Vulnerability Report for OHNO PTE. LTD.

prepared by
JOSEPH MATTHIAS GOH
OHYES SECURITY PTE. LTD.

on 15/12/2016

Contents

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 runs 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.

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

2 Service Agreement Overview

2.1 Summary

OHYES SECURITY will perform an Internal Network Vulnerability Assessment for up to 512 private network IP addresses. The goal of this Assessment is to identify and validate 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 has been agreed to be between 12th December 2016 to 16th December 2016.

2.2 Vendor Responsibilities

- Conduct a scan on the network to confirm the number of computers on the network for up to 512 private 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 Customer with a Machine Vulnerability Assessment Report.

2.3 Customer Responsibilities

- Identify an on-site project manager to assist in coordinating Customer's resource(s).
- Provide OHYES SECURITY with access to the business site during Standard Business Hours including buildings, parking, phone systems, internet access, server rooms and workstations.
- Provide OHYES SECURITY 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 to complete the Services.
- Review with OHYES SECURITY the completed Assessment Report
- Provide sign-off for completed Machine Vulnerability Assessement services.

2.4 Waiver of Liability

- Customer understands and acknowledges that where OHYES SECURITY 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 Customer has authorised OHYES SECURITY to perform.
- Customer represent and warrant that they have sufficient authroity and the rights necessary for Customer to provide and/or facilitiate OHYES SECURITY's access to information, data, networks, systems, and media in connection with these SErvices.
- For all Customer requests under this Service Agreement that OHYES SECURITY posses, access, or analyze particular media, computers, computer networks, communications networks, or other systems and equipment, to the extent Customer provides or facilitates Cisco's access thereto. Customer 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.

- Customer acknowledges that the completion of Services is dependent upon Customer meeting its responsibilities as indicated herein.
- Customer will identify Customer'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.
- Customer will ensure Customers'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.
- Customer expressly understands and agrees that support services provided by OHYES SECURITY comprise technical advice, assistance and guidance only.
- Customer understands that any IP addresses not utilised during the term of the Service will not result in any credit.
- Customer 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 for the Services herin and any unused hours will expire.

2.5 Costing

OHNO PTE LTD has agreed to pay OHYES SECURITY SGD $10,000.00 for the afore-describe service.

3 Background Information

3.1 Network

4 Methodology

4.1 Process

1. Network Discovery

   We proceed by doing a scan of all computers on the Local Area Network

2. Host Isolation
3. Vulnerability Scanning

4.2 Tools

4.2.1 NMap

Nmap[1] is a gree 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.

4.2.2 ZenMap

ZenMap[2] is an open-source cross-platform graphical user interface for Nmap and we shall be using it to visualise the network before we begin our vulnerability scans.

4.2.3 Nessus

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

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

5 Information Gathering

5.1 Local Network

OHNO PTE LTD has furnished 4 IP addresses of which the machine of interest is one:

Information gathering was performed using Nmap using the following command:

```
nmap -T4 -A -v 192.168.108.207 192.168.108.161 192.168.108.88 192.168.108.61
```

Figure 1: Hi

```
Nmap scan report for 192.168.108.161
Host is up (0.0015s latency).
Not shown: 968 closed ports
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)
```

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

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

```
19/tcp    open  chargen
21/tcp    open  ftp           FileZilla ftpd 0.9.41 beta
25/tcp    open  smtp          Mercury/32 smtpd (Mail server account Maiser)
| smtp-commands: localhost Hello nmap.scanme.org; ESMTPs are:, TIME, SIZE 0, HELP,
|_ Recognized SMTP commands are: HELO EHLO MAIL RCPT DATA RSET AUTH NOOP QUIT HELP
|_ VRFY SOML Mail server account is 'Maiser'.
79/tcp    open  finger        Mercury/32 fingerd
| finger: Login: Admin         Name: Mail System Administrator
|
|_[No profile information]
80/tcp    open  http          Apache httpd 2.4.23 ((Win32) OpenSSL/1.0.2h PHP/5.5.38)
|_http-favicon: Unknown favicon MD5: 56F7C04657931F2D0B79371B2D6E9820
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.5.38
| http-title: Welcome to XAMPP
|_Requested resource was http://192.168.108.161/dashboard/
106/tcp   open  pop3pw        Mercury/32 poppass service
110/tcp   open  pop3          Mercury/32 pop3d
|_pop3-capabilities: UIDL APOP TOP USER EXPIRE(NEVER)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
143/tcp   open  imap          Mercury/32 imapd 4.62
|_imap-capabilities: AUTH=PLAIN IMAP4rev1 complete X-MERCURY-1A0001 CAPABILITY OK
443/tcp   open  ssl/http      Apache httpd 2.4.23 ((Win32) OpenSSL/1.0.2h PHP/5.5.38)
|_http-favicon: Unknown favicon MD5: 6EB4A43CB64C97F76562AF703893C8FD
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.5.38
| http-title: Welcome to XAMPP
|_Requested resource was https://192.168.108.161/dashboard/
| ssl-cert: Subject: commonName=localhost
| Issuer: commonName=localhost
| Public Key type: rsa
| Public Key bits: 1024.0
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2009-11-10T23:48:47
| Not valid after:  2019-11-08T23:48:47
| MD5:   a0a4 4cc9 9e84 b26f 9e63 9f9e d229 dee0
|_SHA-1: b023 8c54 7a90 5bfa 119c 4e8b acca eacf 3649 1ff6
|_ssl-date: TLS randomness does not represent time
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)
3306/tcp  open  mysql         MariaDB (unauthorized)
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
| ssl-cert: Subject: commonName=IE10Win7
| Issuer: commonName=IE10Win7
| Public Key type: rsa
| Public Key bits: 2048.0
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2016-12-13T07:00:59
```

```
| Not valid after:  2017-06-14T07:00:59
| MD5:   3d72 d74b af57 40d9 5c5d 9cd7 1ea6 fa4b
|_SHA-1: 32d6 aeaa 0431 b352 89b3 8964 69df 23bc 60ec c216
|_ssl-date: 2016-12-16T06:30:45+00:00; +2s from scanner time.
5357/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
10243/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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
MAC Address: 08:00:27:FF:21:6D (Oracle VirtualBox virtual NIC)
Device type: general purpose|media device
Running: Microsoft Windows 2008|10|7|8.1, Microsoft embedded
OS CPE: cpe:/o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_10
  cpe:/h:microsoft:xbox_one cpe:/o:microsoft:windows_7::-
cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_8
cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Server 2008 SP2, Microsoft Windows Server 2008 SP2
or Windows 10 or Xbox One, Microsoft Windows 7 SP0 - SP1,
Windows Server 2008 SP1, Windows 8, or Windows 8.1 Update 1
Uptime guess: 0.585 days (since Thu Dec 15 11:29:58 2016)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class
Service Info: Hosts: localhost, IE10WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows
```

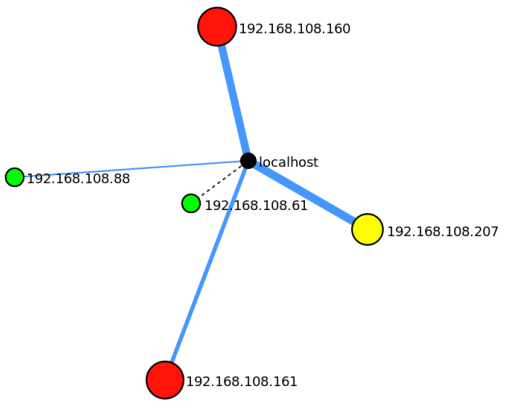

Figure 2: Network graph

6 Vulnerability Scan

7 Recommendations

A Appendix

A.1 Service Agreement