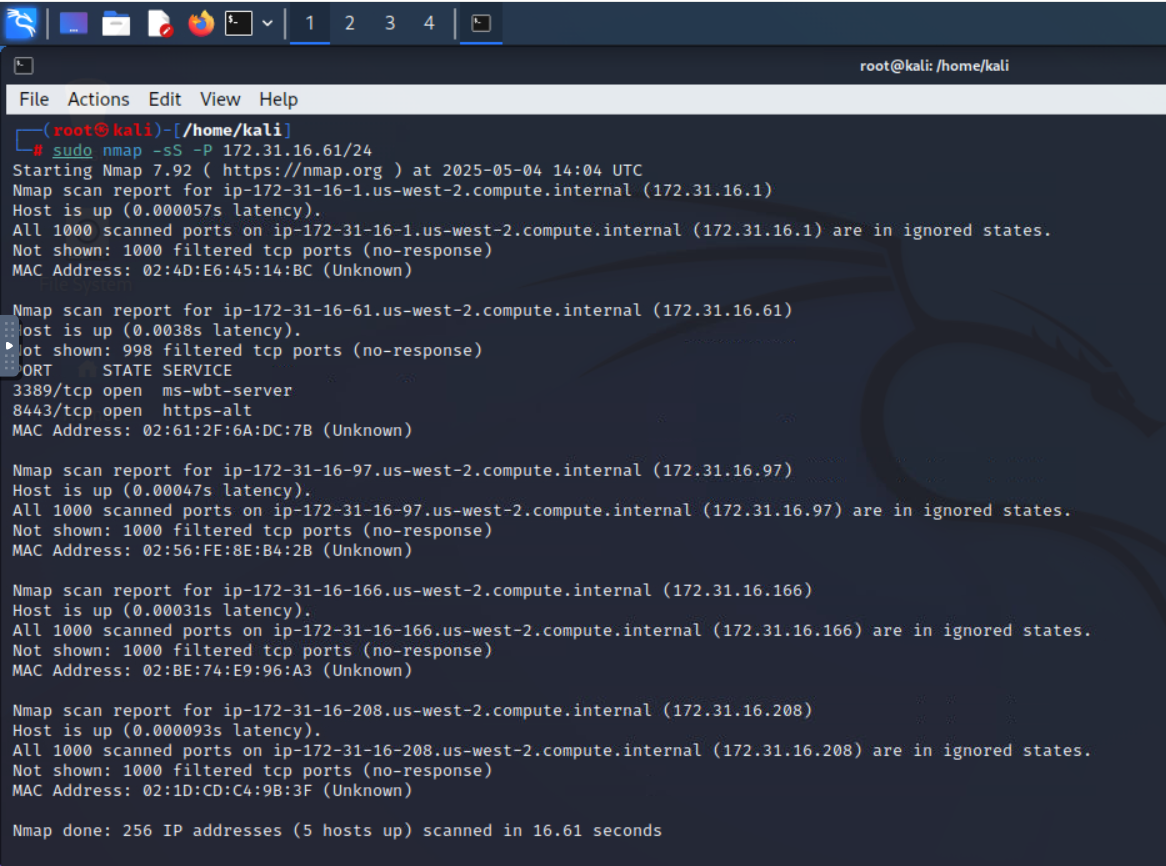
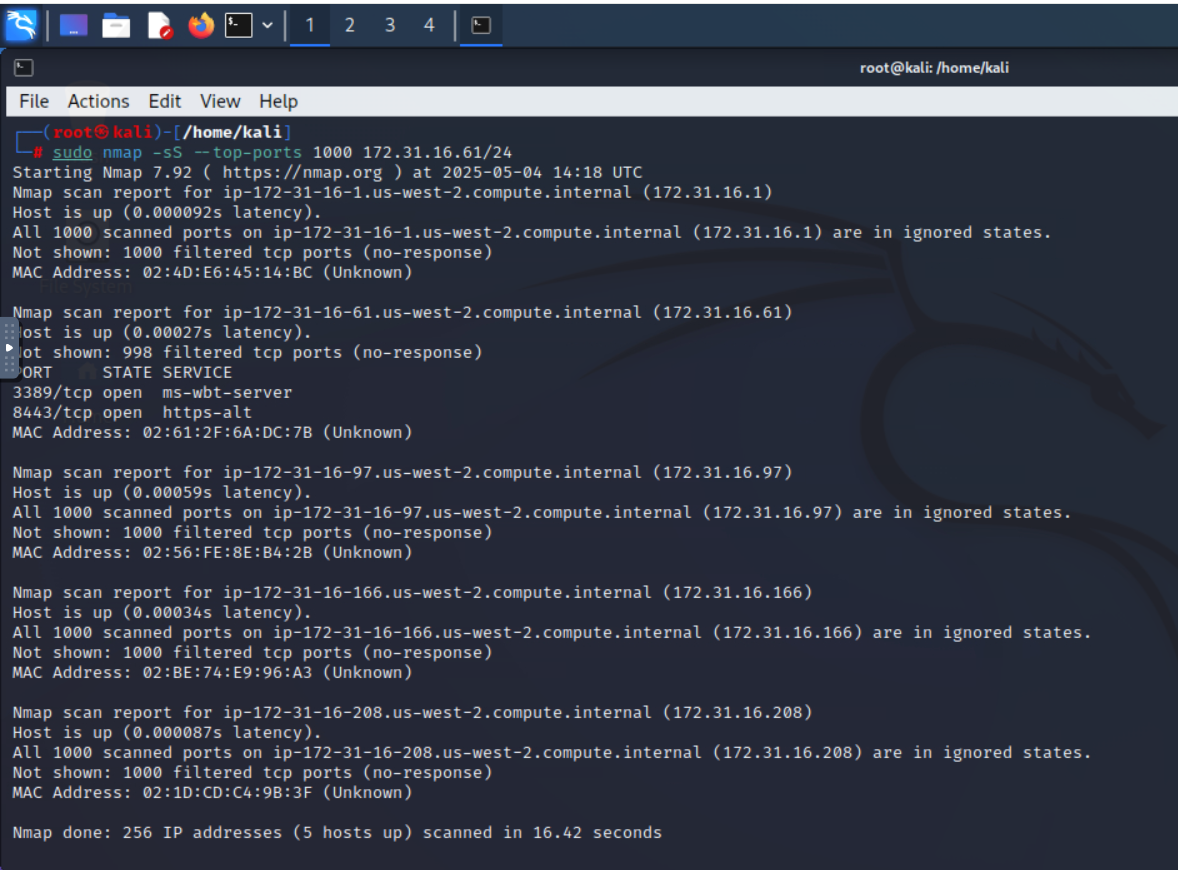
**CAPSTONE4**

**TASK 1:**

Perform a half-open scan against the target network to quickly identify all open ports in the network.

**Answer:**

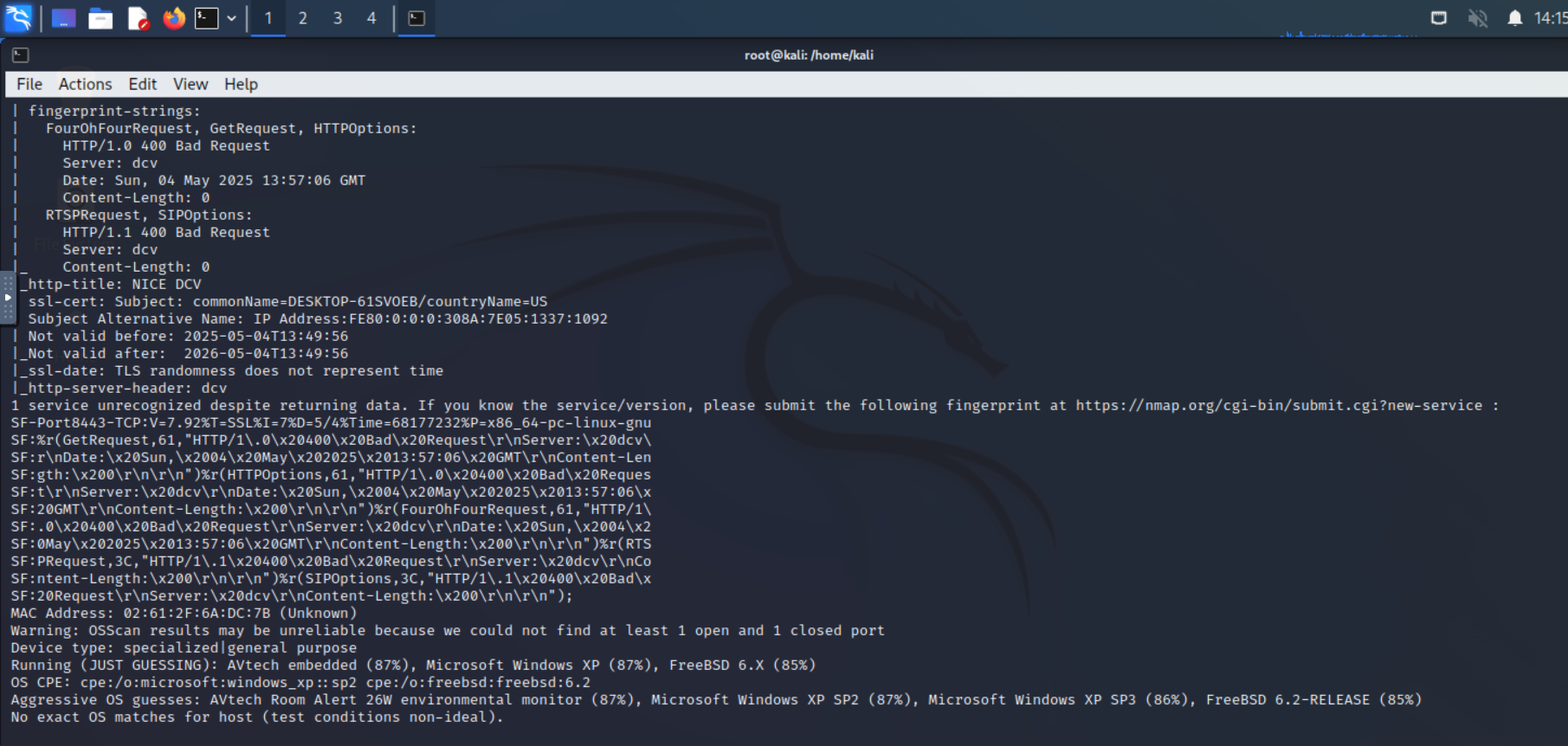
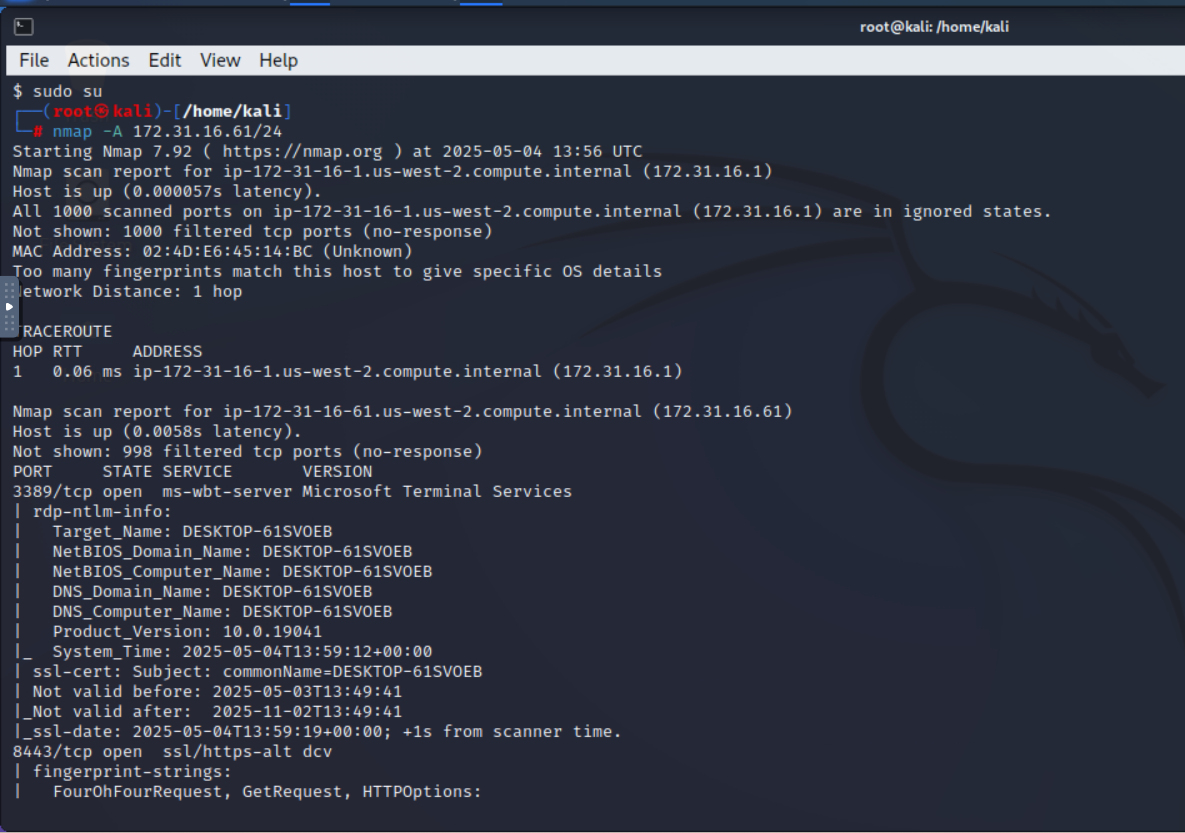
****

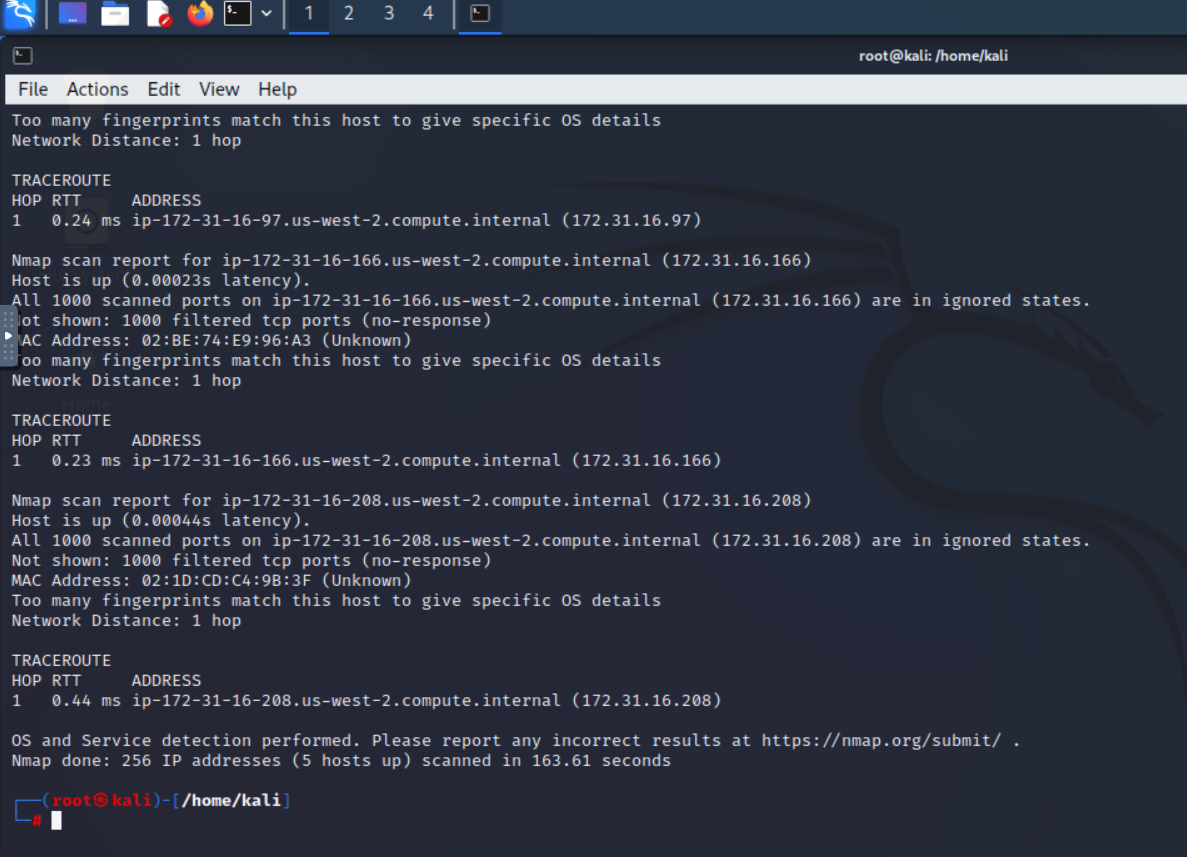
****

**TASK 2:**

Perform an aggressive mode that enables OS detection, version detection, script scanning, and traceroute in the network

**Answer:**

****

****

**TASK 3:**

While examining web server logs, you notice some HyperText Transfer Protocol (HTTP) GET requests that look suspicious. You need to carefully examine the logs, identify the attacks, and determine the appropriate mitigation control.

**Log #1:**

|  |
| --- |
| "18.66.78.71 - - [22/Dec/2021:16:18:20 +0300] "GET /media/system/js/caption.js HTTP/1.1" 200 751 "http://18.66.78.71/?wvstest=javascript:domxssExecutionSink(1,%22'%5C%22%3E%3Cxsstag%3E()locxss%22)" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21"" |

**Log #2**

|  |
| --- |
| "18.66.78.71 - - [22/Dec/2021:15:20:03 +0300] "GET /DVWA/vulnerabilities/fi/?page=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd HTTP/1.1" 200 2190 "http://18.66.78.71/DVWA/" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36"" |

**Log #3**

|  |
| --- |
| "18.66.78.71 - - [22/Dec/2021:15:19:59 +0300] "GET /DVWA/vulnerabilities/fi/?page=%27AND%201%3dcast(0x5f21403264696c656d6d61%20as%20varchar(8000))%20or%20%271%27%3d%27 HTTP/1.1" 200 1433 "http://18.66.78.71/DVWA/" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36"" |

**Answer:**

|  |  |  |
| --- | --- | --- |
| **Log#** | **Attack Type** | **Mitigation Control** |
| #1 | Domain XSS | * Input validations & Encoding. * CSP Header. * JavaScript Sanitization. |
| #2 | Local File Inclusion (LFI) | * Web Application Firewall (WAF). * Restrict File Access. * Input Validation & Whitelisting. |
| #3 | SQL Injection (SQLi) | * Use Prepared Statements (Parameterized Queries). * Least Privilege for Database Access. * Monitoring and Alerting. |