**Vulnerability Assessment Report   
 For**



**บริษัท ไอเน็ต แมเนจด์ เซอร์วิสเซส จำกัด**

**Date : 18 February 2022**

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

| **Version** | **Date** | **Edit Report** | **Editor** |
| --- | --- | --- | --- |
| 1.0 | 18 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

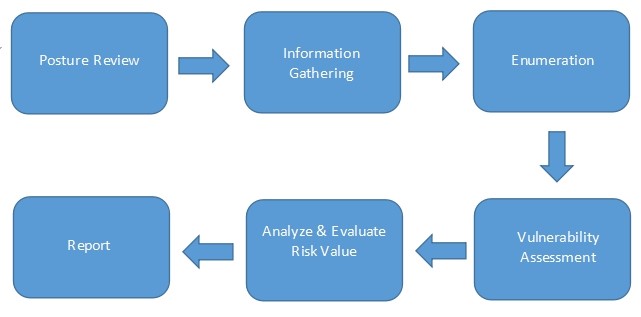


Figure 1: Operation Method

# 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 | 203.150.237.1 | None | None | None | None |
| 2 | None | None | 203.150.237.12 | None | None | None | None |
| 3 | None | None | 203.150.237.2 | None | None | None | None |
| 4 | None | None | 203.150.237.4 | 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 :**

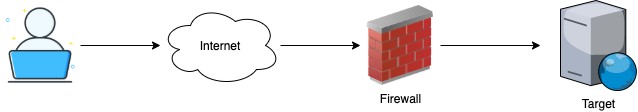


Figure 2: Vulnerability Assessment from Public Access

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

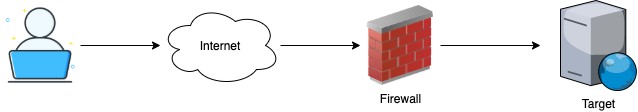


Figure 3: Vulnerability Assessment from Private Access

## 5.1 Target Information

| **No** | **Domain / Server Name** | **IP Address** | **OS/Model** | **Port** |
| --- | --- | --- | --- | --- |
| 1 | None | 203.150.237.1 | None | TCP,80,443 |
| 2 | None | 203.150.237.12 | None | TCP,80,135,139,445,5060 |
| 3 | None | 203.150.237.2 | None | TCP,80,443 |
| 4 | None | 203.150.237.4 | None | TCP,80 |

## 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

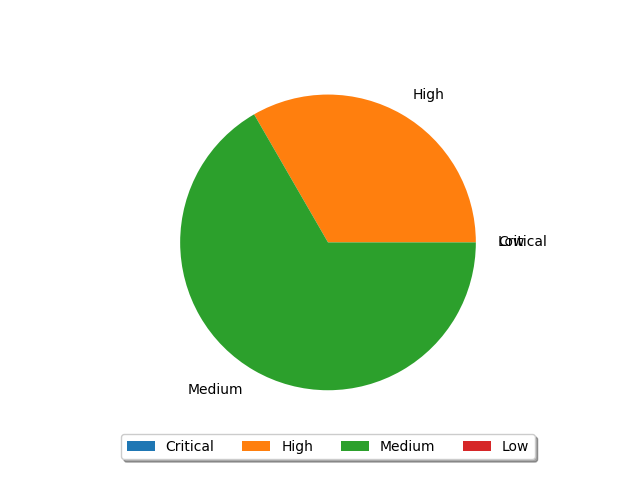


Figure 4: Summary by Severity of Infrastructure Vulnerability Assessment

### 5.2.2 Vulnerability by Target

| **No** | **Domain/Server Name** | **IP Address** | **Critical** | **High** | **Medium** | **Low** | **Total** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | None | 203.150.237.1 | 0 | 1 | 1 | 0 | 2 |
| 2 | None | 203.150.237.12 | 0 | 0 | 2 | 0 | 2 |
| 3 | None | 203.150.237.2 | 0 | 1 | 1 | 0 | 2 |
| **Total** | | | **0** | **2** | **4** | **0** | **6** |

## 5.3 Infrastructure Vulnerability Detail

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 1 | **Finding** | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| **Severity** | **High** | **Port** | TCP 443 |
| **Target** | 203.150.237.1,203.150.237.2 | | |
| **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** | 2 | **Finding** | PRTG Network Monitor < 20.1.57.1745 Information Disclosure (direct check) |
| **Severity** | **Medium** | **Port** | TCP 80 |
| **Target** | 203.150.237.12 | | |
| **Detail** | An information disclosure vulnerability exists in PRTG Network Monitor. An unauthenticated, remote attacker can exploit this, via a crafted HTTP request, to disclose information about probes running or the server itself (CPU usage, memory, Windows version, and internal statistics). | | |
| **Solution** | Upgrade to PRTG Network Monitor 20.1.57.1745 or later | | |
| **Remark** | http://www.nessus.org/u?38e232f8 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | 3 | **Finding** | TLS Version 1.0 Protocol Detection |
| **Severity** | **Medium** | **Port** | TCP 443 |
| **Target** | 203.150.237.1,203.150.237.2 | | |
| **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** | 4 | **Finding** | SMB Signing not required |
| **Severity** | **Medium** | **Port** | TCP 445 |
| **Target** | 203.150.237.12 | | |
| **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 | | |