June 8, 2021

ACME Corporation (Sample Report)

Security Assessment Report

XERVANT

Verifying Trust

Contents

Executive Summary

With every security assessment, our goal is to identify the information security related strengths and weaknesses of the organization and its infrastructure so that we can celebrate the positive and identify the areas that may have opportunities for improvement. In the case of your security assessment, we identified the following strength:

- By performing regular security assessments, you are making a conscious move towards improving the security of your organization by identifying the potential risks. These risks can then be prioritized and used as the catalyst to define a specific remediation plan for the organization.

Although the previous area indicates that the organization has taken strides in properly securing and protecting its infrastructure and data, there were several issues identified which have the potential to be damaging to the organization including:

- We noted the use of deprecated encryption suites and other encryption related weaknesses. By using outdated encryption ciphers, suites, and protocols, the potential exists for sensitive data protected by encrypted tunnels to become exposed via the vulnerabilities associated with these deprecated encryption components.
- There were several software components in use that were outdated due to known unpatched security flaws or that had reached the end of life from a support perspective.
- We identified a number of services using default user credentials or no user credentials at all.
- We identified several services which allow multiple failed authentication attempts without taking any discernible defensive actions. This type of configuration allows an attacker to perform unrestricted brute-force and dictionary-based password guessing attacks.
- We noted authentication mechanisms which didn't require any type of encryption for the user credentials. This type of configuration would allow attackers to utilize network sniffers to capture the user credentials as they traverse the network.
- We noted the use of default web pages which reveals details about the web platform and server.

Overall we believe the organization has a solid foundation from which to build and upon executing the necessary remediation steps, will have a very strong defensive posture from an information security perspective related to the scope of this assessment.

By the Numbers

10	3	1	5/10
Vulnerabilities	High Risk	Strengths	Security Posture

Project Scope

Perform a comprehensive security assessment and penetration test of the information systems infrastructure of ACME Corporation (Sample Report) which included the following:

- Internal network security assessment and penetration test of the following data center networks:

  (IP Addresses Redacted)
  (IP Addresses Redacted)

Methodology

Project Management

Our project management approach can best be compared to the Agile method in that we recognize the nature of information security related assessment projects can often times be unpredictable. For example, if a specific vulnerability is discovered, the project may need to expand to include some additional discovery elements in order to properly identify the risk associated with that vulnerability and to create a successful mitigation strategy. As such, our security assessment projects are globally managed as a series of specific overall goals which may be made up of relatively small tasks that are conceived and executed in an adaptive manner as the situation dictates.

Approach & Perspective

Our security assessment approach is guided by principles of practicality and real-world effectiveness. Although we feel that administrative security controls such as policies and procedures are important, we recognize that without proper execution and evaluation, they don't necessarily translate into improved security for your organization. As such, you will find that our assessments are well-rounded and very technical in nature which yields effective security strategies that will improve your real-world security posture.

Another important aspect of our approach is related to perspective. We approach each engagement from the viewpoint of an attacker. This helps us to identify the potential entry points and then qualify them from a risk standpoint which allows you to easily prioritize addressing them. We have found this type of approach to be most effective in improving the real-world security of an organization.

Methodology *(continued)*

Vulnerability Sources

In order to provide a thoroughly technical security assessment, we compile vulnerability data from a variety of sources and use it to drive our assessment model for a given engagement. In addition to compiling and analyzing vulnerability data, we also incorporate industry-standard security threat models such as OWASP Top 10 and SANS Critical Security Controls.

Techniques Used

- **Security Configuration Questionnaire**
  When applicable, we utilize a security configuration questionnaire to help establish a baseline expectation of the security posture of the organization. In addition, the results of this questionnaire are often used to help define the appropriate security controls that should be evaluated during the security assessment.

- **Assessment Tools**
  We utilize an array of industry standard and custom assessment tools to review configurations and identify potential vulnerabilities. Although not an exhaustive list, some of the industry-standard tools include: OpenVAS, Nmap, Metasploit, Hydra, SSLScan, Airmon and Wireshark.

- **The Human Touch**
  Results identified by our automated tools are manually verified by a SANS Institute GIAC certified information security professional. In addition, we also perform manual analysis of common vulnerabilities to verify the automated tools are properly identifying potential areas of concern from an information security perspective.

Risk Model

We utilize a three-tier risk model to prioritize the potential liability of discovered vulnerabilities as well as the expected impact on the confidentiality, integrity and availability of the organization's systems, infrastructure and/or data.

- **High**
  A high risk vulnerability exhibits the potential for an attacker to substantially exploit the organization and may result in loss of revenue, system/data availability disruptions, compromise of confidential information or otherwise negatively impact the organization.

- **Medium**
  A medium risk vulnerability exhibits the potential for an attacker to exploit the organization, but it would typically require multiple vulnerabilities working in conjunction or some other special condition to be met in order to facilitate the attack. The impact to the organization should still be considered severe, but not as detrimental as a successful exploit against a high risk vulnerability.

- **Low**
  A low risk vulnerability typically identifies a vulnerability that has a minimalistic impact on the organization if exploited or one that requires multiple specialized conditions to be met in order to facilitate the attack. Although a low risk vulnerability is not as severe as its counterparts, it should be considered as a viable risk as it is indicative of weaknesses in one or more security layers within the organization.

Information Security Strengths

We identified the following information security related strengths:

Good Job

Security Assessments

By performing regular security assessments, you are making a conscious move towards improving the security of your organization by identifying the potential risks. These risks can then be prioritized and used as the catalyst to define a specific remediation plan for the organization.

Network Vulnerabilities

We identified the following network vulnerabilities:

High Risk

N1. Default User Credentials

(IP Addresses Redacted)

The services running at the listed hosts are configured with the default administrative user credentials.

High Risk

N2. Outdated Apache Tomcat

(IP Addresses Redacted)

The Apache Tomcat instances running at the listed hosts are running an outdated version (v7.0.33) which is susceptible to numerous known vulnerabilities.

High Risk

N3. Unencrypted Authentication

(IP Addresses Redacted)

The listed services require authentication, but do not invoke any type of encryption for the user credentials as they traverse the network. By allowing the use of the unencrypted services in conjunction with authentication, an attacker may be able to use a network sniffer to capture user credentials during the login cycle.

Medium Risk

N4. Default Web Pages

(IP Addresses Redacted)

The web server instances running at the listed hosts include the default home page and/or example files which may be used to gather information about the server.

Medium Risk

N5. Deprecated SSL Versions Allowed

(IP Addresses Redacted)

The listed hosts/services allow the use of SSLv2 and/or SSLv3 protocols without Transport Layer Security (TLS). These implementations have been deprecated due to confirmed security flaws within these protocols allowing eavesdropping of the encrypted data.

Medium Risk

N6. SMTP Relay

(IP Addresses Redacted)

The Simple Mail Transfer Protocol (SMTP) services running on the listed hosts are configured to allow relaying of messages destined for domains not served by the server. This type of configuration allows attackers to send SPAM and other potentially harmful mail from your server without restriction. In addition, this configuration may allow your SMTP server to become black-listed as an open relay server which will hinder legitimate message delivery for your domain.

Network Vulnerabilities *(continued)*

Medium Risk

N7. SSH Allows Weak Encryption

(IP Addresses Redacted)

The listed hosts allow the use of weak encryption algorithms for Secure Shell (SSH) connections. The weak ciphers offered include one or more of the following:

3DES-CBC
AES128-CBC
AES192-CBC
AES256-CBC
ARCFOUR128
ARCFOUR256
BLOWFISH-CBC
RIJNDAEL-CBC@LYSATOR.LIU.SE
RIJNDAEL128-CBC
RIJNDAEL192-CBC
RIJNDAEL256-CBC

Medium Risk

N8. TLS Uses Weak Diffie-Hellman Group Key SIze

(IP Addresses Redacted)

The listed hosts/services Transport Layer Security (TLS) uses a Diffie-Hellman Group key size with an insufficient key size of 1024 bits or less. An attacker may be able to capture and decrypt the TLS communication offline providing them with the ability to observe sensitive information.

Network Vulnerabilities *(continued)*

Medium Risk

N9. Weak Encryption Allowed

(IP Addresses Redacted)

The listed hosts and services allow the use of weak encryption algorithms. The weak ciphers offered include one or more of the following:

```
TLS_DH_ANON_EXPORT_WITH_RC4_40_MD5
TLS_DH_ANON_WITH_3DES_EDE_CBC_SHA
TLS_DH_ANON_WITH_AES_128_CBC_SHA
TLS_DH_ANON_WITH_AES_256_CBC_SHA
TLS_DH_ANON_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_ANON_WITH_CAMELLIA_256_CBC_SHA
TLS_DH_ANON_WITH_DES_CBC_SHA
TLS_DH_ANON_WITH_RC4_128_MD5
TLS_DH_ANON_WITH_SEED_CBC_SHA
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_ECDH_ANON_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_ANON_WITH_AES_128_CBC_SHA
TLS_ECDH_ANON_WITH_AES_256_CBC_SHA
TLS_ECDH_ANON_WITH_RC4_128_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_PSK_WITH_3DES_EDE_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
```

See Microsoft KB article 245030 for more info
https://support.microsoft.com/en-us/kb/245030

Low Risk

N10. SSH Allows Weak Message Authentication Code (MAC) Algorithms

(IP Addresses Redacted)

The listed hosts allow the use of weak Message Authentication Code (MAC) encryption algorithms for Secure Shell (SSH) connections. The weak algorithms offered include one or more of the following:

```
HMAC-MD5
HMAC-SHA1-96
```

Open TCP Ports

We identified the following external open TCP ports:

IP Address	Open TCP Ports
(IP Addresses Redacted)	22 (SSH)
(IP Addresses Redacted)	25 (SMTP) 80 (HTTP) 443 (HTTPS)

Open UDP Ports

We identified the following external open UDP ports:

IP Address	Open UDP Ports
(IP Addresses Redacted)	*No Open UDP Ports*

Network Remediation Recommendations

N1. Default User Credentials

(IP Addresses Redacted)

1. Update user credentials to something other than the default values.

N2. Outdated Apache Tomcat

(IP Addresses Redacted)

1. Consider updating to the latest release version of Apache Tomcat (v9.0.43).

N3. Unencrypted Authentication

(IP Addresses Redacted)

1. Consider requiring encryption for all services transmitting/receiving sensitive information such as user credentials via the network.

N4. Default Web Pages

(IP Addresses Redacted)

1. Consider removing default and example files.

Network Remediation Recommendations *(continued)*

N5. Deprecated SSL Versions Allowed

(IP Addresses Redacted)

1. Disable support for SSLv2 and SSLv3.

Linux/Apache

1. *Edit the /etc/httpd/conf.d/ssl.conf file*
2. *Add/Update the **SSLProtocol** line as follows:*
   SSLProtocol all –SSLv2 –SSLv3

Windows/IIS

1. *Open the Windows Registry Editor*
2. *Navigate to the following registry key:*
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
3. *Create or navigate to the weak protocol key (**SSL 2.0** or **SSL 3.0**)*
4. *Create or navigate to the **Client** key*
5. *Set the **DisabledByDefault** dword value to **00000001** for each weak protocol*
6. *Create or navigate to the **Server** key*
7. *Set the **DisabledByDefault** dword value to **00000001** for each weak protocol*

N6. SMTP Relay

(IP Addresses Redacted)

1. Contact the SMTP software vendor to see if an update is available which prevents the RCPT TO command from accepting domains that are not serviced by the server.

Network Remediation Recommendations *(continued)*

N7. SSH Allows Weak Encryption

(IP Addresses Redacted)

1. Disable support for all CBC and ARCFOUR (RC4) based ciphers.

Linux

1. *Edit the /etc/ssh/sshd_config file*
2. *Add/Update the Ciphers line as follows (no line break):*
   Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
3. *Restart SSH service*

Cisco

1. *Enter configuration mode by entering the **config t** command.*
2. *Enter the **ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr** command to disable the insecure ciphers.*
3. *Enter the **exit** command to exit configuration mode.*
4. *Enter the **wr mem** command to save the changes to the startup configuration.*

Network Remediation Recommendations *(continued)*

N8. TLS Uses Weak Diffie-Hellman Group Key SIze

(IP Addresses Redacted)

1. Update the TLS protocol Diffie-Hellman Group key size to at least 2048 bits.

Cisco

1. *Enter configuration mode by entering the **config t** command.*
2. *Enter the **ssl server-version tlsv1.2** command to set the minimum server SSL level to TLS v1.2.*
3. *Enter the **ssl client-version tlsv1.2** command to set the minimum client SSL level to TLS v1.2.*
4. *Enter the **ssl cipher tlsv1.2 high** command to set the minimum TLS v1.2 ciphers to AES-256 with SHA-2.*
5. *Enter the **ssl dh-group group24** command to set the Diffie-Hellman Group to Group 24 (2048-bit modulus/256-bit prime - Next Generation Encryption).*

Windows

1. *Open the Windows Registry Editor*
2. *Navigate to the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman*
3. *Set the **ServerMinKeyBitLength** dword value to **00000800** for 2,048 bits*

Network Remediation Recommendations *(continued)*

N9. Weak Encryption Allowed

(IP Addresses Redacted)

1. Disable support for all CBC and ARCFOUR (RC4) based ciphers.

Linux

1. *Edit the /etc/httpd/conf.d/ssl.conf file*
2. *Add/Update the **SSLCipherSuite** line as follows (no line break):*
   SSLCipherSuite HIGH:!aNULL:!MD5

Windows

1. *Open the Windows Registry Editor*
2. *Navigate to the following registry key:*
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers
3. *Create and/or navigate to each of the following keys:*
   Triple DES 168
   RC4 40/128
   RC4 56/128
   RC4 128/128
4. *Set the **Enabled** dword value to **00000000** for each weak cipher*

Network Remediation Recommendations *(continued)*

N10. SSH Allows Weak Message Authentication Code (MAC) Algorithms

(IP Addresses Redacted)

1. Disable support for all MD5 and 96-bit based MAC algorithms.

Cisco

1. *Enter configuration mode by entering the **config t** command.*
2. *Enter the **ip ssh server algorithm mac hmac-sha1** command to disable the insecure MAC algorithm.*
3. *Enter the **exit** command to exit configuration mode.*
4. *Enter the **wr mem** command to save the changes to the startup configuration.*

Linux

1. *Edit the /etc/ssh/sshd_config file*
2. *Add/Update the MACs line as follows:*
   MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-etm@openssh.com
3. *Restart SSH service*