

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Auditing a Checkpoint Firewall

GSNA Practical Assignment
Version 2.0

© SANS Institute 2000 - 2002, Author retains full rights.

Prepared by Paul Nelson
June 7, 2002

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 1 2
Foreword 2
System to be Audited 3
Risk 5
Current State of Practice 6
How can current methods and techniques be improved? 8
Assignment 2 – Audit Checklist 10
Assessment Process: 10
1. Conduct tests on the firewall 11
2. Conduct tests to verify the firewall rules in place 13
3. Verify that there are no additional network connections into ABC Company 16
4. Review the Checkpoint system configuration 18
5. Review the Sun operating system configuration 22
6. Review and test physical security 25
7. Review corporate security policies 27
Assignment 3: Conduct the Audit: 31
1. Test access to the firewall from the Internet and internal network 31
2. Test access to the DMZ network from the Internet and the internal network 33
3. Test access to the internal network from the Internet 37
4. War Dialing test on the ABC Company telephone lines 39
5. Scan the internal network 41
6. Review the Checkpoint system configuration 43
7. Review the Checkpoint rules 47
8. Review the Sun operating system configuration 49
9. Review and test physical security 56
10. Review corporate security policies 58
Is the system securable? 64
Is the system auditable? 64
Assignment 4 – Audit Report 66
Executive Summary 66
Audit Findings: 68
Appendix A - References 79
Appendix B – Checkpoint Firewall-1 Ports 80
Appendix C – Test Results 81
1. Firewall Tests: 81
2. Mail Server Tests: 82

Assignment 1

Foreword

The objective of this project is to provide an independent audit of a Checkpoint Firewall-1 that is in place at ABC Company. This firewall is primarily used by ABC Company

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

employees to access the Internet for business purposes, as well as for the exchange of electronic mail.

Access to the Internet used to be considered a luxury, only required by a select number of employees for web browsing. In today's electronic business world the Internet has become an essential business tool that many companies can not afford to do without. ABC Company is no exception, they depend on this Internet connection to perform daily work functions and heavily rely on electronic mail to communicate with their business suppliers and customers.

Along with the benefits of connecting to a world wide public network come a number of security issues and risks. The risk of unauthorized access from the Internet into a private network is a major concern, especially the stigma around the public exposure that your computer network has been hacked. An effective security program includes a defense in depth approach to security and requires much more than a firewall as the only layer of protection. Any firewall, no matter how advanced it's technology, is only as effective as the configuration and rules applied to it. This audit will identify the key risks associated with this firewall service, perform tests to verify whether the firewall is functioning securely as well as evaluate the administration processes in place to manage and monitor this critical security device.

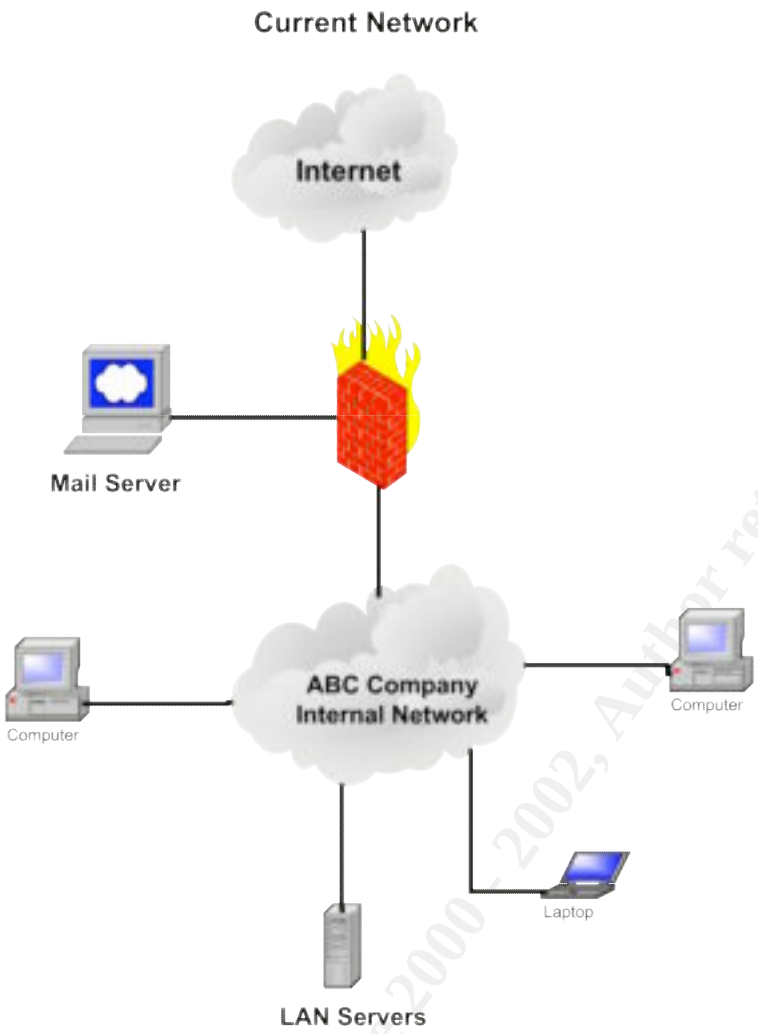
System to be Audited

ABC Company is a relatively small organization with 500-1000 employees located in Canada. Upon request they have provided some advance information regarding their computer network to maximize the efficiency of this audit.

During our initial discussions regarding this firewall audit the following conceptual diagram of the ABC Company computer network was created.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Internet connectivity is through a Checkpoint Firewall version 4.0 running on a Sun SPARCStation system and the Internet connection is through a high speed DBS circuit directly connected to the Ethernet port of the firewall. Connected to a separate port of the firewall in a Demilitarized Zone (DMZ) network is the corporate mail server that is used to send and receive all email messages.

The IP addresses from the Internet were also provided for this assessment. The firewall IP address is 142.162.10.10, while the IP address for the DMZ subnet is 10.10.10.0 subnet mask 255.255.255.248. The internal private network is 10.10.11.0 subnet mask 255.255.255.0. I am aware these are private IP and not addressable from the Internet, the addresses have been adjusted as requested by the client for confidentiality The actual addresses for both the DMZ network and internal network are all public subnets. For that reason, Network Address Translation (NAT) will not be addressed during this audit.

The network that hosts the mail server would be more accurately defined as a service network, rather than a demilitarized zone. However, since ABC Company refers to this network as a DMZ, this description will be used throughout the audit.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Risk

A risk profile has been developed for ABC Company to identify key threats and risks that face this organization regarding IT Security.

Category	Rating	Description / Comments
Customer Target Type	Medium	Widget Manufacturing Company
Size	Medium	500-1000 employees
Internet Exposure / Footprint	Low	Email access only.
Internal Exposure / Footprint	Medium	All internal computing resources available to all network connected users.
Temptation Level	Medium – High	Corporate data would be cause for some temptation for ABC Company's major competitors. Research and Design information on new products would be the prime target.
Impact of Internal Security Breach	Significant	Potential exposure of confidential new product information.
Impact of External Security Breach	Significant	Potential exposure of confidential new product information. Public knowledge of a security breach would have a detrimental affect on the reputation of ABC Company.
Likely Attacker Type	Moderate to highly skilled	Would likely attract amateur, former employee or even skilled hackers wanting to gain competitive information..
Potential Attacker Determination Level	Moderate	The biggest temptation would be the Research and Design information. An amateur might be willing to dedicate some effort to this task, but would probably give up in a relatively short period of time. A former employee or a professional hacker would potentially be more determined.
General Threat Level	**Moderately High**	**Main target for threat is the ABC Company research and design information as well as the potential to cause damage to the corporate reputation.**

A list of the potential risks associated with ABC Company perimeter security and the potential consequences are as follows:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Risk	Likelihood of Occurring	Potential Consequence
Perimeter security is compromised allowing theft of confidential business information.	Medium-Low	The business information considered the most valuable to ABC Company is new product research and design information. If this information was provided to competitors the consequences would be very serious. – High
Loss of business critical services over this communication link.	High	ABC Company rely on Internet access to communicate with their clients and suppliers. Can function without the Internet for only short periods of time. - Medium
Corporate image affected by public disclosure that a computer system or their security was compromised.	Medium	Public image for ABC Company is very important, this would potentially affect their business relationship with clients. - High
Disgruntled employee makes change to firewall configuration or rules to expose corporate network to additional risks	Medium-Low	Employees know the systems and information to target, could cause significant damage. - High
Error is made by the firewall administrator that exposes the corporate computer resources to Internet based risks.	Medium	This type of exposure is difficult to detect and could cause significant level of risk. - High
Vandalism or inappropriate use of the Internet accessible mail server.	High - Medium	This exposure could affect communications with clients as well as potentially affect the corporate image of ABC Company. Unauthorized use of this service could expose ABC Company to potential legal liability. - High

Current State of Practice

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The research that was completed for this firewall audit included researching the security concerns related to the Checkpoint firewall product from a number of reputable organizations. This research included: CERT, Computer Security Institute, SANS and Checkpoint.

Many organizations have realized the necessity of a firewall when connecting to the Internet, however a firewall is only as effective as the rules and configuration parameters that have been applied to it. The Checkpoint product is arguably one of the leading firewall products available on the market today, but relying on this product's technology and reputation is not enough. According to information obtained from CERT "the most common cause of firewall security breaches is a misconfiguration of your firewall system. Knowing this, you need to make thorough configuration testing (of the firewall system itself as well as all of the routing, packet filtering, and logging capabilities) one of your primary objectives.[1]" A recent survey conducted by the Computer Security Institute released in the spring of 2002, identified that even though 89% of their survey respondents used firewalls, 40% still reported having a security penetration from the outside.

This information from CERT and CSI clearly identify why a firewall should be reviewed and identified that the configuration of this firewall should be carefully reviewed. The second area of research included determining what else should be reviewed in this firewall audit. To answer this second question, additional research was conducted into the security configuration issues and checklists associated with a Checkpoint firewall running on a SPARCStation server. This research included gathering and comparing information from a number of sources:

- Auditnet - www.auditnet.org
- SANS – www.sans.org
- CERT – www.cert.org
- CIS Security – www.cisecurity.com
- www.phoneboy.com
- CIAC - www.ciac.org
- Experienced co-workers

This research allowed me to determine that this audit should include not only address the technical configuration and rules applied to the firewall, it should also include administration and monitoring procedures, physical security and extensive testing to confirm that the firewall rules are functioning properly. Another area which I did not initially consider important when auditing a firewall is verifying that no other points of entry into the network are in place. In the SANS firewall checklist the risk of dial up modems was identified. "Modems within the internal network are the biggest threat to subvert a firewall and thus the auditor should ensure that there are no modems within the internal network. It is senseless performing an audit on the firewall when an even bigger

[1] Deploying Firewalls, CERT Coordination Centre, http://www.cert.org/security-improvement/practices/p060.html

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

threat exists via the modem. The auditor should perform war dialing to identify any modems within the internal network with tools like Phonesweeper."[2]

To be able to provide assurance to ABC Company that their firewall meets generally accepted industry security standards, it was concluded through this research that the key areas for review in this audit will include:

1. Conduct tests on the firewall
2. Conduct tests to verify the firewall rules in place
3. Verify that there are no additional network connections into ABC Company
4. Review the Checkpoint system configuration
5. Review the Sun operating system configuration
6. Review and test physical security
7. Determine the corporate security policies through reviewing current policy documents and through interviews

How can current methods and techniques be improved?

It appears that there is a wealth of information in the Information Security field available for technical verification of different computer systems and technologies. For this assessment, security information on Checkpoint and Sun were readily available. Two difficulties were experienced when preparing for this audit:

1. Obtaining information to compile a checklist for the review of the firewall rules.
2. Determining the recommended industry standards to be followed for administration of this security device.

The checklists and information that I gathered regarding the audit of a Checkpoint firewall does not cover the verification of the rules to the extent that I feel is necessary for a firewall. A Checkpoint firewall receives an IP packet for acceptance or rejection and reviews the rules in a particular order. The firewall starts at the global rules (rule 0) then works from rule 1 down to the final rule on the system. As soon as a match is found for the request, the appropriate action is taken. No other subsequent rules are reviewed. In many situations when I have audited a Checkpoint firewall the order that the rules are in has inadvertently created holes in the firewall's security. For example, many firewalls are configured to allow internal users to communicate on select ports to the Internet (ANY). If there isn't a rule in place that specifically blocks access to the DMZ ahead of this rule, internal users have more access into the DMZ network than originally intended.

Information related to auditing security processes for firewall administration is another area where current resources are lacking. During my research I was not able to obtain any information recommending administration practices to use as a guideline. This audit will provide ABC Company with a number of recommendations to correct the current security issues and enhance the overall effectiveness of the firewall. Ensuring that the

[2] Krishni Naidu, "Firewall Checklist", www.sans.org

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

proper security policies and procedures are in place will ensure that the level of security rigor applied to the firewall is maintained for the future. In my experience, weak security practices and procedures cause an unnecessary increase in risks within many organizations.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 2 – Audit Checklist

Assessment Process:

The following process will be followed to assess the perimeter security provided by the Checkpoint Firewall 1 at ABC Company.

1. Conduct tests on the firewall from the Internet and the internal network
    a. Using nmap, SuperScan and nessus
2. Conduct tests to verify the firewall rules in place
    a. Scan the DMZ network from the Internet
        i. Using nmap, SuperScan and nessus
        ii. Connect laptop running tcpdump to the DMZ network during the tests
    b. Scan the DMZ network from the internal network
        i. Using nmap, SuperScan and nessus
        ii. Connect laptop running tcpdump to the DMZ network during the tests
    c. Scan the ABC internal network from the Internet
        i. Using nmap, SuperScan and nessus
        ii. Connect laptop running tcpdump to the internal network during the tests
    d. Manually test any vulnerabilities detected
3. Verify that there are no additional network connections into ABC Company
    a. Conduct war dialing on all telephone lines
        i. All telephone lines used by ABC Company will be dialed to determine whether a modem exists
        ii. Manual investigation of any positive results will be done by ABC Company staff
    b. Scan the internal network using nmap to ensure no other entry points exist
        i. Scan Internal network using nmap and SuperScan
        ii. Determine if a router or communication device is connected to the internal network
    c. Manually verify all positive test results
4. Review the Checkpoint system configuration
    a. Review the firewall Global properties
    b. Review Checkpoint version and patch level
    c. Review the Checkpoint rules
        i. Verify that the rules are in the proper order
    d. Determine the corporate security policy
    e. Verify that the rules match this policy
5. Review the Sun operating system configuration
    a. Review the configuration and hardening standards in place
    b. Review the administration procedures
6. Review and test physical security

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

a. Verify that the firewall is located in a physically and environmentally secure area
b. Test the physical access to the firewall and computer room

7. Determine the corporate security policies through reviewing current policy documents and through interviews
    a. Review all network security policies and standards
    b. Confirm the findings and review administration procedures through interviews
    c. Verify the firewall administration and monitoring procedures
    d. Verify understanding and adherence to the corporate security policies

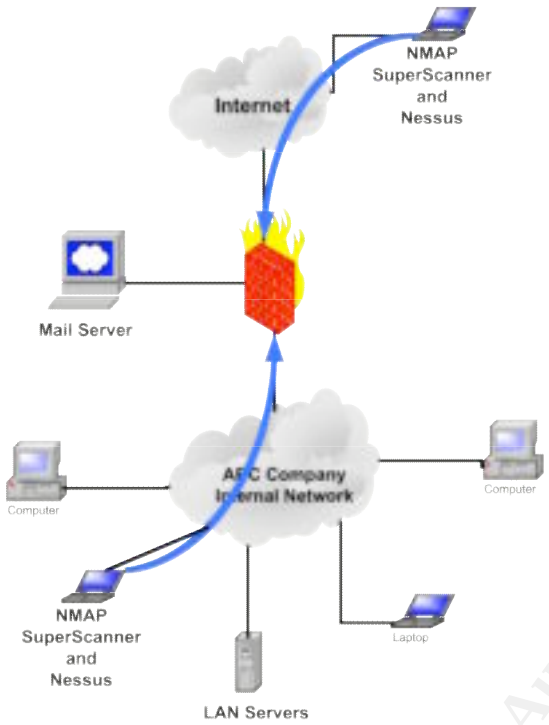
1. Conduct tests on the firewall

These tests will determine the exposure of the ABC Company Checkpoint firewall to resources on the Internet as well as the internal network. These tests will determine what information is provided to a potential Internet based hacker on the firewall and any potential weaknesses that could be exploited. These tests will also determine what information regarding the firewall is provided to employees on the internal network.

As depicted in the following diagram, the first series of tests will consist of a full scan from the Internet to the external port of the Checkpoint Firewall. A properly configured firewall should not respond to any port scans from an Internet address. This will be an objective test to determine if the firewall is providing any unnecessary information to a potential attack from the Internet. The test will consist of a second series of scans from the internal network directed at the internal port of the firewall. Again it is expected that a properly configured firewall will not respond to any portion of these tests.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Test	Expected Response	Pass/Fail
Ping Firewall address from Internet (nmap)	No Response	
Scan all Ports from Internet (nmap and SuperScan)	No Response	
Scan from Internet using nessus (will only be conducted if response received from nmap or SuperScan scans)	No Response	
Ping Firewall address from internal network (nmap)	No Response	
Scan all Ports from internal network (nmap and SuperScan)	No Response	
Scan from internal network using nessus (will only be conducted if response received from nmap or SuperScan scans)	No Response	

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Resources used for this test include training received from SANS, as well as information gathered from www.cert.org and www.auditnet.org.

2. Conduct tests to verify the firewall rules in place

External access to computer resources other than systems that provide an Internet based service, is considered very risky. Testing will determine if access to any unexpected systems or communication ports are available as well as determine what information on ABC Computer systems can be obtained by a hacker from the Internet.

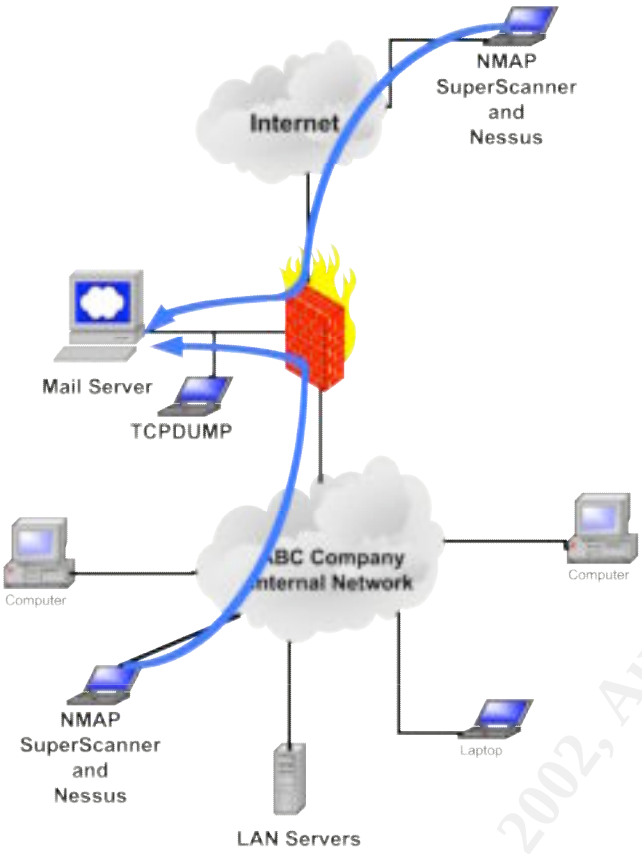
This test will be conducted to determine what access to the DMZ network can be obtained from the Internet. During the initial interview with ABC Company it was identified that only a mail server is located in this network, however to verify this fact this test will include the complete DMZ network subnet (10.10.10.0 subnet mask 255.255.255.248).

Merely performing a port scan from the Internet directed at the DMZ network does not really prove what access is permitted by the firewall, all this test would prove is what ports are permitted through the firewall and receive a response from the target system. To thoroughly test the access permitted by the firewall a laptop running tcpdump will be connected to the DMZ network during this test. The passive monitoring from this system will identify all communications that are permitted through the firewall into the DMZ network.

A second series of tests will be conducted from the internal network directed toward the DMZ network. The firewall design is intended to not only protect the mail server located in the DMZ network from unauthorized Internet access, it is also designed to control unauthorized access from internal systems. A common issue with firewall is that the sequence of the rules can cause unintended security holes. If the rules for the ABC Company firewall are not in the proper order, additional access into the DMZ network may be available. Performing this test will verify that the firewall rules are functioning properly to offer an acceptable level of protection from the internal users as well.

The following diagram shows the tests that will be conducted:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



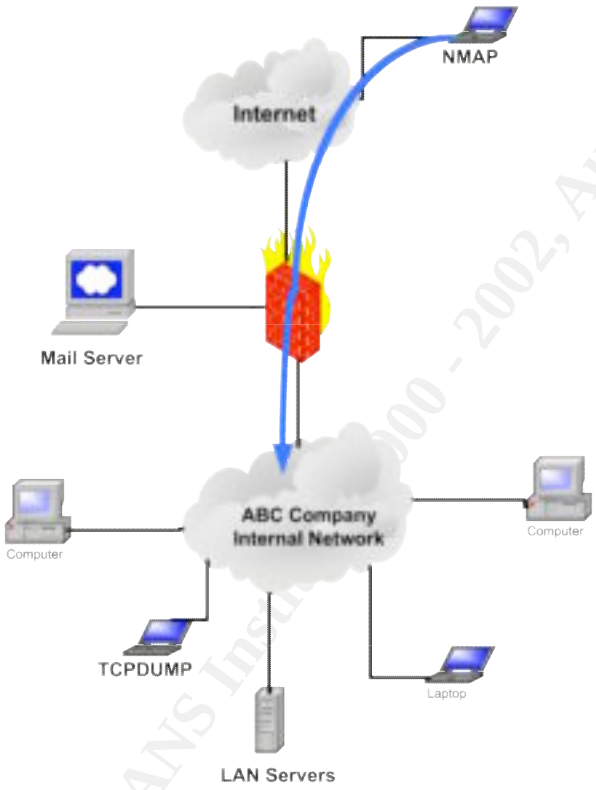
This is an objective test that will positively confirm the access through the firewall that is permitted into the DMZ network. Resources used for this test include training received from SANS, as well as information gathered from www.cert.org and www.auditnet.org.

Test	Expected Response	Pass/Fail
Ping DMZ network from the Internet using nmap	No Ping packets detected on the DMZ network	
Perform port scan on all DMZ network addresses from the Internet using nmap and SuperScan	Only expect to see TCP port 25 directed to the mail server.	
Ping DMZ network from the internal network using nmap	No Ping packets detected on the DMZ network	
Perform port scan on all DMZ network addresses from the internal network using nmap and SuperScan	Only expect to see TCP port 25 directed to the mail server.	

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Scan all responsive addresses using nessus	Expect response from the mail server. Expect that nessus will not detect any weaknesses	
Manually test any vulnerabilities detected by nessus	No weaknesses expected	

A second test will be conducted to verify the security of the internal network provided by the firewall. As with the test of the DMZ network, this test will include connecting the laptop running tcpdump to the Internal private network of ABC Company. This laptop will monitor the network traffic looking for any packets received from the address of my PC that is performing the tests from the Internet.



This is an objective test that will confirm the firewall access permitted into ABC Company's internal network from the Internet. Resources used for this test include training received from SANS, as well as information gathered from www.cert.org and www.auditnet.org.

Test	Expected Response	Pass/Fail
Ping internal network using nmap	No Ping packets detected on the internal network.	
Perform port scan on all internal network	Expect that no IP packets from the test device will be	

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

addresses using nmap	detected on the internal network.	
Scan all responsive addresses using nessus	Expect that nessus will not detect any weaknesses	
Manually test any vulnerabilities detected by nessus	No weaknesses expected	

3. Verify that there are no additional network connections into ABC Company

War Dialing:
Security is only as strong as its weakest link and the best perimeter security can be compromised by a dial up modem connected to computer system. This war dialing test will verify that no telephone lines at ABC Company have been connected to a modem without the proper authorization and security controls in place. This test will include my PC calling every telephone number over two evenings, detecting any modems that answer the telephone call.

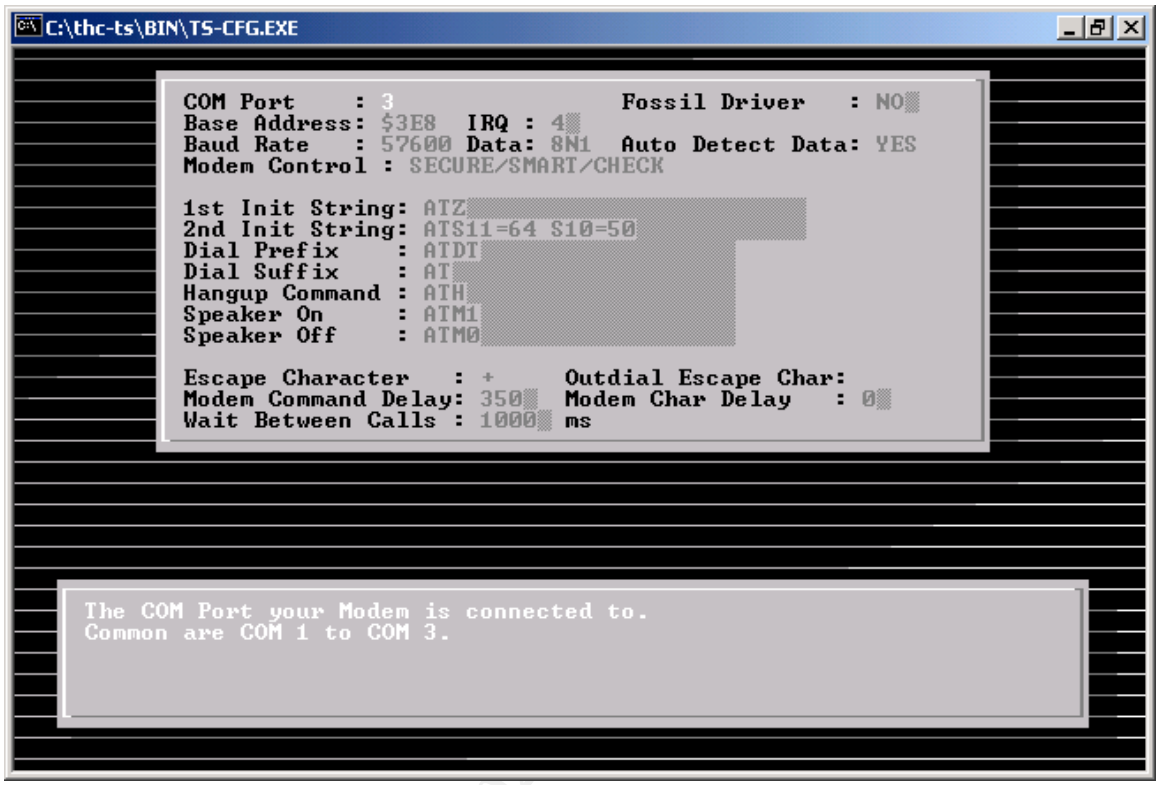
The tool to be used for this exercise is THC-SCAN. Since the numbers do not run in sequence a text file will need to be created with all telephone numbers included. In this file you enter one telephone number per line with no spaces or special characters. For example, you enter the numbers in this manner:

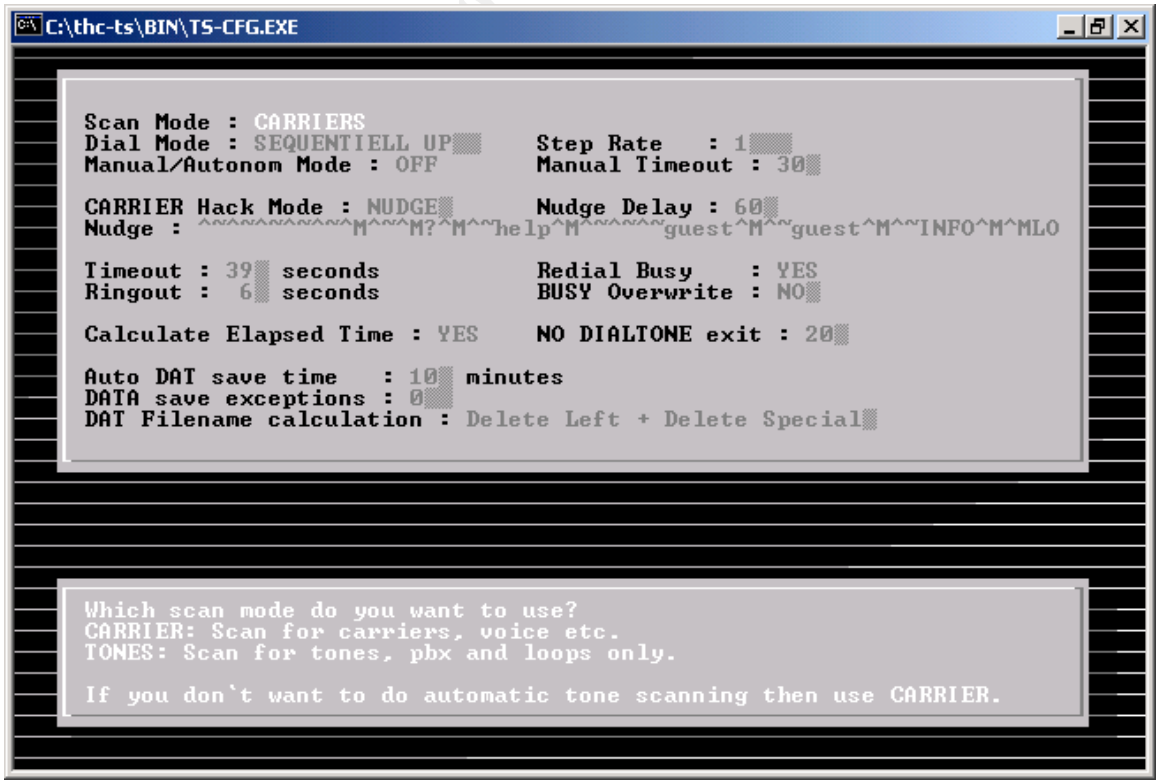
5552101
5552162
5552035

The sequence or order of the numbers does not matter, the key is that you have to have a complete list of numbers for this test to be effective. The list will be saved to a file called "test.txt" and the command used to initiate this test is "THC-SCAN @c:\test.txt"
I have THC-SCAN configured to create three different files during this test:

- Busy – This will include the telephone numbers that have been detected as busy
- Carrier – This will list the telephone numbers that detect a modem or fax tone.
- Carriers – This file will provide the response information received from additional testing of the suspected modems.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.





This is an objective test that will identify any other potential points of entry into ABC Company's private network. This test will identify telephone lines that are

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

suspicious, but will require physical verification to positively confirm that an unauthorized modem is in place. All telephone numbers that are identified by THC-Scan as either a fax, modem or are busy telephone line, will be considered suspicious and require a physical verification. Due to the scope of this audit, I will be identifying the suspicious telephone numbers and the IT Manager will assign an employee to investigate the possible modem.

I do not recall when I first used a war dialer. As a Security Manager at a telecommunications company, this type of tool has been in my testing kit for a number of years. I have recently started to use THC-SCAN because it appears to provide more accurate test results than other war dialing programs that I have used. No additional resources were referenced to perform this war dialing test.

Scan the internal network using nmap and SuperScan
To determine if there are any additional entry points into the network a full nmap and SuperScan scan of the internal network will be conducted. This scan will determine whether there are any additional network connections into the private network of ABC Company. The primary objective of this scan is to determine whether a router or other communications equipment exists. According to the information provide by ABC Company, all of the internal systems should be either Windows 98 and 2000 Personal Computers, NT and 2000 servers and some network printers. During the internal scan the Windows netbios ports should be detected on all systems with the potential exception of the printer. If a router is connected to the internal network the Windows netbios ports would not be present, but other ports such as telnet and TCP small services may be identifiable.

This test is not 100% foolproof, a second network could be connected to a separate port on a PC or server and not detected. Also a router could be connected to the internal network with a complete access control list that will not allow it to be detected during these tests. This test will provide a reasonable confirmation that the firewall is the single point of entry into the ABC Company private network. If any other network connections such as a router is detected, this test will be identified as fail.

This internal network test is an objective measurement of any entry points into the ABC Company network. Any suspicious ports running on the internal systems will be reported to ABC Company for further investigation.

4. Review the Checkpoint system configuration

Checkpoint Firewall:
The Checkpoint checklist has been created from information from two sources:

- SANS GIAC Auditing Networks, Perimeters, and Systems GSNA Practical Assignment, Ruangkrai Rangsiphol

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Checkpoint Firewall Audit Work Program by Terry Cavender (terry.cavender@Vanderbilt.Edu) www.auditnet.org/docs/CheckpointFirewall.txt

Verify the Checkpoint version and patch level.

- The latest patches for the firewall should be in place.

Review the firewall rules

- Verify critical global properties – Checkpoint firewall establishes a number of configuration options by default during installation. These options include opening several ports (256, 257, 258 and ICMP) within the control properties. An effectively configured Checkpoint firewall should have many of these global properties adjusted to strengthen security.
    - TCP session timeout
        - The default session timeout is 3600 seconds. To enhance security it is recommended that this window of opportunity be set at 900 seconds.
    - FW1 Control Connections
        - FW1 Management should not be selected. A specific rule on the firewall should provide controlled access to the firewall for management purposes.
        - If this option is selected the Checkpoint Firewall-1 ports (TCP 256-258) will be allowed through the firewall to any internal address. This means that the Internet would have access on these particular ports to all internal ABC Company systems.
    - ICMP Implied rules
        - ICMP options should not be selected, if ICMP access is required a specific rule should be in place.
    - DNS Implied Rules
        - DNS should not be selected on this configuration screen, if DNS access is required through the firewall a specific rule should be in place.
- Review firewall object
    - Ensure that all ports are properly configured with appropriate subnet values.
        - The configuration for the firewall ports on the operating system and Checkpoint configuration should match.
        - It is also important to confirm that the subnet masks are all set correctly.
    - Verify spoofing rules are in place.
        - The spoofing rules on the Checkpoint firewall will identify any spoofed packets that are directed at the firewall and will as well offer a second layer of protection in case the firewall routing is incorrectly configured.
        - The spoofing rules should specifically include either the network or a list of the addresses connected to this port.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Verify that a specific rule is in place for firewall administration and monitoring.
    - The list of internal addresses that are able to communicate with the firewall should be restricted to just the necessary administrators. All other users, including internal users, should not be able to communicate with the firewall on any communication port.
    - A firewall drop all rule, should immediately follow the firewall administration rule to "hide" the firewall from all other access, both internal and external.
- Review the rules in place
    - Verify that all rules are required.
    - Verify rules are in the correct order
        - The order of rules is critical to the proper secure operation of a firewall.
        - The order of rules should include:
            1. Rules for administrator access to the firewall (FW-1, SSH.. etc)
            2. Rule to drop all other access to the firewall (stealth rule)
            3. Rule to allow incoming access from "ANY" to the DMZ network
            4. Rules to allow communications for specific hosts and ports among firewall connected networks (internal network to DMZ network, between LAN1, and LAN 2...etc)
            5. Rule to drop all other access to the internal network (DMZ network, LAN1, LAN2...etc)
            6. Rules to allow outgoing access to the Internet (destination "ANY")
            7. Rules to drop nuisance traffic with no logging (typically netbios type of traffic)
            8. Rule to drop all other traffic with logging (ANY ANY DROP)
    - Is logging turned on in the rule set
        - Critical events and rules should be logged for future review.
    - Is the comments field used?
        - The comments field is a excellent tool to identify why a rule was put in place, whether it is intended as a permanent or temporary rule, when it was implemented and which administrator made this rule change.
- Review the status screen
    - When was the firewall last rebooted or the rules applied
        - This will provide some indication as to whether a maintenance window after normal work hours is used for these firewall changes.
    - Is the rule set applied the same as the rules reviewed?
        - If the manager has multiple rule policies, this is required to confirm that the audit is reviewing the correct rule set.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

This Checkpoint review is mainly an objective test with specific results required for this audit to pass. However the review of the order of the rules and whether all rules require logging enabled, is subjective. This review will also confirm the rules that in place on the firewall match what was detected during the firewall tests.

Test	Expected Response	Pass/Fail
Verify Checkpoint version and patch level	Latest system patches are applied	
TCP session timeout	Option set for 900 seconds or less is recommended, option set for 3600 seconds or less will be considered a pass	
FW-1 Control global option	Option is not enabled	
ICMP global option	Option is not enabled	
DNS Global option	Option is not enabled	
The firewall object has the ports properly configured	All port addresses and subnet masks are correct	
The firewall object has properly defined spoofing rules	Spoofing rules for the DMZ network and Internal network include the proper network information. The Internet port is defined as "other"	
Rule is in place for the administrators	This rule restricts access to only the system administrators	
Rule is in place that hides the firewall	A drop rule is in place that blocks all other users from access the firewall	
Verify the firewall rules	All rules are essential to the function of this firewall.	
Review the order of the rules	Rules are in the following sequence: • Firewall administration • Stealth rule for firewall • Incoming access • Communications between networks • Drop rule for all internal networks • Outgoing rules to the	

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

	Internet • Drop rule for all other access	
Verify logging	All critical rules have logging enabled	
Comments	The comments field provides information when rules were added and why.	
Date and time of last reboot or rule change	The last change occurred during a maintenance window after normal work hours.	
Review applied rule set in the status window	The rule set last applied to the firewall matches the rule set reviewed in this audit.	

5. Review the Sun operating system configuration

This operating system is a Sun Solaris version 5.7. Particularly for a system running a firewall application, the first key to security is that only the services required to perform the firewall function are active on the system. This checklist is based on information acquired from "http://www.cisecurity.org/ Solaris Benchmark Document" and www.sans.org, as well as my personal experience with auditing a number of Unix systems in the past.

- Server Patch level
  - Maintaining the server at the latest patch level is a key to maximizing the security of this device.
  - Review the current patch level of the system.
- Administrator signon procedure
  - Administrator has an individual account and su's to root when necessary (verify /etc/default//login)
- How many administrators and users are on the system? (more /etc/passwd)
  - The access to the system should be restricted to authorized administrators only.
  - Access for the security officer to view the audit logs is also recommended.
- Password standards
  - Strength of password will be determined through a discussion with the administrators. A more objective test would be to test the passwords but this is outside of the scope of this audit. Additional password standards will be objectively reviewed through the configuration standards.
  - Password expiry
    - To maximize security it is recommended that passwords be changed frequently. The generally accepted standard for

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

password expiry is between 30 and 90 days. For the administrator account on a firewall this should be set for 30 days.
    - Minimum length
        - The strength of the administrator passwords is essential to protect the firewall from unauthorized access. This password should be a minimum of 8 characters.
    - Verify that there are no accounts with empty password (logins –p).
    - Verify that no UID 0 accounts exist other than root (awk –F: '($3 == 0) {print $1}' etc/passwd)
        - UID 0 provides users with root privileges. The firewall administrators should not have UID 0 for their individual accounts.
    - Verify that system users must re-authenticate after a period of inactivity. This timeout period should be set for 10 minutes or less.
- How does the administrator access the server
    - Telnet access to the firewall server is not recommended. The telnet protocol transmits all information, including the passwords, in clear text. A more secure method of communication is using secure shell, which encrypts all information being transmitted.
    - Determine that the telnet OS banner has been changed/eliminated.
        - Default banners can provide valuable information on the system and the version of software.
        - Default banners also do not cover the legal aspect of identifying a system as restricted to authorized personnel only.
- Verify active services on this server (/etc/inetd.conf)
    - Verify why each service is required for this firewall
        - The firewall should have only the services active that are required for this function.
        - Services not required for the firewall should be removed from the system so they can not be activated in the future unintentionally.
- Are static routes used for routing?
    - Routing protocols would enable the routes to be changed on the firewall without authorization.
    - The routes on the firewall should be reviewed to confirm that only static routes are required.
    - The current routes should also be reviewed to ensure that only essential routing rules are in place.
- Are unused ports enabled or disabled?
    - An enabled port can cause a security risk, allowing a network to be accidentally connected to this port.
    - All unused ports on the firewall should be disabled.
- Are system audit logs enabled? (/etc/syslog.conf)
    - Audit logs should be enabled on the system for review of key activities:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

        - Login (successful and unsuccessful)
        - Logout (unsuccessful)
        - Use of privileged accounts
        - System startup and shutdown
        - Attempts to su to root (/var/adm/sulog)
        - Service start and stop
- Review the system audit logs
    - Review the logs for recent activity.
    - Identify any suspicious activity

This review of the operating system is an objective test to verify whether the system meets the recommended baseline for a hardened operating system.

Test	Expected Response	Pass/Fail
Verify system version and patch level	Latest system patches are applied	
Check administrator access to root (/etc/default//login)	Administrator must "su" to root	
Check the user accounts on the system (more /etc/passwd)	Access is limited to the administrators and the security officer	
Verify password expiry times	Passwords automatically expire every 30 days.	
Password length	Password minimum length is 8 characters	
Verify account with empty passwords (logins –p)	No accounts exist with empty passwords	
Verify the accounts with UID 0 (awk –F: '($3 == 0) {print $1}' etc/passwd)	The only account that has UID 0 is root	
Verify inactivity timeout	User must re-authenticate	
Administrator access to the firewall	Administrator uses secure shell and telnet is disabled	
The OS banner does not provide sensitive information	The banner has been changed to not provide system information and identify this as a restricted system. Banner includes a legal disclaimer that unauthorized access is not permitted.	
Verify active services	Only services required for	

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

(/etc/inetd.conf)	the firewall are active	
Review routing protocol	Static routes are being used	
Review system routes	Only essential routes are in place on the system	
Check unused ports on the firewall	All unused ports are disabled	
Are audit logs enabled?	Audit logs are enabled and log key system activities	
Review audit logs	No suspicious activity is detected	

6. Review and test physical security

Physical security is a vital part of an information protection program. It is generally acknowledged security doctrine that if an attacker is able to gain physical access to a computing resource, that system will inevitably be successfully compromised. Physical security for the firewall will be reviewed as part of this audit. This physical security review will include:

- UPS Power
  - Availability of an uninterrupted power supply will ensure that the availability of the firewall is not affected during a commercial power failure.
- Fire Suppression
  - It is important to have fire suppression, but it is also important to ensure that this method of fire suppression does not cause immediate damage to the computer equipment.
- Access Control
  - Physical access to the area housing the firewall should be controlled and limited to authorized personnel only.
  - Physical access into the computer room area should also be logged to ensure that an audit trail is created of who entered this area.
- Room monitoring (cameras)
  - Additional monitoring of physical assets can be provided by technology such as cameras
- Room environmental controls
  - Environmental controls to regulate the humidity and temperature are considered good controls to have in place. Also the control of dust and the tidiness of the computer area is considered important in this review.
- Cabling
  - The cables connected to the firewall should be labeled to ensure that they are always connected to the correct system ports. If cables are not properly configured the likelihood of connecting networks to the wrong port is increased. This could cause a

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

potential security exposure but would definitely affect availability of the firewall service to ABC Company.

The findings from this physical security review are subjective based upon the auditors opinion of an acceptable level of security and acceptable environmental conditions. The only test that is somewhat objective is the presence of a UPS power supply, but due to the scope of this audit, the confirmation test of disconnecting the commercial power to test this backup is not reasonable. To be able to provide a more objective opinion regarding the physical security of the firewall, two tests will be conducted:

- The auditor will attempt to gain access to the computer room during the day.
  - This test will verify that the door is locked
  - Social engineering will be attempted to convince an employee to open the door.
- The auditor will attempt to gain access to the computer room after normal work hours.
  - This test will verify whether access to the building is available after normal work hours.
  - Will also verify whether access to the floor can be gained after work hours.
  - Verify whether the computer room is locked at all times.
  - Social engineering will be attempted to overcome the physical security controls.

This physical security review was compiled with information from http://www.auditnet.org and from personal experience.

Test	Expected Response	Pass/Fail
Availability of UPS Power	UPS power is in place that will maintain the firewall for an extended period of time	
Fire Suppression	Acceptable methods of fire suppression are in place with the computer room The fire extinguishers have been recently inspected	
Logging of access to computer area	Access is logged for each individual gaining access to the room.	
Monitoring of the computer room	Additional surveillance controls are in place, such as video surveillance.	
Environmental conditions	The computer room is an environmentally controlled	

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

	area. Review includes temperature, humidity, dust and general condition of the area.	
Cabling	All connections into the firewall are labeled.	
Test physical access to the computer room during work hours	No unauthorized access should be obtained.	
Test physical access to the computer room after normal work hours	No unauthorized access should be obtained.	

7. Review corporate security policies

Interviews will be conducted with a number of staff members from ABC Company to confirm the findings from our security testing, as well as to determine the corporate security policies and procedures in place. The best technology available is only as good as the configuration and rules applied to it. One of the most often overlooked aspects of security is the necessity to have strong security processes in place to manage, monitor and maintain systems.

Prior to these interviews, a copy of all corporate security policies and procedures will be requested for review. The nature of the interviews will be based upon the information provided. These interviews will either confirm that the corporate policies and procedures are understood and followed, or in the absence of proper documentation, determine the current unwritten policies and procedures in place.

The information obtained through this interview process will be subjective. The issues identified will be based mainly on the opinion of the auditor regarding best practices for the administration and management of a Checkpoint firewall. This process is valuable to understand the current security practices at ABC Company and provides a forum for verification of information obtained earlier in this audit.

The interviews will be conducted privately as much as possible. I have been involved in interviews in the past when two or more administrators attend the same session. My experience has been that in those sessions one person monopolized the conversation and potentially influenced the answers of the other participants.

A template of questions has also been prepared as a guide during these interviews. Depending on the responses to this questions and the nature of the work this individual performs, all or part of these questions will be asked. The questions

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

may also cross over into other fields if the role performed is a combination of tasks.

These interview questions have been compiled based on my past experiences with performing security assessments and audits. This list has been used for some time with questions added, modified and removed over time.

The sample interview questions that will be asked include:

UNIX Admin

Describe your administration role

Creating users:

- When you create a new user, what is the process by which you receive the request?
- Who authorizes the request?
- What access to information standards are provided to all new users?
- Do new users get training/documentation?

Passwords:

- What is the password standard for your system?
    - Password is not displayed during login
        - Perform test to verify
    - Password can be changed by the user
        - Perform test to verify
    - Password is changed frequently
    - Password is not reused for 1-2 years
    - Password standards
        - Upper case letters
        - Lower case letters
        - Numbers
        - Special characters
        - Automatic timeout feature exists
            - Perform test to verify
- Are they enforced by the systems technology? Or just what the user is asked to follow?
- Describe the process followed for a user to get their password changed?
    - How do they verify the persons identity!
- How often are passwords required to be changed?
    - Is this an automated process?

Removing users:

- When an employees leaves ABC Company, what is the process to get their user account removed from the system?
- Who notifies you to remove the account?
- Do you ever get to check the list of users on the system versus active employees?
- Do you remove/disable accounts that have been inactive for a period of time?

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Administration access:

- Who has administration access to this system? How many?
- Do they share an administration account or have separate Login accounts?
- If they share a common admin account what are the password standards in place (length of password, how often is it changed)
- Can you do your administration remotely if necessary?
- If so, how do you get access?
    - Is this using telnet or Secure Shell?

System technical questions

- What is the process to patch the system or upgrade the OS?
- How often is this done?
- Does someone receive security alerts on this system advising that security patches should be applied?
    - What system do they subscribe to?
    - Verify that they have received messages recently.

Change control

- Is there a process in place if a change is needed on this system?
- Who approves the changes?
- How are the changes communicated to you and the other system administrators?
- How is it communicated to the users?

Access to information:

- What information access controls are in place? (all users have access to everything by default or only select users have access to information)
- Who decides/approves access to restricted information?
- What is the process followed to grant a user access to restricted information? (is it a phone call or a written request with an approval signature)

Training:

- What training have you had to administer this system?
- When was this training done?
- Do you know the company security policies to follow when administering this system?
- Do you know who to contact if you have a question regarding the corporate policies?

Backups:

- Do you have backups?
- How often are backups done?
- What is backed up?
    - Full backups, incremental or what combination?
- Where are the backups stored? (on site or off site?, secure or not secure location?)
    - Where is the off site location?
- Who changes and transports the tapes?
- How long are the backup maintained (weeks or months)?
- Do you have a disaster recovery plan in place for this system?

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Do you have a formal or informal process to restore from backup?
- Have you ever tested this restore process.
    - If so, what was the result?

Monitoring:

- If the system fails/crashes, how are you notified?
- Is there a system that monitors the availability?
    - Does this system monitor conditions and alert before failures (monitor drive usage and alert at 95% full)?
- Does this system log user access/activity?
    - If so, do you review this log?
- What would be your procedure if you detected something on the system that could be a serious security breach?
- Is this a formal process (documented)?- Describe the process.

Physical security

- Where is your server(s) located?
- Who has physical access to the server?
- Does the system have UPS power?

Unique issues regarding Unix:

- Do you use shadow passwords?
- Do you use Rlogin type of commands?
    - If so do you use the rhosts configuration?
- Do administrators login direct as root or must "su" to root?
- Review other specific security standards documented in the corporate policies.

Are there any issues or concerns that you have in regards to security that we should be aware of?

Firewall administrator:

- How are rule requests received?
- Do you maintain copies of the firewall rule requests?
- How long are these requests retained?
    - Verify the information by viewing the audit trail of past rule change requests.
- Who authorizes rule changes on the firewall?
    - Is a signature received? (physical or electronic)
- How is the security risk evaluated with these rule changes?
- What is the process to review a rule request for potential security risks?
- When are rule changes applied?
    - During the day or in a maintenance window?
- Do you receive alerts regarding security issues on this server from Checkpoint or another source?
- How often are upgrades made on this system?
- Do you have a backup of the firewall rules?
- Do you monitor the firewall activity?
    - Who performs this monitoring function?
    - How often are logs reviewed?

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Do you have a diagram or document detailing the firewall configuration?
    - Who plans or makes changes to the overall firewall design?

Are there any issues or concerns that you have in regards to security that we should be aware of?

Assignment 3: Conduct the Audit:

As instructed in the assignment details, 10 of the key items/areas of the Checkpoint firewall audit plan have been selected for this assignment The areas selected for inclusion in this assignment include:

1. Test access to the firewall from the Internet and internal network using nmap, SuperScan and nessus.
2. Test access to the DMZ network from the Internet and the internal network using tcpdump, nmap, SuperScan and nessus.
3. Test access to the ABC Company internal network from the Internet using tcpdump, nmap, SuperScan and nessus.
4. Conduct war dialing test on the ABC Company telephone lines using THC-Scan
5. Scan the ABC Company internal network using nmap.
6. Review the Checkpoint system configuration
7. Review the Checkpoint Rules.
8. Review the Sun Operating system configuration.
9. Review and test the physical security.
10. Review corporate security policies

1. Test access to the firewall from the Internet and internal network

The external probe scans from the Internet were directed at the firewall (142.162.10.10)

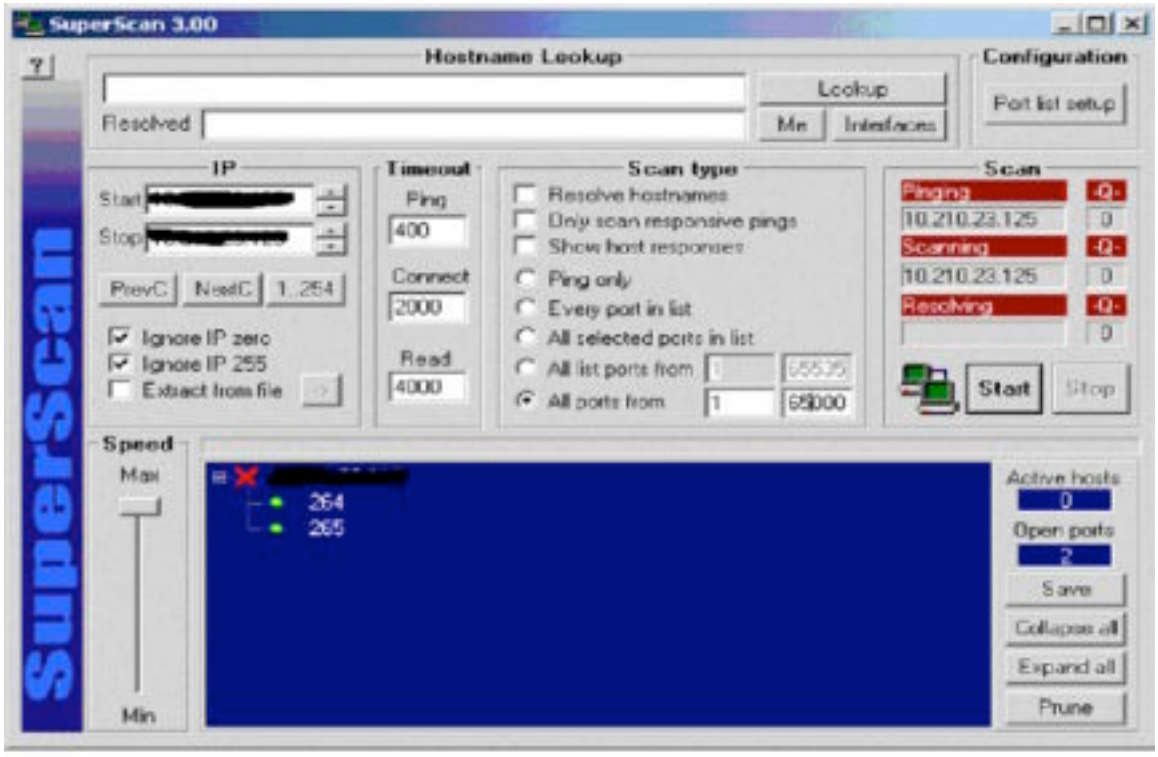
The nmap scan continued to timeout with the report that "Host seems down. If it is really up, but blocking our ping probes, try –P0". It was obvious that this was due to the fact that none of the addresses would respond to a ping and the original nmap option was selected for "Ping and TCP scans"

The nmap command used to complete the firewall scan was :
"nmap –sS –p 1-65000 –P0 142.162.10.10"

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
 Interesting ports on  (142.162.10.10):
(The 64998 ports scanned but not shown below are in state: filtered)
Port       State       Service
264/tcp    open        bgmp
265/tcp    open        unknown
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SuperScan was used to perform a second port scan of the firewall. The following is a screen image of the scan results:



Since a response was received from the firewall during the port scans, nessus was used to further analyze the firewall.

Nessus Scan Report

Number of hosts which were alive during the test : 1
Number of security holes found : 0
Number of security warnings found : 1
Number of security notes found : 0

List of the tested hosts :

- 142.162.10.10 **(Security warnings found)**

142.162.10.10 :
List of open ports :

- *unknown (265/tcp)*
- *unknown (264/tcp) (Security warnings found)*

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Warning found on port unknown (264/tcp)

The remote host seems to be a Checkpoint FW-1 running SecureRemote.
Letting attackers know that you are running FW-1 may enable them to focus their attack or will make them change their attack strategy.
You should not let this information leak out.
Furthermore, an attacker can perform a denial of service attack on the machine.
Solution:
Restrict access to this port from untrusted networks.
Risk factor : Low
For More Information:
http://www.securiteam.com/securitynews/CheckPoint_FW1_SecureRemote_DoS.html

---

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

The responses received from the scans initiated from the internal network were identical. To save space in this report the results from this second scan will not be included.

Test	Expected Response	Notes	Pass/Fail
Ping Firewall address from Internet (nmap)	No Response	No response received	Pass
Scan all Ports from Internet (nmap and SuperScan)	No Response	Received response from ports TCP 264 and 265.	Fail
Scan from Internet using nessus	No Response	Warning received by nessus on the firewall ports 264 and 265.	Fail
Ping Firewall address from internal network (nmap)	No Response	No Response	Pass
Scan all Ports from internal network (nmap and SuperScan)	No Response	Both scanning tools identify TCP ports 264 and 265 responding.	Fail
Scan from internal network using nessus	No Response	Warning received by nessus on the firewall ports 264 and 265	Fail

2. Test access to the DMZ network from the Internet and the internal network

This test includes placing a PC running tcpdump on the DMZ network while a number of scanning tools were used to scan the DMZ subnet (10.10.10.0 255.255.255.248). The first scan will be conducted from the Internet and the second series of scans will be from the internal network.

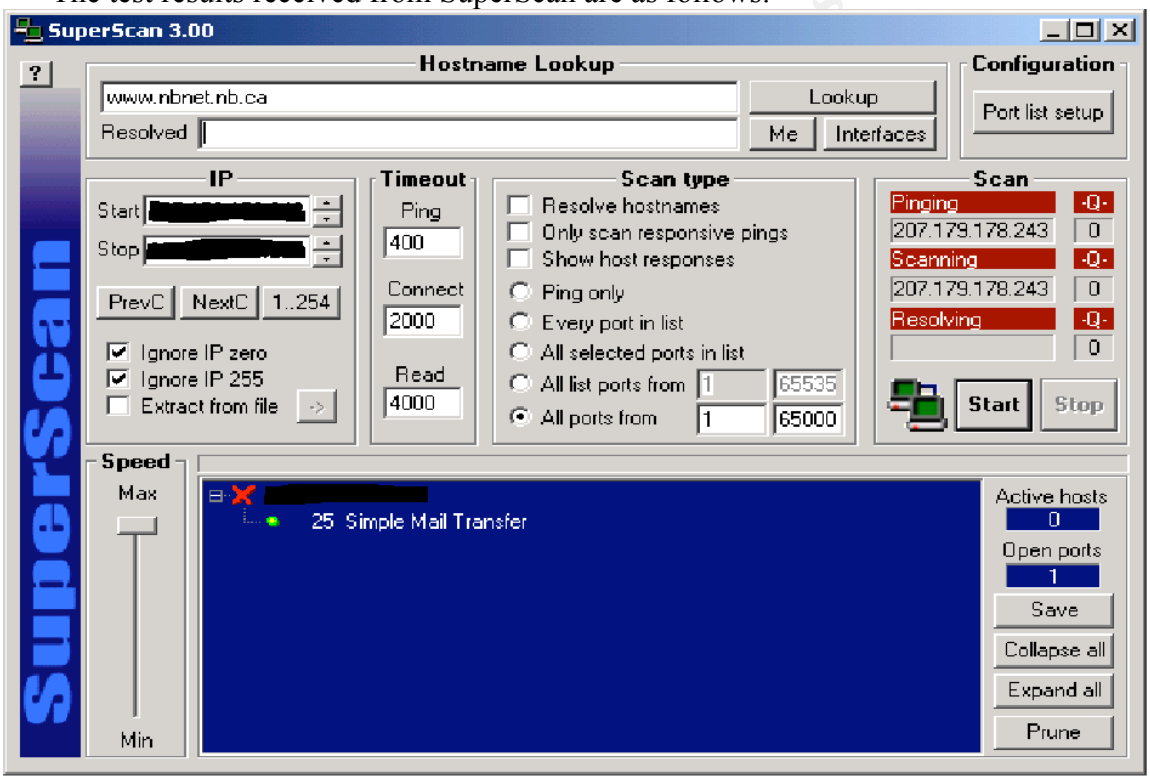
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The nmap command used to scan the DMZ network was :
"nmap –sS –p 1-65000 –P0 10.10.10.1-7"

The Log results from nmap are as follows:

Starting nmap V. 2.53 by fyodor@insecure.org (www.insecure.org/nmap/)
Interesting ports on (10.10.10.1):
(The 64999 ports scanned but not shown below are in state: closed)
Port State Service
25/tcp open smtp

The test results received from SuperScan are as follows:



The system running tcpdump detected only TCP port 25 communications being passed through the firewall:

12:55:44.367781 198.164.221.85.2494 > 10.10.10.1.25: S 99204617:99204617(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
12:55:44.368618 10.10.10.1.25 > 198.164.221.85.2494: S 1355284901:1355284901(0) ack 99204618 win 17520 <mss 1460,nop,nop,sackOK> (DF)
12:55:44.368741 198.164.221.85.2494 > 10.10.10.1.25: . ack 1 win 17520 (DF)
12:55:44.369188 198.164.221.85.2494 > 10.10.10.1.25: F 1:1(0) ack 1 win 17520 (DF)
12:55:44.369846 10.10.10.1.25 > 198.164.221.85.2494: P 1:132(131) ack 1 win 17520 (DF)
12:55:44.369846 10.10.10.1.25 > 198.164.221.85.2494: . ack 2 win 17520 (DF)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The second series of tests were conducted from the Internal network directed at the DMZ network. The PC running tcpdump was still connected to the DMZ network during this test.

The test results from nmap, SuperScan and nessus were identical to the initial test from the Internet. However the test results identified by tcpdump show that additional communication ports were able to pass through the firewall directed toward the DMZ network. The tcpdump information is as follows:

```
[root@localhost bsmith]# tcpdump -vv -nn -r audit4.tcpdump | more
13:59:07.442578 10.10.11.63.2522 > 10.10.10.1.25: S 1049118038: 1049118038(0) win
16384 <mss 1460,nop,nop,sackOK> (DF)
13:59:07.443468 10.10.10.1.25 > 10.10.11.63. 2522: S 2292768418: 2292768418(0) ack
1049118039 win 17520 <mss 1460,nop,nop,sackOK> (DF)
13:59:07.443595 10.10.11.63. 2522 > 10.10.10.1.25: . ack 1 win 17520 (DF)
13:59:07.444153 10.10.11.63. 2522  > 10.10.10.1.25: F 1:1(0) ack 1 win 17520 (DF)
13:59:07.444703 10.10.10.1.25 > 10.10.11.63. 2522: P 1:132(131) ack 1 win 17520 (DF)
13:59:07.444839 10.10.10.1.25 > 10.10.11.63. 2522: . ack 2 win 17520 (DF)
13:59:07.451479 10.10.11.63.2598 > 10.10.10.1.80: S 1049173142: 1049173142(0) win
16384 <mss 1460,nop,nop,sackOK> (DF)
13:59:07.452081 10.10.10.1.80 > 10.10.11.63.2598 R 0:0(0) ack 1049173143 win 0
13:59:07.461442 10.10.11.63.2631 > 10.10.10.1.119: S 1049206783:1049206783(0) win
16384 <mss 1460,nop,nop,sackOK> (DF)
13:59:07.462440 10.10.10.1.119 > 10.10.11.63.2631: R 0:0(0) ack 1049206784 win 0
13:59:07.471450 10.10.11.63.2986 > 10.10.10.1.443: S 1049240443:1049240443(0) win
16384 <mss 1460,nop,nop,sackOK> (DF)
13:59:07.472107 10.10.10.1.443 > 10.10.11.63.2986: R  0:0(0) ack 1049240444 win 0
```

This tcpdump information shows that ports 25, 80, 119 and 443 were permitted through the firewall. The mail server did not respond to the additional ports of 80, 119 and 443, therefore the scan results received from nmap and SuperScan were identical to the scan from the Internet. This test certainly confirmed the value of using a sniffer tool such as tcpdump as part of the testing program. This test result implies that the rules on the firewall are not properly configured. This issue will be evaluated in more detail during the firewall configuration review.

Nessus was configured to test the mail server for any potential vulnerabilities. The nessus results are as follows:

Nessus Scan Report

Number of hosts which were alive during the test : 1
Number of security holes found : 0
Number of security warnings found : 0
Number of security notes found : 1

List of the tested hosts :

- 10.10.10.1*(Security notes found)*

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

10.10.10.1 :
List of open ports :

- *smtp (25/tcp) (Security notes found)*

Information found on port smtp (25/tcp)

Remote SMTP server banner :
--Banner message removed for client privacy--
214-This server supports the following commands:214 HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH TURN ATRN ETRN BDAT VRFY

Nessus determined that the mail server would reply to commands such as helo, mail and data. A test was conducted on the mail server to determine whether mail could be relayed through this server. To conduct this test I used Host Explorer to telnet from the Internet to the server on port 25. Attached is a copy of the telnet session where I was able to create an email message on the server and mail it to my Internet mailbox. This test proved that the mail relay option allowed Internet addresses to forward mail through this server.

220 abc.mail.com --Banner message removed for client privacy--
Ready2
HELO ABCCOMPANY
250 abc.mail.com Welcome ABCCOMPANY
MAIL FROM:P_TEST@ABC.COM
250 P_TEST@ABC.COM ... OK
RCPT TO:TEST@NBNET.NB.CA
250 TEST@NBNET.NB.CA ... OK
DATA
354 Enter mail, end with "." on a line by itself
THIS IS A TEST MESSAGE, TO TEST MAIL RELAY
.
250 Mail accepted

A mail message was successfully delivered to my Internet mail account.

Major Issue: Mail Relay is enabled on the mail server, this would allow Spam mail to be passed through this server and allow someone to spoof email messages as ABC Company.

Test	Expected Response	Notes	Pass/Fail
Ping DMZ network from the Internet using nmap	No Ping packets detected on the DMZ network	No Ping packets detected	Pass

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Perform port scan on all DMZ network addresses from the Internet using nmap and SuperScan	Only expect to see TCP port 25 directed to the mail server.	Only TCP port 25 was passed through the firewall.	Pass
Ping DMZ network from the internal network using nmap	No Ping packets detected on the DMZ network	No Ping packets detected	Pass
Perform port scan on all DMZ network addresses from the internal network using nmap and SuperScan	Only expect to see TCP port 25 directed to the mail server.	Ports 25, 80, 119 and 443 were permitted through the firewall and detected by the system running tcpdump.	Fail
Scan all responsive addresses using nessus	Expect response from the mail server. Expect that nessus will not detect any weaknesses	Security notes received from nessus on the mail server only.	Pass
Manually test any vulnerabilities detected by nessus	No weaknesses expected	Tests conducted prove that mail from the Internet can be relayed through the mail server	Fail

3. Test access to the internal network from the Internet

For this test the PC running tcpdump was connected to the ABC Company internal network. Port scans using nmap and SuperScan were conducted from an Internet connected PC directed at the internal network of 10.10.11.0 subnet mask 255.255.255.0. As requested by ABC Company a denial of service type of attack will not be conducted. The number of addresses scanned through the firewall during this test will be limited. Three valid internal addresses will have the complete range of IP ports scanned, while the remaining network addresses will have the IP ports lower than 1026 scanned. This test was conducted after normal work hours to lessen the potential impact to service for the computer users.

The SuperScan test was run first to determine whether any of the addresses would respond to a Ping. There was no response during this test.

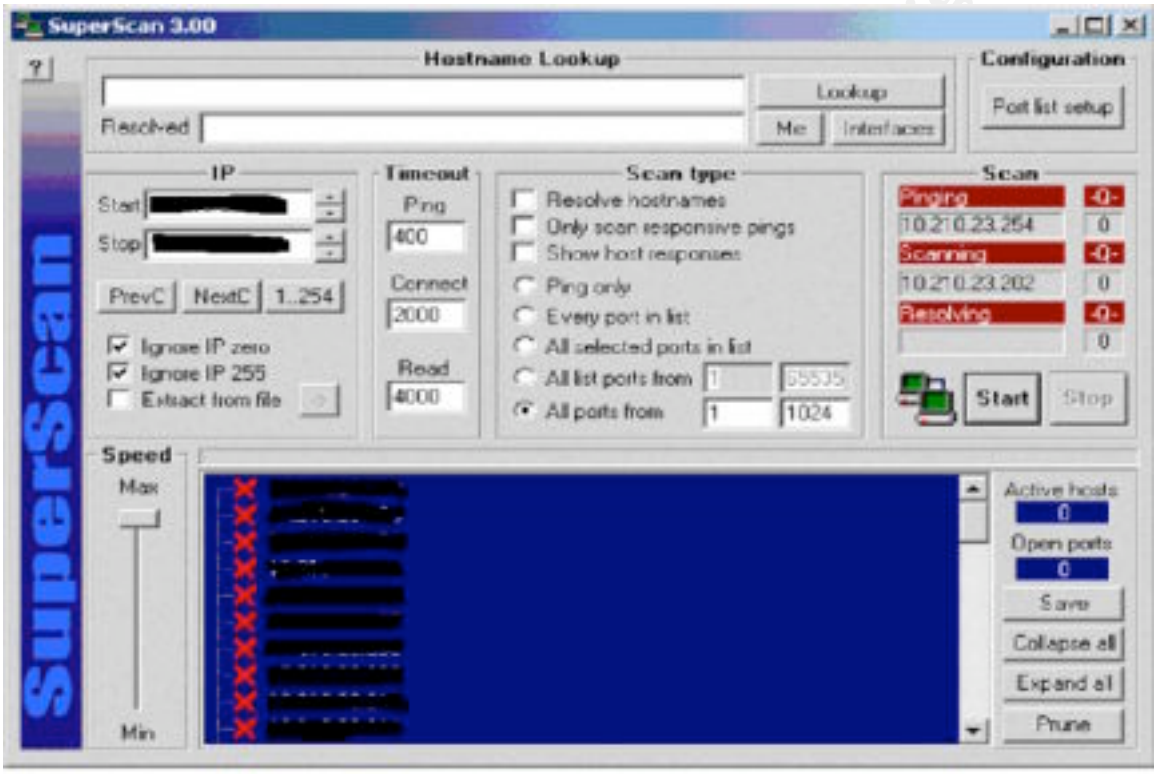
The nmap command used to scan the first three addresses on the ABC Company internal network:
"nmap –sS –p 1-65000 –P0 10.10.11.5,10.10.11.2,10.10.11.3"

nmap did not receive any response from any of the three addresses scanned.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

A additional nmap scan of the complete internal network of ABC Company (ports 1-1026), also did not provide any response.

The SuperScan test included all internal addresses for ABC Company, with the same results:



The results from tcpdump showed that no ports from either scan test were passed through the firewall. The firewall logs were also reviewed and showed that all ports scanned were dropped and logged on the firewall.

Test	Expected Response	Notes	Pass/Fail
Ping internal network using nmap and SuperScan.	No Ping packets detected on the internal network.	No Ping Packets detected by tcpdump on the internal network.	Pass
Perform port scan on all internal network addresses using nmap.	Expect that no IP packets from the test device will be detected on the internal network.	No IP Packets from the scan detected on the internal network.	Pass
Scan all responsive addresses using nessus	Expect that nessus will not detect any weaknesses	No addresses responded, nessus scan was not conducted.	Pass
Manually test any	No weaknesses	No weaknesses	Pass

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

vulnerabilities detected by nessus	expected	detected.	

4. War Dialing test on the ABC Company telephone lines

To ensure that no other entry points such as a modem are connected to the ABC Company computer network a war dialing test was conducted using THC-SCAN. The initial list of telephone numbers was prepared by the IT Manager at ABC Company working with his contacts at the local telephone company (upon request this list was provided by the telephone company in an Excel spreadsheet). The list was then reviewed by the IT Manager to confirm that all numbers appeared accurate, he also removed 2 numbers for the 24 hour security desk. He was concerned that if these numbers were dialed, then disconnected, an unnecessary level of concern could be raised. Together with the IT Manager, I physically confirmed that these two lines were connected to the lobby security desk and a security office and that no modems are in either of these locations.

Procedure for testing:

- The spreadsheet was converted to a text file with each telephone line to be tested on a separate line in the file.
- The war dialing test was conducted over two evenings. Due to time constrains the number of telephone lines tested could not be completed in the first evening. The remaining telephone numbers and the busy lines were tested on the second evening.
- The command used to start the test was: "**thc-scan @c:\test.txt**"

The results of the war dialing test is as follows:

(Please note for confidentiality the telephone numbers have been randomly changed, if these numbers match a valid modem line in another organization this is purely coincidence.)

Carrier:
****** 13-03-2002
5556148 No Carrier(0) 14sec
5556420 No Carrier(0) 32sec
5556195 No Carrier(0) 30sec
5559158 No Carrier(0) 25sec
5556131 No Carrier(0) 29sec
5556992 Carrier(0) 64sec
5552129 No Carrier(0) 21sec
5552707 No Carrier(0) 21sec
5553579 No Carrier(0) 34sec
5558509 No Carrier(0) 34sec
5553547 No Carrier(0) 31sec

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

5553356 Carrier(0) 96sec
5554900 No Carrier(0) 31sec
5554602 No Carrier(0) 31sec
5554992 No Carrier(0) 32sec
5554776 No Carrier(0) 33sec
5557703 No Carrier(0) 28sec
5558879 No Carrier(0) 36sec
5552471 No Carrier(0) 40sec

Busy:
****** 13-03-2002
5552023 Busy(0) 7sec
5552225 Busy(0) 11sec
5556038 Busy(0) 34sec
5552100 Busy(0) 32sec
5552101 Busy(0) 11sec

- In summary 17 fax lines were detected, 2 modem lines were detected and 5 lines were busy.
- These results were provided to ABC Company's IT Manager for verification.
    - The two modem lines detected were determined to be unauthorized modems connected to Personal Computers. Since ABC Company does not have an authorized method to provide remote computer access to employees, these modems were put in place by two employees for remote access into their office computers. These modems were removed upon discovery. **Issue: A properly designed and secured method of remote access for employees into the computer network should be evaluated.**
    - The fax lines were verified by ABC Company. The corporate list of fax numbers matched the test results received from this scan.
    - The telephone lines that are busy are also to be considered suspicious. **Issue: The busy telephone lines should be manually verified.**
- The "carriers" file was reviewed for the two modem lines detected to confirm that they were valid modem responses. The responses received for these lines were:

13-03-2002 22:12:02 Dialing... 5556992

CONNECT 9600 V42bis

fG0
!2g3=7

OUsername : 3

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
OUsername : 3?
Password :
Login Failure!
OUsername : 3GUEST
Password :
Login Failure!
OUsername : 3INFO
Password :
Login Failure!

Too many attempts!

+++

[CARRIER LOST AFTER 30 SECONDS]

NO CARRIER

13-03-2002 22:30:42 Dialing... 5553356

CONNECT 24000 V42bis

 X }
 .Please press <Enter>...
 |
Enter login name: ? :
Enter password:
 {Invalid login. Please try again. |
Enter login name: guest :
Enter password:
 {Invalid login. Please try again. |
Enter login name: INFO :
Enter password:
Login unsuccessful
NO CARRIER

[CARRIER LOST AFTER 21 SECONDS]
```

© SANS Institute 2000 - 2002, Author retains full rights.

5. Scan the internal network

The internal network (10.10.11.0 subnet mask 255.255.255.0) was scanned using nmap and SuperScan. The nmap command that was used to scan the internal network was:

```
nmap –sS –p 1-1026 10.10.11.1-255
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

A sample of the results from nmap are as follows:

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on  (10.10.11.3):
(The 1023 ports scanned but not shown below are in state: closed)
Port       State       Service
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
445/tcp    open        microsoft-ds

Interesting ports on  (10.10.11.4):
(The 1023 ports scanned but not shown below are in state: closed)
Port       State       Service
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
445/tcp    open        microsoft-ds

Interesting ports on  (10.10.11.5):
(The 1024 ports scanned but not shown below are in state: closed)
Port       State       Service
23/tcp     open        telnet
515/tcp    open        printer

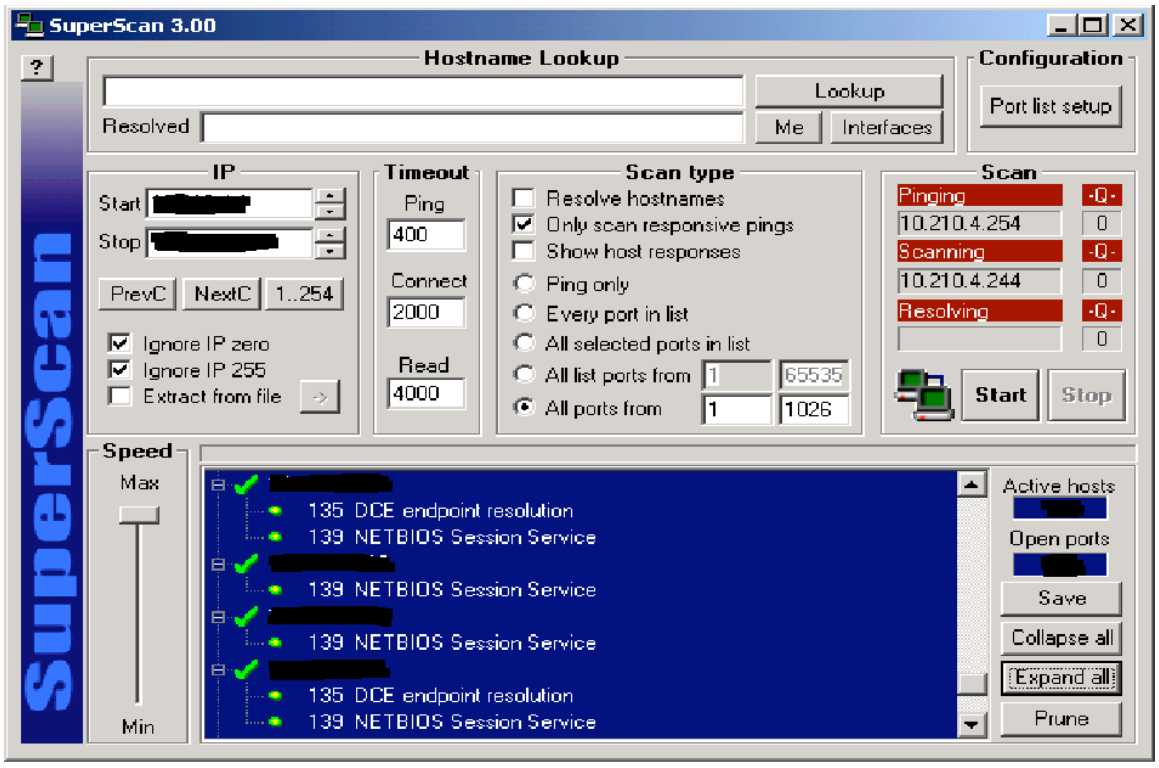
Interesting ports on  (10.10.11.6):
(The 1025 ports scanned but not shown below are in state: closed)
Port       State       Service
139/tcp    open        netbios-ssn

Interesting ports on  (10.10.11.9):
(The 1025 ports scanned but not shown below are in state: closed)
Port       State       Service
139/tcp    open        netbios-ssn
```

SuperScan was used as a second verification of the test results. The following is a screen image of the SuperScan results:

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

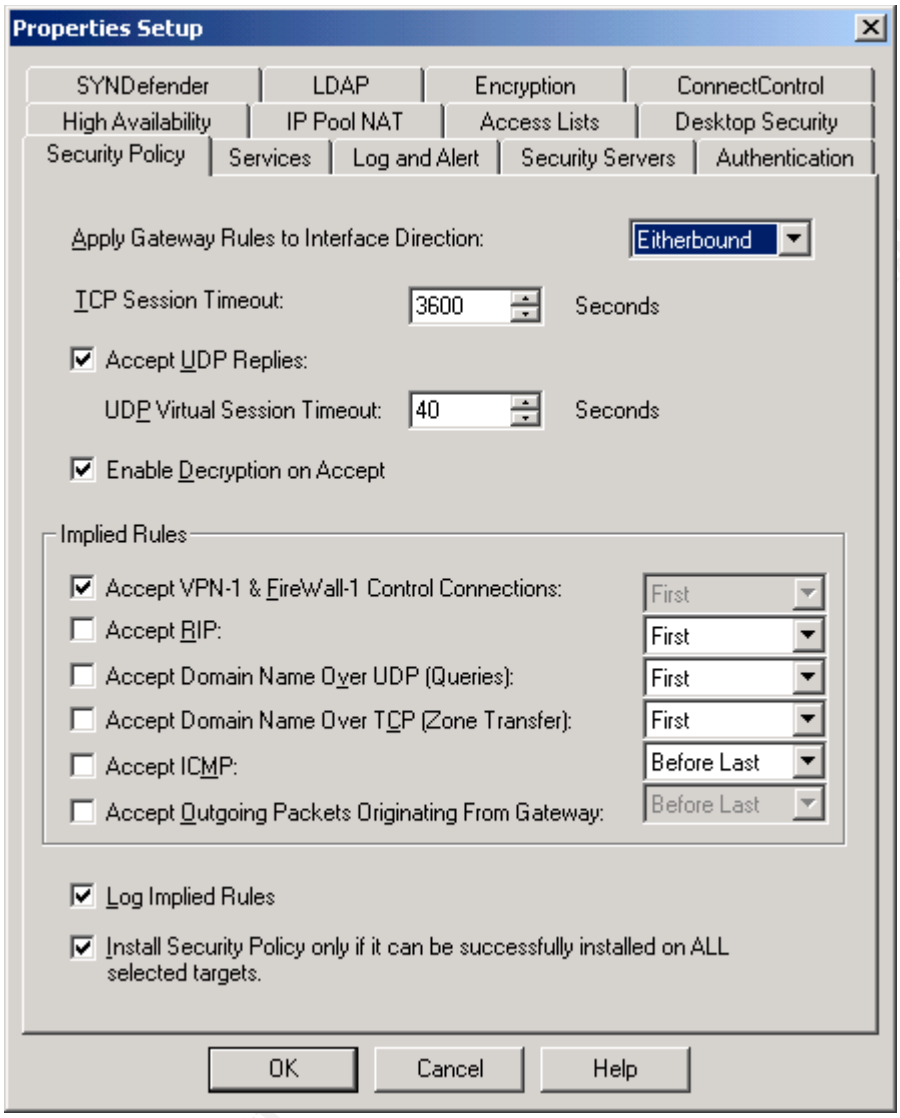


Neither scan detected any systems that appear to be a router or a network switch. The scan detected a number of PC's running Microsoft windows, printers, LAN servers, the corporate billing system and the internal mail server. From these results we have reasonably verified that no additional network connections into the ABC Company are present.

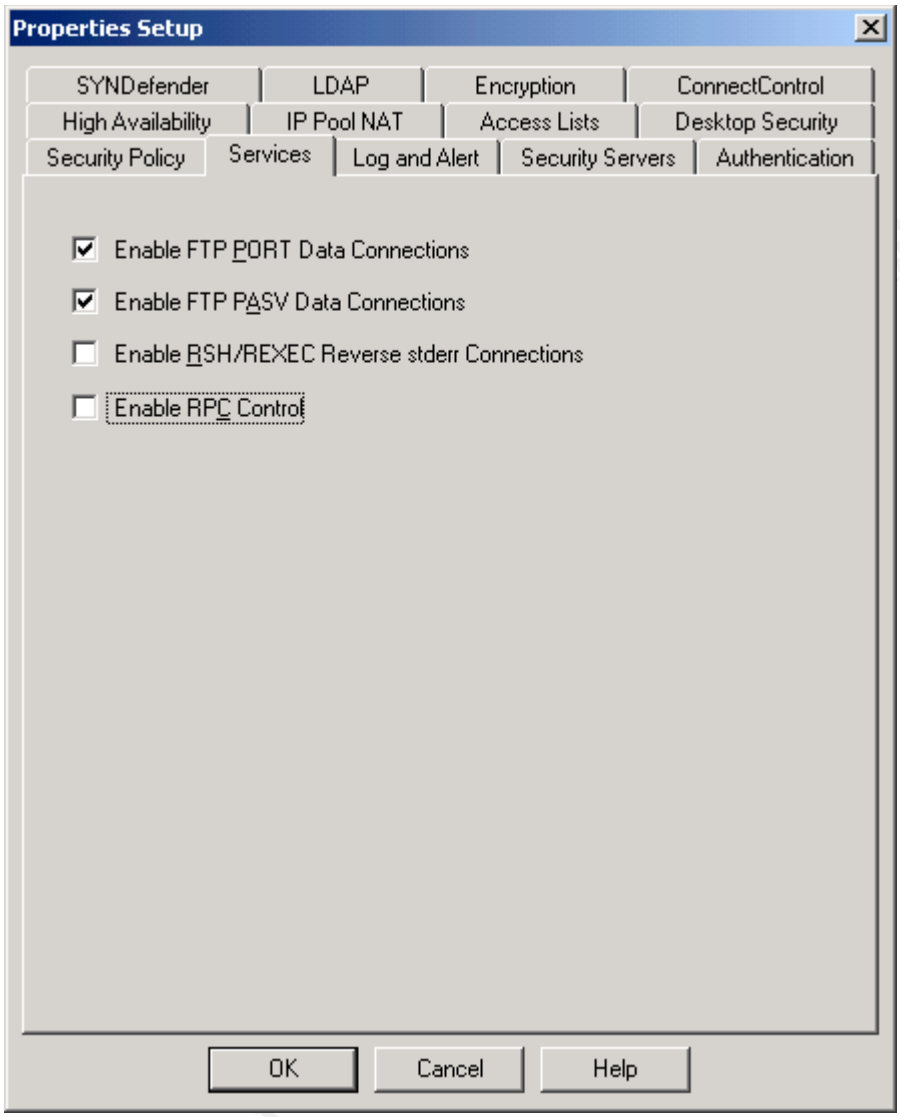
6. Review the Checkpoint system configuration

A review was conducted on the Checkpoint configuration. Attached are some screen shots of the current configuration:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Test	Expected Response	Notes	Pass/Fail
Verify Checkpoint version and patch level	Latest system patches are applied	System is Checkpoint 4.1, latest patches have been applied.	Pass
TCP session timeout	Option set for 900 seconds or less is recommended, option set for 3600 seconds or less will be considered a pass	TCP session timeout set for 3600 seconds.	Pass
FW-1 Control global option	Option is not enabled	FW-1 Control option is enabled.	Fail
ICMP global option	Option is not enabled	ICMP option is disabled.	Pass

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

DNS Global option	Option is not enabled	DNS option is disabled.	Pass
The firewall object has the ports properly configured	All port addresses and subnet masks are correct	The addresses and subnets match the port configuration on the firewall.	Pass
The firewall object has properly defined spoofing rules	Spoofing rules for the DMZ network and Internal network include the proper network information. The Internet port is defined as "other"	No spoofing rules are defined.	Fail
Rule is in place for the administrators	This rule restricts access to only the system administrators	One rule is on place to permit Secure Shell access to only the two administrators. No rule is in place for the Firewall-1 management.	Fail
Rule is in place that hides the firewall	A drop rule is in place that blocks all other users from access the firewall	This rule is in place. However from testing it was determined that the users can access the firewall on ports 256, 257 and 258.	Fail
Verify the firewall rules	All rules are essential to the function of this firewall.	A review of the rules show that all rules are reasonable and appear to be essential.	Pass
Review the order of the rules	Rules are in the following sequence: • Firewall administration • Stealth rule for firewall • Incoming access • Communications between networks • Drop rule for all internal networks • Outgoing rules to the Internet	•The only administration rule in place on the firewall is to permit Secure Shell access from the two administrators. **Fail** •A rule to block all other access to the firewall is in place. **Pass** •Incoming access to the DMZ mail server is the third group of rules. **Pass** •Rules for access	Fail

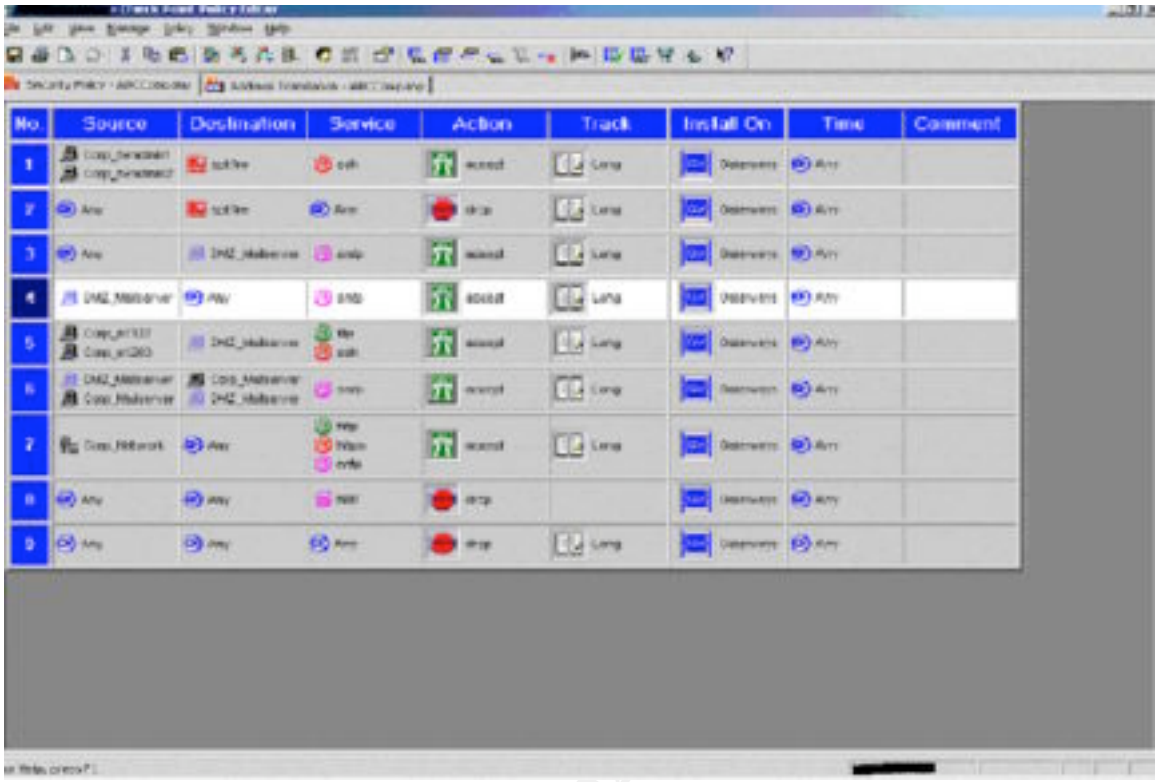
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

	• Drop rule for all other access	between the internal and DMZ mail server is the fourth set of rules. **Pass** •There is no rule in place to restrict access to the internal networks. **Fail** •Rules are in place to allow access to the Internet for specific communication protocols. **Pass** •A final rule to drop all other access is in place. **Pass**	
Verify logging	All critical rules have logging enabled	Logging is enabled on all critical communications allowed and denied.	Pass
Comments	The comments field provides information when rules were added and why.	There are no comments in this field.	Fail
Date and time of last reboot or rule change	The last change occurred during a maintenance window after normal work hours.	The last rule change was at 17:55 on a workday. Outside of the normal work hours. ABC Company do not have a specific maintenance window for computer changes.	Pass
Review applied rule set in the status window	The rule set last applied to the firewall, matches the rule sets reviewed in this audit.	The rule set applied to the firewall matches the only rule set existing on the manager.	Pass

7. Review the Checkpoint rules

Attached is a screen image of the rules currently in place on this firewall.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



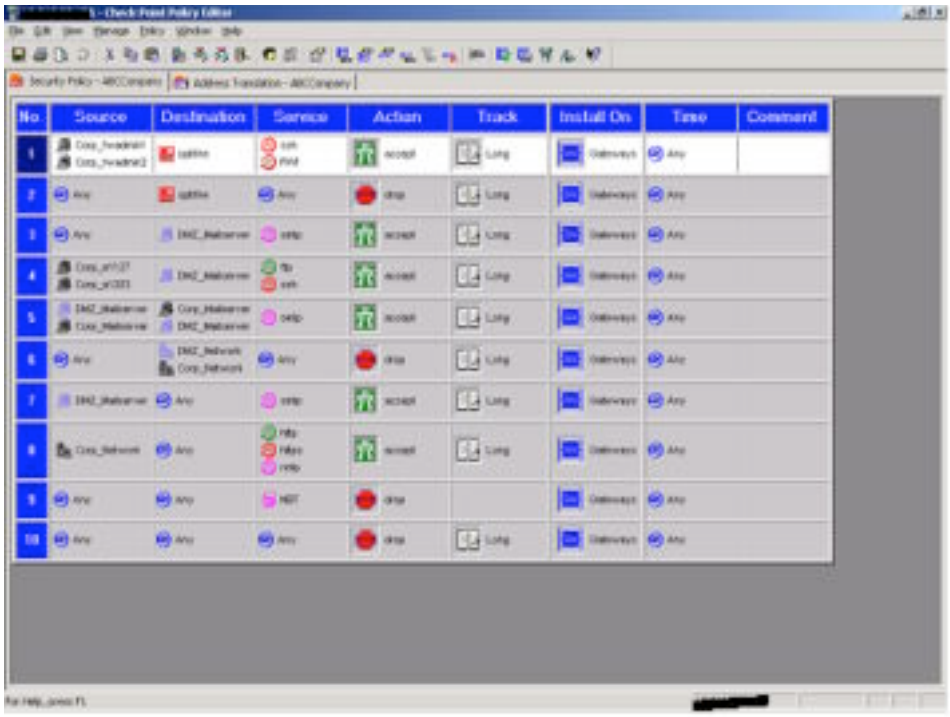
A review of the rules indicate that the mail server on the DMZ network should be permitted by the firewall to communicate on TCP port 25 (SMTP) to any address within the ABC Company internal network. The intended design is for this access to only be permitted between the internal mail server and the DMZ mail server. To perform an objective test on this issue would require a test be conducted from the address of the DMZ mail server to the internal network. Using a system running tcpdump on the internal network, it could be positively proven whether this issue is valid. However since this is a production firewall and network being audited, and ABC Company did not want their DMZ mail server to be affected, the actual test was not conducted for this audit. To confirm that this was in fact an issue, I did simulate this issue on my test firewall and was in fact able to communicate through the firewall on TCP port 25 to all networks connected to this firewall.

The main issue with the rules identified during this review is the order in which they are in place. Two changes are recommended to enhance the security of the firewall:

1. Insert a rule to drop all access to the Internal network and DMZ network. This rule must be placed before any additional rules that use the destination "ANY".
2. Move the rule to allow the DMZ mail server to send mail out to the internet below the rule inserted in the previous recommendation.

Attached is a screen image of the recommended rule configuration:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



In this configuration the firewall rule permitting email to the Internet (source - DMZ Mailserver, Destination – ANY) has been moved from rule #4 to rule #7. Also a new rule has been inserted as rule #6, blocking all communications to the internal network and the DMZ network.

8. Review the Sun operating system configuration

This review of the operating system including reviewing many of the system configuration options. Displaying the results from all of these tests will in my opinion create an unnecessary amount of logs for this report. Some samples of the system reviews are provided as information for this audit:

```
$ more /etc/inetd.conf
##
##ident "@(#)inetd.conf 1.44    99/11/25 SMI"   /* SVr4.0 1.5   */
##
##
## Configuration file for inetd(1M).  See inetd.conf(4).
##
## To re-configure the running inetd process, edit this file, then
## send the inetd process a SIGHUP.
##
## Syntax for socket-based Internet services:
##  <service_name> <socket_type> <proto> <flags> <user> <server_pathname>
<args>
##
## Syntax for TLI-based Internet services:
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
##
##  <service_name> tli <proto> <flags> <user> <server_pathname> <args>
##
## IPv6 and inetd.conf
## By specifying a <proto> value of tcp6 or udp6 for a service, inetd will
## pass the given daemon an AF_INET6 socket.  The following daemons have
## been modified to be able to accept AF_INET6 sockets
##
##      ftp telnet shell login exec tftp finger printer
##
## and service connection requests coming from either IPv4 or IPv6-based
## transports.  Such modified services do not normally require separate
## configuration lines for tcp or udp.  For documentation on how to do this
## for other services, see the Solaris System Administration Guide.
##
## You must verify that a service supports IPv6 before specifying <proto> as
## tcp6 or udp6.  Also, all inetd built-in commands (time, echo, discard,
## daytime, chargen) require the specification of <proto> as tcp6 or udp6
##
## The remote shell server (shell) and the remote execution server
## (exec) must have an entry for both the "tcp" and "tcp6" <proto> values.
##
## Ftp and telnet are standard Internet services.
##
#ftp    stream  tcp6    nowait  root    /usr/sbin/in.ftpd       in.ftpd
#telnet stream  tcp6    nowait  root    /usr/sbin/in.telnetd    in.telnetd
##
## Tnamed serves the obsolete IEN-116 name server protocol.
##
#name   dgram   udp     wait    root    /usr/sbin/in.tnamed     in.tnamed
##
## Shell, login, exec, comsat and talk are BSD protocols.
##
#shell  stream  tcp     nowait  root    /usr/sbin/in.rshd       in.rshd
#shell  stream  tcp6    nowait  root    /usr/sbin/in.rshd       in.rshd
#login  stream  tcp6    nowait  root    /usr/sbin/in.rlogind    in.rlogind
#exec   stream  tcp     nowait  root    /usr/sbin/in.rexecd     in.rexecd
#exec   stream  tcp6    nowait  root    /usr/sbin/in.rexecd     in.rexecd
#comsat dgram   udp     wait    root    /usr/sbin/in.comsat     in.comsat
#talk   dgram   udp     wait    root    /usr/sbin/in.talkd      in.talkd
##
## Must run as root (to read /etc/shadow); "-n" turns off logging in utmp/wtmp.
##
#uucp   stream  tcp     nowait  root    /usr/sbin/in.uucpd      in.uucpd
##
## Tftp service is provided primarily for booting.  Most sites run this
## only on machines acting as "boot servers."
##
##tftp  dgram   udp6    wait    root    /usr/sbin/in.tftpd      in.tftpd -s /tftpboot
##
## Finger, systat and netstat give out user information which may be
## valuable to potential "system crackers."  Many sites choose to disable
## some or all of these services to improve security.
##
#finger stream  tcp6    nowait  nobody  /usr/sbin/in.fingerd    in.fingerd
##systat        stream  tcp     nowait  root    /usr/bin/ps             ps -ef
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
##netstat       stream  tcp     nowait  root    /usr/bin/netstat        netstat -f inet
##
## Time service is used for clock synchronization.
##
#time   stream  tcp6    nowait  root    internal
#time   dgram   udp6    wait    root    internal
##
## Echo, discard, daytime, and chargen are used primarily for testing.
##
#echo   stream  tcp6    nowait  root    internal
#echo   dgram   udp6    wait    root    internal
#discard        stream  tcp6    nowait  root    internal
#discard        dgram   udp6    wait    root    internal
#daytime        stream  tcp6    nowait  root    internal
#daytime        dgram   udp6    wait    root    internal
#chargen        stream  tcp6    nowait  root    internal
#chargen        dgram   udp6    wait    root    internal
##
##
## RPC services syntax:
##  <rpc_prog>/<vers> <endpoint-type> rpc/<proto> <flags> <user> \
##  <pathname> <args>
##
## <endpoint-type> can be either "tli" or "stream" or "dgram".
## For "stream" and "dgram" assume that the endpoint is a socket descriptor.
## <proto> can be either a nettype or a netid or a "*". The value is
## first treated as a nettype. If it is not a valid nettype then it is
## treated as a netid. The "*" is a short-hand way of saying all the
## transports supported by this system, ie. it equates to the "visible"
## nettype. The syntax for <proto> is:
##      *|<nettype|netid>|<nettype|netid>{[,<nettype|netid>]}
## For example:
## dummy/1      tli     rpc/circuit_v,udp       wait    root    /tmp/test_svc   test_svc
##
## Solstice system and network administration class agent server
#100232/10      tli     rpc/udp wait root /usr/sbin/sadmind     sadmind
##
## Rquotad supports UFS disk quotas for NFS clients
##
#rquotad/1      tli     rpc/datagram_v  wait root /usr/lib/nfs/rquotad  rquotad
##
## The rusers service gives out user information.  Sites concerned
## with security may choose to disable it.
##
#rusersd/2-3    tli     rpc/datagram_v,circuit_v        wait root
/usr/lib/netsvc/rusers/rpc.rusersd
        rpc.rusersd
##
## The spray server is used primarily for testing.
##
#sprayd/1       tli     rpc/datagram_v  wait root /usr/lib/netsvc/spray/rpc.sprayd
rpc.sprayd
##
## The rwall server allows others to post messages to users on this machine.
##
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
#walld/1                tli     rpc/datagram_v  wait root /usr/lib/netsvc/rwall/rpc.rwalld
rpc.
rwalld
##
## Rstatd is used by programs such as perfmeter.
##
#rstatd/2-4     tli   rpc/datagram_v wait root /usr/lib/netsvc/rstat/rpc.rstatd
rpc.rstatd
##
## The rexd server provides only minimal authentication and is often not run
##
##rexd/1          tli  rpc/tcp wait root /usr/sbin/rpc.rexd     rpc.rexd
##
## rpc.cmsd is a data base daemon which manages calendar data backed
## by files in /var/spool/calendar
##
#100068/2-5     dgram   rpc/udp wait root /usr/openwin/bin/rpc.cmsd     rpc.cmsd
##
## Sun ToolTalk Database Server
##
#100083/1       tli     rpc/tcp wait root /usr/dt/bin/rpc.ttdbserverd rpc.ttdbserverd
##
## UFS-aware service daemon
##
##ufsd/1        tli     rpc/*   wait    root    /usr/lib/fs/ufs/ufsd    ufsd -p
##
## Sun KCMS Profile Server
##
#100221/1       tli     rpc/tcp wait root /usr/openwin/bin/kcms_server  kcms_server
##
## Sun Font Server
##
#fs             stream  tcp     wait nobody /usr/openwin/lib/fs.auto    fs
##
## CacheFS Daemon
##
#100235/1 tli rpc/tcp wait root /usr/lib/fs/cachefs/cachefsd cachefsd
##
## Kerberos V5 Warning Message Daemon
##
#100134/1       tli     rpc/ticotsord   wait    root    /usr/lib/krb5/ktkt_warnd
ktkt_warnd
##
## Print Protocol Adaptor - BSD listener
##
#printer                stream  tcp6    nowait  root    /usr/lib/print/in.lpd   in.lpd
##
## GSS Daemon
##
#100234/1       tli     rpc/ticotsord   wait    root    /usr/lib/gss/gssd gssd
##
## AMI Daemon
##
#100146/1       tli     rpc/ticotsord   wait    root    /usr/lib/security/amiserv
amiserv
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
#100147/1      tli     rpc/ticotsord   wait    root    /usr/lib/security/amiserv
amiserv
##
## OCF (Smart card) Daemon
##
#100150/1      tli     rpc/ticotsord   wait    root    /usr/sbin/ocfserv       ocfserv

$ more hosts.allow
# Daemons listed separately in case greater restrictions are desired
# for non encrypted (telnet/ftp) traffic than encrypted (ssh) traffic
SSHD:          10.10.11.21/255.255.255.255,10.10.11.43/255.255.255.255
$ more hosts.deny
#Default deny (deny anything not in hosts.allow)
ALL:    ALL

$ more login
#ident  "@(#)login.dfl  1.8     96/10/18 SMI"   /* SVr4.0 1.1.1.1       */
# Set the TZ environment variable of the shell.
#
#TIMEZONE=EST5EDT
# ULIMIT sets the file size limit for the login.  Units are disk blocks.
# The default of zero means no limit.
#
#ULIMIT=0
# If CONSOLE is set, root can only login on that device.
# Comment this line out to allow remote login by root.
#
CONSOLE=/dev/console

# PASSREQ determines if login requires a password.
#
PASSREQ=YES

# ALTSHELL determines if the SHELL environment variable should be
set
#
ALTSHELL=YES

# PATH sets the initial shell PATH variable
#
#PATH=/usr/bin:
# SUPATH sets the initial shell PATH variable for root
#
#SUPATH=/usr/sbin:/usr/bin
# TIMEOUT sets the number of seconds (between 0 and 900) to wait
before
# abandoning a login session.
#
TIMEOUT=200
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
# UMASK sets the initial shell file creation mode mask.  See umask(1).
#
#UMASK=022
# SYSLOG determines whether the syslog(3) LOG_AUTH facility should
be used
# to log all root logins at level LOG_NOTICE and multiple failed login
# attempts at LOG_CRIT.
#
SYSLOG=YES
$
```

Test	Expected Response	Notes	Pass/Fail
Verify system version and patch level	Latest system patches are applied	The patches applied to the system were reviewed and are the current version.	Pass
Check administrator access to root (/etc/default//login)	Administrator must "su" to root	Root can only login direct at the console.	Pass
Check the user accounts on the system (more /etc/passwd)	Access is limited to the administrators and the security officer	Only three accounts on the system, the two administrators and root. **Note:** The security officer does not have access to review the system logs.	Pass
Verify password expiry times	Passwords automatically expire every 30 days.	Password expiry is set for 30 days.	Pass
Password length	Password minimum length is 8 characters	Minimum length password is 8 characters.	Pass
Verify account with empty passwords (logins –p)	No accounts exist with empty passwords	No accounts have empty passwords.	Pass
Verify the accounts with UID 0 (awk –F: '($3 == 0) {print $1}' etc/passwd)	The only account that has UID 0 is root	Root is the only account with UID 0.	Pass
Administrator access to the firewall	Administrator uses secure shell and telnet is disabled	Secure Shell is the only access to administer the operating system. Secure Shell access is also restricted to only the two	Pass

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

		administrators IP addresses.	
The OS banner does not provide sensitive information	The banner has been changed to not provide system information and identify this as a restricted system. Banner includes a legal disclaimer that unauthorized access is not permitted.	Banner message does not provide any information on the system or ABC Company. Banner includes this system as a private system. Banner message received: *This is a private computer system, unauthorized access is not permitted*	Pass
Verify active services (/etc/inetd.conf)	Only services required for the firewall are active	Only the essential services are active on the system. Secure Shell is the only access permitted to communicate direct with the firewall. Secure Shell is restricted by IP address in the operating system configuration.	Pass
Review routing protocol	Static routes are being used	Only static routes are in place.	Pass
Review system routes	Only essential routes are in place on the system	All routes are essential, all routes have traffic.	Pass
Check unused ports on the firewall	All unused ports are disabled	Only the three active ports on the firewall are enabled, all other ports are disabled.	Pass
Are audit logs enabled?	Audit logs are enabled and log key system activities	Audit logs are enabled, log was reviewed during this audit.	Pass
Review audit logs	No suspicious activity is detected	Audit log activity was reviewed. Activity logged included: • Login and logout • Access to root • System startup and system shutdown • Stop and start of firewall service No suspicious activity	Pass

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

		detected.	

9. Review and test physical security

The firewall is physically located in ABC Company computer room on the 6th floor of their main office building. All telecommunications equipment to connect the firewall to the internet and internal network are also located in this computer room. Attached are the results from the physical security review conducted.

Test	Expected Response	Notes	Pass/Fail
Availability of UPS Power	UPS power is in place that will maintain the firewall for an extended period of time	The firewall is connected to a UPS battery backup. The unit has been tested and will only hold the equipment for approximately 30 minutes. ABC Company does have generator backup located in the basement, this unit automatically switches on in the event of a power failure. Not all floors of the building are covered by the generator, however all of the sixth floor is covered.	Pass
Fire Suppression	Acceptable methods of fire suppression are in place with the computer room The fire extinguishers have been recently inspected	This room used to be a part of the floor and was converted to a computer room about two years ago, the sprinkler system is still in place. When asked if the sprinklers are actually charged with water I was informed **YES**. The current sprinkler system has been in place for approximately 10 years, while the computer room was built on the floor about 4 years ago. No changes have been made	Fail

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

		to the sprinkler system to accommodate the needs of the computer room.	
Backup Media	Backup media is stored in a physically secure location	The backup tapes for the other systems are stored in a filing cabinet within the computer room, cabinet doors are closed. The weekly off site backup is stored on the other side of the city in a building owned by ABC Company. The firewall is not backed up, therefore no media is stored.	Fail
Logging of access to computer area	Access is logged for each individual gaining access to the room.	Entry to the room required a proximity card. When questioned who had access to this room I was informed that most of the IT group, approximately 12 people, have access. The proximity card system does record entry to the room, but does not record exits from the room. No card is needed to exit. All use of the proximity card is logged.	Pass
Monitoring of the computer room	Additional surveillance controls are in place, such as video surveillance.	No other surveillance controls such as video surveillance is in place.	Fail
Environmental conditions	The computer room is an environmentally controlled area. Review includes temperature, humidity, dust and general condition of the	The environmental conditions are very good. Room is clean, with raised floor and air conditioning.	Pass

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

	area.		
Cabling	All connections into the firewall are labeled.	All cabling is connected behind the cabinets and while it is a little messy it is not in bad shape. The cables connected to the firewall are not labeled.	Fail
Test physical access to the computer room during work hours	No unauthorized access should be obtained.	Access into the computer room was requested from 3 employees at different times during the day. One employee informed me that they did not have access to the room, while the other two did have access but would not allow me to enter the room without an escort.	Pass
Test physical access to the computer room after normal work hours	No unauthorized access should be obtained.	To be able to enter the building after hours you are required to sign in at the security desk in the lobby. The auditor was able to successfully sign in and gain access to the 6th floor. All doors on the 6th floor were locked and further access could not be obtained.	Pass

10. Review corporate security policies

A review of the corporate security policies was conducted through a review of all documented policies and through interviews with ABC staff. The results of these activities is as follows:

No written security policies exist for ABC Company, there is a project in place to create these security polices, but none are in place at the time of this audit. **Issue: Security policies should be documented, approved and communicated to all employees.**

UNIX Admin
Describe your administration role
Creating users:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- When you create a new user, what is the process by which you receive the request? **Only two users on the system, do not create many user accounts. These two administrators perform both the Unix administration and Checkpoint administration. The primary firewall administrator is estimated to perform 85% of this role, with the backup administrator sharing after hours support and backup during vacation time.**
- Who authorizes the request? **Any new administrators would be authorized by the IT Manager.**
- What access to information standards are provided to all new users? **N/A**
- Do new users get training/documentation? **Both administrators have received Checkpoint Firewall –1 training and basic Unix admin training.**

Passwords:

- What is the password standard for your system?
    - Password is not displayed during login? **NO**
        - Perform test to verify. **This was verified by watching the administrator log on to the system.**
    - Password can be changed by the user. **Yes**
        - Perform test to verify. **Administrator changed their personal password as requested.**
    - Password is changed frequently. **Passwords must be changed on this system every 30 days.**
    - Passwords standards.
        - Upper case letters
        - Lower case letters
        - Numbers
        - Special characters. **This password test included the administrator attempting to change their password to a dictionary word, a word with only lower case and a word with only upper case characters. The system would not permit the use of a password with a word and without a combination of upper case and lower case characters. A strong password standard is in place.**
        - Automatic timeout feature exists. **Yes**
            - Perform test to verify. **The active login session timed out during our interview time, the user was prompted to reenter the password to access the system.**
- Are they enforced by the systems technology? Or just what the user is asked to follow? **Enforced by the system.**
- Describe the process followed for a user to get their password changed? T**here are only two administrators, they must go to the other administrator. This does not occur often. Root password is recorded on paper, sealed in an envelope and secured in the corporate vault. The envelope is labeled that only the two administrators or the IT Manger may open the envelope. When the root password is changed, this envelope must be replaced.**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

        - How do they verify the persons identity! **N/A**
- How often are passwords required to be changed?
    - Is this an automated process?

Removing users:

- When an employees leaves ABC Company, what is the process to get their user account removed from the system? **If an administrator leaves this position the IT Manager is responsible to ensure that access is removed.**
- Who notifies you to remove the account? **IT Manager.**
- Do you ever get to check the list of users on the system versus active employees? **Not asked since there are only two user accounts. This was confirmed during the system configuration review.**
- Do you remove/disable accounts that have been inactive for a period of time? **N/A.**

Administration access:

- Who has administration access to this system? How many? **Two administrators.**
- Do they share an administration account or have separate Login accounts? **They have separate login accounts and must "su" to root. A test was conducted that included the administrator attempting to remotely login as root. The administrator was not able to login directly as root.**
- If they share a common admin account what are the password standards in place (length of password, how often is it changed) **The root password is 8 characters in length, a combination of upper case and lower case characters and includes non-alpha numeric characters. A strong password standard is in place.**
- Can you do your administration remotely if necessary? **Access is available from the administrators desk, but not from home.**
- If so, how do you get access?
    - Is this using telnet or Secure Shell? **Use Secure Shell. This was confirmed during the configuration review and testing, telnet is not active on the system.**

System technical questions

- What is the process to patch the system or upgrade the OS? **The system administrators schedule a maintenance window for all patches and upgrades.**
- How often is this done? **Every 2-3 months.**
- Does someone receive security alerts on this system advising that security patches should be applied? **No**.
    - What system do they subscribe to?
    - Verify that they have received messages recently.

Change control

- Is there a process in place if a change is needed on this system? **There is a change process for all major system changes at ABC Company.**
- Who approves the changes? **The IT Manager approves all changes.**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- How are the changes communicated to you and the other system administrators? **The system change plans are discussed in our team meeting every Monday morning with the IT Manager. This auditor was on site on Monday during the IT team meeting. For privacy reasons I did not sit in on the meeting, but can confirm that this communication process is in place.**
- How is it communicated to the users? **The helpdesk sends out a message advising of the change and the potential impact on users.**

Access to information:

- What information access controls are in place? (all users have access to everything by default or only select users have access to information) **N/A**
- Who decides/approves access to restricted information? **N/A**
- What is the process followed to grant a user access to restricted information? (is it a phone call or a written request with an approval signature). **N/A**

Training:

- What training have you had to administer this system? **Each administrator has received basic Unix administration training. They have not received any advanced training sessions, but with their number of years experience in IT administration (8 years and 11 years), lack of advanced training does not appear to be a risk.**
- When was this training done? **Approximately 3 years ago for both administrators. There are other Unix systems in place at ABC Company.**
- Do you know the company security policies to follow when administering this system? **Demonstrated a good understanding of what the corporate expectations are regarding security. No formal security policies exist.**
- Do you know who to contact if you have a question regarding the corporate policies? **The IT Manager is the prime contact regarding security policies.**

Backups:

- Do you have backups? **No. This was confirmed during the physical security review. Issue: A regular backup of the system should be in place and the media stored in a secure off site location.**
- How often are backups done? **N/A**
- What is backed up? **N/A**
    - Full backups, incremental or what combination? **N/A**
- Where are the backups stored? (on site or off site?, secure or not secure location?) **N/A**
- Do you take a weekly or monthly backup tape off site? **N/A**
    - Where is the off site location? **N/A**
- Who changes and transports the tapes? **N/A**
- How long are the backup maintained (weeks or months)? **N/A**
- Do you have a disaster recovery plan in place for this system? **NO**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- What major or minor failures have you had with this system? **Have had two major failures in the past year. Both were related to a hardware failure on the server. The first failure was due to the server overheating due to the fan engine failing, firewall was out of service for approximately 7 hours (5 hours during the business day). The second failure was a failure of the Ethernet card. This required approximately 3 hours to correct since they did not have a spare card on site. Issue: This firewall is a key component for communications between ABC Company and it's customers, a disaster recovery plan should be in place to ensure that service interruption is minimized. Implementing high availability on the firewall would also greatly lessen the chances that a system failure would affect service.**
- Do you have an formal or informal process to restore from backup? **N/A**
- Have you ever tested this restore process. **N/A**
    - If so, what was the result? **N/A**

Monitoring:

- If the system fails/crashes, how are you notified? **The users would call the helpdesk.**
- Is there an system that monitors the availability? **No Issue: The service availability of the firewall should be monitored to ensure timely response in the event of a failure.**
    - Does this system monitor conditions and alert before failures (monitor drive usage and alert at 95% full)? **N/A**
- Does this system log user access/activity? **Yes**
    - If so, do you review this log? **No**
- What would be your procedure if you detected something on the system that could be a serious security breach? **Escalate to the IT Manager.**
- Is this a formal process (documented)?- Describe the process. **Informal process.**

Physical security

- Where is your server(s) located? **Computer room**
- Who has physical access to the server? **Just the IT group.**
- Does the system have UPS power? **Yes. This was confirmed during the physical security review.**

Unique issues regarding Unix:

- Do you use shadow passwords? **No. This was confirmed during the system configuration review.**
- Do you use Rlogin type of commands? **No. This was confirmed during the system configuration review.**
    - If so do you use the rhosts configuration? **N/A**
- Do administrators login direct as root or must "su" to root? **The administrators must "su" to root. A test was conducted that included the administrator attempting to remotely login as root. The administrator was not able to login directly as root.**
- Review other specific security standards documented in the corporate policies. **N/A**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Are there any issues or concerns that you have in regards to security that we should be aware of? No

Firewall administrator:

- How are rule requests received? **Rule requests are received via email or in some cases verbally. Issue: Proper authorization is not being received for firewall rules changes.**
- Do you maintain copies of the firewall rule requests? **Copies are stored in the administrators email system.**
- How long are these requests retained?
  - Verify the information by viewing the audit trail of past rule change requests. **The email messages are stored for a week or two. Only one email message that was 12 days old could be provided by the administrator as an example of a firewall change request. All other changes were either verbal or deleted. Issue: An audit log of all rule change requests should be maintained for an extended period of time for future reference.**
- Who authorizes rule changes on the firewall? **No one is required to authorize the changes.**
  - Is a signature received? (physical or electronic) **No signature is received on the rule change requests, they rely on the email address.**
- How is the security risk evaluated with these rule changes? **The administrator reviews the requests for security.**
- What is the process to review a rule request for potential security risks? **If the administrator is concerned with the security of the request, the issue is passed to the IT Manager for approval.**
- When are rule changes applied?
  - During the day or in a maintenance window? **Usually after normal work hours, approximately 6:00 PM.**
- Do you receive alerts regarding security issues on this server from Checkpoint or another source? **Manually check some web sites for security alerts, they do not subscribe to a security alert email list. Issue: Subscribing to a security alert mail list such as the alert system offered by CERT and vendor security alerts, will provide timely notification of security issues on the system.**
- How often are upgrades made on this system? **Usually every 2-3 months.**
- Do you have a backup of the firewall rules? **No**
  - **This was verified during the physical security review that no backup mechanism was in place. Issue: A regular backup of the firewall configuration, rules and logs should be in place and the media stored in a secure off site location.**
- Do you monitor the firewall activity? **Yes**
  - Who performs this monitoring function? **The firewall administrator monitors the system logs.**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

    - How often are logs reviewed? **Reviewed every 1-2 days, wants to do this daily but does not always do so. The logs from the tests performed earlier in this audit were also reviewed and the firewall had thousands of log entries created during the firewall testing. Issue: A procedure should be in place to ensure that the system logs are reviewed regularly and consistently.**
- Do you have a diagram or document detailing the firewall configuration? **No**
    - Who plans or makes changes to the overall firewall design? **The firewall administrator. Issue: Potential issue regarding a lack of segregation of duties.**

Are there any issues or concerns that you have in regards to security that we should be aware of? No

Is the system securable?

Through the research conducted for this audit a number of potential weaknesses in the configuration and implementation of a Checkpoint firewall were identified. This research also provided guidelines on how to correct the issues.

A number of issues have been identified through this audit that require action to properly secure the firewall service for ABC Company. Many of these are minor issues on their own, but together they magnify the risk posed to ABC Company. These issues are securable and can be corrected through a combination of technology solutions and effective security processes. The client report in the final assignment will address in detail each of the issues identified and the security controls that can be put in place to correct the issue.

As much as I would like to say that the firewall is completely secured if all of these recommendations are followed, no system is guaranteed to be 100% secure. There may be a weakness in this technology that has not yet been discovered or was not identified during the audit research. As with all computer systems, constant vigilance to any new weaknesses identified in a Checkpoint firewall is essential to maintain the high level of security that is desired by ABC Company.

Is the system auditable?

I believe that the process, tools and procedures that I followed were effective to assess the overall firewall security for this client. The testing procedure that was followed did identify a number of issues that would not be easily detected through a configuration review of the firewall. Of particular concern is the fact that by missing one specific rule to control access into the DMZ network and the Internal network, two security exposures were created. These issues may have been identified during the firewall reviews, but the testing process effectively proved that the issues existed. During the interview process a

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

number of questions were addressed concerning the security procedures followed by ABC Company. To the best of my knowledge, there is no generally accepted industry standards for administration processes. The evaluation of the processes in place at ABC Company and the recommended improvements is purely subjective.

I would also like to improve the checklist that I used for physical security review of the computer room. I believe that all major areas were addressed, but a more extensive list of items to look for should be developed for future security assessments. I am continuing the activity to build better checklists when time is available. Another area where more effective tools would be beneficial is testing the security of the Rule Base. As discussed in this document the order of the rules is critical to the overall security of the firewall. A tool should be developed to provide an administrator with a mechanism to effectively test the rule base before it is loaded onto a production firewall. Testing the firewall after the rule has been implemented is important, but it may be too late.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 4 – Audit Report

Executive Summary

This report documents the findings of a firewall audit conducted for ABC Company. This audit included a review of both the technical and management controls in place on the corporate Checkpoint firewall and a risk analysis of all issues detected. A number of tests were conducted to evaluate the overall security of the firewall, verify that the firewall was functioning as designed and to ensure that no other points of entry into the ABC private computer network were in place. The technical configuration of the firewall was reviewed in detail and interviews were conducted with ABC Company's technical support staff to confirm the test results and to address the security procedures being followed for this system. All areas identified for inclusion in the scope of this audit have been successfully analyzed and are included in this report.

The Checkpoint firewall utilized by ABC Company is recognized as one of the industry leaders in this technology. A system such as a firewall, no matter how advanced the technology, is only as good as the configuration and rules applied to it. This system has been configured following many of the generally accepted industry standards for hardening the operating system and configuring a Checkpoint firewall. ABC Company should be commended for the effort that has been made to configure and secure this system. ABC Company also recognized that an independent review of this system would be beneficial to ensure that the current system is secure and recommend any enhancements that should be made.

Implementing and maintaining a secure computer environment is often misunderstood. Many organizations are under the impression that in order to implement security you have to invest large sums of money in firewalls, intrusion detection and other expensive security devices. While these devices have their value and are an essential component of an overall security strategy in many organizations, security is not always expensive to implement. A strong security program starts with the basics, a sound security policy, effective procedures for the implementation and management of computer systems, and employees who are aware that the security policies are in place to protect them, not to make their life more difficult. Many of the issues identified during this audit can be corrected with minimal cost to ABC Company.

The following is a summary of the recommendations that are addressed in detail within this report:

- Adjust the Global Properties of the firewall to restrict access to the Checkpoint management ports.
- Adjust the firewall rules to enhance protection of the DMZ network from internal ABC Company computer users.
- Reorder the firewall rules to restrict access from the DMZ Mail server into the ABC Company's private internal network.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Review options to reduce the risk of the firewall being a potential a single point of failure.
- Implement a backup system and process for the firewall.
- Formally establish a process for rule changes for the firewall.
- Implement IP spoofing protection on the current firewall.
- Formally establish a firewall administration and monitoring process.
- Evaluate other methods of fire suppression for the computer room.
- Implement restrictions on the mail forwarding feature for the DMZ mail server.
- Review the use of modems connected to corporate PC's.
- Subscribe to a security alert service.
- Develop a security incident response plan.

Once this report is received, it is certainly important that the recommendations be reviewed and acted upon in an organized manner. It is also important that management supports strategic changes at ABC Company, to ensure that this high level of security rigor is maintained into the future. The proven method to maintain a high level of security on an ongoing basis is through effective security policies and the implementation of an Information System Security Officer (ISSO) role. This ISSO role should be empowered to have the necessary authority to properly influence and if necessary insist, that effective security controls are place for all critical IT resources.

In order to place the findings of this audit in context, a client security profile has been included, which describes the general types of security threats that might impact ABC Company. The number of internal users is large enough that inside attacks are a substantial risk. The impact of a successful attack, whether internal or external, would largely be associated with potential loss of Research and Design information and damage to the organization's reputation.

Category	Rating	Description / Comments
Customer Target Type	Medium	Widget Manufacturing Company
Size	Medium	500-1000 employees
Internet Exposure / Footprint	Low	Email access only.
Internal Exposure / Footprint	Medium	All internal computing resources available to all network connected users.
Temptation Level	Medium – High	Corporate data would be cause for some temptation for ABC Company's major competitors. Research and Design information on new products would be the prime target.
Impact of Internal Security Breach	Significant	Potential exposure of confidential new product information.
Impact of External Security Breach	Significant	Potential exposure of confidential new product information. Public knowledge of a security breach would

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

		have a detrimental affect on the reputation of ABC Company.
Likely Attacker Type	Moderate to highly skilled	Would likely attract amateur, former employee or even skilled hackers wanting to gain competitive information.
Potential Attacker Determination Level	Moderate	The biggest temptation would be the Research and Design information. An amateur might be willing to dedicate some effort to this task, but would probably give up in a relatively short period of time. A former employee or a professional hacker would potentially be more determined.
General Threat Level	**Moderately High**	**Main target for threat is the ABC Company research and design information as well as the potential to cause damage to the corporate reputation.**

Audit Findings:

In this audit findings section the risk levels have been identified as Low, Medium and High, to help identify the top priority items requiring immediate action. An effective security program requires establishing a balance between security controls and functionality for the users. Understanding the balance for security that is required at ABC Company, these risks have been rated accordingly.

1. The Checkpoint firewall is configured to permit all internal and external addresses to communicate with the firewall on the Checkpoint management ports (TCP 264 and 265).

   Risk - Medium
   The default installation of a Checkpoint Firewall-1 includes the activation of FW-1 communication ports. This configuration is included in the Global Properties of the firewall, and supercede any specific rules in place on the system. The tests conducted on the firewall identified that a system on the Internet or on the internal network does have access to the firewall on these specific communication ports. While being able to exploit this issue is not a trivial task, a sound security practice includes blocking all access that is not essential. This access is not essential and the issue can be corrected quite easily.

   This TCP timeout setting established the amount of time the firewall will wait before dropping an inactive TCP communications sessions. A high TCP timeout

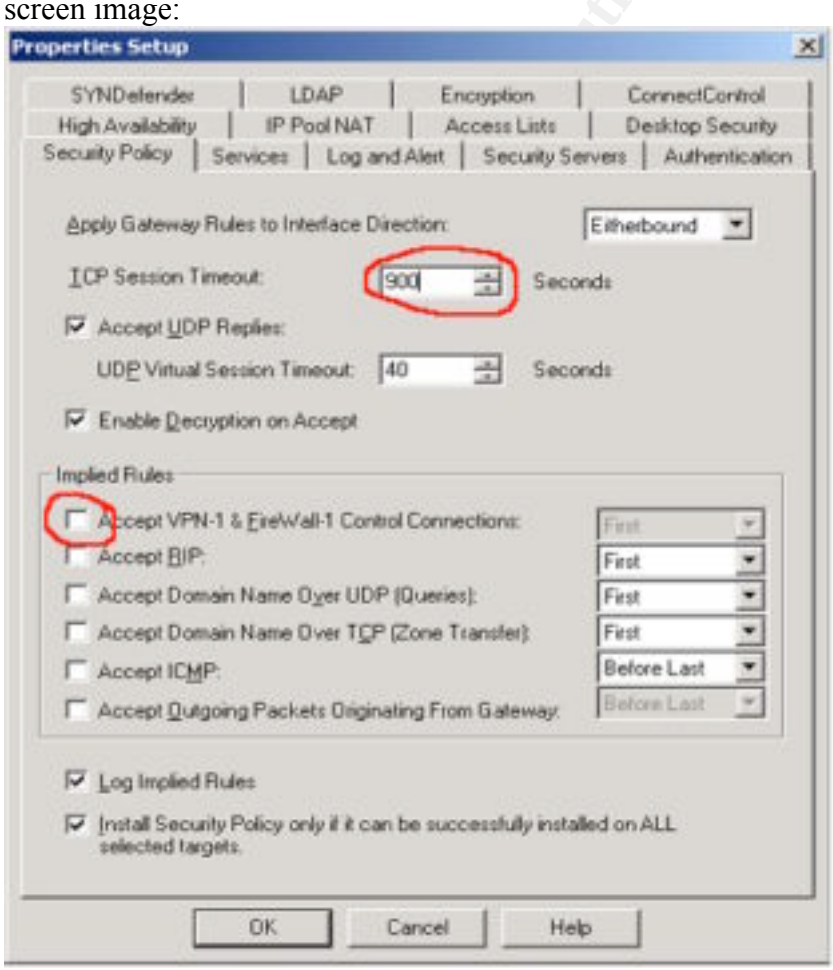
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

setting can increase the risk of the firewall being affected by a denial of service attack. Reducing timeout feature from 3600 seconds to 900 seconds will improve the firewalls resilience to a denial of service attack.

Recommendation:
It is recommended that the "Accept VPN and FW-1 Control Characters" option with the Global Properties be deselected. To enable the two firewall administrators to gain access to the firewall for administration of this system, rule 1 on the firewall should be adjusted.. The recommended rule adjustment is highlighted in **bold**. It is also recommended that the TCP session timeout be adjusted from 3600 seconds to 900 seconds.

No	Source	Destination	Service	Action	Track
1	Corp_fwadmin1 Corp_fwadmin2	spitfire	Ssh **FireWall1**	Accept	Long

The recommended changes to the Global Properties are circled in the attached screen image:



Cost:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The cost involved with this change will be 1-2 hours of the administrators time to make the necessary changes in the Global Properties and the rule base. The administrator will also be required to reload the firewall rule base during a maintenance window and perform a test on the firewall to ensure that this issue has been successfully resolved.

2. Unexpected access into the DMZ network is permitted by the firewall rules

Risk - Low
During testing it was determined that internal ABC Company users could access the DMZ network through a number of communication ports intended for Internet access only. The security design for the DMZ includes restricting access to internal computer users as well as the Internet. This design also allows for two IT support specialists to access the mail server to provide support. Because of the order of the current firewall rules, internal ABC Company users can access this server on TCP communication ports 80, 119 and , 443. Detailed test results on this issue are included in Appendix C. While this issue does not currently create substantial security risks for the mail server, this problem could create more security issues as the use of this DMZ network expands.

Recommendation:
It is recommended that the sequence of the firewall rules be reviewed and corrected to ensure that access into the DMZ network is correctly protected by the firewall. The recommended sequence for rules in the firewall is as follows:

1. Rules for administrator access to the firewall (FW-1, SSH.. etc)
2. Rule to drop all other access to the firewall (stealth rule)
3. Rule to allow incoming access from "ANY" to the DMZ
4. Rules to allow communications between firewall connected networks (internal network to DMZ, DMZ to internal servers)
5. Rule to drop all other access to the internal network (DMZ and Corporate Network)
6. Rules to allow outgoing access to the Internet
7. Rules to drop nuisance traffic with no logging (typically netbios type of traffic)
8. Rule to drop all other traffic with logging enabled

It is recommended that the following rule be added to the Checkpoint firewall:

No	Source	Destination	Service	Action	Track
6	Any	Corp_Network DMZ_Network	Any	Drop	Long

Cost:
The cost to implement this recommendation is less that one hour of time for the system administrator to add a new rule to the firewall rule base. An additional 1-2 hours will be required to reload the firewall rule base during a maintenance window and perform tests to ensure that this issue has been corrected.

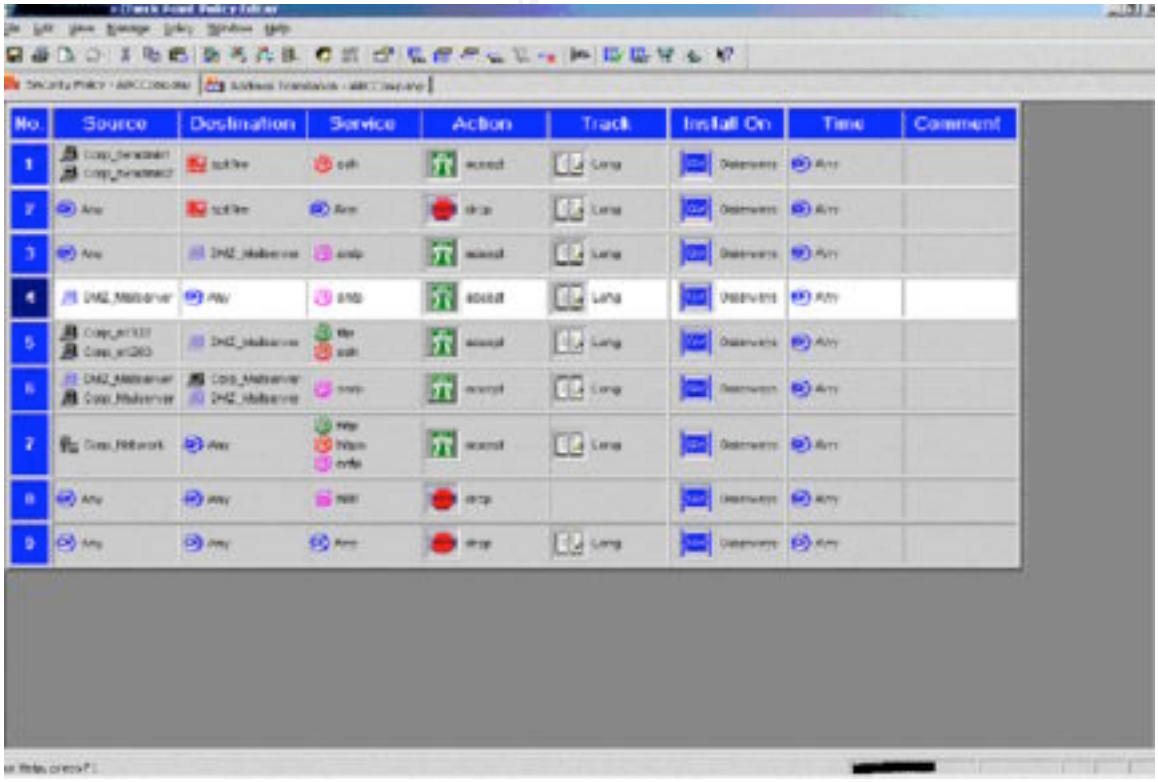
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3. Access from the DMZ mail server into the private ABC Company network is permitted by the firewall

Risk - Low
A review of the firewall rules indicate that the mail server on the DMZ network is permitted by the firewall to communicate on TCP port 25 (SMTP) to any address within the ABC Company internal network. The intended design by technical staff is for this access to only be permitted between the internal mail server and the DMZ mail server. This access creates an unnecessary exposure to all computer systems of ABC Company to a potential security exploit using the mail system. It is a generally accepted best security practice to deny all access that is not required.

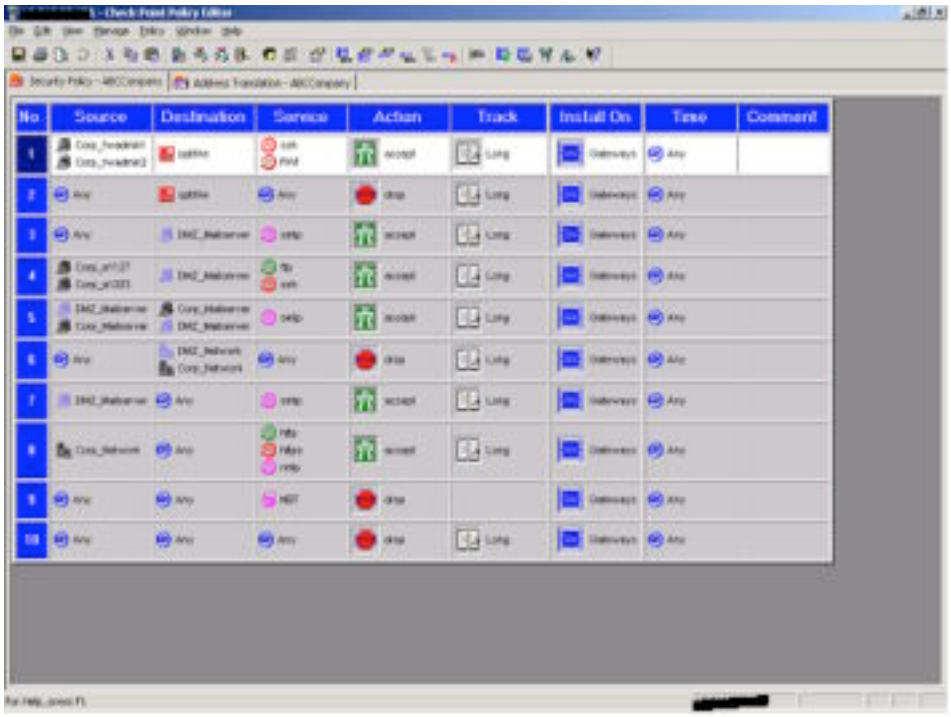
Recommendation:
It is recommended that the sequence of the firewall rules be adjusted to correct this security exposure. The current rule allowing the DMZ mail server to send out mail messages to the Internet, should be moved to rule #7. An example of the current rule changes and the recommended adjustment is as follows:

Current firewall rules:



Recommended rule changes:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Cost:
The cost to implement this recommendation is less that one hour time for the system administrator to add a new rule to the firewall rule base. An additional 1-2 hours will be required to reload the firewall rule base during a maintenance window and perform tests to ensure that this issue has been corrected. This change should be coordinated with the change recommended above for issue #2.

4. The firewall is a single point of failure.

Risk - Low
The firewall is a key component in the communications infrastructure between ABC Company, it's customers and suppliers. The current firewall design includes a number of single points of failure that could potentially disrupt this communications channel.

Recommendation:
It is recommended that ABC Company implement a high availability solution for the firewall service. A number of products are available to offer this high availability and load balancing capability for Checkpoint firewalls. In a high availability situation, if one firewall fails, the second firewall is able to handle all traffic automatically with no interruption in service.

Cost:
The cost for a high availability solution varies, depending on the product selected. It is estimated that this solution would cost between $20,000 and $50,000.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

5. The firewall does not have a backup process in place.

   Risk - Medium
   Establishing a backup procedure of a system is critical to ensure that critical files and information is retained in the event of a full system failure or a disaster. This issue is equally important for a firewall. If lost, the configuration files, activity logs and rules applied to the ABC Company firewall would be extremely difficult to recreate from scratch, and would extend a service outage.

   In the event that a security compromise is suspected on the firewall, a backup will be a valuable tool to recover the system to a known secure state. The firewall backup will also provide ABC Company with the information required to perform a detailed comparison of any changes that may have been made during this incident.

   Recommendation:
   It is recommended that a tape backup unit be purchased for the firewall and that a process be implemented to backup the operating system and Checkpoint information. The firewall backup process is also critical to ensure that firewall logs are retained for extended periods of time to allow for investigation of suspicious network activity. It is recommended that a full system backup be conducted each week and incremental backups are completed nightly. The weekly backup tape should be moved to the secure offsite location each week as well.

   Cost:
   The cost for a backup tape unit and a number of tapes is approximately $3000.00.

6. There is no process in place to administer the firewall rule changes.

   Risk - Medium
   Implementing the technical recommendations in this report will greatly enhance the security of the firewall, however a formal process to manage and monitor this system is required to ensure that the high level of security rigor is maintained. Firewall changes are currently being made with very little formal review of the security risks and these changes are made without an audit trail of why the changes are being made.

   Recommendation:
   It is recommended that ABC Company establish a formal firewall change process that includes written requests for rule changes, a risk analysis of the request and approval from the IT Manager for all rule changes. This process should also include a scheduled maintenance window to activate these changes to minimize the potential impact on computer users.

   Cost:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

There is minimal cost to ABC Company to make this change.

7. The firewall does not have IP spoofing controls in place.

   Risk - Medium
   One of the common methods to circumvent firewall security is by spoofing IP packets. A firewall allows access based on the rules applied to it, analyzing the source address, the destination and communication port. A spoofed packet sent from an untrusted network, that looks like it was sent from a trusted network and matches the rules on the firewall, would be able to pass through the current Checkpoint firewall. The Checkpoint firewall in place at ABC Company does have built in features to mitigate this risk of spoofed packets, however the feature is not currently being used.

   Recommendation:
   It is recommended that the spoofing features of the Checkpoint firewall be activated to ensure that all IP traffic is analyzed for it's originating network before the rules are reviewed. This will effectively add an additional layer of security to the perimeter defense provided by the firewall.

   Cost:
   The anti-spoofing feature is built into the firewall, the cost for this change will include 1-2 hours for the firewall administrator to make the changes. The administrator will also be required to reload the firewall rule base during a maintenance window and perform tests to ensure that this issue has been corrected.

8. No segregation of duties for the firewall.

   Risk - Low
   Currently the configuration and management of the firewall rules as well as the daily review of the system logs are conducted by the primary firewall administrator. This administrator is also a key player in the planning and design of firewall enhancements. The second firewall administrator provide mainly a backup function for after hour support and vacation time. A key concept in maintaining security for your systems while ensuring integrity is a segregation of duties.

   Recommendation:
   It is recommended that the current two firewall administrators share these roles, rather than one individual performing a large majority of the tasks. It would be beneficial for one administrator to be primarily involved in the change process with the second individual monitoring the system logs. All firewall planning and design changes should be conducted by the senior IT resource with input from the firewall administrators.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Cost:
There is no cost to ABC Company to make this change.

9. Water sprinklers are located on the ceiling of this computer room, directly over the computer equipment.

Risk - Medium
The current fire suppression system has been in place for a number of years, even before the computer room was set up on the 6th floor. According to the IT technical staff no changes were made to the sprinkler system since the computer room was in place. Activation of this sprinkler system would potentially destroy all computer equipment in this room. While fire suppression is extremely important, the risk is that even a minor fire that activates the sixth floor sprinkler system could potentially destroy all computer resources in the this computer room. An additional concern would be that a leak or break in the pipes for this sprinkler system could also cause damage to critical computer resources.

Recommendation:
Other more computer friendly methods of fire suppression are available to replace a water based system. A number of the fire suppression agents commonly used to protect sensitive computer equipment include: Inergen, FE36 and CO2.

Alternatively the temperature setting for the sprinklers in the computer room could be adjusted to higher temperature settings to lessen the chance of accidental activation of the system.

Cost:
The costs for a compete fire suppression system vary widely depending on a number of criteria. For this audit I am not able to provide an accurate estimate of these costs.

10. The DMZ mail server allows mail relay

Risk - High
The mail server accepts mail relay from an Internet address. The mail server will act as relay for other mail systems, forwarding mail even when the mail is not destined for, or originating from ABC Company. An attacker could use the ABC Company mail server to flood another Internet connected mail system with junk mail or "Spam" mail. In that situation the mail will look as if it originated from ABC Company. Mail could also be spoofed from the Internet and sent to employees at ABC Company and have the message appear that it was sent by another ABC Company employee. As identified during this audit process, the public image of ABC Company is considered very valuable. An incident where the mail relay issue at ABC Company is exploited for malicious intent, could have a negative effect on the corporate image of ABC Company.

Recommendation:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

It is recommended that the DMZ mail server be reconfigured, implementing restrictions on mail forwarding. For the current Microsoft Exchange mail server, this requires establishing "routing restrictions" that limit access to reroute incoming email messages to a list of authorized IP addresses.

Cost:
There is minimal cost to ABC Company to make this change. The system administrator will require 1-2 hours to make this change and perform the necessary tests.

11. Two unauthorized modem lines were detected.

Risk - High
During the war dialing test, two telephone numbers belonging to ABC Company responded, indicating a modem was in place. These telephone numbers were physically traced to two office computers that did in fact have a modem in place. Additionally 5 telephone numbers were consistently busy during this test conducted over two separate evenings.

The security of a computer network is only as strong as it's weakest link. ABC Company has put great effort and expense into a state of the art firewall to protect the private network. The unauthorized connection of a modem is a quick way to undermine all of these security controls and allow a back door into the private computer network.

Recommendation:
The two telephone numbers that were discovered during this test to have a modem connected were immediately disconnected. It is recommended that the five telephone lines that were identified as busy as well as the fax numbers, be physically reviewed to ensure that a modem is not in place. All unauthorized modems discovered should be immediately removed to maintain the security of the ABC Company computer network.

It should be noted that the employees who did have a modem connected to their corporate computer did not appear to have done this lightly and with total disregard for security. These two individuals felt that the business value gained from being able to access their system remotely, outweighed the potential risk to ABC Company. While the decision to determine the acceptable level of risk for ABC Company must be determined by the Security Officer and not by the computer users, a business case should be reviewed to determine if a secure corporate method of remote access into ABC Company's private network is required.

ABC Company does not have a written security policy that specifies that modems are not to be connected to corporate computer systems. The recommendation to develop corporate security policies is covered in more detail in issue # 13.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Cost:
The cost for ABC Company to review the telephone lines that were identified as busy or having a fax machine is estimated as 6 hours of an administrators time.

12. IT staff do not actively receive security alerts and advisories for the firewall.

Risk - Medium
A number of security issues are identified on virtually all makes and models of computer systems. Once a weakness is detected in a system the manufacturer will issue a security patch to correct the problem. Not only do security professionals and IT administrators receive this information, hackers do as well. The time from the public release of this security alert until the time the correction is applied to your computer is a window of opportunity for a hacker.

Recommendation:
It is recommended that ABC Company subscribe to a security alert service. This should be assigned to two or three individuals to monitor as a team. Not all IT resources need to monitor this information, they should rely on a timely notification of an issue from this team. Some good sites that provide this information include:

- www.sans.org
- www.cert.org

Cost:
There are many good security alert mail lists that are available free of charge.

13. There is no Information System Security Officer (ISSO) in place.

Risk - Medium
Through the interviews it became obvious that ABC Company looks to the IT Manager as the key decision maker related to issues such as security. With the development of security policies and with the new technologies that ABC Company will be looking toward in the future, the role of an ISSO within the organization should be formally established. This position will be key to ensure that these security recommendations are acted upon in an organized fashion and to establish the proper security policies and procedures to ensure that this level of security rigor is maintained into the future.

Recommendation:
It is recommended that initially the IT Manager be formally provided the authority that is required to effectively perform the ISSO role. All firewall changes should require the formal approve from this position upon completion of a risk assessment of the change. It is also recommended that some formal training on the responsibilities of this role be provided.

Cost:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The cost to formally establish the ISSO is minimal, however the responsibilities and authority for the Security Officer should be documented in the IT Security Policy. The cost to establish security policies can vary, depending on the current status of security policies and the level of detail that is required in the new policies. Hiring a security consultant to develop security policies can range from $30,000 to $100,000. Also the formal training for the ISSO role can be provided by a number of credible sources, one example is the SANS organization that offer a specific training track for Information Security Officers. A budgetary estimate for training costs, travel and accommodations is between $5,000 and $8,000.

14. ABC Company does not have an escalation procedure to follow should a security incident occur.

Risk - Low
It is certainly best practice to establish security controls with the objective to prevent security incidents. However even with the best controls in place, incidents can occur. In the unfortunate circumstance that a security incident has occurred, the key issue at that time would be to contain the incident and minimize the potential damage. The main issue that ABC Company is concerned about regarding a potential security incident is the affect this could have on the corporate reputation.

Recommendation:
It is recommended that an incident response plan be developed to ensure that all corporate concerns for minimizing the security breach and protecting the company image are addressed correctly. The timing for a serious security incident is for whatever reason usually at the worst possible time, with junior resources involved. A comprehensive security incident plan will allow even junior IT resources to take the appropriate steps to mitigate the risks and notify the correct management resources regarding the incident.

Cost:
The cost to develop an incident response plan will be 1-2 weeks work for a senior technical resource.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix A - References

"Deploying Firewalls", CERT Coordination Centre, 20 April 2001,
URL http://www.cert.org/security-improvement/modules/m08.html

http://www.cert.org/security-improvement/practices/p060.html

"Improving security on Cisco Routers" , Cisco Systems, 14 March 2002,
URL http://www.cisco.com/warp/public/707/21.html

Rangsiphol, Ruangkrai. SANS GIAC Auditing Networks, Perimeters, and Systems GSNA Practical Assignment , 20 May, 2001 ,
URL http://www.giac.org/practical/Ruangkrai_Rangsiphol_GSNA.zip

Cavender, Terry. CheckPoint Firewall Audit Work Program , 16 January 2001,
(URL www.auditnet.org/docs/CheckpointFirewall.txt

"Solaris Benchmark Version 1.0.1B", 27 September, 2001.
URL http://www.cisecurity.org/

Vallabhaneni, S. Rao. CISSP Examination Textbooks Volume1: Theory . Schaummburg, Illinois, SVR Professional Publications, 2000.

"Which ports does Firewall-1 use ?", 14 November 2001.
URL www.phoneboy.com/faq/0105.html

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix B – Checkpoint Firewall-1 Ports

The following information is provided to identify the communication ports used by a Checkpoint Firewall. This information was acquired from : "Which ports does Firewall-1 use ?", 14 November 2001, www.phoneboy.com/faq/0105.html

- **TCP Port 256** is used for three important things:
  - Exchange of CA and DH keys in FWZ and SKIP encryption between two FireWall-1 Management Consoles
  - SecuRemote build 4005 and earlier uses this port to fetch the network topology and encryption keys from a FireWall-1 Management Console
  - When installing a policy, the management console uses this port to push the policy to the remote firewall.
- **TCP Port 257** is used by a remote firewall module to send logs to a management console.
- **TCP Port 258** is used by the fwpolicy remote GUI.
- **TCP Port 259** is used for Client Authentication.
- **UDP Port 259** is used in FWZ encryption to manage the encrypted session (SecuRemote and FireWall-1 to FireWall-1 VPNs).
- **UDP Port 260** and UDP Port 161 are used for the SNMP daemon that Check Point FireWall-1 Provides.
- **TCP Port 264** is used for Secure Client (SecuRemote) build 4100 and later to fetch network topology and encryption keys from a FireWall-1 Management Console
- **TCP port 265**, Check Point VPN-1 Public Key Transfer Protocol. This is used by FireWall-1 to exchange public keys with other hosts.
- **UDP Port 500** is used for ISAKMP key exchange between firewalls or between a firewall and a host running Secure Client.
- **TCP Port 900** is used by FireWall-1's HTTP Client Authentication mechanism.
- **TCP Ports above 1024** are generally any Security Servers that are active. The actual ports used by these servers will vary.
- **TCP Port 18181** is used for CVP (Content Vectoring Protocol, for anti-virus scanning).
- **TCP Port 18182** is used for UFP (URL Filtering Protocol, for WebSense and the like).
- **TCP ports 18183** is used for SAM (Suspicious Activity Monitoring, for intrusion detection).
- **TCP ports 18184** is used for Log Export API (lea) .

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix C – Test Results

1. Firewall Tests:

The attached nessus report was generated during a test conducted on the Checkpoint firewall from the Internet:

Nessus Scan Report

Number of hosts which were alive during the test : 1
Number of security holes found : 0
Number of security warnings found : 1
Number of security notes found : 0

List of the tested hosts :

- 142.162.10.10 **(Security warnings found)**

142.162.10.10 :
List of open ports :

- *unknown (265/tcp)*
- *unknown (264/tcp) (Security warnings found)*

Warning found on port unknown (264/tcp)

The remote host seems to be a Checkpoint FW-1 running SecureRemote.
Letting attackers know that you are running FW-1 may enable them to focus their attack or will make them change their attack strategy.
You should not let this information leak out.
Furthermore, an attacker can perform a denial of service attack on the machine.
Solution:
Restrict access to this port from untrusted networks.
Risk factor : Low
For More Information:
http://www.securiteam.com/securitynews/CheckPoint_FW1_SecureRemote_DoS.html

---

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2. Mail Server Tests:

The following nessus report details the tests results received during a test conducted on the DMZ mail server from the Internet:

Nessus Scan Report

Number of hosts which were alive during the test : 1
Number of security holes found : 0
Number of security warnings found : 0
Number of security notes found : 1

List of the tested hosts :

- 10.10.10.1*(Security notes found)*

10.10.10.1 :
List of open ports :

- *smtp (25/tcp) (Security notes found)*

Information found on port smtp (25/tcp)

Remote SMTP server banner :
--Banner information removed for client privacy--
214-This server supports the following commands:214 HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH TURN ATRN ETRN BDAT VRFY

Since nessus determined that the mail server would reply to commands such as helo, mail and data. A test was conducted on the mail server to determine whether mail could be relayed through this server. To conduct this test I used Host Explorer to telnet from the Internet to the server on port 25. Attached is a copy of the telnet session where I was able to create an email message on the server and mail it to my Internet mailbox. This test proved that the mail relay option allowed Internet addresses to forward mail through this server.

220 abc.mail.com –Banner information removed for client privacy—Ready2
HELO ABCCOMPANY
250 abc.mail.com Welcome ABCCOMPANY
MAIL FROM:P_TEST@ABC.COM

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

250 P_TEST@ABC.COM ... OK
RCPT TO:TEST@NBNET.NB.CA
250 TEST@NBNET.NB.CA ... OK
DATA
354 Enter mail, end with "." on a line by itself
THIS IS A TEST MESSAGE, TO TEST MAIL RELAY
.
250 Mail accepted

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.