RGPVNOTES.IN

Program : **B.Tech**

Subject Name: **Cyber Security**

Subject Code: **CS-503**

Semester: **5th**

Unit-5

Topics to be covered

UNIT 5

Tools and Methods in Cybercrime: Proxy Servers and Anonymizers, Password Cracking, Key loggers and Spyware, virus and worms, Trojan Horses, Backdoors, DoS and DDoS Attacks , Buffer and Overflow, Attack on Wireless Networks, Phishing : Method of Phishing, Phishing Techniques.

Proxy Servers

A proxy server is a server (a computer system or an application) that acts as an intermediary for requestsfrom clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Proxies were invented to add structure and encapsulation to distributed systems. Today, most proxies are web proxies, facilitating access to content on the World Wide Web, providing anonymity and may be used to bypass IP address blocking.

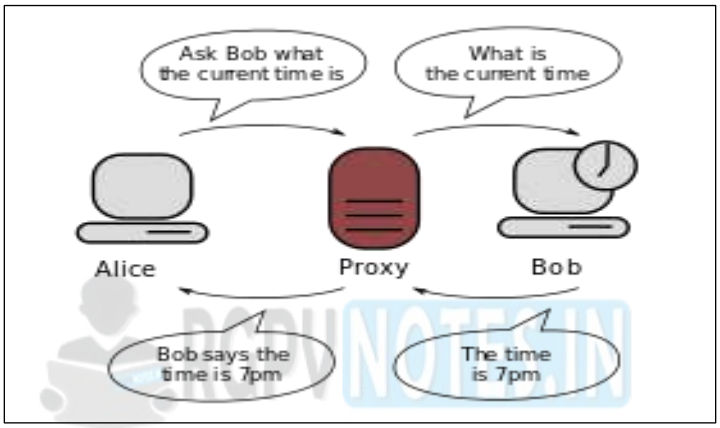

Figure5.1: Communication between two computers connected through a third computer acting as a proxy. Bob does not know to whom the information is going, which is why proxies can be used to protect privacy.

Anonymizers- An Anonymizers or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet. It accesses the Internet on the user's behalf, protecting personal information by hiding the client computer's identifying information. There are many reasons for using Anonymizers. Anonymizers help minimize risk. They can be used to prevent identity theft, or to protect search histories from public disclosure.

Some countries apply heavy censorship on the internet. Anonymizers can help in allowing freeaccess to all of the internet content, but cannot help against persecution for accessing the Anonymizers website itself. **Password Cracking**

Password cracking is the process of recovering passwords from data that have been stored in ortransmitted by a computer system. A common approach (brute-force attack) is to try guesses repeatedly for the password and check them against an available cryptographic hash of the password.

The purpose of password cracking might be to help a user recover a forgotten password (installing an entirely new password is less of a security risk, but it involves System Administration privileges), to gain unauthorized access to a system, or as a preventive measure by system administrators to check for easily crackable passwords. On a file-by-file basis, password cracking is utilized to gain access to digital evidence for which a judge has allowed access but the particular file's access is restricted.

Password cracking refers to various measures used to discover computer passwords. This is usuallyaccomplished by recovering passwords from data stored in, or transported from, a computer

system. Password cracking is done by either repeatedly guessing the password, usually through a computer algorithm in which the computer tries numerous combinations until the password is successfully discovered.

Password cracking can be done for several reasons, but the most malicious reason is in order to gain unauthorized access to a computer without the computer owner's awareness. This results in cybercrime such as stealing passwords for the purpose of accessing banking information.

Key loggers-A Key loggers is a piece of software — or, even scarier, a hardware device — that logs every key you press on your keyboard. It can capture personal messages, passwords, credit card numbers, and everything else you type.

Key loggers are generally installed by malware, but they may also be installed by protective parents, jealous spouses, or employers who want to monitor their employees. Hardware Key loggers are perfect for corporate espionage.

Key loggers can pose a serious threat to users, as they can be used to intercept passwords and other confidential information entered via the keyboard. As a result, cybercriminals can get PIN codes and account numbers for your financial accounts, passwords to your email and social networking accounts and then uses this information to take your money, steal your identity and possibly extort information and money from your friends and family.

Spyware- Spyware is the term given to a category of software which aims to steal personal or organizational information. It is done by performing a set of operations without appropriate user permissions, sometimes even covertly. General actions a spyware performs include advertising, collection of personal information and changing user configuration settings of the computer.

A Spyware is generally classified into adware, tracking cookies, system monitors and Trojans.

The most common way for a spyware to get into the computer is through freeware and shareware as a bundled hidden component. Once a spyware gets successfully installed, it starts sending the data from that computer in the background to some other place.

These days' spywares are usually used to give popup advertisements based on user habits andsearch history. But when a spyware is used maliciously, it is hidden in the system files of thecomputer and difficult to differentiate.

One of the simplest and most popular, yet dangerous is Key loggers. It is used to record the keystrokes which could be fatal as it can record passwords, credit card information etc. In someshared networks and corporate computers, it is also intentionally installed to track user activities.

Presence of spyware in a computer can create a lot of other troubles as spyware intended to monitor the computer can change user preferences, permissions and also administrative right s, resulting in users being locked out of their own computer and in some cases, can also result in full data losses. Spyware running in the background can also amount to increased number of processes and result in frequent crashes. It also often slows down a computer.

Virus- A computer virus is malicious code that replicates by copying itselfto another program, computerboot sector or document and changes how a computer works. The virus requires someone to knowingly or unknowingly spread the infection without the knowledge or permission of a user or system administrator.

A virus can be spread by opening an email attachment, clicking on an executable file, visiting an infected website or viewing an infected website advertisement. It can also be spread through infected removable storage devices, such USB drives. Once a virus has infected the host, it caninfect other system software or resources modify or disable core functions or applications, as well as copy, delete or encrypt data. Some viruses begin replicating as soon as they infect the

host, while other viruses will lie dormant until a specific trigger causes malicious code to be executed by the device or system.

Types of viruses

- **File infectors-** Some file infector viruses attach themselves to program files, usually selected.com or .exe files. Some can infect any program for which execution is requested, including .sys,.ovl, .prg, and .mnu files. When the program is loaded, the virus is loaded as well. Other file infector viruses arrive as wholly contained programsor scripts sent as an attachment to an email note.
- **Macro viruses**- These viruses specifically target macro language commands in applications like Microsoft Word and other programs. In Word, macros are saved sequences for commands or keystrokes that are embedded in the documents. Macro viruses can add their malicious code to the legitimate macro sequences in a Word file. Microsoft disabled macros by default in more recent versions of Word; as a result, hackers have used social engineering schemes to convince targeted users to enable macros and launch the virus. As macro viruses have seen a resurgence in recent years, Microsoft added a new feature in Office 2016 that allows security managers to selectively enable macro use for trusted workflows only, as well as block macros across an organization.
- **Overwrite viruses-** Some viruses are designed specifically to destroy a file or application's data.After infecting a system, an overwrite virus begins overwriting files with its own code. These viruses can target specific files or applications or systematically overwrite all files on an infected device. An overwrite virus can install new code in files and applications that programs them to spread the virus to additional files, applications and systems.
- **Polymorphic viruses-**A polymorphic virus is a type of malware that has the ability to change or mutate its underlying code without changing its basic functions or features. This process helps a virus evade detection from many antimalware and threat detection products that rely on identifying signatures of malware; once a polymorphic virus' signature is identified by a security product, the virus can then alter itself so that it will no longer be detected using that signature.
- **Resident viruses**-This type of virus embeds itself in the memory of a system. The original virus program isn't needed to infect new files or applications; even if the original virus is deleted, the version stored in memory can be activated when the operating system loads a specific application or function. Resident viruses are problematic because they can evade antivirus and antimalware software by hiding in the system's RAM.
- **Rootkit viruses**-A Rootkit virus is a type of malware that installs an unauthorized rootkit on an infected system, giving attackers full control of the system with the ability to fundamentally modify or disable functions and programs. Rootkit viruses were designed to bypass antivirus software, which typically scanned only applications and files. More recent versions of major antivirus and antimalware programs include rootkit scanning to identify and mitigate these types of viruses.
- **System or boot record infectors**-These viruses infect executable code found in certain system areas on a disk. They attach to the DOS boot sector on diskettes and USB thumb drives or the Master Boot Record on hard disks. In a typical attack scenario, the victim receives storage device that contains a boot disk virus. When the victim's operating system is running, files on the external storage device can infect the system; rebooting the system will trigger the boot disk virus. An infected storage device connected to a computer can modify or even replace the existing boot code on the

infected system so that when the system is booted next, the virus willbe loaded and run immediately as part of the master boot record. Boot viruses are less common now as today's devices rely less on physical storage media.

Worms- A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Worms almost always cause at least some harm to the network, even ifonly by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Trojan Horses- A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. Once activated, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system. These actions can include:

- Deleting data
- Blocking data
- Modifying data
- Copying data
- Disrupting the performance of computers or computer networks. Unlike computer viruses and worms, Trojans are not able to self-replicate.

Backdoors- A backdoor is a malware type that negates normal authentication procedures to access a system. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware. Backdoor installation is achieved by taking advantage of vulnerable components in a web application. Once installed, detection is difficult as files tend to be highly obfuscated. Webserver backdoors are used for a number of malicious activities, including:

- Data theft
- Website defacing
- Server hijacking
- The launching of distributed denial of service (DDoS) attacks
- Infecting website visitors (watering hole attacks)

DoS Attack- A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy.

DDoS Attack- A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, frombanks to news websites, and present a major challenge to making sure people can publish and access important information.

Buffer Overflow- A buffer overflow, or buffer overrun, is a common software coding mistake that an attacker could exploit to gain access to your system. To effectively mitigate buffer overflow vulnerabilities, it is important to understand what buffer overflows are, what dangers they pose to your applications, and what techniques attackers use to successfully exploit these vulnerabilities.

Key Concepts of Buffer Overflow

- This error occurs when there is more data in a buffer than it can handle, causing data to overflow into adjacent storage.
- This vulnerability can cause a system crash or, worse, create an entry point for a cyber-attack.
- C and C++ are more susceptible to buffer overflow.
- Secure development practices should include regular testing to detect and fix buffer overflows.
- These practices include automatic protection at the language level and bounds-checking at run- time.

Attack on Wireless Networks- Wireless attacks have become a very common security issue when it comes to networks. This is because such attacks can really get a lot of information that is being sent across a network and use it to commit some crimes in other networks. Every wireless network is very vulnerable to such kinds of attacks and it is therefore very important that all the necessary security measures are taken so as to prevent the mess that can be caused by such attacks. These attacks are normally carried out to target information that is being shared through the networks. It is therefore very important to know of such attacks so that one is in a position to identify it in case it happens. Some of the common network attacks have been outlined below.

- **Rogue access points-**A rouge access point is basically an access point that has been added to one's network without one's knowledge. One totally has no idea that it is there. This is a kind of scenario that can create a kind of back door especially if one is not conversant with it and have complete management of it. This is an access point that can create some very huge security concerns. One is due to the fact that it can be very easy to plug in a wireless access point in it. If one is not doing any type of network access control protocols on one's network, it becomes very easy for additional workstations and access points to be added onto one's network.
- **Jamming/Interference-**Wireless interference basically means disruption of one's network. This is a very big challenge especially owing to the fact that wireless signals will always get disrupted. Such interference can be created by a Bluetooth headset, a microwave oven and a cordless phone. This makes transmission and receiving of wireless signals very difficult. Wireless interference can also be caused by causing service degradation so as to make sure that one denies complete access to a particular service. Jamming can also be used in conjunction with an evil twin.
- **Evil twin-**A wireless evil twin mainly comes into play when criminals are trying to create rogue access points so as to gain access to the network or access to information that is being put through a network. Coming up with an evil twin is very simple since all one need to do is purchase a wireless access point, plug it into the network and configure it as exactly as the existing network. This is possible in open access points that do not have any passwords associated with them. Once one comes up with one's access point, one plugs it into the network so that it becomes the primary access point thus overpowering other existing accesspoints. With this, one's evil twin will tend to have a stronger network signal and therefore people will

choose it. Through this, the individual controlling the access point will be in a position to see all the information being sent around the network.

- **War driving-**War driving is a way that bad guys use so as to find access points wherever they can be. With the availability of free Wi-Fi connection and other GPS functionalities, they can drive around and obtain a very huge amount of information over a very short period of time. One can also use some special type of software to view all the different access points around one. With this information, an individual is in a position to come up with a very large database which he or she can use to determine where he or she can gain access to a wireless signal.
- **Blue Jacking**-Blue jacking is a kind of illegal activity that is similar to hacking where one can be able to send unsolicited messages to another device via Bluetooth. This is considered spam for Bluetooth and one might end up seeing some pop-up messages on one's screen. Blue jacking is possible where a Bluetooth network is present and it is limit end to a distance of ten meters which is the distance a Bluetooth device can send a file to another device. It rarely depends on antennae. Blue jacking works on the basis that it takes advantage of what is convenient for us on our mobile devices and the convenience is being able to communicate and send things back and forth between devices. With this, one can easily send messages to other Bluetooth devices since no authentication is required. Some third party software can also be used to carry out Blue jacking.
- **Bluesnarfing-**Bluesnarfing is far much more malicious than Blue jacking since it involves using one's Bluetooth to steal information. This is where a Bluetooth -enabled device is able to use the vulnerability on the Bluetooth network to be able to get into a mobile device to steal information such as contacts and images. This is a vulnerability that exposes the weakness and vulnerability with the Bluetooth network. This is an act that creates some very serious security issues since an individual can steal a file from one if he or she knows it.
- **War chalking**-War chalking is another method that was used so as to determine where one could get a wireless access signal. In this case, if an individual detected a wireless access point, he or she would make a drawing on the wall indicating that a wireless access point has been found. However, this is not currently used.
- **IV attack-**An IV attack is also known as an Initialization Vector attack. This is a kind of wireless network attack that can be quite a threat to one's network. This is because it causes some modification on the Initialization Vector of a wireless packet that is encrypted during transmission. After such an attack, the attacker can obtain much information about the plaintext of a single packet and generate another encryption key which he or she can use to decrypt other packets using the same Initialization Vector. With that kind of decryption key, attackers can use it to come up with a decryption table which they and use to decrypt every packet being sent across the network.
- **Near field communication**-Near field communication is a kind of wireless communication between devices like smart phones where people are able to send information to near filed communication compatible devices without the need to bring the devices in contact. This allows one device to collect information from another device that is in close range.

Phishing Techniques: Popular Phishing Techniques used by Hackers:

- **Deceptive Phishing**-Deceptive phishing is the most common type of social media phishing. In a typical scenario, a phisher creates an account pretending to be the account of the victim. Next, the phisher sends friend requests to the friends of the victim aswell as amessage such as "I have abandoned my previous Facebook account. From now on, please communicate with me through this account only". Afterwards, the phisher starts sending messages to the friends of the victim that demand the recipient to click on a link. Examples of such messages include:A statement that the receiver of the message has a virus which can be deleted bysigning up for a special anti-virus inspection conducted by the social network. A fictitious invoice which can be cancelled by clicking on a link requesting the user to provide her/his personal information. Content Injection based Phishing-The content-injection social network phishing refers to inserting malicious content in social networks. The malicious content can often be in the form of bogus posts (e.g., tweets, posts in the Facebook feed or in LinkedIn feed) published by users whose accounts were affected with rogue apps. In many cases, the victims are unable to see the bogus posts posted by the malware apps on their behalf. The bogus posts, for example, may contain a photo of the account owner and the text: "I am in the hospital. If you would like to help me, please sign up by clicking on the following link". When the victim clicks on the link, he/she will be requested to provide his/her personal data, which may be used by the phisher for committing identity theft and other scams.
- **Malware Based Phishing**-Malware-based phishing refers to a spread of phishing messages by using malware.For example, the Facebook account of a victim who installed a rogue Facebook app will automatically sendmessages to all the friends of the victim. Such messages often contain links allowing the receivers of the messages to install the rogue Facebook app on their computers or mobile devices. The best way to avoid the installation of rogue Facebook apps is to be very selective when installing any third-party Facebook applications. For example, Facebook apps developed by unknown developers that request access to extensive information should be researched thoroughly. One method often used by phishers to "seduce" the Facebook users to install malware to their computer is to promise them that the malware will enable them to see a list of people who visited their Facebook profile page.
- **Men in the Middle Phishing**-A man-in-the-middle social network attack, also known as social network session hijacking attack, is a form of phishing in which the phisher positions himself between the user and a legitimate social network website. Messages intended for the legitimatesocial networkwebsite pass through the phisher who can inspect the messages and acquire valuable information.

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