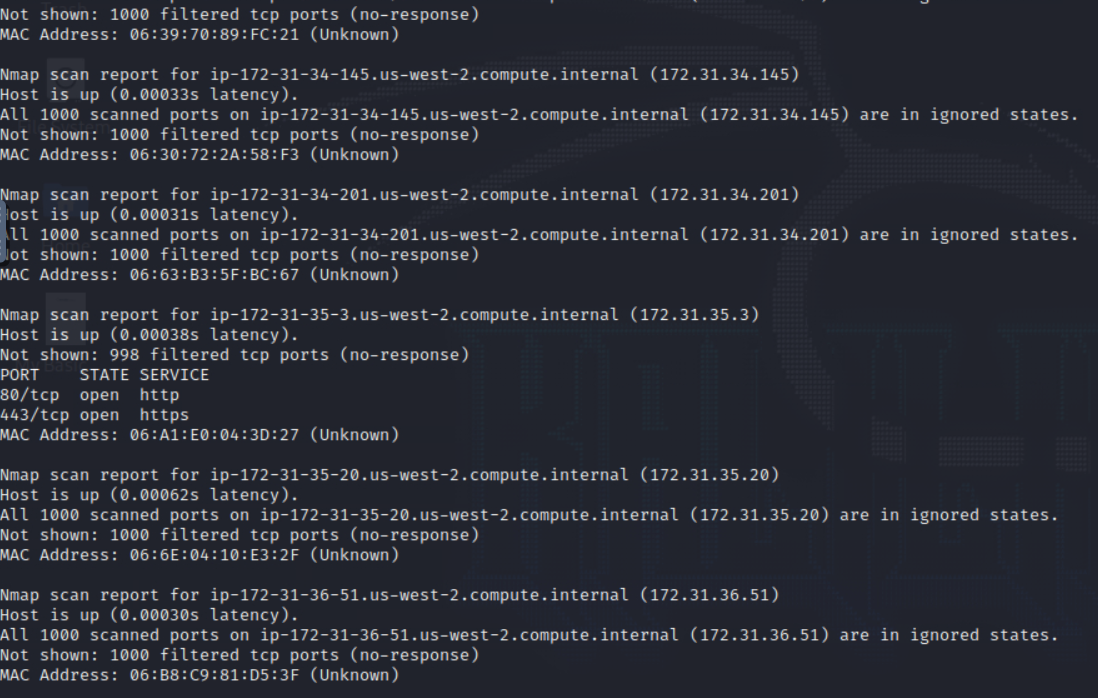
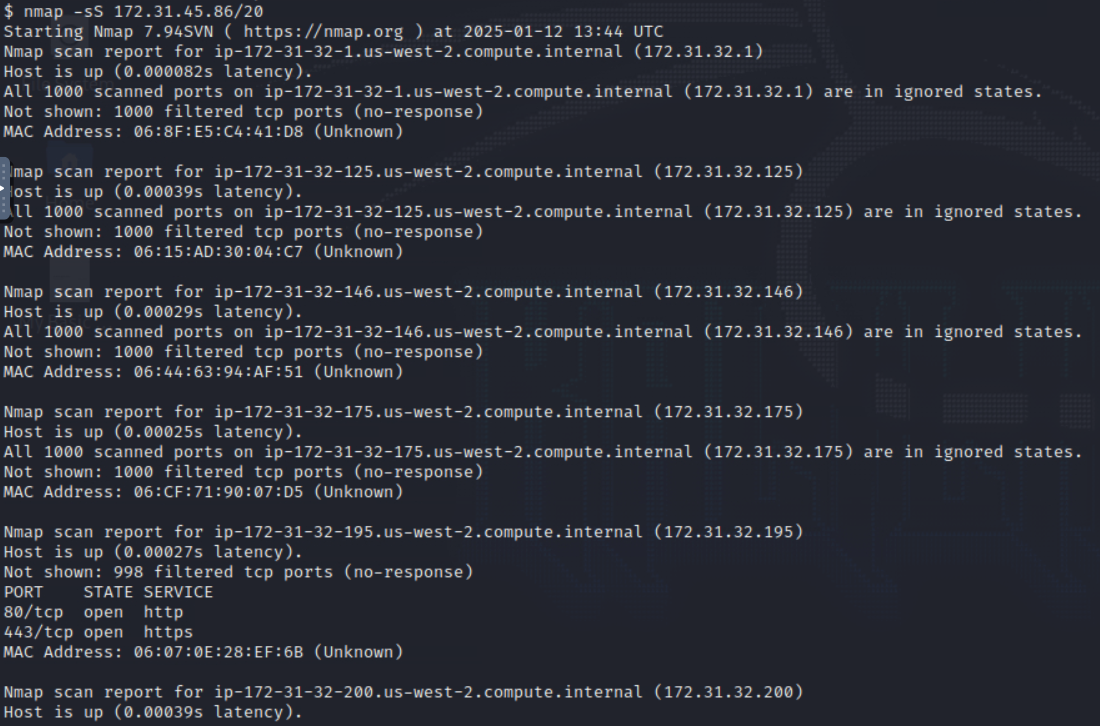
CAPSTONE 4 Penetration tester

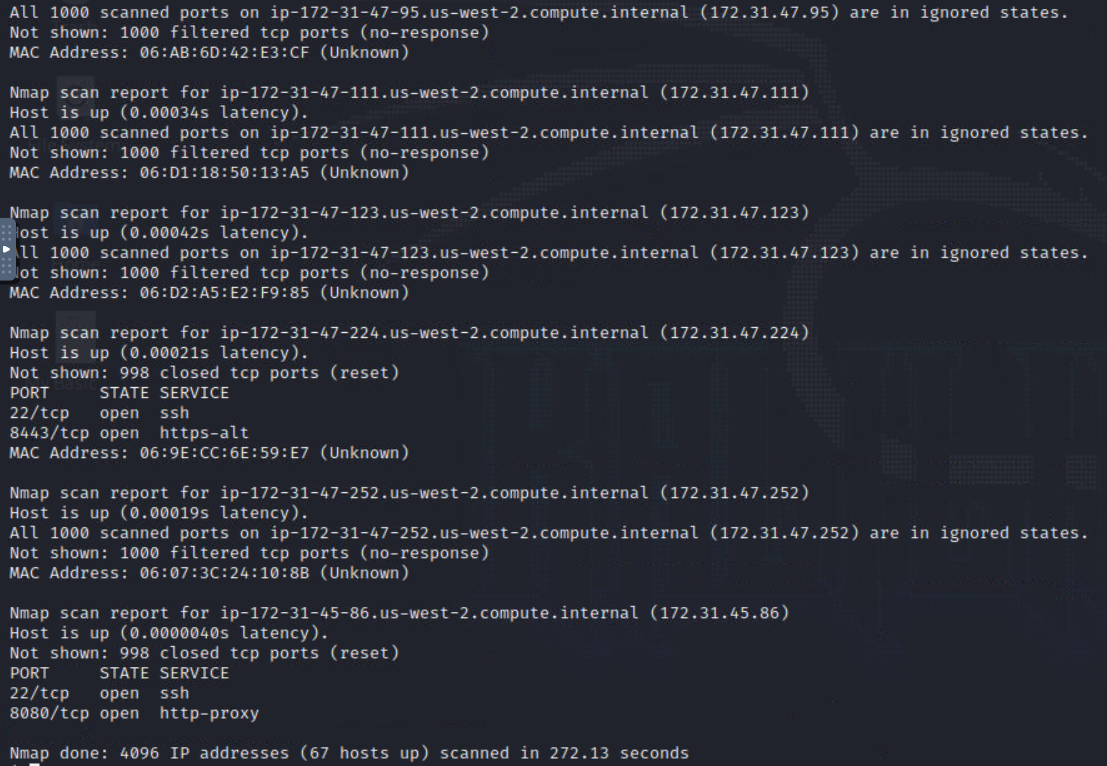
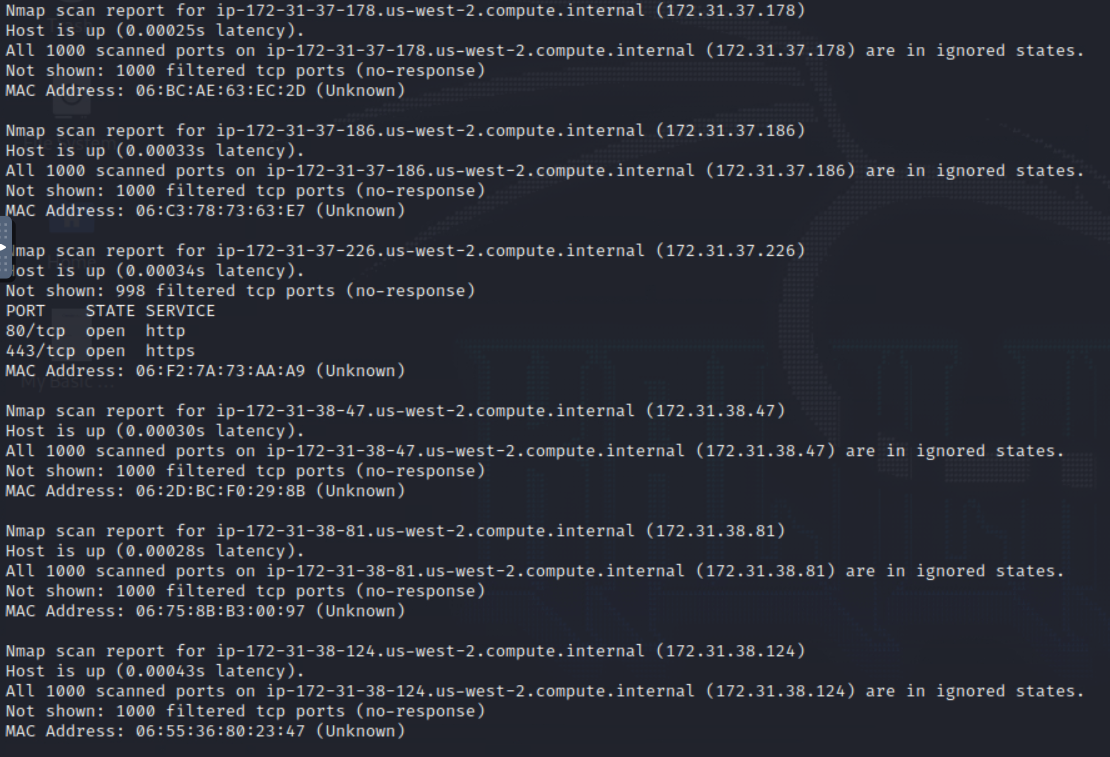
Done by: Sanjana Inchalmath

Task 1:

Nmap -sS ip(172.31.45.86/20)

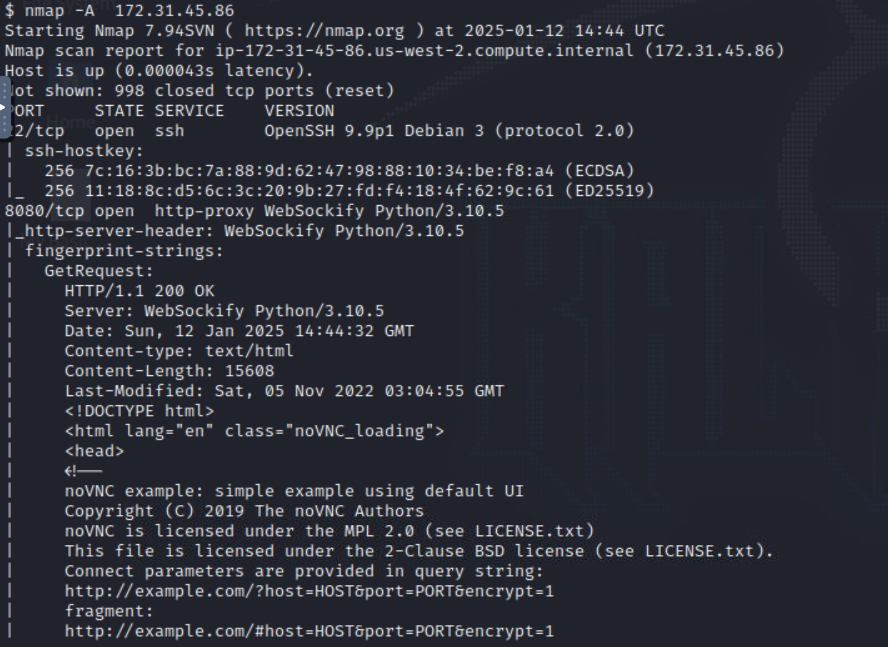
Note: IP Address of kali linux of my LMS

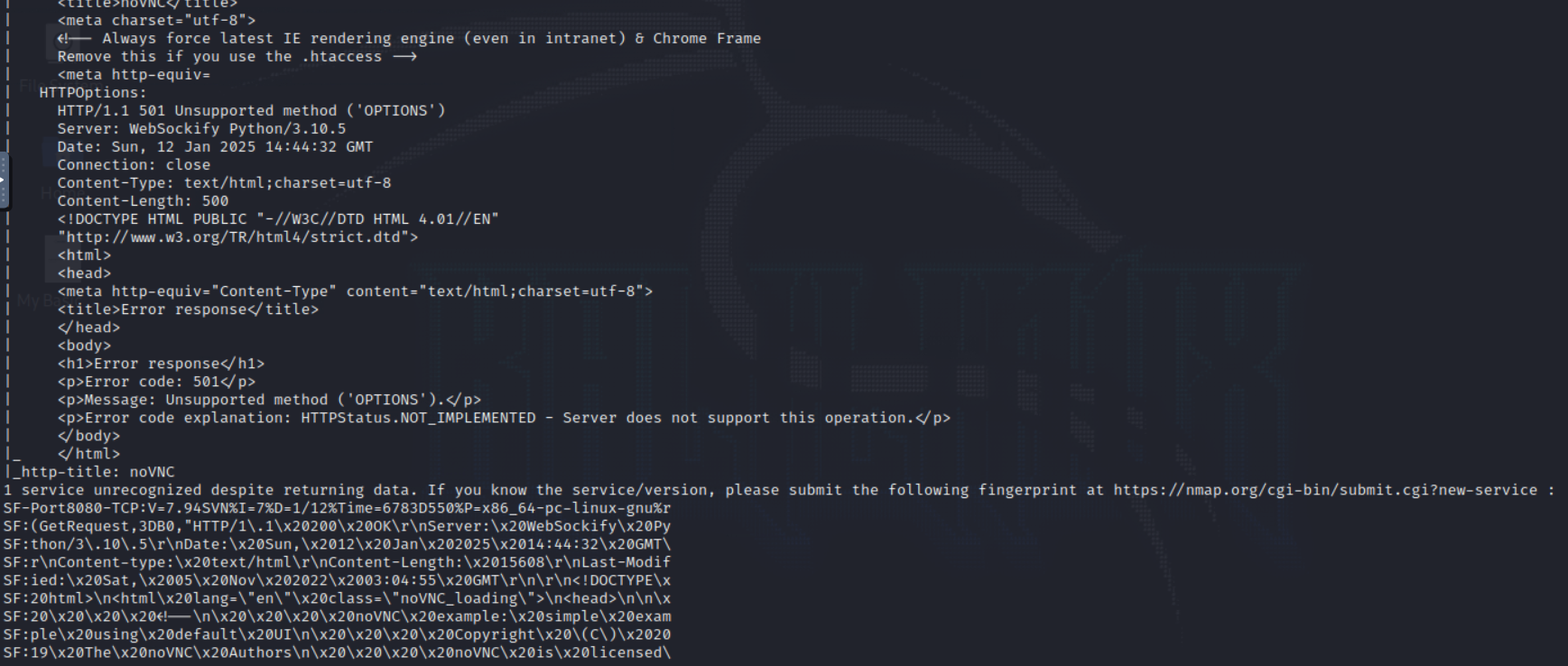


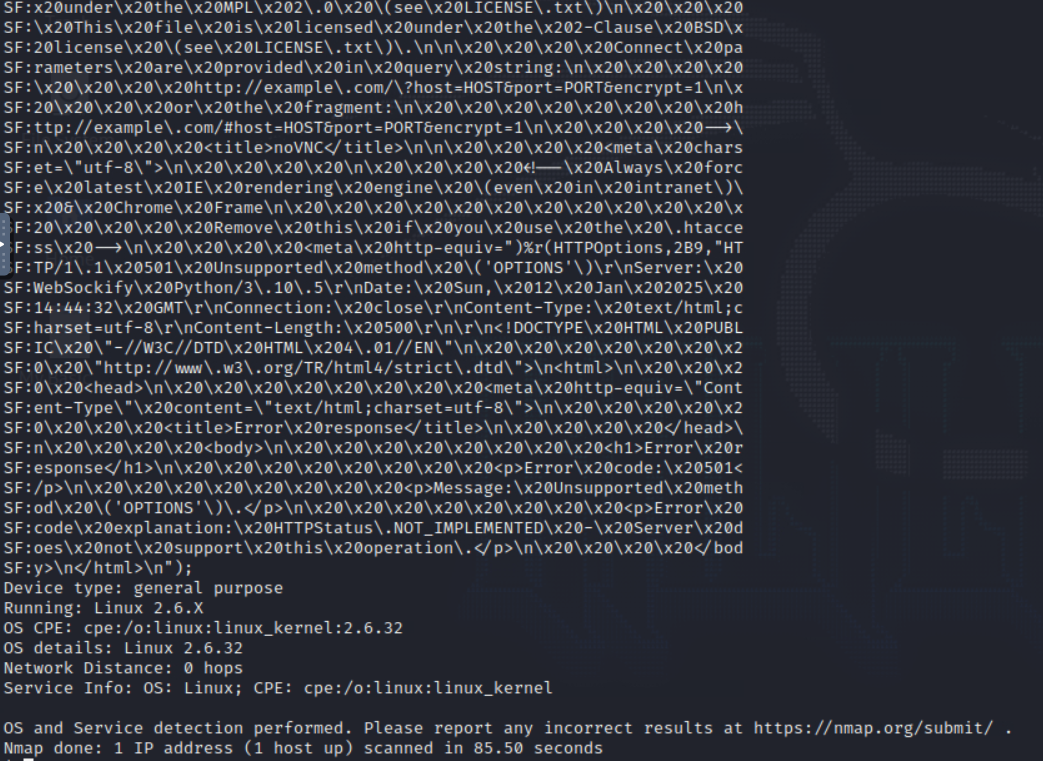


Task 2:

Nmap -A 172.31.45.86







Task 3:

|  |  |  |
| --- | --- | --- |
| Log # | Attack Type | Mitigation Control |
| Log #1 | DOM Based XSS | * Input validation and sanitization * Output encoding * Ensure any dynamic content displayed on the webpage is HTML-encoded to neutralize special characters. * Content security policy (CSP) * Implement a strong CSP to restrict the execution of inline scripts and external resources. * Regular Security Testing * Conduct periodic scans to detect XSS vulnerabilities. * Tools like OWASP ZAP or Burp Suite can identify potential flaws. |
| Log #2 | Directory Traversal Attack | * Input validation * Implement strict input validation to block malicious payloads. * Allow only valid characters for parameters, rejecting sequences like ../ or encoded equivalents (%2f..%2f). * Output encoding * Encode output to prevent direct file path manipulation from user input. * Serve files based on an **allowed list** (whitelisted filenames) instead of processing raw user input. * Web application firewall (WAF) * Sanitization file paths * Limit file access * Restrict web server privileges * Use **chroot jails** or containerization to isolate the application. * Application updates * Ensure all components of the web application are up-to-date. * Vulnerable libraries or applications, like DVWA, should not be deployed in production environments. |
| Log #3 | SQL Injection | * Input Validation * Strictly validate all user inputs to ensure they conform to expected formats (e.g., allow only integers for page). * Reject inputs containing SQL syntax (', --, ;, or encoded versions). * Parameterized Queries/Prepared Statements * Use parameterized queries or ORM frameworks to separate SQL logic from user input. * Escaping Input * If parameterized queries are unavailable, escape special characters in user input to neutralize SQL syntax. * Web application firewall (WAF) * Limit Database Permissions * Use the principle of least privilege for database accounts. * Restrict access to only the required tables and operations. |