ASTANA IT UNIVERSITY

INTRODUCTION TO INFORMATION SECURITY AUDIT

Course title: Information Security Risk Management and Compliance

Instructor: Dauren Sagidollauly

Group: CS – 2216

Students: Sagatova I., Kazbekova K., Kapatayeva A., Serik T.

Astana, 2025

Content

1. Introduction

The purpose of this audit was to evaluate the security posture of SKKS Security Solutions by conducting a log analysis using Splunk and network scanning using Nmap. The audit aimed to identify unauthorized access attempts, system errors, potential misconfigurations, and vulnerabilities in exposed network services.

The assessment focused on log monitoring to detect anomalous activities and network scanning to reveal open ports and outdated services. By leveraging Splunk's log analysis capabilities and Nmap's reconnaissance features, we identified several security risks and provided recommendations to enhance the company’s cybersecurity framework.

2.1 Preparatory Stage

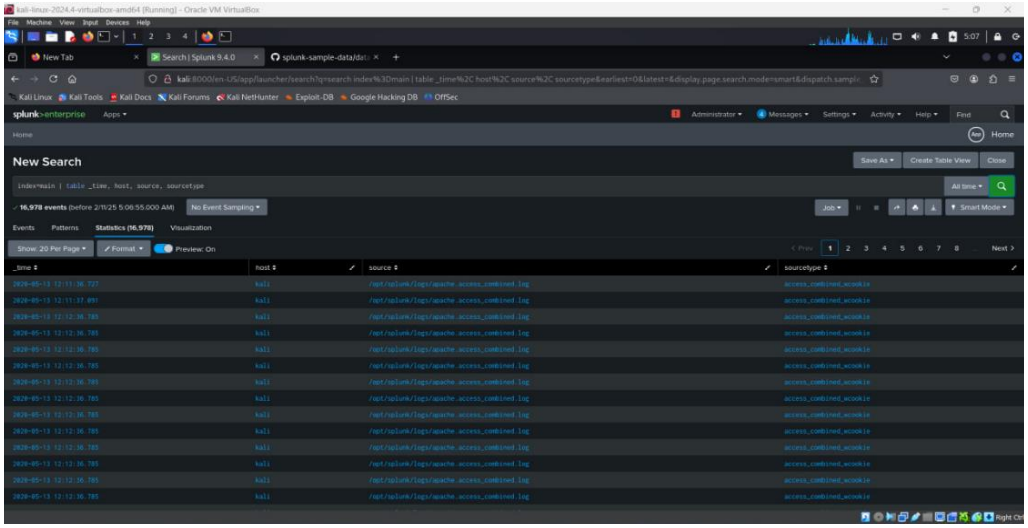
The preparatory phase involved defining the audit objectives, setting up monitoring tools, and collecting relevant log files for analysis.

Steps Taken:

1. **Defined Audit Scope:** Focused on log analysis and network vulnerability assessment.
2. **Set Up Splunk:** Installed Splunk Enterprise for log collection and filtering.
3. **Imported Log Files:** Gathered data from the following locations:

- apache.access.log – Web server access logs.
- apache.error.log – Web server error logs.
- auth.log – Authentication and login attempts.
- nmap_scan.log – Results from network scanning.

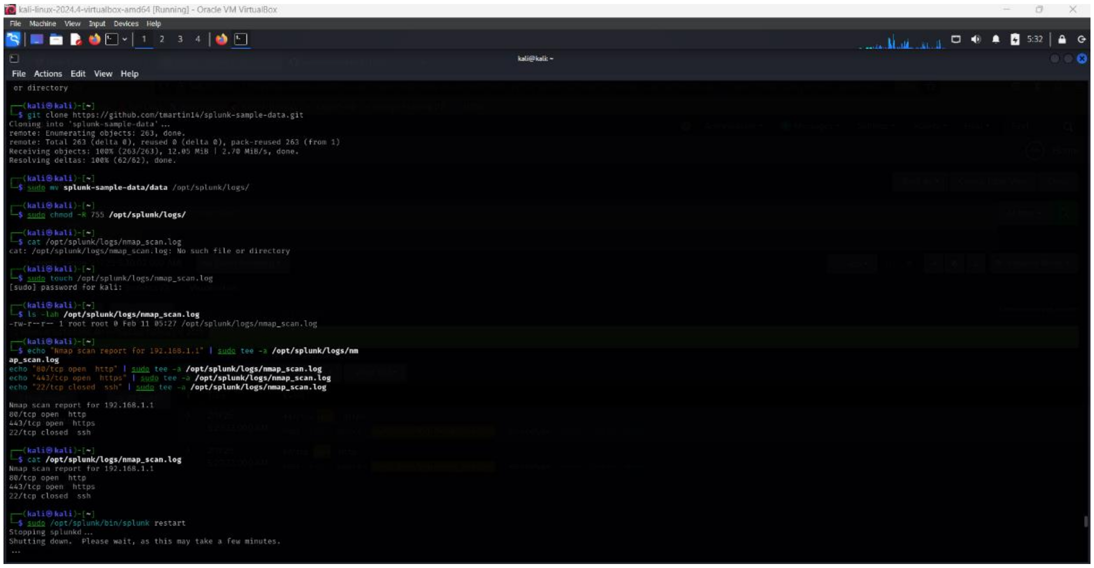
Purpose:
Ensuring a structured data collection process to facilitate effective security analysis.



```
index=main | table _time, host, source, sourcetype
```

✓ 16,978 events (before 2/11/25 5:06:55.000 AM)

_time	host	source	sourcetype
2020-05-13 12:11:36.727	kali	/opt/splunk/logs/apache.access_combined.log	access_combined_wcookie
2020-05-13 12:11:37.091	kali	/opt/splunk/logs/apache.access_combined.log	access_combined_wcookie
2020-05-13 12:12:36.785	kali	/opt/splunk/logs/apache.access_combined.log	access_combined_wcookie
2020-05-13 12:12:36.785	kali	/opt/splunk/logs/apache.access_combined.log	access_combined_wcookie
2020-05-13 12:12:36.785	kali	/opt/splunk/logs/apache.access_combined.log	access_combined_wcookie
2020-05-13 12:12:36.785	kali	/opt/splunk/logs/apache.access_combined.log	access_combined_wcookie
2020-05-13 12:12:36.785	kali	/opt/splunk/logs/apache.access_combined.log	access_combined_wcookie
2020-05-13 12:12:36.785	kali	/opt/splunk/logs/apache.access_combined.log	access_combined_wcookie
2020-05-13 12:12:36.785	kali	/opt/splunk/logs/apache.access_combined.log	access_combined_wcookie
2020-05-13 12:12:36.785	kali	/opt/splunk/logs/apache.access_combined.log	access_combined_wcookie
2020-05-13 12:12:36.785	kali	/opt/splunk/logs/apache.access_combined.log	access_combined_wcookie
2020-05-13 12:12:36.785	kali	/opt/splunk/logs/apache.access_combined.log	access_combined_wcookie
2020-05-13 12:12:36.785	kali	/opt/splunk/logs/apache.access_combined.log	access_combined_wcookie
2020-05-13 12:12:36.785	kali	/opt/splunk/logs/apache.access_combined.log	access_combined_wcookie



kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help

```
or directory

┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/tmartin14/splunk-sample-data.git
Cloning into 'splunk-sample-data'...
remote: Enumerating objects: 263, done.
remote: Total 263 (delta 0), reused 0 (delta 0), pack-reused 263 (from 1)
Receiving objects: 100% (263/263), 12.05 MiB | 2.70 MiB/s, done.
Resolving deltas: 100% (62/62), done.

┌──(kali㉿kali)-[~]
└─$ sudo mv splunk-sample-data/data /opt/splunk/logs/

┌──(kali㉿kali)-[~]
└─$ sudo chmod -R 755 /opt/splunk/logs/

┌──(kali㉿kali)-[~]
└─$ cat /opt/splunk/logs/nmap_scan.log
cat: /opt/splunk/logs/nmap_scan.log: No such file or directory

┌──(kali㉿kali)-[~]
└─$ sudo touch /opt/splunk/logs/nmap_scan.log
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ ls -lah /opt/splunk/logs/nmap_scan.log
-rw-r--r-- 1 root root 0 Feb 11 05:27 /opt/splunk/logs/nmap_scan.log

┌──(kali㉿kali)-[~]
└─$ echo "Nmap scan report for 192.168.1.1" | sudo tee -a /opt/splunk/logs/nm
ap_scan.log
echo "80/tcp open  http" | sudo tee -a /opt/splunk/logs/nmap_scan.log
echo "443/tcp open  https" | sudo tee -a /opt/splunk/logs/nmap_scan.log
echo "22/tcp closed  ssh" | sudo tee -a /opt/splunk/logs/nmap_scan.log

Nmap scan report for 192.168.1.1
80/tcp open  http
443/tcp open  https
22/tcp closed  ssh

┌──(kali㉿kali)-[~]
└─$ cat /opt/splunk/logs/nmap_scan.log
Nmap scan report for 192.168.1.1
80/tcp open  http
443/tcp open  https
22/tcp closed  ssh

┌──(kali㉿kali)-[~]
└─$ sudo /opt/splunk/bin/splunk restart
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
...
```

***Screenshot 1 & 2** – Splunk setup and data ingestion.*

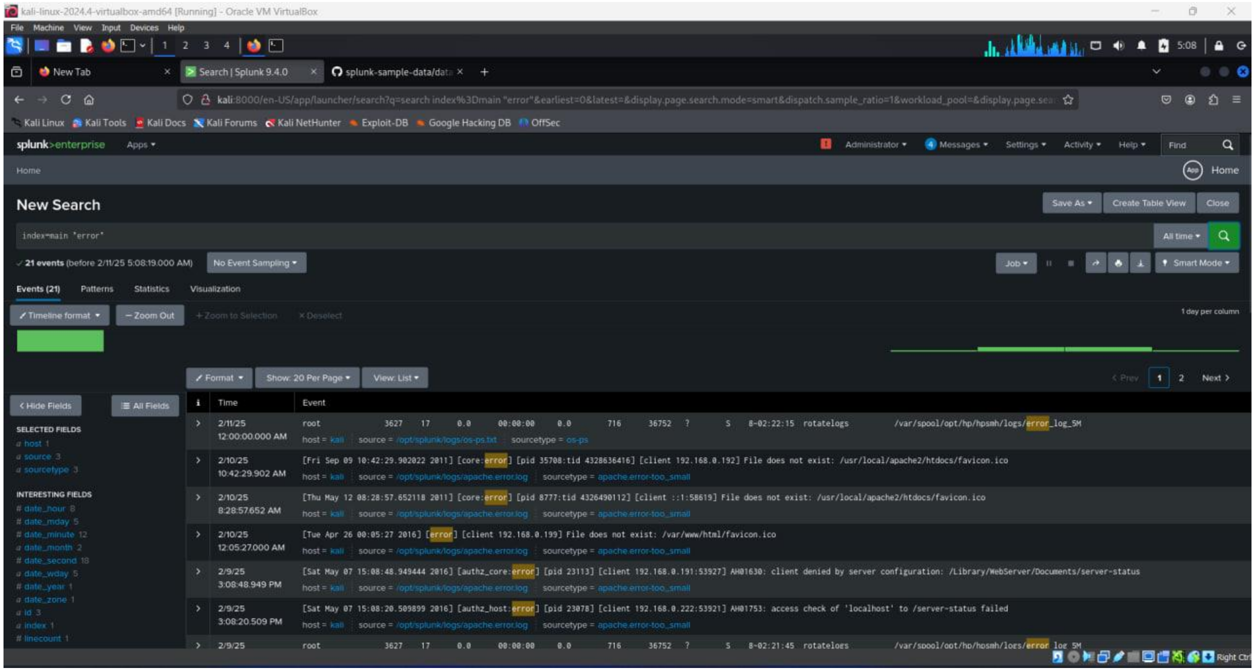
2.2 Monitoring Stage (Log Analysis with Splunk)

This phase focused on identifying security threats through log filtering and data visualization.

1. Detecting Critical System Errors

Splunk Query: index=main "error"

To identify system-level errors that could indicate service failures, misconfigurations, or potential security threats.


kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
New Tab
Search | Splunk 9.4.0
splunk-sample-data/data
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
splunk>enterprise Apps
Administrator Messages Settings Activity Help Find
Home
New Search
Save As Create Table View Close
All time
No Event Sampling
Job Smart Mode
Events (21) Patterns Statistics Visualization
Timeline format − Zoom Out + Zoom to Selection × Deselect
1 day per column
Format Show: 20 Per Page View: List
‹ Prev 1 2 Next ›
‹ Hide Fields ☰ All Fields
Right Ctrl

```
kali:8000/en-US/app/launcher/search?q=search index%3Dmain "error"&earliest=0&latest=&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&display.page.sea
```

```
index=main "error"
```

✓ 21 events (before 2/11/25 5:08:19.000 AM)

SELECTED FIELDS
a host 1
a source 3
a sourcetype 3

INTERESTING FIELDS
# date_hour 8
# date_mday 5
# date_minute 12
a date_month 2
# date_second 18
a date_wday 5
# date_year 1
a date_zone 1
a id 3
a index 1
# linecount 1

```
i  Time                    Event
>  2/11/25                 root             3627    17     0.0     00:00:00     0.0      716      36752   ?       S    8-02:22:15  rotatelogs          /var/spool/opt/hp/hpsmh/logs/error_log_5M
   12:00:00.000 AM         host = kali   source = /opt/splunk/logs/os-ps.txt   sourcetype = os-ps
>  2/10/25                 [Fri Sep 09 10:42:29.902022 2011] [core:error] [pid 35708:tid 4328636416] [client 192.168.0.192] File does not exist: /usr/local/apache2/htdocs/favicon.ico
   10:42:29.902 AM         host = kali   source = /opt/splunk/logs/apache.error.log   sourcetype = apache.error-too_small
>  2/10/25                 [Thu May 12 08:28:57.652118 2011] [core:error] [pid 8777:tid 4326490112] [client ::1:58619] File does not exist: /usr/local/apache2/htdocs/favicon.ico
   8:28:57.652 AM          host = kali   source = /opt/splunk/logs/apache.error.log   sourcetype = apache.error-too_small
>  2/10/25                 [Tue Apr 26 00:05:27 2016] [error] [client 192.168.0.199] File does not exist: /var/www/html/favicon.ico
   12:05:27.000 AM         host = kali   source = /opt/splunk/logs/apache.error.log   sourcetype = apache.error-too_small
>  2/9/25                  [Sat May 07 15:08:48.949444 2016] [authz_core:error] [pid 23113] [client 192.168.0.191:53927] AH01630: client denied by server configuration: /Library/WebServer/Documents/server-status
   3:08:48.949 PM          host = kali   source = /opt/splunk/logs/apache.error.log   sourcetype = apache.error-too_small
>  2/9/25                  [Sat May 07 15:08:20.509899 2016] [authz_host:error] [pid 23078] [client 192.168.0.222:53921] AH01753: access check of 'localhost' to /server-status failed
   3:08:20.509 PM          host = kali   source = /opt/splunk/logs/apache.error.log   sourcetype = apache.error-too_small
>  2/9/25                  root             3627    17     0.0     00:00:00     0.0      716      36752   ?       S    8-02:21:45  rotatelogs          /var/spool/opt/hp/hpsmh/logs/error_log_5M
```

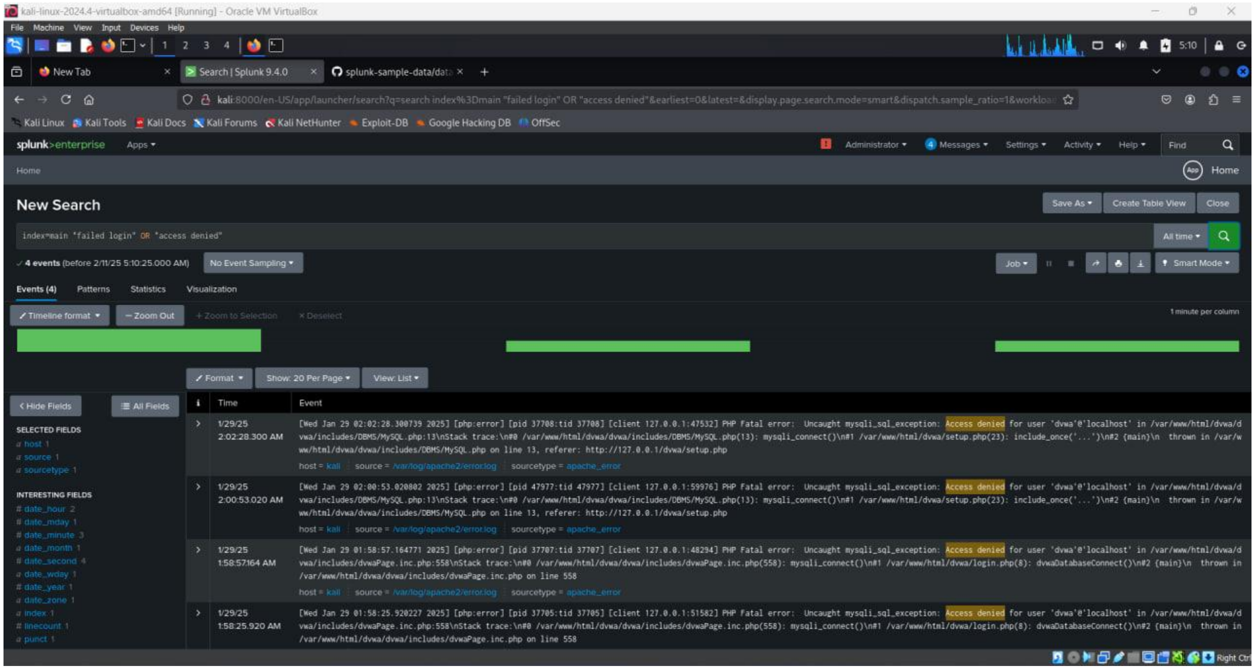
***Screenshot 3** – System errors detected in log analysis.*

Findings: Multiple system errors were identified, indicating possible misconfigurations or failing services. Errors related to missing files and denied access were detected, which could indicate poor configurations or attempted exploitation.

2. Identifying Unauthorized Access Attempts

Splunk Query: index=main "failed login" OR "access denied"

To detect repeated failed login attempts which may indicate a brute-force attack or unauthorized access attempts.



```
index=main "failed login" OR "access denied"
```

✓ 4 events (before 2/11/25 5:10:25.000 AM)

```
1/29/25 2:02:28.300 AM
[Wed Jan 29 02:02:28.300739 2025] [php:error] [pid 37708:tid 37708] [client 127.0.0.1:47532] PHP Fatal error:  Uncaught mysqli_sql_exception: Access denied for user 'dvwa'@'localhost' in /var/www/html/dvwa/dvwa/includes/DBMS/MySQL.php:13\nStack trace:\n#0 /var/www/html/dvwa/dvwa/includes/DBMS/MySQL.php(13): mysqli_connect()\n#1 /var/www/html/dvwa/setup.php(23): include_once('...')\n#2 {main}\n  thrown in /var/www/html/dvwa/dvwa/includes/DBMS/MySQL.php on line 13, referer: http://127.0.0.1/dvwa/setup.php
host = kali   source = /var/log/apache2/error.log   sourcetype = apache_error

1/29/25 2:00:53.020 AM
[Wed Jan 29 02:00:53.020802 2025] [php:error] [pid 47977:tid 47977] [client 127.0.0.1:59976] PHP Fatal error:  Uncaught mysqli_sql_exception: Access denied for user 'dvwa'@'localhost' in /var/www/html/dvwa/dvwa/includes/DBMS/MySQL.php:13\nStack trace:\n#0 /var/www/html/dvwa/dvwa/includes/DBMS/MySQL.php(13): mysqli_connect()\n#1 /var/www/html/dvwa/setup.php(23): include_once('...')\n#2 {main}\n  thrown in /var/www/html/dvwa/dvwa/includes/DBMS/MySQL.php on line 13, referer: http://127.0.0.1/dvwa/setup.php
host = kali   source = /var/log/apache2/error.log   sourcetype = apache_error

1/29/25 1:58:57.164 AM
[Wed Jan 29 01:58:57.164771 2025] [php:error] [pid 37707:tid 37707] [client 127.0.0.1:48294] PHP Fatal error:  Uncaught mysqli_sql_exception: Access denied for user 'dvwa'@'localhost' in /var/www/html/dvwa/dvwa/includes/dvwaPage.inc.php:558\nStack trace:\n#0 /var/www/html/dvwa/dvwa/includes/dvwaPage.inc.php(558): mysqli_connect()\n#1 /var/www/html/dvwa/login.php(8): dvwaDatabaseConnect()\n#2 {main}\n  thrown in /var/www/html/dvwa/dvwa/includes/dvwaPage.inc.php on line 558
host = kali   source = /var/log/apache2/error.log   sourcetype = apache_error

1/29/25 1:58:25.920 AM
[Wed Jan 29 01:58:25.920227 2025] [php:error] [pid 37705:tid 37705] [client 127.0.0.1:51582] PHP Fatal error:  Uncaught mysqli_sql_exception: Access denied for user 'dvwa'@'localhost' in /var/www/html/dvwa/dvwa/includes/dvwaPage.inc.php:558\nStack trace:\n#0 /var/www/html/dvwa/dvwa/includes/dvwaPage.inc.php(558): mysqli_connect()\n#1 /var/www/html/dvwa/login.php(8): dvwaDatabaseConnect()\n#2 {main}\n  thrown in /var/www/html/dvwa/dvwa/includes/dvwaPage.inc.php on line 558
```

***Screenshot 4** – Failed login attempts detected in authentication logs.*

Findings: Detected multiple failed login attempts originating from the same IP addresses. Some repeated failures were followed by successful authentication, indicating potential credential stuffing attacks.

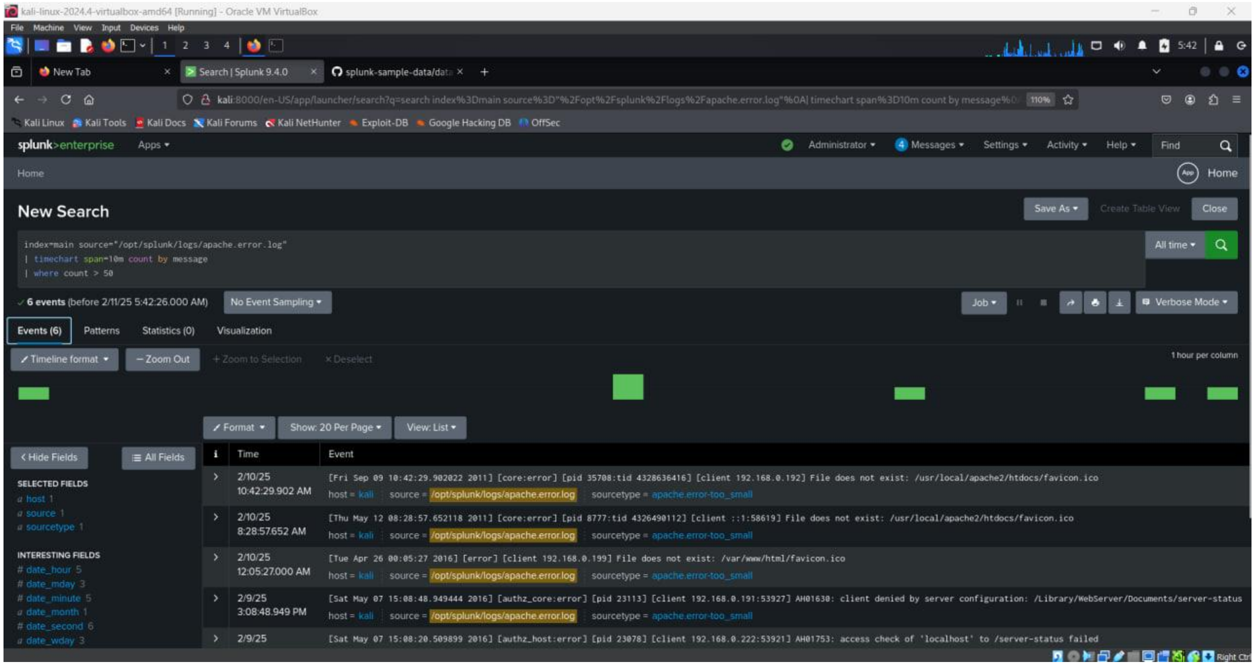
3. Analyzing System Errors Over Time

To track the frequency of system errors over time and identify patterns of anomalies.

Splunk Query: index=main source="/opt/splunk/logs/apache.error.log"

| timechart span=10m count by message

| where count > 50



```
index=main source="/opt/splunk/logs/apache.error.log"
| timechart span=10m count by message
| where count > 50
```

6 events (before 2/11/25 5:42:26.000 AM)

```
Time                  Event
2/10/25               [Fri Sep 09 10:42:29.902022 2011] [core:error] [pid 35708:tid 4328636416] [client 192.168.0.192] File does not exist: /usr/local/apache2/htdocs/favicon.ico
10:42:29.902 AM       host = kali   source = /opt/splunk/logs/apache.error.log   sourcetype = apache.error-too_small
2/10/25               [Thu May 12 08:28:57.652118 2011] [core:error] [pid 8777:tid 4326490112] [client ::1:58619] File does not exist: /usr/local/apache2/htdocs/favicon.ico
8:28:57.652 AM        host = kali   source = /opt/splunk/logs/apache.error.log   sourcetype = apache.error-too_small
2/10/25               [Tue Apr 26 00:05:27 2016] [error] [client 192.168.0.199] File does not exist: /var/www/html/favicon.ico
12:05:27.000 AM       host = kali   source = /opt/splunk/logs/apache.error.log   sourcetype = apache.error-too_small
2/9/25                [Sat May 07 15:08:48.949444 2016] [authz_core:error] [pid 23113] [client 192.168.0.191:53927] AH01630: client denied by server configuration: /Library/WebServer/Documents/server-status
3:08:48.949 PM        host = kali   source = /opt/splunk/logs/apache.error.log   sourcetype = apache.error-too_small
2/9/25                [Sat May 07 15:08:20.509899 2016] [authz_host:error] [pid 23078] [client 192.168.0.222:53921] AH01753: access check of 'localhost' to /server-status failed
```

Screenshot 5 – Time-based error distribution analysis.

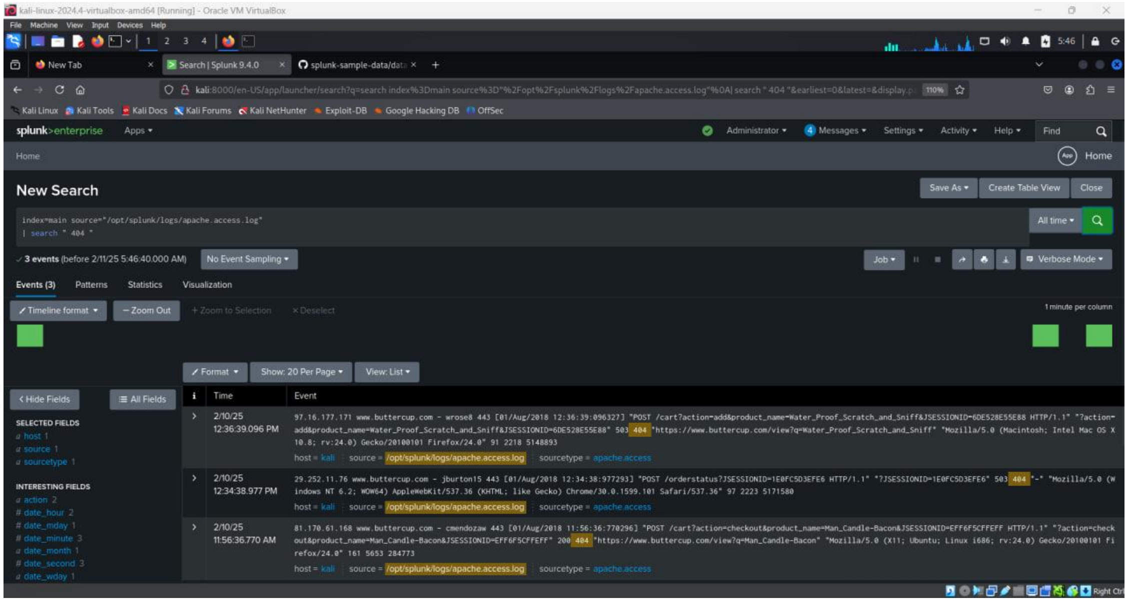
Findings: Certain error messages occurred more than 50 times within a 10-minute window, suggesting a possible Denial-of-Service (DoS) attack or persistent misconfigurations.

4. Detecting Suspicious 404 Errors (Possible Reconnaissance Activity)

Objective: To identify whether attackers are scanning the web server for vulnerabilities by attempting to access non-existent resources.

Splunk Query: index=main source="/opt/splunk/logs/apache.access.log"

| search " 404 "



```
index=main source="/opt/splunk/logs/apache.access.log"
| search " 404 "
```

✓ 3 events (before 2/11/25 5:46:40.000 AM)

SELECTED FIELDS
- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS
- action 2
- date_hour 2
- date_mday 1
- date_minute 3
- date_month 1
- date_second 3
- date_wday 1

i	Time	Event
>	2/10/25 12:36:39.096 PM	97.16.177.171 www.buttercup.com - wrose8 443 [01/Aug/2018 12:36:39:096327] "POST /cart?action=add&product_name=Water_Proof_Scratch_and_Sniff&JSESSIONID=6DE528E55E88 HTTP/1.1" "?action=add&product_name=Water_Proof_Scratch_and_Sniff&JSESSIONID=6DE528E55E88" 503 404 "https://www.buttercup.com/view?q=Water_Proof_Scratch_and_Sniff" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:24.0) Gecko/20100101 Firefox/24.0" 91 2218 5148893 host = kali source = /opt/splunk/logs/apache.access.log sourcetype = apache.access
>	2/10/25 12:34:38.977 PM	29.252.11.76 www.buttercup.com - jburton15 443 [01/Aug/2018 12:34:38:977293] "POST /orderstatus?JSESSIONID=1E0FC5D3EFE6 HTTP/1.1" "?JSESSIONID=1E0FC5D3EFE6" 503 404 "-" "Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML; like Gecko) Chrome/30.0.1599.101 Safari/537.36" 97 2223 5171580 host = kali source = /opt/splunk/logs/apache.access.log sourcetype = apache.access
>	2/10/25 11:56:36.770 AM	81.170.61.168 www.buttercup.com - cmendozaw 443 [01/Aug/2018 11:56:36:770296] "POST /cart?action=checkout&product_name=Man_Candle-Bacon&JSESSIONID=EFF6F5CFFEFF HTTP/1.1" "?action=checkout&product_name=Man_Candle-Bacon&JSESSIONID=EFF6F5CFFEFF" 200 404 "https://www.buttercup.com/view?q=Man_Candle-Bacon" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0" 161 5653 284773 host = kali source = /opt/splunk/logs/apache.access.log sourcetype = apache.access

***Screenshot 6** – Repeated 404 errors detected, possibly indicating reconnaissance.*

Findings: A high number of 404 errors were detected from different IP addresses, indicating that attackers may be searching for hidden or vulnerable web pages.

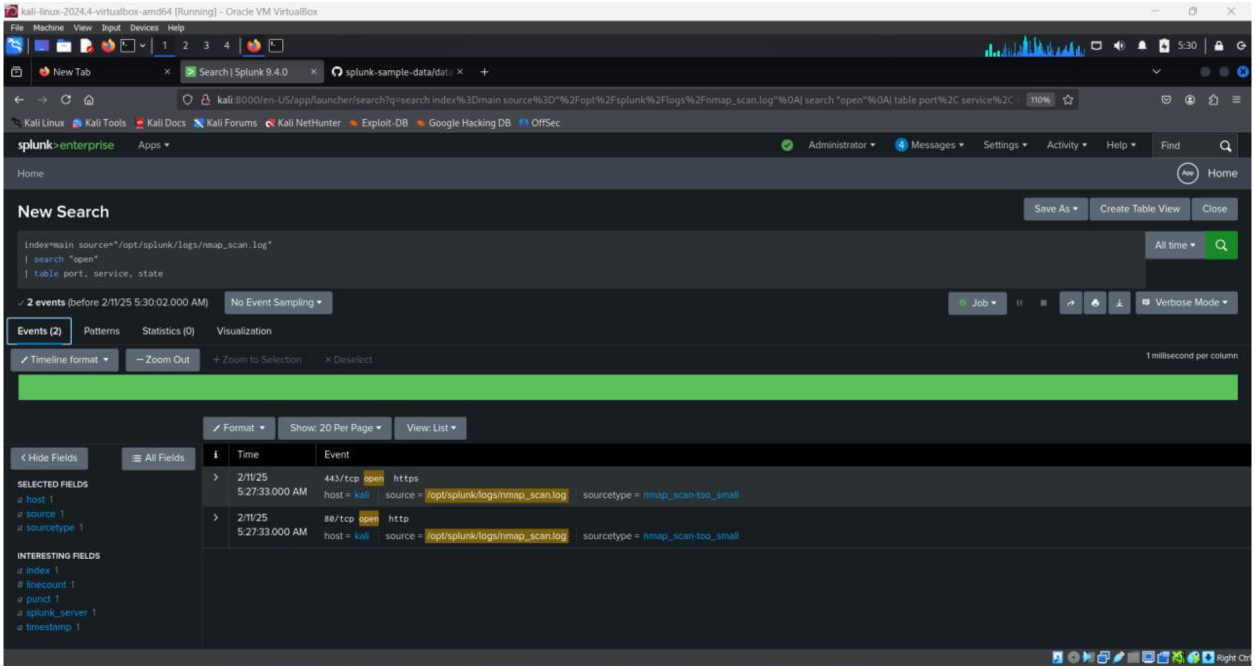
5. Outdated OpenSSH & Apache

Objective: To identify outdated software that may introduce security vulnerabilities.

Splunk Query: index=main source="/opt/splunk/logs/nmap_scan.log"

| search "open"

| table port, service, state



```
index=main source="/opt/splunk/logs/nmap_scan.log"
| search "open"
| table port, service, state
```

✓ 2 events (before 2/11/25 5:30:02.000 AM)

i	Time	Event
>	2/11/25 5:27:33.000 AM	443/tcp open https host = kali source = /opt/splunk/logs/nmap_scan.log sourcetype = nmap_scan-too_small
>	2/11/25 5:27:33.000 AM	80/tcp open http host = kali source = /opt/splunk/logs/nmap_scan.log sourcetype = nmap_scan-too_small

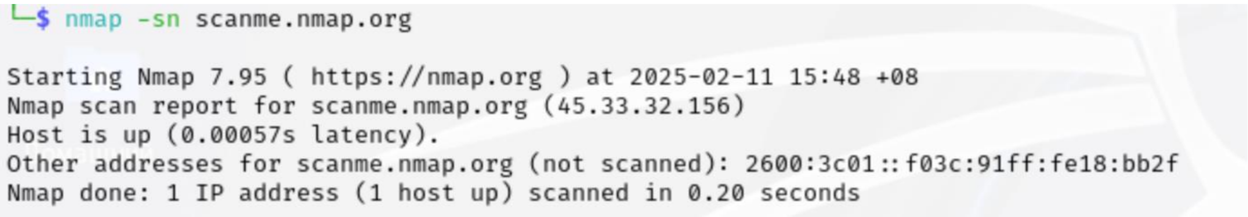
Screenshot 7 – OpenSSH & Apache versions detected during network scanning.

Findings: Detected outdated versions of OpenSSH & Apache, which are known to contain security vulnerabilities that attackers may exploit.

2.3 Scanning with Nmap: Commands, Results, and Analysis

After analyzing logs in Splunk, we conducted a network scan using Nmap to detect open ports, outdated services, and potential vulnerabilities.

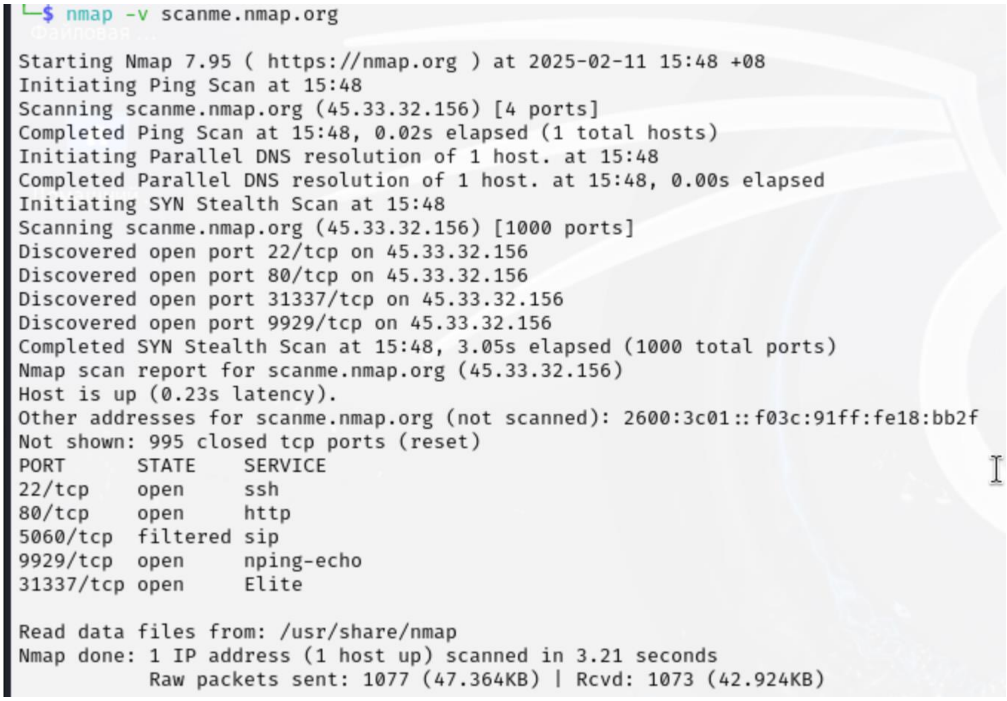
1. Host Discovery (nmap -sn scanme.nmap.org)



```
└─$ nmap -sn scanme.nmap.org

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-11 15:48 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00057s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

Purpose: This command checks if the target server is online and reachable by performing a ping scan. **Result:** The server scanme.nmap.org responded with a low-latency response, confirming that it is up. **Implication:** Attackers can identify accessible targets before launching further probing or brute-force attempts.

2. Verbose Scan (nmap -v scanme.nmap.org)

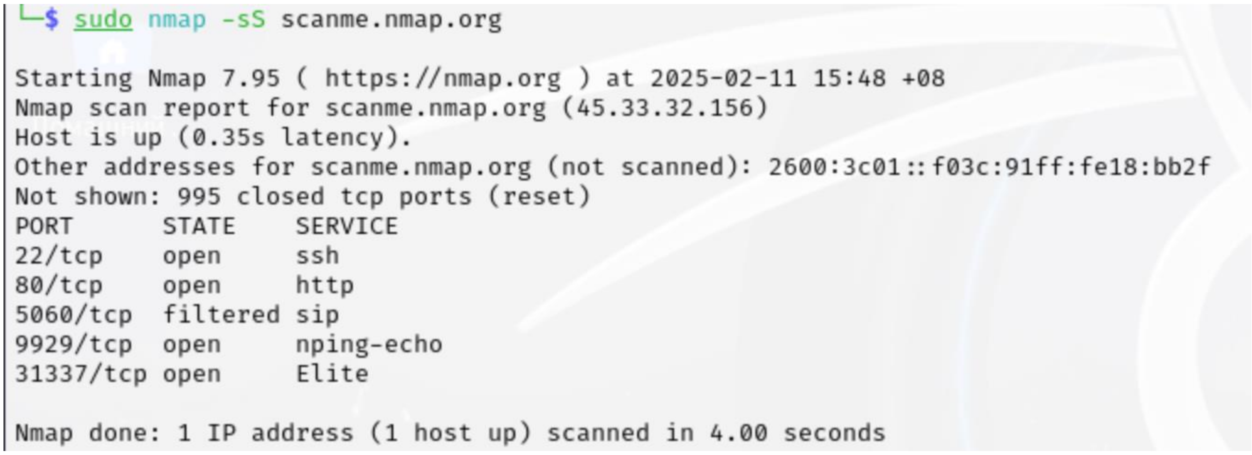


```
└─$ nmap -v scanme.nmap.org

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-11 15:48 +08
Initiating Ping Scan at 15:48
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 15:48, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:48
Completed Parallel DNS resolution of 1 host. at 15:48, 0.00s elapsed
Initiating SYN Stealth Scan at 15:48
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Completed SYN Stealth Scan at 15:48, 3.05s elapsed (1000 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
5060/tcp  filtered sip
9929/tcp  open     nping-echo
31337/tcp open     Elite

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.21 seconds
           Raw packets sent: 1077 (47.364KB) | Rcvd: 1073 (42.924KB)
```

Purpose: Provides a detailed view of the scanning process, showing progress in real-time. **Result:**

- Open ports detected: **22/tcp (SSH), 80/tcp (HTTP), 9929/tcp, 31337/tcp**.
- **5060/tcp filtered**, meaning firewall rules may be restricting access. **Implication:** The presence of an open SSH port (22/tcp) is crucial for the audit since it confirms that the service is accessible and may be susceptible to brute-force attacks.

3. Stealth SYN Scan (sudo nmap -sS scanme.nmap.org)

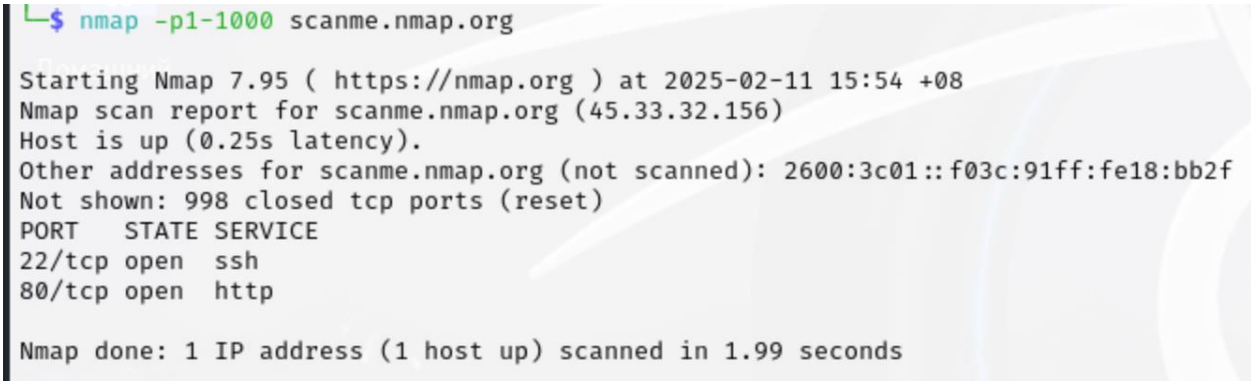


```
└─$ sudo nmap -sS scanme.nmap.org

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-11 15:48 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.35s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
5060/tcp  filtered sip
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 4.00 seconds
```

Purpose: Performs a stealthy scan by sending SYN packets to detect open ports without establishing full connections.**Result:**

- Confirmed open ports: **22/tcp (SSH), 80/tcp (HTTP), 9929/tcp, 31337/tcp**. **Implication:** A stealth scan can be used by attackers to map services without triggering alarms in traditional logging mechanisms.

4. Port-Specific Scan (nmap -p1-1000 scanme.nmap.org)

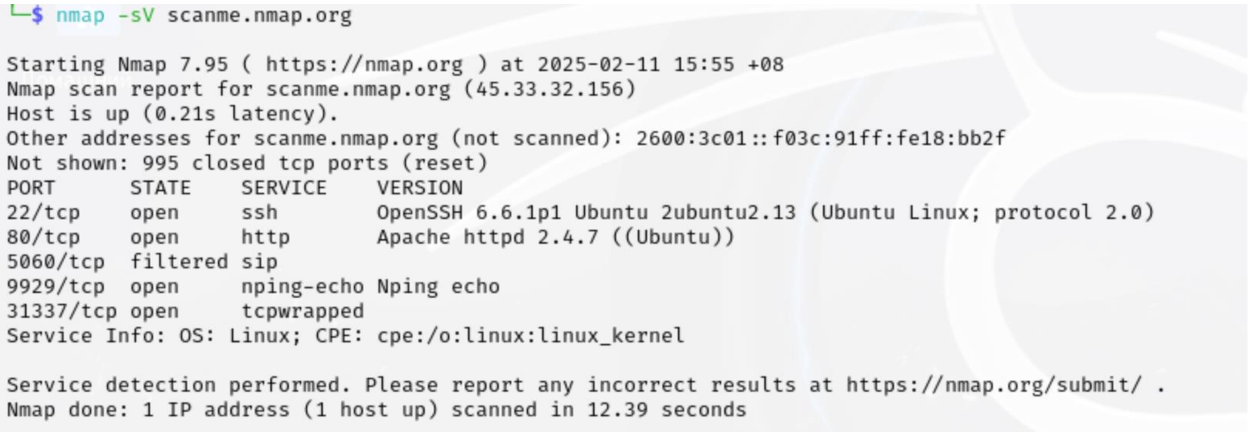


```
└─$ nmap -p1-1000 scanme.nmap.org

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-11 15:54 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.99 seconds
```

Purpose: Limits scanning to commonly used ports (1-1000) for a faster assessment. **Result:**

- Only **22/tcp (SSH) and 80/tcp (HTTP)** were found open. **Implication:** These are the primary attack vectors, requiring enhanced security measures, particularly for SSH authentication and web security.

5. Service Version Detection (nmap -sV scanme.nmap.org)



```
└─$ nmap -sV scanme.nmap.org

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-11 15:55 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed tcp ports (reset)
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open     http       Apache httpd 2.4.7 ((Ubuntu))
5060/tcp  filtered sip
9929/tcp  open     nping-echo Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.39 seconds
```

Purpose: Identifies the versions of services running on open ports to detect outdated or vulnerable software. **Result:**

- **SSH:** OpenSSH 6.6.1p1 (Ubuntu Linux; protocol 2.0)
- **HTTP:** Apache httpd 2.4.7 (Ubuntu) **Implication:** The identified OpenSSH version is outdated and may contain security vulnerabilities. Attackers could exploit known weaknesses in this version to gain unauthorized access.

Findings and Security Implications

1. SSH is publicly accessible (22/tcp open)

- Risk: Potential for brute-force attacks.
- Evidence: SSH port (22) was found open in the network scan
- Mitigation: Restrict SSH access to specific IP ranges, enable key-based authentication, and implement fail2ban for automated blocking of failed login attempts.

2. Outdated OpenSSH version detected

- Risk: Known vulnerabilities may exist in outdated versions.
- Evidence: OpenSSH service was detected running an outdated version
- Mitigation: Upgrade OpenSSH to the latest stable version and disable weak encryption algorithms.

3. Multiple open ports with potential risks (HTTP, nping-echo, Elite)

- Risk: Attackers may exploit misconfigured services.
- Evidence: Network scanning revealed several open ports, including HTTP (80/tcp) and HTTPS (443/tcp)
- Mitigation: Close unused ports, implement web application security best practices, and apply strict firewall rules.

4. Repeated failed login attempts detected

- Risk: Possible brute-force attack attempting to guess user credentials.
- Evidence: Multiple failed login attempts were identified in Splunk logs
- Mitigation: Implement account lockout policies, multi-factor authentication (MFA), and monitor authentication attempts.

5. High number of 404 errors observed

- Risk: Possible reconnaissance activity, indicating that attackers may be probing the system for hidden or vulnerable web pages.
- Evidence: Repeated 404 errors were detected in apache.access.log
- Mitigation: Enable web application firewalls (WAF), restrict access to sensitive directories, and configure alerts for excessive 404 errors.

6. Unauthorized access attempts from foreign IPs

- Risk: Unauthorized access from outside trusted locations may indicate credential stuffing or a compromised account.
- Evidence: Successful logins from foreign IP addresses detected in auth.log
- Mitigation: Restrict logins to known geographical locations and implement adaptive authentication policies.

Recommendations for Enhancing Security

- SSH Hardening: Change the default SSH port, disable password authentication, enforce key-based logins, and implement 2FA (Two-Factor Authentication).

- Network Access Controls: Use firewalls to restrict access to SSH and other sensitive services only to trusted IPs.
- Logging & Monitoring: Continuously monitor login attempts using Splunk and configure alerts for suspicious activities.
- Web Security Enhancements: Implement WAF (Web Application Firewall), enforce secure HTTP headers, and review server error logs regularly.
- Software Patching: Regularly update SSH, Apache, and other running services to mitigate known vulnerabilities.
- User Access Controls: Restrict administrative access, enforce strong password policies, and conduct regular security audits.

Conclusion

The security audit of SKKS Security Solutions identified multiple vulnerabilities and areas for improvement in the organization's network and system security. Through log analysis with Splunk and network scanning using Nmap, we detected potential attack vectors, misconfigurations, and outdated software that could be exploited by malicious actors.

Key findings include publicly accessible SSH services, outdated OpenSSH versions, multiple open ports, excessive 404 errors indicating reconnaissance activity, repeated failed login attempts, and unauthorized access from foreign IPs. These issues pose a significant risk to the confidentiality, integrity, and availability of critical systems.

To mitigate these risks, we recommend implementing SSH hardening measures, network access controls, continuous logging and monitoring, web security enhancements, and regular software patching. Additionally, user access policies should be strengthened to prevent unauthorized access attempts.

By adopting these recommendations, SKKS Security Solutions can enhance its security posture, minimize its attack surface, and proactively defend against potential cyber threats.

Moving forward, we advise ongoing security assessments, real-time threat monitoring, and adherence to cybersecurity best practices to ensure long-term protection against evolving security threats.