

Request POST /ReadNews.aspx HTTP/1.0
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: testaspnet.acunetix.com
Content-Length: 3168
Cookie: ASP.NET_SessionId=dykucralv3lfccr3adewo345
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/3.0 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm

Response HTTP/1.1 500 Internal Server Error
Connection: close
Date: Fri, 24 Mar 2006 09:22:27 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 1.1.4322
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 5190

2. Blind SQL/XPath injection for numeric inputs

Affects /ReadNews.aspx
Details The script has been tested with these query variables: `?id=3+and+1=1`
Severity 3
Type Validation
Description This script is possibly vulnerable to SQL/XPath Injection attacks.
Impact An unauthenticated attacker may execute arbitrary SQL/XPath statements on the vulnerable system. This may compromise the integrity of your database and expose sensitive information.
Recommendation Your script should filter metacharacters from user input.
Reported by module MultiRequest parameter manipulation
References [Acunetix SQL Injection Attack](http://www.acunetix.com/websitesecurity/sql-injection.htm) http://www.acunetix.com/websitesecurity/sql-injection.htm
[What is Blind SQL Injection?](http://www.cgisecurity.com/questions/blindsqli.shtml) http://www.cgisecurity.com/questions/blindsqli.shtml
[Advanced SQL Injection](http://www.nextgenss.com/papers/advanced_sql_injection.pdf) http://www.nextgenss.com/papers/advanced_sql_injection.pdf
[Security Focus - Penetration Testing for Web Applications \(Part Two\)](http://www.securityfocus.com/infocus/1709) http://www.securityfocus.com/infocus/1709
[More Advanced SQL Injection](http://www.ngssoftware.com/papers/more_advanced_sql_injection.pdf) http://www.ngssoftware.com/papers/more_advanced_sql_injection.pdf
[XPath injection in XML databases](http://palisade.paladion.net/issues/2005-01/ul/xpath-injection/) http://palisade.paladion.net/issues/2005-01/ul/xpath-injection/

Request GET /ReadNews.aspx?id=3+and+1=0 HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: testaspnet.acunetix.com
Cookie: ASP.NET_SessionId=dykucralv3lfccr3adewo345
Connection: Close
Pragma: no-cache
Acunetix-Product: WVS/3.0 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm

Response HTTP/1.1 200 OK
Connection: close
Date: Fri, 24 Mar 2006 09:24:36 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 1.1.4322
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 10512

3. Blind SQL/XPath injection for numeric inputs

Affects /ReadNews.aspx
Details The script has been tested with these query variables: `?id=3+and+1=1&NewsAd=ads%2Fdef%2Ehtml`
Severity 3
Type Validation
Description This script is possibly vulnerable to SQL/XPath Injection attacks.
Impact An unauthenticated attacker may execute arbitrary SQL/XPath statements on the vulnerable system. This may compromise the integrity of your database and expose sensitive information.

Severity	3
Type	Validation
Description	This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.
Impact	Malicious users may inject <code><script></code> JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them.
Recommendation	Your script should filter metacharacters from user input.
Reported by module	Parameter manipulation
References	Acunetix Cross Site Scripting Attack Security Focus - Penetration Testing for Web Applications (Part Two) Cross Site Scripting Faq
Request	POST /Comments.aspx?id=3 HTTP/1.0 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322) Host: testaspnet.acunetix.com Content-Length: 19294 Cookie: ASP.NET_SessionId=dykucralv3lfccr3adewo345 Connection: Close Pragma: no-cache Acunetix-Product: WVS/3.0 (Acunetix Web Vulnerability Scanner - NORMAL) Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
Response	HTTP/1.1 200 OK Connection: close Date: Fri, 24 Mar 2006 09:21:07 GMT Server: Microsoft-IIS/6.0 X-Powered-By: ASP.NET X-AspNet-Version: 1.1.4322 Cache-Control: private Content-Type: text/html; charset=utf-8 Content-Length: 33092

6.1 Cross Frame Scripting

Affects	/ReadNews.aspx
Details	The script has been tested with these query variables: <code>?id=3&NewsAd=http://www.long-name-with-some-</code>
Severity	2
Type	Validation
Description	This script is possibly vulnerable to Cross Frame Scripting (XFS) attacks.
Impact	Malicious users may poison a frame allowing them to conduct phishing attacks.
Recommendation	Your script should filter metacharacters from user input.
Reported by module	Parameter manipulation
References	NGS - Understanding & Preventing Phishing Attacks
Request	POST /ReadNews.aspx?id=3&NewsAd=http://www.long-name-with-some-inexistent-host.com/ HTTP/1.0 Accept: */* Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322) Host: testaspnet.acunetix.com Content-Length: 3166 Cookie: ASP.NET_SessionId=dykucralv3lfccr3adewo345 Connection: Close Pragma: no-cache Acunetix-Product: WVS/3.0 (Acunetix Web Vulnerability Scanner - NORMAL) Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
Response	HTTP/1.1 200 OK Connection: close Date: Fri, 24 Mar 2006 09:22:19 GMT Server: Microsoft-IIS/6.0 X-Powered-By: ASP.NET X-AspNet-Version: 1.1.4322 Cache-Control: private Content-Type: text/html; charset=utf-8 Content-Length: 15286

7. ASP.NET custom error message

Affects	/Comments.aspx
Details	We have found <code><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1></code>
Severity	1

Type	Informational
Description	This page contains an error/warning message that may disclose the sensitive information.
Impact	Possibly sensitive information disclosure.
Recommendation	Review the source code for this script.
Reported by module	Text search
References	
Request	<pre>GET /Comments.aspx HTTP/1.0 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322) Host: testaspnet.acunetix.com Cookie: ASP.NET_SessionId=dykucralv3lfccr3adewo345 Connection: Close Pragma: no-cache Referer: http://testaspnet.acunetix.com:80/ Acunetix-Product: WVS/3.0 (Acunetix Web Vulnerability Scanner - NORMAL) Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm</pre>
Response	<pre>HTTP/1.1 500 Internal Server Error Connection: close Date: Fri, 24 Mar 2006 09:16:27 GMT Server: Microsoft-IIS/6.0 X-Powered-By: ASP.NET X-AspNet-Version: 1.1.4322 Cache-Control: private Content-Type: text/html; charset=utf-8 Content-Length: 5261</pre>

8. GHDB: Typical login page

Affects	/login.aspx
Details	We have found inurl:login.asp
Severity	0
Type	Informational
Description	The description for this alert is contributed by the GHDB community, it may contain inappropriate language.
	Category : Pages containing login portals
	This is a typical login page. It has recently become a target for SQL injection. Comsec's article at http://www.governmentsecurity.org/articles/SQLInjectionBasicTutorial.php brought this to my attention.
Impact	Not available. Check description.
Recommendation	Not available. Check description.
Reported by module	GHDB - Google hacking database
References	Acunetix Google hacking http://www.acunetix.com/websitesecurity/google-hacking.htm GHDB Homepage http://johnny.ihackstuff.com/
Request	<pre>GET /login.aspx HTTP/1.0 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322) Host: testaspnet.acunetix.com Cookie: ASP.NET_SessionId=dykucralv3lfccr3adewo345 Connection: Close Pragma: no-cache Referer: http://testaspnet.acunetix.com:80/ Acunetix-Product: WVS/3.0 (Acunetix Web Vulnerability Scanner - NORMAL) Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm</pre>
Response	<pre>HTTP/1.1 200 OK Connection: close Date: Fri, 24 Mar 2006 09:16:27 GMT Server: Microsoft-IIS/6.0 X-Powered-By: ASP.NET X-AspNet-Version: 1.1.4322 Cache-Control: private Content-Type: text/html; charset=utf-8 Content-Length: 10355</pre>

Part II - Network Health Check

As previously mentioned, HiTRUST Web Security Health Check report consists of health check results and recommendation on the (1) web application layer and (2) network layer. The network health check results is shown on the rest of this report.

Network Health Check Summary

Vulnerabilities Total

6

Average Security Risk



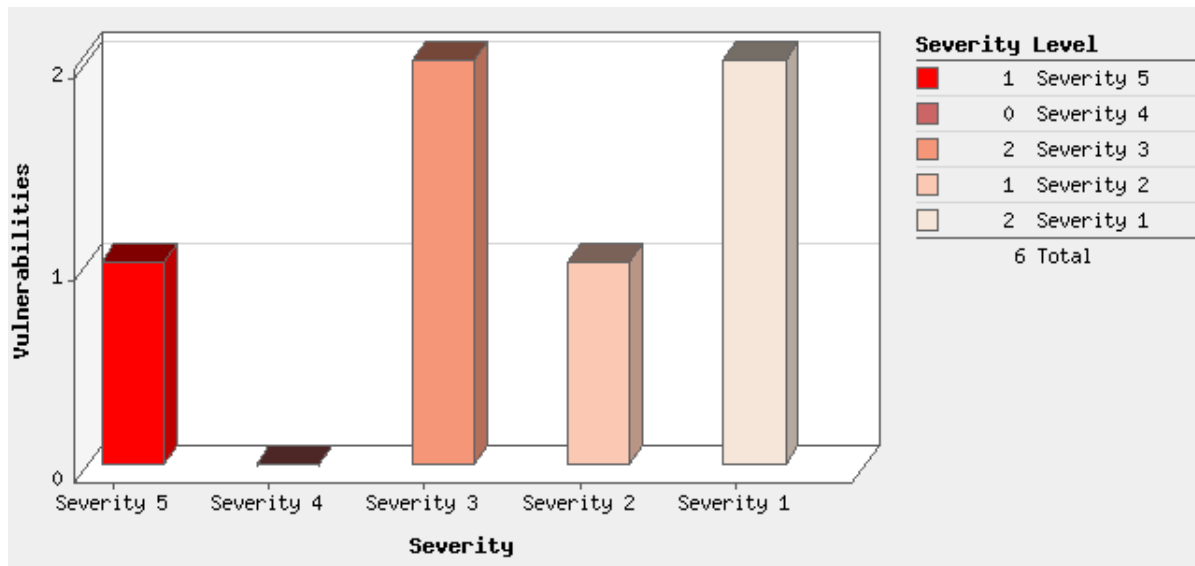
2.5

Business Risk

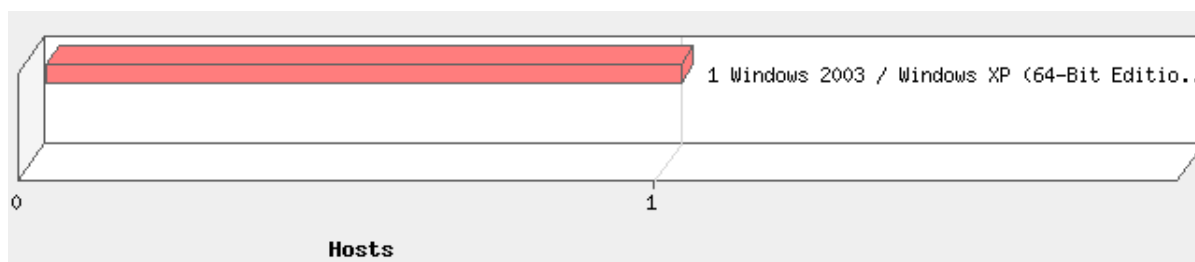


12/100

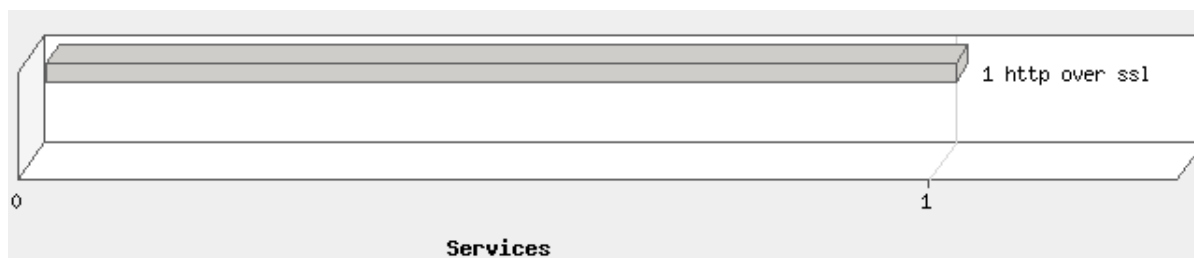
Severity



Operating Systems Detected



Service Detected



Detailed Results

xxx.xxx.xxx.xxx

Windows 2003 / Windows XP (64-Bit Edition)

Vulnerabilities Total

6

Security Risk



2.5

Vulnerabilities (6)



5 Microsoft Windows Graphics Rendering Engine WMF Format Code Execution (MS06-001)

New

QID: 90289
Category: Windows
CVE ID: -
Vendor Reference: MS06-001
Bugtraq ID: 16074
Last Update: 01/02/2006

First Detected: ##/##/#### at ##:##:## Last Detected: ##/##/#### at ##:##:## Times Detected: 1

THREAT:

Microsoft Windows supports the Windows Metafile (WMF) image format. WMF is a 16-bit image format that contains vector and bitmap information. Microsoft Windows WMF graphics rendering engine is affected by a remote code execution vulnerability. The cause of this issue is currently unknown.

The problem presents itself when a user views a malicious WMF formatted file, triggering the vulnerability when the engine attempts to parse the file. Any code execution that occurs will be with SYSTEM privileges due to the nature of the affected engine.

It should be noted that viewing a malicious file in Windows Explorer may automatically trigger this issue. Microsoft Windows XP is considered to be vulnerable at the moment. It is likely that other Windows operating systems are affected as well.

IMPACT:

This issue could be exploited remotely through any means that would allow an attacker to transmit the malicious image to a user, including through a malicious Web site and HTML email or embedding it in an Office document. Attacks could also occur by enticing an unsuspecting user to visit a remote file share hosting the file. User interaction is required in remote attack scenarios.

A local attacker could also exploit this issue to gain elevated privileges without any user interaction. It is noted that any application that is used to view the affected image type may present an attack vector.

SOLUTION:

Please refer Microsoft Bulletin MS06-001 for more information and instructions on installing the patch.

Microsoft has rated this update as Critical.

RESULT:

No results available



SSL Server Supports Weak Encryption Vulnerability

port 443/tcp over SSL

New

QID: 38140
 Category: General remote services
 CVE ID: -
 Vendor Reference: -
 Bugtraq ID: -
 Last Update: 11/03/2006

First Detected: ##/##/#### at ##:##:## Last Detected: ##/##/#### at ##:##:## Times Detected: 1

THREAT:

The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server.

SSL encryption ciphers are classified based on encryption key length as follows:

HIGH - key length larger than 128 bits
 MEDIUM - key length equal to 128 bits
 LOW - key length smaller than 128 bits

Messages encrypted with LOW encryption ciphers are easy to decrypt. Commercial SSL servers should only support MEDIUM or HIGH strength ciphers to guarantee transaction security.

The following link provide more information about this vulnerability:

SSL 3.0 Specification

Please note that this detection only checks for weak cipher support at the SSL layer. Some servers may implement additional protection at the data layer. For example, some SSL servers and SSL proxies (such as SSL accelerators) allow cipher negotiation to complete but send back an error message and abort further communication on the secure channel. This vulnerability may not be exploitable for such configurations.

IMPACT:

An attacker can exploit this vulnerability to decrypt secure communications without authorization.

SOLUTION:

Disable support for LOW encryption ciphers.

Apache

Typically, for Apache/mod_ssl, httpd.conf or ssl.conf should have the following lines:

```

SSLProtocol -ALL +SSLv3 +TLSv1
SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

```

IIS

How to Control the Ciphers for SSL and TLS on IIS (IIS restart required)

How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll (Windows restart required)

How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services (Windows restart required)

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 WEAK CIPHERS					
DES-CBC-MD5	RSA	RSA	MD5	DES(56)	LOW
SSLv3 WEAK CIPHERS					
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW
TLSv1 WEAK CIPHERS					
EXP-RC4-MD5	RSA(512)	RSA	MD5	RC4(40)	LOW



SSL Server Has SSLv2 Enabled Vulnerability

port 443/tcp over SSL

New

QID: 38139
 Category: General remote services
 CVE ID: -
 Vendor Reference: -
 Bugtraq ID: -

Last Update: 23/02/2006

First Detected: ###/###/#### at ##.##.## Last Detected: ###/###/#### at ##.##.## Times Detected: 1

THREAT:

The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server.

There are known flaws in the SSLv2 protocol. A man-in-the-middle attacker can force the communication to a less secure level and then attempt to break the weak encryption. The attacker can also truncate encrypted messages.

These flaws have been fixed in SSLv3 (or TLSv1). Most servers (including all popular web-servers, mail-servers, etc.) and clients (including Web-clients like IE, Netscape Navigator and Mozilla and mail clients) support both SSLv2 and SSLv3. However, SSLv2 is enabled by default for backward compatibility.

The following links provide more information about this vulnerability:

SSL Server Security Survey
SSL 3.0 Specification

IMPACT:

An attacker can exploit this vulnerability to read secure communications or maliciously modify messages.

SOLUTION:

Disable SSLv2.

Typically, for Apache/mod_ssl, httpd.conf or ssl.conf should have the following lines:
SSLProtocol -ALL +SSLv3 +TLSv1
SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

How to disable SSLv2 on IIS : Microsoft Knowledge Base Article - 187498

RESULT:

No results available

    2 Account Brute Force Possible Through IIS NTLM Authentication Scheme port 443/tcp **New**

QID: 86693
Category: Web server
CVE ID: CVE-2002-0419
Vendor Reference: -
Bugtraq ID: 4235
Last Update: 30/01/2006

First Detected: ###/###/#### at ##.##.## Last Detected: ###/###/#### at ##.##.## Times Detected: 1

THREAT:

NTLM authentication is enabled on the Microsoft IIS Web server. This allows a remote user to perform account brute force by requesting a non-existing HTTP resource or an existing HTTP resource that does not actually require authentication. Requests would include the "Authorization: NTLM" field.

IMPACT:

If the host has an account lockout policy in place, a remote user may exploit this vulnerability to lockout a local user, provided that the name of the local user is known.

If the host does not have an account lockout policy in place, a remote user may exploit this vulnerability to brute force user passwords.

Note that the Windows user list may sometimes be obtained by exploiting other vulnerabilities. Windows also has a few easy-to-guess default names for built-in accounts: "Administrator" for administering the computer/domain, "Guest" for guest access, "IUSR_<MachineName>" for anonymous access to IIS, and "IWAM_<Machinename>" for IIS to start out of process applications. Here the machine name <Machinename> may be obtained via Windows UDP Netbios NS (port 137).

THREAT:

Microsoft IIS supports Basic and NTLM authentication. It has been reported that the authentication methods supported by a given IIS server can be revealed to an attacker through the inspection of returned error messages, even when anonymous access is also granted.

When a valid authentication request is submitted (for either method) with an invalid username and password, an error message is returned. This happens even if anonymous access to the requested resource is allowed.

IMPACT:

If this vulnerability is successfully exploited, a malicious user can learn what authentication method is used. This information can then be used in further intelligent attacks against the server, or in a brute force password attack against a known user name.

SOLUTION:

We are not currently aware of any vendor-supplied fixes for this issue. Please check Microsoft's Web site (<http://www.microsoft.com>) for the latest information.

RESULT:

NTLM

 1 Web Server Internal IP Address/Internal Network Name Disclosure Vulnerability port 443/tcp **New**

QID: 86247
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 12/03/2006

First Detected: yy/yy/yyyy at yy:yy:yy Last Detected: yy/yy/yyyy at yy:yy:yy Times Detected: 1

THREAT:

Some Web servers contain a vulnerability giving remote attackers the ability to attain your internal IP address or internal network name.

An attacker connected to a host on your network using HTTPS (typically on port 443) could craft a specially formed GET request from the Web server resulting in a 3XX Object Moved error message containing the internal IP address or internal network name of the Web server.

A target host using HTTP may also be vulnerable to this issue.

IMPACT:

Successful exploitation of this vulnerability results in the disclosure of your internal IP address or internal network name, which could then be used in further attacks against the target host.

SOLUTION:

There are no patches available at this time. Please contact your vendor for updates.

Workarounds:

For IIS Web Server:

Check the Microsoft article on how to set the Hostname instead of internal IP address for IIS.

For Apache Web Server:

Modify the Apache configuration file as follows:

- Set "ServerName" to a proper FQDN.

or

- Use module mod_rewrite to modify the 3xx error message returned by the server.

No workaround information is available for other Web servers at this time. Refer to your vendor for an appropriate workaround.

RESULT:

GET / HTTP/1.0

HTTP/1.1 200 OK

Content-Length: xx

Content-Type: text/html

Content-Location: https://xxx.xxx.xxx.xxx/index.htm

Last-Modified: xxx, xx xxx xxxx xx:xx:xx GMT

Accept-Ranges: bytes

ETag: "ZZZZZZZZZZZZZZZZ"

Server: Microsoft-IIS/6.0

X-Powered-By: ASP.NET

Date: yy. yy yy yyyy yy:yy:yy GMT






Connection: close

Appendices

Report Legend






Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
 1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
 2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
 3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
 4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
 5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Potential Vulnerability Levels




A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
 1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
 2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
 3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
 4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
 5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a

list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
 1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
 2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
 3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.