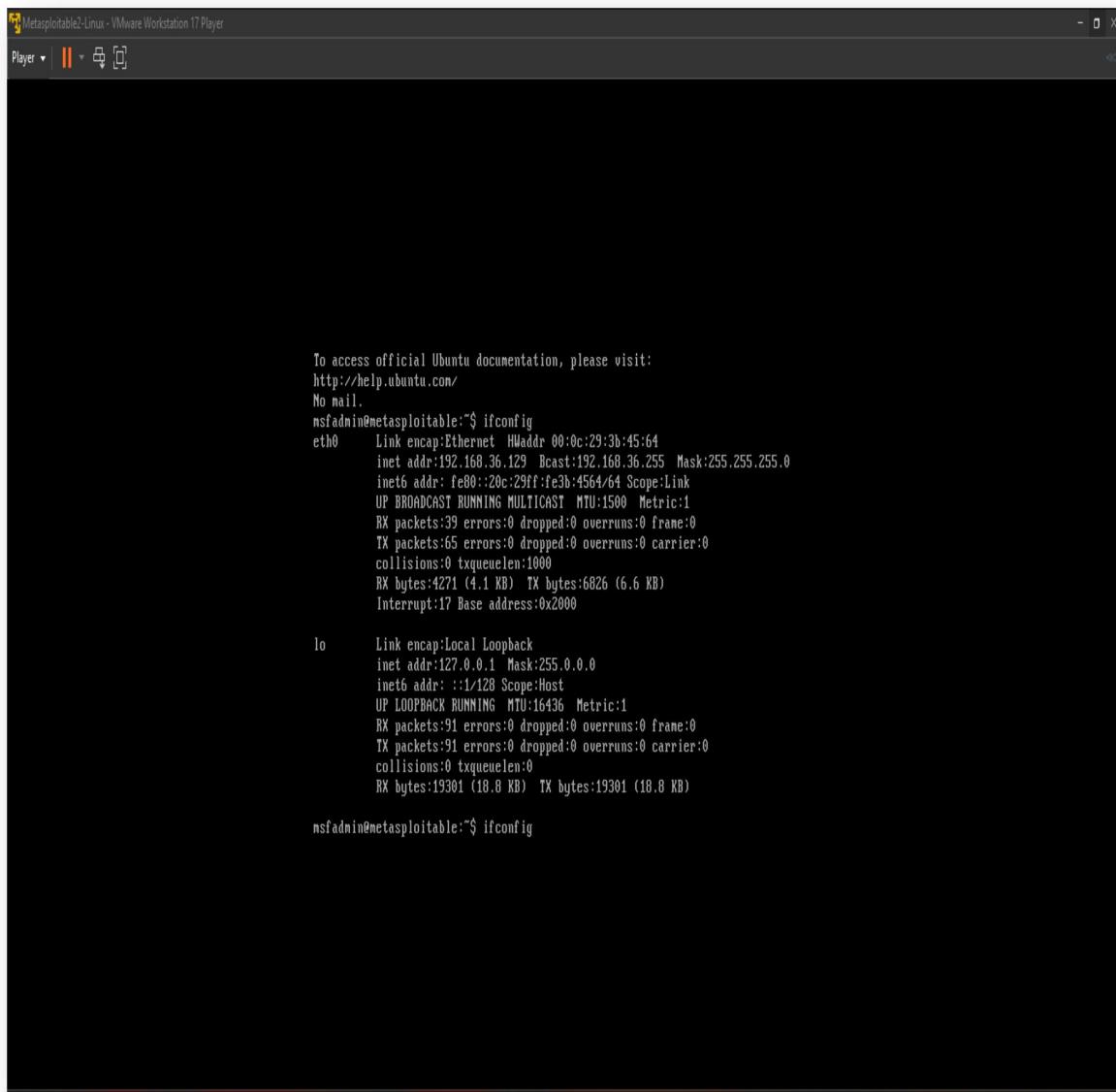


LAB-14

AIM: Conduct Vulnerability assessments and penetration testing of mobile and IOT devices.

Step-1: Find your IP address in metasploitable and scan that IP address in Nessus to scan that IP address to find the vulnerabilities.



```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
nsfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 00:0c:29:3b:45:64  
          inet addr:192.168.36.129 Bcast:192.168.36.255 Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe3b:4564/64 Scope:Link  
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
            RX packets:39 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:65 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:4271 (4.1 KB) TX bytes:6826 (6.6 KB)  
            Interrupt:17 Base address:0x2000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
            UP LOOPBACK RUNNING MTU:16436 Metric:1  
            RX packets:91 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:91 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:0  
            RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)  
nsfadmin@metasploitable:~$ ifconfig
```

Step-2: Scan Target IP of metasploitable Using Nmap to see the open ports.

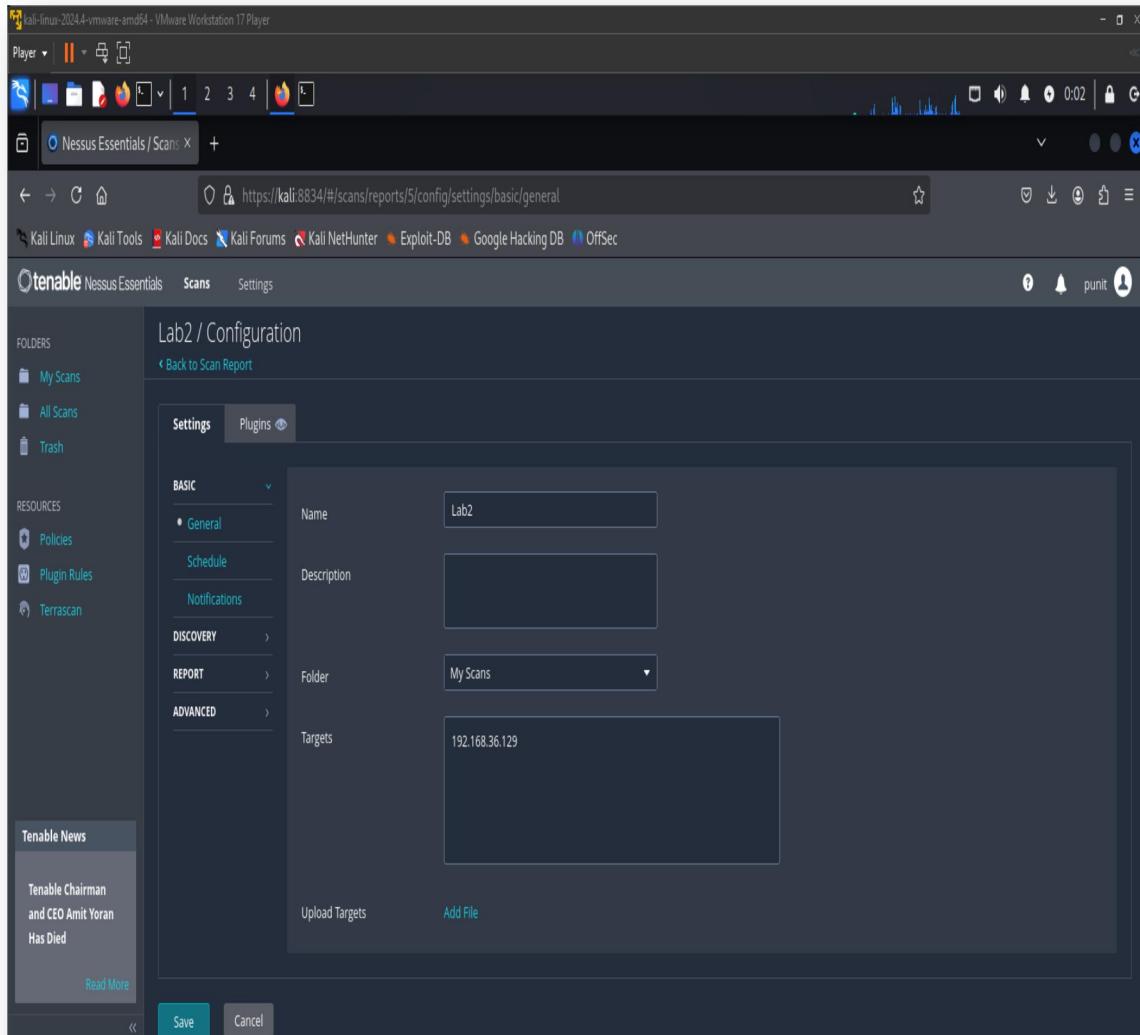
The screenshot shows a terminal window titled "kali-linux-2024.4-vmware-amd64 - VMware Workstation 17 Player". The terminal displays the following Nmap command and its output:

```
(kali㉿kali:[~]/Downloads)
$ nmap -p- 192.168.36.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-16 00:44 EST
Nmap scan report for 192.168.36.129
Host is up (0.0024s latency).
Not shown: 65506 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
109/tcp   open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgrvrv
42408/tcp open  unknown
49014/tcp open  unknown
53905/tcp open  unknown
58733/tcp open  unknown
MAC Address: 00:0C:29:3B:45:64 (VMware)

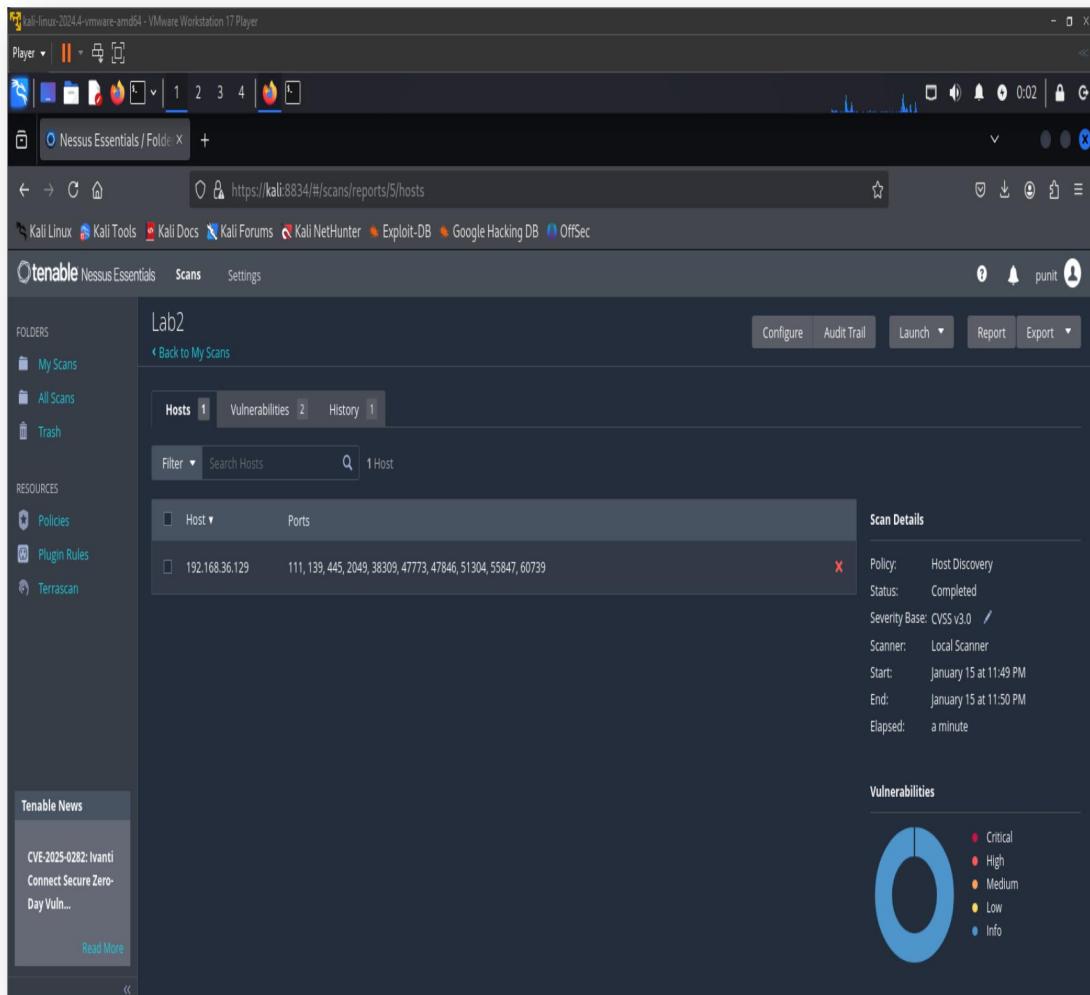
Nmap done: 1 IP address (1 host up) scanned in 5.10 seconds
```

The terminal prompt shows the user is in the "/Downloads" directory. The Nmap scan has completed successfully, identifying 1 host as up. The output lists numerous open TCP ports, including common services like FTP, SSH, Telnet, SMTP, HTTP, and various ports used by MySQL, PostgreSQL, and other applications. A pie chart in the interface indicates the severity of vulnerabilities found.

Step-3: In Nessus Go to Host Discovery and enter the target IP that you want to scan and launch to find Vulnerabilities.



Step-4: After that it will start to scan and after the completion it will show the vulnerabilities that have in the target IP or hosts.



Step-5: Now you are able to see the vulnerabilities that are scanned on that host or target IP and you are able to see the info of that vulnerabilities.

The screenshot shows the Tenable Nessus Essentials interface. The left sidebar includes sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Terrascan), and Tenable News (Microsoft's January 2025 Patch Tuesday). The main content area is titled 'My Scans' and shows a table with the following data:

Name	Scan Type	Schedule	Last Scanned
Lab2	Host Discovery	On Demand	✓ January 15 at 11:50 PM

The screenshot shows the 'Vulnerabilities' page for the 'Lab2' scan. The left sidebar remains the same. The main content area shows the following details:

- Hosts:** 1
- Vulnerabilities:** 2
- History:** 1

The vulnerabilities listed are:

Severity	Description	Family	Count
INFO	Nessus Scan Information	Settings	1
INFO	Ping the remote host	Port scanners	1

Scan Details:

- Policy: Host Discovery
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: January 15 at 11:49 PM
- End: January 15 at 11:50 PM
- Elapsed: a minute

Vulnerabilities:

A pie chart showing the distribution of vulnerabilities by severity: Critical (red), High (orange), Low (yellow), and Info (blue).

→ Also You are able to see the History that you scanned.

The screenshot shows the Tenable Nessus Essentials interface running in a VMware Workstation Player window. The main window displays a completed scan named 'Lab2'. The 'History' tab is selected, showing one entry: 'Current' (January 15 at 11:49 PM) with a status of 'Completed'. The 'Scan Details' panel on the right provides information about the scan, including policy, status, severity base, scanner, start and end times, and elapsed time. A 'Vulnerabilities' section includes a pie chart showing the distribution of vulnerabilities by severity: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (blue).

Conclusion:-

Conducting vulnerability assessments and penetration testing on mobile and IoT devices is essential to identifying and mitigating security risks in today's interconnected world. These assessments help uncover vulnerabilities in device firmware, applications, network communications, and access controls that could be exploited by attackers. By proactively testing and analyzing potential attack surfaces, organizations can strengthen their overall security posture, ensure compliance with industry standards, and protect sensitive user data. As mobile and IoT ecosystems continue to evolve, regular testing and adaptive security measures remain critical to safeguarding both users and infrastructure.