CSDF Unit-2 Notes By OMG 13_159 OmGonjari

What is Unauthorized Access?

Unauthorized access is when someone gains access to a computer system, network, or data without the owner's permission or without having the proper authorization[1]. It's a significant security breach that can result in data theft, modification, or destruction.

Common Causes of Unauthorized Access

The common causes of unauthorized access include:

- **Weak Passwords:** Easily guessable or default passwords make systems vulnerable.
- **Malware:** Viruses, worms, or Trojans can be used to bypass security controls and grant unauthorized access.
- **Phishing:** Deceptive emails or websites that trick users into revealing their login credentials.
- **Social Engineering:** Manipulating people to give up confidential information.
- **Unpatched Software:** Exploiting vulnerabilities in outdated software.
- **Insider Threats:** Employees or individuals with legitimate access who misuse their privileges.
- **Physical Access:** Gaining physical access to a device to bypass its security.

How to Prevent Unauthorized Computer Access

Preventing unauthorized computer access requires a multi-layered approach that includes technical controls, user education, and physical security measures. Here's how to prevent it:

- **Use Strong Passwords and Two-Factor Authentication (2FA):** Enforce complex passwords that include a mix of uppercase and lowercase letters, numbers, and symbols. Additionally, implement 2FA, which requires a second form of verification besides the password.
- **Regularly Update Software and Systems:** Patching software and operating systems promptly helps close security holes that attackers could exploit.
- **Install and Maintain Antivirus and Anti-Malware Software:** These tools can detect and remove malicious software that could lead to unauthorized access.

- **Implement Firewalls:** A firewall acts as a barrier between your computer/network and the internet, monitoring and filtering traffic to block unauthorized connections.
- **Educate Users:** Train users to recognize and avoid phishing attempts, not to open suspicious attachments, and to be cautious about the information they share.
- **Use Encryption:** Encrypting sensitive data makes it unreadable even if an unauthorized person gains access to it.
- **Control Physical Access:** Secure physical access to computers and network equipment to prevent someone from directly manipulating them.
- **Monitor and Log Activity:** Regularly review logs to detect unusual activity that could indicate an attempted or successful unauthorized access.

What is Application Security?

Application security refers to the measures taken throughout an application's lifecycle to prevent unauthorized access, modification, or use[2]. It involves adding security features to the software itself to protect it from threats.

Different Types of Application Security

Application security can be categorized into various types, including:

- **Authentication:** Verifying the identity of a user or process[3].

- **Authorization:** Granting specific permissions to an authenticated user[4].

- **Auditing:** Recording and analyzing application activity to detect security incidents[5].

- **Confidentiality:** Ensuring data is not disclosed to unauthorized parties[6].

- **Integrity:** Protecting data from unauthorized modification[7].

- **Non-Repudiation:** Preventing an entity from denying its actions[8].

How Email Hacking Takes Place?

Email hacking is a process of gaining unauthorized access to an email account[9]. Attackers use various methods to do this:

- **Phishing:** The most common method. Attackers send fake emails that look legitimate to trick users into providing their login credentials on a fraudulent website.
- **Keyloggers:** Malicious software that records every keystroke, including passwords, entered on a computer.
- **Password Guessing/Brute Force Attacks:** Attackers use automated tools to try thousands of common passwords or dictionary words to gain access.
- **Man-in-the-Middle (MitM) Attacks:** An attacker intercepts the communication between the user and the email server to steal credentials.
- **Malicious Attachments:** Opening an infected attachment can install malware that compromises the computer and steals email credentials.

What is Hardware Protection?

Hardware protection refers to security measures that protect the physical components of a computer system, such as the CPU, motherboard, and storage devices, from threats[10]. It is about ensuring the physical integrity and security of the hardware itself.

What are Different Types of Hardware Protection?

There are several types of hardware protection, including:

- **Physical Locks:** Using locks to secure computer cases, servers, and data centers.
- **Tamper-Evident Seals:** Seals that show if a device has been opened or tampered with.
- **Hardware Security Modules (HSMs):** Dedicated devices that perform cryptographic operations and securely store keys.
- **Biometric Scanners:** Using fingerprints, facial recognition, or iris scans to control access to devices.
- **Trusted Platform Module (TPM):** A secure cryptoprocessor that authenticates the hardware and software on a device.

What are the Types of Program and System Threats?

Program threats and system threats are two main categories of security risks.

Program Threats: These are malicious programs that execute specific actions to compromise a system.

- **Viruses:** Programs that attach themselves to legitimate files and self-replicate, causing damage[11].
- **Worms:** Self-replicating programs that spread across networks without human intervention[12].
- **Trojans:** Malicious programs disguised as useful software[13].
- **Ransomware:** Encrypts a user's data and demands a ransom for its release.

System Threats: These threats exploit vulnerabilities in the operating system or network to gain unauthorized access.

- **Denial-of-Service (DoS) Attacks:** Overloading a system with traffic to make it unavailable to legitimate users.
- **Rootkits:** Tools that hide a hacker's presence and activities on a system.
- **Backdoors:** A hidden method to bypass normal authentication and gain access to a system.
- **Buffer Overflow:** Exploiting a programming error to execute malicious code.

What is Internet Hacking & Cracking?

Internet Hacking: Internet hacking is the process of exploiting vulnerabilities in computer systems and networks to gain unauthorized access or control[141414]. It involves a wide range of activities, from simple pranksterism to serious criminal acts like data theft and cyber-espionage.

Cracking: Cracking is a specific type of hacking that involves breaking into a system or software with malicious intent[1515]. Crackers are often associated with criminal activities.

Types of Cracking

- **Software Cracking:** Bypassing software protection, such as serial number checks or copy protection[1616].
- **Password Cracking:** Attempting to recover passwords from data that has been stored or transmitted by a computer system[1717].
- **Network Cracking:** Gaining unauthorized access to a network to steal data or disrupt services[1818].
- **Website Cracking:** Defacing a website or stealing its data[1919].

What are Different Computer Intrusions?

A computer intrusion is any unauthorized access to a computer system or network[2020]. It can take many forms:

- **Remote Intrusion:** Gaining access from a remote location, often over the internet.
- **Insider Intrusion:** A trusted individual, such as an employee, misusing their access.
- **Physical Intrusion:** Gaining physical access to a computer to manipulate it.
- **Malware-Based Intrusion:** Using malicious software like viruses or trojans to breach a system.
- **Social Engineering:** Tricking people into revealing information that allows a breach.

Differentiate Between Virus and Worms

Feature	Virus	Worm

Propagation	Attaches to a host program or file to spread. It requires human action (e.g., running the infected file) to replicate and spread[21].	A standalone, self-replicating program that spreads autonomously across networks without human intervention[22].
Infection Method	Infects files, documents, and programs[23].	Exploits network vulnerabilities to spread from one computer to another[24].
Purpose	Often designed to corrupt files, delete data, or display unwanted messages[25].	Primarily designed to consume network bandwidth and system resources, slowing down or crashing systems[26].
Host	Requires a host file or program to exist and execute[27].	Does not require a host program. It can run as an independent process[28].
Payload	Can have a destructive payload that activates after a specific event[29].	Can carry a payload to install backdoors, create a botnet, or steal data[30].
Network Dependency	Does not require a network to spread, although networks can facilitate its spread[31].	Primarily uses networks to spread from one system to another[32].
Remediation	Often requires scanning and cleaning individual files[33].	Often requires network-wide cleanup and patching of vulnerabilities[34].

Example	The "Melissa" virus, which spread through email attachments[35].	The "Conficker" worm, which infected millions of computers[36].

Describe Firewall Security Technology with a Neat Diagram

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules[37]. Think of it as a gatekeeper between a private internal network and the public internet.

How it Works:
The firewall examines each network packet. It checks the source and destination IP addresses, port numbers, and protocol types. If the packet matches a rule that allows it, it passes through. If not, it is blocked.
A typical firewall diagram shows the firewall positioned between the Internet and a local area network (LAN), protecting the internal network from external threats38. It acts as a filter, allowing legitimate traffic to pass while blocking unauthorized or malicious traffic.

Explain in Detail OS Security

Operating System (OS) security refers to the mechanisms and controls within an OS that protect the system from unauthorized access and malicious activity[39]. It's a fundamental part of cybersecurity, as the OS manages all hardware and software resources.

Key Aspects of OS Security:

- **User Authentication and Authorization:** The OS verifies the identity of users through credentials (e.g., username/password) and then grants them specific permissions based on their role. This prevents unauthorized users from accessing sensitive data or functions[40].

- **File System Security:** The OS provides access control lists (ACLs) to manage who can read, write, or execute files and directories. This ensures that only authorized users can modify or delete important files[41].

- **Memory Protection:** The OS uses memory management techniques to prevent one program from accessing the memory space of another. This isolates applications and prevents malicious code from interfering with critical system processes[42].

- **Kernel Integrity:** The kernel is the core of the OS. Protecting it is crucial. Secure OS designs use mechanisms to prevent unauthorized modifications to the kernel, which could compromise the entire system[43].

- **System Auditing and Logging:** The OS keeps detailed logs of system events, such as login attempts, file access, and application execution. These logs are vital for detecting security breaches and investigating incidents[44].

- **Patch Management:** The OS provides a mechanism to install security updates and patches, which fix known vulnerabilities. Regular patching is essential to maintain a secure system[45].

Explain Internet Hacking and Different Approaches of Hacking

Internet Hacking:
As mentioned earlier, internet hacking is the act of exploiting vulnerabilities to gain unauthorized access to computer systems and networks464646. It's a broad term that covers many malicious activities.
Different Approaches of Hacking:

- **Black Hat Hacking:** These are malicious hackers who break into systems for personal gain, to cause damage, or for other illegal purposes[47]. Their actions are criminal.

- **White Hat Hacking:** These are ethical hackers who use their skills to test and improve system security[48]. They work with a company's permission to find vulnerabilities and fix them before malicious hackers can exploit them. This is also known as penetration testing.

- **Grey Hat Hacking:** These hackers exist in a moral gray area[49]. They may hack into a system without permission but then report the vulnerabilities they find to the owner, sometimes requesting a fee for their services. Their actions are not purely malicious but are still illegal.

- **Phishing:** This is a social engineering approach where hackers send fraudulent emails or messages to trick people into revealing sensitive information like passwords and credit card details[50].

- **DDoS Attacks:** In a Distributed Denial-of-Service (DDoS) attack, hackers use a network of compromised computers to flood a server with traffic, making it unavailable to legitimate users[51].

Explain the Significance of Firewall and VPN Security Technologies

Both firewalls and VPNs are crucial for network security, but they serve different purposes[52].

Firewall Significance:
A firewall is your first line of defense against external threats53. Its significance lies in its ability to:

- **Block Unauthorized Access:** It acts as a barrier, preventing hackers from gaining entry to your network[54].
- **Filter Malicious Traffic:** It can block known malicious IP addresses and ports, protecting you from malware and other attacks[55].
- **Enforce Security Policies:** Organizations can configure firewalls to enforce specific rules, such as restricting access to certain websites or applications.
- **Monitor Network Traffic:** Firewalls provide logs that help administrators track network activity and detect potential threats.

VPN Significance:
A Virtual Private Network (VPN) creates a secure, encrypted tunnel over a public network, such as the internet56. Its significance is in providing:

- **Data Confidentiality:** It encrypts all data transmitted between your device and the VPN server, protecting it from being intercepted and read by third parties, especially on public Wi-Fi networks[57].
- **Anonymity:** It masks your IP address, making it difficult for websites, ISPs, or hackers to track your online activity[58].
- **Secure Remote Access:** It allows remote employees to securely access a company's private network as if they were physically present, protecting sensitive corporate data[59].
- **Bypassing Geo-Restrictions:** It allows users to bypass geographical blocks on websites

and content by routing their traffic through a server in a different country[60].

What Do You Mean by Intellectual Property? Explain Types of Intellectual Property

Intellectual property (IP) refers to creations of the mind, such as inventions, literary and artistic works, designs, and symbols, names, and images used in commerce[61]. These are intangible assets that are protected by law, giving the creator or owner exclusive rights to use their creation.

Types of Intellectual Property

- **Copyright:** This legal right protects original works of authorship, such as books, music, films, and software[62]. It gives the creator exclusive rights to reproduce, distribute, and perform their work[63].
- **Patents:** A patent is an exclusive right granted for an invention[64]. It allows the inventor to prevent others from making, using, or selling the invention for a limited period, typically 20 years[65].
- **Trademarks:** A trademark is a sign, design, or expression that identifies products or services of a particular source from those of others[66]. It protects brand names and logos used in the market[67].
- **Trade Secrets:** A trade secret is confidential information that gives a business a competitive edge[68]. This can include formulas, practices, processes, or designs that are not generally known[69]. Unlike patents, trade secrets are not publicly disclosed and are protected as long as they remain secret.