



Pan Security International Limited
Vienna House
International Square
Birmingham International Park
Bickenhill Lane
Solihull
B37 7GN
Tel: +44(0)121-780 0646

Pan Security International

Daily Summary Report

Prepared for: Sample Reports

Summary of tests for: 21 January 2004

Product: Adhoc Thorough

Report Date: 21 January 2004 11:37:44

Report ID: 1255

Executive Summary

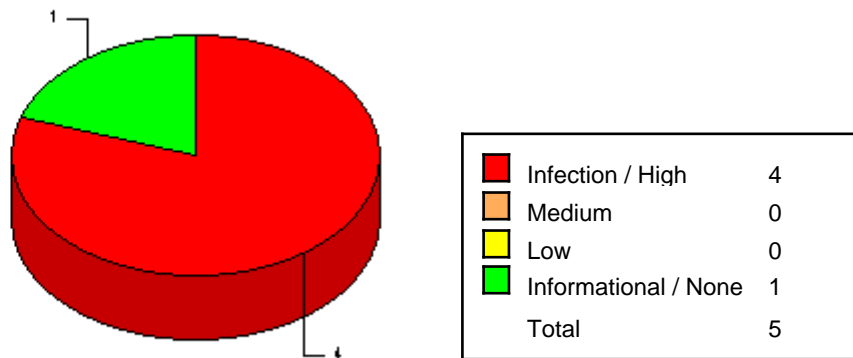
Visibility

5 addresses scanned, 4 found visible.

Address vulnerability ratings

This chart grades the scanned addresses by vulnerability. Each address is categorised in terms of the most severe exposure that is detected on it.

Addresses affected



Changes

No Changes were detected since the last Test.

Exposures

112 Exposures have been detected, of 66 different types, on 4 hosts.
 18 High Risk Exposures of 8 different types were found on 4 hosts.
 38 Medium Risk Exposures of 22 different types were found on 4 hosts.
 39 Low Risk Exposures of 25 different types were found on 4 hosts.
 17 Informational Exposures of 11 different types were found on 4 hosts.

Services

11 different services were detected at 4 different addresses.

Ports

56 different ports have been detected at 4 addresses.



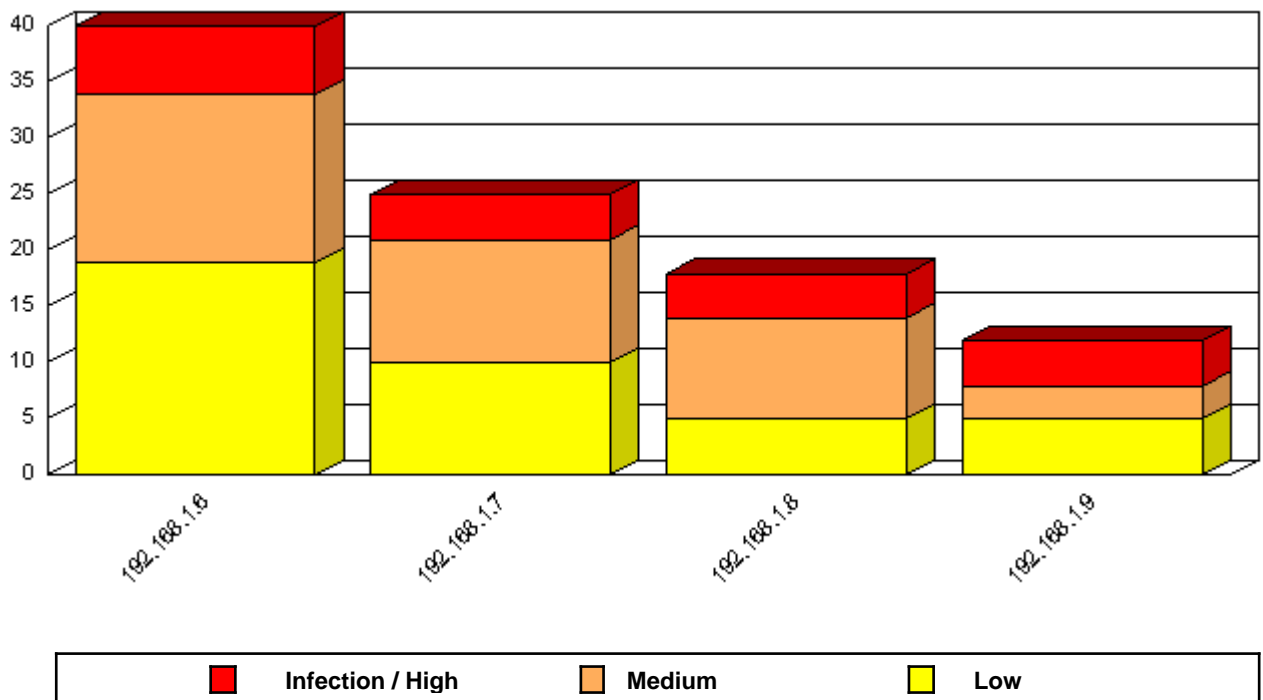
Visibility

5 addresses scanned, 4 found visible.

Note: The symbols in the left margin indicate the presence of Infection/High risk, and Medium exposures. The Exposures column contains counts of exposures detected at each address. Exposures are divided into Infection/High risk (I/H), Medium risk (M), and Low risk (L).

| | Exposures | | | Address | Name | OS | Ping | Ports | |
|---|-----------|----|----|-------------|------|--------------|------|-------|-----|
| | I/H | M | L | | | | | TCP | UDP |
| ◆ | 6 | 15 | 19 | 192.168.1.6 | | Windows 2000 | Yes | 27 | 17 |
| ◆ | 4 | 11 | 10 | 192.168.1.7 | | Linux | Yes | 15 | 9 |
| ◆ | 4 | 9 | 5 | 192.168.1.8 | | Windows 2000 | Yes | 8 | 7 |
| ◆ | 4 | 3 | 5 | 192.168.1.9 | | Windows 2000 | Yes | 7 | 5 |

Exposures per IP Address



Changes

This section summarises changes made at the addresses scanned. It lists Exposures, Ports and Services that have appeared or disappeared compared against a baseline. If no baseline is set the last test for a host is used as a reference.

NOTE: To set new baselines for use in future reports, see the PanSec portal website.

No Changes were detected since the last Test.

Note: The tables below summarise only the number of **changes** (new exposures, new services and new ports, removed exposures, removed services and removed ports) detected on the target hosts since the last time they were tested. See the subsequent sections for information regarding what exposures and/or services were detected on the target host during this test. The symbols in the left margin indicate the appearance of Infection/High or Medium risk exposures. The exposures column contains counts of new or removed exposures since the last test of each address. Exposures are divided into Infection/High risk (I/H), Medium risk (M), Low risk (L) and Informational (Inf.)

No Changes were detected since the last Test.

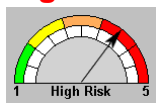
Exposures

This section summarises any exposed vulnerabilities that have been detected

- 112 Exposures have been detected, of 66 different types, on 4 hosts.
- 18 High Risk Exposures of 8 different types were found on 4 hosts.
- 38 Medium Risk Exposures of 22 different types were found on 4 hosts.
- 39 Low Risk Exposures of 25 different types were found on 4 hosts.
- 17 Informational Exposures of 11 different types were found on 4 hosts.

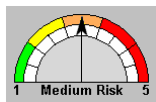
Note: Listed below are all detected exposures.
 Exposures that have appeared are highlighted in bold and with a blue icon.
 For completeness exposures that have disappeared are listed but struck-through and greved.

High Risk



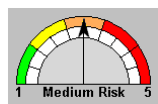
| | | | |
|---|-------------|-------------|-------------|
| Blaster Worm | 192.168.1.6 | 192.168.1.8 | 192.168.1.9 |
| IIS WebDAV Buffer Overflow | 192.168.1.6 | | |
| Microsoft Network Share SMB Request Overflow | 192.168.1.6 | 192.168.1.8 | 192.168.1.9 |
| NetBIOS session service | 192.168.1.6 | 192.168.1.7 | 192.168.1.8 |
| | 192.168.1.9 | | |
| Portmapper service visible | 192.168.1.7 | | |
| SMTP send to programs | 192.168.1.7 | | |
| SNMP Service Exposure | 192.168.1.6 | 192.168.1.7 | |
| Windows RPC Weaknesses | 192.168.1.6 | 192.168.1.8 | 192.168.1.9 |

Medium Risk



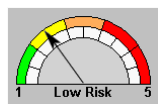
| | | | |
|--|-------------|--|--|
| Anonymous FTP available | 192.168.1.6 | | |
| HTTP Proxy visible | 192.168.1.7 | | |
| IIS Administrative Pages Cross Site Scripting | 192.168.1.6 | | |
| Linux Kernel File Descriptor Resource DoS | 192.168.1.7 | | |
| Microsoft IIS 5.0 Denial of Service | 192.168.1.6 | | |

Medium Risk (Continued)



| | | |
|--|-------------|-------------|
| Microsoft IIS HTR Chunked Encoding Transfer | | |
| 192.168.1.6 | | |
| Microsoft IIS Malformed HTTP HOST Header Field Do | | |
| 192.168.1.6 | | |
| Microsoft IIS WebDAV Denial Of Service | | |
| 192.168.1.6 | | |
| Microsoft SQL Server 2000 Resolution Service | | |
| 192.168.1.6 | 192.168.1.8 | |
| Microsoft SQL Server Buffer Overflow | | |
| 192.168.1.6 | 192.168.1.8 | |
| Multiple IIS Vulnerabilities | | |
| 192.168.1.6 | | |
| NetBIOS name service | | |
| 192.168.1.6 | 192.168.1.7 | 192.168.1.8 |
| 192.168.1.9 | | |
| NetBIOS Shares Visible | | |
| 192.168.1.6 | 192.168.1.7 | 192.168.1.8 |
| 192.168.1.9 | | |
| OpenSSH Authentication Weakness | | |
| 192.168.1.7 | 192.168.1.8 | |
| Samba call_trans2open Buffer Overflow | | |
| 192.168.1.7 | | |
| SMTP open relay | | |
| 192.168.1.7 | | |
| SNMP server insecure community name | | |
| 192.168.1.6 | 192.168.1.7 | |
| SNMP service | | |
| 192.168.1.6 | 192.168.1.7 | |
| Spida Worm | | |
| 192.168.1.6 | 192.168.1.8 | |
| SSH Client Protocol Change Default Warning | | |
| 192.168.1.7 | 192.168.1.8 | |
| Telnet service available | | |
| 192.168.1.8 | | |
| Windows Networking Service Ports Visible | | |
| 192.168.1.6 | 192.168.1.7 | 192.168.1.8 |
| 192.168.1.9 | | |

Low Risk (Continued)



Statd Buffer Overflow

192.168.1.7

TCP Scan Visibility

192.168.1.6

192.168.1.7

192.168.1.8

192.168.1.9

UDP Scan Visibility

192.168.1.6

192.168.1.7

192.168.1.8

192.168.1.9

VNC Service Visible

192.168.1.9

Web server provides version information

192.168.1.6

192.168.1.7

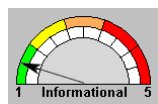
Windows 2000 RPC Service Denial of Service

192.168.1.6

192.168.1.8

192.168.1.9

Informational



HTTP OPTIONS command

192.168.1.6

192.168.1.7

IIS ASP Server-Side Include Buffer Overflow

192.168.1.6

Linux 2.2/2.4 'sysctl' kernel memory read

192.168.1.7

Linux ICMP Kernel Information Leakage

192.168.1.7

Linux kernel 2.2/2.4 ptrace race condition

192.168.1.7

Linux rpc.statd format string vulnerability

192.168.1.7

Microsoft Windows RDP Keystroke Injection

192.168.1.6

Unusual Number of Exposed Ports

192.168.1.6

192.168.1.7

Windows 2000 Insecure Default File Permissions

192.168.1.6

192.168.1.8

192.168.1.9

Windows Encrypted RDP Packet Information

192.168.1.6

Windows Message Subsystem Design Flaw

192.168.1.6

192.168.1.8

192.168.1.9

Services

11 different services have been detected, across 4 different hosts.

Note: Listed below are all detected services.

Services that have appeared are highlighted in bold and with a blue icon.

For completeness services that have disappeared are listed but struck-through and areved.

DNS

192.168.1.6 192.168.1.7

FTP

192.168.1.6

HTTP

192.168.1.6 192.168.1.7

ms-sqlsvr

192.168.1.6 192.168.1.8

NetBIOS

192.168.1.6 192.168.1.7 192.168.1.8 192.168.1.9

POP3

192.168.1.7

Portmapper

192.168.1.7

SMTP

192.168.1.7

SNMP

192.168.1.6 192.168.1.7

SSH

192.168.1.7 192.168.1.8

Telnet

192.168.1.8

Ports

Note: Listed below are all the hosts where a port has been detected. The ports discovered are listed below the host along with this type. The UDP ports listed are either confirmed as open or not confirmed as closed, please see the appropriate engineer's report for full details.

192.168.1.6

TCP 21, 53, 80, 88, 135, 139, 389, 443, 445, 464, 593, 636, 1026, 1029, 1036, 1054, 1056, 1057, 1085, 1086, 1094, 1095, 1433, 3268, 3269, 3372, 3389
UDP 53, 67, 68, 88, 123, 135, 137, 138, 161, 389, 445, 464, 500, 1028, 1037, 1434, 3456

192.168.1.7

TCP 22, 25, 53, 80, 110, 111, 139, 143, 199, 443, 901, 3128, 3306, 6000, 32768
UDP 53, 67, 111, 123, 137, 138, 161, 500, 514

192.168.1.8

TCP 22, 23, 135, 139, 445, 1049, 1057, 1433
UDP 135, 137, 138, 445, 500, 1027, 1434

192.168.1.9

TCP 135, 139, 445, 1048, 3306, 5801, 5901
UDP 137, 138, 445, 500, 1027