Project Report

Vulnerability Assessment on Windows 10 VM

1. Environment Setup

- **Host Machine:** [Your Host OS]
- **Virtual Machines:**
  - **Windows 10 VM (Target)**
  - **Kali Linux VM (Attacker)**

2. Tools Used

Tool	Purpose
Nmap	Network scanning & port discovery
Nikto	Web server vulnerability scanning
Nuclei	Automated vulnerability scanning & templating
Metasploit	Exploit development & verification

3. Assessment Process

1. **Network Discovery & Port Scanning: Nmap**

   - Used **Nmap** to scan Windows VM IP for open ports and services:

   Command:

   nmap -sS -sV -sC -O -p- <window_ip>

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-23 07:24 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid se
Stats: 0:02:45 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 94.12% done; ETC: 07:27 (0:00:08 remaining)
Nmap scan report for [redacted]
Host is up (0.0011s latency).
Not shown: 65518 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-title: IIS Windows
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Windows 10 Pro 19045 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: [redacted]
| Not valid before: 2025-05-08T14:19:18
|_Not valid after:  2025-11-07T14:19:18
| rdp-ntlm-info:
```

Identified running services and OS details.

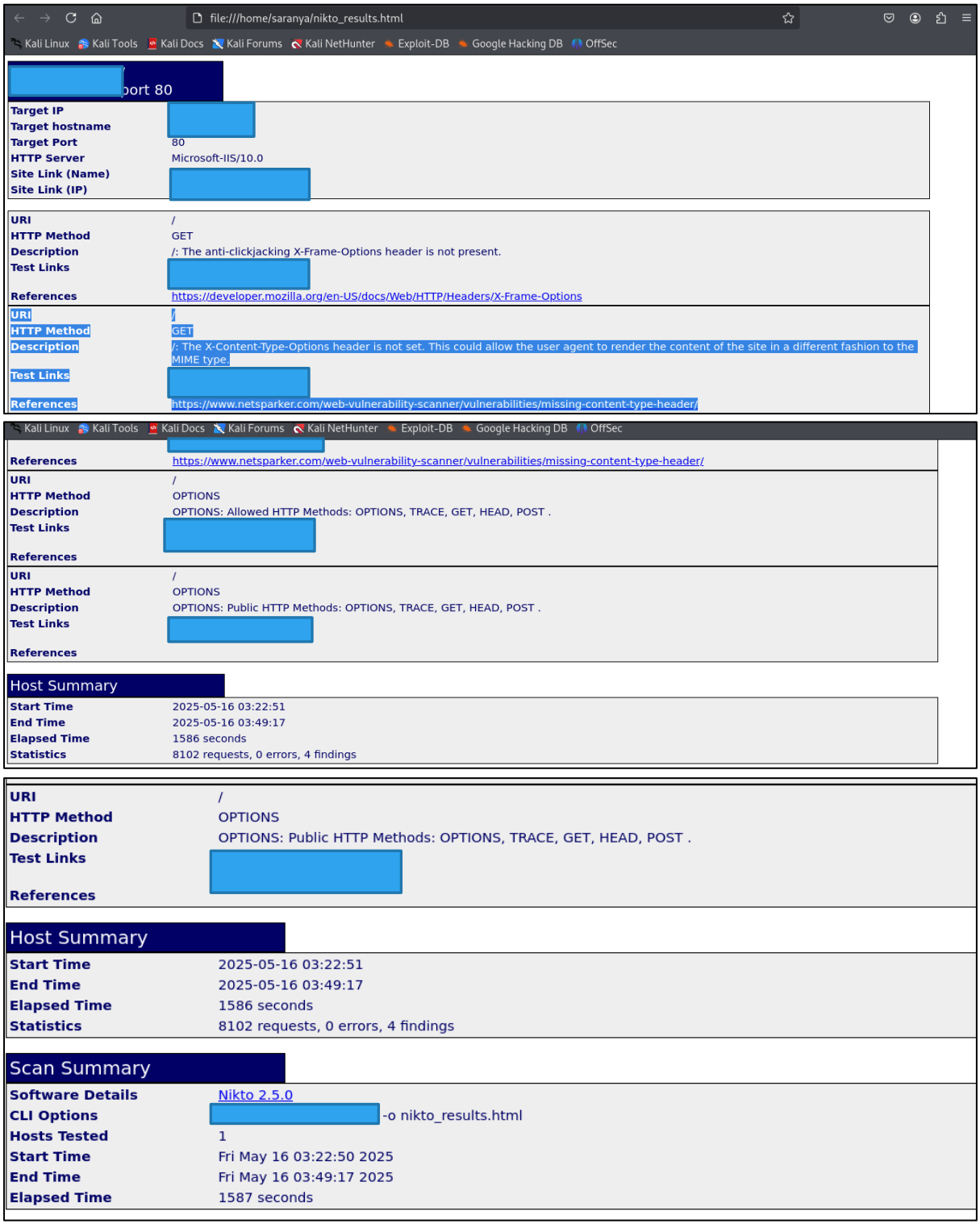
2.Web Server Vulnerability Scan: Nikto

- Ran **Nikto** against Windows VM's web services to detect common vulnerabilities:

Command:

nikto -h <http://<Windows-IP>

```
nikto -h http://[redacted] -o nikto_results.html
```



file:///home/saranya/nikto_results.html

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

[redacted]ort 80

Target IP	[redacted]
Target hostname	
Target Port	80
HTTP Server	Microsoft-IIS/10.0
Site Link (Name)	[redacted]
Site Link (IP)	

URI	/
HTTP Method	GET
Description	/: The anti-clickjacking X-Frame-Options header is not present.
Test Links	[redacted]
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

URI	/
HTTP Method	GET
Description	/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
Test Links	[redacted]
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

References	[redacted]

URI	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
HTTP Method	/
Description	OPTIONS
Test Links	OPTIONS: Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
References	[redacted]

URI	/
HTTP Method	OPTIONS
Description	OPTIONS: Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
Test Links	[redacted]
References	

Host Summary

Start Time	2025-05-16 03:22:51
End Time	2025-05-16 03:49:17
Elapsed Time	1586 seconds
Statistics	8102 requests, 0 errors, 4 findings

URI	/
HTTP Method	OPTIONS
Description	OPTIONS: Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
Test Links	[redacted]
References	

Host Summary

Start Time	2025-05-16 03:22:51
End Time	2025-05-16 03:49:17
Elapsed Time	1586 seconds
Statistics	8102 requests, 0 errors, 4 findings

Scan Summary

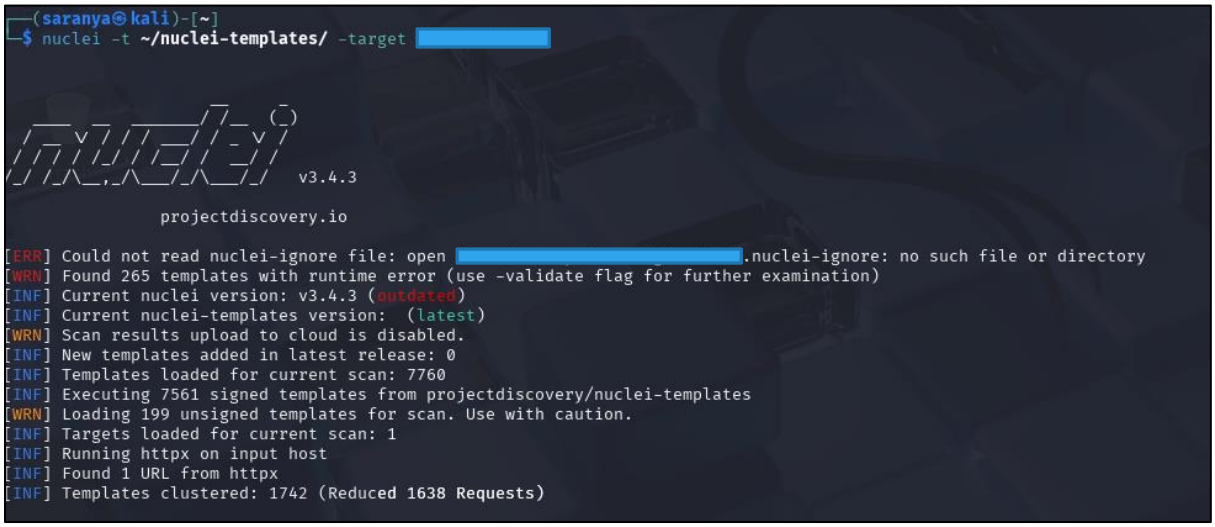
Software Details	Nikto 2.5.0
CLI Options	[redacted] -o nikto_results.html
Hosts Tested	1
Start Time	Fri May 16 03:22:50 2025
End Time	Fri May 16 03:49:17 2025
Elapsed Time	1587 seconds

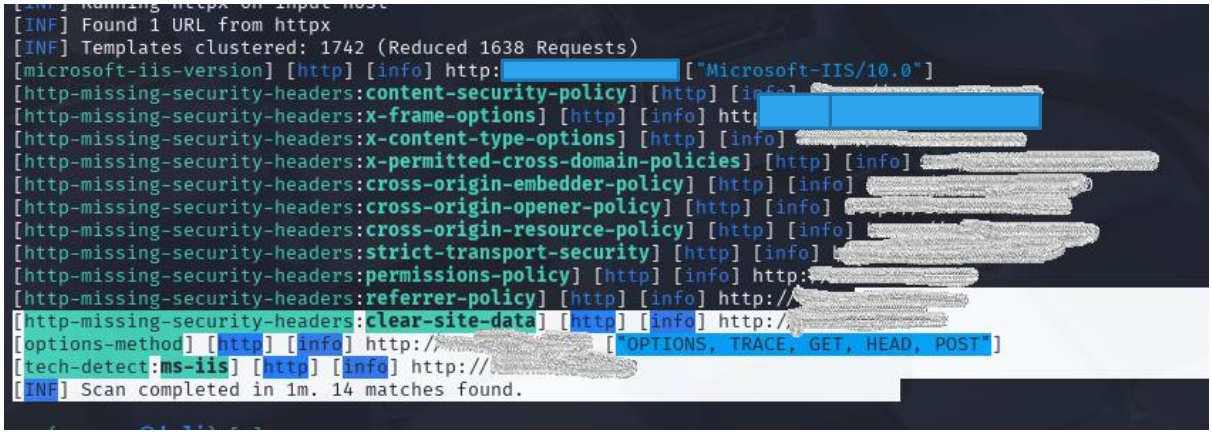
3. Automated Vulnerability Scanning: Nuclei

- Used **Nuclei** templates to detect known CVEs and misconfigurations:

  Command:

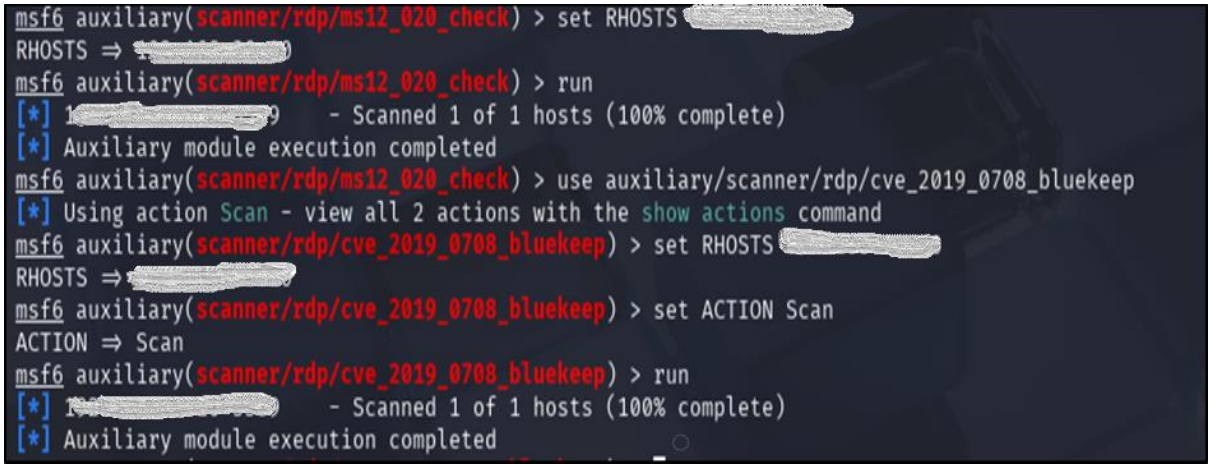
  nuclei -u http://<Windows-IP> -t /path/to/templates/





4. Exploit Verification: Metasploit

- Leveraged **Metasploit Framework** to verify select vulnerabilities by attempting controlled exploits.



4. Findings

- List discovered open ports and vulnerable services.
- Highlight any critical security misconfigurations or outdated software versions.
- Include notes on successful or attempted exploit validations.

5. Skills Developed

- Network reconnaissance and port enumeration
- Vulnerability identification and assessment
- Reporting and documenting security risks
- Using automated and manual scanning tools

6. Summary

This project involved performing a comprehensive vulnerability assessment of a Windows 10 virtual machine in a controlled lab environment using Kali Linux as the attacker platform. The objective was to identify potential security weaknesses, misconfigurations, and exposed services through both automated and manual scanning techniques.

Key tools included **Nmap** for network and service enumeration, **Nikto** for web server vulnerability scanning, **Nuclei** for automated detection of known CVEs and misconfigurations,

and **Metasploit** for verification of vulnerabilities through controlled exploitation. The process provided valuable insights into real-world attack vectors and the importance of proactive system hardening.

The assessment revealed several open ports and services on the Windows machine, including outdated software components and potential misconfigurations. Findings were documented with severity levels and recommended remediation steps to enhance system security.

This project demonstrates practical experience in offensive security techniques and a strong understanding of network-level vulnerability detection and analysis. It reinforces the importance of continuous monitoring and vulnerability management in maintaining a secure system environment