Metasploit & NMAP Installation on Ubuntu

**What is NMAP?**

Nmap, named after network mapper, is an open source tool used for network scanning and vulnerability detection. This free software can be used on linux, mac or windows operating systems. NMAP can give us a lot of information such as accessible IP addresses, mac addresses, open port statuses, running services, host times and operating systems, so we can say that it is indispensable for penetration tests.

The port conditions that may be encountered as a result of NMAP scanning are as follows;

**Open:** Indicates that the port is open, that is, an application accepts a connection over this port.

**Closed:** Indicates that the port is accessible but no application is behind it.

Filtered: There is no information about whether the port is open or closed. This is because a packet filtering is blocking the return packets.

**Unfiltered:** A state where the port is accessible but it is not possible to decide whether it is open or closed. It gives information about whether the ACK packets in the 3-way handshake have been received.

**Open|filtered:** Nmap cannot decide whether ports are open or filtered. (Applies to UDP, IP Protocol, FIN, Null, Xmas Scan.)

**Closed|filtered:** Nmap cannot decide whether ports are closed or filtered. (Only for Idle Scan.)

Our topic is NMAP, which is one of the most important tools that come to mind when it comes to network scanning and vulnerability detection in the field of cyber security.

Some of the topics you can do via Nmap

- Nmap scan port states

- Nmap installation

- Using Nmap

- Nmap scans

-- TCP Syn Scan

-- TCP Connect Scan

-- FIN Scan

-- XMASS Scan

-- PING Scan

-- UDP Scan

-- IDLE Scan

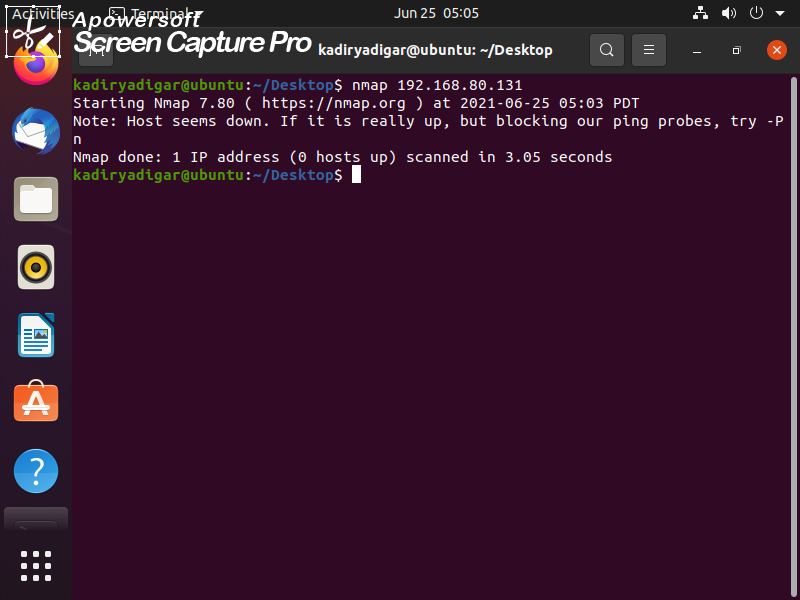
-- NSE – Scanning with Nmap Scripting Engine

Nmap is an open source software. I will show this resource on linux.

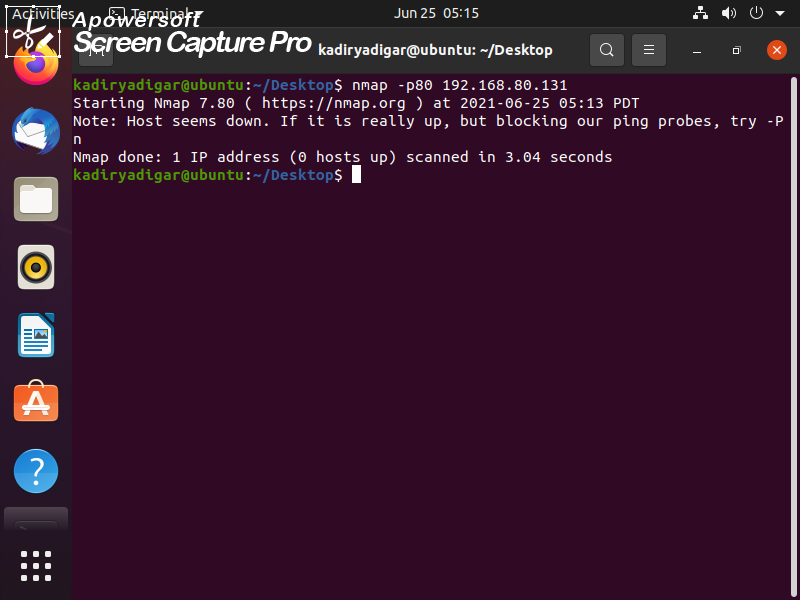


installation part

After the installation process is complete, we can proceed to our scanning processes.



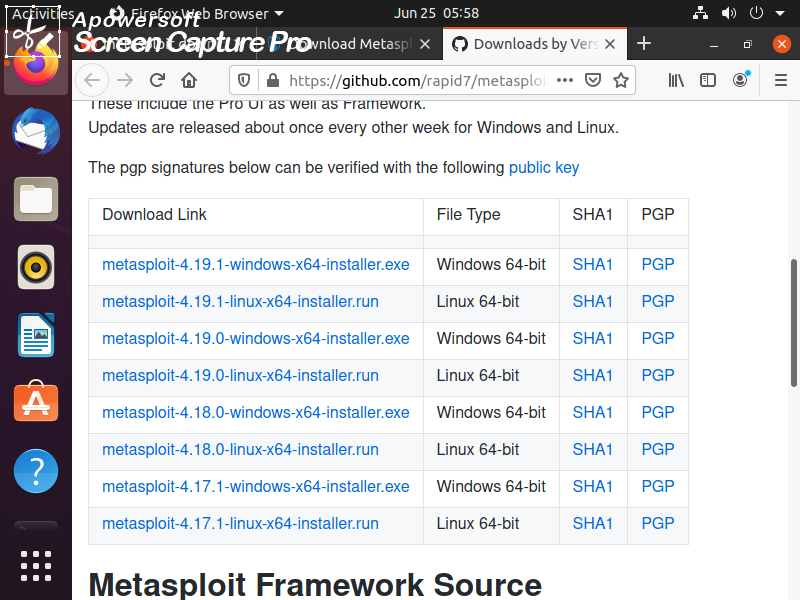
Example, I find a ip adress but I cannot access its ports because this ip adress inaccessible by admin. By doing the transaction here, we saw whether the address is open or not.



Now, Let's go to the installation of the metalsploit program .



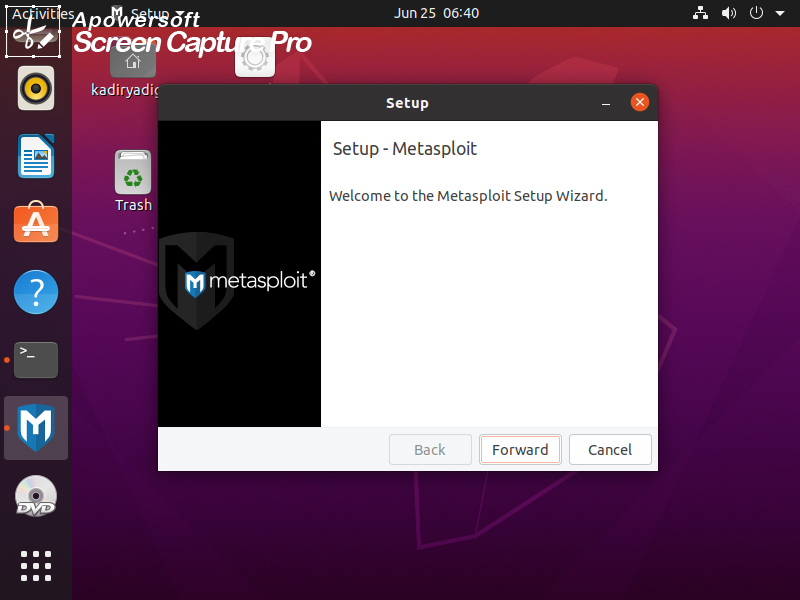
You can access open source software as a pictures



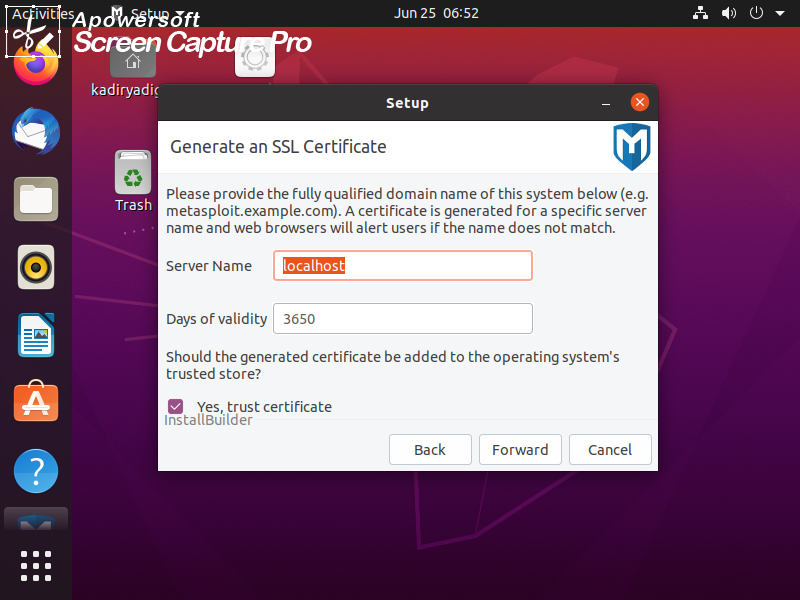
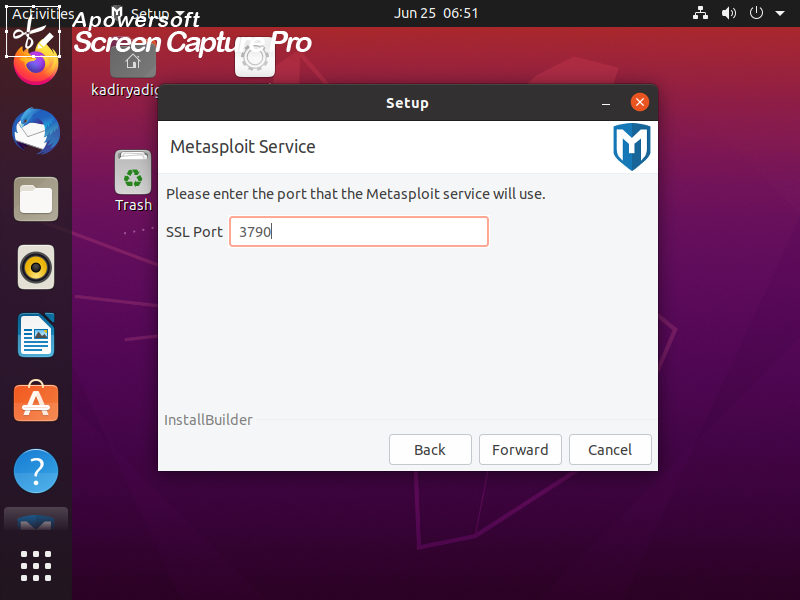
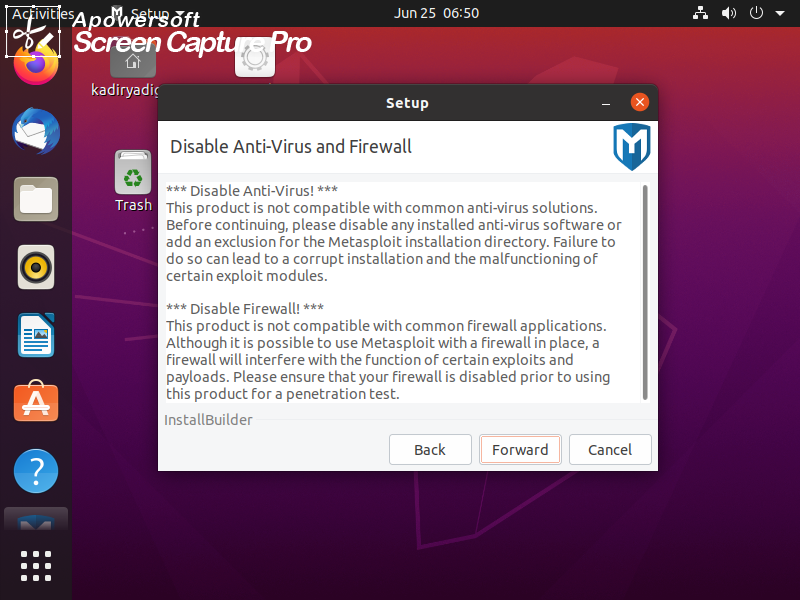
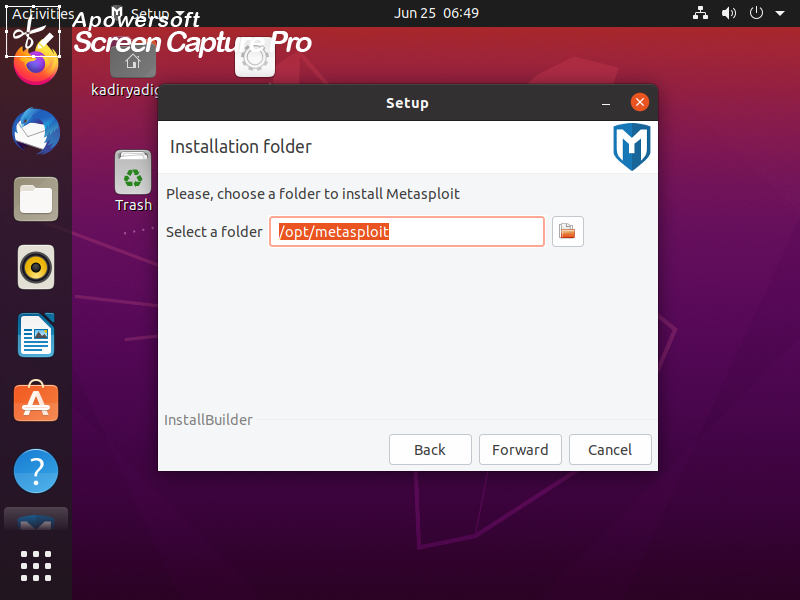
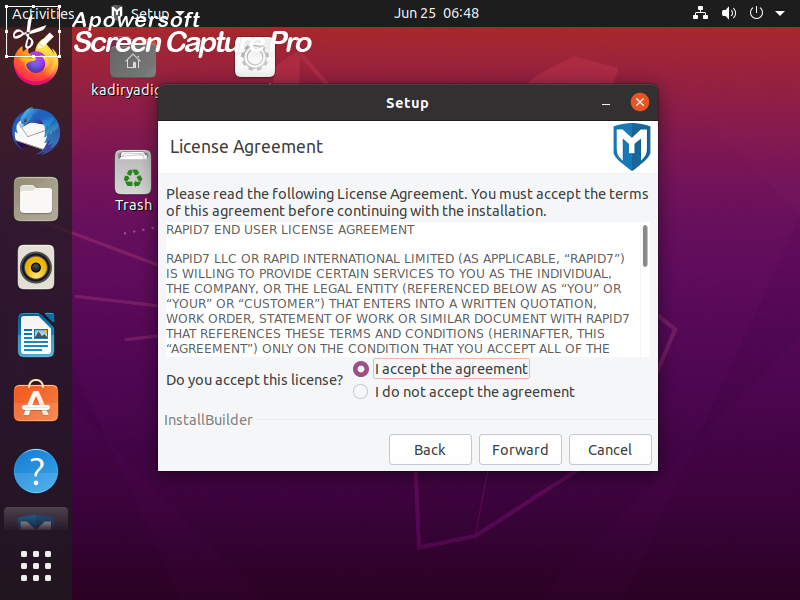
It would be a mistake for you to try to install normally via terminal. First we need to assign yourself as the super user. Then you can type the installation commands.



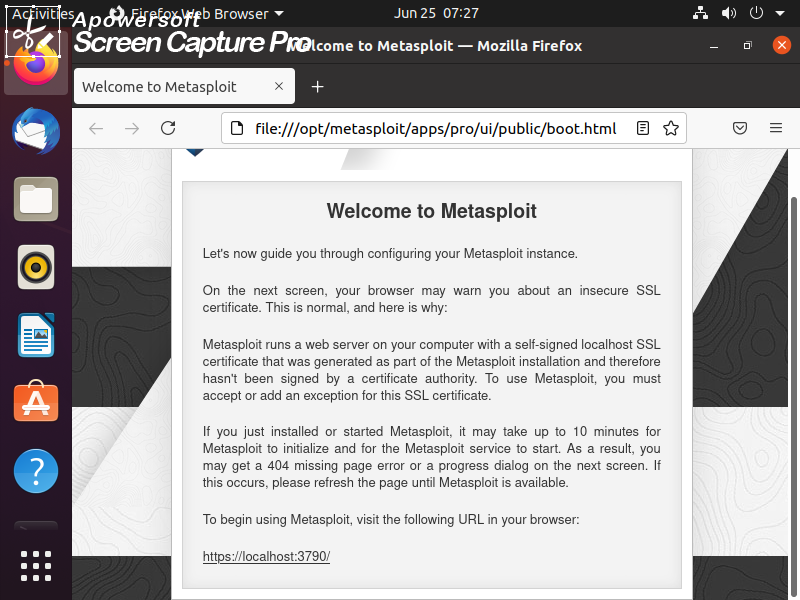
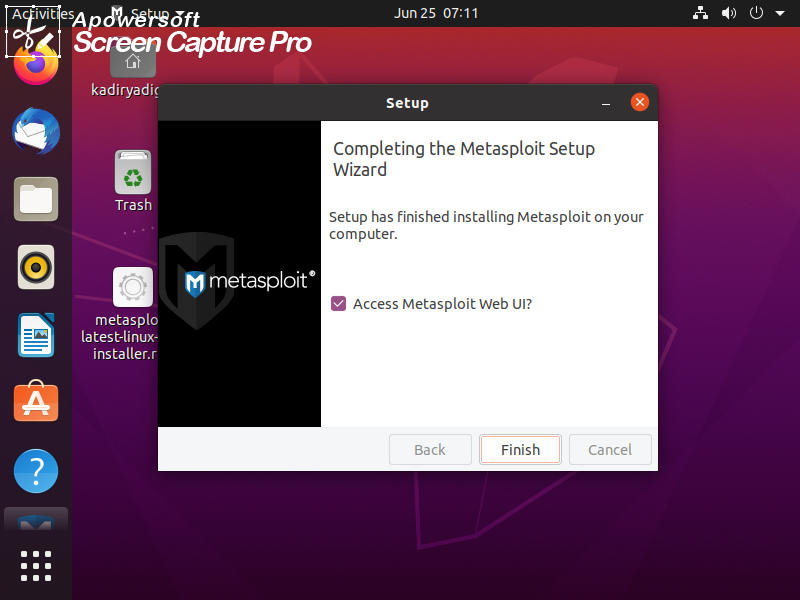
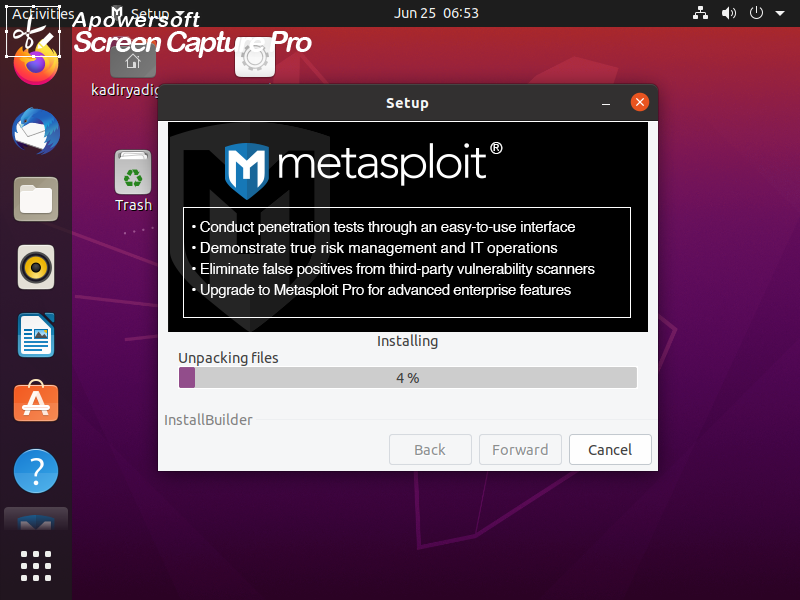
After typing the codes, the loading screen appeared



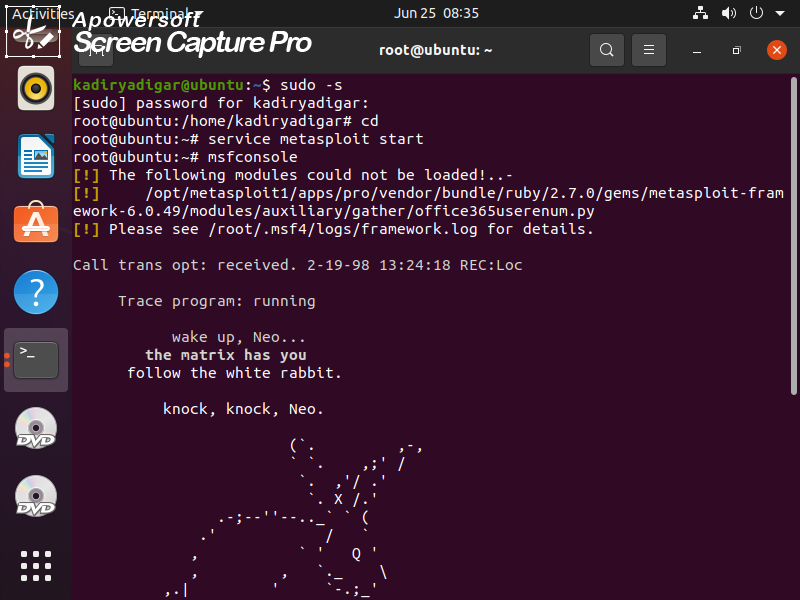
in the next steps..



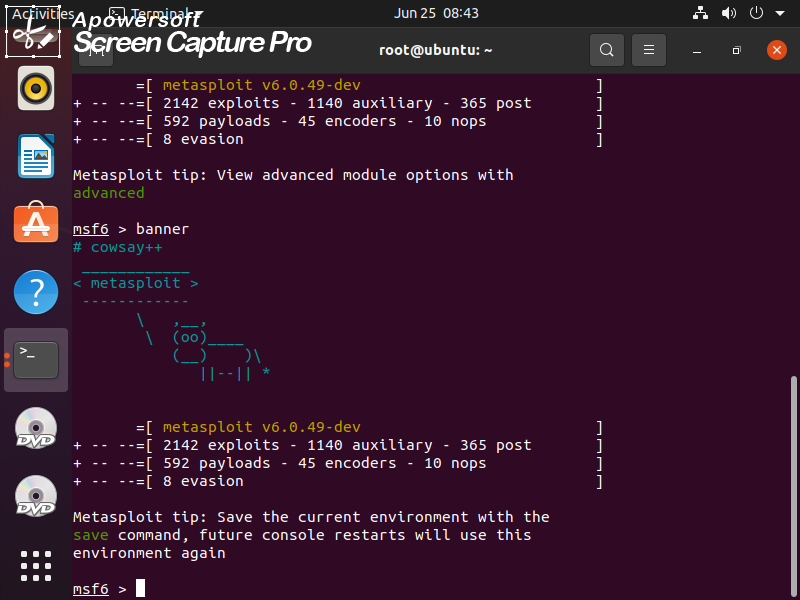
As you can see, loading operation is starting!!



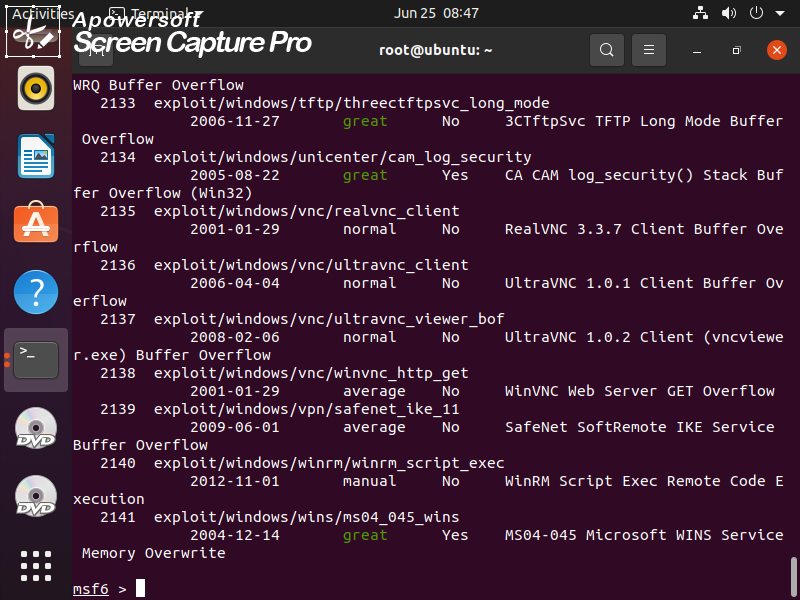
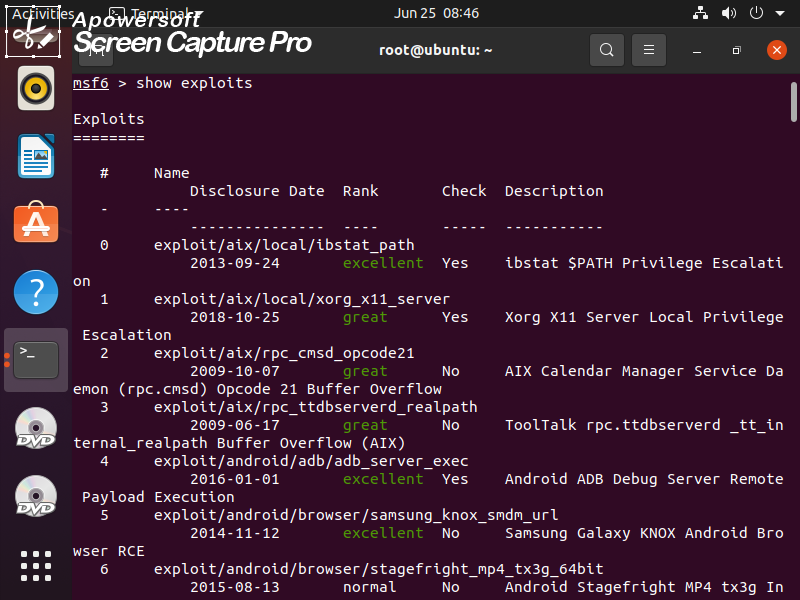
our local server is ready



I wrote the necessary codes to run metasploit from the console. A quote from the matrix movie greeted us.

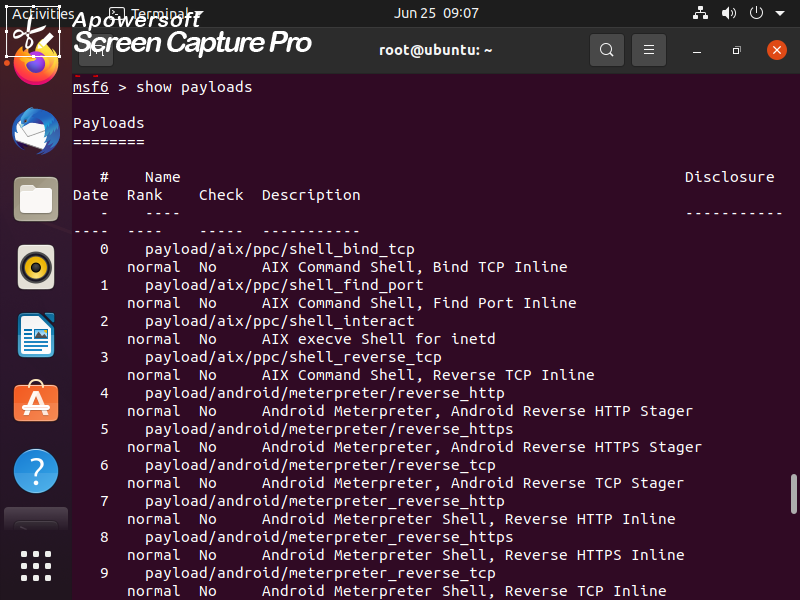


These banners are my favorite part of the app. They appear randomly when the application is installed or when you want it.

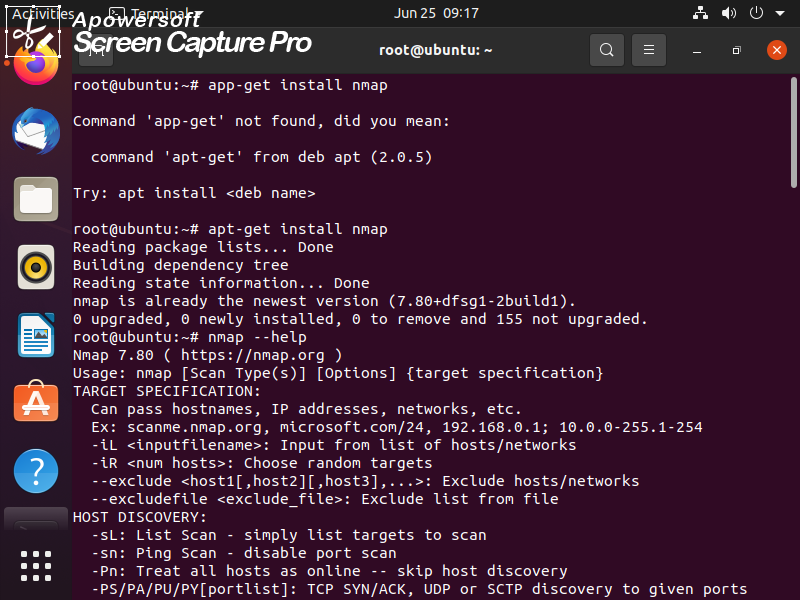


All exploits in the Metasploit Framework will fall into two categories: active and passive. Active exploits will exploit a specific host, run until completion, and then exit. Brute-force modules will exit when a shell opens from the victim. Module execution stops if an error is encountered.

Next, we will use the following command to see what payload we can use with this exploit.

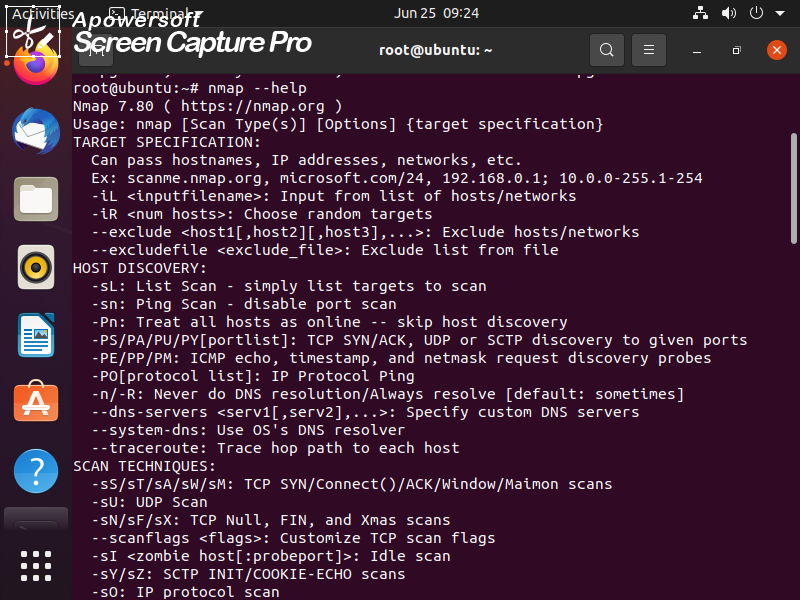


Payload, in simple terms, are simple scripts that the hackers utilize to interact with a hacked system. Using payloads, they can transfer data to a victim system.

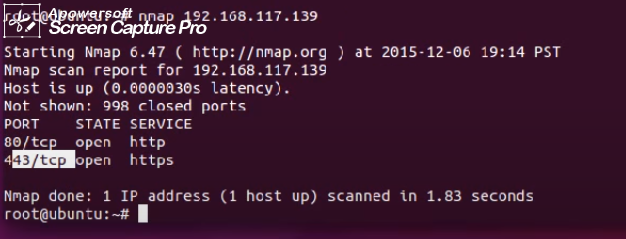


It didn't update because I already have NMAP installed before

You can access everything with this code (nmap – help)



After entering the ip address, we notice that 2 ports are open.



In the nmap scan results, we have 2 ports working!!