Global Information Assurance Certification Paper

Case Study:

From Rogue Web Server to Security Compliant

By Wai Ling Yuen
v1.4b

Abstract/Summary

What happens when your company discovers that you have a web server that does not meet any of the company's security requirements? They threaten to pull the plug.

My client tasked my team and I to develop a Web Server that would provide automatic site publishing for the average non-technical user. He didn't define any requirements for the hardware or software platform. We were the experts, 'Just get it done.' And we did. For 'security' purposes, we installed a separate T1 and physically placed the web server on a separate network infrastructure. If it's not on the internal company infrastructure, we won't have to worry about complying with company web server standards. Or so we thought.

When our company discovered our 'rogue' server, we had to comply with all company-defined security requirements OR they would pull the plug. The following will be a detailed account of our experiences in getting our rogue web server to satisfy the company's stringent security requirements, and the vulnerabilities we discovered along the way.

Before

Early Monday morning, I was called into a meeting with my boss. He had just received a call indicating that the company has discovered our rogue web server because of the domain name registration information. The situation had to be immediately rectified. Our rogue server either HAD to comply with company security standards OR we would have to house the web sites on an internal company server through which we would lose all administrative control.

My team consisted of a network administrator, a senior software developer and myself, the IT Manager. I would be the one assigned to system security. And the rest of the team would assist me in supporting the implementations.

We had configured two (2) identical machines. One was the Domain Controller (DC) for local workstations and hosted Active Directory, Backups and Anti-virus. It was not a public server. We used the DC as our development server for the websites as well. In addition to being a development server, the DC was a 'backup replica' of the web server (production server). All testing was performed on the DC before we updated the files on the production web server. The web server was a standalone server that was not a part of the domain and had a public face.

The two servers were running on a Compaq Proliant 3000, Pentium III/500 with Windows 2000 Advanced Server as the Operating System. Windows 2000 was not yet a company-sanctioned operating system due to insufficient in-house

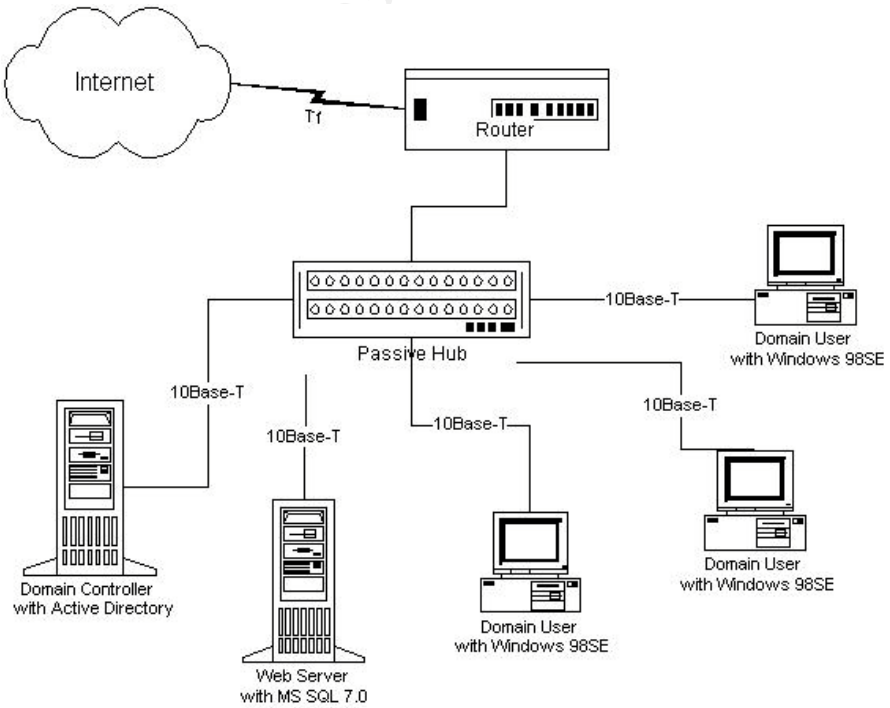
testing but, Microsoft had officially released it for at least a year. I chose Windows 2000 because it was more secure than Windows NT 4.0.

Also running on the 2000 Servers was Internet Information Services (IIS) version 5.0 and Microsoft SQL Server version 7.0.[1]

The company had an Intranet that was behind a firewall with very limited access to Internet users. Users were unable to FTP at all, which made downloading drivers impossible. Thus, we setup our 'rogue' server on it's own T1 and outside of the firewall. A Cisco 2500 router (configured by the Internet Service Provider (ISP)) and a 12-port 3COM passive hub and we were in business. We did not install a firewall immediately because we had no practical experience and very little knowledge about firewalls. We planned to install one in the near future after some training and research.

At a minimum, we did install Symantec Norton Antivirus Corporate Edition version 7.50[2]on the DC to potentially prevent any known virus infections. A quarantine server was setup for detected viruses that could not be cleaned. Automatic updates for up-to-date virus patterns were configured and pushed out to all local workstations and the web server. Also installed were the latest Service Packs for Windows 2000 from Microsoft (SP3). We were diligent about staying patched.

The following is a diagram that illustrates our network configuration:



[1] Microsoft Corporation
[2] Symantec Corporation

The risks were minimal. Our services were known to a select few. On a busy day, we would have six users logged into our Web Site simultaneously. Our data was not sensitive. A loss of data would have a negative effect, but it was not a critical business interruption that would cost the company monetarily.

We ensured that the Internet search engine web crawlers would bypass our web address because we did not want free publicity. We were pretty safe. If no one knows about us, no one will attack us. We had virus protection and Network Address Translation on the router in place and our operating systems were patched with the latest service packs and hot fixes.

During

We were wrong.

As the success of our website grew, the security group became aware of our rogue server. We were immediately asked to bring the server/website into the company infrastructure. This would require us to relinquish our administrative rights to the server and website. Updates to the website would have to go through the Web Services Group and upon approval, updates would be posted. We would also have to redesign our web pages to conform to our company's Web Guide.

This was unacceptable to our client. The nature of our website required updates to be posted immediately. Aware of the politics, it would take days, even weeks, to get modifications to the website posted if we relinquished control. Also, the Web Guide was very limiting and would not allow for creativity. Colors had to be blue-based, no frames, no flash, and no video. Graphics were limited to 'approved' photos and company logos.

We had meetings upon meetings to convey the need for our Server to be exempted from company requirements. If it is physically separate from our company Intranet, we should not have to comply. Their argument was that our website was portraying itself as a 'company' website. This was valid. We did conduct business as our company on the website. Thus, the user's perception would be that our website was a company website and therefore should comply with company standards.

We finally arrived at a compromise. We would have to apply all company defined security settings on our server and website. We would then be allowed to continue to manage the server on a separate T1 as well as maintain complete administrative control. Besides, the increase in utilization of our website had increased our vulnerability and risks. Data loss would be more critical but it

would still not have a monetary effect on the company's business process. The cost of data loss would be the time it took for my team and I to recover the data.

A third-party security audit was performed on our server to identify the flaws in our system. Basically, they blew holes in our 'security' system. There was a laundry list.

After our audit, we were provided with the company requirements on the above security issues. Even WE could see that our network was lacking in physical and system security. We set out to implement the system security changes immediately. THEN we would be safe and secure. The server would not be targeted by the company as non-compliant or 'rogue'. We could then continue to conduct business as usual with our Web Services.

Based on our obvious vulnerabilities, we set out to enhance our overall protection. Implementation of our company security requirements began with applying stringent security settings in Windows 2000. The other issues were not immediately addressed. Key steps taken to enhance Windows 2000 security were as follows:

	Before Audit	After Audit
Physical Security	Our servers were behind a wall by our LAN Administrator's desk The door was never locked There was a window and an Air Conditioner No Sprinklers but we had a Fire Extinguisher for electrical fires Key card access is required for entry into the building, but not during regular business hours	Door to the Network Admin office/Server room would be locked after hours A request for a 'secure' server room to be built is in place
Windows 2000 Advanced Server Operating System Configuration	Active Directory enabled (on DC only) User account passwords never expired Passwords were not required to be complex	Active Directory enabled (on DC Only) Only Administrators (up to 3) user account passwords never expired; all other users required to change their password every 60 days

Windows 2000 Advanced Server Operating System Configuration (cont'd)	No Local Policy Settings (all default settings) No Domain Policy Settings (all default settings) All default services installed were running Server setups were documented Tape Backups were performed nightly Contingency Plan did not exist Disaster Recovery Documentation did not exist Security Policy did not exist NetBIOS was enabled	Passwords are required to be complex and minimum 8 characters Applied Policy Settings Enforce Password History Password Aging enabled Account Lockout Policies enabled Auditing logons, object access, privilege use etc. enabled Modified User Access Rights Security Options set to limit logons, timeouts, floppy drive and CDROM access, etc. Services not necessary for our Web Server application was disabled including: Remote Access Connection Sharing; Routing and Remote Access; Telnet; FTP Server setups are documented Tape Backups are performed nightly Contingency Plan created Disaster Recovery Procedures established and documented Security Policy created NetBIOS disabled on the Web Server NetBIOS is still enabled for Legacy machines to connect on DC

Router Configuration	All ports were open No firewall Network Address Translation (NAT) was configured	All ports were open No firewall Network Address Translation (NAT) was configured
Workstations	All running Windows 98 SE Private IP Addressing All running Norton Antivirus	All running Windows 98 SE Private IP Addressing All running Norton Antivirus

There was little we could do about the physical security since we had to make do with our existing building structure and limitations. I was comfortable that we had reduced our vulnerability and risk significantly. We still had some issues, because we did not restrict file-level access but they were not critical based on our data sensitivity. We were not aware of any tools that could further lockdown our web server. We had no experience with router configurations either.

Still, no one on our team had received any formal security training. The Windows 2000 Servers were more secure than they ever were. We did not realize the impact vulnerabilities on our web server would have on our LAN. We had neglected to see that our server was a gateway to our Intranet.

First, there was an incident that was reported to our company's security department that we were issuing scans on someone's website. The IP was traced back to us and I received a call and the email complaint:

```
Complaint:

Hello!

This is a failed port 445 attack:

Active System Attack Alerts
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
Nov 18 17:49:21 jbarchuk portsentry[861]: attackalert: SYN/Normal scan
from host: zzzzzz.net/192.168.1.50 to TCP port: 445
Nov 18 17:49:21 jbarchuk portsentry[861]: attackalert: Host
192.168.1.50
has been blocked via wrappers with string: "ALL: 192.168.1.50"
Nov 18 17:49:26 jbarchuk portsentry[861]: attackalert: SYN/Normal scan
from host: zzzzzz.net/192.168.1.50 to TCP port: 445
Nov 18 17:49:26 jbarchuk portsentry[861]: attackalert: Host:
zzzzzz.net/192.168.1.50 is already blocked Ignoring
Nov 18 17:49:26 jbarchuk portsentry[861]: attackalert: SYN/Normal scan
from host: zzzzzz.net/192.168.1.50 to TCP port: 445
Nov 18 17:49:26 jbarchuk portsentry[861]: attackalert: Host:
```

```
zzzzzz.net/192.168.1.50 is already blocked Ignoring
Nov 18 17:49:26 jbarchuk portsentry[861]: attackalert: SYN/Normal scan
from host: zzzzzz.net/192.168.1.50 to TCP port: 445
Nov 18 17:49:26 jbarchuk portsentry[861]: attackalert: Host:
zzzzzz.net/192.168.1.50 is already blocked Ignoring
Nov 18 17:49:26 jbarchuk portsentry[861]: attackalert: SYN/Normal scan
from host: zzzzzz.net/192.168.1.50 to TCP port: 445
Nov 18 17:49:26 jbarchuk portsentry[861]: attackalert: Host:
zzzzzz.net/192.168.1.50 is already blocked Ignoring
Nov 18 17:49:26 jbarchuk portsentry[861]: attackalert: SYN/Normal scan
from host: zzzzzz.net/192.168.1.50 to TCP port: 445
Nov 18 17:49:26 jbarchuk portsentry[861]: attackalert: Host:
zzzzzz.net/192.168.1.50 is already blocked Ignoring
Nov 18 17:49:47 jbarchuk portsentry[861]: attackalert: SYN/Normal scan
from host: zzzzzz.net/192.168.1.50 to TCP port: 445
Nov 18 17:49:47 jbarchuk portsentry[861]: attackalert: Host:
zzzzzz.net/192.168.1.50 is already blocked Ignoring
Nov 18 17:49:50 jbarchuk portsentry[861]: attackalert: SYN/Normal scan
from host: zzzzzz.net/192.168.1.50 to TCP port: 445
Nov 18 17:49:50 jbarchuk portsentry[861]: attackalert: Host:
zzzzzz.net/192.168.1.50 is already blocked Ignoring
Nov 18 17:49:57 jbarchuk portsentry[861]: attackalert: SYN/Normal scan
from host: zzzzzz.net/192.168.1.50 to TCP port: 445
Nov 18 17:49:57 jbarchuk portsentry[861]: attackalert: Host:
zzzzzz.net/192.168.1.50 is already blocked Ignoring

My IP address is 192.168.1.26. The timestamp(s) are ET -0500 and are
very accurate.

Please deal with this scripkiddie as appropriate.

Thanks much. Have a :) day!
```

We had to see if our system was infected with something that would go out and scan other servers. We knew WE weren't doing the scanning. We resented being referred to as a "scripkiddie".

Working with our security personnel, we ran virus scans; we checked logs but we did not see any evidence of an intrusion; we ran checks on the router to see if there were unusual amounts of activity. There were no indications that our system had been compromised. The security personnel reported that perhaps we had been spoofed. "Besides, 'the attack' lasted for only about 30 seconds." I was still concerned, but the security personnel said the 'case was closed'. Spoofing seemed to be a lot of trouble for a hacker to go through and not do anything with it. It was probably a virus from us that was trying to infect others. But, we could not track down a source. We would watch very closely.

A couple of weeks later, my network administrator received a call from someone whose server was scanned by our system IP address on November 30th. It sounded similar to the previous issue we had. As a result, he checked out our

server and notified us that we had insecure BIOS shares. Our ports 137-139 and 445 were wide open and he could see our shared resources (specifically, one of our printers). This was a very frightening and eye-opening discovery. A normal person with access to tools could actually see our Intranet with very little effort!

He also suggested that all of our computers on the subnet were infected. Yes, we had NetBIOS because all of our workstations were still Windows 98SE machines. But, we still could not find any evidence of the source although it was obvious there was something. Our security personnel did some more checking but they didn't have a lot to go on.

The auditors did not recommend shutting down unused ports on the router in their initial reports. We didn't even know HOW. I quickly called some router resources for assistance on how to close our vulnerable ports on the router. In order to prevent any further NetBIOS related security breaches, we did a quick fix on the router and blocked ports 137, 138, 139, and 445 on all in-bound traffic.

Two months later, one of development workstations running 2000 Server was hit with the NIMDA32@mm virus. It was detected early by our anti-virus software and we were able to clean it off of the infected machine before it could do any damage to our network and servers.[3]

Enough.

My network administrator and I signed up with SANS Institute to take the SANS Security Essentials Course so that we could protect our system properly. Apparently, what we had done was not enough. We needed to know more.

We learned in class was that we were barely protected at all! The current configurations of our physical and logical environment were not enough to protect us from the world of creative hackers:

Virus Protection was based on legacy logic and should not be our major defense mechanism.[4]
Windows 98 workstations were completely vulnerable.[5]
Our physical security was lacking.[6]
We still had exposed ports on the router[7]
A firewall is a must-have

[3] http://service1.symantec.com/SUPPORT/ent-security.nsf/552ba2f7636bedf088256818006f78bf/33e72f71cb05c61688256b3f00006951?OpenDocument
[4] Cole, Chapter 23, pp.1076-1083
[5] Cole, Chapter 25, pp.1138-1139
[6] Cole, Chapter 6, pp. 275-281
[7] Cole, Chapter 5, pp. 243-250

During the weeklong training, security paranoia slowly crept in. I was SURE that someone was hacking into our system as I sat in class. We were STILL vulnerable! I had no idea the many ways a hacker could penetrate a vulnerable system and wreak havoc.

Fortunately, it was not so. As soon as we go back to work the next week, we implemented some more security settings on our network.

In addition to the ones already disabled (20, 21, 23, 137-139 and 445) we disabled other unused ports via a standard Access-list on the router (port 79 inbound and 137-139 outbound). The data utilization of our network will allow us to implement a reflexive ACL and block all traffic in and out EXCEPT for HTTP.

Things were calm until our web server was infected with the Trojan.ircbounce virus.[8] We were alerted through our Virus Protection program. We immediately applied the fixes and deleted the infected files. Fortunately, it was discovered early enough for us to expunge before any damage had been done to our system. We still have not been able to determine HOW the machine was infected, because we have complex password requirements on the machine.

A couple of months later, the Slammer virus attacked and my husband's company was hit. Their routers were flooded with traffic and their operations came to a standstill until his network operations group isolated the virus and removed it. The only good thing was that it happened late Friday evening and it took them all day Saturday to repair the damage. Fortunately, we were running MS SQL 7.0 and were not affected. But, I immediately closed UDP inbound on port 1434 on our router just in case.[9] Another close call.

Yet, another month later, we received another router vulnerability notification. The attack would send specifically crafted IPv4 packets to an interface on a vulnerable device and allow the intruder to cause the device to stop processing packets destined for that interface.[10] We got the upgrade to the IOS and installed it on our router as recommended. We also closed down ports 53, 55, 77, and 103 on the router as and added security measure.[11]

AFTER

There are still vulnerabilities but I think we have reduced our risk substantially. SANS training and resources on the Internet, have helped me see that we still have more to do to reduce our risk even further. The whole project was a great learning experience for me.

---

[8] http://securityresponse.symantec.com/avcenter/venc/data/trojan.ircbounce.html

[9] http://www.cisco.com/en/US/products/hw/iad/ps497/products_security_advisory09186a0080133399.shtml

[10] http://www.cert.org/advisories/CA-2003-15.html

[11] http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

We had always viewed security as a way to limit access to data and because our data is not sensitive, we didn't think there was a big risk. I've discovered that the sensitivity of the data only played a small role in determining criticality of the data. The 'integrity' of the information and the system it is running on is what might be compromised if we didn't protect our system. The loss of data was not the only issue, whereas the loss of functionality would be more critical.

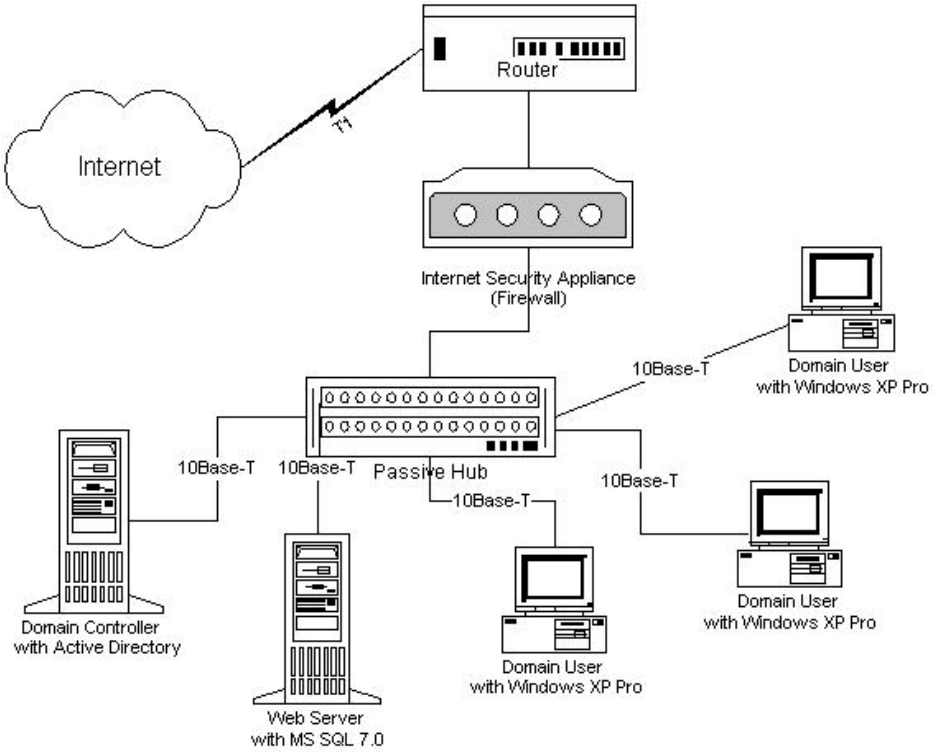
We must also remember that security is defined on several levels; from Physical, to Operating System, to File levels. Vulnerabilities and risks have to be evaluated and addressed at all levels. And each level of security requires different tools and security measures. For example, something as simple as disabling your local floppy drive on the fileserver could potentially prevent a hacker from booting off of a floppy and resetting your admin password.

The attacks we experienced clearly illustrated to us the level of effort needed to recover from any downtime. Data loss may not have been a major cost issue, but the time and manpower spent on recovery was and could be significant. THAT is where it would 'cost' the company. I think we've been very lucky so far, but we may not be so lucky next time.

As we continue our efforts, we are implementing more layers of protection to enhance our security.

We have purchased a firewall appliance that we have installed between the router and our network. It is configured with NAT and also takes the load off of the access-list on the router. In hindsight, the firewall would have been able to give us a little more information on those attacks that we were accused of. We might have been able to trace the packets to determine the source. We could configure our router to do the same things that a firewall does, but with a lot more effort and knowledge. Although the firewall is merely a filtering and monitoring system for packets, it is another level of protection. The more layers, the harder it is for the hackers.

The following is a diagram of our network configuration as it is today:



We have replaced all of our Windows 98 machines with XP Professional Operating Systems. In essence, eliminating NetBIOS on the network and reducing our vulnerability and risk.

We are in the process of building a secure Server Room to address our physical security issues with a door that has a numeric keypad, for authorized personnel only. The room will reduce fire, flood, and electrical threats and regulate temperature controls.

We will continue to stay up to date on the security patches, hot fixes and regular data backups. The recent viruses and worms that targeted known vulnerabilities and could have been avoided if proper patches were installed certainly illustrated the importance of maintaining up-to-date service packs and hot fixes.

After the SANS Training Seminar, we have discovered that there are many resources on the Internet that will provide detailed information and alerts about new viruses and worms.

The seminar also provided a variety of tools for intrusion detection and tracking. A tool like Ethereal[12] might have helped us during the so-called attacks that we were doing. Similar tools are available for detecting attacks on your ports, vulnerability scanners, encryption methods, etc. With the Internet, many tools to aid in your defense against attackers are available. We will use these resources to stay on top of the hacker game.

I hope that in the near future, we will be protected enough to be **pro**active rather then being reactive as we have been in the past. Of course, there are always new vulnerabilities that we don't know about and we cannot be COMPLETELY protected, but we will do our best to apply as many levels of protection as possible to act as deterrents. We will utilize the plethora of resources and tools available to stay one step ahead of the hackers. One can only hope!

[12] Cole, Chapter I, pp. 3-1 through 3-32

REFERENCES

Cole, Eric; Fossen, Jason; Northcutt, Stephen; Pomeranz, Hal. SANS Security Essentials with CISSP CBK version 2.1, Volume One. USA: SANS Press, 2003. pp. 275-281, pp 243-250.

Cole, Eric; Fossen, Jason; Northcutt, Stephen; Pomeranz, Hal. SANS Security Essentials with CISSP CBK version 2.1, Volume Two. USA: SANS Press, 2003. pp. 1076-1083, pp 1138-1139.

Cole. SANS Security Essentials Hands-On Workbook. USA: SANS Institute, 2003. pp. 3-1 to 3-3-32.

Microsoft Corporation. "Microsoft Solution for Securing a Windows 2000 Server". 5 February 2003. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/secwin2k/default.asp

Symantec Corporation. "How to clean Nimda from a partially or totally infected network when Norton AntiVirus Corporate Edition is installed". ID:2002011116032748. 11 July 2003. URL: http://service1.symantec.com/SUPPORT/ent-security.nsf/552ba2f7636bedf088256818006f78bf/33e72f71cb05c61688256b3f00006951?OpenDocument

Symantec Corporation. "Trojan.IrcBounce". 26 November 2002. URL: http://securityresponse.symantec.com/avcenter/venc/data/trojan.ircbounce.html

Cisco Systems. "Cisco Security Notice: MS SQL Worm Mitigation Recommendations". 13 February 2003. URL: http://www.cisco.com/en/US/products/hw/iad/ps497/products_security_advisory09186a0080133399.shtml

Carnegie Mellon Software Engineering Institute. "CERT® Advisory CA-2003-15 Cisco IOS Interface Blocked by IPv4 Packet". 17 July 2003. URL: http://www.cert.org/advisories/CA-2003-15.html

Cisco Systems. "Cisco Security Advisory: Cisco IOS Interface Blocked by Ipv4 Packets". ID: 44020. 02 August 2003. URL: http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml