EH - UNIT - III

CO3:- Explain the process of system hacking, password cracking and the concepts of Trojans, backdoors, worms and virus and it's countermeasures.

Syllabus:- Hacking into system: System Hacking, Password cracking, Default password databases, manual and automated password cracking, Process of system Hacking, using key loggers, Trojans & Backdoors: Trojans, working of Trojans, infection techniques, Attacks, lifecycle and classification of virus, worms Virus construction kit.

→ System Hacking:- In this phase of system hacking, attacker actually performs HACK. This is exploitation phase of hacking. Information gathered from previous phases like scanning and footprinting etc, attacker gathers information about target and finds the vulnerability.

→ Password Cracking

Password cracking attacks are of following types:

1) passive online cracking
2) Active online cracking
3) Offline attacks
4) Non-electric media attacks.

1) Passive online cracking :- In this, the attacker tries to authenticate into system by cracking the passwords using bruteforce, dictionary attacks or rainbows tables.

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

2) Active online cracking :- In this, 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.

3) Offline attacks :- In this, 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.

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 non-electric media attacks.

→ **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 passwords 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.

→ **Manual password cracking :-**

→ Ping the target network to check whether it is live or not. Ultimately choose a valid target.

→ Make a list of all possible passwords (easily available online).

→ Define the priority of each password on the basis of the key defined.

→ Try to get access using password, in case of failure, again try with different password.

Automated Password Cracking :-

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

Mainly Automated Password cracking has two types

A. Dictionary Attack:-

→ In this attack, firstly the encryption algorithm used is found.

→ The encrypted password is than obtained.

→ From the lists of passwords, each and every password is encrypted using the same encryption algorithm and matched with original encrypted password.

→ It matches each encrypted passwords with original encrypted password, until the match is found.

→ If match is found, it show the password, else the procedure is repeated again.

Note:- Attack speed is around 250-300 words per second.

B. Lan Manager Hash:

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

Algorithm:-

* Suppose the password created is 234567xyzabcd_.
* Firstly, all the characters are converted into uppercase letters, i.e., ~~234567ABCD~~ 234567XYZABCD_.
* If the password is less than 14 characters in length, null is added until the length of 14.
* Now the password is split into half, i.e., 234567X and YZABCD_.
* Each half is separately encrypted and the result is concatenated.
* Now to crack the alpha-numeric part, it take more than 20 hours. where as it takes less than 5 minutes to crack the alphabetic part.
*

C. Salting:

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

→ 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 of administrator. This process is known as privilege escalation.

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

→ Key loggers :-

These are specially designer software or hardware which are used to track key stroke activities of the target system. keylogger may also track every activity of the target system depending upon the key logger's construction.

Types :- 1) Software based keyloggers
2) Hardware based key loggers.

→ Software based keyloggers :- These are installed into target system. They have ability to run into background without getting caught by antiviruses. They track every keystroke typed and anonymously send all the data to the attacker on a fixed interval of time.

→ Hardware based keyloggers :- Generally, a Hardware is connected between keyboard and CPU, this intermediate hardware device tracks every key stroke typed and save them into proper log files, which is accessible by the attacker.

Generally software based keyloggers are used. Hence it is not safe to use untrusted system, there may be chances of keyloggers installed. Any sensitive information might get transferred to the attacker without target's knowledge.

→ Refog keylogger :-

* Download refog keylogger from "refog.com".
* Install it into the target system and allows it to run in background.
* Select the details which should be tracked by the keylogger like keystroke, websites visited etc.

* Provide the email to which attacker need to receive the data stored by keylogger.

Note: Paid version only.

→ **Spywares :-**

Spywares are specially designed programs which are used to track each and every activity of the target system.

A spyware is evolution of keyloggers. The main purpose of keylogger is to track keystroke whereas spyware tracks each and every activity.

A spyware can track following activity:

* Processes running on the target system.
* key strokes typed
* Applications opened.
* Websites visited
* chats and IM information
* Email conversations Etc.

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

→ Trojans :-

Trojans 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, they installs the Trojan or backdoors to further maintain the access and for the future access in system.

Trojans mainly have two components :-

1. Overt :- It 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 :- It covers the transmission of data over the network violating policies. In covert component following come into play:

a) Rootkits :- The collection of software designed to give actors control of a computer network or application.

b) Backdoors :- It is a malware type that negates normal authentication procedures to access a system.

c) Keyloggers :- These are specially designer software and hardware which are used to track key stroke activities of the target system.

d) Spy wares :- These are specially designed programs which are used to track each and every activity of the target system.

→ Working of a Trojan :-

* when the trojaned system comes online i.e., when the trojaned system is on active connection, an attacker can acess to that system.

* Access enables attacker to deploy various attacks on the trojaned target.

Attacker → Adive connection → Trojaned Target.

→ Infection Techniques :-

The target can be infected from the trojan by the following ways :-

1) Freeware Software & Games :- It is downloaded from the untrusted websites are bind with trojans, which on installing them automatically gets executed in the background.

2) Attachments :- Attachments in emails or from various medium contains Trojans bind with them. When the target opens the file, trojans automatically get executed in the background.

3) Instant messaging and social media :- Trojan might be spread over the instant messagein 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 & Extension :- web browser and its extensions are sometimes infected with trojans. 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.

→ Behaviour of trojan Infected Target :-

* Automatically opening and closing of programs
* Disappearing of taskbar, desktop icons, changing of wallpapers and screen rotations.
* Unwanted opening and closing of disk drivers.
* Appearance of unwanted messages on the screen.
* changing into system settings like keyboard and mouse pad, sound and display settings.
* Mis-behaviour of file explorer and applications.
* Mis-behaviour of the website(or) browser
* computer restarts or shut down automatically.
* Documents and sensitive information gets deleted.

* Monitor display fed off or on automatically.

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

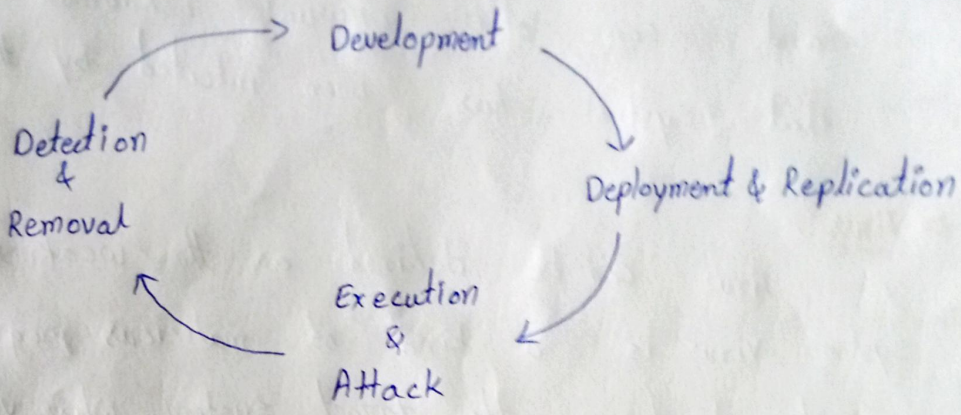
→ **Virus :-**

Virus can be defined as the weakness of the 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.

Viruses have tendency to change their nature by automatically modifying their source code and sometimes this gives an advantages to the virus. It generally hides itself using encryptions or using alternate data streams.

Virus, first 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.

→ Life cycle of a virus :-



* Development :- The first phase is development of virus which can perform the desired tasks in the target system. There are some virus construction kits are also available, which can create a virus with pre-fixed features. Thousand varieties of viruses can be created using virus construction kits.

* Deployment & Replication :- once virus is deployed, the main challenge is to deploy it into the target systems. Virus may be send with in 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 until it completely spread and infects the target system.

* 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.

* 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 anti 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 makes classifications on the basis of the behaviour and source code impact and detects the virus.

→ 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.

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.

→ Threats from a Virus Attack :-

Viruses are one of the powerful weapons used by an attack to compromise the target system. A computer virus effects 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.

② Effect on Hardware part :

a. Sudden power cuts or due to high system usage there may be damage to the hardware.

b. Unwanted keystroke and typo errors or change keyboard layout

c. Drives like USB drivers etc. became unresponsive.

d. Unwanted crash of usb drives.

e. Damage of data stored in removable media.

These are some of the main effects on the computer hardware.

→ Classification of Virus :

Virus may be classified into the following

categories

1. Infection target
2. Method of infection

① 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.

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.

D. Network Based Virus:

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

E. Appending Virus:

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

② 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.

B. Cavity Injector Virus:

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

C. 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.

D. 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.

D. Mutating Virus:

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

F. Extension Virus:

The 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 how 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 have almost same functionality. But worms differ from the viruses.

A worms does not require any kind of human involvement whereas a virus need 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.

→ 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 virues.

A. JPS Virus Maker

DOWNLOAD :- http://sh311-hyck3r.blogspot.in/2011/08/Create-your-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 optious like disable registry, hide services, clear window 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.

- Need now send this executable file to your target, sit back and enjoy