maxapex

MAXPROTECT

VULNERABILITY ASSESSMENT REPORT

Table of Content

Vulnerability Assessment Report

Statement of Confidentiality

The contents of this document have been developed by Information Security Team at MaxAPEX Cloud for Client <Client Name> for <server/domain>. MaxAPEX Cloud considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Client <Client Name>. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Client <Client Name>.

Engagement Contacts

Client Contacts		
Primary Contact	**Company**	**Primary Contact Email**
<Client Name>	Company Name	<client name>@company.com

Assessor Contacts	
Primary Contact	**Primary Contact Email**
MaxAPEX Support	support@maxapex.com

Scope

The scope of this security assessment was strictly limited to the server identified as: <sample server>

Our testing efforts were focused exclusively on evaluating the security posture of this single server, encompassing its system configurations, network services, and associated security protocols.

No other systems, networks, or services outside of this specified server were included in this assessment. The aim was to perform a detailed and focused analysis on <sample server> to identify potential vulnerabilities and assess its resilience against security threats.

Executive Summary

This security assessment report presents the findings from a comprehensive security scan conducted on the server <sample server>. The server was assessed for various security vulnerabilities across multiple service vectors.

The assessment identified a total of several vulnerabilities that need attention to mitigate potential risks.

Risk Assessment	Number of Vulnerability Classes
Critical	0
High	0
Medium	1
Low	1
Informational	3
Total	5

MEDIUM

Key findings include:

HSTS Missing From HTTPS Server: The server does not enforce HTTP Strict Transport Security (HSTS), allowing potential SSL-stripping man-in-the-middle attacks. This medium-risk issue can be remedied by configuring the server to utilize HSTS as per RFC 6797.

LOW

SSL Certificate Issues: The SSL certificate of the server cannot be trusted. This is due to either the absence of intermediate certificates, expired certificates, or signatures that could not be verified. This represents a medium-risk threat to the integrity and confidentiality of data in transit.

INFO

Discouraged SSL/TLS Cipher Suites: The server advertises SSL/TLS cipher suites that are discouraged due to security vulnerabilities. It is advised to configure the server to use only recommended cipher suites to enhance the security of data exchanges.
Additional low-risk vulnerabilities were also detected but do not pose immediate threats. However, addressing these vulnerabilities will further strengthen the server's security posture.

Recommendations

Immediate actions are required to address the identified vulnerabilities:

- Configure the web server to implement HSTS.
- Obtain and configure a valid SSL certificate from a trusted certificate authority.
- Restrict the use of discouraged cipher suites by configuring the server to support only those recommended by recent security standards.

These measures will significantly enhance the security of the server and protect against potential cyber-attacks.

Detailed Analysis

Host Information
DNS Name: <sample server>
IP: XX.XX.XX.XX

Vulnerabilities

1. HSTS Missing From HTTPS Server

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.

Solution
Configure the remote web server to use HSTS.

Risk Factor
Medium

CVSS v3.0 Base Score
5.9 (AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:N)

Proof of Concept
`tcp/443/www`

```
HTTP/1.1 200 OK
Date: Thu, 02 May 2024 07:57:39 GMT
Server: Apache
Content-Length: 202
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

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

2. SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below:

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'not Before' dates, or after one of the certificate's 'not After' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that We either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Low

CVSS v3.0 Base Score

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

Proof of Concept
tcp/443/www

```
The following certificate was part of the certificate chain sent
by the remote host, but it has expired:

|-Subject : CN=*.xxxxxxxxx.net
|-Not After : Dec 13 23:59:59 2023 GMT
```

3. DNS Server BIND version Directive Remote Version Detection

Synopsis
It is possible to obtain the version number of the remote DNS server.

Description
The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution
It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.

Risk Factor
None

Proof of Concept
udp/53/dns

```
Version : 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.7
```

4. DNS Server Detection

Synopsis
A DNS server is listening on the remote host.

Description
The remote service is a Domain Name System (DNS) server, which provides a mapping between host names and IP addresses.

Solution
Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor
None

Proof of Concept
```
53/tcp open  domain  syn-ack ttl 51
53/udp open  domain  syn-ack ttl 51
```

5. 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

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.

Solution
Only enable support for recommended cipher suites.

Risk Factor
None

Proof of Concept

tcp/443/www

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

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name	Code	KEX	Auth	Encryption	MAC
ECDHE-RSA-DES-CBC3-SHA	0xC0, 0x12	ECDH	RSA	3DES-CBC(168)	SHA1
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC(168)	SHA1

High Strength Ciphers (>= 112-bit key)

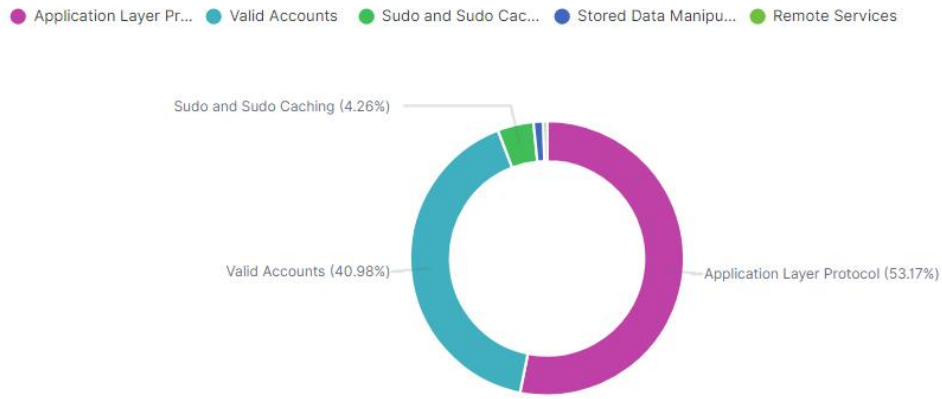
Name	Code	KEX	Auth	Encryption	MAC
ECDHE-RSA-CAMELLIA-CBC-128	0xC0,0x76	ECDH	RSA	Camellia-CBC(128)	SHA256
ECDHE-RSA-CAMELLIA-CBC-256	0xC0,0x77	ECDH	RSA	Camellia-CBC(256)	SHA384
RSA-AES-128-CCM-AEAD	0xC0,0x9C	RSA	RSA	AES-CCM(128)	AEAD
RSA-AES-128-CCM8-AEAD	0xC0,0xA0	RSA	RSA	AES-CCM8(128)	AEAD
RSA-AES-256-CCM-AEAD	0xC0,0x9D	RSA	RSA	AES-CCM(256)	AEAD
RSA-AES-256-CCM8-AEAD	0xC0,0xA1	RSA	RSA	AES-CCM8(256)	AEAD
TLS_AES_128_CCM_SHA256	0x13,0x04	-	-	AES-CCM(128)	AEAD
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
SEED-SHA	0x00,0x96	RSA	RSA	SEED-CBC(128)	SHA1
ECDHE-RSA-AES128-SHA256	0xC0,0x27	ECDH	RSA	AES-CBC(128)	SHA256
ECDHE-RSA-AES256-SHA384	0xC0,0x28	ECDH	RSA	AES-CBC(256)	SHA384
RSA-AES128-SHA256	0x00,0x3C	RSA	RSA	AES-CBC(128)	SHA256
RSA-AES256-SHA256	0x00,0x3D	RSA	RSA	AES-CBC(256)	SHA256
RSA-CAMELLIA128-SHA256	0x00,0xBA	RSA	RSA	Camellia-CBC(128)	SHA256
RSA-CAMELLIA256-SHA256	0x00,0xC0	RSA	RSA	Camellia-CBC(256)	SHA256

MITRE ATT&CK Summary

Server Name	IP address	Operating system	Last keep alive
<sample server>	X.X.X.X	Rocky Linux 8.9	April 30, 2024

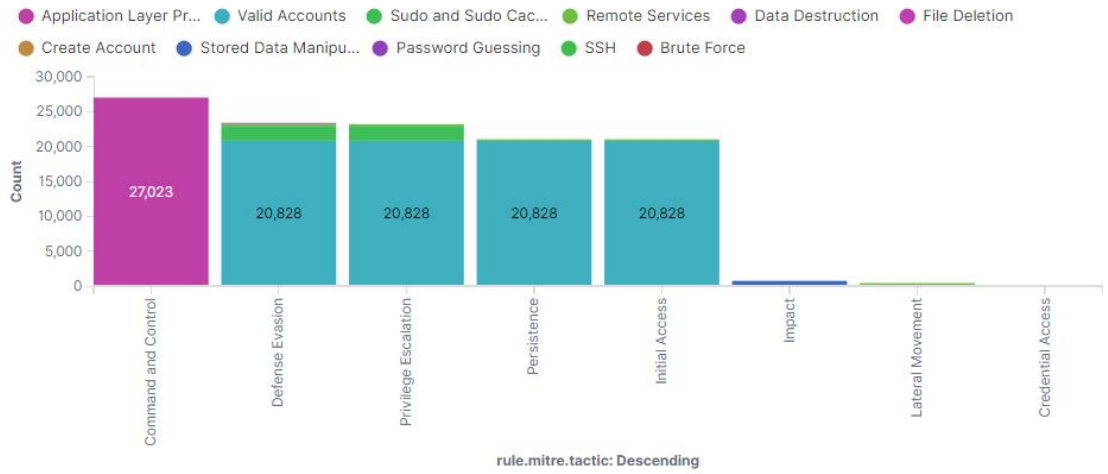
Security events from the knowledge base of adversary tactics and techniques based on real-world observations

Alerts level by attack



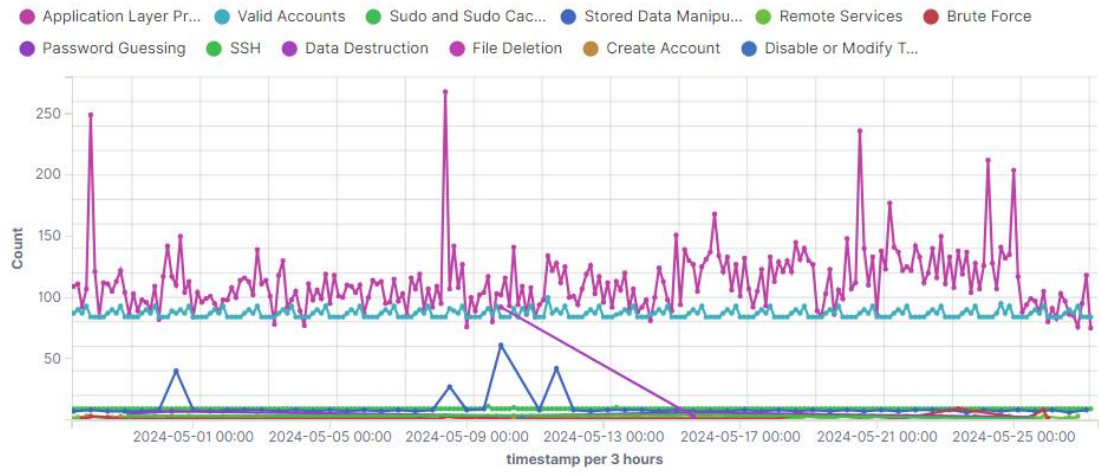
This section presents the distribution and severity of alerts generated due to various attacks detected on the system. Each alert is categorized by its level of importance or potential impact, helping to prioritize responses based on the severity of the threats.

Top tactics



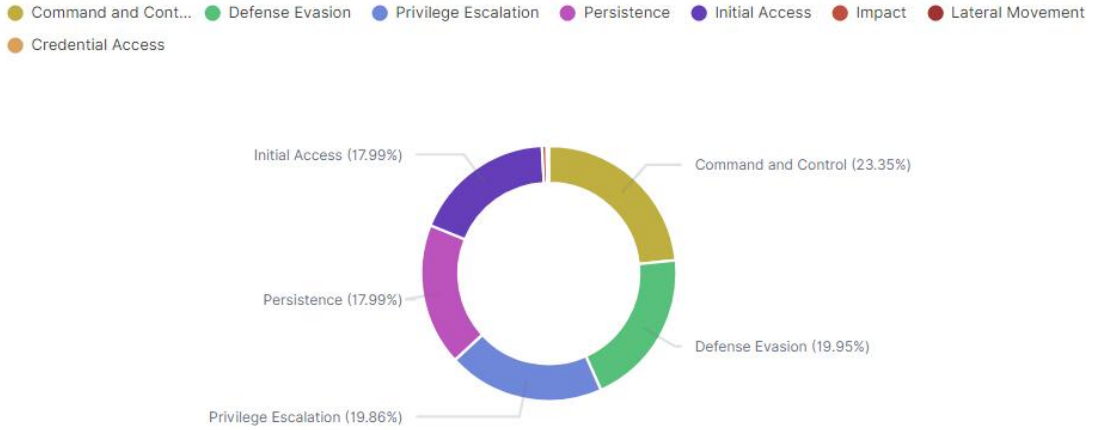
This graph highlights the most frequently used tactics by attackers. It provides a visual representation of the tactics that are most prevalent, indicating common threat vectors and areas where security measures may need reinforcement.

Mitre alerts evolution



This section shows the trend of alerts over time, mapped against various tactics identified in the MITRE framework. It provides insights into how attack patterns evolve, helping in understanding whether certain attacks are increasing in frequency or severity.

Top tactics pie



This section features a pie chart that visually represents the proportion of different tactics employed in attacks, as classified by the MITRE ATT&CK framework. It provides a quick glance at which tactics are most dominant, enabling security teams to quickly assess the primary methods being used by attackers and adjust their defensive strategies accordingly. This visual helps in understanding the distribution and focus areas of current security threats, assisting in prioritizing security measures and responses.

Conclusion

The analysis conducted over the past month provides a clear view of the adversarial tactics and techniques impacting the server at <sample server>. It is evident that while some areas show robust defenses, others require strategic enhancements to align with best security practices and the evolving threat landscape. Moving forward, we must integrate the insights from this assessment into our broader security strategy, focusing on areas with frequent alerts and adopting proactive defense measures. This will not only mitigate current vulnerabilities but also prepare us for future security challenges.