Remote Vulnerability Assessment Results

Executive Summary

<table>
<thead>
<tr>
<th>Test Result: Fail</th>
<th>Date: 2003-03-01</th>
<th>Target IP: 236.10.7.66</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test ID: 193764</td>
<td>Test Length: 45.83 Minutes</td>
<td>DNS Entry: No DNS entry</td>
</tr>
<tr>
<td>Total Risk: 51</td>
<td>Start Time: 02:02:51</td>
<td>Finish Time: 02:48:42</td>
</tr>
<tr>
<td>TCP/IP Fingerprint OS Estimate: Windows Millennium Edition (Me), Win 2000, or WinXP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The computer fails because a risk of 4 or more was found. Look in the Security Vulnerabilities section below for instructions to reduce your security risk.

Attackers typically use port scanning and security vulnerability testing to find security weaknesses on computers. This report provides information on each of these categories.

**Port Scan**

Attackers use a port scan to find out what programs are running on your computer. Most programs have known security weaknesses. Disable any unnecessary programs listed below.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Program</th>
<th>Status</th>
<th>Summary</th>
<th>Turn Off</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL</td>
<td></td>
<td>Firewall</td>
<td>Absent</td>
<td>Your computer does not appear to be behind a firewall. We recommend installing and using a properly configured firewall.</td>
<td></td>
</tr>
<tr>
<td>ICMP</td>
<td>Ping</td>
<td></td>
<td>Accepting</td>
<td>Your computer is answering ping requests. Hackers use Ping to scan the Internet to see if computers will answer. If your computer answers then a hacker will know your computer exists and your computer could become a hacker target. You should install a firewall or turn off Ping requests.</td>
<td>See Below</td>
</tr>
<tr>
<td>TCP</td>
<td>25</td>
<td>smtp</td>
<td>Open</td>
<td>Your computer is running SMTP (Simple Mail Transport Protocol). This can be a security risk since</td>
<td>See Below</td>
</tr>
<tr>
<td>Port</td>
<td>Service</td>
<td>Status</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>--------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>http</td>
<td>Open</td>
<td>Your computer appears to be running http software that allows others to view its web pages. If you don't intend this computer to allow others to view its web pages then turn this service off. There are many potential security vulnerabilities in http software. See Below</td>
<td></td>
<td></td>
</tr>
<tr>
<td>110</td>
<td>pop-3</td>
<td>Open</td>
<td>Some POP3 services are vulnerable to buffer overflows. Download latest version of your POP3 service from vendor. See Below</td>
<td></td>
<td></td>
</tr>
<tr>
<td>119</td>
<td>nntp</td>
<td>Open</td>
<td>The Network News Transfer Protocol (NNTP) service is open on your computer. Typically this service is not open by default. You should turn off this service if it is not required.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>135</td>
<td>loc-srv</td>
<td>Open</td>
<td>Typically opened by Windows NT RPC service (rpcss.exe). A denial of service attack can be used against port 135. This attack allows an attacker with minimal resources to cause a remote NT system to consume 100% CPU usage. See Below</td>
<td></td>
<td></td>
</tr>
<tr>
<td>139</td>
<td>netbios-ssn</td>
<td>Open</td>
<td>NetBIOS is a networking protocol used by Microsoft Windows to provide easy networking. If this port is open, any computer with Microsoft Windows can connect to yours and potentially use shared resources on your computer. This makes it possible for an attacker to copy, delete, or modify your data or install malicious programs on your computer. See Below</td>
<td></td>
<td></td>
</tr>
<tr>
<td>143</td>
<td>imap2</td>
<td>Open</td>
<td>Your computer appears to be running Interactive Mail Access Protocol Version 2 (IMAP2). This service generally does not encrypt data or authenticate users. This means the data transmitted by this service may be viewed by others and is not secure. See Below</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1026</td>
<td>LSA-or-nterm</td>
<td>Open</td>
<td>Your computer is responding to scans on this port. Port 1026 is often one of the first port used by the operating system for outbound connections, therefore, virtually any program that requests a port can be assigned one at this address. If you run netstat you will see if this port is open with a connection established.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Security Vulnerabilities**

An attacker probes your computer for weaknesses using vulnerability detection tools. The following section lists all security vulnerabilities detected on your computer.

Each vulnerability is ranked on a scale of 0 to 9, with 9 being critical. A risk of 4 or more will fail the test.
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Program</th>
<th>Risk</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>443</td>
<td>https</td>
<td>9</td>
<td>One or more copies of the 'iiscrack.dll' exploit were found, it is used to gain SYSTEM privileges on a web server already compromised through another method. One more DLL files were found which indicate the presence of the 'pwdump2.exe' password hash dumping tool. One more DLL files were found which indicate the presence of the 'pwdump3.exe' password hash dumping tool. One more DLL files were found which indicate the presence of the 'ServUFTPD' FTP server, commonly used by crackers to setup rogue FTP services on compromised hosts. One more copies of the 'info.exe' tool were found, this CGI application provides a large amount of information about the server remotely and is often installed by system crackers. Details: iiscrack.dll - /scripts/pwsdata.dll iiscrack.dll - /scripts/md5filt.dll iiscrack.dll - /scripts/pfexedll.dll iiscrack.dll - /msadc/iiscrack.dll - /msadc/httpodbc.dll iiscrack.dll - /msadc/idq.dll iiscrack.dll - /msadc/httpext.dll iiscrack.dll - /msadc/ssinc.dll iiscrack.dll - /msadc/mw3prt.dll iiscrack.dll - /msadc/author.dll iiscrack.dll - /msadc/admin.dll iiscrack.dll - /msadc/shhtml.dll iiscrack.dll - /msadc/sspfil.dll iiscrack.dll - /msadc/compfilt.dll iiscrack.dll - /msadc/pwsdata.dll iiscrack.dll - /msadc/md5filt.dll iiscrack.dll - /msadc/fpexedll.dll vnc - /scripts/vnchooks.dll vnc - /scripts/omnihread_rt.dll vnc - /msadc/vnchooks.dll vnc - /msadc/omnihread_rt.dll pwdump2.exe - /scripts/samdump.dll pwdump2.exe - /msadc/samdump.dll pwdump3.exe - /msadc/lsaext.dll pwdump3.exe - /msadc/lsaext.dll servuftpd - /scripts/jsavf.dll servuftpd - /msadc/jsavf.dll info.exe - /scripts/info.exe info.exe - /msadc/info.exe</td>
</tr>
<tr>
<td>TCP</td>
<td>25</td>
<td>Smtp</td>
<td>7</td>
<td>There is a buffer overflow when this MTA is issued the 'HELO' command passed by an argument that is too long. This problem may allow an attacker to execute arbitrary code on this computer, or to disable your ability to send or receive emails.</td>
</tr>
<tr>
<td>TCP</td>
<td>443</td>
<td>https</td>
<td>4</td>
<td>It is possible to browse the information of the OWA server by accessing as an anonymous user with the following URL: <a href="http://www.example.com/exchange/root.asp?acs=anon">http://www.example.com/exchange/root.asp?acs=anon</a> After this access, the anonymous user can search for valid users in the OWA server and can enumerate all users by accessing the following URL: <a href="http://www.example.com/exchange/finduser/details.asp?obj=XXX">http://www.example.com/exchange/finduser/details.asp?obj=XXX</a> (where XXX is a string of 65 hexadecimal numbers) Data that can be accessed by an anonymous user may include: usernames, server names, email name accounts, phone numbers, departments, office, management relationships... This information will help an attacker to make social engineering attacks with the knowledge gained. This attack can be easily automated since, even if direct access to search is not possible, you only need the cookie given on the anonymous login access. Administrators might be interested in consulting the following URL: <a href="http://support.microsoft.com/support/exchange/content/whitepapers/owa">http://support.microsoft.com/support/exchange/content/whitepapers/owa</a> guide.doc</td>
</tr>
<tr>
<td>TCP</td>
<td>139</td>
<td>netbios-ssn</td>
<td>4</td>
<td>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$ Please see <a href="http://msos.securepoint.com/cgi-bin/get/smetrics-0204/50/1.html">http://msos.securepoint.com/cgi-bin/get/smetrics-0204/50/1.html</a> All the smb tests will be done as &quot;/&quot; in domain.</td>
</tr>
<tr>
<td>TCP</td>
<td>139</td>
<td>netbios-ssn</td>
<td>4</td>
<td>The domain SID could be used to enumerate the names of the users of this domain. (we only enumerated users name whose ID is between 1000 and 1020 for performance reasons) This gives extra knowledge to an attacker, which is not a good thing: - Administrator account name : Administrator (id 500) - Guest account name: Guest (id 501) - IWAM_MAIN (id 1000) - IUSR_MAIN (id 1001) - MAIN$ (id 1002)</td>
</tr>
<tr>
<td>TCP</td>
<td>139</td>
<td>netbios-ssn</td>
<td>4</td>
<td>The guest user belongs to groups other than guest users or domain guests. As guest should not have any privilege, you should fix this.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Port</td>
<td>Service</td>
<td>Risk Factor</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
<td>-----------</td>
<td>-------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TCP</td>
<td>139</td>
<td>netbios-ssn</td>
<td>Medium</td>
<td>The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols. <strong>Solution</strong>: filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14). <strong>Risk Factor</strong>: Low. <strong>CVE</strong>: CAN-1999-0524.</td>
</tr>
<tr>
<td>TCP</td>
<td>139</td>
<td>netbios-ssn</td>
<td>Low</td>
<td>The following accounts are disabled: Guest To minimize the risk of break-in, permanently disabled accounts should be deleted. <strong>Risk Factor</strong>: Low.</td>
</tr>
<tr>
<td>TCP</td>
<td>25</td>
<td>Ssmtp</td>
<td>Low</td>
<td>This detects the http-rpc-epmap service by connecting to the port 593 and processing the buffer received. This endpoint mapper provides CIS (COM+ Internet Services) parameters like port 135 (epmap) for RPC. <strong>Solution</strong>: Deny incoming traffic from the Internet to TCP port 593 as it may become a security threat in the future, if a vulnerability is discovered. For more information about CIS: <a href="http://msdn.microsoft.com/library/en-us/dndcom/html/cis.asp">http://msdn.microsoft.com/library/en-us/dndcom/html/cis.asp</a> <strong>Risk Factor</strong>: Low. <strong>CVE</strong>: CAN-1999-0524.</td>
</tr>
<tr>
<td>TCP</td>
<td>593</td>
<td>unknown</td>
<td>Low</td>
<td>The host SID can be obtained remotely. Its value is: YOURDOMAIN:5-21-1682732203-3904416635-2002596334 An attacker can use it to obtain the list of the local users of this host. <strong>Solution</strong>: filter the ports 137 to 139 and 445. <strong>Risk Factor</strong>: Low <strong>CVE</strong>: CAN-2000-1200. <strong>Solution</strong>: Install an antivirus / upgrade it.</td>
</tr>
<tr>
<td>ICMP</td>
<td>0</td>
<td>general/icmp</td>
<td>Medium</td>
<td>The domain SID can be obtained remotely. Its value is: YOURDOMAIN:5-21-1682732203-3904416635-2002596334 An attacker can use it to obtain the list of the local users of this host. <strong>Solution</strong>: filter the ports 137 to 139 and 445. <strong>Risk Factor</strong>: Low <strong>CVE</strong>: CAN-2000-1200. <strong>Solution</strong>: Install an antivirus / upgrade it.</td>
</tr>
<tr>
<td>TCP</td>
<td>139</td>
<td>netbios-ssn</td>
<td>Medium</td>
<td>The host SID can be obtained remotely. Its value is: YOURDOMAIN:5-21-1682732203-3904416635-2002596334 An attacker can use it to obtain the list of the local users of this host. <strong>Solution</strong>: filter the ports 137 to 139 and 445. <strong>Risk Factor</strong>: Low <strong>CVE</strong>: CAN-2000-1200. <strong>Solution</strong>: Install an antivirus / upgrade it.</td>
</tr>
<tr>
<td>TCP</td>
<td>139</td>
<td>netbios-ssn</td>
<td>Low</td>
<td>The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols. <strong>Solution</strong>: filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14). <strong>Risk Factor</strong>: Low. <strong>CVE</strong>: CAN-1999-0524.</td>
</tr>
<tr>
<td>TCP</td>
<td>139</td>
<td>netbios-ssn</td>
<td>Medium</td>
<td>The following accounts have never logged in: Guest Unused accounts are very helpful to hacker. <strong>Solution</strong>: suppress these accounts. <strong>Risk Factor</strong>: Medium.</td>
</tr>
<tr>
<td>TCP</td>
<td>25</td>
<td>Ssmtp</td>
<td>Medium</td>
<td>The test server sent several emails containing the EICAR test strings in them to the postmaster of the remote SMTP server. The EICAR test string is a fake virus which triggers anti-viruses, in order to make sure they run. The test server attempted to e-mail this string five times, with different codings each time, in order to attempt to fool the remote anti-virus (if any). If there is an antivirus filter, these messages should all be blocked. To determine if the remote host is vulnerable, see if any mail arrived to the postmaster of this host <strong>Solution</strong>: Install an antivirus / upgrade it <strong>Risk Factor</strong>: Low.</td>
</tr>
<tr>
<td>TCP</td>
<td>593</td>
<td>unknown</td>
<td>Medium</td>
<td>This detects the http-rpc-epmap service by connecting to the port 593 and processing the buffer received. This endpoint mapper provides CIS (COM+ Internet Services) parameters like port 135 (epmap) for RPC. <strong>Solution</strong>: Deny incoming traffic from the Internet to TCP port 593 as it may become a security threat in the future, if a vulnerability is discovered. For more information about CIS: <a href="http://msdn.microsoft.com/library/en-us/dndcom/html/cis.asp">http://msdn.microsoft.com/library/en-us/dndcom/html/cis.asp</a> <strong>Risk Factor</strong>: Low. <strong>CVE</strong>: CAN-1999-0524.</td>
</tr>
<tr>
<td>TCP</td>
<td>80</td>
<td>http</td>
<td>Low</td>
<td>The remote web server type is: Microsoft-IIS/5.0. <strong>Solution</strong>: You can use urlscan to change reported server for IIS.</td>
</tr>
<tr>
<td>TCP</td>
<td>443</td>
<td>https</td>
<td>Low</td>
<td>A TLSv1 server answered on this port.</td>
</tr>
<tr>
<td>TCP</td>
<td>443</td>
<td>https</td>
<td>Low</td>
<td>A web server is running on this port through SSL.</td>
</tr>
<tr>
<td>TCP</td>
<td>443</td>
<td>https</td>
<td>Low</td>
<td>Web server responds to bad URL with: HTTP/1.1 401 Access Denied</td>
</tr>
<tr>
<td>TCP</td>
<td>443</td>
<td>https</td>
<td>Low</td>
<td>Some web servers are [mis]configured in that they do not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map or search page instead. This script will retrieve the default page which is issued when a non-existent file is requested, and will use this information to minimize the risks of false positives for the other tests. <strong>Solution</strong>: You can use urlscan to change reported server for IIS. <strong>CVE</strong>: CVE-2000-0708.</td>
</tr>
<tr>
<td>TCP</td>
<td>0</td>
<td>general/tcp</td>
<td>Medium</td>
<td>Nmap found that this host is running Windows Millennium Edition (Me), Win 2000, or WinXP.</td>
</tr>
<tr>
<td>UDP</td>
<td>0</td>
<td>general/udp</td>
<td>Medium</td>
<td>For your information, here is the traceroute to 174.27.34.1 : x.x.x.x 192.41.65.161.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Port</td>
<td>Service</td>
<td>Status</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
<td>---------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>80</td>
<td>http</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>80</td>
<td>http</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>143</td>
<td>imap</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>636</td>
<td>ldaps</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

A web server is running on this port.

Web server responds to bad URL with: HTTP/1.1 401 Access Denied

Some web servers are [mis]configured in that they do not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map or search page instead. This script will retrieve the default page which is issued when a non-existent file is requested, and will use this information to minimize the risks of false positives for the other tests.

Here is the SSLv2 server certificate:

Certificate: Data: Version: 3 (0x2) Serial Number: 05:69:2e:72:00:00:00:00:00:06 Signature Algorithm: sha1WithRSAEncryption Issuer: Email=administrator@carolina.org, C=US, ST=Carolina, L=Columbia, O=YourCo, OU=main office, CN=Main.YourCO.com Validity Not Before: Jun 21 20:23:23 2002 GMT Not After : Jun 21 20:33:22 2004 GMT Subject: CN=main.Yourco.com Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus:

66.35.175.6 10.8.4.106

TCP 80 http 0

Here is the list of available SSLv2 ciphers: RC4-MD5 EXP-RC4-MD5 RC2-CBC-MD5 EXP-RC2-CBC-MD5 DES-CBC-MD5 DES-CBC3-MD5

The SSLv2 server offers 4 strong ciphers, but also 0 medium strength and 2 weak "export class" ciphers. The weak/medium ciphers may be chosen by an export-grade or badly configured client software. They only offer a limited protection against a brute force attack. **Solution:** disable those ciphers and upgrade your client software if necessary.

This TLSv1 server also accepts SSLv2 connections. This TLSv1 server also accepts SSLv3 connections.

The service closed the connection after 0 seconds without sending any data. It might be protected by some TCP wrapper.

A TLSv1 server answered on this port.
Here is the SSLv2 server certificate:

Certificate Data:

Version: 3 (0x2) Serial Number: 05:69:2e:72:00:00:00:00:00:06 Signature Algorithm: sha1WithRSAEncryption
Issuer: Email=admin@yourco.com, C=US, ST=Carolina, L=Columbia, O=yourco.com, OU=main office, CN=main. yourco.com

Subject: CN=main. yourco.com

Subject Public Key Info:
Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit)
Exponent: 65537 (0x10001)
Exponent: 65537 (0x10001) X509v3 extensions:
CRL Distribution Points: URI:ldap:///CN=main.
yourco.com,CN=main,CN=CDP,CN=Public%20KeyServices,CN=Services,CN=Configuration,DC=carolina,DC=adf?certificateRevocationList?base?objectclass=cRLDistributionPoint URI:http://main. yourco.com /CertEnroll/main. yourco.com crl
Authority Information Access: CA Issuers - URI:ldap:///CN=main.
yourco.com,CN=AIA,CN=Public%20KeyServices,CN=Services,CN=Configuration,DC=carolina,DC=adf?certificateRevocationList?base?objectclass=cRLDistributionPoint URI:http://main. yourco.com /CertEnroll/main. yourco.com _main. yourco.com.crt

The SSLv2 server offers 4 strong ciphers, but also 0 medium strength and 2 weak "export class" ciphers. The weak/medium ciphers may be chosen by an export-grade or badly configured client software. They only offer a limited protection against a brute force attack.

Solution: disable those ciphers and upgrade your client software if necessary.

This TLSv1 server also accepts SSLv2 connections. This TLSv1 server also accepts SSLv3 connections.

The remote native lan manager is: Windows 2000 LAN Manager The remote Operating System is: Windows 5.0 The remote SMB Domain Name is: YourDomain

The following accounts have never changed their password: IWAM_MAIN IUSR_MAIN To minimize the risk of break-in, users should change their password regularly.

An NNTP server is running on this port.

The service closed the connection after 0 seconds without sending any data. It might be protected by some TCP wrapper.

A pop3 server is running on this port.

The remote POP server banner is: +OK Microsoft Exchange POP3 server version
### TCP 995 pop3s 0
- The service closed the connection after 0 seconds without sending any data. It might be protected by some TCP wrapper.

### TCP 25 smtp 0
- An SMTP server is running on this port. Here is its banner: 220 main. yourco.com ESMTP Server (Microsoft Exchange Internet Mail Service 5.5.2653.13) ready.

### TCP 25 smtp 0
- Remote SMTP server banner: 220 main. yourco.com ESMTP Server (Microsoft Exchange Internet Mail Service 5.5.2653.13) ready.

### TCP 1029 unknown 0
- There is a CIS (COM+ Internet Services) on this port. Server banner: ncacn_http/1.0.

### TCP 1058 unknown 0
- This port was detected as being open by a port scanner but is now closed. This service might have been crashed by a port scanner or by some information gathering plugin.

### TCP 1059 unknown 0
- This port was detected as being open by a port scanner but is now closed. This service might have been crashed by a port scanner or by some information gathering plugin.

### TCP 1061 unknown 0
- This port was detected as being open by a port scanner but is now closed. This service might have been crashed by a port scanner or by some information gathering plugin.

### TCP 1062 unknown 0
- This port was detected as being open by a port scanner but is now closed. This service might have been crashed by a port scanner or by some information gathering plugin.

### TCP 1135 unknown 0
- There is a CIS (COM+ Internet Services) on this port. Server banner: ncacn_http/1.0.

### TCP 1222 unknown 0
- There is a CIS (COM+ Internet Services) on this port. Server banner: ncacn_http/1.0.

### TCP 1232 unknown 0
- There is a CIS (COM+ Internet Services) on this port. Server banner: ncacn_http/1.0.

### TCP 1265 unknown 0
- There is a CIS (COM+ Internet Services) on this port. Server banner: ncacn_http/1.0.

### TCP 1580 unknown 0
- This port was detected as being open by a port scanner but is now closed. This service might have been crashed by a port scanner or by some information gathering plugin.

### TCP 1581 unknown 0
- This port was detected as being open by a port scanner but is now closed. This service might have been crashed by a port scanner or by some information gathering plugin.

### TCP 1852 unknown 0
- This port was detected as being open by a port scanner but is now closed. This service might have been crashed by a port scanner or by some information gathering plugin.

### TCP 3269 unknown 0
- A TLSv1 server answered on this port.

### TCP 3269 unknown 0
- Here is the list of available SSLv2 ciphers: RC4-MD5 EXP-RC4-MD5 RC2-CBC-MD5 EXP-RC2-CBC-MD5 DES-CBC-MD5 DES-CBC3-MD5.

### TCP 3269 unknown 0
- The SSLv2 server offers 4 strong ciphers, but also 0 medium strength and 2 weak "export class" ciphers. The weak/medium ciphers may be chosen by an export-grade or badly configured client software. They only offer a limited protection against a brute force attack. **Solution:** disable those ciphers and upgrade your client software if necessary.

### TCP 3269 unknown 0
- This TLSv1 server also accepts SSLv2 connections. This TLSv1 server also accepts SSLv3 connections.

### TCP 666 unknown 0
- The service closed the connection after 0 seconds without sending any data. It might be protected by some TCP wrapper.

---

**To turn off ICMP replies:**

---
Windows Workstation

1. We recommend installing a personal firewall.
2. Try Tiny or Zonealarm

Windows Server

1. We recommend changing the configuration of your router or firewall to deny ICMP replies.

Linux Redhat 6.2

If using iptables:

1. As "root" enter the following command
2. `iptables -A INPUT -p icmp -m state --state NEW -j DROP`

   If using ipchains:

1. As "root" enter the following command
2. `ipchains -A input -p icmp --icmp-type echo-request -j DENY`

To close port 25 (smtp):

Windows 2000 - follow these steps:

2. Double click on desired machine then
3. Highlight SMTP Virtual Server
4. On title bar select Action then Stop

Windows XP - follow these steps:

1. Click on Start ? Control Panel
2. Double-click Add/Remove Programs
3. Click on Internet Information Services (IIS) ? Details
4. Make sure SMTP Service is unchecked
5. Click OK
6. Click Next

Linux Redhat 6.2

To Permanently disable:

1. `cd /etc/rc.d/init.d/
2. ./sendmail stop
3. mv sendmail no.sendmail`

To temporarily stop service:

1. `cd /etc/rc.d/init.d/
2. ./sendmail stop`
To close port 80:

Windows 98 - follow these steps:
2. Select Personal Web Manager
3. Under Main click Stop

Windows NT 4.0 - follow these steps:
2. On title bar select Computer ? Services
3. Select World Wide Web Publishing Service then click on Stop

Windows 2000 - follow these steps:
1. Click on Start ? Programs ? Administrative Tools ? Internet Services Manager
2. Double click on desired machine then
3. Highlight "Web Site"
4. On title bar select Action then Stop

Linux Redhat 6.2
To Permanently disable:
1. cd /etc/rc.d/init.d/
2. ./httpd stop
3. mv httpd no.httpd

To temporarily stop service:
1. cd /etc/rc.d/init.d/
2. ./httpd stop

For additional information go to Beckman Institute

To close port 110 (Pop-3):

Linux Redhat 6.2
1. Edit the file /etc/inetd.conf
2. Comment out the line starting with pop-3 by placing a hash # mark at the beginning of the line
3. Type killall -HUP inetd to load new settings

To close port 135 (epmap/loc-srv):

Windows 98
USE THIS FIX AT YOUR OWN RISK!

(may cause some programs to not work.
for more info go to cexx)

1. Click on "Start" ? "Find" ? "Files or Folders"
2. Type "rpcss.exe" into name box
3. Select "Find Now"
4. Right-click on file then select "rename"
5. Rename rpcss.exe to rpc.old
6. Repeat steps 4 & 5 if more than one rpcss.exe exists

Windows NT 4.0
Information not available.

Windows 2000

1. Download Patch
2. Info - Microsoft Security Bulletin
3. Info - Microsoft FAQ's

*Note: Some users may wish to install a personal firewall instead of disabling port 135*

To close port 139 (netbios-nsession):

Windows 98 - follow these steps:

1. Click on "Start" ? "Settings" ? "Control Panel"
2. Double click on "Network"
3. Select the "Configuration" tab
4. Scroll down network component list and find and select item starting with "TCP/IP -> ..."
5. Then select "Properties"
6. Select the "Bindings" tab
7. Deselect each option then click "Ok"
8. Ignore windows warning message "have not selected any drivers to bind with." Click "No"
9. Repeat steps 4-8 until each instance of "TCP/IP -> ..." is changed
10. Restart computer
    (ports 137 & 138 will also be closed)

Windows NT 4.0 - follow these steps:

1. Click on "Start" ? "Settings" ? "Control Panel"
2. Double click on "Network"
3. Select the "Bindings" tab
4. Scroll down "Show bindings for:" list and select "all protocols"
5. Double click on "WINS Client(TCP/IP)"
6. Highlight your network adapter
7. Click on "Disable"
    (ports 137 & 138 will also be closed)

Windows 2000 - follow these steps:

1. Click on "Start" ? "Settings" ? "Network and Dial-up Connections"
2. Double click on "Local Area Network"
3. Click on "Properties"
4. Highlight "Internet Protocol(TCP/IP)"
5. Click on "Properties"
6. Click on "Advanced"
7. Select the "WINS" tab
8. Select "Disable Netbios over TCP/IP"
9. Click "Ok" (ports 137 & 138 will also be closed)

**Windows XP** - follow these steps:

1. Click on "Start" ? "Control Panel"
2. Double click "Network connections"
3. Click on "Properties"
4. Double click Internet Protocol (TCP/IP)
5. Click "Advanced"
6. Click on "WINS"
7. Click "Disable netbios over TCP/IP"
8. Click "Ok" on all of the windows

**Linux Redhat 6.2**

To Permanently disable:

1. cd /etc/rc.d/init.d/
2. smb stop
3. mv smb no.smb
   (ports 137 & 138 will also be closed)

To temporarily stop service:

1. cd /etc/rc.d/init.d/
2. smb stop
   (ports 137 & 138 will also be closed)

For additional information go to [Beckman Institute](#)

*Note: Some users may wish to install a personal firewall instead of disabling port 139*

**To close port 143 (imap/imap2):**

**Linux Redhat 6.2**

1. Edit the file /etc/inetd.conf
2. Comment out the line starting with imap by placing a hash # mark at the beginning of the line
3. Type killall -HUP inetd to load new settings

For additional information go to [Beckman Institute](#)
information transmitted via the Red Cliff Solutions service, and shall not be responsible or liable for any use or application of the information contained in this report.