Penetration Testing and Ethical Hacking

Created By: Arnav Tripathy, Teaching Assistant

1. **Footprinting-** Footprinting (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies**.**
2. **Scanning-**Scanning is a set of procedures for identifying live hosts, ports, and services, discovering Operating system and architecture of target system, Identifying vulnerabilities and threats in the networ**k**
3. **Enumeration**-Enumeration is defined as the process of extracting user names, machine names, network resources, shares and services from a system
4. **Malware**-Malware, or malicious software, is any program or file that is harmful to a computer user
5. **Sniffing**- Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tool
6. **Social Engineering-**Social engineering is an attack vector that relies heavily on human interaction and often involves manipulating people into breaking normal security procedures and best practices in order to gain access to systems, networks or physical locations, or for financial gain.
7. **Denial of Service**- A denial-of-service is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service
8. **Session-hijacking**-Session hijacking, sometimes also known as cookie is hijacking is the exploitation of a valid computer session—sometimes also called a sessionkey—to gain unauthorized access to information or services in a computer system
9. **Web server**- A web server is server software, or hardware dedicated to running said software, that can satisfy World Wide Web client requests
10. **SQL injection**-SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQLstatements are inserted into an entry field for execution

11. **IDS**- IDS. (Intrusion Detection System) Software that detects an attack on a network or computer system. A Network IDS (NIDS) is designed to support multiple hosts, whereas a Host IDS (HIDS) is set up to detect illegal actions within the host
12. **Firewall**-A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system
13. **Honeypot**-honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information system.
14. **IoT**-The Internet of things (IoT) is the extension of Internet connectivity into physical devices and everyday objects. Embedded with electronics, Internet connectivity, and other forms of hardware (such as sensors), these devices can communicate and interact with others over the Internet, and they can be remotely monitored and controlled.The Internet of things (IoT) is the extension of Internet connectivity into physical devices and everyday objects. Embedded with electronics, Internet connectivity, and other forms of hardware (such as sensors), these devices can communicate and interact with others over the Internet, and they can be remotely monitored and controller.
15. **Cloud**- The term cloud is simply how a network or remote servers can be accessed via an internet connection to store and manage information. In other words, it's a place other than your computer that you can use to store your stuff.
16. **Cryptography**-Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries.
17. **Black-hat Hacker**-A black hat hacker is a hacker who violates computer security for personal gain or maliciousness.
18. **White-hat Hacker**- A white hat hacker is an individual who uses hacking skills to identify security vulnerabilities in hardware, software or network
19. **Gray-hat Hacker**-A gray hat hacker (also spelled grey hat hacker) is someone who may violate ethical standards or principles, but without the malicious intent ascribed to black hat hackers.
20. **Banner grabbing**-Banner grabbing is a technique used to gain information about a computer system on a network and the services running on its open ports.
21. **Backdoor**-A backdoor in software or a computer system is generally an undocumented portal that allows an administrator to enter the system to troubleshoot or do upkeep
22. **Hash**- A hash is a function that converts one value to another.
23. **Algorithm**- A process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer.

24. **Jailbreak-**iOS jailbreaking is the privilege escalation of a iDevice for the purpose of removing software restrictions imposed by Apple on iOS, tvOS and watchOS operating systems.
25. **MAC Address-** A media access control address of a device is a unique identifier assigned to a network interface controller. For communications within a network segment, it is used as a network address for most IEEE 802 network technologies, including Ethernet, Wi-Fi, and Bluetooth
26. **Virus-** A piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.
27. **Worm-** A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it.