NETWORK VULNERABILITY ASSESSMENT TO IDENTIFY AND MITIGATE CRITICAL VULNERABILITIES AT SANSYDTECH

PREPARED BY

SETH DENKYIRA WIREDU

A CYBERSECURITY INTERN AT EXTION INFOTECH

DATE: 23TH JULY 2024

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY

This report presents the findings of the recent vulnerability assessment conducted by the cybersecurity team at SansydTech (an imaginary company). The objective was to identify and mitigate critical vulnerabilities within the company to minimize risks to business operations and sensitive data as required by company policies and industry regulations. The assessment revealed several critical vulnerabilities on the company's network affecting some critical servers, and workstations, using Nessus and Nmap (renowned network scanning tools). Some of these vulnerabilities have known exploits which when employed by threat actors can lead to potential data breaches and unauthorized access to highly sensitive data. Each vulnerability is described in detail, including its Common Vulnerabilities and Exposures (CVE) identifier, severity rating (such as the Common Vulnerability Scoring System, or CVSS score), and the specific systems and services affected. The report also includes a risk analysis section (based on the likelihood of exploitation or occurrence and its impact on business) prioritizing which vulnerabilities need immediate remediation. Furthermore, a remediation plan including upgrading outdated software, and applying security patches, has been recommended by the team to the system administrators to mitigate those vulnerabilities. The team suggests that while these identified vulnerabilities be remediated within 30 days, the most critical ones should be remediated within 2 weeks.

2.0 INTRODUCTION

As technology advances the importance of securing information systems cannot be overemphasized. Organizations today are increasingly dependent on technology for their daily operations, making them prime targets for cybercriminals who continuously seek new ways to exploit system and application weaknesses. These weaknesses are referred to as vulnerabilities. It is of prime importance for organizations to be able to use people, processes, and technologies to identify vulnerabilities and prioritize them for remediation, based on organizational risks, before they are exploited by threat actors. This process of identifying and prioritizing vulnerabilities is known as Vulnerability assessment. A vulnerability assessment is a critical component of an organization's overall security strategy, designed to identify, evaluate, and prioritize security flaws that could be exploited by malicious actors. This proactive approach is essential in minimizing the risk of data breaches, financial losses, and reputational damage.

Vulnerability assessments provide a comprehensive understanding of an organization's security posture. By systematically identifying potential vulnerabilities across various assets, including networks, servers, workstations, applications, and even cloud environments, organizations can take preemptive measures to address security gaps. Conducting regular vulnerability assessments allows organizations to stay ahead of emerging threats, ensuring that they proactively identify and address security gaps before they can be exploited, thereby minimizing the risk of data breaches, financial losses, and reputational damage.

Apart from conducting vulnerability assessments to proactively strengthen an organization's information security system, there may be some regulatory requirements that they have to comply with. These requirements vary depending on the industry the organization operates in and the geographical location of the company. Some of them include General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), International Organization for

Standardization (ISO) and the International Electrochemical Commission (IEC) [ISO:IEC 27001] standard, Health Insurance Portability and Accountability Act (HIPAA), only to mention a few. In addition, an organization may adopt some frameworks or best practices that are not enforced by regulatory bodies such as National Institute of Standards and Technologies (NIST) frameworks including NIST 800-53 and NIST CSF, Center for Internet Security (CIS) Controls, etc.

SansydTech is an imaginary company that has a cybersecurity team responsible for establishing, implementing, maintaining, and continually improving the information security management system of the company. There are several reasons for conducting this vulnerability assessment. To begin with, SansydTech is required to comply with cybersecurity regulations and industry compliance standards (ISO 27001, GDPR, PCI DSS) by conducting regular vulnerability assessments. This would be achieved by the collective involvement of the people, processes, and technologies in the networking environment of the company. Also, recent security audits have revealed several misconfigurations on critical servers, unused open ports on some network devices and servers, unauthorized access, etc.

Furthermore, some servers of the company are public-facing, and as such very robust security controls would have to be implemented to ensure the confidentiality and integrity of the data stored and processed by the servers, as well as the availability of the service rendered.

Finally, the significant increase in the number of cyberattacks means to minimize our risks of being attacked, the cybersecurity team would have to proactively identify network vulnerabilities and mitigate them promptly before exploited by threat actors.

This report seeks to unveil how the team governed by the company’s policies and industry regulations, used renowned tools namely, Nessus and Nmap (network mapper) in assessing the company’s network infrastructure.

2.1 SCOPE OF ASSESSMENT

The assessment covered the organization’s internal network infrastructure. This included a comprehensive review of the following assets:

- Network Infrastructure: Routers, switches, firewalls, and other network devices.
- Servers and Workstations: Both physical and virtual servers, as well as employee workstations.
- Web Applications: All web-based applications
- Databases: Database management systems and the data they store.

2.2 DATE AND DURATION OF ASSESSMENT

The assessment was conducted on July 20, 2024

3.0 METHODOLOGY

The assessment was conducted using a combination of automated network scanning tools and manual techniques ensuring a complementary and comprehensive discovery of vulnerabilities. The following steps were performed:

- **Asset Discovery**: Identification of all assets within the assessment scope, creating an inventory of devices, applications, and systems.
- **Vulnerability Scanning**: Nessus Essentials and Nmap (Kali Linux) were used to scan the identified assets for known vulnerabilities and misconfigurations.
- **Analysis**: The scan results were analysed to determine the potential impact and exploitability of the identified vulnerabilities. This analysis involved verifying the findings to eliminate false positives and assessing the context of each vulnerability.
- **Risk Assessment**: Vulnerabilities were prioritized based on their severity, potential impact, and the likelihood of exploitation. This prioritization helps in focusing remediation efforts on the most critical issues
- **Reporting**: Detailed documentation of the findings, including recommended remediation steps.
- **Remediation and Verification**: Implementing the recommended actions to fix or mitigate the vulnerabilities, such as applying patches, changing configurations, or updating software. After remediation, the environment was re-scanned to ensure the effectiveness of the applied fixes.

3.1 TOOLS USED

To perform the vulnerability assessment, the cybersecurity team used the following tools:

- **Nessus:** Nessus is a widely used vulnerability assessment tool developed by Tenable, Inc. It scans systems and networks for vulnerabilities that could be exploited by attackers. It also provides detailed reports and recommendations to help organizations enhance their security posture.
- **Nmap** (Network Mapper): Nmap is an open-source network discovery and security auditing tool. It is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap can identify open ports, operating systems, and vulnerabilities and provide detailed information about network infrastructure.

Using both Nessus and Nmap in a vulnerability assessment leverages the strength of each tool, resulting in a comprehensive analysis of network security. This is because while Nmap is excellent for network discovery and port identification, Nessus specializes in detecting specific vulnerabilities and security issues.

3.2 COMPLIANCE AND INDUSTRY REGULATORY STANDARDS

To ensure that the assessment meets the objectives of the company and the requirements of regulatory standards, our team inferred from the company’s information security policy, and with the help of the Compliance officer, we were able to fine-tune our procedures to align with OWASP Top 10, PCI DSS, GDPR and ISO 27001.

4.0 ANALYSIS AND FINDINGS

The assessment identified a total of 26 vulnerabilities, 21 from Nessus and 5 from Nmap, across the assessed assets. The vulnerabilities were categorized based on their severity using the Common Vulnerability Scoring System (CVSS) which categorizes vulnerabilities into Critical, High, Medium, and Low. Nessus also reported some additional findings that, while not necessarily vulnerabilities provide insights into the security posture. Addressing these informational findings can enhance the overall security posture but do not represent direct vulnerabilities.

Severity	**Number**
Critical	**5**
High	**8**
Medium	**8**
Low	**5**

- **Critical (9.0 - 10.0):** Vulnerabilities in this range are the most severe and demand immediate attention. Exploitation is often very simple, and the consequences are dire, potentially leading to complete system compromise. This could include gaining root or administrative access, complete data loss or theft, or total service disruption. Organizations must respond urgently to these vulnerabilities to prevent catastrophic damage.
- **High (7.0 – 8.9):** High-severity vulnerabilities pose a significant risk to the affected systems. Exploitation is generally more straightforward, and the potential impact is substantial. Successful exploitation can lead to considerable damage, such as extensive data breaches, significant service interruptions, or the ability to execute arbitrary code. Addressing these should be a top priority to safeguard organization’s assets.

- **Medium (4.0 – 6.9):** Medium severity vulnerabilities present a more considerable risk than low-severity ones. These vulnerabilities are often more accessible to exploit and can result in more noticeable impacts. For instance, an attacker might be able to gain limited access to system functions or data, leading to partial system compromise or unauthorized access to sensitive information. Organizations should address these vulnerabilities in a reasonable time frame to prevent potential exploitation.
- **Low (0.1 – 3.9):** Vulnerabilities in this range have a minor impact on the system. They typically require specific conditions to be exploited and might not provide significant benefits to the attacker. The consequences of exploiting these vulnerabilities are usually minimal, causing only slight inconveniences or minor disruptions to services. Examples might include information disclosure where non-sensitive data is exposed.

4.1 RISK ASSESSMENT

Although the assessment included a range of critical to low vulnerabilities, the scope of the report includes only the key vulnerabilities that pose the greatest risk to the organization and should be addressed as a priority.

Overall Risk: The Overall risk posture of the assessed assets is high, with multiple critical vulnerabilities identified that require immediate remediation to prevent unauthorized access and data breaches.

Key Vulnerabilities Identified That Pose The Greatest Risk To The Company

A. CRITICAL VULNERABILITIES

1. KB5040437: Windows Server 2022 / Azure Stack HCI 22H2 Security Update
   - **Asset affected:** Domain controller (DC-05)
     Description: The remote Windows host is missing security update 5040437. It is, therefore, affected by multiple vulnerabilities (CVE-2024-3596, CVE-2024-21417, etc.)

- **CVSS v3.0**: 9.8
- **Exploits available:** Yes
- **Likelihood of Exploitation:** High
- **Impact:** Unauthorized access

2. Apache 2.4.x < 2.4.60 Multiple Vulnerabilities
   - **Vulnerability IDs**: CVE-2024-36387, CVE-2024-38472, CVE-2024-38473, CVE-2024-38474, CVE-2024-38475, CVE-2024-38476, CVE-2024-38477, CVE-2024-39573
   - **Asset affected**: Web Server (WS-S03)
   - **Description:** The version of Apache httpd installed on the remote host is prior to 2.4.60. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.60 advisory.
   - **CVSS v3.0**: 9.1
   - **Exploits available:** No
   - **Likelihood of Exploitation:** Medium
   - **Impact:** Unauthorized access, source code disclosure, unavailability of service

3. OpenSSL 1.1.1 < 1.1.1za Vulnerability
   - **Vulnerability ID**: CVE-2024-5535
   - **Asset affected**: Web Server (WS-S03)
   - **Description:** The version of OpenSSL installed on the remote host is prior to 1.1.1za. It is, therefore, affected by a vulnerability as referenced in the 1.1.1za advisory.
   - **CVSS v3.0**: 9.1
   - **Exploits available:** No
   - **Likelihood of Exploitation:** Medium
   - **Impact:** Potential data breach, unauthorized access, application crash

4. smb-vuln-ms08-067
   - **Vulnerability ID**: CVE-2008-4250
   - **Affected Asset:** Workstation (PC-98)
   - **Description:** Allows remote attackers to execute arbitrary code via a crafted RPC request
   - **CVSS v2.0**: 10.0
   - **Exploits available:** Yes

- **Likelihood of Exploitation:** High
- **Impact:** Remote code execution on host

5. HTTP-SQL-injection with possible queries
   - **Affected Asset:** Web Server (WS-S03)
   - **Description:** There are possible SQL payloads to inject into URLs
   - **Exploits available:** Yes
   - **Likelihood of Exploitation:** High
   - **Impact:** Unauthorized access to sensitive data

B. HIGH VULNERABILITIES

1. WinVerifyTrust Signature Validation Mitigation (EnableCertPaddingCheck)
   - **Vulnerability ID**: CVE-2013-3900
   - **Affected Asset:** Domain controller (DC-05)
   - **Description:** The remote system may be in a vulnerable state due to missing or misconfigured registry keys
   - **CVSS v3.0**: 7.8
   - **Exploits available:** Yes
   - **Likelihood of Exploitation:** High
   - **Impact:** Potential data breach, unauthorized access, arbitrary code execution on host

2. Security Updates for Microsoft .NET Framework (July 2024)
   - **Affected Asset:** Domain controller (DC-05)
   - **Description:** The Microsoft .NET Framework installation on the remote host is missing a security update. It is, therefore, affected by remote code execution vulnerability (CVE-2024-38081)
   - **CVSS v3.0**: 7.3
   - **Exploits available:** No
   - **Likelihood of Exploitation:** Low
   - **Impact:** Remote code execution, unauthorized access

3. Microsoft Edge (Chromium) with Multiple Vulnerabilities

- **Vulnerability IDs:** CVE-2024-5830, CVE-2024-5831, CVE-2024-5832, CVE-2024-5833, CVE-2024-5834, CVE-2024-5835, CVE-2024-5836, CVE-2024-5837
- **Affected Asset:** Domain controller (DC-05)
- **Description:** The version of Microsoft Edge installed on the remote Windows host is prior to 126.0.2592.56. It is, therefore, affected by multiple vulnerabilities as referenced in the June 13, 2024 advisory.
- **CVSS v3.0**: 8.8
- **Exploits available:** No
- **Likelihood of Exploitation:** Low
- **Impact:** Remote code execution, unauthorized access

4. VMware Tools Authentication Bypass (VMSA-2023-0019 and VMware Tools Token Bypass (VMSA-2023-0024)

- **Vulnerability IDs**: CVE-2023-20900, CVE-2023-34058
- **Affected Asset:** Domain controller (DC-05)
- **Description:** The version of VMware Tools installed on the remote Windows host is outdated. It is, therefore, affected by a SAML token signature bypass vulnerability. Furthermore, if granted Guest Operation Privileges in a target virtual machine, attackers may be able to elevate their privileges if that target virtual machine has been assigned a more privileged Guest Alias.
- **CVSS v3.0**: 7.5
- **Exploits available:** No
- **Likelihood of Exploitation:** Low
- **Impact:** Authentication bypass, unauthorized access

5. Windows Defender Anti-malware/Antivirus Signature Definition Check

- **Affected Asset:** Domain controller (DC-05)
- **Description:** Windows Defender Anti-malware/Antivirus signature has not been updated
- Risk Factor: High
- **Exploits available:** No
- **Likelihood of Exploitation:** Low

- **Impact:** Unauthorized access, code execution

6. Splunk Enterprise 9.0.0 with multiple vulnerabilities
   - **Vulnerability IDs:** CVE-2024-36983, CVE-2024-36982
   - **Affected Asset:** Workstation (PC-98)
   - **Description:** The version of Splunk installed on the remote host is prior to tested version. It is, therefore, affected by vulnerabilities as referenced in the SVD advisories (SVD-2024-0703, SVD-2024-0702, SVD-2024-0701)
   - **CVSS v3.0**: 8.0
   - **Exploits available:** No
   - **Likelihood of Exploitation:** Medium
   - **Impact:** Arbitrary code execution, Privilege escalation

C. MEDIUM VULNERABILITIES

1. SMB Signing not required
   - **Affected Asset:** Workstation (PC-98)
   - **Description:** Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.
   - **CVSS v3.0**: 5.3
   - **Exploits available:** Yes
   - **Likelihood of Exploitation:** High
   - **Impact:** Potential data breach, unauthorized access

2. SSL Certificate Cannot Be Trusted /SSL Self-Signed Certificate
   - **Affected Asset:** Workstation (PC-98)
   - **Description:** The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken. Also, if the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
   - **CVSS v3.0**: 6.5
   - **Exploits available:** No
   - **Likelihood of Exploitation:** Medium

- **Impact:** Unauthorized access to sensitive data, potential data breach

3. HTTP TRACE / TRACK Methods Allowed
   - **Vulnerability IDs**: CVE-2003-1567, CVE-2004-2320, CVE-2010-0386
   - **Affected Asset:** Web Server (WS-S03)
   - **Description:** The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.
   - **CVSS v3.0:** 5.3
   - **Exploits available:** No
   - **Likelihood of Exploitation:** Medium
   - **Impact:** Service unavailability

4. PHP file inclusion vulnerability
   - **Vulnerability ID**: CVE-2005-3299
   - **Affected Asset:** Router (R-005)
   - **Description:** PHP file inclusion vulnerability in grab_globals.lib.php in phpMyAdmin 2.6.4 and 2.6.4-pl1 allows remote attackers to include local files via the $__redirect parameter, possibly involving the subform array.
   - **CVSS v2.0**: 5.0
   - **Exploits available:** Yes
   - **Likelihood of Exploitation:** High
   - **Impact:** Denial-of-service, Website defacement. Remote code execution, lateral movement

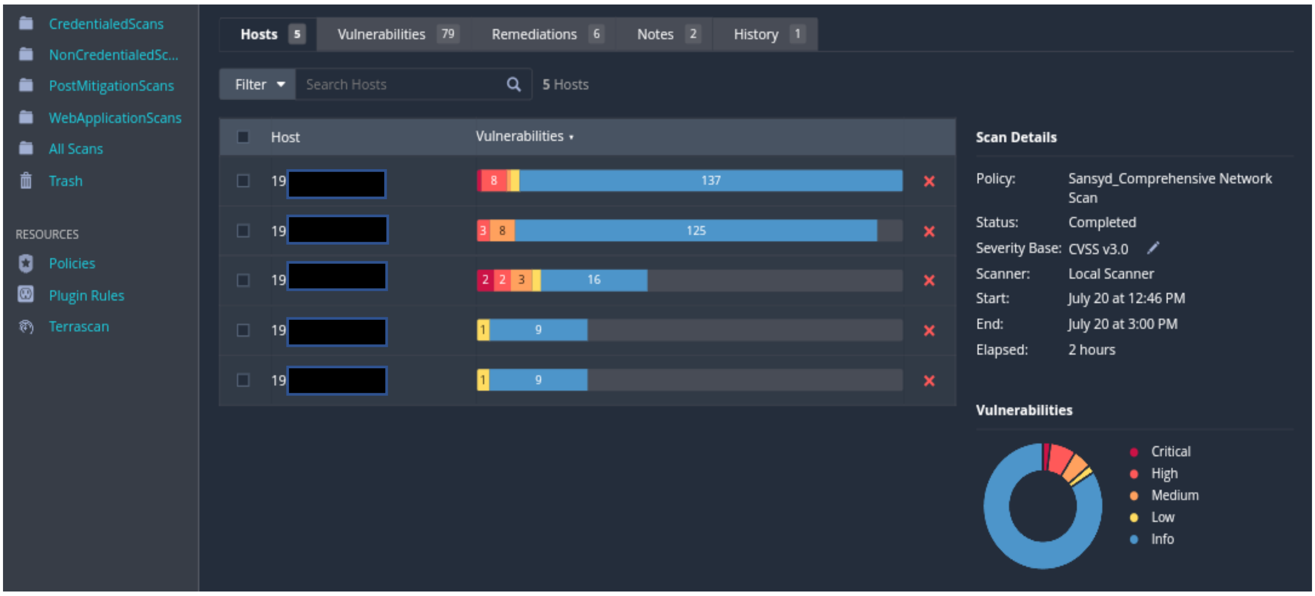
5. Slowloris DOS attack
   - **Vulnerability ID**: CVE-2007-6750
   - **Affected Asset:** Router (R-005)
   - **Description:** The Apache HTTP Server 1.x and 2.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests
   - **CVSS v2.0**: 5.0
   - **Exploits available:** Yes
   - **Likelihood of Exploitation:** High
   - **Impact:** Denial-of-service

Informational Findings On Unknown But Open Ports

ASSET	PORTS
Domain controller (DC-05)	49664, 49665, 49666, 49668, 49669,49670, 49671, 52512, 52513, 52527, 52528, 5751
Workstation (PC-98)	5040,49664, 49665, 49666, 49667, 49668, 49669, 49672, 49673
Router (R-005)	20249, 37215

4.2 SUPPORTING EVIDENCE OF SCAN RESULTS

SCREENSHOTS FROM NESSUS



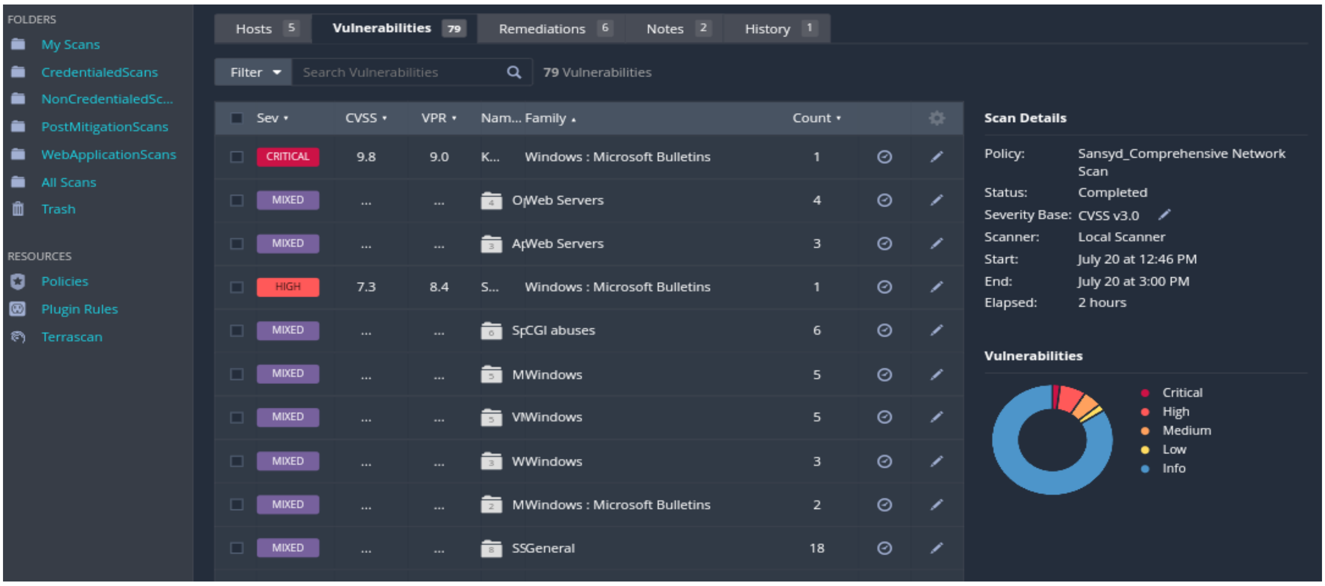
5 Hosts

Host	Vulnerabilities
19 [redacted]	8 137
19 [redacted]	3 8 125
19 [redacted]	2 2 3 16
19 [redacted]	1 9
19 [redacted]	1 9

Scan Details

Policy:	Sansyd_Comprehensive Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	July 20 at 12:46 PM
End:	July 20 at 3:00 PM
Elapsed:	2 hours

Vulnerabilities



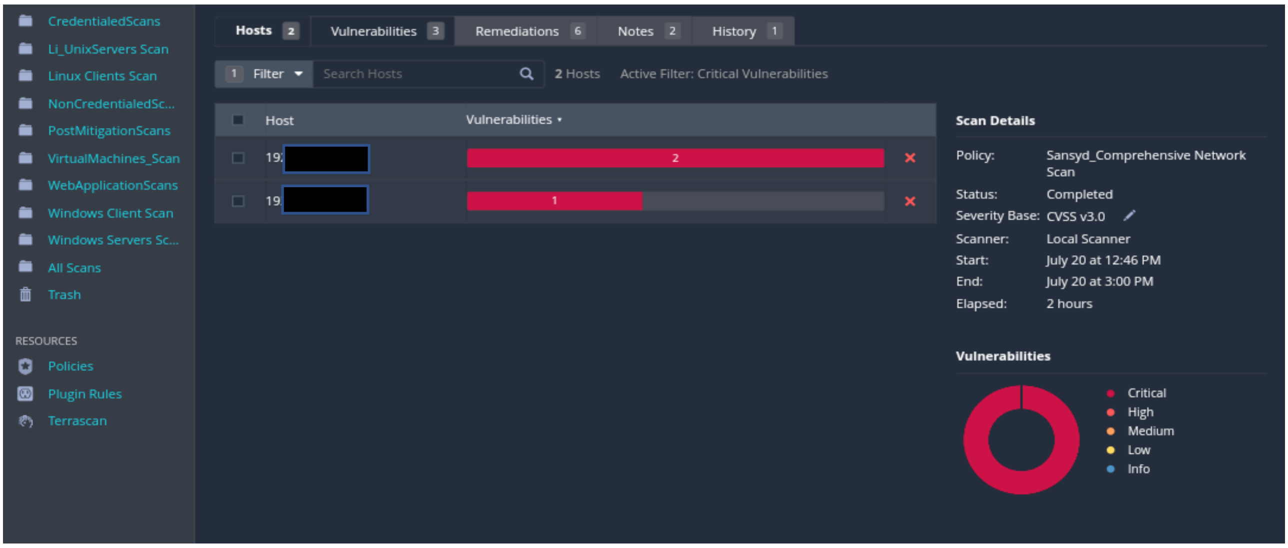
79 Vulnerabilities

Sev	CVSS	VPR	Nam...	Family	Count
CRITICAL	9.8	9.0	K...	Windows : Microsoft Bulletins	1
MIXED	...	...	O	Web Servers	4
MIXED	...	...	A	Web Servers	3
HIGH	7.3	8.4	S...	Windows : Microsoft Bulletins	1
MIXED	...	...	S	CGI abuses	6
MIXED	...	...	M	Windows	5
MIXED	...	...	V	Windows	5
MIXED	...	...	W	Windows	3
MIXED	...	...	M	Windows : Microsoft Bulletins	2
MIXED	...	...	S	General	18

Scan Details

Policy:	Sansyd_Comprehensive Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	July 20 at 12:46 PM
End:	July 20 at 3:00 PM
Elapsed:	2 hours

Vulnerabilities



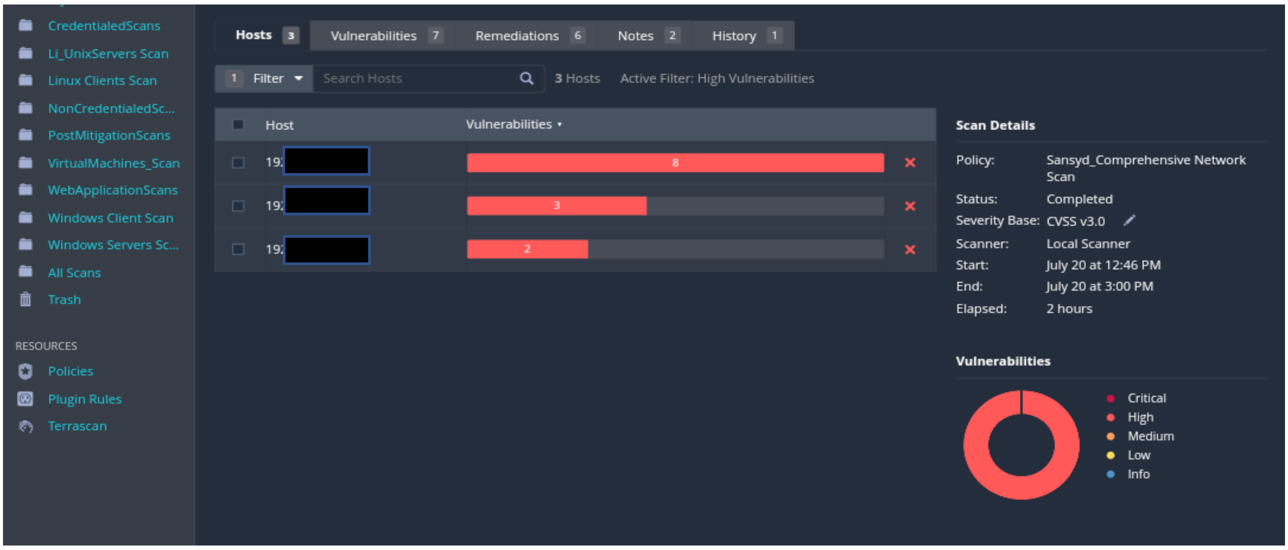
2 Hosts Active Filter: Critical Vulnerabilities

Host	Vulnerabilities
19[redacted]	2
19[redacted]	1

Scan Details

Policy: Sansyd_Comprehensive Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: July 20 at 12:46 PM
End: July 20 at 3:00 PM
Elapsed: 2 hours

Vulnerabilities



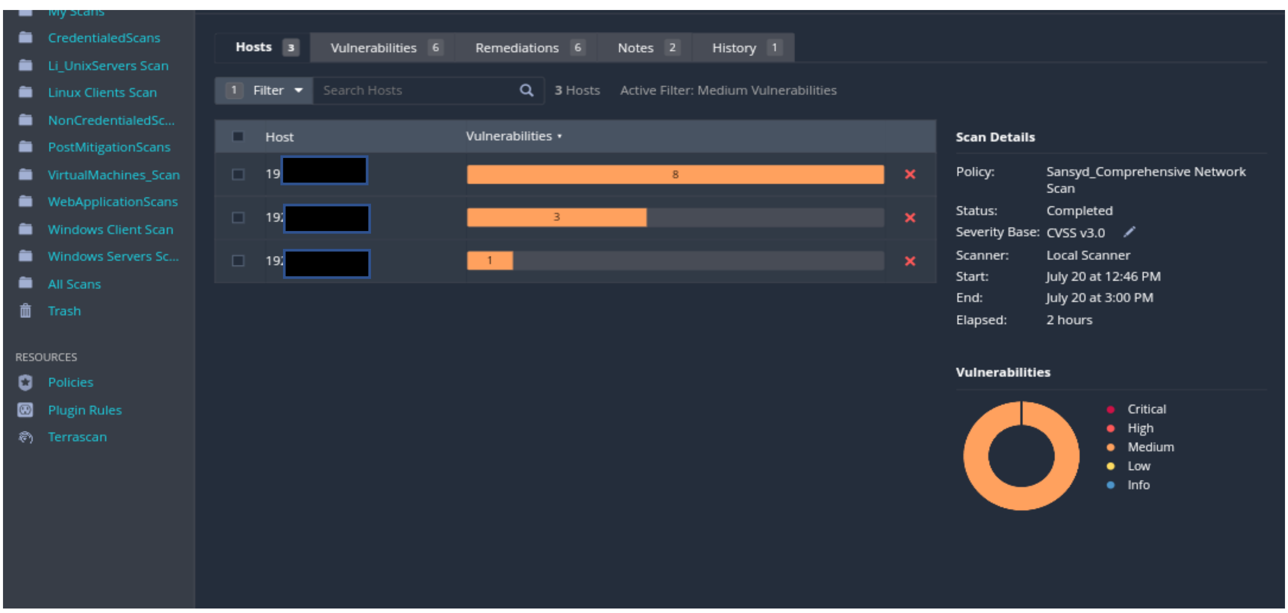
3 Hosts Active Filter: High Vulnerabilities

Host	Vulnerabilities
19[redacted]	8
19[redacted]	3
19[redacted]	2

Scan Details

Policy: Sansyd_Comprehensive Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: July 20 at 12:46 PM
End: July 20 at 3:00 PM
Elapsed: 2 hours

Vulnerabilities



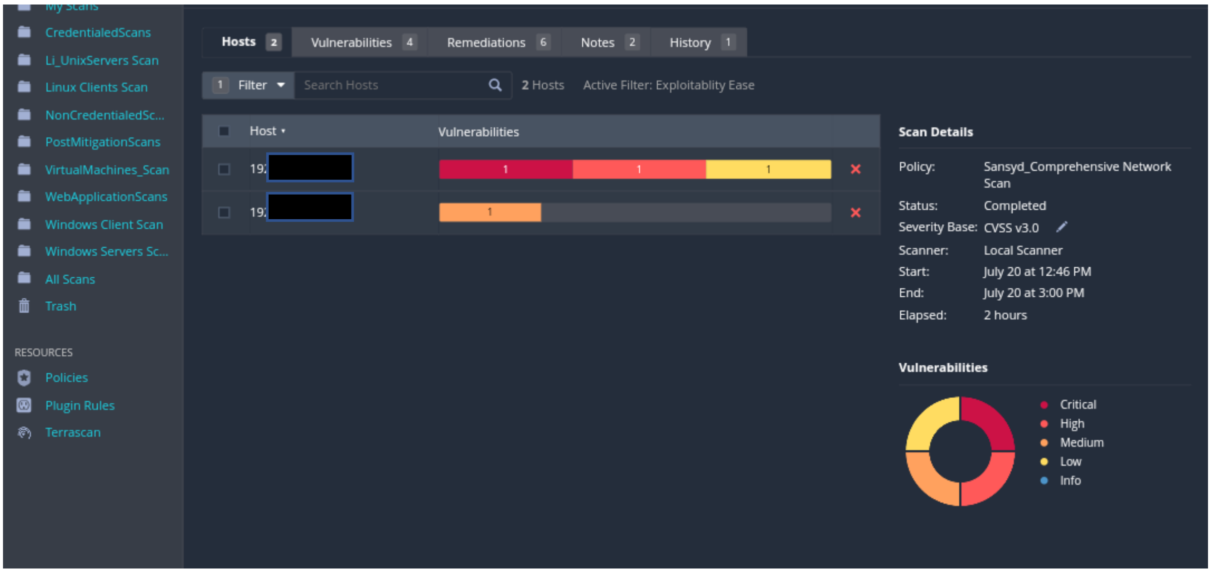
3 Hosts Active Filter: Medium Vulnerabilities

Host	Vulnerabilities
19[redacted]	8
19[redacted]	3
19[redacted]	1

Scan Details

Policy: Sansyd_Comprehensive Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: July 20 at 12:46 PM
End: July 20 at 3:00 PM
Elapsed: 2 hours

Vulnerabilities

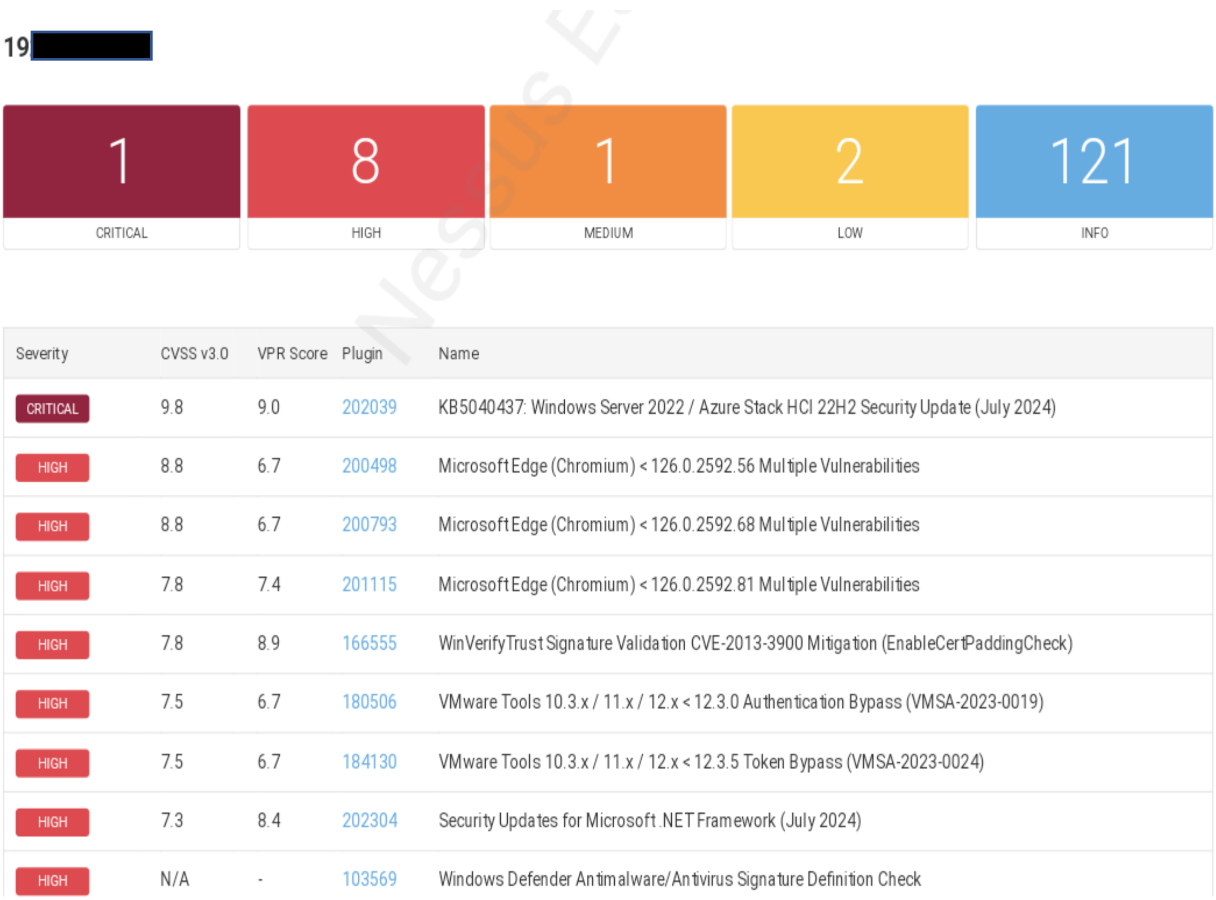


Host	Vulnerabilities
19[redacted]	1 1 1
19[redacted]	1

Scan Details

Policy: Sansyd_Comprehensive Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: July 20 at 12:46 PM
End: July 20 at 3:00 PM
Elapsed: 2 hours

Vulnerabilities

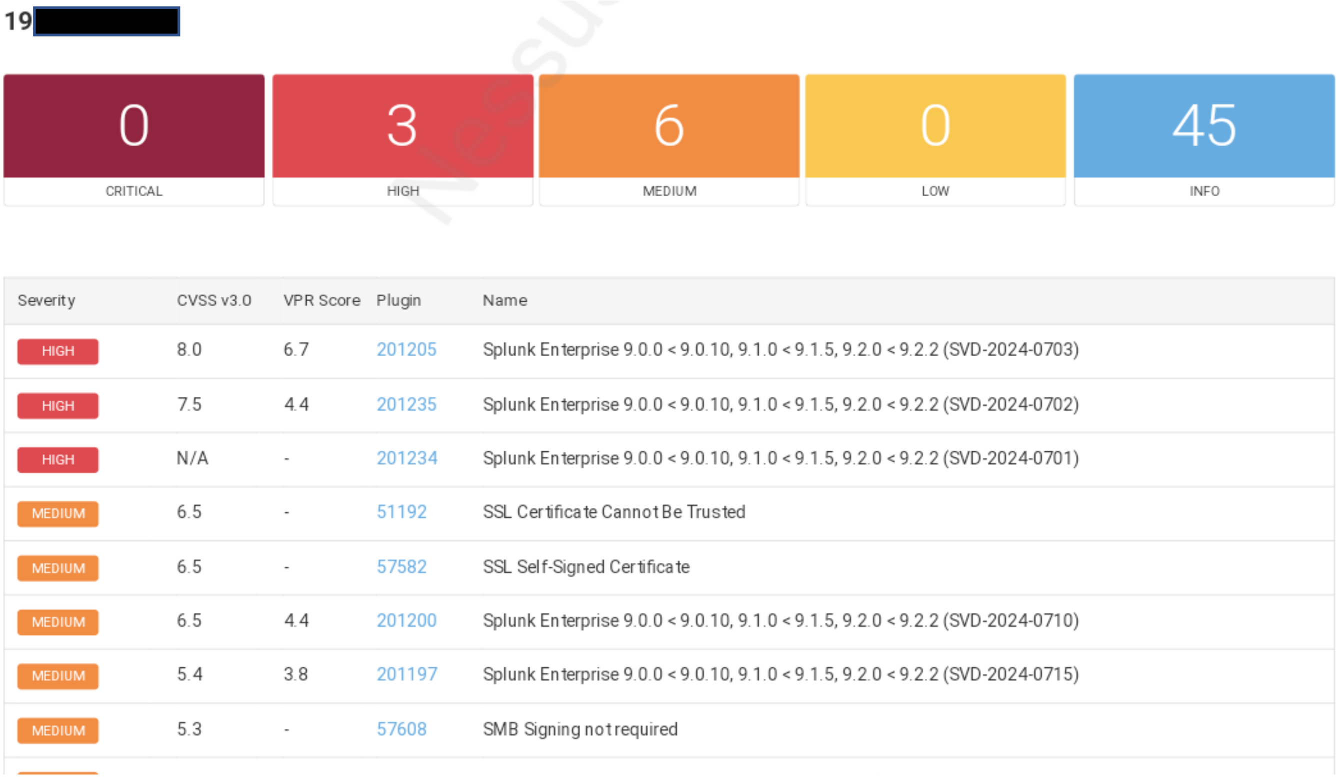


19[redacted]

1	8	1	2	121
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	Plugin	Name
CRITICAL	9.8	9.0	202039	KB5040437: Windows Server 2022 / Azure Stack HCI 22H2 Security Update (July 2024)
HIGH	8.8	6.7	200498	Microsoft Edge (Chromium) < 126.0.2592.56 Multiple Vulnerabilities
HIGH	8.8	6.7	200793	Microsoft Edge (Chromium) < 126.0.2592.68 Multiple Vulnerabilities
HIGH	7.8	7.4	201115	Microsoft Edge (Chromium) < 126.0.2592.81 Multiple Vulnerabilities
HIGH	7.8	8.9	166555	WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)
HIGH	7.5	6.7	180506	VMware Tools 10.3.x / 11.x / 12.x < 12.3.0 Authentication Bypass (VMSA-2023-0019)
HIGH	7.5	6.7	184130	VMware Tools 10.3.x / 11.x / 12.x < 12.3.5 Token Bypass (VMSA-2023-0024)
HIGH	7.3	8.4	202304	Security Updates for Microsoft .NET Framework (July 2024)
HIGH	N/A	-	103569	Windows Defender Antimalware/Antivirus Signature Definition Check

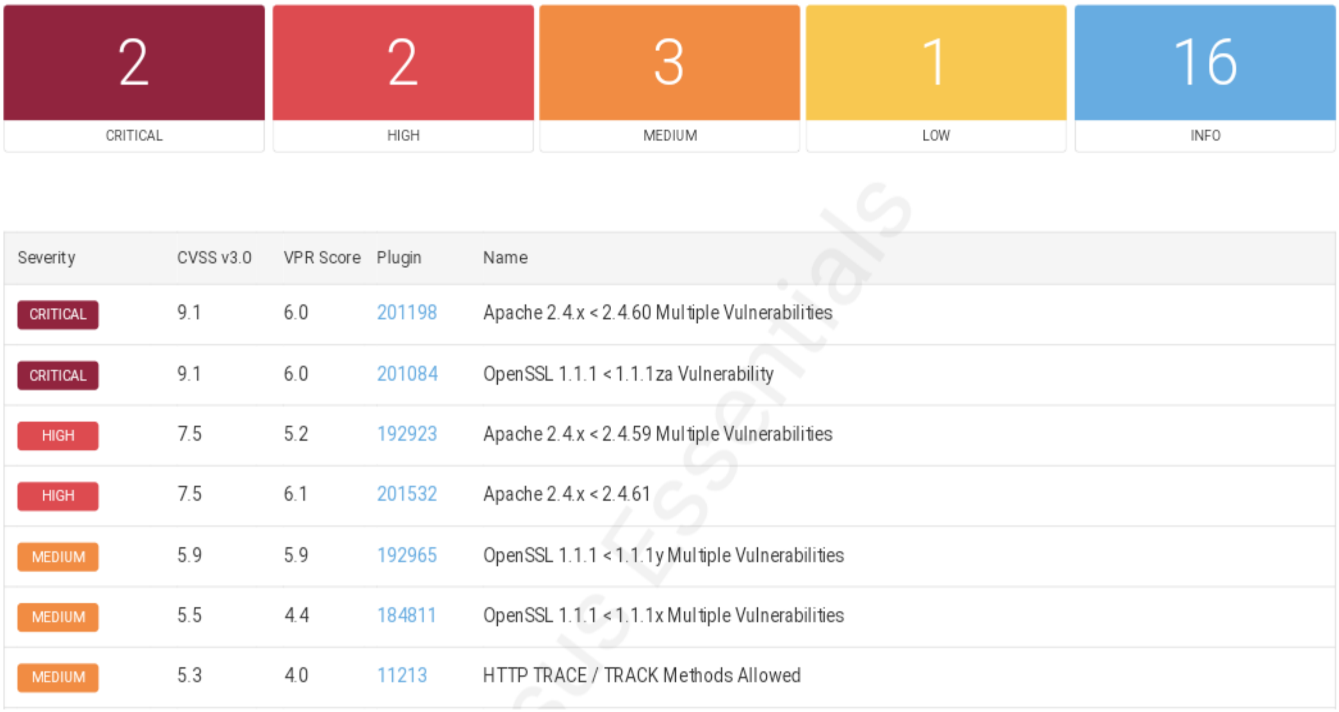
19[redacted]



0	3	6	0	45
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	Plugin	Name
HIGH	8.0	6.7	201205	Splunk Enterprise 9.0.0 < 9.0.10, 9.1.0 < 9.1.5, 9.2.0 < 9.2.2 (SVD-2024-0703)
HIGH	7.5	4.4	201235	Splunk Enterprise 9.0.0 < 9.0.10, 9.1.0 < 9.1.5, 9.2.0 < 9.2.2 (SVD-2024-0702)
HIGH	N/A	-	201234	Splunk Enterprise 9.0.0 < 9.0.10, 9.1.0 < 9.1.5, 9.2.0 < 9.2.2 (SVD-2024-0701)
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	4.4	201200	Splunk Enterprise 9.0.0 < 9.0.10, 9.1.0 < 9.1.5, 9.2.0 < 9.2.2 (SVD-2024-0710)
MEDIUM	5.4	3.8	201197	Splunk Enterprise 9.0.0 < 9.0.10, 9.1.0 < 9.1.5, 9.2.0 < 9.2.2 (SVD-2024-0715)
MEDIUM	5.3	-	57608	SMB Signing not required

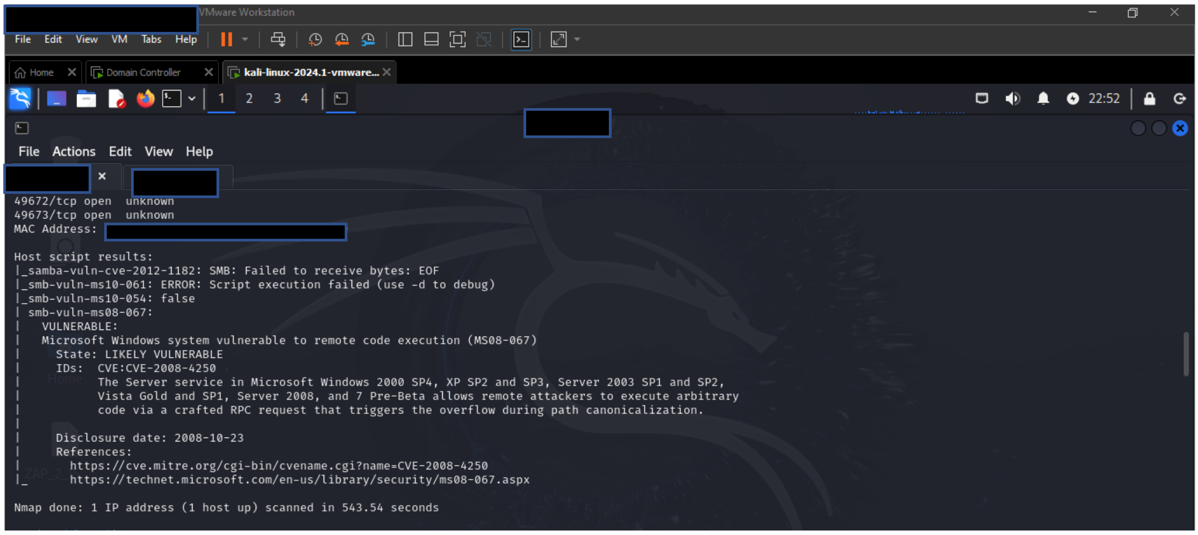
19[redacted]



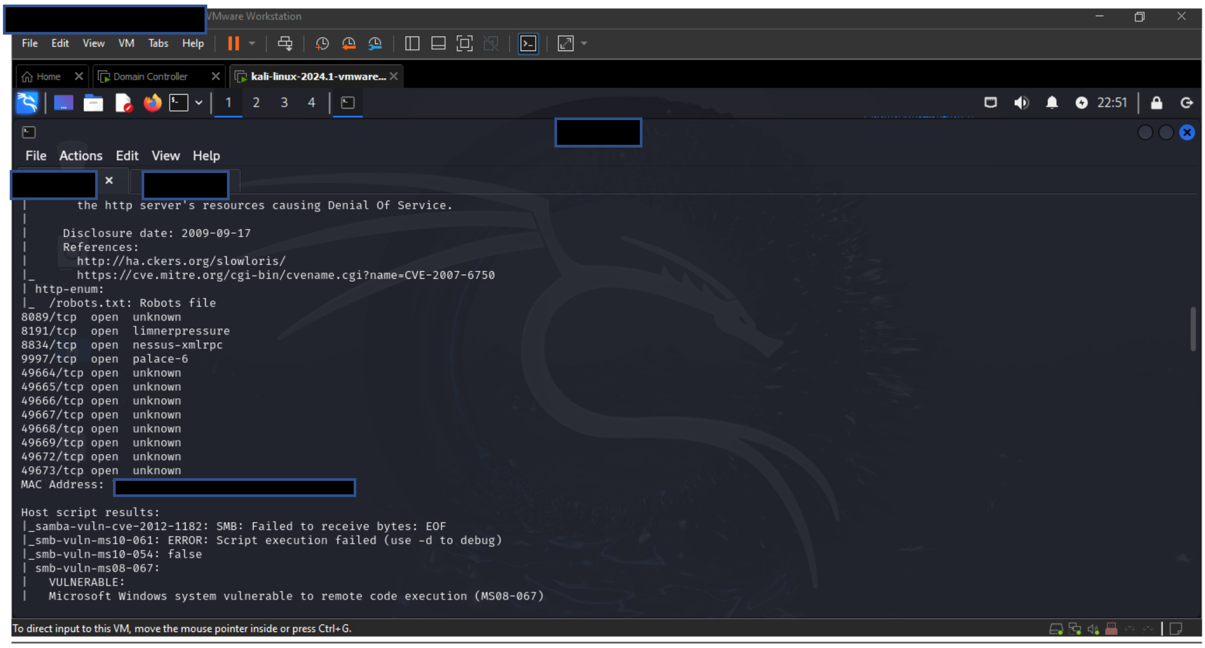
2	2	3	1	16
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	Plugin	Name
CRITICAL	9.1	6.0	201198	Apache 2.4.x < 2.4.60 Multiple Vulnerabilities
CRITICAL	9.1	6.0	201084	OpenSSL 1.1.1 < 1.1.1za Vulnerability
HIGH	7.5	5.2	192923	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
HIGH	7.5	6.1	201532	Apache 2.4.x < 2.4.61
MEDIUM	5.9	5.9	192965	OpenSSL 1.1.1 < 1.1.1y Multiple Vulnerabilities
MEDIUM	5.5	4.4	184811	OpenSSL 1.1.1 < 1.1.1x Multiple Vulnerabilities
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed

SCREENSHOTS FROM NMAP

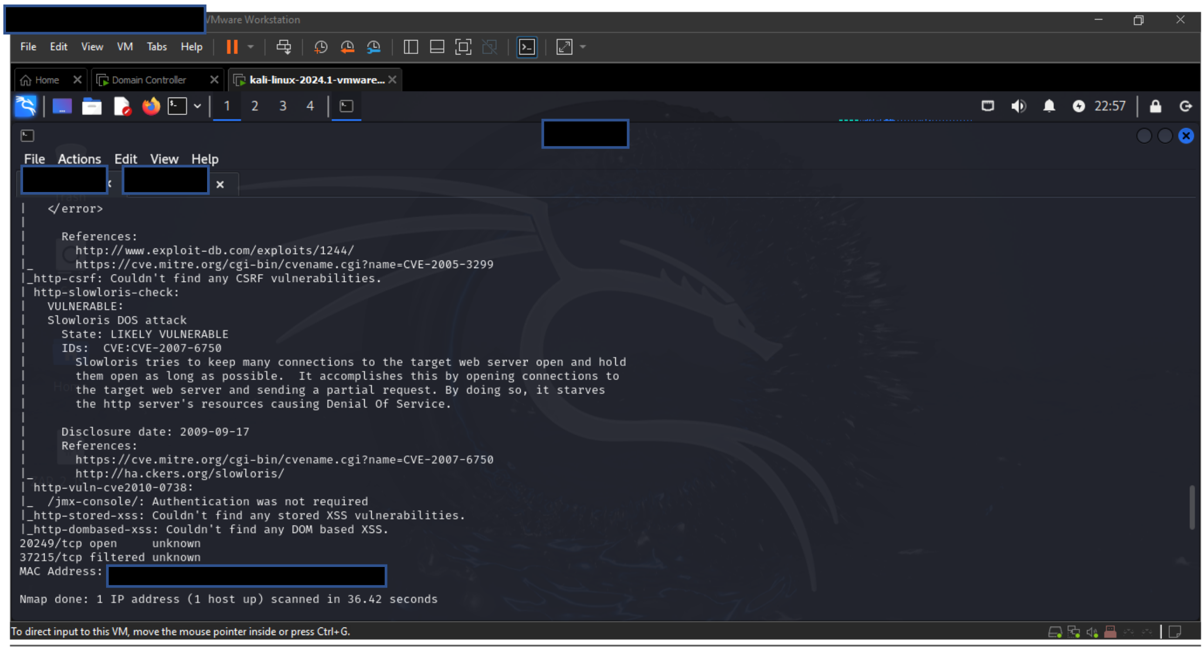

[redacted] VMware Workstation
File Edit View VM Tabs Help
Home
Domain Controller
kali-linux-2024.1-vmware...
1 2 3 4
22:52
[redacted]
File Actions Edit View Help
[redacted]
[redacted]

```
49672/tcp open  unknown
49673/tcp open  unknown
MAC Address: [redacted]

Host script results:
|_samba-vuln-cve-2012-1182: SMB: Failed to receive bytes: EOF
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-054: false
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx

Nmap done: 1 IP address (1 host up) scanned in 543.54 seconds
```


[redacted] VMware Workstation
File Edit View VM Tabs Help
Home
Domain Controller
kali-linux-2024.1-vmware...
1 2 3 4
22:51
[redacted]
File Actions Edit View Help
[redacted]
[redacted]

```
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| http-enum:
|_  /robots.txt: Robots file
8089/tcp  open  unknown
8191/tcp  open  limnerpressure
8834/tcp  open  nessus-xmlrpc
9997/tcp  open  palace-6
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49672/tcp open  unknown
49673/tcp open  unknown
MAC Address: [redacted]

Host script results:
|_samba-vuln-cve-2012-1182: SMB: Failed to receive bytes: EOF
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-054: false
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


[redacted] VMware Workstation
File Edit View VM Tabs Help
Home
Domain Controller
kali-linux-2024.1-vmware...
1 2 3 4
22:57
[redacted]
File Actions Edit View Help
[redacted]
[redacted]

```
|   </error>
|
|     References:
|       http://www.exploit-db.com/exploits/1244/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3299
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
| http-vuln-cve2010-0738:
|_  /jmx-console/: Authentication was not required
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
20249/tcp open     unknown
37215/tcp filtered unknown
MAC Address: [redacted]

Nmap done: 1 IP address (1 host up) scanned in 36.42 seconds
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

5.0 MITIGATION STRATEGIES

To address the identified vulnerabilities and ensure security hardening, the following short-term and long-term actions are recommended:

NOTE: Test all updates first in the staging (virtual) environment before full deployment. Ensure the system is closely monitored for any anomalies post-patch. Re-scan the systems using the vulnerability scanning tools to verify that the CVEs are addressed.

5.1 SHORT-TERM ACTIONS

CRITICAL VULNERABILITIES

1. **Vulnerability**: KB5040437 missing update
   Asset: Domain controller (DC-05)
   Team Responsible: System Administration Team (IT)
   Estimated Timeline: 1 week
   Mitigation: Apply the latest security updates

2. **Vulnerability**: Outdated version of Apache (2.4.x < 2.4.60)
   Asset: Web Server (WS-S03)
   Team Responsible: System Administration Team (IT)
   Estimated Timeline: 1 week
   Mitigation: Upgrade to Apache 2.4.61 or later.

3. **Vulnerability**: Outdated version of OpenSSL (1.1.1 < 1.1.1za)
   Asset: Web Server (WS-S03)
   Team Responsible: System Administration Team (IT)
   Estimated Timeline: 1 week
   Mitigation: Upgrade to OpenSSL 1.1.1za or later.

4. **Vulnerability**: smb-vuln-ms08-067 (CVE-2008-4250)
   Asset: Workstation (PC-98)
   Team Responsible: System Administration Team (IT)

Estimated Timeline: 1 week

Mitigation: Apply the latest MS08-067 security update

5. **Vulnerability:** HTTP-SQL-injection with possible queries

   Asset: Web Server (WS-S03)

   Team Responsible: System Administration Team (IT)

   Estimated Timeline: 1 week

   Mitigation: Implement input validation and parameterized queries to prevent SQL injection attacks. Regularly review and sanitize user inputs

HIGH VULNERABILITIES

1. **Vulnerability**: Missing or misconfigured registry keys (WinVerifyTrust Signature Validation Mitigation)

   Asset: Domain controller (DC-05)

   Team Responsible: System Administration Team (IT)

   Estimated Timeline: 2 weeks

   Mitigation:

   Add and enable registry value EnableCertPaddingCheck:

   - HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck

   Add and enable registry value EnableCertPaddingCheck on 64 Bit OS systems:

   - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck

2. **Vulnerability**: Missing security updates for Microsoft .NET Framework

   Asset: Domain controller (DC-05)

   Team Responsible: System Administration Team (IT)

   Estimated Timeline: 2 weeks

   Mitigation: Apply the latest security updates

3. **Vulnerability**: Microsoft Edge (Chromium) with Multiple Vulnerabilities

   Asset: Domain controller (DC-05)

   Team Responsible: System Administration Team (IT)

Estimated Timeline: 2 weeks
Mitigation: Upgrade to Microsoft Edge version 126.0.2592.56 or later.

4. **Vulnerability**: VMware Tools Authentication Bypass and VMware Tools Token Bypass
   Asset: Domain controller (DC-05)
   Team Responsible: System Administration Team (IT)
   Estimated Timeline: 2 weeks
   Mitigation: Upgrade to VMware Tools version 12.3.0 or later.

5. **Vulnerability:** Windows Defender Anti-malware/Antivirus Signature Definition Check
   Asset: Domain controller (DC-05)
   Team Responsible: System Administration Team (IT)
   Estimated Timeline: 2 weeks
   Mitigation: Trigger an update manually.

6. **Vulnerability**: Splunk Enterprise 9.0.0 with multiple vulnerabilities
   Asset: Workstation (PC-98)
   Team Responsible: System Administration Team (IT)
   Estimated Timeline: 2 weeks
   Mitigation: Upgrade Splunk Enterprise to versions 9.2.2, 9.1.5, and 9.0.10, or higher

MEDIUM VULNERABILITIES

6. **Vulnerability**: SMB Signing not required
   Asset: Workstation (PC-98)
   Team Responsible: System Administration Team (IT)
   Estimated Timeline:30 days
   Mitigation: Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

7. **Vulnerability**: SSL Certificate Cannot Be Trusted /SSL Self-Signed Certificate
   Asset: Workstation (PC-98)
   Team Responsible: System Administration Team (IT)
   Estimated Timeline: 30 days
   Mitigation: Purchase or generate a proper SSL certificate issued by a trusted Certificate Authority for this service.

8. **Vulnerability**: HTTP TRACE / TRACK Methods Allowed
   Asset: Web Server (WS-S03)
   Team Responsible: System Administration Team (IT)
   Estimated Timeline: 30 days
   Mitigation: Disable TRACE and TRACK methods on the web server.

6. **Vulnerability**: PHP file inclusion vulnerability (CVE-2005-3299)
   Asset: Router (R-005)
   Team Responsible: System Administration Team (IT)
   Estimated Timeline: 15-30 days
   Mitigation: Apply the latest security patches to PHP and ensure secure coding practices are in place to prevent inclusion vulnerabilities.

7. **Vulnerability:** Slowloris DOS attack (CVE-2007-6750)
   Asset: Router (R-005)
   Team Responsible: System Administration Team (IT)
   Estimated Timeline: 15-30 days
   Mitigation: Trigger an update manually.

5.2 LONG-TERM ACTIONS

1. **Patch Management**: Implement a robust patch management process to ensure all security updates are applied promptly.
2. **Automated Vulnerability Scanning:** Use automated vulnerability scanning tools to continuously monitor and identify any new vulnerabilities on network assets especially those that store sensitive data.

3. **Access Control Policies**: Review and update access controls to ensure that only authorized users have access to sensitive data and systems. Implement multi-factor authentication (MFA) where applicable.
4. **Security Awareness Training**: Provide ongoing training to administrators on the latest security threats and best practices for managing domain controllers.
5. **Web Application Firewall (WAF):** Deploy a WAF to protect against SQL injection attacks and other web application vulnerabilities.
6. **SSL/TLS Management**: Implement strong SSL/TLS configurations and regularly review cryptographic settings.
7. **Regular Assessments**: Conduct regular configuration audits to ensure the network device settings adhere to security best practices and also, regular vulnerability assessments to continuously monitor and address new security threats.
8. **Code Review and Security Testing**: Conduct regular code reviews and security testing to identify and mitigate vulnerabilities in web applications.
9. **Endpoint Protection**: Deploy advanced endpoint protection solutions to detect and prevent malware and other threats.
10. **Network Segmentation**: Use network segmentation to isolate workstations and limit the spread of malware or attacks.
11. **Intrusion Detection and Prevention**: Deploy IDS/IPS to detect and mitigate potential attacks, such as Slowloris and PHP file inclusion vulnerabilities.
12. **Security Awareness Training:** Provide regular security awareness training to employees to educate them on best practices and the importance of maintaining a secure environment.
13. **Incident Response Planning:** Develop and maintain an incident response plan to ensure a quick and effective response to security incidents. This plan should include procedures for detection, containment, eradication, and recovery.
14. **Backup and Disaster Recovery**: Implement robust backup and disaster recovery solutions to ensure data integrity and availability. Regularly test backup and recovery procedures to ensure they function as expected in the event of an incident.
15. **Assess Unused and Unknown Ports**: Regularly review and close any unnecessary open ports or services to minimize the attack surface.

6.0 LIMITATIONS

1. **False Positives and Negatives:**
   - **False Positives:** The assessment may identify vulnerabilities that do not actually exist, leading to unnecessary remediation efforts and resource allocation.
   - **False Negatives:** Some vulnerabilities may not be detected by the tools used, leaving certain risks unaddressed.
2. **Scope of Tools Used:**
   - **Tool Limitations:** Tools like Nessus and Nmap have their own limitations and may not detect all types of vulnerabilities. They might miss specific or zero-day vulnerabilities.
   - **Tool Configuration:** Improper configuration of scanning tools can result in incomplete or inaccurate vulnerability data.
3. **Environmental Constraints:**
   - **Network Changes:** The network environment may change between the time of the scan and the implementation of remediation measures, potentially introducing new vulnerabilities.
   - **Dynamic Systems:** Highly dynamic environments, such as those with frequent changes to infrastructure or software, can make it difficult to maintain an accurate vulnerability assessment.
4. **Incomplete Asset Inventory:**
   - **Asset Discovery:** If the assessment does not include a comprehensive inventory of all assets, some systems might be overlooked, leaving parts of the network unprotected.
   - **Shadow IT:** Unauthorized or unmanaged devices and applications (shadow IT) may not be detected, posing hidden risks.

5. **Resource Constraints:**
    - **Time and Personnel:** The assessment may be limited by the availability of time and skilled personnel to conduct thorough scans and analyses.
    - **Financial Resources:** Budget constraints can limit the tools and technologies available for a comprehensive assessment.
6. **Interdependency and Complexity:**
    - **System Interdependencies:** Complex interdependencies between systems can make it difficult to accurately assess the impact of vulnerabilities and prioritize remediation efforts.
    - **Complex Configurations:** Advanced configurations and custom applications might not be fully understood or scanned effectively by automated tools.
7. **Focus on Known Vulnerabilities:**
    - **Zero-Day Vulnerabilities:** The assessment primarily focuses on known vulnerabilities and may not account for zero-day vulnerabilities that have not yet been disclosed or patched.
    - **Emerging Threats:** Rapidly evolving threat landscapes mean new vulnerabilities and attack vectors may arise after the assessment is completed.
8. **Assessment Frequency:**
    - **Point-in-Time Assessment:** The vulnerability assessment represents a snapshot in time and does not continuously monitor for new vulnerabilities.
    - **Regular Updates Needed:** Continuous monitoring and regular reassessments are necessary to maintain an up-to-date security posture.
9. **Human Factors:**
    - **Skill Levels:** The effectiveness of the assessment can be influenced by the skill and experience of the personnel conducting the scans and interpreting the results.

- **Human Error:** Misconfigurations, oversights, and errors in the assessment process can lead to incomplete or inaccurate results.

10. **Remediation Challenges:**
    - **Implementation Gaps:** Identified vulnerabilities may not be remediated effectively due to gaps in implementation or follow-up.
    - **Operational Impact:** Remediation measures might have operational impacts, leading to resistance from stakeholders who prioritize uptime and performance over security.

7.0 CONCLUSION

The vulnerability assessment has provided valuable insights into the current security posture of SansydTech. By addressing the identified vulnerabilities and implementing the recommended actions, the organization can significantly reduce its risk of cyberattacks and enhance its overall security. Regular assessments and proactive security measures are essential to maintaining a robust defence against evolving threats.

8.0 REFERENCES

1. https://support.microsoft.com/help/5040437
2. https://www.cve.org/
3. https://msrc.microsoft.com/update-guide/vulnerability
4. https://advisory.splunk.com/advisories
5. https://www.vmware.com/security/advisories
6. https://www.itu.int/rec/T-REC-X.509/en http://www.nessus.org/
7. http://www.apacheweek.com/issues/03-01-24
8. https://download.oracle.com/sunalerts/1000718.1.html
9. https://en.wikipedia.org/wiki/X.509
10. https://nvd.nist.gov/
11. https://www.exploit-db.com/