Week 0 – Class 1 Recap & Resources

Recap:

In Week 0, Class 1 of the **Computer Security** course, we introduced the course layout, project, fundamentals of OWASP, Exploit DB, motivations, and key cybersecurity challenges. We were honored to host **Dr. Mian Muhammad Waseem** (https://scholar.google.com/citations?user=8pAhBrYAAAAJ&hl=en), Cybersecurity Expert and Researcher at Sultan Qaboos University, who underscored the importance of research for higher studies and highlighted exceptional student opportunities in international initiatives at CISPA and SQU.

Key Platforms & Resources for 2025

Enhance your journey with these **cutting-edge tools, platforms, and reports** that are shaping cybersecurity learning, research, and real-world readiness in 2025:

Training & Labs:

- **TryHackMe** – A browser-based platform offering guided cybersecurity labs and interactive challenges
- **Hack The Box** – Advanced penetration testing labs with realistic environments.
- **VulnHub**, **OverTheWire** – Self-paced environments to practice hacking and defensive skills.

CTF & Real-World Practice:

- **European Cybersecurity Challenge (ECSC)** – Annual EU-level CTF competition ("Eurovision of cybersecurity"), next scheduled October 6–10, 2025.
- **OffensiveCon + Pwn2Own Berlin 2025** – Live offensive security training and competitive exploitation events, featuring an AI-specific category.

OSINT & Investigation Tools:

- **1 TRACE** – An advanced OSINT and digital investigation platform (ISO 27001 certified in 2025), integrating SOCMINT, CYBINT, and FININT streams. Used widely by professionals across sectors.

Emerging AI & Automation in Cybersecurity:

- **CAI** – An open-source Cybersecurity AI framework achieving top-tier performance in CTF benchmarks and bug bounty exercises. It's exceptionally efficient—up to 3,600× faster than humans for some tasks.

- **PenTest++** – A hybrid system that combines generative AI and human oversight to automate penetration testing workflows—reconnaissance, scanning, exploitation, and documentation.
- **CyberSentinel** – A real-time threat detection framework targeting emergent AI security threats with techniques like ML-based anomaly detection and phishing analysis.

Top Reports & Trends to Watch:

- **OWASP Top 10:2025** – Industry-standard documentation of the most critical web application risks, scheduled for release late summer/fall 2025.
- **Check Point Cyber Security Report 2025** – Insightful analysis of emerging threats like ransomware, cloud vulnerabilities, and infostealers.
- **Horizon3.ai "State of Cybersecurity 2025"** – Data-driven insights from over 50,000 pentests, emphasizing proactive, continuous security over compliance.
- **Gartner Cyber Security Trends 2025** – Highlights of AI security, Zero Trust, XDR, cloud resilience, ransomware defense, and IoT security.
- **LevelBlue 2025 Futures Report** – A forward-looking view on threats, innovations, and strategic predictions for cybersecurity resilience.
- **Global Cybersecurity Outlook 2025** (World Economic Forum) – Macro-level trends and emerging security issues shaping global strategies