Live Zoom: Additional Materials:

Special session held among the 23 sessions.

- Additional Discussion and Lab 1 Discussion
- HTTP Header
- Broken Authentication & Session Managemen
- Security Missconfiguration
- Two-Factor Authentication (2FA) Bypass
- Captcha Bypass
- SSRF Target Exploitation (Native Web)
- SSRF Target Exploitation (CMS)
- AI-Assisted Brute Force Script Development (utilizing AI for automated script generation)
- Understanding the Role of AI in Penetration Testing (utilizing AI for strategic attack analysis)
- Wordlist Optimization Using NordPass Data (utilizing AI for predictive credential patterns)
- Active Directory and FreeIPA Attack Navigation (utilizing AI for automated privilege path mapping)
- Custom Payload Generation (utilizing AI for advanced exploit obfuscation)
- Source Code Analysis (utilizing AI for deep logic flaw detection)
- Accurate CVSS Scoring Determination (utilizing AI for objective risk assessment)
- Structured Pentest Report Generation (utilizing AI for automated professional documentation)
- Output Validation to Prevent AI Hallucinations (utilizing AI for technical accuracy verification)
- Rapid Bug Identification via CWE Mapping (utilizing AI for instant vulnerability classification)
- Brief Discussion of Lab 2
- Initial Access & foothold pada network terbatas
- Exploit chaining (multi-step exploitation)
- Network pivoting antar subnet
- Lateral movement antar host
- Privilege escalation sampai root access
- Web / service exploitation pada Linux server
- Internal host enumeration & discovery
- Access control bypass (whitelist filtering scenario)
- Red Team shell access objective
- Logically segmented network traversal (router-based restrictions)
- Wazuh-based monitored environment evasion (Blue Team detection layer)
- Cryptography challenge (di VPS Red Team environment)
- Linux application reverse engineering - Internal infrastructure
- Brief Discussion of Lab 3

- HTTP Header Manipulation
- Mobile Static Analysis and Dynamic Analysis to SQL Injection
- JWT Retrieval from API to Application Flaw
- From CVE-2026 to Host: Container Escape Chain (Ubuntu Server 24.04.4)
- Brief Discussion of Lab 4
- Initial Access & Foothold Establishment
- Database Extraction (The Source)
- Non-Interactive Credential Database Dumping
- Automated SAM & LSA Secret Extraction
- Cryptographic Material Harvesting
- Operational Base Expansion (The Pivot)
- Exploitation of Windows
- Workstation Control & Environment Preparation
- Identity Mapping
- Local & Domain Security Identifier (SID) Analytics
- Whoami Identity Verification
- Relative Identifier (RID) Mapping
- Ticket Forging & Internal Domain Persistence
- In-Memory Kerberos Ticket Injection
- Standardized Authentication Protocol Alignment
- Remote File System Enumeration via UNC Paths
- Brief Discussion of Lab 5
- Cross-Domain Escalation (Expert Level)
- Golden Ticket attack
- Cross-Node Security Identifier (SID) Harvesting (ExtraSID)
- Parent-Child trust exploitation - Enterprise Admin takeover
- Brief Discussion of Lab 6
- Enterprise Identity Security: Compromising FreeIPA Domain Controller through Credential Validation
- Full Domain Takeover: Exploiting Identity Management in FreeIPA