**Name: Shangirne Kharbanda**

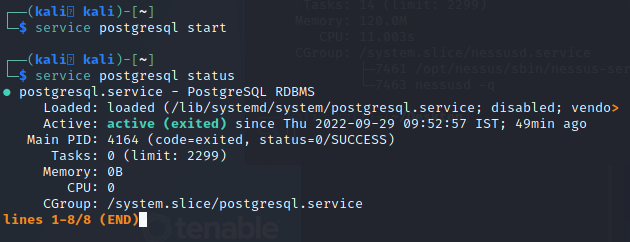
**Registration Number: 20BAI1154**

**ISAA LAB-5**

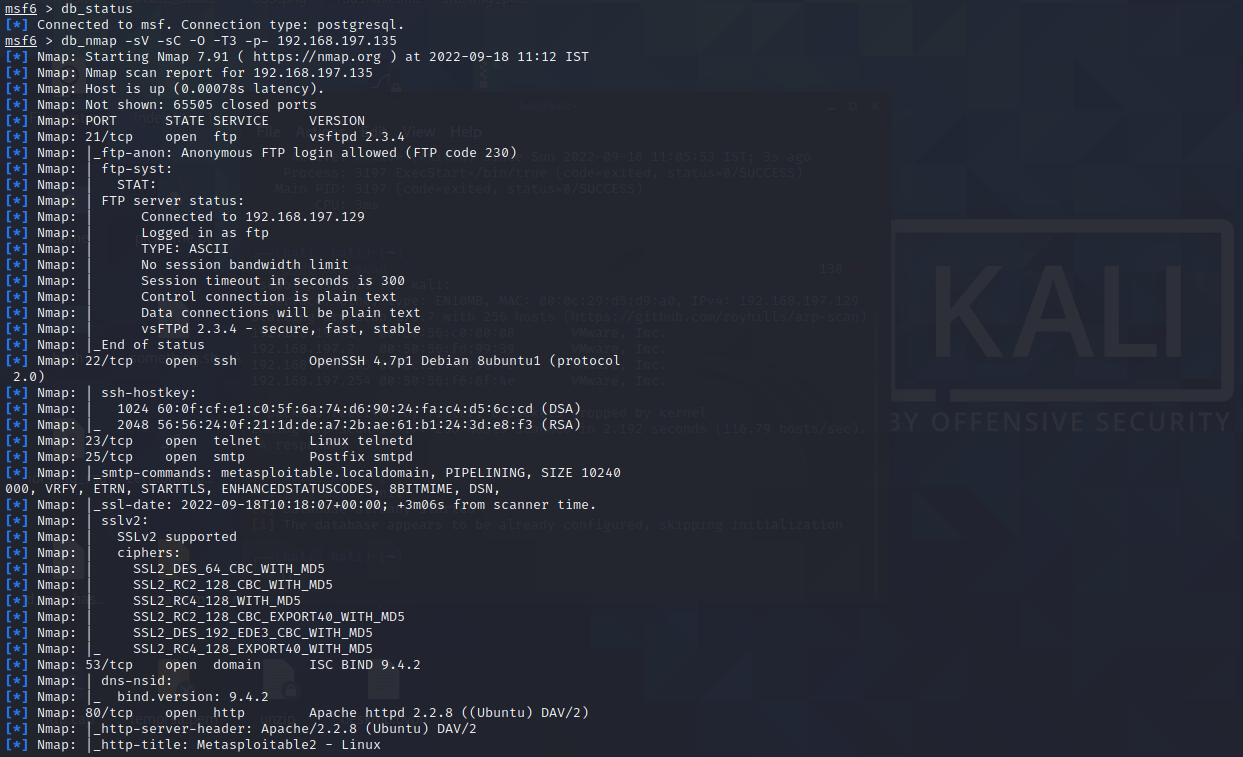
**HUNTING FOR VULNERABILITY USING METASPLOIT**

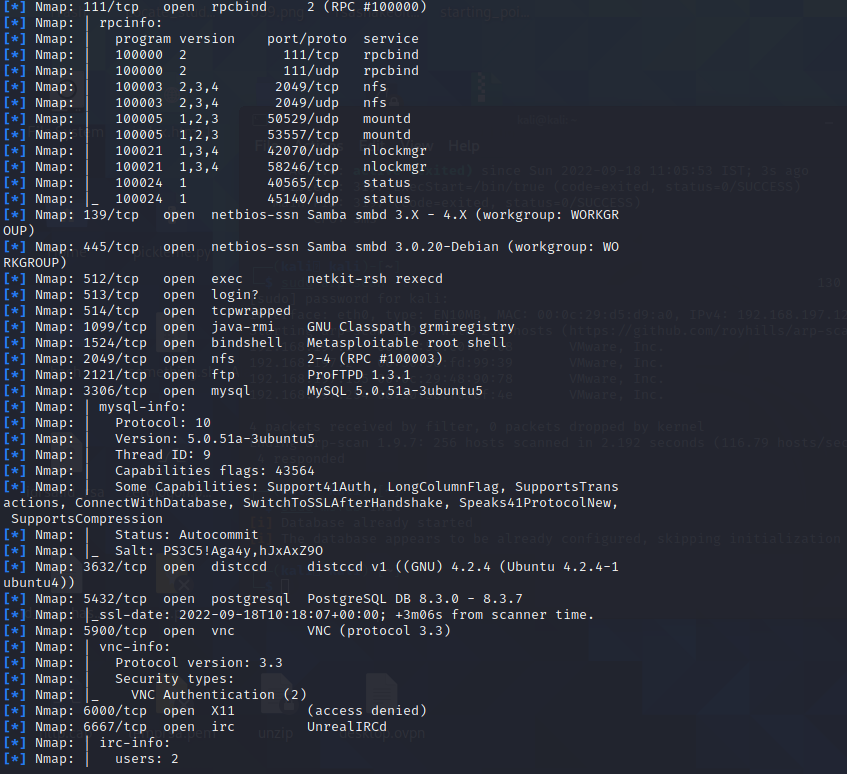
**Scanning Vulnerabilities using Nmap and storing it in the Metasploit database**

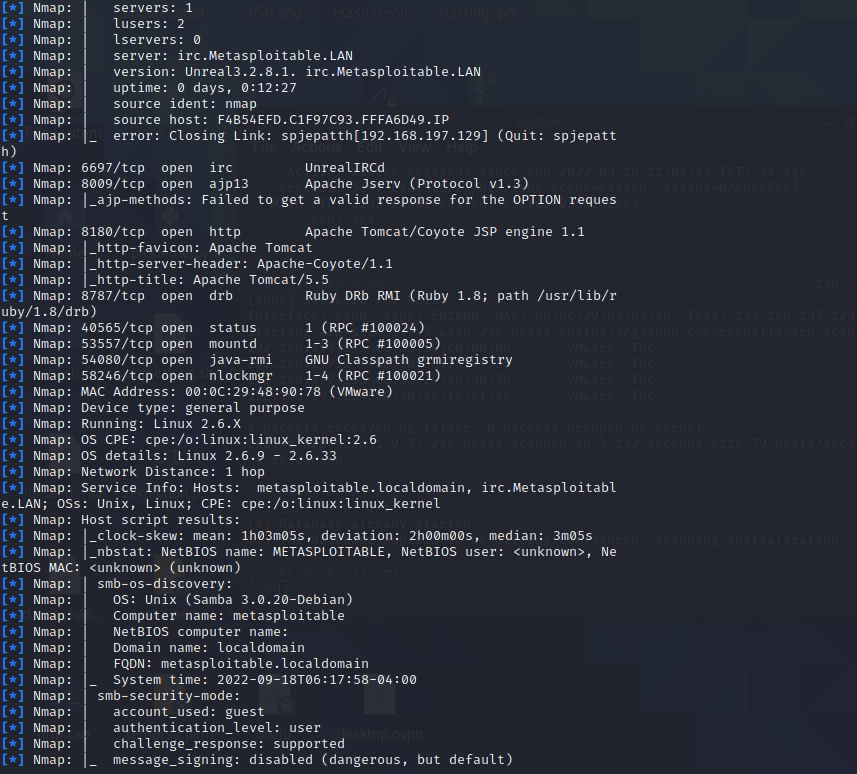
First we will start the postgresql service as follows:

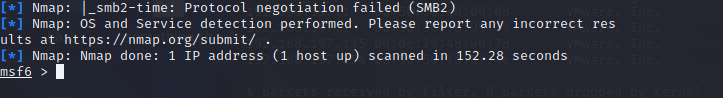


Then, we will start up msfconsole and run an Nmap scan(**db\_nmap**) on the machine in metasploit to see which ports and services are open.

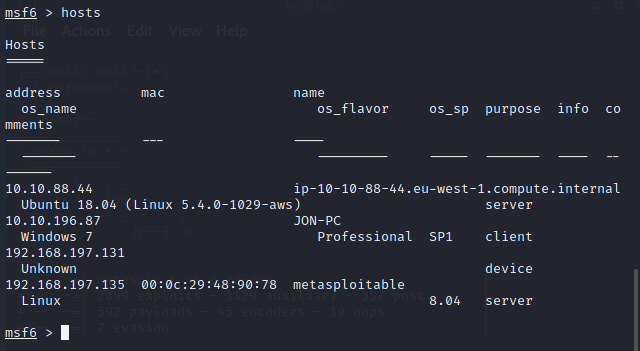




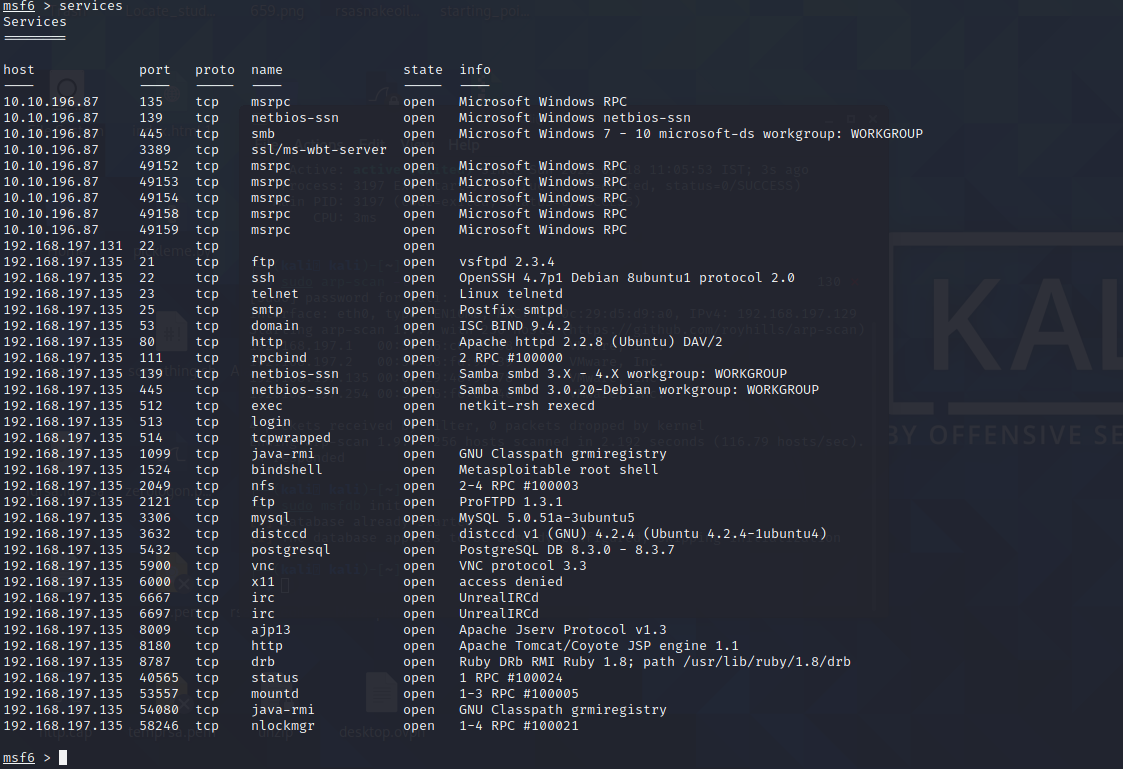




Now we will run the hosts command and see information about our metasploitable machine stored in the backend.

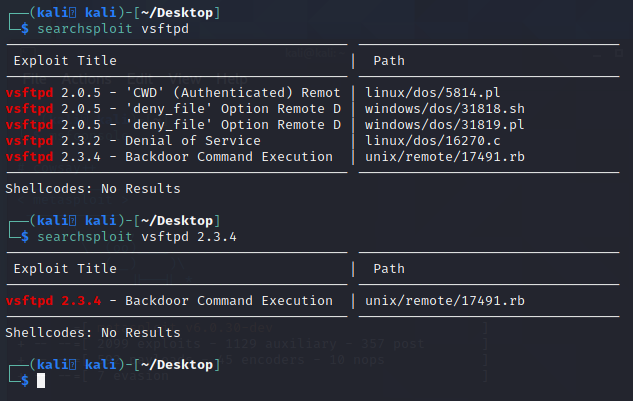


To see which services are open on the target machine, we simply type services in msfconsole as we have our nmap scan results now stored in the database.



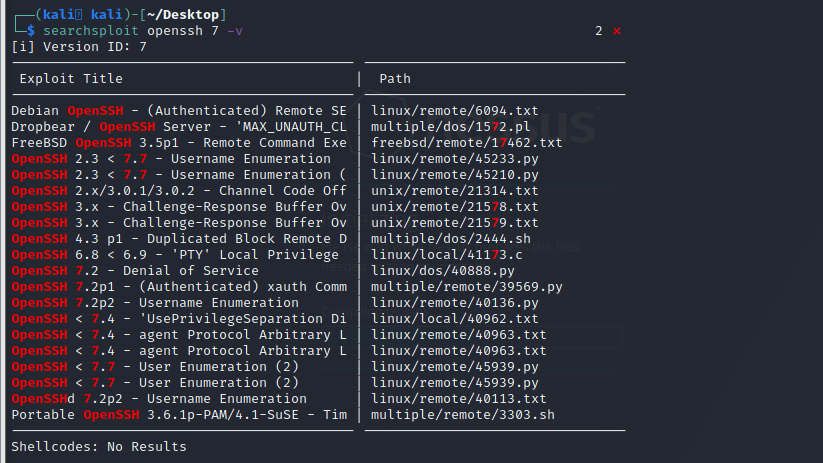
We can see that there are a bunch of services running on the site and we can search some exploits for these services using **searchsploit** in our terminal.

We see that vsfptd is running so we can search an exploit for the version running on the machine.

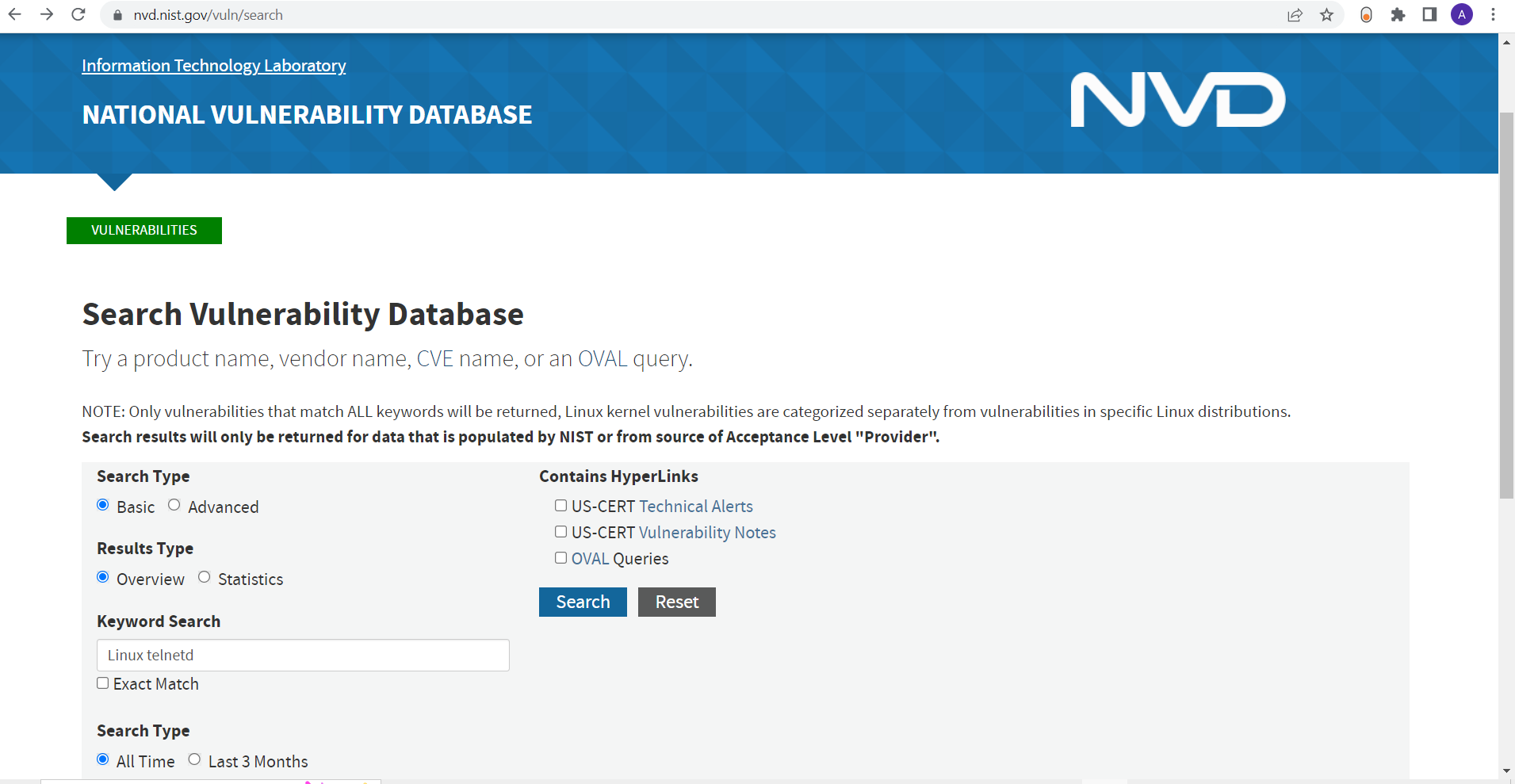


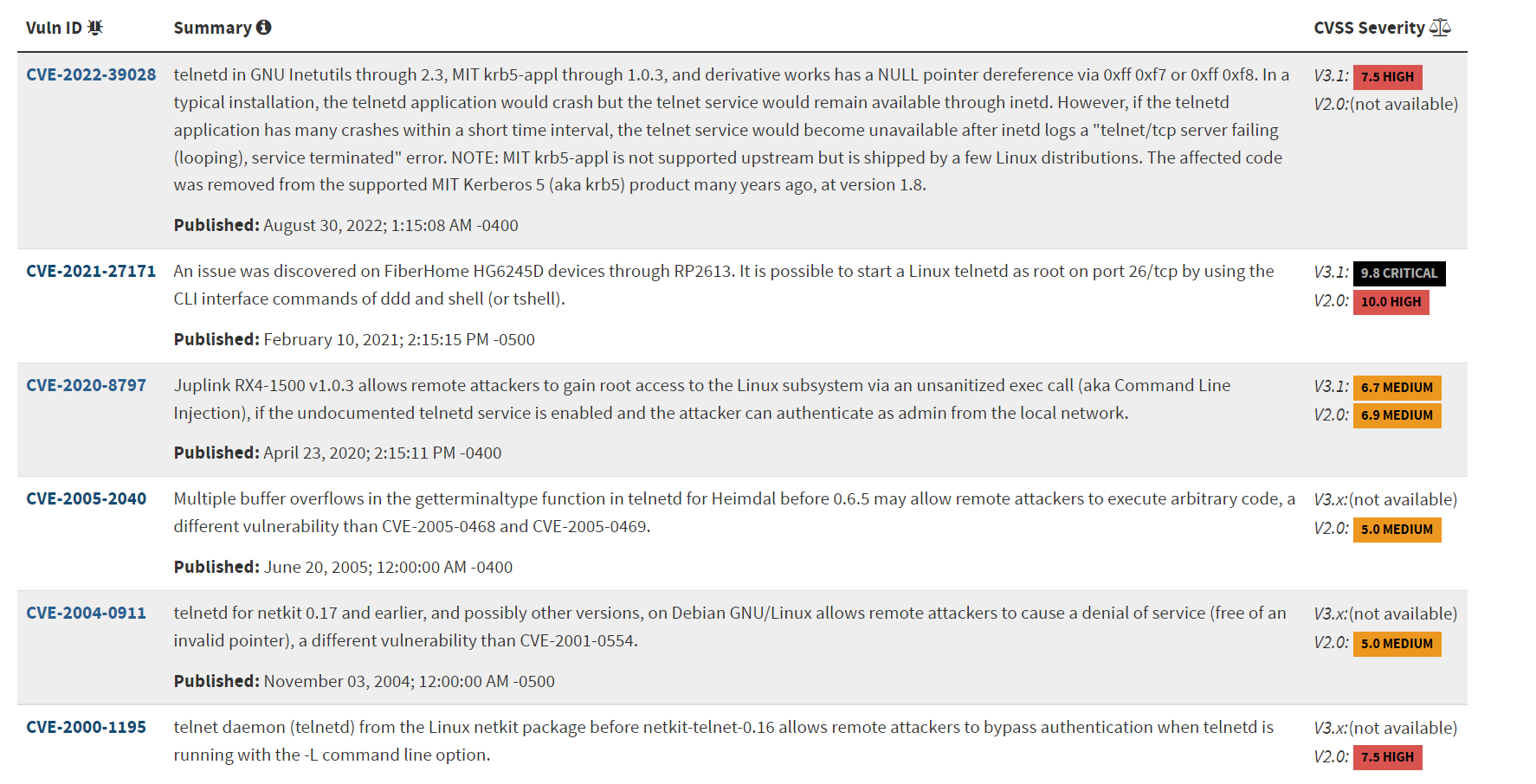
This version has this exploit which we can use to gain access to this machine.

We can see that OpenSSH is running and we can search exploits for it using searchsploit.

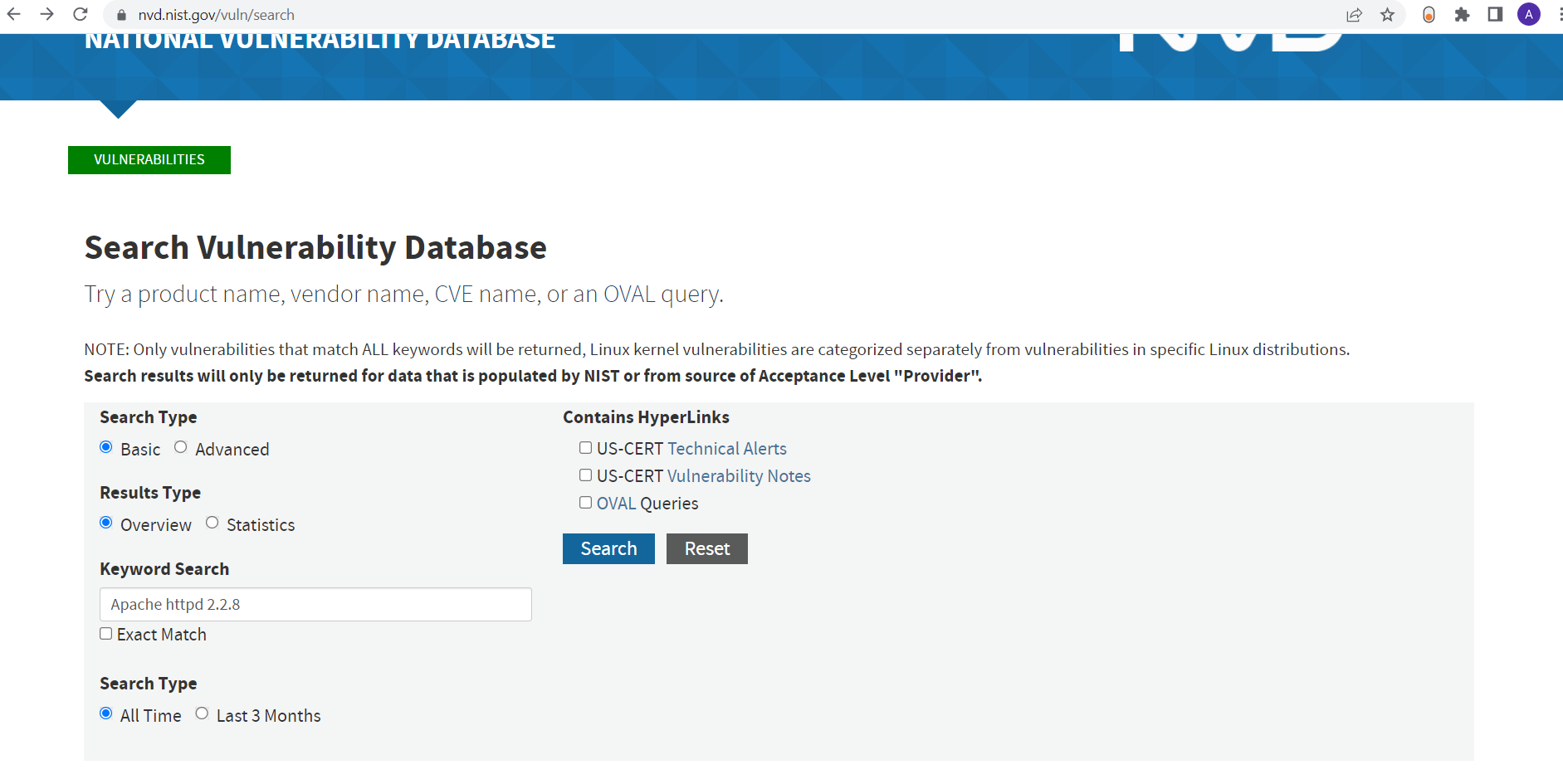


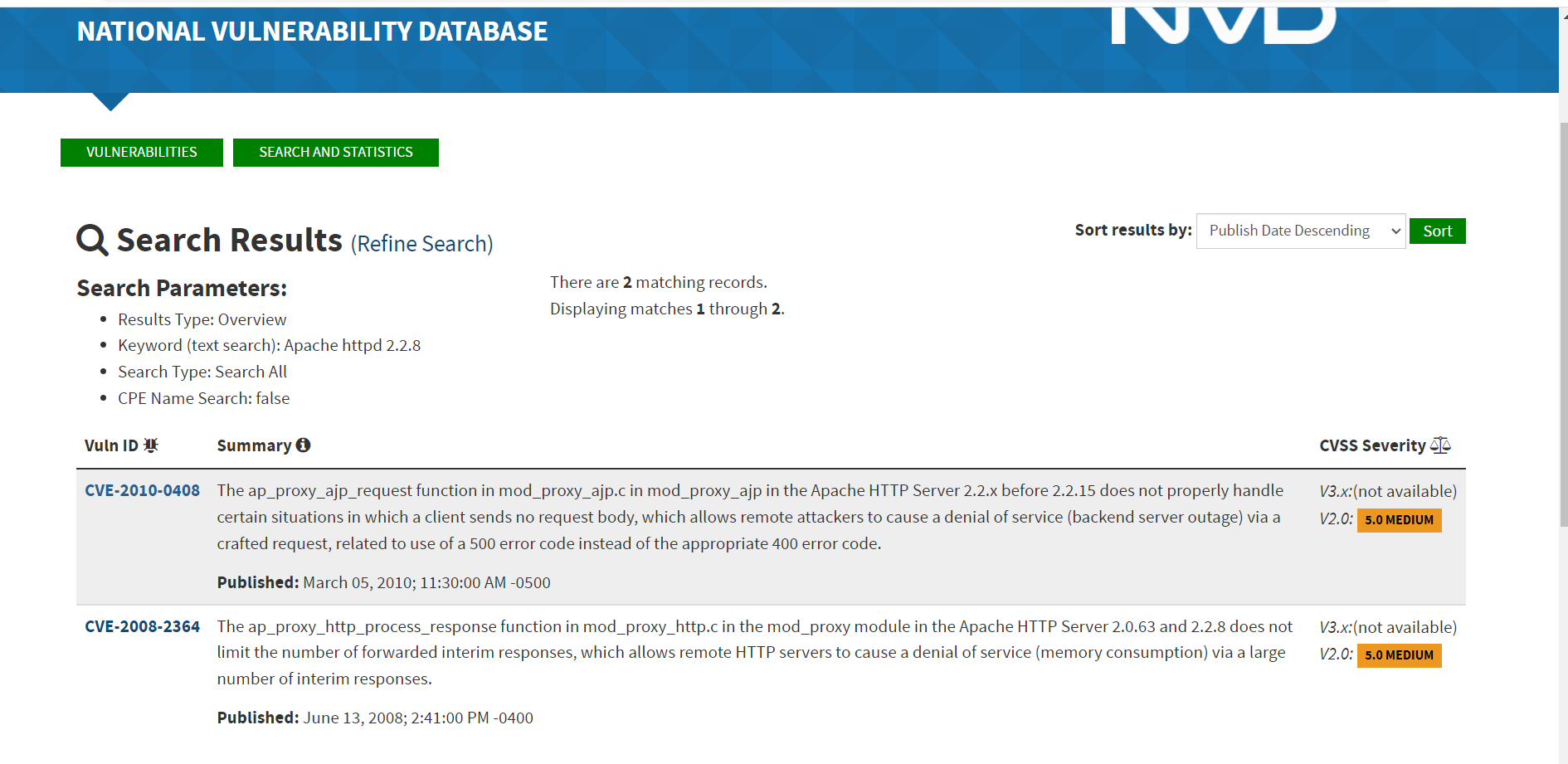
We can also search for exploits online in the NVD database and CVE details database.

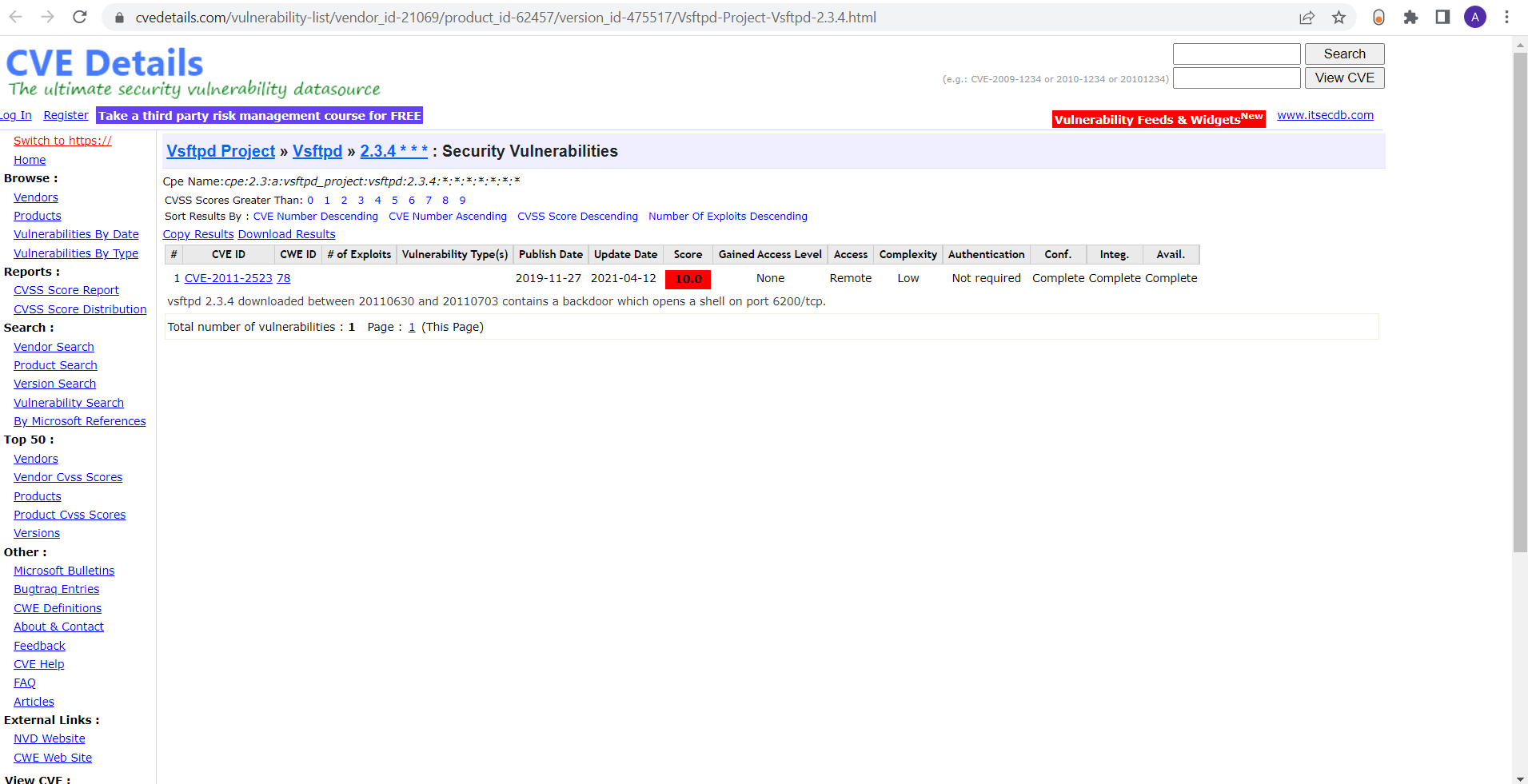




We can search for the Apache httpd 2.2.8 server vulnerability in the database that’s running on the machine which we know from our Nmap scan earlier.

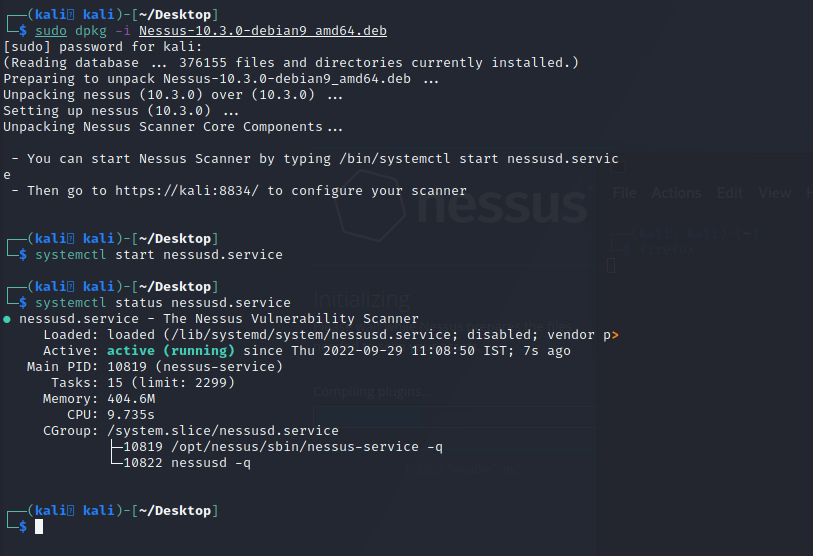




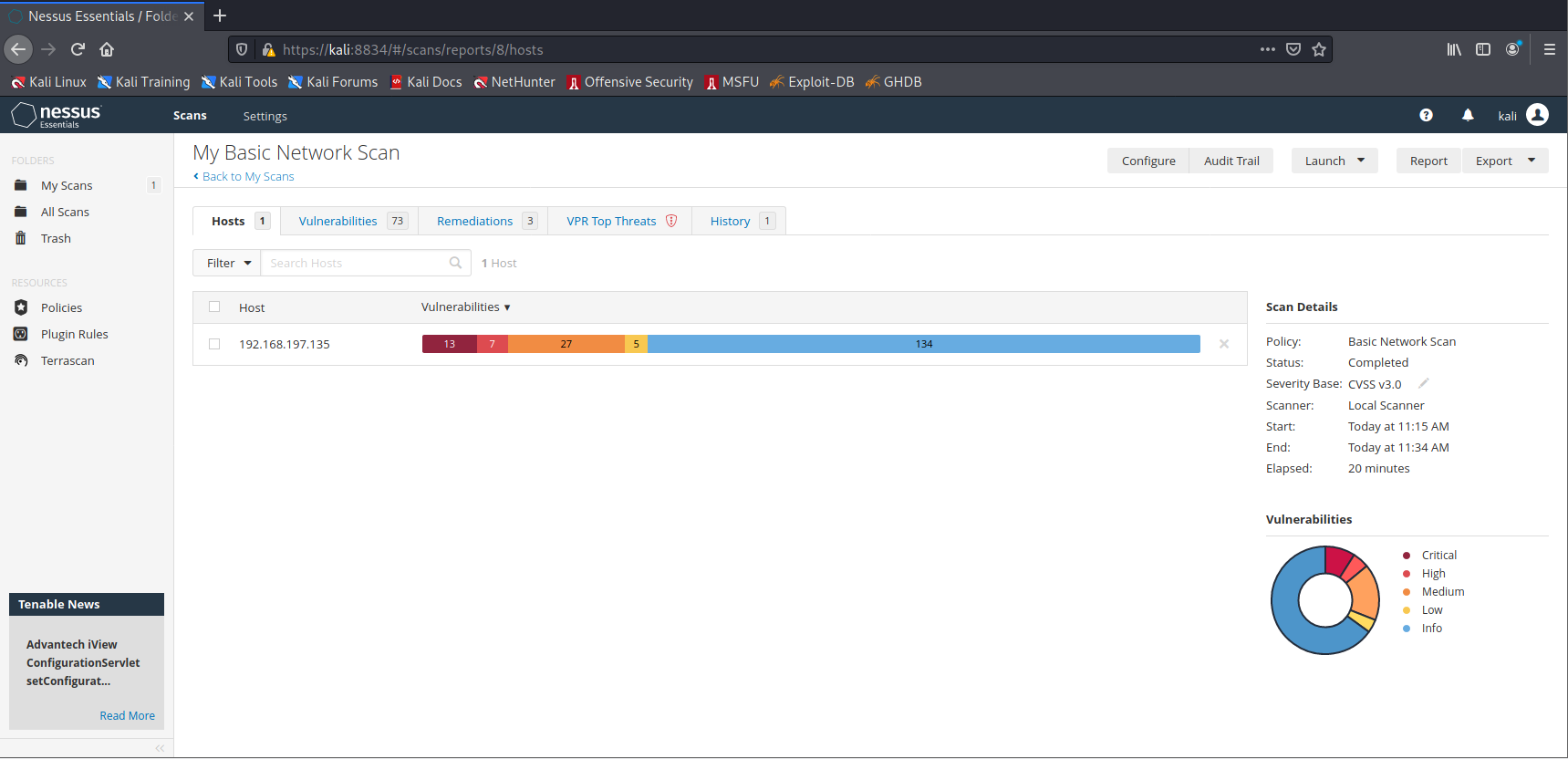


**Nessus:**

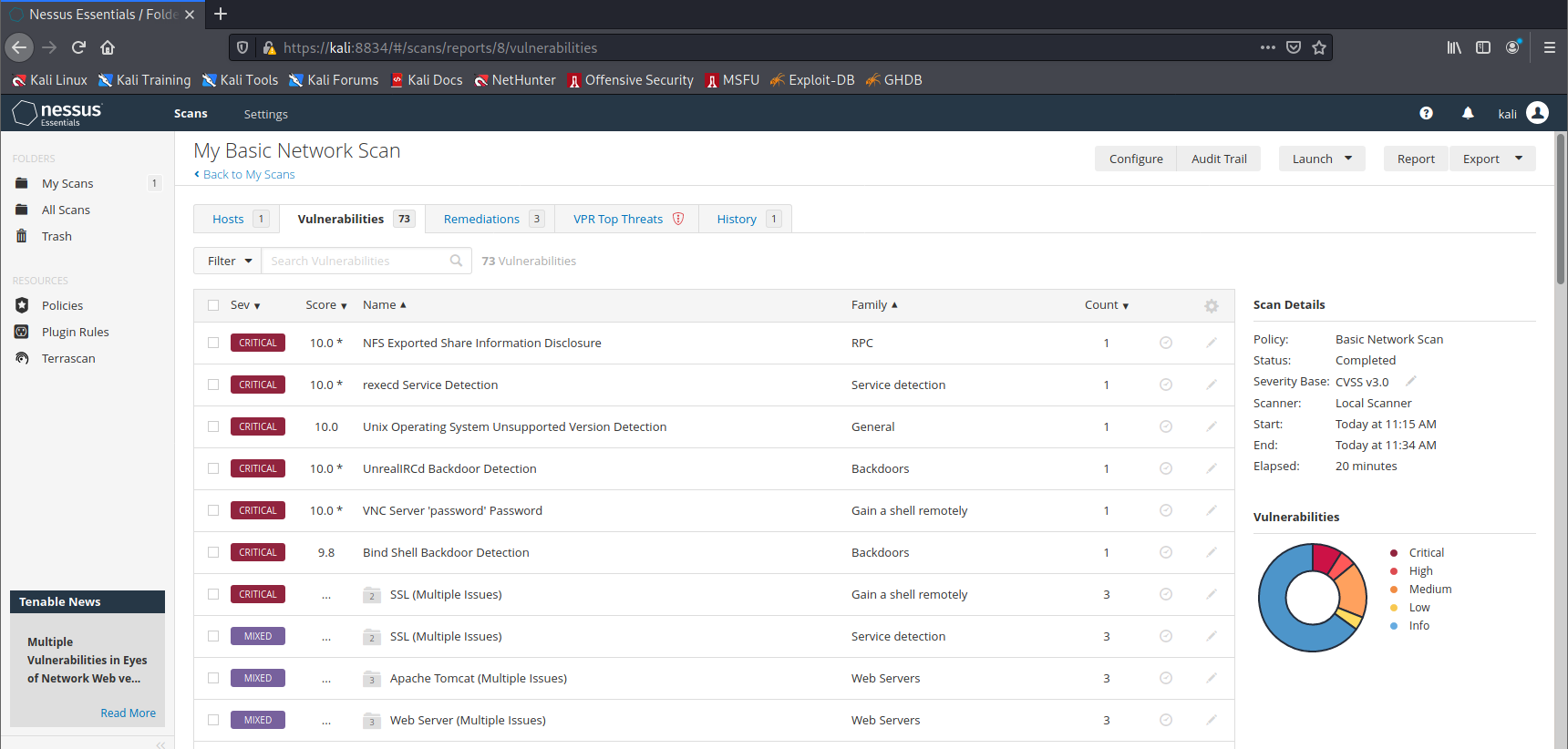
First we install Nessus as follows:



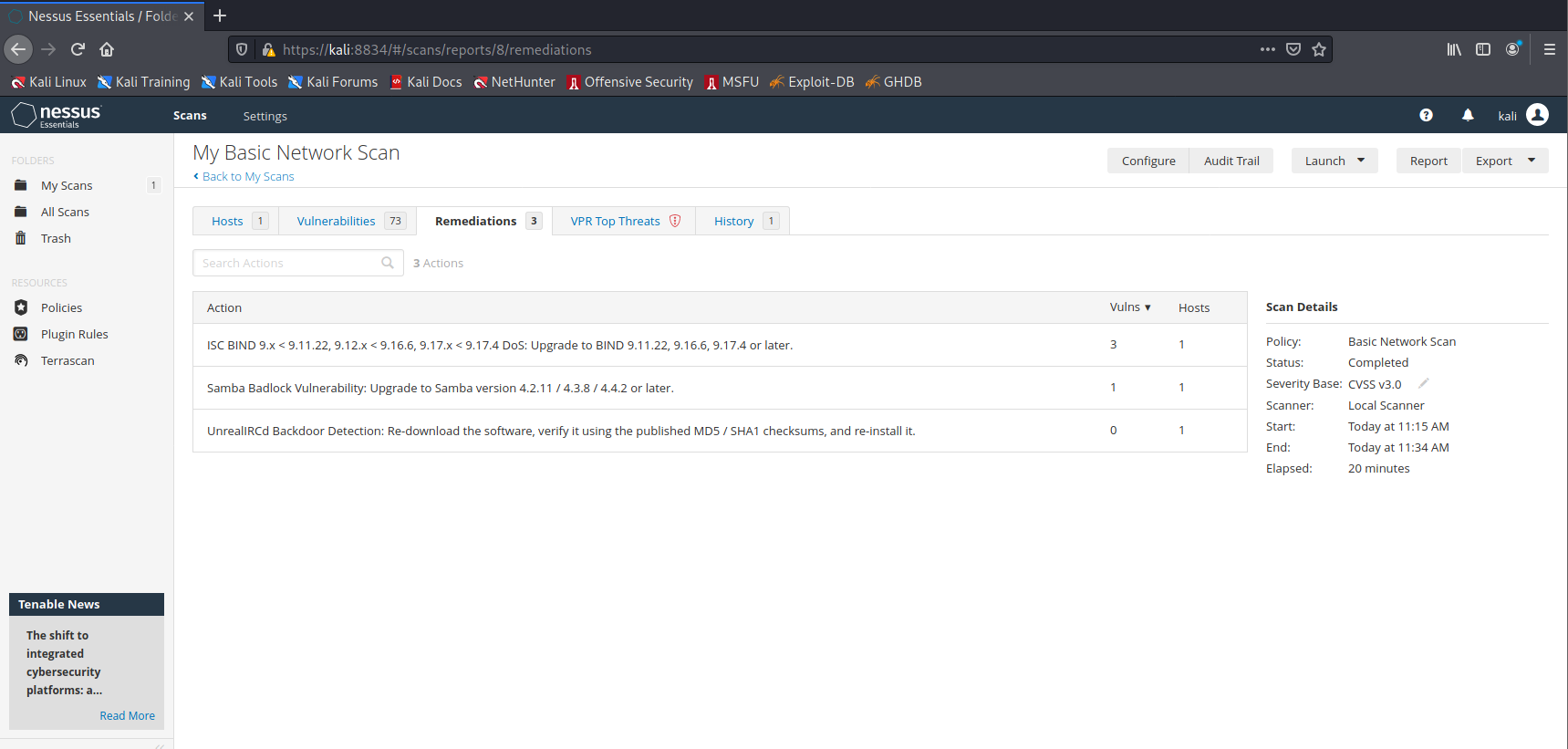
Now we will go to <https://kali:8834/> and run a Nessus scan on the target machine i.e. **192.168.197.135**.



Our Nessus scan found 73 vulnerabilities including 13 critical vulnerabilities with a CVSS score of 10.



Our Nessus scan also provided us with some remediations to remediate.



**Thus, we have hunted for vulnerabilities successfully on the target machine using different approaches.**