Task#6

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

· **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

· **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

· **Information security** protects the integrity and privacy of data, both in storage and in transit.

· **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

· **Disaster recovery and business continuity** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

· **End-user education** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

The scale of the cyber threat

The global cyber threat continues to evolve at a rapid pace, with a rising number of data breaches each year. A report by **RiskBased Security** revealed that a shocking 7.9 billion records have been exposed by data breaches in the first nine months of 2019 alone. This figure is more than double (112%) the number of records exposed in the same period in 2018.

Medical services, retailers and public entities experienced the most breaches, with malicious criminals responsible for most incidents. Some of these sectors are more appealing to cybercriminals because they collect financial and medical data, but all businesses that use networks can be targeted for customer data, corporate espionage, or customer attacks.

Task#6

With the scale of the cyber threat set to continue to rise, the **International Data Corporation** predicts that worldwide spending on cyber-security solutions will reach a massive $133.7 billion by 2022. Governments across the globe have responded to the rising cyber threat with guidance to help organizations implement effective cyber-security practices.

In the U.S., the National Institute of Standards and Technology (NIST) has created a cyber-**security framework**. To combat the proliferation of malicious code and aid in early detection, the framework recommends continuous, real-time monitoring of all electronic resources.

The importance of system monitoring is echoed in the "**10 steps to cyber security**", guidance provided by the U.K. government's National Cyber Security Centre. In Australia, **TheAustralian Cyber Security Centre**(ACSC) regularly publishes guidance on how organizations can counter the latest cyber-security threats.

Types of cyber threats

The threats countered by cyber-security are three-fold:

1. **Cybercrime** includes single actors or groups targeting systems for financial gain or to cause disruption.

2. **Cyber-attack** often involves politically motivated information gathering.

3. **Cyberterrorism** is intended to undermine electronic systems to cause panic or fear.

So, how do malicious actors gain control of computer systems? Here are some common methods used to threaten cyber-security:

Malware

Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

There are a number of different types of malware, including:

· **Virus:** A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.

· **Trojans:** A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.

· **Spyware:** A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.

Task#6

· **Ransomware:** Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.

· **Adware:** Advertising software which can be used to spread malware.

· **Botnets:**Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

SQL injection

An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

Phishing

Phishing is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

Man-in-the-middle attack

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure WiFi network, an attacker could intercept data being passed from the victim's device and the network.

Denial-of-service attack

A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

Latest cyber threats

What are the latest cyber threats that individuals and organizations need to guard against? Here are some of the most recent cyber threats that the U.K., U.S., and Australian governments have reported on.

Dridex malware

In December 2019, the U.S. Department of Justice (DoJ) charged the leader of an organized cyber-criminal group for their part in a global Dridex malware attack. This malicious campaign affected the public, government, infrastructure and business worldwide.

Task#6

Dridex is a financial trojan with a range of capabilities. Affecting victims since 2014, it infects computers though phishing emails or existing malware. Capable of stealing passwords, banking details and personal data which can be used in fraudulent transactions, it has caused massive financial losses amounting to hundreds of millions.

In response to the Dridex attacks, the U.K.'s National Cyber Security Centre advises the public to "ensure devices are patched, anti-virus is turned on and up to date and files are backed up".

Emotet malware

In late 2019, **The Australian Cyber Security Centre** warned national organizations about a widespread global cyber threat from Emotet malware.

Emotet is a sophisticated trojan that can steal data and also load other malware. Emotet thrives on unsophisticated password: a reminder of the importance of creating a secure password to guard against cyber threats.

Pegasus is a **spyware** developed by the Israeli cyberarms firm NSO Group that can be covertly installed on mobile phones (and other devices) running most versions of iOS and Android. The 2021 Project Pegasus revelations suggest that the current Pegasus software can exploit all recent iOS versions up to iOS 14.6.As of 2016, Pegasus was capable of reading text messages, tracking calls, collecting passwords, location tracking, accessing the target device's microphone and camera, and harvesting information from apps.The spyware is named after the mythical winged horse Pegasus—it is a Trojan horse that can be sent "flying through the air" to infect phones.

NSO Group was previously owned by American private equity firm Francisco Partners,but it was bought back by its founders in 2019.The company states that it provides "authorized governments with technology that helps them combat terror and crime.NSO Group has published sections of contracts which require customers to use its products only for criminal and national security investigations and has stated that it has an industry-leading approach to human rights.

Pegasus was discovered in August 2016 after a failed installation attempt on the iPhone of a human rights activist led to an investigation revealing details about the spyware, its abilities, and the security vulnerabilities it exploited. News of the spyware caused significant media coverage. It was called the "most sophisticated" smartphone attack ever, and marked the first time that a malicious remote exploit using jailbreak to gain unrestricted access to an iPhone had been detected.

On August 23, 2020, according to intelligence obtained by the Israeli newspaper *Haaretz*, NSO Group sold Pegasus spyware software for hundreds of millions of US dollars to the United Arab Emirates and the other Gulf States, for surveillance of anti-regime activists, journalists, and political leaders from rival nations, with encouragement and mediation by the Israeli government.Later, in December 2020, the Al Jazeera investigative show The Tip of the

Task#6

Iceberg, *Spy partners*, exclusively covered Pegasus and its penetration into the phones of media professionals and activists; and its use by Israel to eavesdrop on both opponents and allies.

In July 2021, widespread media coverage part of the Project Pegasus revelations along with an in-depth analysis by human rights group Amnesty International uncovered that Pegasus was still being widely used against high-profile targets. It showed that Pegasus was able to infect all modern iOS versions up to iOS 14.6, through a zero-click iMessage exploit.

Task#6

I have learned a lot from verzeo internship program and one of the topic is social engineering attacks.

Learned how hacker's create a clone website and to understand working behind the phishing attack .And how we can protect ourself and society.

To create a clone website and use script to save the entered data in a log file and to identify phishing websites.

Procedure:

1. **Create clone website using html and css or we can also save the web structure directly from the official website in html extension.**
2. **Now we need to create a script to save the credential in a file here,we will be using php for scripting.**
3. **Now we have to create a log.txt file where the credential will be saved.**
4. **After completing the coding part we now have to host the website on a server,we will be hosting it on our local system for that we first need to make our system a server.**
5. **Download xampp or wampp software these are used to make the system a server.**
6. **Now,finally we will upload or copy and paste the all three files to xampp or wampp installation file folder.**
7. **When the victim open's the url received on email or from any social media platform and enters the credentials into the website it gets stored in log.txt file.**

***Warning:Do not try this on any one else as it is illegal and is only for testing purpose.**