CYBER SECURITY

BASIC TERMINOLOGIES:

1. ***VULNERABILITY**: A weakness that can be exploited by cybercriminals to gain unauthorized access to a computer system. After exploiting a vulnerability, a cyber attack can run malicious code, install malware and even steal sensitive data.*

   ***Example**: Taking chances that might lead to rejection.*
   Lack of security cameras.
   Unlocked doors at businesses.
2. ***EXPLOIT**: It is an attack on a computer system, especially one that takes advantage of a particular vulnerability the system offers to intruders.(Used as a verb, exploit refers to the act of successfully making such an attack.)*

   ***Example**: To pretend to befriend an intelligent student in class for the sole purpose of copying his homework.*
3. ***PAYLOAD**: A payload is malware that the threat actor intends to deliver to the victim.*

   ***Example:** Payload is the cargo that produces income, or the bombs or missiles carried by an aircraft. When there are 20 people who paid to go on a plane, these people are an example of the payload.*

4. ***BOT*** ***: A bot is a piece of malware that infects a computer to carry out commands under the remote control of the attacker.***

   Example: ***If someone wrote and posted negative comments about your business on social media platforms such as Facebook etc., but in reality these were generated by fake accounts set up just to post malicious comments.***

5. ***FIREWALL*** ***: A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.***

   Example: ***Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices.***

6. ***DEFENDER*** ***: Defender is in the "position of the interior" Defender serves an organizations goal; attackers have unlimited resources. Defender must defend all points; attackers targets the single weakest link. Defender can only defend against known attacks; attackers can probe for unknown vulnerabilities.***

Example ***: Antivirus and Antispyware programs, Firewall that block unauthorized access to a network and VPNs (Virtual Private Networks) used for secure remote access.***

7. ***MALWARE*** ***: Malware, or malicious software, is any program or file that is intentionally harmful to a computer, network or server.***
   Example : ***computer viruses, worms, Trojan horses, ransomware and spyware.***
8. ***VIRUS*** ***: A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a compute.***
   Example : ***Use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. See malicious code.***
9. ***TROJEN*** ***: A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.***
   Example ***: Zeus Gameover— a peer-to-peer version of the Zeus botnet without a centralized C&C.***
   SpyEye—designed to steal money from online bank account.

10. ***WORM*** ***: A computer worm is a type of malware whose primary function is to self-replicate and infect other computers while remaining active on infected systems. A computer worm duplicates itself to spread to uninfected computers.***

Example: ***Email worms. As you've likely guessed, an email worm's infection vector of choice is email. ...***

Instant messaging worms. ...

File-sharing worms. ...

Internet worms (or network worms) ...

11. ***ADWARE*** ***: can be defined as a bundle of programs that is designed to bombard users with advertisements. The main aim behind it is to redirect the user's search requests to advertising websites and collect marketing data.***

Example ***: Adware tracks user's online activity, slow down the device's performance, displays customized ads and gets malware downloaded at the back end and also eats lots of data costs.***

12. ***CLICKFRAUDClickfraud*** ***:Clickfraud happens when artificially created bogus clicks are used to manipulate Pay-Per-Click (PPC) advertising. The idea behind this practice is to increase the number of payable clicks, in order to generate revenue to advertisers.***

Example: Cybercrooks use Botnet to create these types of scams. Either this practice can be followed by individuals

to manually click the AD hyperlinks or by using automated software or online bots to click these AD links.

13. ***Cyber Espionage : When you hear about Cyber Espionage, characters like James Bond might come to your mind, that pretends to be someone who they're not, infiltrating organizations & also stealing secrets.***
    Example : Similar to that fictional character, Cyber Espionage is the term that describes the practice of spying on someone to gain illicit access to confidential information. The prime target of this cybercrime is typically large institutions and government organizations. But it doesn't mean individuals are too small to fall a victim.
14. ***Dark Web : With so much happening through the Internet, there is so much more in the World Wide Web than it appears. And Dark Web is that part of the Internet that is not visible to regular users.***
    Example : dark sites where all illegal activities are executed.
15. ***Defence-in-Depth : DiD is an approach used to create multiple layers of security to protect information resources/assets and valuable data in an enterprise from attacks. If somehow any mechanism gets fails, another security layer steps up immediately to thwart an attack.***

Example : ***DiD is an approach used to create multiple layers of security to protect information resources/assets and valuable data in an enterprise from attacks. If somehow any mechanism gets fails, another security layer steps up immediately to thwart an attack.***

16. ***Demilitarized Zone : The Demilitarized Zone is known as a firewall setting that separates LAN of an organization from the external network. DMZ makes certain servers available to everyone while keeping the internal LAN access private and accessible to only authorized people.***

    Example : like LAN settings.

17. ***Easter Egg : t's a non-malicious surprise embedded in a program or media which is entertaining and accessible to anyone. It can be found in every software these days, especially in video games.***

    Exampe : It's an intentional joke, hidden message or image usually found on the menu screen.

18. ***End-to-End Encryption: End-to-end encryption is a method of protecting and securing communication that hinders third parties from accessing data when it is transferred from one device to another.***

    Example : For example, whenever you do online shopping using your credit card. Your mobile phone needs to send the credit card to the merchant. It's End-to-end

encryption method that just makes sure that only you and the merchant's device can access the confidential credentials.

19. ***Evil Twin : An evil twin is a fake Wi-Fi hotspot or access point that poses to be original and safe, but it's actually set up to snoop on another wireless network.***
    Example : fake wifi hotspot.
20. ***Exploit Kits: Exploit Kits are basically the package of automated threats that are used by attackers to launch exploits against vulnerable programs. Exploits are designed to cause unexpected behaviors that an attacker can take advantage of to perform harmful actions.***
    Example : by using installation of packages.
21. ***Hashing: Hashing is an encryption algorithm that converts the plaintext password into hashes. It's a form of cryptographic security method that is used to transform strings of characters in shorter fixed-length value that poses as the original string.***
    Example: When a user wants to send a secure message, a hash is generated & encrypted to the intended message & is send along. When the message is sent to the end, the receiver decrypts the hash as well as message to read it.

22. ***IDS : Intrusion Detection System is software or device that functions to monitor network traffic for malicious activity.***

Example : These detection systems help in identifying suspicious activity, log information related and attempts to block and report it.

23. ***IPSPOOFING : IP Spoofing or IP Address Forgery is a hijacking technique in which a cracker pretends as a trusted host to disguise someone's identity, hijack browsers, or gain access to a network. Though it's not illegal to spoof an IP Address, as you're just faking your address to hide your online activities and be anonymous.***

Example :However, if someone uses the technique to masquerades as someone else and indulges in criminal activities such as identity theft, then it's illegal.

24. ***KEYLOGGER: Keylogger is a computer program that keeps a log of your keystrokes on your keyboard. The entire log is saved in a log file which is encrypted and can be shared with different receivers for different purposes. It can be used for both legal and illegal means. It can track all the sensitive information***

Example :like passwords and PIN (Personal Identification Number) in real-time and can be used for hijacking your ***personal accounts.***

25. ***MACROVIRUS*** : ***A macro virus is a small piece of code which is lodged into the macros of different documentation and software programs such as spreadsheets and word documents. Whenever a user opens up the document affected with a macro virus, a series of actions begins automatically.***

EXAMPLE :The macro virus replicates rapidly upon sharing the document with multiple nodes.

26. ***MOBILEBANKING TROJAN:Users who are very frequent in using electronic gadgets for banking purposes are most liable to get affected by Mobile Banking Trojans. The influence begins with overlaying of Trojan's interface over Banking app's interface. When the user input their credentials to login into their account, Trojan loots them and impersonates user's account.***

Example : Acecard family and Faketone Trojans were very effective in a cyber plague in 2016 which took over dozens of banking applications in Russia.

27. ***Passwordsniffing*****: Password Sniffing is the process of intruding between a transfer of data packets which encompasses password. The process is performed by a software application called Password Sniffer which captures the data packets which contains password and stores it for illegal and malicious purposes**.

Example: SniffPass from NirSoft.

Password Sniffer Spy.
FTP password sniffer.

28. QAZ: ***IT is a famous backdoor trojan that launches the untampered version of notepad.exe into systems, that allows hackers to link and gain access to the affected computer.***

Example : This is network worm with backdoor capabilities, which spreads itself under Win32 systems. The worm was reported in-the-wild in July-August, 2000. The worm itself is Win32 executable file and about 120K long, written in MS Visual C++.

29. ***RANSOMEWARE : It can be any malicious software that encrypts data found on an individual's or enterprise system. Once the data gets encrypted in wrong hands, the victim is demanded a huge amount of money i.e. ransom.***

Example : CryptoLocker. CryptoLocker is ransomware that was first spotted in 2007 and spread via infected email attachments.

30. ***PHISHING: a hacker strives to steal your personal information such as passwords and e-mails. Phishing is done primarily through false e-mails that appear to be sent through a legitimate site such as Amazon or e-bay.***

Example :The e-mail asks you to update or validate yourself by providing the username and password in

order to read the information. Scammers then take the total control of your account and thieve your information such as bank account's information etc.