



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

Engineer's Test Report

Prepared for: Sample Reports

Node Test for Host: 192.168.1.7

Product Code: Adhoc Thorough (Node Test Thorough)

Test Date: 21 January 2004 10:38:34

Duration: 00:05:14

Report Date: 21 January 2004 11:33:15

Report ID: 1243

Result ID: 38

Executive Summary

This section summarises the Engineer's Test Report for **192.168.1.7** running Linux

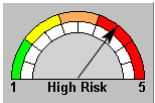
Changes

This node has not been tested previously, therefore no change analysis has taken place.

Exposures

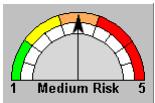
No Infections, 4 High risk, 11 Medium risk, 10 Low risk exposures and 6 Informational items were found.

High Risk Exposures



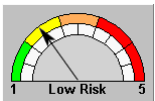
- Exposure:** NetBIOS session service
- Exposure:** Portmapper service visible
- Exposure:** SMTP send to programs
- Exposure:** SNMP Service Exposure

Medium Risk Exposures



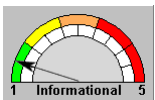
- Exposure:** HTTP Proxy visible
- Exposure:** Linux Kernel File Descriptor Resource DoS
- Exposure:** NetBIOS name service
- Exposure:** NetBIOS Shares Visible
- Exposure:** OpenSSH Authentication Weakness
- Exposure:** Samba call_trans2open Buffer Overflow
- Exposure:** SMTP open relay
- Exposure:** SNMP server insecure community name
- Exposure:** SNMP service
- Exposure:** SSH Client Protocol Change Default Warning
- Exposure:** Windows Networking Service Ports Visible

Low Risk Exposures



- Exposure:** Boot Protocol Server
- Exposure:** Linux Kernel Route Cache Denial Of Service
- Exposure:** Linux SYN Cookie Vulnerability
- Exposure:** Mod_SSL Off-By-One HTAccess Buffer Overflow
- Exposure:** Name server can be abused
- Exposure:** RPC statd Remote Buffer Overflow
- Exposure:** Statd Buffer Overflow
- Exposure:** TCP Scan Visibility
- Exposure:** UDP Scan Visibility
- Exposure:** Web server provides version information

Informational Items



- Exposure:** HTTP OPTIONS command
- Exposure:** Linux 2.2/2.4 'sysctl' kernel memory read
- Exposure:** Linux ICMP Kernel Information Leakage
- Exposure:** Linux kernel 2.2/2.4 ptrace race condition
- Exposure:** Linux rpc.statd format string vulnerability



Technical information

Visibility

This address is visible to the Internet.

Services

The following service(s) were detected or removed:

DNS	HTTP	NetBIOS	POP3	Portmapper	SMTP
SNMP	SSH				

Ports

15 TCP Ports were found to be open, 9 UDP Ports were not confirmed as closed.



Changes

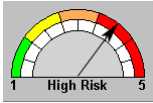
This node has not been tested previously, therefore no change analysis has taken place.

Exposures

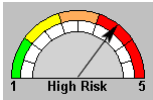
This section details any exposed vulnerabilities that have been detected.

No Infections, 4 High risk, 11 Medium risk, 10 Low risk exposures and 6 Informational items were found.

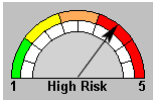
High Risk Exposures



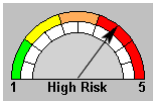
Exposure: NetBIOS session service
Type: Configuration Problem
Description: A Windows Networking NetBIOS service is accessible. This can provide substantial information on user accounts and host services. Release of this data presents a serious security risk.
Advice: Disable this service if not required, or protect with a firewall.
Reference: <http://www.securityfocus.com/bid/2173>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0009>



Exposure: Portmapper service visible
Type: Configuration Problem
Description: The Sun RPC Service, portmapper, is inherently insecure and vulnerable to a packet flood attack. It should not be exposed to the internet.
Advice: Disable this service if not required, or protect with a firewall.
Reference: <http://www.securityfocus.com/bid/1787>



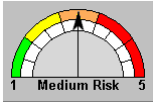
Exposure: SMTP send to programs
Type: Configuration Problem
Description: Your SMTP server appears to allow mail to be sent to or from programs. This allows a remote user to run arbitrary programs and compromise the host.
Advice: Disable this feature in the mailer configuration.
Reference: <http://www.securityfocus.com/bid/1787>



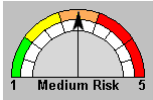
Exposure: SNMP Service Exposure
Type: Remote Access
Data: <PORT:161><PORT:199>
Description: The SNMP service may be visible. This may be vulnerable to a variety of exploits including Denial of Service, Proxy Attacks on other hosts and Remote Control of this host.
Advice: Consult the documentation from CERT and Security Focus
Reference: Disable this service if not required, or protect with a firewall.
<http://www.securityfocus.com/bid/4088>
<http://www.securityfocus.com/bid/4089>
<http://www.cert.org/advisories/CA-2002-03.html>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013>

Medium Risk Exposures

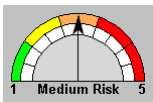
Medium Risk Exposures (continued)



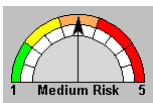
Exposure: HTTP Proxy visible
Type: Unnecessary Service
Data: <PORT:3128>
Description: An HTTP proxy server appears to be running. This could allow external users to masquerade as an internal user and use the proxy's resources against a third party.
Advice: Disable this service if not required, or protect with a firewall.



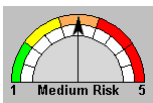
Exposure: Linux Kernel File Descriptor Resource DoS
Type: Denial of Service
Description: Linux is an Open Source operating system.
 It is possible for an attacker to cause a denial of service by exhausting all the available file descriptors.
Advice: Protect the system from malicious users.
Reference: Refer to vendor for more information.
<http://www.securityfocus.com/bid/5178>



Exposure: NetBIOS name service
Type: Configuration Problem
Description: A NetBIOS name server is accessible. This is insecure and provides information on network topology.
Advice: Disable this service if not required, or protect with a firewall.
Reference: <http://www.securityfocus.com/bid/2173>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0009>

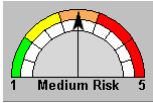


Exposure: NetBIOS Shares Visible
Type: Configuration Problem
Data: <SHARE:\\195.224.123.227\ADMIN\$><SHARE:\\195.224.123.227\IPC\$><SHARE:\\195.224.123.227\print\$>
Description: The Administrative Shares are visible on this host. This presents an attacker with a target for a brute force attempt to access your system.
Advice: Disable Windows Sharing or protect the host with a firewall
Reference: <http://www.securityfocus.com/bid/3330>

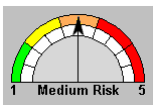


Exposure: OpenSSH Authentication Weakness
Type: Remote Access
Description: A port is open which is usually used by SSH, a secure and encrypted remote access protocol.
 There is a weakness in the challenge-response authentication mechanism of some implementations of OpenSSH which may allow a remote attacker to gain access to the system.
Advice: Upgrade the software to the latest version.
Reference: <http://www.securityfocus.com/bid/5093>
<http://www.cert.org/advisories/CA-2002-18.html>

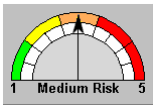
Medium Risk Exposures (continued)



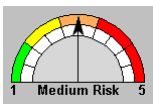
Exposure: Samba call_trans2open Buffer Overflow
Type: Remote Access
Description: Samba is the Unix application used to provide Windows compatible network file and print sharing.
 There is a flaw in versions prior to 2.2.8a that could allow an attacker to run arbitrary programs with elevated privileges.
Advice: Protect the service with a firewall.
 Upgrade to the latest version.
Reference: <http://www.securityfocus.com/bid/7294>



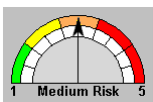
Exposure: SMTP open relay
Type: Configuration Problem
Description: The SMTP server can be used to relay mail to arbitrary third parties. This is known as an open relay and can be used as a staging post for spammers. Ultimately your server may appear on a blacklist and encounter problems delivering mail.
Advice: Disable this feature in the mailer configuration.
Reference: <http://www.securityfocus.com/bid/1787>



Exposure: SNMP server insecure community name
Type: Configuration Problem
Data: <COMMUNITY:public><COMMUNITY:public>
Description: SNMP is accessible from the Internet with an easily guessed community string. This may give away vital information about your network configuration.
Advice: Disable this service if not required, or configure a secure community string and protect with a firewall.
Reference: <http://www.securityfocus.com/bid/1787>

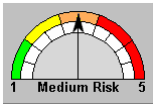


Exposure: SNMP service
Type: Configuration Problem
Description: The SNMP service is accessible from the Internet. There are a number of denial of service exploits which may be run against your host.
Advice: Disable this service if not required or protect with a firewall.
Reference: <http://www.securityfocus.com/bid/1787>



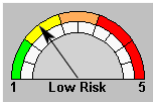
Exposure: SSH Client Protocol Change Default Warning
Type: Remote Access
Description: Secure Shell (SSH) appears to be running on this host.
 OpenSSH and SSH2 are vulnerable to a 'man in the middle' attack through a weakness in server key checking.
Advice: Refer to vendor for further information.
Reference: <http://www.securityfocus.com/bid/5284>

Medium Risk Exposures (continued)

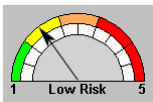


Exposure: Windows Networking Service Ports Visible
Type: Configuration Problem
Description: The Windows Networking ports are visible from the internet. A remote attacker may be able to use this to to gather information or gain access to your system.
Advice: Disable this service if not required, or protect with a firewall.
Reference: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0630>

Low Risk Exposures

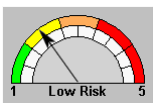


Exposure: Boot Protocol Server
Type: Configuration Problem
Description: A bootp server may be visible. It may be possible to craft a conversation which disrupts traffic to local hosts.
Advice: Disable the service if not required or protect with a firewall.
Reference: <http://www.securityfocus.com/bid/3716>

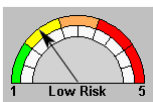


Exposure: Linux Kernel Route Cache Denial Of Service
Type: Denial of Service
Description: The routing table cache for Linux kernels 2.4.1 to 2.4.20 has a flaw which can cause the system to hang. Systems with a large amount of RAM are specially vulnerable.

 It is possible for an attacker to send a specially crafted traffic stream which will cause the Denial of Service.
Advice: Refer to vendor for further advice
Reference: <http://www.securityfocus.com/bid/7601>



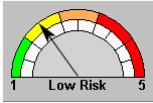
Exposure: Linux SYN Cookie Vulnerability
Type: Backdoor
Description: There is a vulnerability in the Linux Network code where a remote attacker may be able to evade filter rules on the host.
Advice: Upgrade the software to the latest version.
Reference: <http://www.securityfocus.com/bid/3505>



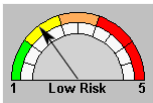
Exposure: Mod_SSL Off-By-One HTAccess Buffer Overflow
Type: Privilege Escalation
Description: Mod_SSL is an Apache module used to facilitate Secure Socket Layer communications.

 An attacker may be able to exploit a buffer overflow by sending a large amount of data to the DATE_LOCALE variable. This could allow the execution of arbitrary code on the system.
Advice: Refer to vendor for further information.
Reference: <http://www.securityfocus.com/bid/5084>

Low Risk Exposures (continued)

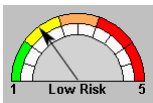


Exposure: Name server can be abused
Type: Configuration Problem
Description: Other sites are able to use your server as a DNS forwarder. This could be misused as part of a larger attack.
Advice: Configure your server to only respond to local addresses.
Reference: <http://www.cert.org/advisories/CA-2001-11.html>



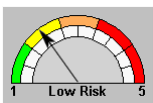
Exposure: RPC statd Remote Buffer Overflow
Type: Remote Access
Description: statd is a server that implements a reboot notification service.

 There is a buffer overflow in RPC statd that may allow a remote attacker to gain root access on the host.
Advice: Disable this service if not required, or protect with a firewall.
Reference: <http://www.securityfocus.com/bid/127>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0018>

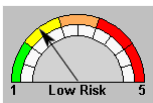


Exposure: Statd Buffer Overflow
Type: Remote Access
Description: statd is a server that implements a reboot notification service.

 There is a vulnerability in the Linux version of statd that may allow a remote attacker to execute arbitrary commands on the host or to cause a Denial of Service against it.
Advice: Upgrade the software to the latest version.
Reference: <http://www.securityfocus.com/bid/1480>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0666>

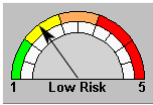


Exposure: TCP Scan Visibility
Type: Configuration Problem
Description: The host is responding to TCP Scans.
Advice: The exposed ports should be checked in order to assess the risk. If necessary, protect the host with policies on the firewall to allow only the required services and apply a default DENY for everything else.
Reference: <http://www.securityfocus.com/bid/3562>



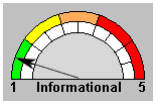
Exposure: UDP Scan Visibility
Type: Configuration Problem
Description: The host is responding to UDP Scans by rejecting probes to closed ports.
Advice: Review the configuration of the firewall and consider blocking ICMP unreachable.
Reference: <http://www.securityfocus.com/bid/3562>

Low Risk Exposures (continued)

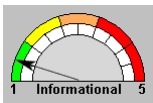


Exposure: Web server provides version information
Type: Configuration Problem
Data: <SERVER:Apache-AdvancedExtranetServer/2.0.47 (Mandrake Linux/1.6.91mdk) mod_perl/1.99_08 Perl/v5.8.0 auth_mysql/1.11 mod_ssl/2.0.47 OpenSSL/0.9.7a><SERVER:squid/2.5.STABLE1-20030121>
Description: The web server advertises its type and version information. Disclosure of version information is not itself a vulnerability, but it helps attackers identify the software behind the service.
Advice: Change the type and version information to something generic.
Reference: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0832>

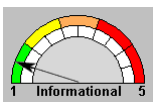
Informational Items



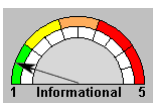
Exposure: HTTP OPTIONS command
Type: Configuration Problem
Description: The Web server supports the OPTIONS command giving remote access to sensitive data. This may reveal information which could be used to compromise the host.
Advice: Configure your web server to disable this command.
Reference: <http://www.securityfocus.com/bid/859>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0219>



Exposure: Linux 2.2/2.4 'sysctl' kernel memory read
Type: Information Gathering
Description: Versions 2.2 and 2.4 of Linux kernel may allow a local attacker to read parts of the Linux kernel memory by passing a negative offset to sysctl().
Advice: Obtain and apply the latest software patches, or upgrade to the latest version.
Reference: <http://www.securityfocus.com/bid/2364>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0316>

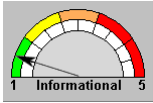


Exposure: Linux ICMP Kernel Information Leakage
Type: Information Gathering
Description: Linux is an Open Source operating system.
 There is a possibility of sensitive data leaking from the kernel in ICMP packets generated by the host. It may be possible for an attacker to steal sensitive data by making repeated requests for ICMP responses.
Advice: Upgrade to the latest version.
Reference: <http://www.securityfocus.com/bid/3950>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0046>

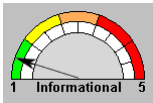


Exposure: Linux kernel 2.2/2.4 ptrace race condition
Type: Remote Access
Description: Race condition in ptrace in Linux kernel 2.2 and 2.4 allows local users to gain privileges by using ptrace to track and modify a running setuid process.
Advice: Obtain and apply the latest software patches or upgrade to the latest version.
Reference: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0317>

Informational Items (continued)



Exposure: Linux rpc.statd format string vulnerability
Type: Remote Access
Description: In Linux distributions, rpc.statd in the nfs-utils package may not properly cleanse untrusted format strings, allowing the remote execution of arbitrary code as root.
Advice: Obtain and apply the latest software patches.
Reference: <http://www.securityfocus.com/bid/1480>
<http://www.cert.org/advisories/CA-2000-17.html>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0666>



Exposure: Unusual Number of Exposed Ports
Type: Configuration Problem
Description: A large number of ports are visible from the internet. This may be a feature of the service provided by this host or it may be a problem with the firewall configuration.
Advice: The exposed ports should be checked in order to assess the risk. If necessary, protect the host with a default DENY Policy on the firewall.
Reference: <http://www.securityfocus.com/bid/1102>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0282>



Visibility

192.168.1.7 is visible to the Internet, and so could be a potential target of malicious attack.

This address was visible because:

It responded to Ping,
It responded to SYN,
It responded to ACK.

OS Detect

This scan determines which operating system is running on 192.168.1.7.

Operating System : Linux 2.3-2.5

Services

Note: Services which have appeared are highlighted in bold and with a blue icon

The following service(s) were detected:

DNS	HTTP	NetBIOS	POP3	Portmapper	SMTP
SNMP	SSH				

TCP Scan

The TCP Scan tests to see if a specific TCP port or a given range of TCP ports is open (i.e. can be connected to) on a target machine. Normal TCP port operation is to return a 'refused' connection when an unrecognised port number is requested by a client.

TCP Scan results:

Open Port Count: 15

Open Ports	Description
22	SSH - SSH Remote Login Protocol
25	SMTP - Simple Mail Transfer
53	DOMAIN - Domain Name Server
80	HTTP - World Wide Web HTTP
110	POP3 - Post Office Protocol - Version 3
111	SUNRPC - SUN Remote Procedure Call
139	NETBIOS-SSN - NETBIOS Session Service
143	IMAP - Internet Message Access Protocol
199	SMUX
443	HTTPS - http protocol over TLS/SSL
901	SMPNAMERES
3128	PROXY - WWW Proxy Port
3306	MYSQL
6000	X11 - X Window System
32768	FILENET-TMS - Filenet TMS



UDP Scan

UDP is used to provide broadcast and datagram services across the Internet. UDP ports are often associated with specific services, some of which are vulnerable to malicious attack.

The UDP Scanner tests to see if specific ports, or given ranges of ports, are accepting information.

UDP Scan results: 9 UDP ports were detected for this host.

Open Port Count: 4

Ports Detected via a Response

53	DOMAIN - Domain Name Server
111	SUNRPC - SUN Remote Procedure Call
123	NTP - Network Time Protocol
161	SNMP

NotClosed Port Count: 5

Ports Detected Through Lack of Response

67	BOOTPS - Bootstrap Protocol Server
137	NETBIOS-NS - NETBIOS Name Service
138	NETBIOS-DGM - NETBIOS Datagram Service
500	ISAKMP
514	SYSLOG - IANA Assigned Service


NOTE: Ports detected through lack of response cannot be positively confirmed as being present, as the lack of response may be due to the ports being firewalled, or to lost or corrupted packets. You may wish to review these ports, to confirm the lack of response is expected and intended.

HTTP Scan

The HTTP Scanner tests a HTTP server for vulnerabilities by checking for the existence of a range of files which, if present, are known to be security risks.

HTTP Scan results:

Port: 80
Server: Apache-AdvancedExtranetServer/2.0.47 (Mandrake Linux/1.6.91mdk) mod_perl/1.99_08 Perl/v5.8.0
auth_mysql/1.11 mod_ssl/2.0.47 OpenSSL/0.9.7a

 OPTION Command Supported.
GET,HEAD,POST,OPTIONS,TRACE
CGI scans matched: 1

Port: 443
Server:
No CGI scans were matched.

Port: 3128
Server: squid/2.5.STABLE1-20030121
No CGI scans were matched.



DNS Scan

DNS servers provide the means to convert a human readable internet address into its equivalent IP address. DNS servers are used invisibly by most browsers and other clients (such as ftp, telnet etc) that access the Internet.

Additionally DNS servers can provide a reverse service i.e. giving a readable host name for an IP address. They also provide facilities for mail forwarding.

The DNS scanner will check for the presence of a DNS server by requesting the target to convert its own name. It will then query for the version number of the Name Server software running on this target. Finally, the scanner will query for name translation of a third party server which is external to the target's domain.

DNS Scan results:

Server: Available
 Version: the chefs special brew
 Third Party Query: Successful
 Protocols: TCP & UDP

POP3 Scan

The component will attempt to connect to a specific POP3 server, and if successful will attempt to ascertain its version. From this it will determine if it is likely to be affected by known security loopholes.

POP3 Scan results:

Port: 110
 Server: +OK POP3 gonzo.bhx.pansec.com v2002.81mdk server ready

SMTP Scan

The SMTP Scan will attempt to connect to a specific mail (SMTP) server, and if successful will initiate various tests designed to probe for security weaknesses.

SMTP Scan results:

Port: 25
 Server: 220 mailhub.pansec.com ESMTP server ready

MAILTOPROGRAMS accepted.
 MAILFROMPROGRAMS accepted.

Share Scan

This scan will attempt to enumerate the netbios shares on the host and then attempt to connect to each share as an anonymous user.

Share Scan results:

Server was Available.

Share	Description
\\195.224.123.227\ADMIN\$	Could not Connect.
♦ \\195.224.123.227\IPC\$	Connected using Anonymous user.
\\195.224.123.227\pdf-generator	Could not Connect.
♦ \\195.224.123.227\print\$	Connected using Anonymous user.



Service Scan

This test attempts to find the netbios services on the host and if successful, a list of services found on the target is displayed.

Service Scan results:

Server was Unavailable

User Scan

This test attempts to find netbios users and groups on the host.

User Scan results:

Server was Available

Group: Domain Admins

Group: Domain Admins(Local)

Group: Domain Users

Group: Domain Users(Local)

Registry Scan

The Registry Scan test determines what information is available from a specified target through the network interface. It attempts to gain read and write access to all of the possible registry root keys, and optionally to a range of specific keys as well. It returns details of the keys found to be readable and writable.

Registry Scan results:

Server was not detected

Name Scan

The Name service uses UDP port 137. If the port is open on a target host then this component will retrieve the Names list from the host.

Name Scan results:

Server was Available.

<i>Name</i>	<i>Type</i>
GONZO	Computer Name,Unique,Registered
MDKGROUP	Domain Name, Group,Registered



SNMP Scan

The SNMP Scan test interrogates a host to see if specified elements are accessible and can be modified.

SNMP Scan results:

Port: 161
Community public

Name: gonzo.bhx.pansec.com
OID: 1.3.6.1.2.1.1.5.0

Name: Linux gonzo.bhx.pansec.com 2.4.21-0.26mdk #1 Sat Nov 29 16:49:06 MST 2003 i686
OID: 1.3.6.1.2.1.1.1.0

PortMapper Service Scan

The PortMapper scanner will attempt to connect to a portmapper service and if successful, will request details of the RPC servers running.

PortMapper Scan results:

Port: 111
Protocol: TCP

<i>Name</i>	<i>Port</i>	<i>Protocol</i>	<i>Version</i>
portmapper	111	TCP	2
status	32768	UDP	1
391002	32769	TCP	2

Port: 111
Protocol: UDP

<i>Name</i>	<i>Port</i>	<i>Protocol</i>	<i>Version</i>
portmapper	111	TCP	2
status	32768	UDP	1
391002	32769	TCP	2

XWindows Scan

The XWindows scanner will attempt to connect to a specific X server, and if successful will test for various security weaknesses. If a test result indicates a potential risk the component will notify its client with an event.

Xwin Scan results:

Port: 6000

An X server is listening on the port at the host, but the server requires users to authenticate.

Msg From Server "No protocol specified"



SSH Detect

The SSH Detection component will attempt to connect to a specific Secure Shell (SSH) server and identify the package being run.

Port 22
Status detected
Banner SSH-1.99-OpenSSH_3.6.1p2
Package OpenSSH
Version 3.6.1p2