**Vulnerability Assessment Report**

**For**



**LABAI-INFRA**

**April 11, 2022**

**Document Security Level:** Confidential

**Document Version:** 1.0

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Edit Report** | **Editor** |
| 1.0 | April 11, 2022 | Creation | INET Managed Services |

|  |  |  |  |
| --- | --- | --- | --- |
| LABAI-INFRA | | INET Managed Services CO., LTD. | |
| Name |  | **Name** |  |
| Position |  | **Position** |  |
| Tel |  | **Tel** |  |
| Signature |  | **Signature** |  |

**Table of Contents**

[1. Restrictions on disclosure and use of information 4](#_Toc98507702)

[2. Operation Method 5](#_Toc98507703)

[3. Project Scope 6](#_Toc98507704)

[3.1 Infrastructure Vulnerability Assessment 6](#_Toc98507705)

[4. Testing Tools 7](#_Toc98507706)

[5. Infrastructure Vulnerability Assessment 7](#_Toc98507707)

[5.1 Target Information 8](#_Toc98507708)

[5.2 Executive summary 9](#_Toc98507709)

[5.2.1 Summary Vulnerability by Severity 9](#_Toc98507710)

[5.2.2 Vulnerability by Target 9](#_Toc98507711)

[5.3 Infrastructure Vulnerability Detail 10](#_Toc98507712)

[6. Appendix 11](#_Toc98507713)

[6.1 About Nessus 11](#_Toc98507714)

[6.1.1 Nessus vulnerabilities 11](#_Toc98507715)

[6.1.2 Nessus risk score 11](#_Toc98507716)

[6.2 About Burp Suite's web vulnerability scanner 13](#_Toc98507717)

[6.2.1 Burp Suite's web vulnerability scanner risk score 13](#_Toc98507718)

# 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.

# Operation Method

* 1. Posture Review
  2. Information Gathering
  3. Enumeration
  4. Vulnerability Assessment
  5. Analyze & Evaluate Risk Value
  6. Report



Figure 1: Operation Method

# 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 | - | - | - | - | - | - | ✓ |

# Testing Tools

|  |  |
| --- | --- |
| **Tool Name** | **Testing Type** |
| Nmap | Host and Service Discovery |
| Nessus Professional | Infrastructure Vulnerability Assessment |
| Burp Suite's web vulnerability scanner | Web Application Vulnerability Assessment |

# Infrastructure Vulnerability Assessment

**Vulnerability Assessment from Public Access (for public target)**

**Testing date:** <<Date SCAN>>

**Tester IP Address:** <<IP Target>>

Diagram

Description automatically generated

Figure 2: Vulnerability Assessment from Public Access

**Vulnerability Assessment from Private Access (for private or restricted access target)**

**Testing date:** <<Date SCAN>>

**Tester IP Address:** Private IP from VPN access

A picture containing diagram

Description automatically generated

Figure 3: Vulnerability Assessment from Private Access

## **5.1 Target Information**

| **No.** | **Domain / Server Name** | **IP Address** | **OS/Model** | **Port** |
| --- | --- | --- | --- | --- |
| 1 | - | 192.168.2.21 | - | TCP: 22, 80, 427, 443, 902, 1720, 5988, 5989, 8000, 8080, 8100, 8300 |
| 2 | - | 192.168.2.148 | - | TCP: 21, 135, 139, 443, 445, 1720, 3306, 3389, 5432, 8080, 49152, 49153, 49154, 49155 |

## **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**

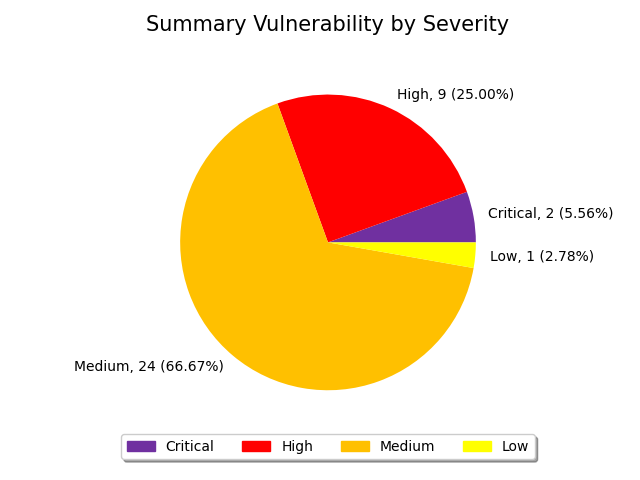


Figure 4: Summary by Severity of Infrastructure Vulnerability Assessment

### **5.2.2 Vulnerability by Target**

| **No.** | **Domain/Server Name** | **IP Address** | **Critical** | **High** | **Medium** | **Low** | **Total** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | - | 192.168.2.21 | 1 | 5 | 6 | 0 | 12 |
| 2 | - | 192.168.2.148 | 1 | 4 | 18 | 1 | 24 |
| **Total** | | | 2 | 9 | 24 | 1 | 36 |

## **5.3 Infrastructure Vulnerability Detail**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 1 | **Finding** | SSL Version 2 and 3 Protocol Detection |
| **Severity** | **Critical** | **Port** | TCP: 443 |
| **Target** | 192.168.2.148(443) | | |
| **Detail** | The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:   - An insecure padding scheme with CBC ciphers.   - Insecure session renegotiation and resumption schemes.  An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.  Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.  NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'. | | |
| **Solution** | Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead. | | |
| **Remark** | https://www.schneier.com/academic/paperfiles/paper-ssl.pdf http://www.nessus.org/u?b06c7e95 http://www.nessus.org/u?247c4540 https://www.openssl.org/~bodo/ssl-poodle.pdf http://www.nessus.org/u?5d15ba70 https://www.imperialviolet.org/2014/10/14/poodle.html https://tools.ietf.org/html/rfc7507 https://tools.ietf.org/html/rfc7568 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 2 | **Finding** | VMware ESX / ESXi Unsupported Version Detection |
| **Severity** | **Critical** | **Port** | TCP: 443 |
| **Target** | 192.168.2.21(443) | | |
| **Detail** | According to its version, the installation of VMware ESX or ESXi on the remote host is no longer supported.  Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. | | |
| **Solution** | Upgrade to a version of VMware ESX / ESXi that is currently supported. | | |
| **Remark** | https://www.vmware.com/support/policies/lifecycle.html https://www.vmware.com/files/pdf/support/Product-Lifecycle-Matrix.pdf | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 3 | **Finding** | SSL Certificate Signed Using Weak Hashing Algorithm |
| **Severity** | **High** | **Port** | TCP: 3389 |
| **Target** | 192.168.2.148(3389) | | |
| **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.** | 4 | **Finding** | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| **Severity** | **High** | **Port** | TCP: 443, 3389 |
| **Target** | 192.168.2.148(443, 3389) | | |
| **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.** | 5 | **Finding** | MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check) |
| **Severity** | **High** | **Port** | TCP: 3389 |
| **Target** | 192.168.2.148(3389) | | |
| **Detail** | The remote Windows host is affected by a remote code execution vulnerability due to improper processing of packets by the Secure Channel (Schannel) security package. An attacker can exploit this issue by sending specially crafted packets to a Windows server.  Note that this plugin sends a client Certificate TLS handshake message followed by a CertificateVerify message. Some Windows hosts will close the connection upon receiving a client certificate for which it did not ask for with a CertificateRequest message. In this case, the plugin cannot proceed to detect the vulnerability as the CertificateVerify message cannot be sent. | | |
| **Solution** | Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2. | | |
| **Remark** | http://www.nessus.org/u?64e97902 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 6 | **Finding** | ESXi 6.0 U1 Build 5251621 / 6.0 U2 Build 5251623 / 6.0 U3 Build 5224934 Multiple Vulnerabilities (VMSA-2017-0006) (remote check) |
| **Severity** | **High** | **Port** | TCP: 0 |
| **Target** | 192.168.2.21(0) | | |
| **Detail** | The version of the remote VMware ESXi 6.0 host is 6.0 U1 prior to build 5251621, 6.0 U2 prior to build 5251623, or 6.0 U3 prior to build 5224934. It is, therefore, affected by multiple vulnerabilities :   - A stack memory initialization flaw exists that allows an  attacker on the guest to execute arbitrary code on the  host. (CVE-2017-4903)   - An unspecified flaw exists in memory initialization that  allows an attacker on the guest to execute arbitrary  code on the host. (CVE-2017-4904)   - An unspecified flaw exists in memory initialization that  allows the disclosure of sensitive information.  (CVE-2017-4905) | | |
| **Solution** | Apply patch ESXi600-201703401-SG, ESXi600-201703002, or ESXi600-201703003 according to the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2017-0006.html http://www.nessus.org/u?29e8975b http://www.nessus.org/u?0ac633b1 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 7 | **Finding** | ESXi 6.0 Build 5485776 Multiple Vulnerabilities (VMSA-2017-0015) (remote check) |
| **Severity** | **High** | **Port** | TCP: 0 |
| **Target** | 192.168.2.21(0) | | |
| **Detail** | The version of the remote VMware ESXi 6.0 host is prior to build 5224529. It is, therefore, affected by multiple vulnerabilities in VMWare Tools and the bundled OpenSSL and Python packages, as well as a NULL pointer dereference vulnerability related to handling RPC requests that could allow an attacker to crash a virtual machine. | | |
| **Solution** | Apply patch ESXi600-201706101-SG according to the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2017-0015.html http://www.nessus.org/u?e03fa029 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 8 | **Finding** | ESXi 5.5 / 6.0 / 6.5 / Multiple Vulnerabilities (VMSA-2017-0021) (VMSA-2018-0002) (Spectre) (remote check) |
| **Severity** | **High** | **Port** | TCP: 443 |
| **Target** | 192.168.2.21(443) | | |
| **Detail** | The remote VMware ESXi host is version 5.5, 6.0, or 6.5 and is missing a security patch. It is, therefore, affected by multiple vulnerabilities that can allow code execution in a virtual machine via the authenticated VNC session as well as cause information disclosure from one virtual machine to another virtual machine on the same host. | | |
| **Solution** | Apply the appropriate patch as referenced in the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2017-0021.html https://www.talosintelligence.com/vulnerability\_reports/TALOS-2017-0369 https://www.vmware.com/us/security/advisories/VMSA-2018-0002.html https://meltdownattack.com/ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 9 | **Finding** | ESXi 6.0 / 6.5 / 6.7 Out-of-Bounds Read Vulnerability (VMSA-2018-0026) (Remote Check) |
| **Severity** | **High** | **Port** | TCP: 443 |
| **Target** | 192.168.2.21(443) | | |
| **Detail** | The remote VMware ESXi host is version 6.0, 6.5, or 6.7 and is missing a security patch. It is, therefore, vulnerable to an out-of-bounds read vulnerability in SVGA devices. An attacker with access to a guest system may be able to execute code on the host system by leveraging this vulnerability. | | |
| **Solution** | Apply the appropriate patch as referenced in the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2018-0026.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 10 | **Finding** | ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2018-0027) (Remote Check) |
| **Severity** | **High** | **Port** | TCP: 443 |
| **Target** | 192.168.2.21(443) | | |
| **Detail** | The remote VMware ESXi host is version 6.0, 6.5, or 6.7 and is missing a security patch. It is, therefore, vulnerable to multiple vulnerabilities. Leveraging the most severe of these vulnerabilities could allow an attacker to execute arbitrary code on the host from the security context of an unprivileged user on the guest system.  Note: CVE-2018-6982 only applies to ESXi 6.5 and 6.7 installations.  ESXi 6.0 installations are not affected. | | |
| **Solution** | Apply the appropriate patch as referenced in the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2018-0027.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 11 | **Finding** | SSL Certificate Expiry |
| **Severity** | **Medium** | **Port** | TCP: 443 |
| **Target** | 192.168.2.148(443) | | |
| **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.** | 12 | **Finding** | Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness |
| **Severity** | **Medium** | **Port** | TCP: 3389 |
| **Target** | 192.168.2.148(3389) | | |
| **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.** | 13 | **Finding** | SSL Certificate Cannot Be Trusted |
| **Severity** | **Medium** | **Port** | TCP: 443, 3389 |
| **Target** | 192.168.2.21(443), 192.168.2.148(443, 3389) | | |
| **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.** | 14 | **Finding** | SSL Self-Signed Certificate |
| **Severity** | **Medium** | **Port** | TCP: 443, 3389 |
| **Target** | 192.168.2.148(443, 3389) | | |
| **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.** | 15 | **Finding** | SMB Signing not required |
| **Severity** | **Medium** | **Port** | TCP: 445 |
| **Target** | 192.168.2.148(445) | | |
| **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.** | 16 | **Finding** | Terminal Services Encryption Level is Medium or Low |
| **Severity** | **Medium** | **Port** | TCP: 3389 |
| **Target** | 192.168.2.148(3389) | | |
| **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.** | 17 | **Finding** | Terminal Services Doesn't Use Network Level Authentication (NLA) Only |
| **Severity** | **Medium** | **Port** | TCP: 3389 |
| **Target** | 192.168.2.148(3389) | | |
| **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.** | 18 | **Finding** | SSL RC4 Cipher Suites Supported (Bar Mitzvah) |
| **Severity** | **Medium** | **Port** | TCP: 443, 3389 |
| **Target** | 192.168.2.148(443, 3389) | | |
| **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.** | 19 | **Finding** | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) |
| **Severity** | **Medium** | **Port** | TCP: 443 |
| **Target** | 192.168.2.148(443) | | |
| **Detail** | The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.  As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.  The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.  This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability. | | |
| **Solution** | Disable SSLv3.  Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled. | | |
| **Remark** | https://www.imperialviolet.org/2014/10/14/poodle.html https://www.openssl.org/~bodo/ssl-poodle.pdf https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 20 | **Finding** | MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) |
| **Severity** | **Medium** | **Port** | TCP: 49155, 51203 |
| **Target** | 192.168.2.148(49155, 51203) | | |
| **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.** | 21 | **Finding** | TLS Version 1.0 Protocol Detection |
| **Severity** | **Medium** | **Port** | TCP: 443, 3389 |
| **Target** | 192.168.2.21(443), 192.168.2.148(443, 3389) | | |
| **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.** | 22 | **Finding** | TLS Version 1.1 Protocol Deprecated |
| **Severity** | **Medium** | **Port** | TCP: 443, 3389 |
| **Target** | 192.168.2.21(443), 192.168.2.148(443, 3389) | | |
| **Detail** | The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1  As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. | | |
| **Solution** | Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. | | |
| **Remark** | https://datatracker.ietf.org/doc/html/rfc8996 http://www.nessus.org/u?c8ae820d | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 23 | **Finding** | ESXi 5.5 / 6.0 / 6.5 / 6.7 Speculative Execution Side Channel Vulnerability (Foreshadow) (VMSA-2018-0020) (remote check) |
| **Severity** | **Medium** | **Port** | TCP: 443 |
| **Target** | 192.168.2.21(443) | | |
| **Detail** | The remote VMware ESXi host is version 5.5, 6.0, 6.5, or 6.7 and is missing a security patch. It is, therefore, vulnerable to a speculative execution side channel attack known as L1 Terminal Fault (L1TF). An attacker who successfully exploited L1TF may be able to read privileged data across trust boundaries. | | |
| **Solution** | Apply the appropriate patch as referenced in the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2018-0020.html https://foreshadowattack.eu/ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 24 | **Finding** | ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0005) (Remote Check) |
| **Severity** | **Medium** | **Port** | TCP: 443 |
| **Target** | 192.168.2.21(443) | | |
| **Detail** | The remote VMware ESXi host is version 6.0, 6.5, or 6.7 and is missing a security patch. It is, therefore, vulnerable to multiple vulnerabilities, including:   - An out-of-bounds read/write vulnerability and a Time-of-check  Time-of-use (TOCTOU) vulnerability in the virtual USB 1.1 UHCI  (Universal Host Controller Interface). Exploitation of these  issues requires an attacker to have access to a virtual machine  with a virtual USB controller present. These issues may allow a  guest to execute code on the host. (CVE-2019-5518, CVE-2019-5519) | | |
| **Solution** | Apply the appropriate patch as referenced in the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2019-0005.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 25 | **Finding** | VMware ESXi 5.5 / 6.0 / 6.5 / 6.7 DoS (VMSA-2018-0018) (remote check) |
| **Severity** | **Medium** | **Port** | TCP: 443 |
| **Target** | 192.168.2.21(443) | | |
| **Detail** | The remote VMware ESXi host is version 5.5, 6.0, 6.5, or 6.7 and is missing a security patch. It is, therefore, vulnerable to a denial of service vulnerability. The vulnerability exists in the RPC handler due to a NULL pointer dereference issue. An authenticated, remote attacker can exploit this issue to cause VMs to stop responding. | | |
| **Solution** | Apply the appropriate patch as referenced in the vendor advisory. | | |
| **Remark** | https://www.vmware.com/security/advisories/VMSA-2018-0018.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 26 | **Finding** | Terminal Services Encryption Level is not FIPS-140 Compliant |
| **Severity** | **Low** | **Port** | TCP: 3389 |
| **Target** | 192.168.2.148(3389) | | |
| **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** | - | | |



# 6 Port Discovery

| **Port** | **Protocol** | **Service** |
| --- | --- | --- |
| 21 | tcp | ftp |
| 22 | tcp | ssh |
| 80 | tcp | http |
| 135 | tcp | msrpc |
| 139 | tcp | netbios-ssn |
| 427 | tcp | svrloc |
| 443 | tcp | https |
| 445 | tcp | microsoft-ds |
| 902 | tcp | iss-realsecure |
| 1720 | tcp | h323q931 |
| 3306 | tcp | mysql |
| 3389 | tcp | ms-wbt-server |
| 5432 | tcp | postgresql |
| 5989 | tcp | wbem-https |
| 8000 | tcp | http-alt |
| 8080 | tcp | http-proxy |
| 8100 | tcp | xprint-server |
| 8300 | tcp | tmi |
| 49152 | tcp | unknown |
| 49153 | tcp | unknown |
| 49154 | tcp | unknown |
| 49155 | tcp | unknown |

# Appendix

## **7.1 About Nessus**

Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. Nessus is trusted by more than 30,000 organizations worldwide as one of the most widely deployed security technologies on the planet - and the gold standard for vulnerability assessment.

Reference: https://www.tenable.com/products/nessus

### **7.1.1 Nessus vulnerabilities**

As information about new vulnerabilities are discovered and released into the public domain, Tenable, Inc. research staff designs programs to enable Nessus to detect them. These programs are named plugins, and are written in the Nessus proprietary scripting language, called Nessus Attack Scripting Language (NASL). Plugins contain vulnerability information, a generic set of remediation actions, and the algorithm to test for the presence of the security issue.

Reference: https://www.tenable.com/plugins

### **7.1.2 Nessus risk score**

There are four risk levels in this document: Critical, High, Medium, and Low. There are methods for determining the risk level. Based on the Common Vulnerability Scoring System (CVSS), a standard for assessing the severity of vulnerabilities in computer systems. Regarded by the NIAC (National Infrastructure Advisory Council), expert assessments are measured in a range of 0 – 10

| **Severity** | **Description** | **Score** |
| --- | --- | --- |
| Critical | Vulnerabilities that score in the critical range usually have most of the following characteristics:   * Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices. * Exploitation is usually straightforward, in the sense that the attacker does not need any special authentication credentials or knowledge about individual victims, and does not need to persuade a target user, for example via social engineering, into performing any special functions.   For critical vulnerabilities, is advised that you patch or upgrade as soon as possible, unless you have other mitigating measures in place. For example, a mitigating factor could be if your installation is not accessible from the Internet. | 9.0 – 10.0 |
| High | Vulnerabilities that score in the high range usually have some of the following characteristics:   * The vulnerability is difficult to exploit. * Exploitation could result in elevated privileges. * Exploitation could result in a significant data loss or downtime. | 7.0 – 8.9 |
| Medium | Vulnerabilities that score in the medium range usually have some of the following characteristics:   * Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. * Denial of service vulnerabilities that are difficult to set up. * Exploits that require an attacker to reside on the same local network as the victim. * Vulnerabilities where exploitation provides only very limited access. * Vulnerabilities that require user privileges for successful exploitation. | 4.0 – 6.9 |
| Low | Vulnerabilities in the low range typically have very little impact on an organization's business. Exploitation of such vulnerabilities usually requires local or physical system access. | 0.1 – 3.9 |

## **7.2 About Burp Suite's web vulnerability scanner**

The web vulnerability scanner behind Burp Suite's popularity has more to it than most. Burp Scanner uses PortSwigger's world-leading research to help its users find a wide range of vulnerabilities in web applications, automatically. Sitting at the core of both Burp Suite Enterprise Edition and Burp Suite Professional, Burp Scanner is the weapon of choice for over 60,000 users across more than 15,000 organizations.

Reference: https://portswigger.net/burp/vulnerability-scanner

### **7.2.1 Burp Suite's web vulnerability scanner risk score**

The level of severity for an issue that was found by a scan. The higher the severity level, the larger the impact is likely to be if an attacker is able to exploit this vulnerability. Note that the severity level is only a rough approximation based on a typical website. You should use your knowledge of the purpose and context of the associated functionality to determine how serious each issue is in your individual case.

Reference: https://portswigger.net/burp/extensibility/enterprise/graphql-api/severity.html

| **Severity** | **Description** |
| --- | --- |
| High | An attacker can **fully** compromise the confidentiality, integrity, or availability, of a target system without specialized access, user interaction or circumstances that are beyond the attacker’s control. Very likely to allow lateral movement and escalation of attack to other systems on the internal network of the vulnerable application. |
| Medium | An attacker can **partially** compromise the confidentiality, integrity, or availability, of a target system. Specialized access, user interaction, or circumstances that are beyond the attacker’s control may be required for an attack to succeed. Very likely to be used in conjunction with other vulnerabilities to escalate an attack. |
| Low | An attacker can **limitedly** compromise the confidentiality, integrity, or availability, of a target system. Specialized access, user interaction, or circumstances that are beyond the attacker’s control is required for an attack to succeed. Needs to be used in conjunction with other vulnerabilities to escalate an attack. |