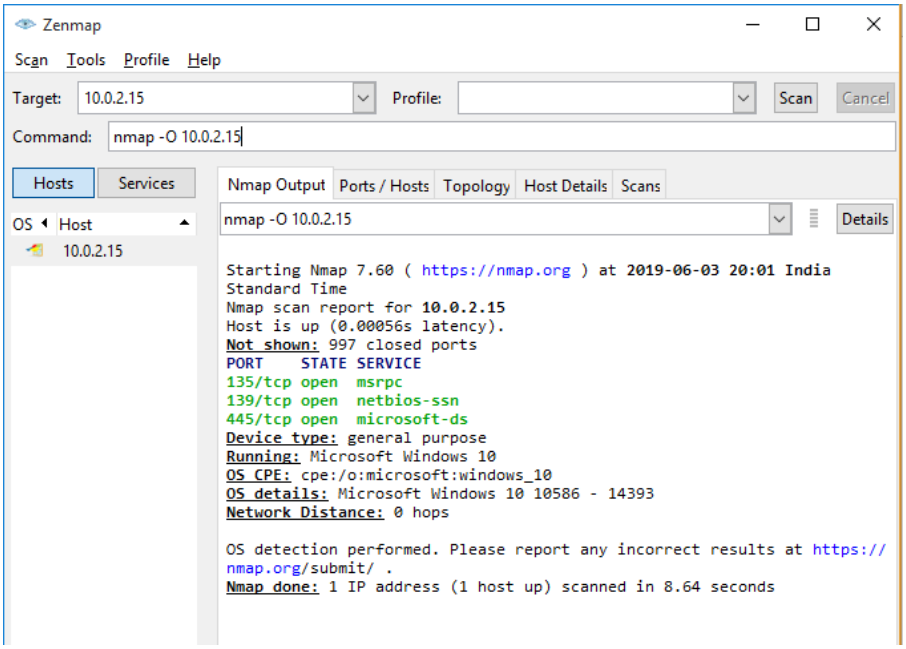
Enumeration

Module – 4 (Lab Assignment)

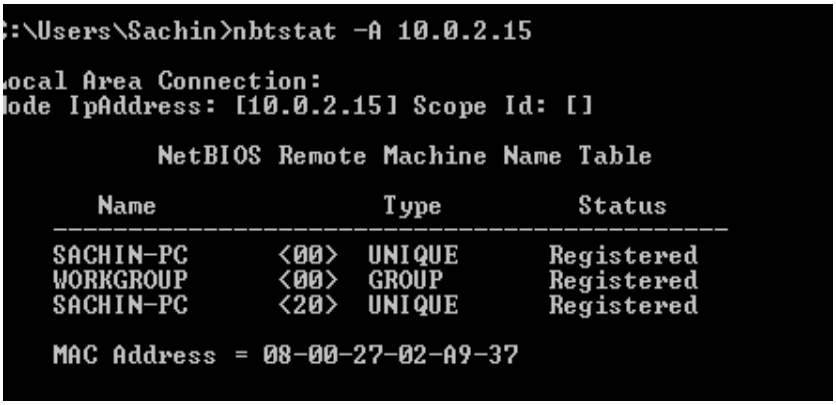
Name : Sachin Saj T K
Roll No: CB.EN.P2CEN18012
Date of Submission: 3/06/2019

Enumerating a Target Network Using Nmap

1. Nmap O Scan (To find Open Ports)



2. Nbtstat (Gives NetBIOS Remote Machine Name Table)



3. nbtstat

```
C:\Users\Sachin>nbtstat -A 10.0.2.15

Ethernet:
Node IpAddress: [10.0.2.15] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    DESKTOP-8R8MD6F<00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    DESKTOP-8R8MD6F<20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered
    WORKGROUP      <1D>  UNIQUE      Registered
    ..__MSBROWSE__.<01>  GROUP       Registered

    MAC Address = 08-00-27-07-69-CA
```

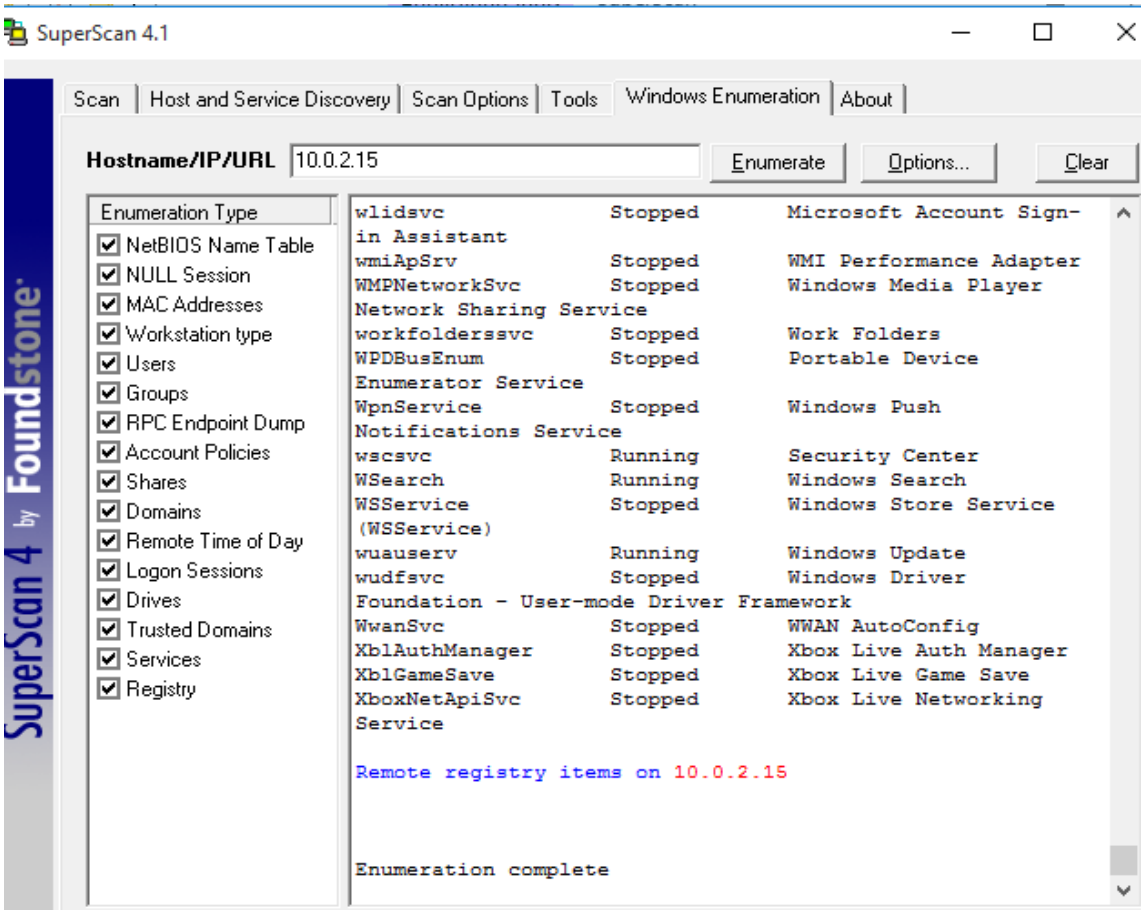
4. Creating null session and net use

```
C:\Windows\system32>net use \\10.0.2.15\IPC$ ""\u:""
The command completed successfully.


C:\Windows\system32>net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
OK                     \\10.0.2.15\IPC$          Microsoft Windows Network
The command completed successfully.
```

Tool/Utility	**Information Collected/Objective Achieved**
Nmap	**Target machine:** 10.0.2.15
	List of Open Ports: 135/tcp, 139/tcp, 445/tcp
	NetBIOS Remote machine IP address: 10.0.2.15
	Output : Successful connection of Null session.

Enumerating NetBIOS Using the SuperScan Tool

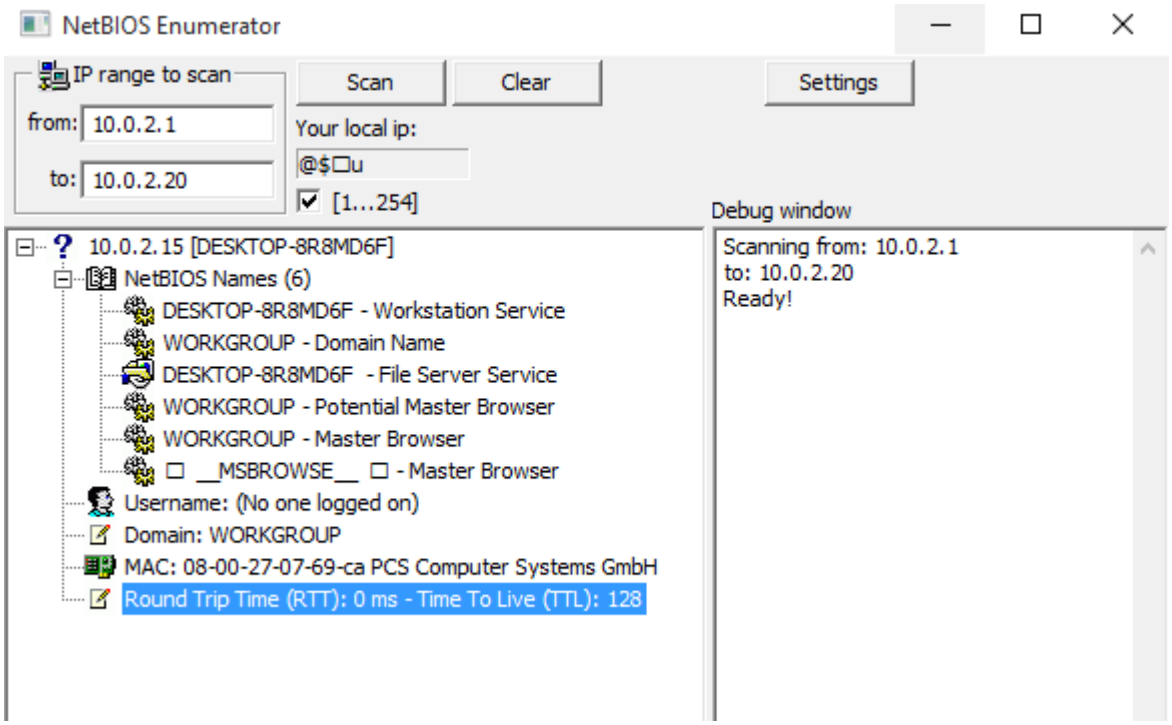
1. Enumeration Scan (On IP Address: 10.0.2.15)



Tool/Utility	Information Collected/Objective Achieved
SuperScan Tool	**Enumerating Virtual Machine IP address:**10.0.2.15
	Performing Enumeration Types: • **Null Session:** 10.0.2.15 • **MAC Address:** 0: 02:00:4C:4F:4F:50 • **Work Station Type:** 10.0.2.15 • **Users:** DESKTOP-8R8MD6F • **Groups:** WORKGROUP • **Domain:** 10.0.2.15 • **Account Policies:** DESKTOP-8R8MD6F • **Registry:** 10.0.2.15

Enumerating NetBIOS Using the NetBIOS Enumerator Tool

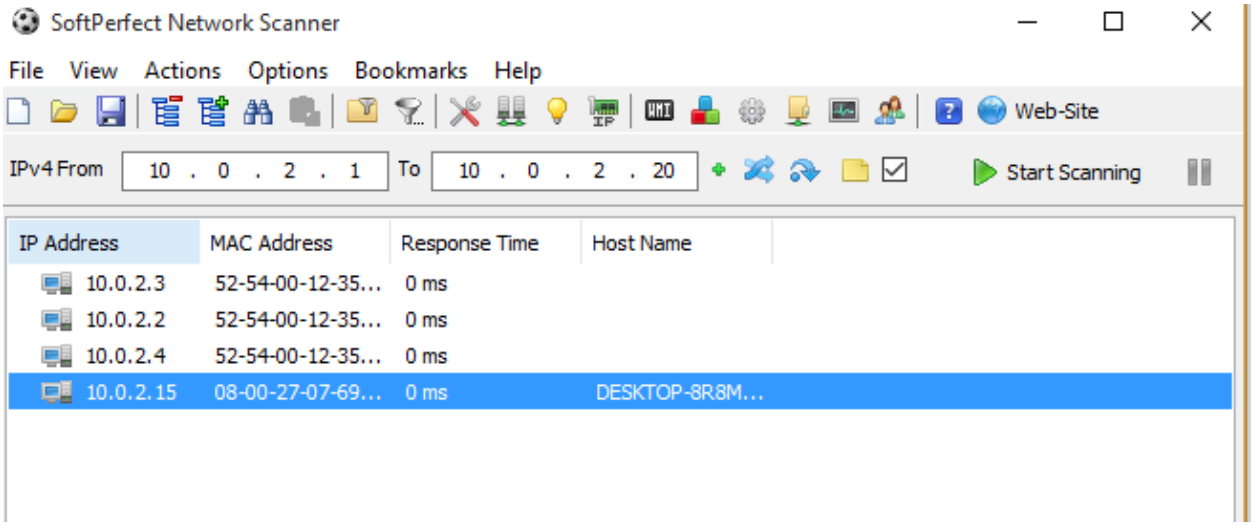
1. Scan of IP address range: 10.0.2.1 – 10.0.2.20



Tool/Utility	**Information Collected/Objective Achieved**
NetBIOS Enumerator Tool	**IP Address Range**: 10.0.2.1 – 10.0.2.20
	Result: • **Machine Name:** DESKTOP-8R8MD6F • **NetBIOS Names**:DESKTOP-8R8MD6F • **User Name:** (No one logged on) • **Domain:** WORKGROUP • **MAC Address:** 08-00-27-07-69-ca • **Round Trip Time:** 0 ms

Enumerating a Network Using SoftPerfect Network Scanner

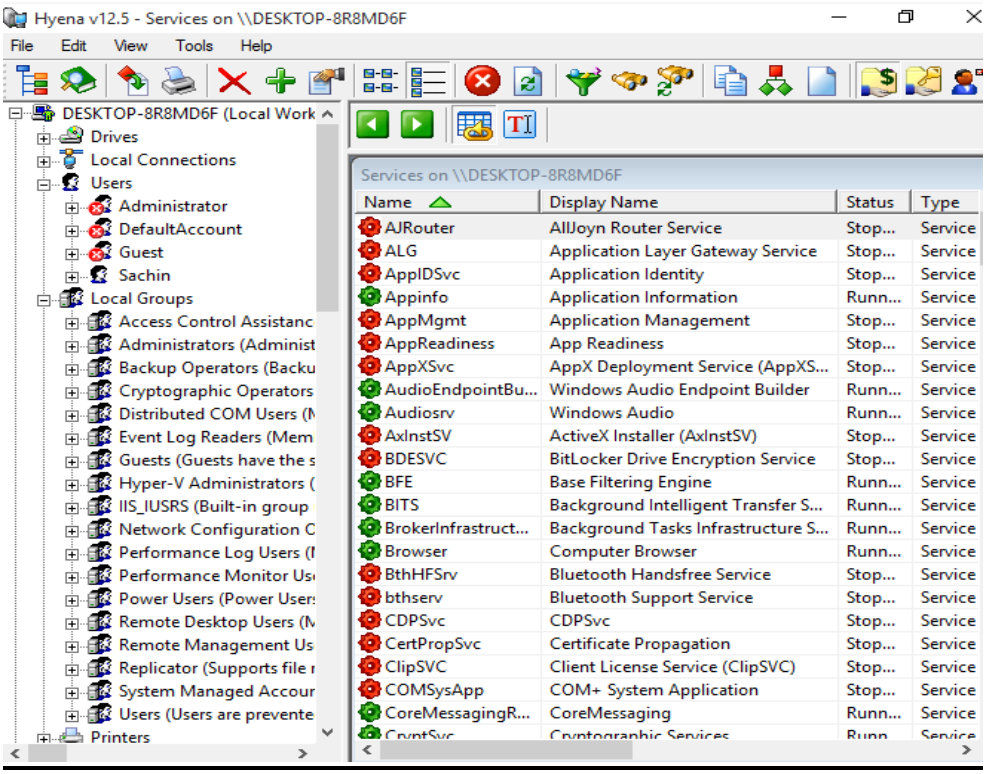
1. Scan IP Address range (10.0.2.1 – 10.0.2.20)



Tool/Utility	**Information Collected/Objective Achieved**
SoftPerfect Network Scanner	**IP Address Range:** 10.0.2.1 – 10.0.2.20
	Result: • **IP Address**: 10.0.2.15 • **Host Names**: DESKTOP-8R8MD6F.amritanet.edu • **MAC Address**: 08-00-27-07-69-CA • **Response Time**: 0 ms

Enumerating the System Using Hyena

1. Enumerating using Hyena.



Tool/Utility	Information Collected/Objective Achieved
Hyena	**Intention:** Enumerating the System
	Output • **Local Connection:** IPC$ Connections • **Users**: Sachin • **Local Group:** Administrators, Backup Operators • **Shares:** ADMIN$ (C:\Windows) • **Sessions**: nil • **Services:** ALG, App,Mgmt • **Events:** Access Denied • **User rights:** SeNetworkLogonRight, SeTCbPrivilege • **Performance**: Process, Network • **Registry**: HKEY_LOCAL_MACHINE • **WMI:** Win32_ComputerSystem