Introduction to Network Security, Computer Security and Cyber Security

Network Security

- Network security is defined as the activity created to protect the integrity of your network and data.
- The most basic example of Network Security is password protection which the user of the network chooses.
- Network security primarily deals with the protection of networks and their infrastructure from unauthorized access, attacks, and disruptions.
- It involves securing network devices such as routers, switches, firewalls, and ensuring the confidentiality, integrity, and availability of data transmitted over networks.
- Network security measures include firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), virtual private networks (VPNs), and secure network protocols.

Computer Security

- Computer security focuses on safeguarding individual computer systems, devices, and data from threats, vulnerabilities, and unauthorized access.
- It involves protecting the hardware, software, and data stored on computers, laptops, servers, and other computing devices.
- Computer security measures include antivirus software, encryption, access control mechanisms, secure boot processes, and regular security updates and patches.

Cyber Security

- Cyber security is a broader term that includes both network security and computer security, along with other aspects related to the protection of digital systems, networks, and data.
- It deals with defending against cyber threats such as malware, phishing attacks, ransomware, data breaches, and cyber espionage.
- Cyber security also involves risk management, incident response, security policies and procedures, security awareness training, and compliance with regulatory requirements.

Security Terminologies and Principles

The different security principles and there terminology are as below

- **Confidentiality:** The confidentiality principle means that only the sender and the intended recipient should be able to access the message. Confidentiality is not achieved if an unauthorized person is able to access a message.
- **Authentication:** The authentication principle help to establish proof of identities. The authentication process makes sure that the sender of an electronic message or document is correctly identified.
- **Integrity:** The integrity principle protects data against active threats like those that may alter it.
- **Non-repudiation:** The principle of non-repudiation prevents either sender or receiver from denying a transmitted message. Therefore, whenever a message is send by the sender, the receiver can prove that the message was sent by that the sender. When a message is received, the sender can prove that the message was received by the receiver.
- **Access control/Authorisation:** The principle of access control means the ability to limit and control the access to host systems and applications through communication links. To achieve this, a user attempting to access must first be identified, or authenticated.
- **Availability:** The principle of availability means that system resources must be available to authorized entities at all times.

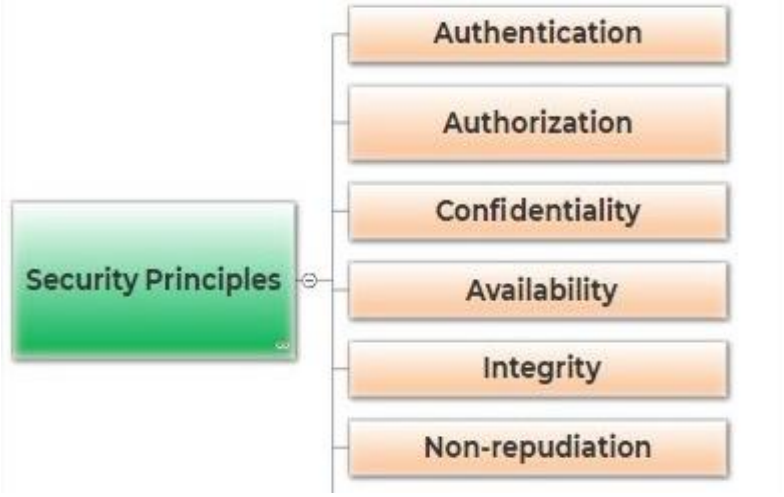


Figure 1: Security Terminologies And Principles

Security Threats

- In computer security a threat is a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm.
- Some of the common security threats you may come across:
  - Malware
  - Computer virus
  - Rogue security software
  - Trojan horse
  - Malicious spyware
  - Computer worm
  - Botnet
  - Spam
  - Phishing
  - Spoofing
  - Rootkit

Malware:

- Malware is short for “malicious software.”
- Malware is a term used to mean a “variety of forms of hostile, intrusive, or annoying software or program code.”
- Malware could be computer viruses, worms, Trojan horses, dishonest spyware, and malicious rootkits

Computer virus:

- A computer virus is a small piece of software that can spread from one infected computer to another.
- The virus could corrupt, steal, or delete data on your computer—even erasing everything on your hard drive.
- A virus could also use other programs like your email program to spread itself to other computers.

Rogue Security Software:

- Rogue security software programs refer to what we also known as “fake antivirus.”
- It is a malicious program that tricks users into thinking their computers are infected by malware so they would buy the software.
- A rogue security software doesn’t protect against cyber security threats.
- It is, in fact, a piece of malware, specifically a scareware that displays fake warnings to fool users into paying for non-existent antivirus solutions.

Trojan horse:

- Users can infect their computers with Trojan horse software simply by downloading an application they thought was legitimate but was in fact malicious.
- Once inside your computer, a Trojan horse can do anything from recording your passwords by logging keystrokes (known as a keystroke logger) to hijacking your webcam to watch and record your every move.

Malicious Spyware:

- Malicious spyware is used to describe the Trojan application that was created by cybercriminals to spy on their victims.
- An example would be key logger software that records a victim's every keystroke on his or her keyboard. The recorded information is periodically sent back to the originating cybercriminal over the Internet.
- Key logging software is widely available and is marketed to parents or businesses that want to monitor their kids' or employees' Internet usage.

Computer Worm:

- A computer worm is a software program that can copy itself from one computer to another, without human interaction.
- Worms can replicate in great volume and with great speed.
- For example, a worm can send copies of itself to every contact in your email address book and then send itself to all the contacts in your contacts' address books.
- Because of their speed of infection, worms often gain notoriety overnight infecting computers across the globe as quickly as victims around the world switch them on and open their email.

Botnet:

- A botnet is a group of computers connected to the Internet that have been compromised by a hacker using a computer virus or Trojan horse.
- An individual computer in the group is known as a "zombie "computer.
- The botnet is under the command of a "bot herder" or a "bot master," usually to perform nefarious activities.
- This could include distributing spam to the email contact addresses on each zombie computer.
- For example, if the botnet is sufficiently big in number, it could be used to access a targeted website simultaneously in what's known as a denial-of-service (DoS) attack.

Spam:

- Spam in the security context is primarily used to describe email spam —unwanted messages in your email inbox.
- Spam, or electronic junk mail, is a nuisance as it can clutter your mailbox as well as potentially take up space on your mail server.
- Unwanted junk mail advertising items you don't care for is harmless, relatively speaking.
- However, spam messages can contain links that when clicked on could go to a website that installs malicious software onto your computer.

Phishing:

- Phishing scams are fraudulent attempts by cybercriminals to obtain private information.
- Phishing scams often appear in the guise of email messages designed to appear as though they are from legitimate sources

- For example, the message would try to lure you into giving your personal information by pretending that your bank or email service provider is updating its website and that you must click on the link in the email to verify your account information and password details.

Spoofing:

- This technique is often used in conjunction with phishing in an attempt to steal your information.
- A website or email address that is created to look like it comes from a legitimate source.
- An email address may even include your own name, or the name of someone you know, making it difficult to discern whether or not the sender is real.
- Sends spam using your email address, or a variation of your email address, to your contact list.
- Recreates websites that closely resemble the authentic site. This could be a financial institution or other site that requires login or other personal information.

Rootkit:

- A rootkit is a collection of tools that are used to obtain administrator-level access to a computer or a network of computers.
- A rootkit could be installed on your computer by a cybercriminal exploiting a vulnerability or security hole in a legitimate application on your PC and may contain spyware that monitors and records keystrokes

Types of Attacks

- An Attack is defined as **"any attempt that made on a network to gain unauthorized access"**.
- This is also called as cyber-attack as the attacker may steal, alter or destroy the information.
- Without security measures and controls in place, one's data might be subjected to an attack.
- Some attacks are passive, meaning information is monitored; others are active, meaning the information is altered with intent to corrupt or destroy the data or the network itself.
- Your networks and data are vulnerable to any of the following types of attacks if you do not have a security plan in place.

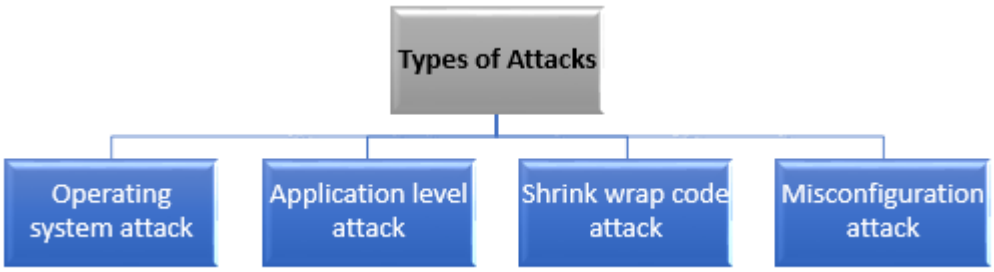


Figure 2: Types of Attacks

Different types of attacks are as follows:

1. Operating system attack
2. Application level attack
3. Shrink wrap code attack
4. Misconfiguration attack

Operating system attack

- In Operating Systems attacks**,** attackers look for vulnerabilities in OS such that they can exploit through vulnerabilities and gain access to the target system or network.
- The vulnerabilities in the OS can be **open ports and services** as most of the operating systems install these services and ports by default.

- These are the most common vulnerabilities found by attackers to gain access to an operating system.
- So, to prevent Operating System Attacks, we need to remove or disable those services and ports which are unnecessary for time being.

Application layer attack

- An application layer attack targets application servers by deliberately causing a fault in a server's operating system or applications.
- This results in the attacker gaining the ability to bypass normal access controls.
- The attacker takes advantage of this situation, gaining control of your application, system, or network, and can do any of the following:
  - Read, add, delete, or modify your data or operating system.
  - Introduce a virus program that uses your computers and software applications to copy viruses throughout your network.
  - Introduce a sniffer program to analyse your network and gain information that can eventually be used to crash or to corrupt your systems and network.
  - Abnormally terminate your data applications or operating systems.
  - Disable other security controls to enable future attacks.

Shrink Wrap code attack

- **Shrink Wrap Code Attacks** are defined as exploiting the default configuration and settings of the libraries and code**.**
- Most of the time, developers use free libraries and licensed code from other sources in their programs to reduce time and cost.
- Due to this importing, **default configuration and settings** of the libraries and code are unchanged which leads to shrink wrap code attacks.
- To prevent these kind of attacks, we have to fine-tune every part of the code and make it more secure.

Misconfiguration attack

- Misconfiguration can be defined as occurrence of errors while implementing all the security controls.
- It may occur either at any stage like developing, deploying, or maintaining, etc.
- Due to this attackers, gain unauthorized access to the systems and affect web servers, databases, etc.
- To prevent these kind of attacks, administrators need to change the default configuration of devices and deploy automated scanners.

Intrusion Detection System

- An intrusion-detection system acquires information about an information system to perform a diagnosis on the security status of the latter.
- The goal is to discover breaches of security, attempted breaches, or open vulnerabilities that could lead to potential breaches.
- A typical intrusion-detection system is shown in Figure.

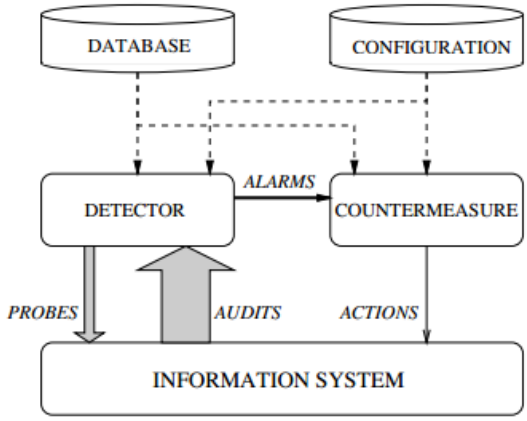


Figure 3: Simple intrusion detection system

- An intrusion-detection system can be described at a very macroscopic level as a detector that processes information coming from the system to be protected.
- This detector can also launch probes to trigger the audit process, such as requesting version numbers for applications.
- It uses three kinds of information: long-term information related to the technique used to detect intrusions (a knowledge base of attacks, for example), configuration information about the current state of the system, and audit information describing the events that are happening on the system.
- The role of the detector is to eliminate unneeded information from the audit trail.
- It then presents either a synthetic view of the security-related actions taken during normal usage of the system, or a synthetic view of the current security state of the system.
- A decision is then taken to evaluate the probability that these actions or this state can be considered as symptoms of an intrusion or vulnerabilities.
- A countermeasure component can then take corrective action to either prevent the actions from being executed or change the state of the system back to a secure state.

Types of Intrusion Detection Systems

- Intrusion Detection System are classified into 5 types:

Network Intrusion Detection System (NIDS):

- Network intrusion detection systems (NIDS) are set up at a planned points within the network to examine traffic from all devices on the network.
- It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks.
- Once an attack is identified or abnormal behaviour is observed, the alert can be sent to the administrator.
- An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.

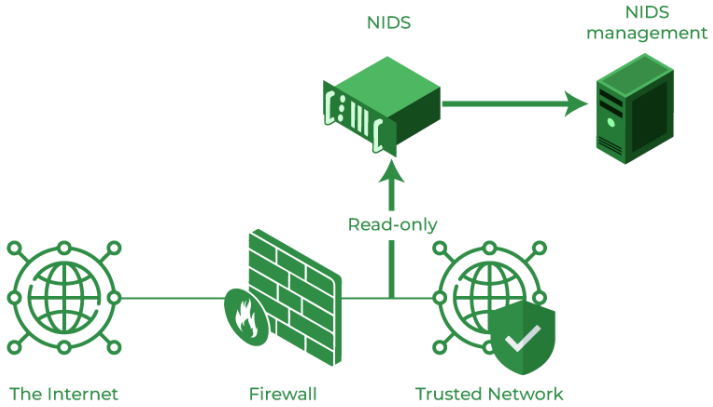


Figure 4: Network Intrusion Detection System

Host Intrusion Detection System (HIDS):

- Host intrusion detection systems (HIDS) run on independent hosts or devices on the network.
- A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected.
- It takes a snapshot of existing system files and compares it with the previous snapshot.
- If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate.
- An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.

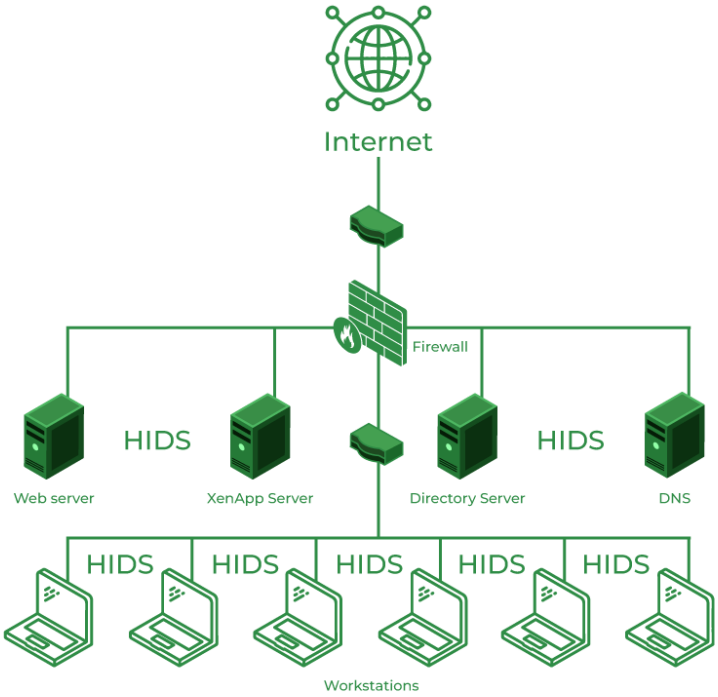


Figure 5: Host Intrusion Detection System

Protocol-based Intrusion Detection System (PIDS):

- Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently reside at the front end of a server, controlling and interpreting the protocol between a user/device and the server.
- It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accepting the related HTTP protocol.
- As HTTPS is unencrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

Application Protocol-based Intrusion Detection System (APIDS):

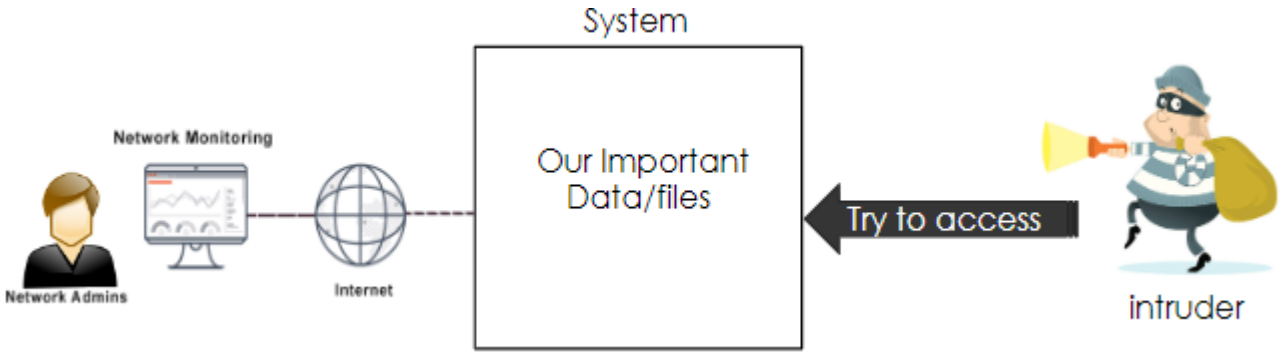
- An application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers.
- It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols.
- For example, this would monitor the SQL protocol explicitly to the middleware as it transacts with the database in the web server.

Hybrid Intrusion Detection System:

- Hybrid intrusion detection system is made by the combination of two or more approaches to the intrusion detection system.
- In the hybrid intrusion detection system, the host agent or system data is combined with network information to develop a complete view of the network system.
- The hybrid intrusion detection system is more effective in comparison to the other intrusion detection system.
- Prelude is an example of Hybrid IDS.

System Integrity Verifiers

- System Integrity Verifiers are some tools that are used to monitor and analyse the systems/networks.
- SIVs finding vulnerable activities in the systems/networks.



- SIVs detects automated scripts if they are present in any folders or files.
- SIVs detects if any files or folders are renamed and resized without administrator permissions.
- SIVs detects intruders when they try to access the systems.
- SIVs see if any normal user is using root/administrator level services in the system.
- SIVs Verifies Signatures of Users.

Indication of Intrusion

- Indications of intrusion or unauthorized access in a computer system or network can vary depending on the type of attack and the specific security controls in place.
- Indications of intrusion categorized into system, file system, and network indicators

System Indications

Unusual Account Activities

- Multiple failed login attempts.
- Irregular login patterns (e.g., logins from different locations in a short time).
- Privilege escalation (e.g., unauthorized elevation of user privileges).
- Unusual file access (e.g., accessing sensitive files without proper authorization).

File System Indications

Unauthorized File Modifications:

- Changes to critical system files or configuration files without authorization.
- Altered file permissions or ownership.

File Integrity Violations:

- Checksum mismatches or unexpected changes in file attributes.
- Suspicious file names or extensions (e.g., executable files with misleading extensions).

Unusual File Access Patterns:

- Abnormal read/write operations on sensitive files.
- Files accessed from unusual locations or by unauthorized users.

Network Indications:

Unusual Network Traffic:

- Sudden spikes in network traffic.
- Large data transfers to suspicious destinations.
- Anomalies in protocol usage or non-standard port activities.

Unexpected Network Connections:

- Connections from internal systems to external hosts, especially suspicious IP addresses.
- Unexplained network connections or activities.

Denial of Service (DoS) Attacks:

- Abnormal patterns consistent with DoS attacks (e.g., high-volume ICMP requests, SYN floods).
- Unexplained network performance degradation or disruptions.

Penetration Testing

- A penetration test, also called a *pen test* or *ethical hacking*, is a cyber-security technique that organizations use to identify, test and highlight vulnerabilities in their security posture.
- These penetration tests are often carried out by ethical hackers.
- These in-house employees or third parties mimic the strategies and actions of an attacker to evaluate the hack ability of an organization's computer systems, network or web applications.
- Organizations can also use pen testing to evaluate their adherence to compliance regulations.
- Pen testing is considered a proactive cyber security measure because it involves consistent, self-initiated improvements based on the reports the test generates.
- This differs from non-proactive approaches, which don't fix weaknesses as they arise
- A non-proactive approach to cyber security, for example, would involve a company updating its firewall after a data breach occurs.
- The goal of proactive measures, such as pen testing, is to minimize the number of retroactive upgrades and maximize an organization's security.

Penetration testing stages

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

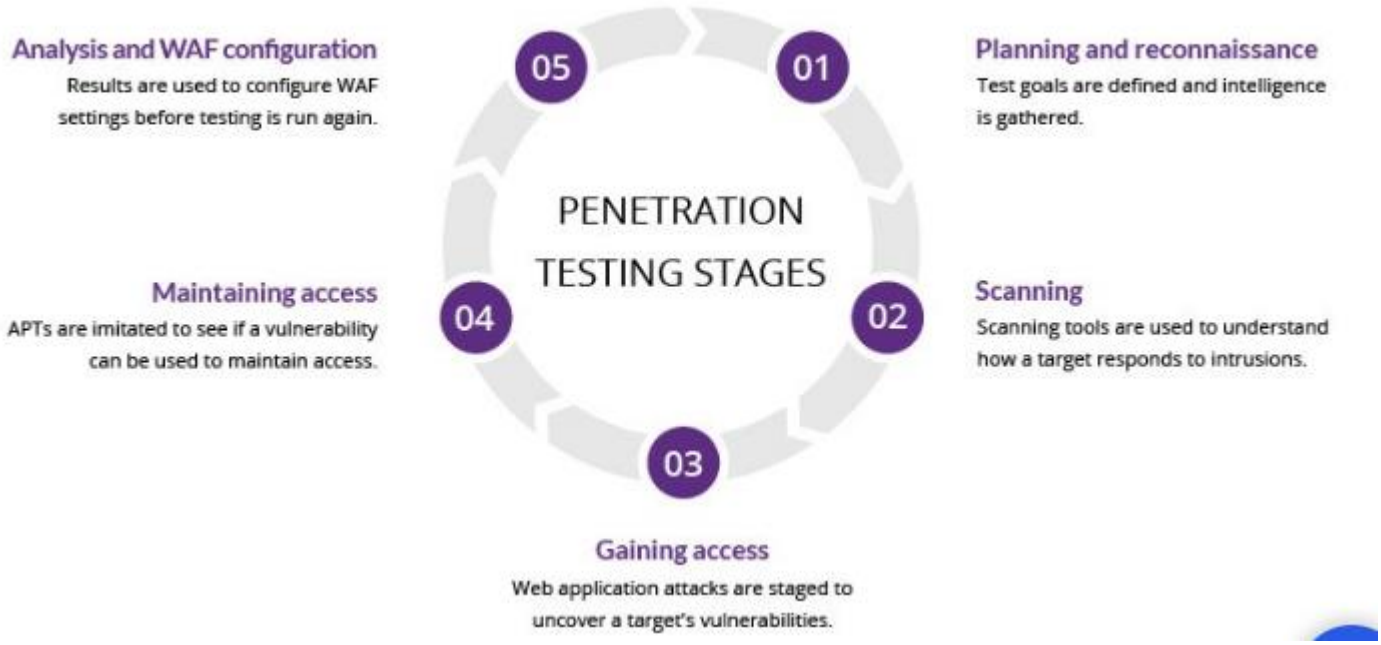


Figure 6: Penetration Testing stages

Planning and reconnaissance

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.

Scanning

the next step is to understand how the target application will respond to various intrusion attempts.

This is typically done using:

- **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.
- **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.

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.

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— long enough for a bad actor to gain in-depth access.
- 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.

Analysis

The results of the penetration test are then compiled into a report detailing:

- Specific vulnerabilities that were exploited
- Sensitive data that was accessed
- The amount of time the pen tester was able to remain in the system undetected

This information is analysed by security personnel to help configure an enterprise's WAF settings and other application security solutions to patch vulnerabilities and protect against future attacks.

Types of Penetration Testing

Black Box Penetration Testing

- In black box penetration testing, tester has no idea about the systems that he is going to test.
- He is interested to gather information about the target network or system.
- For example, in this testing, a tester only knows what should be the expected outcome and he does not know how the outcomes arrive.
- He does not examine any programming codes.

White Box Penetration Testing

- This is a comprehensive testing, as tester has been provided with whole range of information about the systems and/or network such as Schema, Source code, OS details, IP address, etc.
- It is normally considered as a simulation of an attack by an internal source.
- It is also known as structural, glass box, clear box, and open box testing.
- White box penetration testing examines the code coverage and does data flow testing, path testing, loop testing, etc.

Grey Box Testing

- In this type of testing, a tester usually provides partial or limited information about the internal details of the program of a system.
- It can be considered as an attack by an external hacker who had gained illegitimate access to an organization's network infrastructure documents.

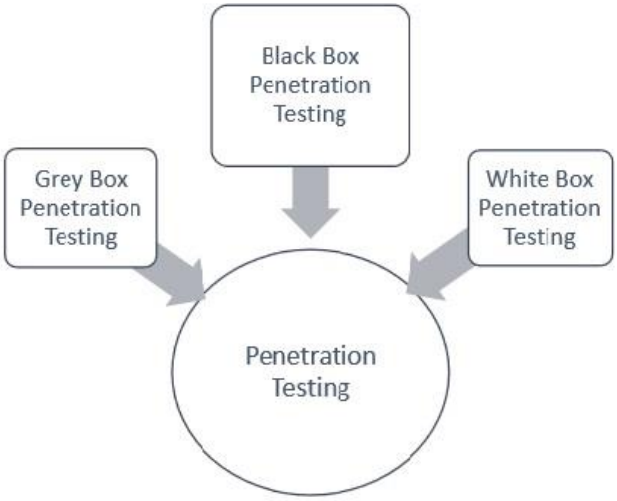


Figure 7: Types of Penetration Testing

APPENDIX

Figure 8: Rouge Security Software