Secure Cyber Space

Part 1: Executive Summary

I. Overview

Securing cyberspace refers to the practice of protecting digital systems, networks, and data from various threats, vulnerabilities, and attacks. As technology continues to advance, the importance of securing cyberspace becomes even more critical to prevent unauthorized access, data breaches, and other cybercrimes. Here are some key aspects and strategies for securing cyberspace:

- Strong Authentication and Access Controls: Implementing robust authentication methods, such as multi-factor authentication (MFA), helps ensure that only authorized users can access systems and data. Access controls should be established to limit user privileges based on their roles and responsibilities.
- Regular Software Updates and Patch Management: Keeping software, operating systems, and applications up-to-date with the latest security patches is crucial to prevent exploitation of known vulnerabilities.
- Network Security Measures: Employing firewalls, intrusion detection and prevention systems (IDPS), and virtual private networks (VPNs) can help protect networks from unauthorized access and attacks.
- Data Encryption: Encrypting sensitive data both at rest and in transit helps safeguard information from unauthorized access. This includes using protocols like HTTPS for web communication and encryption for stored data.
- Employee Training and Awareness: Educating employees about cybersecurity best practices, such as identifying phishing emails, using strong passwords, and recognizing potential threats, can help prevent social engineering attacks.
- Regular Security Audits and Assessments: Conducting regular security audits and assessments helps identify vulnerabilities and weaknesses in systems and networks, allowing for timely remediation.
- Incident Response Plan: Develop and maintain a well-defined incident response plan to handle security breaches effectively. This plan should outline steps to contain, mitigate, and recover from cybersecurity incidents.
- Endpoint Security: Implement security solutions on endpoints (devices like computers, smartphones, and IoT devices) to protect against malware, ransomware, and other threats.
- Application Security: Secure the software applications used within an organization to prevent vulnerabilities that could be exploited by attackers.

- Vendor Risk Management: If your organization relies on third-party vendors for services or software, ensure they follow security best practices to avoid introducing vulnerabilities into your environment.
- Security Policies and Compliance: Establish clear cybersecurity policies and ensure compliance with relevant regulations and standards, such as GDPR, HIPAA, or industry-specific guidelines.
- Backup and Recovery: Regularly backup critical data and systems, and test the restoration process to ensure that data can be recovered in case of data loss or ransomware attacks.
- Security Awareness Training: Train employees and users about cybersecurity risks and best practices to reduce the likelihood of human error leading to security breaches.
- Threat Intelligence: Stay informed about the latest cybersecurity threats and trends through threat intelligence sources to proactively defend against emerging risks.
- Continuous Monitoring: Implement continuous monitoring of systems and networks for any suspicious activities or anomalies that could indicate a breach.

Securing cyberspace is an ongoing process that requires collaboration, dedication, and a proactive approach to adapt to evolving threats and technologies. Organizations and individuals must work together to create a safer digital environment.

II.

S.No.	Name of the vulnerability	Reference -CWE
1	Broken Access Control	CWE -284 Improper Access Control
2.	Cryptographic Failures	CWE-327: Use of a Broken or Risky Cryptographic Algorithm
3	Injection	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
4	Insecure Design	CWE-657:Violation of Secure Design Principles
5	Security Misconfiguration	CWE-16 Configuration
6	Vulnerable and Outdated Components	CWE-1104: Use of Unmaintained Third Party Components
7	Identification and Authentication Failures	CWE-287: Improper Authentication
8	Software and Data Integrity Failures	CWE-494 :Download of Code without Integrity Check
9	Security Logging and Monitoring Failures	**CWE-532** Insertion of Sensitive Information into Log File
10	Server-Side Request Forgery (SSRF)	**CWE-918 -** Request Forgery attack (SSRF)

III

1. **Vulnerability Name: Broken Access control**

CWE : CWE-284 Improper Access Control

OWASP Category: A01:2021

DESCRIPTION: The restriction of access is less it provide easily access without many restrictions Business Impact: In business its access can be very devastated for the user as it can easily give access to hacker which can change or delete accounts.

2. Vulnerability Name :Cryptographic Failures

CWE : CWE-327 Use of a Broken or Risky Cryptographic Algorithm

OWASP Category: A02:2021

DESCRIPTION: Using such an algorithm means that an attacker may be able to easily decrypt the encrypted data.

Bussiness Impact: Attempting to create non-standard and non-tested algorithms, using weak algorithms, or applying algorithms incorrectly will pose a high weakness to data that is meant to be secure.

3. **Vulnerability Name: Injection**

CWE : CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

OWASP Category: A03:2021

DESCRIPTION: Using such an algorithm means that an attacker may be able to easily decrypt the encrypted data.

Bussiness Impact: The unauthorized viewing of user lists, the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database, all of which are highly detrimental to a business.

4. **Vulnerability Name:Insecure Design**

CWE : CWE-657:Violation of Secure Design Principles

DESCRIPTION: It is related to critical design and architectural flaws in web applications that hackers can exploit.

Bussiness Impact: Failing to do so can lead to flaws that threaten your organizational security, compromising sensitive data, granting privileges to individuals who can abuse them, and more.

5. Vulnerability Name: Security Misconfiguration

CWE : CWE-16 Configuration

DESCRIPTION: A security misconfiguration occurs when system or application configuration settings are missing or are erroneously implemented, allowing unauthorized access.

Bussiness Impact: Security misconfigurations allow attackers to gain unauthorized access to networks, systems and data, which in turn can cause significant monetary and reputational damage to your organization.

6 . Vulnerability Name: Vulnerable and Outdated Components

CWE : CWE-1104

OWASP Category: A06:2021

Description: Use of Unmaintained Third Party Components

Business Impact: The product relies on third-party components that are not actively supported or maintained by the original developer or a trusted proxy for the original developer.

Using vulnerable and outdated components is the sixth category in OWASP Top 10 web application security risks and one of the most common and serious mistakes developers and companies make. It can lead to devastating consequences such as data breaches, malware infections, and compromised systems.

7. Vulnerability Name: Identification and Authentication Failures

CWE : CWE-287 Improper Authentication

OWASP Category: A06:2021

Description: When an actor claims to have a given identity, the product does not prove or insufficiently proves that the claim is correct.

Business Impact: Improper authentication can lead to various security threats, such as: Data breaches: Improper authentication can allow unauthorized users to gain access to sensitive data, leading to data breaches, data loss, or unauthorized access to confidential information.

8. Vulnerability Name: Software and Data Integrity Failures

CWE : CWE-494

OWASP Category: A06:2021

Description: Download of Code without Integrity Check

Business Impact: The product downloads source code or an executable from a remote location and executes the code without sufficiently verifying the origin and integrity of the code.

9. Vulnerability Name: Security Logging and Monitoring Failures

CWE : CWE-532

OWASP Category: A06:2021

Description: Insertion of Sensitive Information into Log File

Business Impact: Information written to log files can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information. Sensitive data exposure can be financially costly to your business and damage your reputation and brand. The type of data at risk of exposure includes financial reports, bank account numbers, credit card numbers, usernames, passwords, customers' personal details, and healthcare information.

10. Vulnerability Name: Server-Side Request Forgery (SSRF)

CWE : CWE-918

OWASP Category: A06:2021

Description: The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination. A Server-Side Request Forgery attack (SSRF) is a security vulnerability in which a hacker tricks a server into accessing unintended resources on his behalf. An SSRF attack can lead to sensitive information being leaked or the attacker gaining control of other systems.

Business Impact: In some situations, the SSRF vulnerability might allow an attacker to perform arbitrary command execution. An SSRF exploit that causes connections to external third-party systems might result in malicious onward attacks that appear to originate from the organization hosting the vulnerable application.

Part 2

I. Overview of Nessus

Nessus- A security vulnerability scanning tool. Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it.

Advantages of Nessus when compared to other vulnerability scanners:

- Unlike other scanners, Nessus does not make assumptions about your server configuration (such as assuming that port 80 must be the only web server) that can cause other scanners to miss real vulnerabilities.
- Nessus is very extensible, providing a scripting language for you to write tests specific to your system once you become more familiar with the tool. Its also provides a plug-in interface, and many free plug-ins are available from the Nessus plug-in site. These plugs are often specific to detecting a common virus or vulnerability.
- Up to date information about new vulnerabilities and attacks. The Nessus team updates the list of what vulnerabilities to check for on a daily basis in order to minimize the window between an exploit appearing in the wild, and you being able to detect it with Nessus.
- Open-source. Nessus is open source, meaning it costs nothing, and you are free to see and modify the source as you wish.
- Patching Assistance: When Nessus detects a vulnerability, it is also most often able to suggest the best way you can mitigate the vulnerability.

Nessus comes in two parts, a server called nessusd and a client, which can by any of several options. The server is the part of Nessus that actually runs the tests, and the client is used to tell the server what tests to run on what computers.

The server exists only for Unix/Linux platforms, but there are clients available for Unix/Linux, Windows and Mac. Therefore, once the server is set up and running, an administrator can run regularly scheduled Nessus tests using a client written for almost any platform.

II. Report

Target Host: Sagi Rama Krishnam Raju Engineering College. srkrec.ac.in

Target IP: 68.178.231.130

SRKREC

Report generated by Nessus™ Fri, 04 Aug 2023 20:46:48 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 68.178.231.130......4

Vulnerabilities by Host

68.178.231.130

1	0	11	4	177
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Fri Aug 4 20:05:49 2023
End time:	Fri Aug 4 20:46:47 2023

Host Information

DNS Name:	130.231.178.68.host.secureserver.net
IP:	68.178.231.130
OS:	Polycom SIP Device

Vulnerabilities

58987 - PHP Unsupported Version Detection

Synopsis

The remote host contains an unsupported version of a web application scripting language.

Description

According to its version, the installation of PHP on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

http://php.net/eol.php

https://wiki.php.net/rfc/releaseprocess

Solution

Upgrade to a version of PHP that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

XREF	IAVA:0001-A-0581

Plugin Information

Published: 2012/05/04, Modified: 2022/12/07

Plugin Output

tcp/443/www

```
  Source               : X-Powered-By: PHP/7.3.33
  Installed version    : 7.3.33
  End of support date  : 2021/12/06
  Announcement         : http://php.net/supported-versions.php
  Supported versions   : 8.0.x / 8.1.x
```

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2020/11/17, Modified: 2023/06/08

Plugin Output

tcp/443/www

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

90317 - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

See Also

https://tools.ietf.org/html/rfc4253#section-6.3

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

Risk Factor

Medium

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2016/04/04, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

```

The following weak server-to-client encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256

The following weak client-to-server encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/110/pop3

```
The identities known by Nessus are :

  bhimavaram.online
  bvrmol.in
  cpanel.bvrmol.in
  mail.bhimavaram.online
  mail.bvrmol.in
  webdisk.bvrmol.in
  www.bhimavaram.online
  www.bvrmol.in
  130.231.178.68.host.secureserver.net

The Common Name in the certificate is :

  *.prod.sin2.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.sin2.secureserver.net
```

```
    prod.sin2.secureserver.net
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/143/imap

```
The identities known by Nessus are :

  bhimavaram.online
  bvrmol.in
  cpanel.bvrmol.in
  mail.bhimavaram.online
  mail.bvrmol.in
  webdisk.bvrmol.in
  www.bhimavaram.online
  www.bvrmol.in
  130.231.178.68.host.secureserver.net

The Common Name in the certificate is :

  *.prod.sin2.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.sin2.secureserver.net
```

```
    prod.sin2.secureserver.net
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/465/smtp

```
The identities known by Nessus are :

  bhimavaram.online
  bvrmol.in
  cpanel.bvrmol.in
  mail.bhimavaram.online
  mail.bvrmol.in
  webdisk.bvrmol.in
  www.bhimavaram.online
  www.bvrmol.in
  130.231.178.68.host.secureserver.net

The Common Name in the certificate is :

  *.prod.sin2.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.sin2.secureserver.net
```

```
    prod.sin2.secureserver.net
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/993/imap

```
The identities known by Nessus are :

  bhimavaram.online
  bvrmol.in
  cpanel.bvrmol.in
  mail.bhimavaram.online
  mail.bvrmol.in
  webdisk.bvrmol.in
  www.bhimavaram.online
  www.bvrmol.in
  130.231.178.68.host.secureserver.net

The Common Name in the certificate is :

  *.prod.sin2.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.sin2.secureserver.net
```

```
    prod.sin2.secureserver.net
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/995/pop3

```

The identities known by Nessus are :

  bhimavaram.online
  bvrmol.in
  cpanel.bvrmol.in
  mail.bhimavaram.online
  mail.bvrmol.in
  webdisk.bvrmol.in
  www.bhimavaram.online
  www.bvrmol.in
  130.231.178.68.host.secureserver.net

The Common Name in the certificate is :

  *.prod.sin2.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.sin2.secureserver.net
```

```
    prod.sin2.secureserver.net
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/2078/www

```
The identities known by Nessus are :

  bhimavaram.online
  bvrmol.in
  cpanel.bvrmol.in
  mail.bhimavaram.online
  mail.bvrmol.in
  webdisk.bvrmol.in
  www.bhimavaram.online
  www.bvrmol.in
  130.231.178.68.host.secureserver.net

The Common Name in the certificate is :

  *.prod.sin2.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.sin2.secureserver.net
```

```
    prod.sin2.secureserver.net
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/2080/www

```

The identities known by Nessus are :

  bhimavaram.online
  bvrmol.in
  cpanel.bvrmol.in
  mail.bhimavaram.online
  mail.bvrmol.in
  webdisk.bvrmol.in
  www.bhimavaram.online
  www.bvrmol.in
  130.231.178.68.host.secureserver.net

The Common Name in the certificate is :

  *.prod.sin2.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.sin2.secureserver.net
```

```
   prod.sin2.secureserver.net
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/2083/www

```
The identities known by Nessus are :

  bhimavaram.online
  bvrmol.in
  cpanel.bvrmol.in
  mail.bhimavaram.online
  mail.bvrmol.in
  webdisk.bvrmol.in
  www.bhimavaram.online
  www.bvrmol.in
  130.231.178.68.host.secureserver.net

The Common Name in the certificate is :

  *.prod.sin2.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.sin2.secureserver.net
```

```
    prod.sin2.secureserver.net
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/2096/www

```

The identities known by Nessus are :

  bhimavaram.online
  bvrmol.in
  cpanel.bvrmol.in
  mail.bhimavaram.online
  mail.bvrmol.in
  webdisk.bvrmol.in
  www.bhimavaram.online
  www.bvrmol.in
  130.231.178.68.host.secureserver.net

The Common Name in the certificate is :

  *.prod.sin2.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.sin2.secureserver.net
```

```
    prod.sin2.secureserver.net
```

54582 - SMTP Service Cleartext Login Permitted

Synopsis

The remote mail server allows cleartext logins.

Description

The remote host is running an SMTP server that advertises that it allows cleartext logins over unencrypted connections. An attacker may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used.

See Also

https://tools.ietf.org/html/rfc4422

https://tools.ietf.org/html/rfc4954

Solution

Configure the service to support less secure authentication mechanisms only over an encrypted channel.

Risk Factor

Low

CVSS v2.0 Base Score

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

Plugin Information

Published: 2011/05/19, Modified: 2021/01/19

Plugin Output

tcp/587/smtp

```
The SMTP server advertises the following SASL methods over an
unencrypted channel on port 587 :

  All supported methods : LOGIN, PLAIN
  Cleartext methods     : LOGIN, PLAIN
```

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

VPR Score

2.5

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	32319
CVE	CVE-2008-5161
XREF	CERT:958563
XREF	CWE:200

Plugin Information

Published: 2013/10/28, Modified: 2018/07/30

Plugin Output

tcp/22/ssh

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

153953 - SSH Weak Key Exchange Algorithms Enabled

Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

See Also

http://www.nessus.org/u?b02d91cd

https://datatracker.ietf.org/doc/html/rfc8732

Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2021/10/13, Modified: 2021/10/13

Plugin Output

tcp/22/ssh

```

The following weak key exchange algorithms are enabled :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group1-sha1
```

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk Factor

Low

CVSS v2.0 Base Score

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

Plugin Information

Published: 2013/11/22, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-sha1-96

The following server-to-client Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-sha1-96
```

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

Plugin Information

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

Plugin Output

tcp/0

```
The following hostnames point to the remote host :
  - bvrmol.in
  - webdisk.bvrmol.in
  - www.bhimavaram.online
  - www.bvrmol.in
  - mail.bvrmol.in
  - mail.bhimavaram.online
  - cpanel.bvrmol.in
  - bhimavaram.online
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/07/31

Plugin Output

tcp/80/www

```
URL        : http://130.231.178.68.host.secureserver.net/
Version    : unknown
Source     : Server: Apache
backported : 0
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/07/31

Plugin Output

tcp/443/www

```
URL        : https://130.231.178.68.host.secureserver.net/
Version    : unknown
Source     : Server: Apache
backported : 0
```

166602 - Asset Attribute: Fully Qualified Domain Name (FQDN)

Synopsis

Report Fully Qualified Domain Name (FQDN) for the remote host.

Description

Report Fully Qualified Domain Name (FQDN) for the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/10/27, Modified: 2022/10/27

Plugin Output

tcp/0

```
The FQDN for the remote host has been determined to be:

  FQDN       : 130.231.178.68.host.secureserver.net
  Confidence : 100
  Resolves   : True
  Method     : rDNS Lookup: IP Address

Another possible FQDN was also detected:
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

```
Give Nessus credentials to perform local checks.
```

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

```
Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server -> Apache Software Foundation Apache HTTP Server
  cpe:/a:mysql:mysql -> MySQL MySQL
  cpe:/a:openbsd:openssh:5.3 -> OpenBSD OpenSSH
  cpe:/a:php:php:7.3.33 -> PHP PHP
```

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/0

```
Remote device type : unknown
Confidence level : 56
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2019/11/22

Plugin Output

tcp/21/ftp

```
The remote FTP banner is :

220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 2 of 500 allowed.
220-Local time is now 07:38. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/443/www

```

  The remote HTTPS server does not send the HTTP
  "Strict-Transport-Security" header.

```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/2078/www

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/2080/www

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/2083/www

```

The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/2096/www

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/2078/www

```
Based on the response to an OPTIONS request :

  - HTTP methods  COPY  DELETE  GET  HEAD  LOCK  MKCOL  MOVE  POST
    PROPFIND  PROPPATCH  PUT  UNLOCK OPTIONS are allowed on :

    /
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :

Apache
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/443/www

```
The remote web server type is :

Apache
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/2078/www

```
The remote web server type is :

cPanel
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/2080/www

```
The remote web server type is :

cPanel
```

85805 - HTTP/2 Cleartext Detection

Synopsis

An HTTP/2 server is listening on the remote host.

Description

The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

See Also

https://http2.github.io/

https://tools.ietf.org/html/rfc7540

https://github.com/http2/http2-spec

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2015/09/04, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
The server supports direct HTTP/2 connections
without encryption.
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
68.178.231.130 resolves as 130.231.178.68.host.secureserver.net.
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/80/www

```

Response Code : HTTP/1.1 301 Moved Permanently

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Fri, 04 Aug 2023 14:56:41 GMT
  Server: Apache
  Location: https://130.231.178.68.host.secureserver.net/
  Content-Length: 253
  Keep-Alive: timeout=5
  Connection: Keep-Alive
  Content-Type: text/html; charset=iso-8859-1

Response Body :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://130.231.178.68.host.secureserver.net/">here</a>.</p>
</body></html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/443/www

```

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Fri, 04 Aug 2023 14:56:40 GMT
  Server: Apache
  X-Powered-By: PHP/7.3.33
  Set-Cookie: OCSESSID=cb91bbf718a394d7395d59467e; path=/
  Upgrade: h2,h2c
  Connection: Upgrade, Keep-Alive
  Vary: Accept-Encoding
  Keep-Alive: timeout=5
  Transfer-Encoding: chunked
  Content-Type: text/html; charset=utf-8

Response Body :

<!DOCTYPE html><html dir="ltr" lang="en" class="desktop win ie ie8 oc30 is-guest route-common-
home store-0 skin-1 desktop-header-active mobile-sticky no-wishlist no-compare layout-1 two-
column column-left column-right" data-jb="45643a14" data-jv="3.1.12" data-ov="3.0.3.8"><head
 typeof="og:website"><meta charset="UTF-8" /><meta name="viewport" content="width=device-width,
 initial-scale=1.0"><meta http-equiv="X-UA-Compatible" content="IE=edge"><title>Bhimavaram
 Online</title><base href="https://bhimavaram.online/" /><link rel="preload" href="catalog/
```

```
view/theme/journal3/icons/fonts/icomoon.woff2?v=907f30d557" as="font" crossorigin><link
 rel="preconnect" href="https://fonts.googleapis.com/" crossorigin><link rel="preconnect"
 href="https://fonts.gstatic.com/" crossorigin><meta name="description" content="The Online
 Destination for People of Bhimavaram" /><meta name="keywords" content="Bhimavaram Online,
 Groceries, Vegetables, Fruits, Specials, Online Shopping, Biryani, Games, Housie, Fun, Movies" /
><meta property="fb:app_id" content=""/><meta property="og:type" content="website"/><meta
 property="og:title" content="Bhimavaram Online"/><meta property="og:url" content="https://
bhimavaram.online/"/><meta property="og:image" content="https://bhimavaram.online/image/cache/
catalog/bvrmol_highres-600x315h.png"/><meta property="og:image:width" content="600"/><meta
 property="og:image:height" content="315"/><meta property="og:description" content="The Online
 Destination for People of Bhimavaram"/><meta name="twitter:card" content="summary"/><meta
 name="twitter:site" conte [...]
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/2078/www

```

Response Code : HTTP/1.1 401 Unauthorized

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : OPTIONS, PROPFIND, GET, LOCK, COPY, MKCOL, PROPPATCH, DELETE, MOVE, PUT, HEAD,
 UNLOCK, POST
Headers :

  Date: Fri, 04 Aug 2023 14:56:43 GMT
  Server: cPanel
  Persistent-Auth: false
  Host: 130.231.178.68.host.secureserver.net:2078
  Cache-Control: no-cache, no-store, must-revalidate, private
  Connection: close
  Vary: Accept-Encoding
  WWW-Authenticate: Basic realm="Restricted Area"
  Content-Length: 35
  Content-Type: text/html; charset="utf-8"
  Expires: Fri, 01 Jan 1990 00:00:00 GMT

Response Body :

<html>Authorization Required</html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/2080/www

```

Response Code : HTTP/1.1 401 Unauthorized

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Date: Fri, 04 Aug 2023 14:56:45 GMT
  Server: cPanel
  Persistent-Auth: false
  Host: 130.231.178.68.host.secureserver.net:2080
  Cache-Control: no-cache, no-store, must-revalidate, private
  Connection: close
  Vary: Accept-Encoding
  WWW-Authenticate: Basic realm="Horde DAV Server"
  Content-Length: 35
  Content-Type: text/html; charset="utf-8"
  Expires: Fri, 01 Jan 1990 00:00:00 GMT

Response Body :

<html>Authorization Required</html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/2083/www

```

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Connection: close
  Content-Type: text/html; charset="utf-8"
  Date: Fri, 04 Aug 2023 14:56:47 GMT
  Cache-Control: no-cache, no-store, must-revalidate, private
  Pragma: no-cache
  Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
  Set-Cookie: cpsession=%3atwiw4G_FMwCVxzV4%2c57b798539973cf75e91832272b950856; HttpOnly; path=/;
 port=2083; secure
  Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2083; secure
  Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=130.231.178.68.host.secureserver.net;
 expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.130.231.178.68.host.secureserver.net; expires=Thu,
 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.130.231.178.68.host.secureserver.net;
 expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
```

```
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde;
 port=2083; secure
  Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
  Set-Cookie: imp_key=expired; HttpOnly; domain=130.231.178.68.host.secureserver.net; expires=Thu,
 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.130.231.178.68.host.secureserver.net; expires=Thu,
 01-Jan-1970 00:00:01 GMT; path=/; port=2083
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.130.231.178.68.host.secureserver.net;
 expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083
  Cache-Control: no-cache, no-store, must-revalidate, private
  Content-Length: 37927

Response Body :


<!DOCTYPE html>
<html lang="en" dir="ltr">
<head>
    [...]
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/2096/www

```

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Connection: close
  Content-Type: text/html; charset="utf-8"
  Date: Fri, 04 Aug 2023 14:56:36 GMT
  Cache-Control: no-cache, no-store, must-revalidate, private
  Pragma: no-cache
  Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
 secure
  Set-Cookie: webmailsession=%3azhM1AoWTj6Gg7ikz%2c740a84dc3f5fb80600d4e9914407db19; HttpOnly;
 path=/; port=2096; secure
  Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2096; secure
  Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=130.231.178.68.host.secureserver.net;
 expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.130.231.178.68.host.secureserver.net; expires=Thu,
 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.130.231.178.68.host.secureserver.net;
 expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
 secure
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde;
 port=2096; secure
  Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
 secure
  Set-Cookie: imp_key=expired; HttpOnly; domain=130.231.178.68.host.secureserver.net; expires=Thu,
 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.130.231.178.68.host.secureserver.net; expires=Thu,
 01-Jan-1970 00:00:01 GMT; path=/; port=2096
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.130.231.178.68.host.secureserver.net;
 expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096
  Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sat, 03-Aug-2024 14:56:36 GMT; path=/;
 port=2096; secure
  Cache-Control: no-cache, no-stor [...]
```

11414 - IMAP Service Banner Retrieval

Synopsis

An IMAP server is running on the remote host.

Description

An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/03/18, Modified: 2011/03/16

Plugin Output

tcp/143/imap

```
The remote imap server banner is :

* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ STARTTLS
 AUTH=PLAIN AUTH=LOGIN] Dovecot ready.
```

11414 - IMAP Service Banner Retrieval

Synopsis

An IMAP server is running on the remote host.

Description

An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/03/18, Modified: 2011/03/16

Plugin Output

tcp/993/imap

```
The remote imap server banner is :

* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ AUTH=PLAIN
 AUTH=LOGIN] Dovecot ready.
```

42085 - IMAP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote IMAP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

See Also

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

https://tools.ietf.org/html/rfc2595

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/09, Modified: 2021/02/24

Plugin Output

tcp/143/imap

```
The remote IMAP service responded to the 'STARTTLS' command with an
'OK' response code, suggesting that it supports that command. However,
Nessus failed to negotiate a TLS connection or get the associated SSL
certificate, perhaps because of a network connectivity problem or the
service requires a peer certificate as part of the negotiation.
```

10719 - MySQL Server Detection

Synopsis

A database server is listening on the remote port.

Description

The remote host is running MySQL, an open source database server.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0802

Plugin Information

Published: 2001/08/13, Modified: 2022/10/12

Plugin Output

tcp/3306/mysql

```
The remote database access is restricted and configured to reject access
from unauthorized IPs.  Therefore it was not possible to extract its
version number.
```

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/21/ftp

```
Port 21/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/22/ssh

```
Port 22/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/80/www

```
Port 80/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/110/pop3

```
Port 110/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/143/imap

```
Port 143/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/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/465/smtp

```
Port 465/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/554

```
Port 554/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/587/smtp

```
Port 587/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/993/imap

```
Port 993/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/995/pop3

```
Port 995/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/1723

```
Port 1723/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/2077

```
Port 2077/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/2078/www

```
Port 2078/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/2080/www

```
Port 2080/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/2082

```
Port 2082/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/2083/www

```
Port 2083/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/2095

```
Port 2095/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/2096/www

```
Port 2096/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/3306/mysql

```
Port 3306/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: 2023/07/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.5.4
Nessus build : 20013
Plugin feed version : 202308040957
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : SRKREC
Scan policy used : Basic Network Scan
Scanner IP : 192.168.29.162
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 69.464 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 : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/8/4 20:05 India Standard Time
Scan duration : 2447 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

Plugin Output

tcp/0

```

Remote operating system : Polycom SIP Device
Confidence level : 56
Method : MLSinFP

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

SSH:!:SSH-2.0-OpenSSH_5.3
HTTP:!:Server: Apache

SMTP:!:220-sg2plmcpnl492402.prod.sin2.secureserver.net ESMTP Exim 4.95 #2 Fri, 04 Aug 2023 07:38:09
 -0700
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
SSLcert:!:i/CN:Starfield Secure Certificate Authority - G2i/O:Starfield Technologies, Inc.i/
OU:http://certs.starfieldtech.com/repository/s/CN:*.prod.sin2.secureserver.net
860dad820119f5de81cff83083eb961f3f98230c
i/CN:Starfield Secure Certificate Authority - G2i/O:Starfield Technologies, Inc.i/OU:http://
certs.starfieldtech.com/repository/s/CN:*.prod.sin2.secureserver.net
860dad820119f5de81cff83083eb961f3f98230c

SinFP:!:
   P1:B10113:F0x12:W14600:O0204ffff:M1460:
   P2:B10113:F0x12:W14600:O0204ffff0101040201030309:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:190504_7_p=995R


The remote host is running Polycom SIP Device
```

117886 - OS Security Patch Assessment Not Available

Synopsis

OS Security Patch Assessment is not available.

Description

OS Security Patch Assessment is not available on the remote host.

This does not necessarily indicate a problem with the scan.

Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```

The following issues were reported :

  - Plugin      : no_local_checks_credentials.nasl
    Plugin ID   : 110723
    Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
    Message     :
Credentials were not provided for detected SSH service.
```

48243 - PHP Version Detection

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0936

Plugin Information

Published: 2010/08/04, Modified: 2022/10/12

Plugin Output

tcp/443/www

```
Nessus was able to identify the following PHP version information :

  Version : 7.3.33
  Source  : X-Powered-By: PHP/7.3.33
```

10185 - POP Server Detection

Synopsis

A POP server is listening on the remote port.

Description

The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network link.

See Also

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

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2019/11/22

Plugin Output

tcp/110/pop3

```
Remote POP server banner :

+OK Dovecot ready.
```

10185 - POP Server Detection

Synopsis

A POP server is listening on the remote port.

Description

The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network link.

See Also

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

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2019/11/22

Plugin Output

tcp/995/pop3

```
Remote POP server banner :

+OK Dovecot ready.
```

42087 - POP3 Service STLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote POP3 service supports the use of the 'STLS' command to switch from a cleartext to an encrypted communications channel.

See Also

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

https://tools.ietf.org/html/rfc2595

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/09, Modified: 2021/02/24

Plugin Output

tcp/110/pop3

```
The remote POP3 service responded to the 'STLS' command with an
'+OK' response code, suggesting that it supports that command. However,
Nessus failed to negotiate a TLS connection or get the associated SSL
certificate, perhaps because of a network connectivity problem or the
service requires a peer certificate as part of the negotiation.
```

54580 - SMTP Authentication Methods

Synopsis

The remote mail server supports authentication.

Description

The remote SMTP server advertises that it supports authentication.

See Also

https://tools.ietf.org/html/rfc4422

https://tools.ietf.org/html/rfc4954

Solution

Review the list of methods and whether they're available over an encrypted channel.

Risk Factor

None

Plugin Information

Published: 2011/05/19, Modified: 2019/03/05

Plugin Output

tcp/587/smtp

```
The following authentication methods are advertised by the SMTP
server without encryption :
  LOGIN
  PLAIN
```

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

References

XREF	IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/465/smtp

```
Remote SMTP server banner :

220-sg2plmcpnl492402.prod.sin2.secureserver.net ESMTP Exim 4.95 #2 Fri, 04 Aug 2023 07:38:09 -0700
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
```

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

References

XREF	IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/587/smtp

```
Remote SMTP server banner :

220-sg2plmcpnl492402.prod.sin2.secureserver.net ESMTP Exim 4.95 #2 Fri, 04 Aug 2023 07:37:30 -0700
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
```

42088 - SMTP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote SMTP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

See Also

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

https://tools.ietf.org/html/rfc2487

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/09, Modified: 2019/03/20

Plugin Output

tcp/587/smtp

```
The remote SMTP service responded to the 'STARTTLS' command with a
'220' response code, suggesting that it supports that command. However,
Nessus failed to negotiate a TLS connection or get the associated SSL
certificate, perhaps because of a network connectivity problem or the
service requires a peer certificate as part of the negotiation.
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/22/ssh

```

Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group1-sha1
  diffie-hellman-group14-sha1

The server supports the following options for server_host_key_algorithms :

  ssh-dss
  ssh-dss-cert-v01@openssh.com
  ssh-rsa
  ssh-rsa-cert-v01@openssh.com

The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha2-256
  hmac-sha2-512
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha2-256
  hmac-sha2-512
  umac-64@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

149334 - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

https://tools.ietf.org/html/rfc4252#section-8

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2021/01/19

Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-96

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-96
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_5.3
SSH supported authentication : publickey,password
```

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/110/pop3

```
This port supports TLSv1.2.
```

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/143/imap

```
This port supports TLSv1.2.
```

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 TLSv1.2.
```

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/465/smtp

```
This port supports TLSv1.2.
```

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/993/imap

```
This port supports TLSv1.2.
```

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/995/pop3

```

This port supports TLSv1.2.
```

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/2078/www

```
This port supports TLSv1.2.
```

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/2080/www

```
This port supports TLSv1.2.
```

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/2083/www

```
This port supports TLSv1.2.
```

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/2096/www

```
This port supports TLSv1.2.
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/110/pop3

```

The host name known by Nessus is :

  130.231.178.68.host.secureserver.net

The Common Name in the certificate is :

  *.prod.sin2.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.sin2.secureserver.net
  prod.sin2.secureserver.net
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/143/imap

```

The host name known by Nessus is :

  130.231.178.68.host.secureserver.net

The Common Name in the certificate is :

  *.prod.sin2.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.sin2.secureserver.net
  prod.sin2.secureserver.net
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/465/smtp

```

The host name known by Nessus is :

  130.231.178.68.host.secureserver.net

The Common Name in the certificate is :

  *.prod.sin2.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.sin2.secureserver.net
  prod.sin2.secureserver.net
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/993/imap

```

The host name known by Nessus is :

  130.231.178.68.host.secureserver.net

The Common Name in the certificate is :

  *.prod.sin2.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.sin2.secureserver.net
  prod.sin2.secureserver.net
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/995/pop3

```

The host name known by Nessus is :

  130.231.178.68.host.secureserver.net

The Common Name in the certificate is :

  *.prod.sin2.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.sin2.secureserver.net
  prod.sin2.secureserver.net
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/2078/www

```

The host name known by Nessus is :

  130.231.178.68.host.secureserver.net

The Common Name in the certificate is :

  *.prod.sin2.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.sin2.secureserver.net
  prod.sin2.secureserver.net
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/2080/www

```
The host name known by Nessus is :

  130.231.178.68.host.secureserver.net

The Common Name in the certificate is :

  *.prod.sin2.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.sin2.secureserver.net
  prod.sin2.secureserver.net
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/2083/www

```

The host name known by Nessus is :

  130.231.178.68.host.secureserver.net

The Common Name in the certificate is :

  *.prod.sin2.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.sin2.secureserver.net
  prod.sin2.secureserver.net
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/2096/www

```

The host name known by Nessus is :

  130.231.178.68.host.secureserver.net

The Common Name in the certificate is :

  *.prod.sin2.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.sin2.secureserver.net
  prod.sin2.secureserver.net
```

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

Plugin Output

tcp/110/pop3

```
Subject Name:

Common Name: *.prod.sin2.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 6F 4B 2B DE 9E 8C F8 0D

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 23:12:17 2023 GMT
Not Valid After: Feb 29 23:12:17 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B3 D4 3A 93 73 C1 D4 0E 40 89 C2 EA 82 B2 6F 3E 96 C8 E0
            49 EA 80 E5 DB 0D 75 00 7B C1 76 6F 4D 43 05 4D 4E 54 04 42
            FD 04 89 E2 27 B8 E9 1C 62 3B 35 C3 5F 4E C8 30 B4 EC 1E 81
            58 98 C4 BC 6F 58 3D 1A A0 4C EE EF 06 36 64 4F 20 DD F5 AC
            C5 42 38 D7 2F F7 0A 08 A0 A2 CA 0E 1A D4 8E 6E 04 90 5E 32
            6C 7F 1B E9 4A 5C 19 79 82 D5 4C A5 22 71 6A 43 CC 11 B3 FE
            C8 98 3A 84 68 E1 5C 68 43 85 63 7E 29 48 E4 94 FF 38 94 2D
            2D 3B CE 3E 9A 55 7D 7B 87 8A 40 8A F2 CB 61 2C A4 B8 D2 2F
            66 C7 6F 5D 37 0C 5A 2A 9C C5 C1 2E 0E BA E3 CF 9E C8 0C C1
            AC 90 79 0D 7A 20 C0 F5 B4 B3 AE 58 BD 4A 8C 86 F0 C1 A8 0E
            1A 8D 7A E0 BF 07 ED 16 88 2E B9 D3 0C 77 89 89 3A 4A F1 DE
            58 ED 00 7C 0E F1 73 7D 42 E0 49 F5 90 B2 6D F3 19 C6 D9 9B
            BB 1B 53 7B 3B 60 D4 0E C1 4B 85 32 C8 0E 0B 8E 03
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 82 96 8B 07 1D B4 81 F7 7D DC 3E 89 1A ED 71 3F A4 89 66
           97 AE 96 9F 93 01 02 0E 7E 8E 1F C1 70 5A C2 3F 82 66 8B 5A
           1B 67 BD 79 6E 64 8E 24 78 D4 07 7A 70 1A 84 48 99 3D EE 77
           B6 00 B2 70 C5 2B 40 9D 30 13 DC CF 00 78 07 A1 23 98 58 9D
           36 4F 9D 55 98 BE C9 AC 98 85 5F F3 ED 6F 91 B6 51 13 43 EA
           E4 37 6D 63 50 3F 85 A7 55 0E A1 8A 15 0B D2 BB E4 FC 4F F1
           73 04 60 86 5E 7F 06 20 D9 55 24 62 23 8C A4 C9 1D 2B 7 [...]
```

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

Plugin Output

tcp/143/imap

```
Subject Name:

Common Name: *.prod.sin2.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 6F 4B 2B DE 9E 8C F8 0D

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 23:12:17 2023 GMT
Not Valid After: Feb 29 23:12:17 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B3 D4 3A 93 73 C1 D4 0E 40 89 C2 EA 82 B2 6F 3E 96 C8 E0
            49 EA 80 E5 DB 0D 75 00 7B C1 76 6F 4D 43 05 4D 4E 54 04 42
            FD 04 89 E2 27 B8 E9 1C 62 3B 35 C3 5F 4E C8 30 B4 EC 1E 81
            58 98 C4 BC 6F 58 3D 1A A0 4C EE EF 06 36 64 4F 20 DD F5 AC
            C5 42 38 D7 2F F7 0A 08 A0 A2 CA 0E 1A D4 8E 6E 04 90 5E 32
            6C 7F 1B E9 4A 5C 19 79 82 D5 4C A5 22 71 6A 43 CC 11 B3 FE
            C8 98 3A 84 68 E1 5C 68 43 85 63 7E 29 48 E4 94 FF 38 94 2D
            2D 3B CE 3E 9A 55 7D 7B 87 8A 40 8A F2 CB 61 2C A4 B8 D2 2F
            66 C7 6F 5D 37 0C 5A 2A 9C C5 C1 2E 0E BA E3 CF 9E C8 0C C1
            AC 90 79 0D 7A 20 C0 F5 B4 B3 AE 58 BD 4A 8C 86 F0 C1 A8 0E
            1A 8D 7A E0 BF 07 ED 16 88 2E B9 D3 0C 77 89 89 3A 4A F1 DE
            58 ED 00 7C 0E F1 73 7D 42 E0 49 F5 90 B2 6D F3 19 C6 D9 9B
            BB 1B 53 7B 3B 60 D4 0E C1 4B 85 32 C8 0E 0B 8E 03
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 82 96 8B 07 1D B4 81 F7 7D DC 3E 89 1A ED 71 3F A4 89 66
           97 AE 96 9F 93 01 02 0E 7E 8E 1F C1 70 5A C2 3F 82 66 8B 5A
           1B 67 BD 79 6E 64 8E 24 78 D4 07 7A 70 1A 84 48 99 3D EE 77
           B6 00 B2 70 C5 2B 40 9D 30 13 DC CF 00 78 07 A1 23 98 58 9D
           36 4F 9D 55 98 BE C9 AC 98 85 5F F3 ED 6F 91 B6 51 13 43 EA
           E4 37 6D 63 50 3F 85 A7 55 0E A1 8A 15 0B D2 BB E4 FC 4F F1
           73 04 60 86 5E 7F 06 20 D9 55 24 62 23 8C A4 C9 1D 2B 7 [...]
```

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

Plugin Output

tcp/443/www

```
Subject Name:

Common Name: bvrmol.in

Issuer Name:

Country: US
State/Province: TX
Locality: Houston
Organization: cPanel, Inc.
Common Name: cPanel, Inc. Certification Authority

Serial Number: 32 D0 1E 1B 8F 4B E2 9C 6D EC F4 0E 75 36 F5 0F

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jul 06 00:00:00 2023 GMT
Not Valid After: Oct 04 23:59:59 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 D5 BD F8 02 EF 8D 6F A7 83 9E F5 95 3E 55 CA DA 9B 22 53
            87 6D AD C8 98 D4 C0 57 82 15 78 0B A4 50 BF 5F F6 D7 A5 8E
            1F 88 B0 A3 21 45 17 1E C4 50 95 53 DA 6A 64 F2 40 A7 0C 31
            22 70 0E ED 17 4B 7A 25 F8 87 ED 49 0D 4F 36 44 1E 22 D8 3C
            13 97 74 65 5A 36 4F 36 BB 4A 04 4C D0 58 DA A2 8D 9F 42 33
            4E D0 84 02 8A EF 0A EA 66 35 A9 0D A7 CE 61 68 35 57 00 B4
            8D 19 8A ED 05 DB 5A 30 49 1A FE 47 08 E8 71 98 04 3B 25 5D
            07 CF 7F 95 A6 EF D5 CD 1D 7E CB F4 6A 3B 2A 9B 2F D7 5D A9
            7F 4D AB A6 18 55 A6 FE 95 3F 98 43 CD D5 90 2C DC 40 C2 29
            F4 D0 4E E9 BF BD 7C 8B C9 DD 3D B0 1F D9 5D FB 4E D4 54 02
            8E D6 1C 59 B2 7D 56 D1 AC 6A 37 CD 0B A3 91 25 D4 FE F7 19
            14 C5 BF 9E 3B 15 44 EF B1 6E 60 57 74 2B F0 45 FA FD 07 A2
            E7 F4 4E A1 83 66 D5 03 E4 00 4C B2 B0 E5 64 66 37
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 22 46 7B 19 48 34 E7 1E D5 76 E2 62 A6 1D FD 36 4D B6 5B
           B3 66 C7 1A 37 04 5D AD FD 3A 2C 65 27 7E 09 92 A4 5A 08 1E
           BE 7C F2 04 D1 80 A3 ED D5 00 61 9B AE 27 1E A8 BE 03 62 B2
           D7 40 5A 43 36 8C EF 9A 9A EB 45 13 EA 65 E3 0F EA CE E2 6F
           FB 04 47 8C 69 D9 2A C9 8D FA 06 5E 2D 7D E4 25 46 CB EF D6
           F6 81 9F 7D 97 91 1F B9 31 5F 60 94 EC C2 98 54 20 74 98 DF
           BB 83 4B 4A 6A 31 4D 3C 7B 46 26 20 06 94 A7 04 8D F8 D8 66
           D6 4A 76 B0 30 57 65 16 57 03 8E EE 33 1A B6 83 EB B5 AF 30
           [...]
```

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

Plugin Output

tcp/465/smtp

```
Subject Name:

Common Name: *.prod.sin2.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 6F 4B 2B DE 9E 8C F8 0D

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 23:12:17 2023 GMT
Not Valid After: Feb 29 23:12:17 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B3 D4 3A 93 73 C1 D4 0E 40 89 C2 EA 82 B2 6F 3E 96 C8 E0
            49 EA 80 E5 DB 0D 75 00 7B C1 76 6F 4D 43 05 4D 4E 54 04 42
            FD 04 89 E2 27 B8 E9 1C 62 3B 35 C3 5F 4E C8 30 B4 EC 1E 81
            58 98 C4 BC 6F 58 3D 1A A0 4C EE EF 06 36 64 4F 20 DD F5 AC
            C5 42 38 D7 2F F7 0A 08 A0 A2 CA 0E 1A D4 8E 6E 04 90 5E 32
            6C 7F 1B E9 4A 5C 19 79 82 D5 4C A5 22 71 6A 43 CC 11 B3 FE
            C8 98 3A 84 68 E1 5C 68 43 85 63 7E 29 48 E4 94 FF 38 94 2D
            2D 3B CE 3E 9A 55 7D 7B 87 8A 40 8A F2 CB 61 2C A4 B8 D2 2F
            66 C7 6F 5D 37 0C 5A 2A 9C C5 C1 2E 0E BA E3 CF 9E C8 0C C1
            AC 90 79 0D 7A 20 C0 F5 B4 B3 AE 58 BD 4A 8C 86 F0 C1 A8 0E
            1A 8D 7A E0 BF 07 ED 16 88 2E B9 D3 0C 77 89 89 3A 4A F1 DE
            58 ED 00 7C 0E F1 73 7D 42 E0 49 F5 90 B2 6D F3 19 C6 D9 9B
            BB 1B 53 7B 3B 60 D4 0E C1 4B 85 32 C8 0E 0B 8E 03
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 82 96 8B 07 1D B4 81 F7 7D DC 3E 89 1A ED 71 3F A4 89 66
           97 AE 96 9F 93 01 02 0E 7E 8E 1F C1 70 5A C2 3F 82 66 8B 5A
           1B 67 BD 79 6E 64 8E 24 78 D4 07 7A 70 1A 84 48 99 3D EE 77
           B6 00 B2 70 C5 2B 40 9D 30 13 DC CF 00 78 07 A1 23 98 58 9D
           36 4F 9D 55 98 BE C9 AC 98 85 5F F3 ED 6F 91 B6 51 13 43 EA
           E4 37 6D 63 50 3F 85 A7 55 0E A1 8A 15 0B D2 BB E4 FC 4F F1
           73 04 60 86 5E 7F 06 20 D9 55 24 62 23 8C A4 C9 1D 2B 7 [...]
```

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

Plugin Output

tcp/993/imap

```
Subject Name:

Common Name: *.prod.sin2.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 6F 4B 2B DE 9E 8C F8 0D

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 23:12:17 2023 GMT
Not Valid After: Feb 29 23:12:17 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B3 D4 3A 93 73 C1 D4 0E 40 89 C2 EA 82 B2 6F 3E 96 C8 E0
            49 EA 80 E5 DB 0D 75 00 7B C1 76 6F 4D 43 05 4D 4E 54 04 42
            FD 04 89 E2 27 B8 E9 1C 62 3B 35 C3 5F 4E C8 30 B4 EC 1E 81
            58 98 C4 BC 6F 58 3D 1A A0 4C EE EF 06 36 64 4F 20 DD F5 AC
            C5 42 38 D7 2F F7 0A 08 A0 A2 CA 0E 1A D4 8E 6E 04 90 5E 32
            6C 7F 1B E9 4A 5C 19 79 82 D5 4C A5 22 71 6A 43 CC 11 B3 FE
            C8 98 3A 84 68 E1 5C 68 43 85 63 7E 29 48 E4 94 FF 38 94 2D
            2D 3B CE 3E 9A 55 7D 7B 87 8A 40 8A F2 CB 61 2C A4 B8 D2 2F
            66 C7 6F 5D 37 0C 5A 2A 9C C5 C1 2E 0E BA E3 CF 9E C8 0C C1
            AC 90 79 0D 7A 20 C0 F5 B4 B3 AE 58 BD 4A 8C 86 F0 C1 A8 0E
            1A 8D 7A E0 BF 07 ED 16 88 2E B9 D3 0C 77 89 89 3A 4A F1 DE
            58 ED 00 7C 0E F1 73 7D 42 E0 49 F5 90 B2 6D F3 19 C6 D9 9B
            BB 1B 53 7B 3B 60 D4 0E C1 4B 85 32 C8 0E 0B 8E 03
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 82 96 8B 07 1D B4 81 F7 7D DC 3E 89 1A ED 71 3F A4 89 66
           97 AE 96 9F 93 01 02 0E 7E 8E 1F C1 70 5A C2 3F 82 66 8B 5A
           1B 67 BD 79 6E 64 8E 24 78 D4 07 7A 70 1A 84 48 99 3D EE 77
           B6 00 B2 70 C5 2B 40 9D 30 13 DC CF 00 78 07 A1 23 98 58 9D
           36 4F 9D 55 98 BE C9 AC 98 85 5F F3 ED 6F 91 B6 51 13 43 EA
           E4 37 6D 63 50 3F 85 A7 55 0E A1 8A 15 0B D2 BB E4 FC 4F F1
           73 04 60 86 5E 7F 06 20 D9 55 24 62 23 8C A4 C9 1D 2B 7 [...]
```

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

Plugin Output

tcp/995/pop3

```
Subject Name:

Common Name: *.prod.sin2.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 6F 4B 2B DE 9E 8C F8 0D

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 23:12:17 2023 GMT
Not Valid After: Feb 29 23:12:17 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B3 D4 3A 93 73 C1 D4 0E 40 89 C2 EA 82 B2 6F 3E 96 C8 E0
            49 EA 80 E5 DB 0D 75 00 7B C1 76 6F 4D 43 05 4D 4E 54 04 42
            FD 04 89 E2 27 B8 E9 1C 62 3B 35 C3 5F 4E C8 30 B4 EC 1E 81
            58 98 C4 BC 6F 58 3D 1A A0 4C EE EF 06 36 64 4F 20 DD F5 AC
            C5 42 38 D7 2F F7 0A 08 A0 A2 CA 0E 1A D4 8E 6E 04 90 5E 32
            6C 7F 1B E9 4A 5C 19 79 82 D5 4C A5 22 71 6A 43 CC 11 B3 FE
            C8 98 3A 84 68 E1 5C 68 43 85 63 7E 29 48 E4 94 FF 38 94 2D
            2D 3B CE 3E 9A 55 7D 7B 87 8A 40 8A F2 CB 61 2C A4 B8 D2 2F
            66 C7 6F 5D 37 0C 5A 2A 9C C5 C1 2E 0E BA E3 CF 9E C8 0C C1
            AC 90 79 0D 7A 20 C0 F5 B4 B3 AE 58 BD 4A 8C 86 F0 C1 A8 0E
            1A 8D 7A E0 BF 07 ED 16 88 2E B9 D3 0C 77 89 89 3A 4A F1 DE
            58 ED 00 7C 0E F1 73 7D 42 E0 49 F5 90 B2 6D F3 19 C6 D9 9B
            BB 1B 53 7B 3B 60 D4 0E C1 4B 85 32 C8 0E 0B 8E 03
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 82 96 8B 07 1D B4 81 F7 7D DC 3E 89 1A ED 71 3F A4 89 66
           97 AE 96 9F 93 01 02 0E 7E 8E 1F C1 70 5A C2 3F 82 66 8B 5A
           1B 67 BD 79 6E 64 8E 24 78 D4 07 7A 70 1A 84 48 99 3D EE 77
           B6 00 B2 70 C5 2B 40 9D 30 13 DC CF 00 78 07 A1 23 98 58 9D
           36 4F 9D 55 98 BE C9 AC 98 85 5F F3 ED 6F 91 B6 51 13 43 EA
           E4 37 6D 63 50 3F 85 A7 55 0E A1 8A 15 0B D2 BB E4 FC 4F F1
           73 04 60 86 5E 7F 06 20 D9 55 24 62 23 8C A4 C9 1D 2B 7 [...]
```

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

Plugin Output

tcp/2078/www

```
Subject Name:

Common Name: *.prod.sin2.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 6F 4B 2B DE 9E 8C F8 0D

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 23:12:17 2023 GMT
Not Valid After: Feb 29 23:12:17 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B3 D4 3A 93 73 C1 D4 0E 40 89 C2 EA 82 B2 6F 3E 96 C8 E0
            49 EA 80 E5 DB 0D 75 00 7B C1 76 6F 4D 43 05 4D 4E 54 04 42
            FD 04 89 E2 27 B8 E9 1C 62 3B 35 C3 5F 4E C8 30 B4 EC 1E 81
            58 98 C4 BC 6F 58 3D 1A A0 4C EE EF 06 36 64 4F 20 DD F5 AC
            C5 42 38 D7 2F F7 0A 08 A0 A2 CA 0E 1A D4 8E 6E 04 90 5E 32
            6C 7F 1B E9 4A 5C 19 79 82 D5 4C A5 22 71 6A 43 CC 11 B3 FE
            C8 98 3A 84 68 E1 5C 68 43 85 63 7E 29 48 E4 94 FF 38 94 2D
            2D 3B CE 3E 9A 55 7D 7B 87 8A 40 8A F2 CB 61 2C A4 B8 D2 2F
            66 C7 6F 5D 37 0C 5A 2A 9C C5 C1 2E 0E BA E3 CF 9E C8 0C C1
            AC 90 79 0D 7A 20 C0 F5 B4 B3 AE 58 BD 4A 8C 86 F0 C1 A8 0E
            1A 8D 7A E0 BF 07 ED 16 88 2E B9 D3 0C 77 89 89 3A 4A F1 DE
            58 ED 00 7C 0E F1 73 7D 42 E0 49 F5 90 B2 6D F3 19 C6 D9 9B
            BB 1B 53 7B 3B 60 D4 0E C1 4B 85 32 C8 0E 0B 8E 03
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 82 96 8B 07 1D B4 81 F7 7D DC 3E 89 1A ED 71 3F A4 89 66
           97 AE 96 9F 93 01 02 0E 7E 8E 1F C1 70 5A C2 3F 82 66 8B 5A
           1B 67 BD 79 6E 64 8E 24 78 D4 07 7A 70 1A 84 48 99 3D EE 77
           B6 00 B2 70 C5 2B 40 9D 30 13 DC CF 00 78 07 A1 23 98 58 9D
           36 4F 9D 55 98 BE C9 AC 98 85 5F F3 ED 6F 91 B6 51 13 43 EA
           E4 37 6D 63 50 3F 85 A7 55 0E A1 8A 15 0B D2 BB E4 FC 4F F1
           73 04 60 86 5E 7F 06 20 D9 55 24 62 23 8C A4 C9 1D 2B 7 [...]
```

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

Plugin Output

tcp/2080/www

```
Subject Name:

Common Name: *.prod.sin2.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 6F 4B 2B DE 9E 8C F8 0D

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 23:12:17 2023 GMT
Not Valid After: Feb 29 23:12:17 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B3 D4 3A 93 73 C1 D4 0E 40 89 C2 EA 82 B2 6F 3E 96 C8 E0
            49 EA 80 E5 DB 0D 75 00 7B C1 76 6F 4D 43 05 4D 4E 54 04 42
            FD 04 89 E2 27 B8 E9 1C 62 3B 35 C3 5F 4E C8 30 B4 EC 1E 81
            58 98 C4 BC 6F 58 3D 1A A0 4C EE EF 06 36 64 4F 20 DD F5 AC
            C5 42 38 D7 2F F7 0A 08 A0 A2 CA 0E 1A D4 8E 6E 04 90 5E 32
            6C 7F 1B E9 4A 5C 19 79 82 D5 4C A5 22 71 6A 43 CC 11 B3 FE
            C8 98 3A 84 68 E1 5C 68 43 85 63 7E 29 48 E4 94 FF 38 94 2D
            2D 3B CE 3E 9A 55 7D 7B 87 8A 40 8A F2 CB 61 2C A4 B8 D2 2F
            66 C7 6F 5D 37 0C 5A 2A 9C C5 C1 2E 0E BA E3 CF 9E C8 0C C1
            AC 90 79 0D 7A 20 C0 F5 B4 B3 AE 58 BD 4A 8C 86 F0 C1 A8 0E
            1A 8D 7A E0 BF 07 ED 16 88 2E B9 D3 0C 77 89 89 3A 4A F1 DE
            58 ED 00 7C 0E F1 73 7D 42 E0 49 F5 90 B2 6D F3 19 C6 D9 9B
            BB 1B 53 7B 3B 60 D4 0E C1 4B 85 32 C8 0E 0B 8E 03
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 82 96 8B 07 1D B4 81 F7 7D DC 3E 89 1A ED 71 3F A4 89 66
           97 AE 96 9F 93 01 02 0E 7E 8E 1F C1 70 5A C2 3F 82 66 8B 5A
           1B 67 BD 79 6E 64 8E 24 78 D4 07 7A 70 1A 84 48 99 3D EE 77
           B6 00 B2 70 C5 2B 40 9D 30 13 DC CF 00 78 07 A1 23 98 58 9D
           36 4F 9D 55 98 BE C9 AC 98 85 5F F3 ED 6F 91 B6 51 13 43 EA
           E4 37 6D 63 50 3F 85 A7 55 0E A1 8A 15 0B D2 BB E4 FC 4F F1
           73 04 60 86 5E 7F 06 20 D9 55 24 62 23 8C A4 C9 1D 2B 7 [...]
```

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

Plugin Output

tcp/2083/www

```
Subject Name:

Common Name: *.prod.sin2.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 6F 4B 2B DE 9E 8C F8 0D

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 23:12:17 2023 GMT
Not Valid After: Feb 29 23:12:17 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B3 D4 3A 93 73 C1 D4 0E 40 89 C2 EA 82 B2 6F 3E 96 C8 E0
            49 EA 80 E5 DB 0D 75 00 7B C1 76 6F 4D 43 05 4D 4E 54 04 42
            FD 04 89 E2 27 B8 E9 1C 62 3B 35 C3 5F 4E C8 30 B4 EC 1E 81
            58 98 C4 BC 6F 58 3D 1A A0 4C EE EF 06 36 64 4F 20 DD F5 AC
            C5 42 38 D7 2F F7 0A 08 A0 A2 CA 0E 1A D4 8E 6E 04 90 5E 32
            6C 7F 1B E9 4A 5C 19 79 82 D5 4C A5 22 71 6A 43 CC 11 B3 FE
            C8 98 3A 84 68 E1 5C 68 43 85 63 7E 29 48 E4 94 FF 38 94 2D
            2D 3B CE 3E 9A 55 7D 7B 87 8A 40 8A F2 CB 61 2C A4 B8 D2 2F
            66 C7 6F 5D 37 0C 5A 2A 9C C5 C1 2E 0E BA E3 CF 9E C8 0C C1
            AC 90 79 0D 7A 20 C0 F5 B4 B3 AE 58 BD 4A 8C 86 F0 C1 A8 0E
            1A 8D 7A E0 BF 07 ED 16 88 2E B9 D3 0C 77 89 89 3A 4A F1 DE
            58 ED 00 7C 0E F1 73 7D 42 E0 49 F5 90 B2 6D F3 19 C6 D9 9B
            BB 1B 53 7B 3B 60 D4 0E C1 4B 85 32 C8 0E 0B 8E 03
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 82 96 8B 07 1D B4 81 F7 7D DC 3E 89 1A ED 71 3F A4 89 66
           97 AE 96 9F 93 01 02 0E 7E 8E 1F C1 70 5A C2 3F 82 66 8B 5A
           1B 67 BD 79 6E 64 8E 24 78 D4 07 7A 70 1A 84 48 99 3D EE 77
           B6 00 B2 70 C5 2B 40 9D 30 13 DC CF 00 78 07 A1 23 98 58 9D
           36 4F 9D 55 98 BE C9 AC 98 85 5F F3 ED 6F 91 B6 51 13 43 EA
           E4 37 6D 63 50 3F 85 A7 55 0E A1 8A 15 0B D2 BB E4 FC 4F F1
           73 04 60 86 5E 7F 06 20 D9 55 24 62 23 8C A4 C9 1D 2B 7 [...]
```

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

Plugin Output

tcp/2096/www

```
Subject Name:

Common Name: *.prod.sin2.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 6F 4B 2B DE 9E 8C F8 0D

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 23:12:17 2023 GMT
Not Valid After: Feb 29 23:12:17 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B3 D4 3A 93 73 C1 D4 0E 40 89 C2 EA 82 B2 6F 3E 96 C8 E0
            49 EA 80 E5 DB 0D 75 00 7B C1 76 6F 4D 43 05 4D 4E 54 04 42
            FD 04 89 E2 27 B8 E9 1C 62 3B 35 C3 5F 4E C8 30 B4 EC 1E 81
            58 98 C4 BC 6F 58 3D 1A A0 4C EE EF 06 36 64 4F 20 DD F5 AC
            C5 42 38 D7 2F F7 0A 08 A0 A2 CA 0E 1A D4 8E 6E 04 90 5E 32
            6C 7F 1B E9 4A 5C 19 79 82 D5 4C A5 22 71 6A 43 CC 11 B3 FE
            C8 98 3A 84 68 E1 5C 68 43 85 63 7E 29 48 E4 94 FF 38 94 2D
            2D 3B CE 3E 9A 55 7D 7B 87 8A 40 8A F2 CB 61 2C A4 B8 D2 2F
            66 C7 6F 5D 37 0C 5A 2A 9C C5 C1 2E 0E BA E3 CF 9E C8 0C C1
            AC 90 79 0D 7A 20 C0 F5 B4 B3 AE 58 BD 4A 8C 86 F0 C1 A8 0E
            1A 8D 7A E0 BF 07 ED 16 88 2E B9 D3 0C 77 89 89 3A 4A F1 DE
            58 ED 00 7C 0E F1 73 7D 42 E0 49 F5 90 B2 6D F3 19 C6 D9 9B
            BB 1B 53 7B 3B 60 D4 0E C1 4B 85 32 C8 0E 0B 8E 03
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 82 96 8B 07 1D B4 81 F7 7D DC 3E 89 1A ED 71 3F A4 89 66
           97 AE 96 9F 93 01 02 0E 7E 8E 1F C1 70 5A C2 3F 82 66 8B 5A
           1B 67 BD 79 6E 64 8E 24 78 D4 07 7A 70 1A 84 48 99 3D EE 77
           B6 00 B2 70 C5 2B 40 9D 30 13 DC CF 00 78 07 A1 23 98 58 9D
           36 4F 9D 55 98 BE C9 AC 98 85 5F F3 ED 6F 91 B6 51 13 43 EA
           E4 37 6D 63 50 3F 85 A7 55 0E A1 8A 15 0B D2 BB E4 FC 4F F1
           73 04 60 86 5E 7F 06 20 D9 55 24 62 23 8C A4 C9 1D 2B 7 [...]
```

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 sunsetting 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/110/pop3

```
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=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:39:16 2004 GMT
Valid To            : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLj
+6XGmBIWtDBFk385N78gDGIc/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDIr1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azbl5KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPUxA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvggQQto8PT7dL5WXXp59fkdheMtlb71cZBDzI0fmgAKhynpVSJYACPq4xJDKVtHCN2MQWplBq
D5fs4C8fF5Q=
-----END CERTIFICATE-----
```

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 sunsetting 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/143/imap

```
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=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:39:16 2004 GMT
Valid To            : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLj
+6XGmBIWtDBFk385N78gDGIc/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDIr1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azbl5KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPUxA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvggQQto8PT7dL5WXXp59fkdheMtlb71cZBDzI0fmgAKhynpVSJYACPq4xJDKVtHCN2MQWplB
D5fs4C8fF5Q=
-----END CERTIFICATE-----
```

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 sunsetting 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-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMGh
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjgo
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

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 sunsetting 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/465/smtp

```
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=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:39:16 2004 GMT
Valid To            : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLj
+6XGmBIWtDBFk385N78gDGIc/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDIr1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azbl5KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPUxA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvggQQto8PT7dL5WXXp59fkdheMtlb71cZBDzI0fmgAKhynpVSJYACPq4xJDKVtHCN2MQWplBq
D5fs4C8fF5Q=
-----END CERTIFICATE-----
```

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 sunsetting 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/993/imap

```
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=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:39:16 2004 GMT
Valid To            : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLj
+6XGmBIWtDBFk385N78gDGIc/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDIr1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azbl5KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPUxA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvggQQto8PT7dL5WXXp59fkdheMtlb71cZBDzI0fmgAKhynpVSJYACPq4xJDKVtHCN2MQWplB
D5fs4C8fF5Q=
-----END CERTIFICATE-----
```

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 sunsetting 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/995/pop3

```
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=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:39:16 2004 GMT
Valid To            : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLj
+6XGmBIWtDBFk385N78gDGIc/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDIr1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azbl5KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPUxA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvggQQto8PT7dL5WXXp59fkdheMtlb71cZBDzI0fmgAKhynpVSJYACPq4xJDKVtHCN2MQWplB
D5fs4C8fF5Q=
-----END CERTIFICATE-----
```

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 sunsetting 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/2078/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=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:39:16 2004 GMT
Valid To            : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLj
+6XGmBIWtDBFk385N78gDGIc/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDIr1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azbl5KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPUxA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvggQQto8PT7dL5WXXp59fkdheMtlb71cZBDzI0fmgAKhynpVSJYACPq4xJDKVtHCN2MQWplB
D5fs4C8fF5Q=
-----END CERTIFICATE-----
```

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 sunsetting 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/2080/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=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:39:16 2004 GMT
Valid To            : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
```

```
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLj
+6XGmBIWtDBFk385N78gDGIc/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDIr1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azbl5KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPUxA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvggQQto8PT7dL5WXXp59fkdheMtlb71cZBDzI0fmgAKhynpVSJYACPq4xJDKVtHCN2MQWplBq
D5fs4C8fF5Q=
```

```
-----END CERTIFICATE-----
```

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 sunsetting 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/2083/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=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:39:16 2004 GMT
Valid To            : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLj
+6XGmBIWtDBFk385N78gDGIc/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDIr1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azbl5KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPUxA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvggQQto8PT7dL5WXXp59fkdheMtlb71cZBDzI0fmgAKhynpVSJYACPq4xJDKVtHCN2MQWplBq
D5fs4C8fF5Q=
-----END CERTIFICATE-----
```

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 sunsetting 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/2096/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=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:39:16 2004 GMT
Valid To            : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLj
+6XGmBIWtDBFk385N78gDGIc/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDIr1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azbl5KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPUxA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvggQQto8PT7dL5WXXp59fkdheMtlb71cZBDzI0fmgAKhynpVSJYACPq4xJDKVtHCN2MQWplBq
D5fs4C8fF5Q=
-----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
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-CAMELLIA-CBC-128    0xC0, 0x76       ECDH          RSA      Camellia-CBC(128)
 SHA256
    ECDHE-RSA-CAMELLIA-CBC-256    0xC0, 0x77       ECDH          RSA      Camellia-CBC(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
    DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH            RSA      Camellia-CBC(128)
 SHA1
```

```
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH            RSA      Camellia-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
   AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
SHA1
   AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA               0x00, 0x41       RSA           RSA      Camellia-CBC(128)
SHA1
   CAMELLIA256-SHA               0x00, 0x84       RSA           RSA      Camellia-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
   DHE-RSA-CAMELLIA128-SHA256    0x00, 0xBE       DH            RSA      Camellia-CBC(128)
SHA256
   DHE-RSA-CAMELLIA256-SHA256    0x00, 0xC4       DH            RSA      Camellia-CBC(256)
SHA256
   ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)     [...]
```

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.html

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/110/pop3

```

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

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

The fields above are :

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

Note that this service does not encrypt traffic by default but does
support upgrading to an encrypted connection using STARTTLS.
```

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.html

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/143/imap

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

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

The fields above are :

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

Note that this service does not encrypt traffic by default but does
support upgrading to an encrypted connection using STARTTLS.
```

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.html

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 the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES-128-CCM-AEAD      0xC0, 0x9E       DH            RSA      AES-CCM(128)
 AEAD
    DHE-RSA-AES-128-CCM8-AEAD     0xC0, 0xA2       DH            RSA      AES-CCM8(128)
 AEAD
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES-256-CCM-AEAD      0xC0, 0x9F       DH            RSA      AES-CCM(256)
 AEAD
    DHE-RSA-AES-256-CCM8-AEAD     0xC0, 0xA3       DH            RSA      AES-CCM8(256)
 AEAD
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    DHE-RSA-CHACHA20-POLY1305     0xCC, 0xAA       DH            RSA      ChaCha20-Poly1305(256)
 SHA256
```

```
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-CAMELLIA-CBC-128    0xC0, 0x76       ECDH          RSA      Camellia-CBC(128)
SHA256
   ECDHE-RSA-CAMELLIA-CBC-256    0xC0, 0x77       ECDH          RSA      Camellia-CBC(256)
SHA384
   ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
SHA256
   RSA-AES-128-CCM-AEAD          0xC0, 0x9C       RSA           RSA      AES-CCM(128)
AEAD
   RSA-AES-128-CCM8-AEAD         0xC0, 0xA0       RSA           RSA      AES-CCM8(128)
AEAD
   RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
SHA256
   RSA-AES-256-CCM-AEAD          0xC0, 0x9D       RSA           RSA      AES-CCM(256)
AEAD
   RSA-AES-256-CCM8-AEAD   [...]
```

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.html

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/465/smtp

```

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

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

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
```

```
    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.html

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/993/imap

```

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

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

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
```

```
    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.html

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/995/pop3

```

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

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

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
```

```
    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.html

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/2078/www

```

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

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

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
```

```
    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.html

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/2080/www

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

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

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
```

```
    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.html

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/2083/www

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

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

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
```

```
    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.html

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/2096/www

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

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

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
```

```
    Encrypt={symmetric encryption method}
    MAC={message authentication code}
    {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

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/110/pop3

```

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

The fields above are :
  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

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/143/imap

```

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

The fields above are :
  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

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/www

```
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-AES-128-CCM-AEAD      0xC0, 0x9E       DH            RSA      AES-CCM(128)
 AEAD
    DHE-RSA-AES-128-CCM8-AEAD     0xC0, 0xA2       DH            RSA      AES-CCM8(128)
 AEAD
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES-256-CCM-AEAD      0xC0, 0x9F       DH            RSA      AES-CCM(256)
 AEAD
    DHE-RSA-AES-256-CCM8-AEAD     0xC0, 0xA3       DH            RSA      AES-CCM8(256)
 AEAD
```

```
   DHE-RSA-AES256-SHA384          0x00, 0x9F       DH            RSA      AES-GCM(256)
SHA384
   DHE-RSA-CHACHA20-POLY1305      0xCC, 0xAA       DH            RSA      ChaCha20-Poly1305(256)
SHA256
   ECDHE-RSA-AES128-SHA256        0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384        0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-CAMELLIA-CBC-128     0xC0, 0x76       ECDH          RSA      Camellia-CBC(128)
SHA256
   ECDHE-RSA-CAMELLIA-CBC-256     0xC0, 0x77       ECDH          RSA      Camellia-CBC(256)
SHA384
   ECDHE-RSA-CHACHA20-POLY1305    0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
SHA256
   DHE-RSA-AES128-SHA             0x00, 0x33       DH            RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA             0x00, 0x39       DH            RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA        0x00, 0x45       DH            RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA        0x00, 0x88       DH            RSA      Camellia-CBC(256)
SHA1
   ECDHE-RSA-AES128-SHA           0xC0, 0x13       ECDH          RSA      AES-CBC(128) [...]
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

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/465/smtp

```

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

The fields above are :
  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

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/993/imap

```

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

The fields above are :
  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

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/995/pop3

```

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

The fields above are :
  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

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/2078/www

```

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

The fields above are :
  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

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/2080/www

```
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

The fields above are :
  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

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/2083/www

```

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

The fields above are :
  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

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/2096/www

```

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

The fields above are :
  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication 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)

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/110/pop3

```
The following root Certification Authority certificate was found :

|-Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Issuer              : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Valid From          : Jun 29 17:39:16 2004 GMT
|-Valid To            : Jun 29 17:39:16 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

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)

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/143/imap

```
The following root Certification Authority certificate was found :

|-Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Issuer              : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Valid From          : Jun 29 17:39:16 2004 GMT
|-Valid To            : Jun 29 17:39:16 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

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)

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 Certificate
 Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

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)

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/465/smtp

```
The following root Certification Authority certificate was found :

|-Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Issuer              : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Valid From          : Jun 29 17:39:16 2004 GMT
|-Valid To            : Jun 29 17:39:16 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

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)

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/993/imap

```

The following root Certification Authority certificate was found :

|-Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Issuer              : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Valid From          : Jun 29 17:39:16 2004 GMT
|-Valid To            : Jun 29 17:39:16 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

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)

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/995/pop3

```
The following root Certification Authority certificate was found :

|-Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Issuer              : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Valid From          : Jun 29 17:39:16 2004 GMT
|-Valid To            : Jun 29 17:39:16 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

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)

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/2078/www

```
The following root Certification Authority certificate was found :

|-Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Issuer              : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Valid From          : Jun 29 17:39:16 2004 GMT
|-Valid To            : Jun 29 17:39:16 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

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)

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/2080/www

```
The following root Certification Authority certificate was found :

|-Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Issuer              : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Valid From          : Jun 29 17:39:16 2004 GMT
|-Valid To            : Jun 29 17:39:16 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

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)

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/2083/www

```

The following root Certification Authority certificate was found :

|-Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Issuer              : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Valid From          : Jun 29 17:39:16 2004 GMT
|-Valid To            : Jun 29 17:39:16 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

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)

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/2096/www

```
The following root Certification Authority certificate was found :

|-Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Issuer              : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Valid From          : Jun 29 17:39:16 2004 GMT
|-Valid To            : Jun 29 17:39:16 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

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_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2023/07/10

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)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES-128-CCM-AEAD      0xC0, 0x9E       DH            RSA      AES-CCM(128)
 AEAD
    DHE-RSA-AES-128-CCM8-AEAD     0xC0, 0xA2       DH            RSA      AES-CCM8(128)
 AEAD
    DHE-RSA-AES-256-CCM-AEAD      0xC0, 0x9F       DH            RSA      AES-CCM(256)
 AEAD
    DHE-RSA-AES-256-CCM8-AEAD     0xC0, 0xA3       DH            RSA      AES-CCM8(256)
 AEAD
    ECDHE-RSA-CAMELLIA-CBC-128    0xC0, 0x76       ECDH          RSA      Camellia-CBC(128)
 SHA256
    ECDHE-RSA-CAMELLIA-CBC-256    0xC0, 0x77       ECDH          RSA      Camellia-CBC(256)
 SHA384
    RSA-AES-128-CCM-AEAD          0xC0, 0x9C       RSA           RSA      AES-CCM(128)
 AEAD
    RSA-AES-128-CCM8-AEAD         0xC0, 0xA0       RSA           RSA      AES-CCM8(128)
 AEAD
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
    RSA-AES-256-CCM-AEAD          0xC0, 0x9D       RSA           RSA      AES-CCM(256)
 AEAD
    RSA-AES-256-CCM8-AEAD         0xC0, 0xA1       RSA           RSA      AES-CCM8(256)
 AEAD
    RSA-AES256-SHA384             0x00, 0x9D       RSA           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
    DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH            RSA      Camellia-CBC(128)
 SHA1
    DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH            RSA      Camellia-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH   [...]
```

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/21/ftp

```
An FTP server is running on this port.
```

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/22/ssh

```
An SSH server is running on this port.
```

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/80/www

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

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/110/pop3

```
A POP3 server is running on this port.
```

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/143/imap

```
An IMAP server is running on this port.
```

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

```
A TLSv1.2 server answered on this port.
```

tcp/443/www

```
A web server is running on this port through TLSv1.2.
```

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/465/smtp

```
A TLSv1.2 server answered on this port.
```

tcp/465/smtp

```
An SMTP server is running on this port through TLSv1.2.
```

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/587/smtp

```
An SMTP server is running on this port.
```

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/993/imap

```
A TLSv1.2 server answered on this port.
```

tcp/993/imap

```
An IMAP server is running on this port through TLSv1.2.
```

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/995/pop3

```
A POP3 server is running on this port through TLSv1.2.
```

tcp/995/pop3

```
A TLSv1.2 server answered on this port.
```

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/2078/www

```
A TLSv1.2 server answered on this port.
```

tcp/2078/www

```
A web server is running on this port through TLSv1.2.
```

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/2080/www

```
A TLSv1.2 server answered on this port.
```

tcp/2080/www

```
A web server is running on this port through TLSv1.2.
```

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/2083/www

```
A TLSv1.2 server answered on this port.
```

tcp/2083/www

```
A web server is running on this port through TLSv1.2.
```

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/2096/www

```
A TLSv1.2 server answered on this port.
```

tcp/2096/www

```
A web server is running on this port through TLSv1.2.
```

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/3306/mysql

```
A MySQL server is running on this port.
```

84821 - TLS ALPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS ALPN extension.

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

See Also

https://tools.ietf.org/html/rfc7301

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/17, Modified: 2023/07/10

Plugin Output

tcp/443/www

```
http/1.1
h2
```

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/110/pop3

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

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/143/imap

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

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

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

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/465/smtp

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

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/993/imap

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

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/995/pop3

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

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/2078/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

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/2080/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

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/2083/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

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/2096/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2023/02/13

Plugin Output

tcp/0

```
SSH was detected on port 22 but no credentials were provided.
SSH local checks were not enabled.
```

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

```
For your information, here is the traceroute from 192.168.29.162 to 68.178.231.130 :
192.168.29.162

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.
An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

ttl was greater than 50 - Completing Traceroute.
192.168.29.1
10.248.88.1
172.31.2.118
192.168.171.114
172.17.185.180
172.17.185.163
192.168.90.140
?
180.87.107.0
?

Hop Count: 11
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/80/www

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 301
rather than 404. The requested URL was :

    http://130.231.178.68.host.secureserver.net/KY0YiAUz26tz.html
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/2083/www

```
The following string will be used :
TYPE="password"
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/2096/www

```
The following string will be used :
TYPE="password"
```

11424 - WebDAV Detection

Synopsis

The remote server is running with WebDAV enabled.

Description

WebDAV is an industry standard extension to the HTTP specification.
It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

Solution

http://support.microsoft.com/default.aspx?kbid=241520

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2011/03/14

Plugin Output

tcp/2078/www

Part 3

Achieving Proactive Cybersecurity with SOC and SIEM Integration

- **Soc**

SOC plays a crucial role in continuously monitoring an organization's network, systems, and applications. It can detect and respond to potential security incidents, including malware infections, data breaches, and unauthorized access attempts. When a security incident occurs, time is of the essence. SOC teams are trained to respond swiftly and effectively to contain and mitigate the damage caused by security breaches. SOC doesn't merely react to incidents; it proactively identifies vulnerabilities and weaknesses in the organization's infrastructure. This proactive approach enables companies to strengthen their security posture and implement measures to prevent future attacks. SOC provides 24/7 monitoring, ensuring that security analysts are constantly vigilant and ready to respond to emerging threats, regardless of the time of day. SOC is a critical component of a robust cybersecurity strategy. It empowers organizations todetect, respond to, and prevent cyber threats, safeguarding sensitive data, maintaining business continuity, and preserving the organization's reputation in an increasingly interconnected and threat-prone digital landscape. SOC acts as the central hub for incident coordination and communication. It facilitates collaboration among various teams, such as IT, legal, communications, and executive management, ensuring a cohesive and efficient response to security incidents.

- **SOC - cycle**

The SOC (Security Operations Center) cycle, also known as the SOC lifecycle or SOC workflow, is a continuous process that outlines the key steps involved in managing an organization's cybersecurity. It encompassesactivities from threat detection to incident response and recovery. The SOC cycle typically consists of the following stages:

Threat Detection and Monitoring:

Continuous monitoring of the organization's network, systems, and applications to identify potential security threats and anomalies.

Leveraging various security tools, such as intrusion detection systems(IDS), intrusion prevention systems (IPS), firewalls, SIEM (Security Information and Event Management) solutions, and threat intelligence feeds.

Alert Triage and Analysis:

Analyzing and prioritizing security alerts generated by the monitoring tools based on their severity and potential impact.

Determining if an alert indicates a genuine security incident or a false positive.

Incident Investigation and Response:

If an alert is confirmed as a legitimate security incident, the SOC team conducts a thorough investigation to understand the nature andextent of the attack.

Gathering evidence, analyzing log data, and performing digital forensics to determine the source and impact of the incident.

Initiating the incident response process, which may involve isolating affected systems, containing the threat, and preventing further damage.

Incident Containment and Eradication:

Taking immediate actions to contain the incident and prevent it fromspreading further within the organization's network.

Removing the malicious elements and eradicating the threat torestore the affected systems to a secure state.

Recovery and Remediation:

After the threat is eradicated, the SOC team focuses on restoringaffected systems and services to normal operation.

Implementing remediation measures to address the root cause of theincident and prevent similar attacks in the future.

Post-Incident Analysis and Lessons Learned:

Conducting a thorough post-mortem analysis of the incident to understand how it happened, what was the impact, and what steps were taken to respond.

Identifying areas of improvement in the organization's security posture and incident response procedures.

Updating security policies and procedures based on the lessons learned from the incident.

Threat Intelligence and Proactive Measures:

Integrating threat intelligence into the SOC workflow to stay ahead of emerging threats and known attack patterns.

Proactively hunting for signs of potential threats and vulnerabilities before they lead to full-fledged security incidents.

Continuous Monitoring and Improvement:

The SOC cycle is a continuous process, with ongoing monitoring, analysis, and improvement of security measures to adapt to the evolving threat landscape.

By following this cycle, the SOC team can effectively detect, respond to, and recover from security incidents, minimizing the impact of cyber threats on the organization's assets and data.

- **SIEM**

SIEM Security information and event mangement, or SIEM, is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations. SIEM systems help enterprise security teams detect user behavior anomalies and use artificial intelligence (AI) to automate many of the manual processes associated with threat detection and incidentresponse.

Benefits Regardless of how large or small an organization may be, taking proactive steps to monitor for and mitigate IT security risks is essential. SIEM solutions benefit enterprises in a variety of ways and have become a significant component in streamlining security workflows.

Real-time threat recognition

SIEM solutions enable centralized compliance auditing and reporting across an entire business infrastructure. Advanced automation streamlines the collection and analysis of system logs and security events to reduce internal resource utilization while meeting strict compliance reporting standards.

AI-driven automation

Today's next-gen SIEM solutions integrate with powerful security orchestration, automation and response (SOAR) systems, saving time and resources for IT teams as they manage business security. Using deep machine learning that automatically learns from network behavior, these solutions can handle complex threat identification and incident response protocols in significantly less time than physical teams.

Improved organizational efficiency

Because of the improved visibility of IT environments that it provides,SIEM can be an essential driver of improving interdepartmental efficiencies. A central dashboard provides a unified view of system data, alerts and notifications, enabling teams to communicate and collaborate efficiently when responding to threats and security incidents.

Detecting advanced and unknown threats

Considering how quickly the cybersecurity landscape changes,organizations need to be able to rely on solutions that can detect and respond to both known and unknown security threats. Using integrated threat intelligence feeds and AI technology, SIEM solutions can help securityteams respond more effectively to a wide range of cyberattacks including:

Insider threats - security vulnerabilities or attacks that originate from individuals with authorized access to company networks and digital assets.

Phishing - messages that appear to be sent by a trusted sender, oftenused to steal user data, login credentials, financial information, or other sensitive business information.

Ransomware - malware that locks a victim’s data or device and threatens to keep it locked—or worse—unless the victim pays a ransom to the attacker.

Distributed denial of service (DDoS) attacks - attacks that bombard networks and systems with unmanageable levels of traffic from a distributed network of hijacked devices (botnet), degrading performance of websites and servers until they are unusable.

Data exfiltration – theft of data from a computer or other device, conducted manually, or automatically using malware.

Conducting forensic investigations

SIEM solutions are ideal for conducting computer forensic investigations once a security incident occurs. SIEM solutions allow organizations to efficiently collect and analyze log data from all of their digital assets in one place. This gives them the ability to recreate past incidents or analyze new ones to investigate suspicious activity and implement more effective security processes.

Assessing and reporting on compliance

Compliance auditing and reporting is both a necessary andchallenging task for many organizations. SIEM solutions dramatically reducethe resource expenditures required to manage this process by providing real-time audits and on-demand reporting of regulatory compliance whenever needed.

Monitoring Users and Applications

With the rise in popularity of remote workforces, SaaS applications and BYOD (bring your own device) policies, organizations need the level of visibility necessary to mitigate network risks from outside the traditional network perimeter. SIEM solutions track all network activity across all users,devices, and applications, significantly improving transparency across the entire infrastructure and detecting threats regardless of where digital assetsand services are being accessed.

F**ive Predictions For The Future Of SIEM**

1. Usage-based pricing models will become the norm. With these models, teams only pay for precisely the data throughput and processing incurred each month. This trend follows suit with cloud infrastructure platforms such as AWS and GCP and gives predictability to service usage. Pressure for security teams to reduce the amount of data they use will become a thing of the past.
2. The decoupling of SIEM platforms — which has already started withSOAR coming from SIEM and other extract, transform and load (ETL) tools will continue, and I suspect that the next phase would be building analysis tools on top of a universal SIEM data platform. This way, the companies building tools can focus on specific verticals and produce the most robust, high-quality and scalable software possible.
3. As decoupling continues to occur, security companies will create strong partnerships to provide an elegant integration and improve the time-to-value. These partnerships should help push the security industry forward, help with mutual company growth by referring customers to each other and ensure security teams have the best possible user experience.
4. The cost and complexity of a SIEM will continue to be reduced (perthe availability of cloud services), enabling smaller and newer security teams to get up to speed even quicker. With legacy SIEMs, it could take teams more than six months to get started, which means data onboarding, analysis and alerting integrations are non-trivial.

   Next-gen SIEMs can improve quality and simplicity, enabling security teams to move quickly and focus on the work that matters. This trend will continue to reduce startup time, which is critical for a business's bottom lineand a security team's efficiency.

5. More startups will continue to be funded to address the multifaceted challenges of upholding strong security. Venture funding is at an all-time high, and security breaches continue to be an issue for organizations of all sizes — including the large, sophisticated Fortune 1000 companies.

Healthy competition means that not a single company will own a majority of the market share. This competition gives security teams optionality and the freedom to move to other platforms as they see fit. Then, the battle will become about ease of use, capabilities and flexibility.

- **Siem Cycle**

The lifecycle of a Security Information and Event Management (SIEM)system involves several interconnected stages that ensure the effective implementation, operation, and maintenance of the SIEM solution. The SIEM life cycle typically includes the following phases:

Planning and Assessment:

Define the objectives and scope of the SIEM implementation, considering the organization's security requirements and compliance goals.

Conduct a thorough assessment of the existing security infrastructure,data sources, and log management practices to identify gaps and necessaryimprovements.

Develop a detailed plan for deploying the SIEM solution, including resource allocation, timeline, and responsibilities.

Design and Architecture:

Design the SIEM architecture based on the organization's requirements and data sources, considering factors like scalability, redundancy, and performance.

Determine the best deployment model (on-premises, cloud-based, hybrid) that aligns with the organization's needs and resources.

Plan the integration of data sources into the SIEM, ensuring that relevant security events are collected and centralized for analysis.

Data Collection and Integration:

Implement data collectors and agents to gather logs and events from various sources, such as firewalls, network devices, servers, applications, and endpoints. Normalize and enrich the collected data to facilitate efficient analysis and correlation. Configure connectors and parsers to integrate data feeds from security devices and other sources into the SIEM platform.

Event Correlation and Analysis:

Develop and fine-tune correlation rules and use cases to identifypatterns of malicious activity and security threats. Conduct real-time event correlation and analysis to generateactionable alerts for potential security incidents. Utilize threat intelligence feeds to enhance the SIEM's ability to detectemerging threats and known attack vectors.

Incident Detection and Response:

Respond to generated alerts by investigating potential security incidents. Perform detailed analysis to determine the scope and impact ofidentified security events. Initiate incident response activities, including containment, eradication, and recovery.

Forensics and Investigation:

Conduct in-depth forensics analysis to understand the root cause ofincidents and the methods used by attackers. Preserve and document evidence for potential legal or regulatory purposes.

Reporting and Compliance:

Generate and present security reports and dashboards for various stakeholders, including IT management, executives, auditors, and regulatory authorities. Ensure compliance with relevant industry standards and regulationsby monitoring and reporting on security events and incidents.

Continuous Monitoring and Maintenance:

Continuously monitor the SIEM infrastructure and adjust the configuration as needed to maintain optimal performance. Regularly update correlation rules, threat intelligence feeds, and othercomponents to keep the SIEM effective against evolving threats. Conduct periodic reviews and assessments of the SIEM's performanceand effectiveness to identify areas for improvement.

Training and Knowledge Transfer:

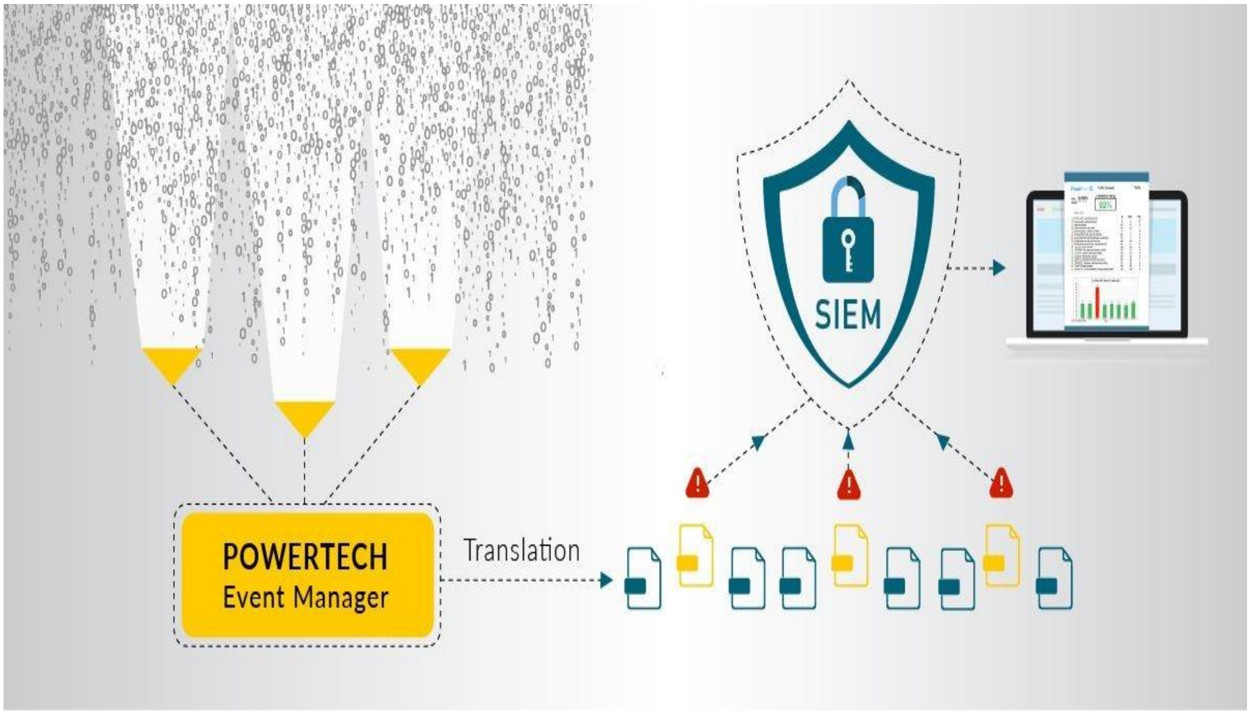
Train SOC personnel and IT staff on the effective use of the SIEM solution. Foster knowledge sharing and best practices from incident investigations and analysis within the organization.

The SIEM lifecycle is a continuous and iterative process, with each phase building upon the insights and experiences gained from previous stages. This approach ensures that the SIEM solution remains relevant, efficient, and effective in helping organizations detect and respond to security threats.

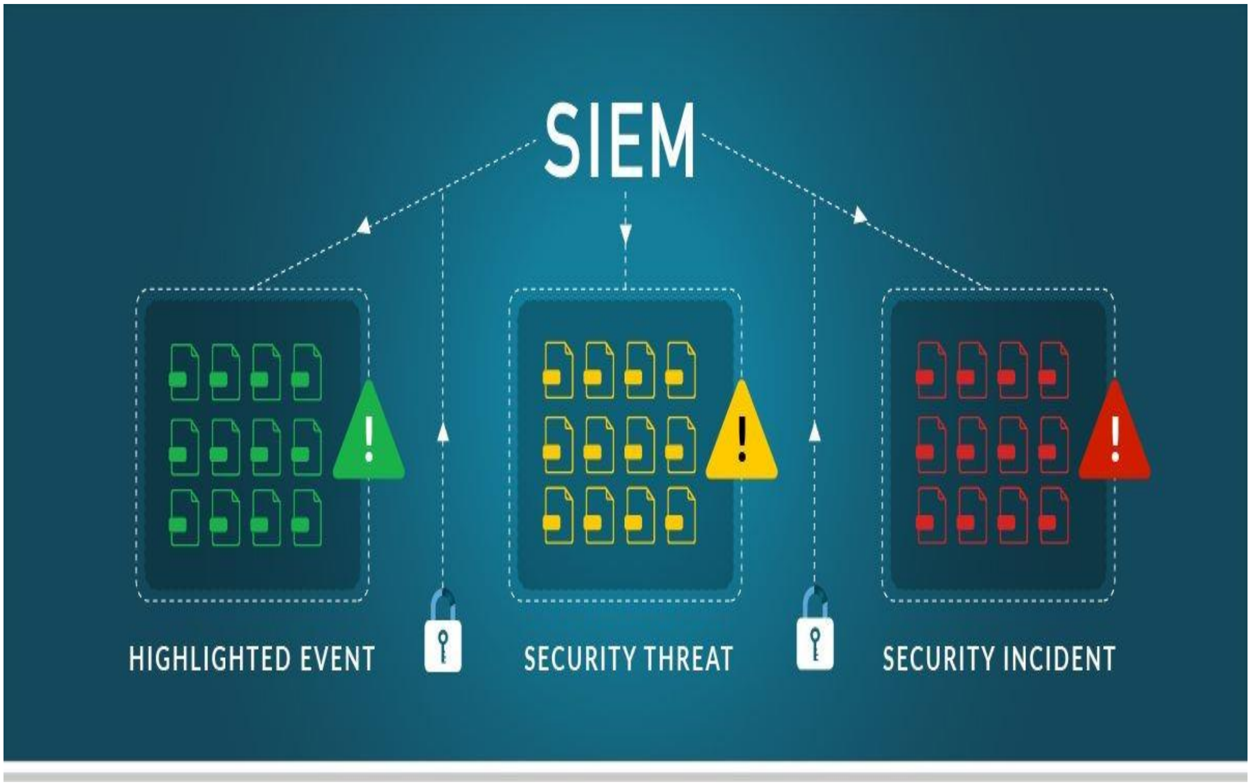
As a syslog server incessantly pings with every security notification, security teams can feel as though they are drowning in a sea of security warnings. Without a SIEM, it’s difficult to know which events are trulycritical and which can be ignored. However, when a SIEM has been implemented, security teams get a much clearer picture of theirenvironment’s security. There could truly be no threats, or multiple incidents may be occurring that simply have not yet affected performance.

Threat Detection

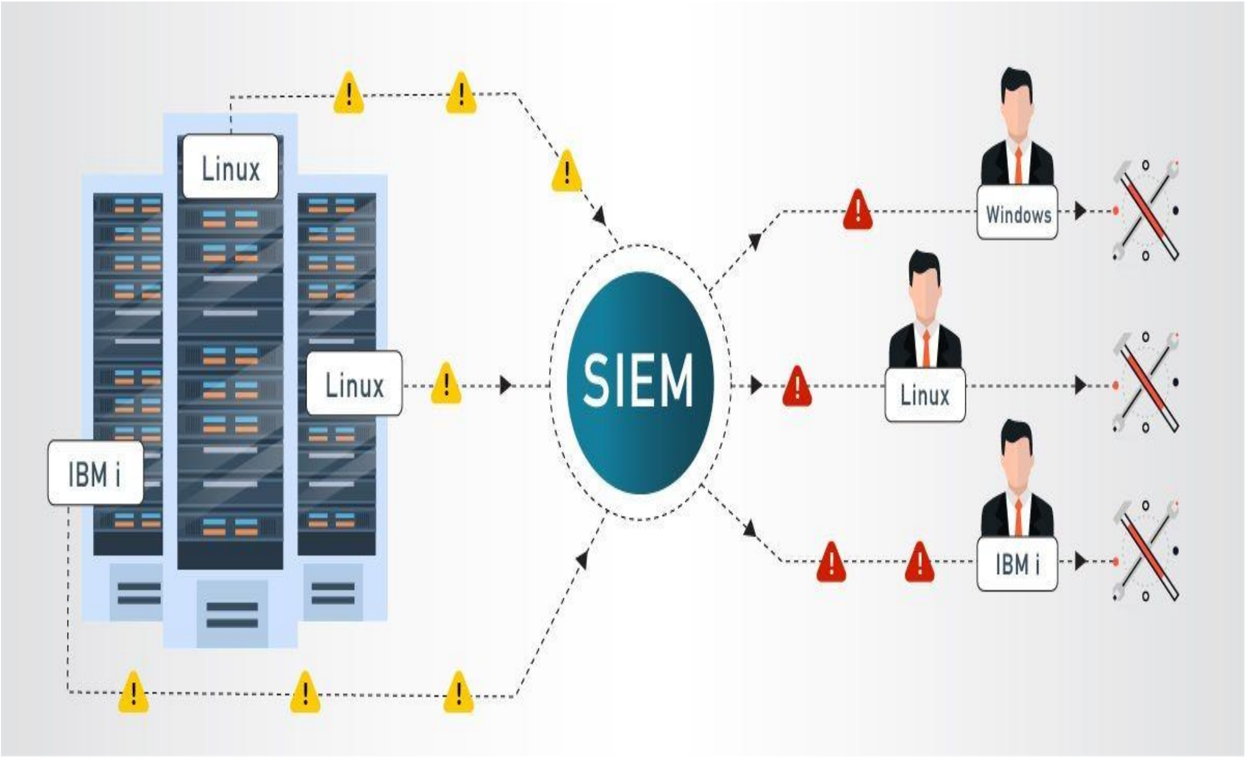
Translation



Prioritization


SIEM
HIGHLIGHTED EVENT
SECURITY THREAT
SECURITY INCIDENT

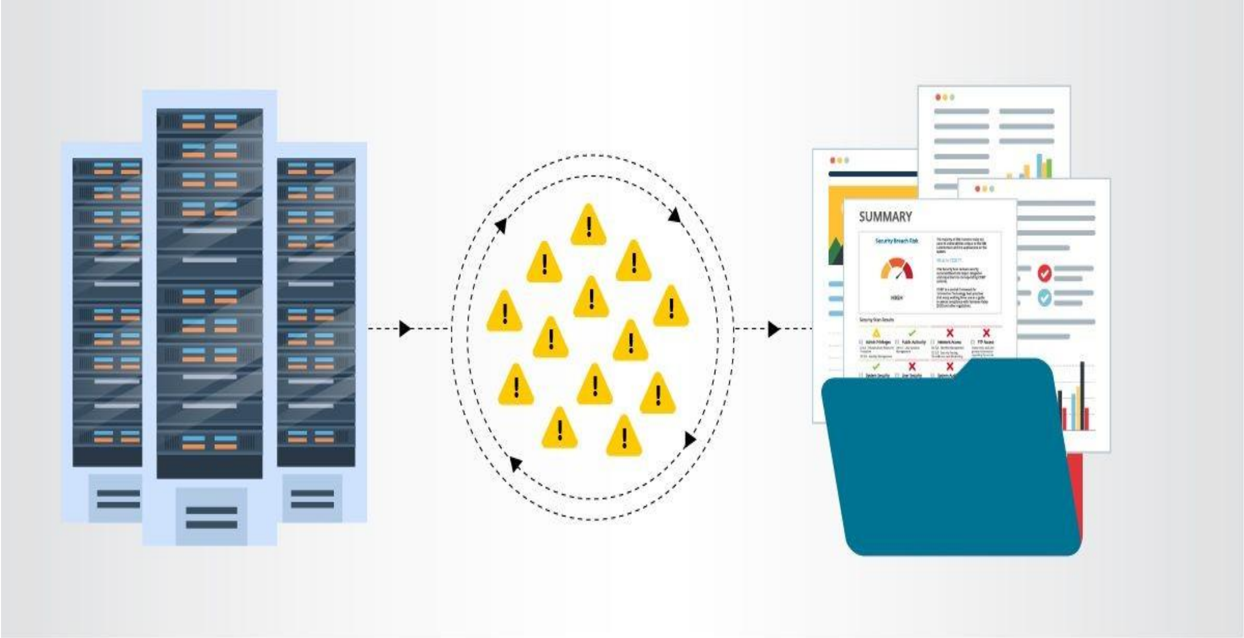
Escalation


Linux
Linux
IBM i
SIEM
Windows
Linux
IBM i

Analysis

SIEM
SUMMARY
Security Breach Risk
HIGH
REPORT

Compliance



- **MISP**

MISP, Malware Information Sharing Platform and Threat Sharing, corefunctionalities are:

An efficient IOC and indicators database, allowing to store technical and non-technical information about malware samples, incidents, attackers and intelligence.

Features of MISP, the open source threat sharing platform

A threat intelligence platform for sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information. Discover how MISP is used today in multiple organisations. Notonly to store, share, collaborate on cyber security indicators, malware analysis, but also to use the IoCs and information to detect and prevent attacks, frauds or threats against ICT infrastructures, organisations or people.

An efficient IoC and indicators database allowing to store technical and non-technical information about malware samples, incidents, attackers and intelligence.

Automatic correlation finding relationships between attributes and indicators from malware, attacks campaigns or analysis. Correlation engine includes correlation between attributes and more advanced correlations like Fuzzy hashing correlation (e.g. ssdeep) or CIDR block matching. Correlationcan be also enabled or event disabled per attribute.

A flexible data model where complex objects can be expressed and linked together to express threat intelligence, incidents or connected elements.

Built-in sharing functionality to ease data sharing using differentmodels of distributions. MISP can synchronize automatically events and attributes among different MISP. Advanced filtering functionalities can be used to meet each organization sharing policy including a flexible sharing group capacity and an attribute level distribution mechanism.

An intuitive user-interface for end-users to create, update and collaborate on events and attributes/indicators. A graphical interface to navigate seamlessly between events and their correlations. An event graph functionality to create and view relationships between objects and attributes. Advanced filtering functionalities and warning list to help the analysts to contribute events and attributes.

storing data in a structured format (allowing automated use of the database for various purposes) with an extensive support of cyber security indicators along fraud indicators as in the financial sector.

export: generating IDS (Suricata, Snort and Bro are supported by default), OpenIOC, plain text, CSV, MISP XML or JSON output to integrate with other systems (network IDS, host IDS, custom tools

import: bulk-import, batch-import, free-text import, import from OpenIOC, GFI sandbox, ThreatConnect CSV or MISP format.

Flexible free text import tool to ease the integration of unstructured reports into MISP.

A gentle system to collaborate on events and attributes allowing MISP usersto propose changes or updates to attributes/indicators.

Data-sharing: automatically exchange and synchronization with other parties and trust-groups using MISP.

Feed import: flexible tool to import and integrate MISP feed and any threatintel or OSINT feed from third parties. Many default feeds are included in standard MISP installation.

Delegating of sharing: allows a simple pseudo-anonymous mechanism to delegate publication of event/indicators to another organization.

Flexible API to integrate MISP with your own solutions. MISP is bundled withPyMISP which is a flexible Python Library to fetch, add or update events attributes, handle malware samples or search for attributes.

Adjustable taxonomy to classify and tag events following your own classification schemes or existing taxonomies. The taxonomy can be local toyour MISP but also shareable among MISP instances. MISP comes with a default set of well-known taxonomies and classification schemes to support standard classification as used by ENISA, Europol, DHS, CSIRTs or many other organizations.

Intelligence vocabularies called MISP galaxy and bundled with existingthreat actors, malware, RAT, ransomware or MITRE ATT&CK which can be easily linked with events in MISP.

Expansion modules in Python to expand MISP with your own services or activate already available misp-modules.

sighting support to get observations from organizations concerning shared indicators and attributes. Sighting can be contributed via MISP user-interface, API as MISP document or STIX sighting documents. Starting with MISP 2.4.66, Sighting has been extended to support false-negative sighting or expiration sighting.

STIX support: export data in the STIX format (XML and JSON) including export/import in STIX 2.0 format.

integrated encryption and signing of the notifications via PGP and/or S/MIME depending on the user preferences.

Real-time publish-subscribe channel within MISP to automatically get all changes (e.g. new events, indicators, sightings or tagging) in ZMQ (e.g. misp-dashboard) or Kafka.

Sharing with humans

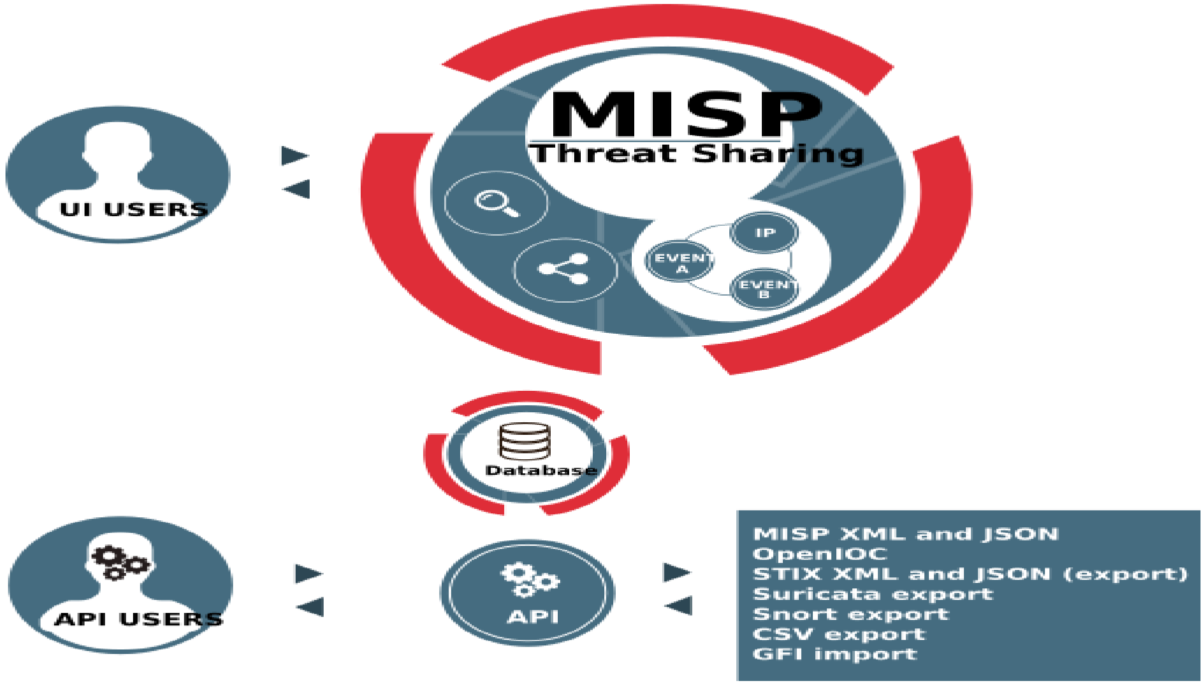
Data you store is immediately available to your colleagues and partners. Store the event id in your ticketing system or be informed by the signed and encrypted email notifications.

Sharing with machines

By generating Snort/Suricata/Bro/Zeek IDS rules, STIX, OpenIOC, text or csv exports MISP allows you to automatically import data in your detection systems resulting in better and faster detection of intrusions. Importing data can also be done in various ways: free-text import, OpenIOC, batch import, sandbox result import or using the preconfigured orcustom templates. If you run MISP internally, data can also be uploaded and downloaded automagically from and to externally hosted MISP instances. Thanks to this automation and the effort of others you are now inpossession of valuable indicators of compromise with no additional work.

Collaborative sharing of analysis and correlation

How often has your team analyzed to realize at the end that acolleague had already worked on another, similar, threat? Or that an external report has already been made? When new data is added MISP willimmediately show relations with other observables and indicators. This results in more efficient analysis, but also allows you to have a better picture of the TTPs, related campaigns and attribution.



MISP XML and JSON
OpenIOC
STIX XML and JSON (export)
Suricata export
Snort export
CSV export
GFI import

- **Your college network information**

Sagi Rama Krishnam Raju Engineering College (Department of CSE

A total of 11 labs and approximately 40 systems in each laboratory are available.

- **How you think you deploy soc in your college**

Deploying a Security Operations Center (SOC) in an organization involvescareful planning, resource allocation, and a structured approach. Here arethe key steps to deploy a SOC:

Assessment and Requirements Gathering:

- Conduct a thorough assessment of the organization's currentcybersecurity posture, including existing security measures, tools, and processes.
- Identify the specific security challenges, risks, and compliancerequirements that a SOC will address.
- Define the goals and objectives of the SOC deployment to alignwith the organization's overall security strategy.

Budget and Resource Allocation:

- Determine the budget and resource requirements forestablishing and maintaining the SOC.
- Allocate personnel, hardware, software, and other necessaryresources to support the SOC operations.

Build a Skilled Team:

- Recruit or assign skilled security professionals to form the SOCteam.
- The team should include security analysts, incident responders,threat hunters, and SOC management personnel.

Infrastructure and Technology Setup:

- Establish the physical or virtual infrastructure for the SOC,including servers, network equipment, and storage.
- Deploy the required security technologies, such as SIEM, intrusion detection and prevention systems (IDS/IPS), firewalls,endpoint protection, and threat intelligence feeds.

Integration and Data Collection:

- Integrate security tools and systems with the SIEM to centralizelog and event data collection.
- Ensure that critical data sources, such as firewalls, servers,network devices, and applications, are sending logs to the SIEM.

Establish Processes and Procedures:

- Define standard operating procedures (SOPs) for various SOCactivities, including incident handling, response protocols, escalation procedures, and communication guidelines.
- Implement incident categorization and prioritizationmechanisms.

Implement Monitoring and Alerting:

- Configure the SIEM to generate real-time alerts based onpredefined correlation rules and security use cases.
- Fine-tune alerting thresholds to minimize false positives andfocus on critical alerts.

Incident Response and Escalation:

- Develop a formal incident response plan that outlines the stepsto be taken in the event of a security incident.
- Define roles and responsibilities for incident handling, andestablish a clear escalation path for severe incidents.

Training and Skill Development:

- Provide comprehensive training to the SOC team on the use ofsecurity tools, incident analysis, threat hunting, and incident response best practices.
- Keep the team updated on the latest cybersecurity trends,attack techniques, and relevant certifications.

Testing and Continuous Improvement:

- Conduct regular tabletop exercises and simulated cyber attackscenarios to test the SOC team's response capabilities.
- Use the insights gained from testing to improve and refine the SOC'sprocesses and procedures.

Monitoring and Reporting:

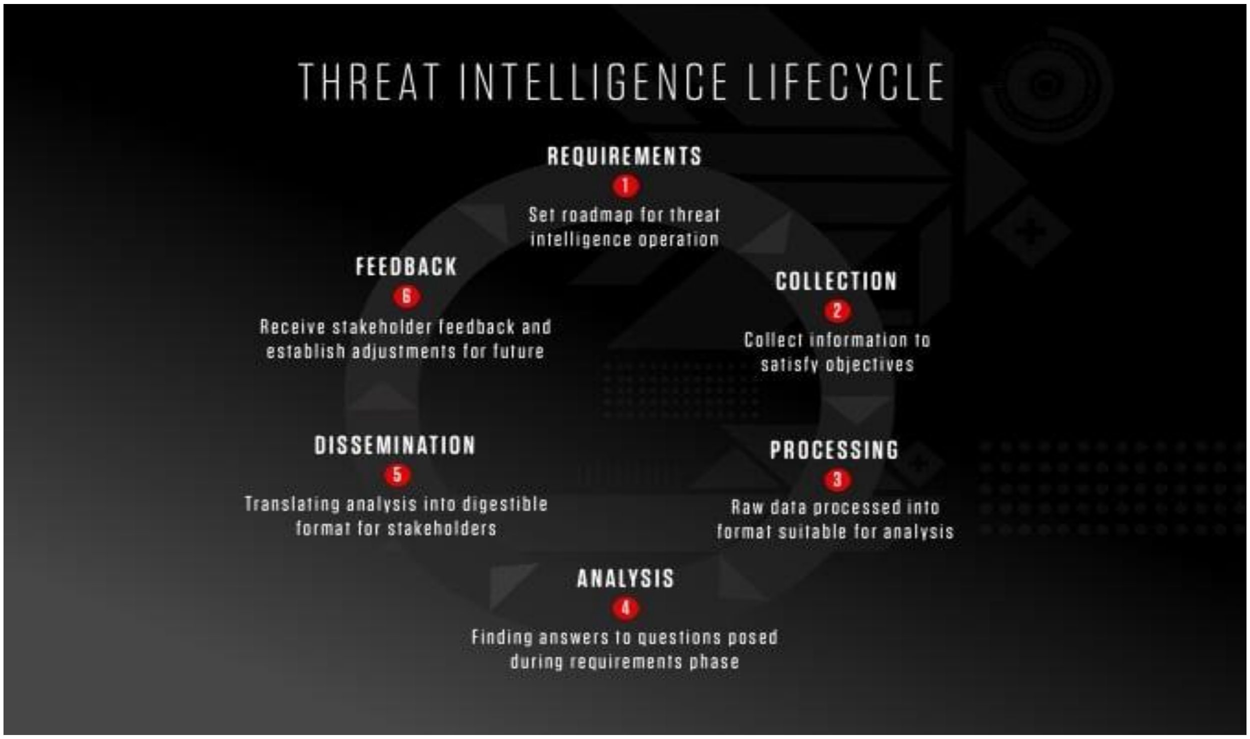
- Continuously monitor the SOC's performance and effectiveness in detecting and responding to security incidents.
- Generate regular reports and metrics to measure the SOC's performance and communicate its value to stakeholders.

Integration with IT and Business Functions:

- Foster collaboration between the SOC and other IT and business unitsto ensure a coordinated approach to security.
- Engage with executive management and board members to gainsupport and buy-in for SOC initiatives
- Deploying a SOC is an ongoing process that requires adaptability andcontinuous improvement. Regular assessments, training, and updatesare essential to ensure that the SOC remains effective in addressing the organization's evolving security challenge

- **Threat intelligence**

Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors. Threat intelligence enables us to make faster, more informed, data-backed securitydecisions and change their behavior from reactive to proactive in the fight against threat actors.


THREAT INTELLIGENCE LIFECYCLE
REQUIREMENTS
1
Set roadmap for threat intelligence operation
COLLECTION
2
Collect information to satisfy objectives
PROCESSING
3
Raw data processed into format suitable for analysis
ANALYSIS
4
Finding answers to questions posed during requirements phase
DISSEMINATION
5
Translating analysis into digestible format for stakeholders
FEEDBACK
6
Receive stakeholder feedback and establish adjustments for future

Threat intelligence is important for the following reasons:

- sheds light on the unknown, enabling security teams to make betterdecisions
- empowers cyber security stakeholders by revealing adversarialmotives and their tactics, techniques, and procedures (TTPs)
- helps security professionals better understand the threat actor'sdecision-making process
- empowers business stakeholders, such as executive boards, CISOs, CIOs and CTOs; to invest wisely, mitigate risk, become more efficientand make faster decisions

From top to bottom, threat intelligence offers unique advantages to everymember of a security team, including:

- Sec/IT Analyst
- SOC
- CSIRT
- Intel Analyst
- Executive Management

- **Incident response**

Incident response is a term used to describe the process by which an organization handles a data breach or cyberattack, including the way the organization attempts to manage the consequences of the attack or breach (the "incident"). Ultimately, the goal is to effectively manage the incident sothat the damage is limited and both recovery time and costs, as well as collateral damage such as brand reputation, are kept at a minimum.

Organizations should, at minimum, have a clear incident response plan in place. This plan should define what constitutes an incident for the company and provide a clear, guided process to be followed when an incident occurs. Additionally, it's advisable to specify the teams, employees, or leaders responsible for both managing the overall incident response initiative and those tasked with taking each action specified in the incident response plan.

Who Handles Incident Responses?

Typically, incident response is conducted by an organization's computer incident response team (CIRT), also known as a cyber incident response team. CIRTs usually are comprised of security and general IT staff, along with members of the legal, human resources, and public relations departments. As Gartner describes, a CIRT is a group that "is responsible for responding to security breaches, viruses, and other potentially catastrophic incidents in enterprises that face significant security risks. In addition to technical specialists capable of dealing with specific threats, it should include experts who can guide enterprise executives on appropriate communication in the wake of such incidents."

Six Steps for Effective Incident Response

Preparation - The most important phase of incident response is preparing for an inevitable security breach. Preparation helps organizations determinehow well their CIRT will be able to respond to an incident and should involve policy, response plan/strategy, communication, documentation, determiningthe CIRT members, access control, tools, and training.

Identification - Identification is the process through which incidents are detected, ideally promptly to enable rapid response and therefore reduce costs and damages. For this step of effective incident response, IT staff gathers events from log files, monitoring tools, error messages, intrusion detection systems, and firewalls to detect and determine incidents and their scope.

Containment - Once an incident is detected or identified, containing it is a top priority. The main purpose of containment is to contain the damage andprevent further damage from occurring (as noted in step number two, the earlier incidents are detected, the sooner they can be contained to minimizedamage). It's important to note that all of SANS' recommended steps withinthe containment phase should be taken, especially to "prevent the destruction of any evidence that may be needed later for prosecution." These steps include short-term containment, system back-up, and long-term containment.

Eradication - Eradication is the phase of effective incident response that entails removing the threat and restoring affected systems to their previousstate, ideally while minimizing data loss. Ensuring that the proper steps have been taken to this point, including measures that not only remove the malicious content but also ensure that the affected systems are completely clean, are the main actions associated with eradication.

Recovery - Testing, monitoring, and validating systems while putting themback into production in order to verify that they are not re-infected or compromised are the main tasks associated with this step of incident response. This phase also includes decision making in terms of the time and date to restore operations, testing and verifying the compromised systems, monitoring for abnormal behaviors, and using tools for testing, monitoring, and validating system behavior.

Lessons Learned - Lessons learned is a critical phase of incident response because it helps to educate and improve future incident response efforts. This is the step that gives organizations the opportunity to update their incident response plans with information that may have been missed duringthe incident, plus complete documentation to provide information for future incidents. Lessons learned reports give a clear review of the entire incident and may be used during recap meetings, training materials for new CIRT members, or as benchmarks for comparison.

Proper preparation and planning are the key to effective incident response. Without a clear-cut plan and course of action, it's often too late to coordinate effective response efforts and a communication plan after a breach or attack has occurred when future attacks or security events hit. Taking the time to create a comprehensive incident response plan can save your company substantial time and money by enabling you to regain controlover your systems and data promptly when an inevitable breach occurs.

The incident response process is the set of procedures taken by an organization in response to a cybersecurity incident. Companies should document their incident response plans and procedures along with information regarding who is responsible for performing the various activities they contain. The failure to develop an incident response plan makes it much more difficult for a business to successfully respond and recover from cyber attacks.

Following are the five steps or pillars of the incident response process.

Identify - Companies need to identify all types of threats and the assets they could affect. This involves inventorying the environment and conducting a risk assessment.

Protect - All critical assets need to have a protection plan that involves protective technological solutions and employee security awareness training.

Detect - In this step, organizations attempt to detect threats promptly before they have a chance to cause extensive damage to the environment.

Respond - After a threat or incident is detected, a defined response should be put into action to mitigate its damage and prevent its spread to other infrastructure components.

Recover - The recovery step returns the system affected to normal operations. It also evaluates the source of the incident with the goal of identifying improved security measures to prevent its recurrence.

What is the NIST incident response model?

The NIST incident response model involves four phases recommended to effectively handle cybersecurity incidents. Some of the phases can befurther subdivided to provide more steps.

Preparation - Organizations should take the necessary steps to be prepared for a cybersecurity incident when one occurs.

Detection and analysis - The cybersecurity response team is responsible for detecting and analyzing incidents to determine how to proceed and who needs to be notified.

Containment, eradication, and recovery - After an incident, the response team should stop its spread, remove the threat from the environment, and begin the process of recovering affected systems.

Post-incident activity - The focus of post-incident activity is identifying lessons learned and using them to strengthen defenses to minimize the probability of similar incidents in the future.

- **Qradar & understanding about tool**

The operation of the QRadar security intelligence platform consists of three layers, and applies to any QRadar deployment structure, regardless of its size and complexity. The following diagram shows the layers that make up the QRadar architecture.

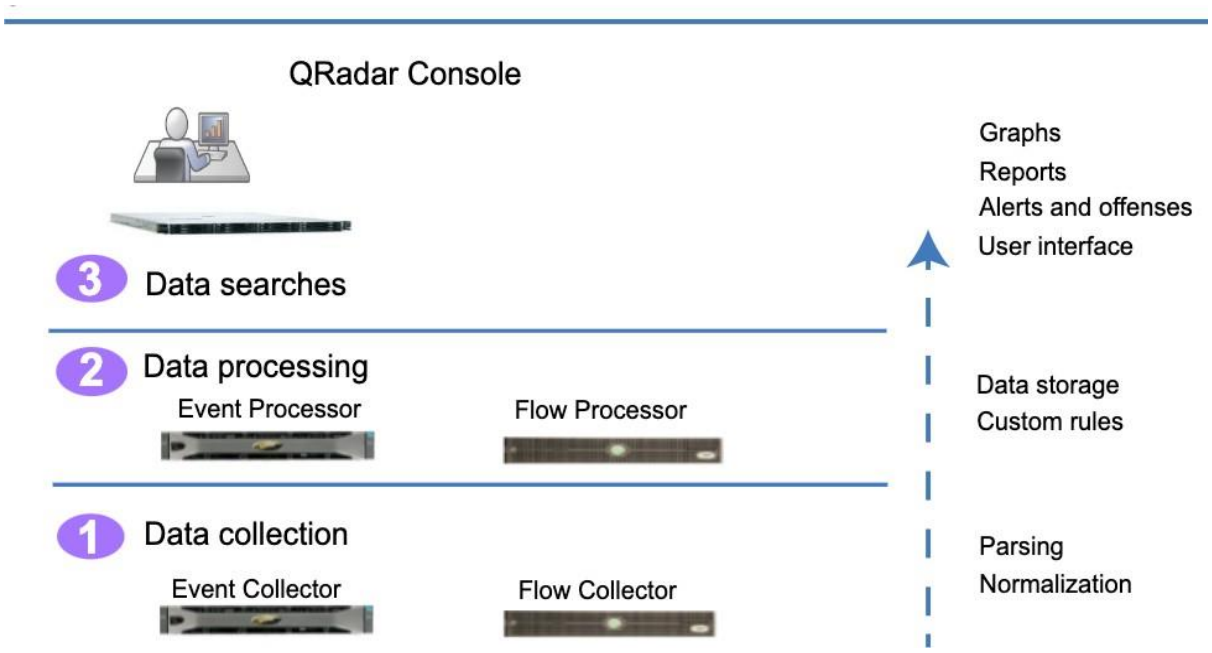


Figure 1. QRadar architecture

The QRadar architecture functions the same way regardless of the size or number of components in a deployment. The following three layers that are represented in the diagram represent the core functionality of any QRadar system.

Data collection

Data collection is the first layer, where data such as events or flows is collected from your network. The All-in-One appliance can be used to collectthe data directly from your network or you can use collectors such as QRadar Event Collectors or QRadar QFlow Collectors to collect event or flow data. The data is parsed and normalized before it passed to the processing layer. When the raw data is parsed, it is normalized to present it in a structured and usable format.

The core functionality of QRadar SIEM is focused on event data collection, and flow collection.

Event data represents events that occur at a point in time in the user's environment such as user logins, email, VPN connections, firewall denys, proxy connections, and any other events that you might want to log in yourdevice logs.

Flow data is network activity information or session information between two hosts on a network, which QRadar translates in to flow records. QRadartranslates or normalizes raw data in to IP addresses, ports, byte and packetcounts, and other information into flow records, which effectively representsa session between two hosts. In addition to collecting flow information with a Flow Collector, full packet capture is available with the QRadar Incident Forensics component.

Data processing

After data collection, the second layer or data processing layer is where event data and flow data are run through the Custom Rules Engine (CRE), which generates offenses and alerts, and then the data is written to storage.

Event data, and flow data can be processed by an All-in-One appliance without the need for adding Event Processors or Flow Processors. If the processing capacity of the All-in-One appliance is exceeded, then you mightneed to add Event Processors, Flow Processors or any other processing appliance to handle the additional requirements. You might also need more storage capacity, which can be handled by adding Data Nodes.

Other features such as QRadar Risk Manager (QRM), QRadar Vulnerability Manager (QVM), or QRadar Incident Forensics collect different types of dataand provide more functions.

QRadar Risk Manager collects network infrastructure configuration, andprovides a map of your network topology. You can use the data to manage risk by simulating various network scenarios through altering configurationsand implementing rules in your network.

Use QRadar Vulnerability Manager to scan your network and process the vulnerability data or manage the vulnerability data that is collected from other scanners such as Nessus, and Rapid7.

The vulnerability data that is collected is used to identify various security risks in your network.

Use QRadar Incident Forensics to perform in-depth forensic investigations, and replay full network sessions.

Data searches

In the third or top layer, data that is collected and processed by QRadar is available to users for searches, analysis, reporting, and alerts or offense investigation. Users can search, and manage the security admin tasks for their network from the user interface on the QRadar Console.

In an All-in-One system, all data is collected, processed, and stored on the All-in-One appliance.

In distributed environments, the QRadar Console does not perform event and flow processing, or storage. Instead, the QRadar Console is used primarily as the user interface where users can use it for searches, reports, alerts, and investigations.

QRadar components

Use IBM QRadar components to scale a QRadar deployment, and to managedata collection and processing in distributed networks.

QRadar maximum EPS certification methodology

IBM QRadar appliances are certified to support a certain maximum events per second (EPS) rate. Maximum EPS depends on the type of data that is processed, system configuration, and system load.

QRadar events and flows

The core functions of IBM QRadar SIEM are managing network security by monitoring flows and events.

Conclusion

Stage 1 :- what you understand from Web application testing .

The outcome of web application testing is to ensure that the application is secure, reliable, and meets its intended functionality. The testing process aims to identify and address potential vulnerabilities, bugs, and usability issues that could impact the application's performance and user experience.The specific outcomes of web application testing include:

- Identification of Security Vulnerabilities
- Bug Detection and Resolution
- Validation of Functional Requirements

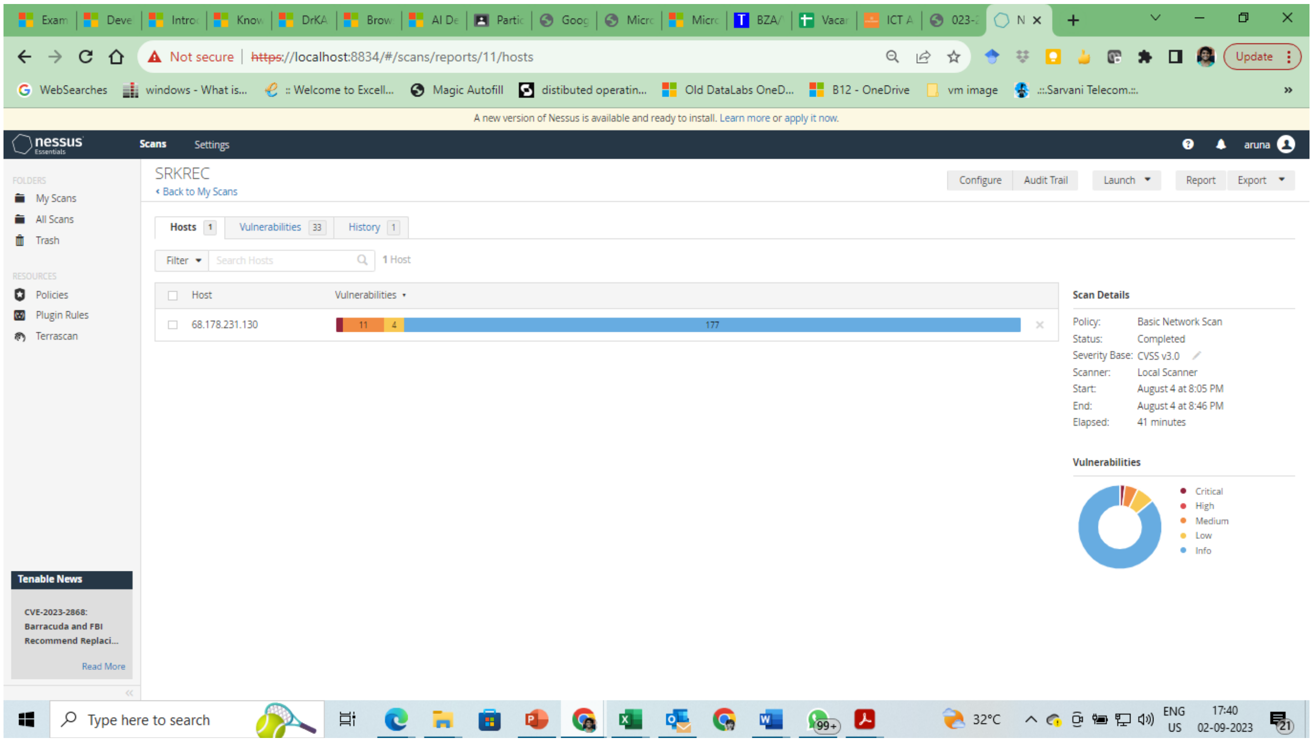
- Usability and User Experience Evaluation
- Performance and Load Testing Results
- Compatibility Testing Insights
- Accessibility Compliance
- Security Compliance and Risk Mitigation
- Optimization Recommendations
- Enhanced Quality Assurance
- Increased Customer Confidence
- Compliance with Regulatory Requirements

In summary, the outcome of web application testing is an enhanced, secure, and reliable web application that meets user expectations and delivers a smooth and seamless experience to its users. It provides developers and stakeholders with the confidence that the application is ready for deployment and can withstand potential security threats and performance challenges.

Stage 2 :- what you understand from the nessus report.

Nessus is a vulnerability scanning tool used to identify and report security issues in computer systems and networks.

The outcome of a Nessus report will depend on the specific target scanned and the vulnerabilities found. Typically, a Nessus report will list the identified vulnerabilities along with their severity levels, detailed descriptions, and recommendations for remediation. The severity levels are usually categorized as critical, high, medium, and low, depending on the potential impact and exploitability of the vulnerability.



A new version of Nessus is available and ready to install. Learn more or apply it now.

SRKREC

‹ Back to My Scans

1 Host

Host	Vulnerabilities
68.178.231.130	11 4 177

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: August 4 at 8:05 PM
End: August 4 at 8:46 PM
Elapsed: 41 minutes

Vulnerabilities

● Critical
● High
● Medium
● Low
● Info

Tenable News

CVE-2023-2868: Barracuda and FBI Recommend Replaci...

Read More

Stage 3 :- what you understand from SOC / SEIM / Qradar Dashboard.

SOC (Security Operations Center): The primary purpose of a SOC is to monitor and defend an organization's IT infrastructure against security threats and incidents. SOC analysts use various tools and technologies to detect, analyze, and respond to security events in real-time. The expected outcomes of a well-functioning SOC include:

a. **Improved Threat Detection**: SOC analysts monitor network traffic, logdata, and security alerts to identify potential threats and security incidents promptly.

b. **Faster Incident Response**: With a SOC in place, organizations can respond quickly to security incidents and mitigate the impact of breaches orattacks.

c. **Enhanced Security Posture:** A proactive SOC helps organizations implement robust security measures and continually improve their overall security posture.

d. **Reduced Downtime and Losses:** Detecting and mitigating security incidents swiftly can minimize downtime and financial losses resulting from cyber-attacks.

SIEM (Security Information and Event Management): SIEM is a technology that helps collect, analyze, and correlate log data from various sources within an organization's IT environment. The main goal of SIEM is to provide a centralized platform for real-time monitoring, threat detection, and incident response. The expected outcomes of using a SIEM system are:

a. Centralized Log Management: SIEM aggregates log data from diverse sources, making it easier for analysts to access and analyze information from a single dashboard.

b. Early Threat Detection: SIEM tools can identify patterns and anomaliesin the data, enabling early detection of security incidents and potential breaches.

c. Simplified Incident Investigation: SIEM allows analysts to correlate events from different sources, providing a comprehensive view of security incidents for faster and more accurate investigations.

d. Compliance and Reporting: SIEM can help organizations meet regulatory compliance requirements by generating security reports andaudits.

QRadar Dashboard (IBM QRadar): QRadar is a popular SIEM solution provided by IBM. The QRadar dashboard is a critical component of the QRadar system, offering a visual representation of security-related data andinsights. The expected outcomes of using QRadar and its dashboard include:

a. Real-Time Visibility: The QRadar dashboard provides real-time visibilityinto security events and incidents, enabling analysts to respond promptly toemerging threats.

b. Customizable Visualizations: Analysts can customize the dashboard todisplay relevant information, such as top threats, network traffic, or securityincidents.

c. Threat Intelligence Integration: QRadar integrates with various threatintelligence feeds, enhancing its ability to detect and respond to advanced threats.

d. Incident Response Automation: The QRadar dashboard can be integrated with automation tools to streamline incident response processes.

It's important to note that the effectiveness of these security measures relies on the expertise of the security team, the quality of data collected, and the organization's commitment to maintaining a strong security posture. Continuous monitoring, analysis, and improvement are crucial for maximizing the outcomes and benefits of SOC, SIEM, and QRadar implementations.

Future Scope

Stage 1 :- Future scope of web application testing

The future scope of web application testing will be shaped by technological advancements, changing user expectations, and the need to ensure securityand reliability in an increasingly interconnected digital world. Testing professionals will need to adapt to these trends and continuously upgrade their skills to meet the evolving demands of web application testing.

Stage 2 :- Future scope of testing process you understood.

The future scope of the testing process will see increased automation, integration with emerging technologies, and a focus on ensuring quality, security, and performance in the ever-evolving software landscape. Testing professionals will need to adapt to these changes and continuously upgrade their skills to stay relevant in the dynamic field of software testing

Stage 3 :- future scope of SOC / SEIM

The future scope of SOC (Security Operations Center) and SIEM (Security Information and Event Management) is expected to expand and evolve in response to the changing cybersecurity landscape and technological advancements. The future scope of SOC and SIEM will involve increased automation, advanced threat detection, integration with emerging technologies, and a proactive approach to cybersecurity. Organizations will need to invest in the latest tools and technologies while continuouslydeveloping the expertise of their cybersecurity teams to stay ahead of evolving threats.

Topics explored :-

Introduction to cybersecurity, Growth of cybersecurity, Data sanity, Cloud service and cloud security, Data breach, Firewall, Antivirus, Digital ecosystem, Data protection, Types of cyber attacks, Essential terminology, Introduction to networking, Web APIs, web hooks, Web shell concepts, Vulnerability stack,OWASP top 10 applications, QRadar, SOC, SIEM

Tools explored :-

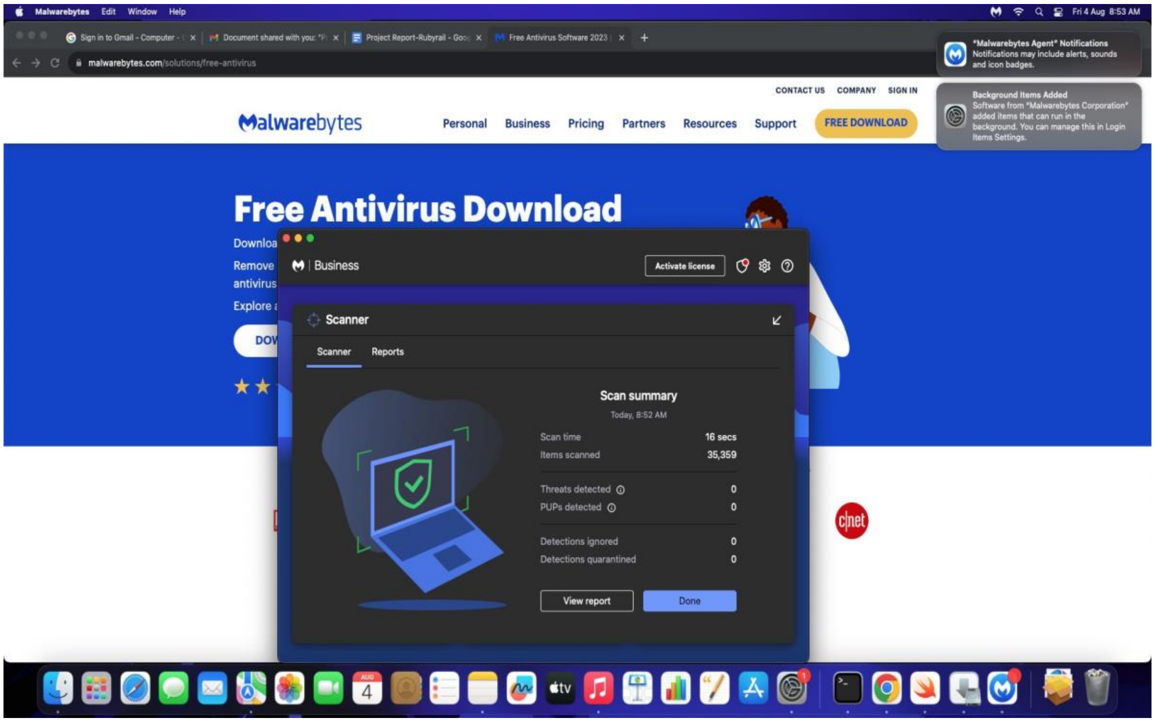
Nessus, cybermap.kaspersky.com, thehackersone.com, chaptgpt,wepik.com (AI image editor), Gamma (AI based PPT), OWASP top 10 vulnerabilities(2021), thehackersnews.com, CWE, exploitDB, virtual box, live websites-bugcrowd, nslookup.io, OSINT framework, mitre framework, IBM fix central, QRadar Installation, mobaxterm, tools-nmtui, Nmap, sqlmap, Identify fixes-wincollect agent, metasploitable, malware bytes, Linux cheatsheet, QRadar for SOC dashboard presentation, Kali linux

MALWAREBYTES

FREE DOWNLOADS

Free Antivirus Software 2023

Looking for free antivirus and malware removal? Scan and remove viruses and malware for free. Malwarebytes free antivirus includes multiple layers of malware-crushing tech. Our anti-malware finds and removes threats like viruses, ransomware, spyware, adware, and Trojans.


Malwarebytes Edit Window Help
Fri 4 Aug 8:53 AM
Sign in to Gmail - Computer
Document shared with you
Project Report-Rubyrail - Goo
Free Antivirus Software 2023
malwarebytes.com/solutions/free-antivirus
CONTACT US COMPANY SIGN IN
Malwarebytes
Personal Business Pricing Partners Resources Support FREE DOWNLOAD
Free Antivirus Download
Business
Activate license
Scanner
Scanner Reports
View report
Done

"Malwarebytes Agent" Notifications
Notifications may include alerts, sounds and icon badges.

Background Items Added
Software from "Malwarebytes Corporation" added items that can run in the background. You can manage this in Login Items Settings.

Scan summary
Today, 8:52 AM

Scan time	16 secs
Items scanned	35,359
Threats detected	0
PUPs detected	0
Detections ignored	0
Detections quarantined	0

Metasploitable2 (Linux) is a framework which is combination Nmap and exploitdatabase.

Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetrationtesting techniques.