Summary Report

External Internet Vulnerability Assessment

Prepared for

COMPANY X

Date: 30th June 2008

Version: 1.0

Confidentiality

This document is presented in strictest confidence, and shall be treated accordingly.

The recipient of this document acknowledges that all information provided within is confidential, commercially sensitive and agrees not to copy, discuss, or disclose its contents, in whole or in part, by any means without the express written permission of Imerja Limited.

Upon formal written or verbal request by an authorised officer of Imerja Limited this document will be immediately returned to the company.

Communications with Imerja Limited

All enquiries regarding the content of this document should in the first instance be directed to:

Jamie Stallwood
Imerja Limited
Kinetic Centre
Theobald Street
Borehamwood WD6 4PJ

Telephone: 0870 8611 488
Fax: 0870 8611 489
Mobile: 07795 840385
Email: jamie.stallwood@imerja.com

Document Control

Version	Author	Date	Status	Issued to
0.1	JPS	20/6/2008	Draft	Internal
0.2	JPS	22/06/2008	Updated	Internal
0.3	RGS	30/06/2008	QA Review	Internal
1.0	RGS	30/06/2008	ISSUED	COMPANY X

CONTENTS

1 Executive Summary

COMPANY X asked Imerja Limited to perform a vulnerability assessment on its internet-facing network.

The IP address ranges tested were:

217.207.xxx.yyy - 217.207.xxx.yyy

82.109.xx.yyy - 82.109.xx.yyy

This report highlights the most potentially serious issues found and an overall assessment of the external internet security posture.

The tests consisted of the following elements:

- A search of public registries including WHOIS, for networks, DNS entries and named personnel identified with the target organisation. Such information may reveal additional connectivity to the organisation, and provide additional targets for both network-based and social engineering-based malicious activity.
- A detailed network scan and service identification, to enumerate all possible entry points to the customer network and possible areas of focus.
- An automated penetration test against the identified entry points, based on the most recent available vulnerability information.
- Manual connection tests to all relevant discovered ports, to identify any weaknesses, such as weak passwords, mis-implementations, etc. including any follow-on penetration tests.
- Documentation of all findings and recommended remedial or other follow-on actions.

The vulnerability assessment found that the overall external Internet security posture of the IP address range tested to have a ***'Potential to cause major disruption to the organisation***'. The findings are categorised as High Risk, Medium Risk, Low Risk, and Information Only, and are detailed in the body of the report.

2 Scanning Parameters

2.1 Port Scanner

Testing software: NMAP

Scan Parameters: SYN scan for 533 Well-Known TCP Ports[1], OS Identification where possible, randomized host order

2.2 Vulnerability Scanner

Testing Software: NESSUS

Plugins Enabled: 3715 (no UNIX-specific plugins or those which may cause service outage were enabled).

Scanning for: WELL KNOWN SERVICES ONLY

2.3 Target Details

Number of Hosts: 128

Target Subnets:

194.xx.xxx.0/25

[1] Port numbers 7, 9, 13, 19, 21, 22, 23, 37, 42, 43, 53, 67, 69, 80, 88, 110, 111, 113, 115, 137-139, 161, 162, 177, 179, 194, 201-206, 213, 256, 259, 261, 311, 321, 600, 617, 628, 631, 636, 666, 691, 704, 709, 711, 723, 783, 808, 873, 888, 989-990, 992-1000, 1008, 1023-1027, 1029-1033, 1098-1099, 1186, 1188, 1194, 1181, 1124, 1132, 1083-1084, 1112, 1155, 1212, 1214, 1234, 1241, 1337, 1433-1434, 1522-1529, 1600, 1650-1652, 1661-1672, 1680, 1720, 1723, 1755, 1761-1764, 1827, 1900, 1935, 1984, 1986-2028, 2030, 2032-2035, 2038, 2040-2049, 2053, 2064-2065, 2067-2068, 2105-2106, 2108, 2111-2112, 2120-2121, 2201, 2232, 2241, 2301, 2307, 2401, 2430-2433, 2500-2501, 2564, 2600-2605, 2627-2628, 2638, 2766, 2784, 2809, 2903, 2998, 3000-3001, 3005-3006, 3025, 3045, 3049, 3052, 3064, 3086, 3128, 3141, 3264, 3268-3269, 3292, 3299, 3306, 3333, 3372, 3389, 3397-3399, 3421, 3455-3457, 3462, 3531, 3632, 3689, 3900, 3984-3986, 3999-4000, 4002, 4008, 4045, 4125, 4132-4133, 4144, 4224, 4321, 4333, 4343, 4444, 4480, 4500, 4557, 4559, 4660, 4662, 4672, 4899, 4987, 4998, 5000-5003, 5010-5011, 5050, 5060, 5100-5102, 5145, 5190-5193, 5232, 5236, 5300-5305, 5308, 5400, 5405, 5432, 5490, 5510, 5520, 5530, 5540, 5550, 5555, 5560, 5631-5632, 5679-5680, 5713-5717, 5800-5803, 5900-5903, 5977-5979, 5997-6009, 6017, 6050, 6101, 6103, 6105-6106, 6110-6112, 6141-6148, 6346-6347, 6400-6401, 6502, 6543-6544, 6547-6548, 6558, 6588, 6666-6668, 6699, 6881, 6969, 7000-7010, 7070, 7100, 7200-7201, 7273, 7326, 7464, 7597, 7937-7938, 8000, 8007, 8009, 8021, 8076, 8080-8082, 8443, 8888, 8892, 9090, 9100-9107, 9111, 9152, 9535, 9876, 9991-9992, 9999-10000, 10005, 10082-10083, 11371, 12000, 12345-12346, 13701-13702, 13705-13706, 13708-13718, 13720-13722, 13782-13783, 14141, 15126, 15151, 16444, 16959, 17007, 17300, 18000, 18181-18185, 18187, 19150, 20005, 22273, 22289, 22305, 22321, 22370, 26208, 27000-27010, 27374, 27665, 31337, 31416, 32770-32780, 32786-32787, 38037, 38292, 43188, 44334, 44442-44443, 47557, 49400, 50000, 50002, 54320, 61439-61441, 65301

3 Scan Results

3.1 Overall Security Position:

1. Network has very high security and low potential for abuse
2. Network has some minor flaws with local effect only
3. Potential to affect local services with some loss of organisation-wide service

X 4. Potential to cause major disruption to organisation

3.2 Asset Discovery

This section lists only noteworthy items and is not an exhaustive list of all nodes discovered

Firewalls and Security Devices	
Routers and Infrastructure	Catalyst 2950-24, Cisco 2950T-48
Outward-facing Services	Microsoft Exchange
Other Devices	Windows 2003 Domain Controller,
	Windows XP Workstation
	Windows Vista Business Edition
	Netgear WG102 & WG302 Wireless Access Points
	HP Color Inkjet C1700 (Low on Toner)
	HP Business Inkjet 1100, HP Laserjet 2430
	Sophos AV

3.3 Major Issues Found

Risk Severity	Issue
High	http://194.xx.xxx.53/express-setup.htm **Switch does not have a password and can be configured from the Internet**
High	http://194.xx.xxx.94/express-setup.htm **Switch does not have a password and can be configured from the Internet**
High	194.xx.xxx.10 (PAL\CURRICULUMxxx) A large number of Windows ports (88, 3268, 636 etc) are visible on this address. Server's surface area provides a range of potential weaknesses.
High	194.xx.xxx.57:445 194.xx.xxx.100:445 The CIFS (Server) service may be vulnerable to exploits. Apply all service packs.
Medium	194.xx.xxx.85:445 Shared Documents folder is shared to Internet.
Medium	194.xx.xxx.10:53 It is possible to use this nameserver to resolve ANY public host record in DNS. This may lead to excessive bandwidth usage and/or "Bounce" denial-of-service attacks.

Risk Severity	Issue
Medium	194.xx.xxx.70:445 By making an anonymous SMB request, a list of accounts can be obtained. This includes the following: Administrator account name : Administrator (id 500) Guest account name : Guest (id 501) Kerberos account name : krbtgt (id 502) HelpServicesGroup (id 1000) SUPPORT_388945a0 (id 1001) TelnetClients (id 1002) DHCP Users (id 1003) DHCP Administrators (id 1004) CURRICULUM001$ (id 1005) DnsAdmins (id 1106) DnsUpdateProxy (id 1107) Global Students (id 1121) computer31 (id 1136) computer35 (id 1140) computer36 (id 1141) computer37 (id 1142) computer38 (id 1143) computer39 (id 1144) computer40 (id 1145) computer42 (id 1147) computer46 (id 1148) computer47 (id 1149) computer48 (id 1150) computer43 (id 1151) computer44 (id 1152) computer45 (id 1153) computer49 (id 1154) computer15 (id 1156) computer16 (id 1157) computer27 (id 1167) computer52 (id 1168) Tutors (id 1170) Pal staff (id 1173) COMPUTER31$ (id 1175) COMPUTER51$ (id 1176) profiles (id 1179) laptop126 (id 1181) EMLibrary Users (id 1182) WINS Users (id 1184) GHOST_COMPUTER (id 1185) computer50 (id 1188) This SID of this machine is: 1-5-21—1600xyz—1780xyz-1631xyz
Information	194.xx.xxx.10:3389 A Windows Terminal Server was found on this port.

Risk Severity	Issue
Information	194.xx.xxx.9:161 194.xx.xxx.7:161 194.xx.xxx.6:161 194.xx.xxx.49:161 194.xx.xxx.44:161 194.xx.xxx.38:161 194.xx.xxx.37:161 It is possible to read information from these hosts via SNMP community ‘public’.
Infoormation	194.xx.xxx.10:389 Using an anonymous LDAP call it is possible to find the AD domain name as PAL.Local.