Global Information Assurance Certification Paper

Augmenting Security with a Utility Firewall – A Case Study in the Benefits of Low-Cost Firewalls

Monte Coulter
August 2004
GSEC Practical Assignment
Version 1.4b, option 2

Abstract

Low cost firewalls can be used in a utilitarian fashion to help solve many problems, as long as they are programmed securely and monitored on an ongoing basis. These firewalls should only be installed with proper planning, a strong understanding of the technologies utilized, and a thorough security review following installation. It is easy to view low cost firewalls as an all around security solution; however these firewalls should only be added to networks when the overall design of the infrastructure prevents the addition of services with adequate security. As referenced in this document, adequate security means a balance of threat and vulnerability in relation to risk. Noted in the formula: Risk=Threat x Vulnerability. [1 – SANS Institute, Defense in-Depth]

This paper addresses three IT requirements I solved by installing a WatchGaurd Firebox III 1000 firewall for Company A, which provided greater remote system access with a high level of security. More specifically, subsequent to installation, security scans were conducted using the Nessus security scanning tool and showed minimal vulnerability.

Background

Over the past five years, Company A (a publicly traded company) had experienced 20 percent growth per year. The growth added an additional 300 employees, two new manufacturing facilities, and two new sales offices. As a result, IT applications were forced to grow to meet the demand of both the users and the outside customer base. While the company grew, the number of IT employees remained static, forcing IT to re-tool and re-train to work more effectively and efficiently. Outsourcing was required to maintain the service levels and technologies required by the expanding business.

IT security at Company A was almost non-existent at the beginning of the five years. At the beginning of this growth period, the only document pertaining to security was a weakly written Acceptable Use Policy, which was not effectively enforced. URL screening was not in place, a wide-open port blocker was in use as the Company's firewall, no password policy was in place, anti-virus software was not being used, and general network security was not considered.

With governmental agencies imposing additional and more stringent regulations with the introduction of HIPAA and Sarbanes-Oxley, the growing onslaught of computer viruses and hacking ease, and the higher visibility the company was obtaining in the world, the necessity to tighten IT systems at Company A became apparent. In a growing trend, companies, starting at the CEO and CFO level, had the general idea that data had to be secure before they attested to the validity of it.[2] Similarly, Company A's focus turned to security.

In the next few years, Company A implemented a Telco managed Internet firewall, a Telco managed remote access solution utilizing VPN technologies, password policies, access control lists to restrict network traffic between departments, anti-virus software, and among many other things, a software patch management system. With the introduction of these systems, Company A experienced increased security posture and awareness. The growth also created a need for higher employee mobility.

Existing Configuration:

The Telco managed Internet service and Telco managed remote access solutions for Company A were implemented a year previous to the Firebox 1000 installation. The implementations consisted of two separate Internet connections, one for each service. Both of these configurations are illustrated in the network drawing included in this document.

> The first of these configurations, the Telco managed Internet service, included a managed firewall, URL filtering, managed intrusion detection system, and several routers with various functions (details are omitted due to irrelevance in this paper). Company A uses the managed Internet service for Web browsing and Web server hosting. The Company's default IP route is pointed to this solution forcing all Internet traffic or unknown destination IP addresses out through the managed firewall and URL filtering.
>
> The second solution, the Telco managed remote access solution, included a router for terminating the serial WAN link and a Nortel Contivity 1600 VPN concentrator running 3DES encryption. Once a VPN connection was made to the Company, the connected computer was fenced into the company network, i.e., split tunneling was not allowed. "In a VPN context, 'split tunneling' is the term used to describe a multiple-branch networking path. A tunnel is split when some network traffic is sent to the VPN server and other traffic is sent directly to the remote location without passing through the VPN server."[3] All network communication on the connected computer was directed towards the company network. This design was successful in stopping real-time "piggyback" attacks on of the Company's computers from the Internet, but simultaneously allowed malicious virus or worm code an unchecked avenue onto the Company network. If the connected computer had become infected prior to connection, the Company had no means of mitigating the infection before the connection was established. Thus, allowing the malicious code access to the Company's network. In fact, Company A experienced a Blaster worm infection in August 2003 from a home computer connecting on a VPN connection. At the time of this Blaster infection, all company owned PCs and laptops ran anti-virus software.

The Problems:

Remote Access:

The Telco managed remote access solution was implemented. Subsequently, users requiring access were provided with remote access to Company resources. The VPN remote access system replaced a RAS solution provided by a modem bank with permissions granted by Windows NT Domain security. Initially, only traveling salespersons, IT personnel, and executives with laptops were allowed this remote access. As time passed, users with home computers were granted access and the VPN client was installed under the assumption that access would be used exclusively for company business. Once more home users obtained broadband or equivalent Internet access at home, the threat of system vulnerabilities and viruses increased for the Company network. A new system for allowing employee owned computers access to company resources was required to mitigate these new security risks.

Business to Business VPN Connections:

One of Company A's IT projects required configuration assistance from an outside remote support company. It was more cost-effective for this outside company to connect remotely to support Company A's IT systems. Remote access using the VPN configuration was proposed but turned down due to the lack of split tunneling. The support company needed access to their own network resources, while configuring and supporting Company A's projects. Several support persons at the support company required access also, which would require extra remote access accounts. Company A and the support company did not want to simply join the networks due to the reliance on each other to maintain patch levels, security, and anti-virus software. Company A needed a means of safely allowing the support company to connect remotely and support their systems.

Wireless Access:

The mobility advantages and the popularity of wireless connectivity both in home and corporate networks created a need for wireless access at Company A's corporate offices. The Company's offices were in a multi tenant office space requiring a solid security model for the wireless configuration to keep unauthorized users off of the company's network. Also, lack of IT personnel experience and time to implement complicated LEAP or PEAP security models presented another problem in maintaining a secure wireless network. Wireless technologies were already being used at Company A's manufacturing facilities

without standardized configuration policies between them. A standard for installing wireless had to be written and had to be both secure enough and flexible enough to meet the needs of the corporate office and the manufacturing facilities.

The Solution

Company A had three problems that were interrelated and seemed to only be solved by three separate solutions. Instead, I chose to implement a WatchGaurd Firebox III 1000 firewall. The Firebox 1000 is a stateful inspection packet filtering firewall with built in application layer proxies. The built in proxies can "Examine content to ensure it matches protocol standards. For example, attacks that send metacharacters intended to trick the victim machine, or attacks that overwhelm the machine with too much data. Proxies can spot illegal characters or overlong fields and block them."[4] Also built in, the Firebox has VPN functionality and intrusion detection. The VPN client is capable of utilizing DES and 3DES encryption with MD5 and SHA1 authentication. (MD5 is capable of 128 bit hash, while SHA1 is capable of 160 bit [5]) I decided to implement this particular firewall because of the ease of management, it's relative low-cost, and the all-in-one functionality it offered.

Home Computer Remote Access Solution:

Utilizing the Firebox's mobile user VPN functionality, all approved home PC users were set up with a profile for remotely connecting to Company A's network. Each user was then given a copy of the VPN client with a preset key for installation. The profile was setup to utilize 3DES encryption and MD5 authentication. MD5 was chosen for its reported better performance over SHA1. Either authentication level would have sufficed.

On the firewall, I restricted the user profiles to port 3389 for remote desktop connections inbound to Company A's network. This restricted the type of connection the home computers were allowed to make through the firewall once securely connected via VPN. All computers in Company A's corporate office run Microsoft Windows XP and upon approval for VPN access, have "Remote Desktop" turned on their work PC. The employees are required to know the IP address of their office PC in the office in order to make a connection from their home computers. Split-tunneling is allowed on the employee's home computer under the assumption that Company A has no need or interest in knowing what the employee does on their personal computer. Only traffic destined on port 3389 will traverse the VPN connection.

This solution works best for the Company based on the premise that higher access levels increases employee productivity. The use of home PCs for work purposes appeared as an untapped resource to Company A.

The level of risk associated with home PC access dramatically decreased from the previous solution of unprotected connections. I found no known port 3389 vulnerabilities during my research for this solution when used with Windows XP, except for DOS attacks. This solution relies on a solid password policy to keep users from logging into other user's computers remotely. Also, the previous solution's one step logon process could have been easily accessed by unauthorized users sitting on the employee's home computer, possibly unleashing havoc on Company A's network. The new solution requires the VPN connection to be made; followed by the start of a remote desktop connection to the employee's specific work computer; then logging in with their domain username and password, thereby creating extra security measures.

I also investigated use of Microsoft Terminal Server rather than the work PCs with remote desktop enabled, but found MS Terminal Server software licensing prohibitive. Per Microsoft's licensing agreements, every profile required a license of the software that the profile would be able to run, requiring 50 additional copies of Microsoft Office. The use of MS Terminal Server would have allowed me to restrict the VPN clients down to one internal LAN IP, thereby tightening security even more.

Business to Business VPN Connections:

To meet business requirements and restrictions, I utilized the Firebox's Branch Office VPN functionality to setup a business to business VPN connection between Company A and the support company. Using the firewall's blocking functionality, I was able to restrict the support company to the specific server requiring support.

During initial setup, the support company's IT personnel and I realized that both companies used the common 10.1.1.0/24 network. We were able to agree on an IP address not in use on either LAN, deciding on 172.16.100.50. I used the Firebox's Network Address Translation (NAT) functionality and statically NAT'ed 10.1.1.4 (the remotely supported server) to 172.16.100.50.

We then setup a static branch office VPN connection between Company A and the support company, again using MD5 for authentication and 3DES for encryption. I further restricted access from the support company on port 3389. This restricted the support company from doing anything other than creating a Microsoft Terminal Server session running on the remotely supported server.

With this configuration, Company A and the support company were mutually protected from each other in the event a virus or worm outbreak occurred. The support company only needs access when maintenance or configuration assistance is needed on the remotely supported server. The branch office tunnel is simple to tear down upon completion of remote support, decreasing one more avenue into the network when unused.

Wireless Access Solution:

First, I wrote a standard installation policy for wireless access points for Company A. The standard detailed the expected wireless access point security levels for manufacturing facilities and offices in multi-tenant office buildings. Manufacturing facilities utilized wireless for different applications as compared to sales offices, thereby requiring a different level of security. Those facilities not currently at or above the security standard are required to fully implement a compliant wireless network by December 2004.

For Company A's corporate office, I used the Firebox's optional interface and set it up as a DMZ with a class c IP subnet. The office layout and size required three wireless access points, which were wired into the DMZ. To secure the wireless access points, MAC address filtering was setup, SSID broadcasting was turned off, DHCP was turned off, and 128 bit WEP encryption was used.

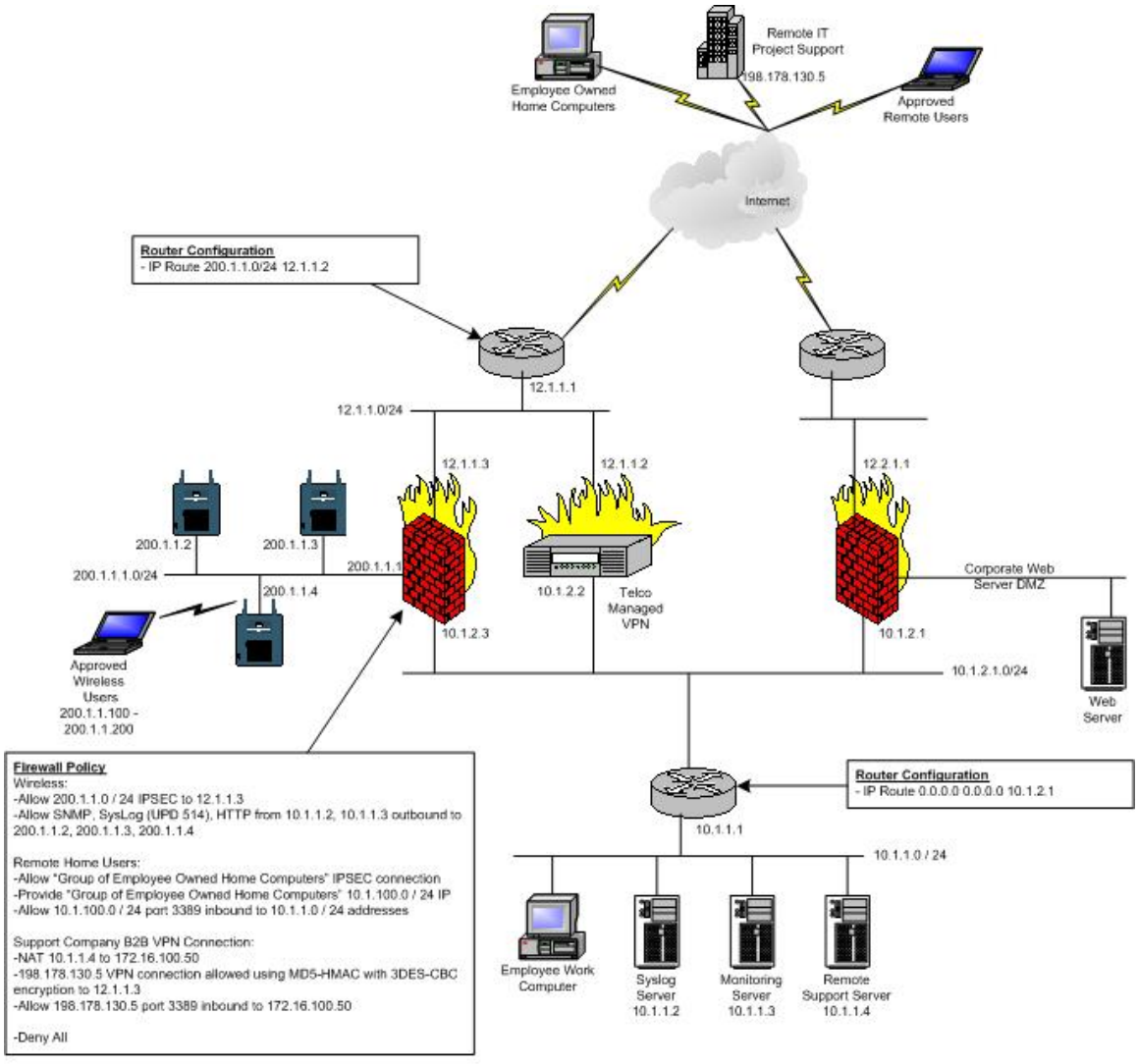
On the Firebox, I then restricted the wireless subnet access to all IP addresses except the public interface of the Telco managed remote access solution. Further, the firewall restricts all access from the DMZ to IPSec ports 500, 4500, and 50. For management of the wireless access point, I utilized one of the FireBox's application proxies, HTTP, restricting access from two servers on Company A's LAN outgoing to the three wireless access points in the DMZ. I also allowed udp port 514 (syslog) inbound from the three wireless access points to the company's syslog server to ensure Company A received log events from these access points.

Together, all of these security measures require the a wireless user to know the SSID, have a correct static IP address, have an approved and added MAC address in the access points, and create a VPN tunnel into the network. [1] [6] Although most of these measures taken solely could be broken by an inexperienced hacker, the measures together create a layered effect and would typically discourage seasoned hackers, moving them on to look for a less hardened target. The HTTP management access makes web based management of the access points easier and syslog access ensures Company A

[1] This configuration almost mirrors the configuration discussed in Eric Peeters' GSEC Practical assignment, Wireless security beyond WEP and WPA, however is a coincidence and provides support for my design. I have listed his paper as a reference because of the similarity between the designs.

captures events. The risk level associated with this configuration is almost equivalent to that of having the Telco managed remote access solution visible on the Internet.

Post Configuration Network Drawing



IP Address have been changed from actuals.

Post Implementation Security Scans [2]

Detailed logs from the Nessus scans follow the scan summaries.

From Company A's LAN - Summary:

Nessus scans were run from the syslog server's IP address of 10.1.1.2. One of the three wireless access points was down for repair during the scan. The two remaining access points and the firewall were scanned and the following reports show:

- The wireless access points at 200.1.1.2 and 200.1.1.3 have port 80 open.
- 200.1.1.2 had one security warning stating it may be vulnerable to a sequence number approximation bug.
- 200.1.1.1 and 10.1.2.3 (the WatchGaurd Firebox) returned only a HTTPS NIDS evasion function notice.

As a result of the scans from the Company A LAN, I asked the wireless network admin to rectify the possible HTTP security hole without limiting management functionality to the Company A LAN management server. The NIDS evasion notice stemmed from an error in the scan configuration.

From the Firebox DMZ – Summary:

Nessus scans were run from the Firebox DMZ with an IP address of 200.1.1.15. One of the three access points, 10.1.1.2, was found vulnerable with several open services. The Firebox did not respond to the Nessus scan.

- Telnet was enabled and Nessus was able to capture the access point's logon banner.
- Nessus identified port 80 being enabled and the access point running a web server.
- The access point did not discard TCP SYN packets with the FIN flag set.
- Nessus identified the device as a Cisco access point running IOS version 12.2.8.
- The access point answered to an ICMP timestamp request.

I furnished this additional information to the wireless network admin to aid in his steps to secure the access points.

From the Internet - Summary:

Nessus scans were run from the Internet against the Firebox. The following was reported.

- HTTPS NIDS evasion functions are enabled.
- The Firebox is enabled to be a VPN server.

[2] IP addresses have been changed from actuals.

The Firebox responded as expected, as a VPN server. Again, the NIDS evasion notice stemmed from an error in the scan configuration.

From Company A's LAN – Detail

Nessus Scan Report
This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan Details	
Hosts which where alive and responding during test	4
Number of security holes found	0
Number of security warnings found	1

Host List	
Host(s)	**Possible Issue**
200.1.1.3	Security note(s) found
200.1.1.2	Security warning(s) found
200.1.1.1	Security note(s) found
10.1.2.3	Security note(s) found

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
200.1.1.3	http (80/tcp)	Security notes found
200.1.1.3	general/tcp	Security notes found
200.1.1.3	general/udp	Security notes found

Security Issues and Fixes: 200.1.1.3		
Type	**Port**	**Issue and Fix**
Informational	http (80/tcp)	An unknown service is running on this port. It is usually reserved for HTTP Nessus ID : 10330
Informational	http (80/tcp)	An unknown service runs on this port. It is sometimes opened by this/these Trojan horse(s): 711 trojan (Seven Eleven) AckCmd Back End Back Orifice 2000 Plug-Ins Cafeini CGI Backdoor Executor God Message God Message 4 Creator Hooker IISworm MTX NCX Noob Ramen Reverse WWW Tunnel Backdoor RingZero RTB 666 Seeker WAN Remote Web Server CT WebDownloader Unless you know for sure what is behind it, you'd better check your system *** Anyway, don't panic, Nessus only found an open port. It may

		*** have been dynamically allocated to some service (RPC...) Solution: if a trojan horse is running, run a good antivirus scanner Risk factor : Low Nessus ID : 11157
Informational	general/tcp	HTTP NIDS evasion functions are enabled. You may get some false negative results Nessus ID : 10890
Informational	general/tcp	Remote OS guess : (null) CVE : CAN-1999-0454 Nessus ID : 11268

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
200.1.1.2	http (80/tcp)	Security notes found
200.1.1.2	general/tcp	Security warning(s) found
200.1.1.2	general/udp	Security notes found

Security Issues and Fixes: 200.1.1.2		
Type	**Port**	**Issue and Fix**
Informational	http (80/tcp)	A web server is running on this port Nessus ID : 10330
Warning	general/tcp	The remote host might be vulnerable to a sequence number approximation bug, which may allow an attacker to send spoofed RST packets to the remote host and close established connections. This may cause problems for some dedicated services (BGP, a VPN over TCP, etc...). Solution : See http://www.securityfocus.com/bid/10183/solution/ Risk factor : Medium CVE : CAN-2004-0230 BID : 10183 Nessus ID : 12213
Informational	general/tcp	HTTP NIDS evasion functions are enabled. You may get some false negative results Nessus ID : 10890
Informational	general/tcp	Remote OS guess : (null) CVE : CAN-1999-0454 Nessus ID : 11268

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
200.1.1.1	general/tcp	Security notes found
200.1.1.1	general/udp	Security notes found

Security Issues and Fixes: 200.1.1.1		
Type	**Port**	**Issue and Fix**
Informational	general/tcp	HTTP NIDS evasion functions are enabled.

	You may get some false negative results Nessus ID : 10890

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
10.1.2.3	general/tcp	Security notes found
10.1.2.3	general/udp	Security notes found

Security Issues and Fixes: 10.1.2.3		
Type	**Port**	**Issue and Fix**
Informational	general/tcp	HTTP NIDS evasion functions are enabled. You may get some false negative results Nessus ID : 10890

This file was generated by Nessus, the open-sourced security scanner.

From the Firebox DMZ - Detail:

Nessus Scan Report	
This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.	
Scan Details	
Hosts which where alive and responding during test	1
Number of security holes found	0
Number of security warnings found	4

Host List	
Host(s)	**Possible Issue**
200.1.1.2	Security warning(s) found

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
200.1.1.2	telnet (23/tcp)	Security warning(s) found
200.1.1.2	http (80/tcp)	Security notes found
200.1.1.2	bootps (67/udp)	No Information
200.1.1.2	bootpc (68/udp)	No Information
200.1.1.2	snmp (161/udp)	No Information
200.1.1.2	snmptrap (162/udp)	No Information
200.1.1.2	general/tcp	Security warning(s) found
200.1.1.2	general/udp	Security notes found
200.1.1.2	general/icmp	Security warning(s) found

Security Issues and Fixes: 200.1.1.2		
Type	**Port**	**Issue and Fix**
Warning	telnet (23/tcp)	The Telnet service is running. This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the telnet client and the telnet server. This includes logins and passwords.

		Solution: If you are running a Unix-type system, OpenSSH can be used instead of telnet. For Unix systems, you can comment out the 'telnet' line in /etc/inetd.conf. For Unix systems which use xinetd, you will need to modify the telnet services file in the /etc/xinetd.d folder. After making any changes to xinetd or inetd configuration files, you must restart the service in order for the changes to take affect. In addition, many different router and switch manufacturers support SSH as a telnet replacement. You should contact your vendor for a solution which uses an encrypted session. Risk factor : Low CVE : CAN-1999-0619 Nessus ID : 10280
Informational	telnet (23/tcp)	A telnet server seems to be running on this port Nessus ID : 10330
Informational	telnet (23/tcp)	Remote telnet banner : User Access Verification Username: Nessus ID : 10281
Informational	http (80/tcp)	A web server is running on this port Nessus ID : 10330
Warning	general/tcp	The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host. An attacker may use this feature to determine traffic patterns within your network. A few examples (not at all exhaustive) are: 1. A remote attacker can determine if the remote host sent a packet in reply to another request. Specifically, an attacker can use your server as an unwilling participant in a blind portscan of another network. 2. A remote attacker can roughly determine server requests at certain times of the day. For instance, if the server is sending much more traffic after business hours, the server may be a reverse proxy or other remote access device. An attacker can use this information to concentrate his/her efforts on the more critical machines. 3. A remote attacker can roughly estimate the number of requests that

		a web server processes over a period of time. Solution : Contact your vendor for a patch Risk factor : Low Nessus ID : 10201
Warning	general/tcp	The remote host does not discard TCP SYN packets which have the FIN flag set. Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules. See also : http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html http://www.kb.cert.org/vuls/id/464113 Solution : Contact your vendor for a patch Risk factor : Medium BID : 7487 Nessus ID : 11618
Informational	general/tcp	Nmap found that this host is running Cisco 801/1720 running 12.2.8 Nessus ID : 10336
Informational	general/tcp	Remote OS guess : Cisco 801/1720 running 12.2.8 CVE : CAN-1999-0454 Nessus ID : 11268
Warning	general/icmp	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. Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14). Risk factor : Low CVE : CAN-1999-0524 Nessus ID : 10114

This file was generated by Nessus, the open-sourced security scanner.

From the Internet - Detail:

Nessus Scan Report	
This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.	
Scan Details	
Hosts which where alive and responding during test	1
Number of security holes found	0
Number of security warnings found	1
Host List	

Host(s)	Possible Issue
12.1.1.3	Security warning(s) found

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
12.1.1.3	general/tcp	Security notes found
12.1.1.3	general/udp	Security notes found
12.1.1.3	isakmp (500/udp)	Security warning(s) found

Security Issues and Fixes: 12.1.1.3		
Type	**Port**	**Issue and Fix**
Informational	general/tcp	HTTP NIDS evasion functions are enabled. You may get some false negative results Nessus ID : 10890
Warning	isakmp (500/udp)	The remote host seems to be enabled to do Internet Key Exchange (IKE). This is typically indicative of a VPN server. VPN servers are used to connect remote hosts into internal resources. Solution: You should ensure that: 1) The VPN is authorized for your Companies computing environment 2) The VPN utilizes strong encryption 3) The VPN utilizes strong authentication Risk factor : Low Nessus ID : 11935

This file was generated by Nessus, the open-sourced security scanner.

References

1. SANS Institute Defense in-Depth 1.2, Track1 – SANS Security Essentials and the CISSP 10 Domains, January 2004, pgs 28-29.
2. Hurley, Edward. "Security and Sarbanes-Oxley." 25 September 2003. URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci929451,00.html (16 August 2004)
3. "Split Tunneling." 30 December 2003 URL: http://www.cites.uiuc.edu/vpn/splittunneling.html (16 August 2004)
4. "Products." URL: http://www.watchguard.com/products/proxy.asp (16 August 2004)
5. Shimonski, Robert J., Shinder, Debra Littlejohn., Shinder, Dr. Thomas W., Crasik-Henmi, Anne. Best Damn Firewall Book Period. Rockland, MA: Syngress, 2003. pg 582.
6. Peeters, Eric. Wireless security beyond WEP and WPA. SANS Institute. May 2004