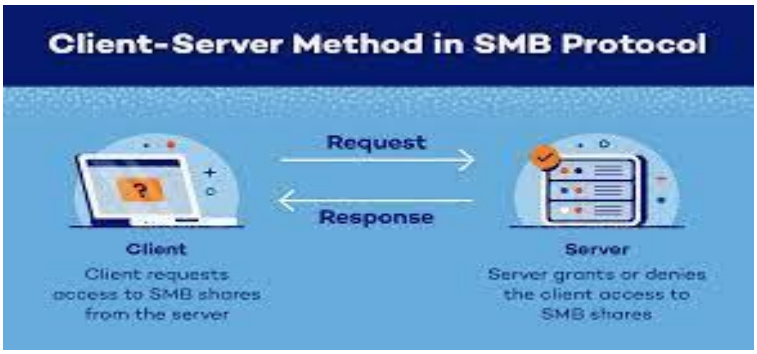
PROTOCOLS AND THEIR FUNCTIONALITY IN DETAIL

Server Message Block protocol (SMB protocol)

The SMB protocol (the Server Message Block) is a network protocol that enables users to communicate with remote computers and servers (e.g., to share resources or files). It's also referred to as the server/client protocol because the server has a resource that it can share with the client

How the SMB protocol works

The SMB protocol is known as the response-request protocol. SMB operates at the application layer (i.e., where the user interacts with software apps). However, it uses lower network levels to transmit data, such as the transport layer like TCP or UDP.



Here's a summary of how the SMB works:

1. First, the client (e.g., a user's computer, mobile device, or printer) sends an SMB request to the server to initiate a connection.

2. The server receives this request and sends an SMB response back to the client.

3. When this response is received, it establishes a communication channel.

4. The device (e.g., a user's computer) can then interact with the server to request access to shared resources or perform specific actions.

SMB protocol types

Over the years, many SMB versions have become available, bringing unique improvements and updates to address performance issues and security risks. Let's look at the main versions of the SMB protocol.

- SMB 1.0 was initially introduced in 1984 by IBM as part of their PC network program for file sharing in a DOS (disk operating system) environment. Implementing SMB 1.0 was a big step towards simplified networked file sharing
- CIFS improved the SMBv1 protocol, delivering better performance, support for long file names, and more advanced security features. Its release in 1996 coincided with the new Windows 95 operating system.

What are ports 139 and 445?

SMB uses open ports (i.e., actively accepting incoming connections and traffic) to facilitate communication across the network. The two main ports the SMB uses are 139 and 445.

- Port 139. The earlier versions of the SMB protocol primarily ran in small-scale LAN environments using the now outdated NetBIOS network architecture. SMB mainly used port 139 to allow communication between different machines on the network.

- Port 445. With the development of Windows 2000, Microsoft changed SMB to operate on top of TCP and use a dedicated IP port — port 445.

NETBIOS

NETBIOS is an application programming interface (API) that operates at the session layer (Layer 5) of the OSI (Open Systems Interconnection) model. It provides various services, such as name service, datagram service, and session service, to facilitate communication between devices on a network.

1. Name service (NetBIOS-NS): This service is responsible for registering, releasing, and resolving computer names to their IP addresses, enabling communication between devices on the network.
2. Datagram service (NetBIOS-DGM): It provides a connectionless communication method for sending messages or data packets between devices in a LAN without establishing a dedicated connection.
3. Session service (NetBIOS-SSN): This service facilitates connection-oriented communication between devices in a LAN, allowing the exchange of data through established sessions.

The Purpose of NETBIOS

- **Name Resolution:** The Name Service (NetBIOS-NS) component of NETBIOS is responsible for registering, releasing, and resolving computer names to their IP addresses. This allows devices on the network to communicate with each other using easily identifiable names rather than relying solely on IP addresses.
- **Connection-Oriented Communication:** The Session Service (NetBIOS-SSN) facilitates connection-oriented communication between devices in a LAN. This allows devices to exchange data through established sessions, providing a reliable communication channel for transmitting larger amounts of data or for applications that require continuous communication between devices.
- **Resource Sharing:** NETBIOS enables computers and devices on a network to share resources, such as files, printers, and other peripherals. This simplifies the process of accessing and managing shared resources within a LAN.

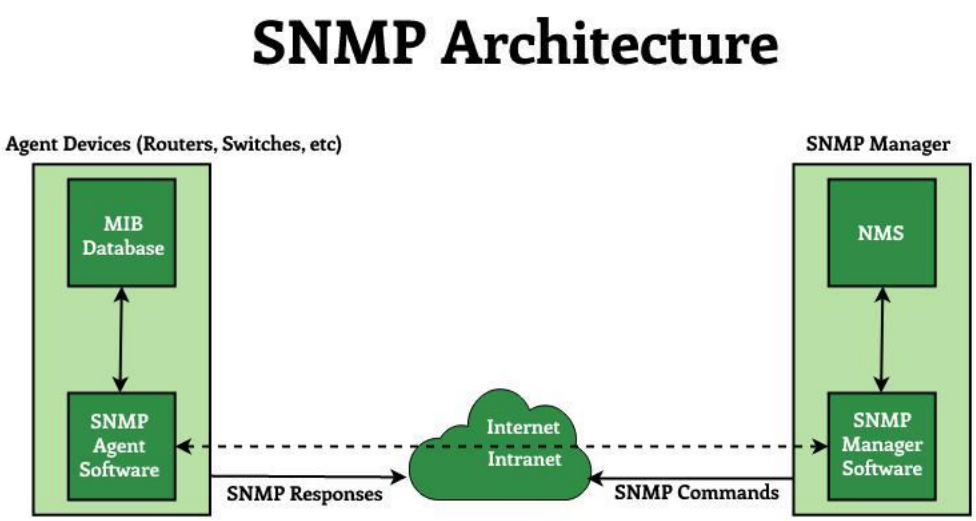
How Does NETBIOS Work

NETBIOS (Network Basic Input/Output System) works by providing a set of services that facilitate communication and resource sharing between computers and devices within a local area network (LAN). NETBIOS operates at the session layer (Layer 5) of the OSI (Open Systems Interconnection) model and typically runs over transport protocols like TCP/IP using NBT (NetBIOS over TCP/IP).

- Name Service (NetBIOS-NS): The name service is responsible for registering, releasing, and resolving computer names to their IP addresses. When a computer joins the network, it registers its unique NETBIOS name with the name service. This enables devices on the network to communicate using easily identifiable names rather than IP addresses.
- Datagram Service (NetBIOS-DGM): The datagram service provides connectionless communication between devices in a LAN. Devices can send messages or data packets to one another without establishing a dedicated connection
- Session Service (NetBIOS-SSN): The session service facilitates connection-oriented communication between devices in a LAN. When two devices need to exchange data, they establish a session using the session service. Once the session is established, the devices can send data to each other over the connection using the Transmission Control Protocol (TCP).

SNMP

Simple Network Management Protocol (SNMP) is a networking protocol used for the management and monitoring of network-connected devices in Internet Protocol networks. The SNMP protocol is embedded in multiple local devices such as routers, switches, servers, firewalls, and wireless access points accessible using their IP address. SNMP provides a common mechanism for network devices to relay management information within single and multi-vendor LAN or WAN environments. It is an application layer protocol in the OSI model framework



There are three different versions of SNMP:

- **SNMP version 1 (SNMPv1)**—This was the first implementation, operating within the structure management information specification, and described in RFC 1157.
- **SNMP version 2 (SNMPv2)**—This version was improved to support more efficient error handling and is described in RFC 1901. It was first introduced as RFC 1441. It is often referred to as SNMPv2c.
- **SNMP version 3 (SNMPv3)**—This version improves security and privacy. It was introduced in RFC 3410.

SNMP Runtime Components

These are the main runtime components in an SNMP-enabled environment:

- **SNMP-managed devices and resources**—These are the devices and network elements on which an agent runs.
- **SNMP agent**—This software runs on the hardware or service being monitored by SNMP, collecting data on various metrics like CPU usage, bandwidth usage or disk space. As queried by the SNMP manager, the agent finds and sends this information back to SNMP management systems.
- **SNMP manager**—(also referred to as SNMP server) This component functions as a centralized management station running an SNMP management application on many different operating system environments. It actively requests agents send SNMP updates at regular intervals.
- **Management information base (MIB)**—This data structure is a text file (with a .mib file extension) that describes all data objects used by a particular device that can be queried or controlled using SNMP including access control.

SNMP Commands

SNMP tools perform many functions that rely on a mix of push and pull communications between network devices and the network management system. At its core set of functions, it can execute read or write commands, such as resetting a password or changing a configuration setting

- **Get Request**—A request to retrieve the value of a variable or list of variables.
- **Set Request**—Sent by the SNMP manager to the agent to issue configurations or commands.
- **GetNext Request**—Sent by the SNMP manager to agent to find the values of the next record in the MIB's hierarchy.
- **GetBulk Request**—Sent by the SNMP manager to the agent to obtain large tables of data by performing multiple GetNext Request commands.
- **SNMP Response**—Sent by the agent to the SNMP manager, issued in reply to a
- **SNMP Trap**—Asynchronous trap messages from SNMP agents alert an SNMP manager that a significant event such as an error or failure, has occurred.
- **SNMP Inform**—Confirms receipt of a trap.

DNS

What is DNS?

A Domain Name System (DNS) turns domain names into IP addresses, which allow browsers to get to websites and other internet resources. Every device on the internet has an IP address, which other devices can use to locate the device. Instead of memorizing a long list of IP addresses, people can simply enter the name of the website, and the DNS gets the IP address for them.

An example of a DNS is that which is provided by Google. The address of Google's primary DNS is 8.8.8.8.

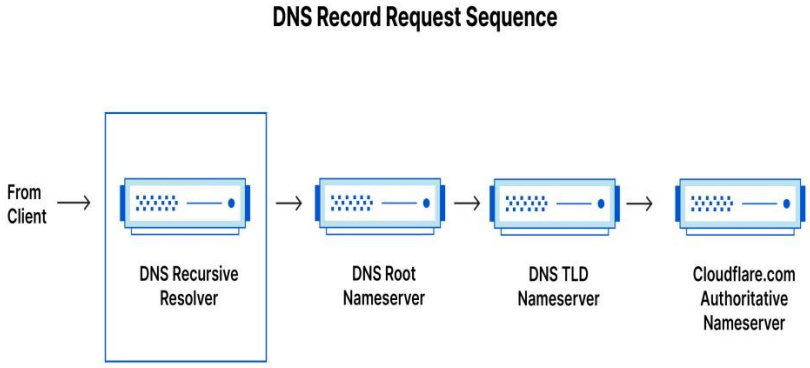
How does DNS work?

The process of DNS resolution involves converting a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the appropriate Internet device - like a street address is used to find a particular home. In

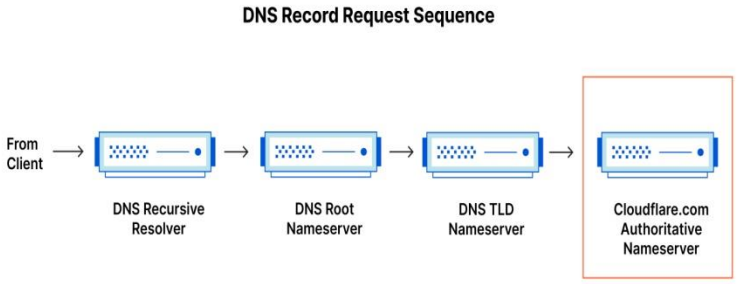
order to understand the process behind the DNS resolution, it's important to learn about the different hardware components a DNS query must pass between. For the web browser, the DNS lookup occurs "behind the scenes" and requires no interaction from the user's computer apart from the initial request.

There are 4 DNS servers involved in loading a webpage:

- DNS recursor - The recursor can be thought of as a librarian who is asked to go find a particular book somewhere in a library. The DNS recursor is a server designed to receive queries from client machines through applications such as web browsers. Typically the recursor is then responsible for making additional requests in order to satisfy the client's DNS query.



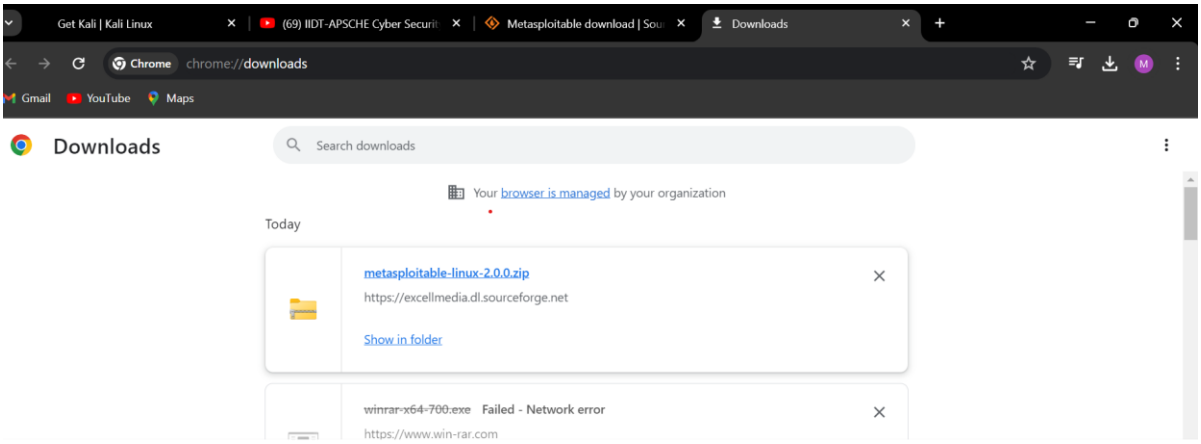
- **Root nameserver** - The root server is the first step in translating (resolving) human readable host names into IP addresses. It can be thought of like an index in a library that points to different racks of books - typically it serves as a reference to other more specific locations.

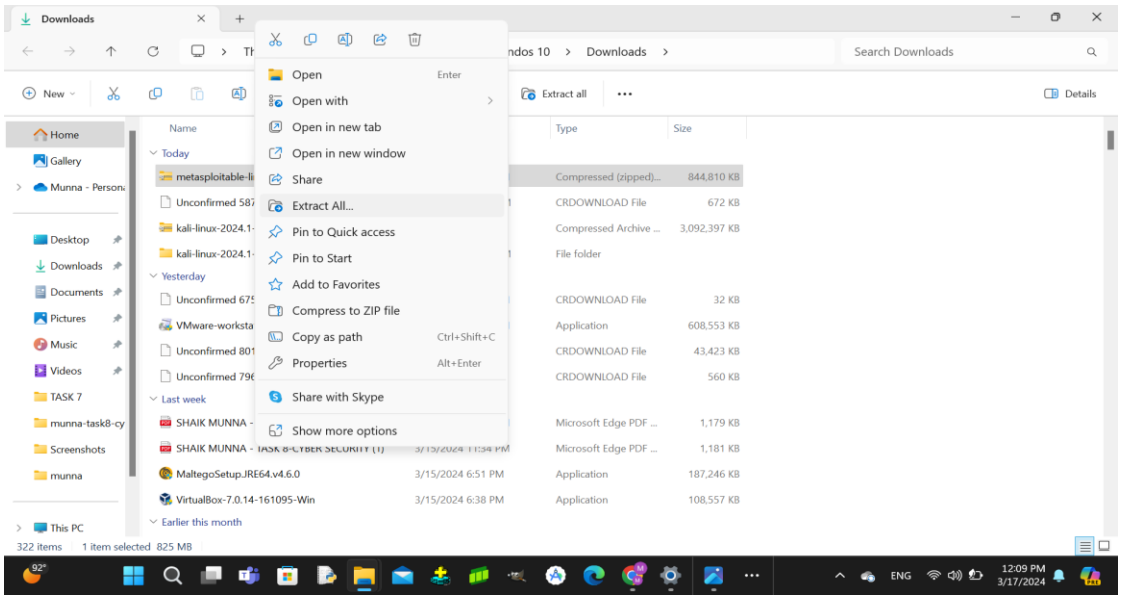


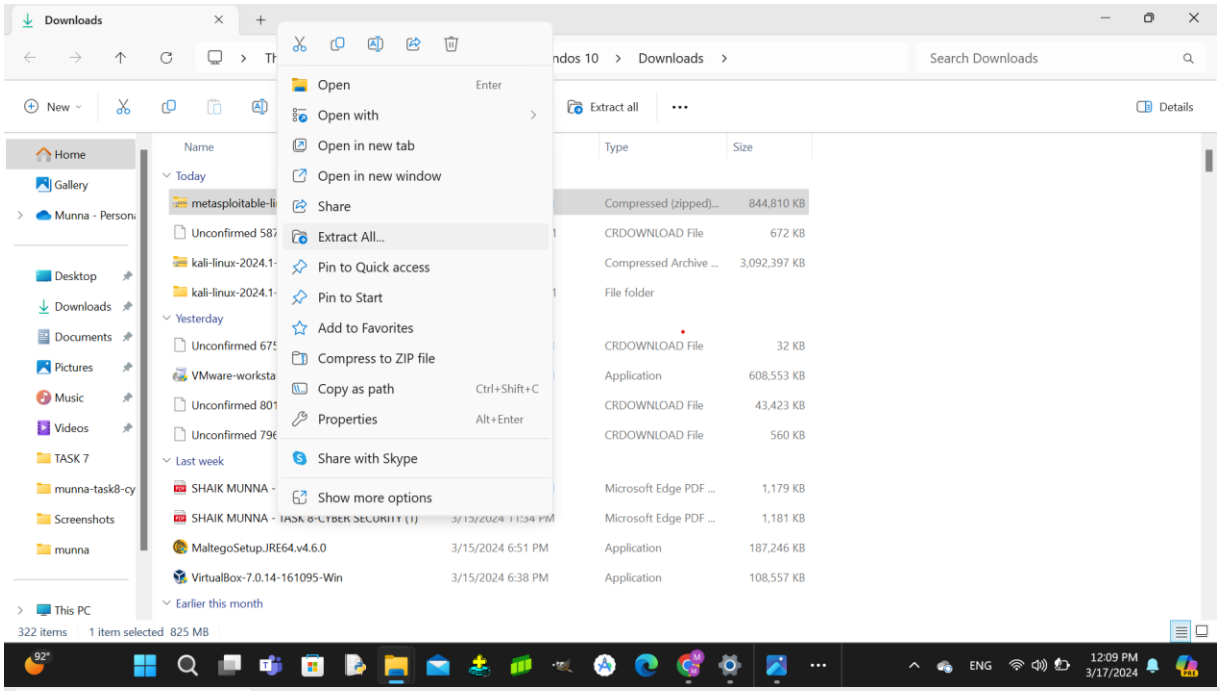
- TLD nameserver - The top level domain server (TLD) can be thought of as a specific rack of books in a library. This nameserver is the next step in the search for a specific IP address, and it hosts the last portion of a hostname (In example.com, the TLD server is “com”).

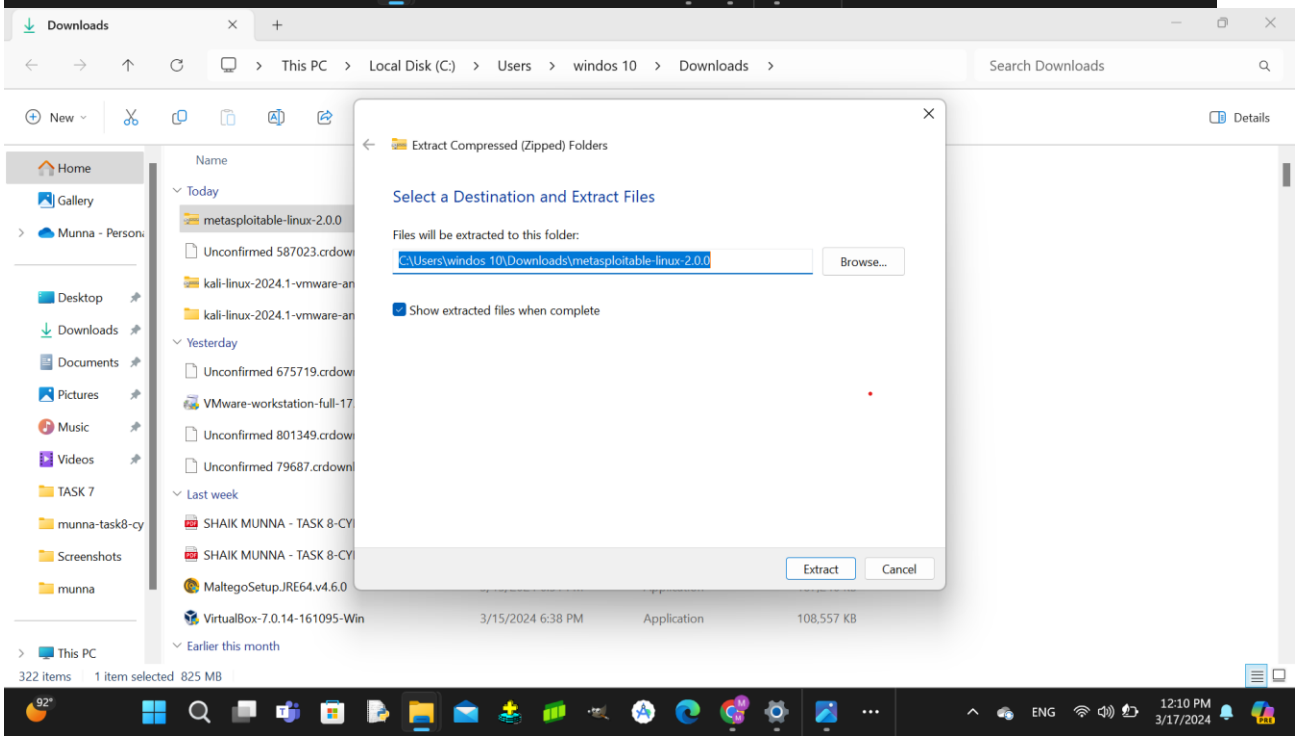
- Authoritative nameserver - This final nameserver can be thought of as a dictionary on a rack of books, in which a specific name can be translated indefinition. The authoritative nameserver is the last stop in the nameserver query. If the authoritative name server has access to the requested record,

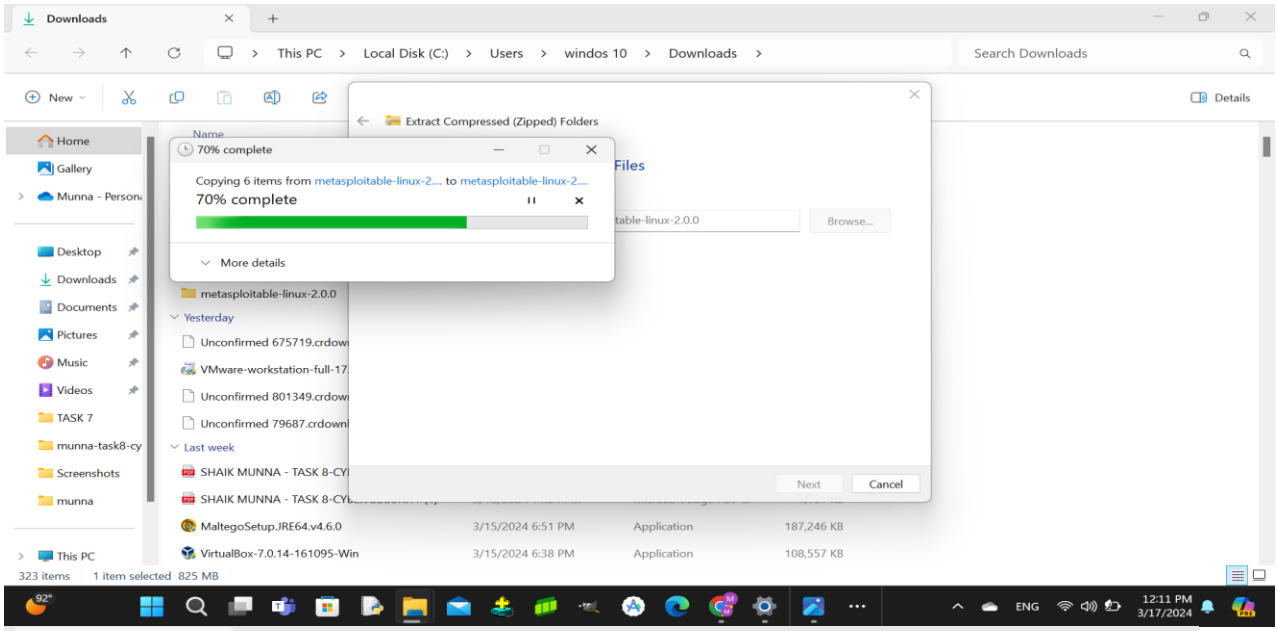
METASPLOITABLE SERVER INSTALLATION

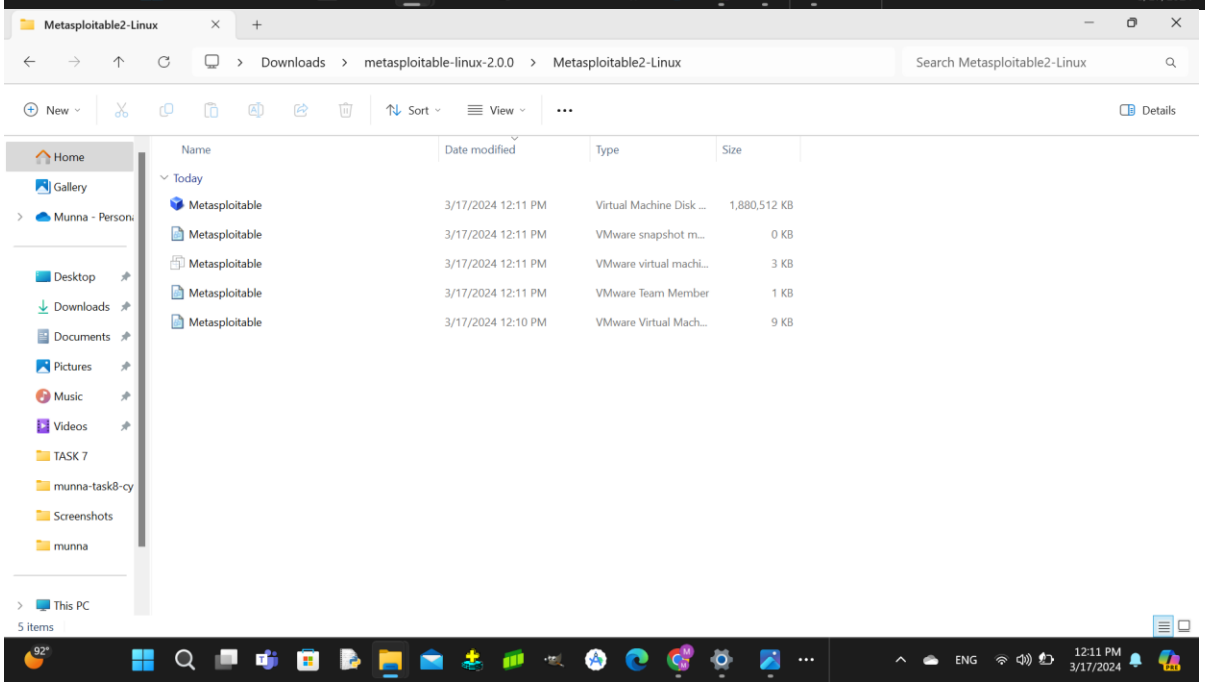


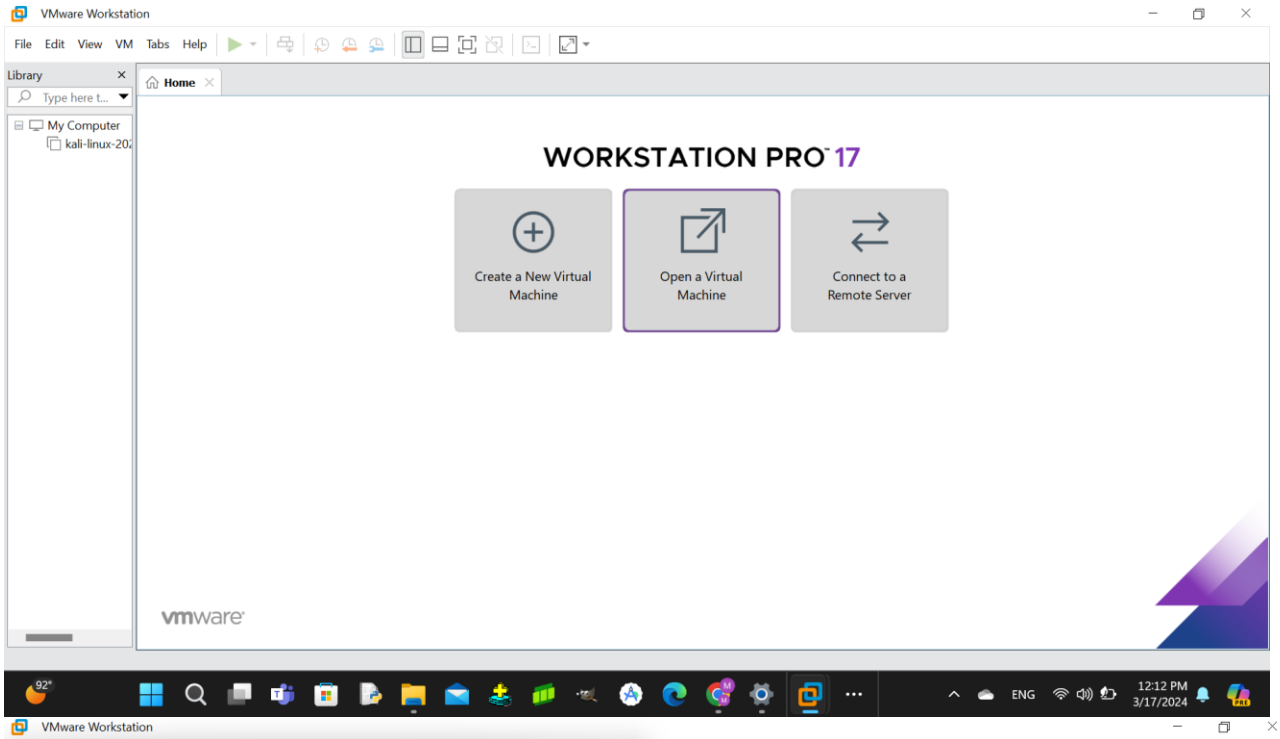


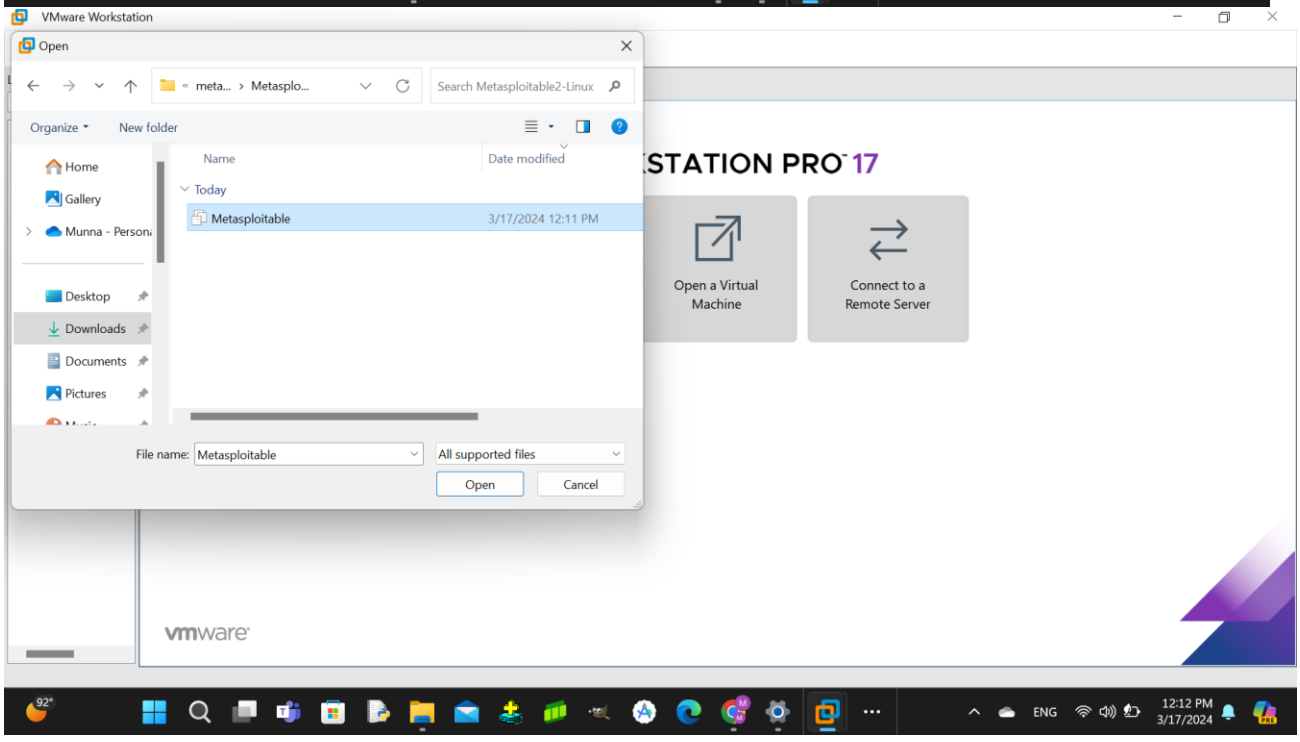

Downloads
Search Downloads
Open
Open with
Open in new tab
Open in new window
Share
Extract All...
Pin to Quick access
Pin to Start
Add to Favorites
Compress to ZIP file
Copy as path
Properties
Share with Skype
Show more options
Extract all
Details
Home
Gallery
Desktop
Downloads
Documents
Pictures
Music
Videos
TASK 7
munna-task8-cy
Screenshots
munna
This PC
Name
Type
Size
Today
Yesterday
Last week
Earlier this month
metasploitable-li
Unconfirmed 587
kali-linux-2024.1-
VMware-worksta
Unconfirmed 801
Unconfirmed 796
SHAIK MUNNA -
MaltegoSetup.JRE64.v4.6.0
VirtualBox-7.0.14-161095-Win
Compressed (zipped)... 844,810 KB
CRDOWNLOAD File 672 KB
Compressed Archive ... 3,092,397 KB
File folder
CRDOWNLOAD File 32 KB
Application 608,553 KB
CRDOWNLOAD File 43,423 KB
CRDOWNLOAD File 560 KB
Microsoft Edge PDF ... 1,179 KB
Microsoft Edge PDF ... 1,181 KB
3/15/2024 6:51 PM Application 187,246 KB
3/15/2024 6:38 PM Application 108,557 KB
322 items 1 item selected 825 MB
ENG 12:09 PM 3/17/2024

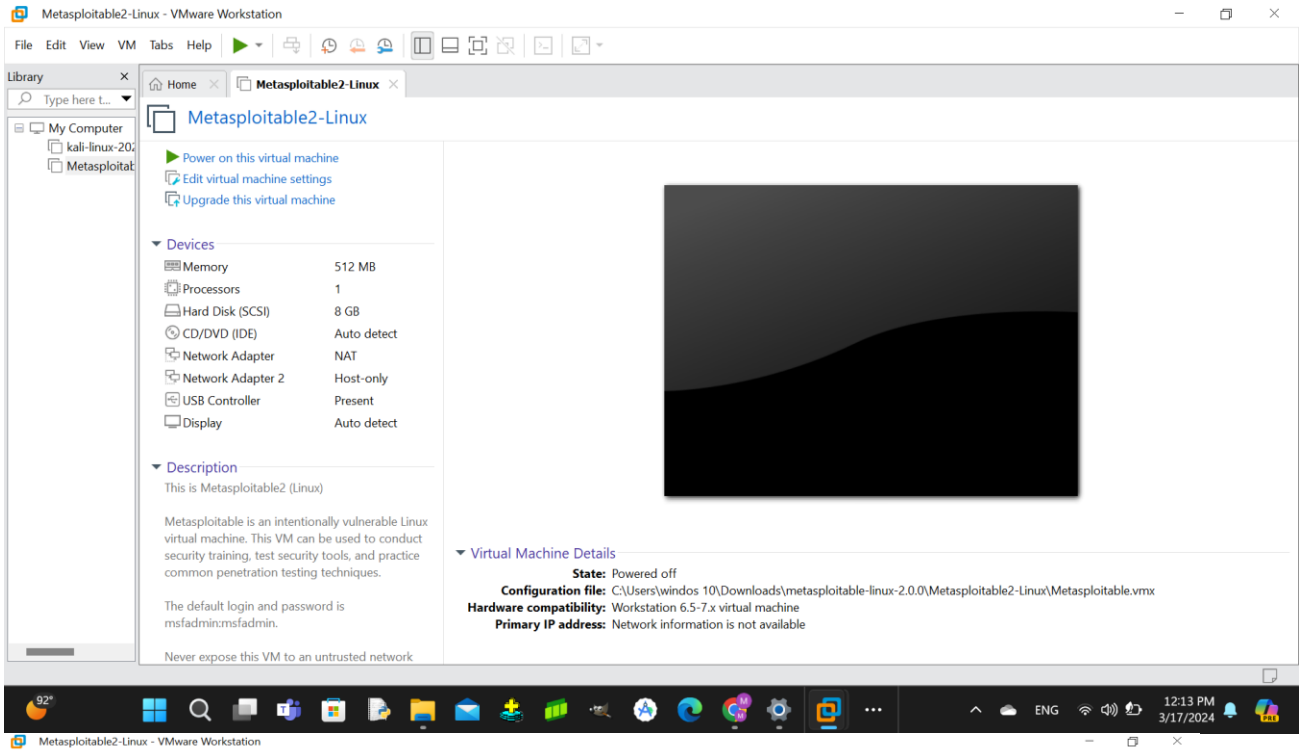

Downloads
This PC › Local Disk (C:) › Users › windos 10 › Downloads ›
Search Downloads
New
Details
Extract Compressed (Zipped) Folders
Select a Destination and Extract Files
Files will be extracted to this folder:
C:\Users\windos 10\Downloads\metasploitable-linux-2.0.0
Browse...
Show extracted files when complete
Extract
Cancel
Home
Gallery
Desktop
Downloads
Documents
Pictures
Music
Videos
TASK 7
munna-task8-cy
Screenshots
munna
This PC
Name
Today
Yesterday
Last week
Earlier this month
metasploitable-linux-2.0.0
Unconfirmed 587023.crdow
kali-linux-2024.1-vmware-an
kali-linux-2024.1-vmware-an
Unconfirmed 675719.crdow
VMware-workstation-full-17
Unconfirmed 801349.crdow
Unconfirmed 79687.crdown
SHAIK MUNNA - TASK 8-CY
SHAIK MUNNA - TASK 8-CY
MaltegoSetup.JRE64.v4.6.0
VirtualBox-7.0.14-161095-Win
3/15/2024 6:38 PM Application 108,557 KB
322 items 1 item selected 825 MB
ENG 12:10 PM 3/17/2024

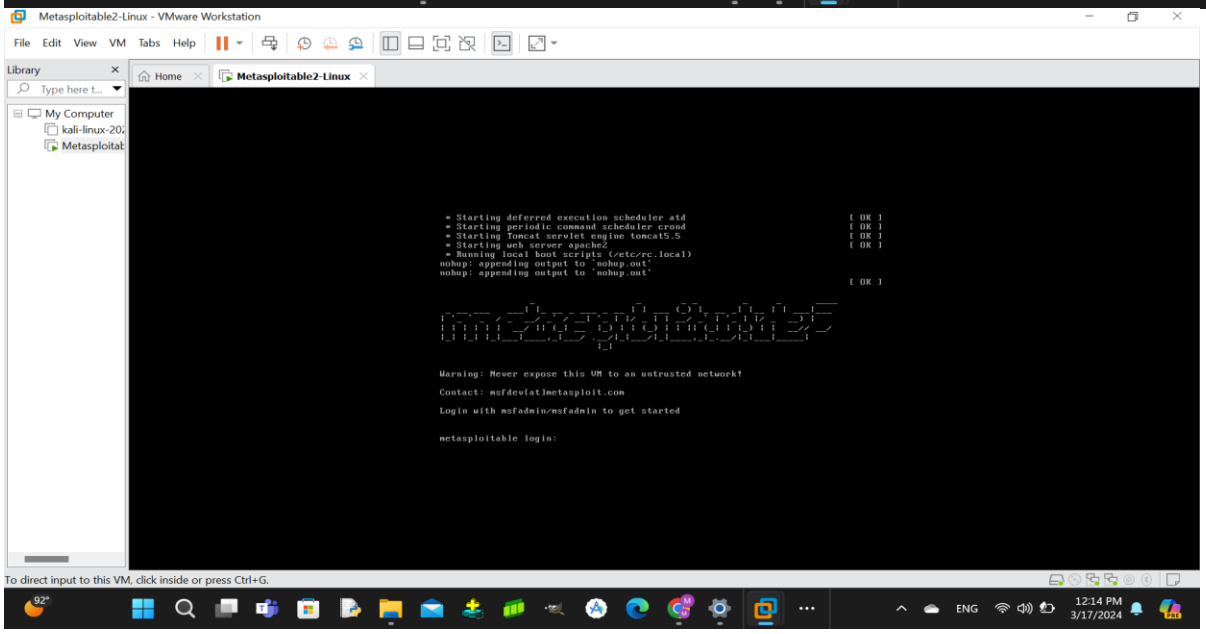

Downloads
This PC > Local Disk (C:) > Users > windos 10 > Downloads >
Search Downloads
New
Details
Home
Gallery
Munna - Person
Desktop
Downloads
Documents
Pictures
Music
Videos
TASK 7
munna-task8-cy
Screenshots
munna
This PC
Extract Compressed (Zipped) Folders
Files
70% complete
Copying 6 items from metasploitable-linux-2.... to metasploitable-linux-2....
70% complete
More details
Browse...
Next
Cancel
metasploitable-linux-2.0.0
Yesterday
Unconfirmed 675719.crdow
VMware-workstation-full-17
Unconfirmed 801349.crdow
Unconfirmed 79687.crdown
Last week
SHAIK MUNNA - TASK 8-CY
SHAIK MUNNA - TASK 8-CY
MaltegoSetup.JRE64.v4.6.0 3/15/2024 6:51 PM Application 187,246 KB
VirtualBox-7.0.14-161095-Win 3/15/2024 6:38 PM Application 108,557 KB
323 items 1 item selected 825 MB
ENG
12:11 PM
3/17/2024

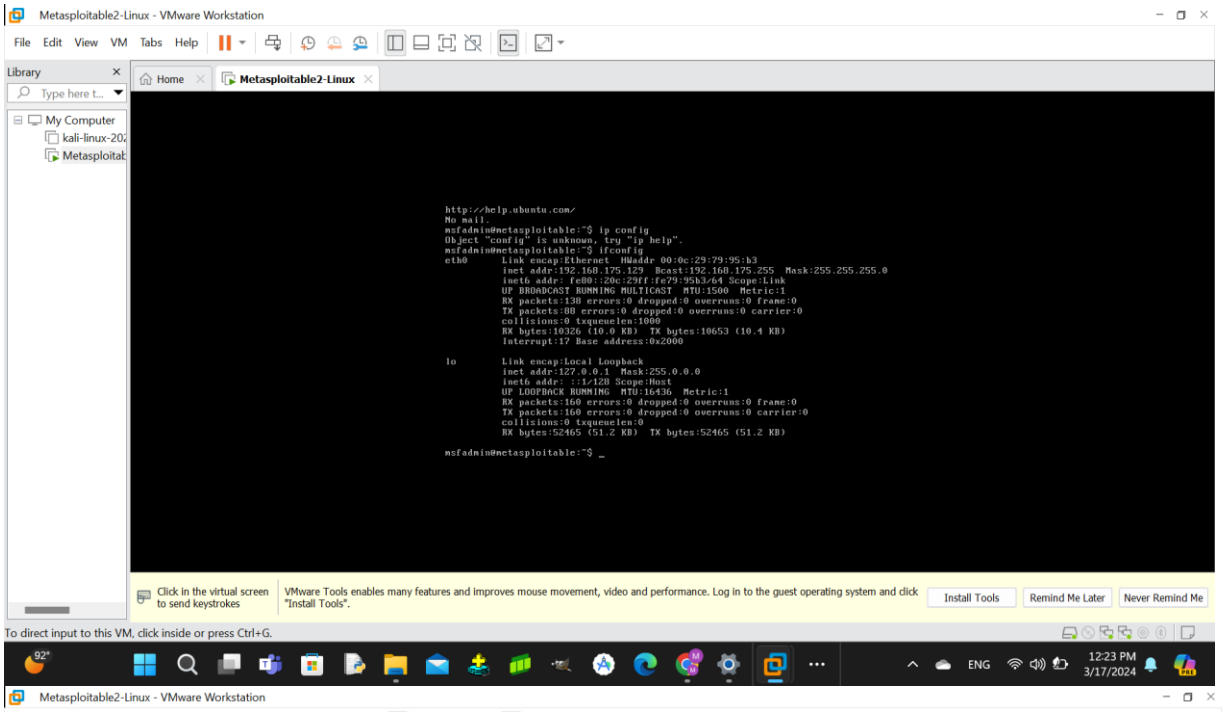

Metasploitable2-Linux
Downloads > metasploitable-linux-2.0.0 > Metasploitable2-Linux
Search Metasploitable2-Linux
New
Sort
View
Details
Home
Gallery
Munna - Person
Desktop
Downloads
Documents
Pictures
Music
Videos
TASK 7
munna-task8-cy
Screenshots
munna
This PC
Name
Date modified
Type
Size
Today
Metasploitable 3/17/2024 12:11 PM Virtual Machine Disk ... 1,880,512 KB
Metasploitable 3/17/2024 12:11 PM VMware snapshot m... 0 KB
Metasploitable 3/17/2024 12:11 PM VMware virtual machi... 3 KB
Metasploitable 3/17/2024 12:11 PM VMware Team Member 1 KB
Metasploitable 3/17/2024 12:10 PM VMware Virtual Mach... 9 KB
5 items
ENG
12:11 PM
3/17/2024

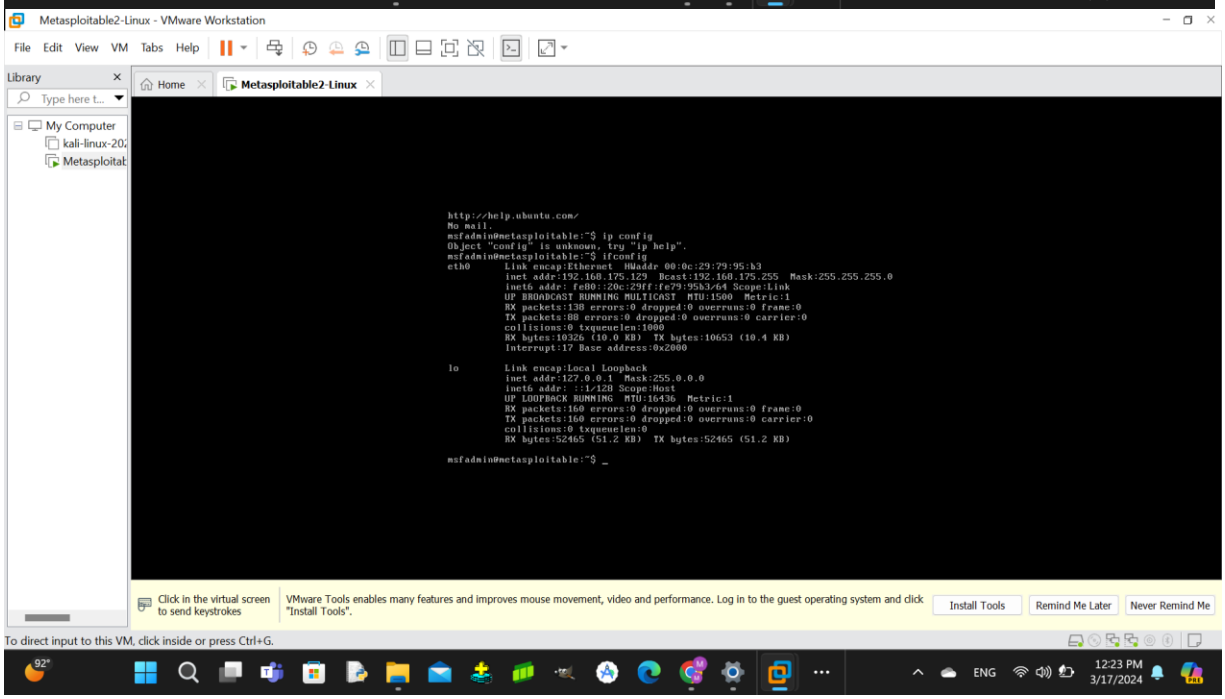

VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
kali-linux-202
Home
WORKSTATION PRO 17
Create a New Virtual Machine
Open a Virtual Machine
Connect to a Remote Server
vmware
ENG
12:12 PM
3/17/2024

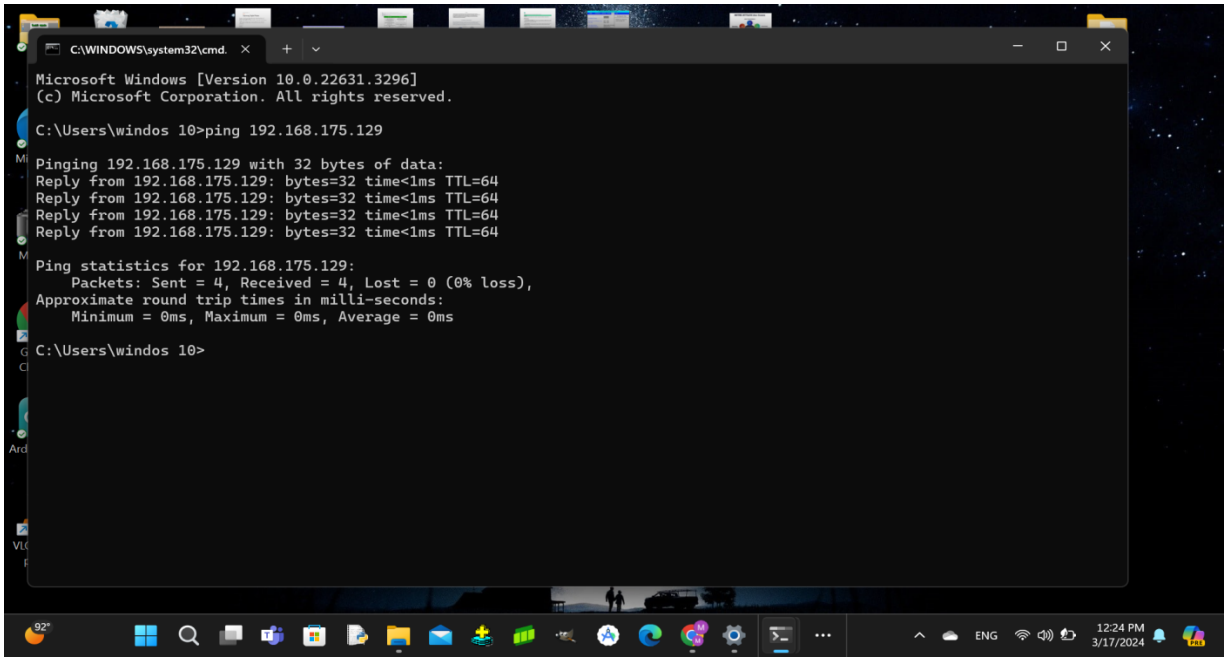

VMware Workstation
Open
meta... › Metasplo...
Search Metasploitable2-Linux
Organize
New folder
Home
Gallery
Munna - Persona
Desktop
Downloads
Documents
Pictures
Name
Date modified
Today
Metasploitable
3/17/2024 12:11 PM
File name: Metasploitable
All supported files
Open
Cancel
STATION PRO 17
Open a Virtual Machine
Connect to a Remote Server
vmware
ENG
12:12 PM
3/17/2024


Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
kali-linux-202
Metasploitabl
Home
Metasploitable2-Linux
Metasploitable2-Linux
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Devices
Memory 512 MB
Processors 1
Hard Disk (SCSI) 8 GB
CD/DVD (IDE) Auto detect
Network Adapter NAT
Network Adapter 2 Host-only
USB Controller Present
Display Auto detect
Description
This is Metasploitable2 (Linux)
Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.
The default login and password is msfadmin:msfadmin.
Never expose this VM to an untrusted network
Virtual Machine Details
State: Powered off
Configuration file: C:\Users\windos 10\Downloads\metasploitable-linux-2.0.0\Metasploitable2-Linux\Metasploitable.vmx
Hardware compatibility: Workstation 6.5-7.x virtual machine
Primary IP address: Network information is not available
ENG
12:13 PM
3/17/2024


Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
kali-linux-202
Metasploitabl
Home
Metasploitable2-Linux
* Starting deferred execution scheduler atd [OK]
* Starting periodic command scheduler crond [OK]
* Starting Tomcat servlet engine tomcat5.5 [OK]
* Starting web server apache2 [OK]
* Running local boot scripts (/etc/rc.local) [OK]
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login:
To direct input to this VM, click inside or press Ctrl+G.
ENG
12:14 PM
3/17/2024


Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
kali-linux-202
Metasploitat
Home
Metasploitable2-Linux
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip config
Object "config" is unknown, try "ip help".
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:79:95:b3
inet addr:192.168.175.129 Bcast:192.168.175.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe79:95b3/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:138 errors:0 dropped:0 overruns:0 frame:0
TX packets:88 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:10326 (10.0 KB) TX bytes:10653 (10.4 KB)
Interrupt:17 Base address:0x2000
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:160 errors:0 dropped:0 overruns:0 frame:0
TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:52465 (51.2 KB) TX bytes:52465 (51.2 KB)
msfadmin@metasploitable:~$ _
Click in the virtual screen to send keystrokes
VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".
Install Tools
Remind Me Later
Never Remind Me
To direct input to this VM, click inside or press Ctrl+G.
ENG
12:23 PM
3/17/2024


Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
kali-linux-202
Metasploitat
Home
Metasploitable2-Linux
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip config
Object "config" is unknown, try "ip help".
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:79:95:b3
inet addr:192.168.175.129 Bcast:192.168.175.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe79:95b3/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:138 errors:0 dropped:0 overruns:0 frame:0
TX packets:88 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:10326 (10.0 KB) TX bytes:10653 (10.4 KB)
Interrupt:17 Base address:0x2000
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:160 errors:0 dropped:0 overruns:0 frame:0
TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:52465 (51.2 KB) TX bytes:52465 (51.2 KB)
msfadmin@metasploitable:~$ _
Click in the virtual screen to send keystrokes
VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".
Install Tools
Remind Me Later
Never Remind Me
To direct input to this VM, click inside or press Ctrl+G.
ENG
12:23 PM
3/17/2024


C:\WINDOWS\system32\cmd.
Microsoft Windows [Version 10.0.22631.3296]
(c) Microsoft Corporation. All rights reserved.
C:\Users\windos 10>ping 192.168.175.129
Pinging 192.168.175.129 with 32 bytes of data:
Reply from 192.168.175.129: bytes=32 time<1ms TTL=64
Reply from 192.168.175.129: bytes=32 time<1ms TTL=64
Reply from 192.168.175.129: bytes=32 time<1ms TTL=64
Reply from 192.168.175.129: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.175.129:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\windos 10>
92°
ENG
12:24 PM
3/17/2024

Exploiting vsftpd 2.3.4 Backdoor Vulnerability

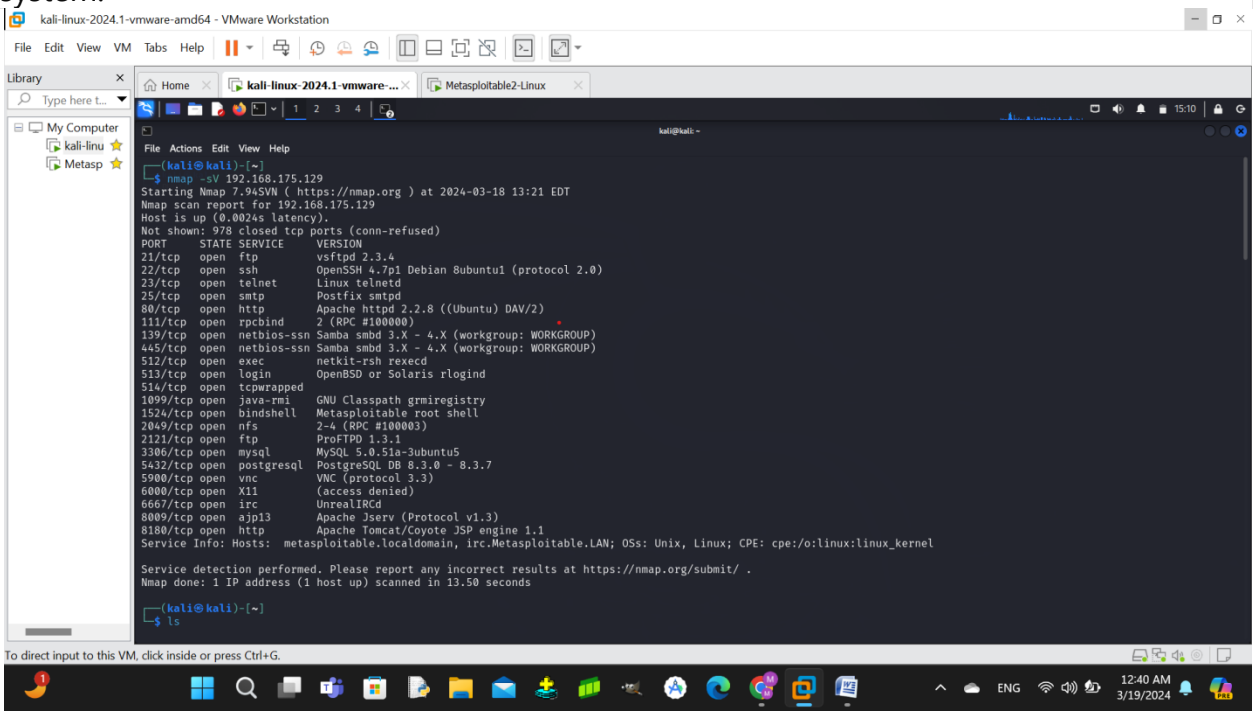
Introduction:

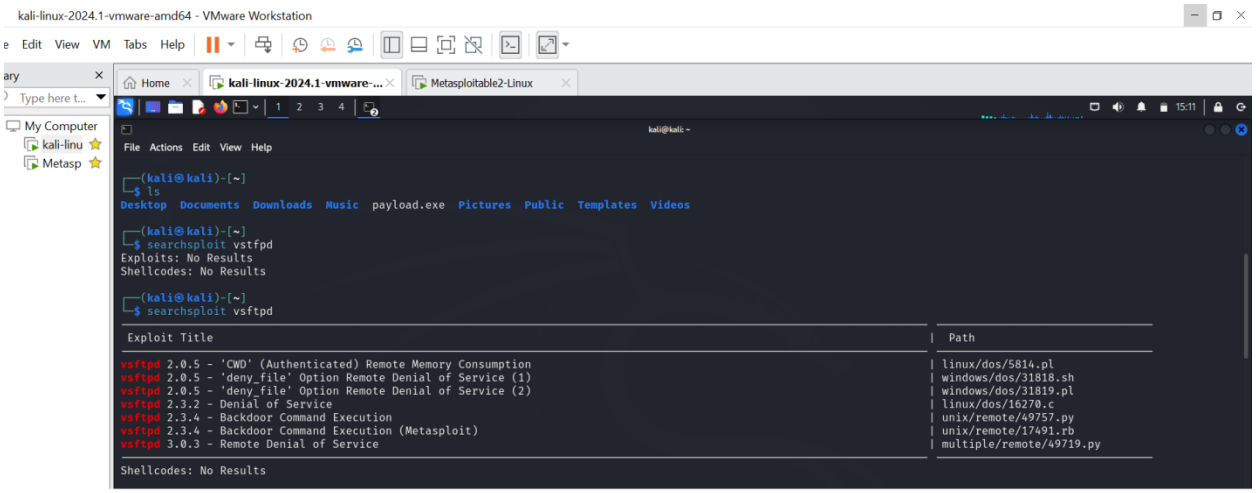
Briefly introduce the purpose of the document, which is to provide a step-by-step guide on exploiting the vsftpd 2.3.4 backdoor vulnerability to gain unauthorized access to a target system.

Step 1: Reconnaissance:

Explain the reconnaissance phase where you gather information about the target system using Nmap:

- Use Nmap to scan the target system (replace `192.168.175.129` with the target's IP address).
- Analyze the Nmap scan results to identify open ports and services running on the target system.

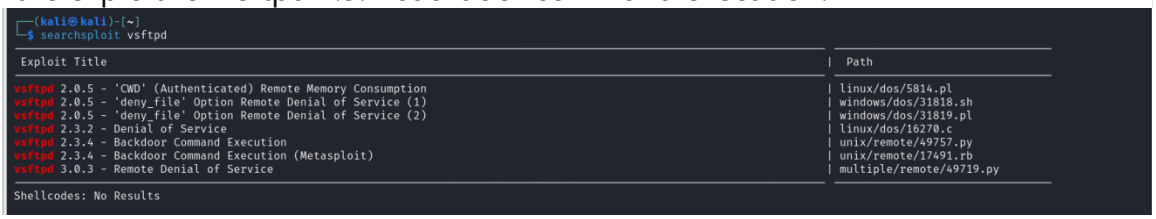




Step 2: Exploit Discovery:

Detail how you discovered the vsftpd 2.3.4 backdoor vulnerability and found an exploit using the **`searchsploit`** command:

- Use **`searchsploit`** to search for vsftpd exploits.
- Identify the exploit for vsftpd 2.3.4 backdoor command execution.



Step 3: Downloading the Exploit:

Explain how you downloaded the exploit script (**`49757.py`**) using **`searchsploit`**:

- Use **`searchsploit -m`** to download the exploit script.
- Specify the path where the exploit script is saved.

Step 4: Exploiting the Vulnerability:

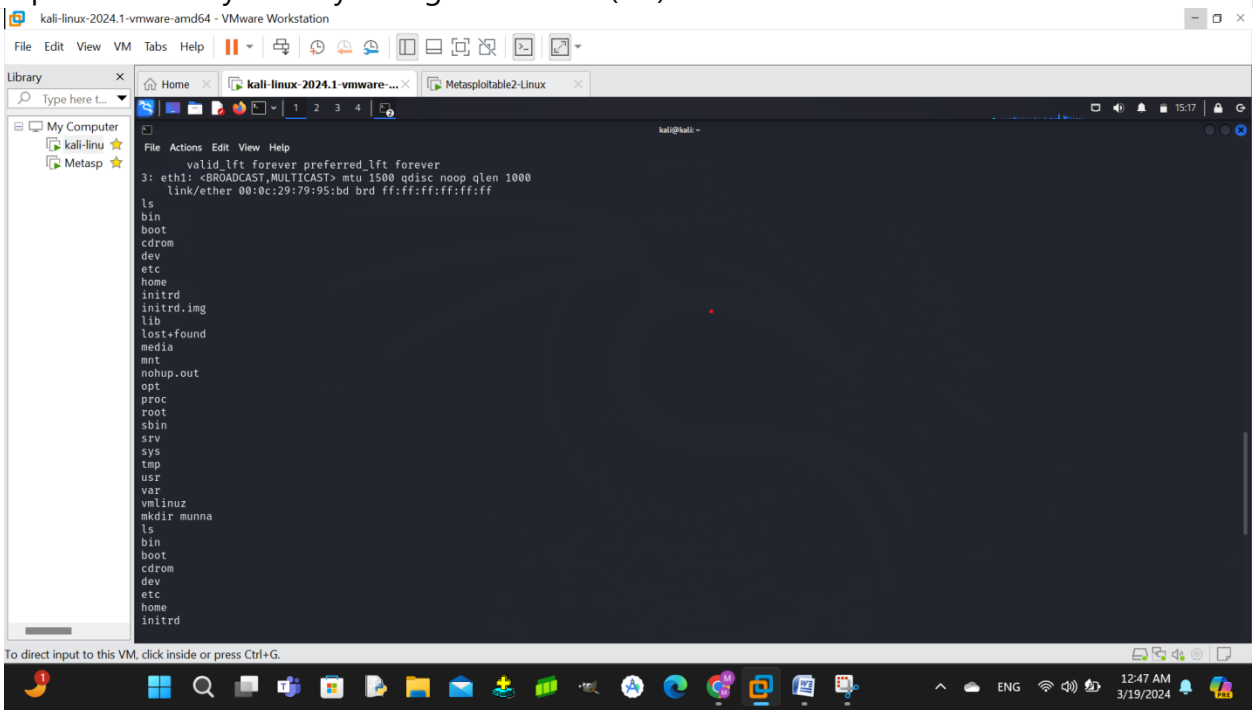
Describe the steps to exploit the vsftpd backdoor vulnerability and gain remote command execution:

- Run the exploit script (**`49757.py`**) with the target's IP address.
- Verify successful exploitation by executing commands (**`whoami`**, **`id`**, etc.) on the target system.

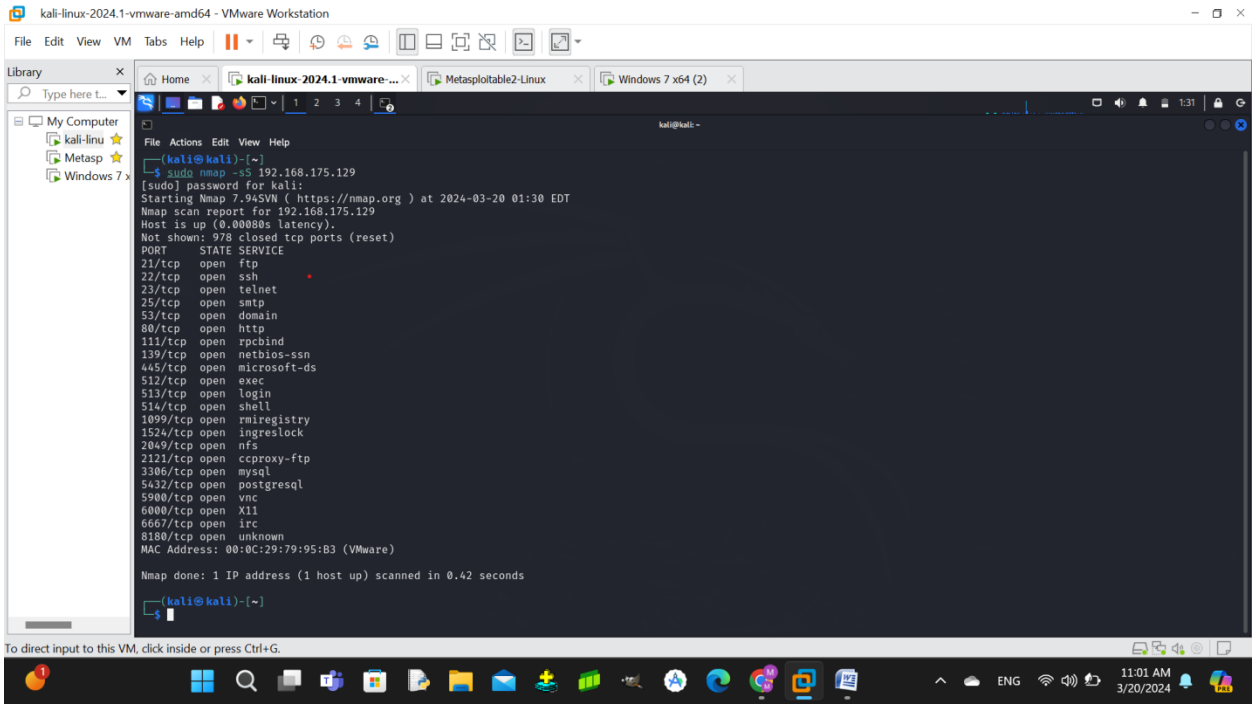
Step 5: Post-Exploitation:

Explain what actions you took after gaining access to the target system:

- Explore the filesystem by listing directories (**`ls`**).

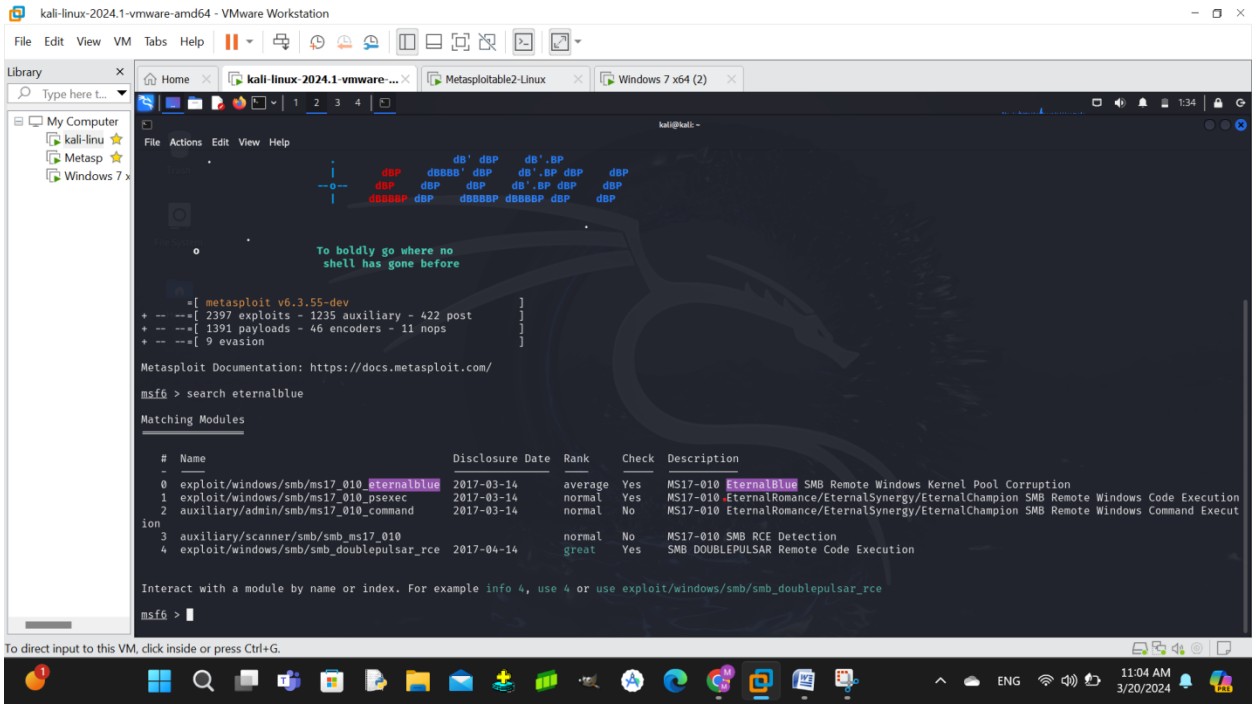


WINDOWS 7 EXPLOITATION

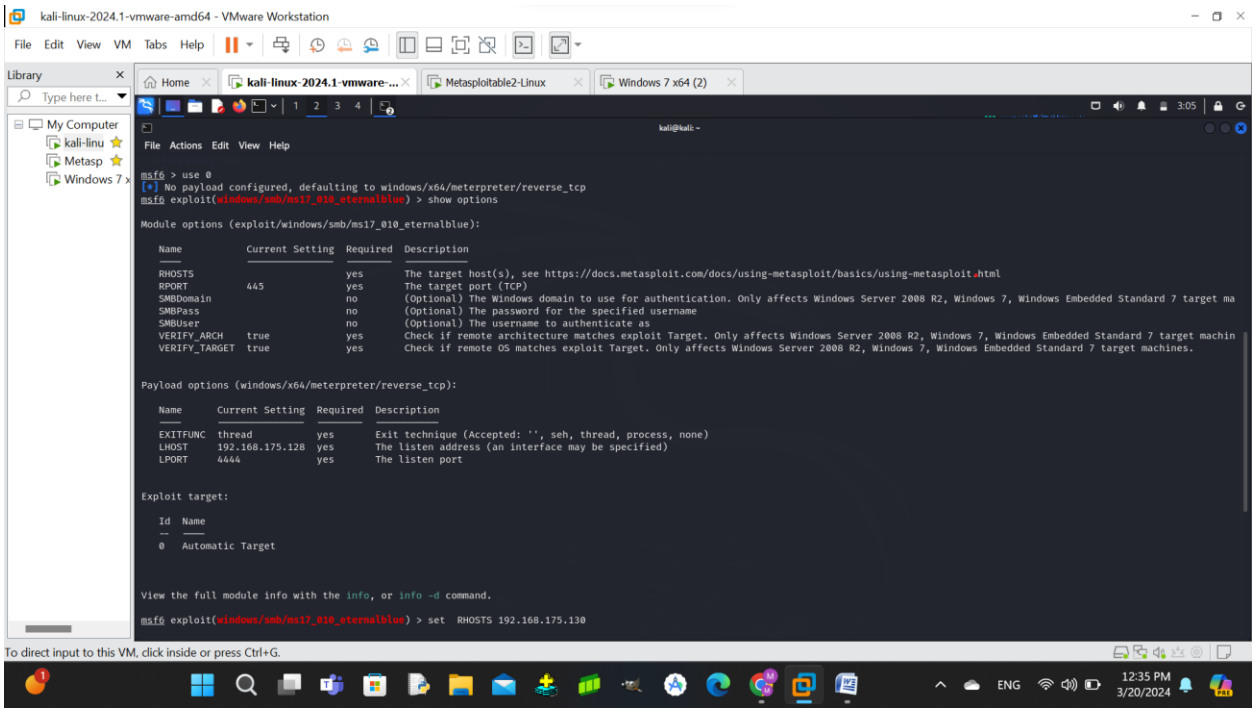


Start Metasploit Framework: Open a terminal and launch the Metasploit Framework by running the `msfconsole` command.

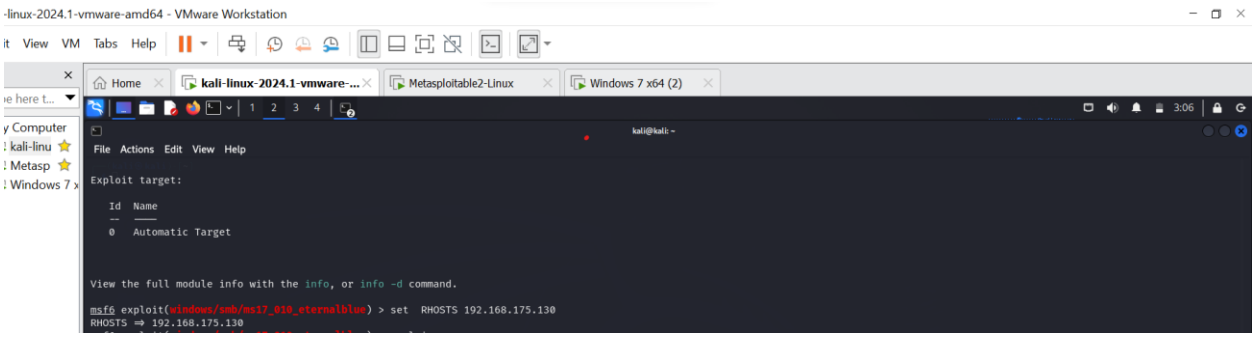
Search for MS17-010 Exploit: Use the `search` command to find the MS17-010 EternalBlue exploit module. In this case, you've already found it, but if you need to search again, you can use:

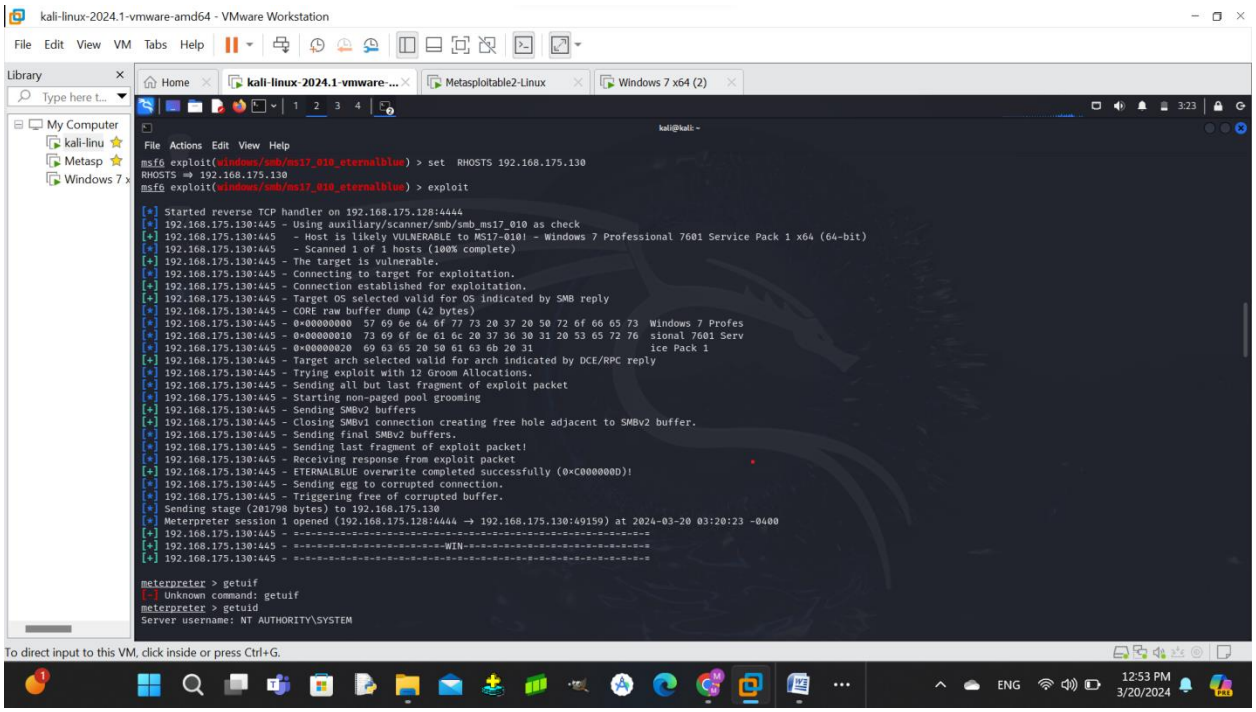


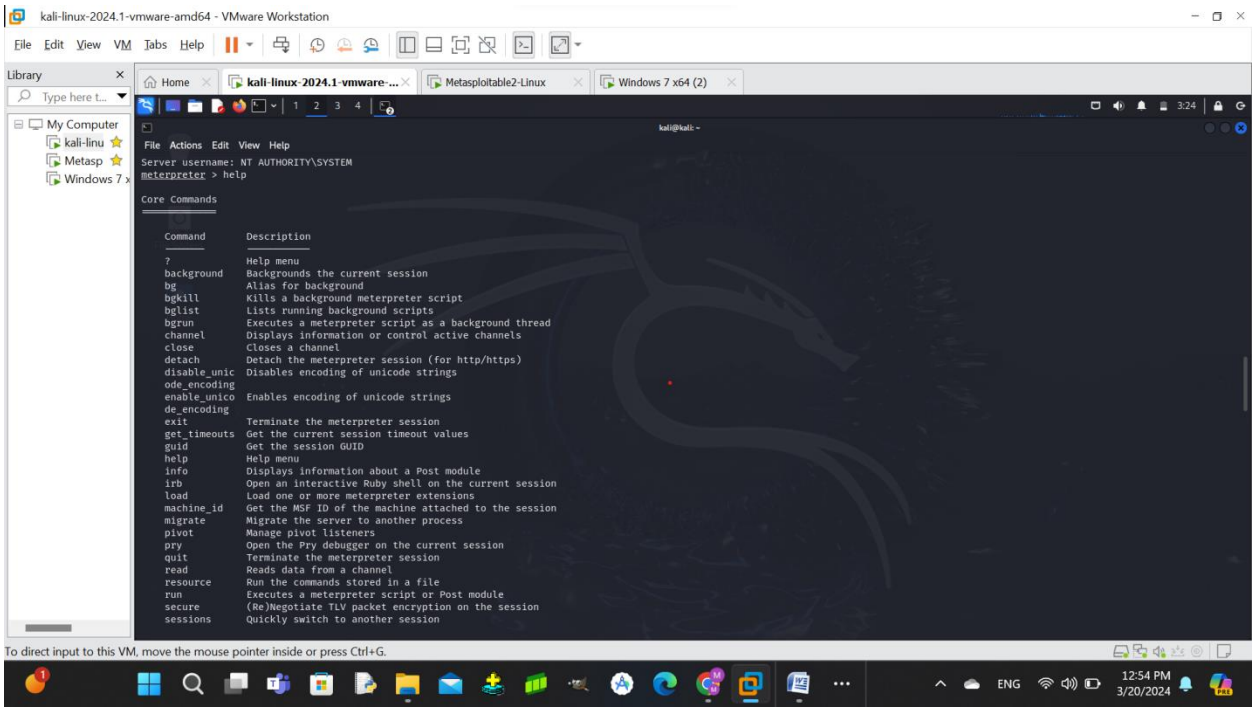
Select the EternalBlue Exploit: Identify the exploit module you want to use from the search results. In this case, it's **`exploit/windows/smb/ms17_010_eternalblue`**

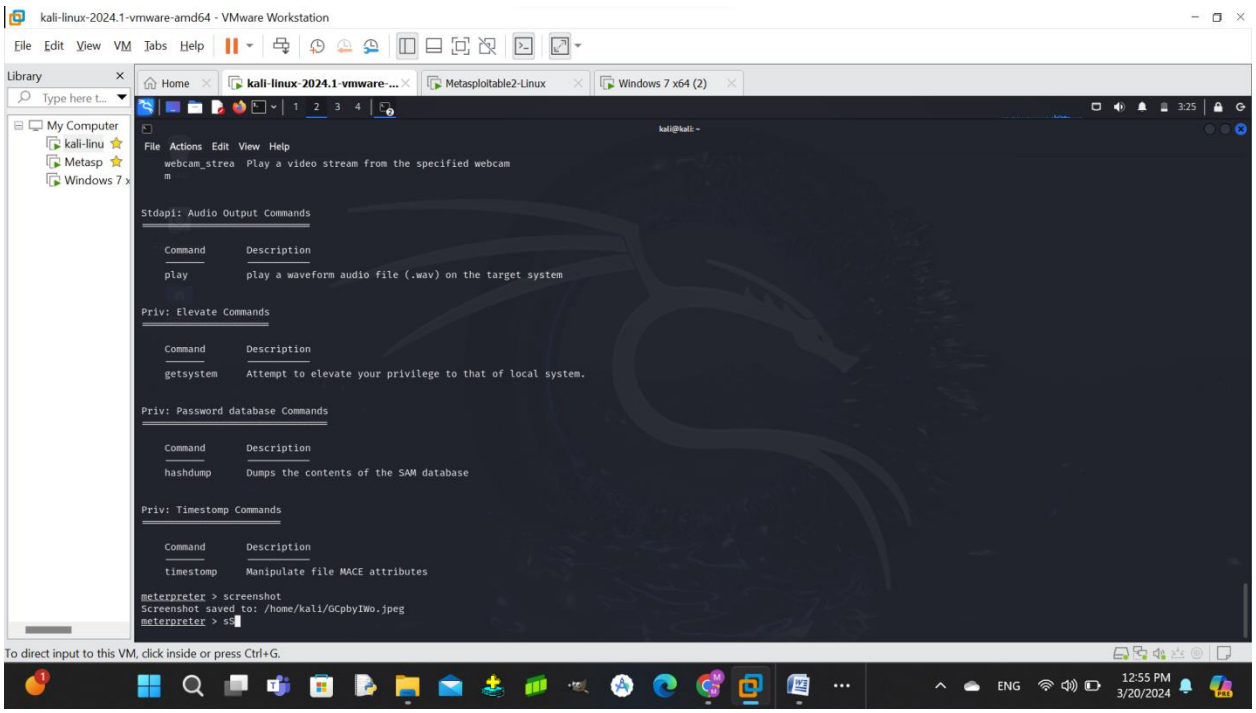


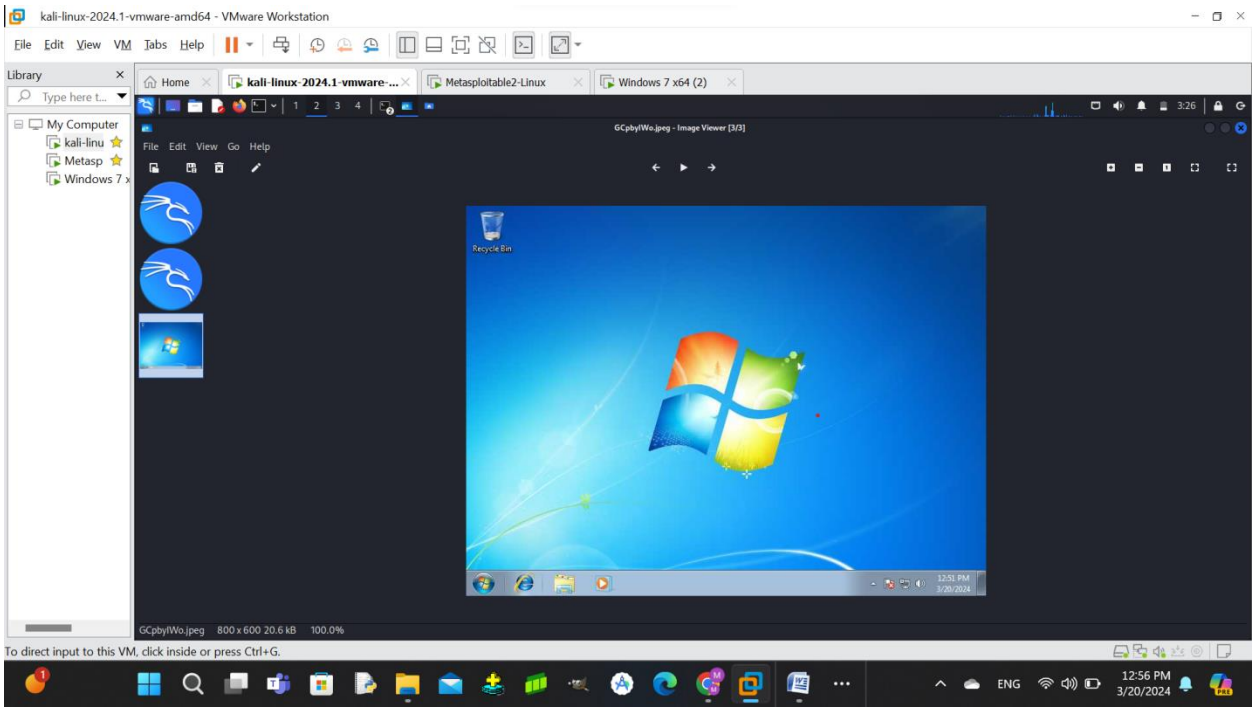
Set Exploit Options: Set the required options for the exploit module. At a minimum, you need to set the `RHOSTS` parameter to the IP address of the target Windows 7 machine.






kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
kali-linu
Metasp
Windows 7 x
Home
kali-linux-2024.1-vmware-...
Metasploitable2-Linux
Windows 7 x64 (2)
kali@kali: ~
File Actions Edit View Help
Server username: NT AUTHORITY\SYSTEM
meterpreter > help
Core Commands
Command Description
? Help menu
background Backgrounds the current session
bg Alias for background
bgkill Kills a background meterpreter script
bglist Lists running background scripts
bgrun Executes a meterpreter script as a background thread
channel Displays information or control active channels
close Closes a channel
detach Detach the meterpreter session (for http/https)
disable_unic ode_encoding Disables encoding of unicode strings
enable_unico de_encoding Enables encoding of unicode strings
exit Terminate the meterpreter session
get_timeouts Get the current session timeout values
guid Get the session GUID
help Help menu
info Displays information about a Post module
irb Open an interactive Ruby shell on the current session
load Load one or more meterpreter extensions
machine_id Get the MSF ID of the machine attached to the session
migrate Migrate the server to another process
pivot Manage pivot listeners
pry Open the Pry debugger on the current session
quit Terminate the meterpreter session
read Reads data from a channel
resource Run the commands stored in a file
run Executes a meterpreter script or Post module
secure (Re)Negotiate TLV packet encryption on the session
sessions Quickly switch to another session
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG
12:54 PM
3/20/2024


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
kali-linu
Metasp
Windows 7 x
Home
kali-linux-2024.1-vmware-...
Metasploitable2-Linux
Windows 7 x64 (2)
kali@kali: ~
File Actions Edit View Help
webcam_strea m Play a video stream from the specified webcam
Stdapi: Audio Output Commands
Command Description
play play a waveform audio file (.wav) on the target system
Priv: Elevate Commands
Command Description
getsystem Attempt to elevate your privilege to that of local system.
Priv: Password database Commands
Command Description
hashdump Dumps the contents of the SAM database
Priv: Timestomp Commands
Command Description
timestomp Manipulate file MACE attributes
meterpreter > screenshot
Screenshot saved to: /home/kali/GCpbyIWo.jpeg
meterpreter > s
To direct input to this VM, click inside or press Ctrl+G.
ENG
12:55 PM
3/20/2024


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
kali-linu
Metasp
Windows 7 x
Home
kali-linux-2024.1-vmware-...
Metasploitable2-Linux
Windows 7 x64 (2)
GCpbylWo.jpeg - Image Viewer [3/3]
File Edit View Go Help
Recycle Bin
GCpbylWo.jpeg 800 x 600 20.6 kB 100.0%
To direct input to this VM, click inside or press Ctrl+G.
ENG
12:56 PM
3/20/2024

ENUMERATION

Enumeration in the context of computer security refers to the process of gathering information about a target system or network to identify potential vulnerabilities or weaknesses. It involves systematically querying various services, protocols, and resources to gather valuable information that can be used in further stages of an attack or for defensive purposes. Here's an overview of enumeration:

Service Enumeration: This involves identifying what services are running on the target system, including open ports and listening services. Tools like Nmap, Masscan, and Unicornscan are commonly used for this purpose.

Version Enumeration: Once services are identified, version enumeration involves determining the specific version numbers of the software running on those services. This information can help identify known vulnerabilities associated with particular software versions.

User Enumeration: User enumeration involves identifying valid usernames on the target system. This can be done through various methods such as querying user accounts, enumerating through user directories, or attempting to log in with common or default usernames.

File and Share Enumeration: This involves identifying accessible files, directories, and network shares on the target system. Enumerating file shares can reveal sensitive data or configuration information that may be useful for an attacker.

Network Enumeration: Network enumeration involves discovering information about the target network, including network topology, devices, and configurations. This can include identifying routers, switches, firewalls, and other network infrastructure components.

DNS Enumeration: DNS enumeration involves querying DNS servers to gather information about the target domain, such as hostnames, IP addresses, mail servers, and other DNS records. This information can be useful for mapping out the target network or identifying potential entry points.

Enumeration of Vulnerabilities: Once information about the target system has been gathered, enumeration may also involve identifying potential vulnerabilities or misconfigurations that could be exploited. This can include searching for known vulnerabilities associated with specific software versions or configurations.

Enumerating Web Applications: For web applications, enumeration involves identifying available web pages, directories, and resources. This can include techniques such as directory brute-forcing, spidering, or analyzing server responses for hidden or sensitive information.

Meterpreter Basics

Since the Meterpreter provides a whole new environment, we will cover some of the basic Meterpreter commands to get you started and help familiarize you with this most powerful tool. Throughout this course, almost every available Meterpreter command is covered. For those that aren't covered, experimentation is the key to successful learning

Command	Description
`?`	Displays the Meterpreter help menu.
`background`	Backgrounds the current session.
`cat`	Displays the content of a file.
`cd`	Changes the current working directory on the target host.
`clearev`	Clears the Application, System, and Security logs.
`download`	Downloads a file from the remote machine.
`edit`	Opens a file located on the target host.
`execute`	Runs a command on the target.
`getuid`	Displays the user that Meterpreter is running as.
`hashdump`	Dumps the contents of the SAM database.
`idletime`	Displays the number of seconds that the user has been idle.
`ipconfig`	Displays the network interfaces and addresses on the remote machine.
`lpwd`	Displays the local working directory.
`lcd`	Changes the local working directory.
`ls`	Lists the files in the current remote directory.
`migrate`	Migrates to another process on the victim.
`ps`	Displays a list of running processes on the target.
`resource`	Executes Meterpreter instructions located inside a text file.
`search`	Locates specific files on the target host.
`shell`	Presents a standard shell on the target system.
`upload`	Uploads a file to the remote machine.
`webcam_list`	Displays currently available webcams on the target host.

Command	Description
`webcam_snap`	Grabs a picture from a connected webcam on the target system.