UNIT-3: Tools and Method used in Cybercrime

- Proxy Servers and Anonymizers
- Phishing
- Password Cracking
- Keyloggers and Spywares
- Virus and Worms
- Trojan-Horses and Backdoors
- Steganography
- DoS and DDoS Attacks
- SQL Injection
- Buffer Overflow
- Attacks on Wireless Networks
- Phishing and Identity Theft Introduction
- Identity Theft (ID Theft)

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

Cyber Security

(BCC301 / BCC401/ BCC301H / BCC401H)

Video Overview:

- Proxy Servers and Anonymizers
- Phishing
- Password Cracking
- Keyloggers and Spywares
- What is Virus and Worms?
- Trojan-Horses and Its Types
- Backdoors
- Steganography

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

What is Proxy Servers?

- A proxy server is an intermediate server that sits between a user's device and the internet.
- When a user makes a request to access a website, the request first goes to the proxy server, which then forwards the request to the website.
- The website's response is sent back to the proxy server, which then sends it back to the user's device.

Communication without proxy server

Communication with proxy server

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Types of Proxy Servers

There are several different types of proxy servers, including:

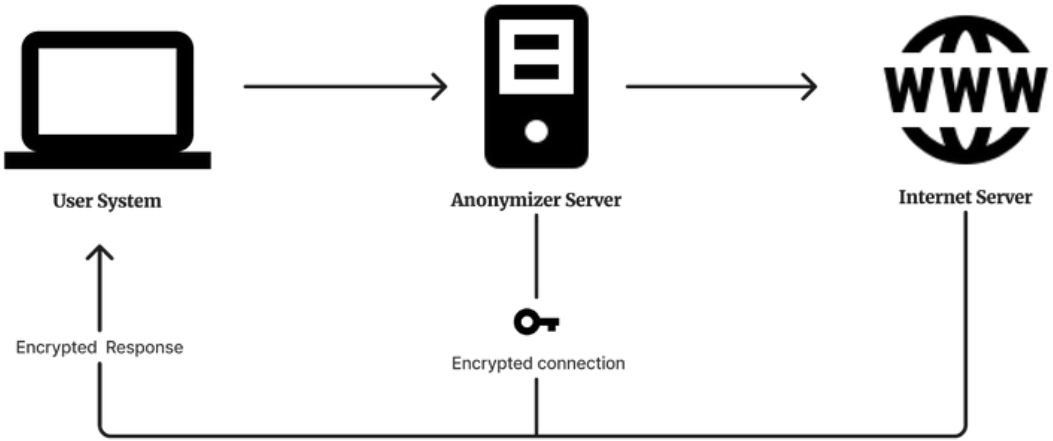
- **Open or Forward Proxy:** A forward proxy is a server that sits between a client and the internet. The client sends a request to the forward proxy, which then sends the request to the internet on behalf of the client.
- **Reverse Proxy:** A reverse proxy is a server that sits between the internet and a server. The reverse proxy receives requests from the internet and then forwards those requests to the appropriate server.
- **Transparent Proxy:** A transparent proxy is a proxy that does not modify the request or response, but simply passes the traffic along. Transparent proxies are often used in corporate environments to monitor and control access to the internet.
- **Anonymous Proxy:** An anonymous proxy is a proxy that hide the user's IP address, providing an additional layer of privacy.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

What are Anonymizers?

- An anonymizer is a tool that is used to hide a user's identity when accessing the internet.
- Anonymizers work by hiding the user's IP address, making it difficult for websites to track the user's online activity.



Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Different Types of Anonymizers

- **VPN:** A Virtual Private Network (VPN) is a type of anonymizer that creates an encrypted connection between the user's device and the internet. All traffic between the device and the internet is routed through the VPN, which hide the user's IP address and provides an additional layer of security.

- **TOR:** The Onion Router (TOR) is a free software program that is used to Hide a user's online activity by routing their traffic through a network of servers. TOR is designed to be extremely difficult to trace, making it a popular choice for users who need to Hide their identity.

- **Web-based anonymizers:** Web-based anonymizers are online tools that allow users to browse the internet without disclose their IP address. These tools work by routing traffic through a third-party server, making it difficult for websites to track the user's online activity.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Phishing Attack

- Phishing is one type of cyber attack.
- Phishing got its name from “phish” meaning fish. It’s a common phenomenon to put bait for the fish to get trapped.
- Similarly, phishing works. It is an unethical way to dupe the user or victim to click on harmful sites.
- The attacker crafts the harmful site in such a way that the victim feels it to be an authentic site, thus falling prey to it.
- The most common mode of phishing is by sending spam emails that appear to be authentic and thus, taking away all credentials from the victim.
- The main motive of the attacker behind phishing is to gain confidential information like
    - Password
    - Credit card details
    - Social security numbers
    - Date of birth

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

How Does Phishing Occur?

- **Clicking on an unknown file or Attachment:** Here, the attacker deliberately sends a mysterious file to the victim, as the victim opens the file, either malware is injected into his system or it prompts the user to enter confidential data.
- **Using an open or free wifi hotspot:** This is a very simple way to get confidential information from the user by luring him by giving him free wifi. The wifi owner can control the user's data without the user knowing it.
- **Responding to social media requests:** This commonly includes social engineering. Accepting unknown friend requests and then, by mistake, leaking secret data are the most common mistakes made by naive users.
- **Clicking on unauthenticated links or ads:** Unauthenticated links have been deliberately crafted that lead to a phished website that tricks the user into typing confidential data.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Types of Phishing Attacks

1. Email Phishing: The most common type where users are tricked into clicking unverified spam emails and leaking secret data. Hackers impersonate a legitimate identity and send emails to mass victims. Generally, the goal of the attacker is to get personal details like bank details, credit card numbers, user IDs, and passwords of any online shopping website, installing malware, etc. After getting the personal information, they use this information to steal money from the user's account or harm the target system, etc.

2. Spear Phishing: In spear phishing or phishing attack, a particular user(organisation or individual) is targeted. In this method, the attacker first gets the full information of the target and then sends malicious emails to his/her inbox to trap him into typing confidential data. For example, the attacker targets someone(let's assume an employee from the finance department of some organisation). Then the attacker pretends to be like the manager of that employee and then requests personal information or transfers a large sum of money. It is the most successful attack.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Types of Phishing Attacks

3. **Whaling:** Whaling is just like spear-phishing but the main target is the head of the company, like the CEO, CFO, etc. a pressurized email is sent to such executives so that they don't have much time to think, therefore falling prey to phishing.

4. Smishing: In this type of phishing attack, the medium of phishing attack is SMS. Smishing works similarly to email phishing. SMS texts are sent to victims containing links to phished websites or invite the victims to call a phone number or to contact the sender using the given email. The victim is

then
invited to enter their personal information like bank details, credit card information, user id/ password, etc. Then using this information the attacker harms the victim.

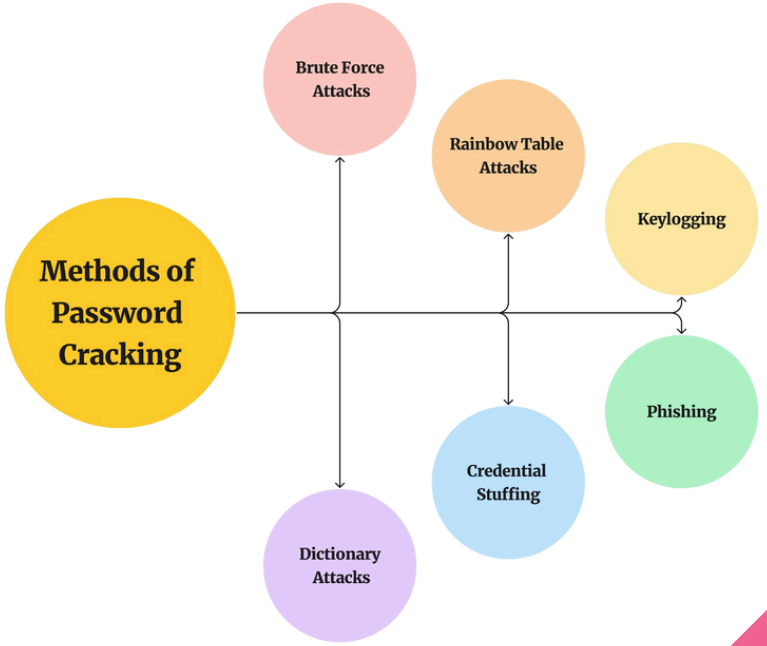
5. Vishing: Vishing is also known as voice phishing. In this method, the attacker calls the victim using modern caller id spoofing to convince the victim that the call is from a trusted source. Attackers also use IVR to make it difficult for legal authorities to trace the attacker. It is generally used to steal credit card numbers or confidential data from the victim.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Password Cracking

It is a cyber attack technique where unauthorised individuals attempt to gain access to user accounts or systems by decrypting or bypassing passwords. This activity is often performed using various methods and tools to exploit weaknesses in password security.



Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Methods of Password Cracking

1. Brute Force Attacks: The attacker systematically tries all possible combinations of passwords until the correct one is found.

- **Countermeasure:** Implement account lockout policies and use strong, complex passwords.

2. Dictionary Attacks: Attackers use precompiled lists of common passwords (dictionaries) to attempt login.

- **Countermeasure:** Enforce strong password policies, including the avoidance of easily guessable passwords.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Methods of Password Cracking

3. Rainbow Table Attacks: Attackers use precomputed tables (rainbow tables) of hashed passwords to quickly crack password hashes.

- **Countermeasure:** Use salting and strong, unique hashing algorithms to protect password hashes.

4. Credential Stuffing: Attackers use known username and password pairs obtained from previous data breaches to gain unauthorised access to other accounts where users have reused passwords.

- **Countermeasure:** Encourage users to use unique passwords for different accounts and implement multi-factor authentication.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Methods of Password Cracking

5. Keylogging: Malicious software records keystrokes to capture usernames and passwords as users type.

Countermeasure: Use updated antivirus software, employ intrusion detection systems, and educate users about the risks of downloading unknown software.

6. Phishing: Attackers trick individuals into revealing their passwords through deceptive emails or fake websites.

Countermeasure: Educate users about phishing risks and implement email filtering solutions.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

What is Keylogger?

- Keylogger is a malicious program that is specifically designed to monitor and log the keystrokes made by the user on their keyboards.
- It is a form of spyware program used by cybercriminals to fetch sensitive information like banking details, login credentials of social media accounts, credit card number, etc.
- A keylogger can monitor and log such information and send those to the cybercriminal behind it.
- A keylogger can not only monitor the keystrokes, but it can also take note of every click and touch on your system.
- First key-logger was invented in 1970's and was a hardware keylogger and first software keylogger was developed in 1983

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Types of keyloggers

1. Software keyloggers: Software keyloggers are computer programs which are developed to steal passwords from the victim's computer. However key loggers are used in IT organisations to troubleshoot technical problems with computers and business networks. Microsoft Windows 10 also has a keylogger installed in it.

- **JavaScript based keylogger:** It is a malicious script which is installed into a web page, and listens for keys to press such as oneKeyUp(). These scripts can be sent by various methods, like sharing through social media, sending as a mail file, or RAT file.
- **Form Based Keyloggers:** These are key-loggers which activate when a person fills a form online and when clicking the button submit all the data or the words written are sent via file on a computer. Some key-loggers work as an API in a running application. It looks like a simple application and whenever a key is pressed it records it.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Types of keyloggers

2. Hardware Keyloggers: These are not dependent on any software as these are hardware key-loggers. keyboard hardware is a circuit which is attached in a keyboard itself that whenever the key of that keyboard is pressed it gets recorded.

- **USB keylogger:** There are USB connector keyloggers which have to be connected to a computer and steal the data. Also some circuits are built into a keyboard so no external wire is used or shows on the keyboard.
- **Smartphone sensors:** Some cool android tricks are also used as keyloggers such as android accelerometer sensor which when placed near to the keyboard can sense the vibrations and the graph then used to convert it to sentences, this technique accuracy is about 80%. Nowadays crackers are using keystroke logging Trojan, a malware which is sent to a victim's computer to steal the data and login details.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Prevention From Keyloggers

- **Anti-Keylogger:** As the name suggests these are the software which are anti / against keyloggers and main task is to detect keyloggers from a computer system.
- **Anti-Virus:** Many anti-virus software also detect keyloggers and delete them from the computer system. These are software anti-software so these can not get rid from the hardware keyloggers.
- **Automatic form filler:** This technique can be used by the user to not fill forms on regular bases instead use automatic form filler which will give a shield against keyloggers as keys will not be pressed .
- **One-Time-Passwords:** Using OTP's as password may be safe as every time we login we have to use a new password.
- **Patterns or mouse-recognition:** On android devices use pattern as a password of applications and on PC use mouse recognition, mouse program uses mouse gestures instead of stylus.
- **Voice to Text Converter:** This software helps to prevent Keylogging which targets a specific part of our keyboard.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

What is Spyware?

- Spyware is malicious software that enters a user's computer, gathers data from the device and user, and sends it to third parties without their consent.
- Spyware collects personal and sensitive information that it sends to advertisers, data collection firms, or malicious actors for a profit.
- Attackers use it to track, steal, and sell user data, such as internet usage, credit card, and bank account details, or steal user credentials to spoof their identities.
- Spyware is one of the most commonly used cyber attack methods that can be difficult for users and
businesses to identify and can do serious harm to networks. It also leaves businesses vulnerable to data breaches and data misuse, often affects device and network performance, and slows down user activity.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Types of Spyware?

- **Adware:** It is a type of Spyware that keeps track of the user's activity and gives advertisements based on the tracked activity of the user.
- **Tracking Cookies:** It is a type of Spyware that tracks a user's activity and supplies the same to third parties.
- **Trojans:** It is a type of Spyware that is the most dangerous. It aims to steal confidential user information such as bank details, passwords and transfers it to a third party to perform illegal transactions or frauds.
- **Keyloggers:** It is a type of Spyware that keeps a track of all the keystrokes that the user enters through the keyboard.
- **Stalkerware:** It is a type of Spyware that is installed on mobile phones to stalk the user. It tracks the movement of the user and sends the same to the third party.
- **System Monitor:** It is a type of Spyware that monitors and keep a track of the entire system including users activity, sensitive information, keystrokes, calls, and chats. It is extremely dangerous to user privacy.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

How to Prevent Spyware?

- **Installing Antivirus/ Antispyware:** The best way to protect your system from spyware is to install a good quality Anti-spyware or Antivirus such as MalwareBytes, Adaware, AVG Antivirus, SpywareBlaster, etc. Installing Antivirus/ Antispyware also protects the system from harmful threats by blocking sites that try to steal data or leak the data to third-party users.
- **Beware of Cookie Settings:** Beware of cookie settings that transfer confidential information alongside cookies. It is always advisable to keep a check on the cookie settings and set the settings to high security.
- **Beware of the Pop-ups on Websites:** Don't click on the pop-ups that appear on your website without reading them. Never accept their terms and conditions as it is highly dangerous. Always close the pop-up windows without clicking on 'ok'.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

How to Prevent Spyware?

- **Never Install Free Software:** Always be very cautious when you install free software on your systems. Free software mostly has spyware attached to them and it can directly leak confidential user information.
- **Always read Terms & Conditions:** Always read Terms and Conditions before installing apps on your system. Never accept policies that breach privacy. Download only trusted and verified apps from Google Play Store or Apple Play Store for mobile phones to protect them from Spyware.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Viruses and Worms

- While discussing the virus and worm, it is important to first understand the larger category of malicious programs, called "Malware".
- Malware can be defined as a special kind of code or application specifically developed to harm electronic devices or the people using those devices.
- Viruses and worms are both types of malware; however, there are significant differences between them.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

What is Virus?

- A Virus is a program developed using malicious code with a nature that links itself to the executable files and propagates device to device.
- Viruses are often transferred through the downloaded files and the shared files.
- They can also be attached with a scripting program and non-executable files like images, documents, etc.
- After the user executes the infected program, the virus gets activated and starts replicating further on its own.

Viruses can harm the system by the following means:

- Filling up the disk space unnecessarily
- Formatting the hard disk drive automatically
- Making the system slow
- Modify, or delete personal data or system files
- Stealing sensitive data

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

How does a virus spread?

- The virus does not have the capability of spreading itself.
- It requires the host and human support to spread.
- The virus is developed in such a way that it attaches itself to the executable files.
- It further spreads when the infected executable file or software is transferred from one device to another.
- As soon as a human launches the infected file or a program, the virus starts replicating itself.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

What is a Worm?

- Worms are the type of virus that can self-replicate and travel from device to device using a computer network. That means worms don't need any host to spread.
- They are standalone computer malware that doesn't even require human support to execute.
- Usually, worms use computer networks by exploiting vulnerabilities, and that makes them spread more quickly.

How does a worm spread?

Unlike viruses, worms don't require host files to spread. This means that worms do not attach themselves with executable files or programs. Instead, worms find a weak spot in the system and enter through a vulnerability in the network. Before we detect and remove worms from our system, they replicate and spread automatically and consume all the network bandwidth. This can result in the failure of the entire network and web servers. Because worms can spread automatically, their spreading speed is comparatively faster than other malware.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Basis	WORMS	VIRUS
Definition	A Worm is a form of malware that replicates itself and can spread to different computers via another Network.	A Virus is a malicious executable code attached to executable file which can be harmless or can modify or delete data.
Objective	The main objective of worms is to eat the system resources. It consumes system resources such as memory and bandwidth and makes the system slow in speed to such an extent that it stops responding.	The main objective of viruses is to modify the information.
Host	It doesn't need a host to replicate from one computer to another.	It requires a host to spread.
Harmful	It is less harmful as compared.	It is more harmful.
Detection and Protection	Worms can be detected and removed by the Antivirus and firewall.	Antivirus software is used for protection against viruses.
Controlled by	Worms can be controlled by remote.	Viruses can't be controlled remotely.
Execution	Worms are executed via weaknesses in the system.	Viruses are executed via executable files.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Basis	WORMS	VIRUS
Prevention	• Keep your operating system and system in updated state • Avoid clicking on links from untrusted or unknown websites • Avoid opening emails from unknown sources • Use antivirus software and a firewall	• Installation of Antivirus software Never • open email attachments Avoid usage of • pirated software Keep your operating • system updated Keep your browser • updated as old versions are vulnerable to linking to malicious websites
Types	Internet worms, Instant messaging worms, Email worms, File sharing worms, Internet relay chat (IRC) worms are different types of worms.	Boot sector virus, Direct Action virus, Polymorphic virus, Macro virus, Overwrite virus, File Infector virus are different types of viruses
Examples	Examples of worms include Morris worm, storm worm, etc.	Examples of viruses include Creeper, Blaster, Slammer, etc.
Interface	It does not need human action to replicate.	It needs human action to replicate.
Speed	Its spreading speed is faster.	Its spreading speed is slower as compared to worms.
Comes from	Worms generally come from the downloaded files or through a network connection.	Viruses generally come from the shared or downloaded files.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

What is a Trojan Horse?

- The name of the **Trojan Horse** is taken from a classical story of the Trojan War. It is a code that is
- malicious in nature and has the capacity to take control of the computer. It is designed to steal,
- damage, or do some harmful actions on the computer. It tries to deceive the user to load and
- execute the files on the device. After it executes, this
  allows cybercriminals to perform many actions on the user's computer like deleting data from files, modifying data from files, and more. Now like many viruses or worms, Trojan Horse does not
- have the ability to replicate itself.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Types of Trojan Horse?

Now there are many Trojans which are designed to perform specific functions. Some of them are: –

- **Backdoor trojan:** A trojan horse of this kind gives the attacker remote access to the compromised machine.
- **Ransom trojan:** This kind of trojan horse is intended to encrypt the data on the compromised system and then demand payment in exchange for its decryption.
- **Trojan Banker:** It is designed to steal the account data for online banking, credit and debit cards, etc.
- **Trojan Downloader:** It is designed to download many malicious files like the new versions of Trojan and Adware into the computer of the victims.
- **Trojan Dropper:** It is designed to prevent the detection of malicious files in the system. It can be used by hackers for installing Trojans or viruses on the victim's computers.
- **Trojan GameThief:** It is designed to steal data from Online Gamers.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Uses of Trojan Horse?

- **Spy:** Some Trojans act as spyware. It is designed to take the data from the victim like social networking(username and passwords), credit card details, and more.
- **Creating backdoors:** The Trojan makes some changes in the system or the device of the victim, So this is done to let other malware or any cyber criminals get into your device or the system.
- **Zombie:** There are many times that the hacker is not at all interested in the victim's computer, but they want to use it under their control.

Prevention from Trojan Horse: The most basic prevention method: –

- Do not download anything like the images, and audios from an unsecured website.
- Do not click on the ads that pop up on the page with advertisements for online games.
- Do not open any attachment that has been sent from an unknown use.
- The user has to install the antivirus program. This anti-virus program has the capacity to detect those files which are affected by a virus.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

What are Backdoors?

- A backdoor is an undocumented way to bypass existing cybersecurity measures and gain access to the computer system or device. Software and hardware developers sometimes install backdoors into their own products to retain access for troubleshooting purposes.
- Backdoor installation helps software developers solve various problems, for example, retrieve data from a device to aid a criminal investigation or restore users' lost passwords. But the backdoors might also be exploited by hackers, but how?

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

How does a Backdoor attack work?

Backdoor attacks work in two ways.

- In the first scenario, hackers use a backdoor to circumvent normal security measures and gain unauthorised access to a computer system and its data.
- In the second one, they exploit system vulnerabilities to gain access into it and implant backdoor software. Once the backdoor is in, attackers can easily re-enter the system whenever they like, even if the vulnerabilities are fixed.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Types of Backdoor Attack

1. Administrative backdoors: Lots of software developers include backdoors in their programs to give them easy administrative access to various areas of their own systems. Doing so can help them to troubleshoot user problems and fix vulnerabilities quickly. However, if these backdoors are discovered by cybercriminals, they can be used to launch cyber attacks.

2. Malicious backdoors: A malicious backdoor is one created for a malicious purpose. This process may involve hackers installing backdoor malware through a targeted phishing email. If the hacker can eventually gain access to the code of an operating system, they can add backdoors to allow for easy access in the future.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Types of Backdoor Attack

3. Accidental backdoors: Many backdoors are just the result of human error. When a developer leaves a weak point in their internet security systems, it can go undetected for a long time. If bad actors find the flaw first, they can use it as a backdoor to the operating system or application.

4. Hardware backdoors: While most backdoor attacks involve hackers gaining remote access to networks and devices through software flaws, it's also possible to include hardware backdoors in the physical structure of a device. A good example is the Clipper chip that the NSA proposed. However, this approach is high risk for a cybercriminal because it requires physical access to a targeted device.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

How to protect yourself from Backdoor Attack

Here are some steps you can take to protect yourself.

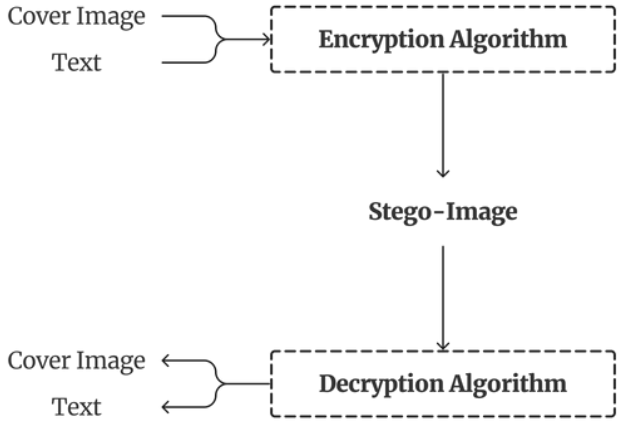
- Don’t use your work device for personal internet activity
- Report any unusual or suspicious incidents
- Use a VPN, especially while travelling
- Use strong passwords
- Enable firewalls
- Monitor network traffic

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

What is Steganography

- Steganography is like hiding a secret message in plain sight.
- Instead of encrypting the message, you hide it within another seemingly innocent file, like an image, audio file, or even a text document.
- The goal is to conceal the existence of the message, making it difficult for others to detect.



Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Different Technique of Steganography

1. Image Steganography: Embedding data within images by subtly altering pixel values. This can be achieved through the least significant bit (LSB) method, where the least significant bits of pixel values are replaced with hidden data.

2. Audio Steganography: Concealing information within audio files by modifying certain components, such as the amplitude or frequency. This can be done without significantly altering the perceived quality of the audio.

3. Text Steganography: Hiding information within text by using techniques like white space manipulation, word or letter arrangement, or embedding messages within seemingly innocent text.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Different Technique of Steganography

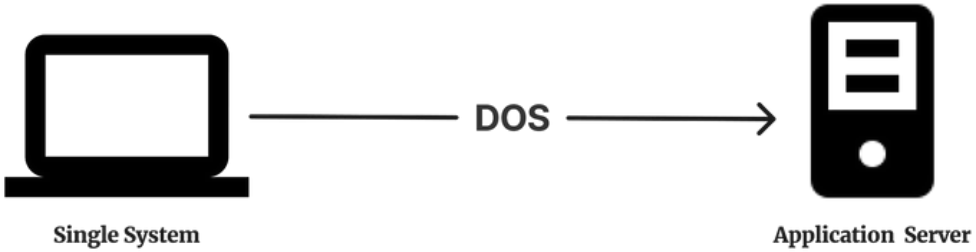
4. Video Steganography: Embedding data within video files, often by modifying specific frames or components of the video stream. Similar to image steganography, this can involve altering pixel values.

5. File Steganography: Hiding data within seemingly innocuous files, such as documents or executable files, by manipulating certain aspects without affecting the overall functionality.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

DoS Attack

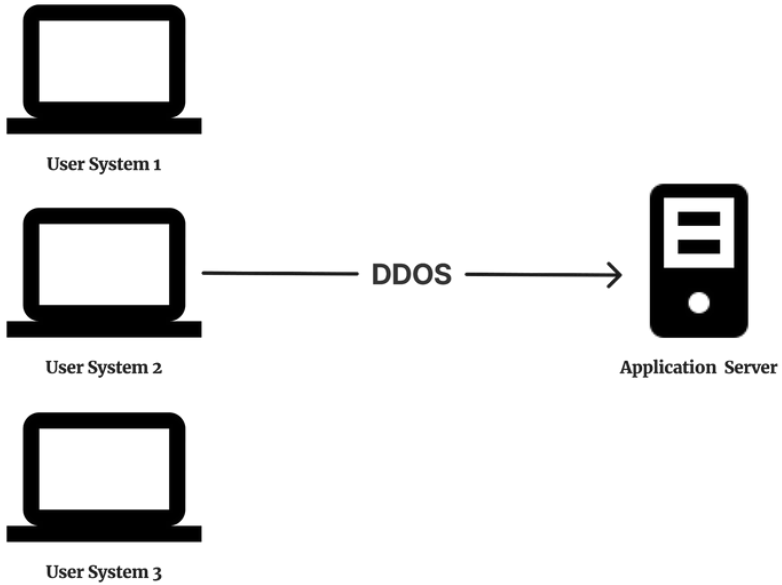
DOS Attack is a denial of service attack, in this attack a computer sends a massive amount of traffic to a victim's computer and shuts it down. Dos attack is an online attack that is used to make the website unavailable for its users when done on a website. This attack makes the server of a website that is connected to the internet by sending a large amount of traffic to it.



UNIT 3

DDoS Attack

A DDoS attack is Distributed Denial of Service (DDoS) Attack which is involves multiple compromised computers, known as botnets, working together to flood a target system with a massive volume of traffic. The distributed nature makes DDoS attacks more challenging to mitigate compared to traditional DoS attacks.



Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

DOS	DDOS
DOS Stands for Denial of service attack.	DDOS Stands for Distributed Denial of service attack.
In Dos attacks, a single system targets the victim system.	In DDoS multiple systems attack the victim's system.
Victim PC is loaded from the packet of data sent from a single location.	Victim PC is loaded from the packet of data sent from Multiple locations.
Dos attack is slower as compared to DDoS.	DDoS attack is faster than Dos Attack.
Can be blocked easily as only one system is used.	It is difficult to block this attack as multiple devices are sending packets and attacking from multiple locations.
In DOS Attack only a single device is used with DOS Attack tools.	In DDoS attacks,The volume Bots are used to attack at the same time.
DOS Attacks are Easy to trace.	DDOS Attacks are Difficult to trace.
Volume of traffic in the Dos attack is less as compared to DDos.	DDoS attacks allow the attacker to send massive volumes of traffic to the victim network.

UNIT 3

What is SQL Injection?

- SQL Injection is a code-based vulnerability that allows an attacker to read and access sensitive data from the database.
- Attackers can bypass security measures of applications and use SQL queries to modify, add, update, or delete records in a database.
- A successful SQL injection attack can badly affect websites or web applications using relational databases such as MySQL, Oracle, or SQL Server.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Types SQL Injection?

1. In-band SQLi: The attackers use the same communication channel to launch their attacks and collect results. The two common types of in-band SQL injections are:

- **Error-based SQL injection:** Here, the attacker performs certain actions that cause the database to generate error messages. Using the error message, you can identify what database it utilises, the version of the server where the handlers are located, etc.
- **Union-based SQL injection:** Here, the UNION SQL operator is used in combining the results of two or more select statements generated by the database, to get a single HTTP response. You can craft your queries within the URL or combine multiple statements within the input fields and try to generate a response.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

Types SQL Injection?

2. Blind SQLi: Here, it does not transfer the data via the web application. The attacker can not see the result of an attack in-band.

- **Boolean-based SQL Injection:** Here, the attacker will send an SQL query to the database asking the application to return a different result depending on whether the query returns True or False.
- **Time-based SQL Injection:** In this attack, the attacker sends an SQL query to the database, which makes the database wait for a particular amount of time before sharing the result. The response time helps the attacker to decide whether a query is True or False.

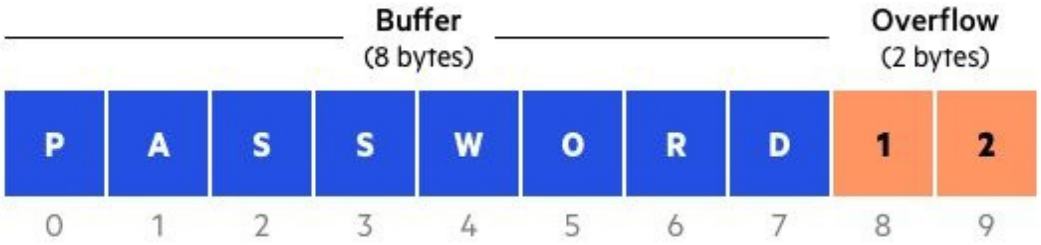
3. Out-of-bound SQL Injection: Out-of-bound is not so popular, as it depends on the features that are enabled on the database server being used by the web applications. It can be like a misconfiguration error by the database administrator.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

What is Buffer Overflow

Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another. A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.



For example, a buffer for login credentials may be designed to expect username and password inputs of 8 bytes, so if a transaction involves an input of 10 bytes (that is, 2 bytes more than expected), the program may write the excess data past the buffer boundary.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

What is Buffer Overflow Attacks

A buffer overflow attack is a type of cybersecurity threat that occurs when a program or application tries to store more data in a buffer (temporary storage) than it can actually hold. This excess data can overflow into adjacent memory locations, potentially overwriting important information or causing the program to crash. In some cases, attackers can exploit this vulnerability to execute malicious code and gain unauthorised access to a system or application.

Types of Buffer Overflow Attacks

- **Stack-based buffer overflows** are more common, and leverage stack memory that only exists during the execution time of a function.
- **Heap-based attacks** are harder to carry out and involve flooding the memory space allocated for a program beyond memory used for current runtime operations.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

What is Identity Theft?

- Identity Theft also called Identity Fraud is a crime that is being committed by a huge number nowadays.
- Identity theft happens when someone steals your personal information to commit fraud.
- This theft is committed in many ways by gathering personal information such as transactional information of another person to make transactions.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Types of Identity Theft?

- **Criminal Identity Theft:** This is a type of theft in which the victim is charged guilty and has to bear the loss when the criminal or the thief backs up his position with the false documents of the victim such as ID or other verification documents and his bluff is successful.
- **Driver's licence ID Identity Theft:** Driver's licence identity theft is the most common form of ID theft. All the information on one's driver's licence provides the name, address, and date of birth, as well as a State driver's identity number. The thieves use this information to apply for loans or credit cards or try to open bank accounts to obtain checking accounts or buy cars, houses, vehicles, electronic equipment, jewellery, anything valuable and all are charged to the owner's name.
- **Medical Identity Theft:** In this theft, the victim's health-related information is gathered and then a fraud medical service need is created with fraud bills, which then results in the victim's account for such services.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Types of Identity Theft?

- **Tax Identity Theft:** In this type of attack the attacker is interested in knowing your Employer Identification Number to appeal to get a tax refund. This is noticeable when you attempt to file your tax return or the Income Tax return department sends you a notice for this.
- **Social Security Identity Theft:** In this type of attack the thief intends to know your Social Security Number (SSN). With this number, they are also aware of all your personal information which is the biggest threat to an individual.
- **Financial Identity Theft:** This type of attack is the most common type of attack. In this, the stolen credentials are used to attain a financial benefit. The victim is identified only when he checks his balances carefully as this is practised in a very slow manner.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Techniques of Identity Theft?

- **Pretext Calling:** Thieves pretending to be an employee of a company over phone asking for financial information are an example of this theft. Pretending as legitimate employees they ask for personal data with some buttery returns.
- **Mail Theft:** This is a technique in which credit card information with transactional data is extracted from the public mailbox.
- **Phishing:** This is a technique in which emails pertaining to be from banks are sent to a victim with malware in it. When the victim responds to mail their information is mapped by the thieves.
- **Card Verification Value (CVV) Code Requests:** The Card Verification Value number is located at the back of your debit cards. This number is used to enhance transaction security but several attackers ask for this number while pretending as a bank official.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 3

Step of Prevention From Identity Theft?

- Use Strong Passwords and do not share your PIN with anyone on or off the phone.
- Use two-factor notification for emails.
- Secure all your devices with a password.
- Don’t install random software from the internet.
- Don’t post sensitive information over social media.
- While entering passwords at payment gateway ensure its authenticity.
- Keep a practice of changing your PIN and password regularly.
- Do not disclose your information over the phone.
- While travelling do not disclose personal information with strangers.
- Never share your Aadhaar/PAN number (In India) with anyone whom you do not know/trust.
- Please never share an Aadhaar OTP received on your phone with someone over a call.
- Do not fill personal data on the website that claims to offer benefits in return.
- Last, be a keeper of personal knowledge.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com