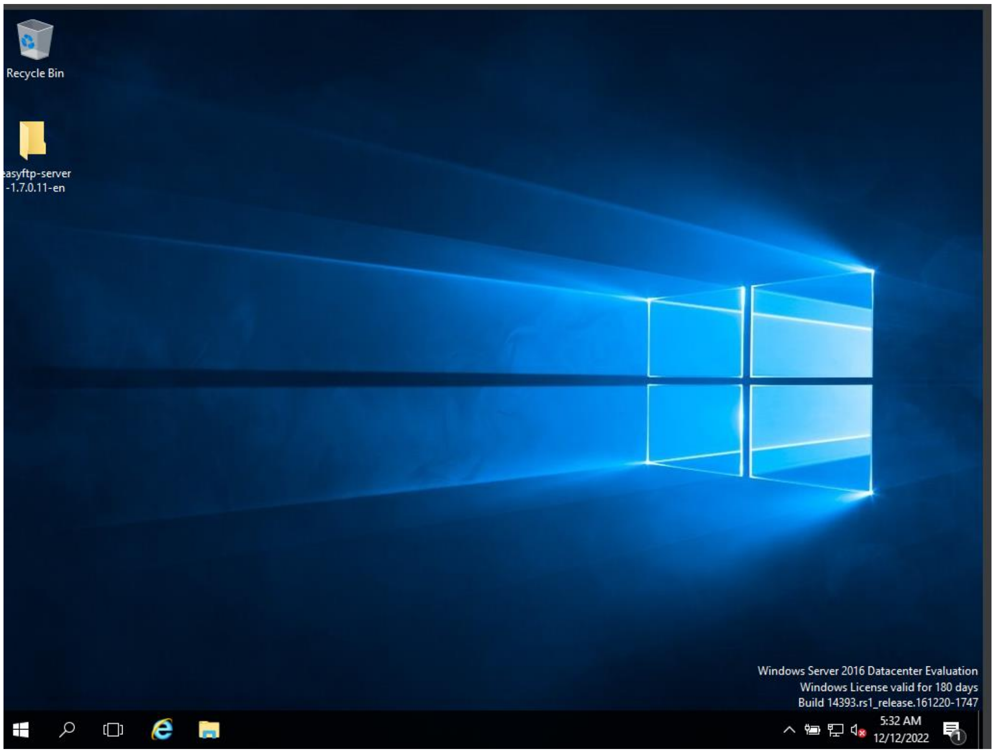
Lab 6 - Attacking Windows Servers, Part 1 Taking Control of a Server with Armitage

Name: Hamza Abdellah Ahmed

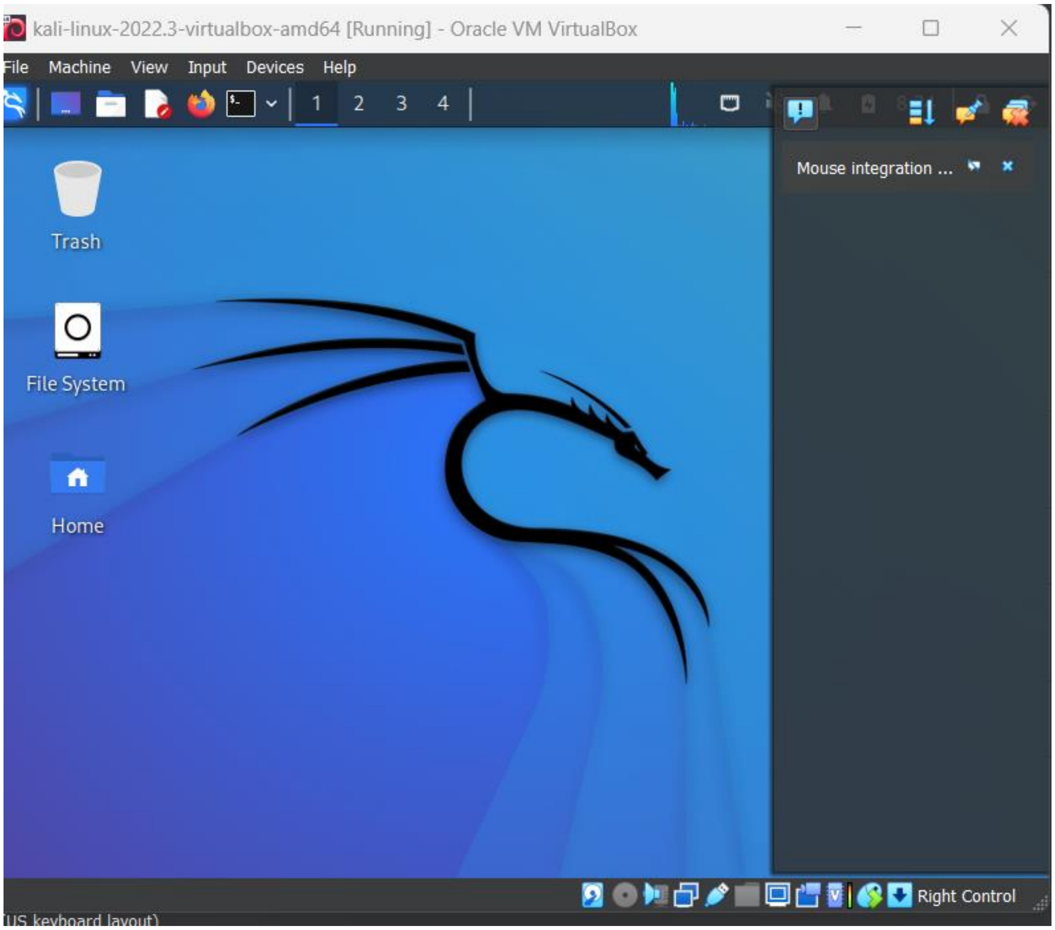
ID :18P7231

Shown are the VMs installed:



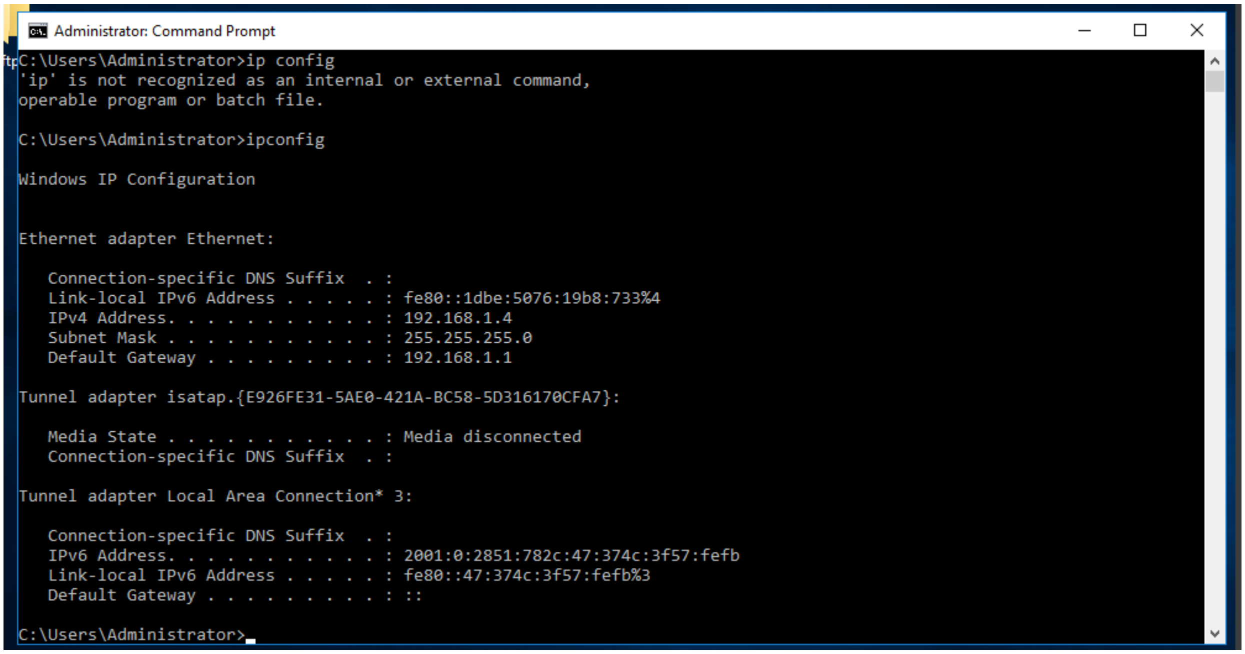
Windows Server 2016 Datacenter Evaluation
Windows License valid for 180 days
Build 14393.rs1_release.161220-1747

Kali Linux:



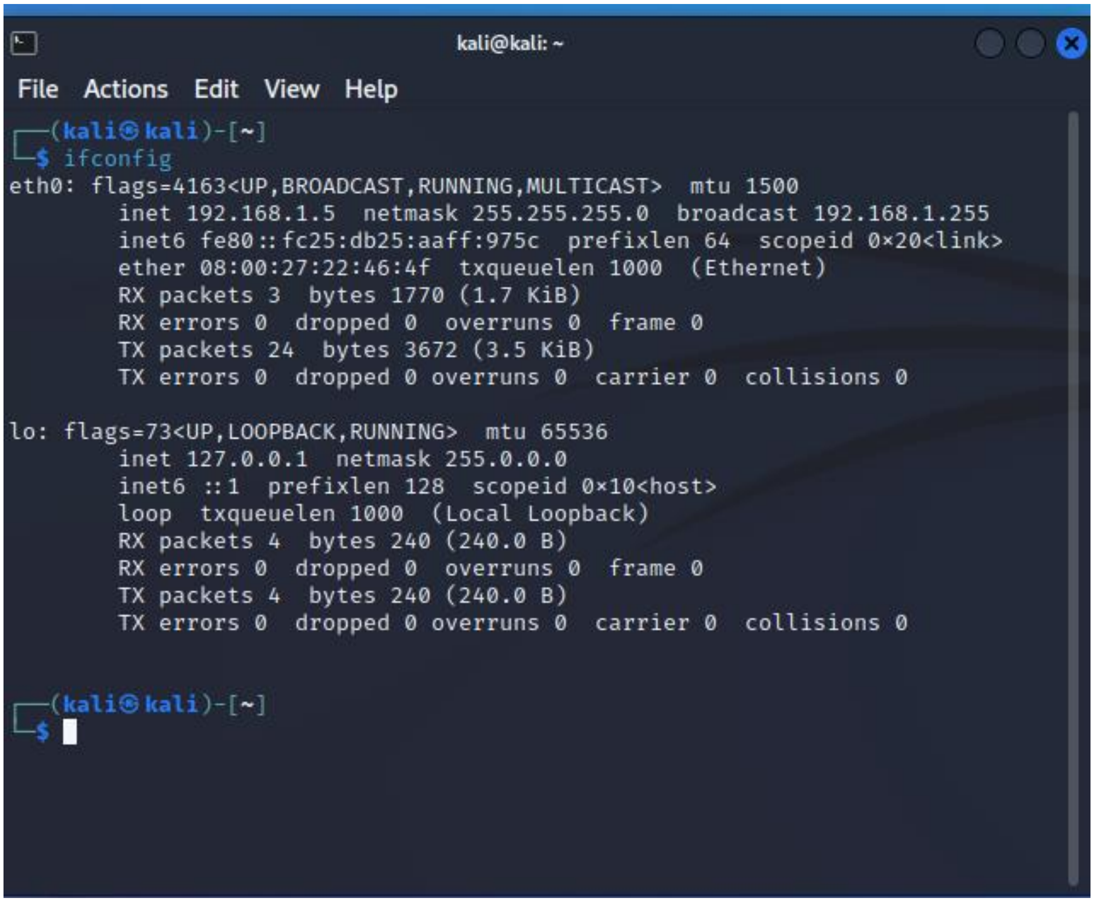
kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
1
2
3
4
Mouse integration ...
Trash
File System
Home
Right Control
(US keyboard layout)

Windows Server:



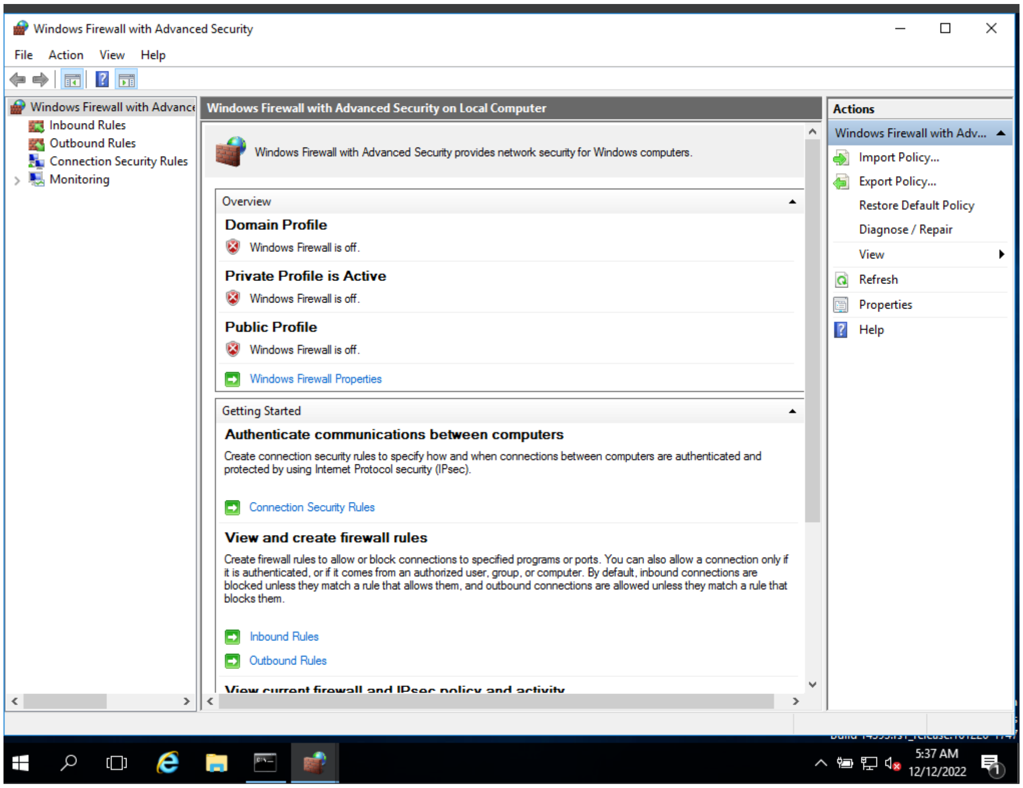
```
C:\Users\Administrator>ip config
'ip' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1dbe:5076:19b8:733%4
   IPv4 Address. . . . . . . . . . . : 192.168.1.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.{E926FE31-5AE0-421A-BC58-5D316170CFA7}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 3:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:2851:782c:47:374c:3f57:fefb
   Link-local IPv6 Address . . . . . : fe80::47:374c:3f57:fefb%3
   Default Gateway . . . . . . . . . : ::

C:\Users\Administrator>
```

Kali Linux:



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.5  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::fc25:db25:aaff:975c  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
        RX packets 3  bytes 1770 (1.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 3672 (3.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ 
```

Firewall off



Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

Windows Firewall is off.

Private Profile is Active

Windows Firewall is off.

Public Profile

Windows Firewall is off.

Windows Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

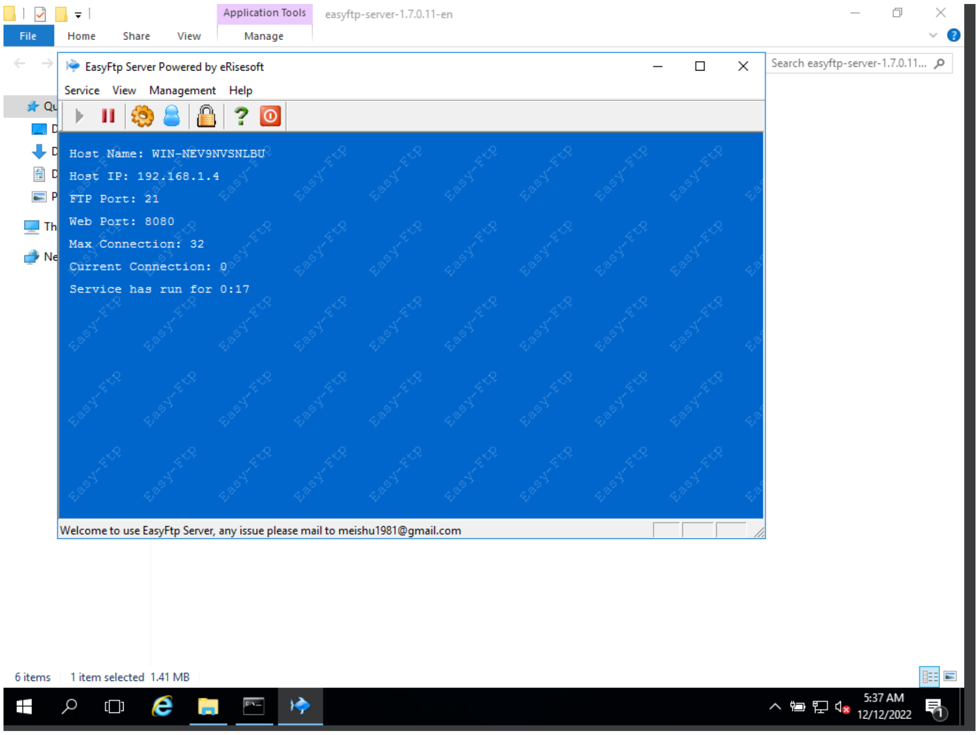
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

Inbound Rules

Outbound Rules

View current firewall and IPsec policy and activity

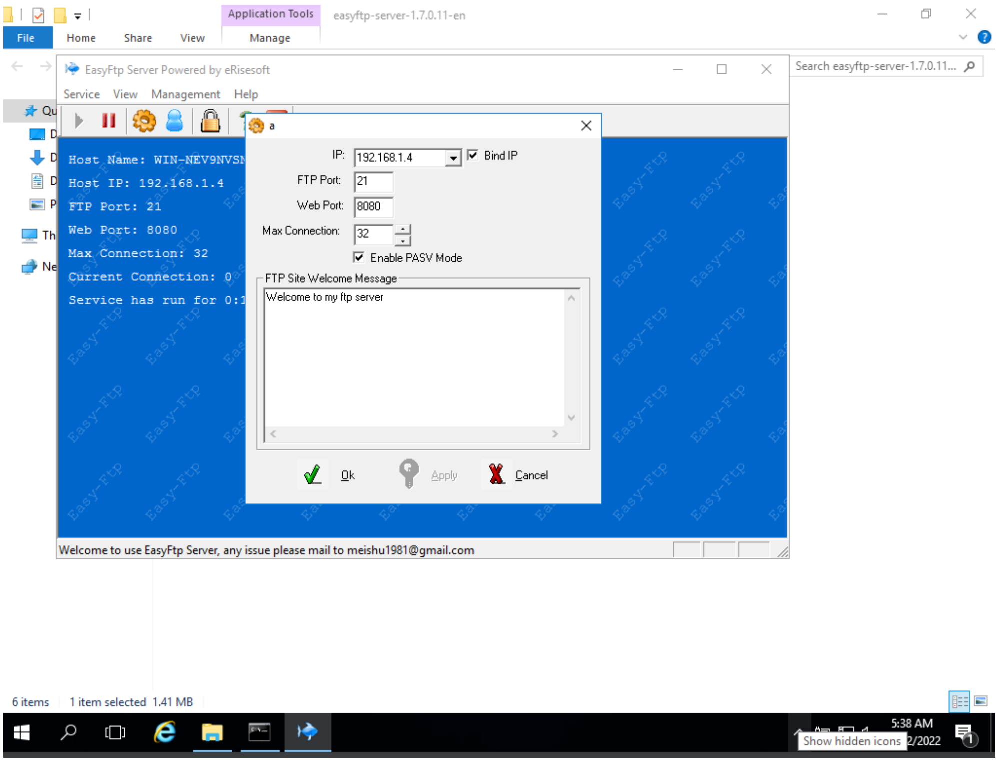
Installing EasyFTP


Application Tools
easyftp-server-1.7.0.11-en
File Home Share View Manage
Search easyftp-server-1.7.0.11...
EasyFtp Server Powered by eRisesoft
Service View Management Help
6 items 1 item selected 1.41 MB
5:37 AM
12/12/2022

```
Host Name: WIN-NEV9NVSNLBU
Host IP: 192.168.1.4
FTP Port: 21
Web Port: 8080
Max Connection: 32
Current Connection: 0
Service has run for 0:17
```

Welcome to use EasyFtp Server, any issue please mail to meishu1981@gmail.com

Binding IP



```
Host Name: WIN-NEV9NVSN
Host IP: 192.168.1.4
FTP Port: 21
Web Port: 8080
Max Connection: 32
Current Connection: 0
Service has run for 0:1
```

IP: 192.168.1.4 ☑ Bind IP

FTP Port: 21

Web Port: 8080

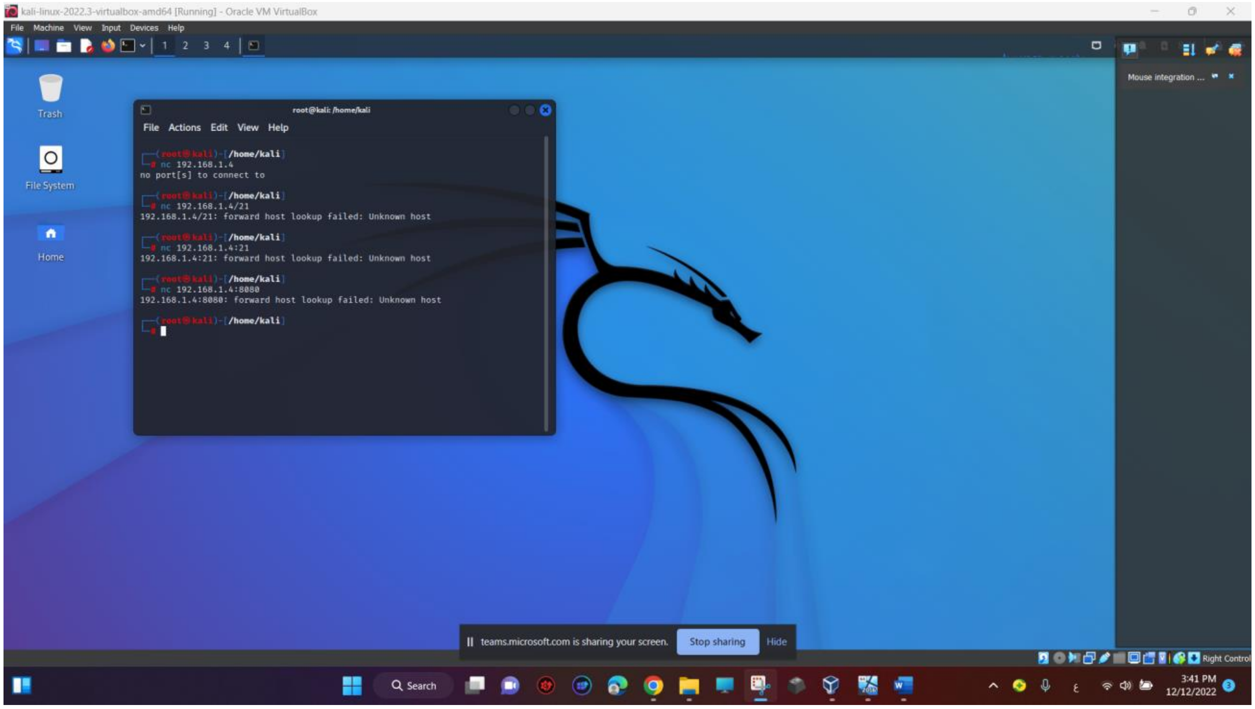
Max Connection: 32

☑ Enable PASV Mode

FTP Site Welcome Message: Welcome to my ftp server

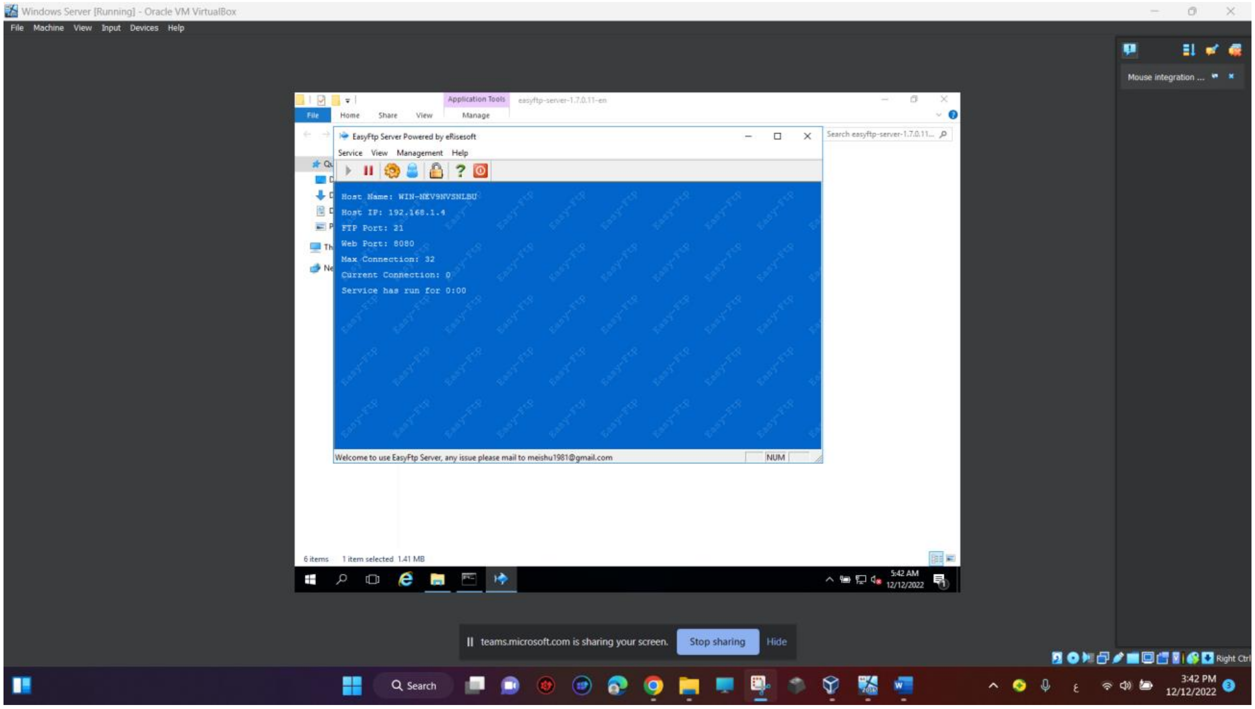
Welcome to use EasyFtp Server, any issue please mail to meishu1981@gmail.com

Executing the given command failed. given error: no port[s] to connect to.



```
┌──(root㉿kali)-[/home/kali]
└─# nc 192.168.1.4
no port[s] to connect to

┌──(root㉿kali)-[/home/kali]
└─# nc 192.168.1.4/21
192.168.1.4/21: forward host lookup failed: Unknown host

┌──(root㉿kali)-[/home/kali]
└─# nc 192.168.1.4:21
192.168.1.4:21: forward host lookup failed: Unknown host

┌──(root㉿kali)-[/home/kali]
└─# nc 192.168.1.4:8080
192.168.1.4:8080: forward host lookup failed: Unknown host

┌──(root㉿kali)-[/home/kali]
└─# 
```

We will perform a restart of EasyFTP server and try again.

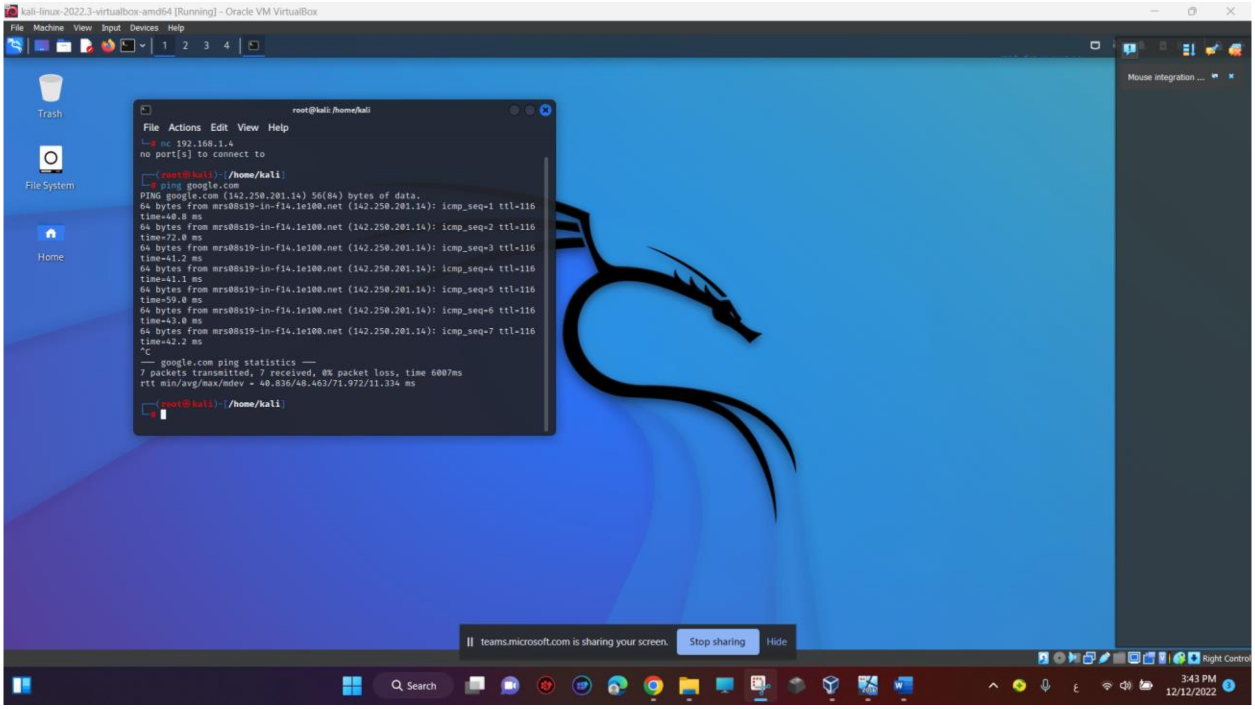

Windows Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Application Tools
easyftp-server-1.7.0.11-en
File Home Share View Manage
EasyFtp Server Powered by eRisesoft
Service View Management Help
Mouse integration ...
teams.microsoft.com is sharing your screen. Stop sharing Hide

```
Host Name: WIN-NEV9NVSNLBU
Host IP: 192.168.1.4
FTP Port: 21
Web Port: 8080
Max Connection: 32
Current Connection: 0
Service has run for 0:00
```

Welcome to use EasyFtp Server, any issue please mail to meishu1981@gmail.com

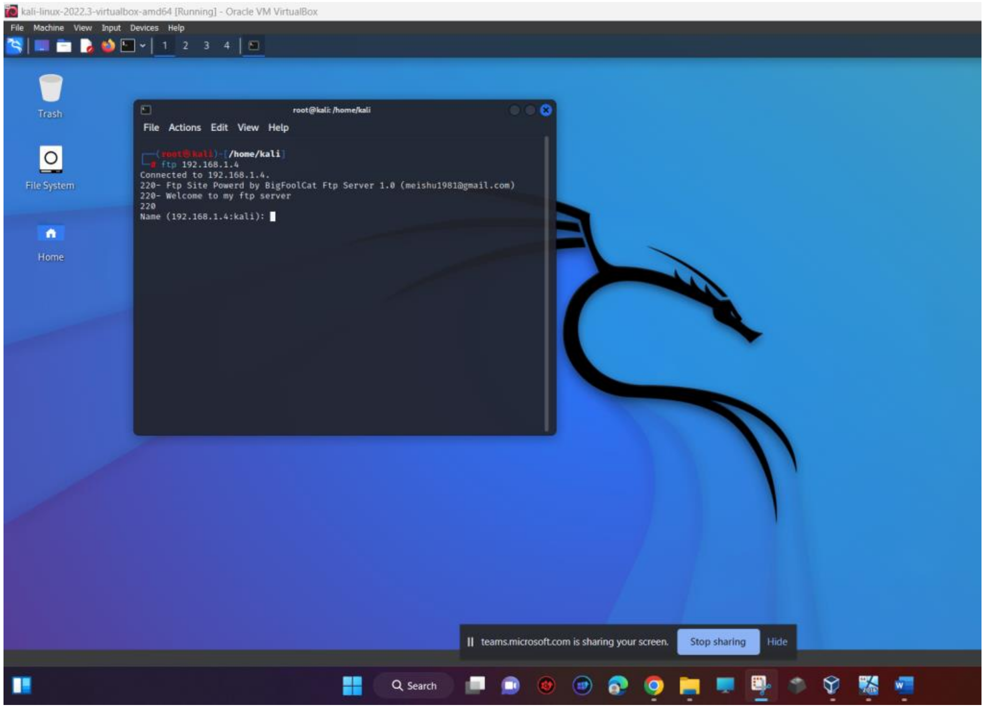
6 items 1 item selected 1.41 MB

Testing nc 192.168.1.4 did not work again.


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
root@kali: /home/kali
File Actions Edit View Help
Mouse integration ...
teams.microsoft.com is sharing your screen. Stop sharing Hide

```
└─# nc 192.168.1.4
no port[s] to connect to

┌──(root㉿kali)-[/home/kali]
└─# ping google.com
PING google.com (142.250.201.14) 56(84) bytes of data.
64 bytes from mrs08s19-in-f14.1e100.net (142.250.201.14): icmp_seq=1 ttl=116
time=40.8 ms
64 bytes from mrs08s19-in-f14.1e100.net (142.250.201.14): icmp_seq=2 ttl=116
time=72.0 ms
64 bytes from mrs08s19-in-f14.1e100.net (142.250.201.14): icmp_seq=3 ttl=116
time=41.2 ms
64 bytes from mrs08s19-in-f14.1e100.net (142.250.201.14): icmp_seq=4 ttl=116
time=41.1 ms
64 bytes from mrs08s19-in-f14.1e100.net (142.250.201.14): icmp_seq=5 ttl=116
time=59.0 ms
64 bytes from mrs08s19-in-f14.1e100.net (142.250.201.14): icmp_seq=6 ttl=116
time=43.0 ms
64 bytes from mrs08s19-in-f14.1e100.net (142.250.201.14): icmp_seq=7 ttl=116
time=42.2 ms
^C
--- google.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6007ms
rtt min/avg/max/mdev = 40.836/48.463/71.972/11.334 ms

┌──(root㉿kali)-[/home/kali]
└─# 
```

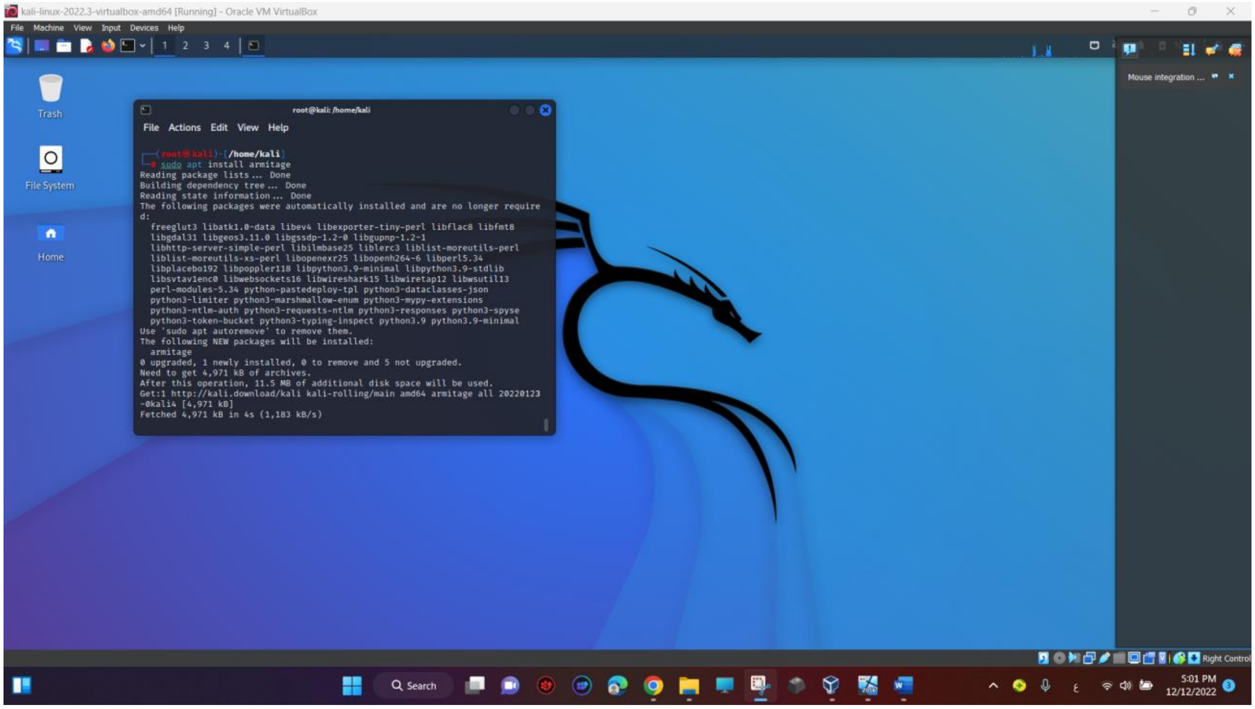
I tried different approach by using the command “ftp 192.168.1.89” instead of “nc 192.168.1.89” and it has successfully connected:



kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
root@kali: /home/kali
File Actions Edit View Help
teams.microsoft.com is sharing your screen.
Stop sharing
Hide
Search

```
┌──(root㉿kali)-[/home/kali]
└─# ftp 192.168.1.4
Connected to 192.168.1.4.
220- Ftp Site Powerd by BigFoolCat Ftp Server 1.0 (meishu1981@gmail.com)
220- Welcome to my ftp server
220
Name (192.168.1.4:kali): 
```

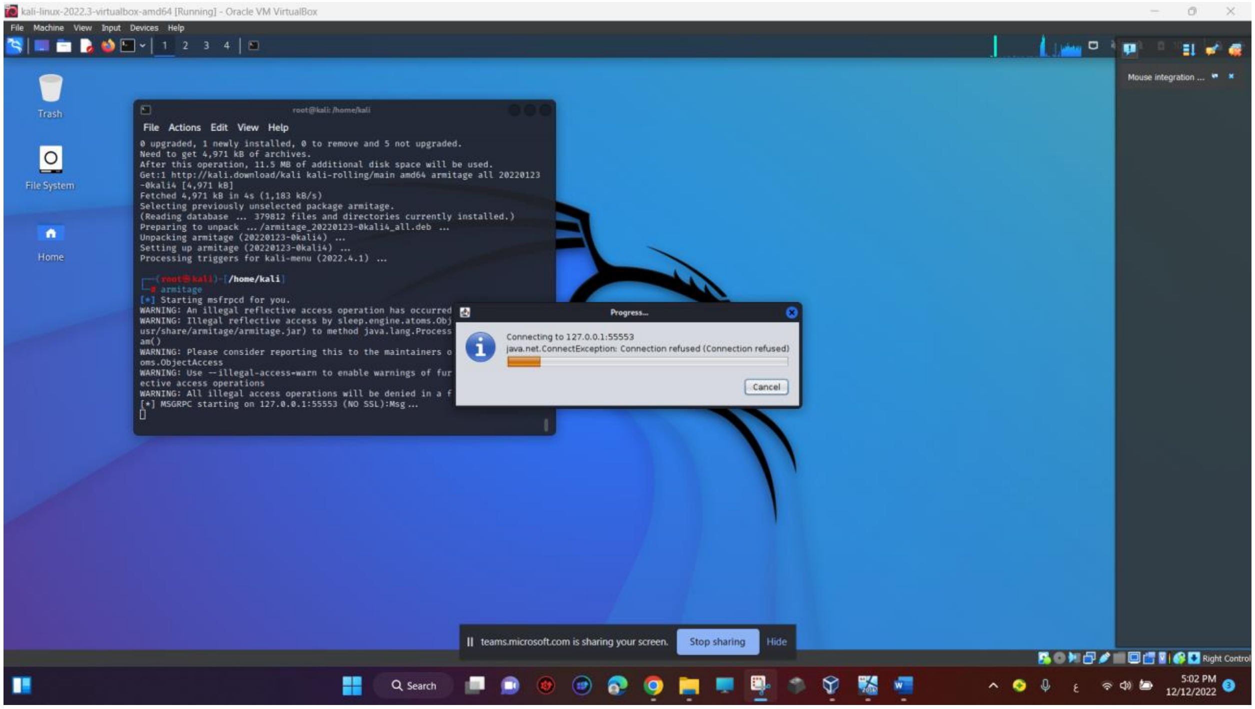
By default, Armitage was not installed



kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
root@kali: /home/kali
File Actions Edit View Help
Mouse integration ...
Right Control
Search
5:01 PM
12/12/2022

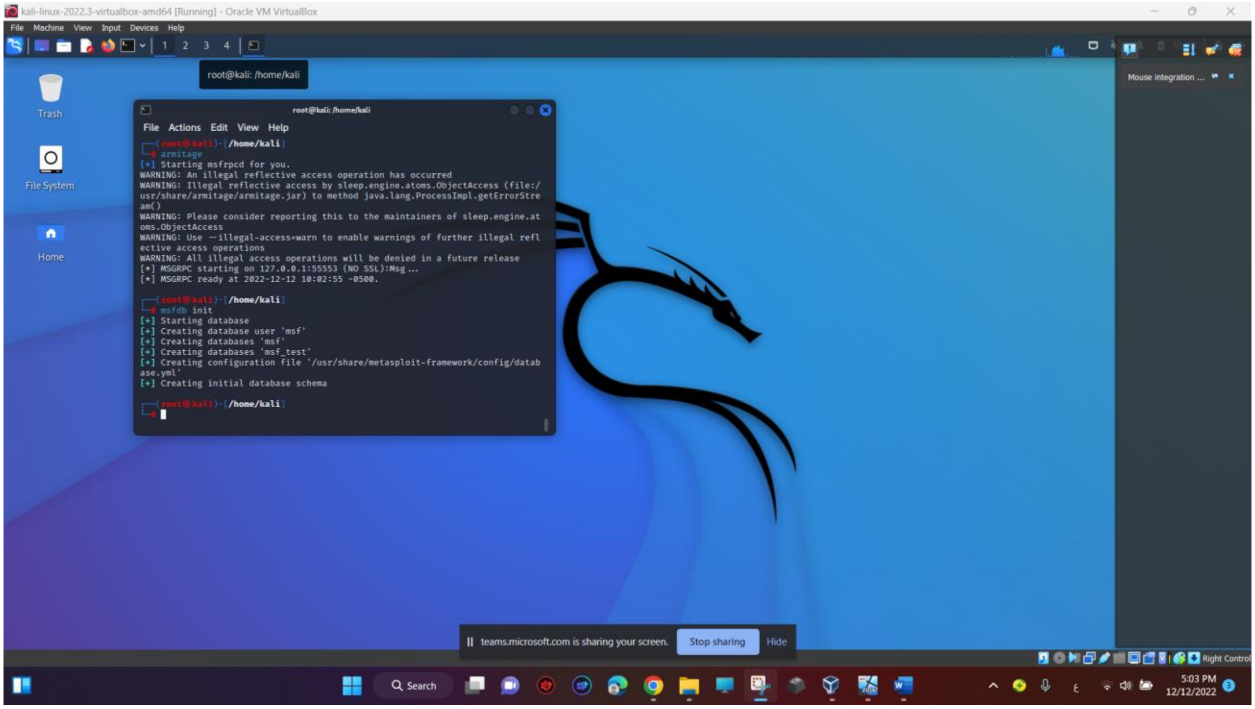
```
┌──(root㉿kali)-[/home/kali]
└─# sudo apt install armitage
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer require
d:
  freeglut3 libatk1.0-data libev4 libexporter-tiny-perl libflac8 libfmt8
  libgdal31 libgeos3.11.0 libgssdp-1.2-0 libgupnp-1.2-1
  libhttp-server-simple-perl libilmbase25 liblerc3 liblist-moreutils-perl
  liblist-moreutils-xs-perl libopenexr25 libopenh264-6 libperl5.34
  libplacebo192 libpoppler118 libpython3.9-minimal libpython3.9-stdlib
  libsvtav1enc0 libwebsockets16 libwireshark15 libwiretap12 libwsutil13
  perl-modules-5.34 python-pastedeploy-tpl python3-dataclasses-json
  python3-limiter python3-marshmallow-enum python3-mypy-extensions
  python3-ntlm-auth python3-requests-ntlm python3-responses python3-spyse
  python3-token-bucket python3-typing-inspect python3.9 python3.9-minimal
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  armitage
0 upgraded, 1 newly installed, 0 to remove and 5 not upgraded.
Need to get 4,971 kB of archives.
After this operation, 11.5 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 armitage all 20220123
-0kali4 [4,971 kB]
Fetched 4,971 kB in 4s (1,183 kB/s)
```

I installed it using “sudo apt install Armitage”


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
root@kali: /home/kali
File Actions Edit View Help
Progress...
Cancel
Mouse integration ...
teams.microsoft.com is sharing your screen.
Stop sharing
Hide
Right Control
Search
5:02 PM
12/12/2022

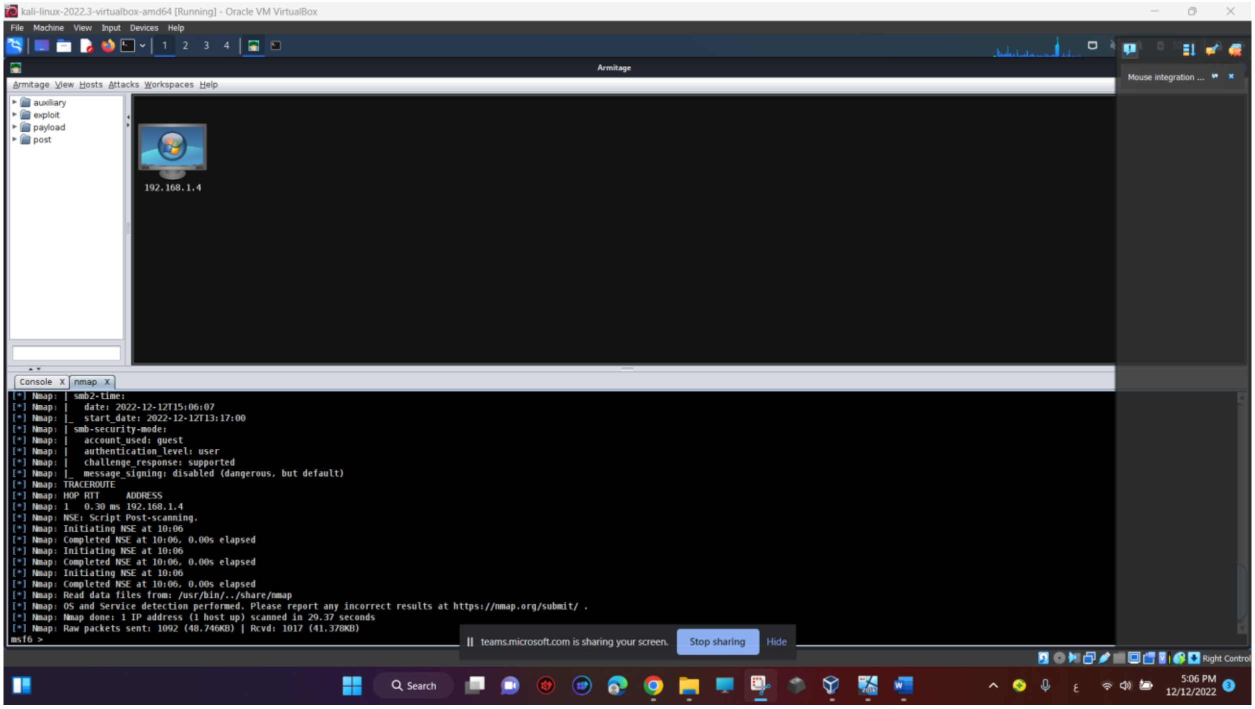
```
0 upgraded, 1 newly installed, 0 to remove and 5 not upgraded.
Need to get 4,971 kB of archives.
After this operation, 11.5 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 armitage all 20220123
-0kali4 [4,971 kB]
Fetched 4,971 kB in 4s (1,183 kB/s)
Selecting previously unselected package armitage.
(Reading database ... 379812 files and directories currently installed.)
Preparing to unpack .../armitage_20220123-0kali4_all.deb ...
Unpacking armitage (20220123-0kali4) ...
Setting up armitage (20220123-0kali4) ...
Processing triggers for kali-menu (2022.4.1) ...

┌──(root㉿kali)-[/home/kali]
└─# armitage
[*] Starting msfrpcd for you.
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by sleep.engine.atoms.Obj
usr/share/armitage/armitage.jar) to method java.lang.Process
am()
WARNING: Please consider reporting this to the maintainers o
oms.ObjectAccess
WARNING: Use --illegal-access=warn to enable warnings of fur
ective access operations
WARNING: All illegal access operations will be denied in a f
[*] MSGRPC starting on 127.0.0.1:55553 (NO SSL):Msg...
```

Connecting to 127.0.0.1:55553
java.net.ConnectException: Connection refused (Connection refused)


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
Trash
File System
Home
root@kali: /home/kali
File Actions Edit View Help
Mouse integration ...
teams.microsoft.com is sharing your screen.
Stop sharing
Hide
Right Control
Search
5:03 PM
12/12/2022

```
┌──(root㉿kali)-[/home/kali]
└─# armitage
[*] Starting msfrpcd for you.
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by sleep.engine.atoms.ObjectAccess (file:/
usr/share/armitage/armitage.jar) to method java.lang.ProcessImpl.getErrorStre
am()
WARNING: Please consider reporting this to the maintainers of sleep.engine.at
oms.ObjectAccess
WARNING: Use --illegal-access=warn to enable warnings of further illegal refl
ective access operations
WARNING: All illegal access operations will be denied in a future release
[*] MSGRPC starting on 127.0.0.1:55553 (NO SSL):Msg...
[*] MSGRPC ready at 2022-12-12 10:02:55 -0500.

┌──(root㉿kali)-[/home/kali]
└─# msfdb init
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/datab
ase.yml'
[+] Creating initial database schema

┌──(root㉿kali)-[/home/kali]
└─#
```

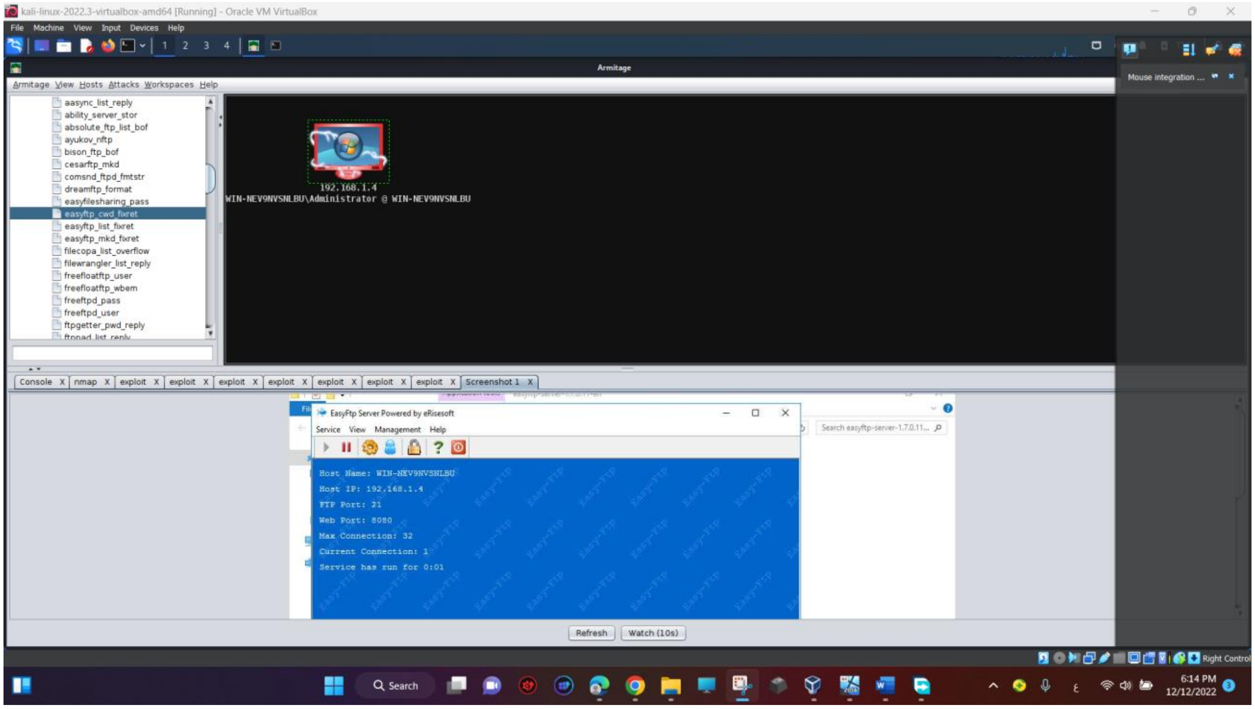
The target machine appears in the upper center part of the Armitage window, with a Windows logo on it:


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.1.4
Console X
nmap X
teams.microsoft.com is sharing your screen.
Stop sharing
Hide
Search
5:06 PM
12/12/2022

```
[*] Nmap: | smb2-time:
[*] Nmap: |   date: 2022-12-12T15:06:07
[*] Nmap: |_  start_date: 2022-12-12T13:17:00
[*] Nmap: | smb-security-mode:
[*] Nmap: |   account_used: guest
[*] Nmap: |   authentication_level: user
[*] Nmap: |   challenge_response: supported
[*] Nmap: |_  message_signing: disabled (dangerous, but default)
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT     ADDRESS
[*] Nmap: 1   0.30 ms 192.168.1.4
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: Initiating NSE at 10:06
[*] Nmap: Completed NSE at 10:06, 0.00s elapsed
[*] Nmap: Initiating NSE at 10:06
[*] Nmap: Completed NSE at 10:06, 0.00s elapsed
[*] Nmap: Initiating NSE at 10:06
[*] Nmap: Completed NSE at 10:06, 0.00s elapsed
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 29.37 seconds
[*] Nmap: Raw packets sent: 1092 (48.746KB) | Rcvd: 1017 (41.378KB)
msf6 >
```

The Target machine's desktop appears in the lower pane of Armitage, as shown below.

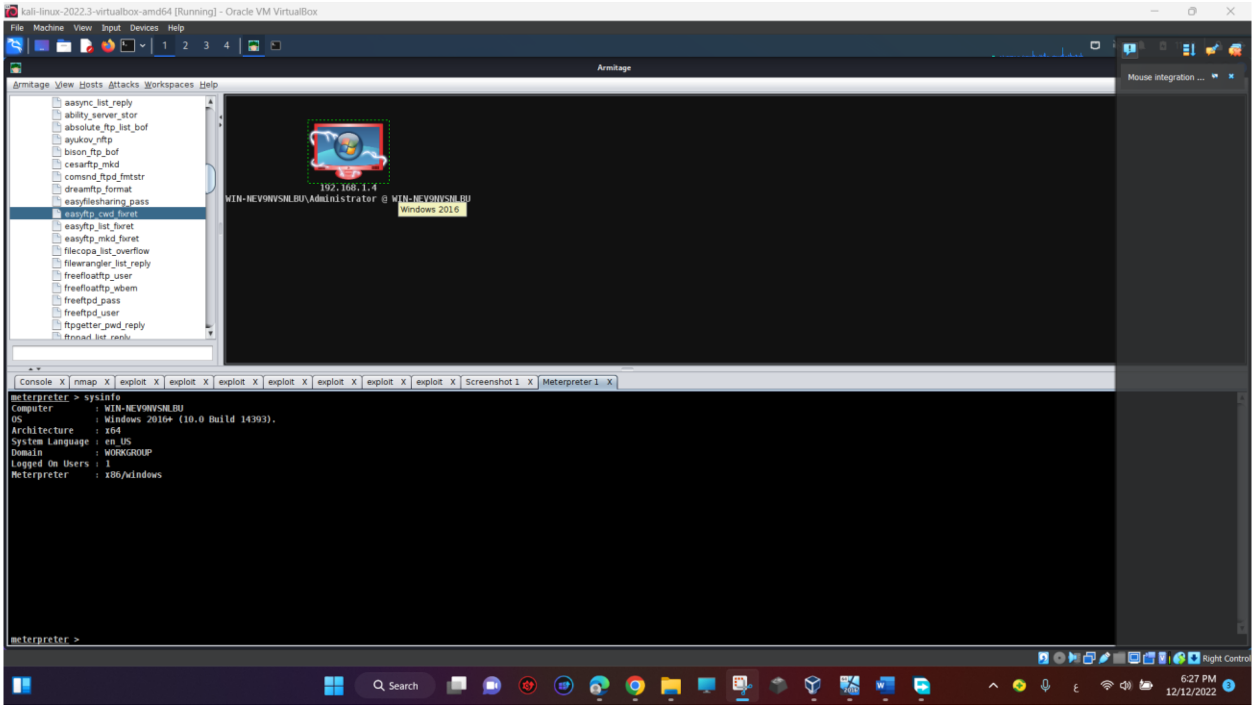
The Target machine's desktop appears in the lower pane of Armitage, as shown below.



```
WIN-NEV9NVSNLBU\Administrator @ WIN-NEV9NVSNLBU
```

```
Host Name: WIN-NEV9NVSNLBU
Host IP: 192.168.1.4
FTP Port: 21
Web Port: 8080
Max Connection: 32
Current Connection: 1
Service has run for 0:01
```

text that is covered by a gray box in the image below.



```
meterpreter > sysinfo
Computer        : WIN-NEV9NVSNLBU
OS              : Windows 2016+ (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows

meterpreter >
```

Describe the functionality of the Armitage Software

Armitage is a fantastic Java-based GUI front-end for the Metasploit Framework developed by Raphael Mudge. Its goal is to help security professionals better understand hacking and help them realize the power and potential of Metasploit