

NARASARAOPETA INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering

ETHICAL HACKING (IV - CSE) – I SEM

UNIT III

Hacking into System: System Hacking, Password Cracking, Default password databases, Manual and Automated Password Cracking, Process of System Hacking, Using Keyloggers, Trojans & Backdoors: Trojans, Working of Trojan, Infection Techniques, Attack, Lifecycle and Classification of Virus, Worms, Virus Construction Kit.

System Hacking

System Hacking In the phase of system hacking, attacker actually performs HACK. This is exploitation phase of hacking. Information gathered from previous phases is required to perform hack. From the various phases like scanning and footprinting, attacker gathers information about target and finds the vulnerability. Now using the same vulnerability, in phase of system hacking, attacker performs the actual HACK. In system hacking, we perform cracking system passwords in order to escalate the privileges.

PASSWORD CRACKING

Password cracking refers to the process of attempting to discover or guess a password used to access a computer system, network, application, or account without the owner's permission or knowledge.

- Password cracking techniques are used to recover passwords from computer systems.
- Attackers use password cracking techniques to gain unauthorized access to the vulnerable system.
- Most of the password cracking techniques are successful due to weak or easily guessable passwords.

Password-Cracking Countermeasures:

1. Min length for passwords 12 recommended.
2. Windows: SYSKEY (128bit) encryption
3. Linux: shadow passwords
4. Don't use anything obvious
5. Policies to force changes, complex, and lockout
6. Monitoring
7. Use CAPTCHA: challenge/response test to ensure that the response is not generated by a computer;

following finding

Password Cracking attacks are of following types:

1. Passive online Cracking :

Passive online password cracking involves a more stealthy approach, where the attacker doesn't directly interact with the target system during the cracking process.

In the passive online cracking, attacker tries to authenticate into system by cracking the passwords using bruteforce, dictionary attacks or rainbow tables.

This method is quite complex and time consuming. Also there is no surety of getting the password cracked.

Key characteristics of passive online password cracking include:

- **Data Collection:** Attackers gather data such as password hashes, intercepted login credentials, or compromised databases.
- **Offline Cracking:** Once the data is obtained, attackers use offline techniques, such as dictionary attacks, rainbow table attacks, or advanced algorithms, to crack passwords without directly accessing the target system.
- **Lower Risk of Detection:** Passive online cracking is often less detectable by security systems since it doesn't involve continuous login attempts.

2. Active online Cracking:

In active online cracking, attacker generally guesses the passwords in order to gain access into the system. Generally, bad passwords and open authentication points are vulnerable to active online cracking. Although it consumes a lot of time and is less efficient way.

Common techniques used in active online password cracking include:

- **Brute Force Attacks:** Trying all possible password combinations until the correct one is discovered.
- **Dictionary Attacks:** Using a list of commonly used words or phrases to guess the password.
- **Hybrid Attacks:** Combining elements of brute force and dictionary attacks.
- **Credential Stuffing:** Using known username-password pairs obtained from previous data breaches to gain access to other accounts where users have reused passwords.

3. Offline attacks:

In offline attacks, attacker tries to exploit Lan manager hash (LM Hash), LM hashes are much vulnerable because of the short length and short key they use. Offline attacks are also take

much time to crack the passwords. Generally in offline attacks, attacker performs dictionary, hybrid or brute force attacks.

Password Hashes - In many systems, instead of storing plaintext passwords, the passwords are hashed before being stored.

Types of Offline Password Attacks:

- **Dictionary Attacks:** Attackers use a list of commonly used words or phrases (a dictionary) and apply the same hash function to each entry.
- **Brute Force Attacks:** Attackers systematically generate all possible password combinations and hash them to compare with stolen hashes.
- **Rainbow Table Attacks:** Rainbow tables are precomputed tables of password hashes and their corresponding plaintext passwords.

4. Non-electric media attacks:

In this, password cracking took place with using any technical medium.

Generally, shoulder surfing, dumpster diving and social engineering is used to gain passwords and sensitive information. Hardware key-logger can also be used to sniff each and every typo by the keyboard. This is commonly used nonelectric media attacks.

Attacker need not posses technical knowledge to crack password, hence known as non-technical attack.

- Shoulder Surfing
- Social Engineering
- Dumpster Diving

DEFAULT PASSWORD DATABASES

There are many website which contains databases of default usernames, passwords, ports and various information of networking or other devices. Sometimes, default password provides the access into target system. From the attacker's point of view each and every possibility should be covered.

Some of the website which contains default password databases are :

1. www.defaultpasswords.com
2. <https://cirt.net/passwords>

defaultpassword.com

default password list


Browse by character: **A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0-9**
Displaying 1812 passwords of total 1812 entries.

Manufacturer	Product	Revision	Protocol	User	Password
3COM			Telnet	adm	(none)
3COM			Telnet	security	security
3COM			Telnet	read	synnet
3COM			Telnet	write	synnet
3COM			Telnet	admin	synnet
3COM			Telnet	manager	manager
3COM			Telnet	monitor	monitor
3COM			Multi	security	security
3COM	3Com SuperStack 3 Switch 3300XM		Multi	n/a	(none)
3COM	AirConnect Access Point	01.50-01	Multi	adm	(none)
3COM	boson router simulator	3.66	HTTP	admin	admin
3COM	cellplex	7000	Telnet	admin	admin
3COM	CellPlex	7000	Telnet	tech	tech
3COM	CellPlex		HTTP	admin	synnet
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	debug	synnet
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	tech	tech
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)
3COM	hub		Multi	n/a	(none)
3COM	LANplex	2500	Telnet	tech	tech
3COM	LANplex	2500	Telnet	tech	(none)
3COM	LANplex	2500	Telnet	debug	synnet
3COM	LinkBuilder		Telnet	n/a	(none)
3COM	LinkSwitch	2000/2700	Telnet	tech	tech
3COM	NetBuilder		SNMP	(none)	admin
3COM	NetBuilder		SNMP		ANYCOM
3COM	NetBuilder		SNMP		ILMI
3COM	Office Connect ISDN Routers	5x0	Telnet	n/a	PASSWORD
3COM	OfficeConnect 812 ADSL		Multi	adminittd	adminittd
3COM	router		Multi	n/a	(none)
3COM	super stack 2 switch		Multi	manager	manager
3COM	super stack II		Console	n/a	(none)
3COM	superstack II	1100/3300	Console	3comcsco	RIP000
3COM	SuperStack II Switch	2700	Telnet	tech	tech
3COM	SuperStack II Switch	2200	Telnet	debug	synnet
3COM	Wireless 11g Firewall Router	3CRWDR100-72	Multi	none	admin
3COM	Wireless AP	ANY	Multi	admin	comcomcom
3M	VOL-0215 etc.		SNMP	volition	volition
a		a	HTTP	9000	iloveyou
a	pussy	1.0	Other	I Love	You!

Manufactor	Product	Revision	Protocol	User	Password
3COM	boson router simulator	3.66	HTTP	admin	Admin
Alcatel	Office 4200		Multi	n/a	1064
Dell	OpenManage Server Console		Console	root	Calvin

<https://cirt.net/passwords>

cirt.net/passwords



Default Password DB

Home

Join Nikto-Announce List

Email Address *

First Name *

Subscribe

Default Passwords

Search Passwords

531 vendors, 2117 passwords

@passdb on Twitter / Firefox Search

Linux SSD Cloud Servers

\$5 /mo. 20GB SSD Disk 512MB Memory

SIGN UP FOR FREE

DigitalOcean

	2Wire, Inc.	360 Systems
3COM	3M	Accelerated Networks
ACCTON	Acer	Actiontec
Adaptec	ADC Kentrox	AdComplete.com
AddPac Technology	Adobe	ADT
Adtech	Adtran	Advanced Integration

1. MySQL - MySQL

Method	all versions
User ID	root
Password	(none)
Level	Administrator
Doc	

2. MySQL - Eventum

Method	HTTP
User ID	admin@example.com
Password	admin
Level	Administrator
Doc	

MANUAL PASSWORD CRACKING

Manual password cracking, also known as "hands-on password cracking," is the process of attempting to guess or discover passwords through human intuition, observation, and analysis, rather than relying solely on automated tools or algorithms. It is a technique often used in ethical hacking and security testing to assess the strength of passwords and identify potential vulnerabilities in authentication systems.

1. Ping the target network to check whether it is live or not. ultimately choose a valid target.
2. Make a list of all possible passwords (easily available online).
3. Define the priority of each password on the basis of the key defined.
4. Try to get access using password, in case of failure, again try with different password.
5. Manual password crackers may observe users entering their passwords, either in person or through surveillance techniques.
6. Social engineering is a technique where attackers manipulate individuals into revealing their passwords or other sensitive information through psychological tactics.

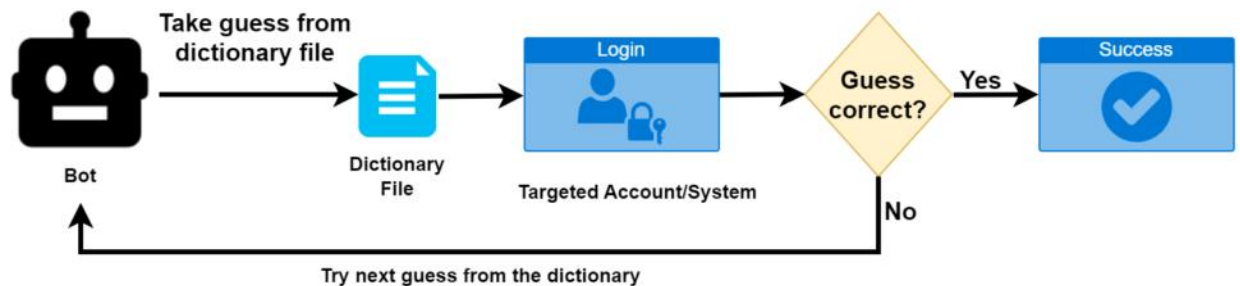
AUTOMATED PASSWORD CRACKING

Automated password cracking uses algorithms to crack passwords. Automated password cracking provides attacker an ease and is quite faster than manual password cracking.

This technique is often employed by both ethical hackers and malicious actors to assess the security of authentication systems, discover weak passwords, and gain unauthorized access to accounts, systems, or data.

A. Dictionary Attack :

In a dictionary attack, an automated tool uses a predefined list of words, phrases, and commonly used passwords as potential password guesses. It systematically tries each entry from the list until a correct password is found.



1. In the dictionary attack, firstly the encryption algorithm used is found.
2. The encrypted password is then obtained.
3. From the lists of passwords, each password is encrypted using the same encryption algorithm and matched with original encrypted password (obtained in step 2).
4. It matches each encrypted password with original encrypted password, until the match is found.
5. If match is found, it shows the password, else the procedure is repeated again.
6. Attack speed is around 250-300 words per second.

B. Lan Manager Hash :

The LAN Manager (LM) hash is a legacy password hashing algorithm primarily used in older versions of Microsoft Windows operating systems, such as Windows 95, Windows 98, and Windows Me. It was designed for backward compatibility and is considered extremely weak from a security perspective.

LM Hash is a algorithm by which the passwords are encrypted.

Algorithm of LM HASH :

1. Suppose the password created is 234567xyzabcd_.
2. Firstly, all the characters are converted into uppercase letters, i.e. 234567XYZABCD_.
3. If the password is shorter than 14 characters, it is padded with null characters to reach a length of 14 characters.
4. Each half is used to create a DES encryption key.
5. These two keys are used to encrypt a fixed string (the challenge). The resulting ciphertext is the LM hash.

Here's an example using the password "Password123":

Convert password to uppercase: "PASSWORD123"

Pad the password: "PASSWORD123\0\0\0\0\0"

Split into two halves: "PASSWORD" and "123\0\0\0\0\0"

C. Salting :

Salting is a prevention mechanism for the passwords. It disables or prevents deriving of passwords from the lists of passwords. In salting, the two different hashes may contain same passwords, hence the representation differs.

- Salting is a fundamental concept in password security and cryptographic hashing.
- It is a technique used to enhance the security of stored passwords and defend against various types of attacks, particularly dictionary attacks and rainbow table attacks.

When a user creates or changes their password, the system generates a random salt for that specific password. The salt is then concatenated (combined) with the user's plaintext password.

For example,

if a user has the password "password123" and a randomly generated salt "R4nd0mS@lt," the combination might look like this:

Salt: R4nd0mS@lt

Password: password123

Salted Password: R4nd0mS@ltpassword123

User's Password: "MySecretPassword123"

In this example, let's say the salt is "S@lt123".

Salt: "S@lt123"

Salted Password: "S@lt123MySecretPassword123"

PROCESS OF SYSTEM HACKING

A. Privilege Escalation :

In this, when the user gained access to the target system by any user account, next requirement is to gain access into administrative account or to gain higher privileges than that of administrator.

Identify and exploit vulnerabilities that allow for privilege escalation, enabling you to gain higher levels of access than initially obtained.

Techniques might include:

- Exploiting software vulnerabilities to gain administrative access.
- Exploiting weak or misconfigured permissions to access sensitive files or systems.
- Leveraging weak user credentials or password hashes to escalate privileges.
- Exploiting misconfigured service configurations to gain control.

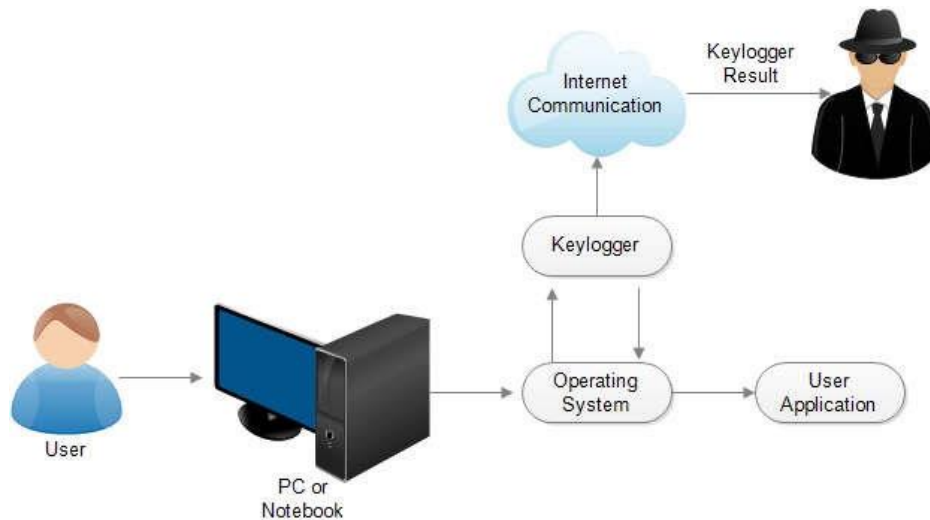
B. Executing Applications to maintain access :

Once the privileges are successfully escalated, attacker executes applications like backdoors or Trojans to maintain his access into the system. This is one of the important phase where attacker needs to be careful, else he might get caught.

Keyloggers:

Keyloggers are specially designer software or hardware which are used to track keystroke activities of the target system. Keylogger may also track every activity of the target system depending upon the keylogger's construction.

A keylogger is a type of **software or hardware device** that records the keystrokes typed on a computer or mobile device's keyboard. Keyloggers can be used for legitimate purposes, such as monitoring computer activity, analyzing user behavior, or diagnosing technical issues. However, they can also be misused for malicious purposes, such as stealing sensitive information like passwords, credit card numbers, or personal messages.



Keyloggers are of two types :

- 1. Software based Keyloggers**
- 2. Hardware based Keyloggers**

Software Keyloggers:

- Software keyloggers are programs or scripts that are installed on a computer or device to capture keystrokes.
- They can be installed deliberately by system administrators, parents, or individuals to monitor computer usage.
- Malicious software keyloggers can be installed by hackers or attackers to capture sensitive information without the user's consent.

Hardware Keyloggers:

- Hardware keyloggers are physical devices that are connected between the keyboard and the computer.
- They capture keystrokes as they are entered and store them in internal memory.
- Hardware keyloggers can be more difficult to detect than software keyloggers because they don't require software installation on the target system.

Using Refog keylogger :-

1. Download relog keylogger from following link :
2. Install it into the target system and allows it to run in background.

3. Tick the details which should be tracked by the keylogger like keystroke, websites visited, etc.
4. Provide the email to which attacker need to receive the data stored by keylogger keylogger (paid version only.) (Refog keylogger shown in the screenshot)

Spywares :

Spywares are specially designed programs programs which are used to track each and every activity of the target system. A spyware is evolution of keylogger. The main purpose of keylogger is to track keystroke whereas spyware tracks each and every activity.

A spyware can track following activity :

1. Processes running on the target system.
2. Keystrokes typed
3. Applications opened
4. Websites visited
5. Chats and IM information
6. Email conversations, Etc.

Anti-keyloggers and anti-spywares are used to detect the presence of keyloggers and spywares.

C. Hiding into target system :

Rootkits:

A rootkit is a type of malicious software or code that is designed to hide itself or other malicious processes from detection by security software, while also granting unauthorized access or control over a computer system. Rootkits are often used by attackers to maintain persistent access to a compromised system, allowing them to manipulate its behavior, steal data, or perform other malicious activities.

Rootkits can be categorized into two main types: user-mode and kernel-mode rootkits.

- User-mode Rootkits: These rootkits operate at the user level and are easier to develop and deploy. They can modify system files, processes, or configurations to hide their presence. User-mode rootkits may intercept API calls or modify system binaries to alter system behavior or conceal malicious activities.
- Kernel-mode Rootkits: These are more sophisticated and operate at the kernel level of the operating system. They have deeper access to the system and can intercept or modify low-level system functions. Kernel-mode rootkits are harder to detect and

remove compared to user-mode rootkits. They can modify the kernel data structures, hooks, and system service tables.

A rootkit allows an attacker to maintain hidden and anonymous access into the system. Hence the attacker is able to plot the viruses & Trojans and can easily maintain the hidden root level access into the target system. Once the target system is infected, it's not easy to get rid of it. Rootkits are invisible inside the system and aren't easily swiped out.

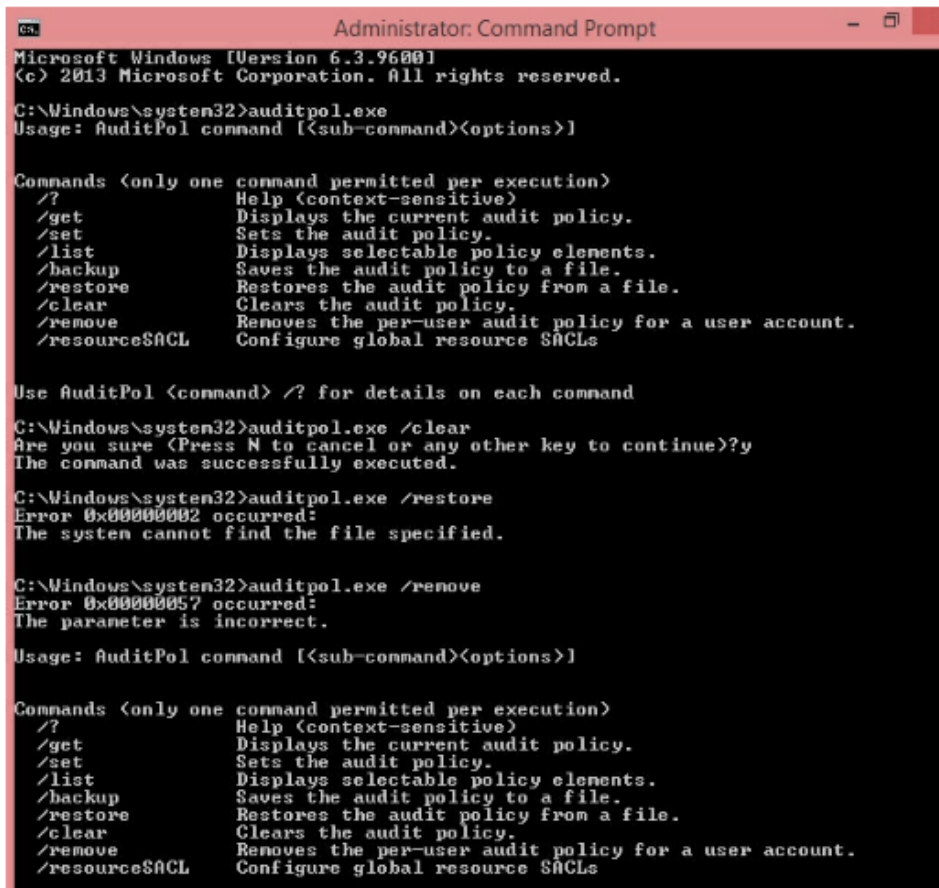
D. Clearing the tracks :

once the attacker maintained the administrative level access into the target system. The target may try to detect the presence of the attacker. When attacker is done with his work inside the target system, he leaves the target system after installing a back door for future access. Before leaving the system, attacker needs to cover all the tracks to not get caught.

Several precautions are performed by the attacker

1. Clearing Audit policy

Once the attacker gain administrative privileges of target system, first step performed is disabling the audit manager. 1. Open command Prompt (run in administrative mode). 2. Type auditpol.exe /clear (shown in screenshot).



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>auditpol.exe
Usage: AuditPol command [<sub-command><options>]

Commands (only one command permitted per execution)
/?          Help (context-sensitive)
/get        Displays the current audit policy.
/set        Sets the audit policy.
/list       Displays selectable policy elements.
/backup     Saves the audit policy to a file.
/restore    Restores the audit policy from a file.
/clear      Clears the audit policy.
/remove     Removes the per-user audit policy for a user account.
/resource$ACL Configure global resource $ACLs

Use AuditPol <command> /? for details on each command

C:\Windows\system32>auditpol.exe /clear
Are you sure (Press N to cancel or any other key to continue)?y
The command was successfully executed.

C:\Windows\system32>auditpol.exe /restore
Error 0x00000002 occurred:
The system cannot find the file specified.

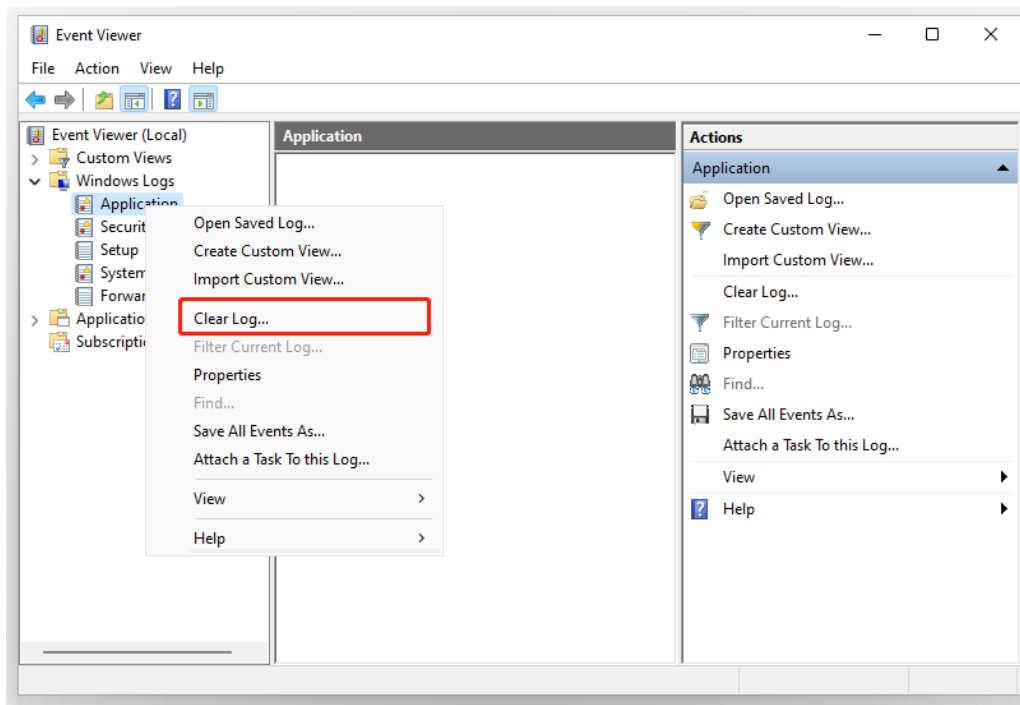
C:\Windows\system32>auditpol.exe /remove
Error 0x00000057 occurred:
The parameter is incorrect.

Usage: AuditPol command [<sub-command><options>]

Commands (only one command permitted per execution)
/?          Help (context-sensitive)
/get        Displays the current audit policy.
/set        Sets the audit policy.
/list       Displays selectable policy elements.
/backup     Saves the audit policy to a file.
/restore    Restores the audit policy from a file.
/clear      Clears the audit policy.
/remove     Removes the per-user audit policy for a user account.
/resource$ACL Configure global resource $ACLs
```

2. Clearing Event viewer

- a. Before leaving the system, attacker clears all the logs from the event viewer.
- b. All the logs are cleared but at last one record of clearing all the logs remains in the event viewer. It shows the presence of attacker into the system.



3. Using alternate data stream

1. Open command prompt and make a directory using “mkdir [name of directory]”

For ex : `cmd > mkdir hack`

2. Go inside the directory using `cd [name of directory]`, for ex : `cmd > cd hack`.

3. Type “dir” to check the files existing in the directory.

4. Now to create a new file in this directory, type “notepad. exe [name of file with file type]”.

For ex : `cmd > notepad. exe myfile.txt` .

5. Notepad window will be opened asking create a file, insert the message into the file and simply save the file.

6. Now type “dir” command to check the existence to file into the directory. To see the contents of the file into terminal type “ type [file name with file type]” . for ex: `cmd > type myfile.txt` .

7. Now to hide a your data into a file and hide that file into existing file, type “ notepad.exe [name of existing file with file type] : [name of new file with file type]. For ex : cmd>notepad.exe myfile.txt : hacked.txt .

8. Again a new notepad window will open up asking to make a file. Create the file, input your secret information and save it normally.

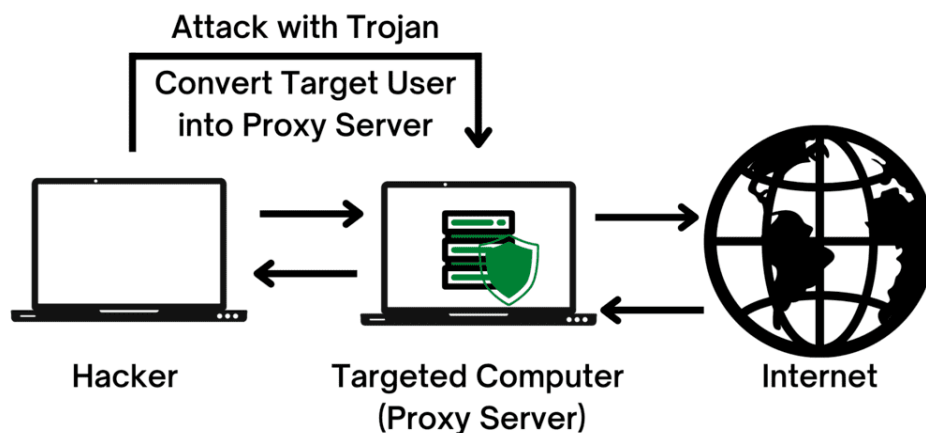
9. Now again type “dir”. There is no existence of the hidden file. It will only show the initial file created.

10. Now to access the hidden file simply type “ notepad.exe [name of file with file type] : [name of hidden file with file type].

TROJANS

Trojan is a malicious application developed for the specific purpose. It is a small program or script which runs hidden or anonymously in a system. With the effect of Trojan, an attacker may access to many credentials and sensitive information like stored passwords, account details from the trojaned target.

- In the trojaned target, an attacker is able to perform several actions like reading the data, showing up a message or change several possible things.
- An attacker may transfer files from target system to attacking system and can harm the target to a very great extent.
- Generally this phase is used after gaining the access into the system.
- Once the attacker gain access into the system, he installs the Trojan or backdoors to further maintain the access and for the future access in system.



Trojans mainly have two components :

1. Overt :

Overt component covers what actually user see. Generally this is the destructive phase where an attacker plots the Trojan by the wrapping them with executable files like freeware software or games which are openly available. Generally the games or freeware applications downloaded from untrusted sources contains Trojans to keep track on your system activity. 2. Covert :

Covert component covers the transmission of data over the network violating policies. In covert component following come into play :

- a. Rootkits.
- b. Backdoors.
- c. Keyloggers.
- d. Spywares.

Working of a Trojan :

Trojan horse, is a type of malicious software (malware) that disguises itself as something legitimate or benign but, once activated, performs malicious activities on a computer system without the user's knowledge or consent.

1. When the trojaned system comes online i.e. when the trojaned system is on active connection, an attacker can access to that system.

Hence, it is must that target system is on active connection in order to have access of it.

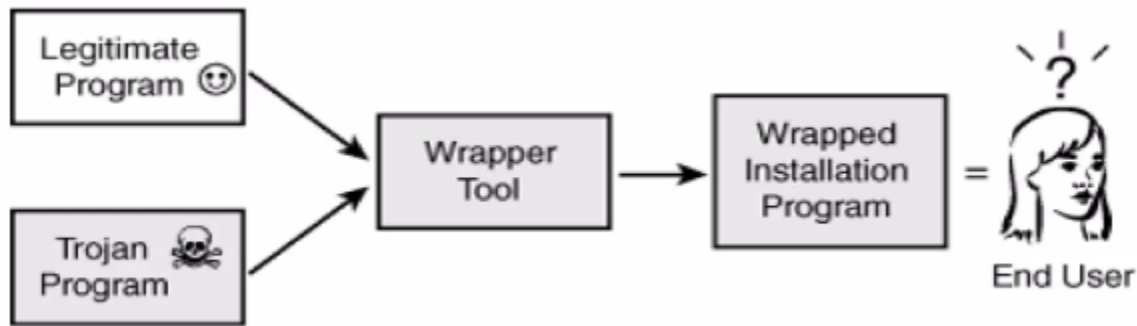
2. Access enables attacker to deploy various attacks on the trojaned target. ATTACKER Active Connection Trojaned Target.

Disguise and Delivery:

Trojans often masquerade as harmless or even desirable software. They may be distributed through email attachments, malicious websites, or bundled with seemingly legitimate programs.

Installation:

Once the user executes the Trojan by opening a file or running a program, the malicious payload is installed on the system. This can happen without the user's awareness.



Infection Techniques

The target can be infected from the Trojan by the following ways :

1. Freeware Software & Games :

Freeware software & games downloaded from the untrusted websites are bind with Trojans, which on installing them automatically gets executed in the background. Hence this is one of the easiest way to deploy the Trojan into any system.

2. Attachments :

Attachments in the emails or from various medium contains Trojan bind with them. When the target opens the file, Trojan automatically get executed in the background.

3. Instant messaging and social media :

Trojan might be spread over the Instant messaging and social media. From the study, it is concluded that attacker send some malicious content or links to the target over IM's and Social media which in turn contains Trojans.

4. Browser & Extensions :

Web browser and its extensions are sometimes infected with Trojan. There are many extensions available which anonymously install the Trojans into the system.

5. Untrusted websites :

Trojan may get transmitted from the untrusted websites.

6. File Sharing and physical access :

Physical access to the system or during file sharing, attacker can transfer the Trojan into target system. Trojan automatically execute itself without being detected.

7. Email Attachments:

Malicious emails may contain attachments that appear to be harmless documents (e.g., PDFs, Word documents) but actually contain a Trojan payload. Opening these attachments can initiate the infection process.

8. USB Drives and Removable Media:

Trojans can spread through infected USB drives or other removable media. When users connect an infected device to their computer, the Trojan may execute and spread to the host system.

9. Man-in-the-Middle (MitM) Attacks:

Trojans can be delivered through MitM attacks, where an attacker intercepts and manipulates communication between two parties. This can be done to inject malicious content into legitimate downloads or updates.

10. Social Engineering:

Trojans often rely on social engineering tactics to trick users into executing malicious files. This can include deceptive emails, fake websites, or messages that prompt users to download and run seemingly harmless files.

Behaviour of Trojan Infected Target:

1. Automatically opening and closing of programs.

It's referring to a symptom or manifestation observed on a compromised computer system. When a system is infected with a Trojan, the Trojan may exhibit control over the system's processes, leading to the involuntary initiation and termination of programs without the user's intervention.

2. Disappearing of Taskbar, desktop icons, changing of wallpapers and screen rotations.

Malware, including trojans, can manipulate the appearance settings of your desktop. They may hide or remove elements like the taskbar and desktop icons, change wallpapers, or alter screen rotation settings.

3. Unwanted opening and closing of disk drives.

This behavior may suggest malicious activity, potentially exploiting autorun.inf files or using scripts to manipulate disk drives.

4. Appearance of unwanted messages on the screen.

Trojans may display messages on the screen to convey information, intimidate the user, or prompt them to take certain actions, such as paying a ransom.

5. Changing into system settings like keyboard and mouse pad, sound and display settings.

Malware can modify system settings to disrupt normal functionality or to suit the attacker's objectives. Changes to keyboard, mouse pad, sound, or display settings could be signs of such interference.

6. Misbehaviour of file explorer and applications.

Trojans may interfere with the normal operation of the file explorer and other applications, causing crashes, errors, or unexpected behavior.

7. Misbehaviour of the web browser.

Web browser misbehavior could include unauthorized changes to homepage settings, redirection to malicious websites, or the injection of unwanted advertisements.

8. Computer restarts or shut down automatically.

Malware may trigger system restarts or shutdowns as part of its activity, disrupting normal use and potentially aiding in the execution of other malicious processes.

9. Documents and sensitive information gets deleted.

Data deletion is a common objective of malware. Trojans might delete files or encrypt them as part of a ransomware attack.

10. Monitor display fed off or on automatically.

Malware could manipulate power settings to turn off or on the monitor, potentially as a means of hiding its activities or causing disruption.

And some other unusual behaviour indicates that system has been infected by the Trojan.

Some Trojans and their respective Ports:

Port Trojan :

1. 21 ADM Worm, Pinochet, Bluefire, Dark FTP, Doly Trojan, The FLU, WinCrash, Alpha force, etc.
 - It's possible that these trojans might use port 21 as a means of communication or to exploit vulnerabilities associated with FTP.
2. 23 ADM Worm, Tiny telnet server, pest, AutoSpy, etc. 80 Seven eleven, cafeini, intruzzo, seeker, ring zero, scalper, etc. 146 (UDP) Infector
 - Ports 23 and 80 are well-known ports for Telnet and HTTP, respectively, and are commonly used for legitimate network communication.

3. 200 CyberSpy:
 - CyberSpy is a type of remote access trojan (RAT) that, when installed on a system, allows unauthorized individuals to remotely control and monitor the infected computer.
4. 520(UDP) A UDP Backdoor
 - Backdoors are a type of malicious software or malware that provides unauthorized access to a system, allowing attackers to control or manipulate the compromised system.
5. 1020 Vampire
 - When dealing with a trojan like Vampire, which could potentially compromise a system and allow unauthorized access or control.
6. 1025 NetSpy, KiLo, DataSpy, BDDT, AcidkoR, etc.
 - In this port, trojan that allows unauthorized access to a compromised system. It may include features such as keylogging, file manipulation, and remote control.
7. 12345 & 12346 Netbus:
 - NetBus is a trojan horse program known for providing unauthorized access to a user's computer over the Internet.
8. 21544 Girlfriend
 - The trojan could potentially enable various malicious activities, such as remote manipulation of files, monitoring user activities, or even acting as a backdoor for additional malware.
9. 2140 & 3150(UDP) Deep Throat
 - Deep Throat is a remote administration tool (RAT) or a backdoor trojan that allows unauthorized access and control over an infected system.

Wrappers:

Wrappers are used to bind the Trojan with executable (.EXE) file such as software or games. Using wrapper, Trojan and EXE file are combined together into a single infected file. When user runs the infected file (contains both original EXE file and Trojan), firstly the Trojan gets executed in the background. Once the Trojan installed in the background the original application starts running normally. User is able to see file as original file.

For example, an attacker bind Trojan.exe with game.exe . now only game.exe will be visible to user whereas game.exe is now contains Trojan.exe associated with it which will be installed in the background while game.exe will be processed in foreground.

1. Software Wrapper:

In software development and cybersecurity, a wrapper is often a piece of code or software that encapsulates or wraps around another program, function, or system component. This can serve various purposes, including providing an interface for easier integration, adding additional functionality, or enhancing security.

2. Encryption Wrapper:

In the context of data protection and encryption, a wrapper can refer to an additional layer of security added around sensitive data. For example, a file wrapper may encrypt the contents of a file, adding a layer of protection to the data within. This is common in various encryption techniques and protocols.

3. Security Wrapper:

Some security solutions use the term "wrapper" to describe a protective layer around applications or processes. This can include tools or technologies that monitor and control the behavior of applications to prevent malicious activities.

4. Network Wrapper:

In network security, a wrapper can be a protective layer around data packets or communication channels. This is commonly seen in encryption protocols where data is wrapped in a secure layer to prevent unauthorized access.

SOME TROJANS IN ACTION:

1. ProRat:

"ProRat" is the name of a remote administration tool (RAT) that gained notoriety as a piece of malware. It was designed to allow remote access and control of computers, often without the user's knowledge or consent. ProRat was created for both legitimate purposes, such as remote technical support, and malicious activities, such as unauthorized access and control of computers for cybercriminal activities.

Using ProRat :-

- ProRat is a remote administrative tool. It is used for system hacking and these rat tools are very powerful up to an extent.
- There are many options available in proRat. You need IP address of target system.
- Click on create and create a server file according to you needs and change its icon (every option is available). Now click on create server button.

- Now a executable server file is created. Rename it with changed icon and send it to target via mail (by compressing) or Hide it into usb drive when your target click on this file it will be started in background and deleted from his system.
- Now put your target's IP address and click on connect. When the connection got established. Now you can trick with your target by doing funny stuff like disabling your targets mouse etc. Remotely shutdown target system and do lots of stuff.

Functionality:

ProRat allowed a remote attacker to control a compromised computer from a remote location. It provided features such as remote desktop access, file transfer, keylogging (recording keystrokes), and various methods of communication between the attacker and the victim's machine.

Legitimate Use:

Like many remote administration tools, ProRat had legitimate use cases, such as enabling IT professionals to troubleshoot and manage systems remotely.

Malicious Use:

Unfortunately, ProRat was often used for malicious purposes, such as unauthorized access, data theft, and even distribution of other malware.

Spread:

ProRat was typically spread through malicious email attachments, infected downloads, or other social engineering techniques that tricked users into executing the malicious file.



2. BEAST :

DOWNLOAD : [https://sites.google.com/site/trojandownloads /beast-2-07](https://sites.google.com/site/trojandownloads/beast-2-07)

Using Beast Trojan:

- Beast is a Trojan. It also requires ip address of the target system. You need to create server file.
- Click on build server for making server file. Configure your server file and send it to your target and let your target open server file.
- Put your target's ip into ip box and click on Go Beast.
- When it starts listening means beast is connected successfully. Now you can do multiple things with your target.
- Like funny stuffs and some more stuff are provided with beast. All these stuff you can do with your target remotely.

Remote Access Trojans are malicious software programs that provide unauthorized access and control over a victim's computer. They allow attackers to perform various actions on the compromised system, such as:

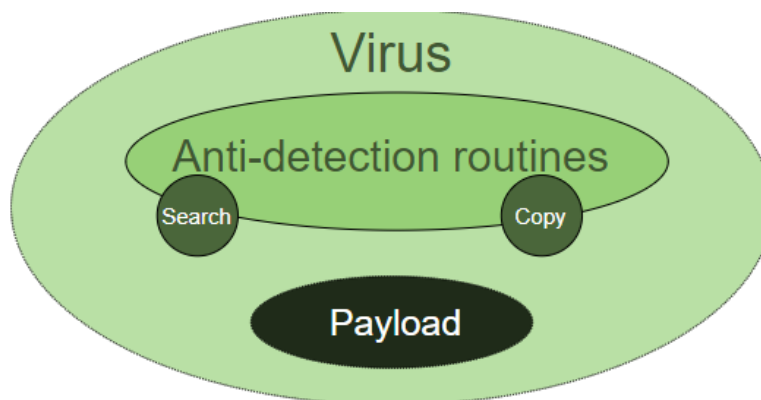
1. Remote Control: The attacker can control the victim's computer remotely, essentially taking over its functions.
2. Data Theft: They can steal sensitive data, including personal information, login credentials, financial data, and more.
3. Keylogging: Capture and record keystrokes entered by the victim, which can reveal usernames, passwords, and other confidential information.
4. File Manipulation: Download, upload, and modify files on the victim's computer.
5. Surveillance: Monitor the victim's activities, including web browsing, emails, and messaging.



VIRUS

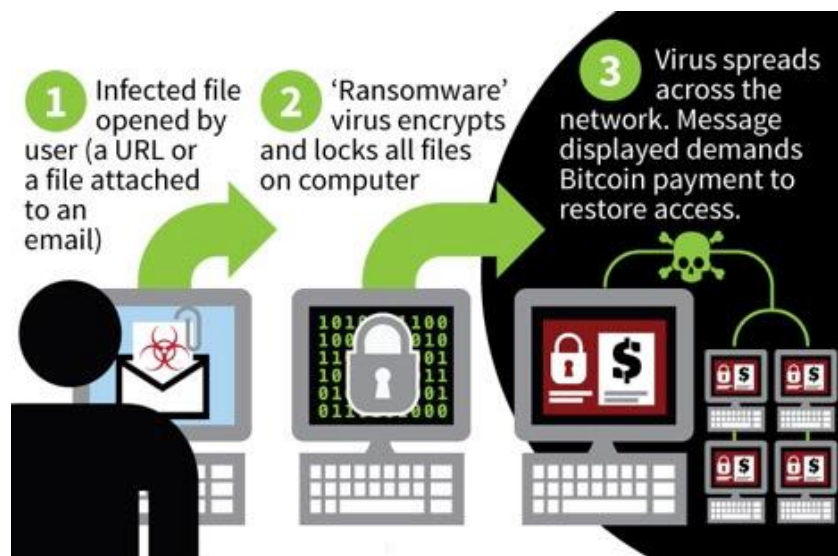
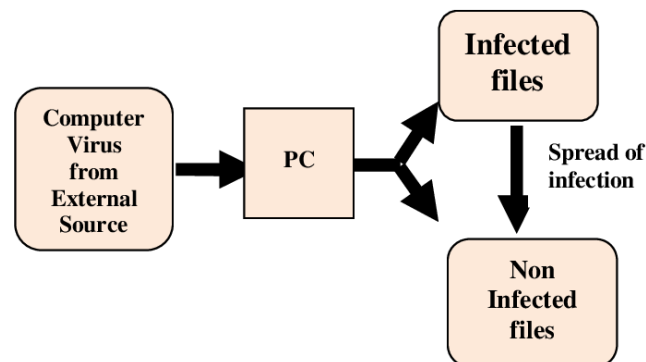
Virus can be defined as the weakness of the system. Virus makes a system more vulnerable to the attacker. Viruses are made to threaten the target system. Virus is a kind of malicious program which is used to harm the target system. When virus is executed into the target system, generally it replicates itself in many copies and infects the target system.

- A computer virus infects data files or program or information stored into the target system.
- Some viruses are designed in such way that they utilize the disk space and make it unavailable resulting into fragmentation.
- Viruses may harm the system in many ways like stealing personal information, infecting the documents and data stored, stealing boot records and many other possibilities are there.
- Viruses contain the property to install themselves without the permission of user. However, hiding property in viruses differs according to their work and use.
- Virus writers mainly code the virus for destructive purposes, generally to exploit system and infect the data stored. Sometimes a virus can also be used for pranking and fun.
- Viruses have tendency to change their nature by automatically modifying their source code and sometimes this gives an advantage to the virus.
- It generally hides itself using encryptions or using alternate data streams (discussed in previous chapters). Generally a computer virus, first get executed into the system and then starts infecting the target system.
- Once it replicates and successfully infects the target system, it starts performing the attacks on the target system. Ultimate aim of a computer virus is to corrupt the system. A virus may corrupt the whole system and make it un-accessible.



Working of a Virus

1. An Attacker somehow manages to let the virus executed into the system. A virus is malicious code which executes without any permission and can replicates itself.
2. Once the virus is deployed into system, it starts infecting the system. Infecting includes replicating the virus, hiding inside data and making system quite slower. Once the desire infection is done attacking virus moves to next phase.
3. Once system is infected and comes under control of the virus, it starts attacking on the target system. It makes the system slower and corrupts the data. Some viruses allow the attacker to gain remote access of the system. At last the private and personal information is under risk of being disclosed to the attacker.
4. A working of virus may vary according the intention of the developer. There are many viruses which are used to defeat the security and compromise companies and take over the data of business personals whereas some viruses are used for fun and prank purposes and are quite harmless.



There are many reasons behind the creation of a virus, following are some main reasons:

1. Research :

Some viruses are developed to study the behaviour and response of the system in the presence of virus. These viruses are generally developed by professionals for study purposes.

2. Compromise :

One of the main reasons behind the creation of virus is to compromise and take over the target system. Mostly the virus is developed for offensive purposes instead of defensive purposes.

3. Fun :

Some harmless viruses are developed for fun and entertainment purpose. These kinds of viruses are generally used for pranking. Their effect is temporary and system can be restored to its normal phase easily without having any loss of data.

4. Tracking :

Viruses developed in the form of spywares or keyloggers are used to track the activities of target system. These are used for record the activity and sending that record to the attacker.

Characteristics of a Virus Attack:

1. System take more time while booting , this is because some viruses are designed in such a way that they enables some process during start up and this result into slower booting of systems.
2. If a software application takes more time in executing than in general, sometimes viruses are bind with particular executable file and when target opens that time, firstly virus gets executed and this slower the execution of original application.
3. Freezing or unresponsive behaviour of system is one of the main characteristics of the virus. Virus makes the system unresponsive and corrupts the system.
4. Unresponsive behaviour of hardware drives like disk-drive or usb ports may be a result of virus attacks.
5. Some viruses infect the hardware which is used in daily activities like usb ports.
6. Data loss or sudden disappearance of files from the system is characteristics of virus attack.
7. Sometimes shortcut folders are created as subfolders in the main folder which also represents virus attack.

8. Unresponsive bios and booting issues.
9. Unwanted application starts running in background or foreground. These are some commonly shown characteristics by each and every computer virus.

Threats from a Virus Attack:

Viruses are one of the powerful weapons used by an attack to compromise the target system. A computer virus affects both hardware and software part. The corruption of system and failure of hardware is the ultimate effect of virus on hardware.

1. Effect on Software Part :

- Slows down the system.
- Unresponsive behaviour of application.
- Increased system usage.
- Delay in booting the system.
- Unwanted deletion of data.
- Unauthorized activities in the system.

And in many other ways a virus may affect the computer software.

1. Data Manipulation.
2. Software Malfunction.
3. File and Program Corruption.
4. Backdoor Installation.
5. Resource Exploitation.
6. Propagation Through Software Vulnerabilities.
7. Disruption of Software Updates.
8. Encryption of Files (Ransomware).
9. Network Communication Interference.

2. Effect on Hardware part:

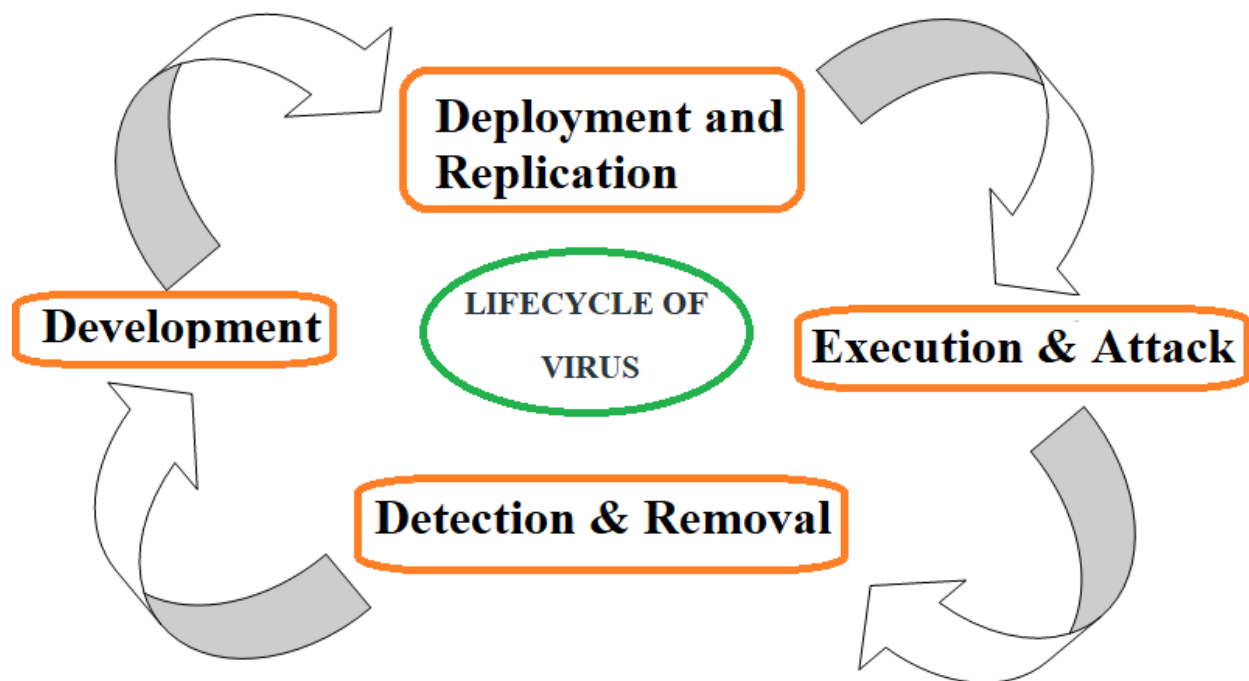
- Sudden power cuts or due to high system usage there may be damage to the hardware.
 - Unwanted keystrokes and typo errors or change keyboard layout.
 - Drives like USB drives etc. become unresponsive. d. Unwanted crash of usb drives.
 - Damage of data stored in removable media.
- These are some of the main effects on the computer hardware.

And in many other ways a virus may affect the Hardware.

1. Overutilization of Resources.
2. Reduced System Performance.
3. Hardware Damage due to Overheating.
4. Increased Wear and Tear.
5. Interrupted Power Supply.
6. Firmware Exploitation.
7. Interference with Peripheral Devices.
8. Propagation Through Removable Media.
9. Disruption of Hardware Communication.
10. Compromised Network Devices.

LIFECYCLE OF A VIRUS

The lifecycle of a computer virus involves several stages, from its creation to its execution on a host system.



1. Development :

The first phase is development of virus which can perform the desired tasks in the target system. For the development of self - controlled virus whose behaviour can be changed as per requirement, one should have sufficient knowledge of programming languages like assembly, bash, c++ etc. .

There are some virus constructions kits are also available, which can create a virus with pre-fixed features. Thousand varieties of viruses can be created using virus construction kits.

2. Deployment & Replication :

Once the virus is developed, the main challenge is to deploy it into the target systems. Virus may be sent within an attachment or can be transferred with a file shared or by other direct or indirect means.

Once the virus gets deployed into the system, it starts replicating itself. A virus have tendency to replicate itself. It replicates itself until it completely spread and infects the target system.

3. Execution & Attack :

After the replication, the virus spreads in the target system and completely infects the target system without any prior knowledge to the target. Now with the specified classes, when user performs or starts something, it automatically activates and launches the virus. Now the virus starts attacking into the system causing the unwanted behaviour of system.

Attacker virus performs specified attacks such as corrupting the data, freezing the system or system failure. This is the main phase where the work of the virus is done and system and information may get vanished.

4. Detection & Removal :

When the target notices about the unwanted activities and unresponsiveness, target starts detecting the root cause. By using anti-viruses or anti-thefts targets starts hunting for the root cause and tries to get rid of it.

General purpose viruses are easily detected by the ant-viruses and can be removed easily but there are some encryption algorithms like jump or shikata encryptions which encrypt the virus and hence make it undetectable. Anti-virus detects viruses as threat or potential risks and removes them immediately.

Anti-virus is pre-configured to detect viruses on the basis of file types, behaviour and program source code. An anti-virus easily detects the presence of some pre-configured viruses whereas it took time to detect modified virus. Anti-virus makes classifications on the basis of the behaviour and source code impact and detects the virus.

CLASSIFICATION OF VIRUS

Virus may be classified into the following categories:

1. Infection target
2. Method of infection

A. Infection Target :

Virus may be classified on the basis of the infection target. Different virus targets different point or different vulnerability in the target system. On the basis of Infection target, virus may be classified as:

B. Information or Data Virus :

These types of virus target the data or information present in the system and make it unusable by corrupting it. Generally executable files easily get infected and sometimes virus is spread using these executable files.

1. Data Corruption: The malware might modify or corrupt specific files or data sets, rendering them unusable or causing errors when they are accessed by legitimate users.
2. Data Theft: The malware could be programmed to steal sensitive or valuable information, such as personal data, financial records, intellectual property, or trade secrets.
3. Data Manipulation: Instead of destroying or stealing data, the malware could subtly alter the content of files or databases, potentially leading to misinformation, confusion, or errors down the line.
4. Data Encryption: Similar to ransomware, the malware might encrypt data and demand a ransom for its decryption. However, in this case, the primary goal could be the data itself rather than the system's functionality.
5. Data Spreading: The malware might be programmed to propagate across networks, targeting specific types of data and copying or transferring it to other systems.
6. Data Surveillance: The malware could monitor data usage or communication patterns to gather intelligence about a target, which could be used for cyber espionage or reconnaissance.

C. Boot or Bios Virus : These types of virus target the boot sector or bios of the system. They corrupt the boot records resulting into system failure or enable the bios lock or interfere with bios.

Boot Virus:

- A boot virus infects the boot sector of a storage device, such as a hard drive or a floppy disk. The boot sector is a small region of the storage device that contains code that's executed when the computer starts up.
- A boot virus can replace or modify this code to ensure that the virus is loaded into memory and executed during the boot process. When an infected device is booted, the boot virus loads into memory and gains control before the operating system is loaded.
- This allows the virus to potentially corrupt files, steal data, or execute other malicious activities. Since the boot process is initiated before any security software or protections are in place, boot viruses were difficult to detect and remove.

BIOS Virus:

- A BIOS virus, also known as a firmware virus, infects the BIOS of a computer. The BIOS is a low-level software that initializes hardware components and provides basic functions for the operating system.
- Infecting the BIOS gives the virus a level of control that is even lower than the operating system, making it challenging to detect and remove.
- BIOS viruses were especially concerning because they could survive even if the operating system was reinstalled or the storage devices were formatted.
- However, modern systems often have protections in place to prevent unauthorized changes to the BIOS, reducing the risk of BIOS virus infections.

D. Network Based Virus :

These viruses are easily transmitted over e-mails or gain access into the system using open network protocols. This leads to the infection of port and protocol communications.

E. Appending Virus :

These viruses have tendency to get merged with executable files by appending their source code with the source code of original file. Generally free software or freeware things contain this type of virus. It automatically gets executed into the system when the file is opened (infected file).

A. Method of Infection :

1. Encrypted Virus :

Using some special encryption algorithm, viruses are encrypted and thus it became undetectable by anti-viruses. Generally encrypted virus is used in compromising big companies or big networks.

2. Cavity Injector Virus :

These virus do not change the original file size while infecting any file i.e. they Maintains original file size and hence user don't get any idea of infection.

3. Boot loader Virus :

These are the virus designed to destroy the data of hardware when booted by the mean of USB or CD. These types of virus are infects the bootable image files. When the image is booted, it gets executed and destroyed the complete data to hard disk.

4. Auto mod virus :

These kinds of virus have special tendency to automatically modify its signature. Generally an anti-virus looks for the virus signature in a file while scanning. This kind of virus modifies its signature for every next infected file and hence the detection rate becomes lower.

5. Mutating Virus :

In the mutating virus, the infection part on each file is different. To enable mutation, the virus needs to contain mutating engine. By the help of mutation, each and every time it left different infection part with the target file and there is no change in original source of the virus.

6. Extension Virus :

This virus changes the file extension. Generally the file extension is turned off. The file appears with the name only.

For Ex : ABC.txt is the original file which is infected by the virus and now the extension becomes ABC.txt.bat .

Now, when attacker sends this file to the target due to the extension showing is off, target will normally see ABC as a text file and opens it. When the target opens the file, virus gets executed.

WORMS:

Worms are malicious programs like viruses and have almost same functionality. But worms differ from the viruses. A worm does not require any kind of human involvement whereas a virus needs some form of human involvement. This is the special property of worm. Worms can be considered as special type of viruses. Worms have ability to replicate itself in the system but they are not able to attach themselves to target program.

- Worms can be spread over the infected network without any human involvement where as a virus is not able to do so. Hence, there are few things which a virus can't do but a worm can but ultimately the worm is special kind of virus.
- Install backdoors on the victim's computers. The created backdoor may be used to create zombie computers that are used to send spam emails, perform distributed denial of service attacks, etc. the backdoors can also be exploited by other malware.
- Worms may also slowdown the network by consuming the bandwidth as they replicate. Install harmful payload code carried within the worm.

Types of worms are as follows:

Email Worms:

- Email Worms spread through malicious email as an attachment or a link of a malicious website. An example of an email worm is ILOVEYOU worm which infected computers in 2000.

Instant Messaging Worms:

- Instant Messaging Worms spread by sending links to the contact list of instant messaging applications such as Messenger, WhatsApp, Skype, etc.

Internet Worms:

- Internet worm searches all available network resources using local operating system services and/or scans compromised computers over the Internet.

IRC Worms:

- IRC Worms spread through Internet Relay Chat (IRC) chat channels, sending infected files or links to infected websites.

File sharing Worms:

- File sharing Worms place a copy of them in a shared folder and distribute them via Peer To Peer network. A worm 'Phatbot' infected computers in 2004 through sharing files. This worm has stolen personal information such as credit card details and destroyed many systems on an unprecedented scale.

Virus Construction Kit :

Virus construction kit is a tool for creating a virus having fixed attack or possibilities. There are many virus construction kits are available over the internet. There is no need of knowledge of any programming knowledge. It's easy to use and construct viruses.

A. JPS Virus Maker:

DOWNLOAD :- <http://sh3ll-h4ck3r.blogspot.in/2011/08/createyour-own-virus-with-jps-virus.html>

Using JPS (Virus Maker 3.0)

- JPS Virus Maker is a virus construction kit. It is freeware and no coding knowledge is required to use it.
- There are many options like disable registry, hide services, clear windows XP etc. which are basically the functions that virus will have.
- Tick all the function you want. Name the virus and click on create virus. Executable virus file will be created.
- Now send this executable file to your target, sit back and enjoy.

