Computer Security

Common Vulnerabilities

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privileges
- Phishing
- Port Scans

Spoofing

- A technique used to gain unauthorized access to computers by fooling network hardware and software. The intruder sends a message to a computer with a different IP address indicating that the message is coming from a trusted host.
- Newer routers and firewall arrangements can offer protection against IP spoofing

Tampering

- Also known as parameter tampering.
- A form of Web-based attack in which certain parameters in the Uniform Resource Locator (URL) or Web page form data entered by a user are changed without the user's authorization.

Repudiation

- Repudiation is the denying of a communication or data transfer between two parties. A data or message sent by one party may not be acknowledged as received by the receiving party even though the message or data has been received.

Information Disclosure

- Disclosing (revealing) sensitive information of a person or an organization without their knowledge.

Denial of Service

- Also known as DOS attacks.
- A type of attack on a network that is designed to bring the network to a congested state by flooding it with useless traffic.
- There are different types of DOS attacks such as the Ping of Death and teardrop attacks, which exploit the limitations in the TCP/IP Protocol.

Elevation of Privileges

- Bugs in certain software may enable a lower-end user to gain access to content which is usually accessible by a higher end user such as an application developer or a system administrator.

Phishing

- Misleading a user by sending emails or directing to web sites where they are asked to update personal information such as passwords, credit card or bank account numbers that the original (legitimate) organization already has.
- These websites are bogus (false) and set up only to steal the information the user enters on the page.

Port Scan

- Scanning a computer's ports to gain access to a computer through a weak point. A port is a place where information goes into and out of a computer.
- Types of port scans
    - Vanilla
    - Strobe
    - Fragmented Packets
    - UDP
    - Sweep
    - FTP Bounce
    - Stealth Scan

Types of attacks

- Hackers and Crackers
- Espionage
- Eavesdropping
- Man in the middle attacks
- IP Session Hijacking

Hackers and Crackers

- Hackers are individuals or teams that use their extensive knowledge in computing to gain unauthorized access in a sneaking manner. This is not done with a harmful purpose in mind, and they are more interested in gaining knowledge about computer systems
- Crackers are computer experts who break into security systems to cause harm and damage to computer systems.

Espionage

Also known as cyber spying, this describes the stealing of secrets stored in digital formats or on computers and IT networks.

Eg:

- Gauss (2012) in Middle East.
- Stuxnet (2010) in Iran.
- Flame (2012) in Iran.
- DuQu (2011)

Eavesdropping

- Network Eavesdropping or network sniffing is a network layer attack consisting of capturing packets from the network transmitted by others' computers and reading the data content in search of sensitive information like passwords, session tokens, or any kind of confidential information.

Man-in-the-middle attack

- Abbreviated as MITM, a man-in-the-middle attack is an active Internet attack where the person attacking attempts to intercept, read or alter information moving between two computers.
- MITM attacks are associated with 802.11 (WLAN) security, as well as with wired communication systems.

IP Session Hijacking

- A security attack on a user session over a protected network. There are two types of session hijacking.
    - ❖ IP Spoofing
    - ❖ Man in the middle attacks
- This is possible because the authentication takes place at the beginning of communication. Once the connection is established, an intruder can send packets and issue commands to the two ends pretending to be authentic commands.

Types of Malware

- Short for malicious software, malware refers to software designed specifically to damage or disrupt a system
- There are several types of malware
    - ❖ Viruses
    - ❖ Hoaxes
    - ❖ Worms
    - ❖ Trojans
    - ❖ Blended Threats
    - ❖ Spams
    - ❖ Spyware

Virus

- A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels.
- Viruses cannot be spread without a human action.
- The damages done can vary depending on the type of virus.

Hoaxes

- In e-mail terms, a hoax is a message which is written to purposely spread fear, uncertainty and doubt. In some cases websites may be attached to prove these false claims.

Worms

- Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action.
- Since worms spread in masses, networks and web servers can be congested and may result in DOS.
- Some advanced types of worms create tunnels in security so that outsiders can gain remote access to a computer system (Eg: Blaster).

Trojans

- The Trojan horse, at first glance will appear to be useful software but will actually do damage once installed or run on your computer.
- Trojans are also known to create a backdoor on a computer system that gives malicious users access to the system.
- Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

Blended Threats

- A blended threat is a more sophisticated attack that bundles some of the worst aspects of viruses, worms,
- Trojan horses and malicious code into one single threat.
- Blended threats are considered to be the worst risk to security since the inception of viruses, as most blended threats also require no human intervention to propagate

Spams

Spam is unsolicited (unwanted) emails. Most often these are electronic junk mail or unwanted newsgroup postings or sometimes emails advertising for some product sent to a mailing list or newsgroup.

Spyware

- Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes.
- Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet

Security precautions: Physical Security

- Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution.
- This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.
- Protection from attackers and natural disasters multiple locks, fencing, walls, fireproof safes, and water sprinklers
- Surveillance and notification systems lighting, heat sensors, smoke detectors, intrusion detectors, alarms, and cameras apprehend attackers and recover quickly.

Security precautions: Software Security

- Encryption
- Antivirus Software
- Firewalls and Proxy servers
- Patches and Updates
- Authentication
- Access Control
- Disable unused Interfaces
- Honeypots and Sugarcanes.

Encryption

- The translation of data into a secret code
- To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.
    - ❖ Plain text - Unencrypted data
    - ❖ Cipher text - Encrypted data
- Uses two types of keys
    - ❖ Public key - known to everyone
    - ❖ Private key - known only to the recipient

Antivirus Software

- An antivirus program is a utility, which scans hard disk drives for viruses, worms and Trojan horses and removes, fixes or isolates any threats that are found.
- Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses.

Firewalls

- A firewall is a system designed to prevent unauthorized access to or from a private network.
- All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.
- Firewalls can be hardware or software

Proxy Servers

- A server that sits between a Web browser, and web server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.
- Proxy servers can also be used to filter requests. For example, a company might use a proxy server to prevent its employees from accessing a specific set of Web sites.

Patches and Updates

- When a software has a bug or a loophole which can become a security threat, a fix called a patch is released by the software company.
- A patch is an actual piece of object code that is inserted into (patched into) an executable program.
- Updates of programs will have bug fixes and patches and are usually available over the internet for free.

Authentication

- The process of identifying an individual, usually based on a username and password.
- In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity.
- Authentication only ensures that the individual is who he or she claims to be.

Access Control/Authorization

- Refers to mechanisms and policies that restrict access to computer resources. Usually this is done by maintaining a list called the ACL.
- The ACL (access control list), is a set of data that informs a computer's operating system which permissions, or access rights, that each user or group has to a specific system object.
- Each object has a unique security attribute that identifies which users have access to such as read, write or execute.

Disabling unused interfaces

- These interfaces refer to the services provided by routers.
- By default, routers come with a lot of services pre-enabled. Which may create a path for intruders to get in to the system.
- It is necessary to disable these unused interfaces by the system administrator to ensure the security.

Honey pots & sugarcanes

- An Internet-attached server that acts as a trap, attracting in possible hackers in order to study their activities and monitor how they are able to break into a system.
- Honeypots are designed to imitate systems that an intruder would like to break into but limit the intruder from having access to an entire network.
- A honeypot that tricks as an open proxy is known as a sugarcane.