Ethical Hacking – Overview

Hacking has been a part of computing for almost five decades and it is a very broad discipline, which covers a wide range of topics. The first known event of hacking had taken place in 1960 at MIT and at the same time, the term "Hacker" was originated.
Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering into them. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.
Hacking is usually legal as long as it is being done to find weaknesses in a computer or network system for testing purpose. This sort of hacking is what we call **Ethical Hacking**.
A computer expert who does the act of hacking is called a "Hacker". Hackers are those who seek knowledge, to understand how systems operate, how they are designed, and then attempt to play with these systems.

Types of Hacking

We can segregate hacking into different categories, based on what is being hacked. Here is a set of examples:

 Website Hacking: Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.

 Network Hacking: Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.

 Email Hacking: It includes getting unauthorized access on an Email account and using it without taking the consent of its owner.

 Ethical Hacking: Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.

 Password Hacking: This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.

 Computer Hacking: This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

Advantages of Hacking

Hacking is quite useful in the following scenarios:
☐ To recover lost information, especially in case you lost your password.

 To perform penetration testing to strengthen computer and network security.
To put adequate preventative measures in place to prevent security breaches.

To have a computer system that prevents malicious hackers from gaining access.

Disadvantages of Hacking

Hacking is quite dangerous if it is done with harmful intent. It can cause:

 Massive security breach.

 Unauthorized system access on private information.

 Privacy violation.

 Hampering system operation.

 Denial of service attacks

 Malicious attack on the system.

Purpose of Hacking

There could be various positive and negative intentions behind performing hacking activities. Here is a list of some probable reasons why people indulge in hacking activities:

- Just for fun
- Show-off
- Steal important information
- Damaging the system
- Hampering privacy
- Money extortion
- System security testing
- To break policy compliance

While malware is passive software usually sent out over the internet, a **malicious hacker** is someone that is actively working to disable security systems with the intent of either taking down a system or stealing information.

Hackers can be classified into different categories such as white hat, black hat, and grey hat, based on their intent of hacking a system. These different terms come from old Spaghetti Westerns, where the bad guy wears a black cowboy hat and the good guy wears a white hat.

White Hat Hackers

White Hat hackers are also known as **Ethical Hackers**. They never intent to harm a system, rather they try to find out weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments.

Ethical hacking is not illegal and it is one of the demanding jobs available in the IT industry. There are numerous companies that hire ethical hackers for penetration testing and vulnerability assessments.

Black Hat Hackers

Black Hat hackers, also known as **crackers**, are those who hack in order to gain unauthorized access to a system and harm its operations or steal sensitive information.

Black Hat hacking is always illegal because of its bad intent which includes stealing corporate data, violating privacy, damaging the system, blocking network communication, etc.

Grey Hat Hackers

Grey hat hackers are a blend of both black hat and white hat hackers. They act without malicious intent but for their fun, they exploit a security weakness in a computer system or network without the owner's permission or knowledge.

Their intent is to bring the weakness to the attention of the owners and getting appreciation or a little bounty from the owners.

Miscellaneous Hackers

Apart from the above well-known classes of hackers, we have the following categories of hackers based on what they hack and how they do it:

Red Hat Hackers

Red hat hackers are again a blend of both black hat and white hat hackers. They are usually on the level of hacking government agencies, top-secret information hubs, and generally anything that falls under the category of sensitive information.

Blue Hat Hackers

A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch. They look for loopholes that can be exploited and try to close these gaps. Microsoft also uses the term **BlueHat** to represent a series of security briefing events.

Elite Hackers

This is a social status among hackers, which is used to describe the most skilled. Newly discovered exploits will circulate among these hackers.

Script Kiddie

A script kiddie is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept, hence the term **Kiddie**.

Ethical Hacking Process

Like all good projects, ethical hacking too has a set of distinct phases. It helps hackers to make a structured ethical hacking attack.

Different security training manuals explain the process of ethical hacking in different ways, but for me as a Certified Ethical Hacker, the entire process can be categorized into the following six phases.

Reconnaissance

Reconnaissance is the phase where the attacker gathers information about a target using active or passive means. The tools that are widely used in this process are NMAP, Hping, Maltego, and Google Dorks.

Scanning

In this process, the attacker begins to actively probe a target machine or network for vulnerabilities that can be exploited. The tools used in this process are Nessus, Nexpose, and NMAP.

Gaining Access

In this process, the vulnerability is located and you attempt to exploit it in order to enter into the system. The primary tool that is used in this process is Metasploit.

Maintaining Access

It is the process where the hacker has already gained access into a system. After gaining access, the hacker installs some backdoors in order to enter into the system when he needs access in this owned system in future. Metasploit is the preferred tool in this process.

Clearing Tracks

This process is actually an unethical activity. It has to do with the deletion of logs of all the activities that take place during the hacking process.

Reporting

Reporting is the last step of finishing the ethical hacking process. Here the Ethical Hacker compiles a report with his findings and the job that was done such as the tools used, the success rate, vulnerabilities found, and the exploit processes.

Footprinting is a part of reconnaissance process which is used for gathering possible information about a target computer system or network. Footprinting could be both **passive** and **active**. Reviewing a company's website is an example of passive footprinting, whereas attempting to gain access to sensitive information through social engineering is an example of active information gathering.

Footprinting is basically the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.

During this phase, a hacker can collect the following information −

- Domain name
- IP Addresses
- Namespaces
- Employee information
- Phone numbers
- E-mails
- Job Information

In the following section, we will discuss how to extract the basic and easily accessible information about any computer system or network that is linked to the Internet.

Domain Name Information

You can use http://www.whois.com/whois website to get detailed information about a domain name information including its owner, its registrar, date of registration, expiry, name server, owner's contact information, etc.

Here is a sample record of www.tutorialspoint.com extracted from WHOIS Lookup −

Finding IP Address

You can use **ping** command at your prompt. This command is available on Windows as well as on Linux OS. Following is the example to find out the IP address of tutorialspoint.com

```
$ping tutorialspoint.com
```

It will produce the following result −

```
PING tutorialspoint.com (66.135.33.172) 56(84) bytes of data.
64 bytes from 66.135.33.172: icmp_seq = 1 ttl = 64 time = 0.028 ms
64 bytes from 66.135.33.172: icmp_seq = 2 ttl = 64 time = 0.021 ms
64 bytes from 66.135.33.172: icmp_seq = 3 ttl = 64 time = 0.021 ms
64 bytes from 66.135.33.172: icmp_seq = 4 ttl = 64 time = 0.021 ms
```

Finding Hosting Company

Once you have the website address, you can get further detail by using ip2location.com website. Following is the example to find out the details of an IP address −

	Field Name	Value
	IP Address	49.205.122.168
☑	Country	India
☐	Region & City	Kukatpalli, Telangana
☐	Latitude & Longitude	17.48333, 78.41667
☐	ZIP Code	508126
☐	ISP	Beam Telecom Pvt Ltd
☐	Domain	beamtele.com
☐	Time Zone	+05:30

Here the ISP row gives you the detail about the hosting company because IP addresses are usually provided by hosting companies only.

IP Address Ranges

Small sites may have a single IP address associated with them, but larger websites usually have multiple IP addresses serving different domains and sub-domains.

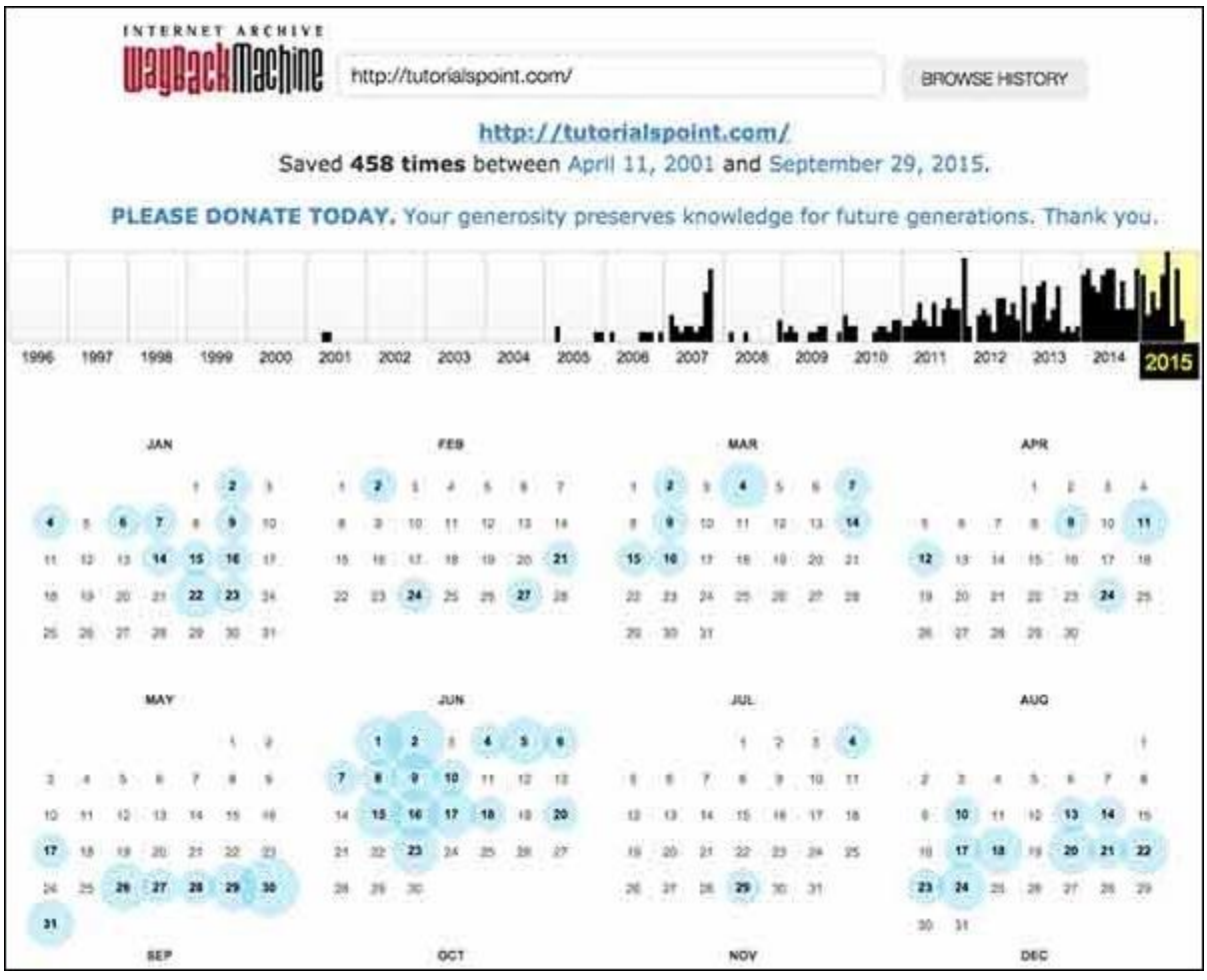
You can obtain a range of IP addresses assigned to a particular company using American Registry for Internet Numbers (ARIN).

You can enter company name in the highlighted search box to find out a list of all the assigned IP addresses to that company.

History of the Website

It is very easy to get a complete history of any website using www.archive.org.

You can enter a domain name in the search box to find out how the website was looking at a given point of time and what were the pages available on the website on different dates.



Footprint and Scanning Tools:

Several tools are used to gather information such as –

- Crawling – Surf the internet to gain information
- Whois – lookup of website to get information like email, registration etc.
- Search engines – Google, Bing and other search sites to get data
- Traceroute – Used to trace a path between user and the target system on the networks.
- Netcraft – tool to gather information about web servers in both server and client side.
- Nslookup – Querying DNS server to extract information

- The Harvester – Used to catalogue email and subdomains.

Scanning tools such as –

- Nmap – Used for scanning and used to find open ports of target.
- Nessus – To find vulnerabilities in the ports.
- Nexpose – Similar to nessus

Network scanning:

Scanning is the second stage of information gathering where the hacker tries to do a deep search into the system to look for valuable information. Ethical hackers tries to prevent organization's attack use this network scanning effectively. The tools and techniques used for scanning are –

- Crafted packets
- TCP flags
- UDP scans
- Ping sweeps

The hackers trie to identify a live system using a protocol, blueprint the same network and perform vulnerability scan to find weaknesses in the system. There are three types of scanning –

- Port scanning – Used to find open ports
- Network scanning – Used to find IP address
- Vulnerability scanning – find weakness or vulnerabilities

Gaining Access:

Here the hacker uses different techniques and tools to gain maximum data from the system. They are –

- Password cracking – Methods like Bruteforce, dictionary attack, rule-based attack, rainbow table are used. Bruteforce is trying all combinations of the password. Dictionary attack is trying a list of meaningful words until the password matches. Rainbow table takes the hash value of the password and compares with pre-computed hash values until a match is discovered.
- Password attacks – Passive attacks such as wire sniffing, replay attack. Active online attack such as Trojans, keyloggers, hash injection, phishing. Offline attacks such as pre-computed hash, distributed network and rainbow. Non electronic attack such as shoulder surfing, social engineering and dumpster diving.

What is Enumeration?

Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system or network. In the enumeration phase, the attacker creates active connections with system and performs directed queries to gain more information about the target. The attackers use the information collected by means of enumeration to identify the **vulnerabilities** or weak points in the system security, which helps them exploit the target system. It allows the attacker to perform **password attacks** to gain unauthorized access to information system resources. Enumeration techniques work in an intranet environment.

Enumeration allows you to collect the following information:

- *Network resources*
- *SNMP and FQDN details*
- *Network shares*
- *Machine names*
- *Routing tables*
- *Users and groups*
- *Audit and service settings*
- *Applications and banners*

During enumeration, attackers may stumble upon a remote IPC share, such as IPC$ in Windows, which they can probe further for null sessions to collect information about other shares and system accounts.

The previous modules highlighted how attackers gather necessary **information** about a target without really getting on the wrong side of the legal barrier. However, enumeration activities may be illegal depending on the organization policies and any laws that are in effect. As an ethical or pentester, you should always acquire proper authorization before performing enumeration.

Related Product : Certified Ethical Hacker | CEH Certification

Techniques for Enumeration

To extract information about a target :

• Extract user names using email IDs

Every email address contains two parts: the user name and the domain name. The structure of an email address is username@domainname. Consider abc@gmail.corn; in this email address, the “abc” (the string of characters preceding the ‘@’ symbol) is the user name and “gmail.com” (the string of characters following the ‘@’ symbol) is the domain name.

• Extract information using default passwords

Many online resources provide a list of default passwords assigned by manufacturers to their products. Users often neglect to change the default usernames and passwords provided by the manufacturer or developer of a product. This eases the task of an attacker in enumerating and exploiting the target system.

• Brute force Active Directory

Microsoft Active Directory is susceptible to a username enumeration at the time of user-supplied input verification. This is a design error in the Microsoft Active Directory implementation. If a user enables the “logon hours” feature, then all the attempts at service authentication result in different error messages. Attackers take advantage of this to enumerate valid user names. An attacker who succeeds in extracting valid user names can conduct a brute-force **attack** to crack the respective passwords.

• Extract information using DNS Zone Transfer

A network administrator can use DNS Zone Transfer to replicate Domain Name System (DNS) data across a number of **DNS servers**, or to back up DNS files. The administrator needs to execute a specific zone transfer request to the name server. If the name server permits zone transfer, it will convert all the DNS names and IP addresses, hosted by that server to ASCII text.

If the network administrators did not configure the DNS server properly, the DNS Zone transfer

is an effective method to obtain information about the organization's network. This information may include lists of all named hosts, sub-zones, and related IP addresses. A user can perform DNS zone transfer using nslookup.

• Extract user groups from Windows

To extract user groups from Windows, the attacker should have a registered ID as a user in the Active Directory. The attacker can then extract information from groups in which the user is a member by using the Windows interface or command line method.

• Extract user names using SNMP

Attack-s can easily guess the read-only or read-write community strings using the SNMP AD to extract user names.

Also Read : What is SNMP Enumeration?

What is NetBIOS?

NetBIOS stands for **Net**work **B**asic **I**nput **O**utput **S**ystem. IBM developed it along with Sytek. The primary intention of NetBIOS was developed as Application Programming Interface (API) to enable access to **LAN** resources by the client's software.

NetBIOS naming convention starts with 16-ASCII character string used to identify the network devices over TCP/IP; 15-characters are used for the device name, and the 16th character is reserved for the service or name record type.

What is SNMP?

SNMP stands for **S**imple **N**etwork **M**anagement **P**rotocol is an application-layer protocol that runs on **U**ser **D**atagram **P**rotocol **(UDP)**. It is used for managing network devices which run on IP layer like routers. SNMP is based on a client-server architecture where SNMP client or agent is located on every network device and communicates with the SNMP managing station via requests and responses. Both SNMP request and responses are configurable variables accessible by the agent software. SNMP contains two passwords for authenticating the agents before configuring the variables and for accessing the SNMP agent from the management station.

SNMP Passwords are:

1. Read Community string are public, and the configuration of the device can be viewed with this password
2. Read/Write community string is private, and the configuration of the device can be modified using this password.

SNMP uses a virtual hierarchical database internally for managing the network objects, and it is called **M**anagement **I**nformation **B**ase (**MIB**). MIB contains a tree-like structure, and object ID uniquely represents each network object. The network objects can be viewed or modified based on the SNMP passwords.

SNMP Enumeration:

Default SNMP password allow attackers to view or modify the SMMP configuration settings. Attackers can enumerate SNMP on remote network devices for the following:

1. Information about network resources such as routers, shares, devices, etc.
2. ARP and routing tables
3. Device-specific information
4. Traffic statistics etc.

SNMP Enumeration Tools:

1. OpUtils
2. SolarWinds

What is LDAP?

LDAP Stands for **L**ight **W**eight **D**irectory **A**ccess **P**rotocol and it is an Internet protocol for accessing distributed directory services like Active Directory or OpenLDAP etc. A directory service is a hierarchical and logical structure for storing records of users. LDAP is based on client and server architecture. LDAP transmits over TCP and information is transmitted between client and server using Basic Encoding Rules (BER).

LDAP Enumeration:

LDAP supports anonymous remote query on the Server. The query will disclose sensitive information such as usernames, address, contact details, Department details, etc.

LDAP Enumeration Tools:

1. Softerra LDAP Administrator
2. Jxplorer

What is NTP?

NTP stands for Network Time protocol designed to synchronize clocks of networked computers. NTP can achieve accuracies of 200 milliseconds or better in local area networks under ideal conditions. NTP can maintain time to within ten milliseconds (1/100 second) over the Internet. NTP is based on agent-server architecture where agent queries the NTP server, and it works on User Datagram Protocol (UDP) and well-known port 123.

NTP Enumeration:

An attacker can enumerate the following information by querying NTP server.

1. List of hosts connected to the NTP server
2. Internal Client IP addresses, Hostnames and Operating system used.

NTP Enumeration Tools:

1. Ntptrace
2. Ntpdc

What is SMTP?

SMTP stands for **S**imple **M**ail **T**ransfer **P**rotocol and it is designed for electronic mail (E-Mail) transmissions. SMTP is based on client-server architecture and works on Transmission Control Protocol (TCP) on well-known port number 25. SMTP uses Mail Exchange (MX) servers to send the mail to via the Domain Name Service, however, should an MX server not detected; SMTP will revert and try an A or alternatively SRV records.

SMTP Enumeration:

SMTP provides three built-in commands

- **VRFY**– validate users on the SMTP servers
- **EXPN**– Delivery addresses of aliases and mailing lists
- **RCPT TO**– Defines the recipients of the message

SMTP servers respond differently to the commands mentioned above, and SMTP enumeration is possible due to varied responses. Attackers can determine the valid users on the SMTP servers with the same technique.

SMTP Enumeration Tools:

1. NetScan Tools Pro
2. SMTP User Enum

What is DNS?

DNS stands for **D**omain **N**ame **S**ervice, and it is primarily designed as hierarchical decentralized distributed naming systems for computers, services, or any resource connected to the network. DNS resolves hostnames to its respective IP addresses and vice versa. DNS internally maintains a database for storing the records. The following are the most commonly used record types in DNS.

- Start of Authority (SOA),
- IP addresses (A and AAAA),
- SMTP mail exchangers (MX),
- Nameservers (NS),
- Pointers for reverse DNS lookups (PTR), and
- Domain name aliases (CNAME)

DNS works on both UDP and TCP on well-known port number 53. It uses UDP for resolving queries and TCP for zone transfers. DNS zone transfer allows DNS databases to replicate the portion of the database from the primary server to the secondary server. DNS zone transfer must only be allowed by other validated secondary DNS servers acting as clients.

DNS Enumeration:

DNS enumeration is possible by sending zone transfer request to the DNS primary server pretending to be a client. It reveals sensitive domain records in response to the request.

DNS Enumeration Tools:

1. Nslookup
2. DNS Dumpster
3. DNS Recon

The most common technique used to search users names and machine name of the target system which hacker do most to find victims. **Infosavvy gives training** on C**ertified Ethical Hacking** in which covers one module on **Enumeration**. Do **CEHv10 Training and Certification from Infosavvy** in **Banglore Location.**

What is System Hacking?

System hacking is defined as the compromise between computer systems and software to access the target computer and steal or misuse their sensitive information. The malware and the attacker identify and exploit the vulnerability of the computer system to gain unauthorized access.

Hacking Linux system

Linux is an operating system based on Unix OS created by Linus Torvalds. It is assembled over the model of open-source software development and distribution.

Hackers use varied techniques to hack into Linux systems:

- Hacking Linux using the SHADOW file.
- Another technique used is bypassing the user password option in Linux.
- Other technique includes detecting the bug on Linux distribution and taking advantage of the same.

Hacking Mac OS

For hackers, hacking a Mac OS is as normal as hacking any other operating system. Various ways that hackers adopt to hack into Mac OS are:

- One Python command to bypass anti-virus
- One Ruby command to bypass anti-virus
- One Tclsh command to bypass
- Use recovery mode to extract and brute-force the hash
- Use single-user mode to configure a backdoor
- Connect to backdoors from anywhere.

Hacking Android phone

Android system hacking is done in the following ways:

- Install malware or a Trojan in the victim's phone and control it remotely via your own device.
- Creating a shell terminal with admin access in the victim's phone.
- Using Spynote can also be one of the modes of android hacking.
- METASPLOIT and MSFVENOM
- Using ADB (Android Debug Bridge)
- Spy apps

Hacking Windows

Out of the several tried techniques of hacking Windows systems, the one that is usually preferred by hackers is Social Engineering. Once the hacker finds a Windows computer open, he can easily modify the existing password and give a new one thereby taking control of the same, without the owner being aware.

Ethical hacking vs Penetration testing:

cal Hacking	Penetration testing
king the system in an ethical way to over vulnerabilities of the system.	Formal procedure to discover security vulnerabilities, flaws and risks.
ducted to identify flaws and prevent real e hacking.	Conducted to strengthen their corporate defense systems.

Phases of System Hacking

There are five phases in penetration testing. It includes –

- **Reconnaissance** – Majorly used to gather data
- **Scanning** – Used to gather further intelligence on the data
- **Gaining access** – Takes control of one or more network devices to extract data.
- **Maintaining access** – Gains more data from the targeted environment
- **Covering tracks** – Remove traces of detecting the attack.

There are various concepts of hacking such as the phase of pen-testing, footprinting, scanning, enumeration, system hacking, sniffing traffic, and so on.

Trojans

Trojans are malicious files which are used by the attacker to create a backdoor without the knowledge of the user. It usually deletes or replaces operating system critical files, steal data, send notifications to remote attacker, and remotely control the target. Trojans

usually hide behind a genuine code or program or file to avoid getting noted by the user. Behind the original program, it establishes a backdoor connection with the remote attacker. It has 3 parts

1. **Dropper:** This is the code which installs malicious code into the target.
2. **Malicious code:** This is the code which exploits the system and gives the attacker control over the target.
3. **Wrapper:** Wrapper wraps dropper, malicious code, genuine code into one exe package.

When victims try to download an infected file, dropper installs the malicious code first and then the genuine program.

Purpose of Trojans

- Steal information such as passwords, security codes, credit card information using keyloggers
- Use victim´s PC as a botnet to perform DDoS attacks
- Delete or replace OS critical files
- Generate fake traffic to create DoS
- Download spyware, adware and malware
- Record screenshots, audio and video of victim´s PC
- Disable fw and av
- Infect victim´s PC as a proxy server for relaying attacks
- Use victim´s PC as a botnet to perform DoS, spamming and blasting email messages

There are various types of Trojans like

- Hypervisior Trojan
- HTTP/HTTPS Trojan
- Remote access Trojan
- FTP Trojans
- VNC Trojans
- Banking Trojans
- DOM based Trojan
- Destructive Trojan
- Botnet Trojan
- Proxy Trojan
- Data hiding Trojan

Countermeasures:

- Avoid opening emails from unknown users
- Do not download free software's from untrusted sites
- Always upgrade and keep firewalls, IDS and anti-virus updated with latest patches and signatures
- Block all unnecessary ports
- Periodically check startup programs and processes running to find any malicious files running.

What is penetration testing

A penetration test, also known as a pen test, is a simulated cyber attack against your computer system to check for exploitable vulnerabilities. In the context of web application security, penetration testing is commonly used to augment a web application firewall (WAF).

Pen testing can involve the attempted breaching of any number of application systems, (e.g., application protocol interfaces (APIs), frontend/backend servers) to uncover vulnerabilities, such as unsanitized inputs that are susceptible to code injection attacks.

Insights provided by the penetration test can be used to fine-tune your WAF security policies and patch detected vulnerabilities.

Penetration testing stages

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

1. 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.

2. 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.

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.

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— 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.

5. 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 analyzed by security personnel to help configure an enterprise's WAF settings and other application security solutions to patch vulnerabilities and protect against future attacks.

Black Box Penetration Test

A **black box security audit** is carried out in the closest conditions to an external attack performed by a remote unknown attacker. This mean that no (or almost no) information is provided to the pentesters before starting the tests.
The black box expression refers to the analysis of the system/the target, which is conducted without knowing its internal working.
Pentesters only know the name of the target organisation and often an IP address or a URL. The attack surface is therefore broad. Time is first spent exploring the various elements included in the target, before prioritising the attacks according to the elements discovered during this recon phase.
Black box penetration testing enables a freedom of choice of targets (when the target includes several assets) in order to maximise the impact of discovered vulnerabilities, as in the case of a real malicious attack. This audit requires very little preparation from you as a contractor.
One of the advantages of this approach is that pentesters bring a fresh look at the target and thus a new assessment of potential entry points from an attacker's point of view. This avoids, for example, focusing tests only on what is perceived as important to secure, while the risks of other elements may be underestimated.

It is possible to conduct a **black box pentest** without notifying the teams in charge of detecting attacks, in order to see the company's ability to detect an attack and react appropriately.

White Box Penetration Test

Contrary to the black box, a **white box** (sometimes crystal box) **security audit** means that the maximum amount of information is shared with the pentesters before the audit. The information necessary for the audit is provided in complete transparency. The working of the target is then known and made visible, hence the term white box.
The information can be architecture documents, administrator access to servers, access to source code…

The **white box security audit** is not a pentest in itself, since auditors do not place themselves from the point of view of an attacker. It is a more thorough security analysis than a penetration test, providing a better understanding of where security problems originate. It also uncovers vulnerabilities that are not visible during a pentest, but which may cause a security risk even so.