B.M.S COLLEGE OF ENGINEERING

Autonomous Institute, Affiliated to VTU

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (IOT & CYBERSECURITY INCLUDING BLOCKCHAIN TECHNOLOGY)

DIGITAL FOOTPRINTS: TRACING CYBER CRIME THROUGH FORENSICS

OBJECTIVES:

- Providing participants with hands-on experience in penetration testing and various cybersecurity techniques
- Educating participants about common vulnerabilities and misconfigurations that can compromise systems.
- Familiarize participants with tools like Netdiscover, Nmap, Nessus, OpenVAS, and sandboxes for vulnerability assessment and exploitation.
- Introducing standard penetration testing methodologies to identify, exploit, and secure vulnerabilities.
- Teaching techniques for collecting publicly available intelligence (OSINT) and leveraging advanced Google Dorking.

DATE – TIME:

- Date: 17th December 2024
- Time: 09:00 AM to 5:00 PM

VENUE:

- PJ Block lab, 6th floor, Department of CSE(ICB)

FACULTY COORDINATOR:

- Ms. Manjula M, Assistant Professor,

  Dept. of CSE((IoT and Cyber Security including Blockchain Technology)

PARTICIPANTS:

- Students of 5rd Semester, Dept. of CSE(ICB)

DESCRIPTION:

The workshop was conducted by Mr. Samarth Bhaskar Bhat, Director of Reverse Engineering at Infosec Pvt. Ltd. This comprehensive workshop was divided into three sessions, each focusing on a distinct aspect of cybersecurity:

Session 1: Exploring Cybersecurity Domains

The first session introduced participants to various cybersecurity domains through interactive challenges hosted on the Infosec training platform. Participants worked on tasks such as decrypting hashes, where they learned about hash functions and explored techniques like dictionary attacks and brute force to crack them. The video forensics segment provided practical experience in extracting metadata and hidden details from multimedia files, which is essential for digital investigations. The steganography section focused on detecting and retrieving concealed information in images, audio, or other file types, offering insights into how malicious actors hide data and how to uncover it effectively. In the Google Dorks session, attendees used advanced Google search operators to identify sensitive information inadvertently exposed online, highlighting the risks associated with poor web security configurations. Lastly, participants explored information gathering, leveraging Open-Source Intelligence (OSINT) to systematically collect and analyze publicly available data from various online sources for comprehensive intelligence gathering.

Session 2: Practical Hacking - Exploiting the Sunrise Machine

After a short break, participants engaged in a real-world penetration testing simulation using a vulnerable machine named Sunrise sourced from VulnHub.com. The session involved the following steps:

1. **Network Discovery:** Using Netdiscover, participants performed an ARP scan to identify the IP address of the Sunrise machine. This step highlighted the importance of understanding network topologies and identifying active hosts within a system.
2. **Port Scanning:** A comprehensive Nmap scan revealed two open ports: FTP (Port 21) and SSH (Port 22). This provided an in-depth analysis of the services running on the identified machine, paving the way for targeted exploitation.

3. **Exploiting FTP Service:** Participants discovered anonymous FTP login was enabled, allowing access to a backup file, which was downloaded using. This activity emphasized how poorly configured services could expose sensitive files to unauthorized users.
4. **Gaining Root Access:** The backup file revealed root credentials, enabling successful SSH login. Participants gained valuable insights into how attackers could escalate privileges and gain full control of compromised systems.

Session 3: Introduction to Advanced Tools

The final session introduced participants to powerful cybersecurity tools and their practical applications. Sandboxes were demonstrated as isolated environments ideal for safely analyzing suspicious files and studying malware behavior without risking broader systems. The Nessus **t**ool was presented as a leading vulnerability scanner used to detect potential security flaws in networks and systems. Participants also explored OpenVAS**,** an open-source solution for vulnerability management and assessment, which equips professionals with scalable tools for securing their infrastructure.

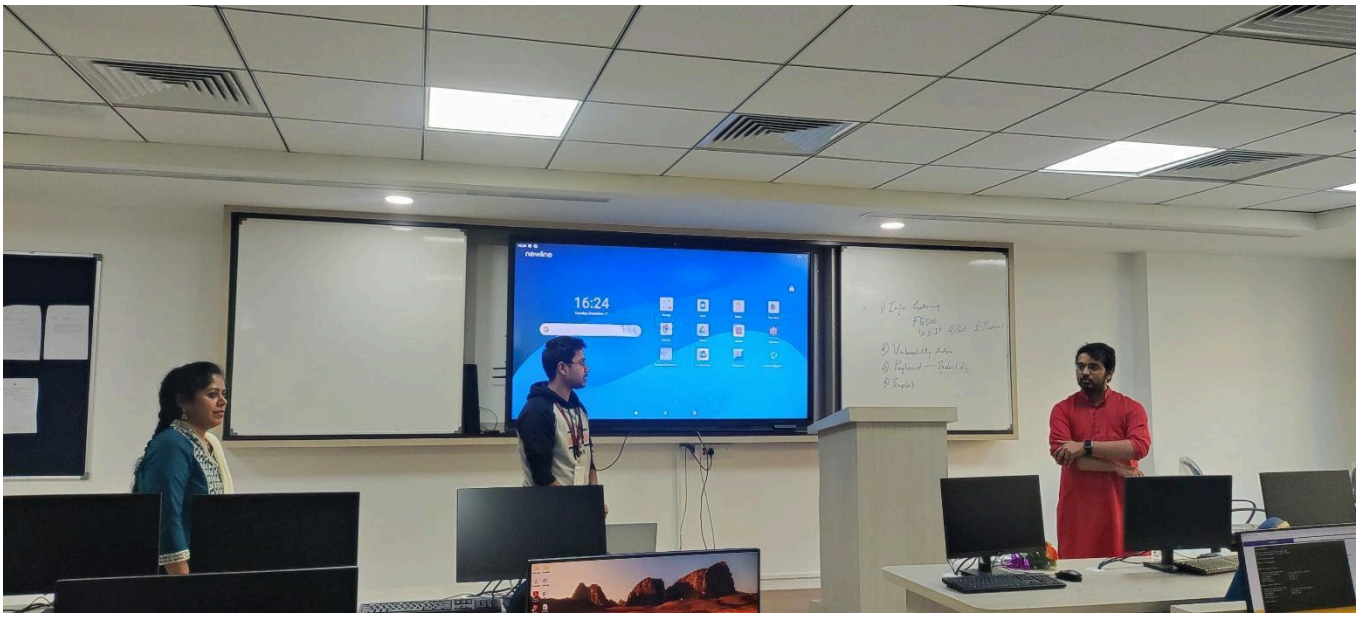
OUTCOMES:

- Participants gained insights into common security flaws and the consequences of misconfigurations, such as anonymous FTP logins.
- Hands-on challenges and the exploitation of a vulnerable machine improved participants' ability to perform network discovery, vulnerability scanning, and penetration testing.
- Participants became familiar with essential security tools like Netdiscover, Nmap, Nessus, and OpenVAS, and learned how to use them effectively in real-world scenarios.
- By solving practical challenges, participants developed problem-solving skills essential for identifying and mitigating security risks.
- The training reinforced ethical hacking principles, emphasizing the importance of securing.

PHOTOS:


GPS Map
Camera Lite
BMS COLLEGE OF ENGINEERING, 6, Mount Joy Extension, NR Colony, Basavanagudi, Bengaluru, Karnataka 560004, India
Latitude
12.9396722°
Longitude
77.564918°
Local 10:53:09 AM
GMT 05:23:09 AM
Altitude 919 meters
Tuesday, 17.12.2024


GPS Map
Camera Lite
69/1, Mount Joy Rd, Mount Joy Extension, Hanumanthnagar, Banashankari 1st Stage, Banashankari, Bengaluru, Karnataka 560050, India
Latitude
12.9415971°
Longitude
77.565345°
Local 04:27:21 PM
GMT 10:57:21 AM
Altitude 913 meters
Tuesday, 17.12.2024


16:24