November 18, 2023

Vulnerability Scan
Report

prepared by

HostedScan Security

hostedscan.com

Overview

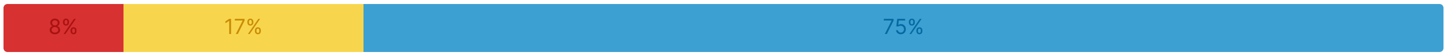
1 Executive Summary

Vulnerability scans were conducted on selected servers, networks, websites, and applications. This report contains the discovered potential risks from these scans. Risks have been classified into categories according to the level of threat and degree of potential harm they may pose.

1.1 Total Risks

Below is the total number of risks found by severity. High risks are the most severe and should be evaluated first. An accepted risk is one which has been manually reviewed and classified as acceptable to not fix at this time, such as a false positive or an intentional part of the system's architecture.

Critical	High	Medium	Low	Accepted
1	0	2	9	0



1.2 Report Coverage

This report includes findings for **4 targets** that were scanned. Each target is a single URL, IP address, or fully qualified domain name (FQDN).

Vulnerability Categories

0	Active Web Application Vulnerabilities
0	Passive Web Application Vulnerabilities
4	Network Vulnerabilities
0	SSL/TLS Security
8	Open TCP Ports
0	Open UDP Ports

2 Risks By Target

This section contains the vulnerability findings for each target that was scanned. Prioritize the most vulnerable assets first.

2.1 Targets Summary

The total number of risks found for each target, by severity.

Target	🔴 Critical	🟠 High	🟡 Medium	🔵 Low	🟢 Accepted
🔴 https://bhrnetwrk.com	1	0	1	5	0
🟡 https://bhrnetwrk.com/	0	0	1	2	0
🔵 www.stytchastory.com	0	0	0	2	0
🟢 122.176.123.159	0	0	0	0	0

2.2 Target Breakdowns

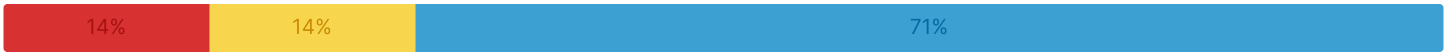
The risks discovered for each target.

Target

https://bhrnetwrk.com

Total Risks

1	0	1	5	0



Network Vulnerabilities	Threat Level	First Detected
TCP Timestamps Information Disclosure cvss score: 2.6	● Low	0 days ago
Weak MAC Algorithm(s) Supported (SSH) cvss score: 2.6	● Low	0 days ago
Operating System (OS) End of Life (EOL) Detection cvss score: 10.0	● Critical	0 days ago
ICMP Timestamp Reply Information Disclosure cvss score: 2.1	● Low	0 days ago

Open TCP Ports	Threat Level	First Detected
Open TCP Port: 22	● Medium	0 days ago
Open TCP Port: 443	● Low	0 days ago
Open TCP Port: 80	● Low	0 days ago

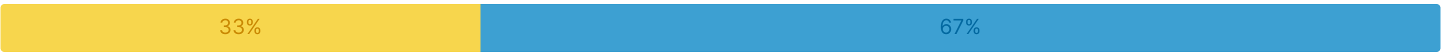
●

Target

https://bhrnetwrk.com/

Total Risks

0	0	1	2	0



Open TCP Ports	Threat Level	First Detected
Open TCP Port: 22	● Medium	0 days ago
Open TCP Port: 443	● Low	0 days ago
Open TCP Port: 80	● Low	0 days ago

Target

www.stytchastory.com

Total Risks

0	0	0	2	0

100%

Open TCP Ports	Threat Level	First Detected
Open TCP Port: 443	● Low	0 days ago
Open TCP Port: 80	● Low	0 days ago

●

Target

122.176.123.159

Total Risks

0	0	0	0	0

No risks found.

3 Active Web Application Vulnerabilities

The OWASP ZAP active web application scan crawls the pages of a web application. It scans for all of the passive scan checks and additionally makes requests and submits forms to actively test an application for even more vulnerabilities. The active scan checks for vulnerabilities such as SQL injection, remote command execution, XSS, and more.

3.1 Total Risks

Total number of risks found by severity.

Critical	High	Medium	Low	Accepted
0	0	0	0	0

3.2 Risks Breakdown

Summary list of all detected risks.

Title	Threat Level	Open	Accepted
No risks detected			

4 Passive Web Application Vulnerabilities

The OWASP ZAP passive web application scan crawls the pages of a web application. It inspects the web pages as well as the requests and responses sent between the server. The passive scan checks for vulnerabilities such as cross-domain misconfigurations, insecure cookies, vulnerable js dependencies, and more.

4.1 Total Risks

Total number of risks found by severity.

Critical	High	Medium	Low	Accepted
0	0	0	0	0

4.2 Risks Breakdown

Summary list of all detected risks.

Title	Threat Level	Open	Accepted
No risks detected			

5 SSL/TLS Security

The SSLyze security scan checks for misconfigured SSL/TLS certificates, expired certificates, weak ciphers, and SSL/TLS vulnerabilities such as Heartbleed.

5.1 Total Risks

Total number of risks found by severity.

Critical	High	Medium	Low	Accepted
0	0	0	0	0

5.2 Risks Breakdown

Summary list of all detected risks.

Title	Threat Level	Open	Accepted
No risks detected			

6 Network Vulnerabilities

The OpenVAS network vulnerability scan tests servers and internet connected devices for over 50,000 vulnerabilities. OpenVAS uses the Common Vulnerability Scoring System (CVSS) to quantify the severity of findings. 0.0 is the lowest severity and 10.0 is the highest.

6.1 Total Risks

Total number of risks found by severity.

Critical	High	Medium	Low	Accepted
1	0	0	3	0

6.2 Risks Breakdown

Summary list of all detected risks.

Title	Threat Level	CVSS Score	Open	Accepted
TCP Timestamps Information Disclosure	● Low	2.6	1	0
Weak MAC Algorithm(s) Supported (SSH)	● Low	2.6	1	0
Operating System (OS) End of Life (EOL) Detection	● Critical	10.0	1	0
ICMP Timestamp Reply Information Disclosure	● Low	2.1	1	0

6.3 Full Risk Details

Detailed information about each risk found by the scan.

TCP Timestamps Information Disclosure

● Low

cvss score: 2.6

Description

The remote host implements TCP timestamps and therefore allows to compute the uptime.

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps

References

https://datatracker.ietf.org/doc/html/rfc1323
https://datatracker.ietf.org/doc/html/rfc7323
https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

Vulnerable Target	First Detected
https://bhrnetwrk.com	0 days ago

Weak MAC Algorithm(s) Supported (SSH)

● Low

cvss score: 2.6

Description

The remote SSH server is configured to allow / support weak MAC algorithm(s).

Solution

Disable the reported weak MAC algorithm(s).

References

https://www.rfc-editor.org/rfc/rfc6668
https://www.rfc-editor.org/rfc/rfc4253#section-6.4

Vulnerable Target	First Detected
https://bhrnetwrk.com	0 days ago

Operating System (OS) End of Life (EOL) Detection

● Critical

cvss score: 10.0

Description

The Operating System (OS) on the remote host has reached the End of Life (EOL) and should not be used anymore.

An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution

Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

Vulnerable Target	First Detected
https://bhrnetwrk.com	0 days ago

ICMP Timestamp Reply Information Disclosure

● Low

cvss score: 2.1

Description

The remote host responded to an ICMP timestamp request.

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely

- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

References

CVE-1999-0524
https://datatracker.ietf.org/doc/html/rfc792
https://datatracker.ietf.org/doc/html/rfc2780

Vulnerable Target	First Detected
https://bhrnetwrk.com	0 days ago

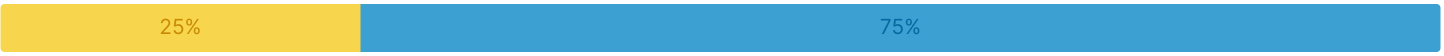
7 Open TCP Ports

The NMAP TCP port scan discovers open TCP ports with a complete scan of ports 0 to 65535.

7.1 Total Risks

Total number of risks found by severity.

Critical	High	Medium	Low	Accepted
0	0	2	6	0



7.2 Risks Breakdown

Summary list of all detected risks.

Title	Threat Level	Open	Accepted
Open TCP Port: 22	● Medium	2	0
Open TCP Port: 443	● Low	3	0
Open TCP Port: 80	● Low	3	0

7.3 Full Risk Details

Detailed information about each risk found by the scan.

Open TCP Port: 22

● Medium

Description

An open port may be an expected configuration. For example, web servers use port 80 to serve websites over http and port 443 to serve websites over https. For a list of commonly used ports see https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.

An unexpected open port could give unintended access to applications, data, and private networks. Open ports can also be dangerous when expected services are out of date and exploited through security vulnerabilities.

Vulnerable Target	First Detected
https://bhrnetwrk.com	0 days ago
https://bhrnetwrk.com/	0 days ago

Open TCP Port: 443

● Low

Description

An open port may be an expected configuration. For example, web servers use port 80 to serve websites over http and port 443 to serve websites over https. For a list of commonly used ports see https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.

An unexpected open port could give unintended access to applications, data, and private networks. Open ports can also be dangerous when expected services are out of date and exploited through security vulnerabilities.

Vulnerable Target	First Detected
www.stytchastory.com	0 days ago
https://bhrnetwrk.com	0 days ago
https://bhrnetwrk.com/	0 days ago

Open TCP Port: 80

● Low

Description

An open port may be an expected configuration. For example, web servers use port 80 to serve websites over http and port 443 to serve websites over https. For a list of commonly used ports see https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.

An unexpected open port could give unintended access to applications, data, and private networks. Open ports can also be dangerous when expected services are out of date and exploited through security vulnerabilities.

Vulnerable Target	First Detected
www.stytchastory.com	0 days ago
https://bhrnetwrk.com	0 days ago
https://bhrnetwrk.com/	0 days ago

8 Open UDP Ports

The NMAP UDP port scan discovers open ports of common UDP services

8.1 Total Risks

Total number of risks found by severity.

Critical	High	Medium	Low	Accepted
0	0	0	0	0

8.2 Risks Breakdown

Summary list of all detected risks.

Title	Threat Level	Open	Accepted
No risks detected			

9 Glossary

Accepted Risk

An accepted risk is one which has been manually reviewed and classified as acceptable to not fix at this time, such as a false positive or an intentional part of the system's architecture.

Active Web Application Vulnerabilities

The OWASP ZAP active web application scan crawls the pages of a web application. It scans for all of the passive scan checks and additionally makes requests and submits forms to actively test an application for even more vulnerabilities. The active scan checks for vulnerabilities such as SQL injection, remote command execution, XSS, and more.

Fully Qualified Domain Name (FQDN)

A fully qualified domain name is a complete domain name for a specific website or service on the internet. This includes not only the website or service name, but also the top-level domain name, such as .com, .org, .net, etc. For example, 'www.example.com' is an FQDN.

Passive Web Application Vulnerabilities

The OWASP ZAP passive web application scan crawls the pages of a web application. It inspects the web pages as well as the requests and responses sent between the server. The passive scan checks for vulnerabilities such as cross-domain misconfigurations, insecure cookies, vulnerable js dependencies, and more.

Network Vulnerabilities

The OpenVAS network vulnerability scan tests servers and internet connected devices for over 50,000 vulnerabilities. OpenVAS uses the Common Vulnerability Scoring System (CVSS) to quantify the severity of findings. 0.0 is the lowest severity and 10.0 is the highest.

Open TCP Ports

The NMAP TCP port scan discovers open TCP ports with a complete scan of ports 0 to 65535.

Open UDP Ports

The NMAP UDP port scan discovers open ports of common UDP services

Risk

A risk is a finding from a vulnerability scan. Each risk is a potential security issue that needs review. Risks are assigned a threat level which represents the potential severity.

SSL/TLS Security

The SSLyze security scan checks for misconfigured SSL/TLS certificates, expired certificates, weak ciphers, and SSL/TLS vulnerabilities such as Heartbleed.

Target

A target represents target is a single URL, IP address, or fully qualified domain name (FQDN) that was scanned.

Threat Level

The threat level represents the estimated potential severity of a particular risk. Threat level is divided into 4 categories: High, Medium, Low and Accepted.

Threat Level

The threat level represents the estimated potential severity of a particular risk. Threat level is divided into 5 categories: Critical, High, Medium, Low and Accepted.

CVSS Score

The CVSS 3.0 score is a global standard for evaluating vulnerabilities with a 0 to 10 scale. CVSS maps to threat levels: 0.1 - 3.9 = Low, 4.0 - 6.9 = Medium, 7.0 - 8.9 = High, 9.0 - 10.0 = Critical

This report was prepared using

HostedScan Security ®

For more information, visit **hostedscan.com**

Founded in Seattle, Washington in 2019, HostedScan, LLC. is dedicated to making continuous vulnerability scanning and risk management much more easily accessible to more businesses.

HostedScan, LLC.

2212 Queen Anne Ave N
Suite #521
Seattle, WA 98109

Terms & Policies
hello@hostedscan.com