# Vulnerability Report for OHNO PTE LTD

prepared by
JOSEPH MATTHIAS GOH
OHYES SECURITY INC

on 15/12/2016

# Contents

**1 Executive Summary 3**

**2 Security Assessment Agreement 4**

2.1 Overview . . . . . . . . . . 4

2.2 Vendor Responsibilities . . . . . . . . . . 4

2.3 Client Responsibilities . . . . . . . . . . 4

2.4 Fees . . . . . . . . . . 5

2.5 Waiver of Liability . . . . . . . . . . 5

2.6 Authorization . . . . . . . . . . 6

**3 Methodology 7**

3.1 Tools . . . . . . . . . . 7

3.1.1 NMap . . . . . . . . . . 7

3.1.2 ZenMap . . . . . . . . . . 7

3.1.3 Nessus . . . . . . . . . . 7

3.2 Process . . . . . . . . . . 7

**4 Information Gathering 9**

4.1 Nmap Command . . . . . . . . . . 9

4.2 Machines on Network . . . . . . . . . . 9

4.3 Host Services . . . . . . . . . . 10

4.4 Miscellaneous Information . . . . . . . . . . 11

**5 Vulnerability Scan 12**

5.1 Scan Configuration . . . . . . . . . . 12

5.2 Scan Results . . . . . . . . . . 13

**6 Remediations 14**

6.1 Solution . . . . . . . . . . 14

6.2 Description of Vulnerability . . . . . . . . . . 14

# 1 Executive Summary

OHNO PTE LTD has indicated unusual behaviour on a machine with a Windows 7 Enterprise operating system installed. The machine in question is being used as a local continuous integration (CI) server for their primary product, Nobuty, and is used to run regression tests 24/7.

Due to a new company policy on being able to access their CI server from anywhere in the world, the development team has disabled the default firewall one year ago but have only recently noticed that the machine shuts down at random times of the day, and the technical lead suspects that the machine has been compromised by hackers. The machine has since been isolated together with another machine that acts as a backup. Both machines are on the same network.

OHYES SECURITY INC has been tasked with doing a general scan of OHNO PTE LTD's networks and to provide recommendations on possible courses of action to the management team.

# 2 Security Assessment Agreement

## 2.1 Overview

OHNO PTE LTD has requested OHYES SECURITY INC to perform an Internal Network Vulnerability Assessment for up to 255 local network IP addresses on a single network with the goal of validating suspected vulnerabilities in OHNO PTE LTD's computing infrastructure. Services will be performed on-site in the presence of a project manager assigned by OHNO PTE LTD.

The engagement period was agreed to be between 12th December 2016 to 31st December 2016.

## 2.2 Vendor Responsibilities

- Conduct a scan on the network to confirm the number of computers on the network for up to 255 local network addresses.
- Identify the offending computer identified by Asset Tag No. XCAON-18553231-A running Windows 7 Enterprise and perform a vulnerability scan on it.
- Perform data correation by researching on vulnerabilities, eliminating false positives where possible, investigating the potential impact of the findings, and providing recommended remediations.
- Provide Client with a Machine Vulnerability Assessment Report.

## 2.3 Client Responsibilities

- Identify an on-site project manager to assist in coordinating Client's resource(s).
- Provide OHYES SECURITY INC with access to the business site during Standard Business Hours including buildings, parking, phone systems, internet access, server rooms and workstations.
- Provide OHYES SECURITY INC with access to a suitable conference room facility for mettings, interviews and facilitated sessions during the engagement period.
- Provide physical and wireless access to the offending network
- Provide access to available resources related to the business and technical environment including operating systems, network and any computing environments necessary for OHYES SECURITY INC to complete the Services.

- Review with OHYES SECURITY INC the completed Assessment Report
- Provide sign-off for completed Machine Vulnerability Assessement services.

### 2.4 Fees

OHNO PTE LTD has agreed to pay OHYES SECURITY INC SGD$10,748.38 for the afore-describe service.

### 2.5 Waiver of Liability

- Client understands and acknowledges that where OHYES SECURITY INC has exercised reasonable precautions in delivering the Service, OHYES SECURITY is not responsible for system outages, degradation of performance or other adverse technology environment consequences of tasks Client has authorised OHYES SECURITY INC to perform.
- Client represents and warrant that they have sufficient authroity and the rights necessary for Client to provide and/or facilitiate OHYES SECURITY's access to information, data, networks, systems, and media in connection with these SErvices.
- For all Client requests under this Service Agreement that OHYES SECURITY INC posses, access, or analyze particular media, computers, computer networks, communications networks, or other systems and equipment, to the extent Client provides or facilitates Cisco's access thereto. Client represents, warrants and covenants that they have all necessary right, title, license and autrhoity to make such requests and grant such access, including permissions from third-party owners of licensed or shared resources.
- Any delays in provision of necessary test access, environments, VPN connections, user accounts, administrative access, or other required technical assets may result in delay of deliverables and/or reduction of the scope of work performed.
- Client acknowledges that the completion of Services is dependent upon Client meeting its responsibilities as indicated herein.
- Client will identify Client's personnel and define their roles in the participation of the Services. Such personnel may include but is not limited to: architecture design and planning engineers, and network engineers.
- Client will ensure Clients's personnel are available to participate during the course of the Services to provide information and to participate in the scheduled information gathering sessions, interviews, meetings and conference calls.

- Client expressly understands and agrees that support services provided by OHYES SECURITY INC comprise technical advice, assistance and guidance only.
- Client understands that any IP addresses not utilised during the term of the Service will not result in any credit.
- Client expressly understands and agrees that the Services shall take place and complete within fifty (50) calendar days from issuing a Purchase Order to OHYES SECURITY INC for the Services herin and any unused hours will expire.

### 2.6 Authorization

We, OHNO PTE LTD, authorize OHYES SECURITY INC to conduct a security assessment on our computing infrastructure according to the terms set forth in Section 2.

____________________________________ ____________________________

OHNO PTE LTD Representative Date

____________________________________ ____________________________

OHYES SECURITY INC Representative Date

# 3 Methodology

## 3.1 Tools

The following section specifies tools that will be used.

### 3.1.1 NMap

Nmap[1] is a free and open source utility for network discovery and security auditing.

Nmap uses raw IP packets to determine available hosts on a network, what services those hosts are offering, what operating systems they are running, and what type of firewalls are in place among other functionalities.

### 3.1.2 ZenMap

ZenMap[2] is an open-source cross-platform graphical user interface for Nmap which we use to visualise the network.

### 3.1.3 Nessus

Nessus[3] is a proprietary vulnerability scanner created by Tenable Network Security.

Related Link: https://www.tenable.com/products/nessus-vulnerability-scanner

## 3.2 Process

1. Host Discovery

   We proceed by first scanning the network using Nmap to confirm the number of hosts.

2. Host Isolation

   A port scan will be run to determine likelihood of vulnerabilities. A service scan will also be run to determine the likelihood of a computer having vulnerabilities.

[1] Related Link: `https://nmap.org/`

[2] Related Link: https://nmap.org/zenmap/

[3] Related Link: https://www.tenable.com/products/nessus-vulnerability-scanner

3. Risk Management

   A visulisation of the network topology will be generated to understand other hosts and identify potential risks in performing a vulnerability scan on the network.

4. Vulnerability Scanning

   After identification of the offending host, we use Nessus to run a vulnerability scan on it to determine exact vulnerabilities which we will generate remdiation steps from.

# 4 Information Gathering

## 4.1 Nmap Command

```
nmap -T4 -A -vv -Pn 192.168.108.15
```

Figure 1: Nmap command used for gathering information about the network

## 4.2 Machines on Network

The scan discovered two hosts, 192.168.108.15 and 192.168.108.88, with a large number of open ports on 192.168.108.15 and none on 192.168.108.88.

```
...
Initiating SYN Stealth Scan at 20:40
Scanning 2 hosts [1000 ports/host]
Completed SYN Stealth Scan against 192.168.108.88 in 8.03s (1 host left)
Discovered open port 49157/tcp on 192.168.108.15
Discovered open port 2103/tcp on 192.168.108.15
Increasing send delay for 192.168.108.15 from 0 to 5 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 192.168.108.15 from 5 to 10 due to 11 out of 12 dropped probes since last increase.
Discovered open port 49152/tcp on 192.168.108.15
Discovered open port 5357/tcp on 192.168.108.15
Discovered open port 9/tcp on 192.168.108.15
Discovered open port 10243/tcp on 192.168.108.15
Discovered open port 17/tcp on 192.168.108.15
Discovered open port 13/tcp on 192.168.108.15
Discovered open port 49158/tcp on 192.168.108.15
Discovered open port 19/tcp on 192.168.108.15
Discovered open port 7/tcp on 192.168.108.15
Discovered open port 2869/tcp on 192.168.108.15
Discovered open port 49153/tcp on 192.168.108.15
Discovered open port 49155/tcp on 192.168.108.15
Discovered open port 49154/tcp on 192.168.108.15
Discovered open port 2107/tcp on 192.168.108.15
Discovered open port 2105/tcp on 192.168.108.15
Discovered open port 49156/tcp on 192.168.108.15
Discovered open port 135/tcp on 192.168.108.15
Discovered open port 21/tcp on 192.168.108.15
Discovered open port 554/tcp on 192.168.108.15
Discovered open port 3389/tcp on 192.168.108.15
Discovered open port 139/tcp on 192.168.108.15
Discovered open port 445/tcp on 192.168.108.15
Discovered open port 80/tcp on 192.168.108.15
Completed SYN Stealth Scan at 20:40, 37.51s elapsed (2000 total ports)
...
```

Figure 2: Host Discovery

A network topology graph was generated using Nmap to visualise machines on the network as shown below in Figure 3.

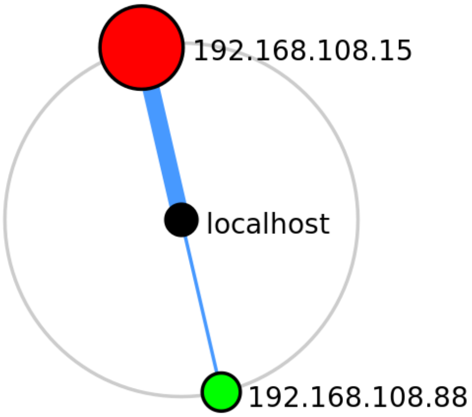


Figure 3: Network graph

## 4.3 Host Services

The service scan on 192.168.108.15 revealed the following host services:

```
...
PORT      STATE SERVICE       VERSION
7/tcp     open  echo
9/tcp     open  discard?
13/tcp    open  daytime       Microsoft Windows USA daytime
17/tcp    open  qotd          Windows qotd (English)
19/tcp    open  chargen
21/tcp    open  ftp           FileZilla ftpd 0.9.30 beta
80/tcp    open  http          Microsoft IIS httpd 7.5
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Windows 7 Enterprise 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2103/tcp  open  msrpc         Microsoft Windows RPC
2105/tcp  open  msrpc         Microsoft Windows RPC
2107/tcp  open  msrpc         Microsoft Windows RPC
2869/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
5357/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  msrpc         Microsoft Windows RPC
49158/tcp open  msrpc         Microsoft Windows RPC
...
```

Figure 4: Port service discovery results

### 4.4 Miscellaneous Information

The machine at 192.168.108.15 was identified with the following information which was in line with data provided by OHNO PTE LTD on the affected machine.

```
MAC Address: 08:00:27:FF:21:6D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::-\
cpe:/o:microsoft:windows_7::sp1\
cpe:/o:microsoft:windows_server_2008::sp1\
cpe:/o:microsoft:windows_8\
cpe:/o:microsoft:windows_8.1\
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows 8, or Windows 8.1 Update 1
Uptime guess: 0.602 days (since Mon Dec 19 06:18:05 2016)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: IE10WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows
```

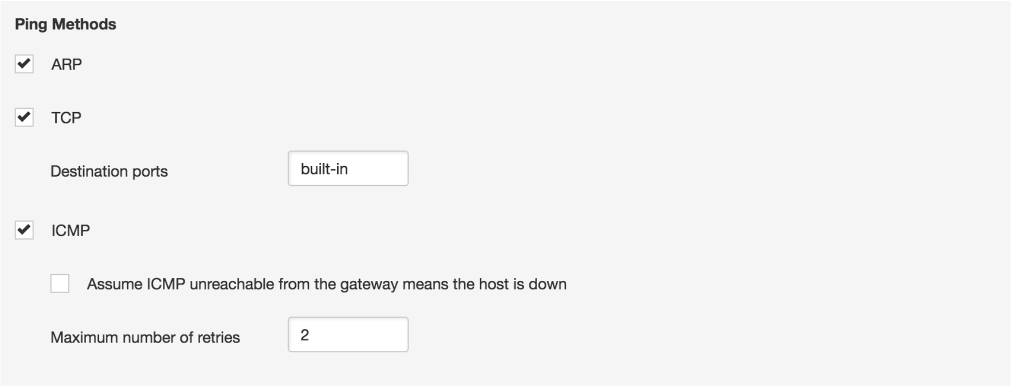
Figure 5: Device details

# 5 Vulnerability Scan

## 5.1 Scan Configuration

A custom policy using all available Plugins and Compliance Checks was used because no information about the underlying network infrastructure has been made known to us.

ARP, TCP and ICMP pings were used.



**Ping Methods**

☑ ARP

☑ TCP

Destination ports: built-in

☑ ICMP

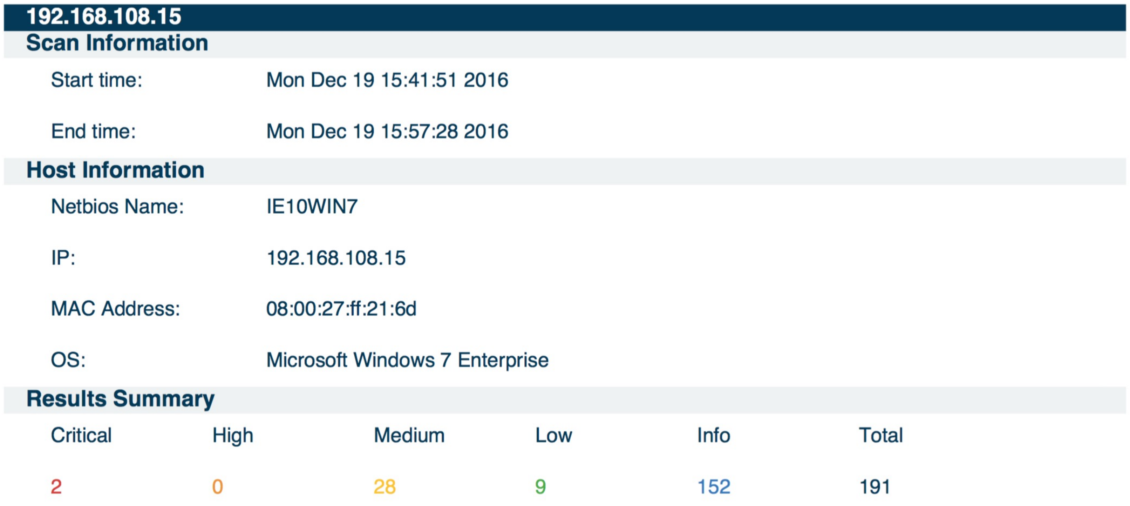
□ Assume ICMP unreachable from the gateway means the host is down

Maximum number of retries: 2

Figure 6: Network graph

## 5.2 Scan Results

The scan on the target as shown in Figure 7 reveals a total of *2* Critical vulnerabilities, *28* Medium level vulnerabilities and *9* Low level vulnerabilitiies. In Remediations on the following pages, we provide recommendations on ameliorating the risk associated with these vulnerabilities.



192.168.108.15

Scan Information

Start time: Mon Dec 19 15:41:51 2016

End time: Mon Dec 19 15:57:28 2016

Host Information

Netbios Name: IE10WIN7

IP: 192.168.108.15

MAC Address: 08:00:27:ff:21:6d

OS: Microsoft Windows 7 Enterprise

Results Summary

| Critical | High | Medium | Low | Info | Total |
|---|---|---|---|---|---|
| 2 | 0 | 28 | 9 | 152 | 191 |

Figure 7: Host Scan Overview

# 6 Remediations

We recommend immediate action to be taken for the following two Critical level vulnerabilities:

1. OpenSSL 1.0.2 ¡ 1.0.2i Multiple Vulnerabilities (SWEET32) on tcp/80
2. OpenSSL 1.0.2 ¡ 1.0.2i Multiple Vulnerabilities (SWEET32) on tcp/443

## 6.1 Solution

This vulnerability can be resolved by upgrading OpenSSL to version 1.0.2i or later, which will fix both vulnerabilities that have been identified.

Note that the GOST ciphersuites vulnerability (VulnDB 144759) is not yet fixed by the vendor in an official release; however, a patch for the issue has been committed to the OpenSSL github repository.

We recommend that this be done as soon as possible to avoid exposing business critical information to potential attackers.

## 6.2 Description of Vulnerability

Critical level of this vulnerability is justified by other vulnerabilities.

More information can be assessed at `https://sweet32.info/`