Module 1

Introduction to Ethical Hacking

Hacking -: Hacking is the practice of modifying the features of a system, in order to accomplish a goal outside of the creator's original purpose. The person who is consistently engaging in hacking activities, and has accepted hacking as a lifestyle and philosophy of their choice, is called a **hacker**.

Computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator's original purpose.

Ethical Hacking- -: Ethical hacking and ethical hacker are terms used to describe hacking performed by a company or individual to help identify potential threats on a computer or network.

An ethical hacker attempts to bypass system security and search for any weak points that could be exploited by malicious hackers. This information is then used by the organization to improve the system security, in an effort to minimize or eliminate any potential attacks.

Ethical Hacking goals

- To determine flaws and Vulnerabilities.
- To provide quantitative metrics for evaluating systems and networks.
- To determine risk to the organization.
- To design mitigating controls.

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

History of Hacking

1970's: Phone Hacker (Phreaks) break to make free call (Blue Box).

1980's: Phone phreaks begin to move into the realm of computer hacking.

Late 1980's: Morris Internet Worm-DOS.

2000's: DNS Spoofing

Important terminologies related to hacking

1. **Hack Value** –It is a notion among hackers that something doing is interesting or worthwhile.

- 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

History of Hacking

1970's: Phone Hacker (Phreaks) break to make free call (Blue Box).

1980's: Phone phreaks begin to move into the realm of computer hacking.

Late 1980's: Morris Internet Worm-DOS.

2000's: DNS Spoofing

Important terminologies related to hacking

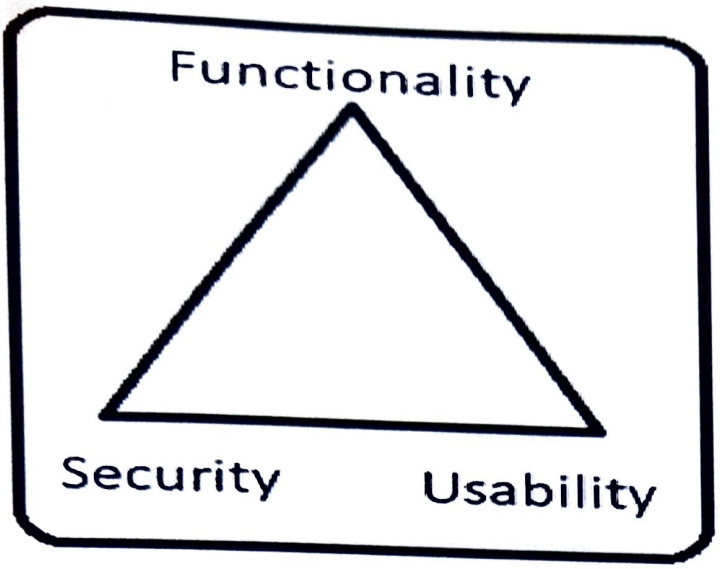
1. **Hack Value** –It is a notion among hackers that something doing is interesting or worthwhile.
2. **Exploit** - Exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to compromise the security of a computer or network system.
3. **Vulnerability**-A vulnerability is a weakness which allows a hacker to compromise the security of a computer or network system.

4. **Target of evaluation-** An IT system product or network that is subject to security analysis or attacks.
5. **Zero day attack** - A zero-day (also known as 0-day) vulnerability is a computer-software vulnerability that is unknown to those who would be interested in mitigating the vulnerability (including the vendor of the target software).
6. **Daisy chaining** -Hackers who get away with database theft usually complete their task, then backtrack to cover their tracks by destroying logs etc. It is like a thief who steals some valuable thing and destroys all the signs of his tracks.

Some more terms

Threat	*Activity or occurrence that is capable of causing potential damage to the information system or networks*
Vulnerability	***Weak point or a loophole which turns out to be an entry point for a threat to enter and exploit the system***
Risk	***Probability of a possible threat becoming successful***
Attack	***The very result of a threat which has materialized***
Exploit	***Using the vulnerability of a system or a network so that it may be attacked***

The security, funcunality and usability triangale



There is an inter dependency between these three attributes. When security goes up, usability and functionality come down. Any organization should balance between these three qualities to arrive at a balanced information system.

Hacker Classes-

Script Kiddies -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**.

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.

Cyber terrorist

- Organized Groups intent on spreading fear of data disruption as means of meet their Goals
- Could be for religious, political, nationalistic or activist goals.

State sponsored hackers

- Trained, funded and supported agents of nation-state or government
- Goals are espionage, cyber warfare.

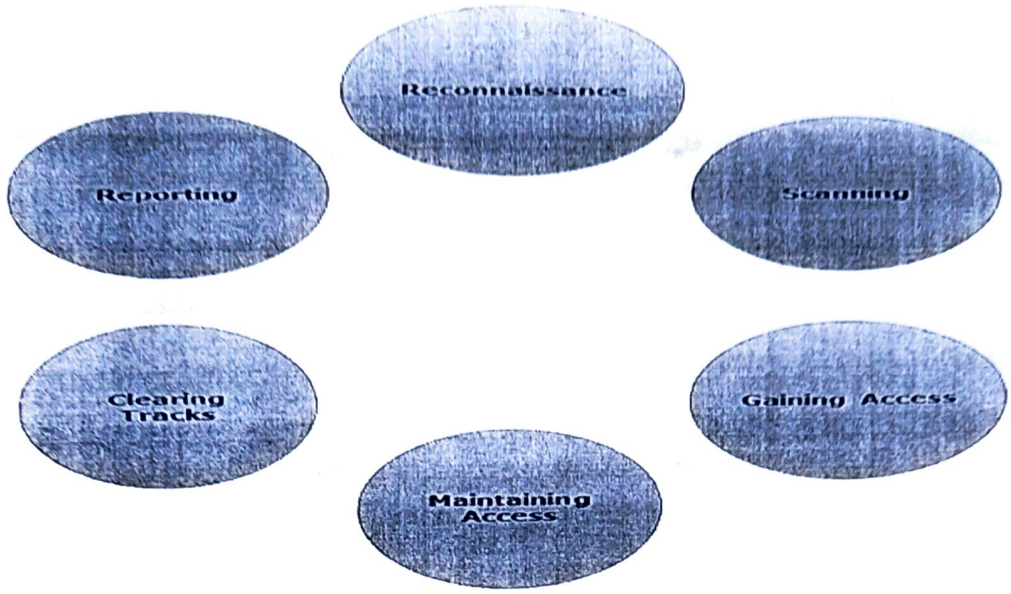
Hacktivists

- Hackers who launch attacks to spread their particular message about a Cause.
- May deface website, cause denial of service attacks, disclose data.

Corporate hackers-

- Target an organizations property data or intellectual properties.
- Goal is to get a competitive advantage, blackmail, or make money.

Hacking methodology



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.

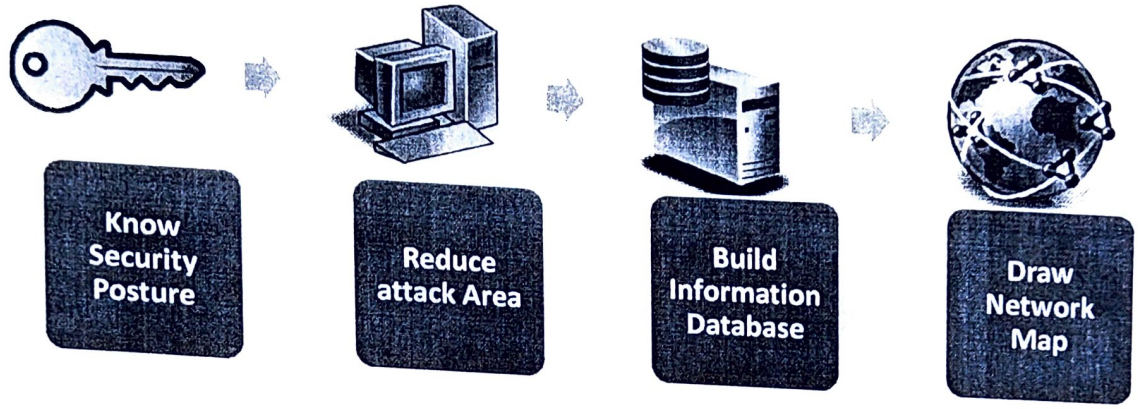
Clearing Tracks

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.

Foot printing

- Foot printing, the first step in ethical hacking, refers to the process of collecting information about a target network and its environment. Using foot printing you can find various ways to intrude into the target organization's network system. It is considered "methodological" because critical information is sought based on a previous discovery.

Why foot printing



Foot printing objectives

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

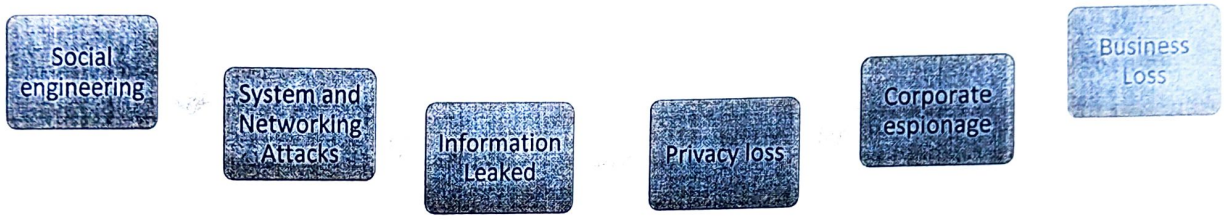
Foot printing is basically the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.

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

- Domain name
- IP Addresses

- Namespaces
- Employee information
- Phone numbers
- E-mails
- Job Information

Footprinting thearts



Reconnaissance

Information Gathering and getting to know the target systems is the first process in ethical hacking. Reconnaissance is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system.

During reconnaissance, an ethical hacker attempts to gather as much information about a target system as possible, following the seven steps listed below –

- Gather initial information
- Determine the network range
- Identify active machines
- Discover open ports and access points
- Fingerprint the operating system
- Uncover services on ports
- Map the network

We will discuss in detail all these steps in the subsequent chapters of this tutorial. Reconnaissance takes place in two parts – **Active Reconnaissance** and **Passive Reconnaissance**.

Active Reconnaissance

In this process, you will directly interact with the computer system to gain information. This information can be relevant and accurate. But there is a risk of getting detected if you are planning active reconnaissance without permission. If you are detected, then system admin can take severe action against you and trail your subsequent activities.

Passive Reconnaissance

In this process, you will not be directly connected to a computer system. This process is used to gather essential information without ever interacting with the target systems.

Scanning

Scanning is a set of procedures for identifying live hosts, ports, and services, discovering Operating system and architecture of target system. Identifying vulnerabilities and threats in the network. Network scanning is used to create a profile of the target organization.

Scanning refers to collecting more information using complex and aggressive reconnaissance techniques.

Network Scanning:

The purpose of each scanning process is given below:

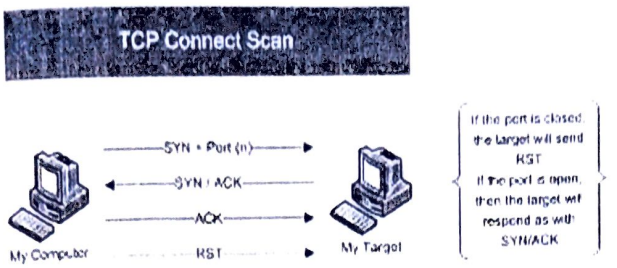
- **Port Scanning** – detecting open ports and services running on the target.
- **Network Scanning** – IP addresses, Operating system details, Topology details, trusted routers information etc
- **Vulnerability scanning** – scanning for known vulnerabilities or weakness in a system

Scanning Methodology

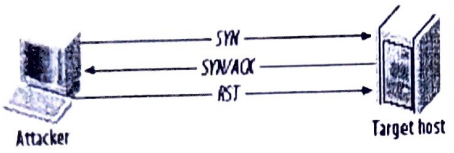
- **Check for Live Systems:** Ping scan checks for the live system by sending ICMP echo request packets. If a system is alive, the system responds with ICMP echo reply packet containing details of TTL, packet size etc.
- **Check for Open Ports:** Port scanning helps us to find out open ports, services running on them, their versions etc. Nmap is the powerful tool used mainly for this purpose.

We have various types of scan:

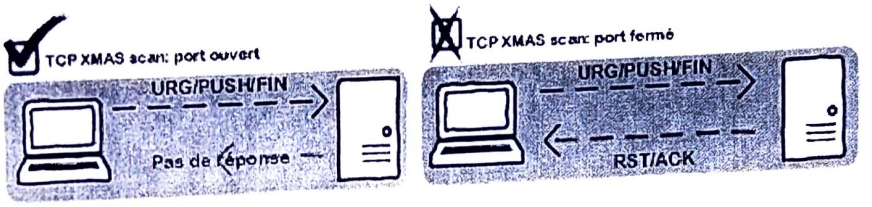
Connect scan: Identifies open ports by establishing a TCP handshake with the target.



Half-open scan otherwise known as Stealth scan used to scan the target in a stealthy way by not completing the TCP handshake by abruptly resetting the communication.

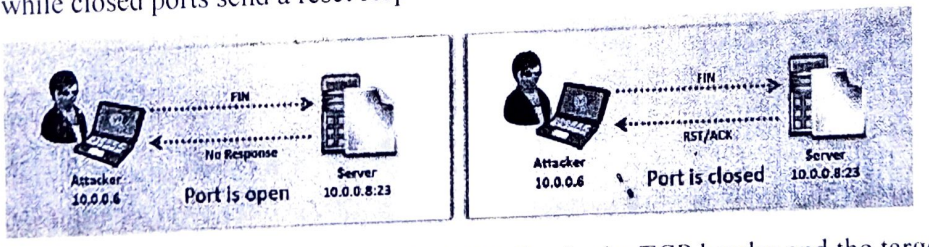


XMAS scan: This is also called as inverse TCP scanning. This works by sending packets set with PSH, URG, FIN flags. The targets do not respond if the ports are open and send a reset response if ports are closed.



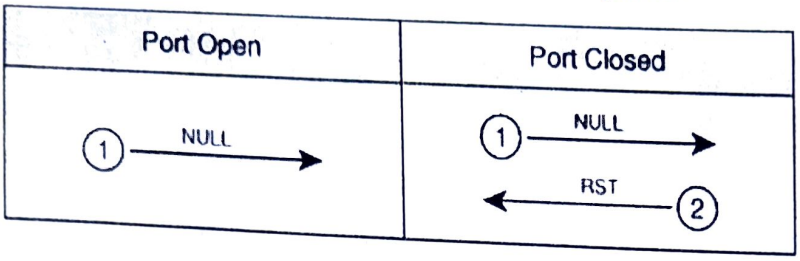
Source: https://www.information-security.fr

FIN scan: Fin flag is set in the TCP packets sent to the target. open ports doe does not respond while closed ports send a reset response.



ACK scan: Here the attacker sets the ACK flag in the TCP header and the target's port status is gathered based on window size and TTL value of RESET packets received from the target.

Null Scan: Works by sending TCP packets with no flags set to the target. Open ports do not respond while closed ports respond with a RESET packet.



TCP Scan	Flags	Host Response	Result
Full scan	SYN (and ACK)	SYN & ACK	Host is alive
SYN (Half open) scan	SYN	SYN&ACK	Host is alive
XMAS scan	FIN,URG, PSH	RST	Port is closed
ACK scan	ACK	No response or RST	Port is filtered or port is not filtered
SYN/FIN (Fragmented) scan	SYN, FIN	No response or RST	Port is filtered or port is not filtered
Inverse TCP Flag scan	FIN, URG, PSH (or NULL)	No response or RST/ACK	Port is open or port is not open

UDP scan-

Enumeration and its Types

Enumeration is defined as the process of extracting user names, machine names, network resources, shares and services from a system. In this phase, the attacker creates an active connection to the system and performs directed queries to gain more information about the target. The gathered information is used to identify the vulnerabilities or weak points in system security and tries to exploit in the System gaining phase.

Types of information enumerated by intruders:

- Network Resource and shares
- Users and Groups
- Routing tables
- Auditing and Service settings
- Machine names
- Applications and banners
- SNMP and DNS details

Techniques for Enumeration

- Extracting user names using email ID's
- Extract information using the default password
- Brute Force Active Directory
- Extract user names using SNMP
- Extract user groups from Windows
- Extract information using DNS Zone transfer

Services and Port to Enumerate

- TCP 53: DNS Zone transfer
- TCP 135: Microsoft RPC Endpoint Mapper
- TCP 137: NetBIOS Name Service
- TCP 139: NetBIOS session Service (SMB over NetBIOS)
- TCP 445: SMB over TCP (Direct Host)
- UDP 161: SNMP
- TCP/UDP 389: LDAP
- TCP/UDP 3368: Global Catalog Service

- TCP 25: Simple Mail Transfer Protocol (SMTP)

NetBIOS Enumeration

NetBIOS stands for Network Basic Input Output System. It Allows computer communication over a LAN and allows them to share files and printers.

NetBIOS names are used to identify network devices over TCP/IP (Windows). It must be unique on a network, limited to 16 characters where 15 characters are used for the device name and the 16th character is reserved for identifying the type of service running or name record type.

Attackers use the NetBIOS enumeration to obtain:

- List of computers that belong to a domain
- List of shares on the individual hosts on the network
- Policies and passwords

Commands and tools used:

Nbtstat: utility used to find protocol statistics, NetBIOS name table and name cache details

Superscan: GUI tool used to enumerate windows machine

Net view: command line tool to identify shared resources on a network

SNMP Enumeration

SNMP (Simple Network Management Protocol) is an application layer protocol which uses UDP protocol to maintain and manage routers, hubs and switches other network devices on an IP network. SNMP is a very common protocol found enabled on a variety of operating systems like Windows Server, Linux & UNIX servers as well as network devices like routers, switches etc.

SNMP enumeration is used to enumerate user accounts, passwords, groups, system names, devices on a target system.

It consists of three major components:

1. **Managed Device:** A managed device is a device or a host (technically known as a node) which has the SNMP service enabled. These devices could be routers, switches, hubs, bridges, computers etc.
2. **Agent:** An agent can be thought of as a piece of software that runs on a managed device. Its primary job is to convert the information into SNMP compatible format for the smooth management of the network using SNMP protocol.
3. **Network Management System (NMS):** These are the software systems that are used for monitoring of the network devices.

SMTP Enumeration

The Simple Mail Transport Protocol is used to send email messages as opposed to POP3 or IMAP which can be used to both send and receive messages. SMTP relies on using Mail Exchange (MX) servers to direct the mail to via the Domain Name Service, however, should an MX server not be detected, SMTP will revert and try an A or alternatively SRV records. SMTP generally runs on port 25.

SMTP enumeration allows us to determine valid users on the SMTP server. This is done with the help built-in SMTP commands, they are

- VRFY - This command is used for validating users.
- EXPN - This command tells the actual delivery address of aliases and mailing lists.
- RCPT TO - It defines the recipients of the message.

Tool:

NestScanTools Pro

Countermeasures:

- Configure SMTP server either to ignore email messages to unknown recipients.
- Don't include information like mail relay systems being used, Internal IP address or host information.
- Disable open relay feature.

NTP Enumeration

The Network Time Protocol is a protocol for synchronizing time across your network. this is especially important when utilizing Directory Services. There exists a number of time servers throughout the world that can be used to keep systems synced to each other. NTP utilizes UDP port 123. Through NTP enumeration you can gather information such as lists of hosts connected to NTP server, IP addresses, system names, and OSs running on the client system in a network. All this information can be enumerated by querying NTP server.

DNS Enumeration

DNS enumeration is the process of locating all the DNS servers and their corresponding records for an organization. DNS enumeration will yield usernames, computer names, and IP addresses of potential target systems. The list of DNS record provides an overview of types of resource records (database records) stored in the zone files of the Domain Name System (DNS). The DNS implements a distributed, hierarchical, and redundant database for information associated with Internet domain names and addresses.

DNS Zone Transfer used to replicate DNS data across a number of DNS servers or to back up DNS files. A user or server will perform a specific zone transfer request from a —name server. If

the name server allows zone transfers by an anonymous user to occur, all the DNS names and IP addresses hosted by the name server will be returned in human-readable ASCII text.

Tools:

Nslookup, maltego, dnenum, dnsrecon

Countermeasures:

1. Disable Zone transfer by untrusted hosts
2. Ensure that private hostnames are not referenced to IP addresses within the DNS zone files of publicly accessible DNS servers.
3. Use premium registration services.

Password cracking Techniques

Dictionary Attack

In a dictionary attack, the hacker uses a predefined list of words from a dictionary to try and guess the password. If the set password is weak, then a dictionary attack can decode it quite fast.

Hydra is a popular tool that is widely used for dictionary attacks. Take a look at the following screenshot and observe how we have used Hydra to find out the password of an FTP service.

Brute-Force Attack

In a brute-force attack, the hacker uses all possible combinations of letters, numbers, special characters, and small and capital letters to break the password. This type of attack has a high probability of success, but it requires an enormous amount of time to process all the combinations. A brute-force attack is slow and the hacker might require a system with high processing power to perform all those permutations and combinations faster.

John the Ripper or **Johnny** is one of the powerful tools to set a brute-force attack and it comes bundled with the Kali distribution of Linux.

Rainbow ATTACKS

A rainbow table contains a set of predefined passwords that are hashed. It is a lookup table used especially in recovering plain passwords from a cipher text. During the process of password recovery, it just looks at the pre-calculated hash table to crack the password.

Rule based Attacks

This attack is used when the attacker gets some information about the password.

Syllable Attack

It is the combination of both brute force attack and the dictionary attack.

Trojans

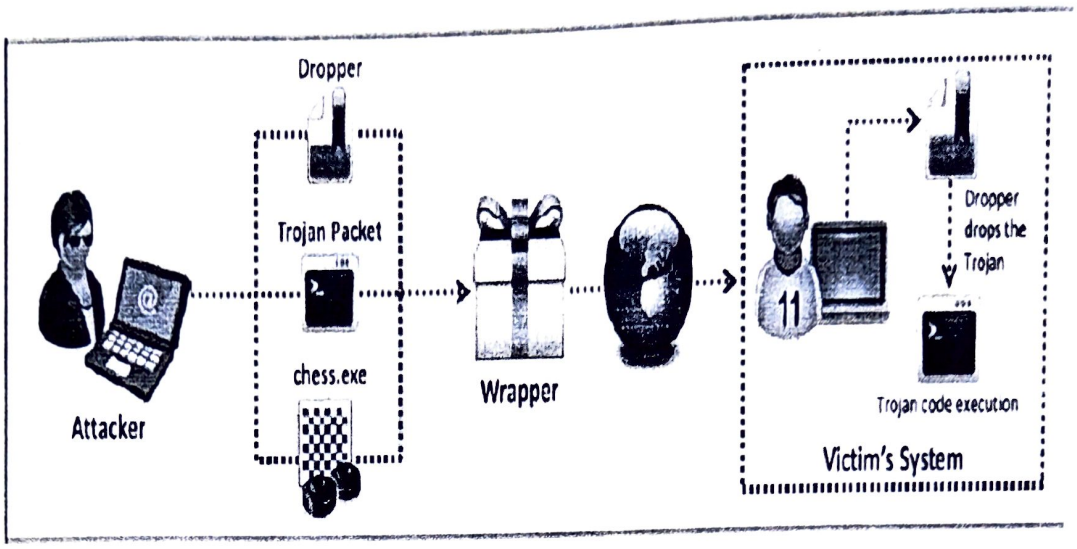
Trojans are non-replication programs; they don't reproduce their own codes by attaching themselves to other executable codes. They operate without the permissions or knowledge of the computer users.

Trojans hide themselves in healthy processes. However we should underline that Trojans infect outside machines only with the assistance of a computer user, like clicking a file that comes attached with email from an unknown person, plugging USB without scanning, opening unsafe URLs.

Trojans have several malicious functions –

- They create backdoors to a system. Hackers can use these backdoors to access a victim system and its files. A hacker can use Trojans to edit and delete the files present on a victim system, or to observe the activities of the victim.
- Trojans can steal all your financial data like bank accounts, transaction details, PayPal related information, etc. These are called **Trojan-Banker**.
- Trojans can use the victim computer to attack other systems using Denial of Services.
- Trojans can encrypt all your files and the hacker may thereafter demand money to decrypt them. These are **Ransomware Trojans**.
- They can use your phones to send SMS to third parties. These are called **SMS Trojans**.

Trojan infection process



Here's a look at some of the most common types of Trojan malware, including their names and what they do on your computer:

Backdoor Trojan

This Trojan can create a "backdoor" on your computer. It lets an attacker access your computer and control it. Your data can be downloaded by a third party and stolen. Or more malware can be uploaded to your device.

Distributed Denial of Service (DDoS) attack Trojan

This Trojan performs DDoS attacks. The idea is to take down a network by flooding it with traffic. That traffic comes from your infected computer and others.

Downloader Trojan

This Trojan targets your already-infected computer. It downloads and installs new versions of malicious programs. These can include Trojans and adware.

Fake AV Trojan

This Trojan behaves like antivirus software, but demands money from you to detect and remove threats, whether they're real or fake.

Game-thief Trojan

The losers here may be online gamers. This Trojan seeks to steal their account information.

Info stealer Trojan

As it sounds, this Trojan is after data on your infected computer.

Mail finder Trojan

This Trojan seeks to steal the email addresses you've accumulated on your device.

Ransom Trojan

This Trojan seeks a ransom to undo damage it has done to your computer. This can include blocking your data or impairing your computer's performance.

Remote Access Trojan

This Trojan can give an attacker full control over your computer via a remote network connection. Its uses include stealing your information or spying on you.

Rootkit Trojan

A rootkit aims to hide or obscure an object on your infected computer. The idea? To extend the time a malicious program runs on your device.

SMS Trojan

This type of Trojan infects your mobile device and can send and intercept text messages. Texts to premium-rate numbers can drive up your phone costs.

Trojan banker

This Trojan takes aim at your financial accounts. It's designed to steal your account information for all the things you do online. That includes banking, credit card, and bill pay data.

Trojan IM

This Trojan targets instant messaging. It steals your logins and passwords on IM platforms.

Penetration testing

- Penetration testing is a method of evaluating security levels of a particular system or network.
- This helps you determine the flaws related to hardware and software.
- The early identification helps protect the network.
- If the vulnerabilities aren't identified early, then they become an easy source for the attacker for the intrusion.

Black box vs white box testing

Black Box Testing	White Box Testing
1. Black box testing techniques are also called functional testing techniques.	1. White box testing techniques are also called structural testing techniques.
2Black Box Testing is a software testing method in which the internal structure/ design/ implementation of the item being tested is NOT known to the tester	2. White Box Testing is a software testing method in which the internal structure/ design/ implementation of the item being tested is known to the tester.
3. It is mainly applicable to higher levels of testing such as Acceptance Testing and System Testing	3. Mainly applicable to lower levels of testing such as Unit Testing and Integration Testing
4. Black box testing is generally done by Software Testers	4. White box testing is generally done by Software Developers
5. Programming knowledge is not required	5. Programming knowledge is required
6. Implementation knowledge is not required.	6. Implementation knowledge is required