RGPVNOTES.IN

Program : **B.Tech**

Subject Name: **Cyber Security**

Subject Code: **CS-503**

Semester: **5th**

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in

RGPVNOTES.IN

**Unit-2**

**Topics to be covered**

*UNIT 2*

*Web jacking, Online Frauds, Software Piracy, Computer Network Intrusions, Password Sniffing, Identity Theft, cyber terrorism, Virtual Crime, Perception of cyber criminals: hackers, insurgents and extremist group etc. Web servers were hacking, session hijacking.*

---------------------------------------------------------------------------------------------------------------------------------------

**Web Jacking-** The Web Jacking Attack Vector is another phishing technique that can be used in social engineering engagements. Attackers that are using this method are creating a fake website and when the victim opens the link a page appears with the message that the website has moved and they need to click another link. If the victim clicks the link that looks real he will redirected to a fake page.

Web jacking is same as like web hijacking but the difference between web jacking and hijacking is in web jacking attack methodhackers compromised with the domain name system but in hijacking they take a full control over the website.

**Web jacking attack method** is another type of social engineering phishing attackwhere an attacker creates a fake web page of victim website and sends it to the victim. And when a victim click on that link, a message display on the browser "the site abc.com has move on another address, click here to go to the new location" and if a victim does click on the link, he/she will redirect on the fake website page where an attacker can ask for any sensitive data such as credit card number, username, password etc. Web jacking attack method is one kind of trap which is speeded by the attacker to steal the sensitive data of any people, and those people got trapped who are not aware about cyber security. And web jacking attack method is very common phishing attack nowadays, so if a people have even a little knowledge about cyber security, those people will never get trap.

RGPVNOTES.IN

The process of web jacking attack method:

- The first step of web jacking attack method is to create a fake page of victim website.
- The second step is to host it either on your local computer or shared hosting.
- The third step is to send the link of a fake page to the victim.

The fourth step victim will open the link and enter their details and submit. And in last step, you will get all the details submitted by victim.

**Online Frauds -** Fraud that is committed using the internet is "online fraud." Online fraud can involve financial fraud and identity theft. The most common types of online fraud are called phishing and spoofing.

**Online Scams-**Online scam is an attempt to trap you for obtaining money. There are many types of online scams; this includes obtaining money with fake names, fake photos, fake e-mails, forged documents, fake job offers and many more.

Generally, it happens by sending fake e-Mails for your personal details like online banking details, credit carddetails. Sometimes e-Mails are sent from lottery companies with fake notice, whenever you participate in online auction and e-Mails received for fake gifts.

**Phishing scam-**Online scammers send you an e-mail and ask your account information or credit card detailsalongwith a link to provide your information. Generally, the links sent will be similar to your bank. So whenever you post your details in the link then the details will be received by scammers and money is misused.

**Lottery scam-**Sometimes you receive an email like "you won a lottery of million dollars" receiving such a kind of mails is a great thing, and really it's a happiest thing. By responding to such a kind of mails huge

RGPVNOTES.IN

amount of money will be lost. Because these e-Mails are not true, scammers try to fool and trap you to obtain money.

**Online Auction-** If you bid for a product you never get the product promised or don't match the product, and the description given to you may be incomplete, wrong, or fake. The scammer accepts the bid from one person and goes for some other sites where they can get less than the winning bid so scammers may not send the product you wanted.

**Forwarding Product or Shipping Scam-**Whenever you answer an online advertisement for a letter or e-mail manager like some US based corporation which lacks address or bank details and needs someone to take goods and sent to their address or ship overseas, and you are asked to accept the transfers into your bank. Generally, it happens for products that are purchased using stolen credit cards and shipped to your address and then you will be fooled and asked to reship the product to others they might have deceived, who reship the product overseas. The stolen money will be transferred to your account.

**E-mail Scam Like --Congratulations you have won Webcam, Digital Camera, etc.-**Sometimes you get an e- mail with a message like -- you have won something special like digital camera webcam , all you need to do is just visit our web site by clicking the link given below and provide your debit or credit card details to cover shipping and managing costs. However the item never arrives but after some days the charges will be shown on your bank account and you will lose money.

**By E-mails-** Generally, fraudsters send you an e-mail with tempting offers of easy access to a large sum ofmoney and ask you to send scanned copies of personal documents like your address proof, passport details and ask you to deposit an advance fee for a bank account. So once you deposit the funds, they take money and stop further communication, leaving you with nothing in return.

RGPVNOTES.IN

**Unscrupulous Websites for Income Tax Refund-** Generally, websites feel like official websites and seek the details of credit card, CVV PIN of ATM and other personal details of the taxpayers in the name of crediting income tax refund through electronic mode.

**E-commerce/ Investment Frauds -** An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered. The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.

**Software Piracy** - Software piracy refers to the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. These kind of crimes also include copyright infringement, trademarks violations, theft of computer source code, patent violations etc.

**Denial of service Attack**- This is an attack in which the criminal floods the bandwidth of the victim network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide. This kind of attack is designed to bring the network to crash by flooding it with useless traffic.

**Sale of illegal articles-** This category of cybercrimes includes sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication.

Get real-time updates from RGPV

**Cyber Defamation-** When a person publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person friends, it is termed as cyber defamation.

**Forgery -** Computers, printers and scanners are used to forge counterfeit currency notes, postage and revenue stamps, mark sheets etc. These are made using computers, and high quality scanners and printers.

**Theft of information contained in electronic form-** This includes theft of information stored in computer hard disks, removable storage media etc.

- Internet time theft - Internet time refers to usage by an unauthorized person of the Internet hours paid for by another person.
- Theft of computer system - This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.
- Physically damaging a computer system- This crime is committed by physically damaging a computer or its peripherals.
-

**Breach of Privacy and Confidentiality -** Privacy refers to the right of an individual/s to determine when, how and to what extent his or her personal data will be shared with others. Breach of privacy means unauthorizeduse or distribution or disclosure of personal information. Confidentiality means non-disclosure of information to unauthorized or unwanted persons. In addition to Personal information some other type of information which useful for business and leakage of such information to other persons may cause damage to business or person, such information should be protected.

**Computer Network Intrusions-** A network intrusion is any unauthorized activity on a computer network. In most cases, such unwanted activity absorbs network resources intended for other uses, and nearly always threatens the security of the network and/or its data.

**Intrusion Detection System –** An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. While anomaly detection and reporting is the primary function, some intrusion detection systems are capable of taking actions when malicious activity or anomalous traffic is detected, including blocking traffic sent from suspicious IP addresses.

**Different types of intrusion detection systems**-Intrusion detection systems come in different flavors and detect suspicious activities using different methods, including the following:

- **Network intrusion detection system-** (NIDS) is deployed at a strategic point or points within the network, where it can monitor inbound and outbound traffic to and from all the devices on the network.
- **Host intrusion detection systems-** (HIDS) run on all computers or devices in the network with direct Access to both the internet and the enterprise internal network. HIDS have an advantage over NIDS in That they may be able to detect anomalous network packets that originate from inside the organization or malicious traffic that a NIDS has failed to detect. HIDS may also be able to identify malicious traffic that Originates from the host itself, as when the host has been infected with malware and is attempting to spread to other systems.
- **Signature-based intrusion detection systems** – It monitors all the packets traversing the network and Compares them against a database of signatures or attributes of known malicious threats,much like antivirus software.
- **Anomaly-based intrusion detection systems** - It monitor network traffic and compare it against an Established baseline, to determine what is considered normal for the network with respect to bandwidth, Protocols, ports and other devices. This type of IDS alerts administrators to potentially malicious activity.

**Password Sniffing**- A password sniffer is a software application that scans and records passwords that are used or broadcasted on a computer or network interface. It listens to all incoming and outgoing network traffic and records any instance of a data packet that contains a password. A password sniffer installs on a host machine and scans all incoming and outgoing network traffic.

**Identity Theft-** Identity theft is the unauthorized collection of personal information and its subsequent use for criminal reasons such as to open credit cards and bank accounts, redirect mail, set up cell phone service, rent vehicles and even get a job. These actions can mean severe consequences for the victim, who will be left with bills, charges and a damaged credit score.

**Cyber Terrorism -** Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc.At this juncture a necessity may be felt that what is the need to distinguish between cyber terrorism and cyber-crime. Both are criminal acts. However there is a compelling need to distinguish between both these crimes. A cyber-crime is generally a domestic issue, which may have international consequences; however cyber terrorism is a global concern, which has domestic as well as international consequences. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate emails, attacks on sensitive computer networks, etc. Technology savvy terrorists are using 512-bit encryption, which is next to impossible to decrypt. The recent example may be cited of – Osama Bin Laden, the LTTE, and attack on America's army deployment system during Iraq war.
Cyber terrorism may be defined to be " the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives" (4). Another definition may be attempted to cover within its ambit every act of cyber terrorism.
A terrorist means a person who indulges in wanton killing of persons or in violence or in disruption of servicesor means of communications essential to the community or in damaging property with the view to –

- Putting the public or any section of the public in fear; or
- Affecting adversely the harmony between different religious, racial, language or regional groups or castesor communities; or
- Coercing or overawing the government established by law; or
- Endangering the sovereignty and integrity of the nation and a cyber-terrorist is the person who uses thecomputer system as a means or ends to achieve the above objectives. Every act done in pursuance thereof isan act of cyber terrorism.

**Virtual Crime-** Virtual crime or in-game crime refers to a virtual criminal act that takes place in a massively multiplayer online game (MMOG), usually an MMORPG. The huge time and effort invested into such games can lead online "crime" to spill over into real world crime, and even blur the distinctions between the two.

**Perception of cyber criminals: Hackers, insurgents and extremist group-**

- Hacker and attackers groups are any skilled computer expert that uses their technical knowledge to overcome a problem. While hacker can refer to any skilled computer programmer, the term has become associated in popular culture with a security hacker, someone who, with their technical knowledge, uses bugs or exploits to break into computer systems.
- Four primary motives have been proposed as possibilities for why hackers attempt to break into computers and networks.
- There is a criminal financial gain to be had when hacking systems with the specific purpose of stealing credit card numbers or manipulating banking systems.

- Many hackers thrive off of increasing their reputation within the hacker subculture and will leave their handles on websites they defaced or leave some other evidence as proof that they were involved in a specific hack.
- Corporate espionage (Spy) allows companies to acquire information on products or services that can be stolen or used as leverage within the marketplace.
- State-sponsored attacks provide nation states with both wartime and intelligence collection options conducted on, in, or through cyberspace.

**Prevention of Cyber Crime:**

Prevention is always better than cure. It is always better to take certain precaution while operating the net. Ashould make them his part of cyber life. Saileshkumar Zarkar, technical advisor and network securityconsultant to the Mumbai Police Cyber-crime Cell, advocates the 5P mantra for online security: Precaution,Prevention, Protection, Preservation and Perseverance. A netizen should keep in mind the following things-

- To prevent cyber stalking avoid disclosing any information pertaining to oneself. This is as good as disclosing your identity to strangers in public place.
- Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
- Always use latest and update antivirus software to guard against virus attacks.
- Always keep back up volumes so that one may not suffer data loss in case of virus contamination
- Never send your credit card number to any site that is not secured, to guard against frauds.
- Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.
- It is better to use a security program that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.
- Website owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
- Use of firewalls may be beneficial.
- Web servers running public sites must be physically separate protected from internal corporate network.

**Web Servers Hacking**

A web server is a program that stores files (usually web pages) and makes them accessible via the network or the internet. A web server requires both hardware and software. Attackers usually target the exploits in the software to gain authorized entry to the server. Let's look at some of the common vulnerabilities that attackers take advantage of.

- **Default settings**– These settings such as default user id and passwords can be easily guessed by the attackers. Default settings might also allow performing certain tasks such as running commands on the server which can be exploited.
- **Misconfiguration operating systems and networks** – certain configuration such as allowing users to execute commands on the server can be dangerous if the user does not have a good password.
- **Bugs in the operating system and web servers–** discovered bugs in the operating system or web server software can also be exploited to gain unauthorized access to the system.
- **Lack of security policy and procedures**– lack of a security policy and procedures such as updating antivirus software, patching the operating system and web server software can create securityloop holes for attackers.

**Types of Web Servers-**The following is a list of the common web servers.

- **Apache–** This is the commonly used web server on the internet. It is cross platform but is it'susually installed on Linux. Most PHP websites are hosted on Apache servers.

- **Internet Information Services (IIS) – It** is developed by Microsoft. It runs on Windows and is the second most used web server on the internet.  Most asp and aspx websites are hosted on IIS servers.
- **Apache Tomcat** – Most Java server pages (JSP) websites are hosted on this type of web server.
- **Other web servers –** These include Novell's Web Server and IBM's Lotus Domino servers.

**Types of Attacks against Web Servers**

- **Directory traversal attacks**– This type of attacks exploits bugs in the web server to gain unauthorized access to files and folders that are not in the public domain. Once the attacker has gained access, they can download sensitive information, execute commands on the server or install malicious software.
- **Denial of Service Attacks–** With this type of attack, the web server may crash or becomeunavailable to the legitimate users.  One of the ways to deploy denial of service attack is to flood syn request to server we will discuss this attack thoroughly in next unit.

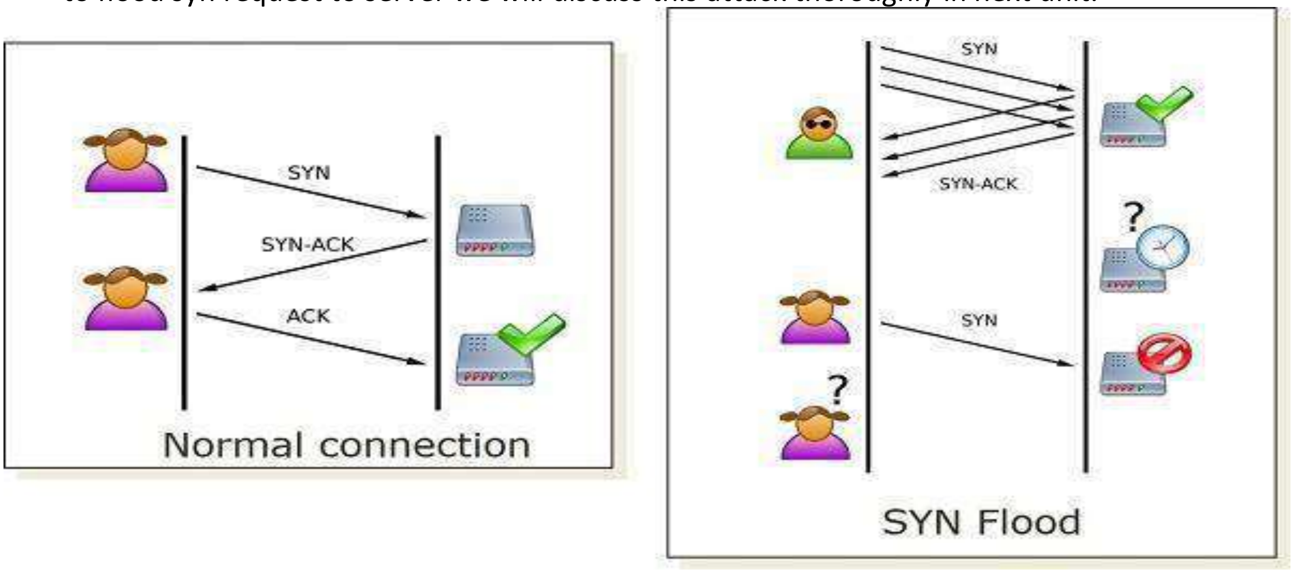

**Figure 2.1: Denial of Service Attacks**

- **Domain Name System Hijacking** – With this type of attacker, the DNS setting are changed to point to the attacker's web server.  All traffic that was supposed to be sent to the web server is redirected to the wrong one.
- **Sniffing**– Unencrypted datasent overthe network may be intercepted and used to gainunauthorized access to the web server.
- **Phishing–** With this type of attack, the attack impersonates the websites and directs traffic to the fake website. Unsuspecting users may be tricked into submitting sensitive data such as login details, credit card numbers, etc.
- **Pharming**– With this type of attack, the attacker compromises the Domain Name System (DNS)servers or on the user computer so that traffic is directed to a malicious site.
- **Defacement**– With this type of attack, the attacker replaces the organization's website with a different page that contains the hacker's name, images and may include background music and messages.

**Effects of successful attacks**

- An organization's reputation can be ruined if the attacker edits the website content and includes malicious information or links to a porn website.
- The web server can be used to install malicious software on users who visit the compromised website.
- The malicious software downloaded onto the visitor's computer can be a virus, Trojan or BotnetSoftware, etc.

- Compromised user data may be used for fraudulent activities which may lead to business loss or lawsuits from the users who entrusted their details with the organization.

**Session hijacking**

Session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session— sometimes also called a session key—to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer.

In other words, The Session Hijacking attack consists of the exploitation of the web session controlmechanism, which is normally managed for a session token. Because http communication uses many different TCP connections, the web server needs a method to recognize every user's connections. The most useful method depends on a token that the Web Server sends to the client browser after a successful client authentication.

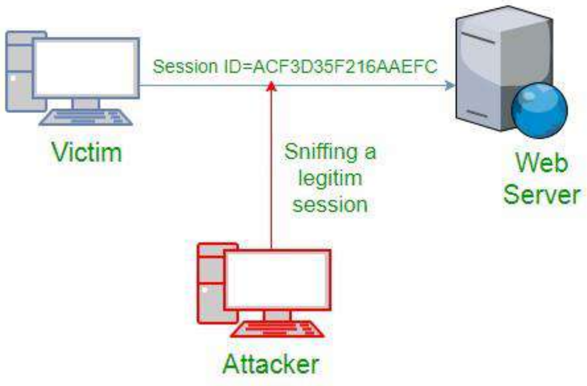

**Figure 2.2: Session Hijacking**

A session token is normally composed of a string of variable width and it could be used in different ways, likein the URL, in the header of the http requisition as a cookie, in other parts of the header of the http request, or yet in the body of the http requisition.

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in