**Vulnerability Assessment Report**

**For**



**KTC\_nessus.csv**

**May 06, 2022**

**Document Security Level:** Confidential

**Document Version:** 1.0

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Edit Report** | **Editor** |
| 1.0 | May 06, 2022 | Creation | INET Managed Services |

|  |  |  |  |
| --- | --- | --- | --- |
| KTC\_nessus.csv | | 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](#_Toc97820996)

[2. Operation Method 5](#_Toc97820997)

[3. Project Scope 6](#_Toc97820998)

[3.1 Infrastructure Vulnerability Assessment 6](#_Toc97820999)

[3.2 Web Application Vulnerability Assessment 6](#_Toc97821000)

[4. Testing Tools 7](#_Toc97821001)

[5. Infrastructure Vulnerability Assessment 7](#_Toc97821002)

[5.1 Target Information 8](#_Toc97821003)

[5.2 Executive summary 9](#_Toc97821004)

[5.2.1 Summary Vulnerability by Severity 9](#_Toc97821005)

[5.2.2 Vulnerability by Target 9](#_Toc97821006)

[5.3 Infrastructure Vulnerability Detail 10](#_Toc97821007)

[6. Web Application Vulnerability Assessment 11](#_Toc97821008)

[6.1 Target Information 12](#_Toc97821009)

[6.2 Executive summary 13](#_Toc97821010)

[6.2.1 Summary Vulnerability by Severity 13](#_Toc97821011)

[6.2.2 Vulnerability by Target 13](#_Toc97821012)

[6.3 Web Application Vulnerability Detail 14](#_Toc97821013)

[7. Port Discovery 15](#_Toc97821014)

[8. Appendix 16](#_Toc97821015)

[8.1 About Nessus 16](#_Toc97821016)

[8.1.1 Nessus vulnerabilities 16](#_Toc97821017)

[8.1.2 Nessus risk score 16](#_Toc97821018)

[8.2 About Burp Suite's web vulnerability scanner 18](#_Toc97821019)

[8.2.1 Burp Suite's web vulnerability scanner risk score 18](#_Toc97821020)

# 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 | - | - | - | - | - | - | ✓ |

## **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** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | - | 172.31.3.115 | - | TCP : 22, 25, 111, 5405, 8000, 8009, 8080, 65389 |
| 2 | - | 172.31.34.115 | - | TCP : 22, 25, 80, 111, 443, 65389 |
| 3 | - | 203.150.12.7 | - | TCP : 443 |

## **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**

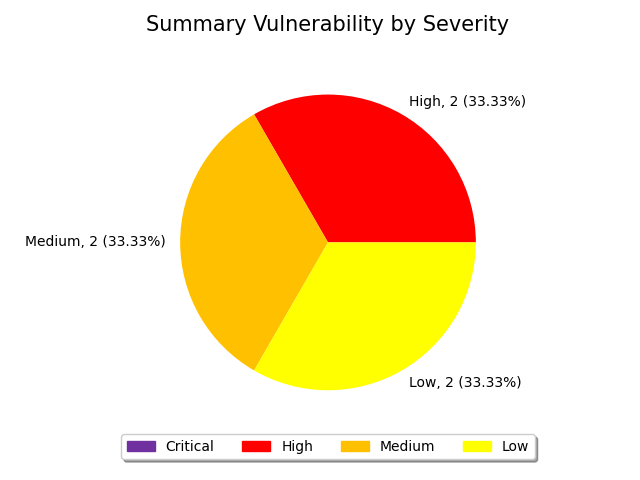


Figure 4: Summary by Severity of Infrastructure Vulnerability Assessment

### **5.2.2 Vulnerability by Target**

| **No.** | **Domain/Server Name** | **IP Address** | **Critical** | **High** | **Medium** | **Low** | **Total** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | - | 172.31.3.115 | 0 | 0 | 1 | 1 | 2 |
| 2 | - | 172.31.34.115 | 0 | 1 | 1 | 1 | 3 |
| 3 | - | 203.150.12.7 | 0 | 1 | 0 | 0 | 1 |
| **Total** | | | 0 | 2 | 2 | 2 | 6 |

## **5.3 Infrastructure Vulnerability Detail**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 1 | **Finding** | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| **Severity** | **High** | **Port** | TCP: 443 |
| **Target** | 172.31.34.115(443), 203.150.12.7(443) | | |
| **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** | mDNS Detection (Remote Network) |
| **Severity** | **Medium** | **Port** |  |
| **Target** | 172.31.3.115(5353), 172.31.34.115(5353) | | |
| **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** | None | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 3 | **Finding** | SSH Weak Key Exchange Algorithms Enabled |
| **Severity** | **Low** | **Port** | TCP: 22 |
| **Target** | 172.31.3.115(22), 172.31.34.115(22) | | |
| **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 | | |



# Web Application Vulnerability Assessment

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

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

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

Diagram

Description automatically generated

Figure 5: Vulnerability Assessment from Public Access

## **6.1 Target Information**

| **No.** | **Domain / Server Name** | **IP Address** | **OS/Model** | **Port** |
| --- | --- | --- | --- | --- |
| 1 | testpaygate.ktc.co.th | 172.31.34.115 | - | TCP : 22, 25, 80, 111, 443, 65389 |

## **6.2 Executive summary**

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

### **6.2.1 Summary Vulnerability by Severity**

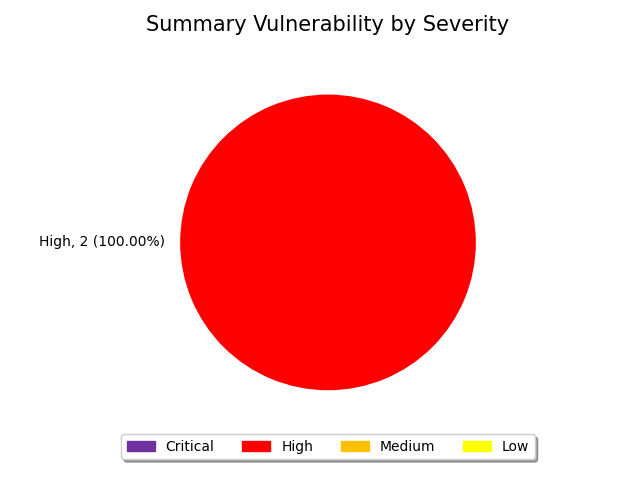


Figure 6: Summary by Severity of Web Application Vulnerability Assessment

### **6.2.2 Vulnerability by Target**

| **No.** | **Domain/Server Name** | **IP Address** | **Critical** | **High** | **Medium** | **Low** | **Total** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | http://testpaygate.ktc.co.th | 172.31.34.115 | 0 | 2 | 0 | 0 | 2 |
| 2 | https://testpaygate.ktc.co.th | 172.31.34.115 | 0 | 0 | 0 | 0 | 0 |
| **Total** | | | 0 | 2 | 0 | 0 | 2 |

## **6.3 Web Application Vulnerability Detail**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 1 | **Finding** | External service interaction (DNS) |
| **Severity** | **High** | **Port** | 80 |
| **Target** | http://testpaygate.ktc.co.th/ | | |
| **Detail** | External service interaction arises when it is possible to induce an application to interact with an arbitrary external service, such as a web or mail server. The ability to trigger arbitrary external service interactions does not constitute a vulnerability in its own right, and in some cases might even be the intended behavior of the application. However, in many cases, it can indicate a vulnerability with serious consequences. In cases where DNS-based interactions can be triggered, it is normally possible to trigger interactions using other service types, and these are reported as separate issues.   If a payload that specifies a particular service type (e.g. a URL) triggers only a DNS-based interaction,   then this strongly indicates that the application attempted to connect using that other service,   but was prevented from doing so by egress filters in place at the network layer. The ability to send requests to other systems can allow the vulnerable server to be used as an attack proxy.  By submitting suitable payloads, an attacker can cause the application server to attack other systems that it can interact with.   This may include public third-party systems, internal systems within the same organization, or services available on the local loopback adapter of the application server itself.   Depending on the network architecture, this may expose highly vulnerable internal services that are not otherwise accessible to external attackers. | | |
| **Solution** | You should review the purpose and intended use of the relevant application functionality,   and determine whether the ability to trigger arbitrary external service interactions is intended behavior.   If so, you should be aware of the types of attacks that can be performed via this behavior and take appropriate measures.   These measures might include blocking network access from the application server to other internal systems, and hardening the application server itself to remove any services available on the local loopback adapter. If the ability to trigger arbitrary external service interactions is not intended behavior, then you should implement a whitelist of permitted services and hosts, and block any interactions that do not appear on this whitelist.  Out-of-Band Application Security Testing (OAST) is highly effective at uncovering high-risk features, to the point where finding the root cause of an interaction can be quite challenging. To find the source of an external service interaction, try to identify whether it is triggered by specific application functionality, or occurs indiscriminately on all requests. If it occurs on all endpoints, a front-end CDN or application firewall may be responsible, or a back-end analytics system parsing server logs. In some cases, interactions may originate from third-party systems; for example, a HTTP request may trigger a poisoned email which passes through a link-scanner on its way to the recipient. | | |
| **Remark** |  | | |



# Port Discovery

| **Port** | **Protocol** | **Service** |
| --- | --- | --- |
| 22 | tcp | ssh |
| 80 | tcp | http |
| 111 | tcp | rpcbind |
| 443 | tcp | https |
| 5405 | tcp | pcduo |
| 8000 | tcp | http-alt |
| 8009 | tcp | ajp13 |
| 8080 | tcp | http-proxy |

# Appendix

## **8.1 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

### **8.1.1 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

### **8.1.2 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 |

## **8.2 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

### **8.2.1 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. |