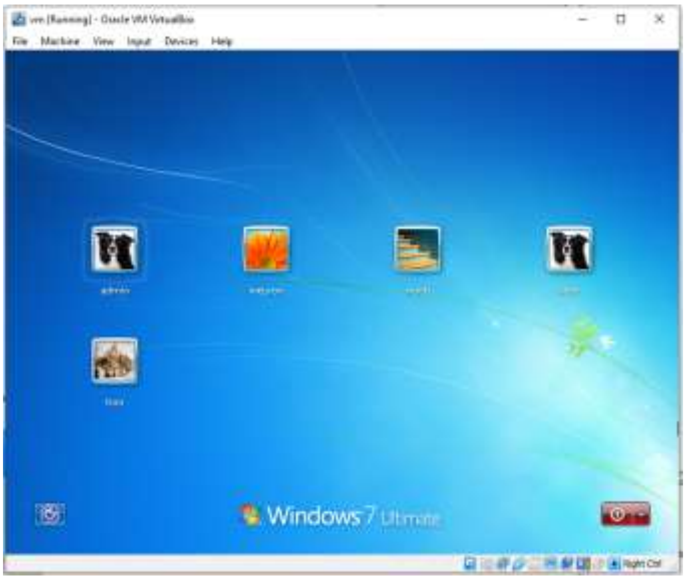
CSM – Exam

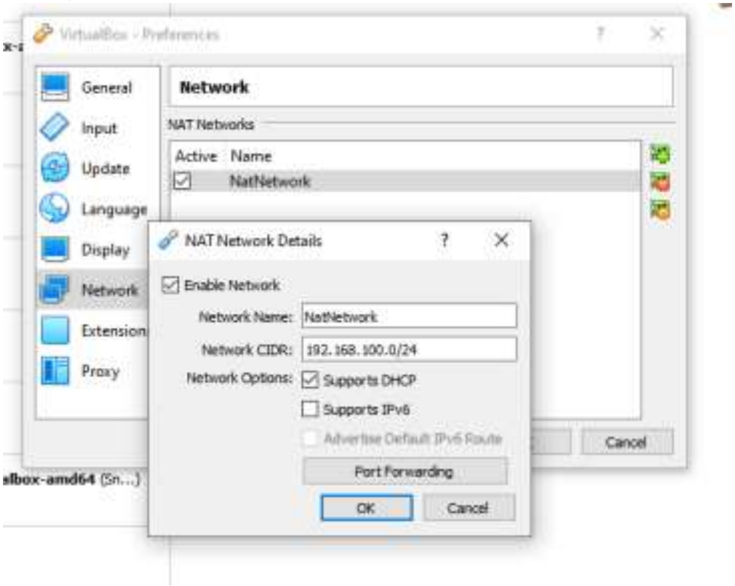
Questions-1 Scanning

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


vm [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows 7 Ultimate
Right Ctrl

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

a) Set NAT Network "NatNetwork" on VirtualBox



Network

NAT Networks

Active	Name
☑	NatNetwork

☑ Enable Network

Network Name: NatNetwork

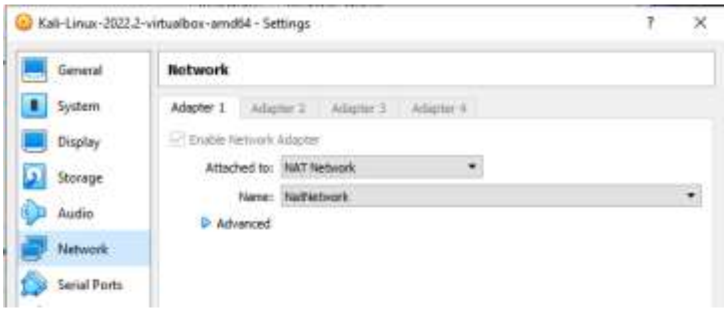
Network CIDR: 192.168.100.0/24

Network Options: ☑ Supports DHCP

□ Supports IPv6

□ Advertise Default IPv6 Route

b) Attach Kali VM to "NatNetwork"



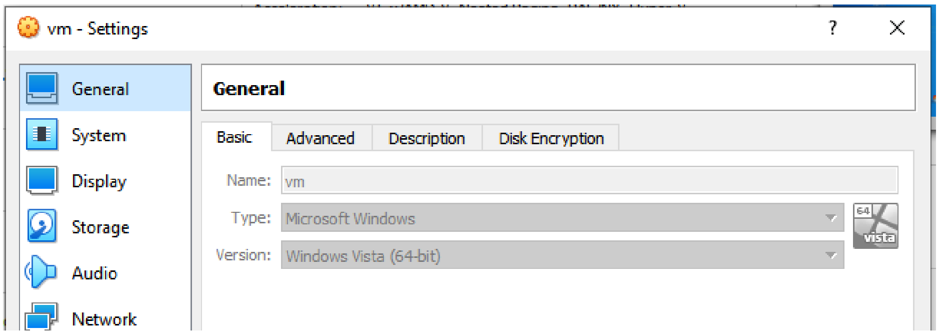
Network

☑ Enable Network Adapter

Attached to: NAT Network

Name: NatNetwork

c) Attach Win 7 VM to “NatNetwork”

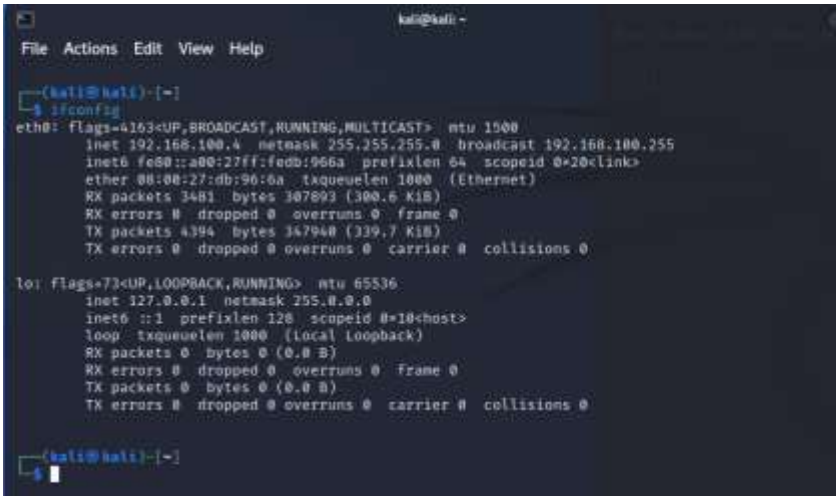


Name: vm

Type: Microsoft Windows

Version: Windows Vista (64-bit)

d) Check Kali VM IP Address



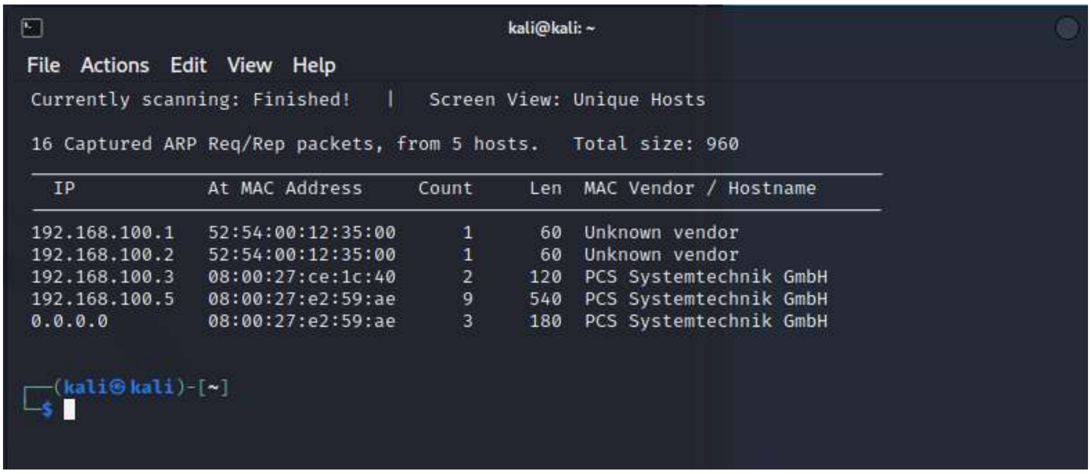
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.4  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::a00:27ff:fedb:966a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:db:96:6a  txqueuelen 1000  (Ethernet)
        RX packets 3481  bytes 307893 (300.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4394  bytes 347940 (339.7 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 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ 
```

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

a) Run netdiscover from Kali VM to find the Win 7 VM IP Address

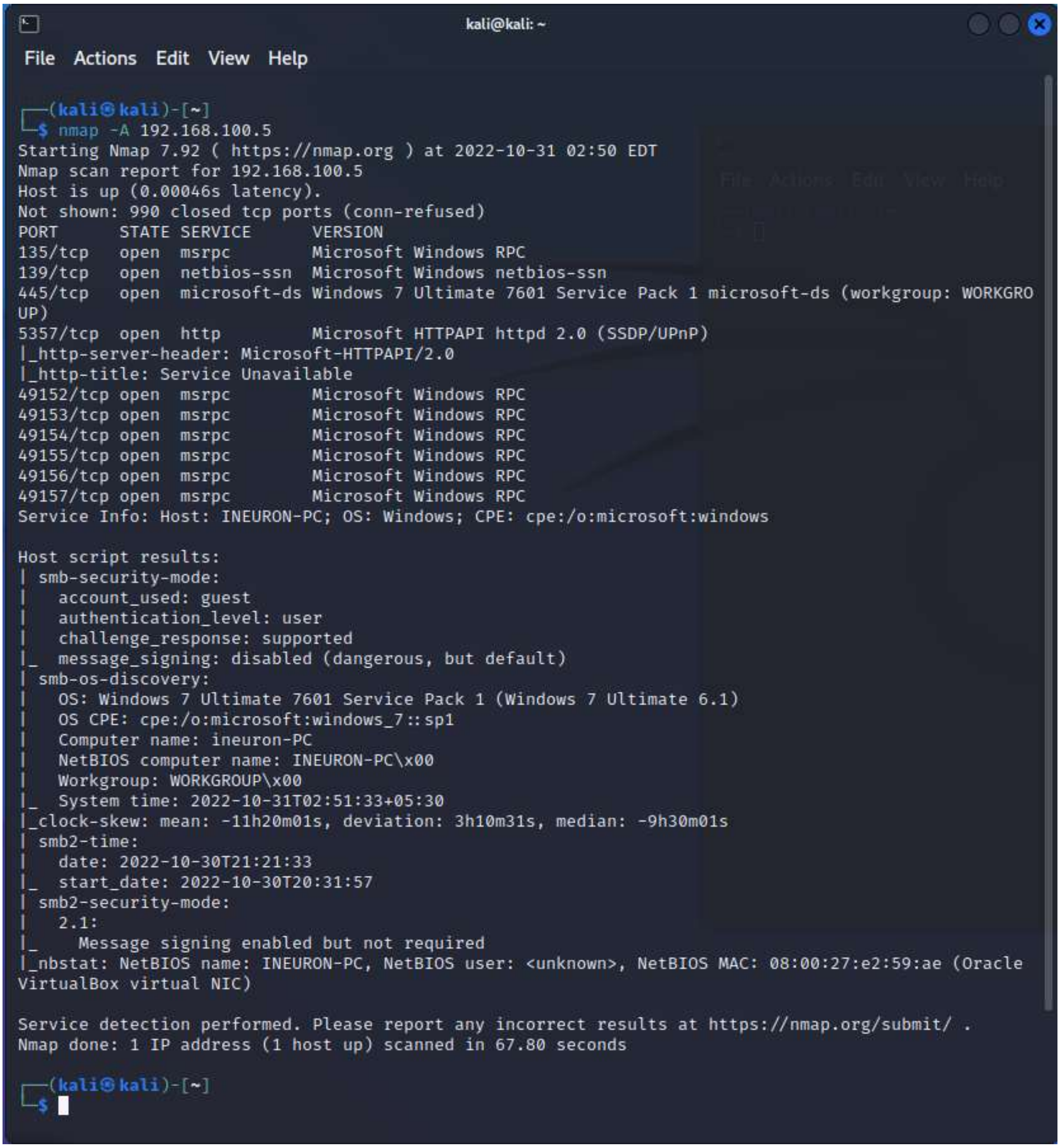


```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 16 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 960
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.100.1   52:54:00:12:35:00      1      60  Unknown vendor
 192.168.100.2   52:54:00:12:35:00      1      60  Unknown vendor
 192.168.100.3   08:00:27:ce:1c:40      2     120  PCS Systemtechnik GmbH
 192.168.100.5   08:00:27:e2:59:ae      9     540  PCS Systemtechnik GmbH
 0.0.0.0         08:00:27:e2:59:ae      3     180  PCS Systemtechnik GmbH


┌──(kali㉿kali)-[~]
└─$ 
```

b) Run nmap –A 192.168.100.5 is the Win 7 VM and to discover open ports



```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.100.5
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-31 02:50 EDT
Nmap scan report for 192.168.100.5
Host is up (0.00046s latency).
Not shown: 990 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: WORKGRO
UP)
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
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: INEURON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| 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: 2022-10-31T02:51:33+05:30
|_clock-skew: mean: -11h20m01s, deviation: 3h10m31s, median: -9h30m01s
| smb2-time:
|   date: 2022-10-30T21:21:33
|_  start_date: 2022-10-30T20:31:57
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: INEURON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:e2:59:ae (Oracle
VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.80 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Questions-2 Exploitation

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

Questions-3 Password Attack

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

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

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

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

Part B - Investigation Phase

Now you understand the offensive Hacking approach in secure environment, that's the part of role we follow as an Ethical Hacker Role in the Industry. Not its time to work on Investigation part.
As after the hacking activity is done, how we analysis the hacking event, that will be done in forensic part, so here we will use a PCAP file available with the Paper attached.

Do take the .pcap file and analysis with Wireshark Tool

Question-6 Wireshark Analysis

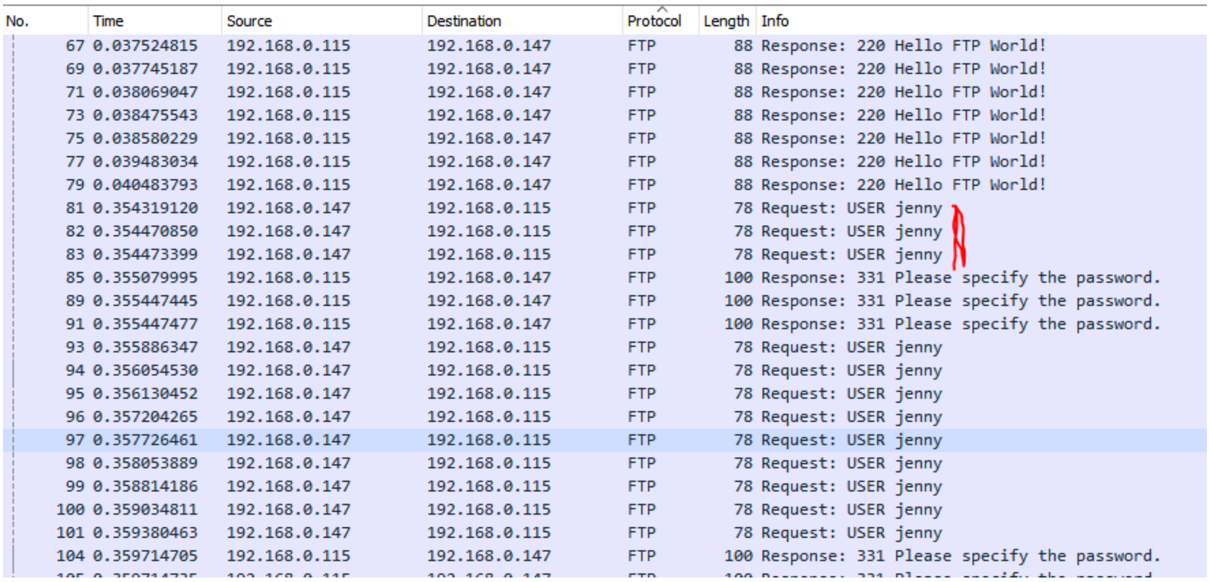
Provide some below answer for the same activity you perform:

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?

Answer: Hydra

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

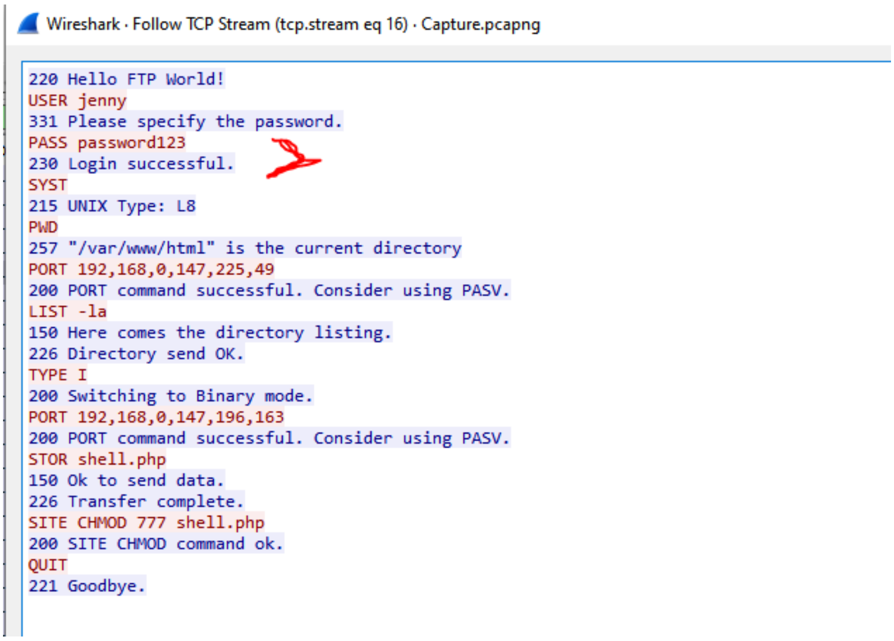
Answer: jenny



No.	Time	Source	Destination	Protocol	Length	Info
67	0.037524815	192.168.0.115	192.168.0.147	FTP	88	Response: 220 Hello FTP World!
69	0.037745187	192.168.0.115	192.168.0.147	FTP	88	Response: 220 Hello FTP World!
71	0.038069047	192.168.0.115	192.168.0.147	FTP	88	Response: 220 Hello FTP World!
73	0.038475543	192.168.0.115	192.168.0.147	FTP	88	Response: 220 Hello FTP World!
75	0.038580229	192.168.0.115	192.168.0.147	FTP	88	Response: 220 Hello FTP World!
77	0.039483034	192.168.0.115	192.168.0.147	FTP	88	Response: 220 Hello FTP World!
79	0.040483793	192.168.0.115	192.168.0.147	FTP	88	Response: 220 Hello FTP World!
81	0.354319120	192.168.0.147	192.168.0.115	FTP	78	Request: USER jenny
82	0.354470850	192.168.0.147	192.168.0.115	FTP	78	Request: USER jenny
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.

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

Answer: password123

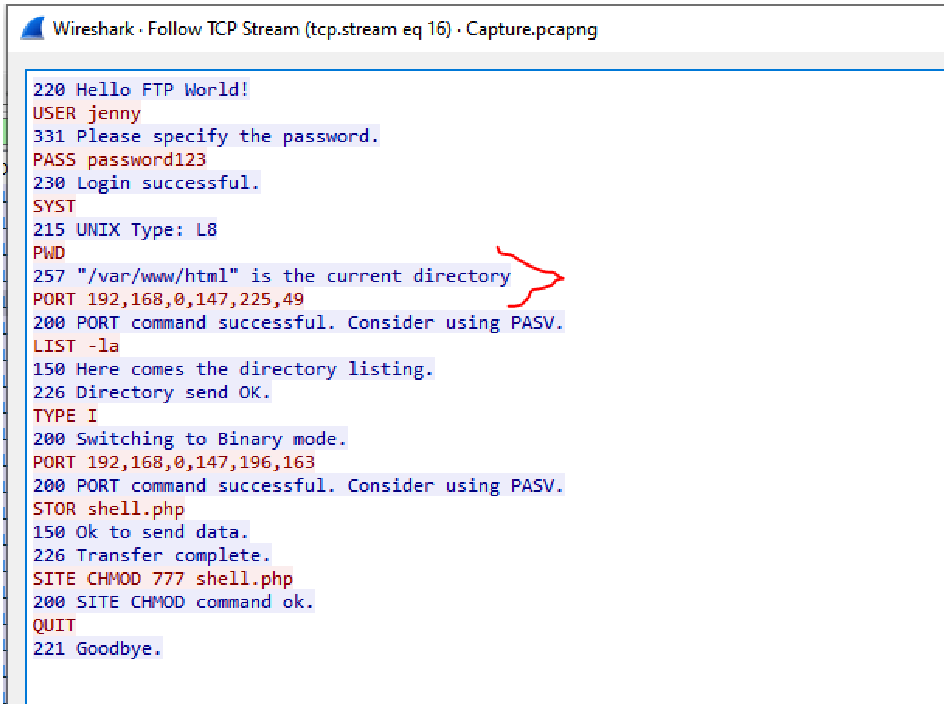


Wireshark · Follow TCP Stream (tcp.stream eq 16) · Capture.pcapng

```
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.
```

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

Answer: /var/www/html

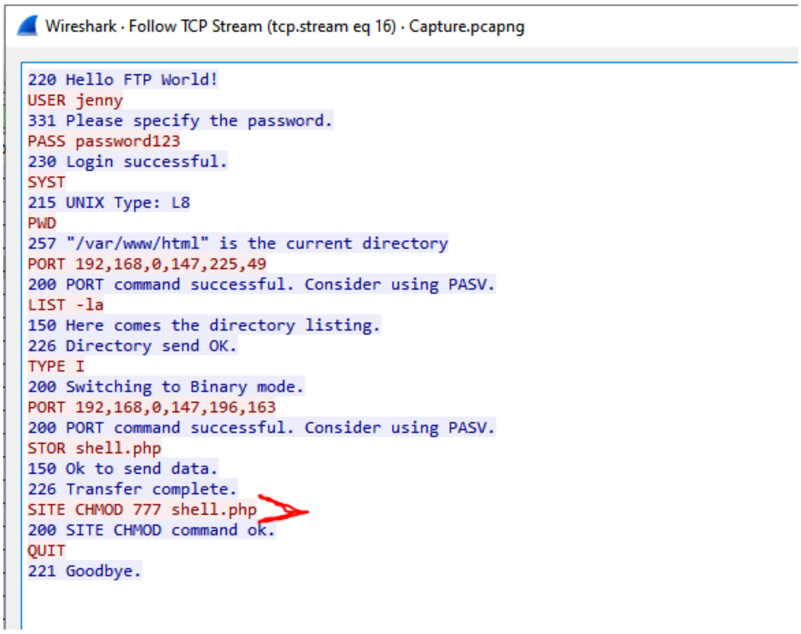


Wireshark · Follow TCP Stream (tcp.stream eq 16) · Capture.pcapng

```
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.
```

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

Answer: shell.php

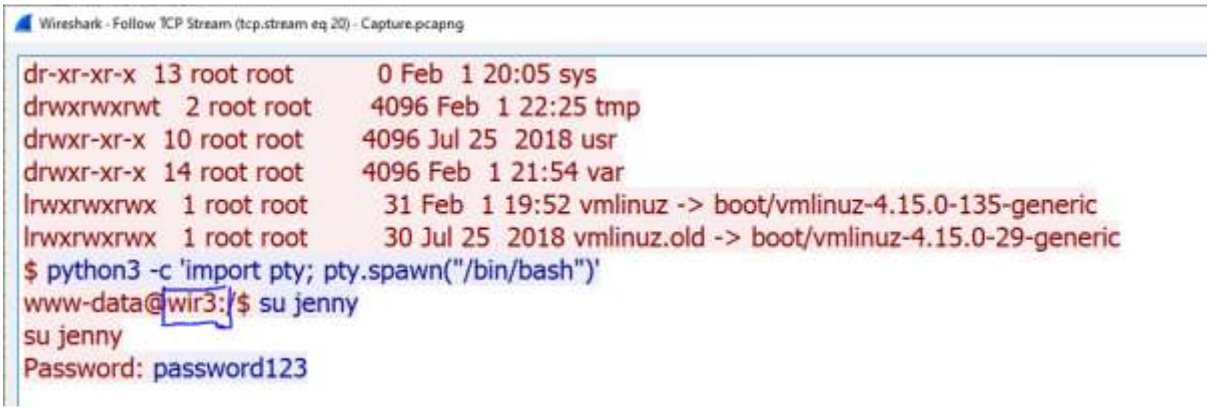


Wireshark · Follow TCP Stream (tcp.stream eq 16) · Capture.pcapng

```
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.
```

q-6 What is the computer's hostname?

Answer : wir3

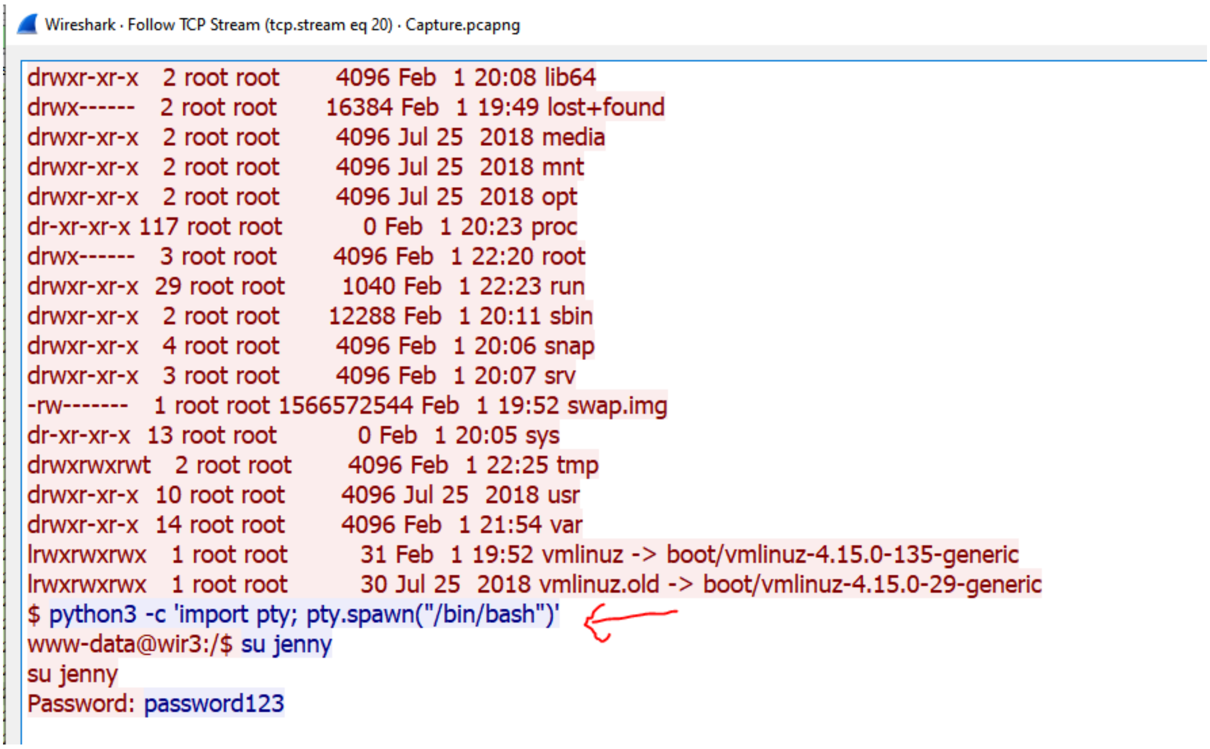


Wireshark · Follow TCP Stream (tcp.stream eq 20) · Capture.pcapng

```
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
```

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

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



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

```
drwxr-xr-x   2 root root       4096 Feb  1 20:08 lib64
drwx------   2 root root      16384 Feb  1 19:49 lost+found
drwxr-xr-x   2 root root       4096 Jul 25  2018 media
drwxr-xr-x   2 root root       4096 Jul 25  2018 mnt
drwxr-xr-x   2 root root       4096 Jul 25  2018 opt
dr-xr-xr-x 117 root root          0 Feb  1 20:23 proc
drwx------   3 root root       4096 Feb  1 22:20 root
drwxr-xr-x  29 root root       1040 Feb  1 22:23 run
drwxr-xr-x   2 root root      12288 Feb  1 20:11 sbin
drwxr-xr-x   4 root root       4096 Feb  1 20:06 snap
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
```

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?

Answer: rootkit