

SMARTINTERN LONG TERM INTERNSHIP

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

BACHELOR OF COMMERCE

SUBMITTED BY

TEAM ID:-LTVIP2023TMID1825

TEAM SIZE:-05

Guttula kavya sri	:-120127104012
Penta Renuka	:-120127104024
Vulla aruna	:-120127103026
Shahanaaz Begam	:- 120127103023
Tammina nandini	:-720127105043

**DEPARTMENT OF COMMERCE
IN
ACTS DEGREE COLLEGE.**

VISHAKAPATNAM.

Network Vulnerability Assessment Altoro Mutual

The screenshot displays the Altoro Mutual website interface. At the top, there is a navigation bar with links for 'Sign In', 'Contact Us', 'Feedback', and a search bar. Below this is a banner image featuring a woman's face and a 'DEMO SITE ONLY' watermark. The main content area is divided into four columns: 'ONLINE BANKING LOGIN', 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. The 'PERSONAL' column lists services like Deposit Product, Checking, Loan Products, Cards, Investments & Insurance, and Other Services. The 'SMALL BUSINESS' column lists Deposit Products, Lending Services, Cards, Insurance, Retirement, and Other Services. The 'INSIDE ALTORO MUTUAL' column lists About Us, Contact Us, Locations, Investor Relations, Press Room, Careers, and Subscribe. The 'PERSONAL' column also features a section for 'Online Banking with FREE Online Bill Pay' and a 'Real Estate Financing' section. The 'SMALL BUSINESS' column features a 'Business Credit Cards' section and a 'Retirement Solutions' section. The 'INSIDE ALTORO MUTUAL' column features a 'Privacy and Security' section and a 'Win a Samsung Galaxy S10 smartphone' section. At the bottom, there is a footer with links for Privacy Policy, Security Statement, Server Status Check, REST API, and a copyright notice for 2023 Altoro Mutual, Inc. A red banner at the bottom right states 'This web application is open source! Get your copy from GitHub and take advantage of advanced features.' A disclaimer box at the bottom left states that the Altoro Mutual website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects.

Altoro Mutual

Sign In | Contact Us | Feedback | Search | Go

DEMO SITE ONLY

ONLINE BANKING LOGIN

PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking with FREE Online Bill Pay

No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

Real Estate Financing

Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it.

Business Credit Cards

You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.

Retirement Solutions

Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

Privacy and Security

The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

Win a Samsung Galaxy S10 smartphone

Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features.

The Altoro Mutual website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SW110>.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.

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

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
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

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]
```


DNS records for testfire.net

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

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	Revalidate in
Start of authority	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**

DOMAINS WEBSITE CLOUD HOSTING SERVERS EMAIL SECURITY WHOIS SUPPORT LOGIN

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**
- teststerfire.com **Buy Now**
- testsfiregames.com **Buy Now**
- datatestfire.com **Buy Now**
- testsfire.net **Buy Now**
- teststerfire.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

.xyz On Sale!
\$.XYZ @ \$2.88 \$13.88

WORDPRESS HOSTING Introducing
\$3.58 /mo
VIEW MORE

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>

65.61.137.117
Regular View
Raw Data

// TAGS: cloud

General Information

Hostnamesaltoromutual.com, demo.testfire.net

DomainsTESTFIRE.NETALTOROMUTUAL.COM

Cloud ProviderRackspace

CountryUnited States

CityDallas

OrganizationRackspace Backbone Engineering

ISPRackspace Hosting

ASNAS33070

Open Ports

80443

// 80 / TCP

Apache Tomcat/Coyote JSP engine 1.1

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=CBCBB953B44DBCC689291CC3766EEDDE; 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



altoroMutual

Vulnerabilities by Host

· 65.61.137.117

.....

·

· **Vulnerabilities by Host**

65.61.137.117



Scan Information

Start time: Sun Jul 30 19:36:58 2023
End time: Sun Jul 30 20:46:19 2023

IP:
OS:

<https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.
Risk Factor Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin

Output

```
TLStls is enabled and the server supports at least one cipher.
```

tcp/443/ww

46180 - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

See Also

https://en.wikipedia.org/wiki/Virtual_hosting

Solution

If you want to test them, re-scan using the special vhost syntax, such as :
www.example.com[192.0.32.10]

Risk Factor None

Host Information

65.61.137.117
CISCO PIX 7.0

Vulnerabilities

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like

1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

Plugin Information

Published: 2010/04/29, Modified: 2022/08/15

Plugin Output tcp/0

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

<http://cpe.mitre.org/>
<https://nvd.nist.gov/products/cpe>

Solution n/a

Risk Factor None

Plugin Information

Published: 2010/04/21, Modified: 2023/07/27

Plugin Output tcp/0

```
The remote operating system matched the following CPE :  
cpe:/o:cisco:pix_firewall:7.0 -> Cisco PIX Firewall
```

Software

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution n/a

Risk Factor None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output tcp/

```
Remote device type :  
firewall Confidence level :  
70
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin

Output

```
Port 80/tcp was found to be open
```

tcp/80

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output tcp/443/www

```
Port 443/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output tcp/8080

```
Port 8080/tcp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used. - The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible. - Whether the display of superseded patches is enabled - The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution n/a

Risk Factor None

Plugin Information

Published: 2005/08/26, Modified: 2023/04/27

Plugin Output tcp

Information about this scan :

Nessus version :
10.5.3 Nessus build :
20005

Plugin feed version :
202307292203 Scanner edition used
: Nessus Home Scanner OS : LINUX

Scanner distribution :

debian10-x86-64 Scan type : Normal
Scan name : altoroMutual

Scan policy used : Basic Network
Scan Scanner IP : 192.168.237.129
Port scanner(s) :
nessus_syn_scanner Port range :
1-65535
Ping RTT : 378.784 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled
: no Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test :
yes Credentialed
checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin
launched) CGI scanning : disabled
Web application tests :
disabled Max hosts : 30
Max checks :
4 Recv
timeout : 5
Backports :
None
Allow post-scan editing : Yes
Scan Start Date : 2023/7/30 19:37
IST Scan duration : 4147 sec
Scan for malware : no

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution n/a

Risk Factor None

Plugin Information

Published: 2003/12/09, Modified: 2022/03/09

```
Remote operating system : CISCO PIX
7.0 Confidence level : 70
Method : SinFP
```

```
The remote host is running CISCO PIX 7.0
```

56984 - SSL / TLS Versions Supported

Synopsis

.....

The remote service encrypts communications.

Description

.....

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution n/a

Risk Factor None

Plugin Information

.....

Published: 2011/12/01, Modified: 2023/07/10

Plugin Output tcp/443/www

```
This port supports TLSv1.0/TLSv1.2.
```

10863 - SSL Certificate Information

Synopsis

.....

This plugin displays the SSL certificate.

Description

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

Solution n/a

Risk Factor None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

```
9A 2F CD 34 CA 3F FE 8D 47 0E 8E E3 28 17 36 34 6C 2E 38 F8
CF 3E E1 31 01 07 55 5C 3A 43 CB 36 17 28 16 16 9C 58 12 58
95 74 B2 59 C9 CC 16 CF E5 AF 26 74 86 1D B8 E0 3E FE C6 3C
8F 4D 00 4A 3A 0E 4F 7F C8 0B 12 0A DC 87 8F 26 8F 6D 39 7A
33 BB 36 59 34 95 14 EE 94 CE D9 E2 9A 95 1F 19 75 FE
68 B6 E6 B9 10 E7 AD CD 62 8A BE C4 E8 D2 AF 62 2F C5
0D
Exponent: 01 00 01
Signature Length: 256 bytes / 2048 bits
Signature: 00 C0 AD 30 34 11 F1 FA E6 17 53 0F 49 30 C1 58 E6 17 42 42
A4 46 88 E5 10 D2 8A 32 E1 C3 54 4E 44 C7 8C F2 A5 8C 62 36
32 7E 53 0C 11 7F 6B BC 81 22 75 07 83 FE 1E 82 10 DF 01 7D
2D B2 7A 3A E8 E8 1F D2 32 4A AE 53 D8 74 85 4D FC 77 85 BC
7E B1 36 8A BF 0F 3C B5 72 3B C0 74 9D 90 31 E0 A9 7A
18 A1 A5 2E A0 25 B1 EB EE 7C 2B C7 FB B7 FB 72 F0 86
9F 73 41 A6 76 14 5A 49 DA 49 AB 54 3F 6D 06 2F F9 97
70 51 AF 47 78 97
2B 47 D0 7F 99 C6 EF 66 CC 64 3 [...]
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunset of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

See Also

.....
<http://www.nessus.org/u?ae636e78>
<https://tools.ietf.org/html/rfc3279>
<http://www.nessus.org/u?9bb87bf2>

Solution

.....
Contact the Certificate Authority to have the certificate reissued.

Risk Factor None

References

BID 11849
BID 33065
XREF CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2022/10/12

Plugin Output tcp/443/www

The following known CA certificates were part of the certificate chain sent by the remote host, but contain hashes that are considered to be weak.

```
Subject      : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate Services
Signature Algorithm : SHA-1 With RSA Encryption Valid From      : Jan 01 00:00:00 2004 GMT
Valid To      : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEAjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHbGJhbnR1eW8ybmhGC1PqY0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
yMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1PqY0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGHCFHdR/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRRome9Hg6jC8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8X1KdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIZ6W8Qfs4q8p74Klf9AwPLQwDg
YDVR0PAQH/BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2Nybc5j21vZG9jYS5jb20vQUFBQ2VydG1maWNhdGVtZXJ2aWN1cy5j
cmwwNqA0oDKGMGH
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9glo1QGE8mTgHj5rC17r
+8dFRBv/38ErjHT1r0iWAff2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqW8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqt1bgT2G9w84FoVxp7Z8V1IMCFLA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF
501KKaU73yqWjgo
+ev+to5lbyrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgrRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

.....
The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.>

html <http://www.nessus.org/u?cc4a822a>

<https://www.openssl.org/~bodo/tls-cbc.txt>

Solution n/a

Risk Factor None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output tcp/443/www

```
Here is the list of SSL CBC ciphers supported by the remote server
: High Strength Ciphers (>= 112-bit key)
```

Name	Code	KEX	Auth	Encryption	MAC
DHE-RSA-AES128-SHA	0x00, 0x33	DH	RSA	AES-CBC (128)	
SHA1 DHE-RSA-AES256-SHA	0x00, 0x39	DH	RSA	AES-CBC (256)	
SHA1 ECDHE-RSA-AES128-SHA	0xC0, 0x13	ECDH	RSA	AES-CBC (128)	
SHA1 ECDHE-RSA-AES256-SHA	0xC0, 0x14	ECDH	RSA	AES-CBC (256)	
SHA1 DHE-RSA-AES128-SHA256	0x00, 0x67	DH	RSA	AES-CBC (128)	
SHA256					

DHE-RSA-AES256-SH	0x00,	D	R	AES-CBC(2
A256 SHA256	0x6B	H	S	56)
ECDHE-RSA-AES128-SH	0xC0,	E	R	AES-CBC(1
A256 SHA256	0x27	C	S	28)
ECDHE-RSA-AES256-SH	0xC0,	D	R	AES-CBC(2
A384 SHA384	0x28	D	S	56)

The fields above are :

```
{Tenable ciphernam}
{Cipher ID code}
Kex={key
exchange}
Auth={authenticat
ion}
Encrypt={symmetric encryption
method} MAC={message
authentication code}
{export flag}
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

[https://www.openssl.org/docs/man1.0.2/man1/ciphers.ht](https://www.openssl.org/docs/man1.0.2/man1/ciphers.html)
[ml http://www.nessus.org/u?e17ffced](http://www.nessus.org/u?e17ffced)

Solution n/a

Risk Factor None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin
Output
tcp/443/www

Here is the list of SSL ciphers supported by
: Each group is reported per SSL Version. the remote server

SSL Version : TLSv12

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
DHE-RSA-AES128-SHA256	0x00, 0x9E	----- DH	----- RSA	----- AES-GCM (128)	
SHA256					
DHE-RSA-AES256-SHA384	0x00, 0x9F	DH	RSA	AES-GCM (256)	
SHA384					
ECDHE-RSA-AES128-SHA256	0xC0, 0x2F	ECDH	RSA	AES-GCM (128)	
SHA256					
ECDHE-RSA-AES256-SHA384	0xC0, 0x30	ECDH	RSA	AES-GCM (256)	
SHA384					
DHE-RSA-AES128-SHA	0x00, 0x33	DH	RSA	AES-CBC (128)	
SHA1					
DHE-RSA-AES256-SHA	0x00, 0x39	DH	RSA	AES-CBC (256)	
SHA1					
ECDHE-RSA-AES128-SHA	0xC0, 0x13	ECDH	RSA	AES-CBC (128)	
SHA1					
ECDHE-RSA-AES256-SH	0xC0, 0x14	ECD	RSA	AES-CBC (256)	
A SHA1					
DHE-RSA-AES128-SHA25	0x00, 0x67	H	RSA)	
6 SHA256					
DHE-RSA-AES256-SHA25		DH	RSA	AES-CBC (128	
6 SHA256	0x00, 0x6B	DH	RSA)	
ECDHE-RSA-AES128-SHA25					
6 SHA256	0xC0, 0x27	ECD	RSA	AES-CBC (256	
ECDHE-RSA-AES256-SHA38					
4 SHA384					
	0xC0, 0x28	H)	
		ECD		AES-CBC (128	
		H)	
				AES-CBC (256	
)	

SSL Version : TLSv1

High Strength Ciphers (>= 112-bit key)

SHA1

DHE-RSA-AES256
-SHA

0x00,
0x39

D
H

RSA
[...]

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>
https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution n/a

Risk Factor None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output tcp/443/ww

Here is the list of SSL PFS ciphers supported by the remote : server
 High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
DHE-RSA-AES128-SHA256	0x00, 0x9E	DH	RSA	AES-GCM (128)	
SHA256 DHE-RSA-AES256-SHA384	0x00, 0x9F	DH	RSA	AES-GCM (256)	
SHA384 ECDHE-RSA-AES128-SHA256	0xC0, 0x2F	ECDH	RSA	AES-GCM (128)	
SHA256 ECDHE-RSA-AES256-SHA384	0xC0, 0x30	ECDH	RSA	AES-GCM (256)	
SHA384 DHE-RSA-AES128-SHA	0x00, 0x33	DH	RSA	AES-CBC (128)	
SHA1 DHE-RSA-AES256-SHA	0x00, 0x39	DH	RSA	AES-CBC (256)	
SHA1 ECDHE-RSA-AES128-SHA	0xC0, 0x13	ECDH	RSA	AES-CBC (128)	
SHA1 ECDHE-RSA-AES256-SHA	0xC0, 0x14	ECDH	RSA	AES-CBC (256)	

SHA1	DHE-RSA-AES128-SHA256	0x00, 0x67	DH	RSA	AES-CBC (128)
SHA256	DHE-RSA-AES256-SHA256	0x00, 0x6B	DH	RSA	AES-CBC (256)
SHA256	ECDHE-RSA-AES128-SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC (128)
SHA256	ECDHE-RSA-AES256-SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC (256)
SHA384					

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication
}
Encrypt={symmetric encryption
method} MAC={message authenticat
code}
{export flag}
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10))

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output tcp/443/www

```

The following root Certification Authority certificate was
found :
|-Subject      : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
  ect
  Servi
  ces
|-Issu        : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
  Certificate
  Signature Algorithm: SHA-1 with RSA
  Encryption
  ces
|-Valid      : Jan 01 00:00:00 2004 GMT
  From
|-Valid      : Dec 31 23:59:59 2028 GMT
  To

```

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384 - 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

[https://wiki.mozilla.org/Security/Server_Side_](https://wiki.mozilla.org/Security/Server_Side_TLS)
[TLS https://ssl-config.mozilla.org/](https://wiki.mozilla.org/Security/Server_Side_TLS)

Solution

Only enable support for recommended cipher suites.

Risk Factor None

Plugin Information

Published: 2022/01/20, Modified: 2023/07/1

Name	Code	KEX	Auth	Encryption	MAC
DHE-RSA-AES128-SHA	0x00, 0x33	DH	RSA	AES-CBC (128)	
SHA1					
DHE-RSA-AES256-SHA	0x00, 0x39	DH	RSA	AES-CBC (256)	
SHA1					
ECDHE-RSA-AES128-SHA	0xC0, 0x13	ECDH	RSA	AES-CBC (128)	
SHA1					
ECDHE-RSA-AES256-SHA	0xC0, 0x14	ECDH	RSA	AES-CBC (256)	
SHA1					
DHE-RSA-AES128-SHA256	0x00, 0x67	DH	RSA	AES-CBC (128)	
SHA256					
DHE-RSA-AES256-SHA256	0x00, 0x6B	DH	RSA	AES-CBC (256)	
SHA256					
ECDHE-RSA-AES128-SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC (128)	
SHA256					
ECDHE-RSA-AES256-SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC (256)	
SHA384					

Plugin Output

tcp/443/www

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below:
```

```
High Strength Ciphers (>= 112-bit key)
```

```
The fields above are :
```

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key  
exchange}  
Auth={authenticat  
ion}  
Encrypt={symmetric encryption  
method} MAC={message  
authentication code}  
{export flag}
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk

Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output tcp/443/www

tcp/443/www

```
A web server is running on this port through TLSv1.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

<https://tools.ietf.org/html/rfc5246>

Solution N/A

Risk Factor None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output tcp/443/www

```
TLShv1.2 is enabled and the server supports at least one cipher.
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution n/a

Risk Factor None

Plugin Information

Published: 1999/11/27, Modified: 2023/06/26

Plugin Output udp/0

Business Impact

Plugin ID: 46180 - Additional DNS Hostnames Synopsis:

The Nessus vulnerability scan has detected potential virtual hosts with different hostnames pointing to the 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 for encrypting 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.509 certificate.

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

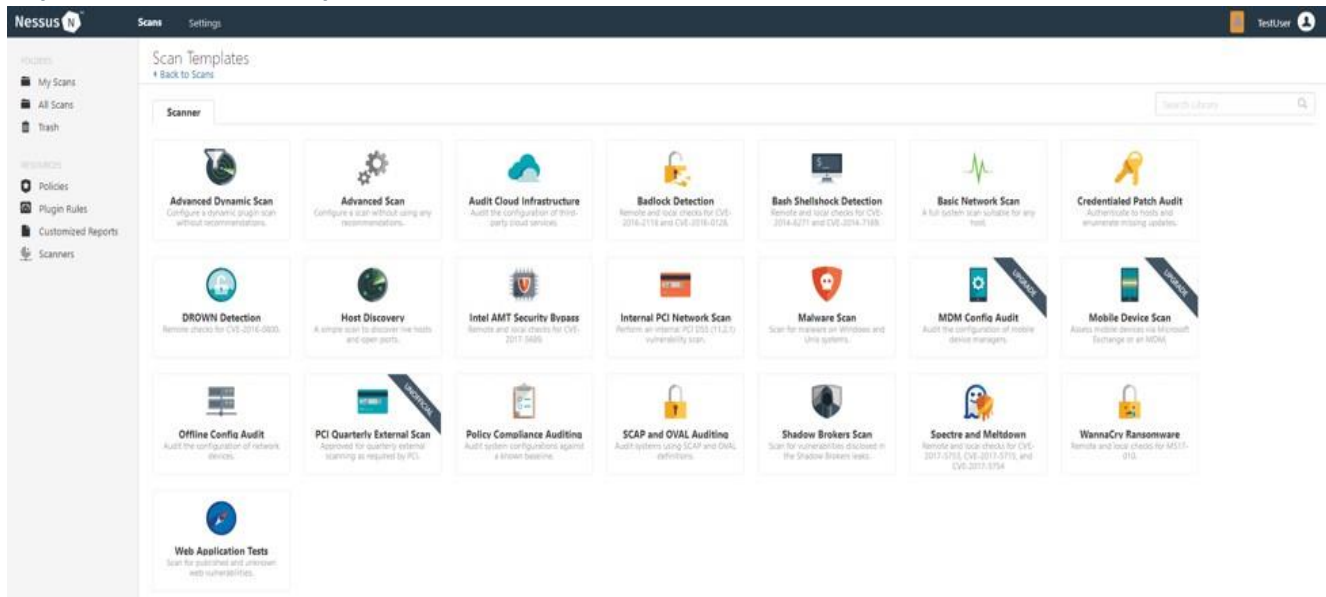
Steps to reproduce the vulnerabilities

Step 1: Creating a Scan

Once you have installed and launched Nessus, 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 Nessus 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 Nessus User Guide.

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

To see a full list of the types of templates available in Nessus, 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:

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 Nessus interface.
Description	(Optional) Specifies a description of the scan or policy.
Folder	The 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.

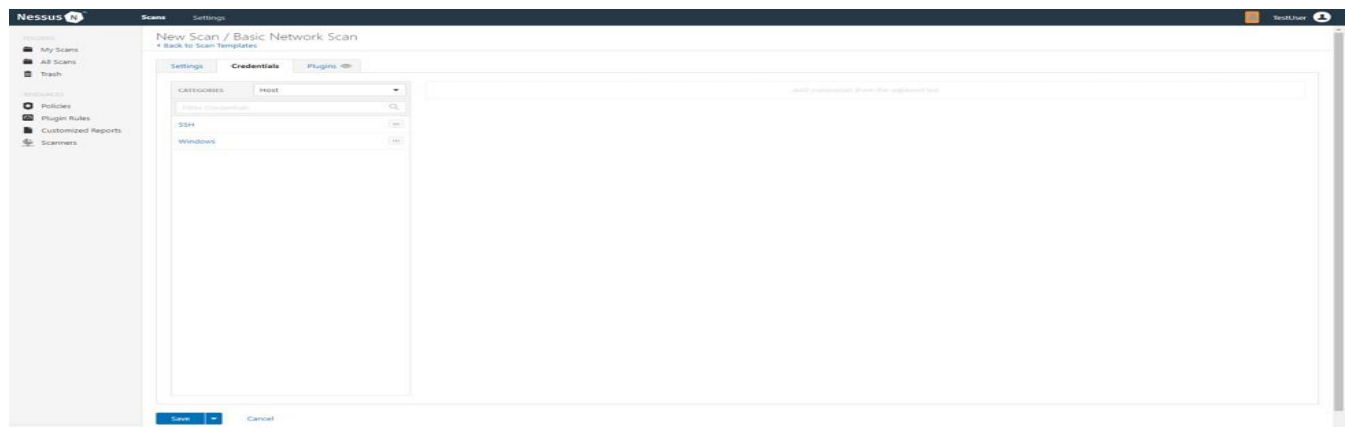
2. Configure remaining settings

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

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

Hosts 1 Vulnerabilities 66 Remediations 2 History 1

Filter ▼ Search Vulnerabilities 🔍 66 Vulnerabilities

<input type="checkbox"/>	Sev -	Name	Family	Count		
<input type="checkbox"/>	CRITICAL	Jenkins < 2.46.2 / 2.57 and Je...	CGI abuses	1	🔍	✎
<input type="checkbox"/>	CRITICAL	MS17-010: Security Update f...	Windows	1	🔍	✎
<input type="checkbox"/>	HIGH	Jenkins < 2.121.2 / 2.133 Mul...	CGI abuses	1	🔍	✎
<input type="checkbox"/>	HIGH	Jenkins < 2.138.4 LTS / 2.150...	CGI abuses	1	🔍	✎
<input type="checkbox"/>	HIGH	Jenkins < 2.150.2 LTS / 2.160 ...	CGI abuses	1	🔍	✎
<input type="checkbox"/>	HIGH	MS12-020: Vulnerabilities in ...	Windows	1	🔍	✎
<input type="checkbox"/>	MEDIUM	Jenkins < 2.107.2 / 2.116 Mul...	CGI abuses	1	🔍	✎
<input type="checkbox"/>	MEDIUM	Jenkins < 2.121.3 / 2.138 Mul...	CGI abuses	1	🔍	✎
<input type="checkbox"/>	MEDIUM	Jenkins < 2.138.2 / 2.146 Mul...	CGI abuses	1	🔍	✎
<input type="checkbox"/>	MEDIUM	Jenkins < 2.73.3 / 2.89 Multip...	CGI abuses	1	🔍	✎
<input type="checkbox"/>	MEDIUM	Jenkins < 2.89.2 / 2.95 Multip...	CGI abuses	1	🔍	✎
<input type="checkbox"/>	MEDIUM	Jenkins < 2.89.4 / 2.107 Multi...	CGI abuses	1	🔍	✎
<input type="checkbox"/>	MEDIUM	Microsoft Windows Remote ...	Windows	1	🔍	✎

Scan Details

Name: Basic Network
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Start: February 25 at 9:03 AM
End: February 25 at 9:07 AM
Elapsed: 4 minutes

Vulnerabilities



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.

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.

THANK YOU.