UNIT - 4

TROJANS AND BACKDOORS -

(1) Trojan or Trojan Horse is a computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate ~~malicious~~ ~~function that~~ authorizations of a system entity that invokes the Trojan Horse Program.

Backdoor (Trapdoor) is any mechanism that bypasses a normal security check; it may allow unauthorized access to functionality.

(2) Overt Channels and Covert Channels -

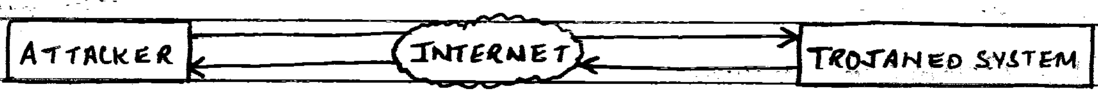
Overt Channel is a legitimate communication path within a computer system, or network, for transfer of data.

An overt channel can be exploited to create the presence of a covert channel by choosing components of the overt channels with care that are idle or not related.

Covert Channel is a channel that transfers information within a computer system, a network, in a way that violates security policy.

Trojans can use covert channels to communicate. Some covert channels rely on a technique called tunneling, which lets one protocol be carried over another protocol.

(3) Working of Trojan -



Trojan ride on the backs of other programs and are usually installed on a system without the users knowledge.

After installation, an attacker gets access to the trojaned system as the system goes online. By the access provided by the Trojan, the attacker can stage different types of attacks.

A Trojan ~~side~~ can be sent to a victim system in many ways, such as the following -

(1) An instant messanger (IM) attachment
(2) IRC (Internet Relay Chat)
(3) An email attachment
(4) NetBIOS file sharing
(5) A downloaded Internet Program.

④ Types of Trojans -

(1) Remote Access Trojans (RATs) - Used to gain remote access to a system.

(2) Data-Sending Trojans - Used to find data on a system and deliver data to a hacker.

(3) Destructive Trojans - Used to delete or corrupt files on a system.

(4) Proxy Trojans - Used to tunnel traffic or launch hacking attacks via other systems.

(5) Denial-of-Service Trojans - Used to launch a denial-of-service attack.

(6) FTP Trojans - Used to create an FTP server in order to copy files onto a system.

(7) Security Software Disabler Trojans - Used to stop antivirus software.

VIRUSES AND WORMS -

① Virus is a malware that, when executed, tries to replicate itself into other executable code; when it succeeds the code is said to be infected. When the infected code is executed, the virus also executes.

Worm is a computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network.

② Characteristics of a Virus -

(1) Virus resides in the memory and replicates itself while the program where it is attached in running.

(2) It does not reside in the memory after the execution of the program.

(3) It can transform themselves by changing codes to appear different.

(4) It hides itself from detection by three ways -

(i) It encrypts itself into the cryptic symbols.

(ii) It alters the disk directory data to compensate the additional virus bytes.

(iii) It uses stealth algorithms to reduce disk data.

③ Working of Virus -

Trigger events and direct attack are the common modes which cause a virus to "go off" on a target system. Most virus operate in two phases -

Infection Phase -

Virus developers decide when to infect the host system's programs.

(1) Some infect each time they are run and executed completely. Eg - Direct Viruses

(2) Some virus codes infect only when users trigger them which include a day, time, or a particular event. Eg - TSR viruses which get loaded in memory and infect at later stages.

Attack Phase -

(1) Some viruses have trigger events to activate and corrupt systems.

(2) Some viruses have bugs that replicate and perform activities like file deletion and increasing the session time.

(3) They corrupt the targets only after spreading completely as intended by their developers

SNIFFERS -

① Sniffer is a packet-capturing or frame capturing tool which captures and displays the data as it is being transmitted from host to host on the network.

② Spoofing -

It is a mechanism in which one person or program successfully masquerades as another by falsifying data, thereby gaining an illegitimate advantage.

IP address spoofing is most common spoofing mechanism.

③ Sniffing -

It is a data interception technology. The objective of sniffing is to steal -

(1) Passwords (from email, the web, SMB (Server Message Block), FTP, SQL, or telnet)

(2) Email text

(3) Files in transfer (email files, ftp files, or SMB)

④ Vulnerable Protocols to sniffing -

(1) Telnet and Rlogin → Keystrokes ~~using~~ including user names and passwords.

(2) HTTP → Data sent in the clear text

(3) SMTP → Passwords and data sent in clear text.

(4) NNTP (Network News Transfer Protocol) - Password & data sent in clear text.

(5) POP (Post Office Protocol) - Password & data sent in clear text,

(6) FTP - Password & data sent in clear text

(7) IMAP (Internet Message Access Protocol) - Password & data sent in clear text

⑤ Types of Sniffing -

(1) Passive Sniffing - It means sniffing through a hub. It is called passive because it is difficult to detect. An attacker simply connects the laptop to a hub and starts sniffing.

(2) Active Sniffing - It means sniffing through a switch. It is difficult to sniff. It can be easily detected. An attacker tries to poison switch by sending bogus MAC address.

Techniques for active sniffing are-

(i) MAC flooding

(ii) ARP (Address Resolution Protocol) spoofing.

PHISHING-

① Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

Phishing will redirect the user to a different website through emails, instant messages, spywares etc.

Phishing attacks can target the audience through mass-mailing millions of email address around the world.

Reasons for successful phishing are-

(1) Lack of knowledge

(2) Visual deception

(3) Not giving attention to Security Indicators.

② Phishing Methods -

~~(1) Mail and Spam~~ (1) Email and Spam → by providing mimic copies of legitimate emails

(2) Web-based delivery - Using third party websites and fake banner advertizements

(3) IRC and Instant Messaging - by sending fake information and links to the users.

(4) Trojaned Hosts - Trojan helps in email propagating and hosting fraudulent websites.

③ Process of Phishing -

The process involved in building a successful phishing site is -

(1) Register a fake domain name

(2) Built a look alike website

(3) Send emails to many users

④ Types of Phishing attacks -

(1) Man-in-the-Middle attacks - In this attack, the attacker's computer is placed between the customer's computer and the real website. This helps the attacker in tracking the communications between the systems.

This attack supports both HTTP and HTTPS communications.

In order to make this attack successful, the attacker has to redirect the customer to proxy server rather than the real server. Techniques used are -

(1) Transparent proxies located at the real server captures all the data by forcing the outbound HTTP and HTTPS traffic towards itself.

(2) DNS Cache Poisoning can be used to disturb the normal traffic routing by establishing false IP address at the key domain names.

(3) Browser proxy configuration is used to set a proxy configuration options by overriding the users web ~~brows~~ browser settings.

(2) URL Obfuscation Attacks - The user is made to follow a URL by sending a message which navigate them to the attacker's server.

The different methods of URL obfuscation are -

(i) Making a few changes to the authorized URL's which makes difficult to identify it as a phishing site.

(ii) Giving ~~fiend~~ friendly login URL's to the users which negates the complexity of authentication that navigates them to the look-a-like target URL.

(iii) Many third party organizations offer to design shorter URL's for free of service, which can be used to obfuscate the true URL.

(v) The IP address of a domain name can be used as a part of the URL to obfuscate the host and also to bypass content filtering systems.

(3) Hidden attacks - Attacker uses the HTML, DHTML, or other scriptable code to -

(i) Change the display of rendered information by interfering with the customer's web browser.

(ii) Disguise content as coming from the real site with fake content.

Methods used for hidden attacks are -

(i) Hidden Frame

(ii) Overriding Page Content

(iii) Graphical substitution.

(4) Client side vulnerabilities - Most customers are vulnerable towards the phishing attack while they browse the web for any software.

These client side vulnerabilities can be exploited in a number of ways similar to the worms and viruses.

The antivirus software are not useful for these vulnerabilities as they are harder to identify.

(5) Deceptive Phishing - The common method of deceptive phishing is email.

Phishers sends a bulk of deceptive emails which command the user to click on the links provided.

Phishers call to action contains daunting information about the recipient's account. Phishers then collects the confidential information given by the user.

(6) Malware-based Phishing - In this method, phishers uses malicious software to attack on the user machines. This phishing attack spreads due to social engineering or security vulnerabilities.

(1) In social engineering, the user is convinced to open an email attachment that attracts the user regarding some important information and download it containing some malware

(2) Exploiting the security vulnerabilities by injecting worms and viruses.

(3) Keyloggers and Screenloggers - It is a program that installs itself into the we
browser or as a device driver that monitors the input data & sends it to the phishing serv

The Technologies used by keyloggers and screenloggers are -

(i) Keylogging → used to monitor & record the key presses by the customer

(ii) Device driver ~~monitoring~~ → monitors the keyboard & mouse inputs by the user.

(iii) Screen logger → monitors both the user inputs and the display.

(4) Web Trojans - These malicious programs are popped up over the login screen when the user is entering information on the website. The information is entered locally rather than on the website which is later transmitted to the phisher.

(5) Host file Poisoning - It is the modification of the host file to make the user navigate to an illegitimate website and give confidential information.

(6) System Reconfiguration attacks - The system DNS server is modified with a faulty DNS information by poisoning the host file. It changes the proxy server setting on the system to redirect the user's traffic to other sites.

(7) DNS based Phishing - It is used to pollute the DNS cache with incorrect information which directs the user to the other location. This type of phishing can be done directly when the user has a misconfigured DNS cache.

The user's DNS server can be changed with a system configuration attack.

(8) Content-Injection Phishing - In this attack, a malicious content is injected into a legitimate site. This malicious content can ~~be~~ direct the user to some other site or it can install malware on the computer.

Types of content-injection phishing are -

(i) Hackers replace the legitimate content with malicious content by compromising the ~~serv~~ server through security vulnerability.

(ii) Malicious content can be injected into a site using cross-site scripting vulnerability

(iii) Illegitimate actions can be performed on a site using an SQL injection vulnerability

(9) Search Engine Phishing - The phishers create an identical websites for fake products and get the pages indexed by the search engine.

Phishers convince the users to give their confidential information by providing interesting offers.

The major success in search engine phishing comes from online banking and online shopping.

WEB APPLICATION SECURITY -

① Hacking web application can be done in five steps -

STEP 1	SCANNING
STEP 2	INFORMATION GATHERING
STEP 3	TESTING
STEP 4	PLANNING THE ATTACK
STEP 5	LAUNCHING THE ATTACK

② Secured authentication mechanism -

It uses cryptographic algorithm to secure the authentication process. Two types of secured authentication mechanism are -

(1) PHP-based authentication mechanism - Users writes its own login procedure using PHP in combination with a MySQL database.

(2) HTTP-based authentication mechanism - Basic authentication is given with the path of name and password provided by HTTP client program or web browser in the form of [illegible]

[illegible]

③ Secured session management [illegible]

Instead of session management, HTTP basic authentication implicitly identifies [illegible] username and password are sent in every packet.

For secured session management, cookie-based session management are used.

Cookies are data that are used by a server to store and retrieve information on a client. The data may be used to encode session information and thereby enable session management on top of the stateless HTTP protocol.

Cookies work as follows. When sending HTTP objects to a client, the server may add information, called a cookies, which is stored on the client by the clients browser. Part of the cookie encodes the range of URLS for which this information is valid. For every future request to a web site within this URL range, the browser will include the cookie.

Cookies have the following attributes -

(i) Name - Cookie's identifier

(ii) Expires – Specifies a date, which defines the cookie's lifetime

(iii) Domain – searches for valid cookies for a given URL

(iv) Path – Specify the valid directory paths for a given domain.

(v) Secure – If the cookie is marked secure, the cookie is only sent over secure connections, namely to HTTPS servers (HTTP over SSL).

④ Web application vulnerabilities–

(1) Cross-site Scripting (XSS) – A parameter entered in a web form is processed by the web application. The correct combination of variables can result in arbitrary command execution. Three types of XSS are–

(i) Persistent XXS attacks – Injected code is stored on the vulnerable server.

(ii) Reflected XSS attacks –(Non-Persistent attacks) – In these attack data is provided by the client is used by the server to generate a page of results for the user.

(iii) DOM-based XSS attacks – The DOM (Document Object Model) allows dynamic modifications of elements of the web page on the client side.

Countermeasures → Validate cookies, query strings, form fields, and hidden fields

(2) SQL Injection – Inserting SQL commands into the URL gets the database server to dump, alter, delete, or create information in the database.

Countermeasures → Validate user variables.

(3) Command Injection – The hacker inserts programming commands into a web form.

Countermeasures → Use ~~specific~~ language-specific libraries for the programming language.

(4) Cookie Poisoning and Snooping – The hacker corrupts or steals cookies.

Countermeasures → Don't store passwords in cookies, implement cookie timeouts and authenticate cookies.

(5) Buffer Overflow – Huge amounts of data are sent to a web application through a web form to execute commands.

Countermeasures → Validate user input length, perform bounds checking.

(6) Authentication Hijacking – The Hacker steals a session once a user has authenticated.

Countermeasures → Use SSL to encrypt traffic.

(7) Directory Traversal/Unicode – The Hacker browses through the folders on a system via a web browser or Windows Explorer.

Countermeasures → Define access rights to private folders on the web server, apply patches and hotfixes.

DENIAL-OF-SERVICE ATTACKS-

① A Denial of Service attack (DoS) is an attack through which a person can render a system unusable, a significantly slow it down for legitimate users, by overloading its resources.

If an attacker is unable to gain access to a machine, the attacker will most likely to crash the machine to accomplish a denial of service attack.

② Types of ~~attacks~~ DOS attacks-

(1) Smurf attack- The perpetrator generates a large amount of ICMP echo (ping) traffic to a network broadcast address with a spoofed source IP set to a victim host.

The result will be lots of ping replies (ICMP echo Reply) flooding the spoofed ho Amplified ping reply stream can overwhelm the victim's network connection.

(2) Buffer overflow attack- It occurs anytime the program writes more information into the buffer than the space allocated in the memory.

The attacker can overwrite the data that controls the program execution path and hijack the control of the program to execute the attacker's code instead of the process code

Sending email messages that have attachments with 256-character file names can cause buffer overflow.

(3) Ping of Death attack - The attacker deliberately sends an IP packet larger than the 65,536 bytes allowed by the IP protocol.

Fragmentation allows a single IP packet to be broken down into smaller segments. The fragments can add up to more than the allowed 65,536 bytes. The O.S, unable to handle oversized packets freezes, reboots, or simply crashes.

The identity of the attacker sending the oversized packet can be easily spoofed.

(4) Teardrop attack- IP requires that a packet that is too large for the next router to handle should be divided into fragments. The attacker's IP puts a confusing offse value into the second or later fragment.

If the receiving OS is not able to aggregate the packets accordingly, it can crash the system. It is a UDP attack, which uses overlapping offset fields to bring down hosts
Unnamed attack → variation of the teardrop attack. Fragments are not overlapping but gaps are incorporated.

(5) SYN attack - The attacker sends bogus TCP SYN requests to a victim server. The host allocates resources (memory sockets) to the connection which cause malicious flooding because of large volumes of TCP SYN ~~request~~ packets to the victim's system with spoofed source IP addresses can cause DoS.

It prevents server from responding to the legitimate requests. This attack exploits the three-way handshake.

(6) SYN Flooding - It takes advantage of a flaw in how most hosts implement the TCP three-way handshake.

When Host receives the SYN request from ~~attacker~~ other host, it must keep track of the partially-opened connection in a 'listen queue' for atleast 75 seconds. A malicious host can exploit the small size of the listen queue by sending multiple SYN requests to a host, but never replying to the SYN&ACK. The victim's listen queue is quickly filled up.

This ability of removing a host from the network for at least 75 seconds can be used as a DoS attack.

③ DDoS attack (Distributed DOS attack) -

It is the attack in which a multitude of compromised systems attack a single target, thereby causing DoS for users of the targeted system.

④ Session Hijacking -

It is when an attacker gets access to the session state of a particular user by stealing a valid session ID.

→ Steps in session hijacking are -

(1) Place yourself between the victim and the target (by sniffing the network)

(2) Monitor the flow of packets

(3) Predict the sequence number

(4) Kill the connection to the victim's machine.

(5) Take over the session

(6) Start injecting packets to the target server

→ There are two types of session hijacking attacks -

(1) Active → An attacker finds an active session and takes over

(2) Passive → An attacker hijacks a session, but sits back, and watches and records all the traffic that is being sent forth.

⑤ Spoofing Vs. Hijacking -

In a spoofing attack, an attacker does not actively take another user offline to perform an attack. He pretends to be another user or machine to gain access.

Hijacking is done only after the victim has connected to the server. With hijacking, an attacker takes over an existing session, which means he relies on the legitimate user to make a connection and authenticate. Subsequently, the attacker takes over the session.

⑥ TCP/IP Hijacking -

It is a hijacking technique that uses a spoofed packets to take over a connection between a victim and a target machine.

The victim's connection hangs, and the hacker is then able to communicate with the host's machine as if the attacker is the victim.

To launch a TCP/IP hijacking attack, the hacker must be on the same network as the victim.

The target and the victim machines can be anywhere.

⑦ Captcha Protection -

A Captcha is a type of challenge-response test used in computing to ensure that the response is not generated by a computer.

CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart.