Technical Cyber security Report

Analysis Using Metasploit for performing Network Scan On My IP Address Utilizing Nmap with the -Sc, -Sv, and -vv Options

By

Cyber Security Personnel : Victor Shedrack

Date : 4th of April, 2025.

Stakeholder: Lucy O. Raymond, PGD (Dublin), MSc (England), CDSA
Devrichard@vephlauni.com
Mentor Ibukun M. CompTIA Security+, CC ISC, CISSP.

REPORT OUTLINE

1. **Executive Summary**

    - **Brief overview of the entire report**
    - **Key findings and recommendations**

2. **Background and purpose**

    - **Scope/aim & Objectives of the report**
    - **Objectives of tools used (Nmap, Metasploit)**

3. **Methodology**

    - **Step-by-step process followed**
    - **Command-line options used (-sC -sV -vv, etc.)**
    - **Tools configuration and execution**

4. **Findings and Analysis**

    - **Behavioral Analysis**
    - **Observations during scanning**
    - **Risk and Impact Assessment**
    - **Potential impacts on systems or networks**

5. **Recommendations**

    - **Immediate Remediation Actions**
    - **Mitigation Strategies**

6. **Conclusion**
    - **Summary of findings**

1. Executive Summary

- **Overview:**

  The analysis conducted on Metasploit expresses the role and how it is used in the penetration testing framework aiding cybersecurity professionals in identifying, validating, and exploiting vulnerabilities in networks and systems. While primarily known for its exploitation capabilities, Metasploit also integrates tools like Nmap for reconnaissance and information gathering key early phases of a penetration test or vulnerability assessment. In this context, Metasploit was employed to perform a network scan on my IP address by utilizing the Nmap scanning engine within its environment. The scan was initiated with specific Nmap options:

  -Sc: Runs a set of default scripts, useful for detecting common services and vulnerabilities.

  -Sv: Attempts to determine service versions on open ports.

  -vv: Enables very verbose output, providing detailed feedback on the scanning process and results.

Within Metasploit, the scanning is done using the **db_nmap command**, it integrates Nmap results directly into Metasploit's database, allowing further exploitation planning based on the findings.

The integration of Nmap within Metasploit streamlines the transition from reconnaissance to exploitation, making the toolset especially effective for structured offensive security assessments.

- **Key Findings:**
  Key Findings from Metasploit Nmap Scan (-sC -sV -vv) on Target IP:
  1. No Open Ports Identified
  2. Service and Version Detection: Using the -sV flag, service versions were accounted for.
  3. Default Script Results (-sC): The default Nmap scripts provided additional details
  4. Detailed Verbose Output (-vv): The scan produced highly detailed feedback, allowing for deeper insight into how Nmap interpreted the responses, which improves confidence in the results and helps plan the next steps.
  5. Data Imported into Metasploit: Results were stored in Metasploit's database, enabling streamlined pivoting to exploitation or vulnerability validation using Metasploit modules.
  6. No potential Vulnerabilities Highlighted: Based on version detection and default scripts on the target IP Address no potential vulnerabilities or misconfigurations were flagged. These findings form the foundation for planning targeted exploitation

attempts, reporting risks to stakeholders, or taking remediation actions.

---

2. Background and Objectives

- **Project Context:**
  The aim of this project was to gather detailed intelligence on my IP address, a crucial step in vulnerability assessment or penetration testing. By using Nmap through Metasploit with the specified flags, i aimed to:
    - Identify open ports and running services on the target.
    - Determine service versions to match with known vulnerabilities.
    - Run default scripts to detect possible misconfigurations or vulnerabilities.
    - Collect rich output for thorough analysis and later use in exploitation or reporting.

- **Objective of the Tool Use:** The objective of Metasploit with Nmap is to identify and analyze vulnerabilities in a target system(IP Address) by scanning for open ports, services, and their versions. This particular process helps in gathering critical information during the reconnaissance phase of a penetration test. The integration streamlines scanning and exploitation, allowing security professionals to efficiently assess risks and prepare for targeted attacks or remediation.

---

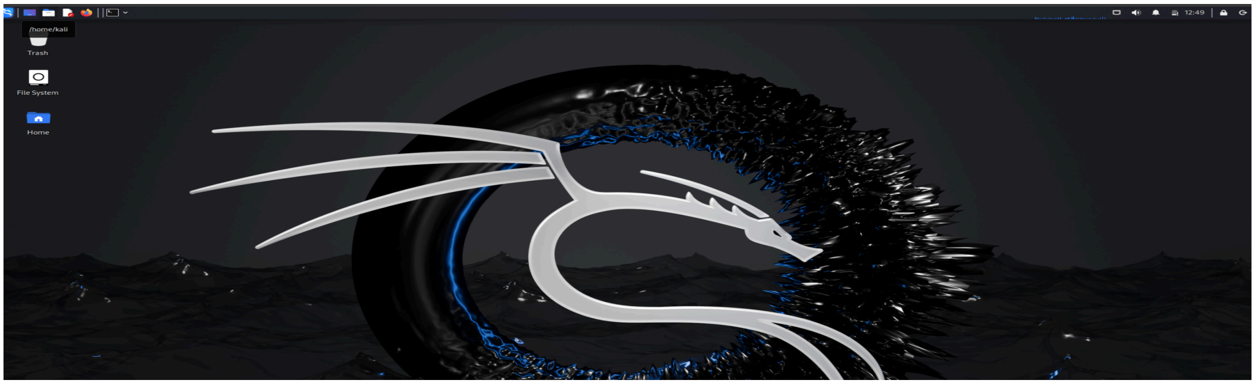
3. Methodology

3.1 Tool Configuration

- **Metasploit with Nmap Configuration:**

  1. Operating System Selection:

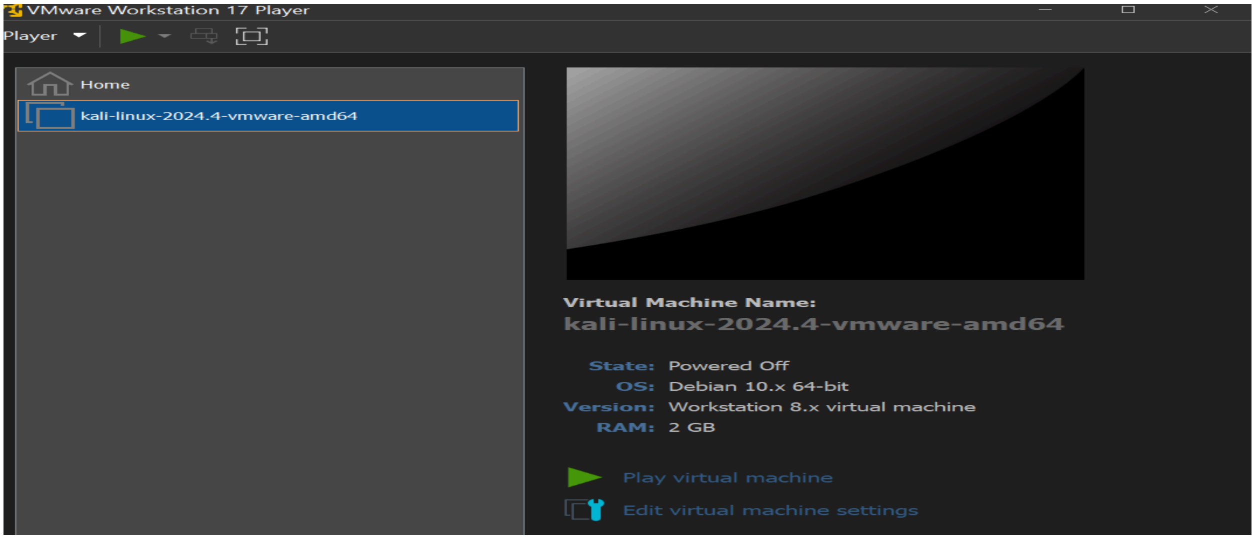
    - **Preferred OS: Kali Linux** – comes pre-installed with Metasploit, Nmap, and other penetration testing tools.



2. Environment Configuration:

System Requirements:

- **Minimum:** 2 CPU cores, 4GB RAM, 20GB disk
- **Recommended:** 4+ CPU cores, 8GB+ RAM
- **Virtualization:** VMware
- Run Metasploit inside a virtual machine (VM) to ensure isolation from the host system.
- **Set up host-only or bridged networking depending on test goals:**
    1. **Host-only:** Safe internal testing
    2. **Bridged:** Simulates real-world network scenarios
    3. **Snapshots:** Take VM snapshots before testing to easily revert if needed.


VMware Workstation 17 Player
Player
Home
kali-linux-2024.4-vmware-amd64
Play virtual machine
Edit virtual machine settings

Virtual Machine Name:
kali-linux-2024.4-vmware-amd64

State: Powered Off
OS: Debian 10.x 64-bit
Version: Workstation 8.x virtual machine
RAM: 2 GB

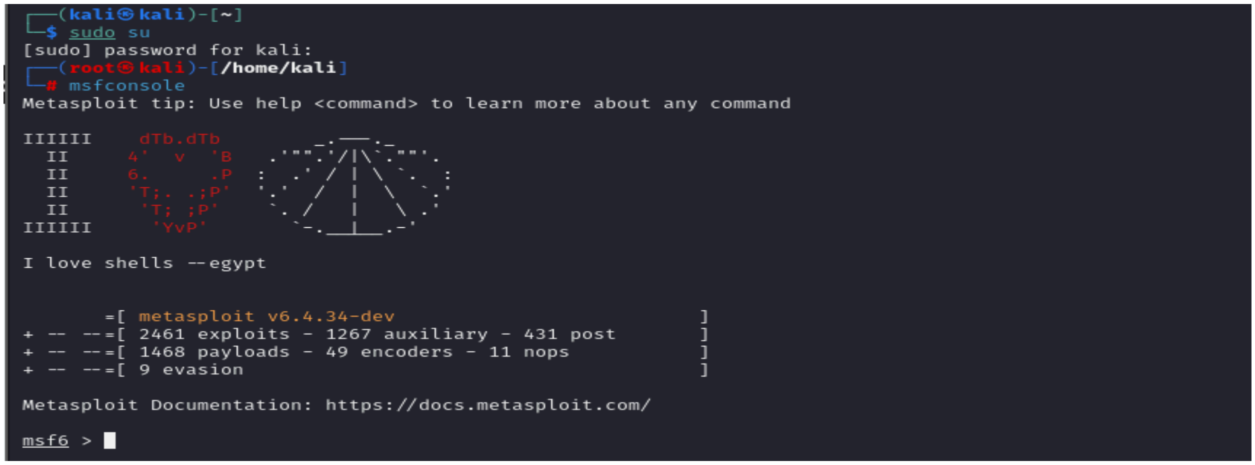
3. Network Monitoring Settings:

- Enable promiscuous mode on VM NIC (if monitoring is required).

- Tools like Wireshark can be run alongside Metasploit to observe traffic during scanning and exploitation.
- Configure firewalls/IDS rules if testing detection/response.

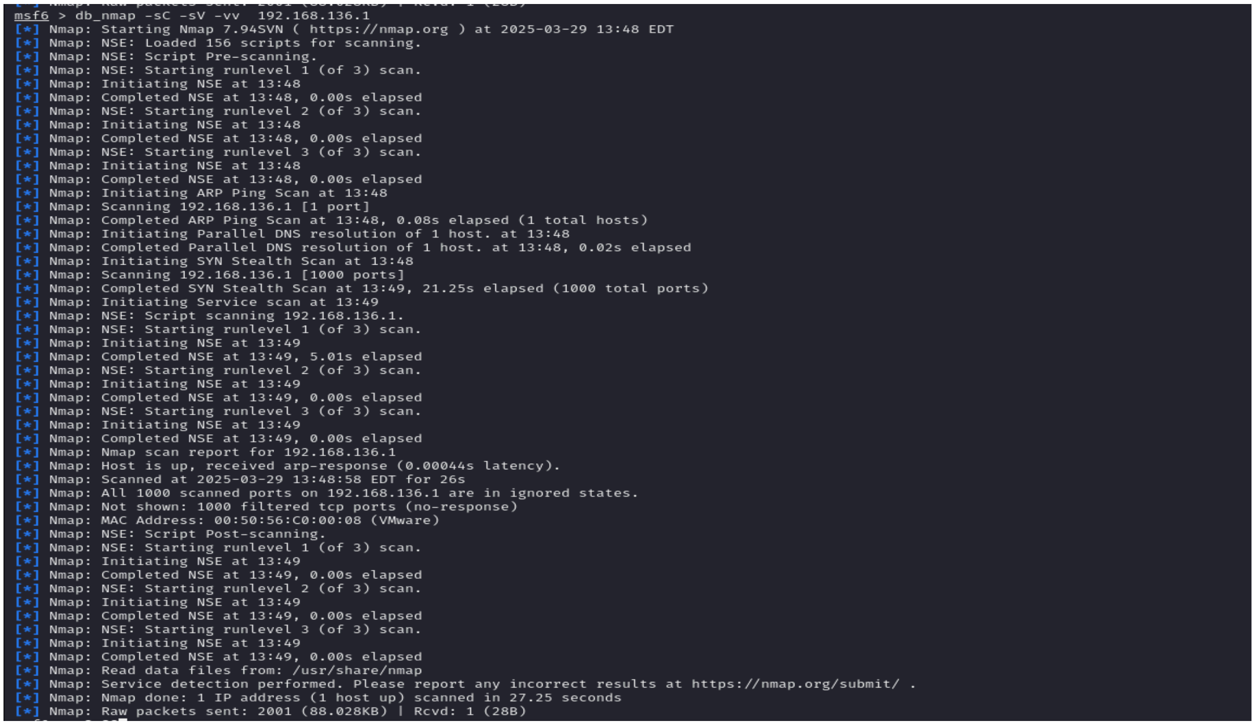
4. Metasploit Configuration:

- **Start Framework: msfconsole**
- **Set up Workspace:**
    - **workspace scan_project**



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Use help <command> to learn more about any command

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1468 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```

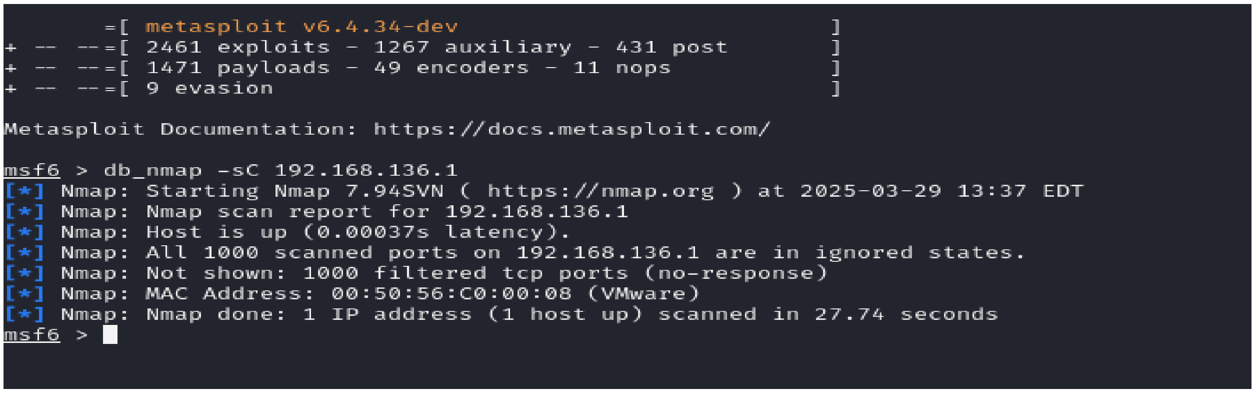
- **Run Nmap Scan from Within Metasploit: db_nmap -sC -sV -vv [192.168.136.1]**



```
[*] Nmap: Raw packets sent: 2001 (88.028KB) | Rcvd: 1 (28B)
msf6 > db_nmap -sC -sV -vv  192.168.136.1
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-29 13:48 EDT
[*] Nmap: NSE: Loaded 156 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: NSE: Starting runlevel 1 (of 3) scan.
[*] Nmap: Initiating NSE at 13:48
[*] Nmap: Completed NSE at 13:48, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 2 (of 3) scan.
[*] Nmap: Initiating NSE at 13:48
[*] Nmap: Completed NSE at 13:48, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 3 (of 3) scan.
[*] Nmap: Initiating NSE at 13:48
[*] Nmap: Completed NSE at 13:48, 0.00s elapsed
[*] Nmap: Initiating ARP Ping Scan at 13:48
[*] Nmap: Scanning 192.168.136.1 [1 port]
[*] Nmap: Completed ARP Ping Scan at 13:48, 0.08s elapsed (1 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 13:48
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 13:48, 0.02s elapsed
[*] Nmap: Initiating SYN Stealth Scan at 13:48
[*] Nmap: Scanning 192.168.136.1 [1000 ports]
[*] Nmap: Completed SYN Stealth Scan at 13:49, 21.25s elapsed (1000 total ports)
[*] Nmap: Initiating Service scan at 13:49
[*] Nmap: NSE: Script scanning 192.168.136.1.
[*] Nmap: NSE: Starting runlevel 1 (of 3) scan.
[*] Nmap: Initiating NSE at 13:49
[*] Nmap: Completed NSE at 13:49, 5.01s elapsed
[*] Nmap: NSE: Starting runlevel 2 (of 3) scan.
[*] Nmap: Initiating NSE at 13:49
[*] Nmap: Completed NSE at 13:49, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 3 (of 3) scan.
[*] Nmap: Initiating NSE at 13:49
[*] Nmap: Completed NSE at 13:49, 0.00s elapsed
[*] Nmap: Nmap scan report for 192.168.136.1
[*] Nmap: Host is up, received arp-response (0.00044s latency).
[*] Nmap: Scanned at 2025-03-29 13:48:58 EDT for 26s
[*] Nmap: All 1000 scanned ports on 192.168.136.1 are in ignored states.
[*] Nmap: Not shown: 1000 filtered tcp ports (no-response)
[*] Nmap: MAC Address: 00:50:56:C0:00:08 (VMware)
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: NSE: Starting runlevel 1 (of 3) scan.
[*] Nmap: Initiating NSE at 13:49
[*] Nmap: Completed NSE at 13:49, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 2 (of 3) scan.
[*] Nmap: Initiating NSE at 13:49
[*] Nmap: Completed NSE at 13:49, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 3 (of 3) scan.
[*] Nmap: Initiating NSE at 13:49
[*] Nmap: Completed NSE at 13:49, 0.00s elapsed
[*] Nmap: Read data files from: /usr/share/nmap
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 27.25 seconds
[*] Nmap: Raw packets sent: 2001 (88.028KB) | Rcvd: 1 (28B)
```

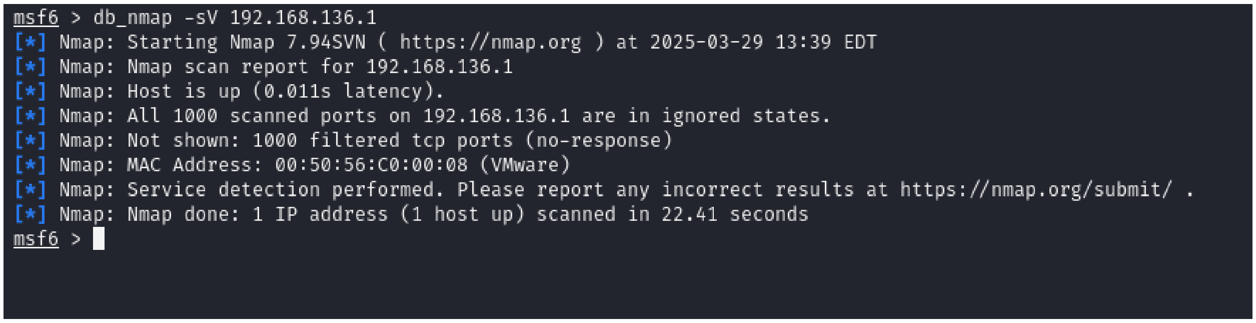
- **Parameters Explained:**

-sC: Runs Nmap's default scripts for vulnerability checks



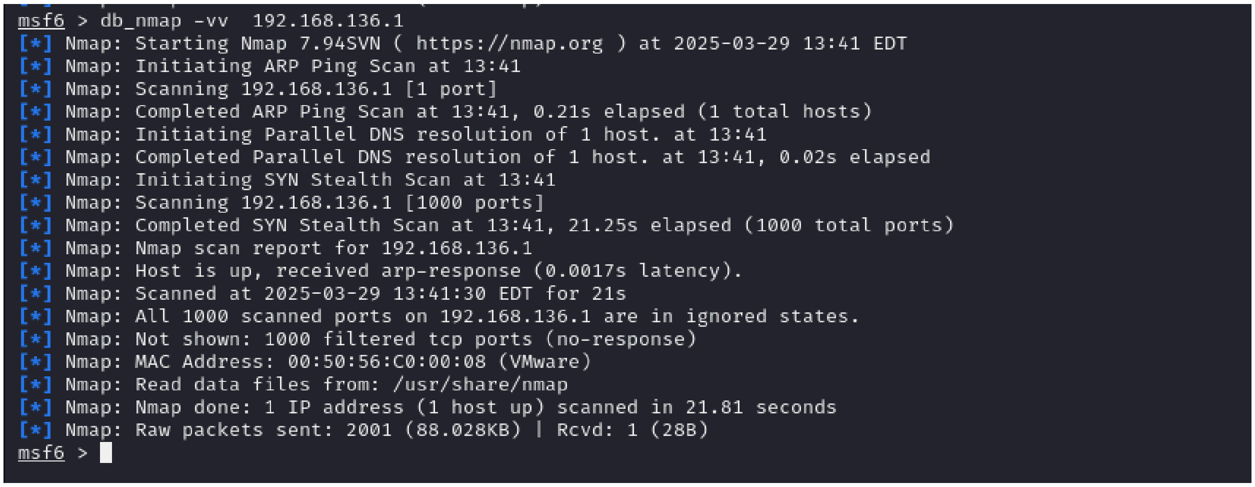
```
       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > db_nmap -sC 192.168.136.1
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-29 13:37 EDT
[*] Nmap: Nmap scan report for 192.168.136.1
[*] Nmap: Host is up (0.00037s latency).
[*] Nmap: All 1000 scanned ports on 192.168.136.1 are in ignored states.
[*] Nmap: Not shown: 1000 filtered tcp ports (no-response)
[*] Nmap: MAC Address: 00:50:56:C0:00:08 (VMware)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 27.74 seconds
msf6 > 
```

-sV: Detects service versions



```
msf6 > db_nmap -sV 192.168.136.1
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-29 13:39 EDT
[*] Nmap: Nmap scan report for 192.168.136.1
[*] Nmap: Host is up (0.011s latency).
[*] Nmap: All 1000 scanned ports on 192.168.136.1 are in ignored states.
[*] Nmap: Not shown: 1000 filtered tcp ports (no-response)
[*] Nmap: MAC Address: 00:50:56:C0:00:08 (VMware)
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 22.41 seconds
msf6 > 
```

-vv: Enables very verbose output for detailed feedback



```
msf6 > db_nmap -vv  192.168.136.1
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-29 13:41 EDT
[*] Nmap: Initiating ARP Ping Scan at 13:41
[*] Nmap: Scanning 192.168.136.1 [1 port]
[*] Nmap: Completed ARP Ping Scan at 13:41, 0.21s elapsed (1 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 13:41
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 13:41, 0.02s elapsed
[*] Nmap: Initiating SYN Stealth Scan at 13:41
[*] Nmap: Scanning 192.168.136.1 [1000 ports]
[*] Nmap: Completed SYN Stealth Scan at 13:41, 21.25s elapsed (1000 total ports)
[*] Nmap: Nmap scan report for 192.168.136.1
[*] Nmap: Host is up, received arp-response (0.0017s latency).
[*] Nmap: Scanned at 2025-03-29 13:41:30 EDT for 21s
[*] Nmap: All 1000 scanned ports on 192.168.136.1 are in ignored states.
[*] Nmap: Not shown: 1000 filtered tcp ports (no-response)
[*] Nmap: MAC Address: 00:50:56:C0:00:08 (VMware)
[*] Nmap: Read data files from: /usr/share/nmap
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 21.81 seconds
[*] Nmap: Raw packets sent: 2001 (88.028KB) | Rcvd: 1 (28B)
msf6 > 
```

5. Logging and Output Storage:

- **Metasploit automatically logs scan results:**
- **View with: hosts, services, vulns**
- **Export logs as needed for reports or further analysis.**

Summary: The tool configuration includes setting up Metasploit on a Linux-based VM (e.g., Kali), isolating the environment using virtualization, enabling network monitoring, and running detailed scans using db_nmap. This setup ensures safe, organized, and effective vulnerability analysis and penetration testing.

3.2 Execution Process

- Upon execution, there was no malicious file, because the analysis carried out using Metasploit automatically log scans the targeted IP address, aiming on Identify open ports and running services on the target and also to determine service versions to match with known vulnerabilities.

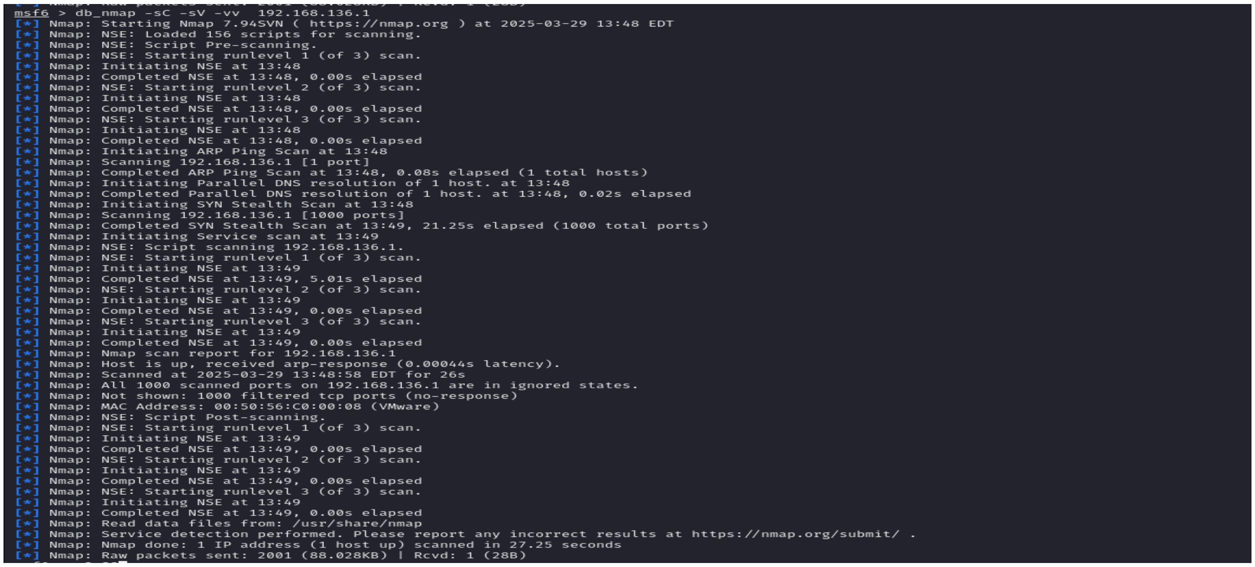
3.3 Monitoring and Analysis:

- **System Monitoring:** Metasploit uses Meterpreter for post-exploitation to capture system activity
    - File system: Browse, upload/download, delete files(manual logging with spool).
    - Network: View active connections (netstat), sniff traffic (sniffer).
    - Registry (Windows): Read/modify registry with reg commands.
    - Logging: Use spool or enable database (msfdb) to auto-log sessions, credentials, and loot.

      It's not a passive monitor but effective for manual or scripted activity tracking during exploitation.

- **Network Monitoring:**
  The workspace was connected to a known network server (Ethernet connection, "wired connection 1 active", which was shown by the tool's integrated threat intelligence feed.

4. Findings and Analysis



```
msf6 > db_nmap -sC -sV -vv  192.168.136.1
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-29 13:48 EDT
[*] Nmap: NSE: Loaded 156 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: NSE: Starting runlevel 1 (of 3) scan.
[*] Nmap: Initiating NSE at 13:48
[*] Nmap: Completed NSE at 13:48, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 2 (of 3) scan.
[*] Nmap: Initiating NSE at 13:48
[*] Nmap: Completed NSE at 13:48, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 3 (of 3) scan.
[*] Nmap: Initiating NSE at 13:48
[*] Nmap: Completed NSE at 13:48, 0.00s elapsed
[*] Nmap: Initiating ARP Ping Scan at 13:48
[*] Nmap: Scanning 192.168.136.1 [1 port]
[*] Nmap: Completed ARP Ping Scan at 13:48, 0.08s elapsed (1 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 13:48
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 13:48, 0.02s elapsed
[*] Nmap: Initiating SYN Stealth Scan at 13:48
[*] Nmap: Scanning 192.168.136.1 [1000 ports]
[*] Nmap: Completed SYN Stealth Scan at 13:49, 21.25s elapsed (1000 total ports)
[*] Nmap: Initiating Service scan at 13:49
[*] Nmap: NSE: Script scanning 192.168.136.1.
[*] Nmap: NSE: Starting runlevel 1 (of 3) scan.
[*] Nmap: Initiating NSE at 13:49
[*] Nmap: Completed NSE at 13:49, 5.01s elapsed
[*] Nmap: NSE: Starting runlevel 2 (of 3) scan.
[*] Nmap: Initiating NSE at 13:49
[*] Nmap: Completed NSE at 13:49, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 3 (of 3) scan.
[*] Nmap: Initiating NSE at 13:49
[*] Nmap: Completed NSE at 13:49, 0.00s elapsed
[*] Nmap: Nmap scan report for 192.168.136.1
[*] Nmap: Host is up, received arp-response (0.00044s latency).
[*] Nmap: Scanned at 2025-03-29 13:48:58 EDT for 26s
[*] Nmap: All 1000 scanned ports on 192.168.136.1 are in ignored states.
[*] Nmap: Not shown: 1000 filtered tcp ports (no-response)
[*] Nmap: MAC Address: 00:50:56:C0:00:08 (VMware)
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: NSE: Starting runlevel 1 (of 3) scan.
[*] Nmap: Initiating NSE at 13:49
[*] Nmap: Completed NSE at 13:49, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 2 (of 3) scan.
[*] Nmap: Initiating NSE at 13:49
[*] Nmap: Completed NSE at 13:49, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 3 (of 3) scan.
[*] Nmap: Initiating NSE at 13:49
[*] Nmap: Completed NSE at 13:49, 0.00s elapsed
[*] Nmap: Read data files from: /usr/share/nmap
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 27.25 seconds
[*] Nmap: Raw packets sent: 2001 (88.028KB) | Rcvd: 1 (28B)
```

4.1 Observation during scanning:

- **Service and Script Behavior:**
    - All services versions detection performed
    - 156 Scripts was loaded for scanning
    - All 1000 scanned ports are in ignored states
    - There was no exposed service

4.2 Behavioral Analysis:

- **Host Behavior**
    - The host responds to NSE Scripts
    - There was no unusual banner outputs (e.g., “Unauthorized access”)

4.3 Risk and Impact Assessment:

- **Potential Impact:**
  Finding vulnerabilities in networks requires the use of tools like Nmap and Metasploit, however inappropriate or unauthorised use can result in ethical issues, service interruptions, and legal repercussions.

5. Recommendations

- Always get authorization
- Target specific IP and ports
- **Monitor network and system behavior using tools like Wireshark or Splunk to track and analyze scan effects in real-time.**

5.1 Immediate Remediation Actions:

- Stop the scan immediately; Terminate the Nmap or Metasploit process if it's still running
- Alert IT/security team and management if the scan was unapproved or impacted the systems
- Provide details: time, IP scanned, command used and potential effects.
- Port Hardening: Maintain strict firewall rules for ports 445 and 8080.

5.2 Mitigation:

- Perform scans in a controlled or test environment
- Use non-intrusive scanning techniques
- Monitor and analyze scan results

6. Conclusion

- **Summary of Findings:** At the end of this analysis involving the use of Metasploit to scan a target IP address by utilizing Nmap using the -Sc, -Sv and -vv Options, The aim which was to gather detailed intelligence on my IP address, a crucial step in vulnerability assessment or penetration testing was achieved through an automatic log scan by Identifying open ports and running services on the target, service versions to match with known vulnerabilities was determined and also running default scripts to detect possible misconfigurations or vulnerabilities.