Stanley College of Engineering and Technology for Women

Chapel Road, Abids, Hyderabad– 500001

(Autonomous)

(Affiliated to Osmania University & Approved by AICTE) (All eligible UG Courses are accredited by NBA & Accredited by NAAC with 'A' Grade)

Report
On
Ethical Hacking Workshop

Department of Information Technology

Ethical Hacking Workshop was organized by **Mr. Kartheek Chanda, a certified instructor and Ethical Hacker by E-Council and founder of ERSEGMENT Solutions PVT LTD.** in association with **"Stanley Women's College pf Engineering and Technology for Women"**, Hyderabad on **24th and 25th February, 2023** through offline mode on the topic **"Ethical Hacking"**. This was a two day workshop where various related subtopics were discussed practically every step was been explained in detail by the resource person Mr. Kartheek Chanda and all participants experienced crystal clear knowledgeable practical sessions.

The workshop was started with an inaugural session on 24th February, 2023 with Ms. Manisha and Ms. Mubeena welcoming everyone and followed by national anthem.

Fig. Department head presenting the boquet to the resource person

Ms. Manisha and Ms. Mubeena from Stanley College of Engineering and Technology introduced all the coordinators and invited the Department head Mr. Dr. B. Srinivasu to present a bouquet to the resource person Mr. Kartheek Chanda.

DAY 1:

"Hacking" is the word we are giving attention to in this fast-moving world. We glimpse and hear about atrocities and thefts in newspapers, Instagram, and all mass media outlets about how a bank is looted. How people are fooled. How money is being disseminated from the owner without approval. These horrors are a piece of "unethical hacking". To comprehend the ways of protecting our system and data we had a workshop on Ethical hacking with the Ethical Hacker, Mr. Kartheek Chanda.

Fig. Explanation of our data safety

The instructor said "To become a hacker one must ponder like a crook, but never turn into a burglar. "

Before moving into the topic of "hacking " we were given a brief knowledge about "cyber security".

Cyber security refers to safeguarding data, systems, networks, applications, or a server. Cyber security guards the data from being breached. A hacker ruptures the guard and enters a system. Hacking is the process of accessing the data of a system.

We were given familiarity with the TYPES OF HACKERS.

- **White hat Hackers**: White hat Hackers are also known as Ethical Hackers or Penetration testers. White hat hackers are the good guys of the hacker world.

- **Black hat Hackers**: Black hat Hackers are also known as Unethical hackers or Security crackers. These people hack the system illegally to steal money or to achieve their own illegal goals. They find banks or other companies with weak security and steal money or credit card information. They can also modify or destroy the data as well.
- **Grey hat Hackers**: Gray hat Hackers are a Hybrid between Black hat Hackers and White hat hackers. They can hack any system even if they don't have permission to test the security of the system but they will never steal money or damage the system.
- **Suicide Hacker**: Suicide hackers are typically less-skilled hackers who are just about capable enough to gain access to systems but are not able to evade detection.

Fig. Explanation of types of Hackers

The instructor displayed the devices employed for hacking.

- **Rubber Ducky**: It looks like a USB. If one inserts this into their system, the hacker or the owner can track the activities of the victim's keyboard. The hacker can dot down the passwords, and data of the victim. The hacker can modify the data and can have access to the keyboard.
- **Bash Bunny**: The main purpose of Bash Bunny is to carry out attacks on a station/mobile phone, provided you have physical access to them.
- Rubber Ducky is a keyboard emulator, plug it in and it executes pre-defined keystrokes. Bash Bunny is a Flash drive, an Ethernet adapter, a serial device, and a keyboard.
- **Rj-45**: RJ45 cables are used to connect every computer on the network but most often only four wires are used out of a standard eight-wire cable. One can access the data through the system network.

- **Shark Jack**: The Shark Jack is a portable network attack and automation tool for pen-testers and systems administrators designed to enable social engineering engagements and opportunistic wired network auditing
- **Wi-fi Pineapple**: Wi-Fi Pineapple is a wireless auditing platform from Hak5 that allows network security administrators to conduct penetration tests.
- HackerRF
- key Proptosis

Fig. Explanation of working of various devices employed for hacking

DAY 2:

Installation of Kali Linux:

Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics, and Reverse Engineering.

We learned how to install and use the Kali Linux source. We were given knowledge about the tools used for hacking as well.

Gateway:

payment gateway is a tunnel that connects your bank account to the platform where you need to transfer your money

2 D and 3 D gateways:

Two dimensions payment gateway is a type of payment gateway that processes payments without an additional security check like OTP. What is required is the customer's credit/debit card details (credit/debit card number, expiry date, CVV). It is easy, convenient, and time-saving.

The transactions using a three-dimension payment gateway have an additional layer of security, i.e., OTP. A One Time Password is required to validate the payment before deducting the amount from the consumer's bank account. The merchant's payment page collects debit/credit card details, after which an OTP is sent to the consumer's mobile, and once they enter the correct OTP, the payment is made.

Fig. Explanation of installation of KALI LINUX

Protection of your device:

1. Ensure the firewall is enabled before going online. You can also purchase a hardware firewall from companies like Cisco, Sophos or Fortinet, depending on your broadband router, which also has a built-in firewall that protects your network. If you have a larger business, you can purchase an additional business networking firewall.

2. Antivirus software plays a major role in protecting your system by detecting real-time threats to ensure your data is safe.

3. Using strong passwords is a crucial way to prevent network intrusions. The more secure your passwords are, the harder it is for hackers to invade your system.

4. Always install operating system updates. Most updates include security fixes that prevent hackers from accessing and exploiting your data. The same goes for apps.

Fig. Group picture at the end of session

The session has been successfully completed with everyone’s contribution to the workshop.