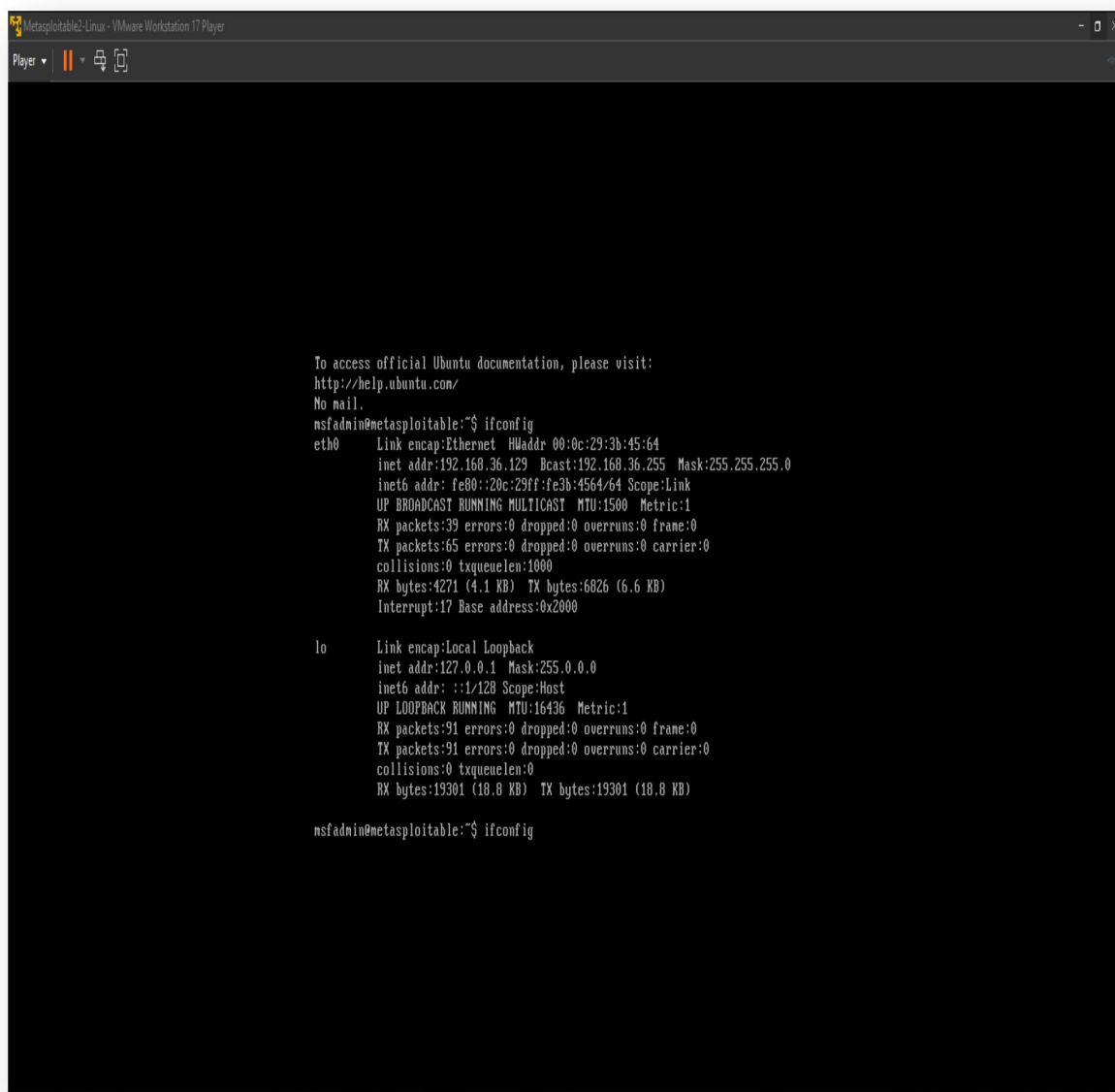


LAB-2

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.

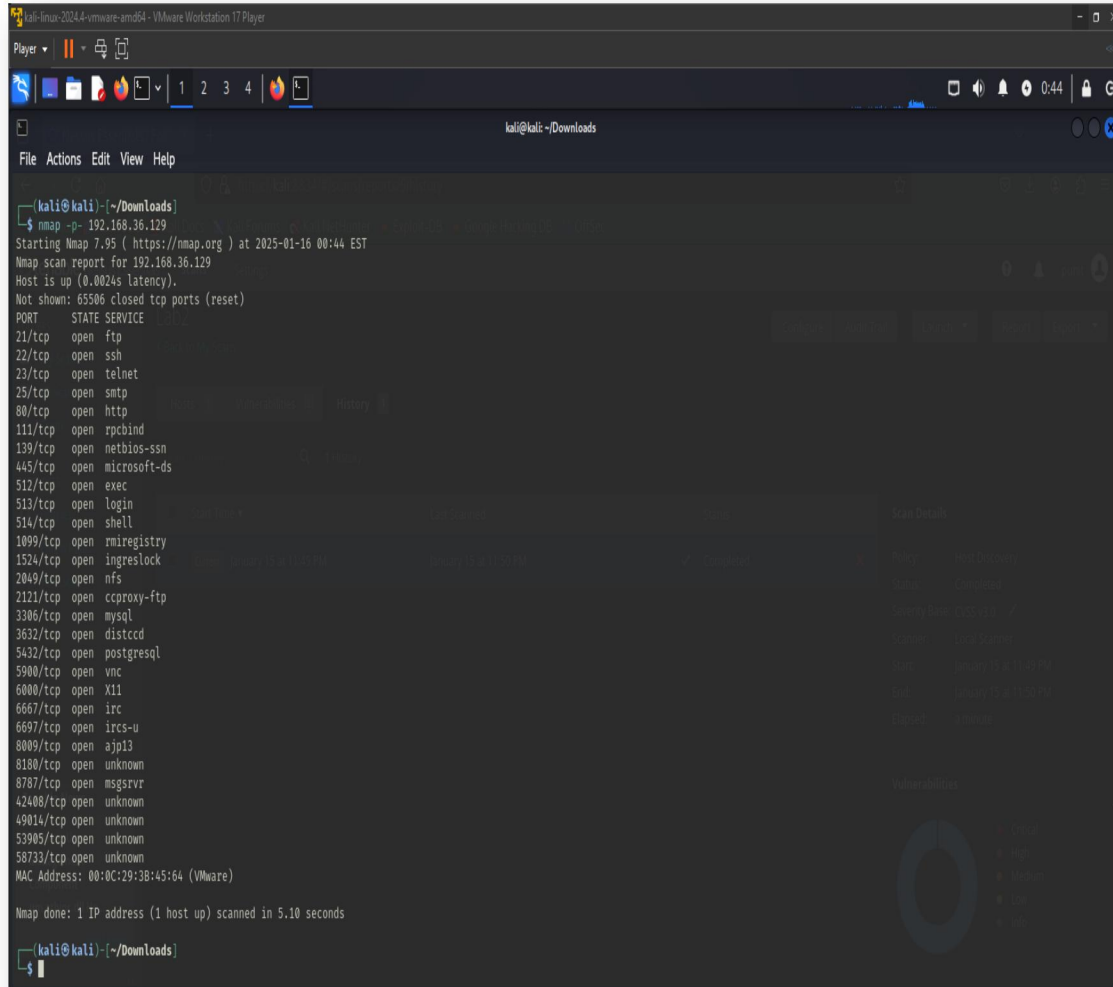


```
nsfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:3b:45:64
          inet addr:192.168.36.129  Bcast:192.168.36.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe3b:4564/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          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
```

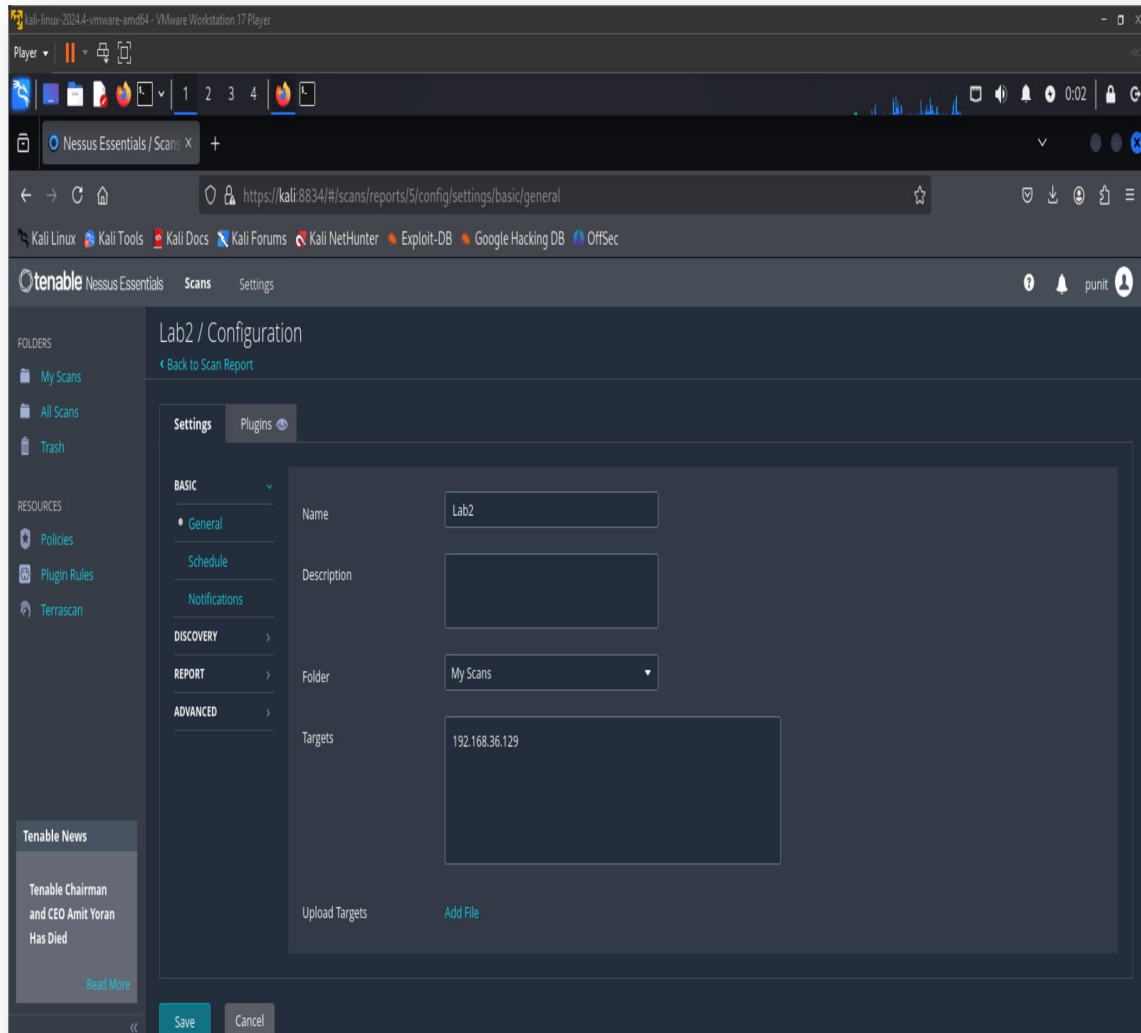
Step-2: Scan Target IP of metasploitable Using Nmap to see the open ports.



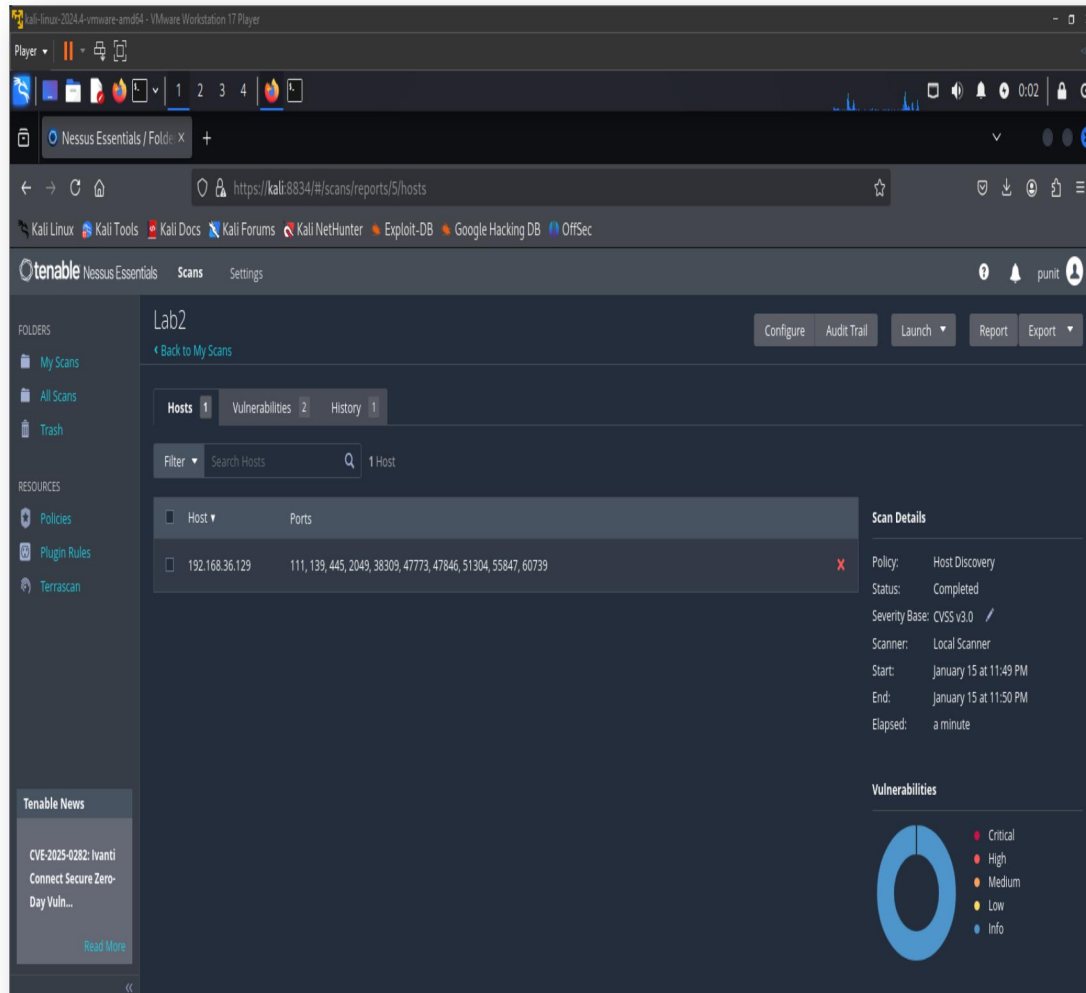
```
(kali@kali)-[~/Downloads]
$ nmap -p- 192.168.36.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-16 00:44 EST
Nmap scan report for 192.168.36.129
Host is up (0.0024s latency).
Not shown: 65506 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rcpbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/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  msgsrvr
42408/tcp open  unknown
49014/tcp open  unknown
53905/tcp open  unknown
58733/tcp open  unknown
MAC Address: 00:0C:29:38:45:64 (VMware)

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

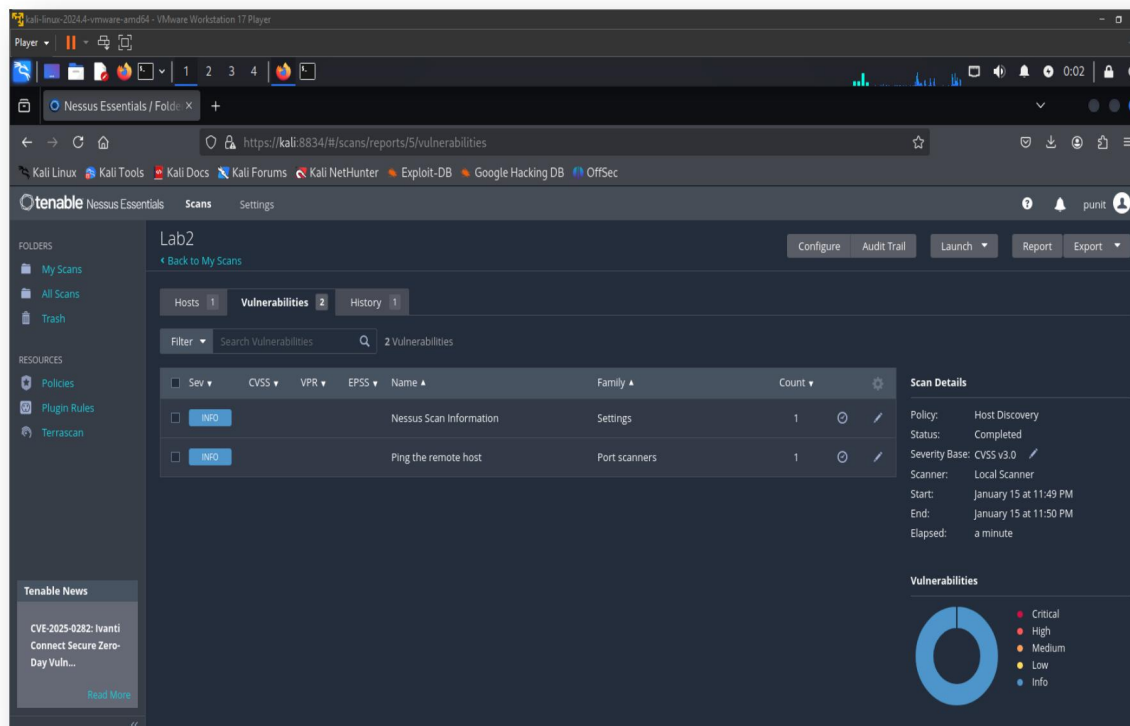
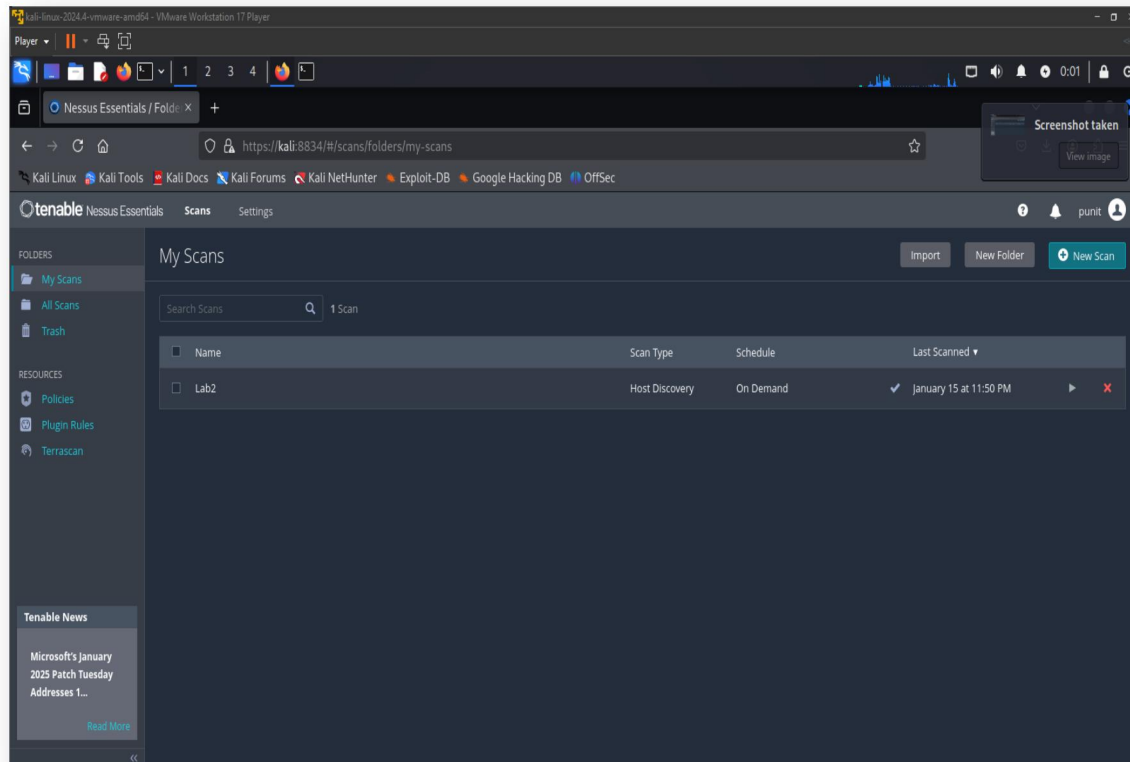
Step-3: In Nessus Go to Host Discovery and enter the target IP that you want to scan and launch to find Vulnerabilities.



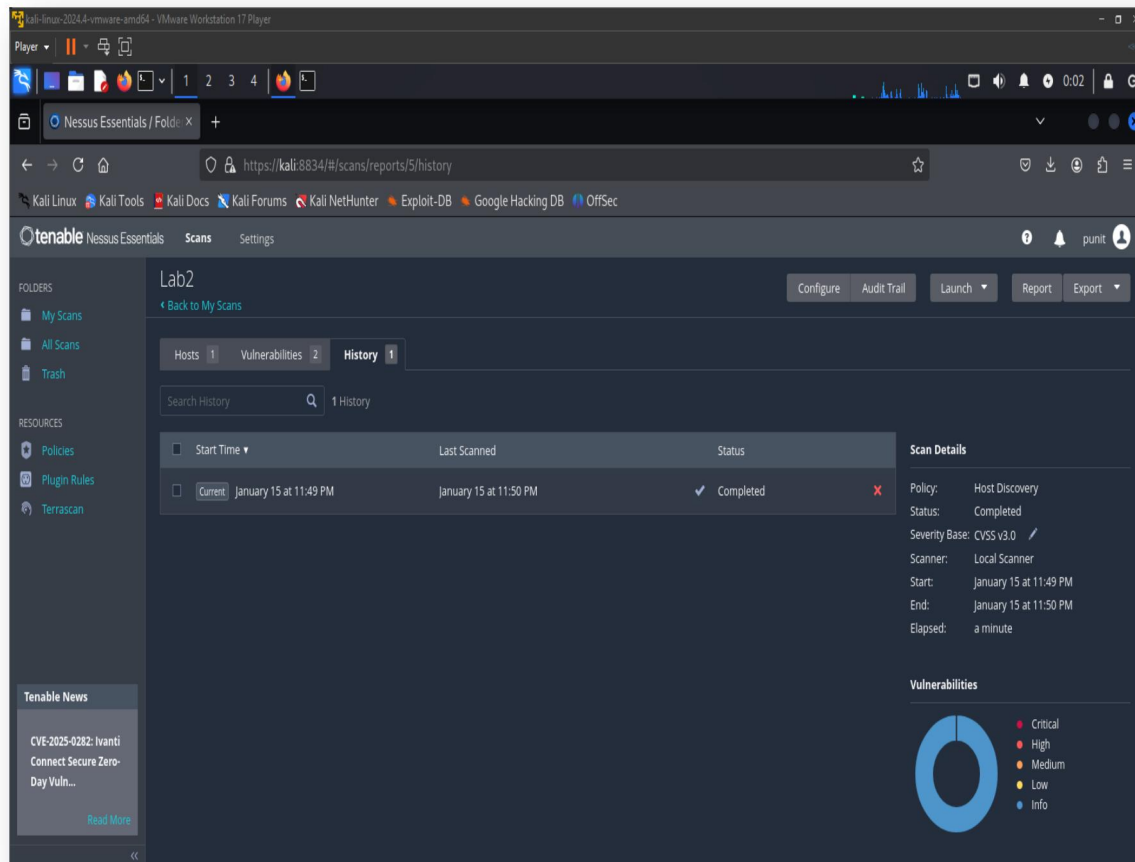
Step-4: After that it will start to scan and after the completion it will show the vulnerabilities that have in the target IP or hosts.



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.



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



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.