Gujarat Technological University
Accredited with A+ Grade by NAAC

Report on "**Cyber Threat Intelligence and Digital Forensics**"

Graduate School of Engineering and Technology

Short Term Training Program
Under
Information Security Education and Awareness

Date: 12th to 16th September 2023
Venue: GTU A2 Hall
Timing: 11:00 AM to 5:00 PM

GTU-GSET had organized an online STTP "Cyber Threat Intelligence and Digital Forensics" from 12th to 16th September 2023. Where 64 students and faculties have participated. Under the coordination of Prof. Dipak Upadhyay and Prof. Margam Suthar, this event is divided into five-sessions.

On the first day we have an inauguration function, where Shri Tushar Y. Bhatt, IAS Managing Director, GIL remain present to encourage the students and Participants. Moreover, Prof. (Dr.) Rajul Gajjar, Vice Chancellor GTU, Dr. K.N.Kher, Registrar GTU and Prof.(Dr.) S. D. Panchal remain present for the Inauguration function. On this occasion the authorities discussed on the importance of cyber awareness and also share some examples of the cyber frauds. At the end we started our first day training.

GPS Map Camera
Ahmedabad, Gujarat, India
4H4V+MF4, Nigam Nagar, Chandkheda, Ahmedabad, Gujarat 382424, India
Lat 23.106272°
Long 72.593829°
12/09/23 11:13 AM GMT +05:30
Google

This STTP is divided into the five expert's sessions which are as bellow:

Date	Expert name	Topic covered
12/09/2023	Dr. Aakash Thakar, Rashtriya Raksha University	Digital Forensics.
13/09/2023	Mr. Jamin Somani	Installation of different OS, ethical hacking.
14/09/2023	Ms. Yamini Savaliya	different Malware and a tools to analysis it.
15/09/2023	Mr. Rohit tyagi, Scientist, ISRO	demo of ethical Hacking and also introduce some case studies.
16/09/2023	Mr. Ankit Gandhi	demonstrate the windows servers and Load balancing

Day: 1 This training covers a wide range of topics, including data recovery, computer and mobile device forensics, network analysis, and cybersecurity. It teaches participants how to gather, preserve, and analyse digital evidence in a forensically sound manner, ensuring that it can be used in legal proceedings. Moreover, it fosters an understanding of the latest technologies and techniques employed by cybercriminals, enabling investigators to stay one step ahead.

Day: 2 Training in the installation of various operating systems and ethical hacking is a powerful combination of skills that equips individuals with the ability to navigate the intricate world of cybersecurity effectively. Installing different operating systems provides a solid foundation for understanding diverse computing environments, making it essential for IT professionals and cybersecurity experts. These experts can then utilize this knowledge to identify, assess, and remediate vulnerabilities in digital systems, which is precisely where ethical hacking comes into play.

Day: 3 Training in different types of malware and the tools used to analyse them is an essential component of modern cybersecurity education. Malware, such as viruses, Trojans, ransomware, and spyware, poses a constant threat to computer systems and networks. Understanding the characteristics, behaviour, and propagation methods of various malware strains is crucial for cybersecurity professionals.

Equally important is the ability to dissect and analyse malware using specialized tools and techniques. Malware analysis training provides individuals with the skills to reverse-engineer malicious code, uncover its functionality, and identify indicators of compromise. This knowledge empowers cybersecurity experts to detect, mitigate, and respond to malware attacks effectively.

Day: 4 Training in the demonstration of ethical hacking is a critical educational component in the field of cybersecurity. Ethical hacking, often referred to as penetration testing or white-hat hacking, involves professionals using their skills to identify and rectify vulnerabilities in computer systems and networks before malicious hackers can exploit them. Demonstrations of ethical hacking techniques are essential for students and aspiring cybersecurity experts to understand the real-world scenarios and methodologies used by cybercriminals. In ethical hacking training demos, individuals learn how to think like malicious hackers, probing for weaknesses, and attempting to breach security defences in controlled environments. These hands-on demonstrations provide valuable insights into the tactics, techniques, and procedures employed by cyber adversaries.

Day: 5 Training in demonstrating Windows Server administration and load balancing is a crucial element of building a resilient and efficient IT infrastructure. Windows Server is a cornerstone in many organizations, providing the foundation for services, applications, and data storage. Training in Windows Server administration equips professionals with the skills needed to set up, configure, and manage these servers effectively.

Load balancing, on the other hand, plays a pivotal role in ensuring high availability and optimal performance of applications and services. Load balancing distributes network traffic across multiple servers, preventing overload on any single server and minimizing downtime. Training in load balancing covers the principles and practices of distributing workloads efficiently, enhancing the reliability of IT systems.

At last we have valedictory program where, students have shared their feedback for the STTP. Moreover, we have certificates distribution program where, students are awarded with the certificates from the GTU-GSET faculties.

Photographs of the Valedictory Session