# H#2.1

A vulnerability is a weakness or flaw that can exist in a hardware’s firmware, in the OS of computer or router, NW services, libraries and application software that can be exploited by a threat actor to gain unauthorized access, cause damage, or perform unauthorized actions.

An exploit is a program/software that take advantage of a vulnerability leading to gain initial access or privilege escalation on the target.

A payload is the malicious code which runs on the compromised system after initial access, enabling actions like remote control, data exfiltration, or persistence.

A cyber-attack is a malicious attempt by individuals or groups to compromise, disrupt, damage, or gain unauthorized access to computer systems, networks, or data.

o Network-based attacks (e.g., Man-in-the-Middle, DoS/DDoS, ARP Spoofing)

o Web-based attacks (e.g., SQL Injection, Cross-Site Scripting, CSRF)

o System-based attacks (e.g., Buffer Overflow, Privilege Escalation, Rootkits)

o Social Engineering attacks (e.g., Phishing, Pretexting, Baiting)

o Malware-based attacks (e.g., Ransomware, Trojans, Worms, Keyloggers)

o Physical attacks (e.g., USB-based attacks, Evil Maid Attacks)

A malware is a malicious software designed to harm, exploit or compromise systems, network or data.



A computer virus is a type of malicious software (malware) that infects a computer system and spreads by replicating itself within files or by attaching itself to executable programs.

A computer worm is a type of malicious software (malware) that, unlike viruses, can self-replicate and spread independently without needing to attach itself to other programs or files

A Trojan horse, often referred to simply as a Trojan is a type of malicious software (malware) that disguises itself as legitimate software or files to deceive users into executing or installing it on their systems. Unlike viruses or worms, Trojans do not self-replicate. Instead, they rely on social engineering tactics to trick users into unwittingly installing them.

Ransomware is a type of malicious software (malware) designed to encrypt files on a victim's computer or entire network, rendering them inaccessible until a ransom is paid.

Spyware is a type of malicious software (malware) designed to secretly gather information about a user's activities on their computer or device without their knowledge or consent.

Adware is a type of software designed to display advertisements on a user's device, often in a disruptive or intrusive manner.

A rootkit is a type of malicious software designed to gain unauthorized access to and maintain control over a computer system while hiding its presence from the user and security software.

A botnet is a network of compromised computers, known as "bots" or "zombies," that are controlled remotely by an attacker, often called a "botmaster" or "bot herder." Botnets are typically used to conduct large-scale cyber-attacks and other malicious activities.

Fileless malware is a type of malicious software that does not rely on traditional files to infect a computer. Instead, it exploits existing, legitimate tools and features within the operating system to carry out malicious activities.

Anonymity refers to the state of being unidentified or untraceable within a digital environment.

1. Directly Connected via LAN
2. Use a Proxy Server
3. Use Multiple Proxies
4. Use Proxy Chains
5. Use Virtual Private Network (VPN) Service
6. Use Tor Browser (The Onion Router): The Onion Router (TOR) is privacy focused web browser that routes your Internet traffic through multiple volunteer-operated servers (nodes) across the globe to anonymize your online activity.
7. TOR Browser + VPN
8. Use a Persistent USB Containing Portable OS

# H#2.2

The tools that we will be using for Reconnaissance and Information gathering in today’s hand out are host, nslookup, dig, whois, knockpy, netdiscover, traceroute, whatweb, theHarvester, sherlock, wfw00f, Google Dorking, OSINT framework.

The host is a utility that performs DNS lookups. Normally used to convert names to IP address and vice versa.

nslookup (Name Server Lookup) is also used for name to IP address mapping and vice versa. It is more versatile as it can be used to get other specific DNS records such as A (Address), AAAA (IPv6 Address), MX (Mail Exchange), NS (Name Server), TXT (Text), and more.

The dig is also a DNS lookup utility that stands for Domain Information Groper. The dig utility is quite similar to nslookup but provides a more detailed and structured output.

The whois command is used to retrieve domain registration information from whois databases. These databases store publicly available information about domain names, such as the registry, registrar, registration and expiration dates, name servers, and the contact details of the domain owner (registrant).

Knockpy is an open-source tool used primarily for subdomain enumeration. It helps in identifying subdomains associated with a target domain

The netdiscover is an active/passive network discovery tool that uses Address Resolution Protocol (ARP) to identify hosts in a local area network (LAN). It can be used for both active as well as passive scanning.

The traceroute command is used to trace the path that packets take from your device to any remote server (a domain name or an IP address) in a LAN or on the Internet.

The whatweb is a tool that is used to identify and recognize all the web technologies available on the target website.

TheHarvester is a command line utility that can be used to gather open-source intelligence (OSINT) about targets, such as domain names, IP addresses, email addresses and more.

Sherlock is a command-line tool used to search for usernames across various social media platforms and websites. I

The wafw00f (Web Application Firewall (WAF) Foot printing Tool) is an essential tool for security professionals looking to access the security posture of web applications.

Google Dorking, also known as Google Hacking, is a technique that utilizes advance search operators to uncover information on the Internet that may not be readily available through standard search queries on Google.

Open-Source Intelligence (OSINT) refers to the process of collecting and analyzing publicly available information from open sources, such as websites, social media, public records, forums, and more.

# H#2.3

Scanning and vulnerability analysis is the second phase of penetration testing in which we scan the Network, ports, and OS services and determine if any of these are vulnerable

Scanning is broader and focuses on identifying what is present (systems, ports, services), while vulnerability analysis digs deeper to determine what is wrong with those systems (misconfigurations, unpatched software, exploitable flaws).

The tools that we normally use for scanning are nmap, zenmap, unicornscan, nikto and so on.

The tools that we normally use for vulnerability analysis are nessus, searchsploit, OpenVAS, MSF, Burp-Suite, SQLMap

Common Weakness Enumeration (CWE) is a general flaw or weakness in s/w design and implementation that could lead to vulnerabilities if not addressed [CWE-NNN].

Common Vulnerabilities and Exposures (CVE) is a specific instance of a vulnerability in a version of a real world application that can be exploited [CVE-YYYY-NNNNN]

An attack vector is the path way through which an attacker can exploit a vulnerability in a system, network or application to gain unauthorized access, steal data, deploy malware, or disrupt a service.

The nmap (Network Mapper) is a free and open-source utility for network discovery and security auditing.

we can use nmap for network scanning, port scanning, and vulnerability scanning.

The 3-way handshake is a fundamental process used in the TCP/IP protocol suite to establish a reliable connection between a client and a server.

SYN (Synchronize):

SYN-ACK (Synchronize-Acknowledge):

ACK (Acknowledge):

The searchsploit is used to search for known vulnerabilities and exploits related to hardware, software, operating systems, web applications, and configurations.

Nessus is a platform developed by Tenable that scans for security vulnerabilities in devices, applications, operating systems, cloud services and other network resources. Unlike nmap, it checks for specific vulnerabilities tied to known CVEs along with their CVSS scores

OpenVAS (Open Vulnerability Assessment System) is an open-source framework used for network vulnerability scanning and management. It is designed to identify security vulnerabilities in networked systems and services, providing comprehensive reporting and remediation guidance.

# H#2.4

Scanning and Vulnerability Analysis Tools:

o OS and NW: nmap, nessus, openVAS, tripwire, wireshark, MSF

o Web Applications: Burp Suite, nikto, OWASP ZAP,

o Mobile Applications: frida, drozer, MobSF, Burp Suite,

MSF provides security professionals and researchers with a comprehensive set of tools that can support all phases of a penetration testing engagement, from information gathering to post-exploitation.

The auxiliary sub-directory contains scripts designed to perform information gathering and vulnerability analysis

The exploits sub-directory contains scripts designed to exploit specific vulnerabilities in operating systems, network services, applications, and so on for different OSs like unix, linux, windows, solaris etc.

The payloads sub-directory contains various payloads that runs remotely on the compromised system.

The encoders sub-directory contains scripts used to encode and obfuscate payloads to evade detection

The nops sub-directory contains scripts that generate No Operation (NOP) sleds, to modify payload signature and thereby avoiding detection.

The evasion sub-directory contains scripts that are designed to evade detection by security mechanisms like firewalls and intrusion detection systems (IDS).

The evasion sub-directory contains scripts that are designed to evade detection by security mechanisms like firewalls and intrusion detection systems (IDS).