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 endures security mechanisms, sometimes by exploiting legitimate mechanisms, functions that authorizations of a system entity that prompts the Trojan Horse Proposal. Backdoor (Trojan) is any mechanism that bypasses normal security check, it may allow unauthorized access to functionality.

2. Attacker and Court Channel -

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

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

Court 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 -

ATTACKER - [INTERNET] - TROJANED SYSTEM

Trojan rides on the backs of other programs and are usually installed on a system without the user's knowledge.

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

A Trojan ride can be sent to a victim system in many ways, such as:

- The following:
  1. An instant message (IM) attachment
  2. IRC (Internet Relay Chat)
  3. An email attachment
  4. A downloaded Internet Program
  5. NetBIOS file sharing
4. Types of Trojans -
   (1) Remote Access Trojans (RATs) - Used to gain remote access to a system.
   (2) Data-Storing Trojans - Used to steal data on a system and deliver data back to a hacker.
   (3) Deceptive Trojans - Used to delete or corrupt files on a system.
   (4) Proxy Trojans - Used to tunnel traffic or launch backdoor 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 Deception Trojans - Used to help anticrime software.

5. Viruses and Worms -
   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 is 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 -
      (a) It encrypts itself into the crypthem symbols.
      (b) It alters the disk sectoring data to camouflage the additional virus bytes.
      (c) It uses stealth algorithms to reduce disk data.

3. Working of Virus -
   Trojans evade and direct attacks on the common modes which cause a virus to 'go off' on a target system. Most viruses 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. E.g. - Direct Virus
(2) Some virus codes infect only when users trigger them which include a day, time, or a particular event. E.g. - TSR viruses which get loaded in memory and infect at later stages.

Attack Phase:
(1) Some viruses have trigger events to activate and corrupt system.
(2) Some viruses have bugs that replicate and perform activities like file deletion and increasing the system time.
(3) They corrupt the target only after spreading completely as intended by their developer.

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 (Secure Message Block), FTP, SQL, or telnet
   (2) E-mail text
   (3) Files in transfer (email files, ftp files, or SMB)

Vulnerable Protocols & sniffing:
(1) Telnet and Rlogin - Keystrokes being including user names and passwords
(2) HTTP - Data sent in the clear text
(3) SNMP - 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) ELP - 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 has to poison switch by sending forged MAC addresses.

Techniques for active sniffing are:
   (a) MAC flooding
   (b) 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 email, instant messages, phone calls etc.

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

Reasons for successful phishing are -
   (1) Lack of knowledge
   (2) Human deception
   (3) Not giving attention to security indicators

2. Phishing Methods -
   (a) Malware and spam
   (b) Email and Spam - by providing mimic copies of legitimate emails
(2) Web-based delivery - Using third-party websites and fake login advertisements.
(3) IRC and Instant Messaging by sending fake information and links to the users.
(4) Trojanized Host - 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) Build a look-alike website
   (3) Send email 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 seduce 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 outward HTTP and HTTPS traffic towards itself.
      (2) DNS Cache Poisoning can be used to disrupt 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 user's web browser's settings.
   (2) URL Obfuscation Attacks - The user is made to follow a URL by sending a message which navigates 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 friendliest 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 shorted URL’s for free of service.
which can be used to obfuscate the true URL.

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

(3) **Hidden Frames** - Attackers use the HTML, DHTML, or other scripted code to:
   - Change the display of render information by manipulating with the customer's web browser.
   - Impose content as coming from the real site with fake content.
   - Methods used for hidden attacks are:
     - Hidden Frame
     - Attacking Page Content
     - Spying 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 above and many more.

The anti-virus software are not useful for these vulnerabilities as they are hard to identify.

(5) **Phishing Email** - The common method of deception phishing is email.

Phishers send a bulk of deceptive emails which command the user to click on the fake James.

Phishing will to action contain deaturing information about the recipient's account. Phishers convert the confidential information given by the user.

(6) **Malware-based Phishing** - In this method, phishers use malicious software to attack on the user's machines. This phishing attack spreads due to social engineering.

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

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

(3) **Keyloggers and Keyscanners** - It is a program that installs itself into the user's device or on a device, device that monitors the input data and send it to the phisher.
The technologies used by keyloggers and mouseloggers are:

(i) **Keylogger** - Used to monitor & record the key presses by the user.
(ii) **Device Driver** - Monitors the keyboard & mouse inputs by the user.
(iii) **Screen logger** - Monitors both the user inputs and the display.

(a) **Web Tamper** - 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.

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

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

(d) **DNS Cache Poisoning** - 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 reconfiguration attack.

(e) **Content Injection Phishing** - In this attack, a malicious content is injected into a legitimate site. This malicious content can be direct the user to form the 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 server through security vulnerability.
(ii) Malicious content can be injected into a site using cross-site scripting vulnerability.
(iii) Unlicensed actions can be performed on a site using SQL injection vulnerability.

(f) **Search Engine Phishing** - The phisher create an identical website for fake product and get the forms include by the search engine.

Phisher convince the user to give their confidential information by providing interesting offers.

The major concern in search engine phishing comes from online banking and online shopping.
1. Hacking web applications can be done in five steps:

<table>
<thead>
<tr>
<th>STEP 1</th>
<th>SCANNING</th>
</tr>
</thead>
<tbody>
<tr>
<td>STEP 2</td>
<td>INFORMATION GATHERING</td>
</tr>
<tr>
<td>STEP 3</td>
<td>TESTING</td>
</tr>
<tr>
<td>STEP 4</td>
<td>PLANNING THE ATTACK</td>
</tr>
<tr>
<td>STEP 5</td>
<td>LAUNCHING THE ATTACK</td>
</tr>
</tbody>
</table>

2. Secured authentication mechanisms:

   - Uses cryptographic algorithms to secure the authentication process.
   - Two types of secured authentication mechanisms:
     - (a) PHP-based authentication mechanism - Uses its own login procedure using PHP in combination with a MySQL database.
     - (b) HTTP-based authentication mechanism - Basic authentication is given with the help of a user and password provided by HTTP client program in URL request in the form of queries.

3. Secured session management:

   - Cookie-based session management, HTTP-based authentication, implicitly identifies the user by using a name and forward or not in every packet.
   - For secured session management, cookie-based session management can be used.

   Cookies are data that are used by a service to store and retrieve information on a client. This data may be used to encode session information and transfer session management on top of the stolen HTTP headers.

   Cookies work as follows: When sending HTTP objects to a client, the user may add information, called a cookie, which is read on the client by the client browser. Part of the cookie encodes the range of URLs for which this information is valid. For every future request to a website within this URL range, the browser will include the cookie.

   Cookies have the following advantages:
   - in Name - Cookies identifiers.
(iii) Expires - Specify a date, which defines the cookie's lifetime.
(iv) Domain - search for valid cookies for a given URL.
(v) Path - Specify the valid directory path for a given domain.
(vi) Secure - If the cookie is marked secure, the cookie is only sent on secure connections, namely to HTTPS server (HTTP over SSL).

3. 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 variable can result in arbitrary command execution. Three types of XSS are -
(i) Persistent XSS 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 and 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 Injections - Injecting SQL commands into the URL get the database issues to dump, alter, delete, or write 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 Stealing - The hacker copies or steal cookie.

Countermeasures - Don't store passwords in cookies; implement cookie timeouts and encryption protocols.

(5) Header Overflows - Large amounts of data are sent to a web application through a web form to execute commands.

Countermeasures - Validate input length, perform bounds checking.

(6) Authentication Hijacking - The Hacker steals a username once a user has authenticated.

Countermeasures - Use SSL to encrypt traffic.

(7) Directory Traversal/Unwinding - The Hacker [have] through the folders on a system via a

web browser or Windows Explorer.
Countermoves - Define access rights to private folders on the web servers, 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 hault down for legitimate uses, by overloading its resources.

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

2. Types of attacks DoS attack

   (1) Flood attack - The perpetrator generates a large amount of ICMP echo (ping) traffic to a network broadcast address with a spoofed source IP set to victim host.
      
      The result will be lots of ping replies (ICMP echo reply) flooding the spoofed host.
      
      Amplified flooding attack can overwhelm the victim's network connection.

   (2) Buffer overflow attack - It occurs anytime the program units 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
     
      sending email messages that have attachments with 256-character file names
      can cause large crashes.

   (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 small
      
      segments. The fragment can add up to more than the allowed 65,536 bytes. The OS
      
      unable to handle oversized packets. Foreage network, or simply crash.

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

   (4) Teardrop attack - IP requires that a packet that is too large for the next network
to handle should be divided into fragments. The attacker's IP puts a confusing offset
value in the record or later fragment.
Of the receiving OS is not able to aggregate the packets accordingly, it can crash the system. It is a UDP attack, which was overlapping offset fields to bring down hosts. Unnumbered attack → Vaccum of the head-of-attack. Fragments are not overlapping but gaps are manipulated.

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

It prevents users 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, it must keep track of the partially opened connection in a ‘listen queue’ for at least 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 SYNACK. 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

The three main types of session hijacking attacks are:

(1) Arachnid: An attacker finds an active session and takes over.
(2) Parnix: An attacker hijacks a session, but stays back and watches and records all the traffic that is being sent back.

5. Spoofing vs. Hijacking

Spoofing involves an attacker pretending 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 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 target 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.