Lab #2:

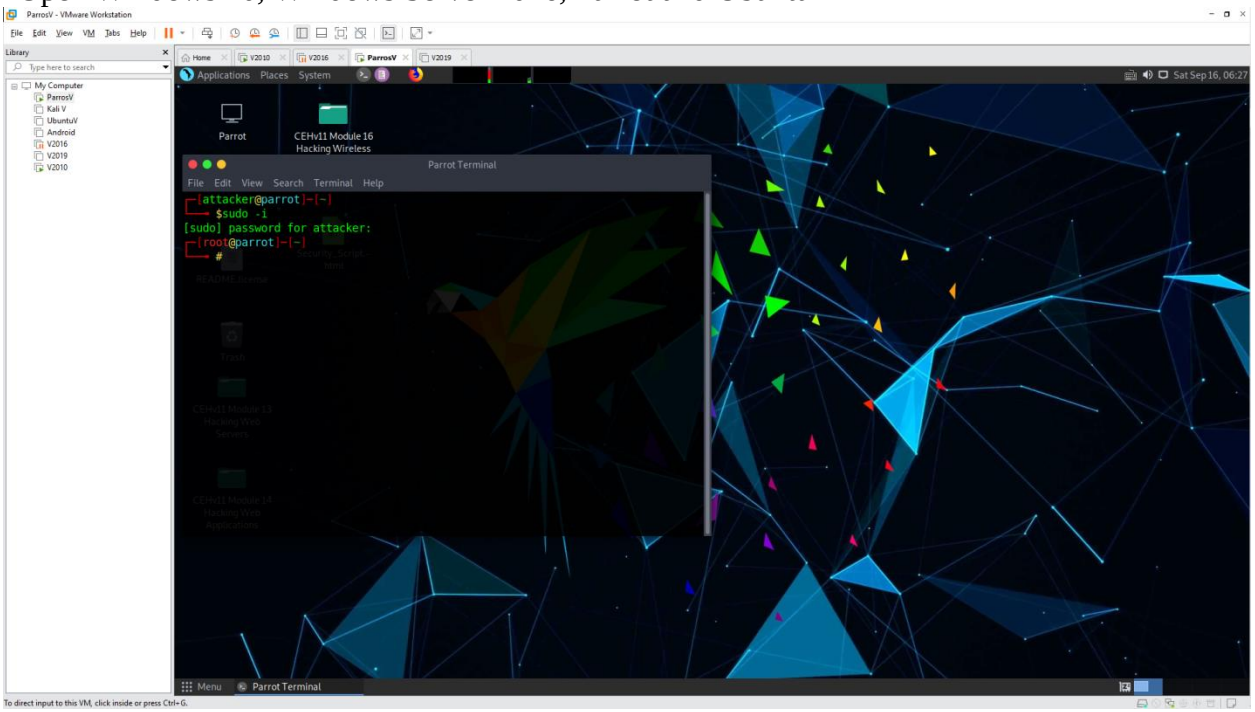
Course Name: Ethical Hacking and Offensive Security (HOD401)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 16/09/2023

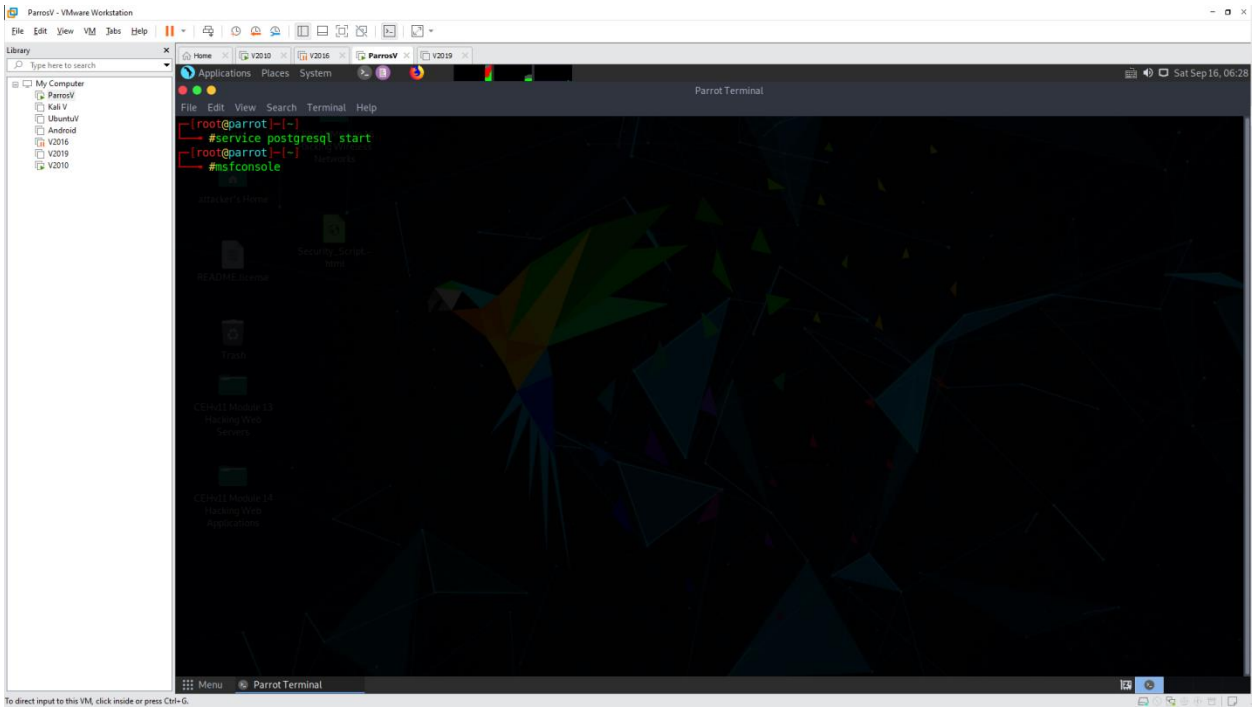
Lab tasks

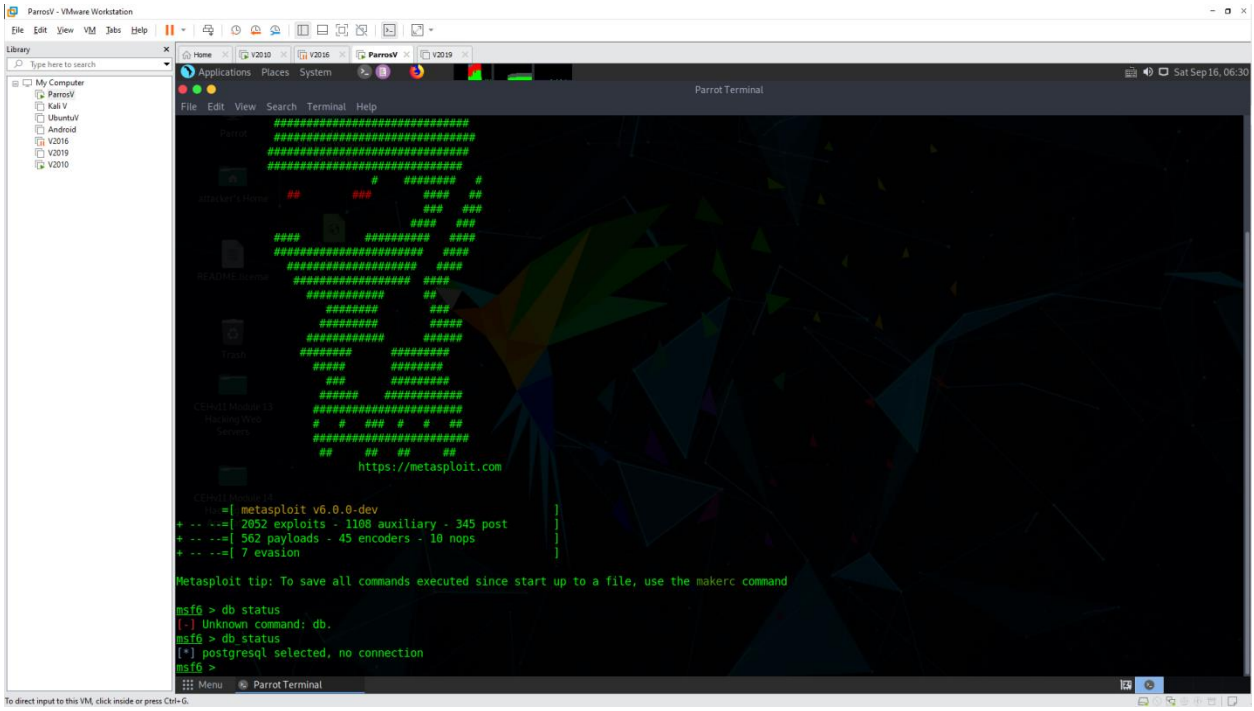
6. Perform Network Scanning using Various Scanning Tools

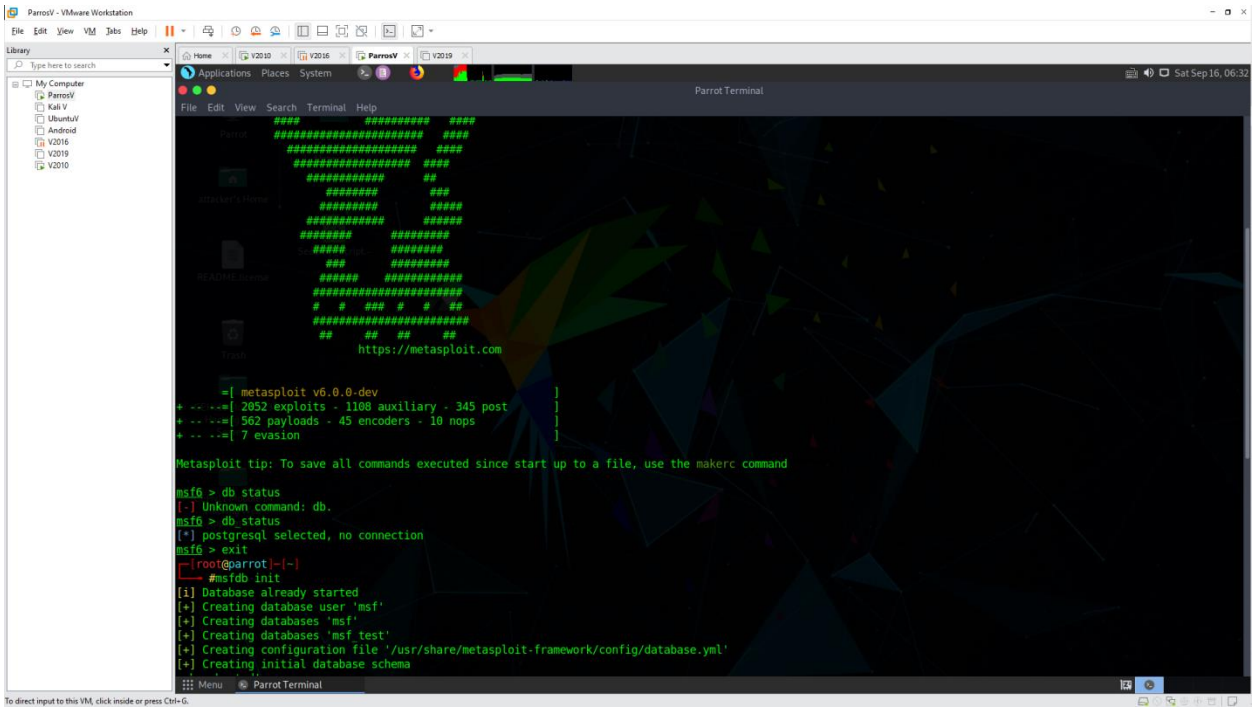
6.1 Scan a Target Network using Metasploit

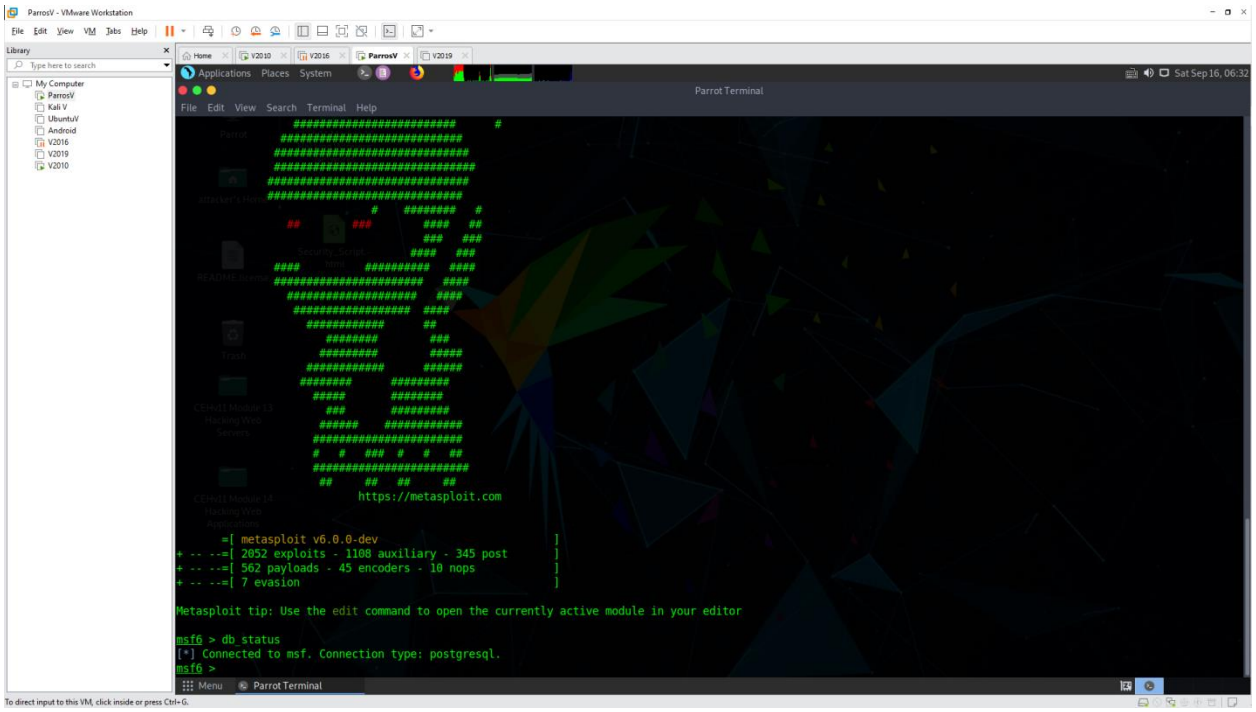
- Open Windows 10, Windows Server 2016, Parrot and Ubuntu

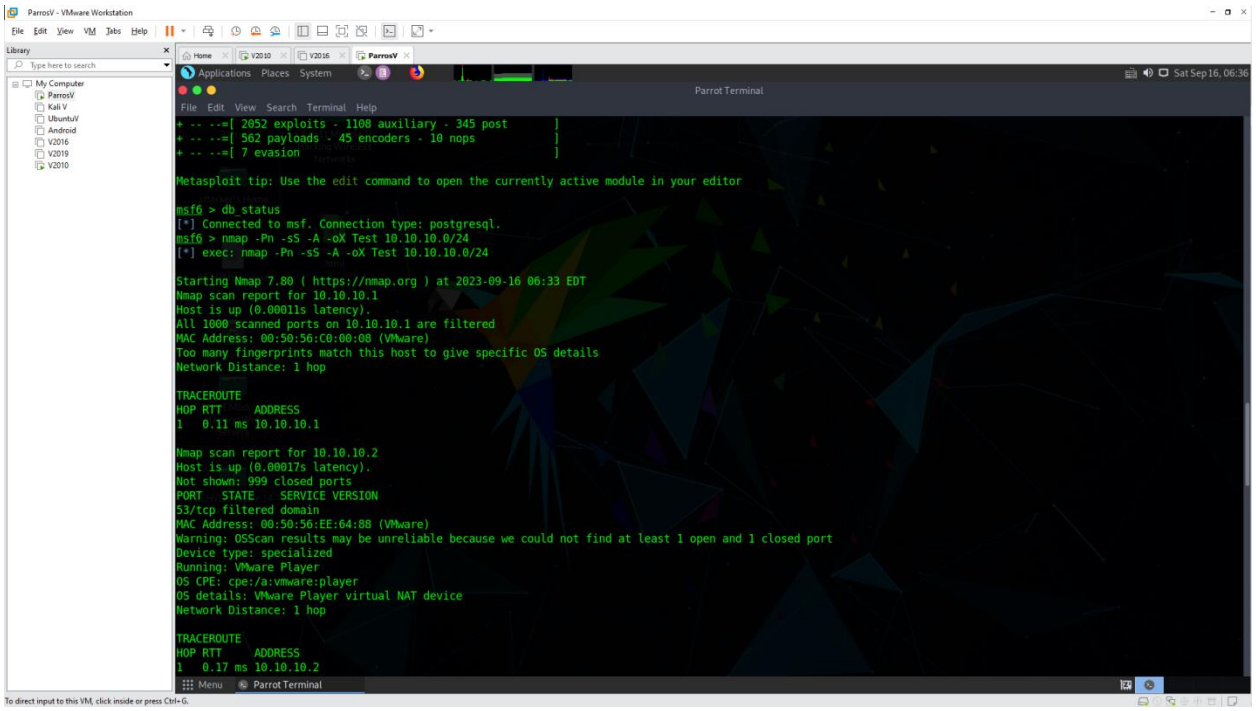


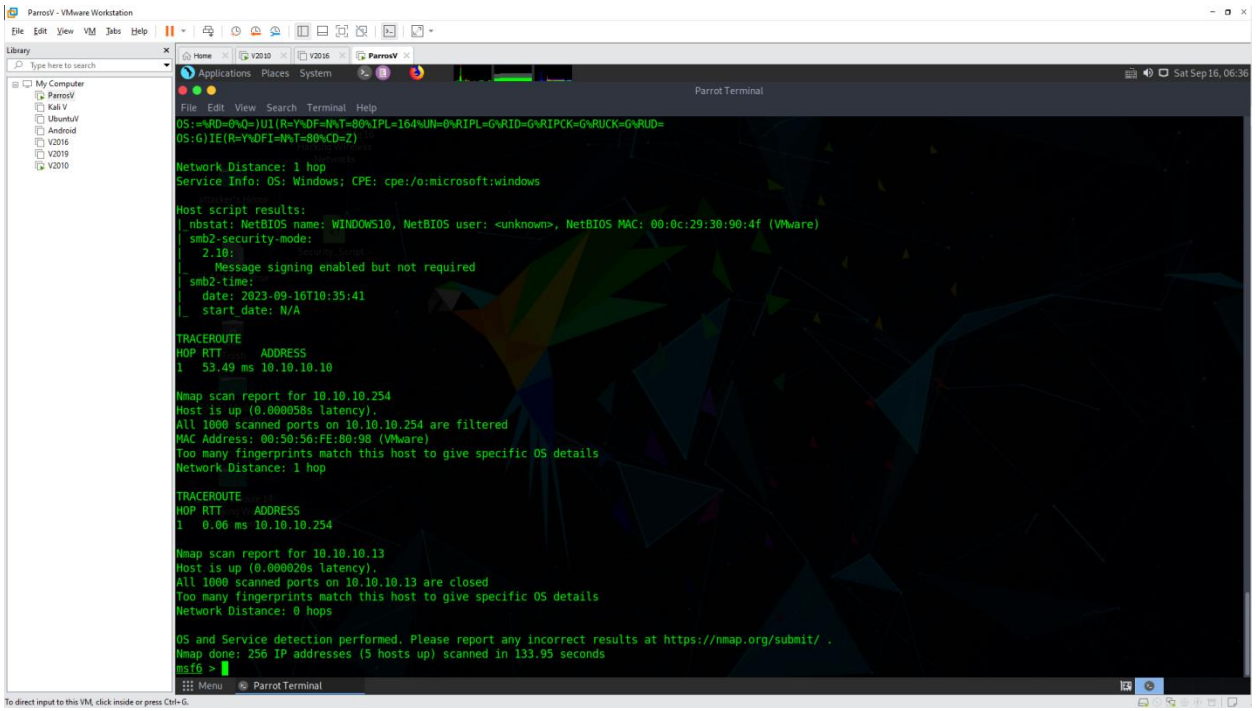

ParrosV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
ParrosV
Kali V
UbuntuV
Android
V2016
V2019
V2010
Home
V2010
V2016
ParrosV
V2019
Applications Places System
Sat Sep 16, 06:28
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#service postgresql start
[root@parrot]-[~]
#msfconsole
Menu
Parrot Terminal
To direct input to this VM, click inside or press Ctrl+G.

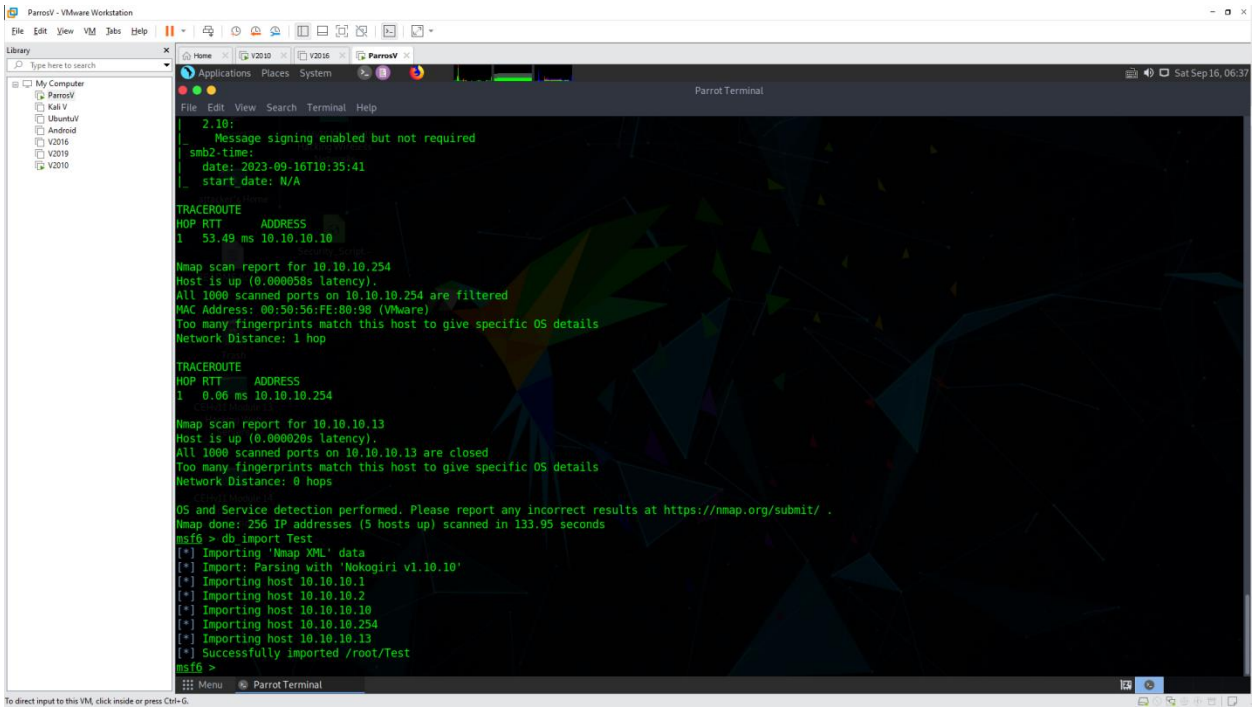

ParrosV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
ParrosV
Kali V
UbuntuV
Android
V2016
V2019
V2010
Home
V2010
V2016
ParrosV
V2019
Applications Places System
Sat Sep 16, 06:30
Parrot Terminal
File Edit View Search Terminal Help
https://metasploit.com
=[metasploit v6.0.0-dev
+ -- --=[2052 exploits - 1108 auxiliary - 345 post
+ -- --=[562 payloads - 45 encoders - 10 nops
+ -- --=[7 evasion
Metasploit tip: To save all commands executed since start up to a file, use the makerc command
msf6 > db_status
[-] Unknown command: db.
msf6 > db_status
[*] postgresql selected, no connection
msf6 >
Menu
Parrot Terminal
To direct input to this VM, click inside or press Ctrl+G.

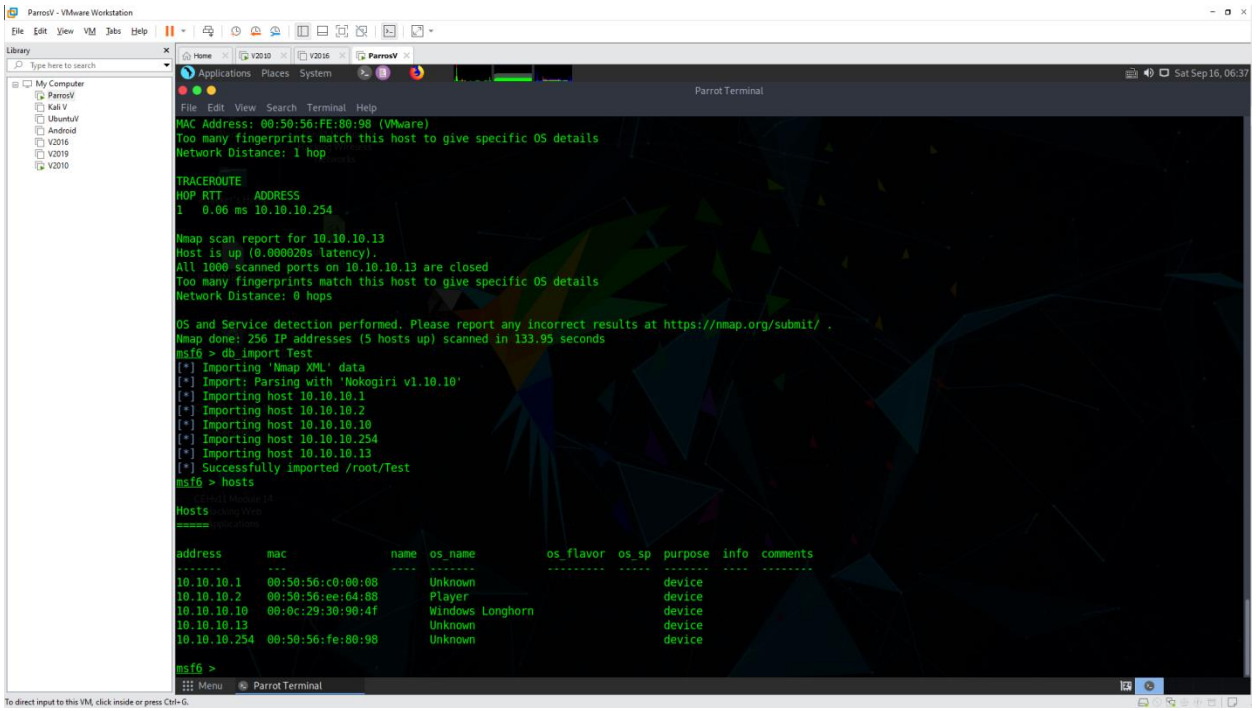

ParrosV - VMware Workstation
Parrot Terminal
Sat Sep 16, 06:32
https://metasploit.com
=[metasploit v6.0.0-dev
+ -- --=[2052 exploits - 1108 auxiliary - 345 post
+ -- --=[562 payloads - 45 encoders - 10 nops
+ -- --=[7 evasion
Metasploit tip: To save all commands executed since start up to a file, use the makerc command
msf6 > db_status
[-] Unknown command: db.
msf6 > db_status
[*] postgresql selected, no connection
msf6 > exit
#msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema

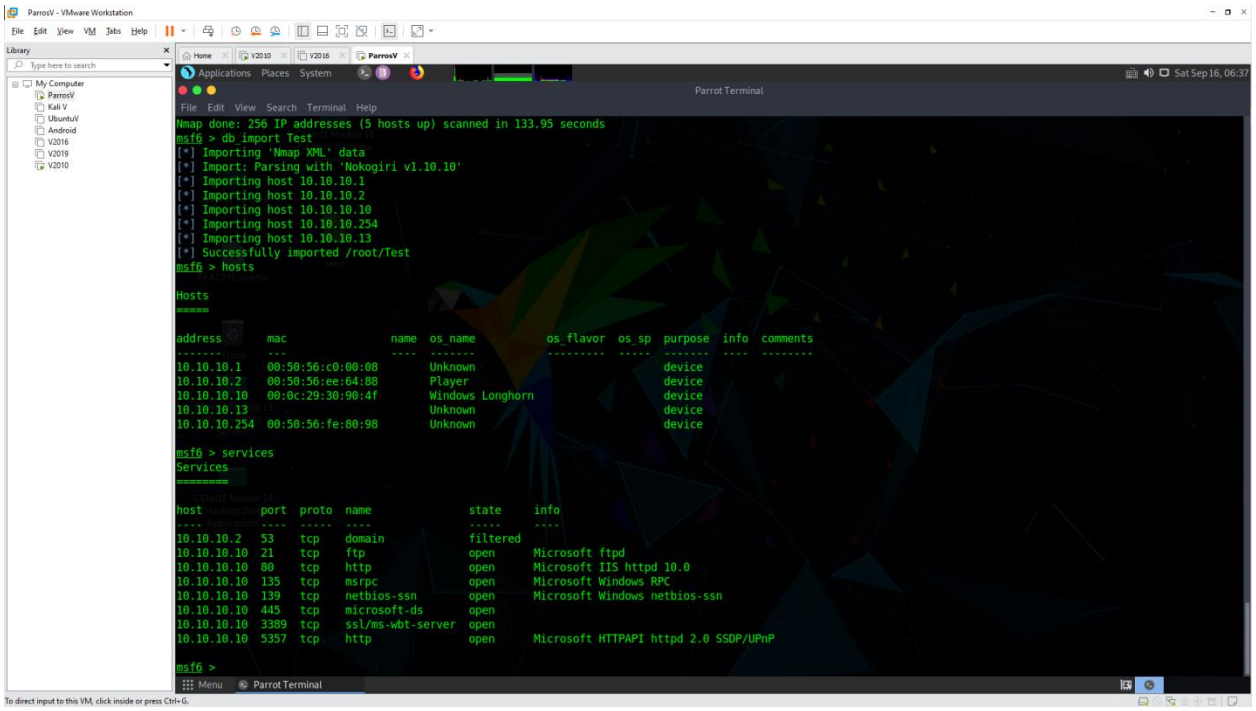

ParrosV - VMware Workstation
Parrot Terminal
Sat Sep 16, 06:32
https://metasploit.com
=[metasploit v6.0.0-dev
+ -- --=[2052 exploits - 1108 auxiliary - 345 post
+ -- --=[562 payloads - 45 encoders - 10 nops
+ -- --=[7 evasion
Metasploit tip: Use the edit command to open the currently active module in your editor
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 >

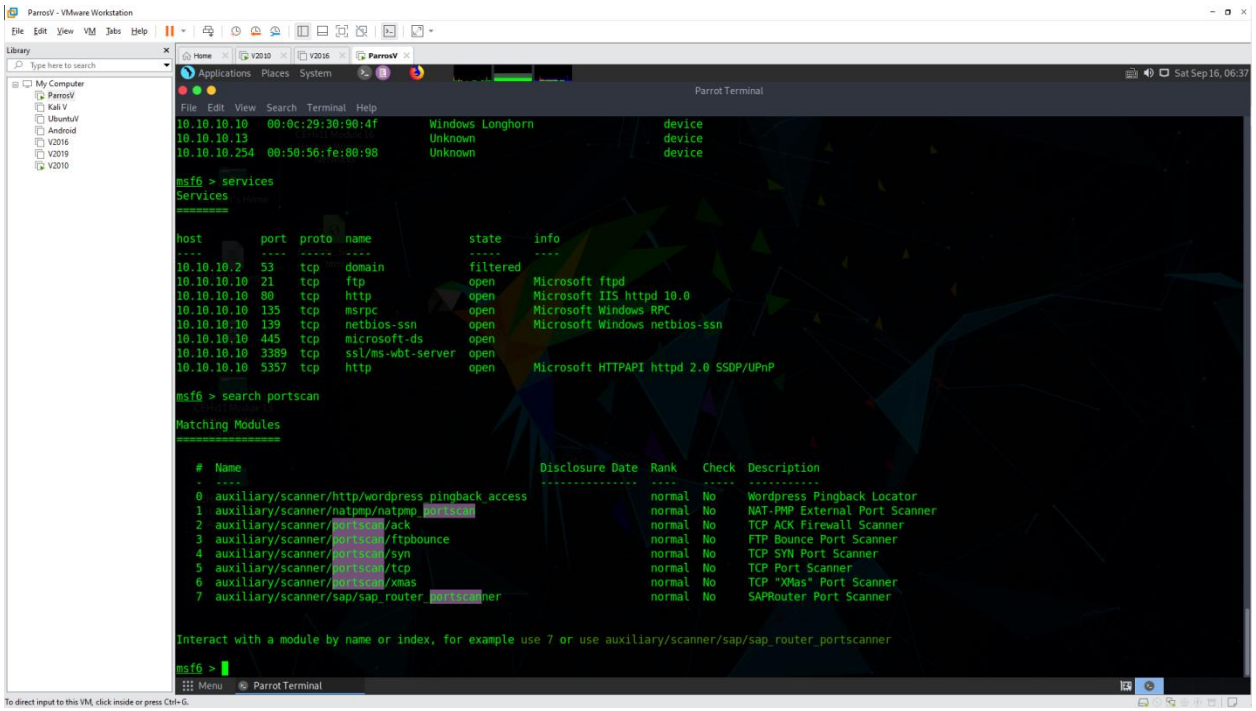

ParrosV - VMware Workstation
Parrot Terminal
+ -- --=[2052 exploits - 1108 auxiliary - 345 post]
+ -- --=[562 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
Metasploit tip: Use the edit command to open the currently active module in your editor
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > nmap -Pn -sS -A -oX Test 10.10.10.0/24
[*] exec: nmap -Pn -sS -A -oX Test 10.10.10.0/24
Starting Nmap 7.80 (https://nmap.org) at 2023-09-16 06:33 EDT
Nmap scan report for 10.10.10.1
Host is up (0.00011s latency).
All 1000 scanned ports on 10.10.10.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 0.11 ms 10.10.10.1
Nmap scan report for 10.10.10.2
Host is up (0.00017s latency).
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
53/tcp filtered domain
MAC Address: 00:50:56:EE:64:88 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized
Running: VMware Player
OS CPE: cpe:/a:vmware:player
OS details: VMware Player virtual NAT device
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 0.17 ms 10.10.10.2

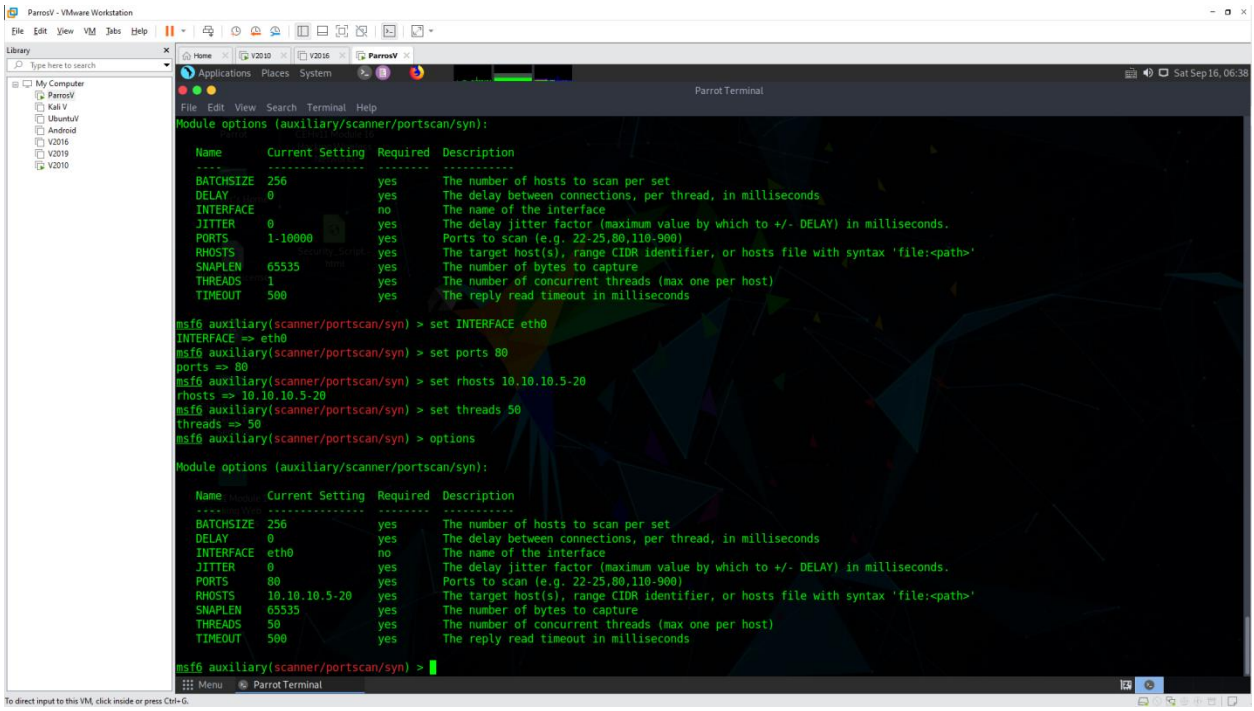

ParrosV - VMware Workstation
Parrot Terminal
OS:=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=
OS:G)IE(R=Y%DFI=N%T=80%CD=Z)
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| nbstat: NetBIOS name: WINDOWS10, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:30:90:4f (VMware)
| smb2-security-mode:
| 2.10:
|_ Message signing enabled but not required
| smb2-time:
| date: 2023-09-16T10:35:41
|_ start_date: N/A
TRACEROUTE
HOP RTT ADDRESS
1 53.49 ms 10.10.10.10
Nmap scan report for 10.10.10.254
Host is up (0.000058s latency).
All 1000 scanned ports on 10.10.10.254 are filtered
MAC Address: 00:50:56:FE:80:98 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 0.06 ms 10.10.10.254
Nmap scan report for 10.10.10.13
Host is up (0.000020s latency).
All 1000 scanned ports on 10.10.10.13 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 133.95 seconds
msf6 >

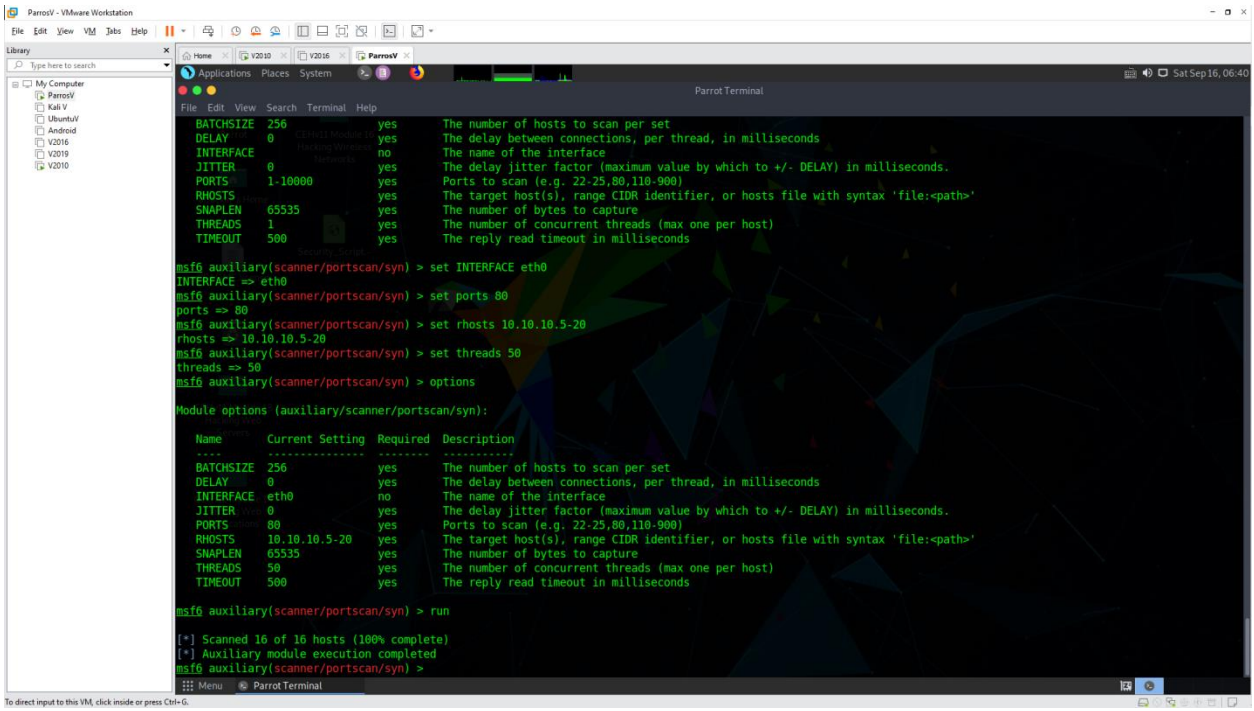

ParrosV - VMware Workstation
Parrot Terminal
Sat Sep 16, 06:37
| 2.10:
|_   Message signing enabled but not required
| smb2-time:
| date: 2023-09-16T10:35:41
|_ start_date: N/A
TRACEROUTE
HOP RTT   ADDRESS
1   53.49 ms 10.10.10.10
Nmap scan report for 10.10.10.254
Host is up (0.000058s latency).
All 1000 scanned ports on 10.10.10.254 are filtered
MAC Address: 00:50:56:FE:80:98 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT   ADDRESS
1   0.06 ms 10.10.10.254
Nmap scan report for 10.10.10.13
Host is up (0.000020s latency).
All 1000 scanned ports on 10.10.10.13 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 133.95 seconds
msf6 > db_import Test
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.10.10'
[*] Importing host 10.10.10.1
[*] Importing host 10.10.10.2
[*] Importing host 10.10.10.10
[*] Importing host 10.10.10.254
[*] Importing host 10.10.10.13
[*] Successfully imported /root/Test
msf6 >
Menu
Parrot Terminal
To direct input to this VM, click inside or press Ctrl+G.

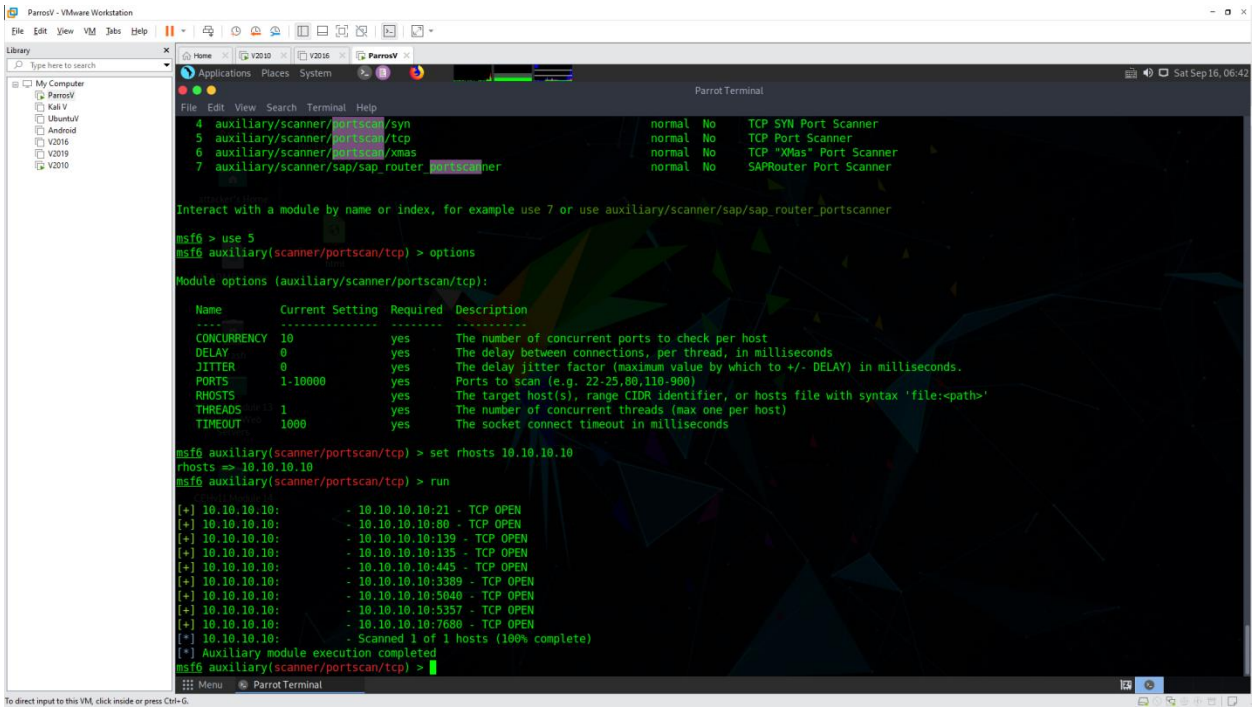

ParrosV - VMware Workstation
Parrot Terminal
Sat Sep 16, 06:37
MAC Address: 00:50:56:FE:80:98 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT   ADDRESS
1   0.06 ms 10.10.10.254
Nmap scan report for 10.10.10.13
Host is up (0.000020s latency).
All 1000 scanned ports on 10.10.10.13 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 133.95 seconds
msf6 > db_import Test
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.10.10'
[*] Importing host 10.10.10.1
[*] Importing host 10.10.10.2
[*] Importing host 10.10.10.10
[*] Importing host 10.10.10.254
[*] Importing host 10.10.10.13
[*] Successfully imported /root/Test
msf6 > hosts
Hosts
address   mac   name os_name   os_flavor os_sp purpose info comments
10.10.10.1   00:50:56:c0:00:08   Unknown   device
10.10.10.2   00:50:56:ee:64:88   Player   device
10.10.10.10   00:0c:29:30:90:4f   Windows Longhorn   device
10.10.10.13   Unknown   device
10.10.10.254 00:50:56:fe:80:98   Unknown   device
msf6 >
Menu
Parrot Terminal
To direct input to this VM, click inside or press Ctrl+G.

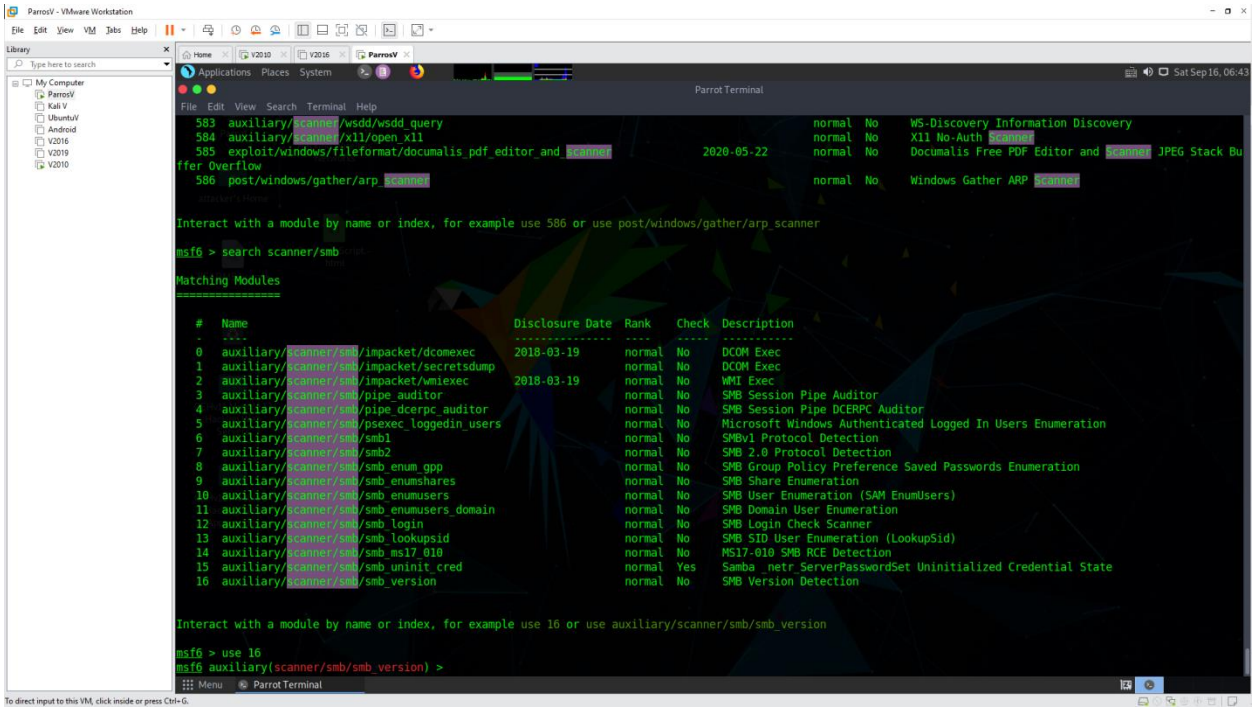

ParrosV - VMware Workstation
Parrot Terminal
Nmap done: 256 IP addresses (5 hosts up) scanned in 133.95 seconds
msf6 > db_import Test
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.10.10'
[*] Importing host 10.10.10.1
[*] Importing host 10.10.10.2
[*] Importing host 10.10.10.10
[*] Importing host 10.10.10.254
[*] Importing host 10.10.10.13
[*] Successfully imported /root/Test
msf6 > hosts
Hosts
address mac name os_name os_flavor os_sp purpose info comments
10.10.10.1 00:50:56:c0:00:08 Unknown device
10.10.10.2 00:50:56:ee:64:88 Player device
10.10.10.10 00:0c:29:30:90:4f Windows Longhorn device
10.10.10.13 Unknown device
10.10.10.254 00:50:56:fe:80:98 Unknown device
msf6 > services
Services
host port proto name state info
10.10.10.2 53 tcp domain filtered
10.10.10.10 21 tcp ftp open Microsoft ftpd
10.10.10.10 80 tcp http open Microsoft IIS httpd 10.0
10.10.10.10 135 tcp msrpc open Microsoft Windows RPC
10.10.10.10 139 tcp netbios-ssn open Microsoft Windows netbios-ssn
10.10.10.10 445 tcp microsoft-ds open
10.10.10.10 3389 tcp ssl/ms-wbt-server open
10.10.10.10 5357 tcp http open Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
msf6 >
Parrot Terminal

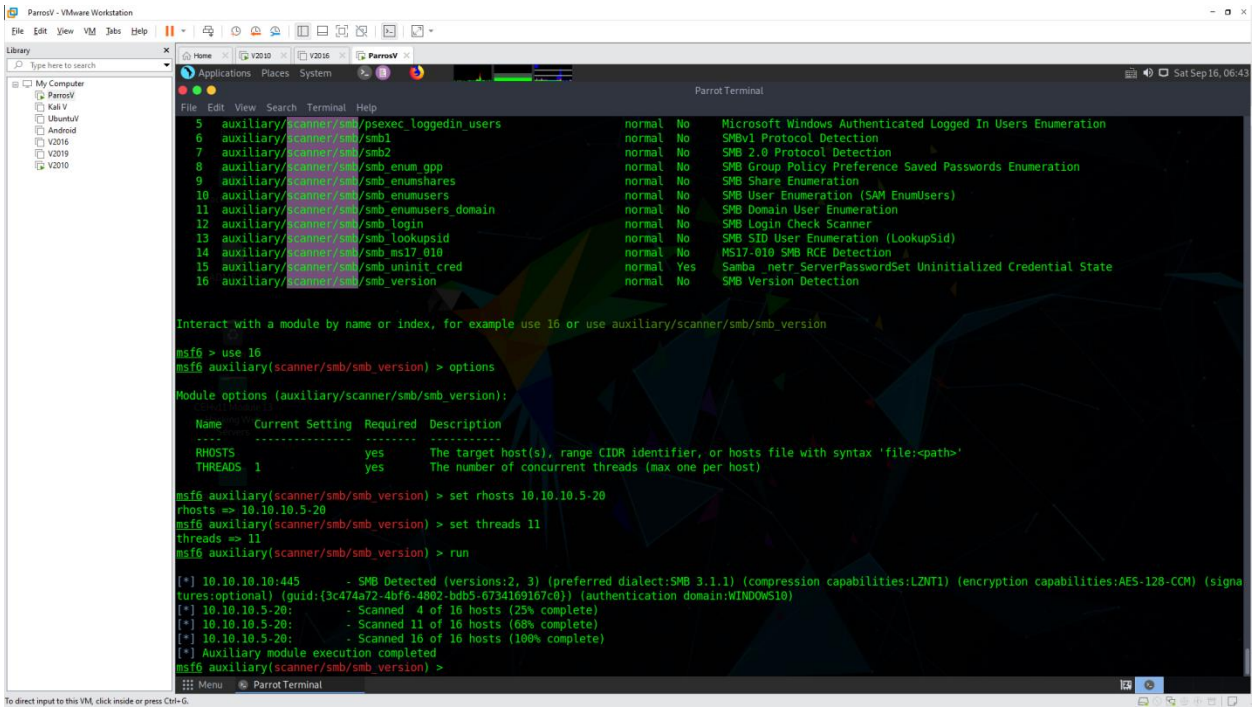

ParrosV - VMware Workstation
Parrot Terminal
10.10.10.10 00:0c:29:30:90:4f Windows Longhorn device
10.10.10.13 Unknown device
10.10.10.254 00:50:56:fe:80:98 Unknown device
msf6 > services
Services
host port proto name state info
10.10.10.2 53 tcp domain filtered
10.10.10.10 21 tcp ftp open Microsoft ftpd
10.10.10.10 80 tcp http open Microsoft IIS httpd 10.0
10.10.10.10 135 tcp msrpc open Microsoft Windows RPC
10.10.10.10 139 tcp netbios-ssn open Microsoft Windows netbios-ssn
10.10.10.10 445 tcp microsoft-ds open
10.10.10.10 3389 tcp ssl/ms-wbt-server open
10.10.10.10 5357 tcp http open Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
msf6 > search portscan
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/scanner/http/wordpress_pingback_access normal No Wordpress Pingback Locator
1 auxiliary/scanner/natpmp/natpmp_portscan normal No NAT-PMP External Port Scanner
2 auxiliary/scanner/portscan/ack normal No TCP ACK Firewall Scanner
3 auxiliary/scanner/portscan/ftpbounce normal No FTP Bounce Port Scanner
4 auxiliary/scanner/portscan/syn normal No TCP SYN Port Scanner
5 auxiliary/scanner/portscan/tcp normal No TCP Port Scanner
6 auxiliary/scanner/portscan/xmas normal No TCP "XMas" Port Scanner
7 auxiliary/scanner/sap/sap_router_portscanner normal No SAPRouter Port Scanner
Interact with a module by name or index, for example use 7 or use auxiliary/scanner/sap/sap_router_portscanner
msf6 >
Parrot Terminal

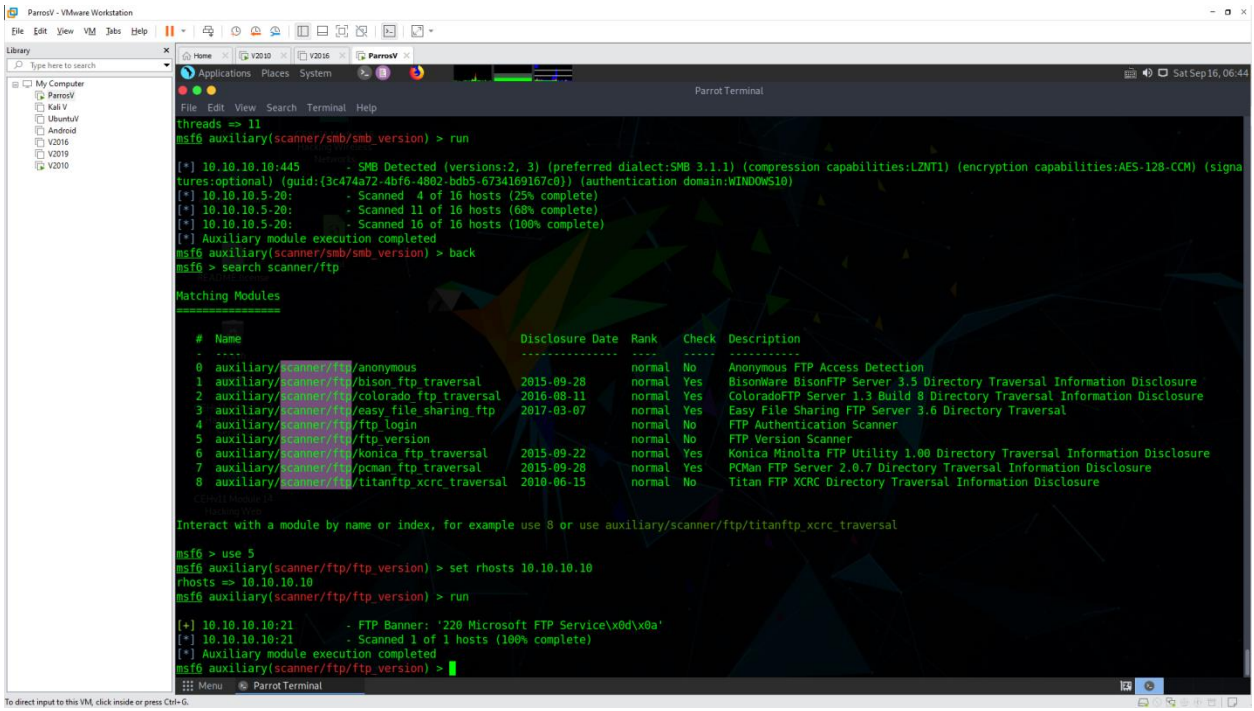

ParrosV - VMware Workstation
Parrot Terminal
Module options (auxiliary/scanner/portscan/syn):
Name Current Setting Required Description
BATCHSIZE 256 yes The number of hosts to scan per set
DELAY 0 yes The delay between connections, per thread, in milliseconds
INTERFACE no The name of the interface
JITTER 0 yes The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS 1-10000 yes Ports to scan (e.g. 22-25,80,110-900)
RHOSTS yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
SNAPLEN 65535 yes The number of bytes to capture
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 500 yes The reply read timeout in milliseconds
msf6 auxiliary(scanner/portscan/syn) > set INTERFACE eth0
INTERFACE => eth0
msf6 auxiliary(scanner/portscan/syn) > set ports 80
ports => 80
msf6 auxiliary(scanner/portscan/syn) > set rhosts 10.10.10.5-20
rhosts => 10.10.10.5-20
msf6 auxiliary(scanner/portscan/syn) > set threads 50
threads => 50
msf6 auxiliary(scanner/portscan/syn) > options
Module options (auxiliary/scanner/portscan/syn):
Name Current Setting Required Description
BATCHSIZE 256 yes The number of hosts to scan per set
DELAY 0 yes The delay between connections, per thread, in milliseconds
INTERFACE eth0 no The name of the interface
JITTER 0 yes The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS 80 yes Ports to scan (e.g. 22-25,80,110-900)
RHOSTS 10.10.10.5-20 yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
SNAPLEN 65535 yes The number of bytes to capture
THREADS 50 yes The number of concurrent threads (max one per host)
TIMEOUT 500 yes The reply read timeout in milliseconds
msf6 auxiliary(scanner/portscan/syn) >

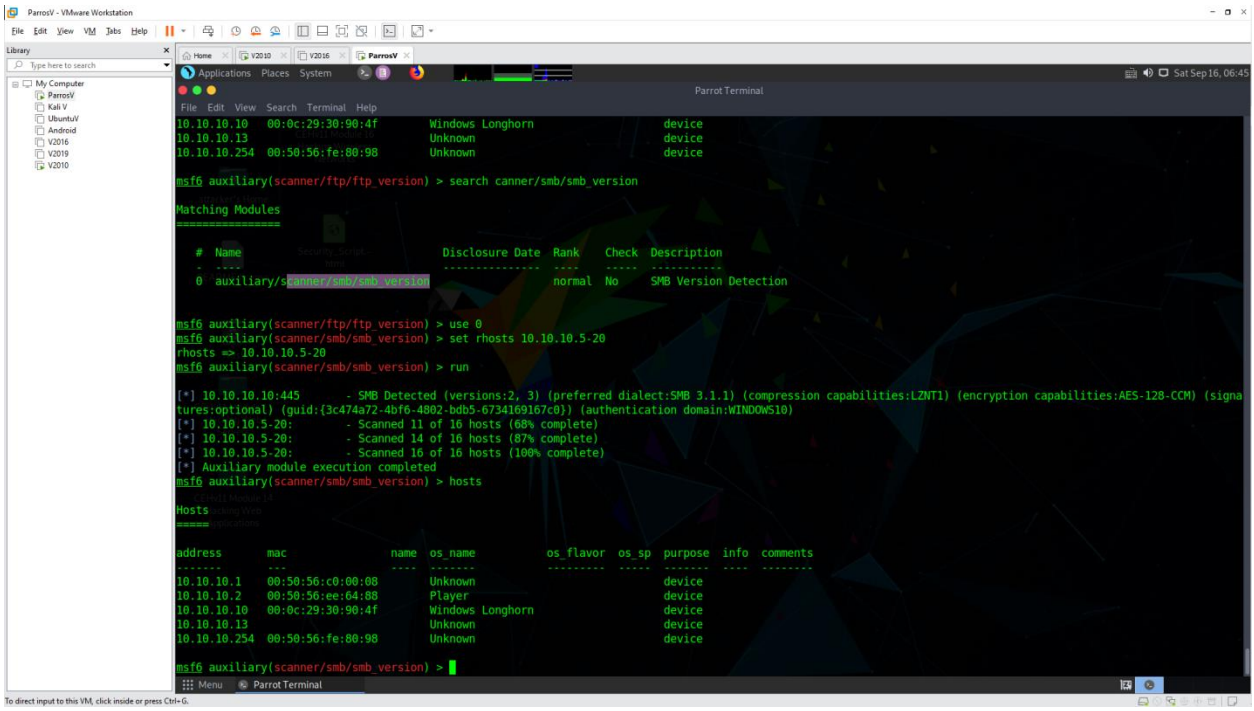

ParrosV - VMware Workstation
Parrot Terminal
BATCHSIZE 256 yes The number of hosts to scan per set
DELAY 0 yes The delay between connections, per thread, in milliseconds
INTERFACE no The name of the interface
JITTER 0 yes The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS 1-10000 yes Ports to scan (e.g. 22-25,80,110-900)
RHOSTS yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
SNAPLEN 65535 yes The number of bytes to capture
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 500 yes The reply read timeout in milliseconds
msf6 auxiliary(scanner/portscan/syn) > set INTERFACE eth0
INTERFACE => eth0
msf6 auxiliary(scanner/portscan/syn) > set ports 80
ports => 80
msf6 auxiliary(scanner/portscan/syn) > set rhosts 10.10.10.5-20
rhosts => 10.10.10.5-20
msf6 auxiliary(scanner/portscan/syn) > set threads 50
threads => 50
msf6 auxiliary(scanner/portscan/syn) > options
Module options (auxiliary/scanner/portscan/syn):
Name Current Setting Required Description
BATCHSIZE 256 yes The number of hosts to scan per set
DELAY 0 yes The delay between connections, per thread, in milliseconds
INTERFACE eth0 no The name of the interface
JITTER 0 yes The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS 80 yes Ports to scan (e.g. 22-25,80,110-900)
RHOSTS 10.10.10.5-20 yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
SNAPLEN 65535 yes The number of bytes to capture
THREADS 50 yes The number of concurrent threads (max one per host)
TIMEOUT 500 yes The reply read timeout in milliseconds
msf6 auxiliary(scanner/portscan/syn) > run
[*] Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/syn) >

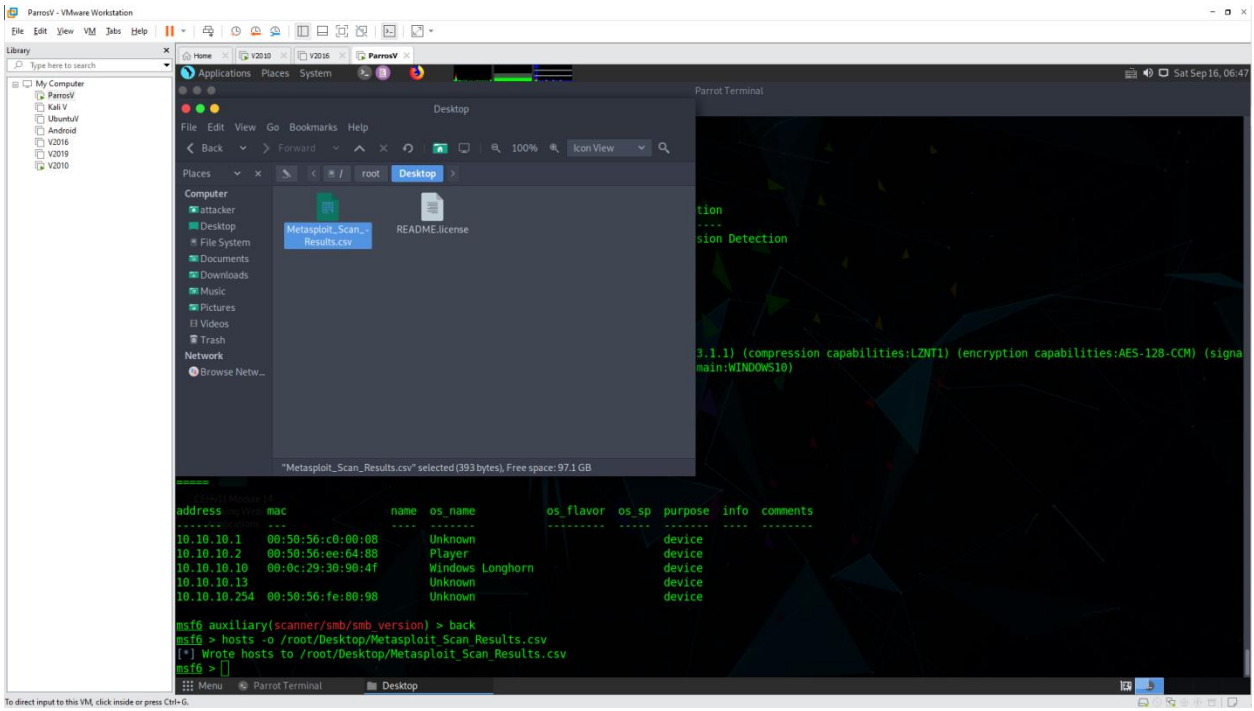

ParrosV - VMware Workstation
Parrot Terminal
Sat Sep 16, 06:42
4 auxiliary/scanner/portscan/syn normal No TCP SYN Port Scanner
5 auxiliary/scanner/portscan/tcp normal No TCP Port Scanner
6 auxiliary/scanner/portscan/xmas normal No TCP "XMas" Port Scanner
7 auxiliary/scanner/sap/sap_router_portscanner normal No SAPRouter Port Scanner
Interact with a module by name or index, for example use 7 or use auxiliary/scanner/sap/sap_router_portscanner
msf6 > use 5
msf6 auxiliary(scanner/portscan/tcp) > options
Module options (auxiliary/scanner/portscan/tcp):
Name Current Setting Required Description
CONCURRENCY 10 yes The number of concurrent ports to check per host
DELAY 0 yes The delay between connections, per thread, in milliseconds
JITTER 0 yes The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS 1-10000 yes Ports to scan (e.g. 22-25,80,110-900)
RHOSTS yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 1000 yes The socket connect timeout in milliseconds
msf6 auxiliary(scanner/portscan/tcp) > set rhosts 10.10.10.10
rhosts => 10.10.10.10
msf6 auxiliary(scanner/portscan/tcp) > run
[+] 10.10.10.10: - 10.10.10.10:21 - TCP OPEN
[+] 10.10.10.10: - 10.10.10.10:80 - TCP OPEN
[+] 10.10.10.10: - 10.10.10.10:139 - TCP OPEN
[+] 10.10.10.10: - 10.10.10.10:135 - TCP OPEN
[+] 10.10.10.10: - 10.10.10.10:445 - TCP OPEN
[+] 10.10.10.10: - 10.10.10.10:3389 - TCP OPEN
[+] 10.10.10.10: - 10.10.10.10:5040 - TCP OPEN
[+] 10.10.10.10: - 10.10.10.10:5357 - TCP OPEN
[+] 10.10.10.10: - 10.10.10.10:7680 - TCP OPEN
[*] 10.10.10.10: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) >

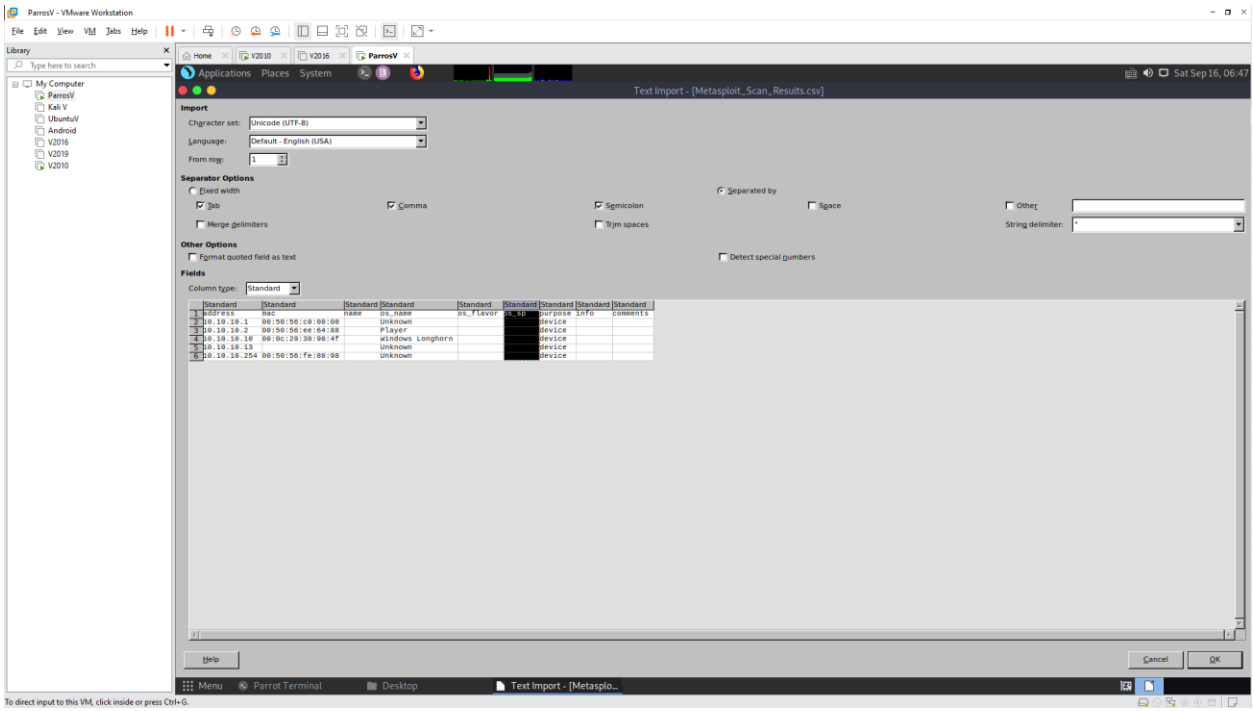

ParrosV - VMware Workstation
Parrot Terminal
Sat Sep 16, 06:43
583 auxiliary/scanner/wsdd/wsdd_query normal No WS-Discovery Information Discovery
584 auxiliary/scanner/x11/open_x11 normal No X11 No-Auth Scanner
585 exploit/windows/fileformat/documalis_pdf_editor_and_scanner 2020-05-22 normal No Documalis Free PDF Editor and Scanner JPEG Stack Buffer Overflow
586 post/windows/gather/arp_scanner normal No Windows Gather ARP Scanner
Interact with a module by name or index, for example use 586 or use post/windows/gather/arp_scanner
msf6 > search scanner/smb
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/scanner/smb/impacket/dcomexec 2018-03-19 normal No DCOM Exec
1 auxiliary/scanner/smb/impacket/secretsdump normal No DCOM Exec
2 auxiliary/scanner/smb/impacket/wmiexec 2018-03-19 normal No WMI Exec
3 auxiliary/scanner/smb/pipe_auditor normal No SMB Session Pipe Auditor
4 auxiliary/scanner/smb/pipe_dcerpc_auditor normal No SMB Session Pipe DCERPC Auditor
5 auxiliary/scanner/smb/psexec_loggedin_users normal No Microsoft Windows Authenticated Logged In Users Enumeration
6 auxiliary/scanner/smb/smb1 normal No SMBv1 Protocol Detection
7 auxiliary/scanner/smb/smb2 normal No SMB 2.0 Protocol Detection
8 auxiliary/scanner/smb/smb_enum_gpp normal No SMB Group Policy Preference Saved Passwords Enumeration
9 auxiliary/scanner/smb/smb_enumshares normal No SMB Share Enumeration
10 auxiliary/scanner/smb/smb_enumusers normal No SMB User Enumeration (SAM EnumUsers)
11 auxiliary/scanner/smb/smb_enumusers_domain normal No SMB Domain User Enumeration
12 auxiliary/scanner/smb/smb_login normal No SMB Login Check Scanner
13 auxiliary/scanner/smb/smb_lookupsid normal No SMB SID User Enumeration (LookupSid)
14 auxiliary/scanner/smb/smb_ms17_010 normal No MS17-010 SMB RCE Detection
15 auxiliary/scanner/smb/smb_uninit_cred normal Yes Samba _netr_ServerPasswordSet Uninitialized Credential State
16 auxiliary/scanner/smb/smb_version normal No SMB Version Detection
Interact with a module by name or index, for example use 16 or use auxiliary/scanner/smb/smb_version
msf6 > use 16
msf6 auxiliary(scanner/smb/smb_version) >


ParrosV - VMware Workstation
Parrot Terminal
Sat Sep 16, 06:43
5 auxiliary/scanner/smb/psexec_loggedin_users normal No Microsoft Windows Authenticated Logged In Users Enumeration
6 auxiliary/scanner/smb/smb1 normal No SMBv1 Protocol Detection
7 auxiliary/scanner/smb/smb2 normal No SMB 2.0 Protocol Detection
8 auxiliary/scanner/smb/smb_enum_gpp normal No SMB Group Policy Preference Saved Passwords Enumeration
9 auxiliary/scanner/smb/smb_enumshares normal No SMB Share Enumeration
10 auxiliary/scanner/smb/smb_enumusers normal No SMB User Enumeration (SAM EnumUsers)
11 auxiliary/scanner/smb/smb_enumusers_domain normal No SMB Domain User Enumeration
12 auxiliary/scanner/smb/smb_login normal No SMB Login Check Scanner
13 auxiliary/scanner/smb/smb_lookupsid normal No SMB SID User Enumeration (LookupSid)
14 auxiliary/scanner/smb/smb_ms17_010 normal No MS17-010 SMB RCE Detection
15 auxiliary/scanner/smb/smb_uninit_cred normal Yes Samba _netr_ServerPasswordSet Uninitialized Credential State
16 auxiliary/scanner/smb/smb_version normal No SMB Version Detection
Interact with a module by name or index, for example use 16 or use auxiliary/scanner/smb/smb_version
msf6 > use 16
msf6 auxiliary(scanner/smb/smb_version) > options
Module options (auxiliary/scanner/smb/smb_version):
Name Current Setting Required Description
RHOSTS yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
THREADS 1 yes The number of concurrent threads (max one per host)
msf6 auxiliary(scanner/smb/smb_version) > set rhosts 10.10.10.5-20
rhosts => 10.10.10.5-20
msf6 auxiliary(scanner/smb/smb_version) > set threads 11
threads => 11
msf6 auxiliary(scanner/smb/smb_version) > run
[*] 10.10.10.10:445 - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:AES-128-CCM) (signatures:optional) (guid:{3c474a72-4bf6-4802-bdb5-6734169167c0}) (authentication domain:WINDOWS10)
[*] 10.10.10.5-20: - Scanned 4 of 16 hosts (25% complete)
[*] 10.10.10.5-20: - Scanned 11 of 16 hosts (68% complete)
[*] 10.10.10.5-20: - Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >


ParrosV - VMware Workstation
Parrot Terminal
Sat Sep 16, 06:44
threads => 11
msf6 auxiliary(scanner/smb/smb_version) > run
[*] 10.10.10.10:445 - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:AES-128-CCM) (signatures:optional) (guid:{3c474a72-4bf6-4802-bdb5-6734169167c0}) (authentication domain:WINDOWS10)
[*] 10.10.10.5-20: - Scanned 4 of 16 hosts (25% complete)
[*] 10.10.10.5-20: - Scanned 11 of 16 hosts (68% complete)
[*] 10.10.10.5-20: - Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > back
msf6 > search scanner/ftp
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/scanner/ftp/anonymous normal No Anonymous FTP Access Detection
1 auxiliary/scanner/ftp/bison_ftp_traversal 2015-09-28 normal Yes BisonWare BisonFTP Server 3.5 Directory Traversal Information Disclosure
2 auxiliary/scanner/ftp/colorado_ftp_traversal 2016-08-11 normal Yes ColoradoFTP Server 1.3 Build 8 Directory Traversal Information Disclosure
3 auxiliary/scanner/ftp/easy_file_sharing_ftp 2017-03-07 normal Yes Easy File Sharing FTP Server 3.6 Directory Traversal
4 auxiliary/scanner/ftp/ftp_login normal No FTP Authentication Scanner
5 auxiliary/scanner/ftp/ftp_version normal No FTP Version Scanner
6 auxiliary/scanner/ftp/konica_ftp_traversal 2015-09-22 normal Yes Konica Minolta FTP Utility 1.00 Directory Traversal Information Disclosure
7 auxiliary/scanner/ftp/pcman_ftp_traversal 2015-09-28 normal Yes PCMan FTP Server 2.0.7 Directory Traversal Information Disclosure
8 auxiliary/scanner/ftp/titanftp_xcrc_traversal 2010-06-15 normal No Titan FTP XCRC Directory Traversal Information Disclosure
Interact with a module by name or index, for example use 8 or use auxiliary/scanner/ftp/titanftp_xcrc_traversal
msf6 > use 5
msf6 auxiliary(scanner/ftp/ftp_version) > set rhosts 10.10.10.10
rhosts => 10.10.10.10
msf6 auxiliary(scanner/ftp/ftp_version) > run
[+] 10.10.10.10:21 - FTP Banner: '220 Microsoft FTP Service\x0d\x0a'
[*] 10.10.10.10:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/ftp_version) >


ParrosV - VMware Workstation
Parrot Terminal
10.10.10.10 00:0c:29:30:90:4f Windows Longhorn device
10.10.10.13 Unknown device
10.10.10.254 00:50:56:fe:80:98 Unknown device
msf6 auxiliary(scanner/ftp/ftp_version) > search canner/smb/smb_version
Matching Modules
0 auxiliary/scanner/smb/smb_version normal No SMB Version Detection
msf6 auxiliary(scanner/ftp/ftp_version) > use 0
msf6 auxiliary(scanner/smb/smb_version) > set rhosts 10.10.10.5-20
rhosts => 10.10.10.5-20
msf6 auxiliary(scanner/smb/smb_version) > run
[*] 10.10.10.10:445 - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:AES-128-CCM) (signatures:optional) (guid:{3c474a72-4bf6-4802-bdb5-6734169167c0}) (authentication domain:WINDOWS10)
[*] 10.10.10.5-20: - Scanned 11 of 16 hosts (68% complete)
[*] 10.10.10.5-20: - Scanned 14 of 16 hosts (87% complete)
[*] 10.10.10.5-20: - Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > hosts
Hosts
address mac name os_name os_flavor os_sp purpose info comments
10.10.10.1 00:50:56:c0:00:08 Unknown device
10.10.10.2 00:50:56:ee:64:88 Player device
10.10.10.10 00:0c:29:30:90:4f Windows Longhorn device
10.10.10.13 Unknown device
10.10.10.254 00:50:56:fe:80:98 Unknown device
msf6 auxiliary(scanner/smb/smb_version) >


ParrosV - VMware Workstation
Desktop
Metasploit_Scan_Results.csv
README.license
"Metasploit_Scan_Results.csv" selected (393 bytes), Free space: 97.1 GB
msf6 auxiliary(scanner/smb/smb_version) > back
msf6 > hosts -o /root/Desktop/Metasploit_Scan_Results.csv
[*] Wrote hosts to /root/Desktop/Metasploit_Scan_Results.csv
msf6 >


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, 06:47
Text Import - [Metasploit_Scan_Results.csv]
Import
Character set: Unicode (UTF-8)
Language: Default - English (USA)
From row: 1
Separator Options
Fixed width
Separated by
Tab
Comma
Semicolon
Space
Other
Merge delimiters
Trim spaces
String delimiter: "
Other Options
Format quoted field as text
Detect special numbers
Fields
Column type: Standard
Standard Standard Standard Standard Standard Standard Standard Standard Standard
1 address mac name os_name os_flavor os_sp purpose info comments
2 10.10.10.1 00:50:56:c0:00:08 Unknown device
3 10.10.10.2 00:50:56:ee:64:88 Player device
4 10.10.10.10 00:0c:29:30:90:4f windows Longhorn device
5 10.10.10.13 Unknown device
6 10.10.10.254 00:50:56:fe:80:98 Unknown device
Help
Cancel
OK
Menu
Parrot Terminal
Desktop
Text Import - [Metasplo...
To direct input to this VM, click inside or press Ctrl+G.