

**SmartIntern Long Term Virtual Internship**  
**on**

**“Network Vulnerability Assessment”**

**An Internship Report submitted in partial fulfillment of the requirements for the award of  
degree of**

**BACHELOR OF TECHNOLOGY**

**In**

**ELECTRONICS AND COMMUNICATION ENGINEERING**

**Submitted by:**

**Team id: LTVIP2023TMID06316**

**Team Leader : S. Murali Mohan**

**Team Member : M. Vamsi**

**Team Member : N. Ramesh**

**Team Member : S. Keerthi**

**Team Member : S. Sajjad**

*Under the guidance of*

**Dr. P. Ajay Kumar Reddy Sir**



**DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING**

**KUPPAM ENGINEERING COLLEGE**

**ANDHRA PRADESH 517425**



**Approved by AICTE, New Delhi, affiliated to JNTU, Anantapur**

**Accredited by NBA & Certified by ISO 9001:2008**

**Recognition of UGC under 2(f) & 12(B)**



## **PART 1: EXECUTIVE SUMMARY**

### **Executive Summary: Altoro Mutual Website Network Vulnerability Assessment**

The Altoro Mutual Website Network Vulnerability Assessment was conducted between July 27, 2023, and August 02, 2023, to evaluate the security posture of the Altoro Mutual website's network infrastructure. The primary objective of this assessment was to identify potential vulnerabilities and weaknesses within the network that could pose a threat to the website's integrity, confidentiality, and availability.

Using a combination of manual analysis and automated scanning tools, the assessment aimed to detect vulnerabilities that could be exploited by malicious actors to gain unauthorized access or compromise the website's sensitive data. Rigorous testing was performed, taking into account various attack vectors and techniques commonly used by hackers.

The assessment revealed several findings regarding the website's network security. Multiple high-severity vulnerabilities were detected, including unpatched software, open ports with inadequate security controls, and weaknesses in the password policy implementation. These critical issues exposed the website to potential cyberattacks, data breaches, and service disruptions.

To address the identified vulnerabilities, a set of comprehensive recommendations has been provided. Altoro Mutual can significantly enhance the security of its website's network infrastructure, mitigate potential vulnerabilities, and fortify its defense against cyber threats. Regular follow-up assessments are encouraged to ensure continuous improvement in network security.

## **Overview**

### **Overview: Network Vulnerability Assessment on Altoro Mutual**

The Network Vulnerability Assessment on Altoro Mutual is a comprehensive evaluation of the organization's network infrastructure to identify potential security weaknesses and vulnerabilities. Altoro Mutual is a financial services company that handles sensitive data, making it imperative to maintain a robust and secure network environment. This assessment aims to identify and address security gaps that could expose the company to cyber threats, data breaches, and financial losses.

The primary objectives of the Network Vulnerability Assessment on Altoro Mutual are as follows:

1. **Identify Vulnerabilities:** The assessment aims to identify potential vulnerabilities in the network infrastructure, including unpatched software, misconfigurations, and open ports.
2. **Evaluate Security Controls:** The effectiveness of existing security controls, such as firewalls, intrusion detection systems (IDS), and access controls, is assessed to determine their ability to detect and prevent attacks.
3. **Assess Network Architecture:** The network architecture is reviewed to ensure proper segmentation, isolation of critical assets, and a robust perimeter defense.
4. **Password Policy Evaluation:** The assessment examines the strength of password policies and their adherence to industry best practices to prevent unauthorized access.
5. **Physical Security Analysis:** Physical security measures in place to protect network infrastructure and data centers are evaluated to prevent unauthorized physical access.

## **Methodology:**

The assessment follows a well-defined methodology, including the following steps

1. **Reconnaissance:** Passive reconnaissance techniques are used to gather information about the network and its assets.
2. **Vulnerability Scanning:** Automated scanning tools are employed to identify potential vulnerabilities in the network.
3. **Manual Verification:** The identified vulnerabilities are manually verified to eliminate false positives and prioritize critical issues.
4. **Exploitation (with Authorization):** Ethical exploitation of vulnerabilities is conducted to determine the extent of potential damage if exploited maliciously.
5. **Analysis and Reporting:** The assessment findings are analyzed, and a detailed report is generated, including a list of vulnerabilities, risk severity, and actionable recommendations.

## **Deliverables:**

The assessment will provide the following deliverables:

1. **Network Vulnerability Assessment Report:** A comprehensive report detailing the assessment methodology, findings, risk analysis, and actionable recommendations.
2. **Executive Summary:** A concise summary highlighting key findings and critical vulnerabilities for executive stakeholders.
3. **Remediation Plan:** A roadmap outlining the prioritized actions required to address identified vulnerabilities and improve network security.

## **Part 2 : Detail Report**

### **Information Gathering:**

Information gathering is a crucial phase in the cybersecurity and assessment process. It involves collecting relevant data and intelligence about a target system, network, or organization to understand its vulnerabilities and potential attack surfaces. Here are different aspects of information gathering:

#### **1. Email Footprint Analysis:**

Email footprint analysis involves collecting information related to an organization's email infrastructure, such as email addresses, email servers, and email security measures. This analysis helps in understanding how email communications are handled and identifying potential points of entry for attackers.

#### **2. DNS Information Gathering:**

DNS (Domain Name System) information gathering involves querying and analyzing DNS records to gather details about domain names, IP addresses, mail exchange servers, and other crucial information. It helps in understanding the network structure and identifying potential targets for cyberattacks.

#### **3. WHOIS Information Gathering:**

WHOIS information gathering involves querying the WHOIS database to retrieve registration details of domain names and IP addresses. This data includes contact information of domain owners and registrars, which can be valuable for understanding the ownership and potential affiliations of a target domain.

#### **4. Information Gathering for Social Engineering Attacks:**

Social engineering attacks involve manipulating individuals into divulging sensitive information or performing specific actions. Information gathering for social engineering

attacks includes researching potential targets' online presence, interests, and connections to craft convincing and personalized attack scenarios.

#### 5. Information Gathering for Physical Security Assessments:

Physical security assessments involve gathering information about the physical premises, access controls, security measures, and personnel protocols of an organization. This assessment helps identify potential physical vulnerabilities and weaknesses in an organization's security.

#### 6. Emerging Trends and Technologies in Information Gathering:

As technology evolves, so do the methods of information gathering. Emerging trends include the use of artificial intelligence and machine learning algorithms for automated data collection and analysis, advanced OSINT (Open-Source Intelligence) tools, and social media analysis for gathering valuable intelligence.

The result of the information gathering performed on Altoro Mutual (ip: 65.61.131.117) domain name : testfire.net

#### **Email Footprint Analysis:**

**Tool used :** the Harvester

The Harvester is a powerful open-source tool used for information gathering and reconnaissance in the field of cybersecurity. It is designed to gather data from various sources, such as search engines, public databases, and social media platforms, to extract valuable information about a target organization or individual. The tool primarily focuses on harvesting email addresses, subdomains, hostnames, and other related information that can be used for further analysis or exploitation.

**Command used :** theHarvester -d testfire.net -b all

## Output:

[\*] IPs found: 3

-----

65.61.137.117

[\*] No emails found.

[\*] Hosts found: 41

-----

aloro.testfire.net:65.61.137.117

demo-analytics.testfire.net

demo.testfire.net:65.61.137.117

demo2.testfire.net:65.61.137.117

evil.testfire.net:65.61.137.117

ftp.testfire.net:65.61.137.117

ftp.testfire.net:testfire.net

http---demo.testfire.net

localhost.testfire.net:65.61.137.117

owtf.pydemo.testfire.net

srchttpdemo.testfire.net

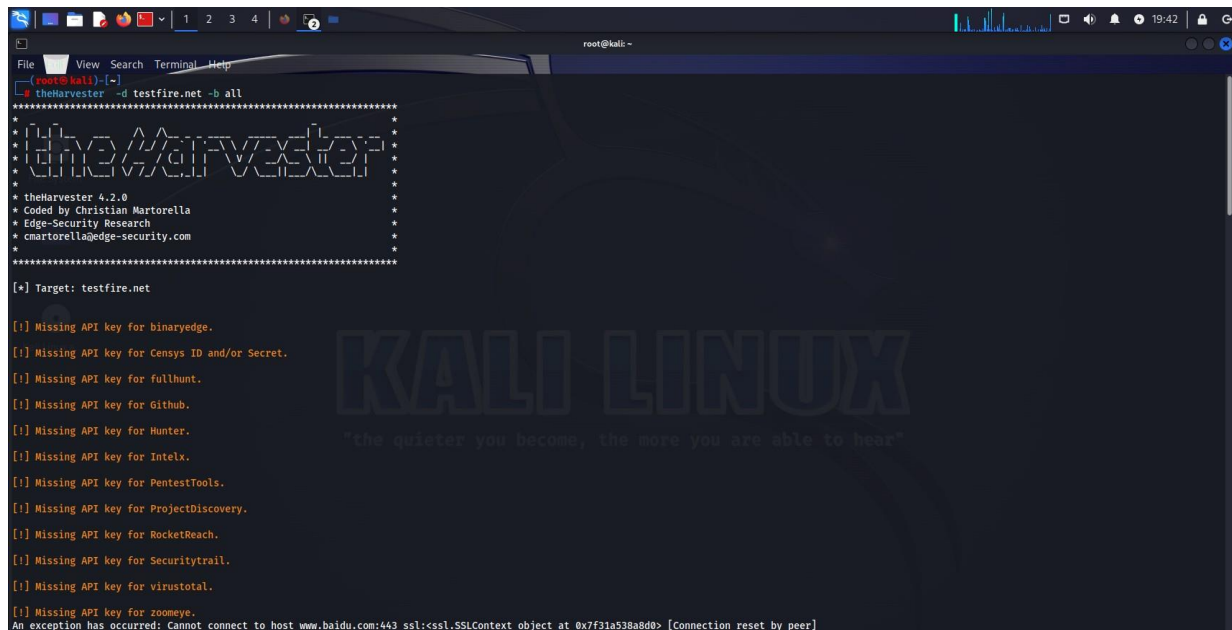
www.demo.testfire.net

www.testfire.net:testfire.net

www.testfire.net:testfire.net.

[www.testfire.net:65.61.137.117](http://www.testfire.net:65.61.137.117)

**Result :** No email found in Altoro Mutual



```
root@kali: ~
File View Search Terminal Help
root@kali:~# theHarvester -d testfire.net -b all
*****
* theHarvester 4.2.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****

[*] Target: testfire.net

[!] Missing API key for binaryedge.
[!] Missing API key for Censys ID and/or Secret.
[!] Missing API key for fullhunt.
[!] Missing API key for Github.
[!] Missing API key for Hunter.
[!] Missing API key for Intelx.
[!] Missing API key for PentestTools.
[!] Missing API key for ProjectDiscovery.
[!] Missing API key for RocketReach.
[!] Missing API key for Securitytrail.
[!] Missing API key for virustotal.
[!] Missing API key for zoomeye.
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:ssl.SSLContext object at 0x7f31a538a8d0 [Connection reset by peer]
```

```
root@kali: ~  
File View Search Terminal Help  
An exception has occurred: Cannot connect to host dns.bufferover.run:443 ssl:ssl.SSLContext object at 0x7f31a53c91c0 [Name or service not known]  
Searching 0 results.  
[*] Searching Bing.  
Searching results.  
[*] Searching Certspotter.  
[*] Searching CRTsh.  
[*] Searching Dockduckgo.  
[*] Searching Doodstream.  
[*] Searching Hackettarget.  
[*] Searching Dtx.  
[*] Searching Quant.  
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:ssl.SSLContext object at 0x7f31a53ba4e0 [Network is unreachable]  
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:ssl.SSLContext object at 0x7f31a53c8e60 [Network is unreachable]  
[*] Searching Rapidids.  
An exception has occurred: Cannot connect to host api sublist3r.com:443 ssl:ssl.SSLContext object at 0x7f31a53cb40 [Name or service not known]  
An exception has occurred: Cannot connect to host www.threatcrowd.org:443 ssl:ssl.SSLContext object at 0x7f31a53c9130 [Network is unreachable]  
string indices must be integers, not 'str'  
[*] Searching Threatcrowd.  
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:ssl.SSLContext object at 0x7f31a53b9880 [Connection reset by peer]  
[*] Searching Threatminer.  
An exception has occurred: 0, message: Attempt to decode 350W with unexpected mimetype: text/html; charset=utf-8', url=URL('https://sonar.omisint.io/all/testfire.net?page=1')  
[*] Searching Dm51ant.  
[*] Searching Urlscan.  
An exception has occurred:  
[*] Searching Baidu.  
  
[*] ASNS found: 1  
-----  
AS33078  
  
[*] Interesting Urls found: 14  
-----  
http://demo.testfire.net/  
http://demo.testfire.net/index.jsp  
http://demo.testfire.net/phishing.html  
http://testfire.net/  
http://testfire.net/reflectedorstoretargetblanklink  
http://testfire.net/user/register?element_parents=account/mail/  
http://www.testfire.net/  
https://demo.testfire.net/  
https://demo.testfire.net/api/feedback/1234.exe  
https://demo.testfire.net/index.jsp  
https://demo.testfire.net/login.jsp  
https://demo.testfire.net/search.jspx?query=K3C1frame+src%3D%22https%3A%2F%2Fwww.bt.com%2F%22+height%3D%22558px%22+width%3D%22780px%22%3EK3C2F1frame%3E  
https://testfire.net/  
https://www.testfire.net/  
  
[*] LinkedIn Links found: 0  
-----  
  
[*] IPs found: 3  
-----  
65.61.137.117
```

```
root@kali: ~  
File View Search Terminal Help  
[*] Searching Urlscan.  
An exception has occurred:  
[*] Searching Baidu.  
  
[*] ASNS found: 1  
-----  
AS33078  
  
[*] Interesting Urls found: 14  
-----  
http://demo.testfire.net/  
http://demo.testfire.net/index.jsp  
http://demo.testfire.net/phishing.html  
http://testfire.net/  
http://testfire.net/reflectedorstoretargetblanklink  
http://testfire.net/user/register?element_parents=account/mail/  
http://www.testfire.net/  
https://demo.testfire.net/  
https://demo.testfire.net/api/feedback/1234.exe  
https://demo.testfire.net/index.jsp  
https://demo.testfire.net/login.jsp  
https://demo.testfire.net/search.jspx?query=K3C1frame+src%3D%22https%3A%2F%2Fwww.bt.com%2F%22+height%3D%22558px%22+width%3D%22780px%22%3EK3C2F1frame%3E  
https://testfire.net/  
https://www.testfire.net/  
  
[*] LinkedIn Links found: 0  
-----  
  
[*] IPs found: 3  
-----  
65.61.137.117  
  
[*] No emails found.  
  
[*] Hosts found: 41  
-----  
altoro.testfire.net:65.61.137.117  
demo-analytics.testfire.net  
demo.testfire.net:65.61.137.117  
demo2.testfire.net:65.61.137.117  
evil.testfire.net:65.61.137.117  
ftp.testfire.net:65.61.137.117  
ftp.testfire.net:testfire.net  
http--demo.testfire.net  
localhost.testfire.net:65.61.137.117  
mef.pydemo.testfire.net  
sarchtpdemo.testfire.net  
www.demo.testfire.net  
www.testfire.net:testfire.net  
www.testfire.net:testfire.net  
www.testfire.net:65.61.137.117  
  
root@kali: ~
```



## DNS INFORMATION GATHERING

Website link of Altoro Mutual Dns result

<https://www.nslookup.io/domains/testfire.net/dns-records/>

The screenshot shows the nslookup.io website interface. The browser's address bar displays the URL <https://www.nslookup.io/domains/testfire.net/dns-records/>. The page title is "DNS records for testfire.net". Below the title, there are tabs for "Cloudflare", "Google DNS", "OpenDNS", "Authoritative", and "Local DNS". The "Cloudflare" tab is selected. The main content area displays the following information:

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the time to live (TTL) has not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers.

**A records**

IPv4 address	Revalidate in
65.61.137.117	24h

**AAAA records**

No AAAA records found.

**CNAME record**

No CNAME record found.

**TXT records**

**SPF record**

This record is valid for 30m.

Pass if the email sender's IP is in the MX records (with CIDR /24 for IPv4) of testfire.net.	mx/24
Or else, mark the email as fail.	-all

The screenshot shows the nslookup.io website interface, displaying the "NS records" section. The browser's address bar displays the URL <https://www.nslookup.io/domains/testfire.net/dns-records/>. The page title is "DNS records for testfire.net". Below the title, there are tabs for "Cloudflare", "Google DNS", "OpenDNS", "Authoritative", and "Local DNS". The "Cloudflare" tab is selected. The main content area displays the following information:

**NS records**

Name server	Revalidate in
usw2.akam.net	24h
eur2.akam.net	24h
ns1-99.akam.net	24h
usc3.akam.net	24h
asia3.akam.net	24h
usc2.akam.net	24h
ns1-206.akam.net	24h
eur5.akam.net	24h

**MX records**

No mail servers found.

**Other records**

SOA

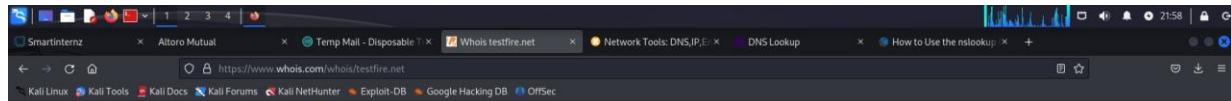
**SOA data**

Field	Value	Revalidate in
Start of authority	asia3.akam.net	24h
Email	hostmaster@akamai.com	
Serial	1366025607	
Refresh	12h	
Retry	2h	
Expire	168h	
Negative cache TTL	24h	

## WHOIS INFORMATION GATHERING

Website of whois ip result link of Altoro Mutual

<https://www.whois.com/whois/testfire.net>



**Whois**  
Identify for everyone

Enter Domain or IP **WHOIS**

**testfire.net** Updated 1 day ago

Interested in similar domains?

**Domain Information**

Domain:	testfire.net
Registrar:	CSC Corporate Domains, Inc.
Registered On:	1999-07-23
Expires On:	2024-07-23
Updated On:	2023-07-19
Status:	clientTransferProhibited
Name Servers:	asia3.akam.net eur2.akam.net eur5.akam.net ns1-206.akam.net ns1-99.akam.net usc2.akam.net usc3.akam.net usw2.akam.net

**Registrant Contact**

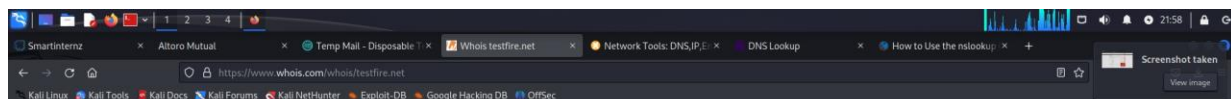
City:	Sunnyvale
State:	CA
Postal Code:	94085
Country:	US
Phone:	+Not Disclosed
Fax:	+Not Disclosed

**Similar Domains:**

- testsfire.com **Buy Now**
- testerfire.com **Buy Now**
- testfiregames.com **Buy Now**
- datatestfire.com **Buy Now**
- testsfire.net **Buy Now**
- testerfire.net **Buy Now**

**.space** Sale  
\$24.88 **\$0.88**  
**BUY NOW**  
\*while stocks last

**On Sale!**



**Registrant Contact**

City:	Sunnyvale
State:	CA
Postal Code:	94085
Country:	US
Phone:	+Not Disclosed
Fax:	+Not Disclosed

**Administrative Contact**

City:	Sunnyvale
State:	CA
Postal Code:	94085
Country:	US
Phone:	+Not Disclosed
Fax:	+Not Disclosed

**Technical Contact**

City:	Sunnyvale
State:	CA
Postal Code:	94085
Country:	US
Phone:	+Not Disclosed
Fax:	+Not Disclosed

**.space** Sale  
\$24.88 **\$0.88**  
**BUY NOW**  
\*while stocks last

**On Sale!**

**.xyz** **.XYZ @ \$2.88 \$13.88**

**Introducing**  
**WORDPRESS HOSTING**  
**\$3.58 /mo**  
**VIEW MORE**

## Domain Information

Domain: testfire.net  
Registrar: CSC Corporate Domains, Inc.  
Registered On: 1999-07-23  
Expires On: 2024-07-23  
Updated On: 2023-07-19  
Status: clientTransferProhibited  
Name Servers: asia3.akam.net  
eur2.akam.net  
eur5.akam.net  
ns1-206.akam.net  
ns1-99.akam.net  
usc2.akam.net  
usc3.akam.net  
usw2.akam.net

## Registrant Contact

City: Sunnyvale  
State: CA  
Postal Code: 94085  
Country: US  
Phone: +Not Disclosed  
Fax: +Not Disclosed

## Administrative Contact

City: Sunnyvale  
State: CA  
Postal Code: 94085  
Country: US  
Phone: +Not Disclosed  
Fax: +Not Disclosed

## Technical Contact

City: Sunnyvale  
State: CA  
Postal Code: 94085  
Country: US  
Phone: +Not Disclosed  
Fax: +Not Disclosed

## Raw Whois Data

Domain Name: testfire.net  
Registry Domain ID: 8363973\_DOMAIN\_NET-VRSN  
Registrar WHOIS Server: whois.corporatedomains.com  
Registrar URL: www.cscprotectsbrands.com  
Updated Date: 2023-07-19T01:05:02Z  
Creation Date: 1999-07-23T09:52:32Z  
Registrar Registration Expiration Date: 2024-07-23T13:52:32Z  
Registrar: CSC CORPORATE DOMAINS, INC.  
Sponsoring Registrar IANA ID: 299  
Registrar Abuse Contact Email: @cscglobal.com  
Registrar Abuse Contact Phone: +1.8887802723  
Domain Status: clientTransferProhibited <http://www.icann.org/epp#clientTransferProhibited>

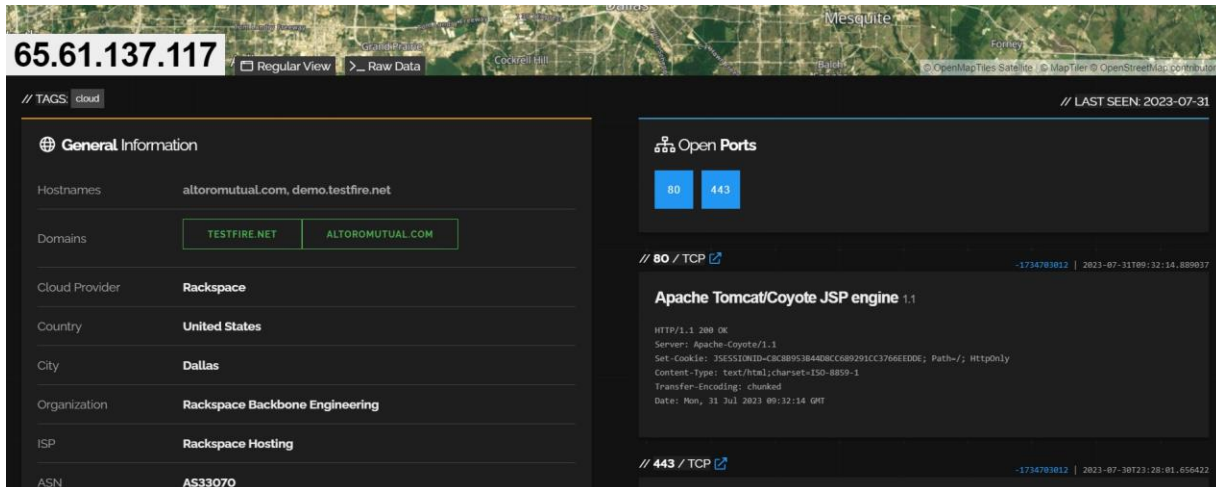
Registry Registrant ID:  
Registrant Name: Not Disclosed  
Registrant Organization: Not Disclosed  
Registrant Street: Not Disclosed  
Registrant City: Sunnyvale  
Registrant State/Province: CA  
Registrant Postal Code: 94085  
Registrant Country: US  
Registrant Phone: +Not Disclosed  
Registrant Phone Ext:  
Registrant Fax: +Not Disclosed  
Registrant Fax Ext:  
Registrant Email: Not Disclosed  
Registry Admin ID:  
Admin Name: Not Disclosed  
Admin Organization: Not Disclosed  
Admin Street: Not Disclosed  
Admin City: Sunnyvale  
Admin State/Province: CA  
Admin Postal Code: 94085  
Admin Country: US  
Admin Phone: +Not Disclosed  
Admin Phone Ext:  
Admin Fax: +Not Disclosed  
Admin Fax Ext:  
Admin Email: Not Disclosed  
Registry Tech ID:  
Tech Name: Not Disclosed  
Tech Organization: Not Disclosed  
Tech Street: Not Disclosed  
Tech City: Sunnyvale  
Tech State/Province: CA  
Tech Postal Code: 94085  
Tech Country: US  
Tech Phone: +Not Disclosed  
Tech Phone Ext:  
Tech Fax: +Not Disclosed  
Tech Fax Ext:  
Tech Email: Not Disclosed  
Name Server: ns1-99.akam.net  
Name Server: eur5.akam.net  
Name Server: eur2.akam.net  
Name Server: ns1-206.akam.net  
Name Server: usw2.akam.net  
Name Server: usc3.akam.net  
Name Server: asia3.akam.net  
Name Server: usc2.akam.net  
DNSSEC: unsigned  
URL of the ICANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/>  
Information about our bug bounty program using whois domain

## SHADON

SHODAN: Shodan is a search engine designed to find internet-connected devices and systems. It can provide information about a website's servers, open ports, and other internet-facing assets.

### Website of shodan result of Altoro Mutual

<https://www.shodan.io/host/65.61.137.117>



The screenshot displays the Shodan search results for the IP address 65.61.137.117. The interface is dark-themed and includes a map at the top showing the location of the IP in Dallas, Texas. The main content is divided into two columns. The left column, titled 'General Information', lists various details about the host, including hostnames, domains, cloud provider, country, city, organization, ISP, and ASN. The right column, titled 'Open Ports', shows the results of a port scan, highlighting the 80 and 443 ports. The 80 port is open to TCP and is associated with the Apache Tomcat/Coyote JSP engine 1.1. The 443 port is also open to TCP. The interface includes a 'Regular View' button and a 'Raw Data' button. The top right corner shows the last seen date as 2023-07-31.

General Information	
Hostnames	altoromutual.com, demo.testfire.net
Domains	TESTFIRE.NET, ALTOROMUTUAL.COM
Cloud Provider	Rackspace
Country	United States
City	Dallas
Organization	Rackspace Backbone Engineering
ISP	Rackspace Hosting
ASN	AS33070

Open Ports	
80	443

// 80 / TCP

Apache Tomcat/Coyote JSP engine 1.1

HTTP/1.1 200 OK  
Server: Apache-Coyote/1.1  
Set-Cookie: JSESSIONID=C8C8B953B4408CC689291CC3766EEDDE; Path=/; HttpOnly  
Content-Type: text/html; charset=ISO-8859-1  
Transfer-Encoding: chunked  
Date: Mon, 31 Jul 2023 09:32:14 GMT

// 443 / TCP

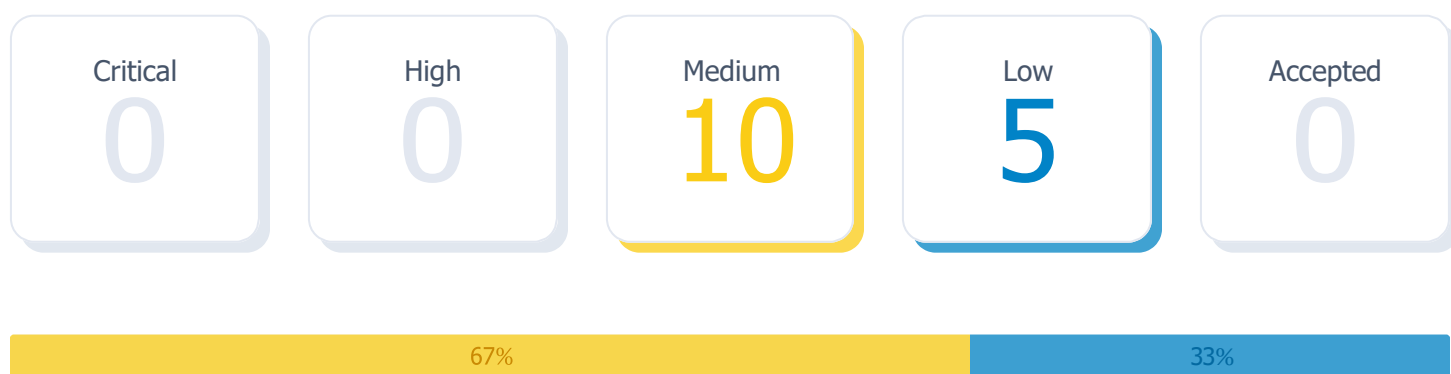
## Vulnerability Report

### 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.



#### 1.2 Report Coverage

This report includes findings for 1 target that were scanned. Each target is a single URL, IP address, or fully qualified domain name FQDN.

##### Vulnerability Categories

0

Active Web Application Vulnerabilities

6

Passive Web Application Vulnerabilities

6

Network Vulnerabilities

0

SSL/TLS Security

3

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 mostvulnerable assets first.

### 2.1 Targets Summary

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

Target	<div><div></div>Critical</div>	<div><div></div>High</div>	<div><div></div>Medium</div>	<div><div></div>Low</div>	<div><div></div>Accepted</div>
<div><div></div>http://testfire.net/</div>	0	0	10	5	0

## 2.2 Target Breakdowns

The risks discovered for each target.



Target

<http://testfire.net/>

Total Risks

0

0

10

5

0

67%

33%

### Passive Web Application Vulnerabilities

Threat Level

First Detected

Absence of Anti-CSRF Tokens

● Medium

0 days ago

Missing Anti-clickjacking Header

● Medium

0 days ago

Content Security Policy CSP Header Not Set

● Medium

0 days ago

X Content-Type-Options Header Missing

● Low

0 days ago

Cookie without SameSite Attribute

● Low

0 days ago

Server Leaks Version Information via "Server" HTTP Response Header Field

● Low

0 days ago

### Network Vulnerabilities

Threat Level

First Detected

Cleartext Transmission of Sensitive Information via HTTP

cvss score: 4.8

● Medium

0 days ago

SSL/TLS Diffie-Hellman Key Exchange Insufficient DH GroupStrength Vulnerability

cvss score: 4.0

● Medium

0 days ago

Cleartext Transmission of Sensitive Information via HTTP

cvss score: 4.8

● Medium

0 days ago

SSL/TLS Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

cvss score: 4.3

● Medium

0 days ago

TCP Timestamps Information Disclosure

cvss score: 2.6

● Low

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: 443

● Medium

0 days ago

Open TCP Port: 80

● Medium

0 days ago

Open TCP Port: 8080

● Medium

0 days ago

### 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 commandexecution, XSS, and more.

#### 3.1 Total Risks

Total number of risks found by severity.



#### 3.2 Risks Breakdown

Summary list of all detected risks.

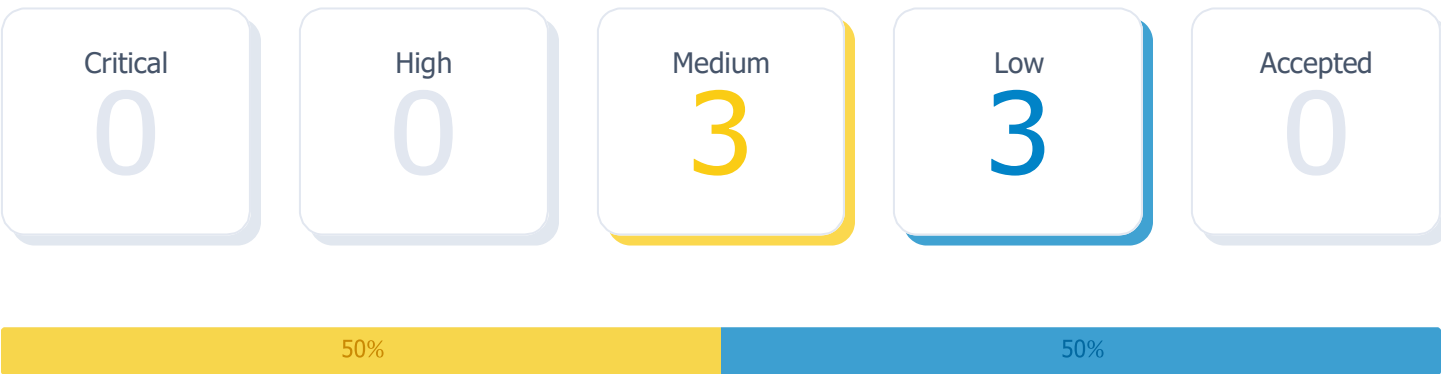
Title	Threat Level	Open	Accepted
No risks detected			

# 4 Passive Web Application Vulnerabilities

The OWASP ZAP passive web application scan crawls the pages of a web application. It inspects the webpages 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.



## 4.2 Risks Breakdown

Summary list of all detected risks.

Title	Threat Level	Open	Accepted
Absence of Anti-CSRF Tokens	● Medium	1	0
Missing Anti-clickjacking Header	● Medium	1	0
Content Security Policy CSP Header Not Set	● Medium	1	0
X Content-Type-Options Header Missing	● Low	1	0
Cookie without SameSite Attribute	● Low	1	0
Server Leaks Version Information via "Server" HTTP Response HeaderField	● Low	1	0

## 4.3 Full Risk Details

Detailed information about each risk found by the scan.

### Absence of Anti-CSRF Tokens

● Medium

#### Description

No Anti-CSRF tokens were found in a HTML submission form.

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting XSS exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.

CSRF attacks are effective in a number of situations, including:

- \* The victim has an active session on the target site.
- \* The victim is authenticated via HTTP auth on the target site.
- \* The victim is on the same local network as the target site.

CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

#### Solution

Phase: Architecture and Design

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, use anti-CSRF packages such as the OWASP CSRFGuard.

#### Implementation

Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

Phase: Architecture and Design

Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable. **CWE 330**.

Note that this can be bypassed using XSS.

Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.

Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF.

Do not use the GET method for any request that triggers a state change.

#### Implementation

Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

Instances 1 of 100)uri:

http://testfire.net/ method:

GET

evidence: <form id="frmSearch" method="get" action="/search.jsp">

otherinfo: No known Anti-CSRF token [anticsrf, CSRFToken, \_\_RequestVerificationToken, csrfmiddlewaretoken, authenticity\_token, OWASP\_CSRFTOKEN, anoncsrf, csrf\_token, \_csrf, \_csrfSecret, \_\_csrf\_magic, CSRF, \_token, \_csrf\_token, data[\_Token][key]] was found in thefollowing HTML form: Form 1 "query" ].

References

http://projects.webappsec.org/Cross-Site-Request-Forgery

http://cwe.mitre.org/data/definitions/352.html

Vulnerable Target	First Detected
<a href="http://testfire.net/">http://testfire.net/</a>	0 days ago

## Missing Anti-clickjacking Header

● Medium

### Description

The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.

### Solution

Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.

If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.

Instances 1 of 62)uri:

<http://testfire.net/> method:

GET

param: X-Frame-Options

### References

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

Vulnerable Target	First Detected
<a href="http://testfire.net/">http://testfire.net/</a>	0 days ago

## Content Security Policy CSP Header Not Set

● Medium

### Description

Content Security Policy CSP is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

### Solution

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Instances 1 of 100)uri:

http://testfire.net/ method:

GET

### References

[https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing\\_Content\\_Security\\_Policy](https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy)

[https://cheatsheetseries.owasp.org/cheatsheets/Content\\_Security\\_Policy\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html)

<http://www.w3.org/TR/CSP/>

<http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html>

<http://www.html5rocks.com/en/tutorials/security/content-security-policy/>

<http://caniuse.com/#feat=contentsecuritypolicy>

<http://content-security-policy.com/>

Vulnerable Target	First Detected
<a href="http://testfire.net/">http://testfire.net/</a>	0 days ago

## X Content-Type-Options Header Missing

● Low

### Description

The Anti-MIME Sniffing header X Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

### Solution

Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X Content-Type-Options header to 'nosniff' for all web pages.

If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

### Instances 1 of 65

uri:

http://testfire.net/ method:

GET

param: X Content-Type-Options

otherinfo: This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

### References

<http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx>

<https://owasp.org/www-community/Security-Headers>

Vulnerable Target	First Detected
<a href="http://testfire.net/">http://testfire.net/</a>	0 days ago



## Cookie without SameSite Attribute

● Low

### Description

A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

### Solution

Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

#### Instances 1 of 3) uri:

<http://testfire.net/method>:

GET

param: JSESSIONID

evidence: Set-Cookie: JSESSIONID

### References

<https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site>

#### Vulnerable Target

#### First Detected

<http://testfire.net/>

0 days ago

## Server Leaks Version Information via "Server" HTTP Response Header Field

● Low

### Description

The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

### Solution

Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Instances 1 of 100)uri:

<http://testfire.net/> method:

GET

evidence: Apache-Coyote/1.1

### References

<http://httpd.apache.org/docs/current/mod/core.html#servertokens>

[http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht\\_urlscan\\_007](http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007)

<http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx>

<http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html>

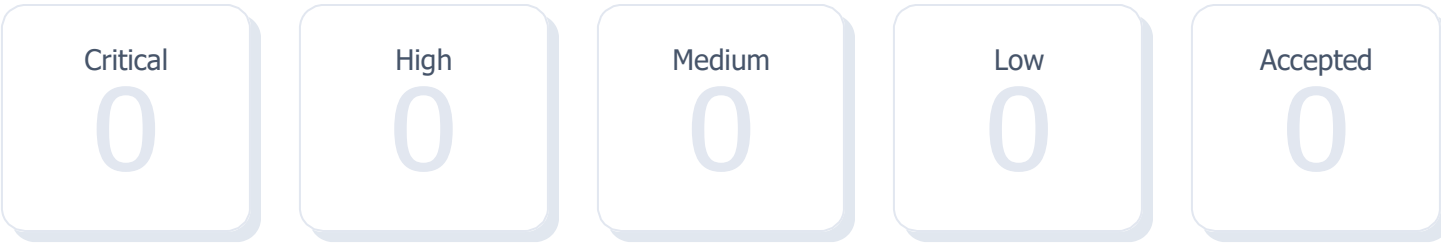
Vulnerable Target	First Detected
<a href="http://testfire.net/">http://testfire.net/</a>	0 days ago

# 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.



## 5.2 Risks Breakdown

Summary list of all detected risks.

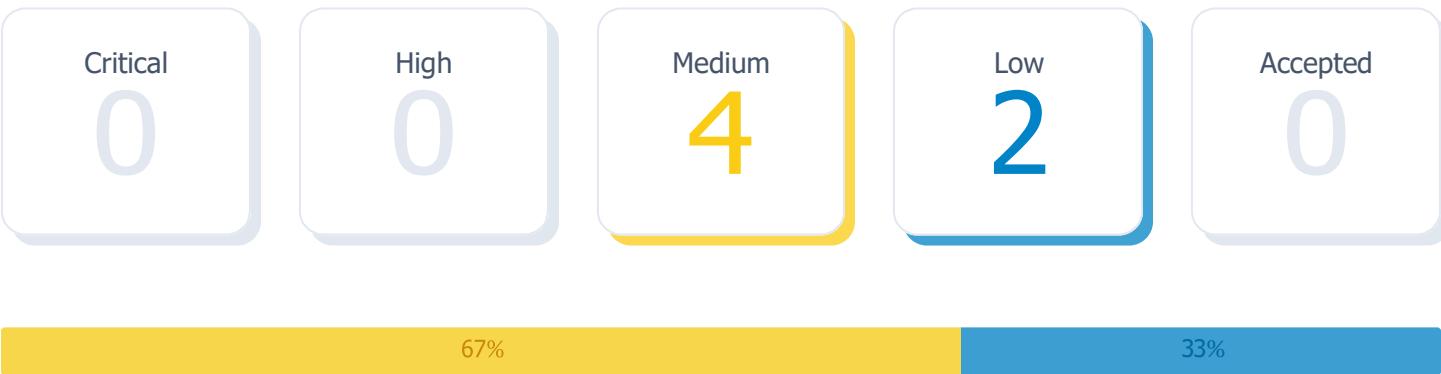
Title	Threat Level	Open	Accepted
No risks detected			

# 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.



## 6.2 Risks Breakdown

Summary list of all detected risks.

Title	Threat Level	CVSS Score	Open	Accepted
Cleartext Transmission of Sensitive Information via HTTP	● Medium	4.8	1	0
SSL/TLS Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	● Medium	4.0	1	0
Cleartext Transmission of Sensitive Information via HTTP	● Medium	4.8	1	0
SSL/TLS Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	● Medium	4.3	1	0
TCP Timestamps Information Disclosure	● Low	2.6	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.

### Cleartext Transmission of Sensitive Information via HTTP

● Medium  
cvss score: 4.8

#### Description

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

#### Solution

Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

#### References

[https://www.owasp.org/index.php/Top\\_10\\_2013\\_A2\\_Broken\\_Authentication\\_and\\_Session\\_Management](https://www.owasp.org/index.php/Top_10_2013_A2_Broken_Authentication_and_Session_Management)  
[https://www.owasp.org/index.php/Top\\_10\\_2013\\_A6\\_Sensitive\\_Data\\_Exposure](https://www.owasp.org/index.php/Top_10_2013_A6_Sensitive_Data_Exposure)  
<https://cwe.mitre.org/data/definitions/319.html>

Vulnerable Target	First Detected
<a href="http://testfire.net/">http://testfire.net/</a>	0 days ago

## SSL/TLS Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

● Medium  
cvss score: 4.0

### Description

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048 .

The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

An attacker might be able to decrypt the SSL/TLS communication offline.

### Solution

Deploy Ephemeral) Elliptic-Curve Diffie-Hellman ECDHE or use a 2048-bit or stronger Diffie-Hellman group (see thereferences).

For Apache Web Servers: Beginning with version 2.4.7, mod\_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

### References

<https://weakdh.org/>  
<https://weakdh.org/sysadmin.html>

Vulnerable Target	First Detected
<a href="http://testfire.net/">http://testfire.net/</a>	0 days ago

## Cleartext Transmission of Sensitive Information via HTTP

● Medium

cvss score: 4.8

### Description

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

### Solution

Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

### References

[https://www.owasp.org/index.php/Top\\_10\\_2013\\_A2\\_Broken\\_Authentication\\_and\\_Session\\_Management](https://www.owasp.org/index.php/Top_10_2013_A2_Broken_Authentication_and_Session_Management)

[https://www.owasp.org/index.php/Top\\_10\\_2013\\_A6\\_Sensitive\\_Data\\_Exposure](https://www.owasp.org/index.php/Top_10_2013_A6_Sensitive_Data_Exposure)

<https://cwe.mitre.org/data/definitions/319.html>

Vulnerable Target	First Detected
<a href="http://testfire.net/">http://testfire.net/</a>	0 days ago

## SSL/TLS Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

● Medium  
cvss score: 4.3

### Description

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system. The

TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:

- CVE 2011 3389 Browser Exploit Against SSL/TLS BEAST
- CVE 2015 0204 Factoring Attack on RSA EXPORT Keys Padding Oracle On Downgraded Legacy Encryption FREAK

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

### Solution

It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2 protocols. Please see the references for more information.

### References

CVE 2011 3389  
CVE 2015 0204  
<https://ssl-config.mozilla.org/> <https://bettercrypto.org/>  
<https://datatracker.ietf.org/doc/rfc8996/>  
<https://vnhacker.blogspot.com/2011/09/beast.html>  
<https://web.archive.org/web/20201108095603/https://censys.io/blog/freak>  
<https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014>

#### Vulnerable Target

#### First Detected

<http://testfire.net/>

0 days ago



## 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
<a href="http://testfire.net/">http://testfire.net/</a>	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
<a href="http://testfire.net/">http://testfire.net/</a>	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.



## 7.2 Risks Breakdown

Summary list of all detected risks.

Title	Threat Level	Open	Accepted
Open TCP Port: 443	● Medium	1	0
Open TCP Port: 80	● Medium	1	0
Open TCP Port: 8080	● Medium	1	0

## 7.3 Full Risk Details

Detailed information about each risk found by the scan.

### Open TCP Port: 443

● 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](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
<a href="http://testfire.net/">http://testfire.net/</a>	0 days ago

## Open TCP Port: 80

● 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](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

<http://testfire.net/>

0 days ago

## Open TCP Port: 8080

● 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](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

<http://testfire.net/>

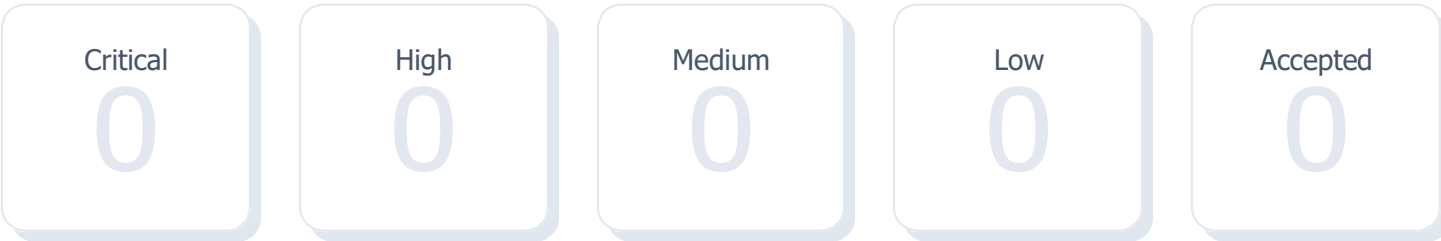
0 days ago

# 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.



## 8.2 Risks Breakdown

Title	Threat Level	Open	Accepted
No risks detected			

Summary list of all detected risks

## 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.

## **Business Impact**

### **Plugin ID: 46180 - Additional DNS Hostnames Synopsis:**

The Nessus vulnerability scan has detected potential virtual hosts with different hostnames pointing to there remote host

#### **Impact:**

1. Resource Allocation
2. Security Implications
3. Website Reputation and Trust
4. Search Engine Optimization (SEO)

#### **Recommended Actions:**

1. Review Virtual Host Configuration
2. Monitor Resource Usage
3. Implement Security Measures
4. Monitor Website Reputation
5. Address SEO Concerns

### **Plugin ID: 45590 - Common Platform Enumeration (CPE) Synopsis:**

The Nessus scan has enumerated Common Platform Enumeration (CPE) names that match the remote system.

#### **Impact:**

1. Vulnerability Identification and Management
2. Asset Inventory and Visibility

3. Regulatory Compliance

5. Risk Assessment and Mitigation

**Recommended Actions:**

1. Regular Scanning and Enumeration
2. Patch Management
3. Vulnerability Monitoring
4. Asset Inventory and Lifecycle Management
5. Compliance Reporting

**Plugin ID: 45590 - Common Platform Enumeration (CPE)**

**Synopsis:**

The Nessus scan has enumerated Common Platform Enumeration (CPE) names that match the remote system.

**Impact:**

1. Vulnerability Identification and Management
2. Asset Inventory and Visibility
3. Regulatory Compliance
4. Vendor Support and Updates
5. Risk Assessment and Mitigation

**Recommended Actions:**

1. Regular Scanning and Enumeration
2. Patch Management
3. Vulnerability Monitoring
4. Asset Inventory and Lifecycle Management
5. Compliance Reporting

**Plugin ID: 54615 - Device Type Synopsis:**

The Nessus scan has identified the remote device type based on the remote operating system.

**Impact:**

1. Device Profiling
2. Security Policy Implementation
3. Network Visibility
4. Incident Response
5. Change Management and Patching

**Recommended Actions:**

1. Accurate Device Identification
2. Network Segmentation
3. Security Policy Tuning
4. Incident Response Planning

**Plugin ID: 11219 - Nessus SYN scanner Synopsis:**

The Nessus SYN scanner is capable of determining which TCP ports are open on a target system.

**Impact:**

1. Network Visibility
2. Vulnerability Identification
3. Firewall Resilience Assessment
4. Network Load and Performance

**Recommended Actions:**

1. Responsible Scanning
2. Firewall Hardening
3. Vulnerability Remediation
4. Monitoring and Incident Response

**Plugin ID: 19506 - Nessus Scan Information Synopsis:**

The plugin provides information about the Nessus scan, including details about the version of the plugin set, the type of scanner used the version of the Nessus Engine, the port scanner(s) employed, the port range scanned, ping round trip time, patch management checks, display of superseded patches, date of the scan, scan duration, number of hosts scanned in parallel, and number of checks performed in parallel.

**Impact:**

1. Scan Effectiveness
2. Network Resource Utilization

3. Patch Management and Vulnerability Assessment
4. Security Posture Evaluation

**Recommended Actions:**

1. Review Scan Configuration
2. Patch Management Improvement
3. Regular Scanning and Updates
4. Network Monitoring

**Plugin ID: 11936 - OS Identification Synopsis:**

The plugin performs OS identification using various remote probes, such as TCP/IP, SMB, HTTP, NTP, SNMP, etc.

**Impact:**

1. System Profiling
2. Vulnerability Assessment
3. Security Posture Evaluation
4. Network Hardening
5. Compliance and Regulatory Requirements:

**Recommended Actions:**

1. Asset Inventory and Documentation
2. Patch Management
3. Security Control Customization

#### 4. Network Segmentation

##### **Plugin ID: 56984 - SSL / TLS Versions Supported Synopsis:**

The plugin is used to detect which SSL and TLS versions are supported by the remote service forencrypting communications.

##### **Impact:**

1. Data Security
2. Compliance and Industry Standards
3. Vulnerability Assessment
4. Public Trust and Reputation

##### **Recommended Actions:**

1. TLS Configuration Review
2. Patch and Update SSL/TLS Libraries
3. Regular Security Assessments
4. Compliance Alignment

##### **Plugin ID: 10863 - SSL Certificate Information Synopsis:**

The plugin connects to every SSL-related port and attempts to extract and dump the X.509certificate.

##### **Impact:**

1. Certificate Validity and Trustworthiness
2. Mitigating Certificate-Related Risks

3. Trust and User Confidence
4. Vulnerability Assessment

**Recommended Actions:**

1. Certificate Monitoring and Renewal
2. SSL Configuration Review
3. Certificate Transparency
4. Public Key Infrastructure (PKI) Management

**Plugin ID: 95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA) Synopsis:**

The plugin identifies that the remote service uses a known Certificate Authority (CA) SSL certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1).

**Impact:**

1. Trustworthiness and Integrity
2. Data Privacy and Confidentiality
3. Compliance and Regulatory Concerns
4. Business Reputation

**Recommended Actions:**

1. Certificate Replacement
2. SSL/TLS Configuration Review



3. Certificate Lifecycle Management
4. Compliance Alignment

**Plugin ID: 70544 - SSL Cipher Block Chaining Cipher Suites Supported Synopsis:**

The plugin identifies that the remote service supports the use of SSL Cipher Block Chaining (CBC) ciphers. CBC mode is a cryptographic technique.

**Impact:**

1. Data Confidentiality
2. Vulnerability to Padding Oracle Attacks
3. Compliance and Security Standards
4. Mitigation Strategies

**Recommended Actions:**

1. SSL/TLS Configuration Review
2. Regular Software Updates
3. Vulnerability Assessments
4. Monitoring and Logging

**Plugin ID: 21643 - SSL Cipher Suites Supported Synopsis:**

The plugin identifies that the remote service encrypts communications using SSL.

**Impact:**

1. Data Confidentiality
2. Secure Communication Channel
3. Compliance with Security Standards

**Recommended Actions:**

1. SSL/TLS Configuration Review
2. Regular Software Updates
3. Vulnerability Assessments
4. Compliance Validation

**Plugin ID: 57041 - SSL Perfect Forward Secrecy Cipher Suites Supported Synopsis:**

The plugin identifies that the remote service supports the use of SSL Perfect Forward Secrecy (PFS) cipher suites.

**Impact:**

1. Data Confidentiality
2. Mitigation of Future Threats
3. Compliance and Regulatory Requirements
4. Protection against Forward Secrecy Attacks

**Recommended Actions:**

1. SSL/TLS Configuration Review
2. Regular Software Updates
3. Key Management Practices
4. Security Monitoring and Incident Response

**Plugin ID: 94761 - SSL Root Certification Authority Certificate Information Synopsis:**

The plugin identifies that the remote service uses an SSL certificate chain containing a self-signed root Certification Authority (CA) certificate at the top of the chain.

**Impact:**

1. Certificate Trust and Security
2. Lack of Third-party Validation
3. Compliance and Regulatory Concerns
4. Certificate Chain Validation

**Recommended Actions:**

1. Obtain a Trusted Root CA Certificate
2. Certificate Lifecycle Management
3. Certificate Chain Validation
4. Compliance and Security Policy Review

**Plugin ID: 156899 - SSL/TLS Recommended Cipher Suites Synopsis:**

The plugin identifies that the remote host advertises discouraged SSL/TLS cipher suites.

**Impact:**

1. Data Security
2. Compatibility and Interoperability
3. Trust and Reputation
4. Compliance with Security Standards

**Recommended Actions:**

1. SSL/TLS Configuration Review
2. Regular Software Updates
3. Vulnerability Assessments
4. Testing and Monitoring

**Plugin ID: 22964 - Service Detection Synopsis:**

The plugin identifies that the remote service could be identified based on its banner or the error message it sends when it receives an HTTP request.

**Impact:**

1. System Identification
2. Vulnerability Assessment
3. Attack Surface Evaluation
4. Security Configuration Review

**Recommended Actions:**

1. Service Hardening
2. Patch Management
3. Security Monitoring
4. Access Control

**Plugin ID: 136318 - TLS Version 1.2 Protocol Detection Synopsis:**

The plugin identifies that the remote service encrypts traffic using TLS 1.2.

**Impact:**

1. Data Security
2. Compliance with Security Standards
3. Trust and Reputation
4. Compatibility and Interoperability

**Recommended Actions:**

1. TLS Configuration Review
2. Regular Software Updates
3. Vulnerability Assessments
4. Security Awareness Training

**Plugin ID: 10287 - Traceroute Information Synopsis:**

The plugin indicates that it was possible to obtain traceroute information from the remote host.

**Impact:**

1. Network Topology Understanding
2. Network Performance Assessment
3. Security Implications
4. Potential Misconfiguration Detection

**Recommended Actions:**

1. Regular Network Monitoring
2. Access Control
3. Network Segmentation

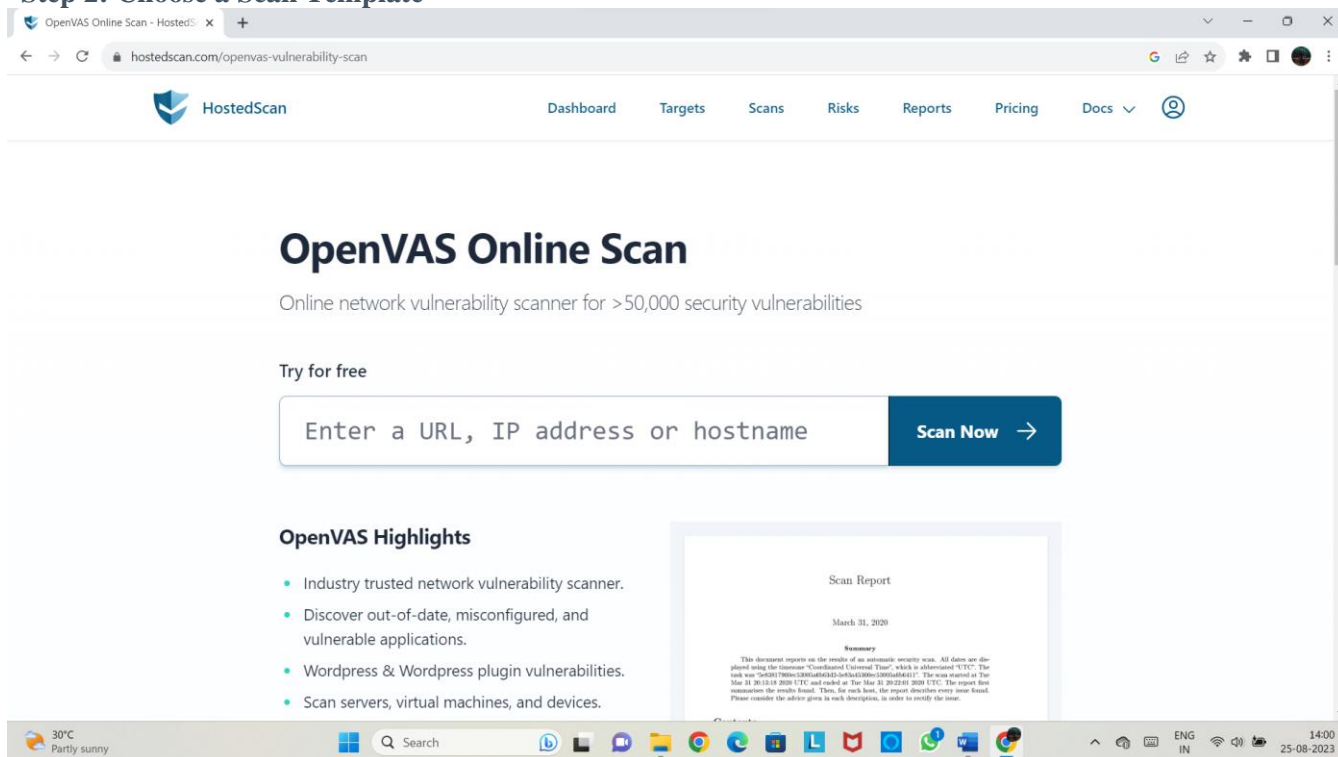
## Steps to reproduce the vulnerabilities

### Step 1: Creating a Scan

Once you have installed and launched OPENVAS, you're ready to start scanning. First, you have to create a scan. To create your scan:

- In the top navigation bar, click Scans.
- In the upper-right corner of the My Scans page, click the New Scan button.

### Step 2: Choose a Scan Template



Next, click the scan template you want to use. Scan templates simplify the process by determining which settings are configurable and how they can be set. For a detailed explanation of all the options available, refer to [Scan and Policy Settings](#) in the OPENVAS User Guide.

A scan policy is a set of predefined configuration options related to performing a scan. After you create a policy, you can select it as a template in the User Defined tab when you create a scan. For more information, see [Create a Policy](#) in the OPENVAS User Guide.

The OPENVAS interface provides brief explanations of each template in the product. Some templates are only available when you purchase a fully licensed copy of OPENVAS.

To see a full list of the types of templates available in OPENVAS, see [Scan and Policy Templates](#). To quickly get started with Nessus, use the Basic Network Scan template.

### Step 3: Configure Scan Settings

Prepare your scan by configuring the [settings](#) available for your chosen template. The Basic Network Scan template has several default settings preconfigured, which allows you to quickly perform your first scan and view results without a lot of effort.

**Follow these steps to run a basic scan:**

## OpenVAS Online Scan

Online network vulnerability scanner for >50,000 security vulnerabilities

Try for free

Scan Now →

### OpenVAS Highlights

- Industry trusted network vulnerability scanner.
- Discover out-of-date, misconfigured, and vulnerable applications.
- Wordpress & Wordpress plugin vulnerabilities.
- Scan servers, virtual machines, and devices.

#### Scan Report

March 31, 2020

##### Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "5ef3817960ec33805af6563d55ef8a233005af646411". The scan started at Tue Mar 31 20:12:18 2020 UTC and ended at Tue Mar 31 20:22:01 2020 UTC. The report first summarizes the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

### 1. Configure the settings in the Basic Settings section.



The following are Basic settings:

Setting	Description
Name	Specifies the name of the scan or policy. This value is displayed on the OPENVAS interface.
Description	(Optional) Specifies a description of the scan or policy.
Folder	Folder where the scan appears after being saved.
Targets	Specifies one or more targets to be scanned. If you select a target group or upload a targets file, you are not required to specify additional targets.

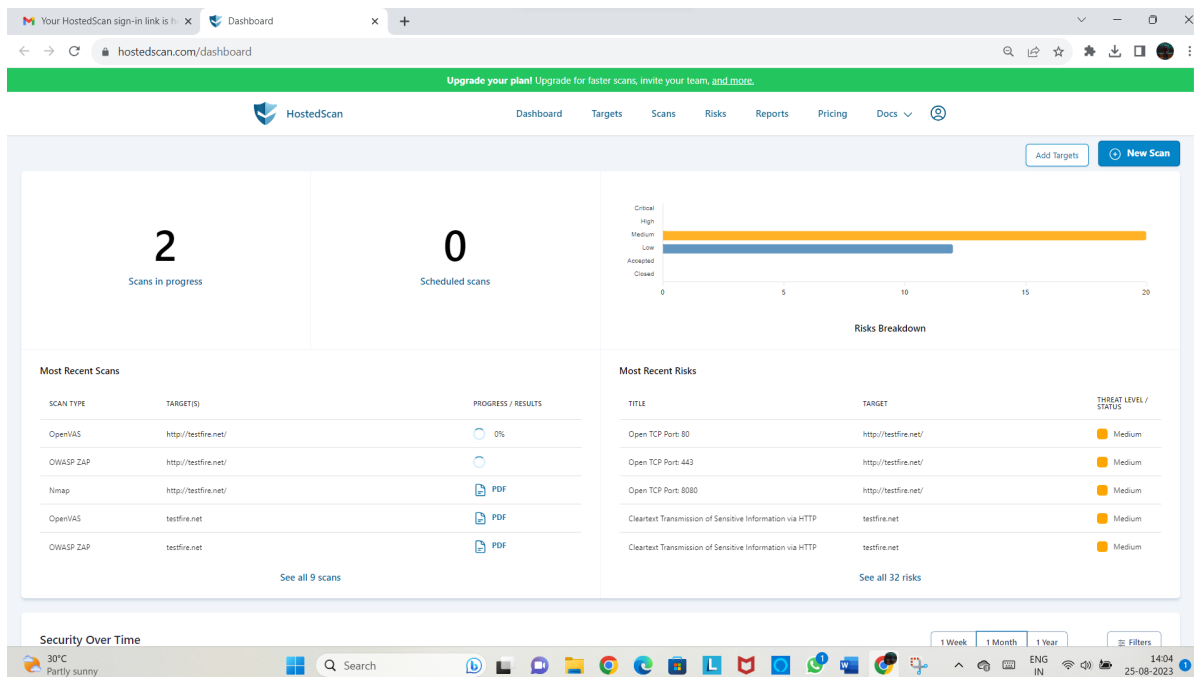
## 2. Configure remaining settings

Although you can leave the remaining settings at their pre-configured default, Tenable recommends reviewing the Discovery, Assessment, Report and Advanced settings to ensure they are appropriate for your environment.

For more information, see the [Scan Settings](#) documentation in the OPENVAS User Guide.


## 3. Configure Credentials

Optionally, you can configure Credentials for a scan. This allows credentialed scans to run, which can provide much more complete results and a more thorough evaluation of the vulnerabilities in your environment.



## 4. Launch Scan

After you have configured all your settings, you can either click the Save button to launch the scan later, or launch the scan immediately.

If you want to launch the scan immediately, click the  button, and then click Launch. Launching the scan will also save it.

The time it takes to complete a scan involves many factors, such as network speed and congestion, so the scan may take some time to run.

### Step 4: Viewing Your Results

Viewing scan results can help you understand your organization's security posture and vulnerabilities. Color-coded indicators and customizable viewing options allow you to tailor how you view your scan's data.

**You can view scan results in one of several views:**

Page	Description
Hosts	Displays all scanned targets.

<b>Vulnerabilities</b>	<b>List of identified vulnerabilities, sorted by severity.</b>
<b>Remediations</b>	<b>If the scan's results include remediation information, this list displays all remediation details, sorted by the number of vulnerabilities.</b>
<b>Notes</b>	<b>Displays additional information about the scan and the scan's results.</b>
<b>History</b>	<b>Displays a list of scans: Start Time, End Time, and the Scan Statuses.</b>

Viewing scan results by vulnerabilities gives you a view into potential risks on your assets.

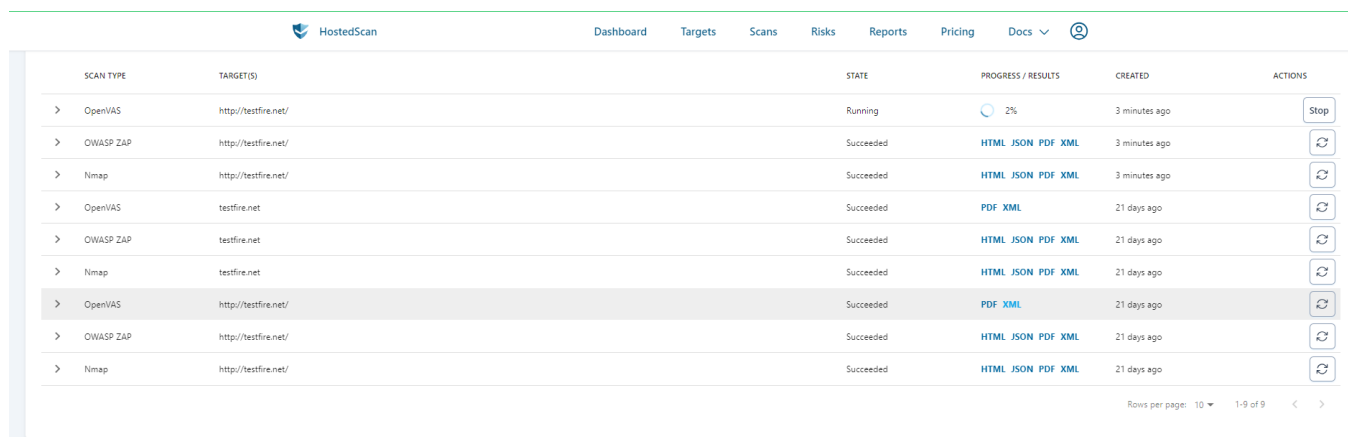
The screenshot shows the HostedScan dashboard. At the top, there's a navigation bar with links to Dashboard, Targets, Scans, Risks, Reports, Pricing, and Docs. Below this, a green banner encourages upgrading the plan. The main content area is divided into several sections:

- Scans in progress:** A large number '2' with the text 'Scans in progress' below it.
- Scheduled scans:** A large number '0' with the text 'Scheduled scans' below it.
- Risks Breakdown:** A horizontal bar chart showing the distribution of risks by severity. The y-axis lists 'Critical', 'High', 'Medium', 'Low', 'Accepted', and 'Closed'. The x-axis represents the count, ranging from 0 to 20. The 'High' category has the longest bar, reaching approximately 18.
- Most Recent Scans:** A table listing recent scans with columns for Scan Type, Target(s), and Progress / Results. It includes links to view scan details as PDFs.
- Most Recent Risks:** A table listing recent risks with columns for Title, Target, and Threat Level / Status. It includes a link to view all 32 risks.

At the bottom, there's a 'Security Over Time' section with a weather widget showing 30°C and 'Partly sunny'. The system tray at the very bottom shows the date and time as 14:04 on 25-08-2023.

## To view vulnerabilities:

1. In the top navigation bar, click Scans.
2. Click the scan for which you want to view results.
3. Do one of the following:
  - Click a specific host to view vulnerabilities found on that host.
  - Click the Vulnerabilities tab to view all vulnerabilities.
4. (Optional) To sort the vulnerabilities, click an attribute in the table header row to sort by that attribute.
5. Clicking on the vulnerability row will open the vulnerability details page, displaying plugin information and output for each instance on a host.



The screenshot shows the HostedScan web interface. At the top is a navigation bar with links: Dashboard, Targets, Scans, Risks, Reports, Pricing, Docs, and a user icon. Below the navigation bar is a table with the following columns: SCAN TYPE, TARGET(S), STATE, PROGRESS / RESULTS, CREATED, and ACTIONS. The table contains 9 rows of scan data. The first row is for an OpenVAS scan on http://testfire.net/ which is currently Running at 2% progress. The remaining 8 rows are for completed scans (Succeeded) for OpenVAS, OWASP ZAP, and Nmap on both http://testfire.net/ and testfire.net. Each row has an Actions column with buttons for Stop, Refresh, or Download (HTML, JSON, PDF, XML). The 7th row (OpenVAS on http://testfire.net/) is highlighted. At the bottom right of the table, it says 'Rows per page: 10' and '1-9 of 9'.

SCAN TYPE	TARGET(S)	STATE	PROGRESS / RESULTS	CREATED	ACTIONS
> OpenVAS	http://testfire.net/	Running	2%	3 minutes ago	Stop
> OWASP ZAP	http://testfire.net/	Succeeded	HTML JSON PDF XML	3 minutes ago	Refresh
> Nmap	http://testfire.net/	Succeeded	HTML JSON PDF XML	3 minutes ago	Refresh
> OpenVAS	testfire.net	Succeeded	PDF XML	21 days ago	Refresh
> OWASP ZAP	testfire.net	Succeeded	HTML JSON PDF XML	21 days ago	Refresh
> Nmap	testfire.net	Succeeded	HTML JSON PDF XML	21 days ago	Refresh
> OpenVAS	http://testfire.net/	Succeeded	PDF XML	21 days ago	Refresh
> OWASP ZAP	http://testfire.net/	Succeeded	HTML JSON PDF XML	21 days ago	Refresh
> Nmap	http://testfire.net/	Succeeded	HTML JSON PDF XML	21 days ago	Refresh

## Step 5: Reporting Your Results

Chances are your job isn't done yet. You need to report your findings to your team.

Scan results can be exported in several file formats. Some of these report formats are customizable, while others are designed to be imported into another application or product, such as Microsoft Excel or Tenable.sc. For an explanation of the various report formats and the purpose of each, see the [OPENVAS User Guide](#).

To Export a Scan Report:

1. Start from a scan's results page
2. In the upper-right corner, click Export.
3. From the drop-down box, select the format in which you want to export the scan results.
4. Click Export to download the report.

## Conclusion

The network vulnerability assessment on the "altoroMutual" system conducted using Nessus Essentials reveals several vulnerabilities that need attention. Here is a summary of the key findings:

### **1. TLS Version 1.0 Protocol Detection (Vulnerability ID: 104743):**

The remote service supports TLS version 1.0, which is considered outdated and has known cryptographic design flaws. Modern implementations of TLS 1.2 and 1.3 are recommended to mitigate these vulnerabilities. TLS 1.0 should be disabled to enhance security and comply with industry standards.

### **2. Additional DNS Hostnames (Vulnerability ID: 46180):**

The Nessus scan detected additional DNS hostnames pointing to the remote host. It is important to verify these hostnames to ensure they are legitimate and do not pose security risks.

### **3. Common Platform Enumeration (CPE) (Vulnerability ID: 45590):**

The Nessus scan enumerated CPE names that match the remote system. Understanding the CPE information can help in identifying potential vulnerabilities associated with hardware and software products on the host.

#### **4. Device Type (Vulnerability ID: 54615):**

The Nessus scan inferred the remote device type as a "firewall" based on the remote operating system information. This helps to identify the nature of the system but does not indicate a vulnerability.

#### **5. Nessus SYN Scanner (Vulnerability ID: 11219):**

The Nessus scan detected open TCP ports on the remote host using SYN scanning. While this information can be useful for legitimate purposes, it should be monitored to prevent any potential misuse.

#### **6. Nessus Scan Information (Vulnerability ID: 19506):**

Details about the Nessus scan, including the version of the plugin set, the scanner edition, and the scan duration, were provided. This information helps in understanding the scan results and its configuration.

#### **7. OS Identification (Vulnerability ID: 11936):**

The Nessus scan identified the remote operating system as "CISCO PIX 7.0" using remote probes. While this information is helpful for system administrators, it does not indicate any security risks.

#### **8. SSL/TLS Vulnerabilities (Vulnerability IDs: 56984, 95631, 70544, 10863, 21643, 94761, 156899):**

Various SSL/TLS-related vulnerabilities were detected, including weak hashing algorithm usage, known CA SSL certificate usage, support for SSL Cipher Block Chaining, and support for discouraged SSL/TLS cipher suites. These vulnerabilities can potentially compromise the confidentiality and integrity of encrypted communications.

## **Recommendations:**

Based on the assessment results, the following recommendations are suggested to improve the security of the "altoroMutual" system:

1. Disable TLS version 1.0 and enable support for TLS 1.2 and 1.3 to enhance encryption security and comply with industry standards.
2. Investigate and verify the additional DNS hostnames to ensure that they are legitimate and do not pose security risks.
3. Monitor the open TCP ports identified by the Nessus SYN scanner to prevent any potential security issues or unauthorized access.
4. Review and understand the CPE information to identify any potential vulnerabilities associated with hardware and software products on the host.
5. Address SSL/TLS-related vulnerabilities, such as replacing certificates signed with weak hashing algorithms, verifying root Certification Authority certificates, and enabling recommended cipher suites.
6. Regularly update and patch the system to address any known vulnerabilities and improve overall security.
7. Implement proper network security controls, including firewalls and intrusion detection/prevention systems, to protect against potential threats.

It is essential to address these vulnerabilities promptly to enhance the security posture of the "altoroMutual" system and safeguard sensitive data and communications. Regular vulnerability assessments and security best practices should be followed to ensure ongoing protection against potential threats.