SCHOOL OF CONTINUING AND DISTANCE EDUCATION

JAWAHARLAL NEHRU TECHNOLOGICALUNIVERSITY - HYDERABAD

Kukatpally, Hyderabad – 500 085, Telangana, India.

SIX MONTH ONLINE CERTIFICATE COURSES – 2023

CYBER SECURITY - ASSIGNMENT - 01

1) Prepare a Case Study on the shortage of cybersecurity professionals in India, its impact on organizations, and the measures needed to address this challenge.

Ans: The field of cybersecurity has recently witnessed several innovative solutions. Businesses can now benefit from technologies such as Zero Trust security, which involves continuous user and device authentication and authorization before network access is granted. Additionally, XDR (Extended Detection and Response) unifies multiple security solutions, automating the detection and response to threats. The combination of Artificial Intelligence (AI) and Natural Language Processing (NLP) has also shown promise in content moderation and detecting harmful content.

On the consumer side, cybersecurity technologies such as GoDeep.AI, a self-aware malware-hunting solution, have significantly reduced threat detection time. Biometric and facial analysis technologies have also been introduced to securely and accurately authenticate users. These innovative solutions utilize various techniques like deep learning, behavioral analysis, and predictive analytics to monitor systems, identify cyber-attacks, and use voice and iris scans to authenticate users. It's important to note that these technologies are continually evolving to cater to the future's cybersecurity needs.

Over the past year, we have witnessed a surge in the frequency and complexity of cyberattacks. Our enterprise arm, SEQRITE, released an annual threat prediction report, which accurately predicted 12 out of 15 cybersecurity threats. The rise in cyberattacks, combined with an increased awareness of the need for robust cybersecurity infrastructure, as reflected in the union budget, will drive individuals, enterprises, and regulators to focus more on cybersecurity. The proliferation of IoT, AI technologies, and 5G has led to a surge in the number of connected devices, which presents a greater risk of vulnerabilities for both individuals and organizations. This, coupled with the lack of cybersecurity awareness, rapid digitization, and remote work caused by the pandemic, creates a perfect storm of vulnerabilities.

Individuals and organizations must allocate adequate resources and prioritize the adoption and strengthening of their cybersecurity infrastructure to prevent and safeguard against these newer and more complex threats. By doing so, we can achieve a cyber-safe India, and mitigate the risks that come with our increasingly digitized and interconnected world.

Increasing demand for skilled cybersecurity professionals

As cyberattacks continue to increase globally, the demand for skilled cybersecurity professionals is growing. Despite adding more than 464,000 workers in the past year, globally cybersecurity workforce gap has grown more than twice as much as the workforce with a 26.2% year-over-year increase. Unfortunately, there is a steep shortage of skilled professionals in this field. Nearly 70% of the enterprises feel they do not have enough cybersecurity professionals to ensure implementation of best practices. Even with growing focus to automate systems, skilled cybersecurity professionals are needed to ensure that the deployed cybersecurity solutions are effective.

2) Analyze a significant cyber attack(s) that has affected an Indian organization or institution. Evaluate the specific challenges faced, the response to the incident, and the lessons learned.

Ans: In computers and computer networks an attack is any attempt to expose, alter, disable, destroy, steal or gain information through unauthorized access to or make unauthorized use of an asset. A cyberattack is any type of offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices. An attacker is a person or process that attempts to access data, functions or other restricted areas of the system without authorization, potentially with malicious intent. Depending on context, cyberattacks can be part of cyberwarfare or cyberterrorism. A cyberattack can be employed by sovereign states, individuals, groups, society or organizations, and it may originate from an anonymous source. A product that facilitates a cyberattack is sometimes called a cyberweapon.

India ranks 3rd in terms of the highest number of internet users in the world after USA and China.

In a recent study, it was revealed that out of 15 Indian cities, Mumbai, New Delhi, and Bengaluru have faced the maximum number of cyber attacks.

JULY 2016 - "UNION BANK OF INDIA HEIST"

MAY 2017 - "WANNACRY RANSOMWARE"

MAY 2017 - "DATA THEFT AT ZOMATO "

1. Cosmos Bank Cyber Attack in Pune:

A recent cyber attack in India 2018 was deployed on Cosmos Bank in Pune. This daring attack shook the whole banking sector of India when hackers siphoned off Rs. 94.42 crore from Cosmos Cooperative Bank Ltd. in Pune.

Hackers hacked into the bank's ATM server and took details of many visas and rupee debit cardholders. Money was wiped off while hacker gangs from around 28 countries immediately withdrew the amount as soon as they were informed.

Prevention: Hardening of the security systems by limiting its functions and performance only to authorized people can be the way forward. Any unauthorized access to the network should immediately set an alarm to block all the access to the bank's network. Also, to minimize risk, enabling a two-factor authentication might help.

2. **Websites Hacked: 2017 - 2018**

Over 22,000 websites were hacked between the months of April 2017 and January 2018. As per the information presented by the Indian Computer Emergency Response Team, over 493 websites were affected by malware propagation including 114 websites run by the government. The attacks were intended to gather information about the services and details of the users in their network.

Prevention: Using a more secure firewall for network and server which can block any unauthorized access from outside the network is perhaps the best idea. Personal information of individuals is critical for users and cannot be allowed to be taped into by criminals. Thus, monitoring and introducing a proper network including a firewall and security system may help in minimizing the risk of getting hacked.

3) Investigate the top cybersecurity problems faced by universities and colleges, with a focus on the specific types of cyberattacks targeting higher education institutions.

Ans: **User accounts and Administration;**

General user accounts

General purpose users should access their accounts as per instruction of faculty.

Special user accounts

Students should not access this account without prior permission of faculty.

Physical Security

(a) Users should maintain the physical security of the system.

(b) Users and lab assistants should monitor the lab and its premises from time to time.

(c) They should make a close watching procedure on CCTV cameras and should maintain CCTV cameras in good working conditions.

(d) Lab in-Charges should ensure security management of entrance and exit of lab premises.

(e) Lab in-Charges should keep the necessary records of lab timing and asset management.

Password handling

(a) Password records should be maintained.

(b) Password policy should be implemented fortnightly.

(c) Passwords of each account should be kept in common records on different pages.

User and access rights assignment

(a) Administrator accounts should be maintained by Institutes.

(b) Administrators should implement security policies as per requirement.

(c) Administrator should audit all computers and keep records.

Network and communication security

(a) Use of network services and its resources will be formulated by the head of the Cyber team and national IT security policy. The policy clears the methodology that users must follow to access authorized networks and resources.

(b) Equipment like network devices and terminals will be configured to automatically identify the device on a network. Devices must confirm its identity to complete the handshake with network devices.

(c) Usage of third-party applications for remote access on a network, like zoom meetings, Teams, Webex, and VNC should be avoided on official networks.

(d) Routing restrictions must follow within the network connections to secure the valuable information of the college/university.

4) Select and analyze three real-world malware attacks, covering different malware types such as viruses, worms, and ransomware. For each case, describe the attack vector, the target, the impact.

Ans: some of these malware attack are:

1. Emotet Trojan

One of the most notorious malware examples in recent years is the Emotet trojan. This highly sophisticated form of malware initially surfaced around 2014 as a banking trojan, aimed at stealing financial data. However, over the years, it has evolved into a far more versatile threat.

Emotet's primary modus operandi involves sending phishing emails to unsuspecting victims. These emails typically contain a malicious attachment or link that, when opened, allows the malware to infiltrate the victim's system. Once inside, Emotet can cause a variety of problems, from stealing sensitive information to damaging software.

Despite numerous attempts to take down the Emotet network, it remains a significant threat in the cyber world. Its ability to adapt and evolve makes it a particularly challenging form of malware to combat.

How this attack could have been prevented: Preventing this attack would involve training and educating individuals about the dangers of phishing emails, and using robust anti-phishing solutions that can detect and block phishing attempts. Up-to-date antivirus software that can detect and remove threats like Emotet would help to protect individual systems.

2. CovidLock

The CovidLock malware is an example of cyber criminals exploiting a global crisis for their malicious intent. As the name suggests, this malware surfaced during the COVID-19 pandemic, preying on people's fears and uncertainties about the virus.

CovidLock masquerades as a legitimate COVID-19 tracking app. However, once downloaded, it locks the user's phone and demands a ransom to unlock it. During the pandemic, CovidLock quickly gained notoriety due to its opportunistic nature.

While authorities have since managed to break the ransomware's encryption code, CovidLock serves as a stark reminder of how cyber threats can emerge in the most unexpected circumstances.

How this attack could have been prevented: This malware attack could have been avoided by educating users to only download apps from trusted sources like the Google Play Store or Apple App Store. Updated antivirus software on mobile devices would also add an extra layer of protection.

3. Kaseya Ransomware

The Kaseya ransomware attack is another example of a high-profile cyber security incident. In July 2021, a Russia-linked ransomware group known as REvil targeted Kaseya, a company that provides software tools to IT outsourcing shops.

The attack affected as many as 1,500 businesses worldwide and resulted in a demand for a staggering $70 million ransom. Although Kaseya swiftly responded to the incident and worked with cybersecurity firms to mitigate its impact, the attack underscored the vulnerability of supply chains to ransomware attacks.

How this attack could have been prevented: On the one hand, Kaseya could have better protected its development environment and prevented attackers from penetrating it and delivering malware to its clients. On the other hand, Kaseya customers should have implemented better software supply chain security, performing careful security testing for software packages deployed in their environments.

Viruses

A virus is one of the most common malware examples. Named for their ability to spread and infect just like a biological virus, these malicious programs attach themselves to clean files and spread throughout a computer system, corrupting files and damaging the system's operation. Viruses can be particularly destructive, as they can delete files or reformat a hard drive.

The primary method of virus transmission is through a carrier, which is usually an executable file. This means the virus can lie dormant on a system until the infected file is executed. Once activated, it can replicate itself, attach to other programs, and continue its spread.

Protective measures: Protection against viruses includes installing a reliable antivirus program, being cautious when downloading and opening files, and regularly updating software to patch any vulnerabilities.

Worms

Unlike viruses, worms can spread without user action. They exploit vulnerabilities in operating systems, automatically spreading from computer to computer. Worms can consume bandwidth or overload a system's resources, causing it to become slow or unresponsive.

Because worms can replicate themselves, they can spread at an alarming rate. A single worm can generate hundreds or thousands of copies of itself, creating a massive network problem in a short period.

Protective measures: To protect against worms, it's essential to keep system and software up-to-date. Regular patching of vulnerabilities and the use of a good firewall can also help to keep these nasty invaders at bay.

Ransomware

Ransomware is a type of malware that locks a user out of their files or computer until they pay a ransom. It essentially holds data hostage. In recent years, ransomware attacks have been on the rise, affecting businesses, governments, and individuals alike.

Ransomware can enter a system through a variety of methods, including phishing emails or exploiting security holes in software. Once installed, it encrypts files and displays a ransom note, demanding payment (usually in cryptocurrency) in exchange for the decryption key.

Traditional protective measures: To protect against ransomware, perform regular backups of important data, update software, and be cautious of suspicious emails and downloads.

Protecting against ransomware with Perception Point: Perception Point Advanced Email Security provides HAP™ (hardware assisted platform), a dynamic engine that combines CPU-level data with innovative software algorithms to neutralize unknown threats, including ransomware. The HAP technology acts earlier in the kill chain than any other solution. It blocks ransomware attacks at the exploit phase, before it is released and causes any damage on the device.

5) Provide Comparative Analysis on DES, AES, RSA.

DES	AES	RSA
DES stands for Data Encryption Standard	AES stands for Advanced Encryption Standard	RSA acronym for Rivest, Adi Shamir
Key length is 56 bits	It uses various lengthsof the key Suchas 128, 192 and 256 bits	>1024 bits
It uses the Symmetric algorithm	It uses the Symmetric algorithm	It uses the Asymmetric algorithm
DES is developed in the year by 1977	AES is developed in the year by 2000	RSA is developed in the year by 1978
DES uses 6 rounds to encrypt and decrypt the text	AES uses 10/12/14 rounds to encrypt and decrypt the text	RSA uses 1 round to encrypt and decrypt the text
Encryption and Decryption process is moderate	Encryption and decryption process is faster	Encryption and Decryption process is slower
Security is not enough	It has excellent security	Low and poor security

Implementation of DES is, when compared with the software,hardware gives the better performance	It will become faster	Not as efficient or competent
Inherent vulnerabilities are Brute-Forced and Cryptanalysis Attack	For this Brute-Force attack only	RSA inherent vulnerabilities are Oracle and Brute-Forced attack