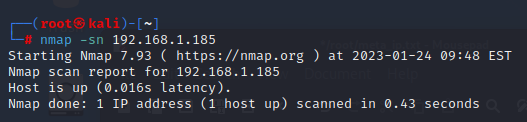
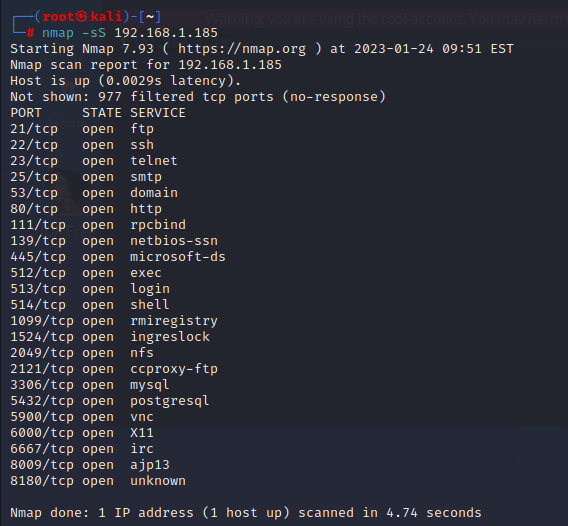
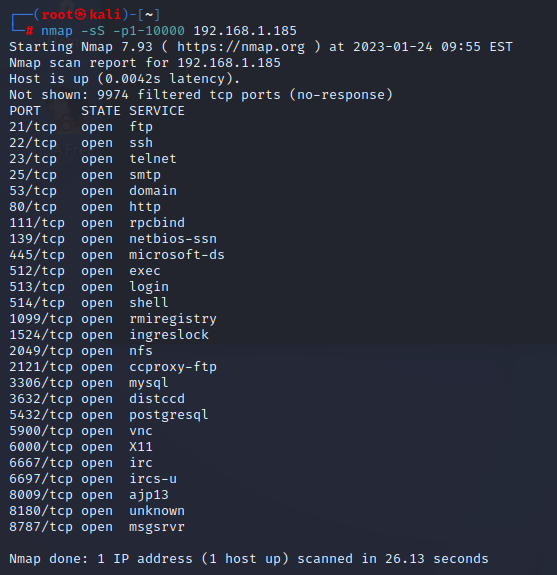
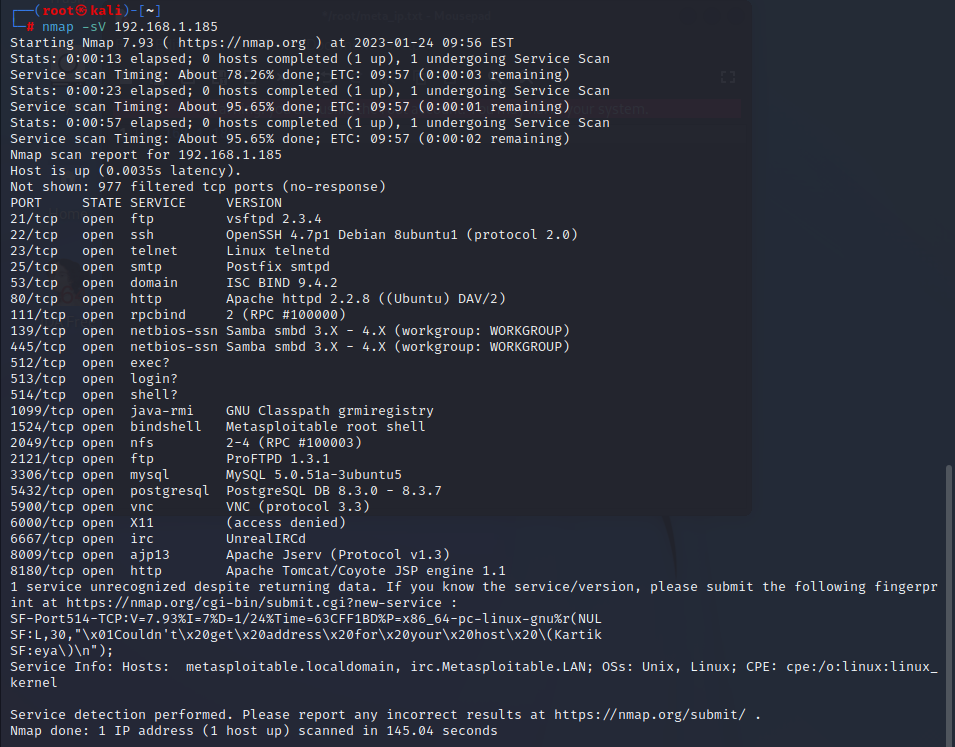
|  |  |
| --- | --- |
| **Name** | Adit Verma |
| **Roll Number** | K062 |

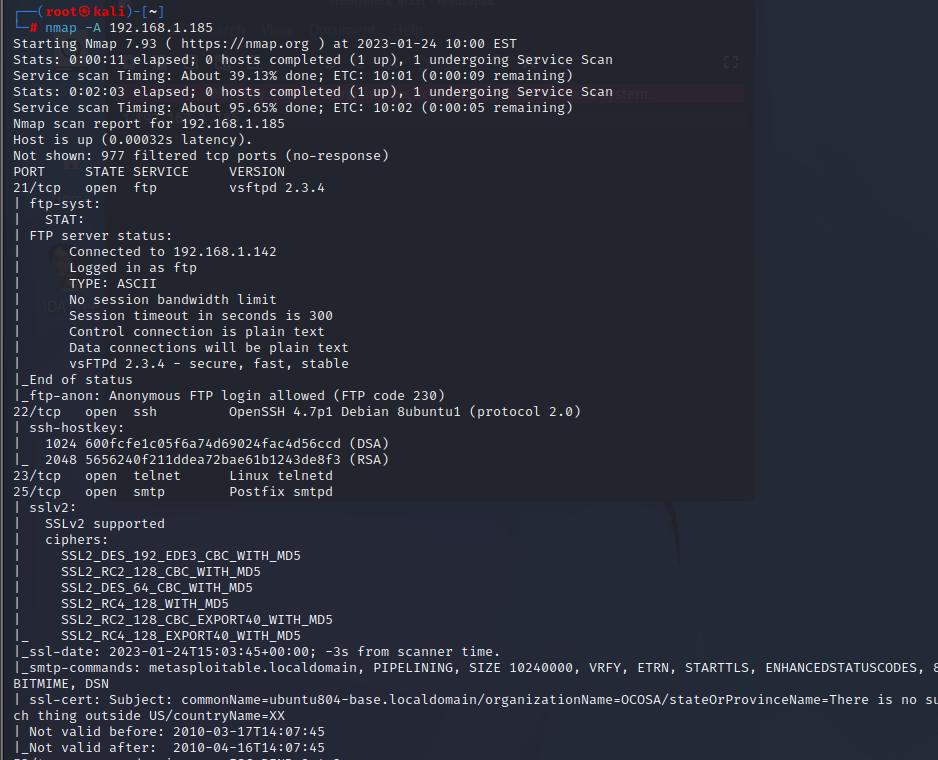
**Screenshots –**

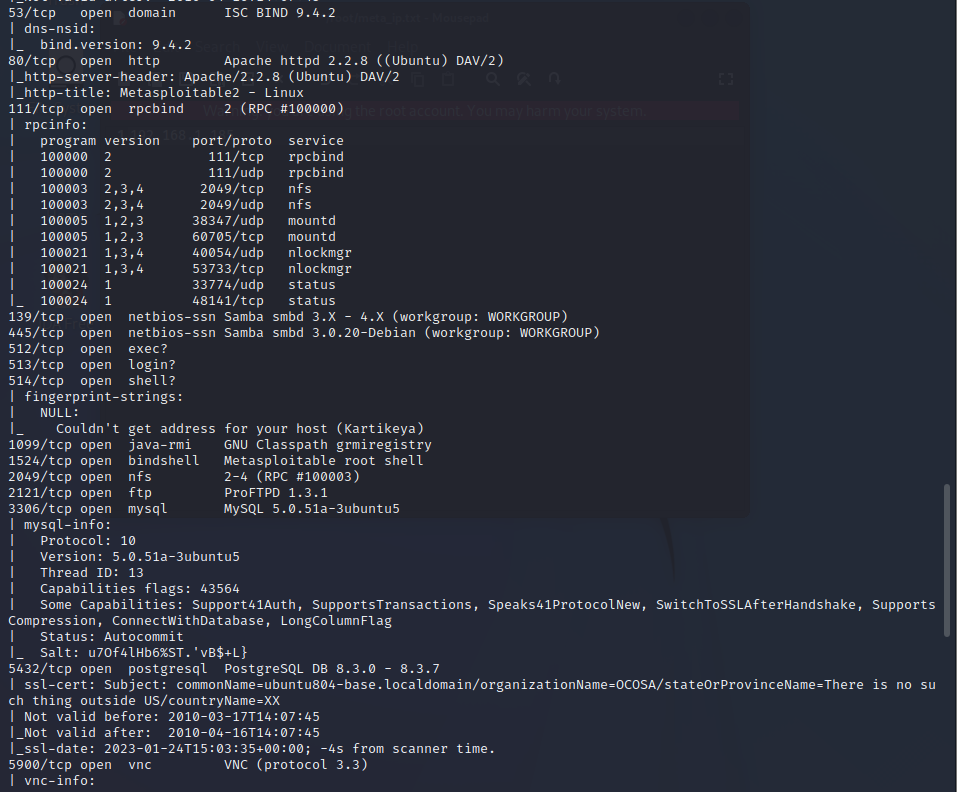


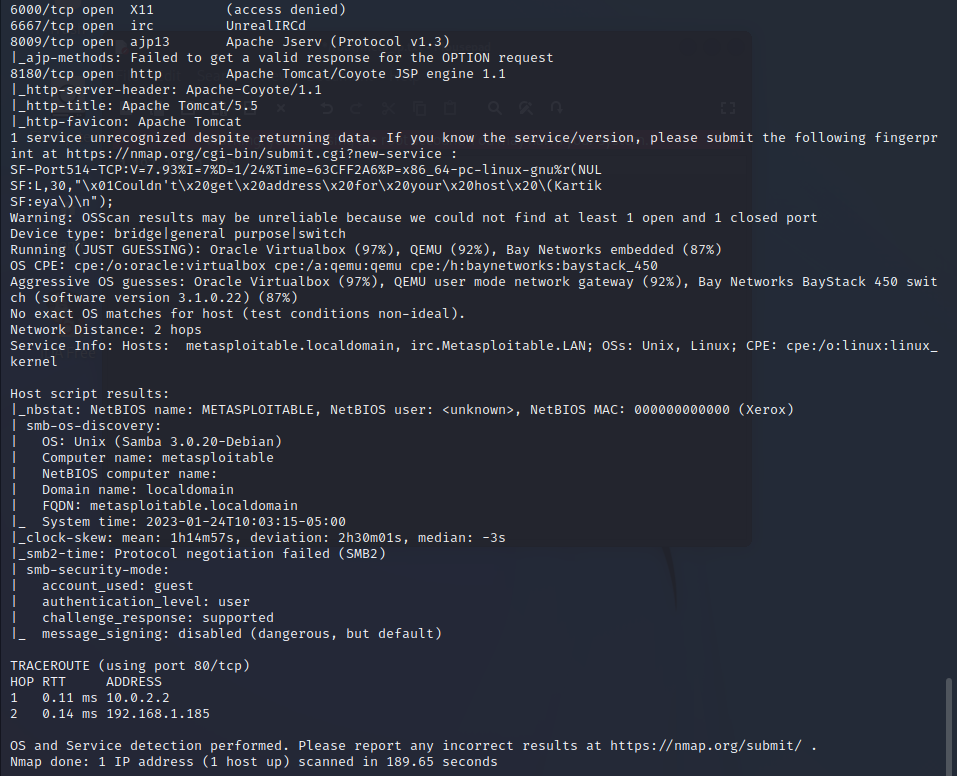


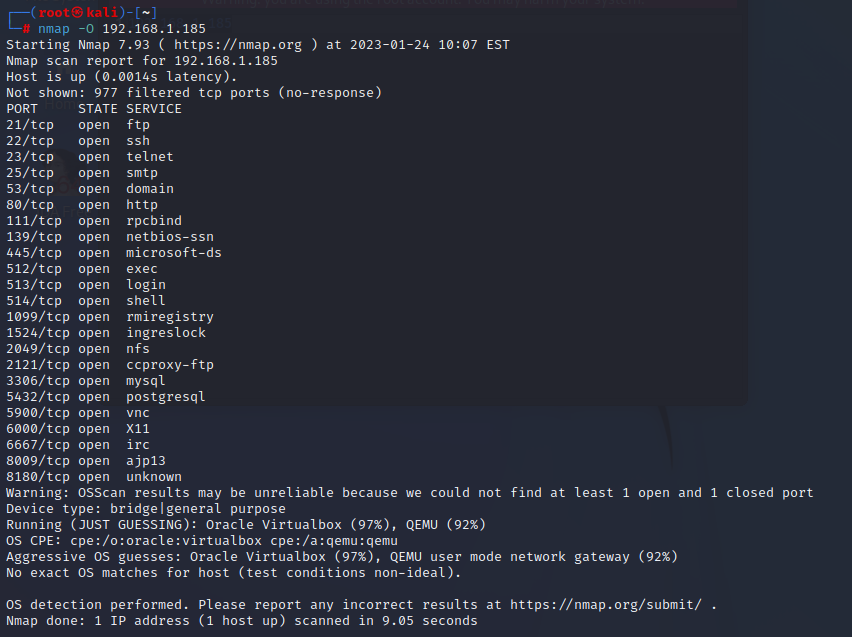


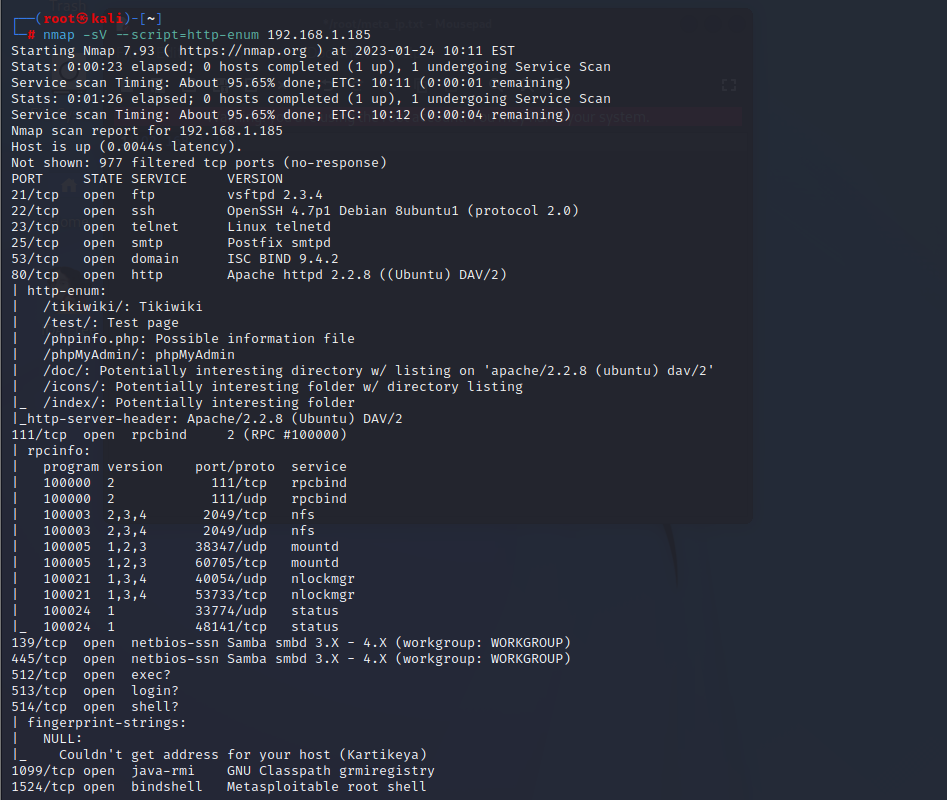


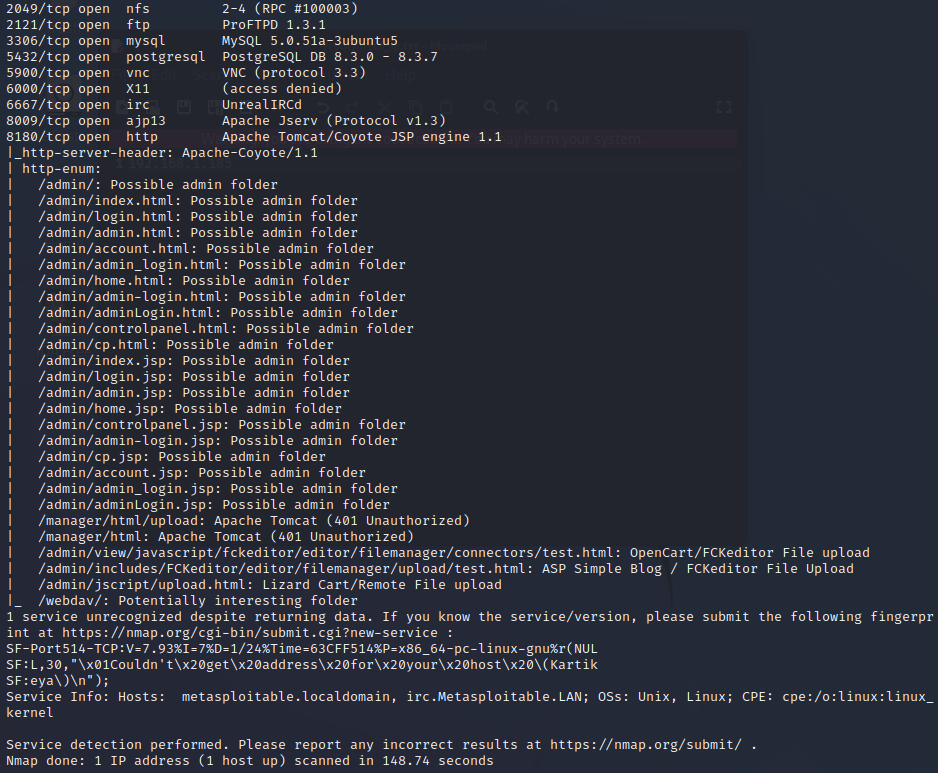




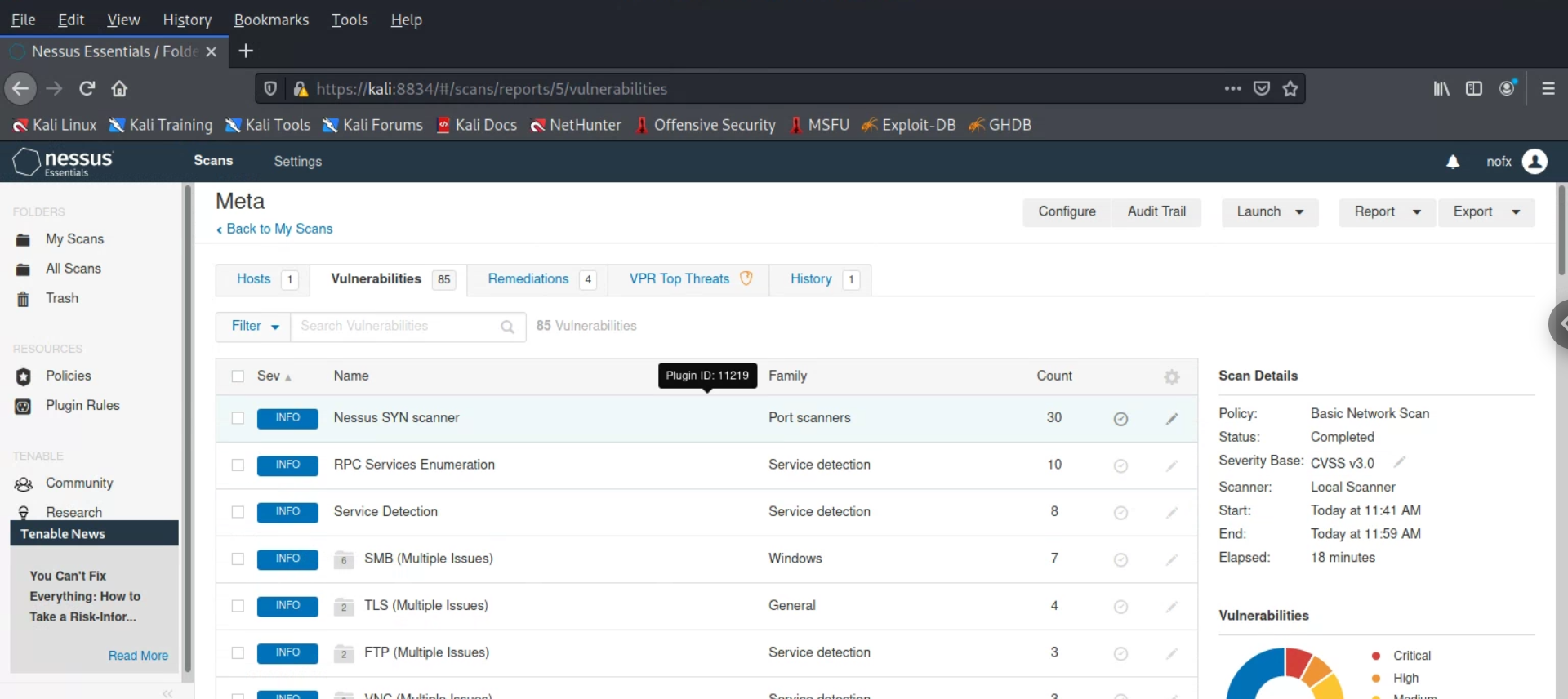


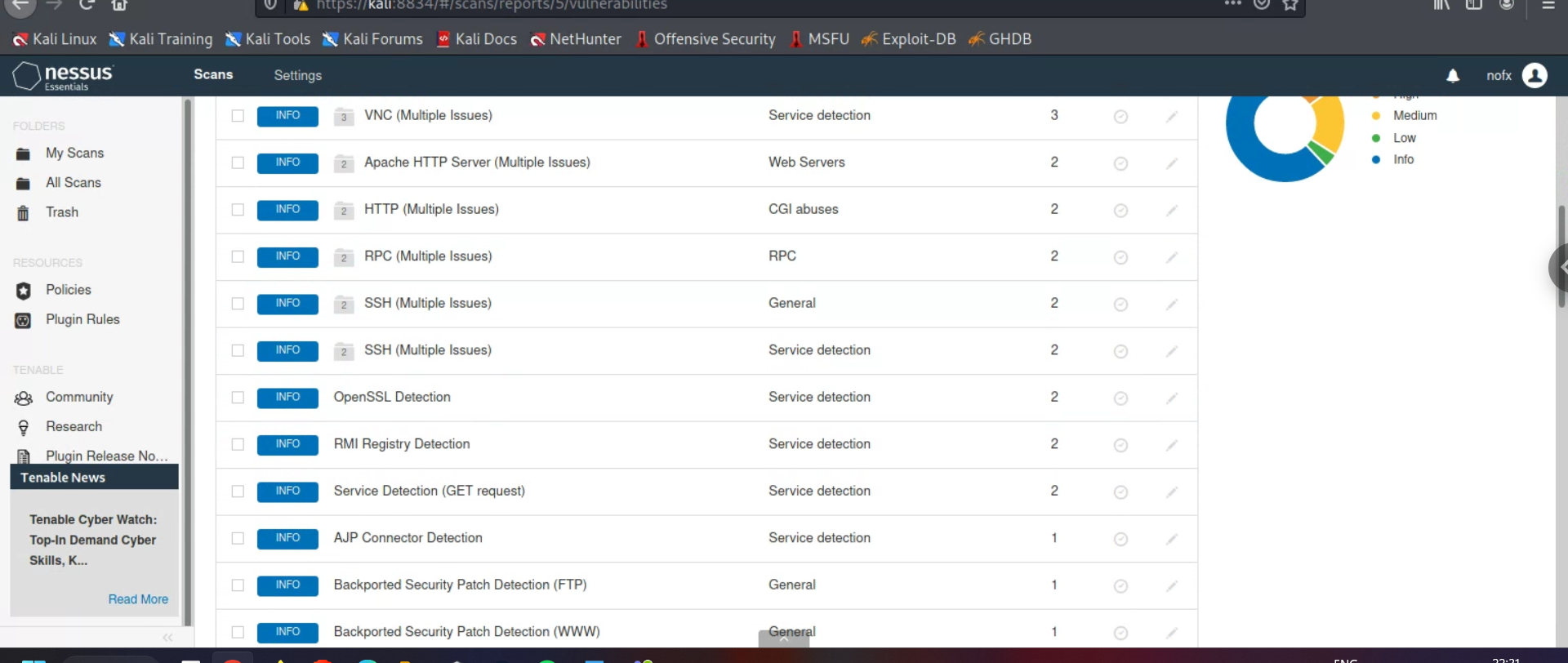


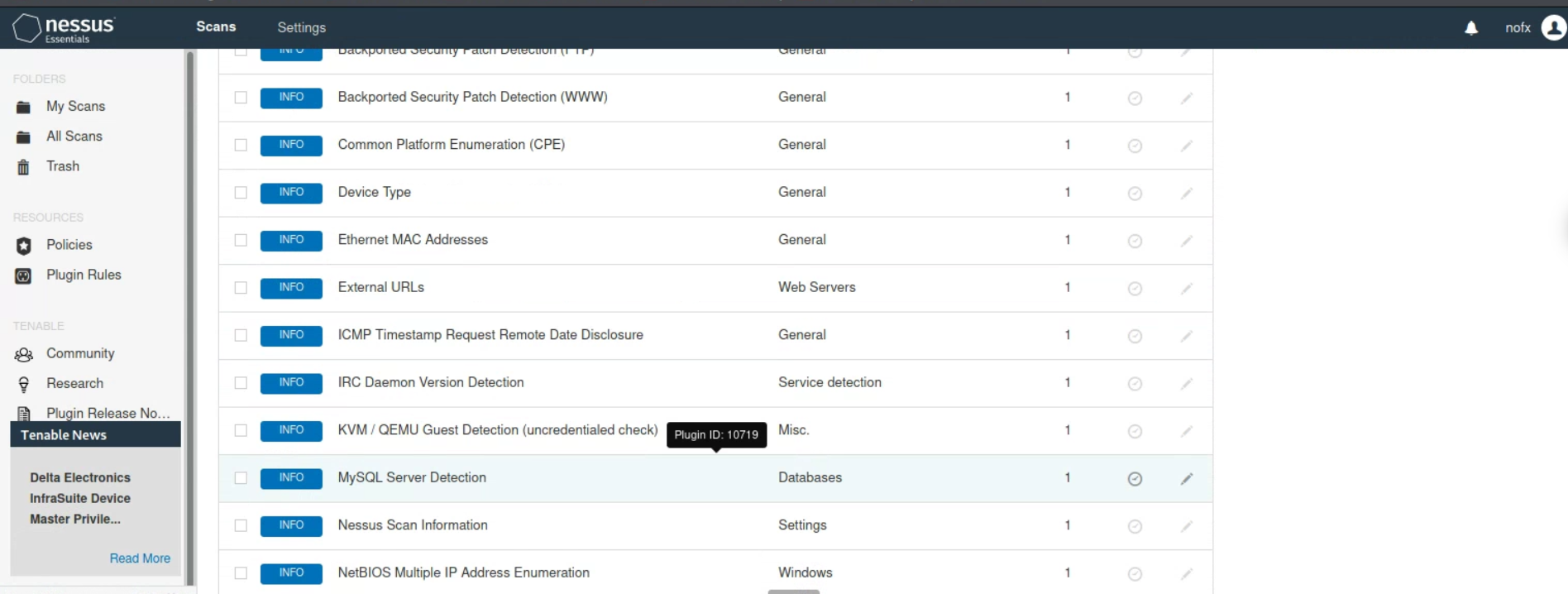


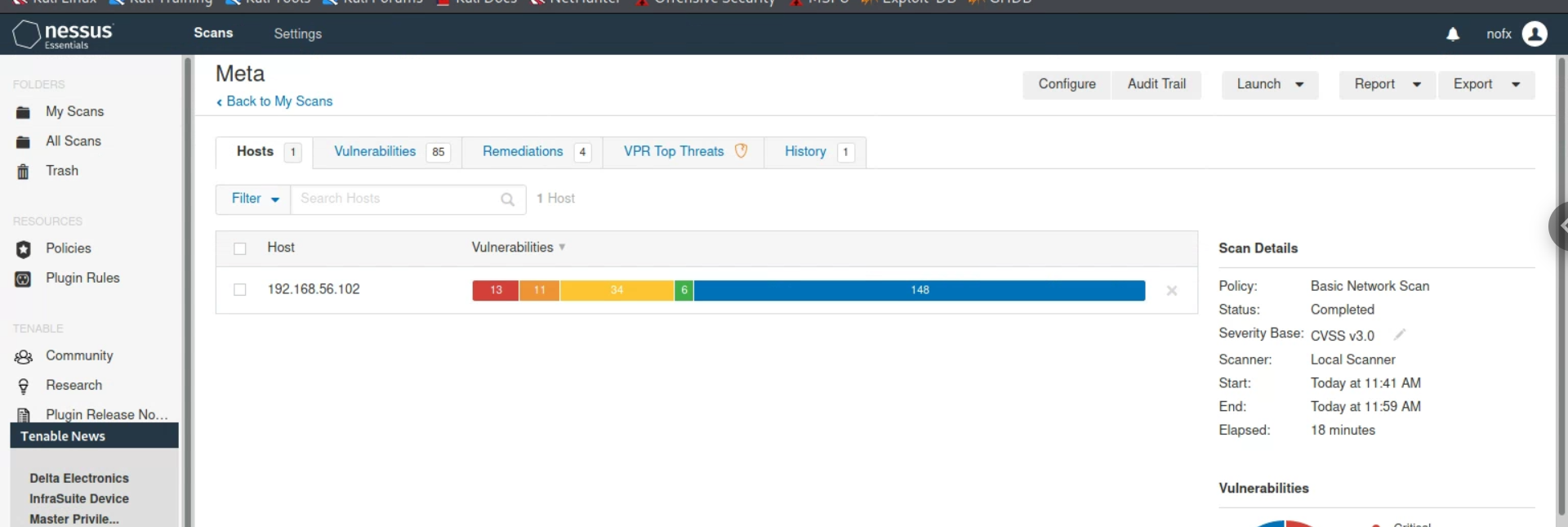


**Part 2**

****

****

****

****

**Questions –**

**Q1) What kind of information is shown when you run this ping scan for Metasploitable2?**

A) The time of the ping, the current state of the target or host, and the remaining scan time are displayed by this ping.

**Q2) Which ports are open on the Metasploitable2 VM?**

A) The list of open ports is - 21,22,23,25,53,80,111,139,445,512,513,514,1099,1524,2049,2121,3306,5432,5900,6000,6667,8009,8180

**Q3) Did you find any additional ports?**

A)The additional port open is 8787

**Q4) What additional information about the open ports on Metasploitable2 were you able to obtain by using the -sV and -A flags?**

A) The -sV flag provides information about the version of the application or service that is currently running on that port. The -A switch provides more information about the port, including the IP address to which the service is linked, as well as host scripts and traceroute.

**Q5) What operating system does nmap report Metasploitable2 to be?**

A) Nmap tells us that Metasploitable2 is running Oracle Virtualbox or QEMU .

**Q6) What web applications are available on Metasploitable2?**

1. The web applications available on Metasploitable2 are –

* http Apache httpd on port 80
* http Apache Tomcat/Cayote on port 8180

**Q7) Which vulnerabilities are critical? Of these, which appear to be most serious? Double-click a vulnerability in the report and read the description.**

A) There are thirteen critical vulnerabilities (DNS, phpMyAdmin, SSL, Apache tomcat, build shell backdoor detection, NSF exported share, rexecd service detection, unix unsupported os, VNC server password). It would appear that the SSL vulnerability is the most serious.