Unit 2

Web jacking :-

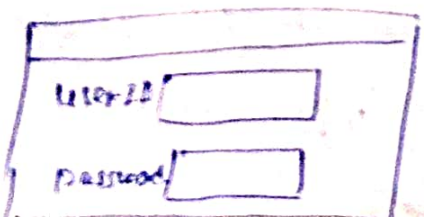
The name web jacking derived from the word aeroplane hijacking. This method is used in social media where ~~taker~~ hacker takes control of a website fraudulently. It can be done by either changing the content of the original site or even redirect the user to another fake similar looking page control by him. In web jacking owner of the website has know control and the attacker may use the web site for his own selfish interest or fulfilling political objectives for money. there are many cases where the attacker has asked for ransom and even posted obscence material on the site. A clone of the web site can be created by using the web Jacking method and it can be presented to the victim with the new link saying that the site has moved.

Key point :-

1) The term web jacking is derived from term hijacking.
2) In those the hacker gains access and control over the website of another forcefully.
3) The hacker can also change the content of information on the site.
4) This may be done for fulfilling political objective or for money.
5) Eg :- The site of MIT (ministery of IT) and site of bombay crime was web jacked.

There are many ways that hacker can use to know password cracking is most common where a cracking s/w is used to guess password.

→ Brute force technique.
→ Dictionary technique.

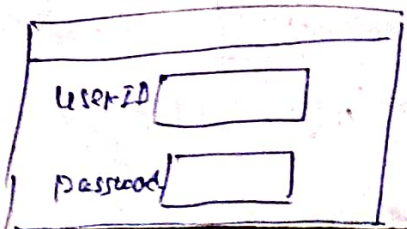


Key point:

1) The term web jacking is derived from term hijacking.
2) In those the hacker gains access and control over the website of another forcefully.
3) The hacker can also change the content or information on the site.
4) This may be done for fulfilling political objective or for money.
5) Eg:- The site of MIT (ministery of IT) and site of bombey crime was web jacked.

There are many ways that hacker can use to know password cracking is most common where a cracking s/w is used to guess password.

→ Brute force technique.
→ Dictionary technique.



Online Fraud :-

→ online fraud involves using online services and s/w. with access to internet to commit fraud and take the advantage of victims.

Tools used for online fraud!

1) Email.
2) Chat rooms.
3) Web sites
4) message board.

Online fraud that target victim can gain million of dollers through fraudulant activity every year.

Types of internet Fraud!-

(1) spoofing / phishing :-

spoofing is the act of sending communication with fraudulant sender addres

(2) Auction fraud:

In this auction frauds people encouraged to participate in online auction and when money must das been paid for specific items. the fraudster would send either a lower standard or not send.

(3) Data breach!. (online data lick)

Stealing confidential data, protected sensitive data from a source. location and mooving it into a untrusted or unauthorized environment. this data which are moving in unsafe environment. this data may be misused by unauthorized person.

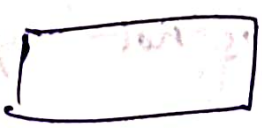
(4) Identity theft:-

Identity theft also known as "Identity fraud." is a crime in which an imposter obtain personal or financial information of another person to use their identity commit fraud.

Imposter = fraud person.

(5) Denial of service attack:-

A denial of service attack is a tactic युक्ति overloading a machine or network to make it unavailable to actual users.



Flipcart

Amazon.

A hacker can achive it by more trafic

than the target machine can handle causing to fail.

DoS! Example: overloading shopping website on festive season by competitors.

S/w piracy (चोरी)

S/w piracy is the act of illegally using, copying, modifying, distributing, sharing or selling computer s/w protected by copyright laws. A s/w pirate is any one who intentionally or unintentionally commits these illegal acts.

S/w piracy can be defined as the use of s/w that is not properly licensed.

→ s/w piracy has been worst problem. s/w company facing todays.

⇒ s/w piracy is a crime defined as illegal copying downloading, sharing and installing of copyrighted s/ws.

→ The majority of s/w today are purchased as end user license. ie. only one authorized user can use it in one or more machines.

→ making multiple copy and sharing it with friends or families is also considered to be violation of terms and conditions.

s/w piracy in different forms:

Unauthorized copy can be done for different purposes such as personal use, business use. an even selling as copy of pirated s/ws.

There are 6 form of s/w piracy.

1) Soft lifting :- → Soft lifting is an act of illegal copy of s/w and distributing it to friends ~~are~~ or organizations.

→ many personal users and enterprises are doing it knowingly and ~~unknowingly~~ unknowingly.

→ Such activities leads s/w companies to loose billions of ~~dollar~~ dollars every year.

→ It often happens when organization purches one legal license of s/w and install it on several machines.

(2) Internet piracy :-

→ Internet piracy is one of the ~~fast~~ fastest and eisiest way to receive

Q1 what is s/w piracy.

Q2 Different forms of s/w piracy.

Q3 major factor behind s/w piracy.

Pirated s/w.

→ there are several websites that makes s/w available for free down load.

→ many users download the pirated s/w from websites itself. and there is no need to copy the s/w in CD Rom or floppy disk.

(3) counter feiting!.

(4) End user piracy.

(5) Hard disk piracy.

(6) Client server overuse.

(3) Counter feiting s/w piracy:-

counterfeiting means

Producing face copies of a s/w, making it look authentic. this involves. providing the box, CD, and manuals all designed to look as much like the original product as possible. Microsoft products are the one most commonly counterfieted. because of their widespread use.

(4) End user piracy:-

This occurs when an individual reproduces. copies of s/w. without authorization. these include using one licensed copy to install a program on multiple computers. Copying discs for installation or distribution. In other word end customer is the last consumer of a product or service.

Start → cmd → run as administrator → SLMGR. / XPR

window khulega → volume activate date expire

than s/w is piracy.

inorder to develop successfull products or service. business must identifying and find way to solve customer needs.

(5) Hard disk piracy:-

Another s/w piracy example is known as hard loading. This is the name given to one of the types of s/w piracy that happens when a business installs unauthorized copies of s/w onto the hard disk of any computers it sells.

Client server over use:-

This type of piracy occurs when too many users on a n/w are using a central copy of a program at the same.

If you have a local area n/w and install program on the server for several people to use you have to be sure you licence entitles you to do so.

Computer Network Intrusions :- (अनधिकृत घुसपैठ)

→ A network intrusion is any illegal activity that is ~~~~ carried out in a digital netwok. ic called computer network intrusion,

→ The computer ~~intr~~ network intrusion always effect the security of data and network

→ To deal with network intrusion, organization must have. cyber security team to detect and prevent from intrusions.

Computer network intrusion are done

→ Steal or destroy personal Information

→ Attacks are made to obtain access to internal system.

→ Financial loss to organization.

To save the network from harmful activity, Intrusion detection system (IDS) need to be installed in n/w or any system.

Computer Network Intrusion techniques: IDS

1) multi Routing.

This method is also called Asymmetric Routing. In this technique, intrusion use multiple routes to intrude targeted device or n/w.

→ This allows them to avoiding detected by intrusion detection system - as most of the packets in the network - are suspicious. Some packets bypass certain network segments.

SMTP

→ Simple mail transfer protocol.

ARP → Address resolution protocol.

(2) Buffer overflow attack:

→ In this technique the intruder override any specific part of computer memory of targeted device.

→ The intruder insert harmful commands which are harmful for the targated computer.

→ To prevent this effect network designers need to install boundry checking logic that identifies block executable code to be written in memory..

3) Protocol specific attack :-

→ To transmit data from one computer to another computer, computer needs to follow certain set of rules and regulation. These set of rules and regulation is called protocols.

→ Some protocols are SMTP, ARP, IP, TCP, UDP etc.

→ This protocol has certain loopholes which give chance for ~~intruder~~ intruder to attack.

Example : SMTP protocol — used in mailing, and ARP protocol does not provide any authentication mechanism.

Smtp (simple mail transfer protocol)
ARP (Address Resolution protocol)
IP (Internet protocol) TCP → Transmission control protocol.
UDP (User Data gram Protocol)

4) Traffic Flooding:-

In this technique attacker create too large traffic which can not be handled by network system. this would then create confusion and congestion in network environment as a result some unauthorized activity can possible.

Password sniffing (सूँघना):-

→ Password sniffing is an attack on the internet that is used to steal username and password from the network

→ It was the worst security problem on the internet in 1990.

→ Password sniffing can also be termed as network sniffing.

→ It is act of intercepting, monitoring and capturing of data packets in traffic of a N/W specially in LAN.

→ The motive of N/W sniffing is to steal info such as username password, n/w message etc.

→ The password sniffing problem was mostly solved by SSH. which replaced several prior insecure protocols.

→ many development have made password sniffing difficult besides adding encryption.
→ SSH (Secure shell protocol)

Virtual crime:-

→ The increasing popularity of online world or virtual world (metaverse) leads to the debate of whether there are such things as virtual crime.

→ The virtual crime has evolved from relatively to huge and popular graphics based (online game) online games) AVTAR games such as "second life" and world of war craft".

→ Given the million of people are participating in online ~~forms~~ forums. it give room to crime. people can harm ~~each other~~ abuse each others's Avaturs.

→ The issue first comes to the picture some years ago in an online community. "Lambdamoo" text based virtual community

where member can create their own character and interact with text based commands.

→ The criminal law addresses physical conduct & in virtual world no one is harmed physically.

→ How much harmfull is the virtual crime totally depend on ~~the crime~~ the perception of users.

1) Internal perception :- (View point of user)

these are those perception in which user can create their own AVTAR. and communicate to other by through text.

2) External perception (View point of outsiders)

The virtual crime falls under one of the bellow three categories.

1) Virtual murder.
2) offenses against property.
3) Virtual property.

Perception of cyber criminals :-

(1) Hackers :-

→ The meaning of the word hacker has been changed over the years with the change of technology.

→ The people who were highly knowledgeable about computing, were considered as hackers.

→ The process of gaining unauthorized access into a computer system for different purpose is known as hacking.

→ Hacking has been used as a political or social demonstration during International crises.

→ These are different types of hackers based on phenomena.

(i) Crackers

(ii) Hacktivists.

(iii) cyber terrorists

→ There are different types of hackers.

(i) Black Hat Hackers.

(ii) White hat hackers

(iii) Gray hat hackers

(iv) Suicide hackers.

→ Black hat Hacker:-

Black hats are the bad guys. the milicious hackers are crackers who use their skills for illegal purposes.

→ White Hat hackers :.

White hat hackers are group considers itself to be the good guys. White hat hackers have very good knowledge about networking, programming etc.

→ Grey hat hackers!.

Grey hat hacker are those hackers who may work offensively or defensively depending on situation.

Hacking of web servers:-

→ The term server is related to hardware and software so there are two meaning as hacking web server.

→ In hardware context- a web server is a virtual program. that run on a computer to deliver the content- such as web page & documents using HTTP over the www.

→ A web server is used to provide various types of services such as sending and receiving emails, downloading request for a file and even more.

→ There are following possible method to hack web servers.

(i) Types of web server vulnerabilities
(ii) Web server defacement
(iii) IIS exploit (internet information servers)
(iv) Web server protection checklist.

Session Hijacking :-

→ TCP session hijacking is a security attack on a user session over a protected network.

→ The most common method of session hijacking is called IP spoofing.

→ This type of attack is possible because authentication typically is only done at the start of a TCP session.

→ Different way of session hijacking

(i) Using packet sniffers

(ii) Cross site scripting (XSS Attack)

(iii) IP spoofing

(iv) Blind attack