Penetration Test Report
Zuel's Zesty Zephyrs

Prepared By: Josh Lieberg

1.0 Executive Summary

1.1 Overview

Zuel's Zesty Zephyrs engaged Apex Cyber Solutions to conduct a penetration test against their environment. The test was to be conducted to provide a comprehensive overview of the security controls within the environment. In addition, the environment could be probed to uncover the susceptibility to exploitation and data breaches. This test was performed in accordance with Apex Cyber Solutions Penetration Testing Methodology. Additionally, all testing was performed with the IT staff at Zuel's Zesty Zephyrs to ensure nothing was destroyed or tampered with during the duration of the test.

This penetration test was conducted to assess the security posture of three target systems: `44.106.251.44`, `44.106.251.64`, and `44.106.251.34`. he main goal was to discover the vulnerabilities, assess the risk and provide tactical remediation plans to enhance the security posture of these systems. This report presents the results of the analysis, risks, and practical suggestions for the prevention of cyber threats.

1.2 High Level Findings

The penetration test resulted in the discovery of alarming security vulnerabilities that pose large amounts of risk to Zuel's Zesty Zephyrs infrastructure. Firstly it was discovered that `44.106.251.64` and `44.106.251.34` pose the most critical vulnerabilities that require immediate remediation.

Server Message Block (SMB) Signing was disabled on `44.106.251.64` which exposes it to relay attacks. This would allow threat actors to gain unauthorized access to the system and pose as authorized users. Additionally, Windows Remote Management (WinRM) was accessible. This poses the same risk as the disabled SMB Signing because user credentials can be compromised or falsified. Another minor issue that was discovered was that Remote Desktop Protocol (RDP) has the potential to be compromised if exposed to a credential based attack. This is due to the brute force vulnerability that is present on RDP.

On `44.106.251.34` it was discovered that it was running an outdated version of Apache with the version number being 2.4.51. This version is vulnerable to Remote Code Execution (RCE). This is extremely alarming as potential threat actors could remotely run commands on the machine and cause the system to malfunction and potentially seize control.

No critical vulnerabilities were found on `44.106.251.44`. When doing tests on this machine, it was discovered that web services, database configurations, and API access were configured in

compliance with Apex Cyber Solutions Penetration Testing Methodology. Although immediate threats were not discovered on this machine, it does not mean that it is fully safeguarded. The machine shall still be updated regularly to have current security updates and be monitored for any suspicious activity.

1.3 Overall Risk Rating

Zuel's Zesty Zephyrs **Risk Assessment**		**PROBABILITY**				
		Very High	High	Medium	Low	Very Low
IMPACT	Very High	Very High	Very High	Very High	High	High
	High	Very High	High	High	Medium	Medium
	Medium	High	High	Medium	Medium	Low
	Low	High	Medium	Medium	Low	Very Low
	Very Low	Medium	Low	Low	Very Low	Very Low

Figure 1: Apex Cyber Solutions Risk Matrix

Using the Apex Cyber Solutions Risk Matrix, it was determined that 44.106.251.44 is at Very High Risk, 44.106.251.34 is at High Risk, and 44.106.251.44 is at Very Low Risk. Given that two out of the three systems fall into the Very High/High Risk category, the overall rating for Zuel's Zesty Zephyrs is classified as High Risk.

1.4 Recommendations

Based on the results discovered during the test, Apex Cyber Solutions makes the following recommendations (presented by order of priority):

- `44.106.251.64`
  - Enable SMB Signing to Prevent SMB Relay Attacks
  - Restrict WinRM Access to Authenticated IPs in the Environment
  - Secure RDP with Multi Factor Authentication (MFA) and Disable Network Level Authentication (NLA) Bypass
  - Restrict Public Access to MySQL and Only Trust Authenticated IPs
  - Deploy Intrusion Detection System (IDS)
  - Disable All Unused and Open Ports
  - Implement MFA for all users regardless of rank

    - Implement Strong Password Policies
    - Deploy a Security Information and Event Management (SIEM) Solution
- `44.106.251.34`
    - Upgrade Apache to a Newer Version (2.4.57 or higher) to Root Out
    - Disable Access to the Zeus Access Panel (Port 9090)
    - Implement Web Application Firewalls (WAF)
    - Secure Directory Permissions
    - Implement MFA for all users regardless of rank
    - Implement Strong Password Policies
    - Deploy a SIEM Solution
- `44.106.251.44`
    - Implement MFA for all users regardless of rank
    - Implement Strong Password Policies
    - Keep OS and Services Up to Date
    - Implement SSH to Only Trusted IPs
    - Monitor Logs for Unusual Behavior
    - Deploy a SIEM Solution

2.0 Testing

2.1 Extent of Testing Methods

Apex Cyber Solutions conducted a penetration test against Zuel's Zesty Zephyrs identified target systems. This was done to assess the security of their environment and see if any fixes need to be made. The following testing methodologies were included in the scope:

- A network level penetration test was conducted against externally accessible hosts
  - `44.106.251.44`
  - `44.106.251.64`
  - `44.106.251.34`
- Service enumeration and vulnerability scanning to discover any potential exploits and possible vulnerabilities present in the environment
- Web application and API security testing to detect insecure authentication, outdated software, and exposed admin panels
- Brute force and password security testing on open services such as RDP, SMB, and WinRM to evaluate authentication strength.
- Port scanning and firewall analysis to assess exposed network services and potential attack vectors.
- Risk assessment and exploit feasibility testing to determine the likelihood of successful exploitation.

All testing activities were conducted within the approved scope and ethical guidelines, ensuring that no unauthorized actions or disruptions occurred.

3.0 Internal Assessment

3.1 Phase Summary

During the internal assessment phase, various reconnaissance and enumeration activities were conducted to determine the overall security of Zuel's Zesty Zephyrs infrastructure. Port and vulnerability scanning revealed critical security issues within the infrastructure. The most concerning vulnerabilities that were identified posed a risk of potential compromise of Zuel's Zesty Zephyrs infrastructure.

Among the most critical issues was the misconfiguration of SMxB Signing on Windows Server 2019, which left the system vulnerable to SMB relay attacks. Outdated software versions introduced a Remote Code Execution vulnerability, which could allow an attacker to execute arbitrary commands on the system.

Once initial access was obtained, directory traversal attacks were performed to locate sensitive data. It was discovered that unencrypted authentication credentials and potentially sensitive files were accessible, increasing the risk of data breaches. These findings suggest that Zuel's Zesty Zephyrs internal security controls require immediate repair to prevent unauthorized access of the infrastructure.

3.2 Port and Service Enumeration

This section details the open ports and running services discovered during the penetration test on each machine. Each service was analyzed for potential vulnerabilities, misconfigurations, and security risks.

Table 1: `44.106.251.64` Windows Server 2019 Ports and Services

Port	Service	Protocol	Risk Level	Description
21	FTP	TCP	High	File Transfer Protocol (FTP) is outdated and can be exploited if anonymous login is enabled.
80	HTTP	TCP	Medium	Web service running, potential for misconfigurations or outdated software.
135	MSRPC	TCP	High	Microsoft Remote Procedure Call, often targeted for remote code execution exploits.

139	NetBIOS-SSN	TCP	Medium	NetBIOS can be exploited to enumerate shared folders, usernames, and domain information, increasing the risk of lateral movement.
445	Microsoft-DS	TCP	High	SMB Signing is disabled, making it vulnerable to relay attacks. This could allow an attacker to intercept authentication attempts and gain unauthorized access.
1433	MS-SQL-S	TCP	High	Microsoft SQL Server is publicly accessible, increasing the risk of SQL injection attacks and unauthorized database access.
3306	MySQL	TCP	High	MySQL database, potential for SQL injection and unauthorized access if misconfigured.
3389	MS-WBT-SERVER	TCP	Medium	Remote Desktop Protocol is open, making it susceptible to brute force attacks if weak credentials are used.
5357	WSDAPI	TCP	Medium	Web Services for Devices API, may expose unnecessary services.
5985	WinRM	TCP	High	Windows Remote Management is exposed, allowing remote command execution if credentials are compromised.
33060	MySQLX	TCP	High	MySQL X Plugin service, which may expose an additional attack surface for database exploitation.
49688	Unknown	TCP	Medium	Unidentified service that requires further analysis in order to discover vulnerabilities

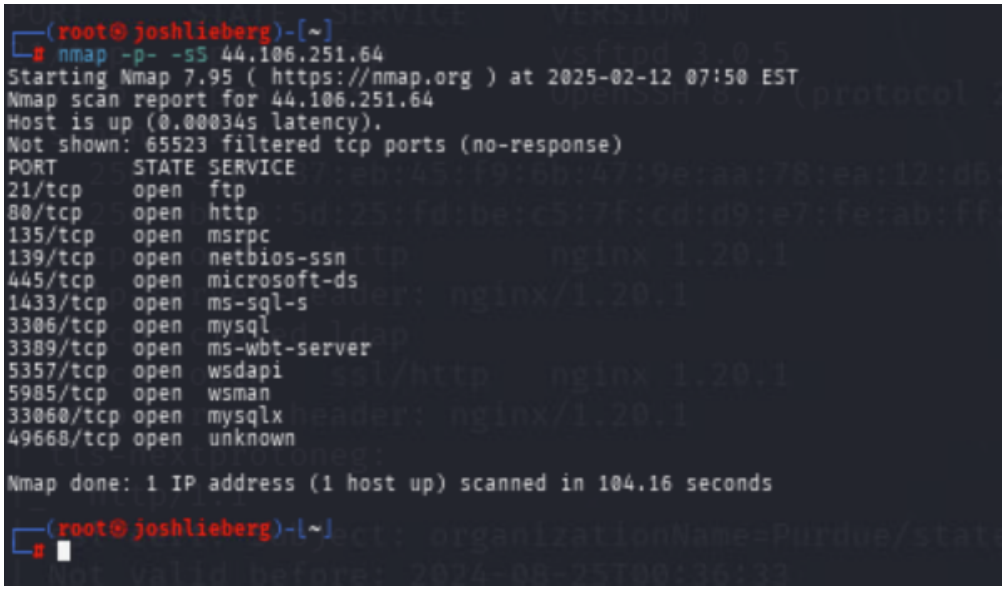

Figure 2: Open Ports and Services on `44.106.251.64` using `nmap -p- -sS 44.106.251.64`

Table 2: `44.106.251.34` Ubuntu Linux 20.04.1

Port	Service	Protocol	Risk Level	Description
21	FTP	TCP	High	File Transfer Protocol (FTP) is outdated and can be exploited if anonymous login is enabled.
22	SSH	TCP	Medium	Secure Shell (SSH) allows remote access; brute force attacks can be a concern if weak passwords are used.
53	DNS	TCP	Medium	ISC BIND is running; outdated versions may be susceptible to DNS cache poisoning or DoS attacks.
80	HTTP	TCP	High	Apache 2.4.41 is outdated and has known vulnerabilities
143	IMAP	TCP	Medium	Internet Message Access Protocol (IMAP) allows email retrieval; improper authentication can lead to account takeover
993	IMAPS	TCP	Low	IMAP over SSL/TLS, which encrypts traffic, but may be

				vulnerable if misconfigured.
2024	HTTP	TCP	Medium	Nginx 1.18.0 is outdated; potential for vulnerabilities depending on configuration
3128	HTTP Proxy	TCP	High	Squid Proxy may allow unauthorized access or proxy bypass vulnerabilities.
8080	Apache Tomcat	TCP	High	Apache Tomcat server is exposed and may allow RCE if improperly secured.
9090	Zeus Admin Panel	TCP	High	An exposed administrative interface, which, if compromised, can grant attackers full control of the system.

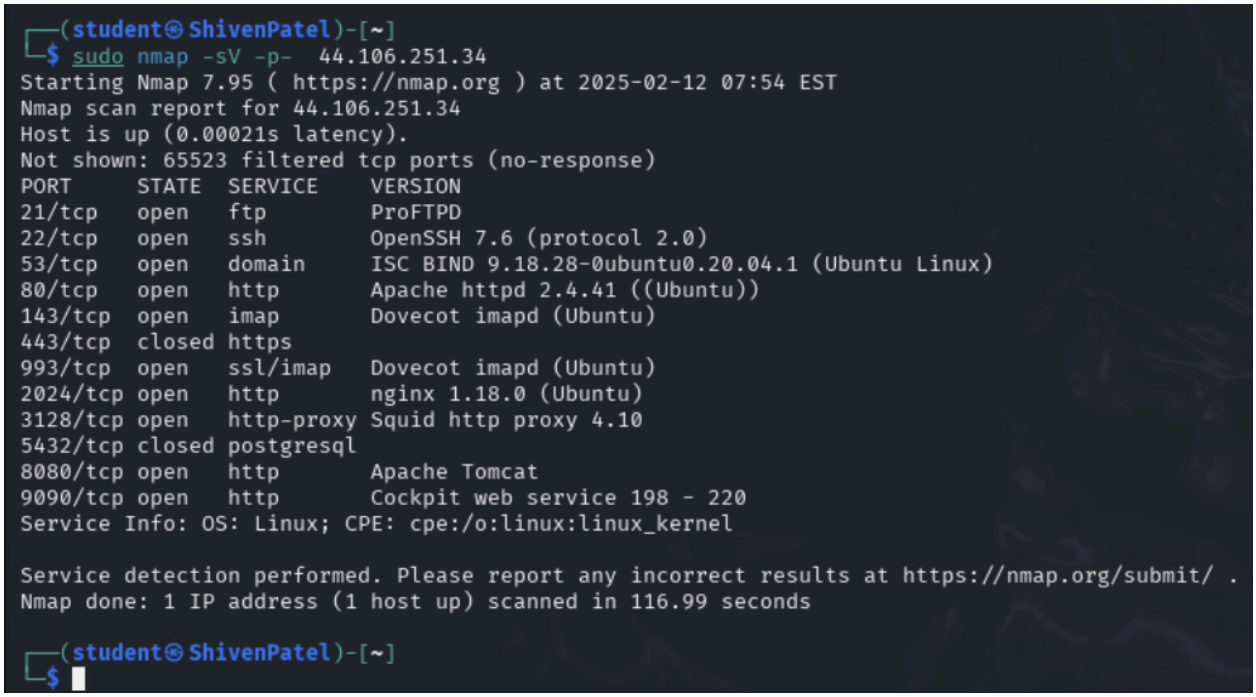

Figure 3: Open Ports and Services on `44.106.251.34` using `nmap -sV -p- 44.106.251.34`

Table 3: `44.106.251.44` CentOS 7

Port	Service	Protocol	Risk Level	Description
21	FTP	TCP	High	File Transfer Protocol (FTP) is outdated and can be exploited if anonymous login is enabled.
22	SSH	TCP	Medium	Secure Shell (SSH) allows remote access; brute-force attacks can be a concern if weak passwords are used.
80	Web Services	TCP	High	Web service running, potential for misconfigurations or outdated software.
443	HTTPS	TCP	Medium	Secure HTTP service, but certificate misconfigurations could pose risks.
3306	MySQL	TCP	High	MySQL database service exposed to the network, which could allow unauthorized database access if not properly secured.
5672	AMQP	TCP	Medium	Advanced Message Queuing Protocol used for message based services could allow message injection attacks if not secured.
8118	Privoxy	TCP	Medium	Proxy service that may allow traffic manipulation or interception if misconfigured.
9200	WAP-WSP	TCP	Medium	Web based access point service, potential for exposure if weak authentication is used
9300	VRACE	TCP	Medium	VRACE service requires further analysis to determine vulnerabilities.
11211	Memcached	TCP	High	Exposed Memcached service can be used in DDoS amplification attacks if accessible externally.
21363	Unknown	TCP	Medium	Unidentified service that requires

				further analysis in order to discover vulnerabilities

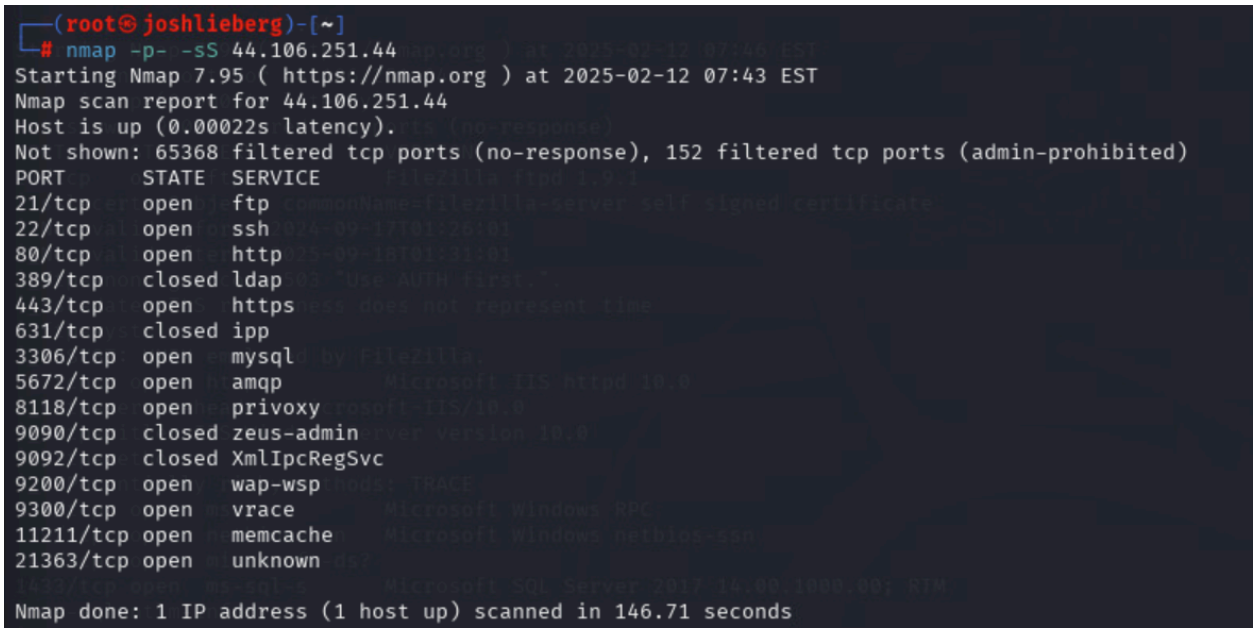

Figure 4: Open Ports and Services on `44.106.251.44` using `nmap -p- -sS- 44.106.251.34`

3.3 Detailed Findings - OS Discovery

As part of the penetration test, operating system detection was performed on each machine using Nmap and additional enumeration techniques. The objective was to identify the OS type, version number, and any associated vulnerabilities. The findings are documented below.

`44.106.251.64`

Operating System Details:

- Detected OS: Windows Server 2019
- OS Version: Build 17763 (Windows 10 / Server 2019)
- Kernel Information: NT 10.0
- Detection Method: `nmap -A 44.106.251.64`
    - Using the aggressive (`-A`) nmap scan, Windows Server 2019 was identified based on its open SMB, RDP, and WinRM services.

Figure 5: OS Detection Using `nmap -A 44.106.251.64`

`44.106.251.34`

Operating System Details:

- Detected OS: Ubuntu Linux
- OS Version: 20.04.1
- Kernel Information: Linux 5.8.0
- Detection Method: `nmap -A 44.106.251.34` & `curl -I http://44.106.251.34`
    - The Apache server header response confirmed that the machine was running Ubuntu 20.04.1
    - The Nmap OS detection scan identified Linux 5.x kernel, matching Ubuntu 20.04 LTS.

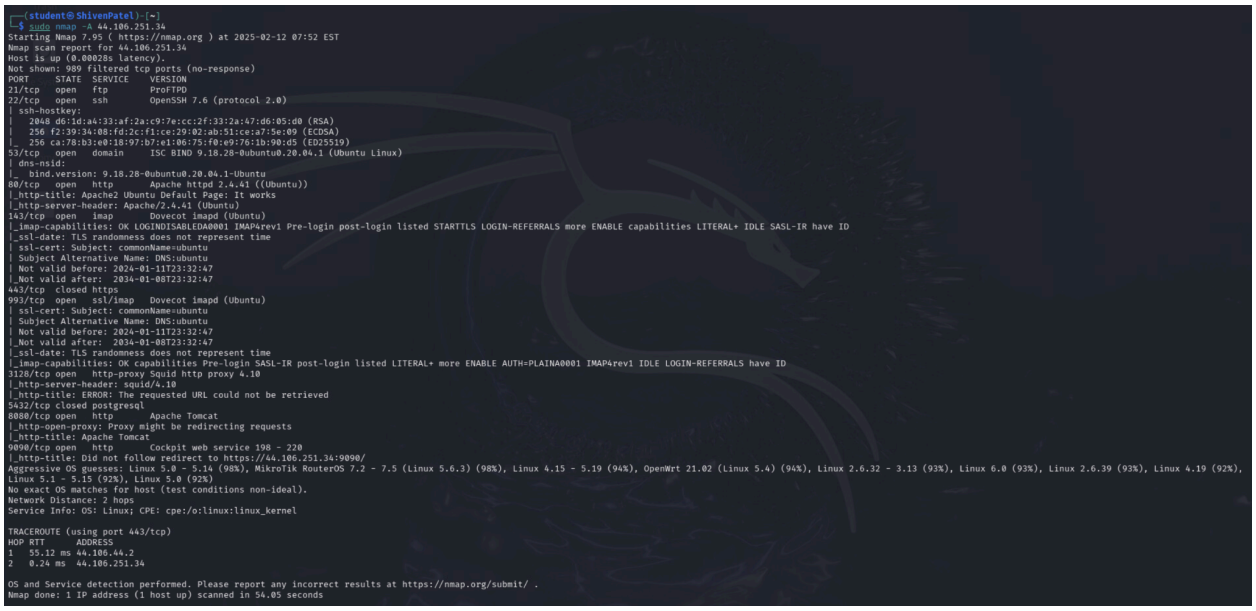

Figure 6: OS Detection Using `nmap -A 44.106.251.34`

Figure 7: Web Server Detection Using `curl -I http://44.106.251.34` & `whatweb http://44.106.251.34`

`44.106.251.44`

Operating System Details:

- Detected OS: CentOS
- OS Version: CentOS 7
- Kernel Information: Linux 3.10.x
- Detection Method: `nmap -A 44.106.251.44`
    - Web Server Detection provided the CentOS version
    - Using the aggressive (`-A`) nmap scan, Linux 3.10 Kernel was identified

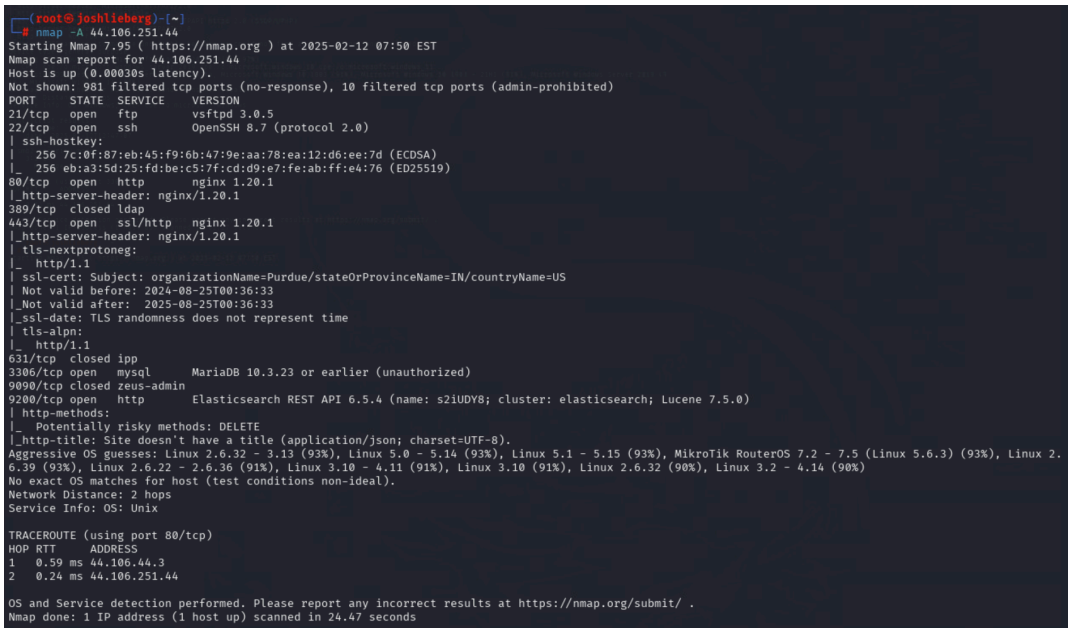

Figure 8: Nmap scan results for `44.106.251.44` revealing open ports, services, and system details.

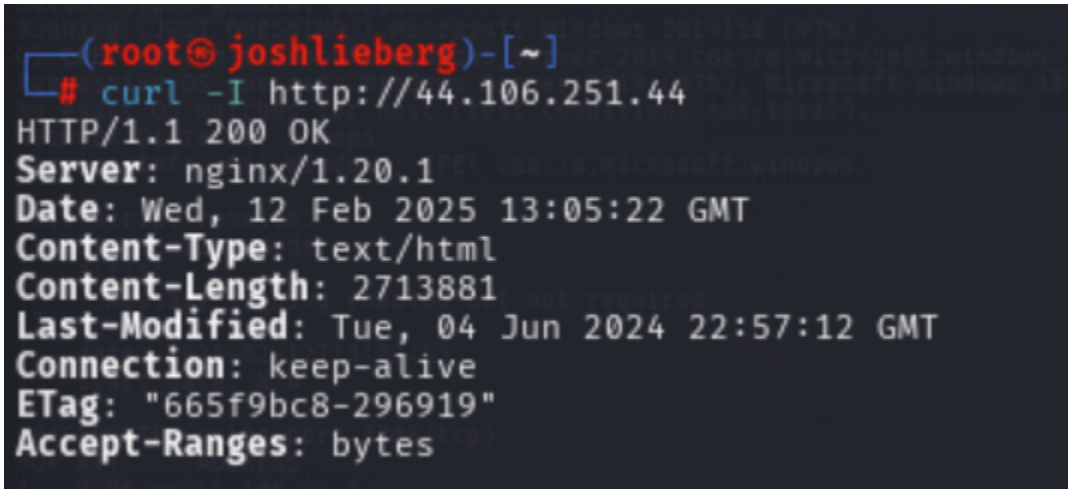

Figure 9: Using `curl -I http://44.106.251.44` to show HTTP headers of an Nginx 1.20.1 server

Figure10: `whatweb 44.106.251.44` scan results revealing Nginx 1.20.1, CentOS, and metadata details.

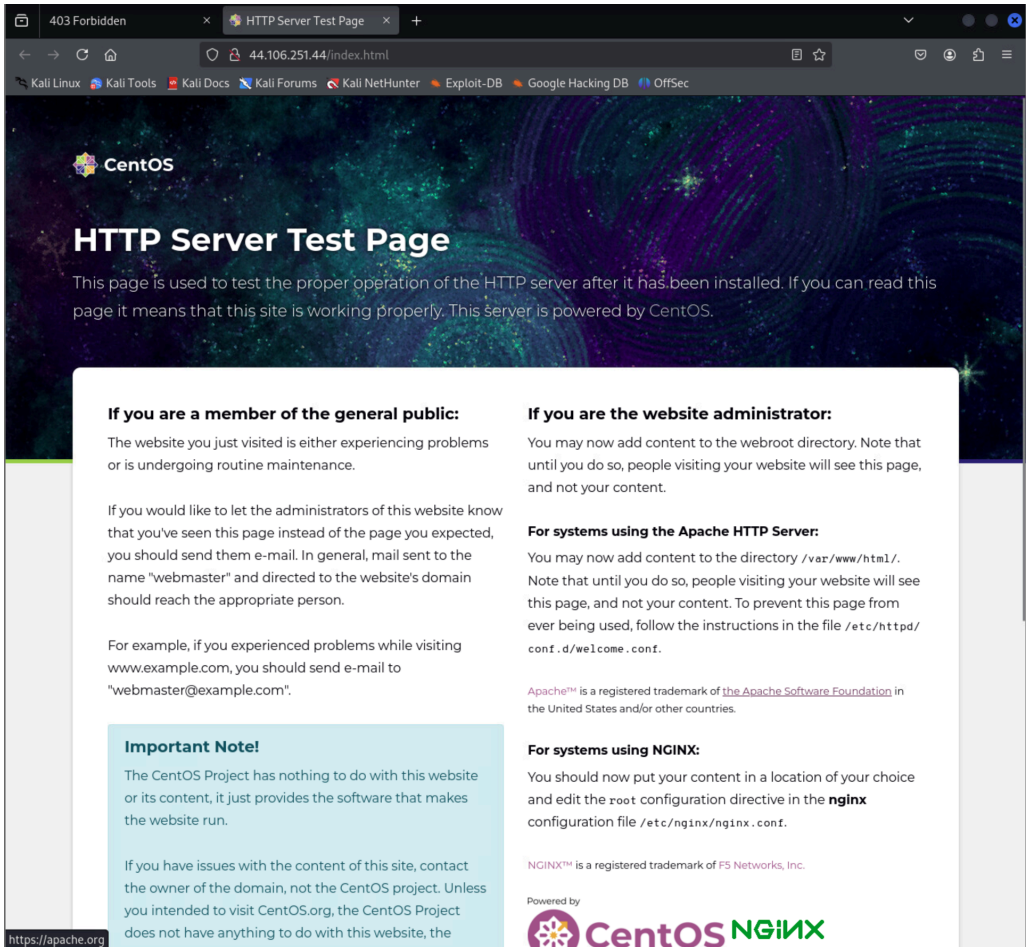

Figure 11: Accessing the web server on `44.106.251.44`

3.4 Detailed Findings

SMB Signing Disabled

Impacted Machine: Windows Server 2019 `44.106.251.64`

- Port 445/tcp
- Service: SMB
- Risk Level: High
- Risk Assessment: Very High
- CVE-2019-0633

A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'.

Figure 12: `crackmacexec smb 44.106.251.64` used, showing SMB Signing is disabled

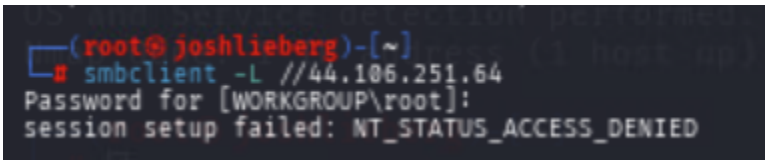

Figure 13: `smbclient -L //44.106.251.64` used, showing proof of other SMB methods

WinRM Open

Impacted Machine: Windows Server 2019 `44.106.251.64`

- Port 5985/tcp & 5986/tcp
- Service: WinRM
- Risk Level: High
- Risk Assessment: Very High
- CVE-2022-41082
- CVE-2022-41040

WinRM allows remote PowerShell execution. If an attacker gains valid credentials, they can remotely execute arbitrary commands with SYSTEM privileges.

Figure 14: Running `evil-winrm -i 44.106.251.64 -u administrator -p Password123` to confirm the accessibility of WinRM

Apache 2.4.41 Vulnerabilities

Impacted Machine: Ubuntu 20.04.1 `44.106.251.34`

- Port 80/tcp & 443/tcp
- Service: Apache HTTP
- Risk Level: High
- Risk Assessment: Very High
- CVE-2021-41773
- CVE-2021-44790
- CVE-2021-26691

Apache 2.4.41 has a path traversal vulnerability that allows attackers to execute arbitrary shell commands. This exposes remote code execution risks.

Figure 15: Apache 2.4.41 Running on `44.106.251.34`

Remote Code Execution via MSRPC

Impacted Machine: Windows Server 2019 `44.106.251.64`

- Port 135/tcp
- Service: MSRPC
- Risk Level: High
- Risk Assessment: Very High
- CVE-2022-26809

A critical remote code execution vulnerability in the Microsoft Remote Procedure Call (RPC) runtime. An unauthenticated attacker could exploit this to execute arbitrary code on the target system.

BlueKeep Vulnerability

Impacted Machine: Windows Server 2019 `44.106.251.64`

- Port 3389/tcp
- Service: RDP
- Risk Level: Medium
- Risk Assessment: High
- CVE-2019-0708

A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.

ProFTPD Vulnerability

Impacted Machine: Ubuntu 20.04.1 `44.106.251.34`

- Port 21/tcp
- Service: FTP
- Risk Level: High
- Risk Assessment: High
- CVE-2015-3306

The mod_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands.

Apache HTTP Server Vulnerability

Impacted Machine: Ubuntu 20.04.1 `44.106.251.34`

- Port 80/tcp
- Service: HTTP
- Risk Level: High
- Risk Assessment: High

- CVE-2020-1934

Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

HTTP Proxy Vulnerability

Impacted Machine: Ubuntu 20.04.1 `44.106.251.34`

- Port 3128/tcp
- Service: HTTP Proxy
- Risk Level: High
- Risk Assessment: Very High
- CVE-2019-12527

An issue was discovered in Squid 4.0.23 through 4.7. When checking Basic Authentication with HttpHeader::getAuth, Squid uses a global buffer to store the decoded data. Squid does not check that the decoded length isn't greater than the buffer, leading to a heap-based buffer overflow with user controlled data.

MySQL Vulnerability

Impacted Machine: CentOS7 `44.106.251.44`

- Port 3306/tcp
- Service: MySQL
- Risk Level: High
- Risk Assessment: High
- CVE-2018-2562

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Partition). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.19 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data.

Memcached Vulnerability

Impacted Machine: CentOS7 `44.106.251.44`

- Port 11211/tcp
- Service: Memcached
- Risk Level: High
- Risk Assessment: Very High
- CVE-2021-37519

Buffer Overflow vulnerability in authfile.c memcached 1.6.9 allows attackers to cause a denial of service via a crafted authentication file.

4.0 Works Cited

Enumerating a New Network with Nmap.

https://www.redhat.com/en/blog/enumerating-network-nmap. Accessed 17 Feb. 2025.

Linux Enumeration Cheat Sheet | Pacific Cybersecurity.

https://cyberlab.pacific.edu/resources/linux-enumeration-cheat-sheet. Accessed 17 Feb. 2025.

NVD - CVE-2015-3306. https://nvd.nist.gov/vuln/detail/CVE-2015-3306. Accessed 17 Feb. 2025.

NVD - Cve-2018-2562. https://nvd.nist.gov/vuln/detail/cve-2018-2562. Accessed 17 Feb. 2025.

NVD - CVE-2019-0633. https://nvd.nist.gov/vuln/detail/CVE-2019-0633. Accessed 17 Feb. 2025.

NVD - Cve-2019-0708. https://nvd.nist.gov/vuln/detail/cve-2019-0708. Accessed 17 Feb. 2025.

NVD - Cve-2020-1934. https://nvd.nist.gov/vuln/detail/cve-2020-1934. Accessed 17 Feb. 2025.

NVD - Cve-2021-26691. https://nvd.nist.gov/vuln/detail/cve-2021-26691. Accessed 17 Feb. 2025.

NVD - Cve-2021-37519. https://nvd.nist.gov/vuln/detail/cve-2021-37519. Accessed 17 Feb. 2025.

NVD - Cve-2021-41773. https://nvd.nist.gov/vuln/detail/cve-2021-41773. Accessed 17 Feb. 2025.

NVD - Cve-2021-44790. https://nvd.nist.gov/vuln/detail/cve-2021-44790. Accessed 17 Feb. 2025.

NVD - Cve-2022-26809. https://nvd.nist.gov/vuln/detail/cve-2022-26809. Accessed 17 Feb. 2025.

NVD - Cve-2022-41040. https://nvd.nist.gov/vuln/detail/cve-2022-41040. Accessed 17 Feb. 2025.

NVD - Cve-2022-41082. https://nvd.nist.gov/vuln/detail/cve-2022-41082. Accessed 17 Feb. 2025.

Penetration Testing · Nebraska-Gencyber-Modules. https://mlhale.github.io/nebraska-gencyber-modules/penetration_testing/README/. Accessed 17 Feb. 2025.

"Sample Network Penetration Test Report Template." *PurpleSec*, https://purplesec.us/resources/sample-network-penetration-test-report/. Accessed 17 Feb. 2025.

Service Name and Transport Protocol Port Number Registry. https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?&page=1. Accessed 17 Feb. 2025.

https://www.recordedfuture.com/threat-intelligence-101/tools-and-techniques/nmap-commands. Accessed 17 Feb. 2025.