SAFEGUARDING ORGANIZATIONAL CYBER LANDSCAPE

PART I - EXECUTIVE SUMMARY

Overview

Implementing effective cyber security in an organization involves a holistic approach encompassing the development of a well-defined cyber security policy aligned with business goals, conducting thorough risk assessments, training employees on best practices, implementing strong access controls, deploying network and endpoint security measures, encrypting sensitive data, managing patches diligently, creating an incident response plan, conducting regular audits, establishing comprehensive monitoring and logging systems, and ensuring clear communication channels for reporting incidents and engaging stakeholders. This multifaceted approach ensures protection against cyber threats while fostering a security-conscious culture and adaptability to the evolving threat landscape.

Cyber security is an ongoing process, and staying vigilant and adaptable is essential. Threat landscapes evolve over time, so regular updates and adjustments to your cyber security strategy are crucial to maintaining a strong defense against cyber threats. A comprehensive and proactive approach to implementing cyber security within an organization covers various aspects of cyber security, from policy development to incident response. Here's a more detailed breakdown of each step:

Develop a Clear Cyber security Policy and Strategy

- Define the organization's cyber security goals and objectives.
- Align the cyber security strategy with business objectives and risk tolerance.
- Clearly outline roles and responsibilities for cyber security management.

Conduct a Thorough Risk Assessment

- Identify potential threats and vulnerabilities specific to the organization.
- Prioritize risks based on impact and likelihood.
- Develop a risk management plan to address identified vulnerabilities.

Employee Training and Education

- Provide cyber security awareness training to all employees.
- Educate employees about common attack vectors, such as phishing and social engineering.
- Foster a security-conscious culture and encourage reporting of suspicious activities.

Implement Strong Access Control Measures

- Enforce least privilege access for employees.
- Utilize multi-factor authentication (MFA) for critical systems and data.
- Regularly review and update access permissions.

Network Security

- Deploy firewalls, intrusion detection/prevention systems, and secure gateways.
- Monitor and control network traffic to detect and prevent unauthorized access.

Endpoint Protection

- Install antivirus software, endpoint protection tools, and host-based firewalls on all devices.
- Regularly update and patch endpoint security software.

Data Encryption

- Encrypt sensitive data both at rest and in transit.
- Ensure that encryption keys are securely managed.

Patch Management

- Establish a process to promptly apply security patches and updates.
- Regularly update software, operating systems, and firmware to address vulnerabilities.

Incident Response Planning

- Develop a well-defined incident response plan (IRP).
- Include guidelines for identifying, reporting, containing, eradicating, and recovering from incidents.
- Conduct regular drills and exercises to test the effectiveness of the IRP.

Security Audits and Assessments

- Perform regular internal and external security audits.
- Evaluate the organization's security posture and identify weaknesses or gaps.
- Use audit results to improve security measures.

Monitoring and Logging

- Implement centralized logging and real-time monitoring of network and system activities.
- Set up alerts for suspicious activities and incidents.

Communication and Reporting

- Establish clear channels for reporting security incidents.
- Communicate with stakeholders, including employees, customers, partners, and regulatory authorities.

2. List of Vulnerable Parameter, Location discovered

Vulnerability Name	CWE Reference
A01:Broken Access Control	CWE-285: Improper Authorization
A02:Cryptographic Failures	CWE-326: Inadequate Encryption Strength
A03:Injection	CWE-94: Improper Control of Generation of Code ('Code Injection')
A04:Insecure Design	CWE-657: Violation of Secure Design Principles
A05:Security Misconfiguration	CWE-555: J2EE Misconfiguration: Plaintext Password in Configuration File
A06:Vulnerable and Outdated Components	CWE-1104: Use of Unmaintained Third-Party Components
A07:Identification and Authentication Failures	CWE-287: Improper Authentication
A08:Software and Data Integrity Failures	CWE-353: Missing Support for Integrity Check
A09:Security Logging and Monitoring Failures	CWE-532: Insertion of Sensitive Information into Log File
A10:Server-Side Request Forgery	CWE-918: Server-Side Request Forgery (SSRF)

1.1 . Vulnerability Name: Improper Authorization

CWE: 285

OWASP Category: Broken Access Control

Description: The product does not perform or incorrectly performs an authorization check when an actor attempts to access a resource or perform an action**.**

Business Impact: When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

1.2. Vulnerability Name: Inadequate Encryption Strength

CWE: 326

OWASP Category: Cryptographic Failures

Description: The product stores or transmits sensitive data using an encryption scheme that is theoretically sound, but is not strong enough for the level of protection required.

Business Impact: The product stores or transmits sensitive data using an encryption scheme that is theoretically sound, but is not strong enough for the level of protection required. A weak encryption scheme can be subjected to brute force attacks that have a reasonable chance of succeeding using current attack methods and resources**.**

1.3. Vulnerability Name: Improper Control of Generation of Code ('Code Injection')

CWE: 94

OWASP Category: Injection

Description: The product constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.

Business Impact: The product constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.

1.4. Vulnerability Name: Violation of Secure Design Principles

CWE: 657

OWASP Category: Insecure Design

Description: The product violates well-established principles for secure design

Business Impact: The product violates well-established principles for secure design. This can introduce resultant weaknesses or make it easier for developers to introduce related weaknesses during implementation. Because code is centered around design, it can be resource-intensive to fix design problems.

1.5. Vulnerability Name: J2EE Misconfiguration: Plaintext Password in Configuration File

CWE: 555

OWASP Category: Security Misconfiguration

Description: The J2EE application stores a plaintext password in a configuration file.

Business Impact: The J2EE application stores a plaintext password in a configuration file. Storing a plaintext password in a configuration file allows anyone who can read the file to access the password-protected resource, making it an easy target for attackers.

1.6. Vulnerability Name: Use of Unmaintained Third-Party Components

CWE: 1104

OWASP Category: Vulnerable and Outdated Components

Description: 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.

Business Impact: Reliance on components that are no longer maintained can make it difficult or impossible to fix significant bugs, vulnerabilities, or quality issues. In effect, unmaintained code can become obsolete.This issue makes it more difficult to maintain the product, which indirectly affects security by making it more difficult or time-consuming to find and/or fix vulnerabilities. It also might make it easier to introduce vulnerabilities.

1.7. Vulnerability Name: Improper Authentication

CWE: 287

OWASP Category: Identification and Authentication Failures

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 violations of regulatory compliance requirements, such as data protection regulations. Reputation damage: A successful attack exploiting improper authentication can lead to loss of customer trust and reputational damage for the organization.

1.8. Vulnerability Name: Missing Support for Integrity Check

CWE: 353

OWASP Category: Software and Data Integrity Failures

Description: The product uses a transmission protocol that does not include a mechanism for verifying the integrity of the data during transmission, such as a checksum.

Business Impact: If integrity check values or "checksums" are omitted from a protocol, there is no way of determining if data has been corrupted in transmission. The lack of checksum functionality in a protocol removes the first application-level check of data that can be used.

1.9. Vulnerability Name: Insertion of Sensitive Information into Log File

CWE: 532

OWASP Category: Security Logging and Monitoring Failures

Description: Information written to log files can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information.

Business Impact: Because this can be used to exploit other threats related to CWE-284: Improper Access Control I rank it with a Moderate severity. An insider with knowledge of this could do many mischievous things and get away with them for a long time without victims knowing about it.

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

CWE: 918

OWASP Category: Server-Side Request Forgery

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.

Business Impact: A successful SSRF attack can often result in unauthorized actions or access to data within the organization, either in the vulnerable application itself or on other back-end systems that the application can communicate with.

Stage: 2 Report

NESSUS Vulnerability Report

Overview

Vulnerability Assessment Report for College Website using Nessus tool. This report outlines the results of a vulnerability assessment conducted on the college website using Nessus, a widely used vulnerability scanning tool. The purpose of this assessment was to identify potential vulnerabilities that could expose the website to security risks.

The assessment focused on the college website's public-facing components, including web servers, applications, and associated infrastructure. Nessus was employed to scan the target assets for known vulnerabilities. The assessment was carried out using a combination of active and passive scans. The assessment identified the following key vulnerabilities:

1. Outdated Software Versions
Several instances of outdated software versions were detected on web servers and backend systems. These vulnerabilities could potentially be exploited by attackers targeting known vulnerabilities in older software.

2. Weak SSL Configuration
The SSL configuration on the website's login page was found to be weak, potentially leaving sensitive user data exposed to eavesdropping or man-in-the-middle attacks.

3. Missing Security Patches
Several systems were missing critical security patches, increasing the risk of exploitation by attackers seeking to target known vulnerabilities.

4. Cross-Site Scripting (XSS) Vulnerabilities:
A few web application pages were found to be susceptible to Cross-Site Scripting attacks. These vulnerabilities could allow attackers to inject malicious scripts into the website, potentially compromising user data or spreading malware.

5. Directory Traversal Attack Possibility
A directory traversal vulnerability was detected on the website, which could potentially allow attackers to access files outside of the intended directory structure and gain unauthorized access to sensitive information.

Based on the findings, the following recommendations are suggested to mitigate the identified vulnerabilities and enhance the security posture of the college website:

- Regular Software Updates - Maintain up-to-date software versions on all web servers and backend systems to reduce the risk of known vulnerabilities being exploited.
- SSL/TLS Enhancement - Improve SSL configurations to ensure the encryption and integrity of sensitive user data. Use strong encryption protocols and ciphers.
- Patch Management - Establish a routine patch management process to promptly apply security updates to all systems and software components.
- Web Application Security - Implement input validation mechanisms to prevent Cross-Site Scripting vulnerabilities. Regularly test and secure web applications against common attack vectors.
- Directory Access Restrictions - Implement proper access controls to prevent directory traversal attacks. Ensure that user input is sanitized and validated before being used in file operations.

This vulnerability assessment using Nessus highlighted several vulnerabilities that, if left unaddressed, could expose the college website to potential security risks. By implementing the recommended measures, the college can enhance its cyber security posture and reduce the likelihood of successful attacks. It's important to note that vulnerability assessments provide insights into potential security weaknesses, but they do not guarantee the absence of other vulnerabilities. The findings and recommendations in this report are based on the assessment conducted at a specific point in time and may not reflect changes or updates made after the assessment.

Target WebSite : Kumaraguru College of Technology – www.kct.ac.in
Target IP : 176.67.187.85

S.No	Vulnerability name	Severity	Plugin	Description	Solution	Business Impact	Port
1	HTTP Server Type and Version	Low	10107	This plugin attempts to determine the type and the version of the remote web server.	n/a		8880
2	Nessus SYN scanner	Low	11219	This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled	Protect your target with an IP filter.		443

				target.			
3	Service Detection		22964	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.			80
4	HyperText Transfer Protocol (HTTP) Information		24260	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.			443
5	Common Platform Enumeration (CPE)		45590	By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for	n/a		0

				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.			

Report generated by Nessus™

stack

Fri, 04 Aug 2023 18:28:21 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Expand All | Collapse All

172.67.187.85

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	58

Scan Information

Start time: Fri Aug 4 18:01:16 2023

End time: Fri Aug 4 18:28:21 2023

Host Information

IP: 172.67.187.85

OS: Linux Kernel 4.1

Vulnerabilities

45590 - Common Platform Enumeration (CPE)

-

Synopsis

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

Description

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

cpe:/o:linux:linux_kernel -> Linux Kernel
```

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
```

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 :

cloudflare
```

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 :

cloudflare
```

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/2052/www

```
The remote web server type is :

cloudflare
```

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/2053/www

```
The remote web server type is :

cloudflare
```

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/2082/www

```
The remote web server type is :

cloudflare
```

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/2083/www

```
The remote web server type is :

cloudflare
```

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/2086/www

```
The remote web server type is :

cloudflare
```

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/2087/www

```
The remote web server type is :

cloudflare
```

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/2095/www

```
The remote web server type is :

cloudflare
```

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/2096/www

```
The remote web server type is :

cloudflare
```

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/8080/www

```
The remote web server type is :

cloudflare
```

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/8443/www

```
The remote web server type is :

cloudflare
```

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/8880/www

```
The remote web server type is :

cloudflare
```

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/1.1 403 Forbidden

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

Date: Fri, 04 Aug 2023 12:42:34 GMT
Content-Type: text/plain; charset=UTF-8
Content-Length: 16
Connection: close
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Server: cloudflare
CF-RAY: 7f16e18a8bc5f435-BOM

Response Body :

error code: 1003
```

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/1.1 400 Bad Request

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

Server: cloudflare
Date: Fri, 04 Aug 2023 12:42:32 GMT
Content-Type: text/html
Content-Length: 655
Connection: close
CF-RAY: -

Response Body :

<html>
<head><title>400 The plain HTTP request was sent to HTTPS
port</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<center>The plain HTTP request was sent to HTTPS port</center>
<hr><center>cloudflare</center>
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

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/2052/www

```
Response Code : HTTP/1.1 403 Forbidden
```

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

Date: Fri, 04 Aug 2023 12:42:36 GMT
Content-Type: text/plain; charset=UTF-8
Content-Length: 16
Connection: close
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Server: cloudflare
CF-RAY: 7f16e1997d6241a5-BOM

Response Body :

error code: 1003
```

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/2053/www

```
Response Code : HTTP/1.1 400 Bad Request

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

Server: cloudflare
Date: Fri, 04 Aug 2023 12:42:33 GMT
Content-Type: text/html
Content-Length: 655
Connection: close
CF-RAY: -

Response Body :
```

```
<html>
<head><title>400 The plain HTTP request was sent to HTTPS
port</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<center>The plain HTTP request was sent to HTTPS port</center>
<hr><center>cloudflare</center>
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

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/2082/www

```
Response Code : HTTP/1.1 403 Forbidden

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

Date: Fri, 04 Aug 2023 12:42:32 GMT
Content-Type: text/plain; charset=UTF-8
Content-Length: 16
Connection: close
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Server: cloudflare
CF-RAY: 7f16e1840c8d3f5b-BOM

Response Body :

error code: 1003
```

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/1.1 400 Bad Request

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

Server: cloudflare
Date: Fri, 04 Aug 2023 12:42:37 GMT
Content-Type: text/html
Content-Length: 655
Connection: close
CF-RAY: -

Response Body :

<html>
<head><title>400 The plain HTTP request was sent to HTTPS
port</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<center>The plain HTTP request was sent to HTTPS port</center>
<hr><center>cloudflare</center>
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

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/2086/www

```
Response Code : HTTP/1.1 403 Forbidden

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

Date: Fri, 04 Aug 2023 12:42:34 GMT
Content-Type: text/plain; charset=UTF-8
Content-Length: 16
Connection: close
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Server: cloudflare
CF-RAY: 7f16e18cb9f5445a-BOM

Response Body :

error code: 1003
```

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/2087/www

```
Response Code : HTTP/1.1 400 Bad Request

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

Server: cloudflare
Date: Fri, 04 Aug 2023 12:42:36 GMT
Content-Type: text/html
Content-Length: 655
Connection: close
CF-RAY: -

Response Body :

<html>
<head><title>400 The plain HTTP request was sent to HTTPS
port</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<center>The plain HTTP request was sent to HTTPS port</center>
<hr><center>cloudflare</center>
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

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/2095/www

```
Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
```

```
Options allowed : (Not implemented)
Headers :

Date: Fri, 04 Aug 2023 12:42:36 GMT
Content-Type: text/plain; charset=UTF-8
Content-Length: 16
Connection: close
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Server: cloudflare
CF-RAY: 7f16e1976bce3a19-BOM

Response Body :

error code: 1003
```

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/1.1 400 Bad Request

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

Server: cloudflare
Date: Fri, 04 Aug 2023 12:42:32 GMT
Content-Type: text/html
Content-Length: 655
Connection: close
CF-RAY: -

Response Body :

<html>
<head><title>400 The plain HTTP request was sent to HTTPS
port</title></head>
```

```
<body>
<center><h1>400 Bad Request</h1></center>
<center>The plain HTTP request was sent to HTTPS port</center>
<hr><center>cloudflare</center>
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

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/8080/www

```
Response Code : HTTP/1.1 403 Forbidden

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

Date: Fri, 04 Aug 2023 12:42:35 GMT
Content-Type: text/plain; charset=UTF-8
Content-Length: 16
Connection: close
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Server: cloudflare
CF-RAY: 7f16e1951de71bd1-BOM

Response Body :

error code: 1003
```

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/8443/www

```
Response Code : HTTP/1.1 400 Bad Request

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

Server: cloudflare
Date: Fri, 04 Aug 2023 12:42:33 GMT
Content-Type: text/html
Content-Length: 655
Connection: close
CF-RAY: -

Response Body :

<html>
<head><title>400 The plain HTTP request was sent to HTTPS
port</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<center>The plain HTTP request was sent to HTTPS port</center>
<hr><center>cloudflare</center>
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

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/8880/www

```
Response Code : HTTP/1.1 403 Forbidden

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

Date: Fri, 04 Aug 2023 12:42:37 GMT
Content-Type: text/plain; charset=UTF-8
Content-Length: 16
Connection: close
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Server: cloudflare
CF-RAY: 7f16e1a019094412-BOM

Response Body :

error code: 1003
```

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/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/2052/www

```
Port 2052/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/2053/www

```
Port 2053/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/www

```
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/2086/www

```
Port 2086/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/2087/www

```
Port 2087/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/www

```
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/8080/www

```
Port 8080/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/8443/www

```
Port 8443/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/8880/www

```
Port 8880/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 : 202308040201
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : stack
Scan policy used : Basic Network Scan
Scanner IP : 192.168.1.6
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 56.991 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/8/4 18:01 India Standard Time
Scan duration : 1562 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 : Linux Kernel 4.1
Confidence level : 56
Method : MLSinFP


The remote host is running Linux Kernel 4.1
```

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/443/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/2052/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/2053/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/2082/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/2083/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/2086/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/2087/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/2095/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/2096/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/8080/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/8443/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/8880/www

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

25220 - TCP/IP Timestamps Supported

-

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/03/06

Plugin Output

tcp/0

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 192.168.1.6 to
172.67.187.85 :
192.168.1.6

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.
192.168.1.1
117.255.112.1
218.248.106.202
?
172.69.82.3
172.67.187.85
?
172.67.187.85
Hop Count: 10
```


Stage 3 Report

Role of SOC in the organizations security

3.1 SOC

A Security Operations Center (SOC) is a centralized unit within an organization that is responsible for monitoring, detecting, responding to, and mitigating cybersecurity threats and

incidents. The primary goal of a SOC is to ensure the security of an organization's information systems, digital assets, and sensitive data. It acts as a nerve center for managing and coordinating cybersecurity activities.

Key functions and components of a Security Operations Center include:

1.Monitoring and Analysis- SOC analysts continuously monitor network and system activities using various security tools and technologies. They analyze logs, traffic patterns, and behavior to identify potential security incidents or anomalies.

2.Threat Detection and Response- SOC teams are trained to detect signs of cyber threats, including unauthorized access, malware infections, data breaches, and other malicious activities. When a threat is detected, the SOC initiates a response process to mitigate and contain the threat.

3.Incident Response- SOC personnel are responsible for managing cybersecurity incidents. They follow predefined procedures to contain, eradicate, and recover from incidents. This includes coordinating with various teams within the organization, such as IT, legal, and communication teams, to ensure a coordinated response.

4.Security Incident Management- SOC analysts document and track security incidents throughout their lifecycle. This documentation is important for analysis, reporting, and improving incident response processes.

5.Vulnerability Management- SOC teams often work alongside the organization's IT team to identify vulnerabilities in systems, applications, and infrastructure. They prioritize vulnerabilities based on risk and criticality and ensure that appropriate patches and updates are applied.

6. Threat Intelligence- SOC analysts stay up-to-date with the latest threat intelligence, which includes information about emerging threats, attack techniques, and vulnerabilities. This knowledge helps them proactively defend against potential threats.

7.Security Tools and Technologies-SOCs use a wide range of security tools, such as intrusion detection/prevention systems (IDS/IPS), firewalls, SIEM (Security Information and Event Management) systems, threat hunting tools, and more, to monitor, analyze, and respond to security events.

8. Automation and Orchestration- To handle the volume of security events efficiently, SOCs often use automation and orchestration tools. These tools help streamline processes, improve response times, and reduce the manual workload for analysts.

9.24/7 Monitoring- Cyber threats can occur at any time, so many SOCs operate around the clock, providing continuous monitoring and response capabilities.

10.Training and Skill Development: SOC personnel require specialized skills and training to effectively analyze and respond to complex cybersecurity incidents. Continuous training and skill development are crucial to staying effective in a rapidly evolving threat landscape.

In summary, a Security Operations Center plays a crucial role in maintaining an organization's cybersecurity posture by actively monitoring for threats, responding to incidents, and ensuring a rapid and effective defense against cyber attacks.

3.2 SOC Cycle

The Security Operations Center (SOC) operates within a cyclical process known as the SOC cycle. This cycle consists of several interconnected phases that help the SOC effectively manage and respond to cyber security threats and incidents. The SOC cycle typically follows these stages:

1.Detection and Monitoring:

In this phase, the SOC continuously monitors network traffic, system logs, and security events using various tools and technologies. The goal is to detect anomalies, potential threats, and unauthorized activities. This could include activities like intrusion attempts, malware infections, or unusual user behavior.

2.Analysis and Triage:

Detected security events are analyzed to determine their severity and potential impact on the organization. SOC analysts assess the context of each event, investigate suspicious activities, and classify events as false positives, true positives, or requiring further investigation.

3. Incident Identification:

Events that are identified as potential security incidents are further investigated to confirm their nature and scope. This involves deeper analysis to understand the attack vectors, techniques used, and potential vulnerabilities exploited.

4.Containment and Eradication:

Once an incident is confirmed, the SOC works to contain its impact and prevent further spread. This might involve isolating affected systems, disabling compromised accounts, and mitigating the root cause of the incident. The goal is to limit damage and stop the attacker's progression.

5.Recovery and Remediation:

After containment, the SOC focuses on the recovery process. This includes restoring affected systems, applications, and data to their normal state. Additionally, any security gaps or vulnerabilities that contributed to the incident are addressed to prevent future occurrences.

6.Communication and Reporting:

Throughout the incident response process, the SOC maintains clear communication with relevant stakeholders, including internal teams, management, legal, and, in some cases, external entities such as law enforcement or regulatory bodies. Regular updates are provided, and incident reports are documented for analysis and compliance purposes.

7.Lessons Learned and Improvement:

Post-incident, the SOC conducts a thorough analysis of the incident, looking into what went well and areas for improvement. Lessons learned are documented, and recommendations are made to enhance the organization's security posture, policies, and response procedures.

8.Threat Intelligence Integration:

Throughout the cycle, threat intelligence is gathered and integrated into the SOC's activities. This information helps the SOC proactively identify emerging threats, understand attacker techniques, and improve the accuracy of event detection.

The SOC cycle is continuous and iterative, allowing the SOC team to adapt to evolving threats and refine their processes over time. This cycle ensures a structured and efficient approach to managing cyber security incidents while minimizing the potential impact on the organization.

3.3 SIEM

SIEM stands for Security Information and Event Management. It's a comprehensive cybersecurity solution that provides organizations with the capability to collect, analyze, and correlate data from various sources within their IT environment. The primary goal of a SIEM system is to provide real-time visibility into an organization's security posture, detect and respond to security incidents, and help in compliance reporting.

Key features of a SIEM system include:

Log Management: SIEM solutions collect and store logs from a wide range of sources, including network devices, servers, applications, and security appliances. These logs contain valuable information about events and activities happening within an organization's IT infrastructure.

Event Correlation: SIEM systems analyze and correlate the collected log data to identify patterns, anomalies, and potential security threats. By connecting the dots between seemingly unrelated events, SIEM can uncover sophisticated attacks that might otherwise go unnoticed.

Real-time Monitoring: SIEM tools provide real-time monitoring of security events and activities. They can generate alerts and notifications when suspicious or potentially malicious activities are detected. This allows organizations to respond swiftly to security incidents.

Threat Detection: SIEM solutions use predefined rules, machine learning, and behavioral analysis to identify known and unknown threats. These threats can include malware infections, unauthorized access attempts, data breaches, and more.

Incident Response: When a potential security incident is detected, SIEM tools facilitate the incident response process. They can help contain the incident, mitigate its impact, and support the recovery process.

Forensic Analysis: SIEM systems enable forensic investigations by providing historical data and context. This is crucial for understanding the timeline of events leading up to an incident and for post-incident analysis.

Compliance and Reporting: SIEM solutions help organizations meet regulatory compliance requirements by generating reports that demonstrate adherence to security policies and standards. These reports are often required for audits and assessments.

8.Integration with Security Tools: SIEM systems can integrate with various security tools and technologies, such as intrusion detection/prevention systems (IDS/IPS), firewalls, antivirus solutions, and more. This integration allows for a more comprehensive view of an organization's security landscape.

9.Centralized Dashboard: SIEM platforms provide a centralized dashboard that allows security teams to monitor and manage security events and incidents from a single interface. This improves operational efficiency and reduces the complexity of managing multiple security tools.

10.Threat Intelligence Integration: Many SIEM systems incorporate threat intelligence feeds that provide up-to-date information about emerging threats, vulnerabilities, and attacker tactics. This helps organizations stay proactive against evolving threats.

In summary, a SIEM system serves as a central hub for collecting, analyzing, and responding to security events within an organization's IT environment. It empowers security teams to identify and address potential threats in a timely manner, enhancing overall cybersecurity posture.

3.4 SIEM Cycle

The Security Information and Event Management (SIEM) cycle outlines the iterative process that SIEM systems follow to ensure effective monitoring, detection, and response to security events within an organization's IT environment. The SIEM cycle typically involves the following stages:

- Data Collection-The cycle begins with the collection of data from various sources, including logs, events, and activities generated by network devices, servers, applications, security appliances, and more. This data provides a comprehensive view of the organization's IT landscape.
- Data Normalization- Raw data collected from different sources often comes in various formats. In this stage, the SIEM normalizes and standardizes the data, converting it into a consistent format that can be easily analyzed and correlated.

- Data Aggregation and Correlation- The SIEM system aggregates and correlates the normalized data to identify patterns and relationships between events. This helps the system distinguish between normal activities and potentially malicious behavior.
- Alert Generation-Based on predefined rules, behavioral patterns, and threat intelligence, the SIEM system generates alerts for events that exhibit suspicious or anomalous behavior. These alerts are categorized by severity levels to help prioritize responses.
- Alert Investigation-Security analysts review and investigate the generated alerts to determine their validity and potential impact. Analysts analyze contextual information, historical data, and related events to make informed decisions about the significance of each alert.
- Incident Response - For confirmed security incidents, the SIEM system supports the incident response process. It provides data and context to help security teams understand the incident's scope, timeline, and affected assets. This aids in containment, eradication, and recovery efforts.
- Forensic Analysis- In this stage, analysts perform detailed forensic analysis on incidents to reconstruct the sequence of events leading to the incident. This helps organizations understand the attack methods and techniques used by threat actors.
- Reporting and Compliance - SIEM systems generate reports and dashboards that provide insights into security events, incidents, and trends. These reports are essential for compliance reporting, audits, and communicating the organization's security posture to stakeholders.
- Continuous Monitoring and Improvement - The SIEM cycle is continuous. After each incident, the organization reviews the incident response process, identifies areas for improvement, and adjusts its rules and configurations to enhance the system's accuracy and effectiveness.
- Threat Intelligence Integration - Throughout the cycle, the SIEM system integrates threat intelligence feeds that provide real-time information about emerging threats, vulnerabilities, and attacker tactics. This helps the system stay current and proactive against evolving threats.
- By following this cycle, organizations can maintain a proactive stance against cyber threats, quickly detect and respond to security incidents, and continually improve their overall security posture.

3.5 MISP

MISP, short for "Malware Information Sharing Platform & Threat Sharing," is an open-source solution designed to facilitate the exchange of structured threat intelligence among cybersecurity professionals, organizations, and communities. Serving as a centralized hub, MISP enables the collection, storage, and dissemination of various threat data, including indicators of compromise, threat actor details, and malware samples. By supporting standardized data formats like STIX and OpenIOC, MISP enhances the machine-readable representation of threat information. Organizations can share this intelligence privately or publicly with trusted partners, leveraging automated correlation, enrichment, and tagging

features. With customizable taxonomies and integration with external threat feeds, MISP empowers users to collaboratively track threats, attribute indicators, and strengthen their collective defense against cyber threats.

3.6 INFORMATION OF KCT NETWORK

KCT provides campus-wide Internet, wired / Wi-Fi facilities (100 access points) and ERP software for campus management connected through 1 Gbps Internet bandwidth. IT facilities of KCT includes (i) hardware and (ii) software facilities to connect various facilities and provide necessary facilities, services and supports. Entire Campus is connected through optical fibre cable (OFC) spanning over a length of 5950 Meters. Hardware facilities of the Campus include computers, printers, Optical Character Recognition (OCR) machine, Dummy Number Preparation Machine, RFID / Barcode systems for campus entry and exit for both students and faculty members. IP Cameras are installed at various locations in the campus for safety and surveillance. Biometric devices are installed at various points to capture the fingerprint / facial recognition of the faculty and hostel students to mark their attendance.

3.7 DEPLOYMENT OF SOC IN KUMARAGURU COLLEGE OF TECHNOLOGY

Establishing a Security Operations Center (SOC) within an engineering institution is a strategic move to bolster its cybersecurity defenses. The deployment process involves careful planning, coordination, and resource allocation. The initial step involves assessing the institution's existing cybersecurity infrastructure, identifying potential risks, and setting clear objectives for the SOC's role. This assessment guides the allocation of resources, including budget and personnel, to ensure the SOC's effectiveness in monitoring, detecting, and responding to security incidents.

Once objectives are defined, the SOC deployment focuses on building a robust technological foundation. This includes acquiring necessary hardware, software, and security tools such as intrusion detection/prevention systems (IDS/IPS), firewalls, and Security Information and Event Management (SIEM) platforms. Creating a dedicated physical space for the SOC team is crucial to ensure secure operations, with considerations for equipment placement, access controls, and monitoring systems.

Personnel play a pivotal role in SOC operations. Hiring or training a skilled cyber security team proficient in threat analysis, incident response, and modern security practices is essential. This team will execute incident response plans, continuously monitor network activities, and collaborate with other departments to strengthen the institution's overall security posture. The SOC's role extends beyond technical functions—it requires strong collaboration, clear communication, and the ability to adapt to emerging threats. Regular training sessions keep the team updated on evolving threat landscapes and sophisticated attack methods.

Ultimately, a well-deployed SOC enhances the engineering institution's ability to identify and mitigate potential cyber risks, ensuring the security and integrity of its digital infrastructure, research data, and operational processes. By implementing a strategic and well-coordinated deployment plan, the institution sets the foundation for proactive cyber security management and effective incident response.

3.8 THREAT INTELLIGENCE

Threat intelligence is a critical component of modern cyber security, offering organizations valuable insights into the ever-evolving landscape of cyber threats and vulnerabilities. At its core, threat intelligence encompasses the collection, analysis, and dissemination of information that enables organizations to comprehend the methods, motivations, and indicators associated with potential and existing cyber threats. By staying informed about emerging attack techniques, tactics, and procedures used by threat actors, organizations can enhance their ability to detect, prevent, and respond to cyber incidents effectively.

Threat intelligence comes in various forms, tailored to different organizational needs. Strategic intelligence provides a broad overview of the global threat landscape, including geopolitical factors that might influence cyber attacks. Tactical intelligence delves into specific threats and attack methods that are currently in play, aiding organizations in understanding the tools and vulnerabilities exploited by attackers. Operational intelligence offers real-time insights into ongoing attacks and incidents, enabling swift response actions to mitigate risks. Additionally, technical intelligence offers granular technical details such as indicators of compromise (IoCs), malware analysis, and attack signatures, which are crucial for fine-tuning security tools and systems.

Organizations gather threat intelligence from diverse sources, including publicly available data, commercial threat intelligence feeds, government reports, and collaborative information-sharing communities. This wealth of information empowers organizations to proactively identify threats, fortify their defenses, improve incident response capabilities, and make informed decisions to safeguard their digital assets. By embracing threat intelligence as a proactive strategy, organizations strengthen their cyber security posture and contribute to a more robust collective defense against the rapidly evolving landscape of cyber threats.

3.9 INCIDENT RESPONSE

Incident response is a structured and methodical approach that organizations employ to effectively manage and mitigate the impact of cyber security incidents. These incidents can range from data breaches and malware infections to cyber attacks and unauthorized access. The overarching goal of incident response is to minimize damage, contain threats, and swiftly restore normal operations.

The first stage of incident response involves Preparation. This entails the creation of a comprehensive incident response plan (IRP) that outlines the roles, responsibilities, and protocols to be followed during an incident. The plan defines communication channels, establishes escalation procedures, and identifies the necessary technical resources for

effective incident management. Regular training and simulations ensure that personnel are well-versed in their roles and familiar with the plan's execution.

The Detection and Identification phase revolves around monitoring networks, systems, and applications for any signs of abnormal or suspicious activity. When potential incidents are detected, they are meticulously assessed to ascertain their nature, scope, and potential impact. This stage is critical for swiftly identifying threats and launching an appropriate response. Subsequently, the Containment phase comes into play, where immediate actions are taken to prevent the incident from escalating. This might involve isolating compromised systems, disabling compromised accounts, or disconnecting affected parts of the network. The objective is to curtail the attacker's access and limit the damage.

The Eradication and Recovery phases are aimed at restoring normalcy. Eradication entails eliminating the root cause of the incident, which could involve removing malware, patching vulnerabilities, or strengthening security measures. Following eradication, the Recovery phase involves systematically bringing affected systems and services back online. This requires meticulous testing to ensure that restored systems are secure and fully functional. Post-incident, organizations engage in a Lessons Learned assessment to analyze the incident response process, pinpoint areas for improvement, and refine the incident response plan. Documentation is a consistent thread throughout these phases, enabling organizations to maintain a record of actions taken, evidence collected, and decisions made, which is vital for compliance, analysis, and future readiness.

In a rapidly evolving threat landscape, incident response remains a crucial pillar of an organization's cyber security strategy. By having a well-prepared incident response plan, a vigilant approach to detection, and a meticulous process for containment, eradication, and recovery, organizations can effectively mitigate the impact of cyber security incidents and ensure the resilience of their operations and digital assets.

3.10 QRADAR

IBM QRadar is a comprehensive and advanced security information and event management solution. It offers organizations a powerful platform for collecting, analyzing, and correlating data from various sources across their IT environment to detect and respond to cybersecurity threats effectively. QRadar provides real-time visibility into an organization's security landscape, enabling proactive threat detection, incident response, and compliance management.

With its robust capabilities, QRadar assists organizations in monitoring network traffic, system logs, application activities, and user behavior to identify potential security breaches and anomalies. The platform employs advanced analytics, machine learning, and threat intelligence integration to enhance its detection accuracy and identify patterns indicative of cyber threats.

One of QRadar's key strengths is its ability to correlate disparate data points from different sources, allowing security teams to gain a holistic view of potential threats and attacks. This correlation enhances the understanding of attack tactics, techniques, and procedures used by cybercriminals. Additionally, QRadar offers customizable dashboards, real-time alerts, and reporting features that help security professionals make informed decisions and respond swiftly to incidents.

As a trusted SIEM solution, IBM QRadar empowers organizations to strengthen their cyber security defenses by providing insights, automation, and a centralized platform for managing security incidents and risks. Its capabilities contribute to a proactive and adaptive approach to cyber security, ensuring that organizations can effectively safeguard their digital assets and sensitive data in today's dynamic threat landscape.