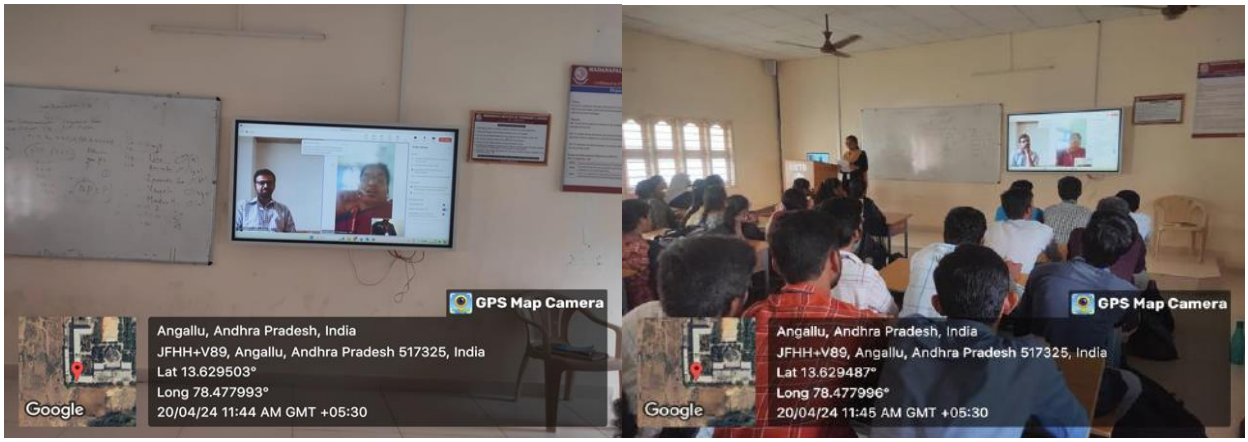
MITS
MADANAPALLE INSTITUTE OF TECHNOLOGY & SCIENCE
(UGC-AUTONOMOUS INSTITUTION)
Estd 1998

NBA NATIONAL BOARD OF ACCREDITATION
CIVIL,CSE,ECE,EEE,MECH, MBA & MCA

Accredited by NAAC A+ Grade

nirf NATIONAL INSTITUTIONAL RANKING FRAMEWORK
MITS ranked in the band 251-300-NIRF 2022

A Report on Alumni Guest Lecture titled "Cybersecurity Trends and Career Paths - A Journey into Digital Defense" Organized by Department of Computer Science & Engineering on 20.04.2024



Submitted By: Mr. BSH Shayeez Ahamed, Assistant Professor, Dept. of CSE
Resource Person: Dr. G. N. Vivekananda (Alumnus of CSE 2006-2010 Batch), Working as Associate Professor, School of Computer Science Engineering and Information Systems, Vellore Institute of Technology, Vellore.
Participants: II Year B. Tech – Computer Science & Engineering Students – MITS
Report Received on 24.04.2024.
Mode of Conduct: Online

A Guest Lecture on "**Cybersecurity Trends and Career Paths - A Journey into Digital Defense**" was organized by the Department of ComputerScience & Engineering for II B.Tech students.

The inauguration of the Guest Lecture was started at 11:10 A.M in WB – 308, the dignitaries were Dr. R. Kalpana, HOD CSE, Dr. G.N. Vivekananda (Alumnus of CSE 2006 – 2010 Batch), Working as **Associate Professor, School of Computer Science Engineering and Information Systems, Vellore Institute of Technology, Vellore.**, Dr. R. Kiran Kumar, Alumni Relation Officer, Mr. A. Kumar, Event Coordinator, Mr. BSH. Shayeez Ahamed, Department Alumni Coordinator.The lecture was started with opening remarks by, Dr. R. Kalpana who thanked Managementfor this great initiation of creating an opportunity to invite the Alumni members of the institute and enabling them to interact with the students and enlightening them with the current developments in the corporate world. Dr. R. Kiran Kumar has shown pleasure and promised to conduct many more lectures in future for the benefit of the students.

Mr. BSH. Shayeez Ahamed has introduced the speaker and invited him to share his valuable experiences to the students. The number of students participated in the lecture were around 78.
After inaugural session, the main session was started at 11:20 A.M, Dr. G.N. Vivekananda explained about Cybersecurity Trends and Career Paths in Computer Science.

In a world that is becoming increasingly interconnected, the demand for skilled cybersecurity professionals is at an unprecedented level. By 2025, there will be 4.5 million unfilled cybersecurity positions, according to a recent report. The ever-increasing reliance on technology, the rise in cyber threats, and the requirement for comprehensive data protection across industries all contribute to this surge in demand.

Securing sensitive information and digital infrastructure is becoming increasingly important to businesses of all sizes, from large corporations to small businesses. As a result, people looking for a challenging and rewarding career will find plenty of opportunities in the cybersecurity industry. The following Key Points were discussed by Resource Person.

Acquire the right education and certification:

Building a successful career in cybersecurity begins with obtaining the necessary education and certifications. According to industry experts, around 70 percent of cybersecurity job postings require at least a bachelor's degree in a relevant field. A strong educational background provides you with a solid foundation in cybersecurity principles, technologies, and best practices.

Consider pursuing a degree in computer science, information technology, or cybersecurity. Additionally, industry-recognized certifications such as Certified Information Systems Security Professional (CISSP) or Certified Ethical Hacker (CEH) can enhance your credibility and marketability.

Specialize in a niche area:

As the cybersecurity field expands, specializing in a specific area can set you apart from the competition. According to a recent study by Cybersecurity Ventures, there will be 4.5 million unfilled cybersecurity jobs by 2025.

This shortage of skilled professionals presents an excellent opportunity to carve out a niche for yourself. Specializations can include network security, cloud security, digital forensics, or secure software development.

By becoming an expert in a specific area, you can position yourself as an invaluable asset to organizations seeking specialized knowledge.

Gain hands-on experience:

While education and certifications are essential, practical experience is equally vital in the cybersecurity field. According to a report by Burning Glass Technologies, 84 percent of cybersecurity job postings require at least three years of experience. Look for opportunities to gain hands-on experience through internships, apprenticeships, or entry-level positions.

Seek out organizations that offer exposure to real-world cybersecurity challenges and allow you to work alongside experienced professionals. Practical experience will help you develop the skills and confidence necessary to handle complex cybersecurity issues.

Stay current with continuous learning:

Cybersecurity is an ever-evolving field, with new threats and technologies emerging constantly. It is crucial to commit to continuous learning and professional development to stay ahead of the curve. Stay updated with the latest industry trends, advancements, and best practices.

Attend conferences, webinars, and workshops to expand your knowledge and network with industry experts. According to a study by (ISC)², 72 percent of cybersecurity professionals believe that continuous education is essential to staying current in the field. Embrace a mindset of lifelong learning to remain competitive and adaptable.

Build a strong professional network

Networking is vital in any career, and cybersecurity is no exception. Building a robust professional network can open doors to job opportunities, mentorship, and valuable industry insights. Attend industry events, join online forums and social media groups, and engage with professionals in the field.

What Is a Cyber Attack?

A **cyber-attack** is an attempt by cybercriminals, hackers or other digital adversaries to access a computer network or system, usually for the purpose of altering, stealing, destroying or exposing information.

Cyberattacks can target a wide range of victims from individual users to enterprises or even governments. When targeting businesses or other organizations, the hacker’s goal is usually to access sensitive and valuable company resources, such as intellectual property (IP), customer data or payment details.

The 10 Most Common Types of Cyber Attacks:

Malware:

Malware — or malicious software — is any program or code that is created with the intent to do harm to a computer, network or server. Malware is the most common type of cyberattack, mostly because this term encompasses many subsets such as ransomware, trojans, spyware, viruses, worms, keyloggers, bots, crypto jacking, and any other type of malware attack that leverages software in a malicious way.

Denial-of-Service (DoS) Attacks:

A Denial-of-Service (DoS) attack is a malicious, targeted attack that floods a network with false requests in order to disrupt business operations.

In a DoS attack, users are unable to perform routine and necessary tasks, such as accessing email, websites, online accounts or other resources that are operated by a compromised computer or network. While most DoS attacks do not result in lost data and are typically resolved without paying a ransom, they cost the organization time, money and other resources in order to restore critical business operations.

The difference between DoS and Distributed Denial of Service (DDoS) attacks has to do with the origin of the attack. DoS attacks originate from just one system while DDoS attacks are launched from multiple systems. DDoS attacks are faster and harder to block than DOS attacks because multiple systems must be identified and neutralized to halt the attack.

Phishing:

Phishing is a type of cyberattack that uses email, SMS, phone, social media, and social engineering techniques to entice a victim to share sensitive information — such as passwords or account numbers — or to download a malicious file that will install viruses on their computer or phone.

Spoofing:

Spoofing is a technique through which a cybercriminal disguises themselves as a known or trusted source. In so doing, the adversary is able to engage with the target and access their systems or devices with the ultimate goal of stealing information, extorting money or installing malware or other harmful software on the device.

Identity-Based Attacks:

CrowdStrike's findings show that **80% of all breaches use compromised identities** and can take up to 250 days to identify.

Identity-driven attacks are extremely hard to detect. When a valid user's credentials have been compromised and an adversary is masquerading as that user, it is often very difficult to differentiate between the user's typical behavior and that of the hacker using traditional security measures and tools.

Code Injection Attacks:

Code injection attacks consist of an attacker injecting malicious code into a vulnerable computer or network to change its course of action. There are multiple types of code injection attacks like SQL Injection, Malvertising **&** Data Poisoning**.**

Supply Chain Attacks:

A supply chain attack is a type of cyberattack that targets a trusted third-party vendor who offers services or software vital to the supply chain. **Software supply chain attacks** inject malicious code into an application in order to infect all users of an app, while **hardware supply chain attacks** compromise physical components for the same purpose. Software supply chains are particularly vulnerable because modern software is not written from scratch: rather, it involves many off-the-shelf components, such as third-party APIs, open-source code and proprietary code from software vendors.

Insider Threats:

IT teams that solely focus on finding adversaries external to the organization only get half the picture. Insider threats are internal actors such as current or former employees that pose danger to an organization because they have direct access to the company network, sensitive data, and intellectual property (IP), as well as knowledge of business processes, company policies or other information that would help carry out such an attack.

Internal actors that pose a threat to an organization tend to be malicious in nature. Some motivators include financial gains in exchange for selling confidential information on the dark web, and/or emotional coercion using social engineering tactics, such as pretexting, business email compromise (BEC) attacks or disinformation campaigns. On the other hand, some insider threat actors are not malicious in nature but instead are negligent in nature. To combat this, organizations should implement a comprehensive cybersecurity training program that teaches stakeholders to be aware of any potential attacks, including those potentially performed by an insider.

DNS Tunneling:

DNS Tunneling is a type of cyberattack that leverages domain name system (DNS) queries and responses to bypass traditional security measures and transmit data and code within the network.

Once infected, the hacker can freely engage in command-and-control activities. This tunnel gives the hacker a route to unleash malware and/or to extract data, IP or other sensitive information by encoding it bit by bit in a series of DNS responses.

DNS tunneling attacks have increased in recent years, in part because they are relatively simple to deploy. Tunneling toolkits and guides are even readily accessible online through mainstream sites like YouTube.

IoT-Based Attacks:

An IoT attack is any cyberattack that targets an Internet of Things (IoT) device or network. Once compromised, the hacker can assume control of the device, steal data, or join a group of infected devices to create a botnet to launch DoS or DDoS attacks.

Given that the number of connected devices is expected to grow rapidly over the next several years, cybersecurity experts expect IoT infections to grow as well. Further, the deployment of 5G networks, which will further fuel the use of connected devices, may also lead to an uptick in attacks.

The session is completed at 12:15 P.M, and he clarified the queries of enthusiastic young minds with a great zeal during the interaction time.

The resource person was honored by a token of respectable appreciation by Dr. R. Kalpana CSE – HOD, Dr. R. Kiran Kumar, Alumni Relation Officer and all faculty members of the department.

Vote of Thanks:

Mr. BSH. Shayeez Ahamed proposed a vote of thanks to the Resource person, HOD and AlumniRelations Officer for attending the function. He extended his thanksto the Principal, and the Management for their support to conduct the training.

Outcomes of this Guest Lecture:

1. Inspiration & Motivation.
2. Valuable Learning Insights & Ideas.
3. Students will Analyze & Evaluate the Cyber Security needs of an organization.
4. Students will Measure the Performance & Troubleshoot Cyber Security Systems.
5. Students will get new prospectives & opinions that are often missed in regular class.
6. Students learned the different types of Cyber Security Attacks.