UNIT III

Tools and methods used in Cyber Crime:

In cybercrime, attackers follow a systematic process to compromise a network.

- The first stage is "Initial Uncovering," where the attacker gathers information about the target through legal means, such as searching online.
- In the "Network Probe" stage, more invasive techniques are used, like scanning network IP addresses to find potential targets.
- The third stage, "Crossing the line toward electronic crime (E-crime)," involves exploiting vulnerabilities in the target system.
- "Capturing the network" follows, where the attacker gains control by compromising low-priority systems and removes evidence of the attack.
- "Grabbing the data" comes next, allowing the attacker to steal confidential information and potentially cause harm.
- The final stage, "Covering Tracks," involves activities to extend misuse of the system without being detected.

Proxy Servers and Anonymizers:

A proxy server is like a middleman computer on a network that helps connect to other computers.

- In cyber-attacks, the attacker connects to a proxy server first and then reaches the target system through that connection.
- Proxy servers have different purposes, like keeping systems secure, speeding up access to resources, and filtering unwanted content.
- They can also be used to connect multiple computers to the Internet using just one IP address.
- An advantage is that the proxy server's cache memory can make webpages load faster for users.

Anonymizers, or anonymous proxies, are tools that aim to make online activities untraceable by accessing the Internet on behalf of the user, hiding the source computer's information.

- Some websites provide free proxy servers and more information about anonymizers, helping users protect their privacy online.

How Phishing works?

Phishing is a term related to "fishing for information," and it was first used in 1996. Here's how phishing works:

- First, phishers, who are essentially online criminals, choose their target and figure out how to obtain email addresses, often using methods like spammers.
- After identifying the target, they set up ways to deliver a deceitful message, usually involving emails and fake webpages.
- The next step is the attack, where the phisher sends a fake message that seems trustworthy.
- Once recipients interact with this message, the phishers collect their information through webpages or pop-up windows.
- Finally, they use the gathered information for identity theft and fraud, making unauthorized purchases or committing illegal activities.

Password Cracking:

Password cracking is like trying to find the key to a computerized lock.

- It's about recovering passwords that are stored or sent by a computer system.
- People might try to crack passwords for a few reasons: to remember a forgotten password, to check if passwords are too easy to crack, or to gain unauthorized access to a system.
- The process involves attempting to log in with different passwords.
- Some weak passwords are easily guessed, like common names or simple sequences of letters or numbers.
- Online attacks involve automated programs trying passwords, while offline attacks are done from a different location.
- Strong passwords are longer, include a mix of characters, and are harder to remember.
- It's essential to have good password policies, like unique passwords for each user, regular changes, and account freezes after multiple failed attempts, to keep systems secure.

Key loggers and Spywares:

Keystroke logging, or keylogging, is when someone secretly records the keys you press on a keyboard.

- Software keyloggers are programs that do this on a computer, recording every keystroke.
- Some examples include SC-KeyLog PRO, Spytech SpyAgent Stealth, and All in one Keylogger.
- Hardware keyloggers are small devices that need physical access to the computer to be installed.
- They can be found on websites like keyghost.com or keelog.com.
- Antikeylogger tools, like those at anti-keyloggers.com, can detect and remove keyloggers from a computer.
- They help prevent unauthorized access and protect personal information.

Spyware is a type of malware that secretly collects information about users.

- Spyware features go beyond simple monitoring and can include things like recording websites visited and capturing keystrokes.
- Examples of spyware are 007 Spy, Spector Pro, and eBlaster.
- They can record chats, emails, and even block certain websites.
- These tools can invade privacy, so it's crucial to be aware of them and use anti-spyware measures.

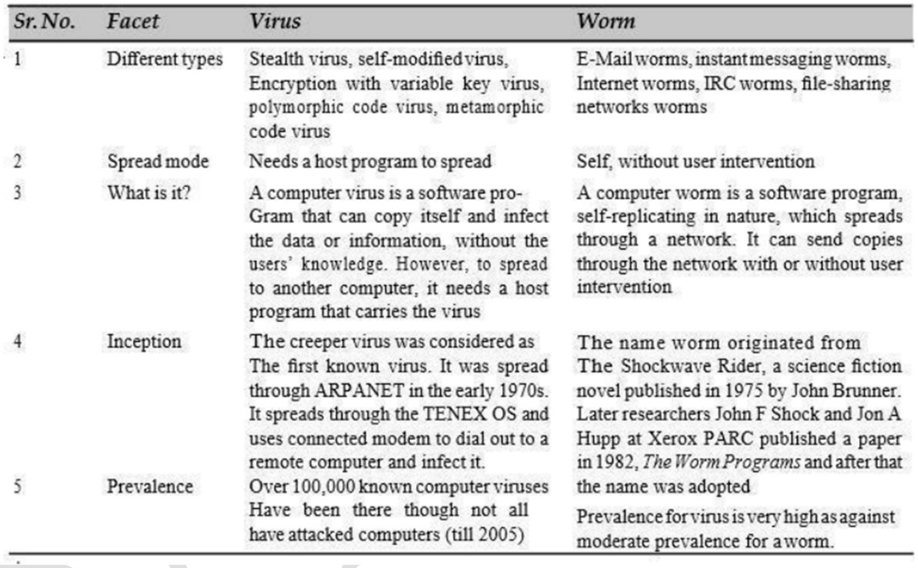
Viruses and Worms:

A computer virus is like a program that can sneak into other programs, changing them to include a copy of itself.

- These viruses spread without you knowing and can cause trouble by displaying messages, deleting files, messing up data, or even stopping your computer.
- They can also make copies of themselves to spread and harm more programs.
- Viruses can spread in different ways: through the internet, on stand-alone computers, and through local networks.

Computer viruses come in different types, each with its own way of causing trouble for your computer and personal data.

- Boot sector viruses infect the part of your computer that helps it start up, like floppy disks and hard drives.
- Program viruses become active when you open a program, making copies of themselves and infecting other programs.
- Multipartite viruses are a mix of boot sector and program viruses, infecting both when an infected program runs.
- Stealth viruses are tricky to detect because they disguise themselves so well, even fooling antivirus software.
- Polymorphic viruses act like chameleons, changing their appearance each time they spread.
- Macro viruses sneak into programs like Microsoft Word or Excel and use special commands.
- Web browsers have settings related to ActiveX and Java Controls that you should be aware of to protect against viruses.
- In simple terms, viruses can attack specific files, manipulate programs to do things they shouldn't, create more viruses, run silently in the background, and change to avoid being caught.
- It's important to stay vigilant and protect your computer from these tricky viruses.



Sr. No.	*Facet*	*Virus*	*Worm*
1	Different types	Stealth virus, self-modified virus, Encryption with variable key virus, polymorphic code virus, metamorphic code virus	E-Mail worms, instant messaging worms, Internet worms, IRC worms, file-sharing networks worms
2	Spread mode	Needs a host program to spread	Self, without user intervention
3	What is it?	A computer virus is a software proGram that can copy itself and infect the data or information, without the users' knowledge. However, to spread to another computer, it needs a host program that carries the virus	A computer worm is a software program, self-replicating in nature, which spreads through a network. It can send copies through the network with or without user intervention
4	Inception	The creeper virus was considered as The first known virus. It was spread through ARPANET in the early 1970s. It spreads through the TENEX OS and uses connected modem to dial out to a remote computer and infect it.	The name worm originated from The Shockwave Rider, a science fiction novel published in 1975 by John Brunner. Later researchers John F Shock and Jon A Hupp at Xerox PARC published a paper in 1982, *The Worm Programs* and after that the name was adopted
5	Prevalence	Over 100,000 known computer viruses Have been there though not all have attacked computers (till 2005)	Prevalence for virus is very high as against moderate prevalence for a worm.

Steganography:

Steganography is a technique that hides messages or communications, and the name comes from Greek words meaning "covered writing."

- It's like a secret way of sharing information.
- Steganography tools, such as DiSi-Steganograph, Invisible Folders, Invisible Secrets, and Stealth Files, help embed data or make files and folders invisible to protect sensitive information.
- For example, Invisible Secrets not only encrypts files but also hides them in places like pictures or sound files.

Steganalysis is like the detective work of finding hidden messages using steganography.

- It uses automated tools to detect and uncover information hidden in images, audio, or video files.
- The goal is to identify and recover any hidden content that might be concealed within these files.

- So, steganography is all about cleverly hiding messages, and steganalysis is about figuring out if there's anything hidden.

DoS and DDoS attacks:

Denial of Service (DoS) attacks aim to disrupt or shut down a system, and they can be classified based on various factors.

- One classification is by the types or levels of DoS attacks, which include volumetric attacks that overwhelm network bandwidth, protocol attacks exploiting vulnerabilities in network protocols, and application-layer attacks targeting specific applications or services.
- Tools employed for launching DoS attacks range from simple ones like Ping floods to more sophisticated tools such as LOIC (Low Orbit Ion Cannon).
- Additionally, Distributed Denial of Service (DDoS) attacks involve multiple systems, making them more potent.
- Protection from DoS/DDoS attacks often requires a combination of strategies, including traffic filtering, rate limiting, and the use of specialized hardware or cloud-based DDoS protection services to mitigate the impact of such attacks on a network or system.

SQL Injection:

Structured Query Language (SQL) is a language used for managing data in databases, and SQL injection is a sneaky technique that takes advantage of vulnerabilities in a database application's security.

- This vulnerability arises when user input is not properly filtered for special characters in SQL statements or when input is not strictly defined, leading to unexpected execution.
- In simple terms, it's like tricking the system into doing things it shouldn't by injecting rogue SQL commands.
- The steps for a SQL injection attack involve finding web pages that accept user data, checking the webpage's source code for potential vulnerabilities, and testing input fields with a single quote to see if the server interprets it literally.
- Blind SQL injection is used when the attacker can't directly see the results but can still gather information or manipulate the database.
- Tools like AppDetectivePro and DbProtect can be used for SQL Server penetration.
- To prevent SQL injection, it's crucial to validate user inputs, modify error reports, and implement other security measures in website administration and coding.

Buffer Overflow:

Buffer overflow is like a computer program hiccup where data spills out of the designated memory area and messes with nearby information, potentially causing the program to act strangely, produce errors, or even crash.

- In languages like C and C++, there's no automatic check to make sure you're not writing too much data into a buffer.
- For example, if a program intends to store data in a container with space for 10 items, but someone tries to put something in the 20th slot, that's a problem.
- There are two main types: stack-based, which messes with a program's call stack, and heap-based, which deals with dynamically allocated memory.

- Minimizing these overflows involves secure coding practices, disabling certain types of memory execution, and using compiler tools to catch potential issues.
- It's like making sure the right amount of water goes into a cup without overflowing and causing a mess.

Attacks on Wireless Networks:

As work extends beyond traditional offices, people find themselves working remotely in various locations.

- Different types of mobile workers include those who work remotely but stay in one place, employees in versatile environments, individuals needing solutions in various locations, and the ultimate road warrior who spends minimal time in the office.
- Wireless technology plays a crucial role in facilitating this flexibility, with components such as modems, routers, hubs, firewalls, and specific elements for wireless networks.
- The 802.11 standards set by the IEEE govern wireless local area networks, specifying requirements for communication.
- Access points act as central transmitters and receivers for WLAN radio signals.
- Various types of Wi-Fi hotspots, security measures like SSID, WEP, and WPA/WPA2, and the use of MAC addresses are integral to wireless network setups.
- Traditional attack techniques on wireless networks include sniffing, which involves intercepting unsecured wireless data, spoofing to falsify data and gain unauthorized advantages, denial-of-service attacks, man-in-the-middle attacks, and encryption cracking.
- These threats highlight the importance of securing wireless networks in our increasingly mobile work landscape.