A Two Day Workshop on Emerging Technologies in Cyber Security and Forensics

No Of Students Attended: 86

Date: 23-12-2021 & 24-12-2021

Resource Persons: Mrs. N. Chaitanya Rani, Entrepreneur, Founder & CEO

&

Miss. R. Devi Supraja, HR, Spypro Security Solutions Pvt. Ltd., Vijayawada.

Description of the Programme:

Intelligence or Investigations reports are important for the success of an investigation. But how do you make sure that they are written in a way that makes sense for anyone who needs to read it, regardless of technical background?

Cybersecurity has become a top priority for many boards. As a result, cybersecurity reports have become increasingly important and relevant to them. They give the board a good understanding of the security posture of the organisation. Effective cybersecurity reporting requires that information be presented clearly and succinctly so that priorities can be identified, issues can be addressed, and decisions can be made in accordance with the organisation's strategic goals and risk appetite.

DAY-1

Mrs. **N. Chaitanya Rani** enlightened the students which focuses on technology, management, compliance and legal issues which work with forensic tools and techniques used to investigate and analyse network-related incidents and preserve digital evidence.

IT jobs require computer and technology expertise. If you have IT qualifications, you'll find it easier to learn the profession and get jobs. If you already work in the IT sector, you will have experience and knowledge of network basics, operating systems, scripting language which are key for this job.

An ethical hacker's job also requires understanding and knowing how to use several tools. The following are vital:

- NMap, to carry out security audits.
- Wireshark, to monitor networks to detect data leakage.
- BadMod, to measure web application security.

Mrs. Chaitanya explained the following steps for the process of hacking include:

Reconnaissance which is also called Footprinting and information gathering about a target before launching an attack such as old passwords, names of important employees. Scanning are probably seeking information that can help them to penetrate attack such as computer names, IP addresses and user accounts. Hackers identifies a quick way to gain access to the network, information and use tools like dialers, port scanners, network mappers, sweepers and vulnerability scanners to scan data.

DAY-2

Gaining Access has the information he needs to design the network map and then he has to decide how to carry out the attack? There are many options, for example:

- Phishing Attack
- Man in the middle Attack
- Brute Force Attack
- Spoofing Attack
- Dos Attack
- Buffer Overflow Attack

Maintaining Access is used when he has gained access for future exploitation and launches additional attacks on the network until he finishes the task he plans to accomplish in that target. Clearing tracks always clear all evidence so that in the later point of time no one will find any traces leading to him/her. They will do this by:

Clearing the cache & cookies, modifying registry values, modifying/corrupting /deleting the values of logs, clearing out sent emails, closing all the open ports, uninstalling all applications that he/she be used

These steps of hacking include the process which is predominantly used in computer and mobile forensic investigations and consists of three steps: acquisition, analysis and reporting.

Presentation By Mrs. N. Chaitanya Rani