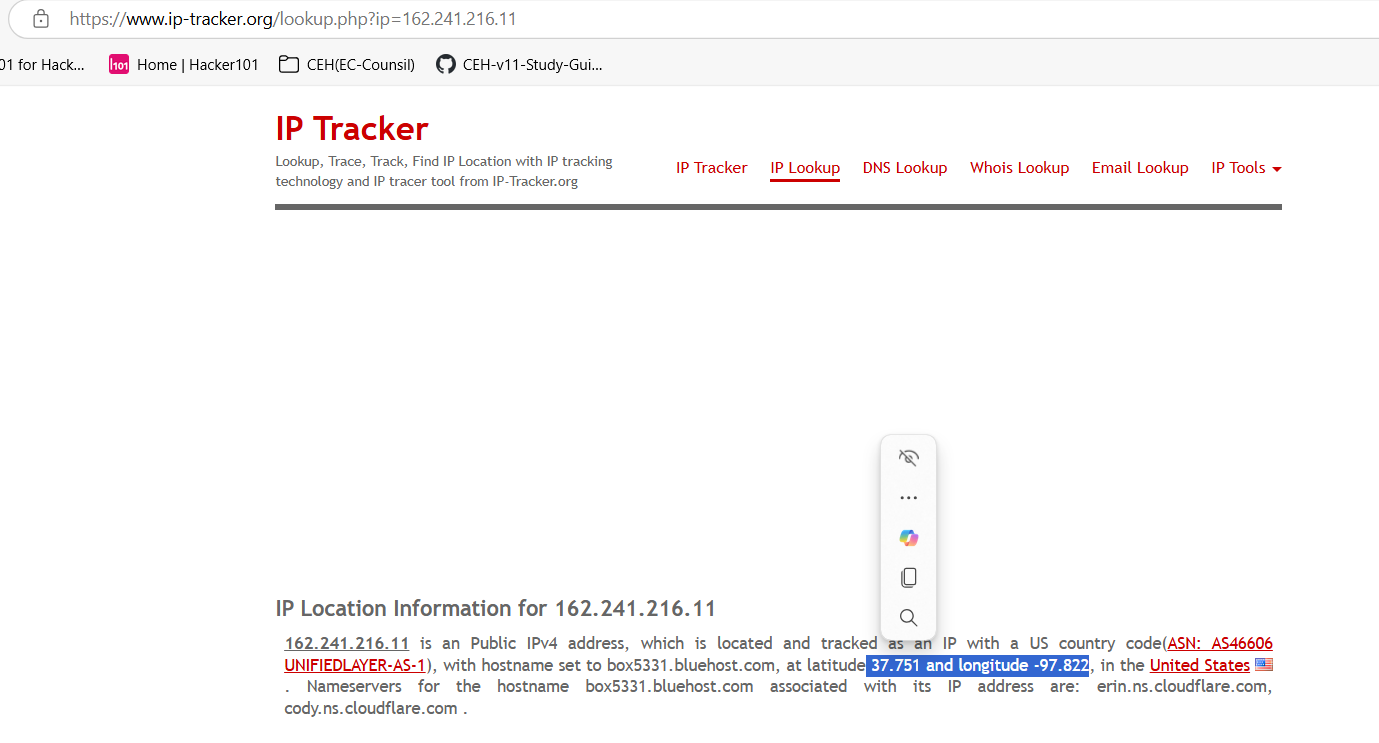
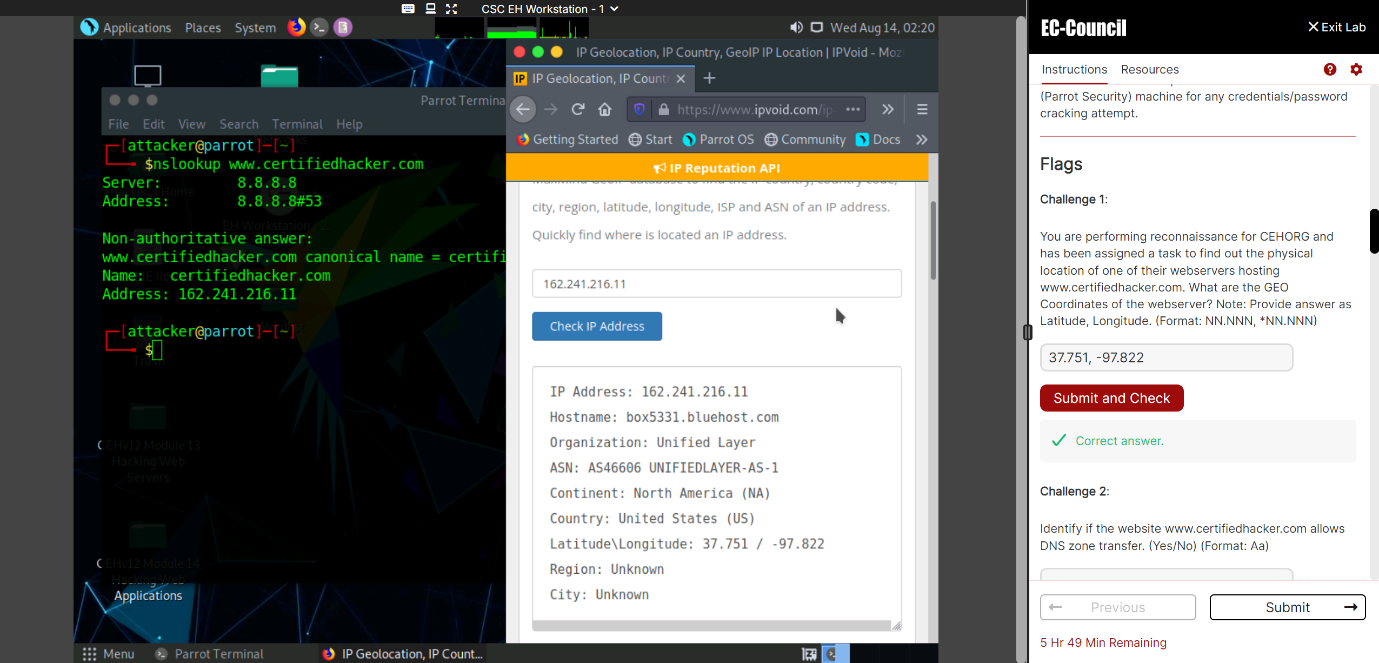
1] You are performing reconnaissance for CEHORG and has been assigned a task to find out the physical location of one of their webservers hosting www.certifiedhacker.com. What are the GEO Coordinates of the webserver? Note: Provide answer as Latitude, Longitude. (Format: NN.NNN, \*NN.NNN)

Ans: 37.751, -97.822

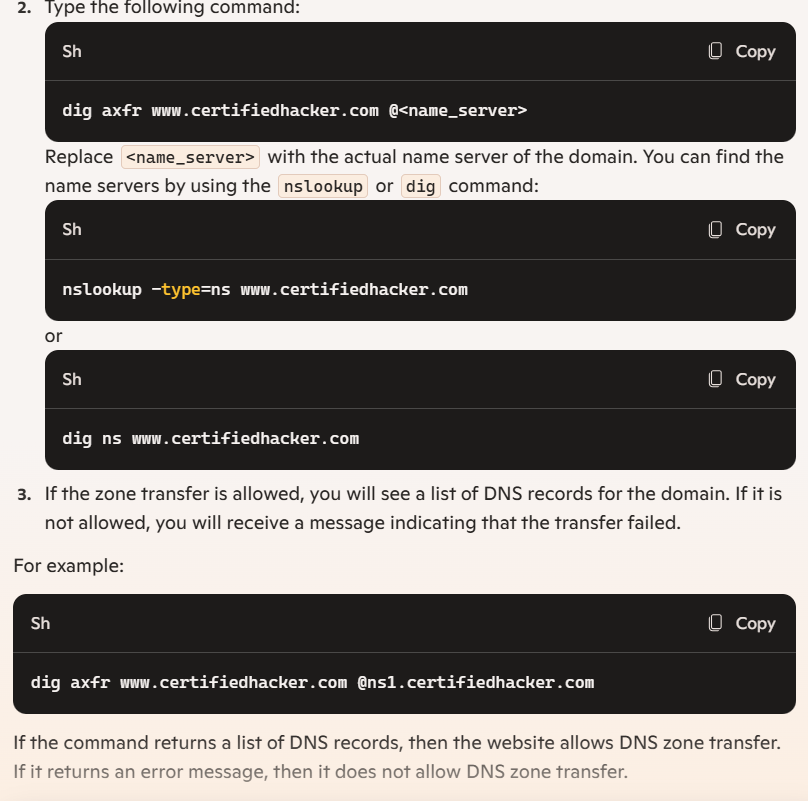
Use nslookup and find ip of server and then paste it in ip-logger.org





2] Identify if the website www.certifiedhacker.com allows DNS zone transfer. (Yes/No) (Format: Aa)

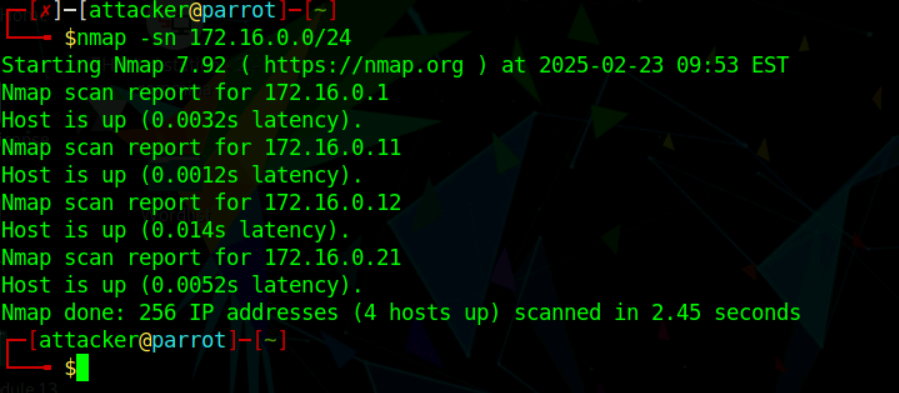
Answer: No



3] Identify the number of live machines in 172.16.0.0/24 subnet. (Format: N)

Ans: 3

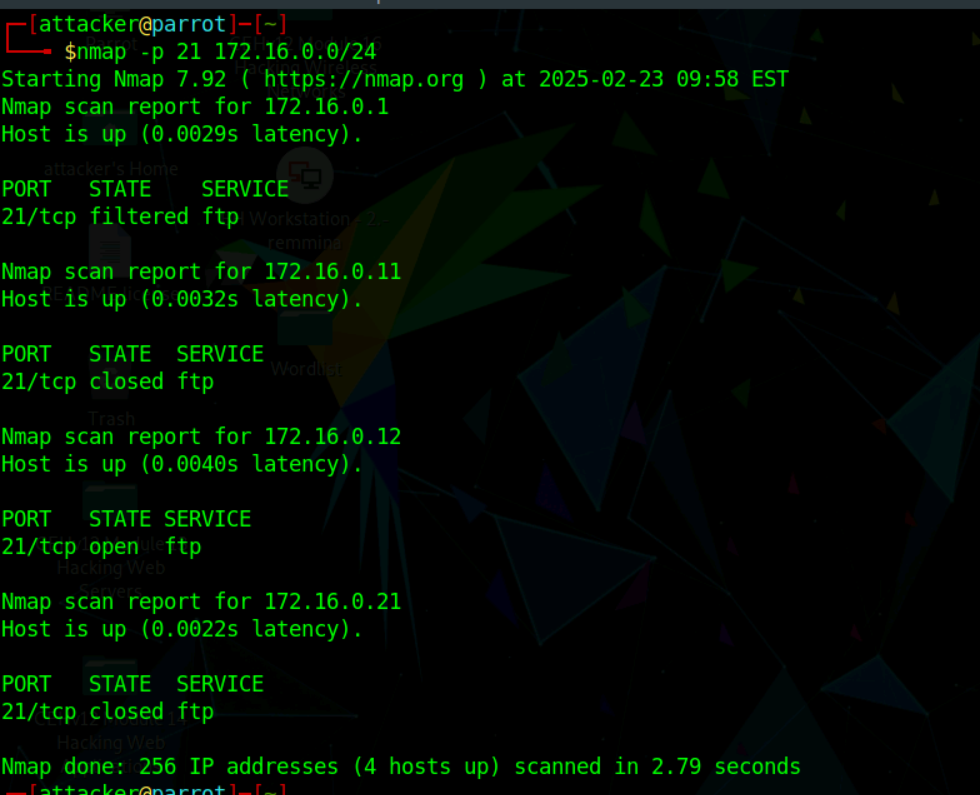
Use command nmap -sn 172.16.0.0/24 and may be number will be aamtem



4] Find the IP address of the machine which has port 21 open. Note: Target network 172.16.0.0/24 (Format: NNN.NN.N.NN)

Answer: 172.16.0.12

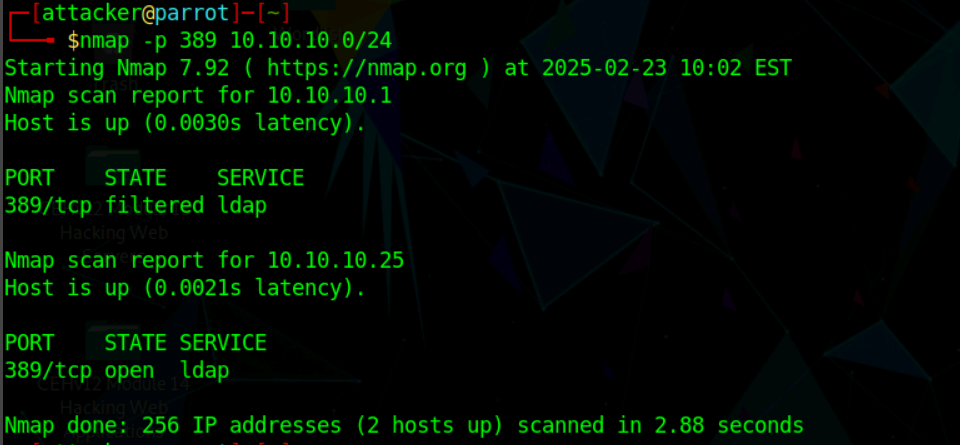
se any nmap command



5] Find the IP address of the Domain Controller machine in 10.10.10.0/24. (Format: NN.NN.NN.NN)

Answer: 10.10.10.25

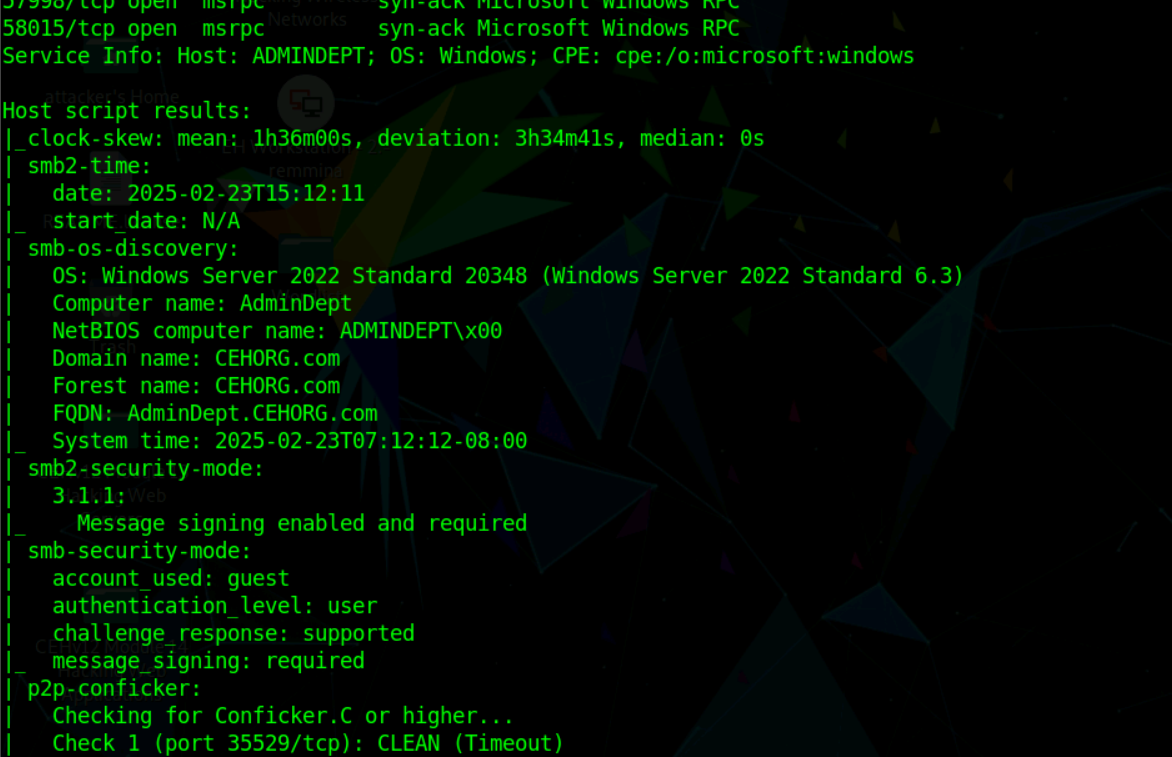
Here we can use our regular command (-p- -A -vv) and in 10.10.10.25 ip we can see full details which include domain controller machine name, netbios name etc. so prefere full scan



6] Perform a host discovery scanning and identify the NetBIOS name of the host at 10.10.10.25. (Format: AAAAAAAAA)

Answer: ADMINDEPT

Nmap -p- -A -vv 10.10.10.25

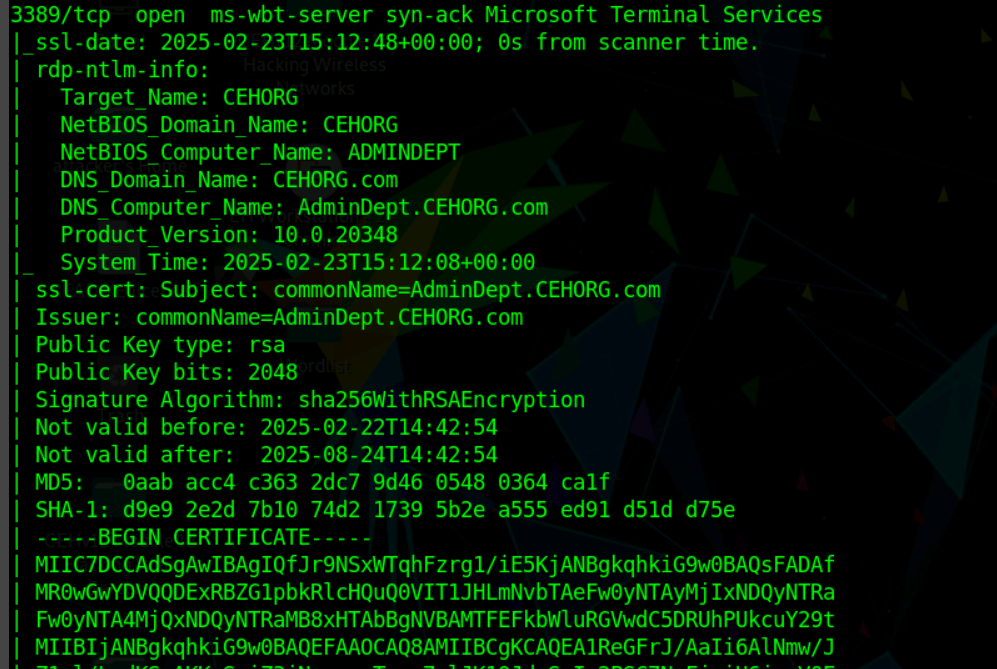


ADMINDEPT

7] Perform an intense scan on 10.10.10.25 and find out the FQDN of the machine in the network. (Format: AaaaaAaaa.AAAAAA.aaa)

Answer: AdminDept.CEHORG.com

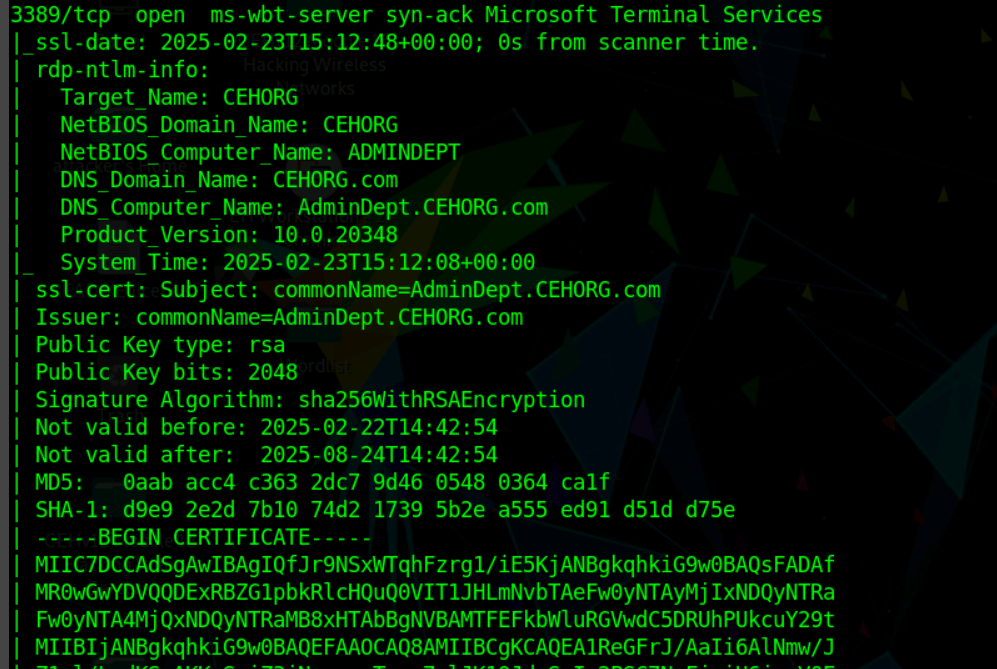
Above same command (Nmap -p- -A -vv 10.10.10.25)



8] What is the DNS Computer Name of the Domain Controller? (Format: AaaaaAaaa.AAAAAA.aaa)

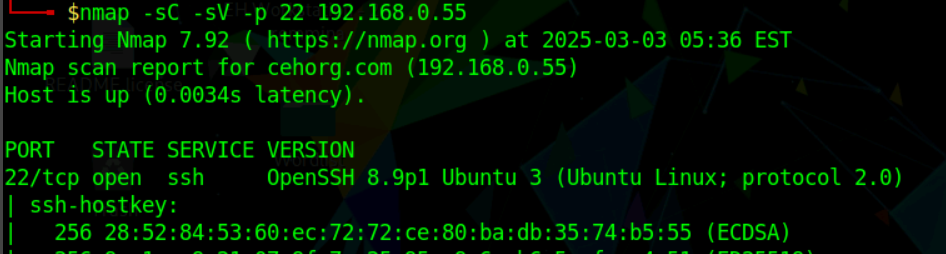
Answer: AdminDept.CEHORG.com

Same above command (Nmap -p- -A -vv 10.10.10.25)



9] While performing a security assessment against the CEHORG network, you came to know that one machine in the network is running OpenSSH and is vulnerable. Identify the version of the OpenSSH running on the machine. Note: Target network 192.168.0.0/24. (Format: N.NaN)

Ans: 8.9p1



10] During a security assessment, it was found that a server was hosting a website that was susceptible to blind SQL injection attacks. Further investigation revealed that the underlying database management system of the site was MySQL. Determine the machine OS that hosted the database. (Format: Aaaaaa)

Answer: linux as above image mention or use -O in nmap scan

11] Perform LDAP enumeration on the target network and find out how many user accounts are associated with the domain. (Format: N)

Answer: 8 (count the user we got)

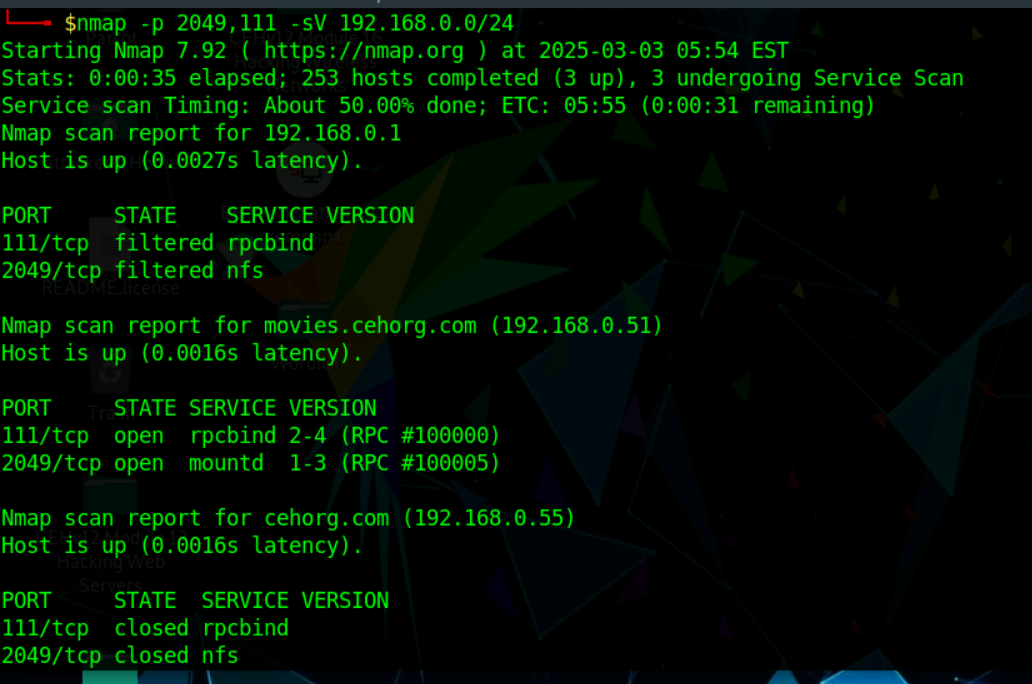


12] Perform an LDAP Search on the Domain Controller machine and find out the latest version of the LDAP protocol. (Format: AAAAaN)

ANSWER: LDAPv3 view in above image

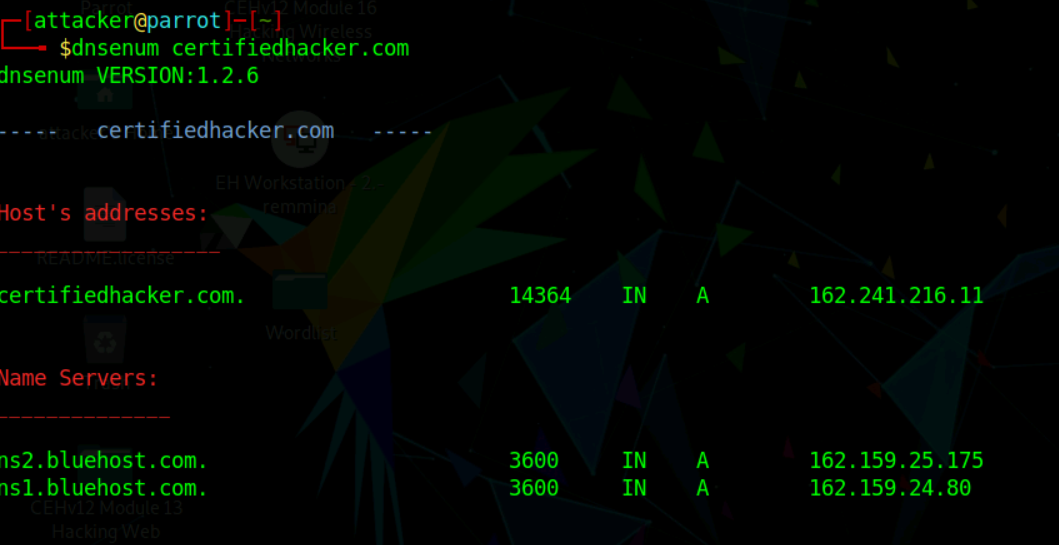
13] What is the IP address of the machine that has NFS service enabled? Note: Target network 192.168.0.0/24. (Format: NNN.NNN.N.NN)

Answer: 192.168.0.51



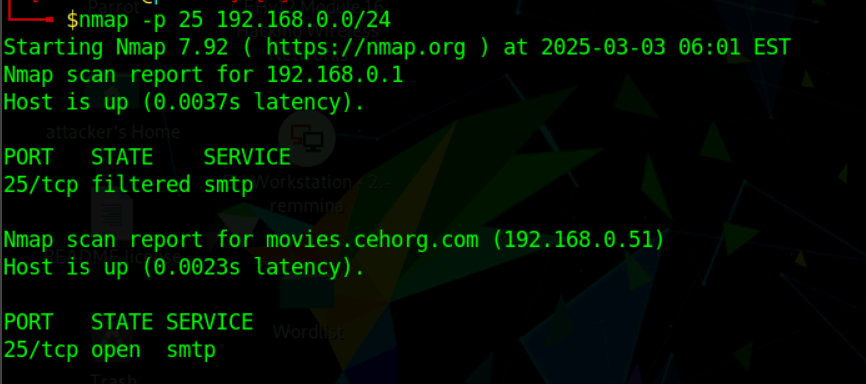
14] Perform a DNS enumeration on www.certifiedhacker.com and find out the name servers used by the domain. (Format: aaN.aaaaaaaa.aaa, aaN.aaaaaaaa.aaa)

Answer: ns1.bluehost.com, ns2.bluehost.com



15] Find the IP address of the machine running SMTP service on the 192.168.0.0/24 network. (Format: NNN.NNN.N.NN)

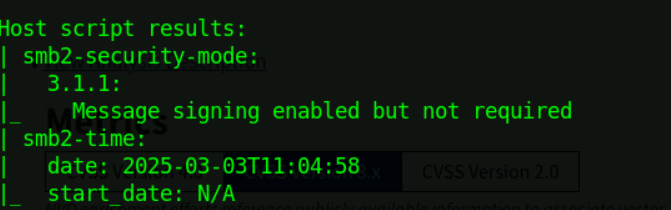
Answer: 192.168.0.51



16] Perform an SMB Enumeration on 192.168.0.51 and check whether the Message signing feature is enabled or disabled. Give your response as Yes/No. (Format: Aaa)

Answer: Yes, in last we get message





17] Perform a vulnerability research on CVE-2022-30171 and find out the base score and impact of the vulnerability. (Format: N.N Aaaaaa)

Answer: 5.5 Medium

Search on nvd and check for all cvss 2.0, 3.0

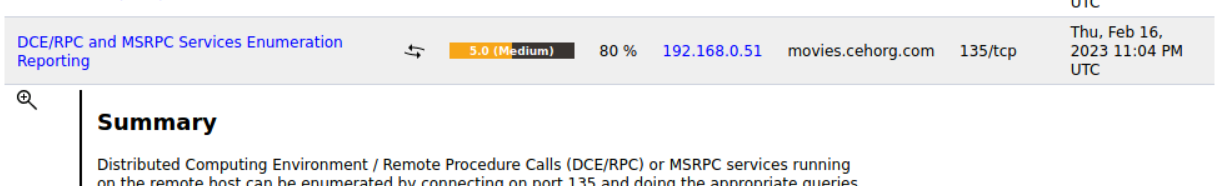
18] Perform vulnerability scanning for the domain controller using OpenVAS and identify the number of vulnerabilities with severity level as "medium". (Format: N)

Answer: 3

Check result tab

19] Perform vulnerability scanning for the webserver hosting movies.cehorg.com using OpenVAS and identify the severity level of RPC vulnerability. (Format: N)

Answer: 5 means 5.0



20] Perform vulnerability scanning for the Linux host in the 172.16.0.0/24 network using OpenVAS and find the number of vulnerabilities with severity level as medium. (Format: N)

Answer: 7 check in result tab

