UNIT 2:- CYBER OFFENSES: HOW CRIMINALS PLAN THEM

How criminals plan the attacks, Social Engineering, cyberstalking, cybercafe and cybercrimes, Botnets: The fuel for cybercrime, Attack vector and Cloud computing.

2.1 How criminals plan the attacks:-

Criminals use many methods and tools to locate the vulnerabilities of their target. The target can be an individual and/or an organization. The following phases are involved in planning cybercrime:

1. Reconnaissance (Information gathering) is the first phase
2. Scanning and Scrutinizing the gathered info for validity is second phase
3. Launching an attack is the final phase.

1. Reconnaissance:- This phase begins with "footprinting". The objective of this phase is to understand the system, its networking ports & services and any other aspects of its security that are needed to launch an attack.

The attacker gathers info in two ways.

1. passive attacks
2. Active attacks

Passive attacks:- A passive attack involves gathering info about a target without his/her (individual or company) knowledge. It is usually done by

1. Google search
2. Surfing online groups [Eg: Facebook, Linkedin.. etc]
3. Organization's website
4. Blogs, news groups, press releases etc
5. Network Sniffing

Some of the tools used for passive attacks are

1. Google earth
2. Internet archive
3. Dns stuff
4. Traceroute
5. Website watcher etc.

Active attacks:- An active attack involves probing the network to discover individual hosts to confirm the information, gathered in the passive attack. It invokes risk of detection & is called as "Active Reconnaissance"

Some of the tools used during active attacks are

1. Arphound
2. Bing
3. Bugtraq
4. Dsniff
5. Hping etc.

2. Scanning & Scrutinizing Information :-

Scanning is a key step to examine intelligently while gathering info. The objectives of scanning are

1. port Scanning :- Identify open/close ports & services

A port is an interface on a computer to which one can connect a device. The port number are divided as:

a) well known ports (from 0 to 1023)
b) registered ports
c) dynamic and/or private ports.

2. Network Scanning :- understand about IP addresses and related information about the computer network systems.

3. Vulnerability Scanning :- To understand the existing weakness in the system.

The categories of vulnerabilities are:

a) Inadequate border protection
b) Remote access servers with weak access controls
c) Application servers with well known exploits.

Scrutinizing phase is always called "enumeration" in hacking world.

The objectives are to identify:

a) The valid user accounts/groups
b) N/w resources and/or shared resources
c) OS & diff apps that are running on the OS.

3. Attack :- After the first 2 stages, the attack is launched using the following steps:

1) Crack the password
2) Exploit the privileges
3) Execute the malicious commands
4) Hide the files
5) Cover the tracks.

2.2 Social Engineering :-

It is the "technique to influence" and "persuasion to deceive" people to obtain the information or perform some action.

It is an art of exploiting the trust of people, which is not doubted while speaking in a normal manner.

Ex:- calling a user and pretending to be someone from the service desk working on a n/w issue; the attacker then proceeds to ask questions about what the user is working on, what files shares he/she uses, what is his/her password, and so on.

Social Engg is classified into 2 types.

1. Human based social Engineering :-

It refers to person to person interaction to get the required/desired information.

a) Impersonating an employee or valid user :-

Impersonation (posing oneself as an employee of same organisation) is perhaps the greatest technique used to deceive people.

b) Posing as an important user :-

The attacker pretends to be an important user - for ex, as a CEO or high level manager who needs immediate assistance to gain access to a system. Most of the low level employees donot ask any question to someone who appears to be in a position of authority.

c) using a third person :-

This trick is useful when the supposed authorized personel is on vacation or cannot be contacted for verification.

d) Calling Technical support :-

Help desk and technical support personnel are trained to help users which makes them good prey for Social engineering attacks.

e) Shoulder Surfing :-

It is a technique to gather info by watching over a person's shoulder while he/she logs into the system.

f) Dumpster diving :-

It involves looking into the trash for info written on pieces of paper or computer printouts. other names are Scavenging/binning/skipping.

2. Computer based Social Engineering :-

This is an attempt made to get the desired information by using Computer Software / Internet.

a) Fake e-mails (phishing) :-

Attacker sends fake e-mails in such a way that user finds it as a legitimate mail. This activity is also called as "phishing" which is an attempt to fool the netizens to reveal their sensitive personal info.

Sometimes phishing is carried out by Instant messaging.

b) E-mail attachments :-

E-mail attachments are used to send malicious code to a victim's System, which will automatically gets executed.

Viruses, Worms, Trojans etc can be included cleverly into the attachments to fool a victim to open the attachments.

c) pop-up windows :-

These are similar to attachments but seperately in a pop up window. pop-up windows with Special offers or free stuff can encourage a user to unintentionally install malicious s/w.

Social Engineering Succeeds by exploting the trust of the victim. Hence continuous training / awareness sessions about such attacks are one of the effective Countermeasures.

Strict policies about Service desk staff never asking for personally Identifying Information such as username and passwords, over the phone or in person can also educate potential victims and recognize a Social engineering attempt.

2.3 Cyber Stalking:-

Cyber stalking has been defined as the use of information & communication technology, (Particularly Internet) by an individual or group of individuals to harass another individual, group of individuals or organisation.

The behaviour includes
a) false accusations
b) monitoring
c) transmission of threats
d) damage to data or equipment
e) solicitation of minors for sexual purposes

Types of Stalkers:-

1) online stalkers:- The attackers starts interaction with victim directly using Internet. E-mail and chat rooms are the most popular communication medium to get connected with victim, rather than traditional instruments like telephone/mobile.

2) Offline stalkers:- The attackers attack using traditional methods such as following the victim, watching the daily routine of the victim etc. Searching on message boards, personal websites are most common ways to gather info about victim using Internet, where victim is not aware of the upcoming attack.

The majority of cyberstalkers are men & majority of victims are women. Some cases also have been reported where women are attackers and men are victims, as well as cases of same sex cyberstalking.

In many cases, the stalker and the victim had a prior relationship, and the cyberstalking begins when the victim attempts to break off the relationship, for example ex-lover, ex-spouse, boss/subordinate & neighbour. However many instances by strangers are also there.

How Stalking works?

1) Personal info gathering about victim (Name, DOB, Cell no etc)
2) Establish a contact with victim through telephone/mobile. (or) through e-mail (Stalker may use multiple names while contact establishment)
3) once the contact was established, the stalker may make calls to the victims to threaten/harass. Sometimes repeated calls or e-mails for various kinds of favors or threaten the victim.

4) The stalker may post the victim's personal info on any website related to illicit services such as sex workers services or dating services, posing as if the victim has posted the info and invite the people to call the victim on the given contact details. The stalker will use bad/ and offensive/attractive language to invite the interested persons.

5) whosoever comes across this info, start calling the victim on the given contact details

6) Some stalkers subscribe/register the e-mail account of the victim to pornographic and sex sites because of which victim will start recieving unsolicited e-mails.

2.4 CyberCafe and CyberCrimes:-

In the past several years, many instances were reported in India, where cybercafes are used for stealing of bank p/w, subsequent fraudulent withdrawal of money, sending obscene mails to harass people, either for real or false terrorist communication.

cybercafes hold two types of risks.

First, we don't know what programs are installed on the computer (ie) risk of malicious programs such as keyloggers or spyware which may be running in the background that can capture the confidential information.

Second, over-the-shoulder peeping (shoulder surfing) can enable others to find out your passwords.

A recent survey conducted on cybercafes in one of the cities in India reveals the following facts:

1) Pirated s/w such as OS, browser, office automation s/w are installed
2) Antivirus s/w is found to be not updated
3) Several cybercafes installed "Deep Freeze" s/w for protecting their PC from malware which is a good intention, but this s/w wipe out the details of all activities carried out when 'restart' button was clicked. This practice presents challenges to police when they visit cafes to pick up clues based on IP addresses.

4) Pornographic and other indecent websites aren't blocked
5) Cafe owners have very less awareness about IT security & governance.
6) Govt/ State police/ ISP's do not seem to provide IT governance guideline to cybercafe owners.
7) police do not seem to conduct periodic visits to cybercafes.

Tips for Safety & Security while using Computer in cybercafe:

1) Always logout from e-mail / chat services / instant messengers/ or any other service that requires username & password, before leaving the system.
2) Stay with the computer while surfing/browsing. If one has to go out, logout and close all browser windows.
3) Clear history and temporary files
4) Be alert about shoulder surfing and dumpster diving
5) Avoid online financial transactions. In case of urgency, if one has to do it, then change all the p/w as soon as possible using a more trusted computer at home/ office.
6) use virtual keyboard
7) Security warnings: one should take utmost care while accessing the websites of any bank/ financial institution.

Moreover, one should not forget that whatever is applicable for cybercafes (i.e from security perspective) is also true in the case of all other public places (hotels, resorts, airport, etc.), where Internet is made available public. Hence, one should follow all tips about Security and Safety while operating the systems from publicly Connected (Wi-fi) Internet facilities.

2.5 Botnets: The fuel for cybercrime.

* A Bot is "an automated program for doing some particular task, often over a network".
* A Botnet (also called Zombie n/w) is a network of computers infected with malicious program that allows cybercriminals to control the infected machines remotely without the user's knowledge.
* Botnets are often used to conduct range of activities, from distributing spam and viruses to conducting denial-of-service (DoS) attacks.
* If someone wants to start a "business" and has no programming skills then there are plenty "Bots for sale" offers on forums.

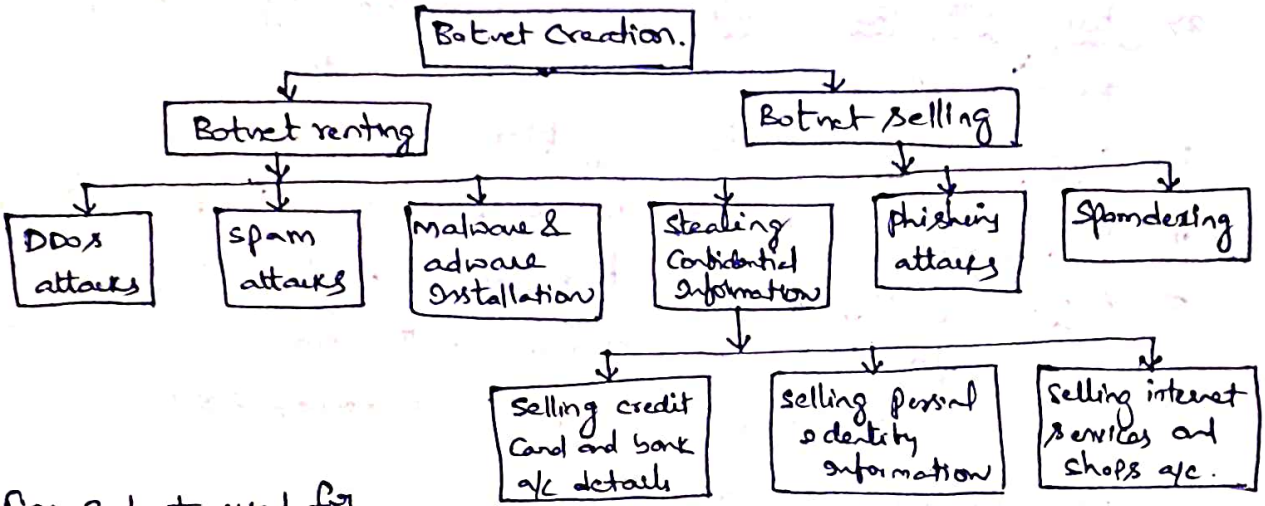

Fig:- Botnets used for gainful purposes.

* one can reduce the chances of becoming part of a bot by ensuring:

1) use antivirus and anti spyware software & keep it up to date.
2) Set the OS to download and install security patches automatically
3) Use a firewall to protect the system while it is connected to internet.
4) Disconnect the internet when you are away from your computer
5) Download the freeware only from known and trustworthy websites.
6) Check regularly the folders in mail box — "Sent items"
7) Take an immediate action if your system is infected.

2.6 Attack Vector:-

* An "attack vector" is a path or means by which an attacker can gain access to a computer or a n/w to deliver a payload or malicious outcome.
* Attack vectors enable attackers to exploit system vulnerabilities including human element.
* Attack vectors include viruses, e-mail attachments, web-pages, pop-up windows, instant messages, chat rooms, and deception. All of these involve programming except deception in which human is fooled.
* Firewalls and antivirus s/w can block attack vectors to some extent but no method is totally attack proof. Eg: Zero day attack.
* If an attack vector is thought of as a guided missile, its payload can be compared to the warhead in the tip of missile.

Some of the attack vectors are:-

1) Attack by e-mail:-
The hostile content is either embedded in the message or linked to by the message. Spam is almost always carrier for scams, fraud, dirty tricks, malicious action of some kind. Any link that offers something "free" or tempting is a suspect.

2) Attachments:- (other files):-
Malicious attachments install malicious code. The code could be a virus, trojan horse, spyware etc. Attachments attempt to install their payload as soon as you open them.

3) Attack by deception:-
Deception is used aimed at the user/operator as a vulnerable entry point. Social engineering is a form of deception which is used as an attack vector.

4) Hackers:-
Hackers use a variety of hacking tools, heuristics, and social engg to gain access to computers and online accounts.

5) Headless guests (attack by webpage):-
Counterfeit websites are used to extract personal information. Such websites look very much like the genuine websites they imitate. Pop-up webpages may install spyware, Adware & Trojans.

6) Attack of the worms:-
Many worms are delivered as e-mail attachments, but n/w worms use holes in n/w protocols directly. Any remote access service like file sharing is likely to be vulnerable to this sort of worm. In most cases, a firewall will block system worms.

A system with weak firewall is infected, and with that system other systems were effected. If the worm is successful, it propagates rapidly.

7) Malicious macros:-
Microsoft word & Excel are examples that allows macros. A macro does something like automating a spread sheet, for eg: macros can also be used for malicious purposes.

8) Foistware (sneakware):-
Foistware is the s/w that adds hidden components to the system on the sly. spyware is the most common form of foistware. Sneak s/w often hijacks your browser and diverts you to some "revenue opportunity" that the foistware has set up.

9) Viruses:-
These are malicious computer codes that hitch a ride and make the payload.

2.7 Cloud Computing:-

Cloud Computing is Internet based development and use of computer technology. It is a term used for hosted services delivered over the Internet.

A cloud service differentiates from traditional hosting in 3 ways:

1) It is sold on demand - typically by the minute or the hour
2) It is elastic in terms of usage - a user can have as much or as little as he/she wants at any given time.
3) The service is fully managed by provider - user just needs pc & Internet.

Why Cloud Computing?

1) Applications & data can be accessed from anywhere at any time. Data may not be held on a hard drive of one user's computer.
2) It could bring hardware costs down.
3) No need to buy a set of software licences for every employee as organization pays a metered fee to a cloud computing company.
4) No need to rent a physical space to store servers & databases.

The cloud computing services can be either private or public. A public cloud sell services to anyone on internet. A private cloud supplies the hosted services to limited people. When a service provider uses public cloud resources to create a private cloud, it is "virtual private cloud".

Various cloud computing service providers are

1) Amazon
2) 3Tera
3) Force.com
4) Appistry CC middleware
5) AppNexus
6) Google App Engine
7) GoGrid
8) Flexiscale

Types of services: Service provided by CC are as follows:

1) **Infrastructure-as-a-service (IaaS):** It is like Amazon web services that provide virtual servers with unique IP addresses and blocks of storage on demand. Customers benefit from an API from which they can control their servers. This service also called utility computing.

2) Platform-as-a-service (PaaS) :- It is a set of s/w & development tools hosted on the provider's servers. Developers can create application using the provider's APIs. Google Apps is one of the most famous PaaS providers.

3) Software-as-a-service (SaaS) :- It is the case where provider allows the customer only to use its application. The s/w interacts with the user through a user interface. These appn's can be anything from web based mail to appn's such as twitter, 98.6 fm etc.

Cybercrime & Cloud Computing :-

The prime area of the risk in cloud computing is protection of user data.

Area	What is the Risk?	How to remediate the risk?
1. Elevated user access	Any data processed outside the organization with it an inherent level of risk, as outsourced services may bypass the physical, logical and personnel controls.	Customer should obtain as much info as he/she can about the service provider who will be manging the data.
2. Location of the data	The organizations obtaining cloud service may not be aware about where the data is hosted and may not even know in which country it was hosted	Organizations should ensure that service provider is committed to obey local privacy requirements on behalf of organization to store and process data in specific jurisdictions.
3. Segregation of data	As the data is stored under a common environment, encryption mechanism should be strong enough to segregate the data from other organizations, whose data also stored under same server.	The service provider should display encryption schemes and testing of mechanism by the experts.
4. Recovery of Data	Business continuity in case of any disaster is a great risk.	Service provide should ensure the organisation about complete restoration of data within the stipulated timeframe.
5. Info security violation	Due to complex IT environment and several customers logging in & logging out of the hosts, it becomes difficult to trace inappropriate and/or illegal activity.	Organizator should enforce the contracted liability toward providing security violation logs at frequent intervals.