# ASSIGNMENT -2 AI FOR CYBER SECURITY

NAME: NARTU HARIKA

REG NO.:21BEC7236

In this let's explore Metasploit tool in kali Linux OS and scan the own computer and find the vulnerabilities and exploits in it.

#### Step-1:

First we have to get the ipv4 address of the system then we are checking and scan the system using nmap command.

Command: map 192.168.0.109

```
_$ nmap 192.168.0.109
Lsmmap 192.168.0.109
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-26 09:45 IST Nmap scan report for 192.168.0.109
Host is up (0.0080s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/trp open stp
 25/tcp
              open domain
80/tcp open http
111/tcp open rpcbind
                        netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
 513/tcp open
                        login
1099/tcp open rmiregistry
1524/tcp open ingreslock
 2049/tcp open nfs
 2121/tcp open ccproxy-ftp
 3306/tcp open mysql
 5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
 6667/tcp open irc
 8009/tcp open
8180/tcp open unknown
 Nmap done: 1 IP address (1 host up) scanned in 2.75 seconds
```

#### Step-2:

Command: map 192.168.0.109 -sV

```
**S maps 192.168.0.109 -sV
Starting Mamp 7.94 (https://nmap.org ) at 2023-09-26 09:46 IST
Nmap scan report for 192.168.0.109
Host is up (0.00080s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
22/tcp open ssh OpenSSH 4.7pl Debian Subuntu1 (protocol 2.0)
23/tcp open stellet Linux telnetd
25/tcp open smtp Postfix smtpd
53/tcp open domain ISC BIND 9.4.2
88/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
111/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
113/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
113/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
113/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1152/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1152/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1152/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1152/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1152/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1152/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1152/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1152/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
1172/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
118/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
118/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
118/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
118/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
119/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
119/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
119/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
119/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
119/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
119/tcp open netbios-ssn Samba s
```

- We can see port no 139 and 445 resembles SMB. So we have to explore for exploits in smb.
- Now lets open Metasploit in our kali Linux which is exploit on framework that gives access to on resystem.

### Step-3:

Command: sudo msfconsole

### Step-4:

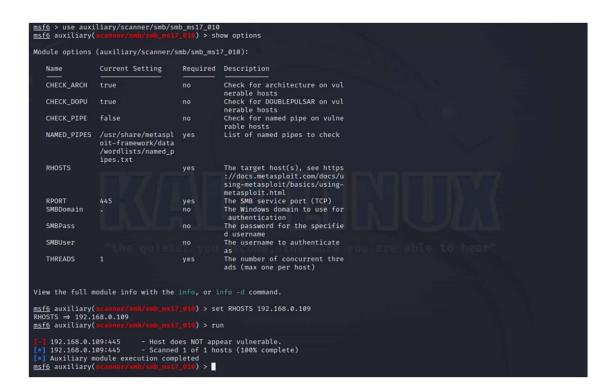
Command: grep scanner search smb

We can enter "search smb" or "grep scanner search smb".

```
### Sunctionary Second Principles of Part Se
```

## **Step-5**:

Command: use auxiliary/scanner/smb/smb\_ms17\_010



In this way we can run a scan on any system. we can gain the access of the system too if it is we find the vulnerabilities in that auxiliary scan.