1.1 LEARNING OBJECTIVES

This unit purports at making you understand:

- What constitutes a cyber-attack,
- Types of cyber-attacks, and
- What motivates attacker(s) to do carry out attack(s).

1.2 INTRODUCTION

Everyone among us has one time or another has come across some form of attack. It could be physical or emotional or of some other kind. The intent is to cause some sort of harm – though sometimes it turn into a blessing in disguise. However, cyber attacks always aim at causing harm. They can be varied in their nature of approach and type of harm they inflict, depending on the motive, but the purpose is certainly malicious.

All of you must have encountered a situation when some unwanted changes, like installing some software or change your search engine, are made to your system or seen unwanted advertisements popping up while surfing Internet. These are examples of cyber attacks. These can range from being minor nuisance, like occasional popups, to creating havoc, like formatting hard disk.

1.3 CYBER ATTACK

Farhat et al[1] on 'What is a cyber attack' state as below:

A cyber attack is an attack initiated from a computer against a website, computer system or individual computer (collectively, a computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it.

According to Anonymous[2], "Cyber-attack is any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous

[1] http://www.hklaw.com/files/Publication/bd9553c5-284f-4175-87d2849aa07920d3/Presentation/PublicationAttachment/1880b6d6-eae2-4b57-8a97 9f4fb1f58b36/CyberAttacksPreventionand ProactiveResponses.pdf

[2] https://en.wikipedia.org/wiki/Cyber-attack

source that either steals, alters, or destroys a specified target by hacking into a susceptible system. These can be labeled as either a Cyber campaign, cyber warfare or cyber terrorism in different context. Cyber-attacks can range from installing spyware on a PC to attempts to destroy the infrastructure of entire nations."

In a nutshell, use of a device/system against another system/device with a malicious intent constitutes a cyber-attack.

1.4 TYPES OF CYBER ATTACK OR THREATS

Anonymous[3] gives a comprehensive list of cyber-attacks/threats which is reproduced below:

1. Backdoors – Backdoors[4] is bypassing normal authentication. Backdoor is a type of cyber threat in which the attacker uses a back door to install a key logging software, thereby allowing an illegal access to your system. This threat can turn out to be potentially serious as it allows for modification of the files, stealing information, installing unwanted software or even taking control of the entire computer.

   Default passwords can function as backdoors if they are not changed by the user. Some debugging features can also act as backdoors if they are not removed in the release version.

   Many computer worms, such as Sobig and Mydoom, install a backdoor on the affected computer (generally a PC on broadband running Microsoft Windows and Microsoft Outlook). Such backdoors appear to be installed so that spammers can send junk e-mail from the infected machines. Others, such as the Sony/BMG rootkit distributed silently on millions of music CDs through late 2005, are intended as DRM measures—and, in that case, as data gathering agents, since both surreptitious programs they installed routinely contacted central servers.

   A sophisticated attempt to plant a backdoor in the Linux kernel, exposed in November 2003, added a small and subtle code change by subverting the revision

[3] http://www.cybersecuritycrimes.com/types-of-cyber-attacks/

[4] https://en.wikipedia.org/wiki/Backdoor_(computing)

control system. In this case, a two-line change appeared to check root access permissions of a caller to the sys_wait4 function, but because it used assignment = instead of equality checking ==, it actually granted permissions to the system. This difference is easily overlooked, and could even be interpreted as an accidental typographical error, rather than an intentional attack.

In January 2014, a backdoor was discovered in certain Samsung Android products, like the Galaxy devices. The Samsung proprietary Android versions are fitted with a backdoor that provides remote access to the data stored on the device. In particular, the Samsung Android software that is in charge of handling the communications with the modem, using the Samsung IPC protocol, implements a class of requests known as remote file server (RFS) commands, that allows the backdoor operator to perform via modem remote I/O operations on the device hard disk or other storage. As the modem is running Samsung proprietary Android software, it is likely that it offers over-the-air remote control that could then be used to issue the RFS commands and thus to access the file system on the device.

2. Denial-of-Service Attack – A denial-of-service (DoS) attack is attacking the network to bring it down completely with useless traffic by affecting the host device which is connected to the Internet. DoS attack targets websites or services which are hosted on the servers. This type of attack can aim bank servers and credit card payment gateways.
3. Direct-access Attack – A direct-access attack simply means gaining physical access to the computer or its part and performing various functions or installing various types of devices to compromise security. The attacker can install software loaded with worms or download important data, using portable devices.
4. Eavesdropping – As the name suggests, eavesdropping means secretly listening to a conversation between the hosts on a network. There are various programs such as Carnivore and Narus Insight that can be used to eavesdrop.
5. Spoofing – Spoofing is a cyber attack where a person or a program impersonate another by creating false data in order to gain illegal access to a system. Such threats are commonly found in emails where the sender’s address is spoofed.
6. Tampering – Tampering is a web based attack where certain parameters in the

URL are changed without the customer's knowledge; and when the customer keys in that URL, it looks and appears exactly the same. Tampering is basically done by hackers and criminals to steal the identity and obtain illegal access to information.

7. Repudiation Attack – A repudiation attack occurs when the user denies the fact that he or she has performed a certain action or has initiated a transaction. A user can simply deny having knowledge of the transaction or communication and later claim that such transaction or communication never took place.
8. Information Disclosure – Information disclosure breach means that the information which is thought to be secured is released to unscrupulous elements who are not trustworthy.
9. Privilege Escalation Attack – A privilege escalation attack is a type of network intrusion which allows the user to have an elevated access to the network which was primarily not allowed. The attacker takes the advantage of the programming errors and permits an elevated access to the network.
10. Exploits – An exploit attack is basically a software designed to take advantage of a flaw in the system. The attacker plans to gain easy access to a computer system and gain control, allows privilege escalation or creates a DOS attack.
11. Social Engineering – An attack by a known or a malicious person is known as social engineering. They have knowledge about the programs used and the firewall security and thus it becomes easier to take advantage of trusted people and deceive them to gain passwords or other necessary information for a large social engineering attack.
12. Indirect Attack – Indirect attack means an attack launched from a third party computer as it becomes more difficult to track the origin of the attack.
13. Computer Crime – A crime undertaken with the use of a computer and a network is called as a computer crime.
14. Malware – Malware refers to malicious software that are being designed to damage or perform unwanted actions into the system. Malware is of many types like viruses, worms, Trojan horses, etc., which can cause havoc on a computer's hard drive. They can either delete some files or a directory or simply gather data

without the actual knowledge of the user.

15. Adware – Adware is a software that supports advertisements which renders ads to its author. It has advertisements embedded in the application. So when the program is running, it shows the advertisement. Basically, adware is similar to malware as it uses ads to inflict computers with deadly viruses.
16. Bots – Bots is a software application that runs automated tasks which are simple and repetitive in nature. Bots may or may not be malicious, but they are usually found to initiate a DoS attack or a click fraud while using the internet.
17. Ransomware – Ransomware is a type of cyber security threat which will restrict access to your computer system at first and will ask for a ransom in order for the restriction to be removed. This ransom is to be paid through online payment methods only which the user can be granted an access to their system.
18. Rootkits – A rootkit is a malicious software designed in such a way that hides certain process or programs from normal anti-virus scan detection and continues to enjoy a privilege access to your system. It is that software which runs and gets activated each time you boot your system and are difficult to detect and can install various files and processes in the system.
19. Spyware – Spyware, as the name suggests, is a software which typically spies and gathers information from the system through a user's internet connection without the user's knowledge. A spyware software is majorly a hidden component of a freeware program which can be downloaded from the internet.
20. Scareware – Scareware is a type of threat which acts as a genuine system message and guides you to download and purchase useless and potentially dangerous software. Such scareware pop-ups seem to be similar to any system messages, but actually aren't. The main purpose of the scareware is to create anxiety among the users and use that anxiety to coax them to download irrelevant softwares.
21. Trojan Horses – Trojan Horses are a form of threat that are malicious or harmful codes hidden behind genuine programs or data which can allow complete access to the system and can cause damage to the system or data corruption or loss/theft of data. It acts as a backdoor and hence it is not easily detectable.

22. Virus – A computer virus is a self replicating program which, when executed, replicates or even modifies by inserting copies of itself into another computer file and infects the affected areas once the virus succeeds in replicating. This virus can be harmful as it spreads like wildfire and can infect majority of the system in no time.

23. Worm – Just like a virus, worm is a self replicating program which relies on computer network and performs malicious actions and spreads itself onto other computer networks. Worms primarily rely on security failures to access the infected system.

24. Phishing – Phishing is a cyber threat which makes an attempt to gain sensitive information like passwords, usernames and other details for malicious reasons. It is basically an email fraud where the perpetrator sends a legitimate looking email and attempts to gain personal information.

25. Identity Theft – Identity theft is a crime wherein your personal details are stolen and these details are used to commit a fraud. An identity theft is committed when a criminal impersonates individuals and use the information for some financial gain.

26. Intellectual Property Theft – Intellectual Property theft is a theft of copyrighted material where it violates the copyrights and the patents. It is a cybercrime to get hands onto some trade secrets and patented documents and research. It is basically a theft of an idea, plan and the methodology being used.

27. Password Attacks – Password attack is a form of a threat to your system security where attackers usually try ways to gain access to your system password. They either simply guess the password or use an automated program to find the correct password and gain an entry into the system.

28. Bluesnarfing – Bluesnarfing is a threat of information through unauthorized means. The hackers can gain access to the information and data on a Bluetooth enabled phone using the wireless technology of the Bluetooth without alerting the user of the phone.

29. Bluejacking – Bluejacking is simply sending of texts, images or sounds, to another Bluetooth enabled device and is a harmless way of marketing. However, there is a thin line between bluejacking and bluesnarfing and if crossed it results

into an act of threat.

30. DDoS – DDoS basically means a Distributed Denial of Service. It is an attempt to make any online service temporarily unavailable by generating overwhelming traffic from multiple sources or suspend services of a host connected to the internet.

31. Keylogger – A keylogger is a spyware that has the capability to spy on the happenings on the computer system. It has the capability to record every stroke on the keyboard, web sites visited and every information available on the system. This recorded log is then sent to a specified receiver.

1.5 MOTIVATION

Depending on the motivation, according to Ray[5], Verisign iDefense Security Intelligence Services classifies cyber-attacks into three categories: hacktivism, cyber crime and cyber- espionage.

Hacktivism is the act of hacking, or breaking into a computer system, for a politically or socially or ideologically motivated purpose. It is basically used as a means to promote an agenda. Hacktivists are responsible for denial-of-service (DoS), distributed denial of service (DDoS), information theft, data breaches, web site defacement, typosquatting(URL hijacking relying on typographical errors in URL spelling) and many other acts of digital sabotage.

Cyber crime, though, in a broad sense, covers any illegal activity that is committed through a digital means, here it refers to an activity with the monetary gain in mind. Such an activity can be a direct one, e.g., fraudulent bank transaction, or an indirect one, e.g., selling stolen information in black market. Frequently used cyber crime tools are ATM and point-of-sale (PoS) skimming, RAM scrapping, code injection, key logging and phishing to extract confidential personal information.

Cyber espionage is unauthorized spying by computer[6]. However, a more

[5] http://www.circleid.com/posts/understanding_the_threat_landscape_cyber_attack_actors_and_motivations

[6] http://www.pcmag.com/encyclopedia/term/64376/cyber-espionage

comprehensive definition, and the associated tools, is given by Anonymous[7] which is as below:

Cyber spying, or cyber espionage, is the act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers through the use of cracking techniques and malicious software including Trojan horses and spyware. It may wholly be perpetrated online from computer desks of professionals on bases in far away countries or may involve infiltration at home by computer trained conventional spies and moles or in other cases may be the criminal handiwork of amateur malicious hackers and software programmers.

John Arquilla (a US expert on national security affairs and defense analysis) added to new dimension to motivation behind cyber attacks by coining the term cyber warfare or cyber war. Cyber warfare has been defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption," but other definitions also include non-state actors, such as terrorist groups, companies, political or ideological extremist groups, hacktivists, and transnational criminal organizations[8].

The above definition of cyber espionage is very likely to raise some confusion as to whether it does not cover cyber war. It does not, which has been made clear by Anonymous[8] as below:

‘Cyber "war" is simply the act of fighting on an electronic battlefield with digital weapons. To attack an adversary’s capabilities in an effort to disable or destroy their ability to get things done. This may be completely digital in nature (such as communication and information systems) or the electronics that monitor and manage physical infrastructure, like power and water systems. Hostile code like StuxNet is an example of such weapons for cyber warfare.

Cyber "espionage" on the other hand is the act of obtaining information that is held in secrecy by the adversary. This in itself is not the end game - this information is

[7] https://en.wikipedia.org/wiki/Cyber_spying
[8] https://en.wikipedia.org/wiki/Cyberwarfare

then used for some sort of gain or strategic advantage. It must have an intrinsic value to the adversary, or its useless. In many cases, this may be to gain financial / competitive advantage in the business world, or strategic advantage over political communities of conflict.

Now here is where it gets complicated and is the source of much of the confusion. Cyber espionage is routinely used as a precursor to a cyber warfare strike. This allows an adversary to do reconnaissance in aid of an attack. In the movies, this would be sending in the recon patrol in the military to disable an enemy's capabilities before a major attack, or sending a spy into the enemy territory to gather intel before the strike. And this happens in the real world too.

Typically though cyber espionage is a covert operation that takes months or years to commit. It usually comes with signs of exfiltration and with the right tools can be tracked back to the source, with some level of certainty. Cyber warfare is different. The attack is usually pretty fast, striking in seconds and causing damage for use with other objectives.'

It must be noted that a perpetrator may belong to more than category of attack. For example, politically motivated cyber attacks may be carried out by members of extremist groups who use cyberspace to spread propaganda, attack websites, and steal money to fund their activities or to plan and coordinate physical-world crime[9].

The figure below shows worldwide motivation statistics, typically for April 2015. It clearly shows that most attacks (> 50%) fall under category 'cyber crime' whereas about one third belong to hacktivism. This is obvious from the fact that these two categories consist of mainly individuals and groups and require less resources whereas 'cyber espionage' and 'cyber warfare' usually require greater resources and, in many cases, government backing.

[9] https://en.wikipedia.org/wiki/Cyberwarfare

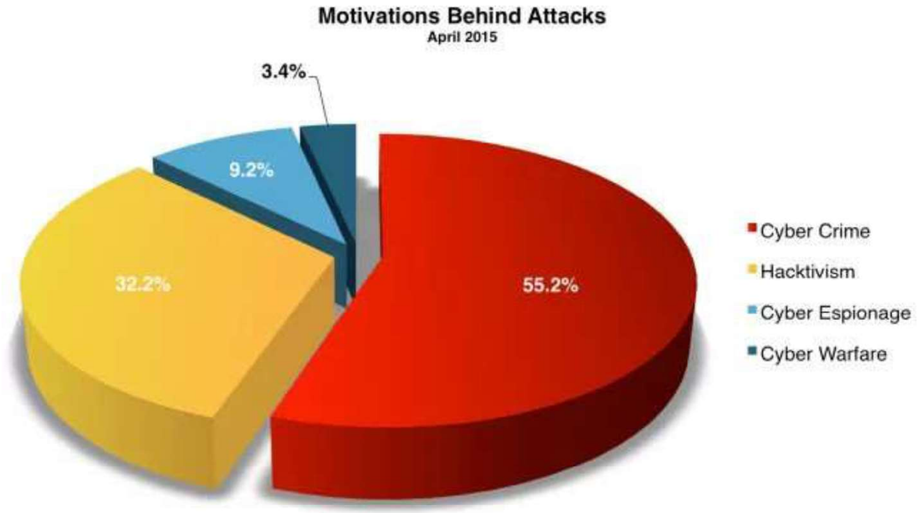

Figure 1: Motivation behind attacks[10]

1.6 LET US SUM UP

1. A **cyber attack** is an attack initiated from a computer against a website, computer system or individual computer (collectively, a computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it.
2. **Hacktivism** is the act of hacking, or breaking into a computer system, for a politically or socially or ideologically motivated purpose.
3. **Cyber crime,** though, in a broad sense, covers any illegal activity that is committed through a digital means, here it refers to an activity with the monetary gain in mind.
4. **Cyber espionage** is unauthorized spying by computer.
5. **Cyber war** is simply the act of fighting on an electronic battlefield with digital weapons

[10] http://www.hackmageddon.com/category/security/cyber-attacks-statistics/