09th Dec 2024

Mastering the SOC: WEEK 2 (What I Know, Learn, and Apply)

Last week I delved into the essentials of incident management, network-based cyberattacks, and hands-on learning with Kali Linux. Here's a snapshot of my progress and key takeaways!

What I Revised:

Difference between an Event and an Incident.

Understanding Security Incidents: Explored what defines a security incident and the importance of triage in mitigating risks.

Network-Based Cyber Attacks: Gained foundational knowledge about attack types and detection strategies.

Incident Escalation: Studied the general escalation process based on priorities critical, high, medium, low (corresponding to “immediate action”, “prompt response”, “steady management”, “routine oversight” respectively) and how to tailor responses for client environments.

What I Learned:

Effective triage can drastically reduce response time and limit the impact of incidents.

The anatomy of common network-based attacks, such as DDoS and MITM, and how they exploit vulnerabilities.

Communication is key: tailoring incident reports for clients improves understanding and trust.

The most interesting topic I found was “analyst notes”. What are analyst notes?

Practical Application:

(I personally find VMware and VirtualBox very convenient to use. The fastest and easiest way to install an OS into your VM is via ISO file. Download the ISO file from the official Linux website and upload it into VM. That’s it!)

Set up a Kali VM and executed a basic network scan attack (only used Nmap) in a controlled environment to understand attacker methodologies.

Observed how network scans are detected by monitoring tools, bridging theory with practice.

Outcomes and Reflections:

- Sharpened my analytical thinking for incident triage.

- Enhanced technical skills in setting up secure test environments and executing network scans.
- Built confidence in aligning technical insights with client needs.

Event: is any observable occurrence in a system, network, or IT environment. It can be routine, harmless, or potentially suspicious. Ex. a user logging into a system, file being accessed or modified, network packet being sent or received, antivirus software detecting a suspicious file.

Incident: is a confirmed or suspected violation of security policies, processes, or laws that could harm the organisation's systems, data, or reputation. Ex. successful phishing attack leading to unauthorised access, malware infection spreading across endpoints, Denial of Service (DoS) attack disrupting services, data exfiltration by an insider threat.

Every incident is an event, but every event is NOT an incident.

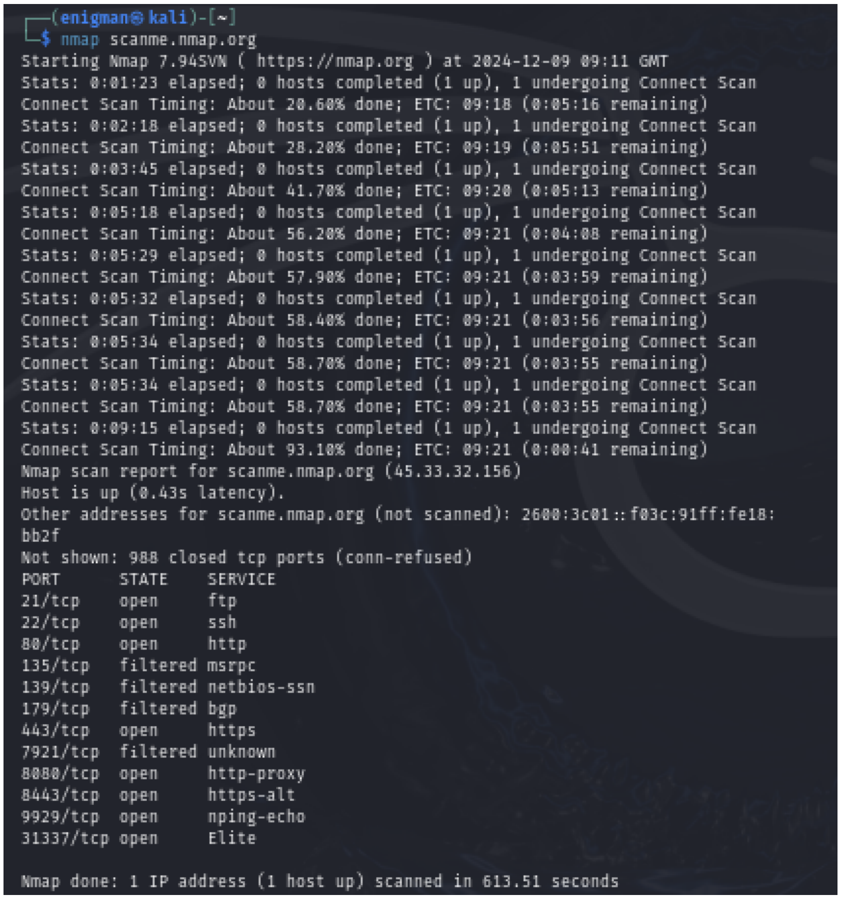
Analyst Notes: Recording of any alert that comes, documenting it, especially an incident. This analyst note is then contributed to the senior specialist the incident is escalated to. The specialist then reviews the incident based on the analyst notes created by the SOC analyst.

Components of Analyst Notes:

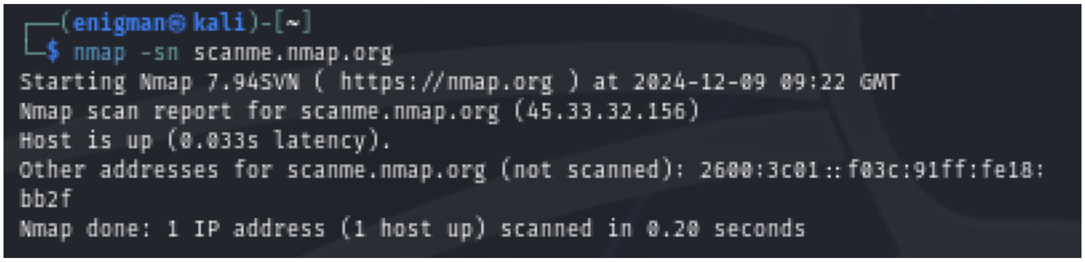
- Timestamps – Setting the Chronology – Record of all the event sequences that take place during an alert, so that the next person who reads it gets a clear understanding of what took place before the alert was raised, before the incident was raised, checking the logs of time.
- Analysis Steps – Tells the story of what the SOC analyst actually did. It's a comprehensive account navigation through the alert that came in, details the decision making process, and the path that was selected. It's like a Blueprint for future analysts, that come in and review that note to get a good understanding of what we as SOC analyst did and also helps the understanding of escalation of an alert into an incident.
- Identified threats or False positives – In both the cases, as much information needed goes into the analyst notes, to be thorough with all situations.
- Remediation Actions – Proactive or reactive countermeasures are noted down, eg. When an application is vulnerable to critical severity exploit, then we as SOC analyst can immediately update the remediation actions component of the analyst notes.
- Additional Observations – Beyond the standard recording of the event or alerts, there can be certain insights or speculations that can enrich the notes depth, offering clarity for those navigating similar cybersecurity alerts or instances to come in. Eg. There might be research we have done in Google that helps us understand the cyberattack better, so we should be putting all of the information in there, even the references that we have got from some people, so that other analysts and team can go back and get an understanding of our mindset and what we're looking at to determine that specific situation at that point in time. They should be able to understand the evidence that made us to make a particular decision in time.

Running some of the Nmap scans on Linux terminal on the following websites: (screenshots below with description of each flag) scanme.nmap.org: Hosted by the Nmap project, this website is explicitly set up for safe testing of Nmap capabilities. It is for educational purposes and testing only.

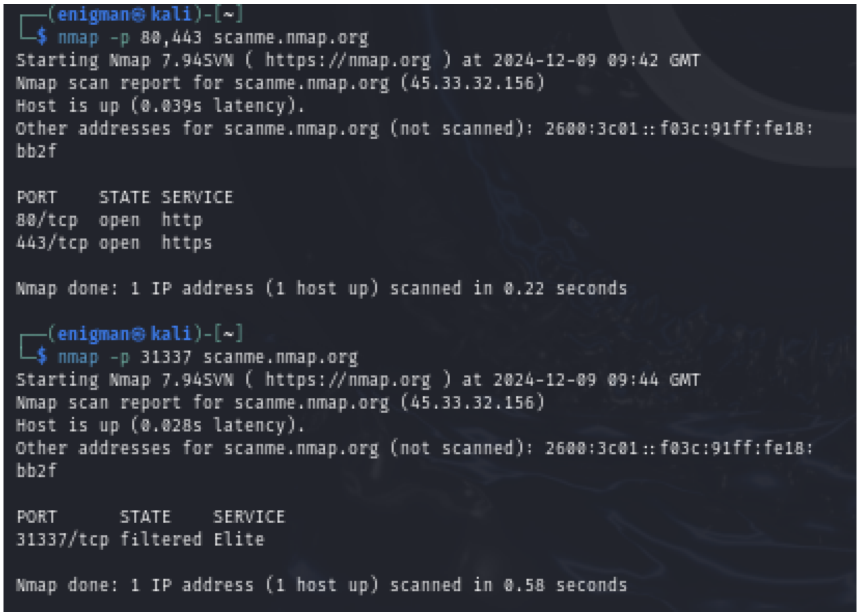
testfire.net (offered by IBM): A sample web application for security testing purposes.



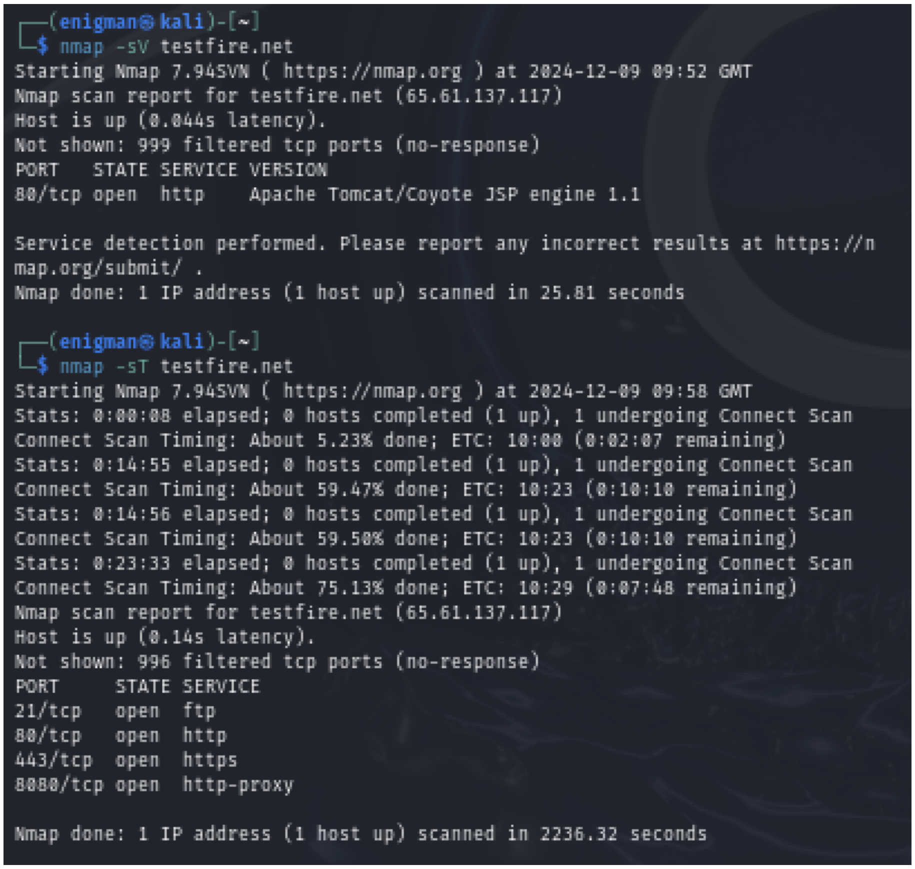
```
┌──(enigman㉿kali)-[~]
└─$ nmap scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 09:11 GMT
Stats: 0:01:23 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 20.60% done; ETC: 09:18 (0:05:16 remaining)
Stats: 0:02:18 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 28.20% done; ETC: 09:19 (0:05:51 remaining)
Stats: 0:03:45 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 41.70% done; ETC: 09:20 (0:05:13 remaining)
Stats: 0:05:18 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 56.20% done; ETC: 09:21 (0:04:08 remaining)
Stats: 0:05:29 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 57.90% done; ETC: 09:21 (0:03:59 remaining)
Stats: 0:05:32 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 58.40% done; ETC: 09:21 (0:03:56 remaining)
Stats: 0:05:34 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 58.70% done; ETC: 09:21 (0:03:55 remaining)
Stats: 0:05:34 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 58.70% done; ETC: 09:21 (0:03:55 remaining)
Stats: 0:09:15 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 93.10% done; ETC: 09:21 (0:00:41 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.43s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
179/tcp   filtered bgp
443/tcp   open     https
7921/tcp  filtered unknown
8080/tcp  open     http-proxy
8443/tcp  open     https-alt
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 613.51 seconds
```



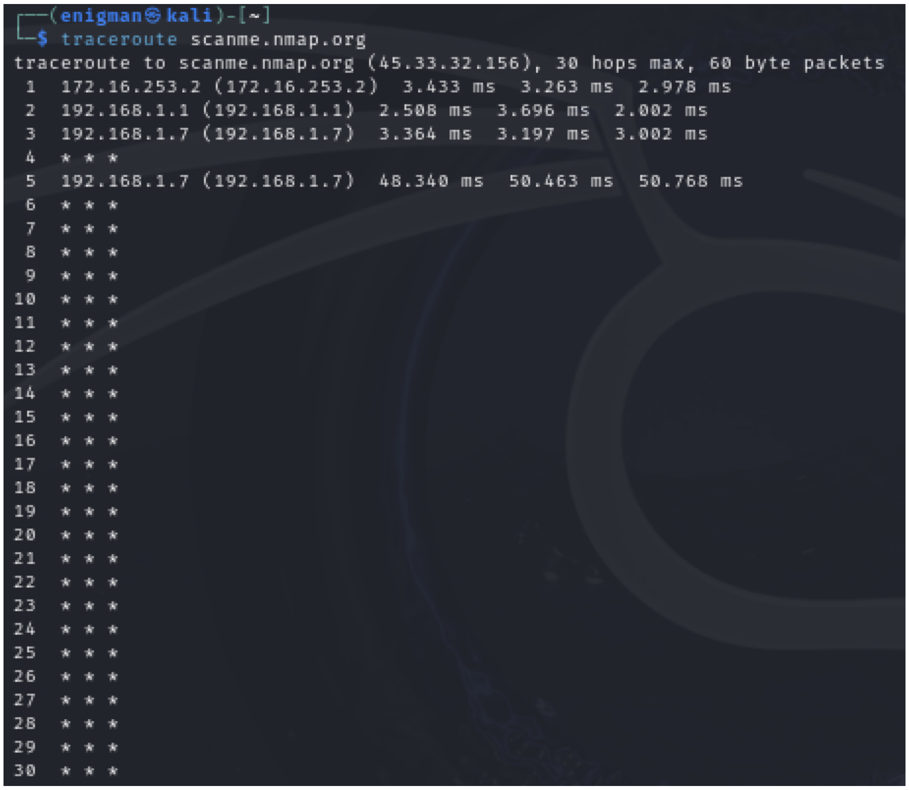
```
┌──(enigman㉿kali)-[~]
└─$ nmap -sn scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 09:22 GMT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.033s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```



```
┌──(enigman㉿kali)-[~]
└─$ nmap -p 80,443 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 09:42 GMT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.039s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f

PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds

┌──(enigman㉿kali)-[~]
└─$ nmap -p 31337 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 09:44 GMT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.028s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f

PORT      STATE    SERVICE
31337/tcp filtered Elite

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
```



```
┌──(enigman㉿kali)-[~]
└─$ nmap -sV testfire.net
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 09:52 GMT
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.044s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.81 seconds

┌──(enigman㉿kali)-[~]
└─$ nmap -sT testfire.net
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 09:58 GMT
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 5.23% done; ETC: 10:00 (0:02:07 remaining)
Stats: 0:14:55 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 59.47% done; ETC: 10:23 (0:10:10 remaining)
Stats: 0:14:56 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 59.50% done; ETC: 10:23 (0:10:10 remaining)
Stats: 0:23:33 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 75.13% done; ETC: 10:29 (0:07:48 remaining)
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.14s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 2236.32 seconds
```



```
┌──(enigman㉿kali)-[~]
└─$ traceroute scanme.nmap.org
traceroute to scanme.nmap.org (45.33.32.156), 30 hops max, 60 byte packets
 1  172.16.253.2 (172.16.253.2)  3.433 ms  3.263 ms  2.978 ms
 2  192.168.1.1 (192.168.1.1)  2.508 ms  3.696 ms  2.002 ms
 3  192.168.1.7 (192.168.1.7)  3.364 ms  3.197 ms  3.002 ms
 4  * * *
 5  192.168.1.7 (192.168.1.7)  48.340 ms  50.463 ms  50.768 ms
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Nmap command flags:

1. Simple Host Discovery

Command: nmap -sn [Target IP or range]

Flag Explanation: The -sn flag initiates a simple host discovery (ping scan) to check which hosts are up without scanning ports.

Why It’s Used: This scan is primarily used to identify live hosts on a network without triggering a more intrusive port scan. It's often the first step to establish a baseline of active devices in an environment.

Information to Look For:

- List of live hosts.
- Unexpected devices on the network (indicating unauthorized access or rogue devices).

SOC Relevance: Understanding which devices are live helps to maintain an accurate asset inventory and identify suspicious or unauthorized devices that shouldn't be on the network. This step is crucial for threat hunting and asset discovery in a SOC environment.

2. Basic Port Scan

Command: nmap -p 80,443 [target IP]

Flag Explanation: The -p flag specifies which ports to scan (e.g., ports 80 and 443 for HTTP and HTTPS).

Why It’s Used: This scan targets specific ports to identify if common services, like web servers, are accessible on a host. This can reveal what services are running and whether these ports are unexpectedly open.

Information to Look For:

- Open ports that indicate running services.
- Services that shouldn’t be accessible externally (e.g., database or management interfaces).

SOC Relevance: In a SOC role, you need to verify that only authorized services are accessible on a network. If critical ports like SSH (22) or RDP (3389) are exposed when they shouldn't be, it might indicate a misconfiguration or a security gap.

3. Service Version Detection

Command: nmap -sV [target IP]

Flag Explanation: The -sV flag attempts to detect the versions of services running on open ports.

Why It’s Used: Service version detection helps identify the exact version of software running on a target. This is essential for vulnerability assessment, as specific versions may have known vulnerabilities.

Information to Look For:

- Service names and version numbers.
- Deprecated or vulnerable software versions.

SOC Relevance: Accurate version information is vital in a SOC role to correlate services with known vulnerabilities. For example, detecting an outdated version of Apache or a vulnerable FTP service would require immediate attention and remediation to prevent potential exploits.

4. Full TCP Scan

Command: nmap -sT [target IP]

Flag Explanation: The -sT flag initiates a full TCP connection scan, providing accurate results but is noisier.

Why It’s Used: A full TCP scan (also known as a connect scan) establishes a complete TCP handshake with each port, making it more reliable in detecting open services compared to a SYN scan.

Information to Look For:

- Comprehensive list of open ports and running services.
- High number of unexpected open ports.

SOC Relevance: In a SOC environment, a full TCP scan can help map the complete attack surface of a device. This information is useful for conducting detailed security assessments and identifying potential attack vectors.

5. Aggressive Scan

Command: nmap -A [target IP]

Flag Explanation: The -A flag enables aggressive scanning, combining multiple advanced scanning techniques into one command.

Techniques Included:

- Operating System Detection (-O): Attempts to identify the OS of the target, providing insight into the system type and potential vulnerabilities.
- Service Version Detection (-sV): Determines the versions of services running on open ports, useful for vulnerability identification.
- Script Scanning (-sC): Runs a set of default Nmap Scripting Engine (NSE) scripts for vulnerability detection, like checking for misconfigurations or weak authentication.
- Traceroute: Maps the network route to the target, useful for identifying intermediary devices and understanding the network topology.

Why It’s Used: This scan is ideal for gathering a comprehensive view of a target in one command, especially during a deep assessment or when facing time constraints.

Information to Look For:

- Detailed service and version information.
- Operating system and network layout.
- Script output that highlights potential vulnerabilities.

SOC Relevance: Aggressive scans can be useful in a SOC for thorough security assessments or to identify detailed information during incident response. However, they should be used cautiously in a production environment as they generate a lot of noise and could trigger security alerts.

Summary

Each of these scans serves a distinct purpose for a SOC analyst:

- Host Discovery is used to identify the presence of assets and potential threats.
- Basic Port Scans reveal service exposure that could be exploited.
- Service Version Detection maps the services to specific vulnerabilities.
- Full TCP Scans ensure a complete understanding of the network’s attack surface.
- Aggressive Scans gather a holistic view of the system’s state, useful for detailed assessments or investigations.