Network VAPT

BY

CyberSapiens United LLP

Report on [redacted]

CyberSapiens
THE CYBER SECURITY EXPERTS

Table of Contents

1. Document Attributes

Date	**21-02-2023**
Version	**3.0**
Prepared by	[redacted]
Reviewed by	[redacted]
Approved by	[redacted]
Submitted to	[redacted]

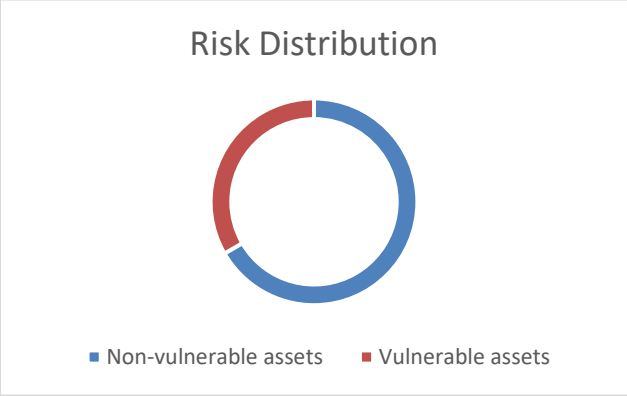
2. Executive Summary

CyberSapiens was contracted by [redacted] to conduct a network vulnerability assessment to determine its exposure to the targeted attacks and ensure that [redacted] network is secure from advanced attack techniques.
This activity was conducted in a manner that malicious attacker is engaged to assess the provided scope of [redacted]. The goals of the vulnerability assessment and Penetration Testing scan were:

- Identifying the threats or vulnerabilities that might be present on the organizations network
- Confidentiality of the [redacted] data that are stored on the company storage/servers

3. VAPT Test Graph

Type	Count
Non-Vulnerable assets	6
Vulnerable assets	3



4. AUDITING SCOPE

Detailed list of assets is given in the below table.

SL NO	IP	Type of Asset	Internal/External
1	[redacted]	Internal Server	Internal
2	[redacted]	Internal Server	Internal
3	[redacted]	Internal Server	Internal
4	[redacted]	Internal Server	Internal
5	[redacted]	Host	External
6	[redacted]	Host	External
7	[redacted]	Host	External
8	[redacted]	Host	External
9	[redacted]	Host	External

5. Methodologies and Standards

The following methodologies and standards were used during the project.

- OWASP testing guide
- PTES
- NIST Guidelines
- CIS benchmarks

6. VAPT Project Timeframe

The VAPT activity was conducted between **23-01-2023 to 16-02-2023**

7. Risk Ratings and Threat Level

Severity	Description
Critical	Loss of business / Breach of internal data / Non-bearable financial and reputational loss / Breakdown of assets / Access and modification of critical data
High	Loss of customer / Exposure of internal data / Noncompliance to regulations / Unavailability of the services / Access to configurational changes / High financial and reputational loss / Access and modification of internal data
Medium	Customer service affected for one day / Noncompliance with internal requirements / Bearable financial and reputational loss / Disclosure of non-public data
Low	Internal services affected / Minor inconvenience to customers / Very minimal financial and reputation loss

8. Vulnerability Summary

A summary of vulnerabilities that have been discovered while performing web application security assessment are given bellow:

Critical 0	**High 0**	**Medium 3**
Low 1	**Info 0**	**Total 4**

9. Observations

Vulnerability #1	SMB null/anonymous login
IP Address	[redacted]
Port	[redacted]
Risk	**Medium**
Description	SMB anonymous login is enabled on the server.

Impact	Attacker can successfully login to SMB shares and access the sensitive information containing in local shares.
CVE	CVE-1999-0519
Proof of Concept (POC)	
Remediation	• Disable SMB null/anonymous login

Vulnerability #2	SMB null/anonymous login
IP Address	[redacted]
Port	[redacted]
Risk	**Medium**
Description	SMB anonymous login is enabled on the server.
Impact	Attacker can successfully login to SMB shares and access the sensitive information containing in local shares.
CVE	CVE-1999-0519
Proof of Concept (POC)	
Remediation	• Disable SMB null/anonymous login

Vulnerability #3	SMB null/anonymous login
IP Address	[redacted]
Port	[redacted]
Risk	**Medium**
Description	SMB anonymous login is enabled on the server.

Impact	Attacker can successfully login to SMB shares and access the sensitive information containing in local shares.
CVE	CVE-1999-0519
Proof of Concept (POC)	
Remediation	Disable SMB null/anonymous login

Vulnerability #4	RDP Information Disclosure
IP Address	[redacted]
Port	[redacted]
Risk	**Low**
Description	RDP service discloses the host system information.
Impact	Attacker can use the information's disclosed for brute-forcing other open services which will lead to access control.
CVE	CVE-2022-22015
Proof of Concept (POC)	
Remediation	• Enable RDP only when the service is required. • Impose strong & regular change in passwords.

10.Tools used for the Assessment

The VAPT activities utilizes many automated tools and manual exploitation methodologies to identify security vulnerabilities. A detailed list of tools used is given below.

Tool Name	Description
nmap	Nmap is an open source utility for network exploration and security auditing.

Kali Linux	Open-source security testing toolkit to identify and exploit security issues.
Additional tools	Smbclient, Telnet, Shodan, Hydra etc

11.Conclusion

With the overall testing performed, the Network seems to working perfectly and is secure. However, we have noted a few observations/vulnerabilities that needs to be taken into consideration on priority for fixing them.