**Vulnerability Assessment Report   
 For**



**บริษัท ไอเน็ต แมเนจด์ เซอร์วิสเซส จำกัด**

**Date : 14 February 2022**

**Document Security Level : Confidential   
Document Version: 1.0**

| Version | Date | Edit Report | Editor |
| --- | --- | --- | --- |
| 1.0 | 14 February 2022 | Creation | INET Managed Service |

| Example Company Limited. | | INET Managed Services CO., LTD. | |
| --- | --- | --- | --- |
| Name |  | Name |  |
| Position |  | Position |  |
| Tel |  | Tel |  |
| Signature |  | Signature |  |

**Table of Contents**

# 1. Restrictions on disclosure and use of information

Restriction on Disclosure and Use of Confidential Information. The Executive understands and agrees that the Confidential Information constitutes an asset of the Company and its affiliated entities and may not be converted to the Executive's own use. Accordingly, the Executive hereby agrees that the Executive shall not, directly, or indirectly, at any time, reveal, divulge, or disclose to any Person not expressly authorized by the Company any Confidential Information, and the Executive shall not, directly, or indirectly, use or make use of any Confidential Information in connection with any business activity other than that of the Company. The parties acknowledge and agree that this Agreement is not intended to, and does not, alter either the Company's rights or the Executive's obligations under any state or federal statutory or common law regarding trade secrets and unfair trade.

# 2. Operation Method

## 2.1 Posture Review

## 2.2 Information Gathering

## 2.3 Enumeration

## 2.4 Vulnerability Assessment

## 2.5 Analyze & Evaluate Risk Value

## 2.6 Report

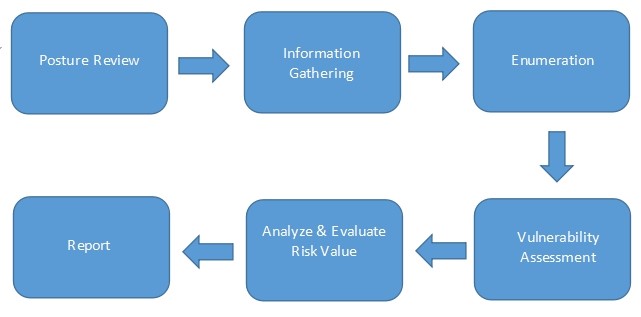


Figure 1: Operation Method

# 3. Project Scope

## 3.1 Infrastructure Vulnerability Assessment

**Target / IP Address:**

| No | Domain / Server Name | Public IP Address | Private IP Address | OS/Model | Functions | Public Assessment | Private Assessment |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | None | None | 192.168.128.250 | None | None | None | None |
| 2 | None | None | 192.168.128.3 | None | None | None | None |
| 3 | None | None | 192.168.128.4 | None | None | None | None |
| 4 | None | None | 192.168.128.5 | None | None | None | None |
| 5 | None | None | 192.168.128.6 | None | None | None | None |
| 6 | None | None | 192.168.128.7 | None | None | None | None |
| 7 | None | None | 192.168.128.8 | None | None | None | None |
| 8 | None | None | 192.168.200.11 | None | None | None | None |
| 9 | None | None | 192.168.200.12 | None | None | None | None |
| 10 | None | None | 192.168.200.2 | None | None | None | None |
| 11 | None | None | 192.168.200.3 | None | None | None | None |
| 12 | None | None | 192.168.200.31 | None | None | None | None |
| 13 | None | None | 192.168.200.32 | None | None | None | None |
| 14 | None | None | 192.168.200.51 | None | None | None | None |
| 15 | None | None | 192.168.200.52 | None | None | None | None |
| 16 | None | None | 192.168.200.53 | None | None | None | None |

## 3.2 Web Application Vulnerability Assessment

**Target / IP Address:**

| No | Domain / Server Name | Public IP Address | Private IP Address | OS/Model | Functions | Public Assessment | Private Assessment |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |

# 4. Testing Tools

| Tool Name | Testing Type |
| --- | --- |
| Nmap | Host and Service Discovery |
| Nessus | Infrastructure Vulnerability Assessment |
| Acunetix | Web Application Vulnerability Assessment |

# 5. Infrastructure Vulnerability Assessment

**Vulnerability Assessment from Public Access   
 Testing data :  
 Tester IP Address :**

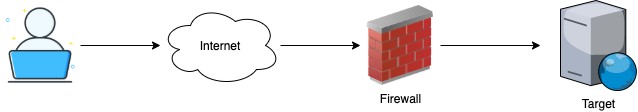


Figure 2: Vulnerability Assessment from Public Access

**Vulnerability Assessment from Private Access (for private or restricted access target)   
 Testing data :  
 Tester IP Address :**

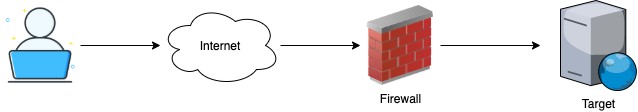


Figure 3: Vulnerability Assessment from Private Access

## 5.1 Target Information

| No | Domain / Server Name | IP Address | OS/Model | Port |
| --- | --- | --- | --- | --- |
| 1 | None | 192.168.128.250 | None | TCP,135,139,445 |
| 2 | None | 192.168.128.3 | None | TCP,22,80,443,8080,8443 |
| 3 | None | 192.168.128.4 | None | TCP,22,80,443,8080,8443 |
| 4 | None | 192.168.128.5 | None | TCP,22,80,443,8080 |
| 5 | None | 192.168.128.6 | None | TCP,22,80,443,8080,8443 |
| 6 | None | 192.168.128.7 | None | TCP,22,8080 |
| 7 | None | 192.168.128.8 | None | TCP,22,8080 |
| 8 | None | 192.168.200.11 | None | TCP,22,8080 |
| 9 | None | 192.168.200.12 | None | TCP,22,8080 |
| 10 | None | 192.168.200.2 | None | TCP,22,80 |
| 11 | None | 192.168.200.3 | None | TCP,22,80,3307 |
| 12 | None | 192.168.200.31 | None | TCP,22,3306,4567,9200 |
| 13 | None | 192.168.200.32 | None | TCP,22 |
| 14 | None | 192.168.200.51 | None | TCP,80,135,139,445,3389,8080,27017 |
| 15 | None | 192.168.200.52 | None | TCP,80,135,139,445,3389,8080,27017 |
| 16 | None | 192.168.200.53 | None | TCP,80,135,139,445,3389,8080,27017 |

## 5.2 Executive summary

The purpose of this activity is to find the vulnerability on the target infrastructure.

### 5.2.1 Summary Vulnerability by Severity

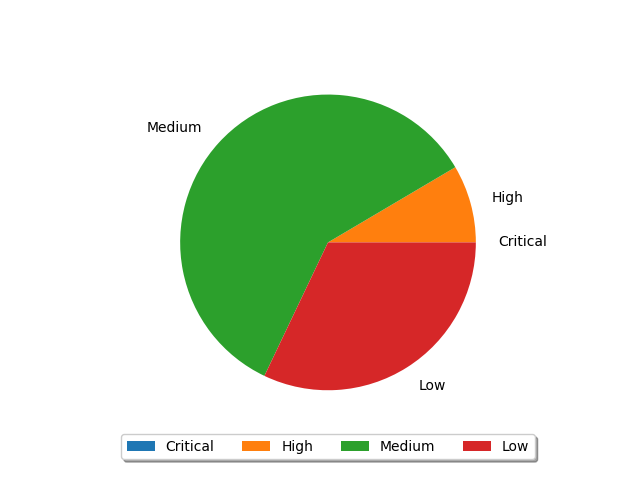


Figure 4: Summary by Severity of Infrastructure Vulnerability Assessment

### 5.2.2 Vulnerability by Target

| No | Domain/Server Name | IP Address | Critical | High | Medium | Low | Total |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | None | 192.168.128.250 | 0 | 0 | 2 | 0 | 2 |
| 2 | None | 192.168.128.3 | 0 | 0 | 1 | 4 | 5 |
| 3 | None | 192.168.128.4 | 0 | 0 | 1 | 4 | 5 |
| 4 | None | 192.168.128.5 | 0 | 0 | 3 | 3 | 6 |
| 5 | None | 192.168.128.6 | 0 | 0 | 5 | 4 | 9 |
| 6 | None | 192.168.128.7 | 0 | 0 | 1 | 2 | 3 |
| 7 | None | 192.168.128.8 | 0 | 0 | 1 | 2 | 3 |
| 8 | None | 192.168.200.11 | 0 | 0 | 1 | 2 | 3 |
| 9 | None | 192.168.200.12 | 0 | 0 | 1 | 2 | 3 |
| 10 | None | 192.168.200.2 | 0 | 0 | 1 | 2 | 3 |
| 11 | None | 192.168.200.3 | 0 | 0 | 1 | 2 | 3 |
| 12 | None | 192.168.200.31 | 0 | 0 | 1 | 2 | 3 |
| 13 | None | 192.168.200.32 | 0 | 0 | 1 | 2 | 3 |
| 14 | None | 192.168.200.51 | 0 | 3 | 15 | 1 | 19 |
| 15 | None | 192.168.200.52 | 0 | 3 | 13 | 1 | 17 |
| 16 | None | 192.168.200.53 | 0 | 3 | 15 | 1 | 19 |
| Total | | | 0 | 9 | 63 | 34 | 106 |

## 5.3 Infrastructure Vulnerability Detail

|  |  |  |  |
| --- | --- | --- | --- |
| ID | 1 | Finding | SSL Certificate Signed Using Weak Hashing Algorithm |
| Severity | High | Port | ,27017 |
| Target | ,192.168.200.51,192.168.200.52,192.168.200.53 | | |
| Detail | The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.  Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.  Note that certificates in the chain that are contained in the Nessus CA database (known\_CA.inc) have been ignored. | | |
| Solution | Contact the Certificate Authority to have the SSL certificate reissued. | | |
| Remark | https://tools.ietf.org/html/rfc3279 http://www.nessus.org/u?9bb87bf2 http://www.nessus.org/u?e120eea1 http://www.nessus.org/u?5d894816 http://www.nessus.org/u?51db68aa http://www.nessus.org/u?9dc7bfba | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | 2 | Finding | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| Severity | High | Port | ,3389,27017 |
| Target | ,192.168.200.51,192.168.200.51,192.168.200.52,192.168.200.52,192.168.200.53,192.168.200.53 | | |
| Detail | The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or  else that uses the 3DES encryption suite.  Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network. | | |
| Solution | Reconfigure the affected application if possible to avoid use of medium strength ciphers. | | |
| Remark | https://www.openssl.org/blog/blog/2016/08/24/sweet32/ https://sweet32.info | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | 3 | Finding | MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) |
| Severity | Medium | Port | ,49157 |
| Target | ,192.168.128.250 | | |
| Detail | The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database. | | |
| Solution | Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10. | | |
| Remark | http://www.nessus.org/u?52ade1e9 http://badlock.org/ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | 4 | Finding | Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness |
| Severity | Medium | Port | ,3389 |
| Target | ,192.168.200.51,192.168.200.52,192.168.200.53 | | |
| Detail | The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP  client makes no effort to validate the identity of the server when  setting up encryption. An attacker with the ability to intercept  traffic from the RDP server can establish encryption with the client  and server without being detected. A MiTM attack of this nature would  allow the attacker to obtain any sensitive information transmitted,  including authentication credentials.  This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack. | | |
| Solution | - Force the use of SSL as a transport layer for this service if supported, or/and  - Select the 'Allow connections only from computers running Remote  Desktop with Network Level Authentication' setting if it is available. | | |
| Remark | http://www.nessus.org/u?8033da0d http://technet.microsoft.com/en-us/library/cc782610.aspx | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | 5 | Finding | Terminal Services Doesn't Use Network Level Authentication (NLA) Only |
| Severity | Medium | Port | ,3389 |
| Target | ,192.168.200.51,192.168.200.52,192.168.200.53 | | |
| Detail | The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication,  NLA also helps protect the remote computer from malicious users and  software by completing user authentication before a full RDP  connection is established. | | |
| Solution | Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows. | | |
| Remark | https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11) http://www.nessus.org/u?e2628096 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | 6 | Finding | SSL Certificate Expiry |
| Severity | Medium | Port | ,443,8443 |
| Target | ,192.168.128.5,192.168.128.6,192.168.128.6 | | |
| Detail | This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired. | | |
| Solution | Purchase or generate a new SSL certificate to replace the existing one. | | |
| Remark |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | 7 | Finding | SSL RC4 Cipher Suites Supported (Bar Mitzvah) |
| Severity | Medium | Port | ,3389 |
| Target | ,192.168.200.51,192.168.200.51,192.168.200.52,192.168.200.52,192.168.200.53,192.168.200.53 | | |
| Detail | The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.  If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext. | | |
| Solution | Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support. | | |
| Remark | https://www.rc4nomore.com/ http://www.nessus.org/u?ac7327a0 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ https://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | 8 | Finding | SSL Certificate with Wrong Hostname |
| Severity | Medium | Port | ,3389,27017 |
| Target | ,192.168.200.51,192.168.200.51,192.168.200.53,192.168.200.53 | | |
| Detail | The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. | | |
| Solution | Purchase or generate a proper SSL certificate for this service. | | |
| Remark |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | 9 | Finding | MongoDB 2.x, 3.0.x < 3.0.15, 3.1.x < 3.2.14, 3.3.x < 3.3.14 Mongo Shell Information Disclosure Vulnerability (SERVER-25335) |
| Severity | Medium | Port | ,27017 |
| Target | ,192.168.200.51,192.168.200.52,192.168.200.53 | | |
| Detail | The version of the remote MongoDB server is 2.x, 3.x < 3.0.15, 3.2.x < 3.2.14, 3.3.x < 3.3.14. It is, therefore, affected by an information disclosure in mongo shell due to the MongoDB client having world-readable permissions on  .dbshell history files. An unauthenticated, local attacker can exploit this by reading these files to disclose  potentially sensitive information.  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| Solution | Upgrade to MongoDB version 3.0.15, 3.2.14, 3.3.14, 3.4 or later. | | |
| Remark | http://www.nessus.org/u?fabe3381 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | 10 | Finding | TLS Version 1.0 Protocol Detection |
| Severity | Medium | Port | ,3389,27017 |
| Target | ,192.168.200.51,192.168.200.51,192.168.200.52,192.168.200.52,192.168.200.53,192.168.200.53 | | |
| Detail | The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.  As of March 31, 2020, Endpoints that aren’t enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.  PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits. | | |
| Solution | Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0. | | |
| Remark | https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | 11 | Finding | mDNS Detection (Remote Network) |
| Severity | Medium | Port | ,5353 |
| Target | ,192.168.128.3,192.168.128.4,192.168.128.5,192.168.128.6,192.168.128.7,192.168.128.8,192.168.200.11,192.168.200.12,192.168.200.2,192.168.200.3,192.168.200.31,192.168.200.32 | | |
| Detail | The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.   This plugin attempts to discover mDNS used by hosts that are not on the network segment on which Nessus resides. | | |
| Solution | Filter incoming traffic to UDP port 5353, if desired. | | |
| Remark |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | 12 | Finding | SMB Signing not required |
| Severity | Medium | Port | ,445 |
| Target | ,192.168.128.250 | | |
| Detail | Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server. | | |
| Solution | Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. | | |
| Remark | http://www.nessus.org/u?df39b8b3 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html http://www.nessus.org/u?a3cac4ea | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | 13 | Finding | SSL Self-Signed Certificate |
| Severity | Medium | Port | ,3389,27017 |
| Target | ,192.168.200.51,192.168.200.51,192.168.200.52,192.168.200.52,192.168.200.53,192.168.200.53 | | |
| Detail | The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. | | |
| Solution | Purchase or generate a proper SSL certificate for this service. | | |
| Remark |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | 14 | Finding | Apache Tomcat Default Files |
| Severity | Medium | Port | ,8080 |
| Target | ,192.168.200.51,192.168.200.52,192.168.200.53 | | |
| Detail | The default error page, default index page, example JSPs and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself. | | |
| Solution | Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to  replace or modify the default error page. | | |
| Remark | http://www.nessus.org/u?4cb3b4dd https://www.owasp.org/index.php/Securing\_tomcat | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | 15 | Finding | Terminal Services Encryption Level is Medium or Low |
| Severity | Medium | Port | ,3389 |
| Target | ,192.168.200.51,192.168.200.52,192.168.200.53 | | |
| Detail | The remote Terminal Services service is not configured to use strong cryptography.   Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes. | | |
| Solution | Change RDP encryption level to one of :   3. High   4. FIPS Compliant | | |
| Remark |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | 16 | Finding | SSL Certificate Cannot Be Trusted |
| Severity | Medium | Port | ,443,8443,3389,27017 |
| Target | ,192.168.128.5,192.168.128.6,192.168.128.6,192.168.200.51,192.168.200.51,192.168.200.52,192.168.200.52,192.168.200.53,192.168.200.53 | | |
| Detail | 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 'notBefore' dates, or after one of the  certificate's 'notAfter' 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 Nessus 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. | | |
| Remark | https://www.itu.int/rec/T-REC-X.509/en https://en.wikipedia.org/wiki/X.509 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | 17 | Finding | SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) |
| Severity | Low | Port | ,443,8443 |
| Target | ,192.168.128.3,192.168.128.3,192.168.128.4,192.168.128.4,192.168.128.5,192.168.128.6,192.168.128.6 | | |
| Detail | The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections. | | |
| Solution | Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater. | | |
| Remark | https://weakdh.org/ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | 18 | Finding | Terminal Services Encryption Level is not FIPS-140 Compliant |
| Severity | Low | Port | ,3389 |
| Target | ,192.168.200.51,192.168.200.52,192.168.200.53 | | |
| Detail | The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant. | | |
| Solution | Change RDP encryption level to :   4. FIPS Compliant | | |
| Remark |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | 19 | Finding | SSH Weak Key Exchange Algorithms Enabled |
| Severity | Low | Port | ,22 |
| Target | ,192.168.128.3,192.168.128.4,192.168.128.5,192.168.128.6,192.168.128.7,192.168.128.8,192.168.200.11,192.168.200.12,192.168.200.2,192.168.200.3,192.168.200.31,192.168.200.32 | | |
| Detail | The remote SSH server is configured to allow key exchange algorithms which are considered weak.  This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:   diffie-hellman-group-exchange-sha1   diffie-hellman-group1-sha1   gss-gex-sha1-\*   gss-group1-sha1-\*   gss-group14-sha1-\*   rsa1024-sha1  Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions. | | |
| Solution | Contact the vendor or consult product documentation to disable the weak algorithms. | | |
| Remark | http://www.nessus.org/u?b02d91cd https://datatracker.ietf.org/doc/html/rfc8732 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ID | 20 | Finding | SSH Server CBC Mode Ciphers Enabled |
| Severity | Low | Port | ,22 |
| Target | ,192.168.128.3,192.168.128.4,192.168.128.5,192.168.128.6,192.168.128.7,192.168.128.8,192.168.200.11,192.168.200.12,192.168.200.2,192.168.200.3,192.168.200.31,192.168.200.32 | | |
| Detail | The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.   Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions. | | |
| Solution | Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption. | | |
| Remark |  | | |