CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY (AUTONOMOUS)

Gandipet, Hyderabad

Department of Computer Engineering and Technology

organizes Bootcamp on

Emerging Trends in Mobile Security

From 1st February 2025 – 22nd February 2025

(Conducted on 4 Saturdays)

About the Bootcamp

This Bootcamp aims to provide participants with both fundamental and advanced skills in mobile network security. It emphasizes hands-on experience in setting up, analysing, and securing wireless networks, ensuring a practical understanding of LTE, Wi-Fi, VPNs, and mobile security mechanisms. Through real-world simulations and security assessments, attendees will gain the expertise needed to identify vulnerabilities, implement defence strategies, and explore security models in Android and iOS platforms. This Bootcamp was conducted on 4 Saturdays (i.e., 1st February, 8th February, 15th February, 15th March).

Organizing Team

- **Convener:**
  Dr. Sangeeta Gupta, Professor & Head, CET Department
- **Faculty Coordinators:**

  Smt. P. Vimala Manohara Ruth, Assistant Professor, CET Department

  Smt. Kavita Agarwal, Assistant Professor, CET Department
- **Resource Person:**
  Ajinkya Lohakare, CTO & Founder, Ditto Security

Objectives of the Bootcamp

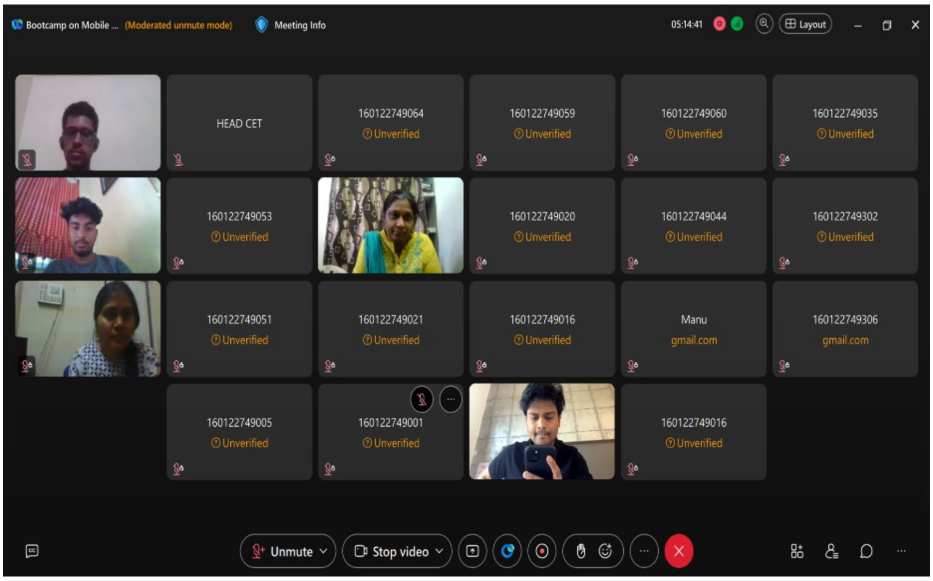
- Set up and simulate mobile networks
- Analyze Wi-Fi traffic and captive portals
- Configure and test mobile security and VPN tunnels
- Scan networks, identify vulnerabilities, and assess risks
- Perform wireless MITM attacks and study Bluetooth security
- Explore Industry 4.0 concepts by integrating IoT and AI for smart manufacturing

Outcomes of the Bootcamp

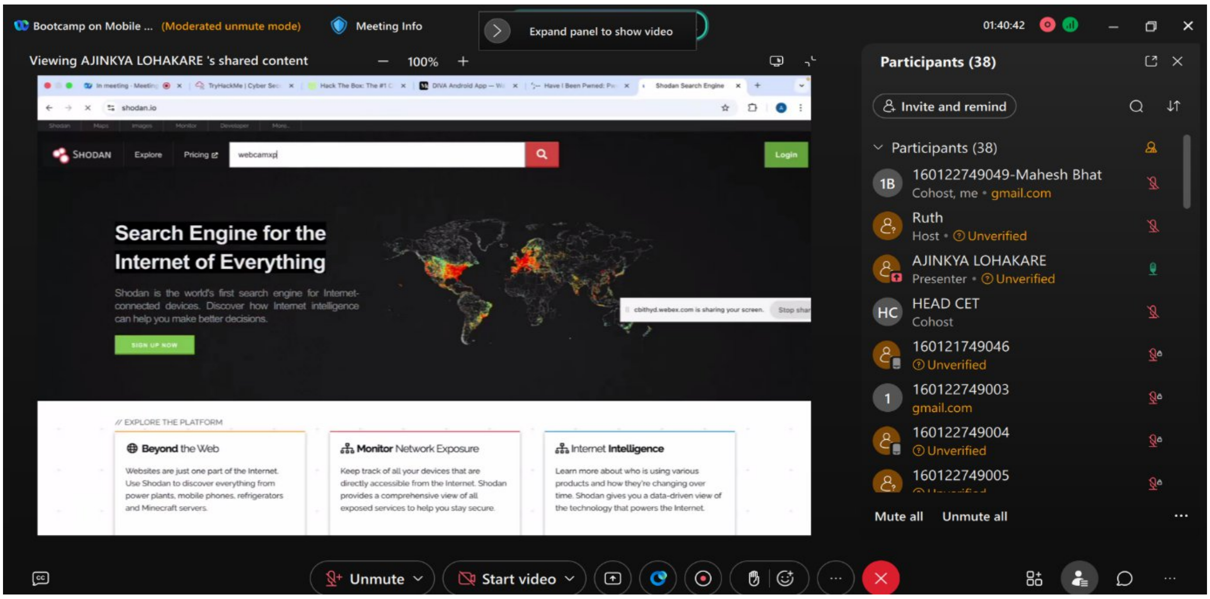
- Gained practical skills in mobile network simulation and Wi-Fi analysis
- Conducted scans to detect vulnerabilities in wireless systems

- Executed MITM attacks and monitored intrusion detection mechanisms
- Explored Bluetooth security and mobile app security (Android & iOS)
- Implemented VPN security and practiced risk mitigation on mobile platforms

Session 1 was about the basics of ethical hacking. It explained who ethical hackers are and why they are needed in today's world. The session covered different types of hackers – white hat (ethical), black hat (criminal), and grey hat (in between). It also discussed important terms like vulnerability (a weakness in a system), exploit (a way to use that weakness), and payload (the code that gets executed after an exploit). The ethical hacking process was explained step by step – starting from information gathering (reconnaissance), scanning the system for weaknesses, gaining access, maintaining that access, and finally covering tracks (used by bad hackers to hide their actions). Real-life examples like the Yahoo data breach, Facebook data leak, and the WannaCry ransomware attack were shared to show the importance of finding and fixing security issues early. Basic tips to stay safe like using strong passwords, avoiding unknown links, keeping software updated, and using VPNs were also mentioned.



Session 2 was about Linux and networking basics. It started with why Linux is mostly used in hacking – it is open-source, lightweight, and has built-in tools like Metasploit, Nmap, and Aircrack-ng. The session covered commonly used Linux commands like ls, cd, rm, chmod, and explained user roles like root user and normal user. File permission concepts were taught using read, write, and execute rights for owner, group, and others. Then, the session moved to networking. Key terms like IP address (unique address for each device), MAC address (hardware ID), and ports (used by services like HTTP, HTTPS, FTP) were explained. Concepts like DNS and port numbers were discussed. Nmap was introduced as a tool to scan networks, detect open ports, and check for weak points. The session ended with how hackers use networking to perform attacks like MITM, sniffing, and DoS. Simple safety tips like not using public Wi-Fi without a VPN, closing unused ports, and checking URLs were shared.



Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

// EXPLORE THE PLATFORM

Beyond the Web

Websites are just one part of the Internet. Use Shodan to discover everything from power plants, mobile phones, refrigerators and Minecraft servers.

Monitor Network Exposure

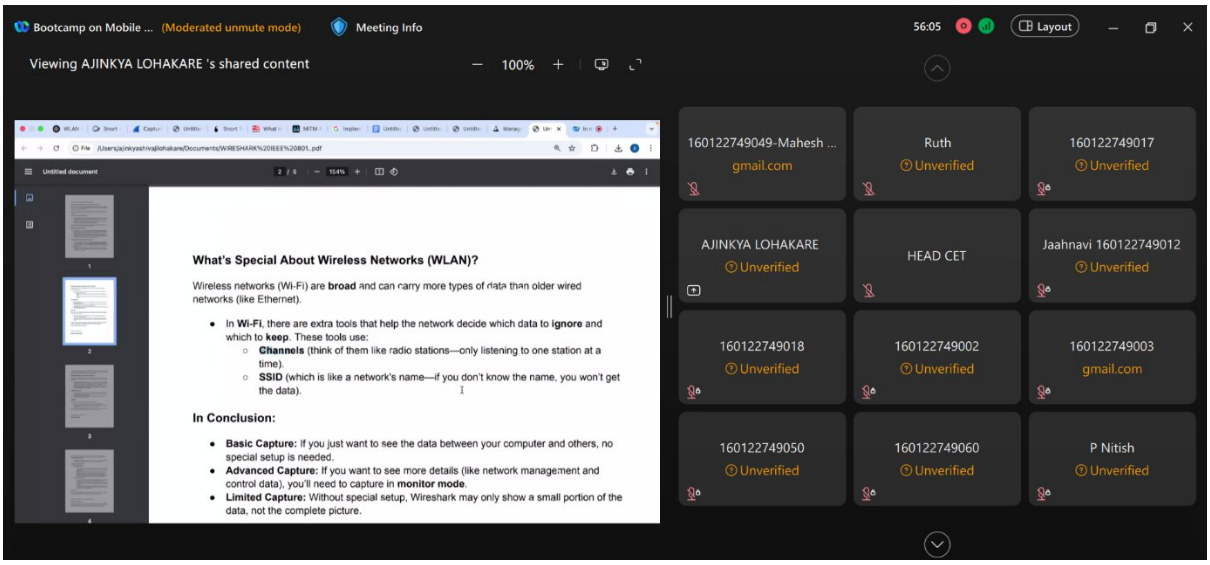
Keep track of all your devices that are directly accessible from the Internet. Shodan provides a comprehensive view of all exposed services to help you stay secure.

Internet Intelligence

Learn more about who is using various products and how they're changing over time. Shodan gives you a data-driven view of the technology that powers the Internet.

Session 3 was about website security. The session started with how websites store a lot of user data, and if there are weak points in the website code, hackers can steal this data. It explained common web application vulnerabilities from the OWASP Top 10 list. The main topics included **SQL Injection (SQLi)**, where hackers insert malicious SQL commands in input fields to access the website database; **Cross-Site Scripting (XSS)**, where attackers inject scripts into websites to steal user info like cookies or session data; **Broken Authentication**, where weak login systems allow hackers to guess or bypass passwords; and **Sensitive Data Exposure**, where important data like passwords are not stored securely. Tools used in testing web security like **Burp Suite**, **SQLmap**, **Nikto**, and **Dirb** were discussed. The session also covered how to perform web penetration testing by gathering information about the website, scanning for weak points, testing those weak points, and finally reporting them. Real cases like Facebook's bug bounty report, the Equifax breach, and Indian government website hacks were shared. Tips to protect websites included using parameterized queries, enabling HTTPS, updating software, and blocking malicious scripts using CSP.

Session 4 was about system hacking and how attackers try to break into computers. The session discussed how **brute force attacks** try every possible password until the right one is found, and how tools like **Hydra** and **John the Ripper** automate this. **Phishing** was explained with examples like fake login pages and emails tricking users to enter passwords. **Keyloggers** were discussed – these are programs that record everything typed on a keyboard, like passwords and credit card details. Other attacks included exploiting old, unpatched software using tools like **Metasploit**. Password cracking methods like **dictionary attacks** (using a list of common passwords), **rainbow table attacks** (pre-computed hash values), and **credential stuffing** (using stolen credentials from one site on another) were also taught. Safety tips included using strong, unique passwords, turning on 2FA, not clicking suspicious links, and keeping systems updated. Real examples included the LinkedIn data breach, RockYou password leaks, and Facebook storing passwords in plain text.



What's Special About Wireless Networks (WLAN)?

Wireless networks (Wi-Fi) are **broad** and can carry more types of data than older wired networks (like Ethernet).

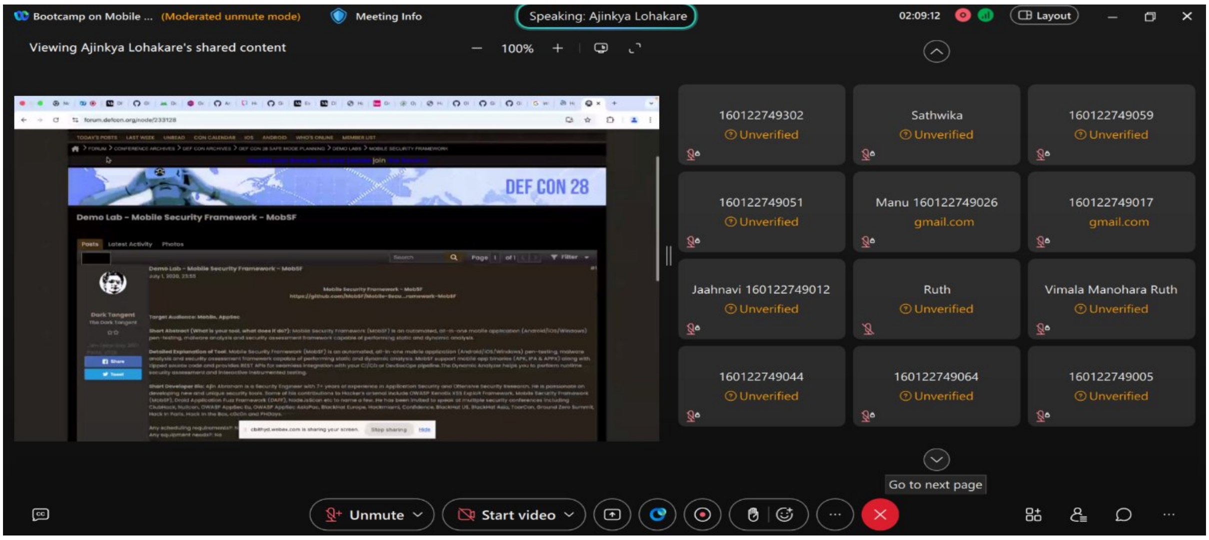
- In **Wi-Fi**, there are extra tools that help the network decide which data to **ignore** and which to **keep**. These tools use:
  - **Channels** (think of them like radio stations—only listening to one station at a time).
  - **SSID** (which is like a network's name—if you don't know the name, you won't get the data).

In Conclusion:

- **Basic Capture:** If you just want to see the data between your computer and others, no special setup is needed.
- **Advanced Capture:** If you want to see more details (like network management and control data), you'll need to capture in **monitor mode**.
- **Limited Capture:** Without special setup, Wireshark may only show a small portion of the data, not the complete picture.

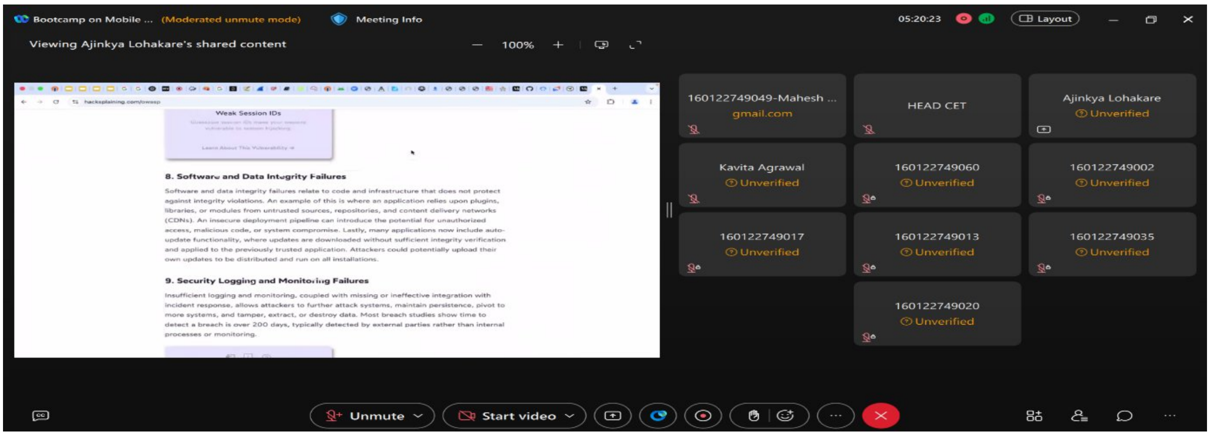
Session 5 was about WiFi hacking and wireless network security. The session explained how hackers can break into WiFi networks and steal user data. One method is **packet sniffing**, where tools like **Wireshark** capture data being transferred over a network. If websites don't use HTTPS, passwords and other private data can be easily seen. Another attack is the **Evil Twin Attack**, where hackers create fake WiFi hotspots with similar names to real ones (like "Free_Airport_WiFi"), tricking users into connecting. Once connected, the hacker can see everything the user does online. The session also covered **WPA cracking** using tools like **aircrack-ng**, where the attacker captures the handshake between a device and a router and then uses a dictionary to guess the password. **Deauthentication attacks**, done using **aireplay-ng**, force devices to disconnect from WiFi, making them reconnect through the fake network. To stay safe, users were advised to set strong WiFi passwords, enable WPA2/WPA3, disable WPS, hide their SSID, use MAC filtering, and update router firmware. Real-world WiFi attacks like the **KRACK attack**, **Mirai botnet**, and **hotel WiFi hacks** were discussed to show how common these threats are.

Session 6 focused on **malware** and **social engineering**, which are very common attack types today. Malware types like **viruses**, **trojans**, **ransomware**, **spyware**, **keyloggers**, and **worms** were explained. Viruses attach to files and spread when opened, trojans look like normal software but contain harmful code, and ransomware locks files and demands payment. Spyware and keyloggers track what the user does, and worms can spread without any action from the user. Real examples like the **ILOVEYOU virus**, **WannaCry**, and **Stuxnet** were discussed. The second part of the session covered **social engineering** – when attackers trick people into giving away passwords or installing malware. Techniques like **phishing**, **spear phishing**, **vishing**, **pretexting**, **baiting**, and **tailgating** were taught using real-life cases like the **Twitter Bitcoin scam**, **Google/Facebook $100M phishing fraud**, and **Target's data breach**. Tips to stay safe included never sharing OTPs or passwords, using MFA, not clicking on unknown links, and staying alert for fake offers or messages pretending to be from banks or companies.



Session 7 focused on Android penetration testing and the tools required for it. The session explained how Android applications can have security issues that need to be tested using proper tools and setups. Tools like **Genymotion**, an Android emulator for app testing, were used along with **VirtualBox** to create virtual devices for testing. Installation steps and account activation processes for Genymotion were covered. Other important tools discussed were **ADB (Android Debug Bridge)**, used for connecting and communicating with Android devices from a computer, and **DIVA (Damn Insecure and Vulnerable App)**, which is a purposely weak app created to practice Android security testing. Participants learned how to download and install DIVA and how to use platforms like **GitHub**, **Danish Zia's blog**, and **XDA Developers** to get APKs and walkthroughs. The session also covered **Frida**, a dynamic instrumentation toolkit used for reverse engineering Android apps. With Frida, participants were shown how to hook into functions, change app behavior, and study security flaws. Topics like insecure data storage, hardcoded secrets, and weak input validation were also covered. Students explored blogs and platforms like **Cybrary**, **Hackersploit**, **NullByte**, and **Payatu** to improve their understanding of Android security.

Session 8 introduced **iOS and reverse engineering basics**, especially tools like **IDA Free**, **Ghidra**, and **Frida**. The session explained how reverse engineering is useful to understand how apps work and to find vulnerabilities. Students were guided on how to create accounts on platforms like **Hex-Rays** and download **IDA Free**, which is used for static analysis of binaries. **Ghidra**, developed by the NSA, was also introduced as an open-source reverse engineering suite. Participants learned how to use it to analyze apps and understand logic and flow. Frida was again highlighted, this time for iOS testing. Installation steps and real-life blogs like "Quick Start with Frida" and "Instrumenting Windows APIs" were shared for better understanding. The session also touched on **wireless network setups** using tools like **CoovaChilli**, **Hostapd**, and **Raspbian/Ubuntu**, based on open-source GitHub projects. This included setting up WiFi hotspots with captive portals, which is useful in pentesting scenarios. Participants browsed through resources like **DEFCON**, **BlackHat**, and **Android Developer Docs** to stay updated on current tools and practices in mobile and wireless security testing. These sessions gave students hands-on experience with mobile security tools and reverse engineering methods that are used in real-world scenarios.



Bootcamp on Mobile ... (Moderated unmute mode)
Meeting Info
05:20:23
Layout
Viewing Ajinkya Lohakare's shared content
100%
hacksplaining.com/owasp

Weak Session IDs

Guessable session IDs make your website vulnerable to session hijacking.

Learn About This Vulnerability →

8. Software and Data Integrity Failures

Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. An example of this is where an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks (CDNs). An insecure deployment pipeline can introduce the potential for unauthorized access, malicious code, or system compromise. Lastly, many applications now include auto-update functionality, where updates are downloaded without sufficient integrity verification and applied to the previously trusted application. Attackers could potentially upload their own updates to be distributed and run on all installations.

9. Security Logging and Monitoring Failures

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.