Chapter Five

Application Security

What are Virus & Malicious Code

- Malicious code refers to a broad category of programs that can cause damage or undesirable effects to computers or networks.
- Potential damage can include modifying, destroying or stealing data, gaining or allowing unauthorised access to a system, bringing up unwanted screens, and executing functions that a user never intended.

Continued...

Examples of malicious code include computer

1. Viruses, is a program that infects a computer by attaching itself to another program, and propagating itself when that program is executed.

2. Worms, is a standalone malware computer program that replicates itself in order to spread to other computers

3. Trojan horses, A Trojan horse is a harmful program that misrepresents itself to trick as a regular, kind program or utility in order to persuade a victim to install it.

A Trojan horse usually carries a hidden destructive function that is activated when the application is started.

4. Logic bombs, piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

Continued...

5. Spyware, is a type of software that secretly forwards information about a user to third parties without the user's knowledge or consent. This information can include a user's online activities, files accessed on the computer, or even user's keystrokes.

6. Adware, is a type of software that displays advertising banners while a program is running. Some adware can also be spyware. They first spy on and gather information from a victim's computer, and then display an advertising banner related to the information collected.

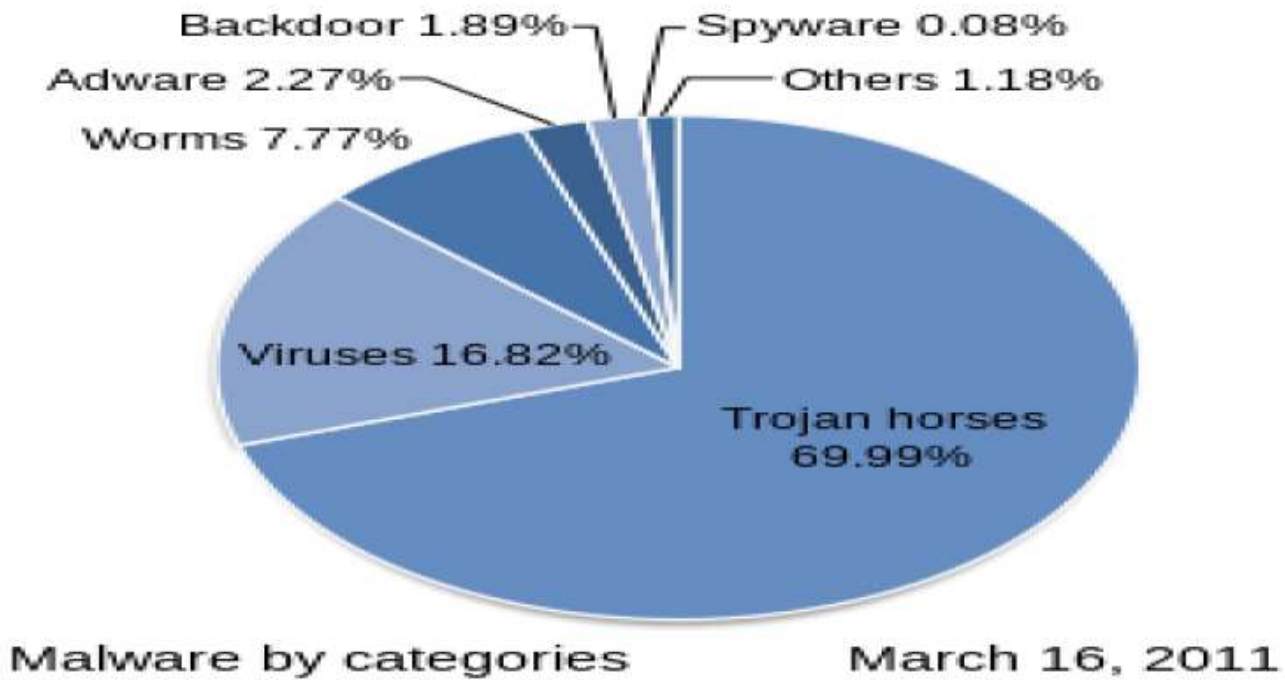
Continued...

- Because they pose a serious threat to software and information processing facilities, users and administrators must take precautions to detect and prevent malicious code outbreaks.
- **Computer viruses are still the most common form of malicious code**.
- Another frequently encountered malicious code is the worm, which is a computer program that can make copies of itself, spreading through connected systems and consuming resources on affected computers or causing other damage.
- Some malicious codes, including most viruses, are fragments of programs that cannot exist alone and need to attach themselves to host programs. Other types of malicious code are able to spread and replicate by themselves (such as worms) and are able to propagate from computer to computer across a network.

Continued...

- It should be noted that some malicious programs are able to exhibit the behaviours of more than one type of malicious code. For example, certain programs may be a virus and a trojan horse at the same time.
- A virus can be either transient or resident.
- A **transient** virus has a life that depends on the life of its host; the virus runs when its attached program executes and terminates when its attached program ends. (During its execution, the transient virus may have spread its infection to other programs.)
- A **resident** virus locates itself in memory; then it can remain active or be activated as a stand-alone program, even after its attached program ends.

Continued…


Backdoor 1.89%
Spyware 0.08%
Adware 2.27%
Others 1.18%
Worms 7.77%
Viruses 16.82%
Trojan horses
69.99%
Malware by categories
March 16, 2011

Computer Virus

- A computer virus is a self replicating computer program which can attach itself to other files/programs, and can execute secretly when the host program/file is activated. When the virus is executed, it can perform a number of tasks, such as erasing your files/hard disk, displaying nuisance information, attaching to other files, etc.
- **Type of virus**

1) **Memory-Resident Virus** - This type will reside in main system memory. Whenever the operating system executes a file, the virus will infect a file if it is a suitable target, for example, a program file.

2) **Program File Virus** - This will infect programs like EXE, COM, SYS etc.

3) **Polymorphic Virus** -The virus itself can change form using various polymorphism techniques.

Continued...

4) **Boot Sector Virus** -This type will infect the system area of a disk, when the disk is accessed initially or booted.

5) **Stealth Virus** - A virus which uses various stealth techniques in order to hide itself from detection by anti-virus software.

6) **Macro Virus** - Unlike other virus types, these viruses attack data files instead of executable files.

7) **Email virus** - A virus spread by email messages.

Continued...

Tips for Prevention

- Install a file and directory integrity checker.
- Be alert to suspicious hard disk activity and/or network activity e.g. if your hard disk access LED light is always on.
- Be alert to suspicious deletion or modification of files.
- Check if your system is accessed without your knowledge, e.g. your email accounts.
- Not download / install software from suspicious sources such as websites, peer-to-peer file sharing sources, etc.

Continued...

- Read the terms and conditions of use, even before downloading and installing a legitimate piece of software, because they may require you to accept that an adware or spyware system be installed.
- Read the terms of use carefully when you are asked to install a plug-in or use active content when visiting some websites.
- Review the information provided by certain search engines whose search results may contain malicious code. This may help in avoiding dangerous or untrustworthy websites via search links.
- Install browser toolbars that can help filter out adware and spyware.
- Install anti-spyware and anti-adware software.

Detection and Recovery

- The following symptoms may indicate a computer is infected with a virus or malicious code:
- A program takes longer time than usual to execute.
- A sudden reduction in system memory or available disk space.
- A number of unknown or new files, programs or processes on the computer.
- Popping up of new windows or browser advertisements.
- Abnormal restarts or shutdowns of the computer.
- An increase in network usage.

Threats in computer

- Computer crime, Vulnerability, Eavesdropping
- Malware, Spyware, Ransom ware
- Trojans, Viruses, Worms1q3
- Rootkits, Boot kits, Key loggers
- Screen scrapers, Exploits, Backdoors
- Logic bombs, Payloads, Denial of service

II. Securing Services

- **Secure Shell** (**SSH**) is a cryptographic network protocol for operating network services securely over an unsecured network.
- The best known example application is for remote login to computer systems by users. SSH provides a secure channel over an unsecured network in a client-server architecture, connecting an SSH client application with an SSH server.
- Common applications include remote command-line login and remote command execution, but any network service can be secured with SSH. The protocol specification distinguishes between two major versions, referred to as SSH-1 and SSH-2

Secure Email:

- We rely on e-mail's confidentiality and integrity for sensitive and important communications, even though ordinary e-mail has almost no confidentiality or integrity.
- Here we investigate how to add confidentiality and integrity protection to ordinary e-mail.
- E-Mails are just like postcards from which the information can be viewed by anyone.
- When a mail is transferred from one mail server to another mail server there are various stops at which there is a possibility of unauthorized users trying to view the information or modify it.

Continued...

Examples:

- Say you have won a lottery of million dollars. So ignore such kind of e-Mails, do not participate in it and consider it as a scam.
- Sometimes e-Mails offering free gifts and asking personal information are received from unknown addresses. This is one way to trap your personal information.
- One way of stealing the password is standing behind an individual and looking over their password while they are typing it or searching for the papers where they have written the password.

Continued...

- Another way of stealing the password is by guessing. Hackers try all possible combinations with the help of personal information of an individual.
- When there are large numbers of combinations of passwords the hackers use fast processors and some software tools to crack the password. This method of cracking password is known as “Brute force attack”.
- Generally spammers or hackers try to steal e-Mail address and send malicious software or code through attachments, fake e-Mails, and spam and also try to collect your personal information

E-MAIL THREATS:

- **Attachments**
- Sometimes attachments come with e-mails and may contain executable code like macros, .EXE files and ZIPPED files. Sometimes attachments come with double extensions like “attachment.exe.doc”.
- **Fake e-Mails**
- Sometimes e-Mails are received with fake e-mail
- **Spam e-Mails**
- Spam messages may trouble you by filling your inbox or your e-mail database. Spam involves identical messages sent to various recipients by e-Mail. Sometimes spam e-mails come with advertisements and may contain a virus. It is always recommended to ignore or delete spam e-mails.

Continued...

E-Mails offering free gifts

- Sometimes e-Mails are targeted at you by unknown users by offering gifts, lottery, prizes, which might be free of cost, and this may ask your personal information for accepting the free gift or may ask money to claim lottery and prizes it is one way to trap your personal information.

Hoaxes

- Hoax is an attempt to make the person believe something which is false as true. It is also defined as an attempt to deliberately spread fear, doubt among the users.

HOW TO PREVENT?

- **Using filtering software's -** Use e-Mail filtering software to avoid Spam so that only messages from authorized users are received. Most email providers offer filtering services.
- **Ignore e-mails from strangers**
- Avoid opening attachments coming from strangers, since they may contain a virus along with the received message. Be careful while downloading attachments from e-Mails into your hard disk. Scan the attachment with updated antivirus software before saving it.

GUIDELINES FOR USING E-MAIL SAFELY

- Since the e-Mail messages are transferred in clear text, it is advisable to use some encryption software like PGP (pretty good privacy) to encrypt email messages before sending, so that it can be decrypted only by the specified recipient only.
- Use Email filtering software to avoid Spam so that only messages from authorized users are received. Most e-Mail providers offer filtering services.
- Do not open attachments coming from strangers, since they may contain a virus along with the received message.
- Be careful while downloading attachments from e-Mails into your hard disk. Scan the attachment with updated antivirus software before saving it.

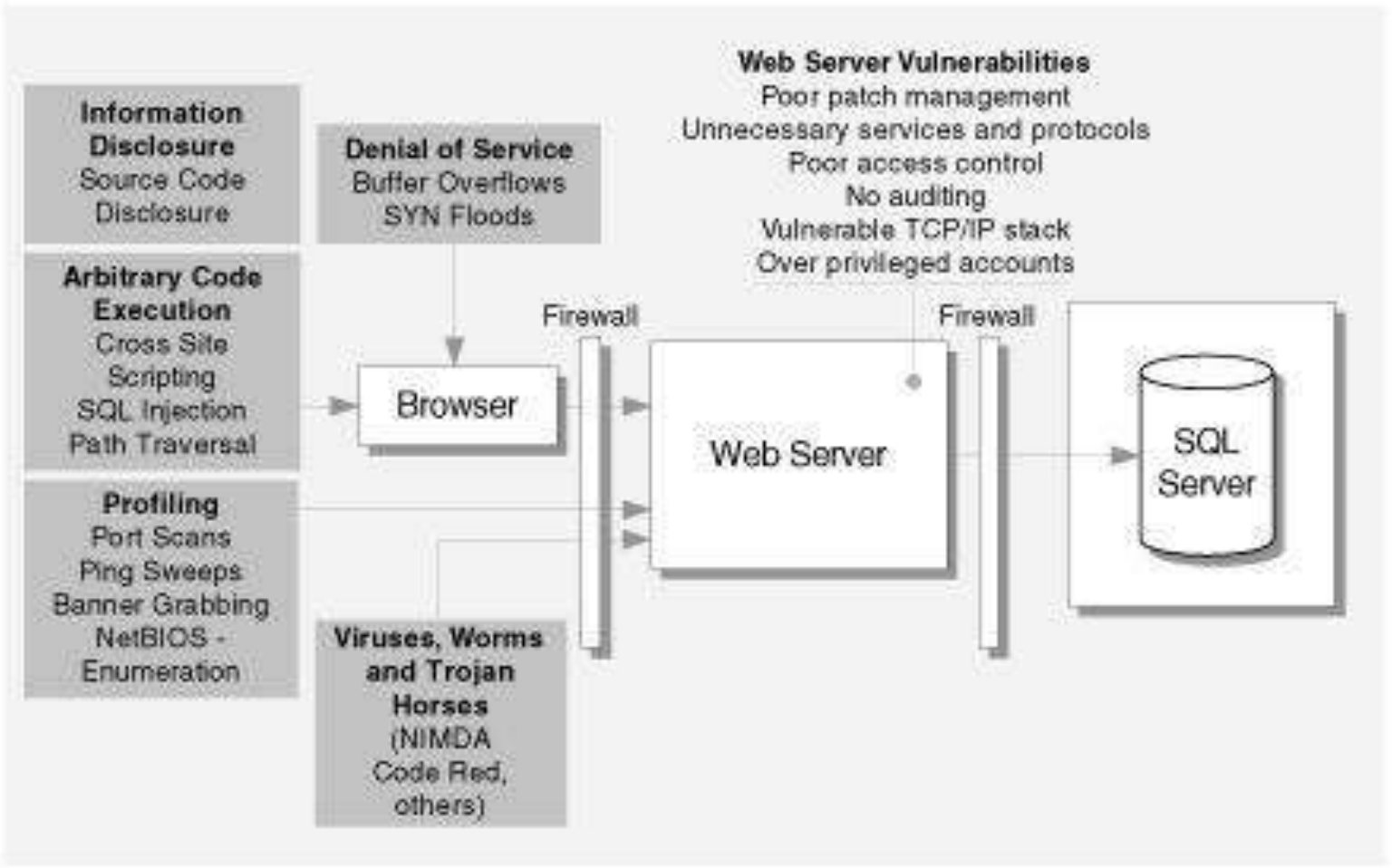
Continued...

- Do not send messages with attachments that contain executable code like Word documents with macros, .EXE files and ZIPPED files. We can use Rich Text Format instead of the standard .DOC format. RTF will keep your formatting, but will not include any macros. This may prevent you from sending virus to others if you are already infected by it.
- Avoid sending personal information through e-Mails.
- Avoid filling forms that come via e-Mail asking for your personal information and do not click on links that come via e-Mail.
- Do not click on the e-Mails that you receive from un trusted users as clicking itself may execute some malicious code and spread into your system.

Web servers

- Below we've provided some specific guidance on problems we often see with the two most common web servers: Apache, and Microsoft's Internet Information Server (IIS). A secure Web server provides a protected foundation for hosting your Web applications, and Web server configuration plays a critical role in your Web application's security.
- **Threats and Countermeasures**
- The fact that an attacker can strike remotely makes a Web server an appealing target.
- **The main threats to a Web server are:**
- **Profiling**
- **Denial of service**
- **Unauthorized access**
- **Arbitrary code execution**
- **Elevation of privileges**
- **Viruses, worms, and Trojan horses**

Continued...



- **Figure 16.1 Architecture summarizes the more prevalent attacks and common vulnerabilities.**

Web Server Security

- Securing a web server is as important as securing the website or web application itself and the network around it.
- Below is a list of tasks one should follow when securing a web server.

1. Remove Unnecessary Services

- Default operating system installations and configurations, are not secure.
- The more services running on an operating system, the more ports will be left open, thus leaving more open doors for malicious users to abuse.
- Switch off all unnecessary services and disable them, so next time the server is rebooted, they are not started automatically. Switching off unnecessary services will also give an extra boost to your server performances, by freeing some hardware resources.

Continued...

2. Remote access

- Although nowadays it is not practical, when possible, server administrators should login to web servers locally.
- If remote access is needed, one must make sure that the remote connection is secured properly, by using tunneling and encryption protocols.

3. Separate development / testing / production in server environment

- Since it is easier and faster for a developer to develop a newer version of a web application on a production server, it is quite common that development and testing of web applications are done directly on the production servers itself.

Continued...

- **4 .Web application content and server-side scripting**
- 0partition or drive other than that of the operating system, logs and any other system files
- **5. Permissions and privileges**
- File and network services permissions play a vital role in web server security. If a web server engine is compromised via network service software, the malicious user can use the account on which the network service is running to carry out tasks, such as execute specific files.

Continued...

6. Install all security patches on time

- Although having fully patched software does not necessarily mean your server is fully secure, it is still very important to update your operating system and any other software running on it with the latest security patches.

7. Monitor and audit the server

- All the logs present in a web server, should ideally be stored in a segregated area. All network services logs, website access logs, database server logs (e.g. Microsoft SQL Server, MySQL, Oracle) and operating system logs should be monitored and checked frequently.

8. User accounts

- Unused default user accounts created during an operating system install should be disabled. There is also a long list of software that when installed, user accounts are created on the operating system.

Continued...

9. Remove all unused modules and application extensions

- A default Apache installation has a number of pre-defined modules enabled, which in a typical web server scenario are not used, unless they are specifically needed. Turn off such modules to prevent targeted attacks against such modules.

10. Use security tools provided with web server software

- Microsoft released a number of tools to help administrator's secure IIS web server installations, such as URL scan. There is also a module called mod security for Apache.

Continued...

Most Common Attacks Affecting Today's Websites

- The Goal of Website Crackers (Hackers) the motive behind online attacks are varied.
- SQL Injection (SQLi).
- Cross-Site Scripting (XSS).
- Inclusion Vulnerabilities: LFI and RFI.
- Brute Force.

III. Identifying Vulnerability tools and techniques:

- A vulnerability is any mistakes or weakness in the system security procedures, design, implementation or any internal control that may result in the violation of system's security policy Or, in other words, the possibility for intruders (hackers) to get unauthorized access.

Continued...

What is Vulnerability Assessment?

- Vulnerability Assessment is a software testing technique performed to evaluate the sudden increase of risks involved in the system in order to reduce the probability of the event. It depends on two mechanisms:-

1. Vulnerability Assessment

2. Penetration Testing

- **Why to do Vulnerability Assessment**

Continued…

Continued...

- It is important for the security of the organization.
- The process of locating and reporting the vulnerabilities, which provide a way to detect and resolve security problems by ranking the vulnerabilities before someone or something can exploit them.
- In this process Operating systems, Application Software and Network are scanned in order to identify the occurrence of vulnerabilities, which include inappropriate software design, insecure authentication, etc.

Vulnerability Methodologies

1. **Setup:**

- Begin Documentation, Secure Permission, Update Tools, Configure Tools

2. **Test Execution:**

- Run the Tools, and process the vulnerability testing over the Application software, OS, and Network.

3. **Vulnerability Analysis:**

- Defining and classifying network or System resources, Assigning priority to the resource (Ex: - High, Medium, Low), Identifying potential threats to each resource. Developing a strategy to deal with the most prioritize problems first. Defining and implementing ways to minimize the consequences if an attack occurs.

4. **Reporting**

- Reporting the problems.

- 5. **Remediation:**

The process of fixing the vulnerabilities, For every vulnerability

Types of vulnerability scanner

1. **Host Based**

- Identifies the issues in the host or the system. The process is carried out by using host-based scanners and diagnose the vulnerabilities.
- The host-based tools will load a mediator software onto the target system; it will trace the event and report it to the security analyst.

2. **Network Based**

- It will detect the open port, and identify the unknown services running on these ports. Then it will disclose possible vulnerabilities associated with these services.
- This process is done by using Network-based Scanners

Continued...

3. **Database Based**

- It will identify the security exposure in the database systems using tools and techniques to prevent from SQL Injections. (SQL Injections: - Injecting SQL statements into the database by the malicious users, which can read the sensitive data's from database and can update the data in the Database.)

Continued…

Tools for Vulnerability Scanning

Category	Tool	Description
Host Based	STAT	Scan multiple systems in the network
	TARA	Tiger Analytical Research Assistant.
	Cain & Abel	Recover password by sniffing network, cracking http password.
	Metasploit	Open source platform for developing, testing and exploit code.
Network Based	Cisco Secure Scanner	Diagnose and Repair Security Problems.
	WireShark	Open Source Network Protocol Analyzer for Linux and Windows.
	Nmap	Free Open Source utility for security auditing.
	Nessus	Agent less auditing, Reporting and patch management integration.
Database Based	SQL diet	Dictionary Attack tool door for SQL server.
	Secure Auditor	Enable user to perform enumeration, scanning, auditing and penetration testing and forensic on OS.
	DB-scan	Detection of Trojan of database, detecting hidden Trojan by baseline scanning.

Continued...

Advantages of Vulnerability Assessment

- Open Source tools are available.
- Identifies almost all vulnerabilities
- Automated for Scanning.
- Easy to run on regular basis.

Disadvantages of Vulnerability Assessment

- High false positive rate
- Can easily detect by Intrusion Detection System Firewall.
- Often fail to notice the latest vulnerabilities.

Vulnerability Testing Methods

1. **Active Testing**

- Active Testing, a tester introduces new test data and analyzes the results.
- During the testing process, the testers create a mental model of the process, and it will grow further during the interaction with the software under test.
- While doing the test, the tester will actively involve in the process of finding out the new test cases and new ideas. That's why it is called Active Testing.

2. **Passive Testing**

- Passive testing, monitoring the result of running software under test without introducing new test cases or data.

Continued...

3. **Network Testing**

- Network Testing is the process of measuring and recording the current state of network operation over a period of time.
- Testing is mainly done for predicting the network operation under load or to find out the problems created by new services.

We need to Test the following Network Characteristics:-

1. Utilization levels
2. Number of Users
3. Application Utilization

Continued...

4. **Distributed Testing**

- Distributed Tests are applied for testing distributed applications, which means, the applications that are working with multiple clients simultaneously. Basically, testing a distributed application means testing its client and server parts separately, but by using distributed testing method, we can test them all together.
- The test parts will interact with each other during the Test Run. This makes them synchronized in an appropriate manner. Synchronization is one of the most crucial points in distributed testing.

PENETRATION TESTING

- A penetration test, colloquially known as a pen test, is an authorized simulated attack on a computer system, performed to evaluate the security of the system.
- The test is performed to identify both weaknesses (also referred to as vulnerabilities), including the potential for unauthorized parties to gain access to the system's features and data, as well as strengths, enabling a full risk assessment to be completed.
- A penetration test can help determine whether a system is vulnerable to attack if the defences were sufficient, and which defences (if any) the test defeated.

Continued...

- Security issues that the penetration test uncovers should be reported to the system owner.
- Penetration test reports may also assess potential impacts to the organization and suggest countermeasures to reduce risk.
- The goals of a penetration test vary depending on the type of approved activity for any given engagement with the primary goal focused on finding vulnerabilities that could be exploited by a nefarious actor and informing the client of those vulnerabilities along with recommended mitigation strategies.
- Penetration tests are a component of a full security audit.

PENETRATION TESTING STAGES

- The pen testing process can be broken down into five stages.

1. **Planning and investigation**

- The first stage involves, Defining the scope and goals of a test, including the systems to be addressed and the testing methods to be used. Gathering intelligence (e.g., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities.

2. **Scanning**

- The next step is to understand how the target application will respond to various intrusion attempts. This is typically done using:
- o **Static analysis** – Inspecting an application's code to estimate the way it behaves while running. These tools can scan the entirety of the code in a single pass.

Continued...

- o **Dynamic analysis** – Inspecting an application's code in a running state. This is a more practical way of scanning, as it provides a real-time view into an application's performance.
- 3. **Gaining access**
- This stage uses web application attacks, such as cross-site scripting, SQL injection and backdoors, to uncover a target's vulnerabilities. Testers then try and exploit these vulnerabilities, typically by escalating privileges, stealing data, intercepting traffic, etc., to understand the damage they can cause.

Continued...

4. **Maintaining access**

- The goal of this stage is to see if the vulnerability can be used to achieve a persistent presence in the exploited system. The idea is to imitate advanced persistent threats, which often remain in a system for months in order to steal an organization's most sensitive data.

5. **Analysis**

- The results of the penetration test are then compiled into a report detailing:
- o Specific vulnerabilities that were exploited
- o Sensitive data that was accessed
- o The amount of time the pen tester was able to remain in the system undetected

Thank You!