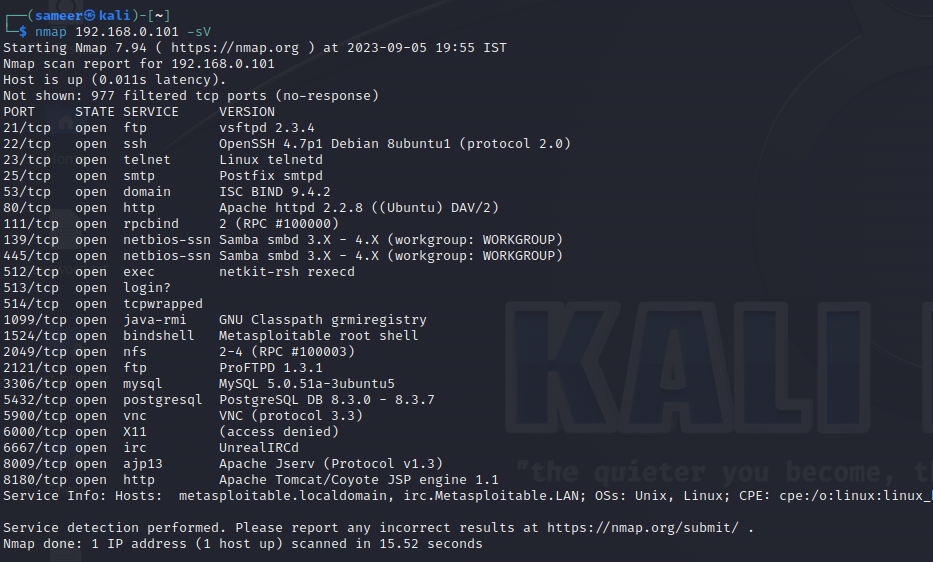
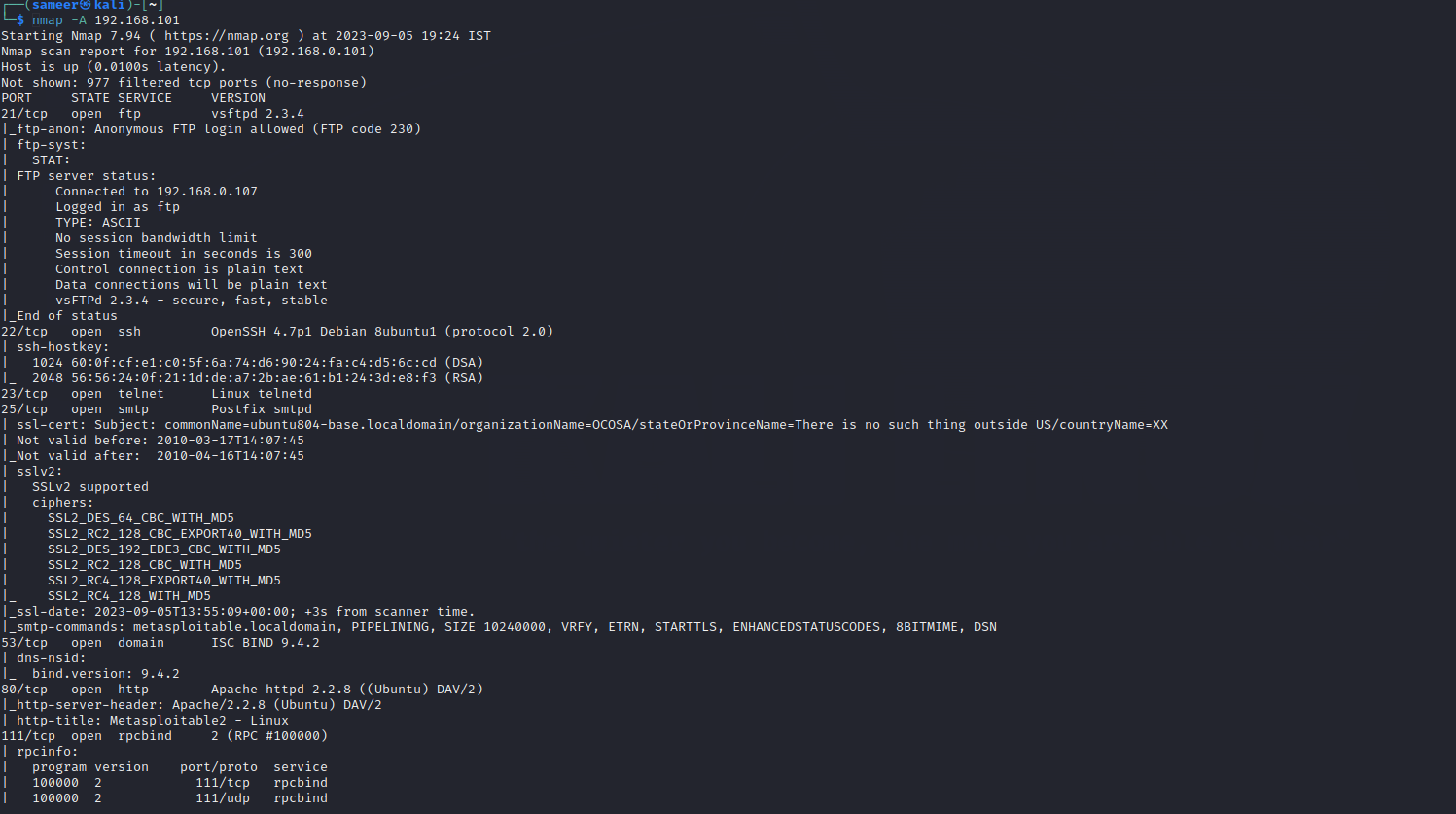
**Task -9 05-09-23 Tuesday by Sameer Chauhan**

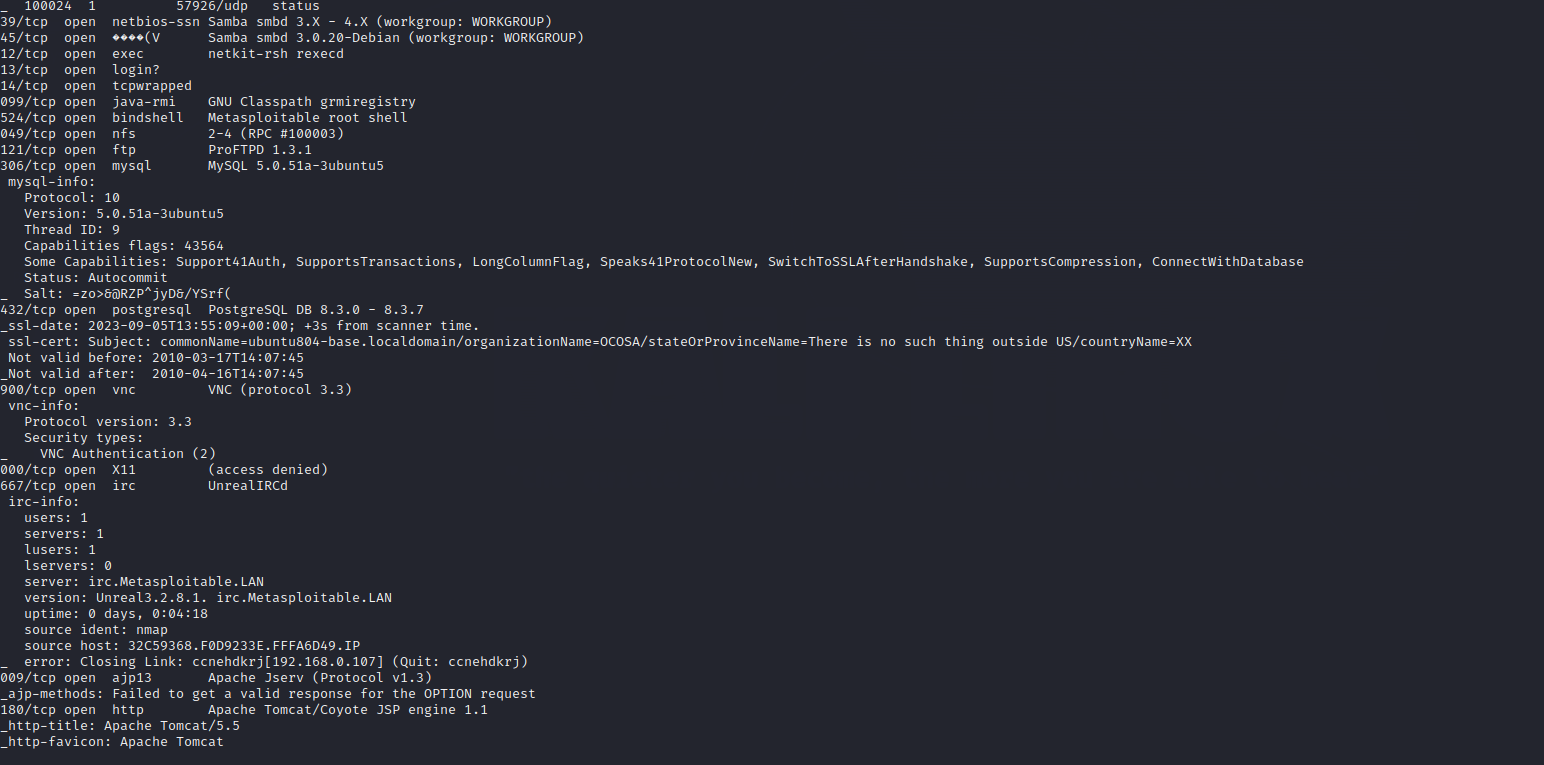
**Aim-We have to explore nmap -network mapper tool and try to scan our metasploitable 2 using various commands of nmap**

**In this task we will setup up a metasploitable 2 victim machine we will note its ip address by ifconfig -191.168.0.101 and peform the scanning by nmap**

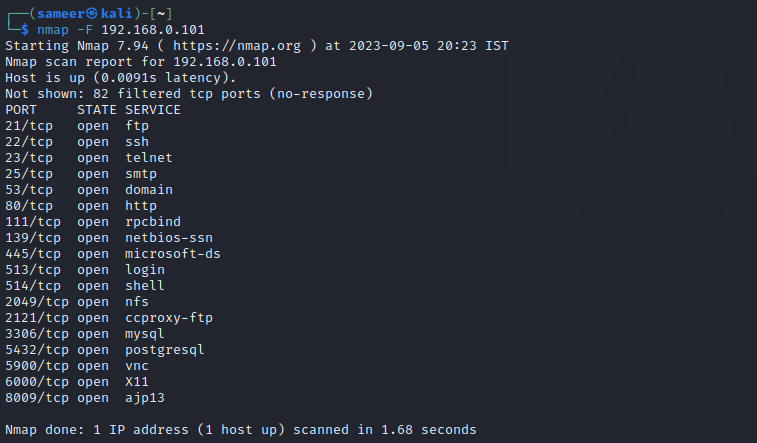


**By using the command nmap ip -sV we check the various services and their corresponding versions.**

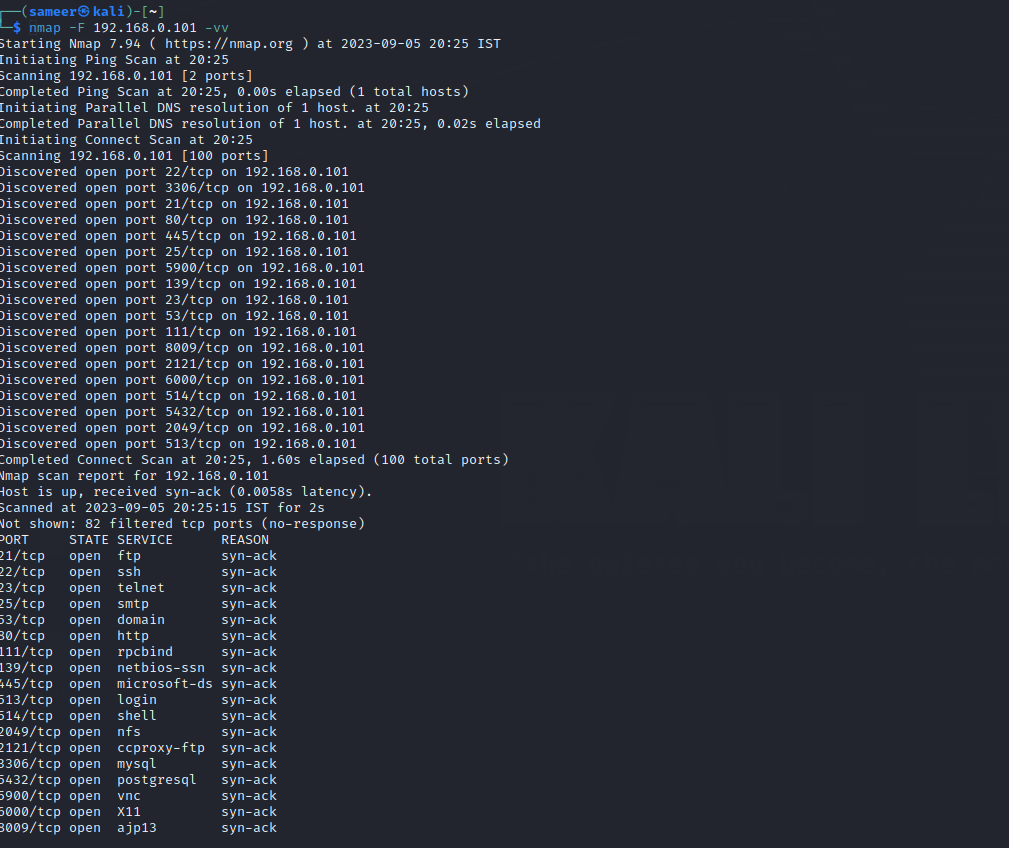




**Here we used Aggressive scanning command in nmap -we got various results like open ports, their versions, status,Security types,of our target machine.**



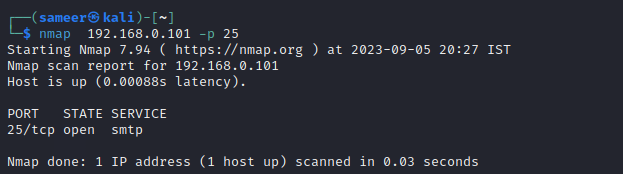
**Here we used command -f which stands for fast scanning it roughly scan about 100 ports which are very common as we can see in the screenshot it says Host is up,how much time it took for the scan**



**Here we used command fast scan+double verbose mode which do in depth scan showing us all steps of scan plus speed is also fast**



**In the above command we inferred how to save our scan report as it is very important to save our scan as we may close the terminal by mistake then all the data scanned will be lost so we use >>Desktop/sam.text to save our scan.**



**Suppose we have to scan a particular port like we know smtp-25 port number so we will simply give the command**

**Nmap 192.168.0.101 -p (port number here 25 for smtp)**

**We have some other common ports which we should remember like –**

**20-ftp Data channel**

**21-ftp control channel**

**22-Ssh**

**23-telnet**

**25-Smtp**

**80-Http**

**443-Https**

**53-DNS**

**110-Pop3**

**123-Ntp**

**143-IMAP**

**69-TFTP**

**We should remember these common ports number.**