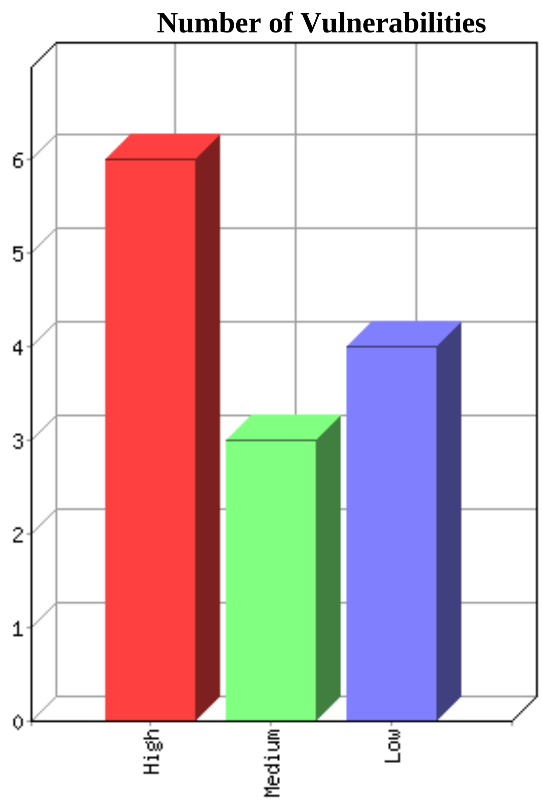
BLISS Vulnerability Assessment

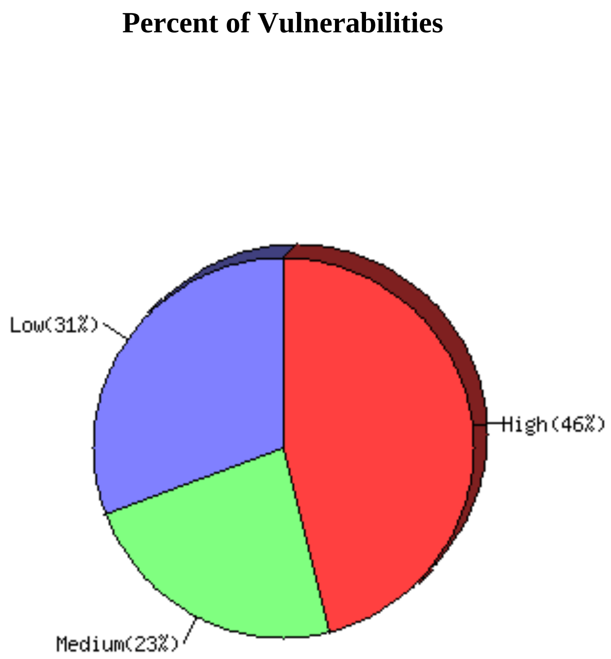
Scan Information	
Organization:	Acme Widget, Inc.
Date:	29 November 2001
Start Time:	11:41
End Time:	11:41
Responding Hosts:	7
Network Scanned:	192.168.1.100 192.168.1.101 192.168.1.102 192.168.1.103 192.168.1.104 192.168.1.105 192.168.1.106

Table of Contents

1 Executive Summary

1.1 Vulnerabilities Discovered, By Severity

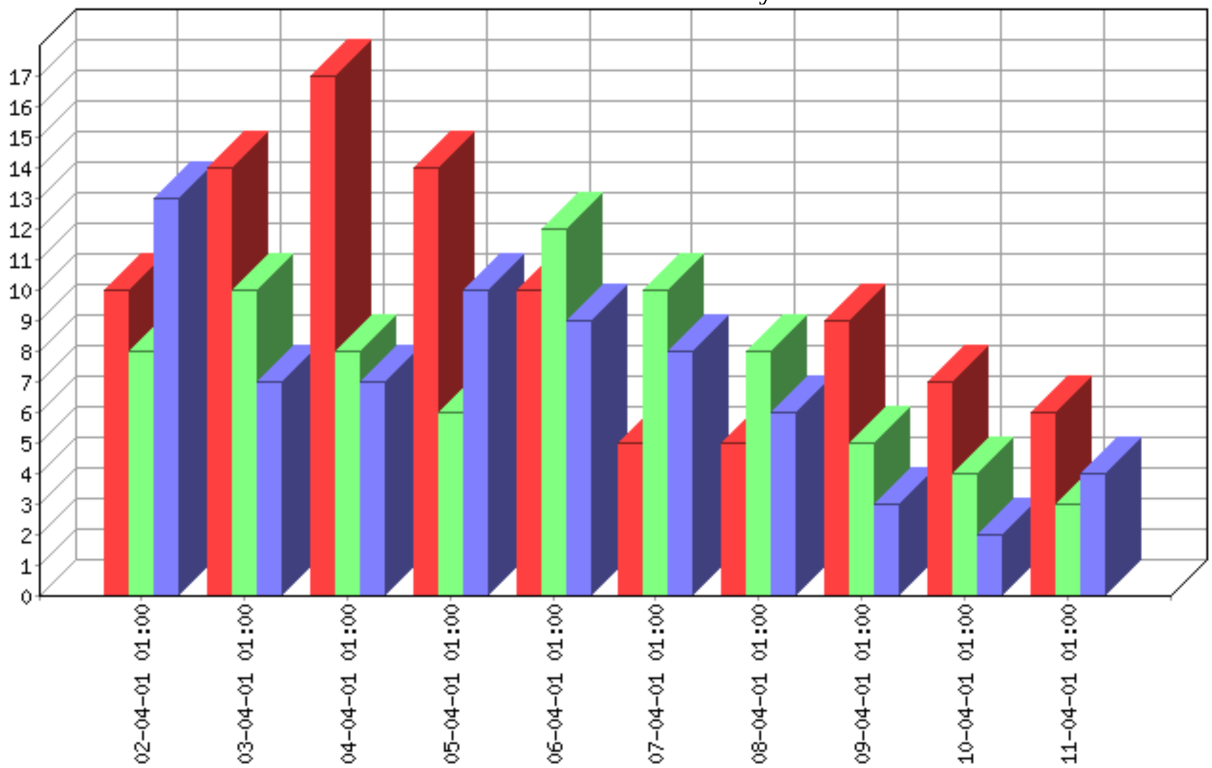




Severity	Definition	Number	Percent
High	High risk vulnerabilities are those that may allow access to the affected host, with the potential result of loss of data, exposure of confidential information or further access into the network. Also included in this category are vulnerabilities to denial−of−service attacks that can cause a system to hang or crash. All high risk vulnerabilities should be corrected immediately.	6	46%
Medium	Medium risk vulnerabilities allow attackers to mask their activities using your systems, or make you and your systems appear as if they are the attacker. Also included in this category are vulnerabilities to any activities that cause annoyance, such as mild denial−of−service attacks that use unnecessary bandwidth but do not completely eliminate access.	3	23%
Low	Low risk vulnerabilities are those that may provide information about the host or network that is not inherently dangerous but may compromise your privacy policy or would be useful in an attack.	4	31%

1.2 Vulnerability Trends

Recent Overall Vulnerability Results



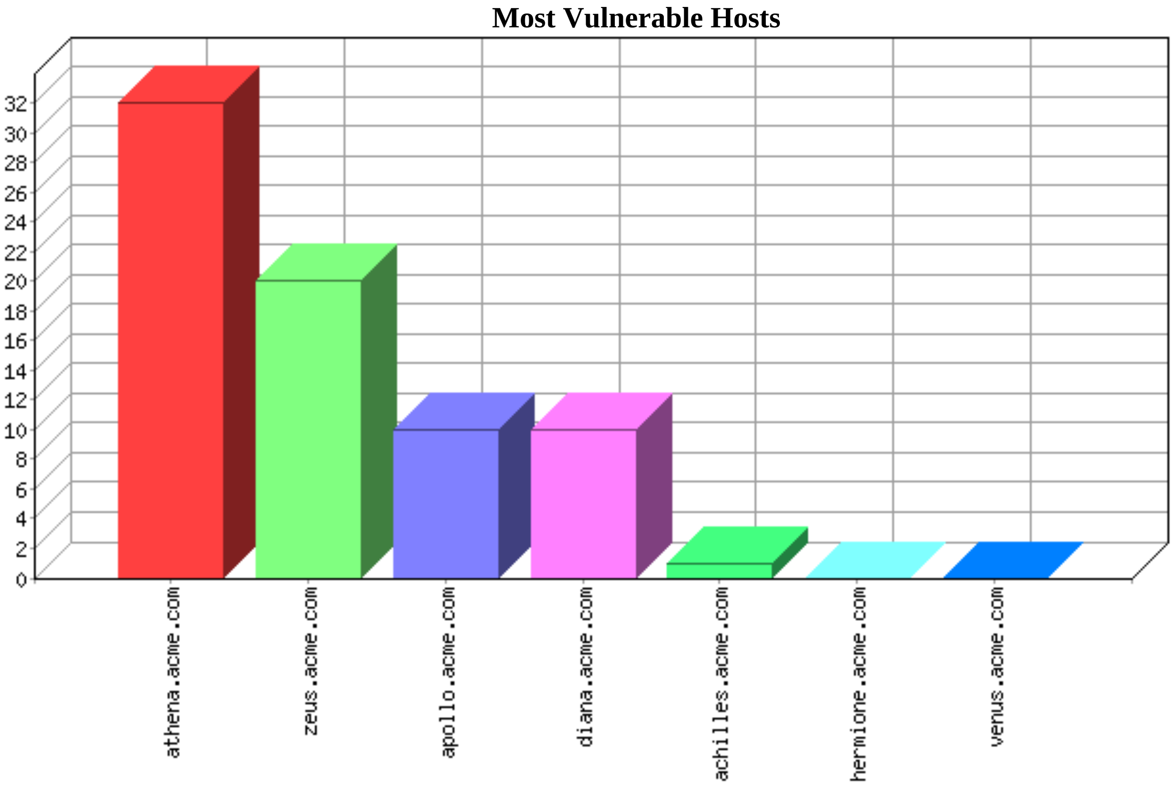
About this report: The Vulnerability Trends report lists the total number and severity of vulnerabilities found on the network. Use this report to track progress in addressing network security issues.

	Number Of Vulnerabilities		
Scan Date	**High**	**Medium**	**Low**
02−04−01 01:00	10	8	13
03−04−01 01:00	14	10	7
04−04−01 01:00	17	8	7
05−04−01 01:00	14	6	10
06−04−01 01:00	10	12	9
07−04−01 01:00	5	10	8
08−04−01 01:00	5	8	6
09−04−01 01:00	9	5	3
10−04−01 01:00	7	4	2

11−04−01 01:00	6	3	4

2 Security Manager Reports

2.1 Host Vulnerability Index Report



About this report: The Host Vulnerability Index report lists the number and severity of vulnerabilities found on each host, and calculates a vulnerability index to identify those hosts most vulnerable to attack. Use this report to focus IT resources on those hosts that most raise the level of risk to the organization. (The index weights high risk vulnerabilties with a value of 10, medium with a value of 3, and low with a value of 1.) This report is sorted is descending order by index value.

			Number Of Vulnerabilities		
Vuln. Index	DNS Name	IP Address	High	Medium	Low
32	athena.acme.com	192.168.1.100	3	0	2
20	zeus.acme.com	192.168.1.101	1	3	1
10	apollo.acme.com	192.168.1.106	1	0	0
10	diana.acme.com	192.168.1.102	1	0	0
1	achilles.acme.com	192.168.1.104	0	0	1
0	hermione.acme.com	192.168.1.105	0	0	0

0	venus.acme.com	192.168.1.103	0	0	0

2.2 New Vulnerability Summary

About this report: The New Vulnerability Summary lists vulnerabilities discovered since the last scan. Use this report to identify changes in your security posture. It is sorted by host, then severity level.

DNS Name	IP Address	Severity	Vulnerability
athena.acme.com	192.168.1.100	Low	FTP server reports version number in greeting banner
		Low	Your system answers to ICMP timestamp requests from anyone on the network

2.3 Host Vulnerability Summary

About this report: The Host Vulnerability Summary provides an overview of the vulnerabilities found on each host. Use this report to identify common security issues throughout the network and allocate IT resources to resolve the most severe risks. It can be used as a checklist for addressing security problems. This report is sorted by host, then severity level. Hosts that have no detected vulnerabilities do not appear in this report.

DNS Name	IP Address	Severity	Vulnerability
achilles.acme.com	192.168.1.104	Low	FTP server reports version number in greeting banner
apollo.acme.com	192.168.1.106	High	The Microsoft IIS web server allows any file with a .cnf extension to be viewed by anyone on the network.
athena.acme.com	192.168.1.100	High	The CGI programs loadpage.cgi and search.cgi contain security vulnerabilities
		High	RDS vulnerability in IIS allows anyone on the network to execute any command as Administrator.
		High	Windows NT 4.0 DNS server is vulnerable to denial−of−service.
		Low	FTP server reports version number in greeting banner
		Low	Your system answers to ICMP timestamp requests from anyone on the network
diana.acme.com	192.168.1.102	High	The Back Orifice backdoor software was found on your system, allowing full remote access over the Internet
zeus.acme.com	192.168.1.101	High	Qualcomm qpopper 2.5x server allows anyone on the network to execute commands on your system
		Medium	The Linuxconf service may allow unauthorized access to your server
		Medium	Your system answers to telnet requests.
		Medium	The /robot(s).txt file on your server reveals private information
		Low	Your SMTP mail server reveals private information

2.4 Network Vulnerability Summary

About this report: The Network Vulnerability Summary groups the hosts affected by a specific vulnerability together so that IT resources can be allocated more efficiently according to the type of problem to be addressed. For example, if multiple servers require the same patch or configuration change, those servers are listed together. This report is sorted by severity level.

		Affected Machines	
Severity	**Vulnerability**	**DNS Name**	**IP Address**
High	The CGI programs loadpage.cgi and search.cgi contain security vulnerabilities	athena.acme.com	192.168.1.100
	The Microsoft IIS web server allows any file with a .cnf extension to be viewed by anyone on the network.	apollo.acme.com	192.168.1.106
	RDS vulnerability in IIS allows anyone on the network to execute any command as Administrator.	athena.acme.com	192.168.1.100
	The Back Orifice backdoor software was found on your system, allowing full remote access over the Internet	diana.acme.com	192.168.1.102
	Qualcomm qpopper 2.5x server allows anyone on the network to execute commands on your system	zeus.acme.com	192.168.1.101
	Windows NT 4.0 DNS server is vulnerable to denial−of−service.	athena.acme.com	192.168.1.100
Medium	The Linuxconf service may allow unauthorized access to your server	zeus.acme.com	192.168.1.101
	Your system answers to telnet requests.	zeus.acme.com	192.168.1.101
	The /robot(s).txt file on your server reveals private information	zeus.acme.com	192.168.1.101
Low	FTP server reports version number in greeting banner	athena.acme.com	192.168.1.100
		achilles.acme.com	192.168.1.104
	Your system answers to ICMP timestamp requests from anyone on the network	athena.acme.com	192.168.1.100
	Your SMTP mail server reveals private information	zeus.acme.com	192.168.1.101

2.5 Fixed Vulnerability Summary

About this report: The Fixed Vulnerability Summary lists vulnerabilities repaired since the last scan. Use this report to identify changes in your security posture. It is sorted by host, then severity level.

DNS Name	IP Address	Severity	Vulnerability
achilles.acme.com	192.168.1.104	High	The Microsoft IIS server allows program execution
		Medium	The /robot(s).txt file on your server reveals private information

2.6 New Network Services

About this report: The New Network Services Report lists new services discovered since the last scan. Use this report to ensure that only authorized and properly configured servers are active. This report is sorted by host, then service name.

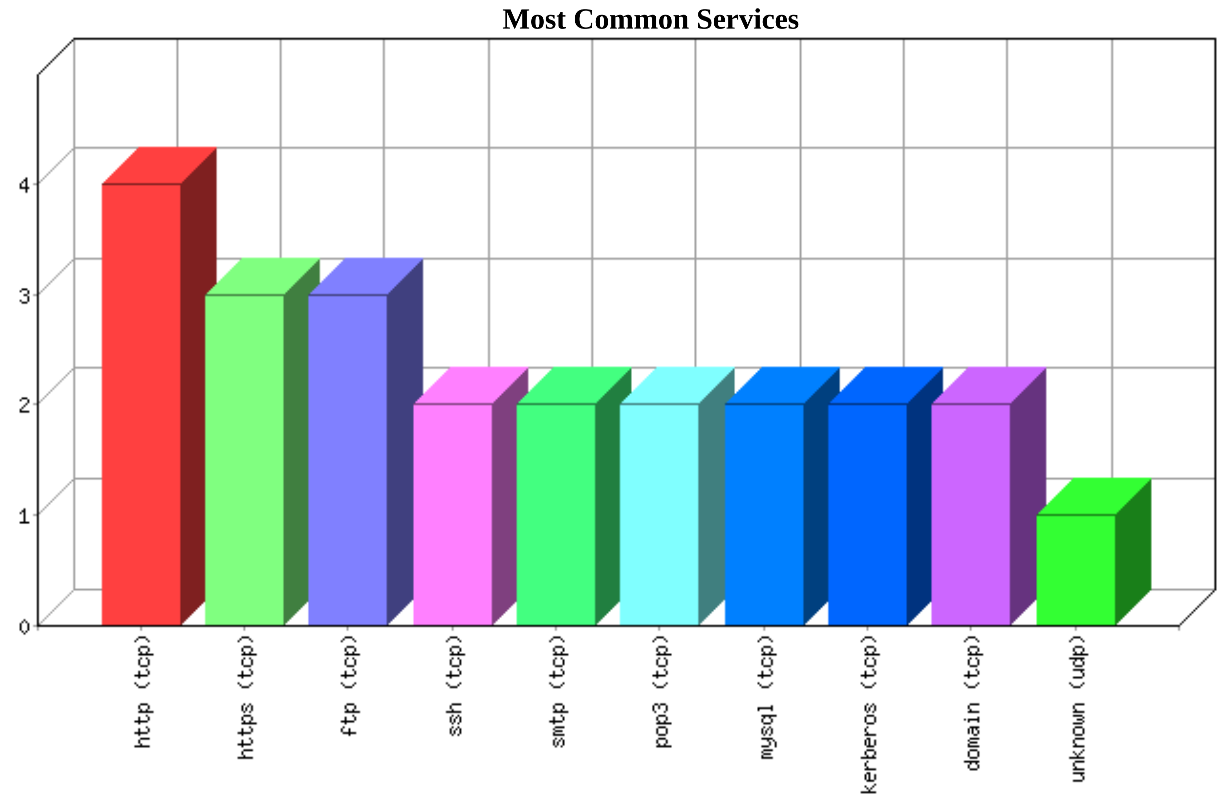
DNS Name	IP Address	Service	Version/Remote Banner
athena.acme.com	192.168.1.100	ftp (21/tcp)	athena.acme.com microsoft ftp service (Version 5.0)

2.7 Removed Network Services

About this report: The Removed Network Services Report lists services that have been disabled since the last scan. Use this report to ensure that all appropriate servers are active. This report is sorted by host, then service name.

DNS Name	IP Address	Service	Version/Remote Banner
achilles.acme.com	192.168.1.104	http (80/tcp)	

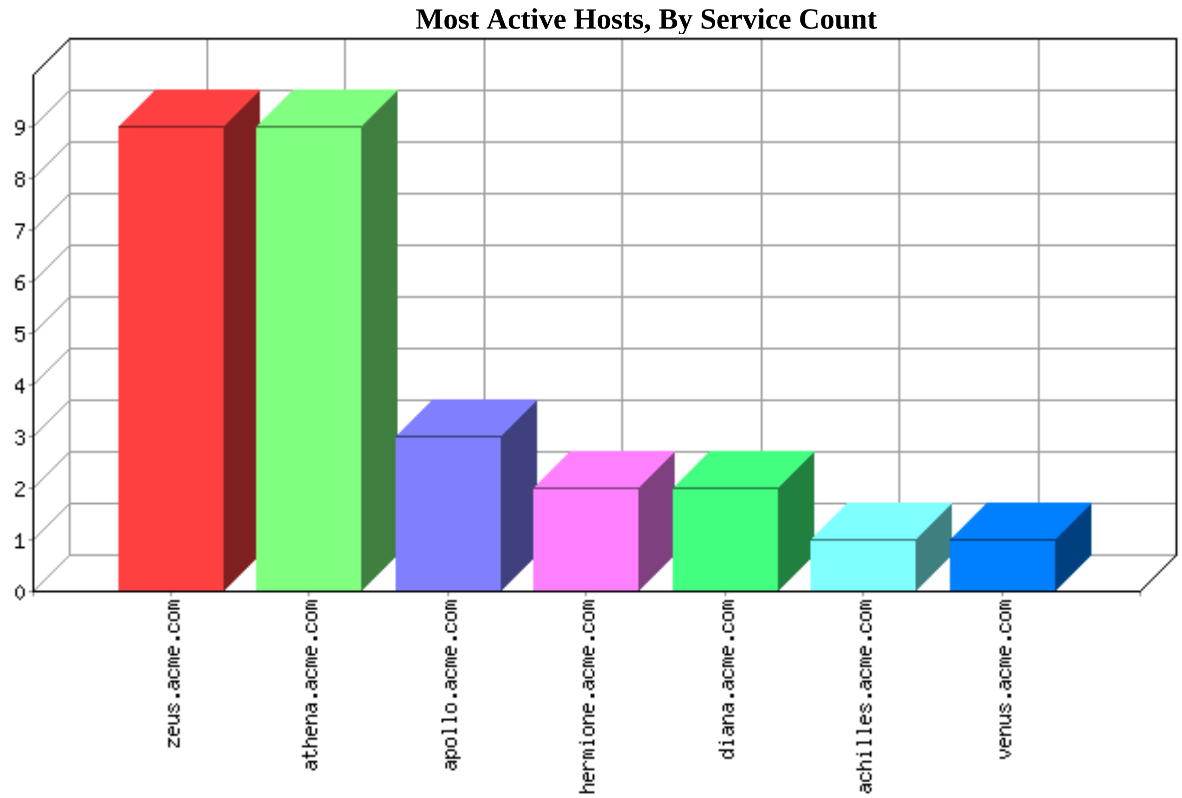
2.8 Most Common Services



About this report: The Most Common Services report lists the type of network services that are the most prevalent in your network. Because each service requires a different configuration and different expertise to be operated securely, the most common services are identified so that IT resources can be focused to the greatest effect.

Service	TCP/UDP	# Of Hosts
http	tcp	4
https	tcp	3
ftp	tcp	3
ssh	tcp	2
smtp	tcp	2
pop3	tcp	2
mysql	tcp	2
kerberos	tcp	2
domain	tcp	2
unknown	udp	1

2.9 Most Active Hosts, By Service Count



About this report: The Most Active Hosts report lists those hosts that offer the greatest number of network services. A basic principle of security is to disable unnecessary services, thus denying an intruder a potential pathway to compromise a host. Review the services running on the hosts listed on this report and disable those you find to be unnecessary.

DNS Name	IP Address	# Of Services
zeus.acme.com	192.168.1.101	9
athena.acme.com	192.168.1.100	9
apollo.acme.com	192.168.1.106	3
hermione.acme.com	192.168.1.105	2
diana.acme.com	192.168.1.102	2
achilles.acme.com	192.168.1.104	1
venus.acme.com	192.168.1.103	1

3 Security Technician Reports

3.1 Host Vulnerability Technical Detail

About this report: The Host Vulnerability Report lists specific details of each vulnerability found on each host, along with instructions on how to mitigate the problem, references to provide further background information and, if applicable, responses from the host when it was tested. This report is sorted by host, then severity level.

3.1.1 Detail for host achilles.acme.com (192.168.1.104)

Low	**FTP server reports version number in greeting banner**	**ftp (21/tcp)**
Description		
Your FTP server reports its version information in the initial greeting. This information can be used to target an attack against this specific version of FTP.		
Solution		
Change the login banner to a generic greeting, for example 'Authorized use only'		
Remote System Output		
`achilles.acme.com microsoft ftp service (version 5.0).`		
References		
See the ftpaccess man page section "greeting". http://mirrors.ccs.neu.edu/cgi−bin/unixhelp/man−cgi?ftpd+1 http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/iis/maintain/optimize/custom.asp		

3.1.2 Detail for host apollo.acme.com (192.168.1.106)

High	The Microsoft IIS web server allows any file with a .cnf extension to be viewed by anyone on the network.	www (80/tcp)

Description

The Microsoft IIS web server by default allows anybody on the network to read any .cnf files on your system. These are typically configuration files that contain private information.

Solution

Either:

Delete all .cnf files from your server

Use a different web server instead of IIS

Set permissions on all .cnf files to disallow general read access

Remote System Output

```
/_vti_pvt/access.cnf
/_vti_pvt/svcacl.cnf
/_vti_pvt/writeto.cnf
/_vti_pvt/service.cnf
/_vti_pvt/services.cnf
```

References

http://microsoft.com/technet

3.1.3 Detail for host athena.acme.com (192.168.1.100)

High	The CGI programs loadpage.cgi and search.cgi contain security vulnerabilities	www (80/tcp)

Description

One or both of the following CGI programs was found on your web server:

loadpage.cgi
search.cgi

If they come from the package EZShopper 3.0, they may be vulnerable to some security vulnerabilities that can allow anyone on the network to view any file on your server or execute any command.

Solution

Upgrade to the latest stable version of EZShopper, available at http://www.ahg.com/software.htm#ezshopper

References

http://www.ahg.com/software.htm#ezshopper

High	RDS vulnerability in IIS allows anyone on the network to execute any command as Administrator.	www (80/tcp)

Description

The IIS web server software has a well−documented vulnerability documented by Rain Forest Puppy, that allows anyone on the network to gain access to ODBC databases and subsequently execute any command on the system as Administrator, thereby gaining control over your server.

Remote Data Services (RDS) is installed by default as part of Windows NT Server Internet Information Service (IIS) 4.0, via the Microsoft Windows NT Option Pack. The RDS component enables Internet access to remote data resources in IIS. The RDS DataFactory, which is a component of RDS, allows implicit data access requests from the network.

Any web client can issue a SQL command along with the IP address of a your SQL Server system, a SQL account and password, a database name, and a SQL query string. If the request is valid (the remote server is reachable by the Windows NT IIS server, the user account and password are correct, and the database name is valid), the query results will be sent through HTTP back to the client.

The risk caused by the DataFactory is greater if newer OLE DB Providers are installed on the server, such as Microsoft DataShape Provider and Microsoft JET OLE DB provider (which are part of MDAC 2.0 in Visual Studio 98) which allow shell commands to be executed.

Solution

Delete the following registry keys from the Registry Editor or a batch file:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\RDSServer.DataFactory
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\AdvancedDataFactory
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\VbBusObj.VbBusObjCls

To delete the registry keys:

1. Open the Registry Editor. From the Windows NT Start menu, select Run. Type regedt32 and click OK.
2. Go to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch registry key.
3. Select the RDSServer.DataFactory key.
4. From the Edit menu, select Delete and verify the deletion.
5. Repeat steps 3 and 4 to delete the AdvancedDataFactory and VbBusObj.VbBusObjCls keys.

or
Use the REGDEL.exe command−line utility to remove DataFactory functionality. REGDEL.exe is a tool available as part of the Windows NT Resource Kit utilities that can be used to delete registry entries from the command line:

1. Copy the following text into a .bat file (for example, c:\dfremove.bat) and run the batch file on machines on which you want to remove the RDS components.

```
REM Batch file to remove RDS components
REM Make sure that REGDEL.exe from the Resource Kit is in your PATH
REGDEL SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\AdvancedDataFactory
REGDEL SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\RDSServer.DataFactory
REGDEL SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\VbBusObj.VbBusObjCls
Echo RDS Keys Removed
```

2. Execute or run the batch file on the web server.

To disable the implicit remoting functionality of RDS, remove the following registry entries from the server hosting IIS:
Hive:HKEY_LOCAL_MACHINE **Key:** SYSTEM\ CurrentControlSet\Services\W3SVC\Parameters\ ADCLaunch\RDSServer.DataFactory

Hive:HKEY_LOCAL_MACHINE **Key:**SYSTEM\ CurrentControlSet\Services\W3SVC\Parameters\ ADCLaunch\AdvancedDataFactory

Hive:HKEY_LOCAL_MACHINE **Key:**SYSTEM\ CurrentControlSet\Services\W3SVC\Parameters\ ADCLaunch\VbBusObj.VbBusObjCls

References

Microsoft Security Bulletin MS98−004: Unauthorized ODBC Data Access with RDS and IIS

Microsoft Knowledge Base Article Q184375: Security Implications of RDS 1.5, IIS 3.0 or 4.0, and ODBC

Microsoft Security Bulletin MS99−025: Re−Release: Unauthorized Access to IIS Servers through ODBC Data Access with RDS

CIAC Information Bulletin J−054: Unauthorized Access to IIS Servers through ODBC Data Access with RDS

Microsoft Security Bulletin (MS99−025): Frequently Asked Questions

CERT Incident Note IN−99−08: Attacks against IIS web servers involving MDAC

Microsoft Knowledge Base article Q184375: Security Implications of RDS 1.5, IIS 4.0, and ODBC

CVE: CVE−1999−1011

High	**Windows NT 4.0 DNS server is vulnerable to denial−of−service.**	**domain (53/tcp)**

Description

The Windows NT 4.0 DNS server is vulnerable to several denial of service attacks that are well−documented on the Internet and easy to execute, including flooding port 53 with characters, telnet to port 53, certain network packets, certain DNS names, and specific software flaws (see references).

In addition, the DNS server may allow access to private information via certain spoofed information.

Solution

Update your DNS server. See Microsoft's FTP site for details at ftp://ftp.microsoft.com/bussys/winnt/winnt−public/fixes/.

Also

Apply the latest Windows NT 4.0 Service Pack or the post−SP2 dns−fix patch.To apply the latest Windows NT Service Pack:

1. Open a web browser.
2. Go to http://support.microsoft.com/support/ntserver/Content/ServicePacks/ and follow the directions to download the appropriate service pack for your computer.
3. Find the installation program you downloaded to your computer.
4. Double−click the program icon to start the installation.
5. Follow the installation directions.

or

If Windows NT 4.0 Service Pack 3 (SP3) or later cannot be applied, Windows NT 4.0 SP2 users must obtain and install the post−SP2 dns−fix hotfix available from ftp://ftp.microsoft.com/bussys/winnt/winnt−public/fixes/usa/NT40/hotfixes−postSP2/dns−fix .

References

Fyodor's Exploit World, Another way to crash NT DNS server, http://www.insecure.org/sploits/NT.DNS.character_flood.html
Microsoft Knowledge Base Article Q169461, Access Violation in DNS.EXE Caused by Malicious Telnet Attack, http://support.microsoft.com/support/kb/articles/Q169/4/61.asp
Microsoft Knowledge Base Article Q142047, Bad Network Packet May Cause Access Violation (AV) on DNS Server, http://support.microsoft.com/support/kb/articles/Q142/0/47.asp
Microsoft Knowledge Base Article Q154984, DNS Server May Not Recursively Resolve Some Names, http://support.microsoft.com/support/kb/articles/Q154/9/84.asp
Microsoft Knowledge Base Article Q154985, DNS Registry Key Not Updated When Changing Zone Type, http://support.microsoft.com/support/kb/articles/Q154/9/85.asp
Microsoft Knowledge Base Article Q167629, Predictable Query IDs Pose Security Risks for DNS Servers, http://support.microsoft.com/support/kb/articles/Q167/6/29.asp
Common Vulnerabilties and Exposures: CVE−1999−0275
Reference: XF:nt−dnscrash
Reference: XF:nt−dnsver
Reference: MS:Q169461

Low	FTP server reports version number in greeting banner	ftp (21/tcp)

Description

Your FTP server reports its version information in the initial greeting. This information can be used to target an attack against this specific version of FTP.

Solution

Change the login banner to a generic greeting, for example 'Authorized use only'

Remote System Output

```
athena.acme.com microsoft ftp service (Version 5.0)
```

References

See the ftpaccess man page section "greeting".
http://mirrors.ccs.neu.edu/cgi−bin/unixhelp/man−cgi?ftpd+1
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/iis/maintain/optimize/custom.asp

Low	Your system answers to ICMP timestamp requests from anyone on the network	general/icmp

Description

Your system answers to network ICMP timestamp requests. This can allow anyone on the network to identify the exact time that is set on your system, which can be used to defeat authentication and to hijack your network sessions.

Solution

Filter out the icmp timestamp requests (13), and the outgoing icmp timestamp replies (14).

References

http://www.freesoft.org/CIE/Topics/81.htm

3.1.4 Detail for host diana.acme.com (192.168.1.102)

High	The Back Orifice backdoor software was found on your system, allowing full remote access over the Internet	unknown (31337/udp)
Description		
Back Orifice is a trojan program that allows remote operation of Windows 9x and Windows NT machines. This program was designed with stealth in mind, and as such is very difficult to detect with scanning, cleansing, and intrusion detection tools.		
Solution		
Since your system is no longer under your control, re−install the operating system from scratch and then carefully restore your data, avoiding re−infection of your system. Remove Back Orifice. To remove Back Orifice, obtain the latest version of anti−virus software from your anti−virus vendor. Back Orifice is very difficult to detect on a machine because it is so highly configurable. By default, it will install itself in the Windows system directory as the fileUMGR32.EXE. On Windows NT, it will install a service listed as "Remote Administration Service." This is the default name and can be changed.		
References		
Microsoft Security Bulletin, What Customers Should Know About 'BackOrifice', http://www.microsoft.com/security/bulletins/bo2k.asp Cult of the Dead Cow (cDc), Back Orifice, http://www.bo2k.com/indexnews.html ISS Security Advisory #31, Back Orifice, http://xforce.iss.net/alerts/advise31.php Trend Micro Security Alert, Back Orifice, http://www.antivirus.com/vinfo/security/sa071299.htm Symantec AntiVirus Research Center, BackOrifice2K.Trojan, http://www.norton.com/avcenter/venc/data/back.orifice.2000.trojan.html		

3.1.5 Detail for host hermione.acme.com (192.168.1.105)

No vulnerabilities discovered for this host.

3.1.6 Detail for host venus.acme.com (192.168.1.103)

No vulnerabilities discovered for this host.

3.1.7 Detail for host zeus.acme.com (192.168.1.101)

<table>
<tr><th>High</th><th>Qualcomm qpopper 2.5x server allows anyone on the network to execute commands on your system</th><th>pop3 (110/tcp)</th></tr>
<tr><td colspan="3"><b>Description</b></td></tr>
<tr><td colspan="3">The version of Qualcomm qpopper on your system is 2.5x, which contains a well−known vulnerability that allows anyone on the network with a POP account on your server to execute commands on your system by sending themselves a mail message.</td></tr>
<tr><td colspan="3"><b>Solution</b></td></tr>
<tr><td colspan="3">Upgrade to the latest stable version of qpopper, 3.0.2 or later
available at: ftp://ftp.qualcomm.com/Eudora/servers/unix/popper</td></tr>
<tr><td colspan="3"><b>Remote System Output</b></td></tr>
<tr><td colspan="3">+OK QPOP (version 2.53) at zeus.acme.com starting.</td></tr>
<tr><td colspan="3"><b>References</b></td></tr>
<tr><td colspan="3">BugTraq Mailing List, More problems with QPOPPER − <sigh>, http://www.netspace.org/cgi−bin/wa?A2=ind9806EandL=bugtraqandP=R252
CERT Advisory CA−98.08, Buffer overflows in some POP servers, http://www.cert.org/advisories/CA−98.08.qpopper_vul.html
Silicon Graphics Inc. Security Advisory 19980801−01−I, BSD/Qualcomm qpopper Vulnerability, ftp://sgigate.sgi.com/security/19980801−01−I</td></tr>
</table>

Medium	The Linuxconf service may allow unauthorized access to your server	linuxconf (98/tcp)
Description		
The Linuxconf service was found to be running on your server. This software, used for Linux adminstration, can be exploited to reconfigure or take over your system.		
Solution		
Disable the Linuxconf service, or block access to it		
Remote System Output		
`linuxconf/1.26`		

Medium	Your system answers to telnet requests.	telnet (23/tcp)
Description		
A telnet server is running on your system, allowing anyone on the network to attempt connections to your system. When legitimate users connect to the system with telnet, it is relatively easy for unauthorized persons on the Internet to capture account names and passwords. This will allow them to log in to your system. Private data transferred over the telnet connection can also be intercepted.		
Solution		
Use SSH instead if possible, and disable the telnet service		
Remote System Output		
`Linux 2.1.1/i386 (zeus.acme.com) (ttyp0)`		
References		
SSH: http://www.openssh.com		

Medium	The /robot(s).txt file on your server reveals private information	www (80/tcp)

Description

Some Web Servers use a file called /robot(s).txt to make search engines and any other indexing tools visit their WebPages more frequently and more efficiently. By connecting to the server and requesting the /robot(s).txt file, anyone on the network can gain private information about your system, such as restricted directories, hidden directories, cgi script directories and more.

Solution

Take special care not to tell the robots not to index sensitive directories, since this tells attackers exactly which of your directories are sensitive.

Remote System Output

```
User-agent: *
Disallow: /adimages/
Disallow: /cgi-bin/
Disallow: /docs/
Disallow: /images/
Disallow: /mail/
Disallow: /support/
Disallow: /upload/
```

Low	Your SMTP mail server reveals private information	smtp (25/tcp)

Description

The SMTP server running on your system accepts the EXPN and VRFY commands. These result in information about accounts on your systems, as well as email addresses and mailing lists. This information can be used to target attacks against specific accounts, or to send spam to your account holders.

Solution

If you are using sendmail, add the option

O PrivacyOptions=goaway

to /etc/sendmail.cf

Remote System Output

```
zeus.acme.com ESMTP Sendmail 8.11.3/8.9.3
Wed, 3 Oct 2001 15:07:35 -0400 (EDT)
214-2.0.0 This is Sendmail version 8.11.3214-2.0.0 Topics:

214-2.0.0 HELO EHLO MAIL RCPT DATA

214-2.0.0 RSET NOOP QUIT HELP VRFY
```

```
214−2.0.0 EXPN VERB ETRN DSN

214−2.0.0 For more info use "HELP
".

214−2.0.0 To report bugs in the implementation send email to

214−2.0.0 sendmail−bugs@sendmail.org.

214−2.0.0 For local information send email to Postmaster at your site.

214 2.0.0 End of HELP info
```

3.2 Network Services, By Host

About this report: The Network Services Report lists each service found to be running on each host. A basic principle of security is to disable network services that are unnecessary, thus denying an intruder a potential pathway to compromise a host. Use this report to review the services running on each host. In addition, this report lists the version number (or greeting banner) displayed by each service. In general, as little information as possible should be available externally, to avoid giving a potential intruder guidance to use version−specific attacks. This report is sorted by host, then service name.

DNS Name	IP Address	Service	Version/Remote Banner
achilles.acme.com	192.168.1.104	ftp (21/tcp)	achilles.acme.com microsoft ftp service (version 5.0).
apollo.acme.com	192.168.1.106	ftp (21/tcp)	
		http (80/tcp)	Microsoft−IIS/5.0
		https (443/tcp)	
athena.acme.com	192.168.1.100	domain (53/tcp)	
		ftp (21/tcp)	athena.acme.com microsoft ftp service (Version 5.0)
		http (80/tcp)	Microsoft IIS/5.0
		https (443/tcp)	
		imap2 (143/tcp)	
		mysql (3306/tcp)	
		pop3 (110/tcp)	
		smtp (25/tcp)	220 athena.acme.com Microsoft ESMTP MAIL Service, Version: 5.0.2195.2966 ready at Sat, 04 Nov 2001 14:20:18 −0800
		ssh (22/tcp)	ssh−1.99−openssh_2.9p2
diana.acme.com	192.168.1.102	ssh (22/tcp)	ssh−1.99−openssh_2.9p2
		unknown (31337/udp)	
hermione.acme.com	192.168.1.105	http (80/tcp)	Microsoft−IIS/5.0
		kerberos (88/tcp)	
venus.acme.com	192.168.1.103	kerberos (88/tcp)	
zeus.acme.com	192.168.1.101	domain (53/tcp)	
		http (80/tcp)	

		https (443/tcp)	
		linuxconf (98/tcp)	linuxconf/1.26
		mysql (3306/tcp)	
		pop3 (110/tcp)	+OK QPOP (version 2.53) at zeus.acme.com starting.
		smtp (25/tcp)	zeus.acme.com ESMTP Sendmail 8.11.3/8.9.3 Wed, 3 Oct 2001 15:07:35 −0400 (EDT);214−2.0.0 This is Sendmail version 8.11.3214−2.0.0 Topics:;;214−2.0.0 HELO EHLO MAIL RCPT DATA;;214−2.0.0 RSET NOOP QUIT HELP VRFY;;214−2.0.0 EXPN VERB ETRN DSN;;214−2.0.0 For more info use "HELP
		sunrpc (111/tcp)	
		telnet (23/tcp)	Linux 2.1.1/i386 (zeus.acme.com) (ttyp0)

3.3 Network Services Summary

About this report: The Network Services Summary lists the services found running on your network, and the number of hosts offering those services. Use this report to confirm that only those services that necessary are offered. This report is sorted alphabetically by service name.

Service	Port #	TCP/UDP	Number of hosts
domain	53	tcp	2
ftp	21	tcp	3
http	80	tcp	4
https	443	tcp	3
imap2	143	tcp	1
kerberos	88	tcp	2
linuxconf	98	tcp	1
mysql	3306	tcp	2
pop3	110	tcp	2
smtp	25	tcp	2
ssh	22	tcp	2
sunrpc	111	tcp	1
telnet	23	tcp	1
unknown	31337	udp	1

4 General Information

4.1 Operating System Fingerprints

About this report: The Operating System Fingerprint table lists the best guess that can be made as to the OS running on each host. Use this report to determine the level of visibility into your network from the outside. Because knowledge of the make and version of the operating system is the first piece of information that a potential intruder is likely to use to guide an attack, the ideal result would be for this report to list "Unknown" for each host. The information listed in this report is derived from low−level characteristics of TCP/IP connections, application greeting banners or error messages, and file system attributes.

IP Address	DNS Name	Probable Operating System
192.168.1.104	achilles.acme.com	Microsoft Windows
192.168.1.106	apollo.acme.com	Microsoft Windows
192.168.1.100	athena.acme.com	Unix
192.168.1.102	diana.acme.com	Microsoft Windows
192.168.1.105	hermione.acme.com	Microsoft Windows
192.168.1.103	venus.acme.com	Unknown
192.168.1.101	zeus.acme.com	Unix

4.2 Address Ownership

About this report: The Address Ownership section lists the information registered with the internet address registry service used for this network. This information is publicly available.

```
Acme Widget, Inc. (ACME−DOM)
   123 Main St.
   Anytown, CA 91356
   US

   Netname: ACME−192−168−1
   Netblock: 192.168.1.1 − 192.168.1.255

   Coordinator:
      Acme, Inc.  (SH99−ORG−ARIN)  hostmaster@ACME.COM
      (800) 555−1212

   Domain System inverse mapping provided by:

   NS1.ACME.COM                 192.168.1.99

   Record last updated on 19−May−1998.
   Database last updated on 2−Oct−2001 23:19:58 EDT.
```

4.3 Domain Ownership

About this report: This Domain Ownership section lists the information registered with the internet domain registry service used for this network. This information is publicly available.

```
Acme Widget, Inc. (ACME−DOM)
   123 Main St.
   Anytown, CA 91356
   US

   Domain Name: ACME.COM

   Administrative Contact, Technical Contact, Billing Contact:
      Hostmaster  (HOS999−ORG)  hostmaster@ACME.COM
      Acme Widget, Inc. (ACME−DOM)
      123 Main St.
      Anytown, CA 91356
      US
      800−555−1212

   Record last updated on 15−Jun−2001.
   Record expires on 03−Jul−2010.
   Record created on 02−Jul−1996.
   Database last updated on 3−Oct−2001 06:49:00 EDT.

   Domain servers in listed order:

   NS1.ACME.COM         192.168.1.99
```

DISCLAIMER:INTEK provides this service "As Is", without any warranty of any kind. INTEKmakes no warranty that this service will find every vulnerability in your network, or that the suggested solutions and advice provided in this report will be complete or error−free. INTEK shall not be responsible or liable for any use or application of the information contained in this report.