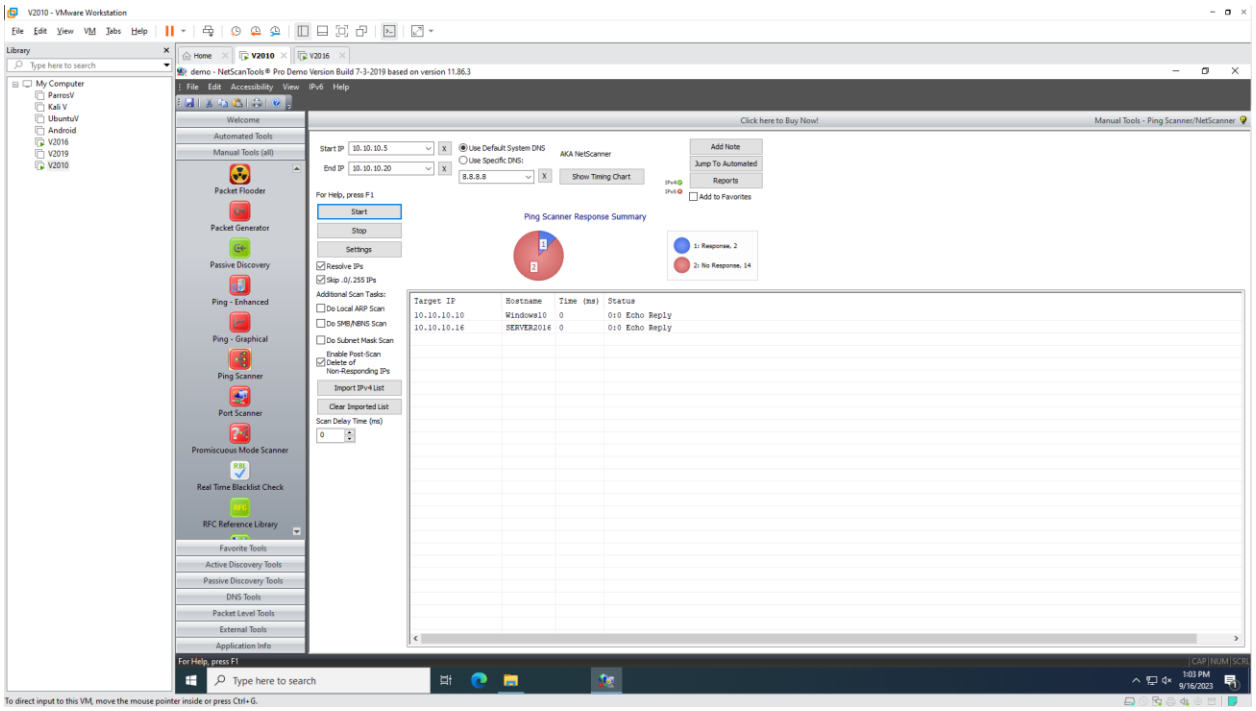

V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
ParrosV
Kali V
UbuntuV
Android
V2016
V2019
V2010
Home
V2010
V2016
Recycle Bin
Acrobat Reader DC
Avast Free Antivirus
Firefox
Google Chrome
Microsoft Edge
Manage
NetScanTools Pro
File Home Share View Application Tools
CEH-Tools › CEHv11 Module 03 Scanning Networks › Scanning Tools › NetScanTools Pro
Search NetScanTools Pro
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
Network
Name
Date modified
Type
Size
nstp11demo
9/20/2019 5:46 PM
Application
78,631 KB
1 item
1 item selected 76.7 MB
State: Shared
Type here to search
12:57 PM
9/16/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

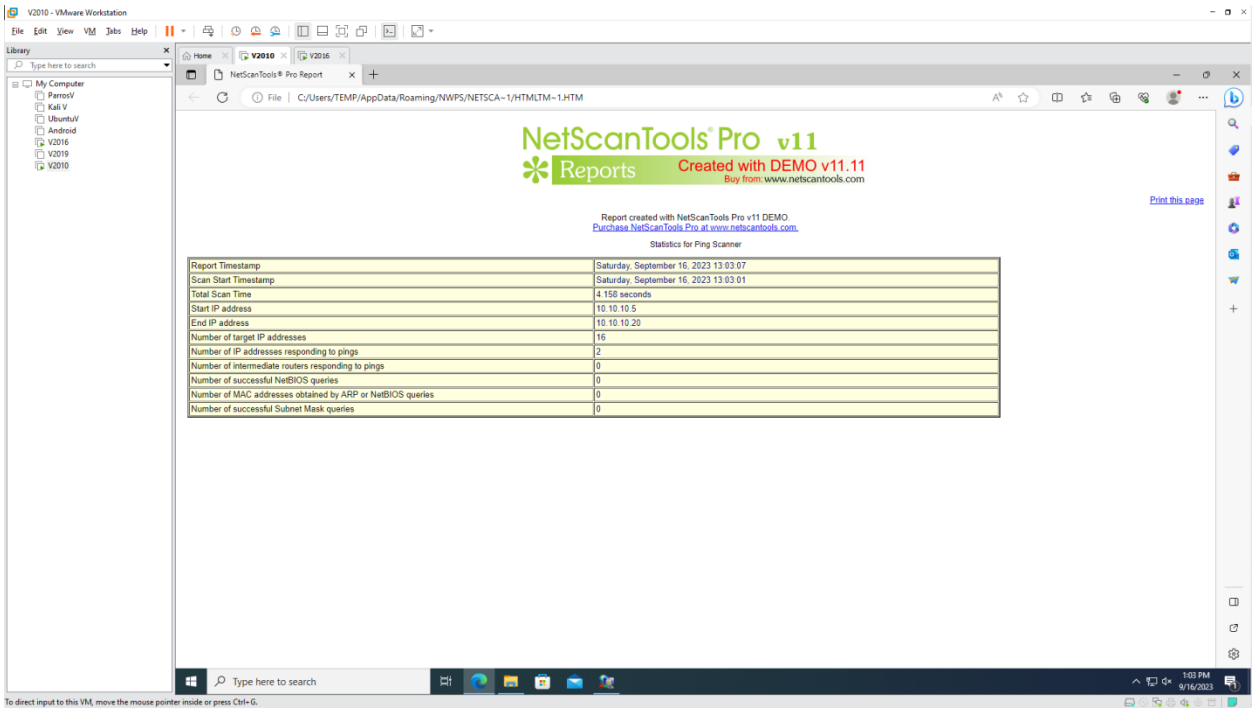

V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
ParrosV
Kali V
UbuntuV
Android
V2016
V2019
V2010
Home
V2010
V2016
Recycle Bin
Acrobat Reader DC
Avast Free Antivirus
Firefox
Google Chrome
NetScanTools Pro Demo
Microsoft Edge
Manage
NetScanTools Pro
File Home Share View Application Tools
CEH-Tools › CEHv11 Module 03 Scanning Networks › Scanning Tools › NetScanTools Pro
Search NetScanTools Pro
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
nstp11demo
9/20/2019 5:46 PM
Application
78,631 KB
Setup - NetScanTools Pro Demo
NetScanTools Pro 11 DEMO
Version 11
www.NetScanTools.com
DEMO
www.netscantools.com
Completing the NetScanTools Pro Demo Setup Wizard
Setup has finished installing NetScanTools Pro Demo on your computer. The application may be launched by selecting the installed shortcuts.
Click Finish to exit Setup.
Launch NetScanTools Pro Demo
< Back
Finish
1 item
1 item selected 76.7 MB
State: Shared
Type here to search
12:59 PM
9/16/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



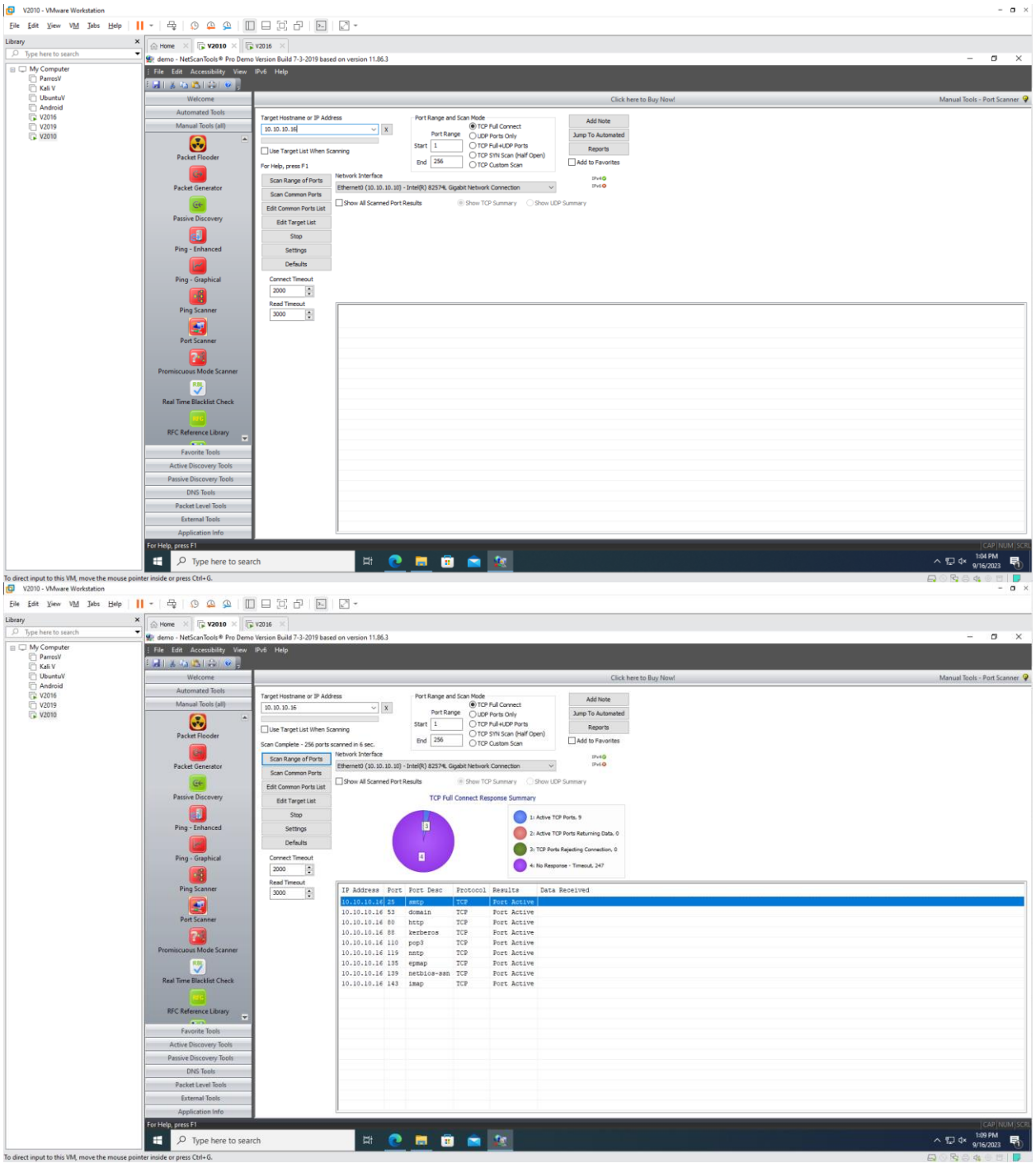
- Ping Scanner



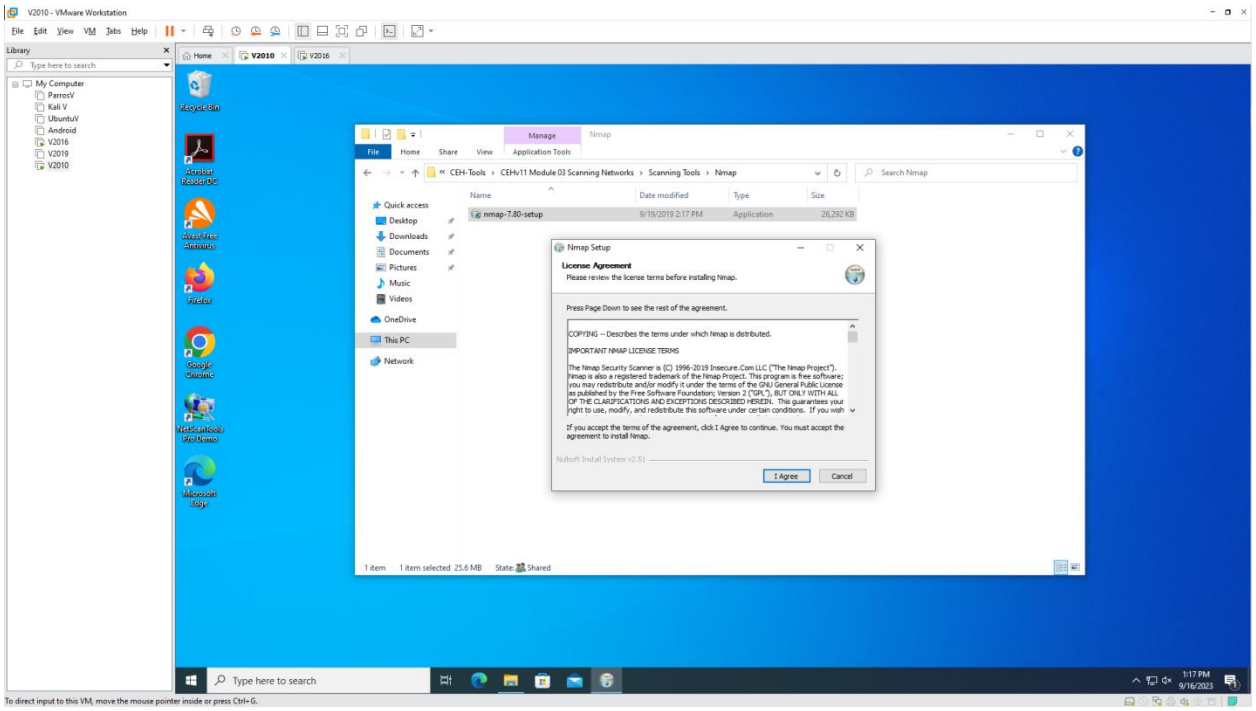




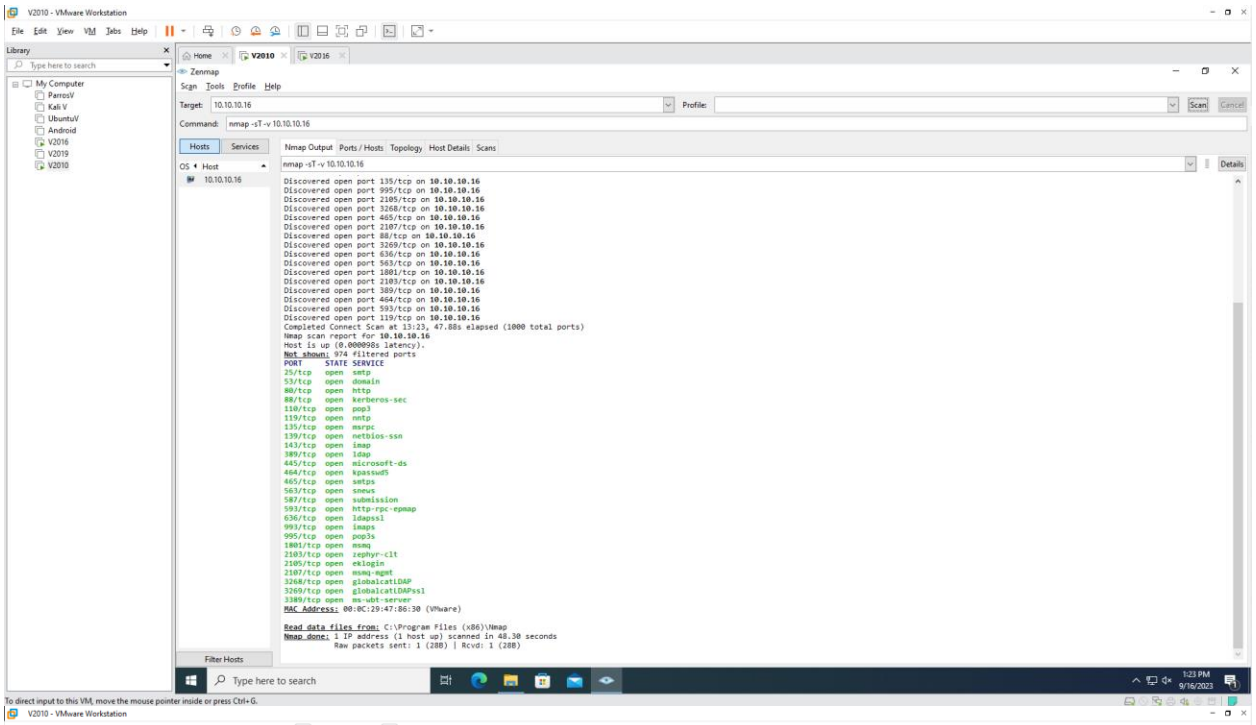
- Port Scanner

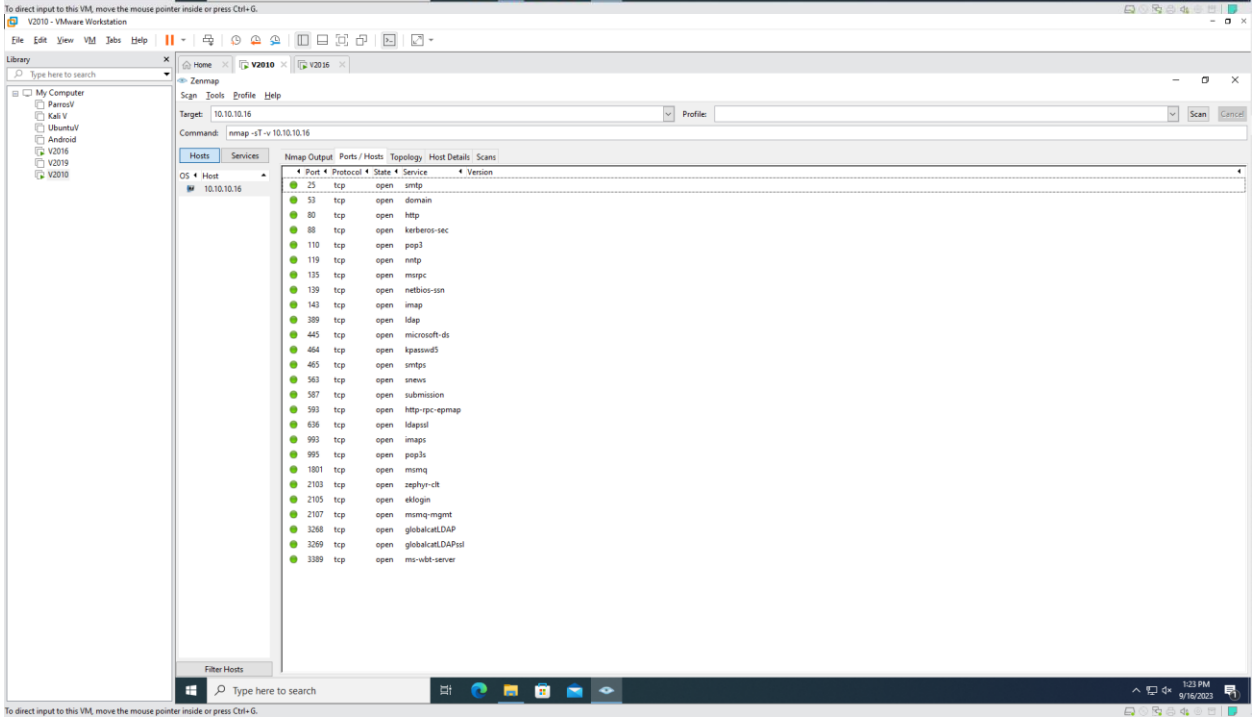


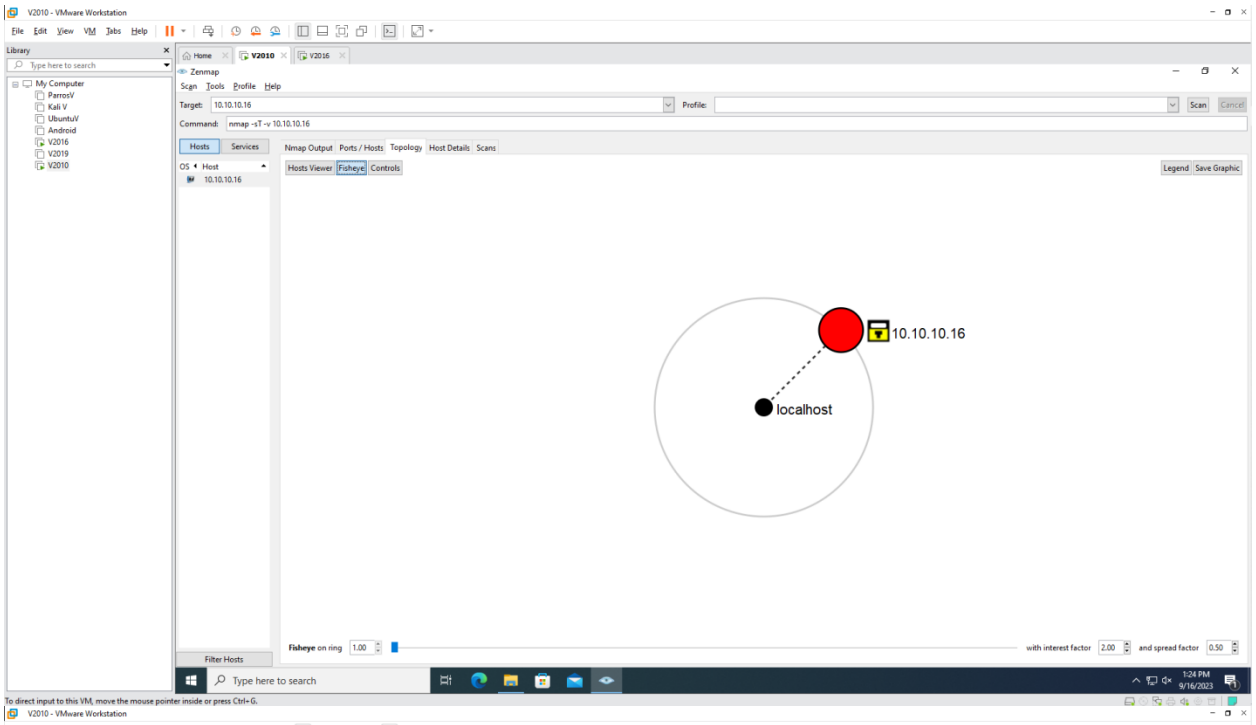
2.1 Explore Various Network Scanning Techniques using Nmap
- Install Nmap

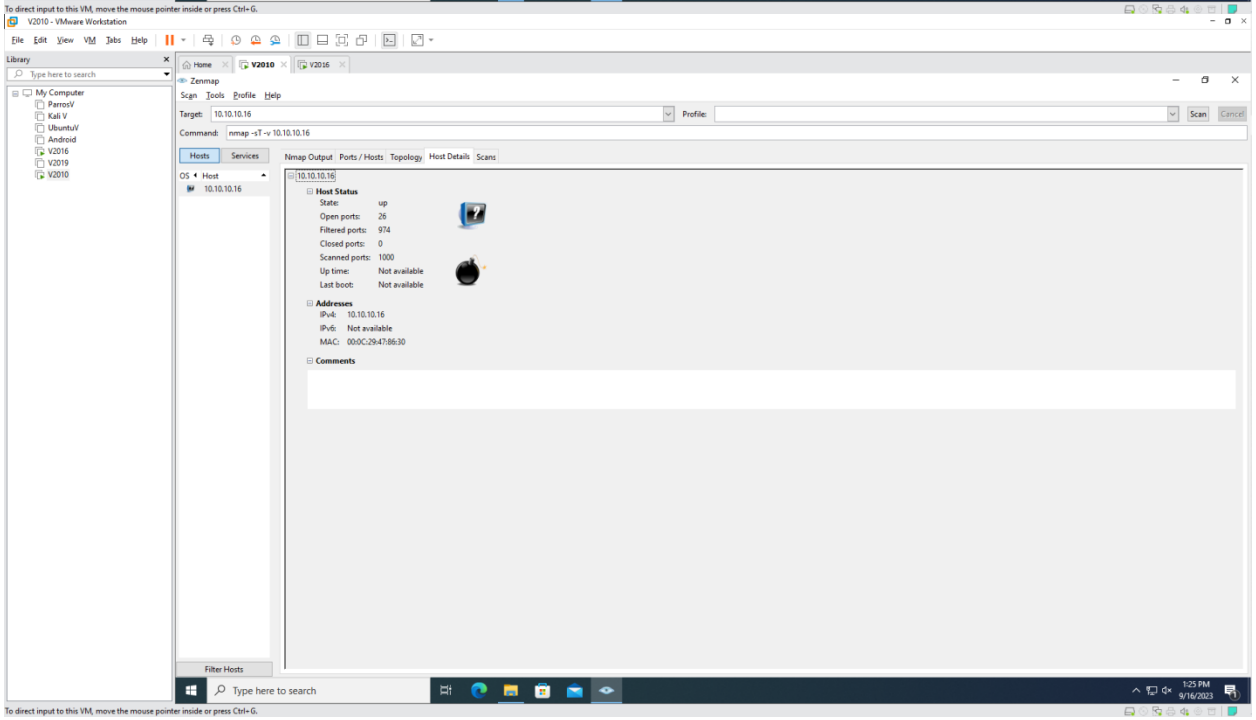

V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
ParrosV
Kali V
UbuntuV
Android
V2016
V2019
V2010
Home
V2010
V2016
Recycle Bin
Acrobat Reader DC
Avast Free Antivirus
Firefox
Google Chrome
NetSpotTools Pro Demo
Microsoft Edge
Manage
Nmap
File Home Share View Application Tools
CEH-Tools › CEHv11 Module 03 Scanning Networks › Scanning Tools › Nmap
Search Nmap
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
nmap-7.80-setup
9/19/2019 2:17 PM
Application
26,292 KB
Nmap Setup
License Agreement
Please review the license terms before installing Nmap.
Press Page Down to see the rest of the agreement.
COPYING -- Describes the terms under which Nmap is distributed.
IMPORTANT NMAP LICENSE TERMS
The Nmap Security Scanner is (C) 1996-2019 Insecure.Com LLC ("The Nmap Project"). Nmap is also a registered trademark of the Nmap Project. This program is free software; you may redistribute and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; Version 2 ("GPL"), BUT ONLY WITH ALL OF THE CLARIFICATIONS AND EXCEPTIONS DESCRIBED HEREIN. This guarantees your right to use, modify, and redistribute this software under certain conditions. If you wish
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Nmap.
Nullsoft Install System v2.51
I Agree
Cancel
1 item
1 item selected 25.6 MB
State: Shared
Type here to search
1:17 PM
9/16/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

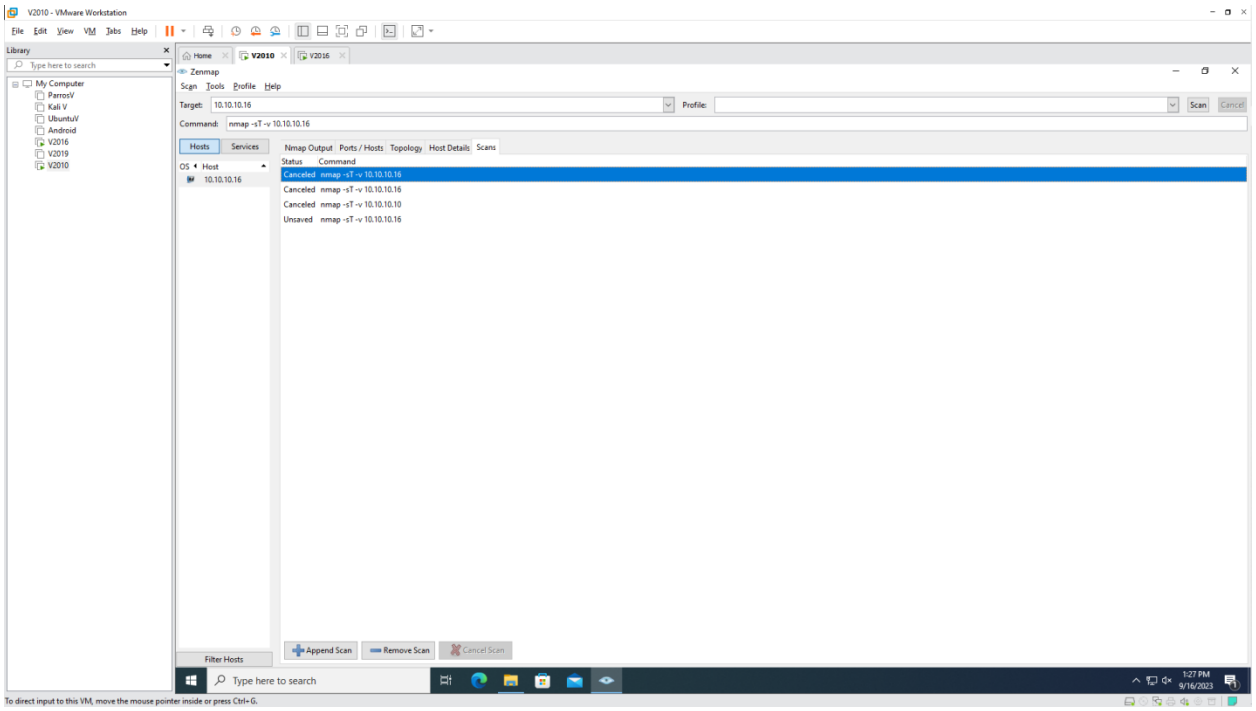
- Scan port


V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
ParrosV
Kali V
UbuntuV
Android
V2016
V2019
V2010
Home
V2010
V2016
Zenmap
Scan Tools Profile Help
Target: 10.10.10.16
Profile:
Scan
Cancel
Command: nmap -sT -v 10.10.10.16
Hosts
Services
OS Host
10.10.10.16
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -sT -v 10.10.10.16
Details
Discovered open port 135/tcp on 10.10.10.16
Discovered open port 995/tcp on 10.10.10.16
Discovered open port 2105/tcp on 10.10.10.16
Discovered open port 3268/tcp on 10.10.10.16
Discovered open port 465/tcp on 10.10.10.16
Discovered open port 2107/tcp on 10.10.10.16
Discovered open port 88/tcp on 10.10.10.16
Discovered open port 3269/tcp on 10.10.10.16
Discovered open port 636/tcp on 10.10.10.16
Discovered open port 563/tcp on 10.10.10.16
Discovered open port 1801/tcp on 10.10.10.16
Discovered open port 2103/tcp on 10.10.10.16
Discovered open port 389/tcp on 10.10.10.16
Discovered open port 464/tcp on 10.10.10.16
Discovered open port 593/tcp on 10.10.10.16
Discovered open port 119/tcp on 10.10.10.16
Completed Connect Scan at 13:23, 47.08s elapsed (1000 total ports)
Nmap scan report for 10.10.10.16
Host is up (0.0000098s latency).
Not shown: 974 filtered ports
PORT STATE SERVICE
25/tcp open smtp
53/tcp open domain
80/tcp open http
88/tcp open kerberos-sec
110/tcp open pop3
119/tcp open nntp
135/tcp open msrpc
139/tcp open netbios-ssn
143/tcp open imap
389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
465/tcp open smtps
563/tcp open snews
587/tcp open submission
593/tcp open http-rpc-epmap
636/tcp open ldapssl
993/tcp open imaps
995/tcp open pop3s
1801/tcp open msmq
2103/tcp open zephyr-clt
2105/tcp open eklogin
2107/tcp open msmq-mgmt
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
3389/tcp open ms-wbt-server
MAC Address: 00:0C:29:47:86:30 (VMware)
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 48.30 seconds
Raw packets sent: 1 (28B) | Rcvd: 1 (28B)
Filter Hosts
Type here to search
1:23 PM
9/16/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

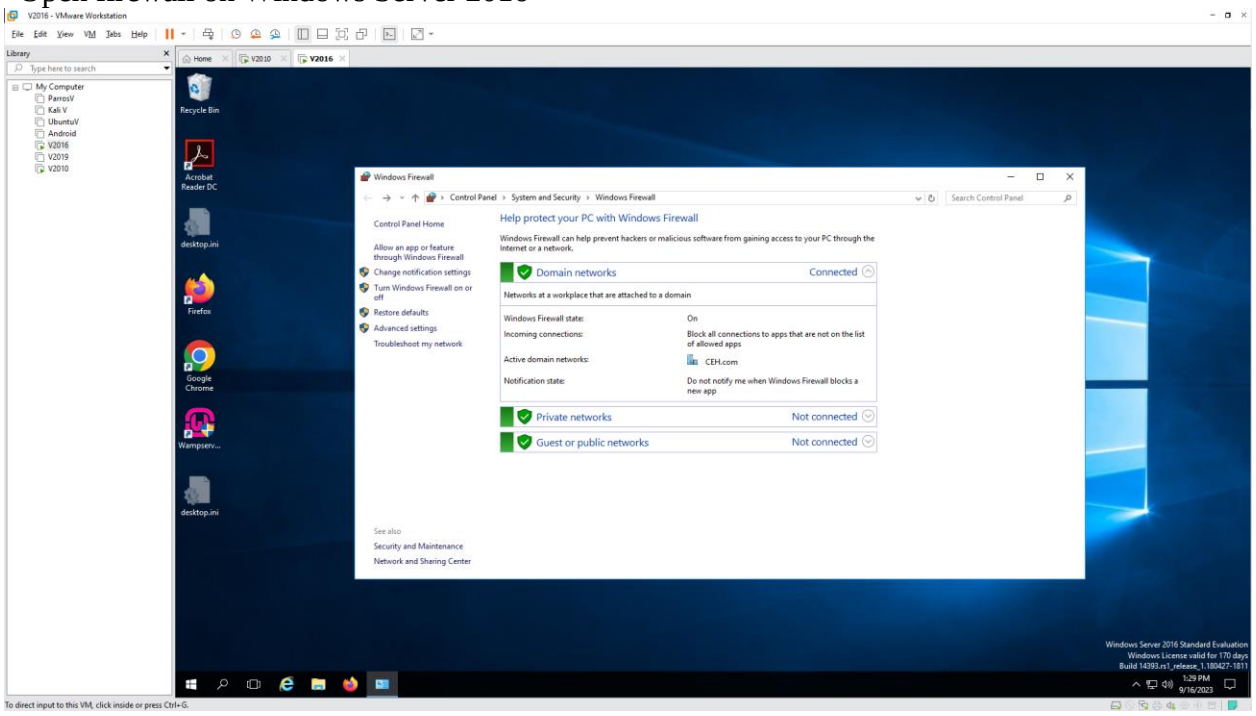

V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
ParrosV
Kali V
UbuntuV
Android
V2016
V2019
V2010
Home
V2010
V2016
Zenmap
Scan Tools Profile Help
Target: 10.10.10.16
Profile:
Scan
Cancel
Command: nmap -sT -v 10.10.10.16
Hosts
Services
OS Host
10.10.10.16
Nmap Output Ports / Hosts Topology Host Details Scans
Port Protocol State Service Version
25 tcp open smtp
53 tcp open domain
80 tcp open http
88 tcp open kerberos-sec
110 tcp open pop3
119 tcp open nntp
135 tcp open msrpc
139 tcp open netbios-ssn
143 tcp open imap
389 tcp open ldap
445 tcp open microsoft-ds
464 tcp open kpasswd5
465 tcp open smtps
563 tcp open snews
587 tcp open submission
593 tcp open http-rpc-epmap
636 tcp open ldapssl
993 tcp open imaps
995 tcp open pop3s
1801 tcp open msmq
2103 tcp open zephyr-clt
2105 tcp open eklogin
2107 tcp open msmq-mgmt
3268 tcp open globalcatLDAP
3269 tcp open globalcatLDAPssl
3389 tcp open ms-wbt-server
Filter Hosts
Type here to search
1:23 PM
9/16/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


V2010 - VMware Workstation
Zenmap
Target: 10.10.10.16
Command: nmap -sT -v 10.10.10.16
Topology
10.10.10.16
localhost

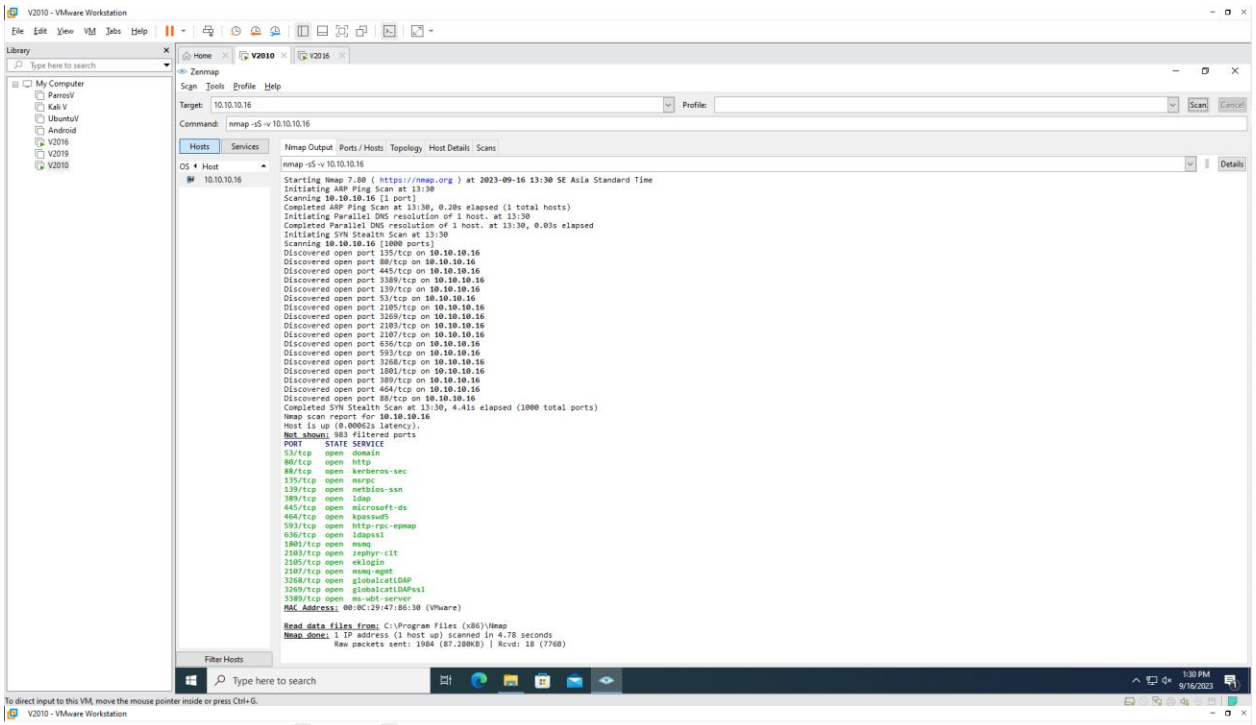

V2010 - VMware Workstation
Zenmap
Target: 10.10.10.16
Command: nmap -sT -v 10.10.10.16
Host Details
Host Status
State: up
Open ports: 26
Filtered ports: 974
Closed ports: 0
Scanned ports: 1000
Up time: Not available
Last boot: Not available
Addresses
IPv4: 10.10.10.16
IPv6: Not available
MAC: 00:0C:29:47:86:30
Comments

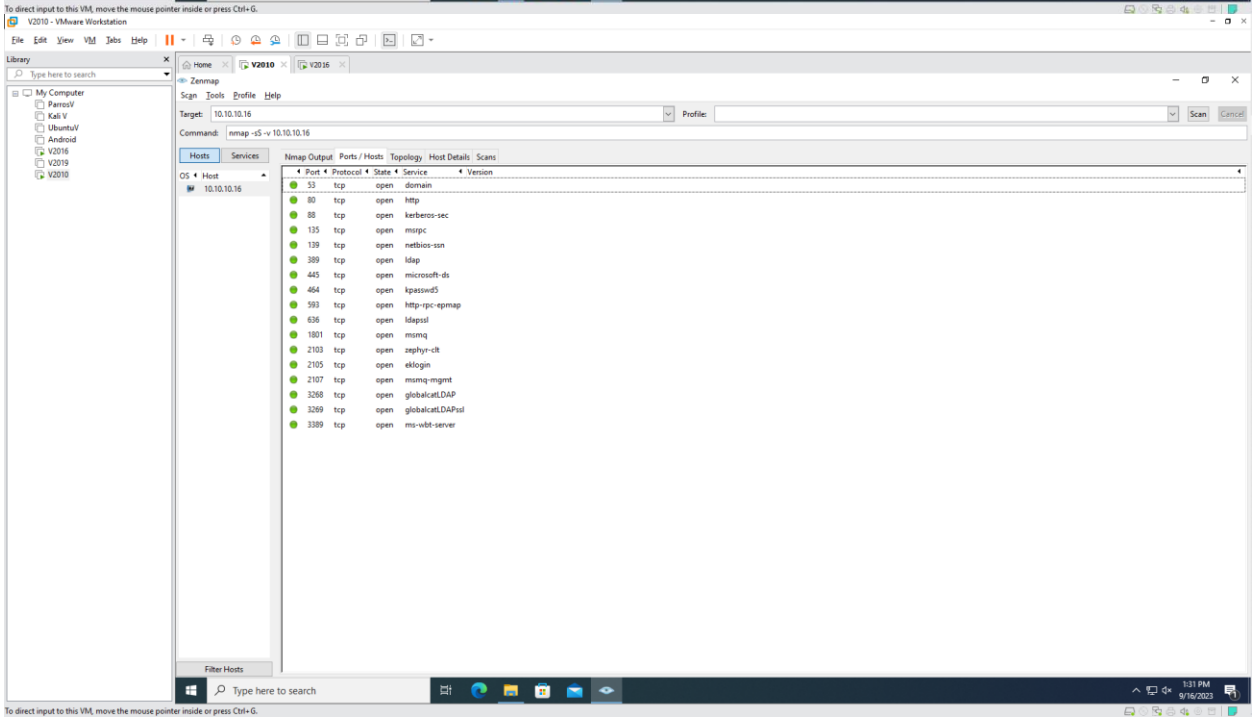


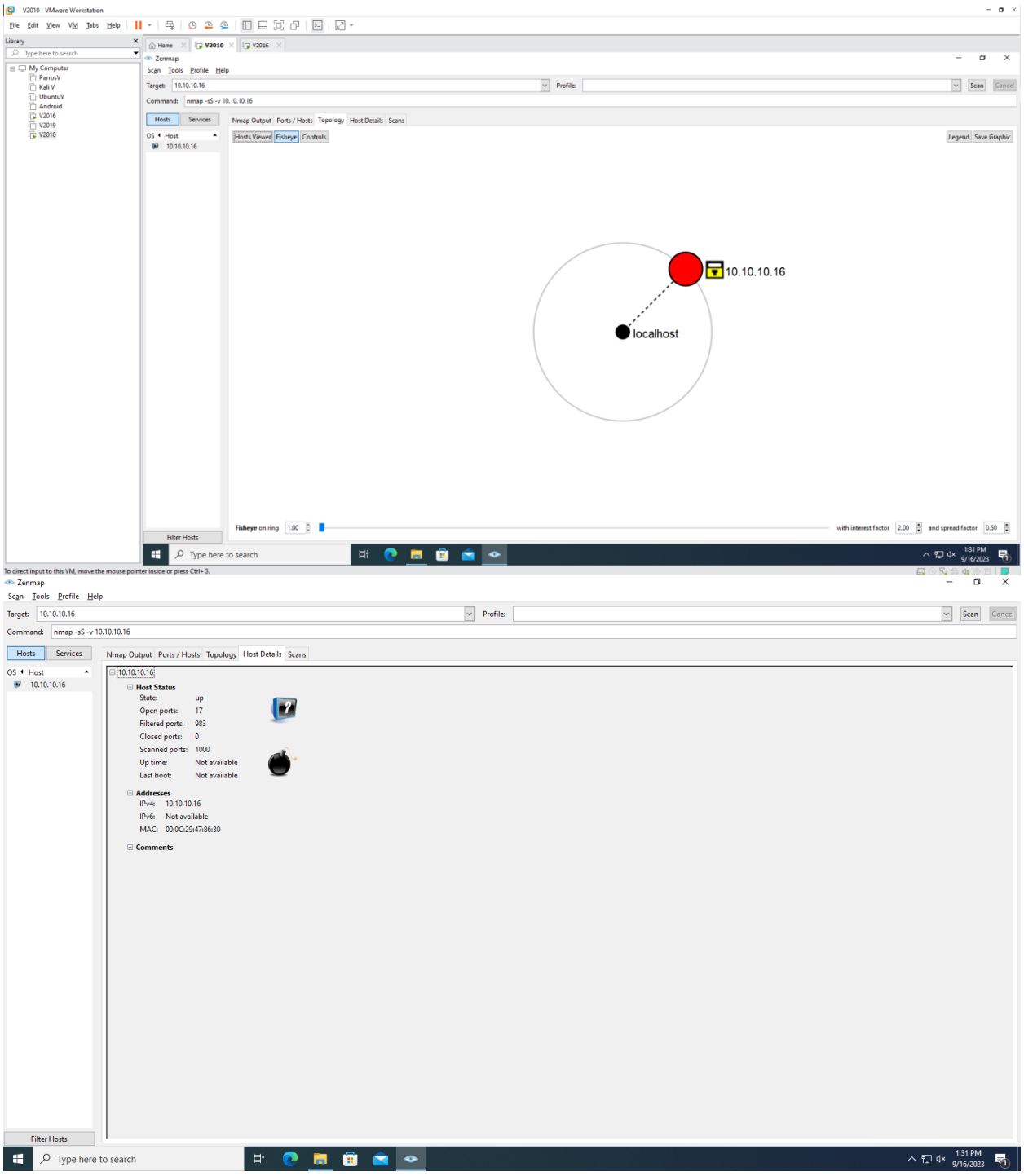
- Open firewall on Windows Server 2016

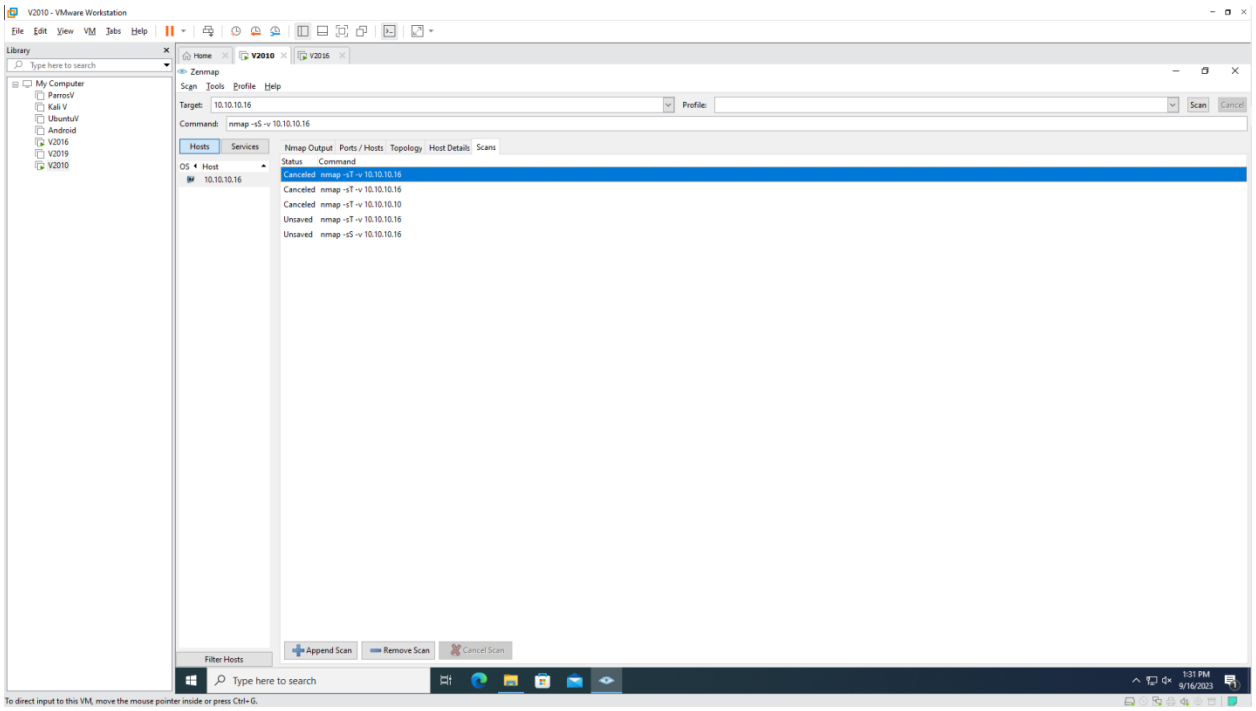


- Stealth scan on Windows 10

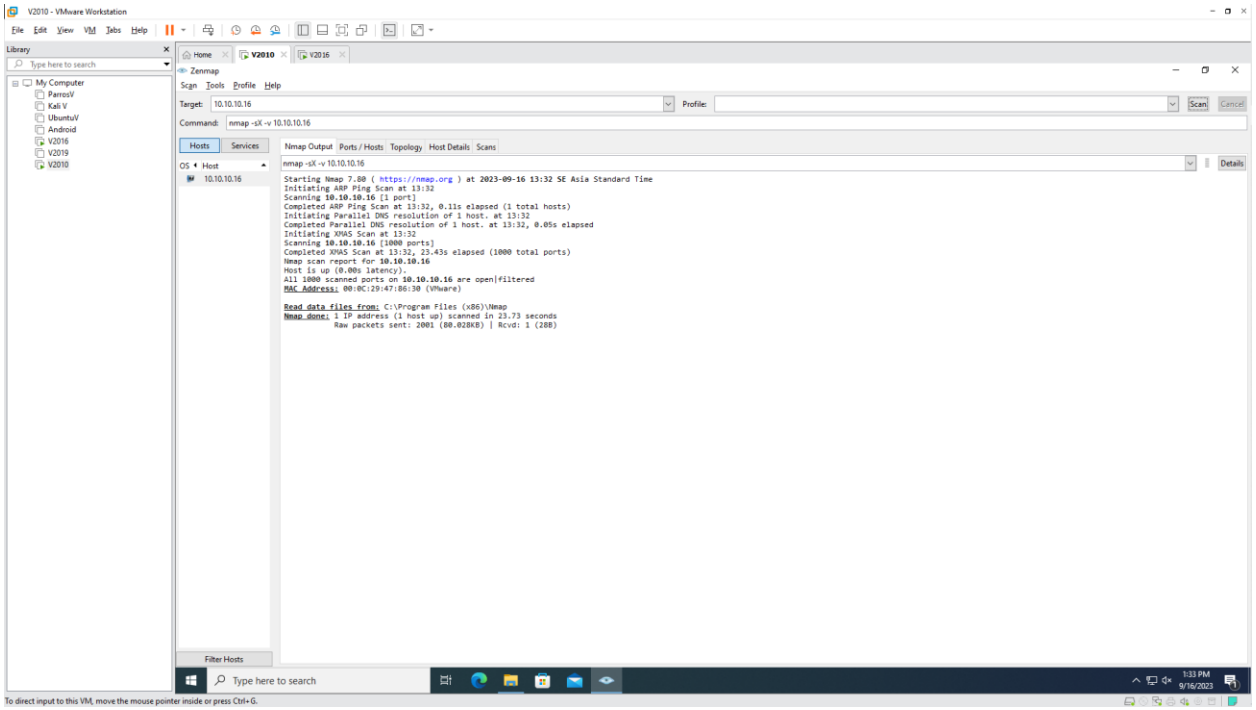

V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
ParrosV
Kali V
UbuntuV
Android
V2016
V2019
V2010
Home
V2010
V2016
Zenmap
Scan Tools Profile Help
Target: 10.10.10.16
Profile:
Scan
Cancel
Command: nmap -sS -v 10.10.10.16
Hosts
Services
OS Host
10.10.10.16
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -sS -v 10.10.10.16
Details
Starting Nmap 7.80 (https://nmap.org) at 2023-09-16 13:30 SE Asia Standard Time
Initiating ARP Ping Scan at 13:30
Scanning 10.10.10.16 [1 port]
Completed ARP Ping Scan at 13:30, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:30
Completed Parallel DNS resolution of 1 host. at 13:30, 0.03s elapsed
Initiating SYN Stealth Scan at 13:30
Scanning 10.10.10.16 [1000 ports]
Discovered open port 135/tcp on 10.10.10.16
Discovered open port 80/tcp on 10.10.10.16
Discovered open port 445/tcp on 10.10.10.16
Discovered open port 3389/tcp on 10.10.10.16
Discovered open port 139/tcp on 10.10.10.16
Discovered open port 53/tcp on 10.10.10.16
Discovered open port 2105/tcp on 10.10.10.16
Discovered open port 3269/tcp on 10.10.10.16
Discovered open port 2103/tcp on 10.10.10.16
Discovered open port 2107/tcp on 10.10.10.16
Discovered open port 636/tcp on 10.10.10.16
Discovered open port 593/tcp on 10.10.10.16
Discovered open port 3268/tcp on 10.10.10.16
Discovered open port 1801/tcp on 10.10.10.16
Discovered open port 389/tcp on 10.10.10.16
Discovered open port 464/tcp on 10.10.10.16
Discovered open port 88/tcp on 10.10.10.16
Completed SYN Stealth Scan at 13:30, 4.41s elapsed (1000 total ports)
Nmap scan report for 10.10.10.16
Host is up (0.00062s latency).
Not shown: 983 filtered ports
PORT STATE SERVICE
53/tcp open domain
80/tcp open http
88/tcp open kerberos-sec
135/tcp open msrpc
139/tcp open netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldapssl
1801/tcp open msmq
2103/tcp open zephyr-clt
2105/tcp open eklogin
2107/tcp open msmq-mgmt
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
3389/tcp open ms-wbt-server
MAC Address: 00:0C:29:47:86:30 (VMware)
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 4.78 seconds
Raw packets sent: 1984 (87.280KB) | Rcvd: 18 (776B)
Filter Hosts
Type here to search
1:30 PM
9/16/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
ParrosV
Kali V
UbuntuV
Android
V2016
V2019
V2010
Home
V2010
V2016
Zenmap
Scan Tools Profile Help
Target: 10.10.10.16
Profile:
Scan
Cancel
Command: nmap -sS -v 10.10.10.16
Hosts
Services
OS Host
10.10.10.16
Nmap Output Ports / Hosts Topology Host Details Scans
Port Protocol State Service Version
53 tcp open domain
80 tcp open http
88 tcp open kerberos-sec
135 tcp open msrpc
139 tcp open netbios-ssn
389 tcp open ldap
445 tcp open microsoft-ds
464 tcp open kpasswd5
593 tcp open http-rpc-epmap
636 tcp open ldapssl
1801 tcp open msmq
2103 tcp open zephyr-clt
2105 tcp open eklogin
2107 tcp open msmq-mgmt
3268 tcp open globalcatLDAP
3269 tcp open globalcatLDAPssl
3389 tcp open ms-wbt-server
Filter Hosts
Type here to search
1:31 PM
9/16/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

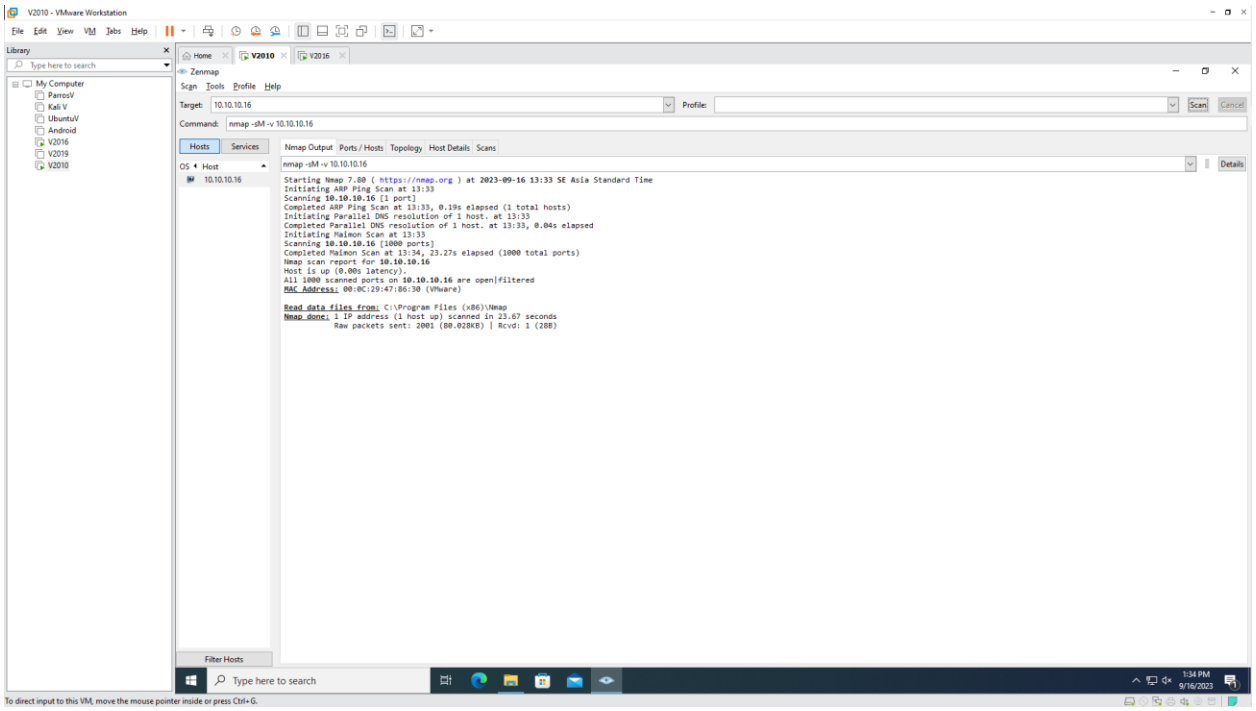

V2010 - VMware Workstation
Zenmap
Target: 10.10.10.16
Command: nmap -sS -v 10.10.10.16
Profile:
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
10.10.10.16
localhost
Host Status
State: up
Open ports: 17
Filtered ports: 983
Closed ports: 0
Scanned ports: 1000
Up time: Not available
Last boot: Not available
Addresses
IPv4: 10.10.10.16
IPv6: Not available
MAC: 00:0C:29:47:86:30
Comments
Filter Hosts
Type here to search
1:31 PM
9/16/2023



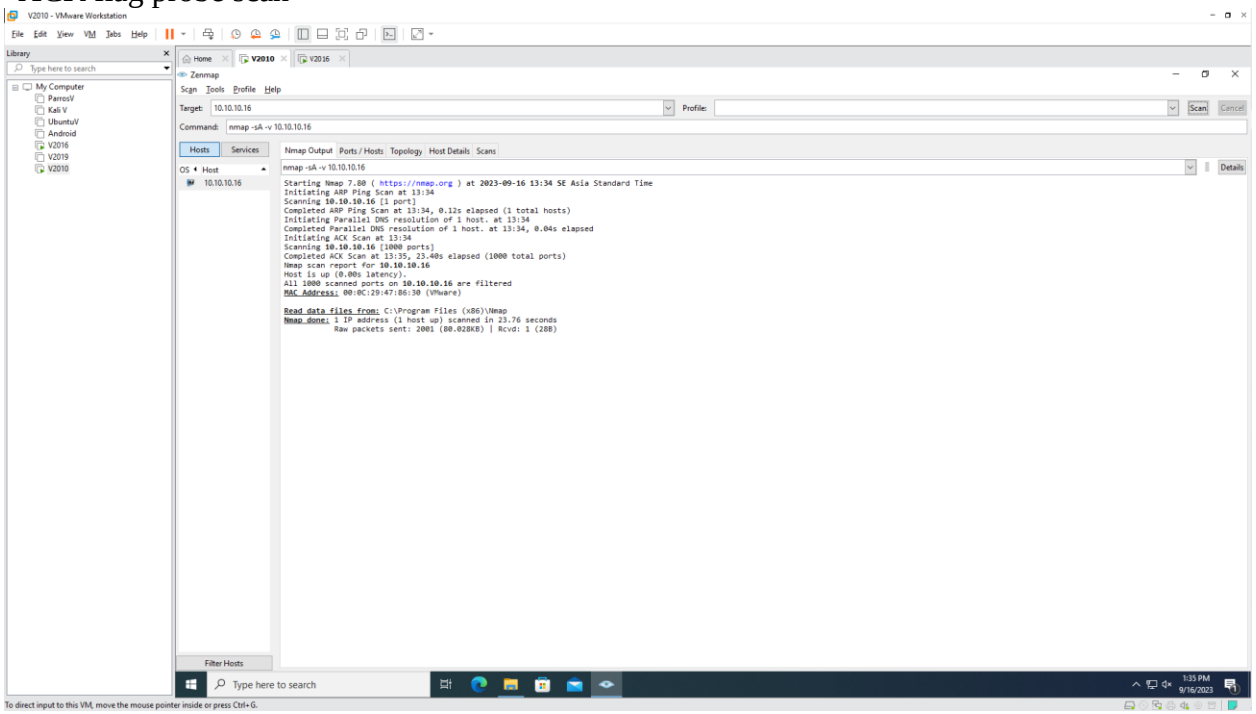
- Xmas Scan



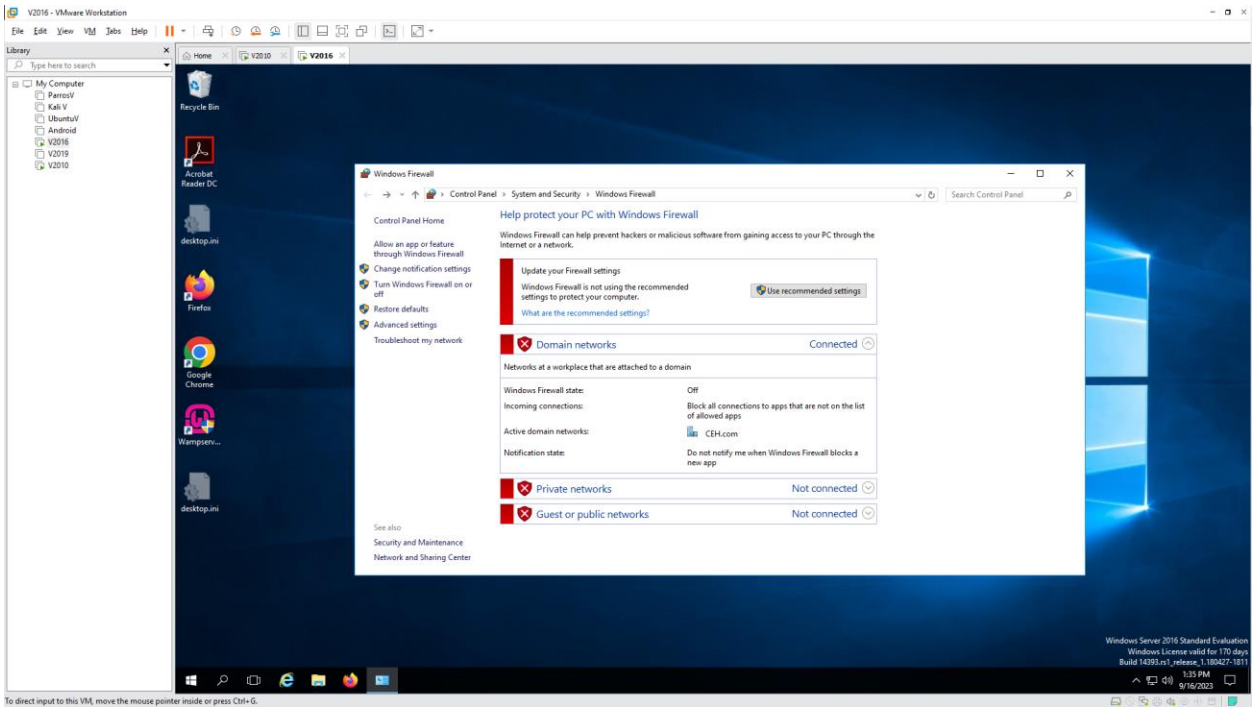
- Maimon scan



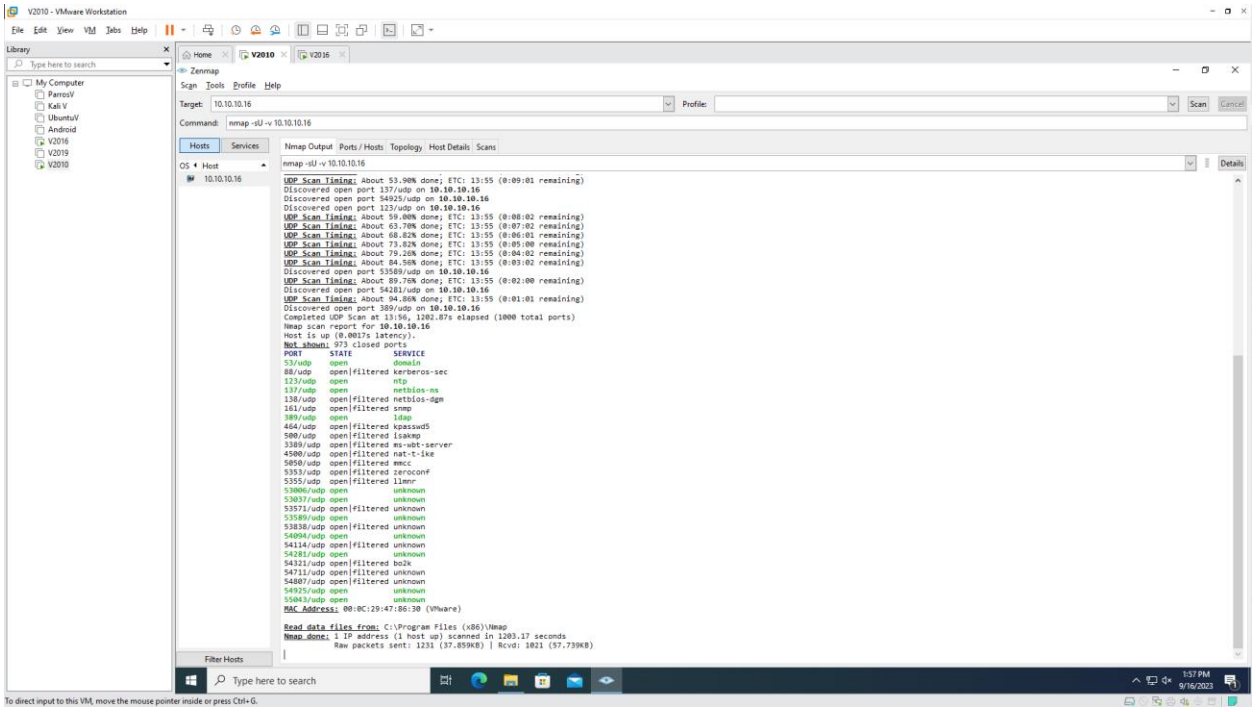
- ACK flag probe scan



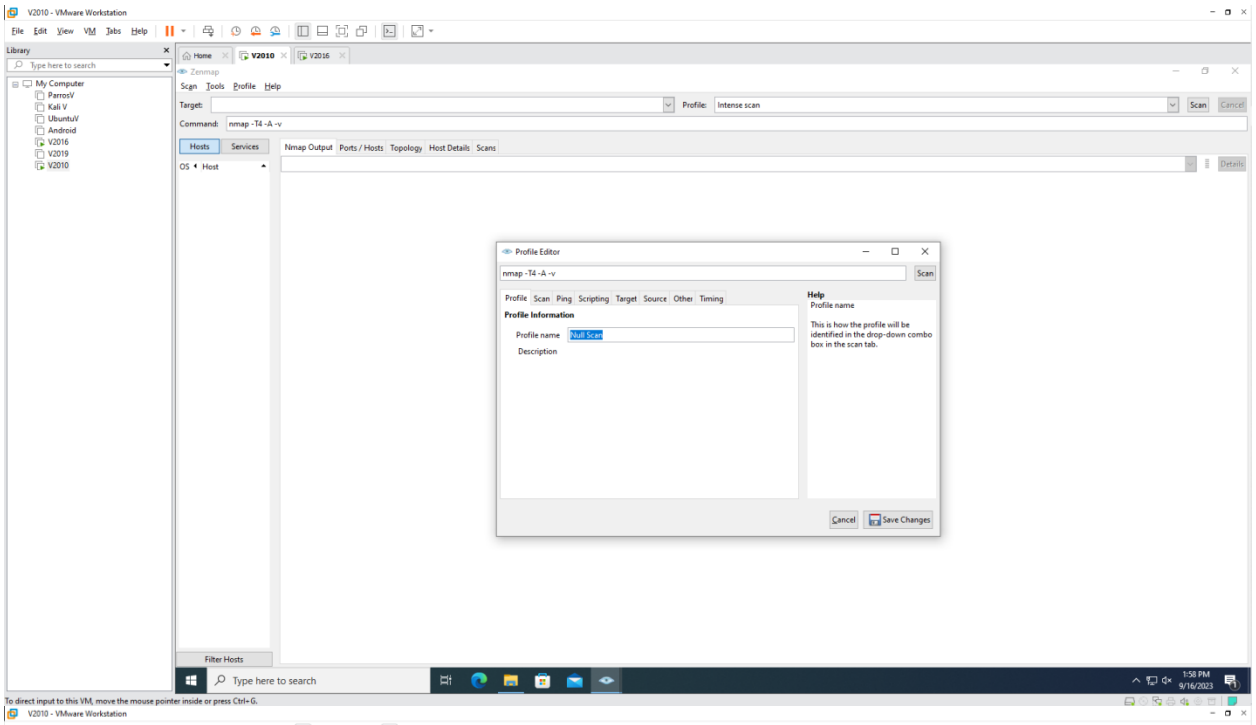
- Turn off firewall

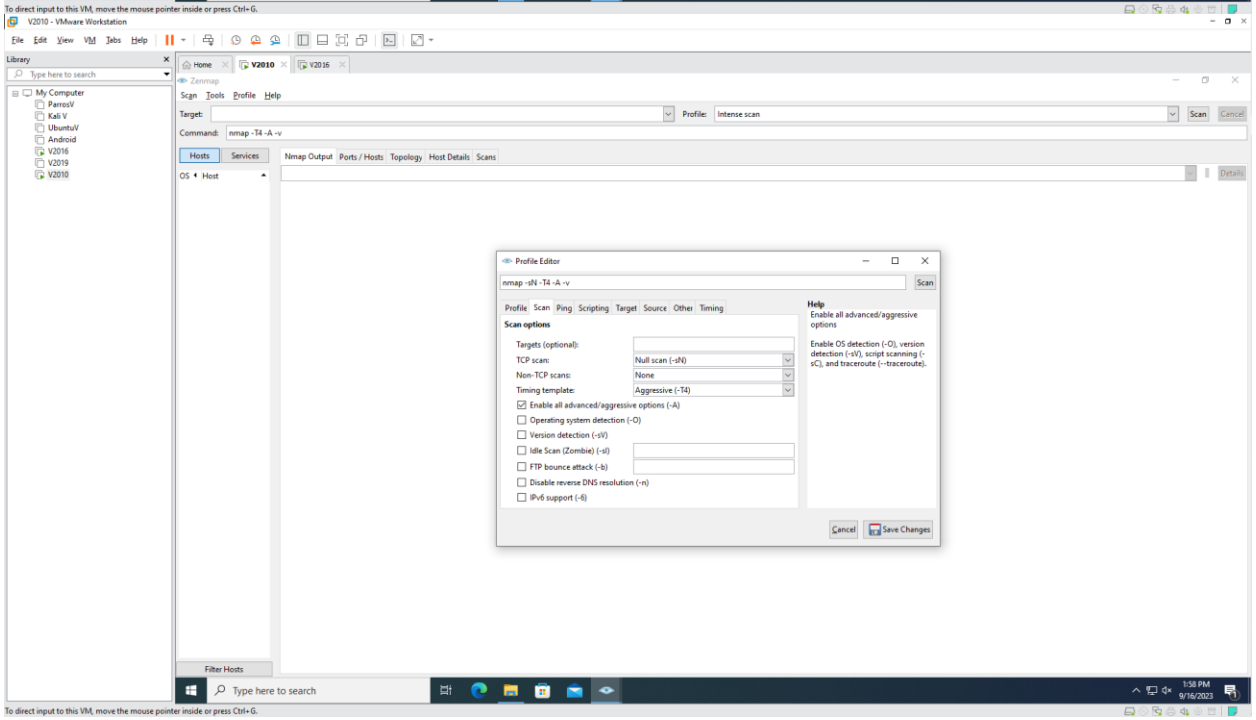


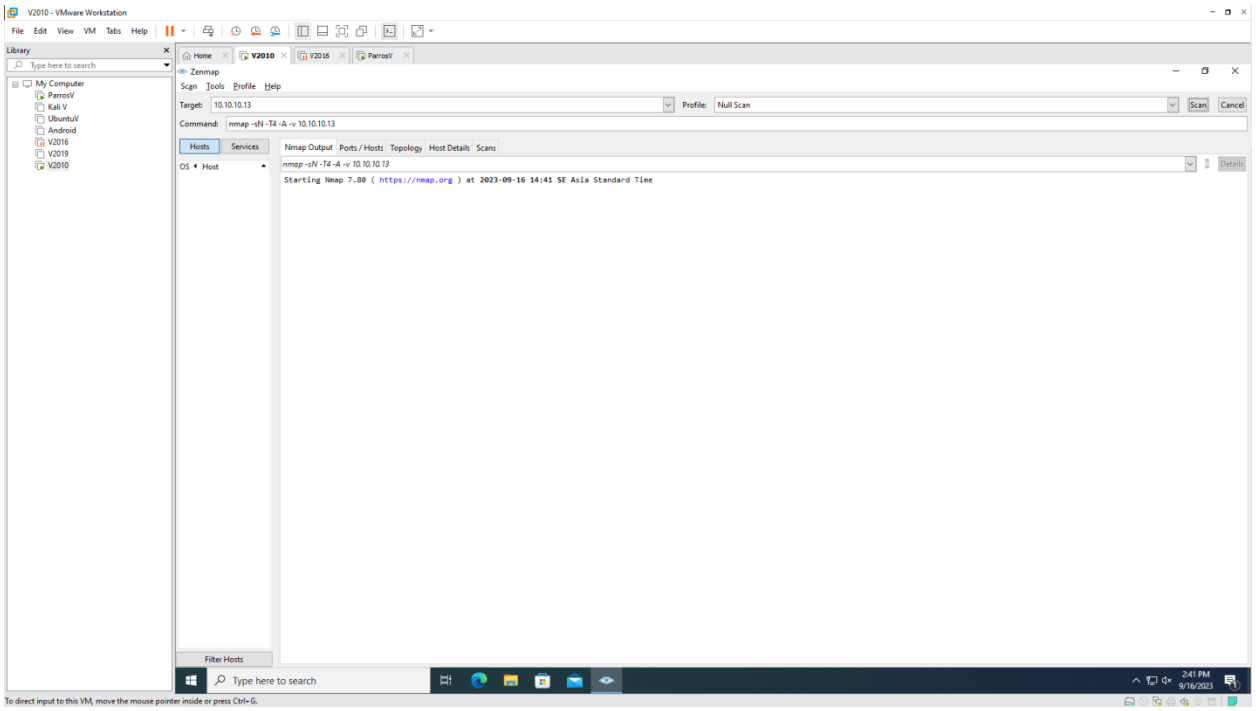
- UDP scan



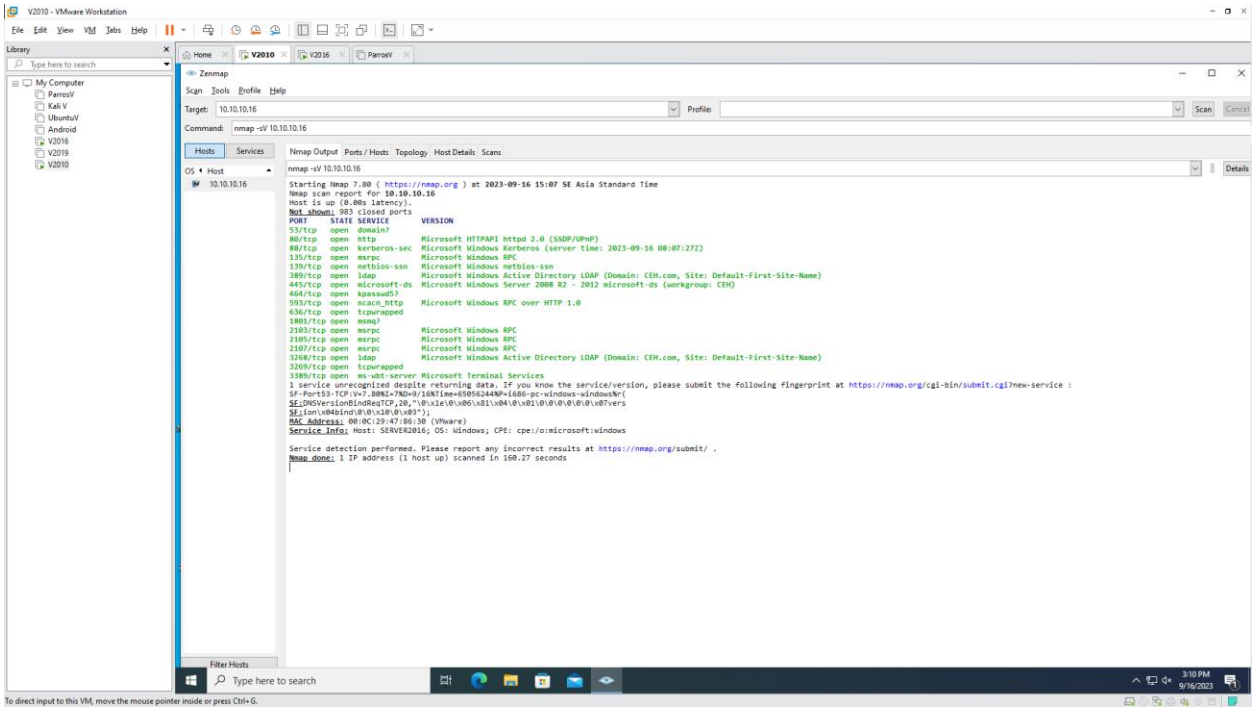
- Null Scan


V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
ParrosV
Kali V
UbuntuV
Android
V2016
V2019
V2010
Home
V2010
V2016
Zenmap
Scan Tools Profile Help
Target:
Profile:
Intense scan
Scan
Cancel
Command:
nmap -T4 -A -v
Hosts
Services
OS Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
Filter Hosts
Profile Editor
nmap -T4 -A -v
Scan
Profile Scan Ping Scripting Target Source Other Timing
Profile Information
Profile name
Null Scan
Description
Help
Profile name
This is how the profile will be identified in the drop-down combo box in the scan tab.
Cancel
Save Changes
Type here to search
1:58 PM
9/16/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

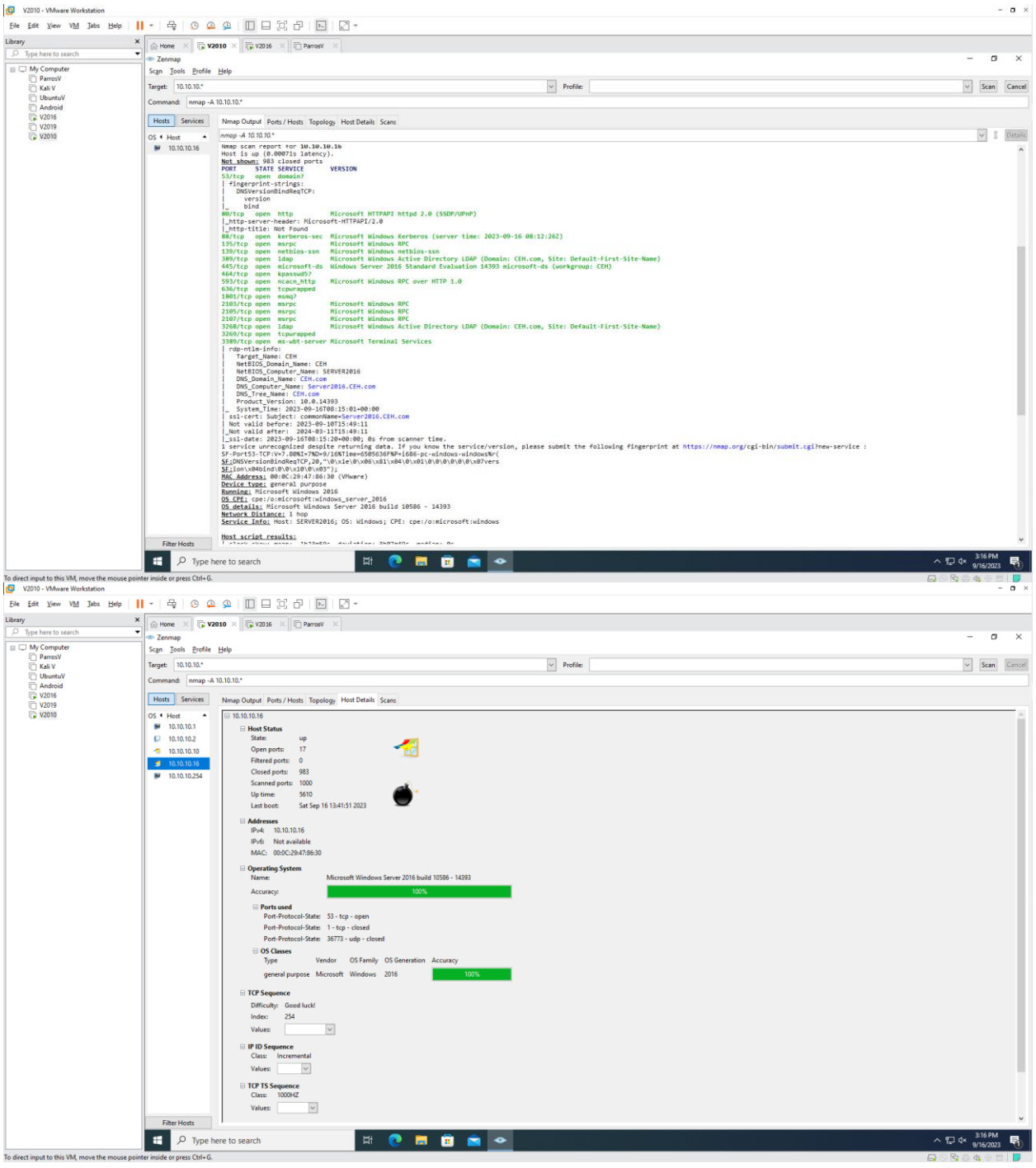

V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
ParrosV
Kali V
UbuntuV
Android
V2016
V2019
V2010
Home
V2010
V2016
Zenmap
Scan Tools Profile Help
Target:
Profile:
Intense scan
Scan
Cancel
Command:
nmap -T4 -A -v
Hosts
Services
OS Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
Filter Hosts
Profile Editor
nmap -sN -T4 -A -v
Scan
Profile Scan Ping Scripting Target Source Other Timing
Scan options
Targets (optional):
TCP scan:
Null scan (-sN)
Non-TCP scans:
None
Timing template:
Aggressive (-T4)
Enable all advanced/aggressive options (-A)
Operating system detection (-O)
Version detection (-sV)
Idle Scan (Zombie) (-sI)
FTP bounce attack (-b)
Disable reverse DNS resolution (-n)
IPv6 support (-6)
Help
Enable all advanced/aggressive options
Enable OS detection (-O), version detection (-sV), script scanning (-sC), and traceroute (--traceroute).
Cancel
Save Changes
Type here to search
1:58 PM
9/16/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



- detects service version



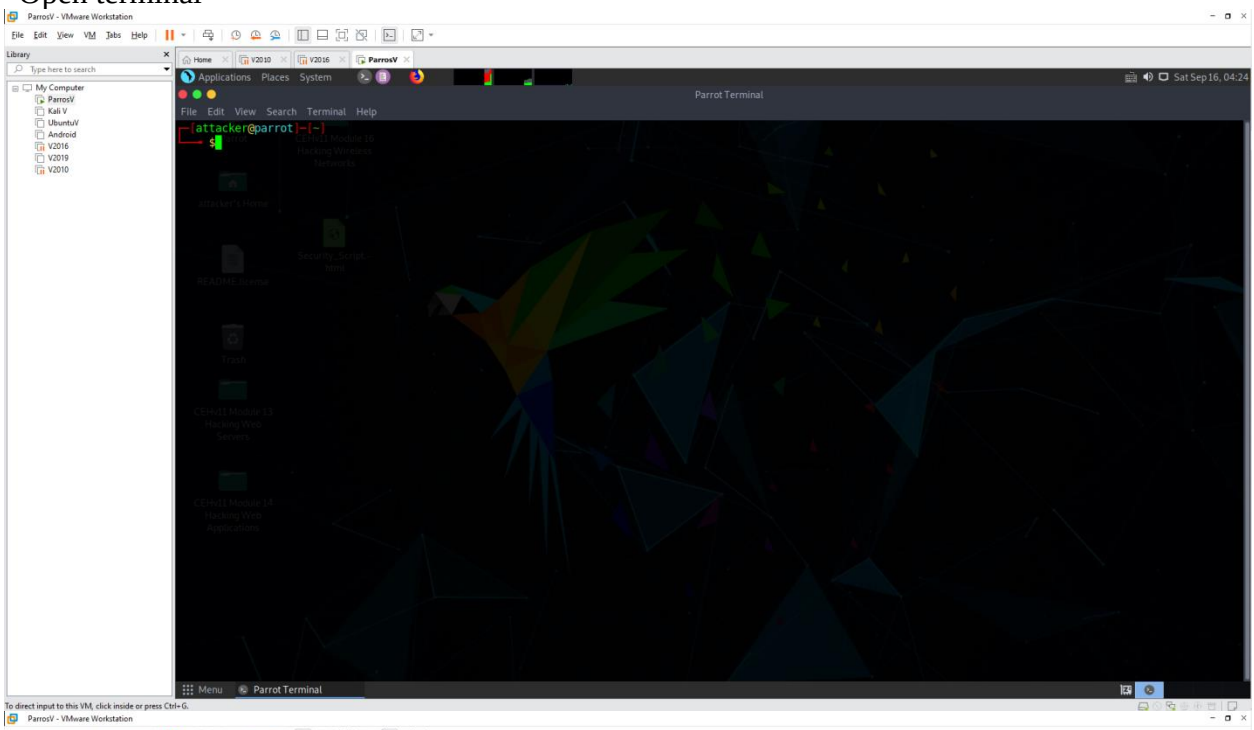
- enable aggressive scan

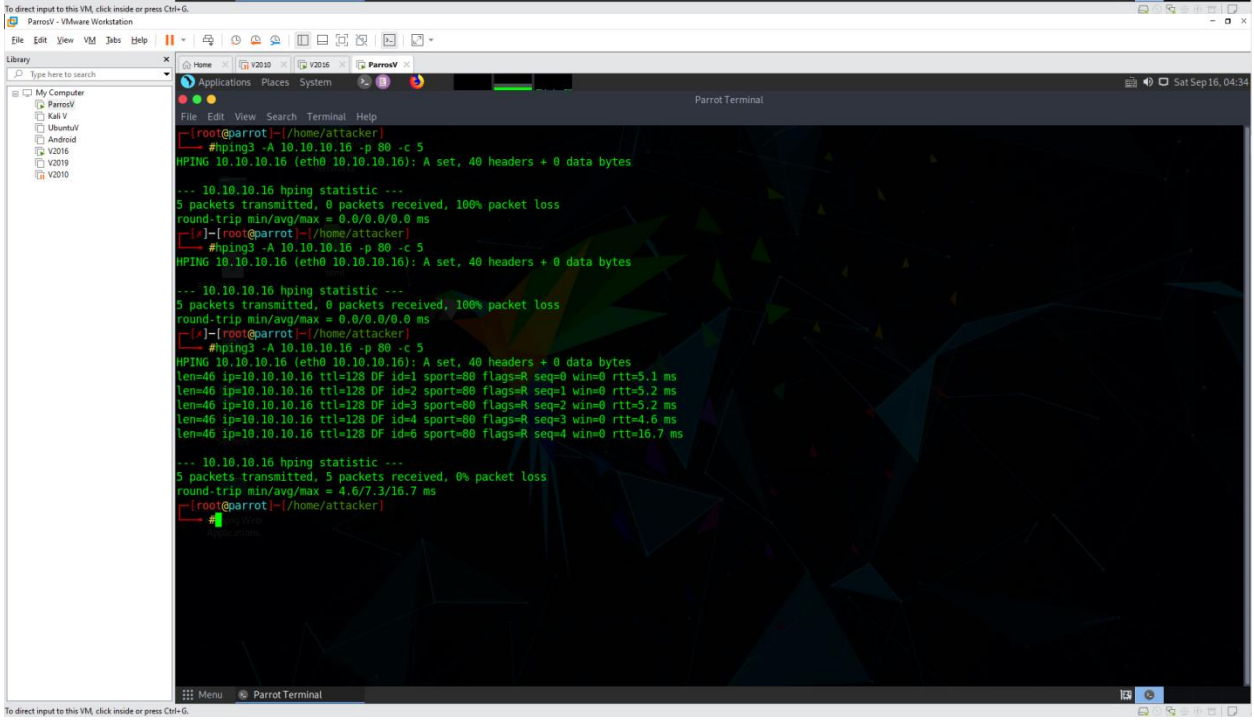


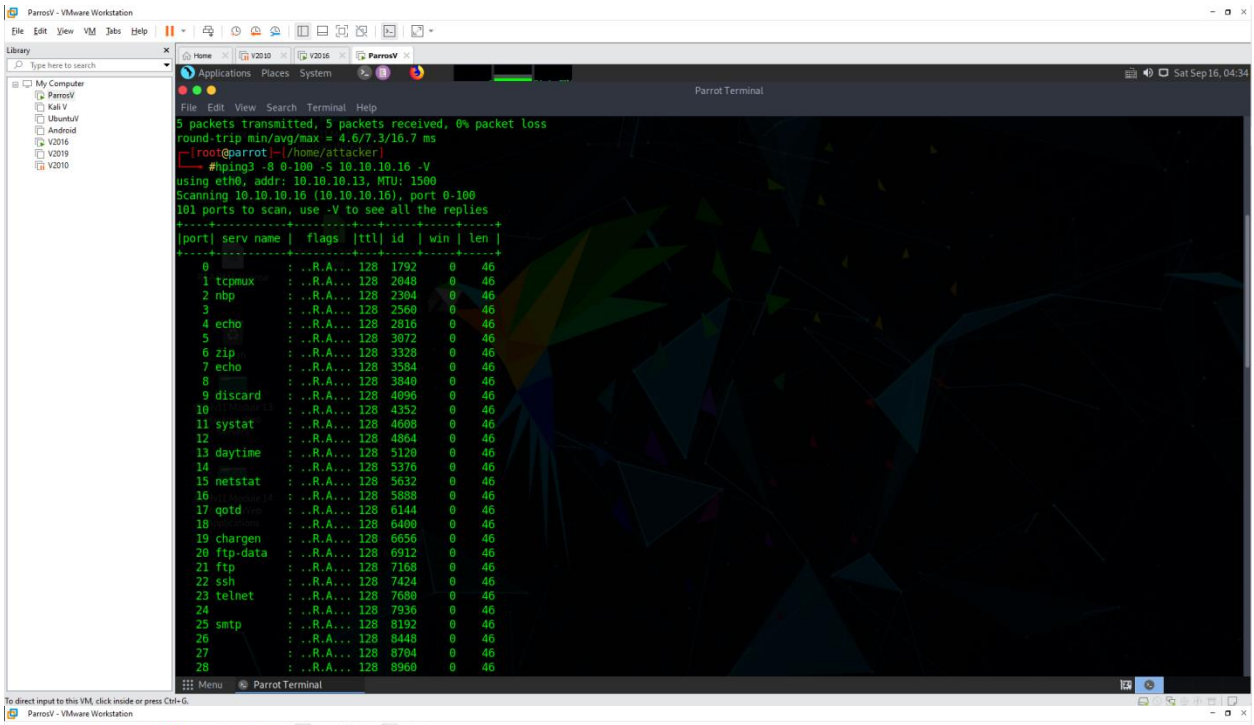
2.4 Explore Various Network Scanning Techniques using Hping3

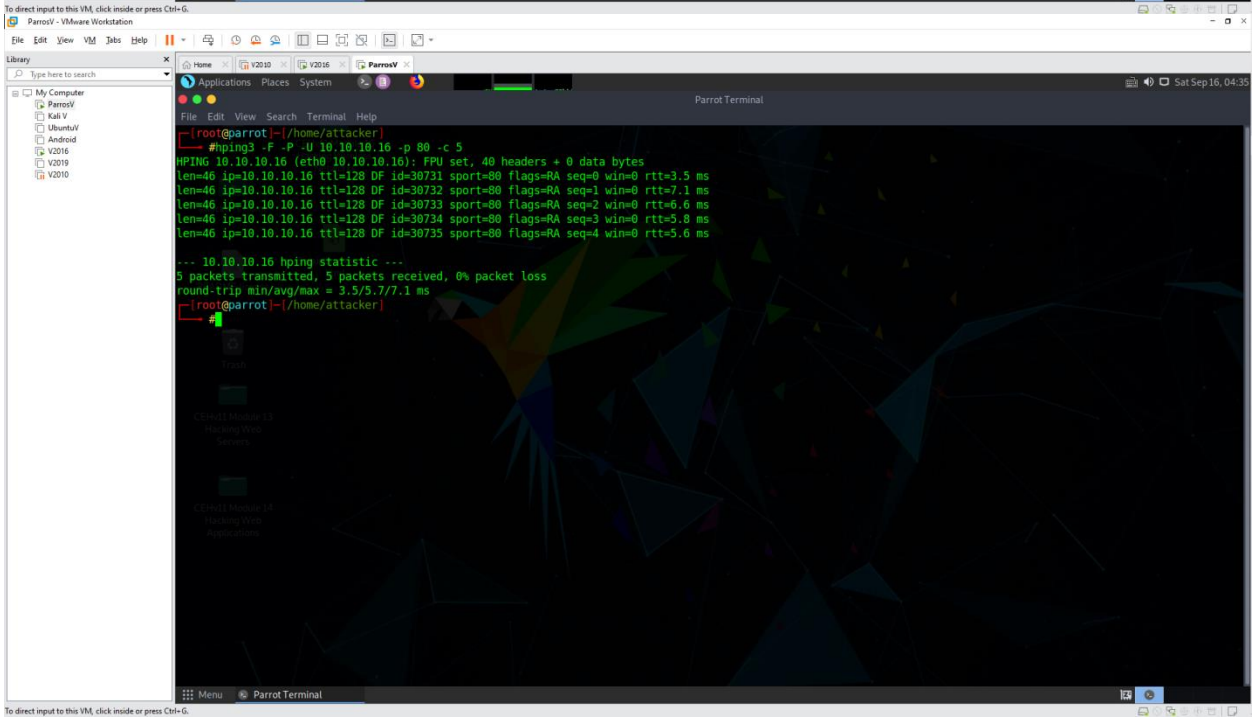
- Open Parrot

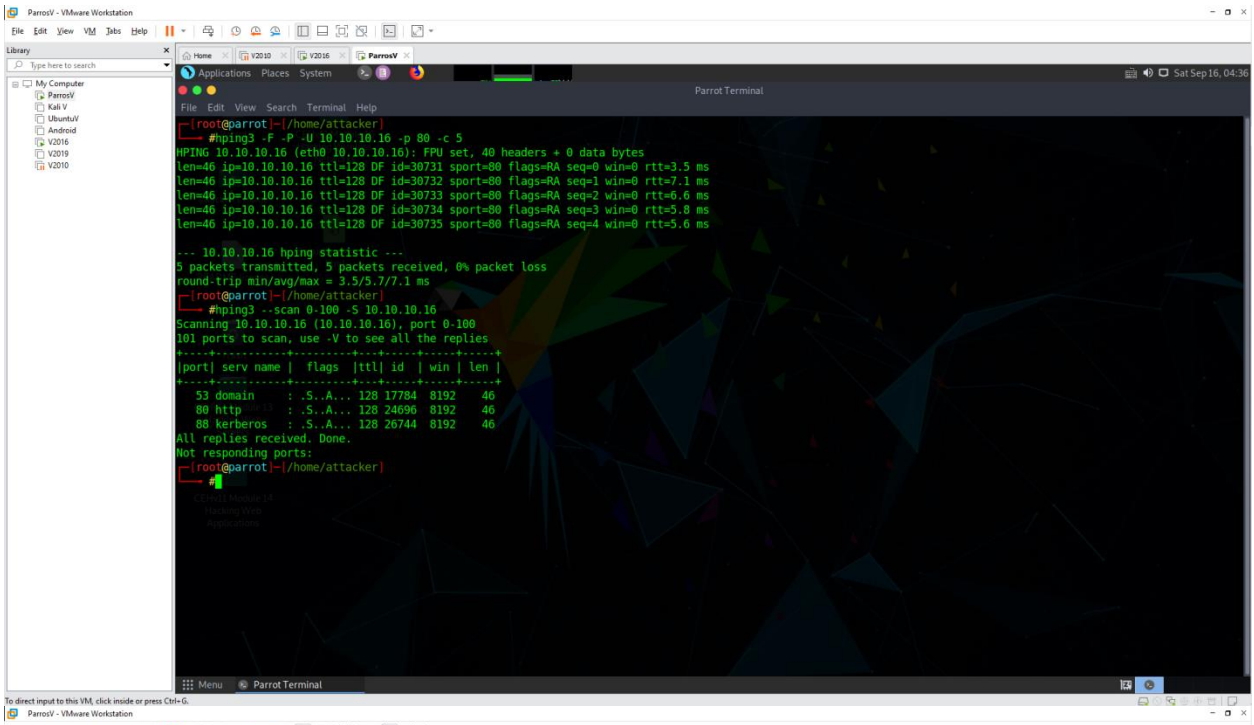
- Open terminal

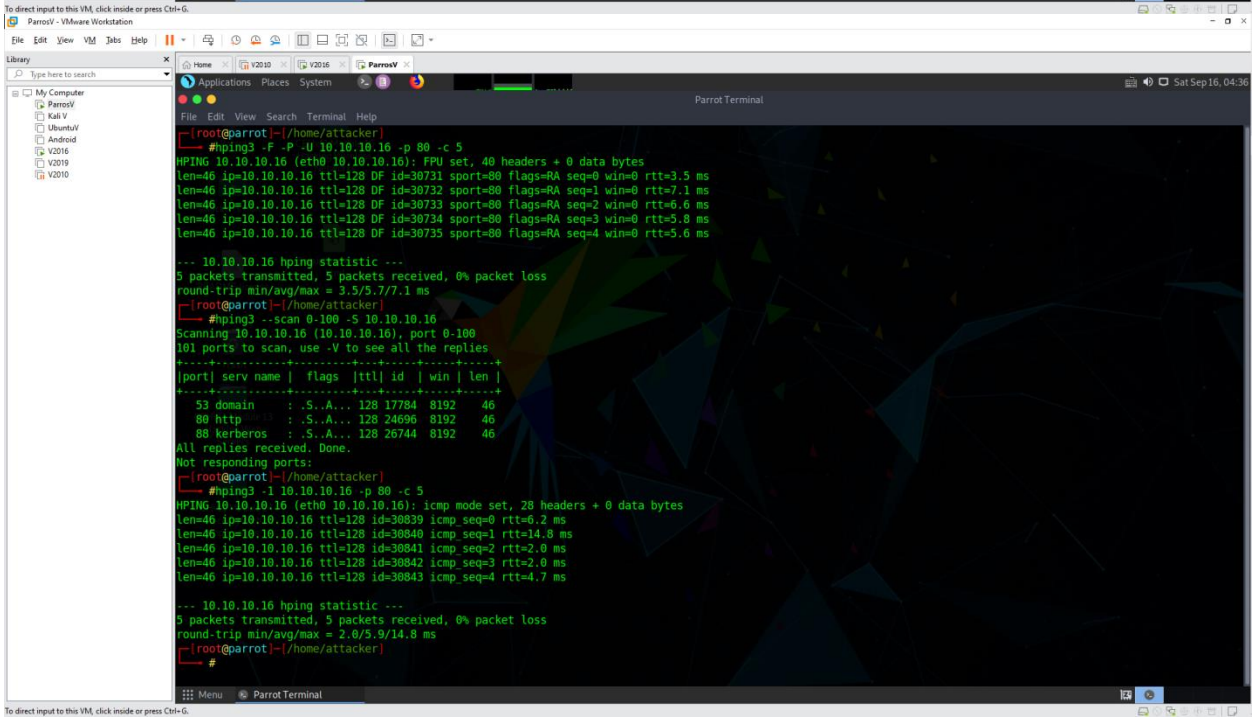





ParrosV - VMware Workstation
Parrot Terminal
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 4.6/7.3/16.7 ms
#hping3 -8 0-100 -S 10.10.10.16 -V
using eth0, addr: 10.10.10.13, MTU: 1500
Scanning 10.10.10.16 (10.10.10.16), port 0-100
101 ports to scan, use -V to see all the replies
|port| serv name | flags |ttl| id | win | len |
0 : ..R.A... 128 1792 0 46
1 tcpmux : ..R.A... 128 2048 0 46
2 nbp : ..R.A... 128 2304 0 46
3 : ..R.A... 128 2560 0 46
4 echo : ..R.A... 128 2816 0 46
5 : ..R.A... 128 3072 0 46
6 zip : ..R.A... 128 3328 0 46
7 echo : ..R.A... 128 3584 0 46
8 : ..R.A... 128 3840 0 46
9 discard : ..R.A... 128 4096 0 46
10 : ..R.A... 128 4352 0 46
11 systat : ..R.A... 128 4608 0 46
12 : ..R.A... 128 4864 0 46
13 daytime : ..R.A... 128 5120 0 46
14 : ..R.A... 128 5376 0 46
15 netstat : ..R.A... 128 5632 0 46
16 : ..R.A... 128 5888 0 46
17 qotd : ..R.A... 128 6144 0 46
18 : ..R.A... 128 6400 0 46
19 chargen : ..R.A... 128 6656 0 46
20 ftp-data : ..R.A... 128 6912 0 46
21 ftp : ..R.A... 128 7168 0 46
22 ssh : ..R.A... 128 7424 0 46
23 telnet : ..R.A... 128 7680 0 46
24 : ..R.A... 128 7936 0 46
25 smtp : ..R.A... 128 8192 0 46
26 : ..R.A... 128 8448 0 46
27 : ..R.A... 128 8704 0 46
28 : ..R.A... 128 8960 0 46


ParrosV - VMware Workstation
Parrot Terminal
#hping3 -F -P -U 10.10.10.16 -p 80 -c 5
HPING 10.10.10.16 (eth0 10.10.10.16): FPU set, 40 headers + 0 data bytes
len=46 ip=10.10.10.16 ttl=128 DF id=30731 sport=80 flags=RA seq=0 win=0 rtt=3.5 ms
len=46 ip=10.10.10.16 ttl=128 DF id=30732 sport=80 flags=RA seq=1 win=0 rtt=7.1 ms
len=46 ip=10.10.10.16 ttl=128 DF id=30733 sport=80 flags=RA seq=2 win=0 rtt=6.6 ms
len=46 ip=10.10.10.16 ttl=128 DF id=30734 sport=80 flags=RA seq=3 win=0 rtt=5.8 ms
len=46 ip=10.10.10.16 ttl=128 DF id=30735 sport=80 flags=RA seq=4 win=0 rtt=5.6 ms
--- 10.10.10.16 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.5/5.7/7.1 ms


ParrosV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
ParrosV
Kali V
UbuntuV
Android
V2016
V2019
V2010
Home
V2010
V2016
ParrosV
Applications Places System
Sat Sep 16, 04:36
Parrot Terminal
File Edit View Search Terminal Help
┌─[root@parrot]─[/home/attacker]
└──╼ #hping3 -F -P -U 10.10.10.16 -p 80 -c 5
HPING 10.10.10.16 (eth0 10.10.10.16): FPU set, 40 headers + 0 data bytes
len=46 ip=10.10.10.16 ttl=128 DF id=30731 sport=80 flags=RA seq=0 win=0 rtt=3.5 ms
len=46 ip=10.10.10.16 ttl=128 DF id=30732 sport=80 flags=RA seq=1 win=0 rtt=7.1 ms
len=46 ip=10.10.10.16 ttl=128 DF id=30733 sport=80 flags=RA seq=2 win=0 rtt=6.6 ms
len=46 ip=10.10.10.16 ttl=128 DF id=30734 sport=80 flags=RA seq=3 win=0 rtt=5.8 ms
len=46 ip=10.10.10.16 ttl=128 DF id=30735 sport=80 flags=RA seq=4 win=0 rtt=5.6 ms
--- 10.10.10.16 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.5/5.7/7.1 ms
┌─[root@parrot]─[/home/attacker]
└──╼ #hping3 --scan 0-100 -S 10.10.10.16
Scanning 10.10.10.16 (10.10.10.16), port 0-100
101 ports to scan, use -V to see all the replies
|port| serv name | flags |ttl| id | win | len |
53 domain : .S..A... 128 17784 8192 46
80 http : .S..A... 128 24696 8192 46
88 kerberos : .S..A... 128 26744 8192 46
All replies received. Done.
Not responding ports:
┌─[root@parrot]─[/home/attacker]
└──╼ #
Menu
Parrot Terminal
To direct input to this VM, click inside or press Ctrl+G.


ParrosV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
ParrosV
Kali V
UbuntuV
Android
V2016
V2019
V2010
Home
V2010
V2016
ParrosV
Applications Places System
Sat Sep 16, 04:36
Parrot Terminal
File Edit View Search Terminal Help
┌─[root@parrot]─[/home/attacker]
└──╼ #hping3 -F -P -U 10.10.10.16 -p 80 -c 5
HPING 10.10.10.16 (eth0 10.10.10.16): FPU set, 40 headers + 0 data bytes
len=46 ip=10.10.10.16 ttl=128 DF id=30731 sport=80 flags=RA seq=0 win=0 rtt=3.5 ms
len=46 ip=10.10.10.16 ttl=128 DF id=30732 sport=80 flags=RA seq=1 win=0 rtt=7.1 ms
len=46 ip=10.10.10.16 ttl=128 DF id=30733 sport=80 flags=RA seq=2 win=0 rtt=6.6 ms
len=46 ip=10.10.10.16 ttl=128 DF id=30734 sport=80 flags=RA seq=3 win=0 rtt=5.8 ms
len=46 ip=10.10.10.16 ttl=128 DF id=30735 sport=80 flags=RA seq=4 win=0 rtt=5.6 ms
--- 10.10.10.16 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.5/5.7/7.1 ms
┌─[root@parrot]─[/home/attacker]
└──╼ #hping3 --scan 0-100 -S 10.10.10.16
Scanning 10.10.10.16 (10.10.10.16), port 0-100
101 ports to scan, use -V to see all the replies
|port| serv name | flags |ttl| id | win | len |
53 domain : .S..A... 128 17784 8192 46
80 http : .S..A... 128 24696 8192 46
88 kerberos : .S..A... 128 26744 8192 46
All replies received. Done.
Not responding ports:
┌─[root@parrot]─[/home/attacker]
└──╼ #hping3 -1 10.10.10.16 -p 80 -c 5
HPING 10.10.10.16 (eth0 10.10.10.16): icmp mode set, 28 headers + 0 data bytes
len=46 ip=10.10.10.16 ttl=128 id=30839 icmp_seq=0 rtt=6.2 ms
len=46 ip=10.10.10.16 ttl=128 id=30840 icmp_seq=1 rtt=14.8 ms
len=46 ip=10.10.10.16 ttl=128 id=30841 icmp_seq=2 rtt=2.0 ms
len=46 ip=10.10.10.16 ttl=128 id=30842 icmp_seq=3 rtt=2.0 ms
len=46 ip=10.10.10.16 ttl=128 id=30843 icmp_seq=4 rtt=4.7 ms
--- 10.10.10.16 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.0/5.9/14.8 ms
┌─[root@parrot]─[/home/attacker]
└──╼ #
Menu
Parrot Terminal
To direct input to this VM, click inside or press Ctrl+G.