Automated Scanning Vulnerability Report
Performed by Beyond Security's Automated Scanning
www.AutomatedScanning.com
Host/s Tested: 192.168.1.6
Report Generated: 19:13:30 28/01/2003

Table of Contents

Introduction	**Open Ports**
Executive Summary	**Security Tests**
Possible Vulnerabilities	**What Next?**

Introduction:

We have scanned your host/s 192.168.1.6 for 983 known security holes.

This scan took place on 19:06:14 28/01/2003 and took 0 hours and 7 minutes to complete.

The '**Possible Vulnerabilities'** section of this report lists security holes found during the scan, sorted by risk level. Note that some of these reported vulnerabilities could be 'false alarms' since the hole is *never* actually exploited during the scan.

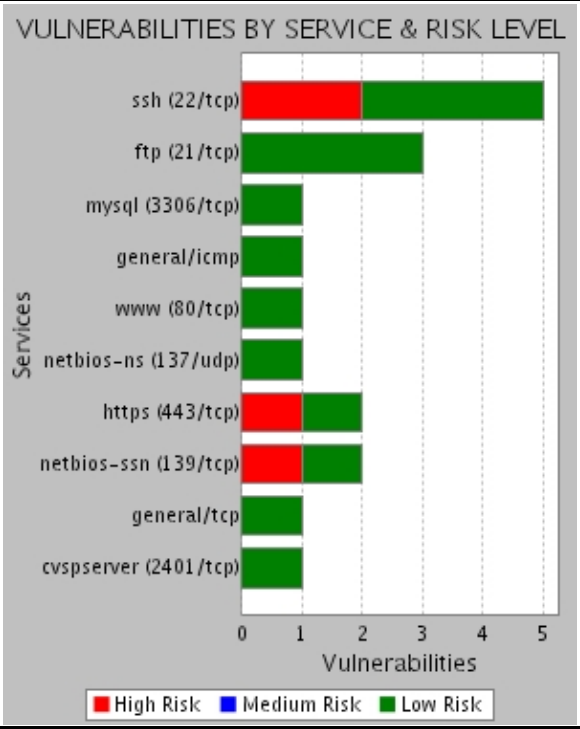
Some of what we found is purely informational; It will not help an attacker to gain access, but it will give him information about the local network or hosts. These results appear in the **'Low Risk / Intelligence Gathering'** section.

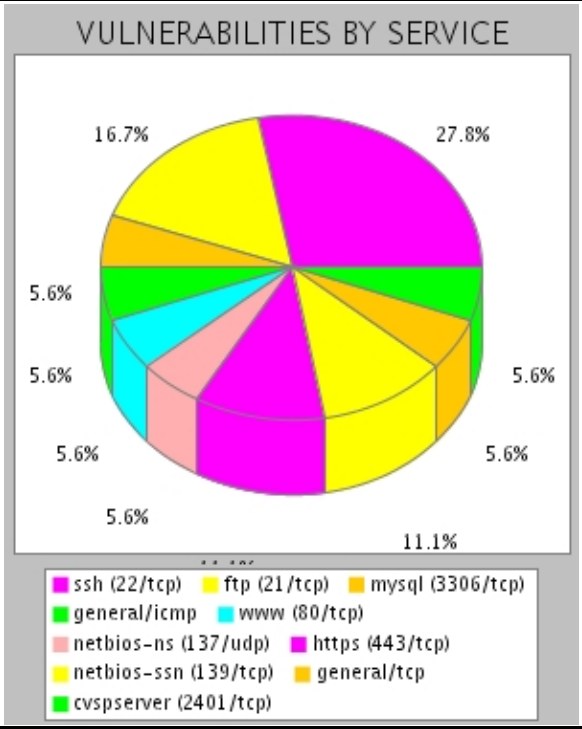
The last section of this report (**'Security Tests'**) lists the security tests that were performed in this scan by category of vulnerability.

Executive Summary:

Vulnerabilities by Service and Risk Level

Service	Total Vulnerabilities	High Risk	Medium Risk	Low Risk
ssh (22/tcp)	5	2	0	3
ftp (21/tcp)	3	0	0	3
mysql (3306/tcp)	1	0	0	1
general/icmp	1	0	0	1
www (80/tcp)	1	0	0	1
netbios−ns (137/udp)	1	0	0	1
https (443/tcp)	2	1	0	1
netbios−ssn (139/tcp)	2	1	0	1
general/tcp	1	0	0	1
cvspserver (2401/tcp)	1	0	0	1





Possible Vulnerabilities:

High	***Medium***	***Low***

Risk Factor: ***High***

A Total of* 4 *High Risk Vulnerability/ies was/were discovered.

1. Shared directory access

No of hosts affected: 1

Hosts affected: 192.168.1.6 (on port: netbios-ssn (139/tcp))

We tried to access the password protected shared directory using several login/password combinations.
It was possible to log into the remote host using a NULL session.
The concept of a NULL session is to provide a null username and
a null password, which grants the user the 'guest' access

To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and
Q246261 (Windows 2000).
Note that this won't completely disable null sessions, but will
prevent them from connecting to IPC$

Impact: Attackers have read/write access to your shares, and can possibly
login to the server remotely.

Possible Solution: Disable 'file and printer' sharing for any network interface that is
visible from the Internet.
To disable anonymous (unauthenticated) access to the Windows machine do the following:

a. Run Registry Editor (Regedt32.exe).

b. Go to the following key in the registry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA
c. On the Edit menu, click Add Value and use the following entry:

Value Name: RestrictAnonymous
Data Type: REG_DWORD
Value: 1

References:
http://support.microsoft.com/support/kb/articles/Q143/4/74.asp (NT 4)
http://support.microsoft.com/support/kb/articles/Q289/6/55.ASP (Win 2k)
http://support.microsoft.com/support/kb/articles/Q132/6/79.ASP (general explanation)

For More Information:
http://www.securiteam.com/windowsntfocus/3E5PUR5QAY.html

2. OpenSSH AFS/Kerberos ticket/token passing

No of hosts affected: 1
Hosts affected: 192.168.1.6 (on port: ssh (22/tcp))

You are running a version of OpenSSH older than OpenSSH 3.2.1

A buffer overflow exists in the daemon if AFS is enabled on
your system, or if the options KerberosTgtPassing or
AFSTokenPassing are enabled. Even in this scenario, the
vulnerability may be avoided by enabling UsePrivilegeSeparation.

Impact: Versions prior to 2.9.9 are vulnerable to a remote root
exploit. Versions prior to 3.2.1 are vulnerable to a local
root exploit.

Possible Solution: Upgrade to the latest version of OpenSSH.

For More Information:
http://www.securiteam.com/unixfocus/5DP0P0K6UO.html

3. OpenSSH < 3.3

No of hosts affected: 1
Hosts affected: 192.168.1.6 (on port: ssh (22/tcp))

You are running a version of OpenSSH which is older than 3.3

There is a flaw in this version that can be exploited remotely.
Version 3.3 is affected only if UsePrivilegeSeparation is disabled.

Details on this flaw have not yet been published.

Impact: Attackers can execute commands as root remotely.

Possible Solution: Upgrade to OpenSSH 3.3, which minimizes the problem due
to privileges separation, then wait for a patched version (probably 3.3.1)

For More Information:
http://www.securiteam.com/securitynews/5HP0L1F7FA.html

4. OpenSSL overflow

No of hosts affected: 2
Hosts affected: 192.168.1.6 (on port: https (443/tcp)), 192.168.1.6 (on port: www (80/tcp))

The remote host is using a version of OpenSSL which is older than 0.9.6e or 0.9.7−beta3

This version is vulnerable to a buffer overflow which allows an attacker to execute code remotely.

Impact: Attackers can execute code on the server.

Possible Solution: Upgrade to version 0.9.6e (0.9.7beta3) or newer.

Risk Factor: ***Low***
A Total of* 14 *Low Risk Vulnerability/ies was/were discovered.

1. A CVS pserver is running

No of hosts affected: 1
Hosts affected: 192.168.1.6 (on port: cvspserver (2401/tcp))

A CVS (Concurrent Versions System) server is installed, and it
is configured to have its own password file, or use that of the
system.

Impact: Attackers can gain critical information about the host.

2. Anonymous FTP enabled

No of hosts affected: 1
Hosts affected: 192.168.1.6 (on port: ftp (21/tcp))

The FTP service allows anonymous logins. If you do not want
to share data with anyone you do not know, then disable the
anonymous account, since it can only give you trouble.

Possible Solution: Under most Unix system, doing:
echo ftp >> /etc/ftpusers will correct this.

Under Windows NT/2000 IIS based FTP:
You need to reach the FTP Service Properties via the normal IIS configuration GUI,
in the ""Service"" tab you should see a checkbox: ""Allow Anonymous Connections"".
Setting it off, will block anonymous connections.

3. FTP Server type and version

No of hosts affected: 1
Hosts affected: 192.168.1.6 (on port: ftp (21/tcp))

An FTP server was detected:
Remote FTP server banner :
220 ready, dude (vsFTPd 1.0.1: beat me, break me)

Impact: When attackers know your FTP daemon version, they can search

for holes specific for that server type.

Possible Solution: Make sure the welcome banner does not include sensitive information such as operating system type, version, etc.

4. HTTP Server type and version

No of hosts affected: 2
Hosts affected: 192.168.1.6 (on port: www (80/tcp)), 192.168.1.6 (on port: https (443/tcp))

This test produced different output for each host tested.

192.168.1.6 (on port: www (80/tcp)):

We were able to detect your web server type and version.
The remote web server type is :

Apache/1.3.27 (Unix) (Red−Hat/Linux) mod_ssl/2.8.12 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26

192.168.1.6 (on port: https (443/tcp)):

We were able to detect your web server type and version.
The remote web server type is :

Apache/1.3.27 (Unix) (Red−Hat/Linux) mod_ssl/2.8.12 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26

Impact: Attackers can gain critical information about the host.

Possible Solution: Configure your server to use an alternate name like:
'Wintendo httpd with Dotmatrix display'. See the URL below for more information.
For apache, add the lines:
ServerSignature Off
ServerTokens Prod
in httpd.conf

For IIS, you can use urlscan to hide the IIS version number.

For More Information:
http://www.securiteam.com/securitynews/5RP0L1540K.html

5. ICMP timestamp request

No of hosts affected: 1

Hosts affected: 192.168.1.6 (on port: general/icmp)

The remote host answers to an ICMP timestamp request. This
allows an attacker to know the time and date on your host.

Impact: This may help attackers to defeat time based authentications
schemes.

Possible Solution: Filter out the icmp timestamp requests (type 13) and replies (type 14).

6. Using NetBIOS to retrieve information from a Windows host

No of hosts affected: 1

Hosts affected: 192.168.1.6 (on port: netbios−ns (137/udp))

We tried to use NETBIOS over TCP/IP to find information about
your computer. The following information was retrieved:
. The following 7 NetBIOS names have been gathered :
STORMTEST = This is the computer name registered for workstation services by a WINS client.
STORMTEST = Computer name that is registered for the messenger service on a computer that is a WINS client.
STORMTEST
__MSBROWSE__
MYGROUP = Workgroup / Domain name
MYGROUP
MYGROUP = Workgroup / Domain name (part of the Browser elections)

. This SMB server seems to be a SAMBA server (this is not a security
risk, this is for your information). This can be told because this server
claims to have a null MAC address

Impact: If NETBIOS is enabled and open to the outside, attackers may
try to reach shared directories and files.
This also gives sensitive information to the attacker such as the
computer name, domain, or workgroup.

Possible Solution: The recommended solution is to block it in your firewall (or even your router, using ACLs). If you have 2 network interfaces, remove the binding for 'disk and printer' sharing from the external network interface.

For your general information, here is how to disable NetBIOS:
http://www.securiteam.com/windowsntfocus/3E5PUR5QAY.html

7. SSH Server type and version

No of hosts affected: 1

Hosts affected: 192.168.1.6 (on port: ssh (22/tcp))

An SSH daemon was detected and the following information was received as the 'welcome' banner:
Remote SSH version : SSH−1.99−OpenSSH_3.1p1
Make sure this doesn't include information about the server's type or version. Change it to something generic like 'welcome'.

8. Services

No of hosts affected: 5

Hosts affected: 192.168.1.6 (on port: ftp (21/tcp)), 192.168.1.6 (on port: https (443/tcp)), 192.168.1.6 (on port: https (443/tcp)), 192.168.1.6 (on port: www (80/tcp)), 192.168.1.6 (on port: ssh (22/tcp))

This test produced different output for each host tested.

192.168.1.6 (on port: ftp (21/tcp)):

The following system service was found:
An FTP server is running on this port.
Here is its banner :
220 ready, dude (vsFTPd 1.0.1: beat me, break me)

192.168.1.6 (on port: https (443/tcp)):

The following system service was found:
A web server is running on this port through SSL

192.168.1.6 (on port: https (443/tcp)):

The following system service was found:
A TLSv1 server answered on this port

192.168.1.6 (on port: www (80/tcp)):

The following system service was found:
A web server is running on this port

192.168.1.6 (on port: ssh (22/tcp)):

The following system service was found:
An ssh server is running on this port

---

9. Nmap

No of hosts affected: 1

Hosts affected: 192.168.1.6 (on port: general/tcp)

Nmap found that this host is running Linux Kernel 2.4.0 − 2.5.20, Linux 2.4.19−pre4 on Alpha

(Note that operating system guessing is not completely accurate,
and is meant to give a picture of what the attacker may see)

Possible Solution: Make sure you applied the latest patches/service pack to your operating system.

For More Information:
If your machine is Windows based, see: http://www.microsoft.com/technet/security/bulletin/fq99−046.asp . Otherwise, download the latest patches for your operating system.

10. MySQL Server version

No of hosts affected: 1
Hosts affected: 192.168.1.6 (on port: mysql (3306/tcp))

We detected a MySQL Server running on this port.
This is what your MySQL server told us about itself:
Remote MySQL version : 3.23.54

Impact: Attackers can gain critical information about the host.

Possible Solution: Change the version number to something generic (like: 0.0.0.0).

11. SMB NativeLanMan

No of hosts affected: 1
Hosts affected: 192.168.1.6 (on port: netbios−ssn (139/tcp))

The remote native lan manager is : Samba 2.2.7
The remote Operating System is : Unix
The remote SMB Domain Name is : MYGROUP

(note: Windows XP will be identified as Windows 2000)

12. SSH protocol versions supported

No of hosts affected: 1
Hosts affected: 192.168.1.6 (on port: ssh (22/tcp))

We tried to detect the SSH versions that are used by the remote
server. This is what we found:
The remote SSH daemon supports the following versions of the
SSH protocol :

. 1.33
. 1.5
. 1.99
. 2.0

13. SSH protocol version 1 enabled

No of hosts affected: 1
Hosts affected: 192.168.1.6 (on port: ssh (22/tcp))

The remote SSH daemon supports connections made
using the version 1.33 and/or 1.5 of the SSH protocol.

These protocols are not completely cryptographically
safe so they should not be used.

Impact: SSH protocol version 1 is weaker than SSH2

Possible Solution: If you use OpenSSH, set the option 'Protocol' to '2' only.
If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'

14. Directory Scanner

No of hosts affected: 2
Hosts affected: 192.168.1.6 (on port: https (443/tcp)), 192.168.1.6 (on port: www (80/tcp))

This test produced different output for each host tested.

192.168.1.6 (on port: https (443/tcp)):

We found some common directories on the web server:
The following directories were discovered:
, /bugzilla, /icons

192.168.1.6 (on port: www (80/tcp)):

We found some common directories on the web server:
The following directories were discovered:
, /bugzilla, /icons

Impact: This is not a security vulnerability, only an information gathering.

Open Ports:

The following ports are open on the host/s:

Host: 192.168.1.6	Open Ports		
	https (443/tcp)	netbios-ssn (139/tcp)	www (80/tcp)
	ssh (22/tcp)	ftp (21/tcp)	netbios-ns (137/udp)
	cvspserver (2401/tcp)	mysql (3306/tcp)	

Security Tests:

The following security checks were performed (checks that appear in the report are highlighted):

Note that not all the tests are relevant (some are platform specific or only make sense when a certain service is running). The irrelevant tests were not performed, but they still appear in the list below.

Backdoors:		
BackOrifice	CA Unicenter's Transport Service is running	INN version check
NetBus 2.x	Microsoft Frontpage 'authors' exploits	Kuang2
VNC detected	shtml.exe reveals full path	bizdb1−search.cgi detected
SMB Registry : Service Pack version	Extent RBS ISP	HTTP dangerous methods
HTTP version detection	PHP−Nuke security vulnerability (bb_smilies.php)	ustorekeeper
anacondaclip	Pi3Web tstisap.dll overflow	Trinity v3
Lion worm	PHP3 Physical Path Disclosure Vulnerability	Novell Web Server NDS Tree Browsing
HealthD detection	Microsoft's SQL TCP/IP listener is running	GirlFriend
Handler	CVSWeb detection	IIS possible DoS using ExAir's advsearch
LCDproc server detection	NetSphere	webgais
VNC HTTP	PC Anywhere detection (TCP)	RemotelyAnywhere SSH detection
RemotelyAnywhere WWW detection	Unauthenticated FTP Access	JRun Sample Files
MPEi/X Default Accounts	alya.cgi	radmin detection
Bugbear worm	Alcatel OmniSwitch 7700/7800 switches backdoor	4553 Parasite Mothership Detect
CGI abuses:		
Web server path climbing	alibaba.pl	tst.bat
bootparamd service	Enumerate Lanman users via SNMP	Campas
Cfinger's search.**@host feature	Daytime	DeepThroat
Echo port open	Finger	FTP Server type and version
netstat	Portal of Doom	database service
Usable remote proxy on any port	X25 service	amd service
automountd service	nfsd service	statd service
statmon service	Mail relaying	An SNMP Agent is running
SSH Server type and version	SSH Insertion Attack	SSH Overflow
Systat	Telnet	Telnet Banner information
Web server traversal	WFTP login check	Cobalt siteUserMod cgi
WebSpeed remote configuration	/cgi−bin directory browsable	LinuxConf grants network access
Shaft Detected	rpm_query CGI	Chargen
/doc directory browsable	FormHandler.cgi	Exchange Malformed MIME header
cgiforum	NetBeans Java IDE	Domain account lockout vulnerability
sadmin service	Napster was detected	Talkd server port and protocol version detection
Passwordless Cayman DSL router	fam service	ASP source viewing using ::$DATA
TalentSoft Web+ Input Validation Bug	windmail.exe CGI	IRIX Objectserver
Piranha's RH6.2 default password	PIX's smtp content filtering	Win2k Service Pack version detection
mstream handler detection	mstream agent detection	Shared directory access
DBMan exposes environment and Setup information (db.cgi)	Cart32 backdoor password	Telnet Client NTLM Authentication Vulnerability
Buffer overrun in O'Reilly Website Pro	The alerter service is running	/doc/packages directory is browsable

NetBIOS Name Server Protocol Spoofing patch	Analogx Web server traversal	NT IP fragment reassembly patch not applied (jolt2)
registry accessible	Guild FTPd allows remote checking for files existence	PDC/BDC detection
ipop2d reads arbitrary files	CVSweb gives remote shell for cvs committers	bb−hostsvc.sh
Apache::ASP security hole	Check for Apache Multiple / vulnerability	Amanda client version
OpenSSH UseLogin option allows remote access with root privileges	YaBB	Simple Web Counter exploitable buffer overflow
thttpd SSI file retrieval	IIS directory listing through WebDAV	Anaconda remote file retrieval
calendar_admin.pl	Sun's Java Web Server Remote Command Execution on Admin Module	Axis Camera Default Password
FreeBSD 4.1.1 Finger	Usable remote name server	Enumerate Lanman services via SNMP
Enumerate Lanman shares via SNMP	Lotus Domino SMTP overflow	Allaire ColdFusion DoS (large password)
Quote of the day	sawmill allows the reading of the first line of any file	BIND vulnerable
Stacheldraht detected	Obtain network interfaces list via SNMP	Serv−U Directory traversal
HSWeb document path	empower cgi path	Oracle XSQL Sample Application Vulnerability
sendtemp.pl	OpenSSH 2.3.1 authentication bypassing vulnerability	Winsock Mutex vulnerability
pagelog.cgi	IIS SHTML Cross Site vulnerability	MySQL buffer overflow
php IMAP overflow	Lotus Domino administration databases	Multiple Vendors FTP Denial of Service
mailnews.cgi	processit	PHP−Nuke's opendir
Bad Registry Value (SFCDisable)	SubSeven	Default community names of the snmp agent
rquotad service	nlockmgr service	DNS AXFR
ASP source viewing using %2e	TFTP get file	Resin directory traversal
ShowCode possible	perlcal	Relative Shell Path
Directory pro web traversal	Test Microsoft IIS Source Fragment Disclosure	BroadVision Physical Path Disclosure Vulnerability
ttawebtop	php safemode	Apache Directory Listing
ICMP netmask request	IMP Session Hijacking Bug	EXPN and VRFY commands
Oracle tnslsnr version query	BEA WebLogic Scripts Server scripts Source Disclosure	ncbook/book.cgi
Default password router Zyxel	Cayman DSL router one char login	SHOUTcast Server DoS detector vulnerability
Mediahouse Statistics Web Server Detection	Sendmail 8.11 local overflow	VisualRoute Web Server Detection
Finger dot at host feature	FTP bounce check	FTPd tells if a user exists
FTP site exec	Linux TFTP get file	etherstatd service
keyserv service	llockmgr service	RPC portmapper
rexd service	rje mapper service	rstatd service
rusersd service	sched service	showfhd service
snmp service	sprayd service	sunlink mapper service
tfsd service	tooltalk service	ypbind service

yppasswd service	ypupdated service	Sendmail DEBUG
Sendmail 'decode' flaw	SMTP Server type and version	view_source
Passwordless Wingate installed	Zope DoS	Relative IP Identification number change
Unprotected SiteScope Service	E−Shopping Cart Arbitrary Command Execution (WebDiscount)	Bypassing web authentication through SQL injection
Finger zero at host feature	Finger redirection check	ICMP timestamp request
Buffer Overrun in ITHouse Mail Server v1.04	JRun's viewsource.jsp	Standard &Poors' ComStock severe security vulnerabilities
NIS server	PC Anywhere	Detect presence of PGPNet server and its version
SMB services enumeration	Malformed RPC Packet DoS vulnerability	SMB Registry : permissions of keys that can change common paths
format string attack against statd	TFN was detected	Jakarta Tomcat path exposure
MacOS X Finder reveals contents of Apache Web files	MacOS X Finder reveals contents of Apache Web directories	phpMyExplorer dir traversal
PHP−Nuke copying files security vulnerability (admin.php)	Power Up Information Disclosure	sglMerchant Information Disclosure Vulnerability
ShopPlus Arbitrary Command Execution	SQLQHit Directory Structure Disclosure	Zope ZClass permission mapping bug
Textor Webmasters CGI Allows Remote Command Execution	Novell Groupwise WebAcc Information Disclosure	WFTP RNTO DoS
Raptor FW version 6.5 detection	Textor Webmasters CGI Allows Remote Command Execution	Nimda Worm infected HTML files
CGIEmail's CGICso (Send CSO via CGI) Command Execution Vulnerability	CGIEmail's Cross Site Scripting Vulnerability (cgicso)	ht://Dig's htsearch potential exposure/dos
PCCS−Mysql User/Password Exposure	Outlook Web anonymous access	ColdFusion Debug Mode
IBM−HTTP−Server View Code	msmmask.exe	Lotus Notes ?OpenServer Information Disclosure
Allaire JRun directory browsing vulnerability	PHP−Nuke Gallery Add−on File View	Redhat Stronghold File System Disclosure
Jakarta Tomcat Path Disclosure	Alchemy Eye HTTP Command Execution	PIX Firewall Manager Directory Traversal
Interactive Story Directory Traversal Vulnerability	SilverStream database structure	Agora CGI Cross Site Scripting
FAQManager Arbitrary File Reading Vulnerability	FastCGI Echo.exe Cross Site Scripting	PHP.EXE / Apache Win32 Arbitrary File Reading Vulnerability
PHP Rocket Add−in File Traversal	zml.cgi Directory Traversal	ASP.NET Cross Site Scripting
ASP.NET path disclosure	mrtg.cgi	SilverStream directory listing
Oracle XSQLServlet XSQLConfig.xml File	Oracle 9iAS Dynamic Monitoring Services	Oracle 9iAS DAD Admin interface
Oracle 9iAS Globals.jsa access	Oracle 9iAS Java Process Manager	Oracle 9iAS Jsp Source File Reading
Oracle 9iAS mod_plsql directory traversal	Oracle 9iAS mod_plsql cross site scripting	DCP−Portal Root Path Disclosure
Website Pro Path Disclosure	php POST file uploads	AdMentor Login Flaw
Avenger's News System Command Execution	BadBlue Directory Traversal Vulnerability	GroupWise Web Interface 'HTMLVER' hole
GroupWise Web Interface 'HELP' hole	SQL Injection Test for MS Access	mod_ssl overflow
WEB−INF folder accessible	Snitz Forums SQL Injection Vulnerability	Sambar Content Viewing Vulnerability
csSearch.cgi	CVS/Entries	IIS .HTR ISAPI filter applied

Apache Remote Command Execution via .bat files	BEA WebLogic Scripts Server scripts Source Disclosure (2)	Apache mod_python vulnerability
Aeromail Web based Mail Detection	ASP.NET Session Information Leakage	Back Office Web Administration Authentication Bypass
BayStack Instant Internet Detection	Citrix Nfuse Directory Traversal with boilerplate.asp	Demarc PureSecure Allows Users to Bypass Login Restrictions
EMU Webmail Allows Reading of Arbitrary Files and View Directories	FileSeek Arbitrary File Viewing	FileSeek Command Execution Vulnerability
Greymatter Detection	Greymatter Remote Login/Pass Exposure	HTTP Server Directory Traversal
PHPImageView XSS Vulnerability	SWS Administrative Access Vulnerability	vqServer Default Administrative Password
vqServer Respond.pl Cross Site Scripting	PHPImageView Disclosure Vulnerability	Authentication bypassing in Lotus Domino
JServ Cross Site Scripting	IIS 5.0 Form_JScript.asp vulnerable to cross−site scripting	IIS 5.0 Sample App reveals physical path of web root
Microsoft IIS 5.0 CodeBrws.asp Source Disclosure	ServletExec 4.1 ISAPI File Reading	ServletExec 4.1 ISAPI Physical Path Disclosure
ping.asp	IIS Global.asa Retrieval	IIS ASP.NET Application Trace Enabled
MRTG mrtg.cgi File Disclosure	ActiveState's Perl allows execution of arbitrary commands	Directory.php Arbitrary Code Execution
Lotus Domino Banner Information Disclosure	MS Site Server Information Leak	NetCommerce SQL injection
WebSphere Cross Site Scripting	PHP4 Physical Path Disclosure	AlienForm CGI script
Malicious PHP Source Injection in phpBB	MetaCart eCommerce Systems Database Exposure	PHP source injection in osCommerce
PHP Source Injection in PHP−Address	SalesCart Database Storage Insecurity	mod_ssl off by one
Apache Tomcat DOS Device Name XSS	Apache Tomcat /servlet Cross Site Scripting	Apache Tomcat TroubleShooter Servlet Installed
iPlanet Search Engine File Viewing	Resin DOS device path disclosure	php 4.2.x malformed POST
BadBlue invalid null byte vulnerability	SunSolve CD CGI user input validation	PGPMail.pl detection
ASP source using %20 trick	Basilix webmail dummy request vulnerability	readmsg.php detection
OfficeScan configuration file disclosure	Snapstream PVS web directory traversal	Apache 2.0.39 non−UNIX directory traversal
ibillpm.pl	PHPAdsNew code injection	Arbitrary Code Execution Problem in Achievo
Awol code injection	Directory Manager's edit_image.php	NetTools command execution
viralator	webcart.cgi	gallery code injection
phpMyAdmin arbitrary files reading	phpPgAdmin arbitrary files reading	vBulletin's Calender Command Execution Vulnerability
wpoison	Microsoft IIS IDC Extension Cross Site Scripting Vulnerability	MidiCart Shopping Cart Software Database Vulnerability
MondoSearch Show Source of Arbitrary Files	phpGB MySQL Injection Vulnerability	XSS Vulnerability in Mojo Mail Sign−Up Form
XSS Vulnerability in MyMarket	XSS Vulnerability in paFileDB	Multiple Vulnerabilities in mailreader.com
PHP Allows Bypassing of safe_mode And Injecting ASCII Control Chars With mail()	KF Web Server /%00 bug	vpasswd.cgi
Tomcat 4.x JSP Source Exposure	DB4Web directory traversal	DB4Web TCP Connects to Arbitrary IP and Port

overflow.cgi detection		
Cisco:		
Cisco 675 passwordless router	Cisco IOS HTTP Configuration Arbitrary Administrative Access	Cisco Catalyst Web Execution
Cisco password not set	Cisco IOS predictable Initial Sequence Numbers (TCP)	IOS Reload after Scanning
Cisco Catalyst Memory Leak	Cisco IOS PPTP Vulnerability	Catalyst 5000 Packet Forwarding
Cisco 6400 Access Concentrator Passwordless Router	Cisco IOS NTP Daemon DoS	Cisco Express Forwarding Leaks Packet Information
Cisco IOS Address Resolution Protocol DoS	Cisco IOS Firewall Feature Bypassing	Cisco CatOS Telnet Buffer Vulnerability
Malformed SNMP Message−Handling Vulnerabilities for Cisco Non−IOS Products	ATA−186 password circumvention / recovery	GSR ACL pub
GSR ICMP unreachable	Cisco Multiple SSH Vulnerabilities	CSCdi34061
IOS TFTP long filename		
Communication devices:		
3Com Superstack II switch with default password		
Denial of Service:		
webdist.cgi	wu−ftpd buffer overflow	wu−ftpd SITE NEWER vulnerability
cgitest.exe buffer overrun	htimage.exe overflow	IIS phonebook
bftpd chown overflow	Sambar Server search CGI vulnerability	wwwwais
FTP PASV denial of service	ftp 'glob' overflow	yppasswdd overflow
POST buffer overflow	CERN httpd problem	Communigate Pro overflow
CSM Mail server MTA 'HELO' denial	proftpd mkdir buffer overflow	TFS SMTP 3.2 MAIL FROM overflow
thttpd 2.04 buffer overflow	WFTPD multiple DoS	XTramil MTA 'HELO' denial
Xtramail pop3 overflow	DoSable squid proxy server	VirusWall catinfo overflow
qpopper buffer overflow	w3−msql overflow	Oracle WebCache Server DoS
AnalogX SimpleServer:WWW DoS	IIS FrontPage ISAPI Denial of Service	BIND9 DoS
AppSocket DoS	Pi3Web Webserver v2.0 Buffer Overflow	Sambar web server DOS
Firewalls:		
Faxsurvey	FTP empty username/password	Proxy accepts POST requests
rexecd	formmail.pl	Unify eWave ServletExec upload vulnerability
Check Point SecuRemote detection	webdriver	Netscape Server ?PageServices bug
mmstdod cgi	Check Point Firewall−1 Web Authentication	Apache /server−status accessible
Netscape Messaging Server User List		
FTP:		
Windows NT ftp 'guest' account	pfdispaly	uw−imap buffer overflow
Tektronix /ncl_items.html	/iisadmin is world readable	Netscape publishingXpert 2 PSUser
rsh on finger output	Poll It CGI exposes local files	proftpd 1.2.0preN check
Service Control Manager Named Pipe Impersonation	eXtropia Web Store remote file retrieval	KW whois
bftpd format string vulnerability	ht://Dig's htsearch reveals web server path	Anonymous FTP enabled
Novell webserver default files	IIS .cnf file leakage	ftp writeable directories
Apache /server−info accessible	FTP CWD ~root	Writeable FTP root

imagemap.exe	ProFTPd pre6 buffer overflow	WebSite 1.0 buffer overflow
wu−ftpd SITE EXEC vulnerability	DCShop exposes sensitive files	FTPD glob Heap Corruption
Multiple WarFTPd DoS	EFTP File existence leakage	Microsoft FTP Server DoS (STAT)
Passwordless Zaurus FTP server	EFTP installation directory disclosure	WS_FTP SITE CPWD Buffer Overflow
Generic FTP traversal	Windows Administrator NULL FTP password	vxworks ftpd buffer overflow
Gain a shell remotely:		
POP3 Server type and version	SWAT detected	Pocsag default password
Webserver file request parsing	TalentSoft Web+ version detection	Arbitrary file disclosure through PHP file upload
IIS viewcode.asp	iPlanet Directory Server traversal	store.cgi
AFS client version	IIS Remote Command Execution	AppleShare IP Server status query
McAfee myCIO Directory Traversal	DCE Services Enumeration	PHProjekt security vulnerability (setup.php)
Netwin's DMail ETRN overflow	FakeBO buffer overflow	OpenSSH 2.5.x −> 2.9.x adv.option
rwhois format string attack	IMAP4rev1 buffer overflow after logon	OpenSSH < 3.0.1
rwhois format string attack (2)	Apache−SSL overflow	Squid overflows
SSH 3 AllowedAuthentication	IMAP4buffer overflow in the BODY command	Apache chunked encoding
rsh with null username	OpenSSL overflow	Multiple MySQL Vulnerabilities (COM_TABLE_DUMP, COM_CHANGE_USER, read_rows, read_one_row)
Cyrus IMAP pre−login buffer overrun	BitKeeper remote command execution	
Gain root remotely:		
BIND buffer overrun	RedHat 6.0 cachemgr.cgi	Check Point FW−1 identification
A CVS pserver is running	RealServer Memory Content Disclosure	Atrium Mercur Mailserver
SMB shares enumeration	X Server	Bad Registry Permissions (winlogon)
Sambar /sysadmin directory 2	htgrep CGI	Oracle XSQL Stylesheet Vulnerability
hpux ftpd PASS vulnerability	snmpXdmid overflow	ntpd overflow
IIS ISAPI Overflow	Compaq WBEM Server Detection	Knox Arkeia buffer overflow
ftpd buffer overflow	SyGate Backdoor	iPlanet Certificate Management Traversal
SMTP daemon MAIL FROM overflow	UltraSeek 3.1.x Remote DoS	Samba Remote Arbitrary File Creation
IIS buffer overflow	XMail APOP Overflow	SysV /bin/login buffer overflow (rlogin)
SysV /bin/login buffer overflow (telnet)	OpenSSH UseLogin Environment Variables	Webalizer Cross Site Scripting Vulnerability
dtspcd overflow	OpenSSH Channel Code Off by 1	EFTP buffer overflow
rpc.walld format string	cachefsd overflow	OpenSSH AFS/Kerberos ticket/token passing
lpd, dvips and remote command execution	irix rpc.passwd overflow	OpenSSH < 3.3
dwhttpd format string	HTTP Cookie overflow	HTTP header overflow
Boozt index.cgi overflow	Avirt gateway insecure telnet proxy	rpc.nisd overflow
rlogin −froot	WS FTP overflows	SOCKS4A hostname overflow
HTTP 1.1 header overflow	BIND vulnerable to cached RR overflow	Samba Unicode Buffer Overflow
SOCKS4 username overflow	SSH setsid() vulnerability	Webserver4everyone long URL
X Font Service Buffer Overflow	SSH Multiple Vulns	

General:		
Identd enabled	Cognos Powerplay WE Vulnerability	guestbook.cgi
WinSATAN	MySQL password handling problem	Dansie Shopping Cart backdoor
Insecure Napster clone	Buffer overflow in WebSite Pro webfind.exe	Translate:f vulnerability exposes IIS files source
Boa file retrieval	passwordless MySQL	BIND vulnerable to buffer overflow
hsx directory traversal	Solaris FTPd user existance leakage	404 check
RFP exploit (msadcs.dll) located	SimpleServer remote execution	Check Point SecuRemote Information Leakage
Sambar webserver pagecount hole	sdbsearch.cgi	SIX Webboard's generate.cgi
Determine if Bind 9 is running	SiteScope Web Administration Server Detection	WorldClient for MDaemon Server Detection
AOLserver Default Password	Sun JavaServer Default Admin Password	Cobalt RaQ2 cgiwrap
IIS possible DoS using ExAir's query	HP LaserJet direct print	ipop2d buffer overflow
Microsoft Exchange Public Folders Information Leak	RTSP Server type and version	Shopping Cart Arbitrary Command Execution (Hassan)
Ultraseek Web Server Detection	Apache Auth Module SQL Insertion Attack	Content−Location HTTP Header
Kazaa and Morpheus Expose Sensitive Information	Formmail Version Information Disclosure	Mediahouse Statistics Web Server Detect
A Nessus Daemon is running	Cobalt Web Administration Server Detection	IRC daemon identification
SSH protocol version 1 enabled	F5 Device Default Support Password	Unprotected Netware Management Portal
Scan for UPNP responding hosts	PHP−Nuke sql_debug Information Disclosure	Microsoft's SQL Server Brute Force
Hewlett Packard AdvanceStack Switch Management Authentication Bypass	Delta UPS Daemon Detection	Sun Cobalt Adaptive Firewall Detection
SSH protocol versions supported	BIND vulnerable to DNS storm	IIS Sensitive Authentication Information Disclosure
Misc information on News server	NTP read variables	Redline Networks Accelerator Detection
Oracle Jserv Executes outside of doc_root	Gnutella Servent Detection	IIS Internal IP Address Disclosure
Usage Statistics Detection	Compaq Web Based Management Agent Proxy Vulnerability	Linksys Router Default Password
WhatsUp Gold Default Admin Account	Netware NDS Object Enumeration	Wireless Access Point detection
HTTP TRACE	redhat Interchange	UDDI detection
DameWare Mini Remote Control Detection		
IIS:		
IIS directory traversal (unicode)	IIS .IDA ISAPI filter applied	Code Red version X detection
IIS XSS via 404 error		
Intelligence gathering:		
HTTP Server type and version		

Misc.:		
Finger cgi	nph−test−cgi	nsed service
jj cgi	Dragon−Fire IDS − dfire.cgi	Domino HTTP server exposes the set up of the filesystem
guestbook.pl	HTTP Server type and version	ICEcap default password vulnerability
Netscape Administration Server Password Disclosure	MBDMS overflow	NAI Management Agent leaks info
SMB Registry : permissions of the RAS key	PHPix directory traversal vulnerability	ROADS' search.pl
auktion.cgi	cfinger version detection	Determine which version of BIND name daemon is running
PFTP login check	IIS 5.0 PROPFIND Vulnerability	IIS FrontPage extensions DoS
WebLogic Server /%00/ bug	McAfee myCIO detection	PPTP detection
InterScan VirusWall Remote Configuration Vulnerability	Amanda Index Server version	GateCrasher
CDK Detect	HP LaserJet display hack	NetBus 1.x
qpopper euidl problem	Bad Registry Permissions (run)	Alcatel ADSL Modem with Firewalling off
Apache UserDir Sensitive Information Disclosure	'HELP' Inteligence gathering	Web Server Cross Site Scripting
Rich Media E−Commerce Stores Sensitive Information Insecurely	AppShield Detection	qpopper options buffer overflow
AirConnect Default Password	Cabletron Web View Administrative Access	IPSwitch IMail SMTP Buffer Overflow
Shiva LanRover Blank Password	Alcatel PABX 4400 detection	RedHat 6.2 inetd
Directory Scanner	xtel detection	xtelw detection
QMTP	Apache < 1.3.27	Undocumented Account Vulnerability in Avaya P550/P550R/P580/P880/P882 Switches
Crystal Reports RDC Runtime License Detection	Seagate Crystal Reports Web Samples	Webserver 4D Cleartext Passwords
ColdFusion Administrator Detection	ColdFusion Path Disclosure	ColdFusion Reindexing CPU Exhaustion Detection
FrontPage Counter Buffer Overflow	Open WebMail User Dislcosure	Nortel/Bay Networks/Xylogics Annex default password
Netware:		
Novell NetWare HTTP POST Perl Code Execution Vulnerability		
NIS:		
Lotus Domino ?open Vulnerability	glimpse	
Nortel:		
Nortel Networks passwordless router (user level)	Nortel Networks passwordless router	Nortel/Bay Networks default password
Port scanners:		
AnyForm CGI	Sendmail 8.6.9 ident	Services
Open Port		
Pre attack intelligence:		
bigconf	Registry permissions of WinVNC's key	IIS Malformed Hit−Highlighting Argument
Excite for WebServers	Kerberos PingPong attack	Using NetBIOS to retrieve information from a Windows host
Bad Registry Permissions (schedule)	Netscape Enterprise INDEX request	php.cgi

akfingerd		
pre−attack intelligence:		
Solaris finger disclosure		
Remote file access:		
get32.exe	MetaInfo servers	3270 mapper service
test−cgi	OmniHTTPd visadmin exploit	AltaVista Intranet Search
vqServer detected	PlusMail vulnerability	Passwordless Alacatel ADSL Modem
sawmill password	Feartech's FTP browser allows access to local files	Bad Registry Permissions (HKLM)
passwordless PostgreSQL	Sambar /cgi−bin/mailit.pl installed	Shiva Integrator Default Password
BIND vulnerable to ZXFR bug	Broker FTP files listing	Sendmail mime overflow
40X HTML Cross Site Scripting vulnerability	FTP directory traversal	LDAP allows null bases
SiteScope Web Managegment Server Detect	iChat	News Server type and version
Passwordless HP LaserJet	selection service	ColdFusion Vulnerability
CA Unicenter's File Transfer Service is running	remwatch	WebSite pro shows the web file path
robot(s).txt exists on the Web Server	Informix traversal	LocalWeb2000 remote read
Root compromise:		
Shell Command Execution Vulnerability	Shell Command Execution Vulnerability	
RPC:		
IIS perl.exe problem	Web server lower 'get' vulnerability	perl interpreter can be launched as a CGI
Usable remote proxy	Upload cgi	uploader.exe
Webcart misconfiguration	infosrch.cgi	Netscape Enterprise Server and '?wp' tags
nph−publish.cgi	printenv	Oracle Web Listener
mkilog.exe CGI	newdsn.exe detection	Roxen Server /%00/ bug
MiniVend security hole can lead to complete security compromise (view_page &source)	Directory listing through WebDAV	multihtml cgi
Still Image Service Privilege Escalation	Web Shopper remote file retrieval	php log
LPC and LPC Ports Vulnerabilities	bdir.htr files detected	technote's main.cgi
/iisadmpwd/aexp2.htr	NFS export	Reading CGIs sources using /cgi−bin−sdb
phorum's common.cgi	Incomplete TCP/IP packet vulnerability	Sambar Server exposes sensitive information (ECHO)
repost.asp detected	Oracle Applications One−Hour Install Detection	icat
thttpd flaw	IIS reveals directory structure of web sites	info2www
SMB Registry : Autologon	tooltalk format string	vqServer web travesal vulnerablity
Kcms Profile Server	rpcinfo −p	
Settings:		
HTTP login page		

SMTP:		
IMC SMTP EHLO Buffer Overrun	Count.cgi	WebShield
Home Free search.cgi directory traversal	IIS dangerous sample files	Lanman browse listing
NT ResetBrowser frame &HostAnnouncement flood patch	IIS IDA/IDQ Path Disclosure	news desk
Netauth	SMTP Authentication Error	quickstore traversal
/perl directory browseable	Sendmail −bt option	MS SMTP DoS
Sendmail custom configuration file	Sendmail debug mode leak	Sendmail queue manipulation &destruction
eXtremail format strings		
SNMP:		
whois_raw	Obtain processes list via SNMP	Zope Image updating Method
webspirs.cgi	Savant original form CGI access	way−board
pals−cgi	Enumerate network interfaces list via SNMP	Obtain OS type via SNMP
Obtain Cisco type via SNMP		
Useless services:		
bb−hist.sh	Dumpenv	Proxy accepts CONNECT requests
LPRng malformed input	WebActive world readable log file	INN version check (2)
Basilix includes download	Shells in /cgi−bin	Htmlscript
rsh	Web application checks	rlogin
Webmin	mldonkey telnet	X Display Manager Control Protocol (XDMCP)
Check for a Citrix server	Windows Terminal Service Enabled	eDonkey detection
xtux server detection	mldonkey www	mldonkey telnet
mldonkey www		
Windows:		
Web server directory traversal	/scripts directory browsable	MS Personal WebServer ...
alis service	websendmail	ht://Dig information exposure
WWWBoard passwords vulnerability	Trin00 for Windows Detect	wrap
sojourn.cgi	The ACC router shows configuration without authentication	Getting the domain SID
SMB users list	Registry accessible remotely	Zope DocumentTemplate vulnerability
Read any file due to ~nobody/ vulnerability	SSH Kerberos issue	Jakarta Tomcat's admin CGIs can be used to add, delete, or view sensitive information (/admin)
Winreg Registry key missing	Local Security Policy Corruption	dcforum CGI
Trin00 detected	Malformed request to domain controller	Allaire JRun Directory Listing
ICECast Format String	Malformed PPTP Packet Stream vulnerability	commerce.cgi
SQL Query Abuse Vulnerability	SSH1 CRC−32 compensation attack	in.fingerd |command@host bug
MySQL various flaws	SWAT exposes user names by brute force	phf
Oracle tnslsnr security	cfingerd format string attack	DHCP server info gathering
tektronix's _ncl_items.shtml	Microsoft's SQL UDP Info Query	Microsoft's SQL Blank Password
Check Point Firewall−1 Telnet Authentication	GuildFTPD Directory Traversal	NTLMSSP Privilege Escalation
XML Core Services patch (Q318203)	SSH Secure Shell 3.0.0 Allows Passwordless Logons	MySQL Server version

LDAP allows anonymous binds	OmniPro httpd 2.08 scripts source full disclosure	Index Server Search Function Buffer Overflow Vulnerability
IrDA access violation patch	IIS 5.0 WebDav Memory Leakage	Tripwire for Webpages Detection
Oracle Web Administration Server Detection	FTP real path	nsemntd service
walld service	ypxfrd service	Microsoft Frontpage extensions
IIS possible DoS using ExAir's search	cmsd service	Microsoft Windows 9x NETBIOS password verification vulnerability
The messenger service is running	Zeus Web server allows remote attacker to view source code of CGIs	Detect the HTTP RPC endpoint mapper
Shared directory access	Detect CIS ports	SMB NativeLanMan
Unprotected PC Anywhere Service	RPC Endpoint Mapper can Cause RPC Service to Fail	IE 5.5 6.0 Cumulative patch (Q313675)
Unchecked Buffer in XP upnp	SMB get host SID	IE 5.01 5.5 6.0 Cumulative patch (Q316059)
SMB use host SID to enumerate users	Microsoft Hostfix for SNMP Vulnerability	Users in the 'Account Operator' group
Users in the 'Admin' group	Users in the 'Backup Operator' group	Users in the 'Print Operator' group
Users in the 'Replicator' group	Users in the 'System Operator' group	Guest belongs to a group
Obtains the lists of users aliases	Obtains the lists of users groups	Obtains user information
Windows locked out users detection	Windows can't change password user detection	Windows disabled accounts detection
Windows never changed password detection	Windows user has never logged on detection	Windows passwords never expires detection
Users in the Domain Admin group	IE VBScript Handling patch (Q318089)	Opening Group Policy Files (Q318089)
Unchecked buffer in the Multiple UNC Provider Could Enable Code Execution	Cumulative Patch for Internet Information Services (Q319733)	Windows Debugger flaw can Lead to Elevated Privileges (Q320206)
Port 445 open when 139 is not	Windows RAS overflow (Q318138)	Modem Detection
Windows Network Manager Privilege Elevation (Q326886)	ARCserve hidden share	Exchange 2000 Exhaust CPU Resources (Q320436)
Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates	Certificate Validation Flaw Could Enable Identity Spoofing	Cryptographic Flaw in RDP Protocol Can Lead to Information Disclosure
Unchecked Buffer in Decompression Functions	Unchecked Buffer in Windows Help	Flaw in Microsoft VM JDBC Classes Could Allow Code Execution
Unchecked Buffer in PPTP Implementation Could Enable DOS Attacks	Flaw in Windows WM_TIMER Message Handling Could Enable Privilege Elevation	Unchecked Buffer in XP Shell Could Enable System Compromise
Windows : User management:		
Local users information : automatically disabled accounts	Local users information : Can't change password	Local users information : disabled accounts
Local users information: Password not changed	Local users information : User has never logged on	Local users information : Passwords never expires
Obtains local user information		

What Next?

Knowing is just half the battle. Now you have to go and fix the problems we reported above. Intelligence gathering attacks may give attackers a good lead when trying to break into your host. Denial−of−Service attacks are much more dangerous than they seem at first glance (for more information take a look at:
http://www.securiteam.com/securitynews/2JUQ6QAQTE.html

High Risk vulnerabilities should be dealt with immediately. They give an attacker almost immediate access to your system! This is also a good time to review your logs and see if you could have identified this scan if it was performed without your knowledge. Conduct these penetration tests periodically to check for the newest attacks.