



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 permitted without express written permission.

Administrator's Report on Auditing a Netscreen-100 Firewall

GSNA Practical Version 2.1 (amended 5 February 2002)
Option 1

Author: Jeff Lowder
Date: 7 August 2003

© SANS Institute 2003, Author retains full rights.

Table of Contents

<u>ABSTRACT</u>	4
<u>INTRODUCTION – WHY THIS PRACTICAL IS NOT JUST ANOTHER PRACTICAL ON HOW TO AUDIT FIREWALLS</u>	5
<u>ASSIGNMENT 1 – RESEARCH IN AUDIT, MEASUREMENT, PRACTICE AND CONTROL</u>	6
<u>IDENTIFY THE SYSTEM TO BE AUDITED</u>	6
<u>EVALUATE THE RISK TO THE SYSTEM</u>	7
<u>Firewall Security Control Objectives</u>	7
<u>Firewall Risk Analysis</u>	9
<u>CURRENT STATE OF PRACTICE</u>	16
<u>Description of Research Process</u>	16
<u>Dan Strom's Netscreen-5 Audit Checklist</u>	17
<u>Stephen Gill's Checklist for Hardening Netscreen Firewalls</u>	17
<u>Terry Cavendar's Checkpoint Firewall Audit Work Program</u>	17
<u>Cheswick, Bellovin, and Rubin's List of "Particularly Serious Risks" for Firewalls</u> ..	17
<u>Lance Spitzner's Firewall Audit Methodology</u>	18
<u>AuditNet's Generic Firewall Work Program</u>	18
<u>Charles Cresson Wood's Information Security Policies Made Easy</u>	18
<u>ASSIGNMENT 2 – CREATE AN AUDIT CHECKLIST</u>	19
<u>INTRODUCTION</u>	19
<u>SCOPE</u>	19
<u>Conventions</u>	19
<u>NETSCREEN-100 AUDIT CHECKLIST</u>	20
<u>A. Change Management Section</u>	20
<u>B. Firewall Hardening Section</u>	20
<u>C. Netscreen-100 Policies / Non-Leakage Section</u>	27
<u>D. Ability to Withstand Specific Attacks Section</u>	38
<u>E. High Availability (HA) Section</u>	47
<u>F. Logging Section</u>	49
<u>G. Miscellaneous Section</u>	52
<u>ASSIGNMENT 3 – AUDIT EVIDENCE</u>	53
<u>CHECKLIST ITEM B1: PASS</u>	53
<u>NetScreen Command Line Interface (CLI)</u>	53
<u>NetScreen.com "Current Release" Web Page</u>	53
<u>CHECKLIST ITEM B4: PASS</u>	53
<u>CHECKLIST ITEM B7: PASS</u>	54
<u>CHECKLIST ITEM B8: FAIL</u>	55
<u>CHECKLIST ITEM C2: FAIL</u>	56
<u>CHECKLIST ITEM C4: PASS</u>	57
<u>Scan of DMZ from Untrust: PASS</u>	57

<u>Scan of Trust from Untrust: PASS</u>	60
<u>Scan of Untrust from DMZ: PASS</u>	62
<u>Scan of Trust from DMZ: PASS</u>	65
<u>Scan of Untrust from Trust: PASS</u>	67
<u>Scan of DMZ from Trust: PASS</u>	71
<u>Overall Assessment for Checklist Item C4</u>	92
<u>CHECKLIST ITEM C9: FAIL</u>	92
<u>Nessus Vulnerability Scan: Configuration and Results</u>	93
<u>Results of the Nessus Scan Recorded with the Sniffer Snort</u>	110
<u>CHECKLIST ITEM E3: PASS</u>	121
<u>CHECKLIST ITEM F1: PASS</u>	122
<u>CHECKLIST ITEM F2: PASS</u>	123
<u>CHECKLIST ITEM F3: PASS</u>	123
<u>CHECKLIST ITEM G1: FAIL</u>	124
<u>MEASURE RESIDUAL RISK</u>	125
<u>IS THE SYSTEM AUDITABLE?</u>	133
<u>ASSIGNMENT 4 – RISK ASSESSMENT</u>	134
<u>EXECUTIVE SUMMARY</u>	134
<u>B8: Web-based firewall management sessions are not encrypted.</u>	135
<u>C2: An unauthorized service was running on the firewall's management interface.</u>	135
<u>C9: The firewall allowed access to vulnerable services running on internal hosts.</u>	137
<u>G1: Firewall configuration back up and restore procedures are not documented.</u>	150
<u>LIST OF REFERENCES</u>	151

List of Figures

<u>FIGURE 1 – GROSSLY SIMPLIFIED NETWORK DIAGRAM</u>	7
<u>FIGURE 2 – LOGIN SCREEN FOR WEB-BASED MANAGEMENT SESSION</u>	54
<u>FIGURE 3 – UNAUTHORIZED ERROR MESSAGE AFTER REPEATED FAILED LOGINS</u>	54
<u>FIGURE 4 – NESSUS CONSOLE WINDOW AFTER SCAN</u>	92
<u>FIGURE 5 – LOCAL CERTIFICATES CONFIGURATION ON NETSCREEN-100</u>	136
<u>FIGURE 6 – WEB ADMINISTRATION SETTINGS ON NETSCREEN-100</u>	136
<u>FIGURE 7 – INTERFACE CONFIGURATION FOR UNTRUST INTERFACE</u>	137
<u>FIGURE 8 – ATTEMPT TO DOWNLOAD A NON-EXISTENT HTML PAGE</u>	144

List of Tables

<u>TABLE 1. SUMMARY OF FIREWALL CONTROL OBJECTIVES</u>	8
<u>TABLE 2. LIST OF ASSETS</u>	10
<u>TABLE 3. PRE-AUDIT RISK ANALYSIS</u>	11
<u>TABLE 4. SEARCH ENGINES AND QUERIES USED</u>	16
<u>TABLE 5. POST-AUDIT RESIDUAL RISK ANALYSIS</u>	125
<u>TABLE 6. UNFULFILLED CONTROL OBJECTIVES</u>	133

Abstract

While there is a vast and growing literature on auditing Internet firewalls, the audit of Netscreen firewalls has been a neglected topic. In this paper, I will attempt to counter that trend by outlining and defending a technically rigorous methodology for auditing the Netscreen-100 firewall. I begin by providing an exhaustive list of firewall security control objectives. I then conduct a formal pre-audit risk assessment using Tom Peltier's Facilitated Risk Assessment Process, in order to ensure that security controls are aligned with business objectives. Next, I delineate and justify an audit checklist designed specifically for Netscreen-100 firewalls. I then use that checklist to conduct an audit of a Netscreen-100 firewall that protects an e-commerce system. Finally, I conduct a post-audit risk assessment, in order to measure the effectiveness of compensating controls.

© SANS Institute 2003, Author retains full rights.

Introduction – Why This Practical Is Not Just Another Practical on How to Audit Firewalls

While firewalls are hardly a new security technology—and the audit of firewalls is not an unusual topic—I have tried to make an original contribution to the literature of network security with this paper. In support of that goal, my paper accomplishes the following goals.

- Provide a comprehensive list of firewall security control objectives.
- Advance the state of the discussion on pre-audit risk assessment by adopting Tom Peltier's Facilitated Risk Assessment Process (FRAP) methodology. The FRAP methodology is designed to ensure that security controls are aligned with business objectives.
- Discuss the neglected topic of how to audit a Netscreen firewall, namely, the Netscreen-100.
- Evaluate the risk of the firewall's configuration in the context of the services behind the firewall that are reachable through the firewall.
- After using Nessus to identify potentially vulnerable services on internal services accessible through the firewall, I heavily scrutinize each finding. In the process, I discuss a broad variety of security vulnerabilities on systems behind the firewall, including vulnerabilities in Apache, OpenSSH, and Oracle. I also identify the conditions that led Nessus to report false positives. This "big picture" perspective allows me to describe the residual risk in terms of the specific software running on the systems behind the firewall.

I hope readers get out of the practical as much as I tried to put into it.

© SANS Institute

Assignment 1 – Research in Audit, Measurement, Practice and Control

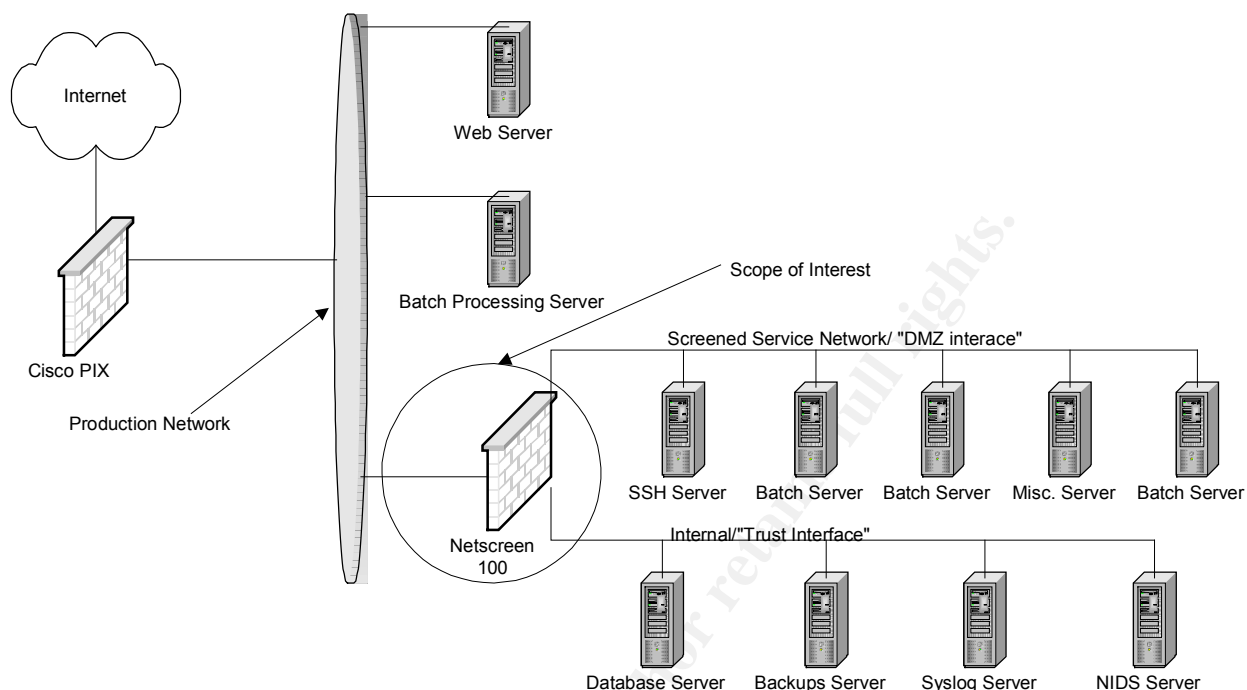
Identify the system to be audited

I am auditing a Netscreen firewall that is used by a technology company to protect a production e-commerce environment. Although I am conducting the audit as a system administrator—that is, I have privileged or administrative control over the firewall—in other ways my role resembles that of an independent auditor. When I began the audit, I was a new employee and had no pre-existing knowledge of the system. Moreover, although I have administrative control over the firewalls, I quickly learned that I did not have complete "political" control over them. If I wanted to change the firewall configuration or network perimeter architecture, I had to persuade both the affected business units and senior IT management to implement my recommendations.

In order to audit a firewall, the auditor must measure the firewall against a standard. Ideally, that standard is codified as part of an organizational security policy document. Unfortunately, my organization did not have an approved security policy at the time of the audit. Although management recognized the importance of having an approved and enforced security policy, policy creation can be time-consuming and management could not afford to delay the audit while a policy was written and approved; they needed the audit report immediately. In this situation, I chose to audit the firewall against recognized industry best practices.

The firewall is responsible for protecting the database server in the back end of the e-commerce network. Administrative access to the firewall is restricted by ACLs that require the management session to originate from an authorized IP address, as well as password authentication. With administrative access, the firewall administrator can perform any task related to firewall management, including policy administration, event analysis, performance monitoring, and interface configuration.

The particular firewall I am auditing is a Netscreen 100 firewall running version 3.0.1r2.0 of the Netscreen ScreenOS. As shown in Figure 1, the firewall is not Internet facing; instead, it is an internal firewall that segregates our e-commerce environment from the rest of our production network. Multiple layers of router Access Control Lists (ACLs), firewalls, and load balancer NQLs separate the e-commerce environment from the Internet; these other layers of perimeter defense are not indicated in figure 1.

Figure 1 – Grossly Simplified Network Diagram

Evaluate the Risk to the System

There are two main components to risk evaluation for security audits. The first is identifying the security control objectives of the system to be audited. The second is assessing risks that could mitigate that system's effectiveness in meeting its security control objectives.

Firewall Security Control Objectives

Before we can begin a security audit of any system, we first need to understand how the system is intended to contribute to security. In other words, we need to understand the *security control objectives* of the system. According to the IT Governance Institute's *Control Objectives for Information and related Technology* (COBIT), an IT Control Objective as "a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity."¹ Thus, the security control objectives of the system are directly related to the role of the system.

The security control objectives for the firewall that constitutes the scope of my audit are defined in Table 1.

¹ COBIT Steering Committee and the IT Governance Institute, p. 5.

Table 1. Summary of Firewall Control Objectives

No.	Control Objective
CO1	An e-commerce system on a production network must be specially segregated from the rest of the production network through an additional layer of security provided by one or more dedicated internal firewalls.
CO2	For any network protected by a firewall, the firewall must be the single point of connection between the untrusted network and the protected network.
CO3	The firewall(s) must be kept current with the latest vendor upgrades, security patches, and security problem fix software.
CO4	The firewall(s) must act as a single point of network access where traffic can be analyzed and controlled.
CO5	The firewall(s) should control any application and infrastructure management flows in <i>both</i> directions.
CO6	The firewall(s) must deny by default any services not explicitly authorized.
CO7	All ports on the firewall itself should be disabled by default; only ports that have been specifically authorized should be open.
CO8	The firewall(s) should protect the e-commerce system against denial of service attacks and any unauthorized access to the e-commerce system.
CO9	No vulnerable services should be accessible through the perimeter's countermeasures.
CO10	The firewall(s) must be able to hide details of the internal network architecture through various methods, including but not limited to the use of Network Address Translation (NAT) with RFC 1918 addressing.
CO11	Only authorized personnel may be permitted to administer the firewall(s). Administrative access to the firewall(s) must be strictly limited to those personnel responsible for maintaining the firewall(s).
CO12	Firewall administrators must have at least two user-IDs. One of these user-IDs (e.g., root) must provide privileged access and have its activities be logged; the other must be a normal user-ID for the day-to-day work of an ordinary user.
CO13	Firewall policies must not be changed unless the proposed change(s) have been approved by both the Security team and the Change Control Board.
CO14	Firewall management sessions are extremely sensitive and must be encrypted.
CO15	IP spoofing detection must be enabled on the firewall.
CO16	The firewall architecture must provide high availability, by having two firewalls in parallel, so that if one firewall fails, traffic can seamlessly flow through the other.
CO17	All HA master-slave firewall pairs must maintain synchronized configurations.
CO18	The firewall(s) must provide an audit trail or log of all attempted and successful network connections.
CO19	The audit trail or log must include action taken by administrators, including user IDs; login date/time; log-out date/time; changes to policies; changes or additions to user privileges; and system start-ups and shut-downs.
CO20	Firewall logs must be stored on a dedicated syslog server.
CO21	The audit trails must be retained in accordance with the organization's data retention policy.

CO22	Firewall configuration back up and restore procedures must be documented.
------	---

Firewall Risk Analysis

Prior to assessing the risks to the system, I first evaluated the importance of this potential security audit. Given that my organization's security team was understaffed, would conducting this audit be a good use of company time? The answer was immediately obvious. Not only would the audit be worthwhile, but also it should be made a high priority for the company in order to prevent *substantial* damage to the business, including lost revenue and damage to the company's reputation.

Having satisfied myself with the need for and priority of this audit, my next (pre-audit) step was to evaluate specific risks of particular concern. Unfortunately, this task was complicated by the fact that I was unable to obtain any documentation or network diagrams concerning this firewall. To their credit, management was well aware of these shortcomings and the importance of fixing them. Indeed, fixing those gaps were part of the reason I was hired! Nevertheless, it was obvious that a large number of important *procedural* controls were entirely missing. Moreover, based on what little I knew at the time about the firewall configuration and network architecture, I was also worried about the presence and effectiveness of the *technical* controls.

I therefore decided to conduct a formal risk analysis, in order to help tailor the scope of the audit according to the business needs of the company. A complete risk analysis methodology includes the following steps.

1. Identify the asset to be protected.
2. Ascertain threats, risks, concerns, or issues to that asset.
3. Prioritize the risk or determine the asset's vulnerability to the threat.
4. Implement corrective measures, controls, safeguards, or accept the risk.
5. Monitor the effectiveness of the controls.²

Since this risk analysis was a *pre-audit* risk analysis, I would only be completing steps 1-3; moreover, my progress on step 3 would obviously be limited by incomplete information. In the following pages, I summarize the results of my pre-audit risk analysis.

Step 1. Asset Identification.

There are two types of assets: physical (i.e., hardware) and logical (i.e., intellectual property). In my case, the assets may be summarized as follows:

² Peltier, p. 5.

Table 2. List of Assets

Asset	Type
Netscreen 100 Appliance	Physical
Access to Screened Service Network (SSN) or internal network	Logical
Detailed information about our internal network architecture, including hostnames, communication protocols, and information flow.	Logical
Netscreen 100 Policies (similar to ACLs) and Configuration	Logical
Financial information (to the extent that an intruder might be able to aggregate data based on the number of connections to the e-commerce database)	Logical
Potential forensic information, including logs.	Logical
Company reputation (to the extent that a firewall compromise could cause damage to that reputation)	Logical

Steps 2-3. Threat Identification and Vulnerability Determination

Before I summarize the threats, I first want to clarify the distinction between threats and vulnerabilities. Although those terms are often used as if they were synonymous, they are not. A threat is not a vulnerability; a vulnerability is not a threat. A *threat* may be defined as "an event with the potential to cause unauthorized access, modification, disclosure, or destruction of information resources, applications, or systems" (emphasis mine).³ In contrast, a *vulnerability* is a condition of "weakness in a system, application, infrastructure, control or design flaw that can be exploited to violate system integrity."⁴ For example, if the asset I wish to protect is an expensive car, one threat to that asset would be physical theft of the asset (an event), while a vulnerability would be the situation in which the car is unattended with the doors unlocked (a condition).

With that distinction in mind, I first identified the threats to each asset. I then determined the vulnerability of each asset to each of the threats just identified. Since this is a *pre-audit* risk assessment, my vulnerability determination would have to be based upon my *background knowledge* of the company, the system, and the relevant set of controls. In addition, for each of the vulnerabilities, I determined the degree of risk that I could use to refine the audit scope and prioritizing tasks. The degree of risk is a qualitative measurement of the likelihood of occurrence. Possible values for the degree of risk include high, medium, low, and unknown.

³ Peltier, p. 21.

⁴ Peltier, p. 21.

Table 3. Pre-Audit Risk Analysis

Asset	Threat	Vulnerability	Degree of Risk	Impact
Netscreen 100 Appliance	Physical access to data center	Physical access is restricted by security guards, two-factor biometric authentication, and an access control list.	Low	Could lead to destruction, theft, or tampering with physical assets.
	Unauthorized modification to physical interface connections (e.g., switching or unplugging connections)	All authorized personnel have successfully completed a background check. Video surveillance in and outside of data center.	Low	Disruption or degradation of service.
	Unauthorized disclosure of firewall hardware	Someone with knowledge of our firewall hardware could disclose to an unauthorized party. Nevertheless, this is unlikely, given our procedural controls. All authorized personnel must successfully complete a background check and sign a nondisclosure agreement. Mitigating controls for unauthorized personnel include all of the above physical security controls.	Low	Greater probability of an attacker successfully compromising the security of the network.

Asset	Threat	Vulnerability	Degree of Risk	Impact
	Destruction of or damage to hardware	The hardware could be destroyed by the forces of nature (i.e., fire) or a human (accidentally or intentionally). Nevertheless, this is unlikely given our numerous compensating controls, including disaster recovery controls, background checks for all authorized personnel; and fire detection and suppression systems.	Low	Disruption or degradation of service.
	Theft of hardware	See above.	Low	Disruption of service, financial loss to company.
Access to SSN or Internal Network	Unauthorized network access to SSN or internal network	Existing (authorized) firewall policy allows an attacker to gain access to resources on either the SSN or internal network.	High	Greater probability of an attacker successfully compromising the security of servers in the SSN or internal network.

Asset	Threat	Vulnerability	Degree of Risk	Impact
	Denial of Service attack	Denial-of-Service attacks are a well-known problem. Given the lack of an approved security policy, it seemed likely that security vulnerabilities were not being updated in a timely manner, if at all.	High	A prolonged disruption of firewall availability would be a customer-visible outage and have a direct impact on revenue.
Details of our internal network architecture.	Unauthorized disclosure of internal network architecture	Although controls are in place to prevent the unauthorized disclosure of the architecture by an employee, it is not known if an outsider would be able to gain knowledge of our internal architecture.	Unknown	Greater probability of an attacker successfully compromising the security of the network.
Netscreen 100 Policies and Configuration	Unauthorized access to policies or configuration	Netscreen 100s offer two methods of administrative access: command-line (via SSH) and web-based (via SSL). An exploit in the Netscreen's implementation of either service could result in an intruder gaining unauthorized access.	Unknown	An intruder with unauthorized administrative access could deliberately bring the firewall down, disrupting network availability. The intruder could also modify the firewall configuration to make it easier to compromise the other machines on the network. A compromise of the e-commerce server could lead to theft of sensitive customer data, which would be a disaster for the business.

Asset	Threat	Vulnerability	Degree of Risk	Impact
	Unauthorized modification of policies or configuration	An attacker with unauthorized access could make unauthorized changes to the firewall policies or configuration.	Un-known	Greater probability of an attacker successfully compromising the security of the network. Disruption or degradation of service.
	Unauthorized disclosure of policies or configuration	An attacker with unauthorized access would be able to view the firewall policies and configuration, which would be an unauthorized disclosure of sensitive information.	Un-known	Greater probability of an attacker successfully compromising the security of the network.
	Destruction of policies or configuration	An attacker with unauthorized access could delete the policies or configuration.	Un-known	Partial or total disruption of service.
Financial information	Unauthorized access to (confidential) corporate financial data	Given that the firewall sees all connections between the batch processing server and the e-commerce database, it might be possible for an intruder with access to the firewall to determine aggregate information about the number of transactions between the two systems.	Un-known	Using that information, the intruder could make educated guesses about some of the company's financial data. This could be useful to a competitor.

Asset	Threat	Vulnerability	Degree of Risk	Impact
Potential forensic data	Unauthorized access to forensic data	Unauthorized access to forensic data might allow an intruder to learn confidential information about the company's financial condition, internal network architecture, usernames of authorized firewall administrators, as well as the contents of the forensic data.	Medium	The knowledge gained from this information could help an attacker compromise the SSN or internal networks.
	Unauthorized modification of forensic data	An attacker with administrative access on the firewall might be able to modify the firewall logs.	Medium	Unauthorized modifications to forensic data might hamper investigations into security incidents. It would also disrupt the chain of custody of evidence. The data might not be usable in court.
	Unauthorized disclosure of forensic data	Unauthorized access to forensic data might allow an intruder to learn confidential information about the company's financial condition, internal network architecture, usernames of authorized firewall administrators, as well as the contents of the forensic data.	Medium	The knowledge gained from this information could help an attacker successfully compromise security.
	Unauthorized destruction of forensic data	An attacker with administrative access on the firewall might be able to delete the firewall logs.	Medium	Destruction of the firewall logs could hamper security incident investigations.
Company	Damage to	A security compromise	Medium	Public

Asset	Threat	Vulnerability	Degree of Risk	Impact
reputation	reputation	could lead to public embarrassment.		embarrassment can cause loss of customer and shareholder confidence.

Based on the results of my pre-audit risk analysis, I decided to forego an audit of the physical asset (the firewall appliance hardware and associated cables) and instead audit all of the logical assets. In some cases, prior to conducting my audit, I already had reason to be concerned, while in other cases the degree of risk was unknown and needed investigation.

Current State of Practice

Given the prevalence of Internet firewalls, suggestions for auditing firewalls are not hard to find. For example, a Google search for "firewall audit" return about 172,000 hits. In my experience, many of the relevant resources tended to fall into one of two categories: those that focus heavily on procedural controls and those that focus primarily on technical controls. It was less common to find an audit checklist that provided a comprehensive set of tests for both procedural and technical controls. Nevertheless, audit checklists designed specifically for Netscreen firewalls were not nearly as common. A Google search for "Netscreen audit" returned only 3,010 hits. Moreover, I was unable to locate a single audit checklist written specifically for the Netscreen 100.

Description of Research Process

I began my research by using a standard set of search queries on various Internet search engines. The search engines and search queries are summarized in Table 4.

Table 4. Search Engines and Queries Used

Search Engine	Search Queries
www.google.com	firewall audit
www.altavista.com	Netscreen audit
www.metacrawler.com	Netscreen 100 audit
www.yahoo.com	ScreenOS audit

Next, I consulted specific sites, that specialize in information systems security and information systems security audit. These sites included:

- SecurityFocus (<http://www.securityfocus.com/>)
- AuditNet (<http://www.auditnet.org/>)
- ISACA – Information Systems Audit and Control Association (<http://www.isaca.org/>)

- SANS Reading Room (<http://rr.sans.org>)
- SANS Posted Practicals for GIAC Systems and Network Auditor (GSNA) and GIAC Certified Firewall Analysts (GCUX) – (<http://www.giac.org/cert.php>)

Finally, I consulted numerous security reference books in my own personal library. As a result, I was able to locate a number of resources I could use in developing an audit checklist for the Netscreen 100. In this section, I will briefly summarize the highlights of some of the more interesting audit checklists and related material I was able to locate.

Dan Strom's Netscreen-5 Audit Checklist

In his practical for GSNA certification, Dan Strom developed an audit checklist for Netscreen-5s.⁵ The Netscreen-5 is the smallest appliance in the Netscreen product line; it is suitable for small office or home office usage. Strom's checklist includes specific audit tests to check the strength of administrative options such as the version of ScreenOS, enabling of built-in Netscreen options for blocking certain kinds of attacks, standard firewall ruleset checks, and VPN configuration.

Stephen Gill's Checklist for Hardening Netscreen Firewalls

In the course of my research, I also discovered an interesting paper by Stephen Gill describing various methods for hardening Netscreen firewalls.⁶ (Gill's paper focuses on Netscreen-500s, but most of his suggestions can also be implemented on Netscreen-100s.) Although not written as an audit checklist, all of Gill's hardening steps could be useful in building an audit checklist for Netscreen-100s.

Terry Cavendar's Checkpoint Firewall Audit Work Program

Cavendar's Checkpoint firewall audit work program is another example of a related audit checklist that could be useful in building an audit checklist specifically for Netscreen-100s.⁷ Cavendar's work program includes an examination of firewall documentation, logical access, configuration, logs, physical security, business continuity, as well as port scanning the firewall from all interfaces.

Cheswick, Bellovin, and Rubin's List of "Particularly Serious Risks" for Firewalls

In the second edition of their landmark book *Firewalls and Internet Security: Repelling the Wily Hacker*, respected security professionals William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin provide a list of "particularly serious risks" for Internet firewalls in general.⁸ The list is exclusively composed of technical vulnerabilities and includes such items as, "IP source routing can subvert address-based authentication," "UDP-based services can be abused to create broadcast storms," and so forth.

⁵ Strom.

⁶ Gill.

⁷ Cavendar.

⁸ Cheswick, Bellovin, and Rubin, pp. 389-390.

Lance Spitzner's Firewall Audit Methodology

In his article, "Auditing Your Firewall Setup," Lance Spitzner describes a generic methodology for auditing firewalls.⁹ Spitzner's methodology consists of two steps. First, the auditor must test the firewall itself. Second, the auditor must test the rulebase to determine if unauthorized traffic can pass through the firewall. Spitzner's article describes specific tests that can be performed under each step.

AuditNet's Generic Firewall Work Program

I chose to include the generic firewall work program on the AuditNet website because it provided the most comprehensive set of tests relating to non-technical controls.¹⁰ Specific areas of testing include firewall management practices, maintenance, policies and procedures concerning the operation and maintenance of the firewall (not to be confused with ACLs or what Netscreen calls "policies"), and documentation.

Charles Cresson Wood's Information Security Policies Made Easy

Finally, I used Charles Cresson Wood's popular book, Information Security Policies Made Easy.¹¹ Although the book is designed primarily as a reference work on information security policies, it also contains an excellent discussion of the risks associated with not having each policy.

⁹ Spitzner, Lance. "Auditing Your Firewall Setup." URL: <http://www.spitzner.net/audit.html> (8 July 2003).

¹⁰ "Firewall Review." URL: <http://www.auditnet.org/docs/Firewall%20Review%20May%2028,%202004.pdf> (8 July 2003).

¹¹ Wood, Charles Cresson. Information Security Policies Made Easy. 8th ed. Houston: Pentasafe, 2001.

Assignment 2 – Create an Audit Checklist

Introduction

The object of this checklist is to assist one in performing an audit of a network perimeter. Completion of this checklist will require the usage of freeware tools, including nmap, Nessus, and some mechanism for capturing network packets (e.g., Snort).

Note: Several of these tests have the potential to be disruptive. Be sure to obtain proper authorization before conducting this audits; the only thing that differentiates legitimate auditors from the bad guys is having permission.

Scope

The scope of the network perimeter audit is limited to the firewall protecting the company's e-commerce environment. The tests performed as part of this audit fall into the following categories.

- Change Management
- System Hardening
- Netscreen-100 Policies / Non-Leakage
- Ability to withstand specific attacks
- High Availability
- Logging

Conventions

The Netscreen-100 Audit Checklist is organized as a table for convenience. The columns of the checklist may be summarized as follows:

Control Objective and Reference: the control objective summarizes one or more particular control objectives for the system to be audited. Remember that the "Firewall Security Control Objectives" were summarized in Assignment 1, [Table 1](#). The reference provides the source for the item.

Risk: what can go wrong, how likely that event is, and the consequences of that event.

Compliance: how the auditor can *know* if the system is compliant.

Testing: how the auditor can *check* to see if the system is compliant. When appropriate, commands to be issued at the command-line interface (CLI) are displayed in **Terminal Bold** font.

Type: the "type" column in the audit checklist is used to identify whether a given test is objective ("O") or subjective ("S").

Netscreen-100 Audit Checklist

#	Control Objective and Reference	Risk	Compliance	Test	Type
A. Change Management Section					
1	<p>CO13. Firewall policies must not be changed unless the proposed change(s) have been approved by both the Security team and the Change Control Board (CCB).</p> <p><u>Reference</u>: Wood, Charles Cresson. <u>Information Security Policies Made Easy</u>. Eighth ed. Houston: Pentasafe, 2001, p. 134.</p>	Firewall changes that are not approved by Security or the CCB risk disrupting critical production systems, not to mention creating unnecessary security exposures.	This is a binary compliance item. The firewall is compliant if all variations between the current configuration and the baseline configuration are documented in formal, approved CCB change tickets. Otherwise, the firewall is not compliant.	Verify that all changes to the firewall policies were authorized by the CCB, by performing the following steps. First, compare the current firewall configuration against the baseline configuration. Second, validate that all configuration changes were formally approved in an official CCB change ticket.	O
B. Firewall Hardening Section					
1	<p>CO3. The firewall(s) must be kept current with the latest vendor upgrades, security patches, and security problem fix software.</p>	Older versions or unpatched versions of operating systems often have security vulnerabilities that are exploitable either	There is a range of conditions for compliance for this item. If the Netscreen-100 is running the latest	Verify that the latest patches have been applied to the firewall software or appliance. Consult the firewall vendor's website to determine which patches or upgrades are available. Then compare that information to	O

	<p><u>Reference</u>: Spitzner, Lance. "Auditing Your Firewall Setup." December 12, 2000. URL: http://www.spitzner.net/audit.html (8 July 2003).</p>	remotely or locally on the server.	<p>version of the ScreenOS, it is compliant. If the Netscreen-100 is running an older version but newer version(s) do not address security vulnerabilities, it is compliant. Otherwise, the system is non-compliant.</p>	<p>the current firewall configuration.</p> <ul style="list-style-type: none"> • get system <p>The software version will appear near the top of the output and look similar to the following:</p> <p>SW Version/Checksum: 3.0.3r6.0/6b60e662</p> <ul style="list-style-type: none"> • Compare that output with the list of current releases on the Netscreen website at http://www.netscreen.com/services/download_soft/current_releases.jsp. • If the firewall is not running the latest version, investigate vendor documentation to determine if the latest software version fixes known security vulnerabilities. 	
2	<p><u>CO19</u>. The audit trail or log must include action taken by administrators, including user IDs; login date/time; log-out date/time; changes to policies; changes or additions to user privileges; and system start-ups and shut-downs.</p> <p><u>Reference</u>: Garfinkel, Simson and Gene Spafford. <u>Practical Unix & Internet Security</u>. Second ed. O'Reilly & Associates, 1996. p. 513.</p>	If the system clock is not accurate, it becomes more difficult to correlate events among the firewall logs and other sources of data.	<p>This is a binary compliance item. A system is compliant if the displayed system clock date, time, and time zone are accurate. Otherwise, the system is not compliant.</p>	<p>Verify the system clock date, time, and time zone on the firewall is accurate.</p> <ul style="list-style-type: none"> • get clock • Compare the system date and time displayed in the upper-right hand corner against a trusted time source. 	O

		If the firewall is not configured to synchronize its system clock with a reliable, accurate timeserver, it becomes more difficult to correlate events in the firewall logs with events in other logs (i.e., Unix syslogs). <i>Note: determining the accuracy of the local time server is outside the scope of this audit.</i>	This is a binary compliance item. A system is compliant if the firewall has been configured to synchronize its system clock with a local time server. In response to the audit command, compliant firewalls will respond with "NTP is enabled." Otherwise, the system is not compliant.	Verify the accuracy of the Network Time Protocol (NTP) server settings. <ul style="list-style-type: none"> <code>get ntp</code> 	O
3	<p>CO11. Only authorized personnel may be permitted to administer the firewall(s). Administrative access to the firewall(s) must be strictly limited to those personnel responsible for maintaining the firewall(s).</p> <p><u>Reference:</u> Lowder, Jeffery J. "Firewall Management and Internet Attacks." <u>Information Security Management Handbook</u>. Ed. Harold F. Tipton and Mi[k]ki Krause. 4th ed. Vol.</p>	Management access to the firewall should be restricted in order to ensure the firewall is not susceptible to an exploit that could result in an attacker being able to login to the firewall. There is no reason why web management sessions initiated from a non-company IP address should be allowed. (Note: this statement does not	This is a binary compliance item. A system is compliant if management of the firewall has been restricted to a source IP address that resides within the company's network. Otherwise, the system is not compliant.	Ensure that management of the firewall is only permitted from a valid company source IP address. <ul style="list-style-type: none"> <code>get admin</code> (look for the lines that begin with "Mng Host IP") Compare that output with documentation or interviews with network administrators regarding the company's network address space. 	O

	1. Boca Raton, Florida: Auerbach, 2000, p. 126.	apply to web management sessions initiated over a VPN connection.)			
4	<p>CO11. Only authorized personnel may be permitted to administer the firewall(s). Administrative access to the firewall(s) must be strictly limited to those personnel responsible for maintaining the firewall(s).</p> <p>Wood, Charles Cresson. <u>Information Security Policies Made Easy</u>. Eighth ed. Houston: Pentasafe, 2001, p. 87.</p>	The intention of this policy is to ensure that no unauthorized persons access organizational computers or communication systems.	This is a binary compliance item. A system is compliant if administrative access can be gained only after successful authentication. Otherwise, the system is not compliant.	<p>Verify that firewall administrators must be authenticated by attempting to establish a management session.</p> <ul style="list-style-type: none"> Initiate an SSH session to the management interface of the firewall(s). Initiate an HTTPS connection to the management interface of the firewall(s). 	O
5	<p>CO11. Only authorized personnel may be permitted to administer the firewall(s). Administrative access to the firewall(s) must be strictly limited to those personnel responsible for maintaining the firewall(s).</p> <ul style="list-style-type: none"> If supported by the firewall, strong authentication should be required for administrative access to 	Strong authentication greatly decreases the likelihood of administrative access by an unauthorized user.	This is a binary compliance item. A system is compliant if administrative access requires strong authentication (i.e., RADIUS). Otherwise, the system is not compliant.	<p>If applicable, ensure that strong authentication is required for firewall administration, by attempting to log onto the firewall.</p> <ul style="list-style-type: none"> get auth (look for the line that begins with "User authentication type") 	O

	<p>the firewalls. The strong authentication shall consist of two factors. First, the user will be required to supply a one-time password generated by a SecurID "keyfob." (The Netscreens support this indirectly through a RADIUS server.) Second, the user will be required to supply a reusable password.</p> <p><u>Reference:</u> International Standards Organization. <u>ISO 17799: Information Technology—Code of Practice for Information Security Management.</u> London: BSI, 2000, p. 35.</p>				
6	<p>CO11. Only authorized personnel may be permitted to administer the firewall(s). Administrative access to the firewall(s) must be strictly limited to those personnel responsible for maintaining the firewall(s).</p> <p><u>Reference:</u> International</p>	<p>Providing access on the firewall to users without a business need significantly increases security risks.</p>	<p>This is a binary compliance item. A system is compliant if the only user accounts on the system belong to actual administrators of the firewall(s). Otherwise, the</p>	<p>Ensure that the only personnel with accounts on the firewall are those with a business need for such accounts.</p> <ul style="list-style-type: none"> • <code>get admin user</code> 	O

	Standards Organization. <u>ISO 17799: Information Technology—Code of Practice for Information Security Management.</u> London: BSI, 2000, p. 34.		system is not compliant.		
7	<p>CO12. Firewall administrators must have at least two user-IDs. One of these user-IDs (e.g., root) must provide privileged access and have its activities be logged; the other must be a normal user-ID for the day-to-day work of an ordinary user.</p> <p><u>Reference:</u> International Standards Organization. <u>ISO 17799: Information Technology—Code of Practice for Information Security Management.</u> London: BSI, 2000, p. 34.</p>	If each firewall administrator does not have their own account, it becomes more difficult to track administrative activities back to a particular user, decreasing accountability.	This is a binary compliance item. A system is compliant if each firewall administrator has his or her own unique account and uses that account for day-to-day administration. Otherwise, the system is not compliant.	<p>Ensure that each firewall administrator has his or her own unique account.</p> <ul style="list-style-type: none"> • get admin user • Compare the output of that command with a list of known firewall administrators. <p>Then verify that the firewall administrators are using their personal (unique) accounts for firewall administration by checking the logs:</p> <ul style="list-style-type: none"> • get log event <p>Then verify that administrative is logged by modifying a policy and then checking the logs:</p> <ul style="list-style-type: none"> • get log event 	O

8	<p>CO14. Firewall management sessions are extremely sensitive and must be encrypted.</p> <p><u>Reference</u>: International Standards Organization. <u>ISO 17799: Information Technology—Code of Practice for Information Security Management</u>. London: BSI, 2000, pp. 9-10.</p>	<p>Forcing all management sessions through SSH or SSL tunnels inserts another layer of protection against eavesdropping attacks. This is especially significant if password authentication is used for management sessions.</p>	<p>This is a binary compliance item. A system is compliant if the following conditions apply to <u>each interface</u>:</p> <ul style="list-style-type: none"> • "telnet disabled" • If web management is allowed ("web enabled"), the sessions are encrypted via SSL ("SSL enabled"). <p>Otherwise, the system is not compliant.</p>	<p>Ensure that remote management of the firewall may only be performed via SSH or SSL. Telnet and (non-SSL) HTTP access must be disabled.</p> <p>Get a list of all interfaces by issuing the following command:</p> <ul style="list-style-type: none"> • <code>get interface</code> <p>Then, for each interface, issue the following command:</p> <ul style="list-style-type: none"> • <code>get interface <interface></code> 	O
9	<p>Web management sessions that have been idle for 10 minutes should be timed out.</p> <p><u>Reference</u>: Wood, Charles Cresson. <u>Information Security Policies Made Easy</u>. Eighth ed. Houston: Pentasafe, 2001, p. 68.</p>	<p>The longer a management session is idle, the greater the risk of an unauthorized person gaining privileged access to the firewall.</p>	<p>This is a binary compliance item. A system is compliant if a web management idle timeout has been set for 10 minutes or fewer. Otherwise, the system is not compliant.</p>	<p>Verify that a web management idle timeout has been set for 10 minutes or fewer.</p> <ul style="list-style-type: none"> • <code>get admin auth</code> 	O

C. Netscreen-100 Policies / Non-Leakage Section					
1	<p>CO15. IP spoofing detection must be enabled on the firewall.</p> <p><u>Reference:</u> Cheswick, William R., Steven M. Bellovin, and Aviel D. Rubin. <u>Firewalls and Internet Security: Repelling the Wily Hacker</u>. Second ed. Boston: Addison-Wesley, 2003, p. 20; Northcutt, Stephen. Mark Cooper, Matt Fearnow, and Karen Frederick. <u>Intrusion Signatures and Analysis</u>. Boston: New Riders, 2001, p. 143.</p>	In an IP Spoof attack, the attacker attempts to bypass firewall security by imitating a valid client IP address. When protection is enabled, the NetScreen device checks its own route table before permitting the traffic to pass through. If the originating IP address is not in the device route table, the device denies traffic from that source and drops any packets from it.	This is a binary compliance item. A system is compliant if "IP Address Spoofing Protection" has been set to "On". Otherwise, the system is not compliant.	<p>Verify that IP Spoofing detection is enabled on the firewall.</p> <ul style="list-style-type: none"> <code>get firewall</code> (look for the line that begins with "IP Address Spoofing Protection") 	O
2	<p>CO7. All ports on the firewall itself should be disabled by default; only ports that have been specifically authorized should be open.</p> <p><u>Reference:</u> The SANS Institute, "7.2 Auditing the Perimeter" (2003), p. 4-6.</p>	The more services that are allowed by the firewall, the greater the risk of a security compromise.	This is a binary compliance item. A system is compliant if all ports have been disabled by default and only specific, authorized ports have been opened. Otherwise, the system is not compliant.	<p>Port scan the firewall itself, scanning for ICMP, TCP, and UDP.</p> <ul style="list-style-type: none"> <code>nmap -T Aggressive -sP <ip address range> -oN <output file></code> <code>nmap -P0 -T Aggressive -sT <ip address range> -oN <output file></code> <code>nmap -P0 -T Aggressive -sU <ip address range> -</code> 	O

				oN <output file>	
3	<p>CO2 and CO4. For any network protected by a firewall, the firewall must be the single point of connection between the untrusted network and the protected network. The firewall(s) must act as a single point of network access where traffic can be analyzed and controlled.</p> <p><u>Reference:</u> Lowder, Jeffery J. "Firewall Management and Internet Attacks." <u>Information Security Management Handbook</u>. Ed. Harold F. Tipton and Mi[k]ki Krause. 4th ed. Vol. 1. Boca Raton, Florida: Auerbach, 2000, p. 117.</p>	It is impossible to control the volume and type of traffic entering and leaving the network if there is an undocumented or unauthorized access point such as modems, other firewalls, or network drops patched directly to the hub outside the firewall. The firewall cannot protect against traffic that does not pass through it.	This is a binary compliance item. The firewall is compliant if it is the single point of connection between the untrusted network and the protected network. If the tracert output does not consistently list the firewall (or a blank hop representing the firewall) for each machine, this may indicate the machine is not firewalled and hence the firewall is not compliant. Otherwise, the system is not compliant.	<p>Determine if the firewall is the single point of connection to the untrusted network from the protected network. First, check the hosts on the firewall's DMZ interface.</p> <ul style="list-style-type: none"> nmap -v -P0 -T Aggressive -g 22 -sA <IP address> -o <output file> tracert <IP address> (repeat for each individual machine on the DMZ interface) <p>Then repeat the above steps for machines on the firewall's trusted interface.</p>	O
4	CO1 , CO5 , and CO6 . An e-commerce system on a production network must be specially segregated from the rest of the production network through an	A firewall that allows unauthorized traffic to pass through it increases the exposure of protected servers. It	This is a binary compliance item. A system is compliant if all ports have been disabled by default in both	Validate that the firewall is accepting <u>ONLY</u> the traffic that you allow, <u>by scanning every network segment from every other network segment</u> to see what packets can and cannot get through the firewall. For each	O

	<p>additional layer of security provided by one or more dedicated internal firewalls. The firewall(s) should control any application and infrastructure management flows in <i>both</i> directions. The firewall(s) must deny by default any services not explicitly authorized.</p> <p><u>Reference:</u> The SANS Institute, "7.2 Auditing the Perimeter" (2003), p. 4-25.</p>	<p>is important to ensure that the firewall is passing only allowed inbound traffic.</p> <p>Effective outbound filtering is also important. Why? Because of outbound hacking, unauthorized use, risky behavior, and Trojan program activity.</p>	<p>directions and only specific, authorized ports have been opened. Otherwise, the system is not compliant.</p>	<p>segment-to-segment test, you will place your auditing system on one side of the firewall and scan a target host on the other side of the firewall. Run a sniffer on the other side or monitor network intrusion detection system (NIDS) logs to record any packets that pass through the firewall:</p> <ul style="list-style-type: none"> • <code>tail -f fast.alert</code> <p>Once tcpdump is running, then initiate the scan:</p> <ul style="list-style-type: none"> • <code>nmap -v -T Aggressive -sP <IP address> -o <output file></code> • <code>nmap -v -P0 -T Aggressive -g 22 -sA <IP address> -o <output file></code> • <code>nmap -v -P0 -T Aggressive -g 53 -sU <IP address> -o <output file></code> <p>If the firewall has a dedicated interface for a screened service network (SSN, sometimes called a demilitarized zone or DMZ), position the audit system on the SSN and attempt to penetrate the internal</p>	
--	---	--	---	--	--

				network. If possible, take one of your production systems offline and replace the IP address with your auditing system. This simulates if one of your SSN systems is compromised and that your internal network is still protected by the firewall.	
--	--	--	--	---	--

5	<p>CO5. The firewall(s) should control any application and infrastructure management flows in <i>both</i> directions.</p> <p>CO10. The firewall(s) must be able to hide details of the internal network architecture through various methods, including but not limited to the use of Network Address Translation (NAT) with RFC 1918 addressing.</p> <ul style="list-style-type: none"> • ICMP responses should be limited to routers and hosts in the SSN. • Outbound ICMP should be blocked unless needed by a particular application to work. If necessary, the destination IP addresses should be restricted. <p><u>Reference:</u> The SANS Institute, “7.4 Network Auditing Essentials” (2003), pp. 6-9 and 6-21.</p>	<p>ICMP is extremely useful for network troubleshooting and maintenance. Unfortunately, it is also extremely useful for attacks and reconnaissance. Examples include: (1) the combination of source routing and spoofing is dangerous; and (2) inbound ICMP redirects. While "security through obscurity" as the <i>only</i> layer of security is unwise, obscurity <i>can</i> be useful as <i>one of several</i> layers of security.¹²</p> <p>Outbound ICMP is also risky. Examples include: (1) if “host unreachable” messages are not filtered, an attacker can determine which IP addresses represent valid, running hosts; and (2) the ability to “tunnel” traffic through specially crafted ICMP packets (e.g., Stacheldraht which uses echo-</p>	<p>This is a binary compliance item. A system is compliant if both of the following conditions are true.</p> <p>(1) ICMP responses are limited to routers and hosts in the SSN.</p> <p>(2) Outbound ICMP is blocked in all cases except where needed. If needed, the destination IP addresses must be restricted.</p> <p>Otherwise, the system is not compliant.</p>	<p>Audit inbound ICMP rules using nmap.</p> <ul style="list-style-type: none"> • <code>nmap -T Aggressive -sP <ip address range> -o <output file></code> <p>Audit outbound ICMP rules using nmap.</p> <ul style="list-style-type: none"> • <code>nmap -T Aggressive -sP <ip address range> -o <output file></code> 	O
---	---	--	--	--	---

6	<p>CO5 and CO6. The firewall(s) should control any application and infrastructure management flows in <i>both</i> directions. The firewall(s) must deny by default any services not explicitly authorized.</p> <p><u>Reference:</u> The SANS Institute, “7.4 Network Auditing Essentials” (2003), p. 6-23.</p>	<p>If a site reveals open ports in response to a SYN scan, an attacker may be able to perform reconnaissance without appearing in the logs.</p> <p>Effective outbound filtering is also important, given that it can limit outbound hacking, unauthorized use, risky behavior, and Trojan program activity.</p>	<p>This is a binary compliance item. The firewall is compliant if does not reveal open ports in response to a SYN scan. Otherwise, the system is not compliant.</p>	<p>Audit inbound TCP rules with a “SYN” scan, by running nmap -sS.</p> <ul style="list-style-type: none"> nmap -P0 -T Aggressive -sS <ip address range> -o <output file> <p><i>Note: SYN scans do not work against proxy firewalls.</i></p>	O
				<p>Audit <i>outbound</i> TCP rules with a “SYN” scan.</p> <ul style="list-style-type: none"> nmap -P0 -T Aggressive -sS <ip address range> -o <output file> 	O
7	<p>CO5 and CO6. The firewall(s) should control any application and infrastructure management flows in <i>both</i> directions. The firewall(s) must deny by default any services not explicitly authorized.</p> <p><u>Reference:</u> The SANS Institute, “7.4 Network Auditing Essentials” (2003), p. 6-29.</p>	<p>A firewall that allows unauthorized traffic to pass through it increases the exposure of protected servers. It is important to ensure that the firewall is passing only allowed inbound traffic.</p> <p>Effective outbound filtering is also important, given that it can limit outbound hacking, unauthorized use, risky behavior, and Trojan program activity.</p>	<p>This is a binary compliance item. The firewall is compliant if does not reveal unauthorized TCP ports. Otherwise, the system is not compliant.</p>	<p>Audit inbound TCP rules with a TCP Full Connect Scan, by running nmap -sT.</p> <ul style="list-style-type: none"> nmap -P0 -sT <ip address range> -o <output file> <p><i>Note: TCP Full Connect scans do not require root privilege. Since Full Connect scans complete the 3-way handshake, they should be logged by Unix hosts.</i></p>	O

				<p>Audit <i>outbound</i> TCP rules with a TCP Full Connect Scan.</p> <ul style="list-style-type: none"> <code>nmap -P0 -sT <ip address range> -o <output file></code> 	O
				<p>Audit inbound UDP rules with a UDP scan, by running <code>nmap -sU</code>.</p> <ul style="list-style-type: none"> <code>nmap -P0 -sU <ip address range> -o <output file></code> <p><i>Note: performing UDP scans with nmap requires root privilege.</i></p>	O
				<p>Audit outbound UDP rules with a UDP scan.</p> <ul style="list-style-type: none"> <code>nmap -P0 -sU <ip address range> -o <output file></code> 	O
8	<p>CO6. All services should be disabled on each host by default. Only those services that are actually needed should be enabled.</p> <p><u>Reference:</u> Spitzner, Lance. "Auditing Your Firewall Setup." December 12, 2000. URL: http://www.spitzner.net/audit.html (8 July 2003).</p>	<p>Even if there are no known vulnerabilities against a specific service, there is no reason to risk system compromise by running a service if it is not needed.</p>	<p>This is a binary compliance item. The firewall is compliant if services are disabled by default. Otherwise, the system is not compliant.</p>	<p>Verify that no extraneous ports are open on machines in the SSN, by conducting both TCP connect and UDP scans against each host in the SSN.</p> <ul style="list-style-type: none"> <code>nmap -sT <IP address> -o <output file></code> <code>nmap -sU <IP address> -o <output file></code> <p><i>Note: be sure to schedule the scanning time in advance with operations.</i></p>	O
9	CO9 . No vulnerable	If a vulnerable	This is a binary	Verify that no vulnerable services	O

	<p>services should be accessible through the perimeter's countermeasures.</p> <p><u>Reference:</u> The SANS Institute, "7.4 Network Auditing Essentials" (2003), p. 6-48.</p>	<p>service is accessible through the perimeter's countermeasures, then an attacker who knows how to exploit the vulnerable service will be able to successfully attack the system.</p>	<p>compliance item. The firewall is compliant if no vulnerable services are accessible through the perimeter's countermeasures. Otherwise, the system is not compliant.</p>	<p>can be accessed through the perimeter's countermeasures.</p> <p>Use nmap to scan behind the firewall for "internal" hosts that run the externally accessible services identified in steps 5-8.</p> <ul style="list-style-type: none"> • <code>nmap -sT <IP address range> -p <port range></code> • <code>nmap -sU <IP address range> -p <port range></code> <p>Since this (hopefully) is a much-reduced set of ports, the scan should go much more quickly. The result of this scan is a list of which hosts run which services in our "permitted services" list.</p> <p>Using that list, then target the hosts in that list with Nessus.</p> <ul style="list-style-type: none"> • Access a server running Nessus via the Nessus client to conduct the vulnerability assessment. The Nessus client/server configuration is beyond the scope of this document. <p>The product of this step is a list of hosts running vulnerable services, which can be accessed through the</p>	
--	---	--	---	---	--

				perimeter's countermeasures.	
10	<p>CO7. All ports on the firewall itself should be disabled by default; only ports that have been specifically authorized should be open.</p> <p><u>Reference:</u> Spitzner, Lance. "Auditing Your Firewall Setup." December 12, 2000. URL: http://www.spitzner.net/audit.html (8 July 2003).</p>	<p>Even if there are no known vulnerabilities against a specific service, there is no reason to risk system compromise by running a service if it is not needed. The more services that are allowed by the firewall, the greater the risk of a security compromise.</p>	<p>This is a binary compliance item. The firewall is compliant if all of the policies have been used in the last three months. Otherwise, the system is not compliant.</p>	<p>Conduct a manual review of the firewall policies (rules). For each rule, verify that the policy is actually being used, by searching for evidence that it has been used in the last three months.</p> <p>First, get a list of all policies.</p> <ul style="list-style-type: none"> • <code>get policy</code> <p>Next, get the traffic log for each policy.</p> <ul style="list-style-type: none"> • <code>get log traffic policy <policy ID></code> <p><i>Note: depending on how far back the logs are stored on the Netscreen-100 itself, you may need to check the logs on the syslog server.</i></p>	O
11	<p>CO5. The firewall(s) should control any application and infrastructure management flows in <i>both</i> directions.</p> <ul style="list-style-type: none"> • The firewall must be able to properly handle fragmented IP packets. <p><u>Reference:</u> The SANS Institute, "7.4 Network</p>	<p>Packet fragmentation can be used to bypass firewalls. The idea is to break a packet up into little bitty pieces and send them one at a time. For example, the ACK or SYN bits in a TCP packet could end up in a different</p>	<p>This is a binary compliance item. The firewall is compliant if it is able to handle fragmented IP packets. Otherwise, the system is not compliant.</p>	<p>Verify the firewall's ability to handle fragmented IP packets.</p> <ul style="list-style-type: none"> • <code>nmap -f -sT <ip address></code> 	O

	Auditing Essentials” (2003), p. 6-24.	fragment from the port number. The fragments are then reassembled on the other side of our firewall (at the destination host); they pass unmolested. In these situations, a firewall cannot know if it should let something through, because it does not know if it is part of an existing conversation. There is thus little information on which to base a filtering decision.			
--	---------------------------------------	--	--	--	--

D. Ability to Withstand Specific Attacks Section					
1	<p>CO5. The firewall(s) should control any application and infrastructure management flows in <i>both</i> directions.</p> <ul style="list-style-type: none"> Source-routed packets must be denied or dropped by the firewall. <p><u>Reference:</u> Northcutt, Stephen, Lenny Zeltser, Scott Winters, Karen Kent Frederick, and Ronald W. Ritchey. <u>Inside Network Perimeter Security</u>. Boston: New Riders, 2003, p. 156; The SANS Institute, "7.2 Auditing the Perimeter" (2003), p. 3-70.</p>	Using source-routed packets, an attacker can enter a network with a false IP address and have data from the network sent to his actual IP address.	This is a binary compliance item. The firewall is compliant if the "Source Route IP Option Filter" has been set to "On". Otherwise, the system is not compliant.	<p>Validate that source-routed packets are denied or dropped by the firewall.</p> <ul style="list-style-type: none"> get firewall (look for the line that begins with "Source Route IP Option Filter") 	O
2	<p>CO8. The firewall(s) should protect the e-commerce system against denial of service attacks and any unauthorized access to the e-commerce system.</p> <ul style="list-style-type: none"> SYN attack detection must be enabled on the firewall. 	A SYN Flood attack inundates a site with SYN packets containing forged ("spoofed") IP source addresses with nonexistent or unreachable addresses. The firewall responds with SYN/ACK packets to	This is a binary compliance item. The firewall is compliant if "SYN Flood Protection" has been set to "On". Otherwise, the system is not compliant.	<p>Verify that SYN attack detection has been enabled on the firewall.</p> <ul style="list-style-type: none"> get firewall (look for the line that begins with "Syn Flood Protection") 	O

	<p><u>Reference:</u> Wood, Charles Cresson. <u>Information Security Policies Made Easy</u>. Eighth ed. Houston: Pentasafe, 2001, p. 103; cf. Northcutt, Stephen. Mark Cooper, Matt Fearnow, and Karen Frederick. <u>Intrusion Signatures and Analysis</u>. Boston: New Riders, 2001, p. 198.</p>	<p>these addresses and then waits for responding ACK packets. Because the SYN/ACK packets are sent to nonexistent or unreachable IP addresses, they never elicit responses and eventually time out. By flooding a server or host with connections that cannot be completed, the attacker eventually fills the host's memory buffer. Once this buffer is full, no further connections can be made and the host's operating system might be damaged. Either way, the attack disables the host and its normal operations. A SYN Flood attack is classified as a denial-of-service (DoS) attack.</p>			
--	--	--	--	--	--

3	<p>CO8. The firewall(s) should protect the e-commerce system against denial of service attacks and any unauthorized access to the e-commerce system.</p> <ul style="list-style-type: none">• ICMP flood detection must be enabled on the firewall. <p><u>Reference</u>: Wood, Charles Cresson. <u>Information Security Policies Made Easy</u>. Eighth ed. Houston: Pentasafe, 2001, p. 103; cf. Northcutt, Stephen. Mark Cooper, Matt Fearnow, and Karen Frederick. <u>Intrusion Signatures and Analysis</u>. Boston: New Riders, 2001, p. 198.</p>	<p>An ICMP flood occurs when ICMP echo requests are broadcast with the purpose of flooding a system with so much data that it first slows down, and then times out and is disconnected. An ICMP flood is classified as a DOS attack.</p>	<p>This is a binary compliance item. The firewall is compliant if "ICMP Flood Detection" has been set to "On". Otherwise, the system is not compliant.</p>	<p>Verify that ICMP Flood detection has been enabled on the firewall.</p> <ul style="list-style-type: none">• get firewall (look for the line that begins with "ICMP Flood Detection")	O
---	---	--	--	---	---

4	<p>CO8. The firewall(s) should protect the e-commerce system against denial of service attacks and any unauthorized access to the e-commerce system.</p> <ul style="list-style-type: none">• UDP flood detection must be enabled on the firewall. <p><u>Reference:</u> Wood, Charles Cresson. <u>Information Security Policies Made Easy</u>. Eighth ed. Houston: Pentasafe, 2001, p. 103; cf. Gill, Stephen. "Application Note: Hardening Netscreen Firewalls." Version 1.2. 18 July 2002. URL: http://www.qorbit.net/documents/screenos-hardening-appnote.pdf (8 July 2003).</p>	<p>UDP flooding occurs when UDP packets are sent with the purpose of slowing down the system to the point that it can no longer process valid connection requests. A UDP flood is classified as a DoS attack.</p>	<p>This is a binary compliance item. The firewall is compliant if "UDP Flood Detection" has been set to "On". Otherwise, the system is not compliant.</p>	<p>Verify that UDP Flood detection has been enabled on the firewall.</p> <ul style="list-style-type: none">• get firewall (look for the line that begins with "UDP Flood Protection")	O
---	---	---	---	--	---

5	<p>CO8. The firewall(s) should protect the e-commerce system against denial of service attacks and any unauthorized access to the e-commerce system.</p> <ul style="list-style-type: none">• Ping of Death detection must be enabled on the firewall. <p><u>Reference:</u> Wood, Charles Cresson. <u>Information Security Policies Made Easy</u>. Eighth ed. Houston: Pentasafe, 2001, p. 103; cf. Northcutt, Stephen. Mark Cooper, Matt Fearnow, and Karen Frederick. <u>Intrusion Signatures and Analysis</u>. Boston: New Riders, 2001, p. 316.</p>	<p>Although the TCP/IP protocol specifies a specific packet size, some ping implementations permit users to set a desired packet size. In a Ping of Death attack, the attacker sends a packet of a size that greatly exceeds the maximum limit for TCP/IP, resulting in DoS, and crashing, freezing, and rebooting of the firewall.</p>	<p>This is a binary compliance item. The firewall is compliant if "Ping-of-Death Protection" has been set to "On". Otherwise, the system is not compliant.</p>	<p>Verify that Ping of Death detection has been enabled on the firewall.</p> <ul style="list-style-type: none">• get firewall (look for the line that begins with "Ping-of-Death Protection")	O
---	--	---	--	--	---

6	<p>CO8. The firewall(s) should protect the e-commerce system against denial of service attacks and any unauthorized access to the e-commerce system.</p> <ul style="list-style-type: none">• Teardrop attack detection must be enabled on the firewall. <p><u>Reference:</u> Wood, Charles Cresson. <u>Information Security Policies Made Easy</u>. Eighth ed. Houston: Pentasafe, 2001, p. 103; cf. Northcutt, Stephen. Mark Cooper, Matt Fearnow, and Karen Frederick. <u>Intrusion Signatures and Analysis</u>. Boston: New Riders, 2001, pp. 304-11.</p>	<p>In a Teardrop attack, the attacker changes one of the options in an IP header so that the sum of the offset and one fragmented packet differ from that of the next fragmented packet. This causes the packets to overlap, which can cause the server attempting to reassemble the packet to crash. These packets are dropped when the NetScreen device detects the discrepancy.</p>	<p>This is a binary compliance item. The firewall is compliant if "Tear Drop Protection" has been set to "On". Otherwise, the system is not compliant.</p>	<p>Verify that Tear Drop Attack detection has been enabled on the firewall.</p> <ul style="list-style-type: none">• get firewall (look for the line that begins with "Tear Drop Protection")	O
---	--	--	--	---	---

7	<p>CO10. The firewall(s) must be able to hide details of the internal network architecture through various methods, including but not limited to the use of Network Address Translation (NAT) with RFC 1918 addressing.</p> <ul style="list-style-type: none">• Port Scan Attack detection must be enabled on the firewall. <p><u>Reference:</u> Wood, Charles Cresson. <u>Information Security Policies Made Easy</u>. Eighth ed. Houston: Pentasafe, 2001, p. 103; cf. Northcutt, Stephen. Mark Cooper, Matt Fearnow, and Karen Frederick. <u>Intrusion Signatures and Analysis</u>. Boston: New Riders, 2001, pp. 304-11.</p>	<p>In a Port Scan attack, the attacker sends packets that have different port numbers to scan the available services and find a port that responds.</p>	<p>This is a binary compliance item. The firewall is compliant if "Port Scan Protection" has been set to "On". Otherwise, the system is not compliant.</p>	<p>Verify that Port Scan Attack detection has been enabled on the firewall.</p> <ul style="list-style-type: none">• get firewall (look for the line that begins with "Port Scan Protection")	O
---	--	---	--	---	---

8	<p>CO10. The firewall(s) must be able to hide details of the internal network architecture through various methods, including but not limited to the use of Network Address Translation (NAT) with RFC 1918 addressing.</p> <ul style="list-style-type: none">• Address Sweep Attack Detection must be enabled on the firewall. <p><u>Reference:</u> Wood, Charles Cresson. <u>Information Security Policies Made Easy</u>. Eighth ed. Houston: Pentasafe, 2001, p. 103; cf. Cheswick, William R., Steven M. Bellovin, and Aviel D. Rubin. <u>Firewalls and Internet Security: Repelling the Wily Hacker</u>. Second ed. Boston: Addison-Wesley, 2003, p. 4.</p>	<p>The Address Sweep attack is similar to the ICMP Flood attack; the attacker sends ICMP echo requests (pings) to different destination addresses to locate one that responds. The responding address is targeted by the attacker.</p>	<p>This is a binary compliance item. The firewall is compliant if "IP Sweep Protection" has been set to "On". Otherwise, the system is not compliant.</p>	<p>Verify that Address Sweep Attack detection has been enabled on the firewall.</p> <ul style="list-style-type: none">• get firewall (look for the line that begins with "IP Sweep Protection")	O
---	--	--	---	--	---

9	<p>CO8. The firewall(s) should protect the e-commerce system against denial of service attacks and any unauthorized access to the e-commerce system.</p> <ul style="list-style-type: none">Land Attack detection must be enabled on the firewall. <p><u>Reference:</u> Wood, Charles Cresson. <u>Information Security Policies Made Easy</u>. Eighth ed. Houston: Pentasafe, 2001, p. 103; cf. Northcutt, Stephen. Mark Cooper, Matt Fearnow, and Karen Frederick. <u>Intrusion Signatures and Analysis</u>. Boston: New Riders, 2001, pp. 190-195.</p>	<p>When launching a Land Attack, the attacker sends spoofed SYN packets that contain the IP address of the victim as both the source IP address and the destination IP address, thus creating a combination of IP spoofing and a SYN attack. When this happens, the receiving system sends the SYN-ACK packet to itself, creating an empty connection that continues until the time exceeds the system's Idle Timeout threshold. A flood of these empty connections overwhelms the system and results in DoS.</p>	<p>This is a binary compliance item. The firewall is compliant if "Land Attack Protection" has been set to "On". Otherwise, the system is not compliant.</p>	<p>Verify that Land Attack detection has been enabled on the firewall.</p> <ul style="list-style-type: none">get firewall (look for the line that begins with "Land Attack Protection")	O
---	---	---	--	--	---

E. High Availability (HA) Section					
1	<p>CO16. The firewall architecture must provide high availability by having two firewalls in parallel, so that if one firewall fails, traffic can seamlessly flow through the other.</p> <p><u>Reference:</u> The SANS Institute, “7.2 Auditing the Perimeter” (2003), p. 4-37.</p>	If the firewall does not detect the failure of the HA link between the master and the slave, the HA feature will not work.	This is a binary compliance item. The firewall is compliant if the HA link failure detection works. If the firewall state was "master" before the test, it should be "slave" after the test (and vice versa). Otherwise, the system is not compliant.	<p>First, identify which firewall in the HA pair—either the master or the slave—is currently active.</p> <ul style="list-style-type: none"> • <code>get ha</code> (look for the line that begins "state:") <p>Next, verify the high availability (HA) link failure detection.</p> <ul style="list-style-type: none"> • Unplug the interface cables between the HA master and the HA slave. <p>Then determine if the other firewall is active.</p> <ul style="list-style-type: none"> • <code>get ha</code> <p><i>Note: Be sure to schedule the testing time in advance with operations.</i></p>	O
2	<p>CO17. All HA master-slave firewall pairs must maintain synchronized configurations.</p> <p><u>Reference:</u> The SANS Institute, “7.2 Auditing the Perimeter” (2003), p. 4-37.</p>	Before you can run your NetScreen-100 in an HA configuration, the master unit and the slave unit must have identical system configurations.	This is a binary compliance item. The firewall is compliant if the master and slave have synchronized configurations. Otherwise, the system is not compliant.	<p>Check to see if there are any log entries in the Event Alarm complaining of “inconsistent configuration between master and slave”.</p> <ul style="list-style-type: none"> • <code>get log event</code> 	O

3	<p>CO14. Firewall management sessions are extremely sensitive and must be encrypted.</p> <ul style="list-style-type: none">HA traffic must be authenticated and encrypted. <p><u>Reference:</u> Gill, Stephen. "Application Note: Hardening Netscreen Firewalls." Version 1.2. 18 July 2002. URL: http://www.qorbit.net/documents/screenos-hardening-appnote.pdf (8 July 2003), p. 11.</p>	<p>If HA traffic is not encrypted, it is theoretically possible for an attacker to learn policy and topology information. If HA traffic is not authenticated, it is possible for an attacker to make unauthorized modifications to the policies.</p> <p>These attacks are not possible, however, if a crossover cable is used.</p>	<p>This is a binary compliance item. The firewall is compliant if HA traffic encryption and authentication are set to "enable". Otherwise, the system is not compliant.</p>	<p>Verify that HA traffic is authenticated and encrypted.</p> <ul style="list-style-type: none">get ha (look for "encryption:" and "authentication:")	O
---	---	--	---	--	---

F. Logging Section					
1	<p>CO18. The firewall(s) must provide an audit trail or log of all attempted and successful network connections.</p> <p><u>Reference:</u> Spitzner, Lance. "Auditing Your Firewall Setup." December 12, 2000. URL: http://www.spitzner.net/audit.html (8 July 2003); Gill, Stephen. "Application Note: Hardening Netscreen Firewalls." Version 1.2. 18 July 2002. URL: http://www.qorbit.net/documents/screenos-hardening-appnote.pdf (8 July 2003), p. 6.</p>	<p>Firewall logs are an important source of data for network troubleshooting and for security incident response. If the firewall is not capturing the proper log data, this may adversely affect network troubleshooting or security incident response.</p>	<p>This is a binary compliance item. The firewall is compliant if the firewall is logging as expected. Otherwise, the system is not compliant.</p>	<p>Manually inspect each policy and verify that each policy has been configured to record an entry in the log file whenever traffic matches the conditions specified in the policy.</p> <ul style="list-style-type: none"> • get policy (look for the column titled "STLC" to the far right) <p>STLC stands for "Schedule, Traffic, Log, and Content." If logging for a given policy has been enabled, you should see an "X" in the third character position. For example:</p> <p>--X-</p> <p>If logging has not been enabled, you will see an "-" in the third character position.</p>	O

2	<p>CO19. The audit trail or log must include action taken by administrators, including user IDs; login date/time; log-out date/time; changes to policies; changes or additions to user privileges; and system start-ups and shut-downs.</p> <p><u>Reference</u>: Wood, Charles Cresson. <u>Information Security Policies Made Easy</u>. Eighth ed. Houston: Pentasafe, 2001, pp. 102-109.</p>	<p>Such logs could be useful when troubleshooting connectivity problems. In addition, although a malicious firewall administrator could erase any logs on the firewall, there is some security value in logging administrative activity.</p>	<p>This is a binary compliance item. The firewall is compliant if the firewall records administrative activity. Otherwise, the system is not compliant.</p>	<p>Verify that the firewall records all firewall management activity.</p> <ul style="list-style-type: none">• get log event <p>Inspect the log entries to determine if administrative activity is in fact logged. If you cannot find evidence that a particular type of administrative activity, consider making the relevant kind of test change to force the appropriate kind of confirmation to appear in the Netscreen-100's event log.</p>	O
---	---	--	---	--	---

3	<p>C20. Firewall logs must be stored on a dedicated syslog server.</p> <p><u>Reference:</u> Cheswick, William R., Steven M. Bellovin, and Aviel D. Rubin. <u>Firewalls and Internet Security: Repelling the Wily Hacker</u>. Second ed. Boston: Addison-Wesley, 2003, p. 159; cf. Gill, Stephen. "Application Note: Hardening Netscreen Firewalls." Version 1.2. 18 July 2002. URL: http://www.qorbit.net/documents/screenos-hardening-appnote.pdf (8 July 2003), p. 6.</p>	<p>In the event of a firewall compromise or of system failure, the log data would be lost. Storing the log data on a second, hardened server greatly reduces the risk of log data being lost.</p>	<p>This is a binary compliance item. The firewall is compliant if the syslog hostname, security facility, and facilities have been configured and if the module field is not blank. Otherwise, the system is not compliant.</p>	<p>Verify that the firewall is logging to a dedicated syslog server.</p> <ul style="list-style-type: none"> • Verify the firewall has been configured to send logs to a dedicated syslogs server <p>get syslog config</p> <ul style="list-style-type: none"> • Check the logs on the relevant syslog server to validate that it is capturing the firewall logs as expected. 	O
4	<p>CO21. The audit trails must be retained in accordance with the organization's data retention policy.</p> <p><u>Reference:</u> Wood, Charles Cresson. <u>Information Security Policies Made Easy</u>. Eighth ed. Houston: Pentasafe, 2001, p. 105.</p>	<p>The importance of log data may not be known immediately. If the firewall logs are retained for a reasonable amount of time, important data may be lost by the time it is determined relevant as part of an Incident Response Team investigation.</p>	<p>This is a binary compliance item. The firewall is compliant if the logs are retained in accordance with the data retention policy. Otherwise, the system is not compliant.</p>	<p>Verify that firewall logs are kept as long as required by the organization's data retention policy.</p>	O

G. Miscellaneous Section					
1	<p>CO22. Procedures for backing up and restoring the firewall configuration must be documented.</p> <p><u>Reference:</u> Lowder, Jeffery J. "Firewall Management and Internet Attacks." <u>Information Security Management Handbook</u>. Ed. Harold F. Tipton and Mi[k]ki Krause. 4th ed. Vol. 1. Boca Raton, Florida: Auerbach, 2000, p. 126; The SANS Institute, "7.2 Auditing the Perimeter" (2003), p. 4-16.</p>	<p>If the procedures for backing up and restoring firewall configuration are not documented, the configuration may not be properly backed up or restored. A change in personnel could mean that a firewall administrator might be unfamiliar with the procedure. Having documented procedures also increases the likelihood that the procedures have been thought through, presumably in a non-crisis situation.</p>	<p>This is a binary compliance item. The organization is compliant if there are documented procedures for backup and restoration of the firewall configuration. Otherwise, the system is not compliant.</p>	<p>Determine whether documented procedures exist for backup and restoration of the firewall configuration.</p>	

Assignment 3 – Audit Evidence

In this section, I will summarize the evidence relating to the ten tests I believe are the most critical to determining the degree of risk posed by the firewall's current configuration and management practices. Five of the tests are stimulus-response: B4, B7, C2, C4, C9.

Checklist Item B1: PASS

Control Objective: The firewall(s) must be kept current with the latest vendor upgrades, security patches, and security problem fix software.

NetScreen Command Line Interface (CLI)

Execution of the "get system" command at the ScreenOS CLI revealed the firewall is running ScreenOS version 3.0.3r6.

Remote Management Console

```
ns100(M)-> get system
Serial Number: <censored>, Control Number: 00000000
SW Version/Checksum: 3.0.3r6.0/6b60e662, HW Version: 3110(0)-(11)
Image: ns100.3.0.3r6, Firewall+VPN, FPGA checksum: 00000000 (0/0)
```

Note: the remainder of the "get system" command output was omitted.

NetScreen.com "Current Release" Web Page

According to Netscreen's website, the latest version of the ScreenOS for Netscreen-100s in production is 3.0.3r5.¹³

Checklist Item B4: PASS

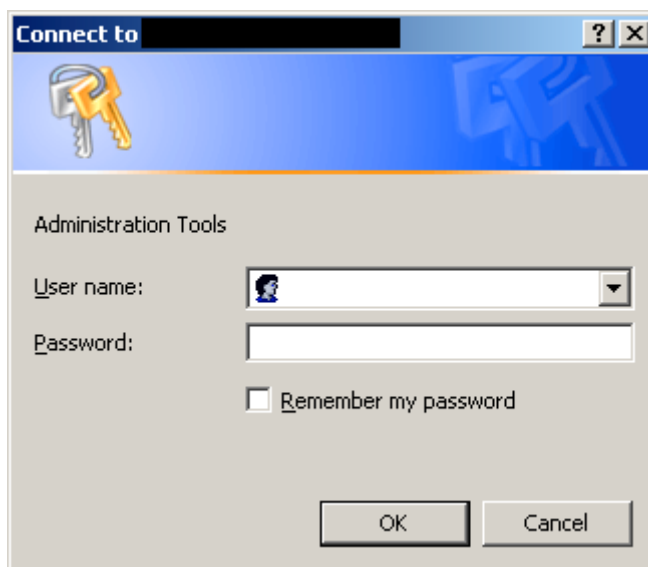
Objective: Only authorized personnel may be permitted to administer the firewall(s). Administrative access to the firewall(s) must be strictly limited to those personnel responsible for maintaining the firewall(s).

```
# ssh -c 3DES <firewall management IP censored>
jlowder@<firewall management IP censored>'s password:
Permission denied, please try again.
jlowder@<firewall management IP censored>'s password:
Permission denied, please try again.
jlowder@<firewall management IP censored>'s password:
Permission denied.
#
```

When I pressed <ENTER> without supplying a password, the firewall presented the "Permission denied, please try again" error message and then prompted me for my

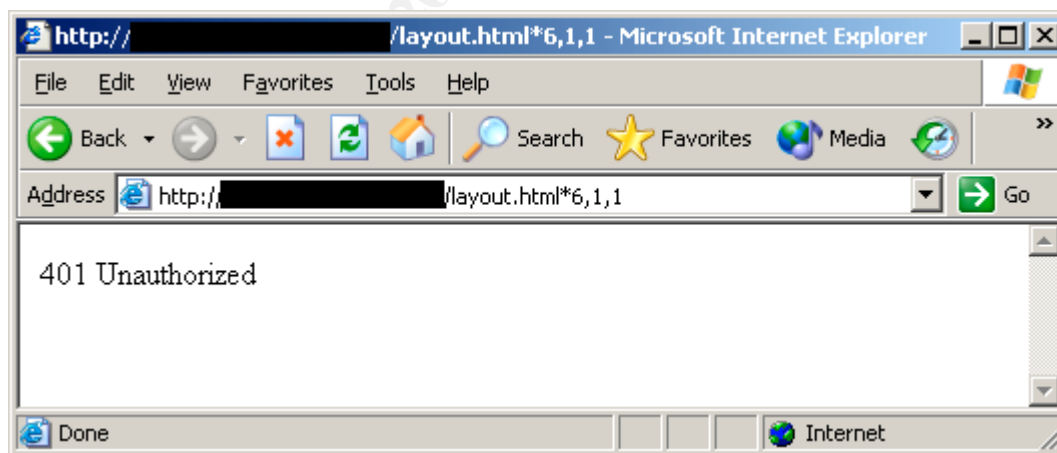
password again. After the third failed attempt, it displayed a "Permission denied" error message.

Figure 2 – Login Screen for Web-Based Management Session



When I pressed "OK" without supplying a username or password, the firewall presented the "Connect to" dialog box again. After three failed attempts, it displayed a "401 Unauthorized" error message.

Figure 3 – Unauthorized Error Message after Repeated Failed Logins



Since both SSH and HTTP connections to the management interface required me to supply a valid username and password, the firewall is compliant with item B4.

Checklist Item B7: PASS

Objective: Firewall administrators must have at least two user-IDs. One of these user-IDs (e.g., root) must provide privileged access and be logged; the other must be a normal user-ID for the day-to-day work of an ordinary user.

```
ns100(M)-> get admin user
User Name          Privilege
<privileged>      ROOT
<user1>           All
<backup>          READ-ONLY
<user2>           All
ns100(M)->
```

Note: I have censored the actual account names and instead replaced them with descriptions that should indicate the type of account they are.

The first user-ID is the privileged account. The second and fourth user-IDs belong to the employees responsible for firewall administration. I compared those user-IDs against an organizational chart provided by the Human Resources department. I confirmed that the employees with firewall user IDs are indeed members of the security team responsible for administering the firewall. The third user-ID has read-only access and is used for backups.

I then checked the event log to determine which accounts were being used for day-to-day firewall administration and maintenance. Although I cannot include the entire output of the command here, I will provide a representative sample of what I observed.

```
ns100(M)-> get log event
2003-07-17 00:21:01 system warn 00515 Admin <backup> has logged out via SCS
from <IP address censored>:49547
2003-07-17 00:21:01 system warn 00515 Admin <backup> has logged on via SCS
from <IP address censored>:49547
2003-07-17 00:21:00 system notif 00528 SCS: SSH user <backup> has been
authenticated using password from <IP address censored>:49547.
2003-07-16 14:32:07 system info 00767 <user1>: System Config saved from host
<IP address censored>
2003-07-16 14:32:17 system notif 00018 <user1>: Policy 91 has been moved
before 65
2003-07-16 14:32:07 system notif 00018 <user1>: Policy (91, <censored>) has
been added from host <IP address censored>
2003-07-16 14:29:24 system warn 00515 <user1>: Admin "<user1>" has logged on
via the WebUI(http) to port 80 from <IP address censored>:23751.
```

In the above example, <user1> changed the firewall policies, not <privileged> user. This is what I consistently observed when I examined a representative sample of the firewall logs: all policy configuration changes were made by either <user1> or <user2>, not <privileged>. Thus, the control objective is being met.

Checklist Item B8: FAIL

Objective: Firewall management sessions are extremely sensitive and must be encrypted.

Remote Management Console

```
ns100(M)-> get interface
Interface:
Name      Stat IP Address      Subnet Mask      MAC              Manage IP
trust     up   <censored>      255.255.255.128 <censored>      <censored>
untrust   up   <censored>      255.255.255.128 <censored>      <censored>
DMZ       up   <censored>      255.255.255.128 <censored>      <censored>
ns100(M)-> get interface trust
interface trust, mode route, up/full-duplex
  ip <censored>/255.255.255.128 gateway 0.0.0.0, virtual mac 0010.dbff.0100
  gateway 0.0.0.0, manage ip <censored>, mac <censored>
  ping enabled, telnet disabled, SCS enabled, SNMP enabled
  Global-Pro disabled, web enabled, ident-reset disabled
  SSL enabled
  bandwidth: physical 100000kbps, configured 0kbps, current 0bps
              total configured gbw 0kbps, total allocated gbw 0kbps
ns100(M)-> get interface untrust
interface untrust, up/full-duplex
  ip <censored>/255.255.255.128 gateway <censored>, virtual mac
0010.dbff.0101
  gateway <censored>, manage ip <censored>, mac <censored>
  ping enabled, telnet disabled, SCS enabled, SNMP disabled
  Global-Pro enabled, web enabled, ident-reset enabled
  SSL disabled
  bandwidth: physical 100000kbps, configured 0kbps, current 0bps
              total configured gbw 0kbps, total allocated gbw 0kbps
ns100(M)-> get interface dmz
interface DMZ, up/full-duplex
  ip <censored>/255.255.255.128 gateway 0.0.0.0, virtual mac 0010.dbff.0102
  gateway 0.0.0.0, manage ip <censored>, mac <censored>
  ping enabled, telnet disabled, SCS disabled, SNMP disabled
  Global-Pro disabled, web disabled, ident-reset disabled
  SSL disabled
  bandwidth: physical 100000kbps, configured 0kbps, current 0bps
              total configured gbw 0kbps, total allocated gbw 0kbps
```

The "trust" interface is compliant because both CLI-based and web-based management sessions are encrypted. CLI sessions use "SCS" or Secure Command Shell (i.e., SSH), while web-based sessions use SSL. The "dmz" interface is also compliant since all management activity has been prohibited on that interface. Nevertheless, the "untrust" interface is not compliant. While CLI sessions must use SSH ("SCS enabled"), web-based sessions use unencrypted HTTP ("web enabled" and "SSL disabled"). Therefore, because of the configuration of the "untrust" interface—arguably the most critical of all three interfaces with respect to the need for encryption—the firewall is not compliant.

Checklist Item C2: FAIL

Objective: All ports on the firewall itself should be disabled by default; only ports that have been specifically authorized should be open.


```
$ nmap -sT <management IP> -oA untrusted-to-firewall-tcp.txt
$ cat untrusted-to-firewall-tcp.txt
Interesting ports on <hostname censored> (<IP address censored>):
(The 65532 ports scanned but not shown below are in state: filtered)
Port      State      Service
22/tcp    open       ssh
80/tcp    open       http
113/tcp   closed     auth

$ nmap -sU <management IP> -oA untrusted-to-firewall-udp.txt
$ cat untrusted-to-firewall-udp.txt
All 65535 scanned ports on <hostname censored> (<IP address censored>) are:
filtered

$ nmap -sP <management IP> -oA untrusted-to-firewall-icmp.txt
$ cat untrusted-to-firewall-icmp.txt
Host <hostname censored> (<IP address censored>) appears to be up.
```

The HTTP service (TCP port 80) should not be running on the untrusted management interface of the firewall, according to best practices. (Notice the correspondence between this finding and the related finding under checklist item B8.) Therefore, the firewall fails checklist item C2.

Checklist Item C4: PASS

Objective: The firewall(s) should control any application and infrastructure management flows in *both* directions. The firewall(s) must deny by default any services not explicitly authorized.

Scan of DMZ from Untrust: PASS

Nmap Output

```
# nmap -sP -iL nmap-input.txt
Reading target specifications from FILE: nmap-input.txt

Starting nmap 3.20 ( www.insecure.org/nmap/ ) at 2003-07-23 16:39 PDT
Host host4.foo.com (<IP address censored>) appears to be up.
Nmap run completed -- 5 IP addresses (1 host up) scanned in 1.226 seconds
# /usr/local/bin/nmap -v -g53 -P0 -sS -T Aggressive -iL nmap-input.txt -oN
untrust-to-dmz-tcp-syn.txt
Reading target specifications from FILE: nmap-input.txt

Starting nmap 3.20 ( www.insecure.org/nmap/ ) at 2003-07-23 17:08 PDT
Host host2.foo.com (<IP address censored>) appears to be up ... good.
Initiating SYN Stealth Scan against host2.foo.com (<IP address censored>) at
17:08
Adding open port 22/tcp
The SYN Stealth Scan took 123 seconds to scan 1611 ports.
Interesting ports on host2.foo.com (<IP address censored>):
(The 1610 ports scanned but not shown below are in state: filtered)
Port      State      Service
```

22/tcp open ssh

Host host3.foo.com (<IP address censored>) appears to be up ... good.
Initiating SYN Stealth Scan against host3.foo.com (<IP address censored>) at 17:10

Adding open port 22/tcp

The SYN Stealth Scan took 114 seconds to scan 1611 ports.

Interesting ports on host3.foo.com (<IP address censored>):

(The 1610 ports scanned but not shown below are in state: filtered)

Port	State	Service
22/tcp	open	ssh

Host host4.foo.com (<IP address censored>) appears to be up ... good.

Initiating SYN Stealth Scan against host4.foo.com (<IP address censored>) at 17:12

Adding open port 1521/tcp

Adding open port 22/tcp

The SYN Stealth Scan took 300 seconds to scan 1611 ports.

Interesting ports on host4.foo.com (<IP address censored>):

(The 1574 ports scanned but not shown below are in state: filtered)

Port	State	Service
22/tcp	open	ssh
1400/tcp	closed	cadkey-tablet
1401/tcp	closed	goldleaf-licman
1402/tcp	closed	prm-sm-np
1403/tcp	closed	prm-nm-np
1404/tcp	closed	igi-lm
1405/tcp	closed	ibm-res
1406/tcp	closed	netlabs-lm
1407/tcp	closed	dbsa-lm
1408/tcp	closed	sophia-lm
1409/tcp	closed	here-lm
1410/tcp	closed	hiq
1411/tcp	closed	af
1413/tcp	closed	innosys-acl
1414/tcp	closed	ibm-mqseries
1415/tcp	closed	dbstar
1416/tcp	closed	novell-lu6.2
1417/tcp	closed	timbuktu-srv1
1418/tcp	closed	timbuktu-srv2
1419/tcp	closed	timbuktu-srv3
1420/tcp	closed	timbuktu-srv4
1422/tcp	closed	autodesk-lm
1423/tcp	closed	essbase
1425/tcp	closed	zion-lm
1426/tcp	closed	sas-1
1427/tcp	closed	mload
1428/tcp	closed	informatik-lm
1429/tcp	closed	nms
1430/tcp	closed	tpdu
1450/tcp	closed	dwf
1500/tcp	closed	vlsci-lm
1501/tcp	closed	sas-3
1502/tcp	closed	shivadiscovery
1503/tcp	closed	imtc-mcs
1504/tcp	closed	evb-elm
1505/tcp	closed	funkproxy

1521/tcp open oracle

Host host5.foo.com (<IP address censored>) appears to be up ... good.
Initiating SYN Stealth Scan against host5.foo.com (<IP address censored>) at 17:17

Adding open port 22/tcp

The SYN Stealth Scan took 115 seconds to scan 1611 ports.

Interesting ports on host5.foo.com (<IP address censored>):

(The 1610 ports scanned but not shown below are in state: filtered)

Port	State	Service
22/tcp	open	ssh

Host host1.foo.com (<IP address censored>) appears to be up ... good.

Initiating SYN Stealth Scan against host1.foo.com (<IP address censored>) at 17:19

Adding open port 22/tcp

The SYN Stealth Scan took 113 seconds to scan 1611 ports.

Interesting ports on host1.foo.com (<IP address censored>):

(The 1610 ports scanned but not shown below are in state: filtered)

Port	State	Service
22/tcp	open	ssh

Nmap run completed -- 5 IP addresses (5 hosts up) scanned in 764.949 seconds

/usr/local/bin/nmap -v -g53 -P0 -sU -T Aggressive -iL nmap-input.txt -oN untrust-to-dmz-udp.txt

Host host2.foo.com (<IP address censored>) appears to be up ... good.

Initiating UDP Scan against host2.foo.com (<IP address censored>) at 17:27

(no udp responses received -- assuming all ports filtered)

All 1470 scanned ports on host2.foo.com (<IP address censored>) are: filtered

Host host3.foo.com (<IP address censored>) appears to be up ... good.

Initiating UDP Scan against host3.foo.com (<IP address censored>) at 17:33

(no udp responses received -- assuming all ports filtered)

All 1470 scanned ports on host3.foo.com (<IP address censored>) are: filtered

Host host5.foo.com (<IP address censored>) appears to be up ... good.

Initiating UDP Scan against host5.foo.com (<IP address censored>) at 17:39

(no udp responses received -- assuming all ports filtered)

All 1470 scanned ports on host5.foo.com (<IP address censored>) are: filtered

Host host4.foo.com (<IP address censored>) appears to be up ... good.

Initiating UDP Scan against host4.foo.com (<IP address censored>) at 17:45

(no udp responses received -- assuming all ports filtered)

All 1470 scanned ports on host4.foo.com (<IP address censored>) are: filtered

Host host1.foo.com (<IP address censored>) appears to be up ... good.

Initiating UDP Scan against host1.foo.com (<IP address censored>) at 17:51

(no udp responses received -- assuming all ports filtered)

All 1470 scanned ports on host1.foo.com (<IP address censored>) are: filtered

Nmap run completed -- 5 IP addresses (5 hosts up) scanned in 1889.080 seconds

Results of the Nmap Scan Recorded with the Sniffer Snort

Since we are running the Snort Intrusion Detection System in the e-commerce system, I checked the Snort logs to learn how much of my Nmap scan was detected by Snort. Snort monitors network traffic on both the DMZ and Trust interfaces of the Netscreen-100 firewall. When it detects traffic that matches an enabled signature, it writes data in a binary format into the appropriate directory tree: `dmz` for DMZ interface traffic and `trust` for Trust interface traffic. Barnyard is a separate Snort process that converts the raw, binary data into a human-readable text format. Barnyard creates two files: `fast.alert` and `dump.log`. The `fast.alert` file is an executive summary of the day's alerts, while the `dump.log` file contains both the alerts and the raw data dump of that alert.

Although my Nmap scan ran between approximately 4:45 and 6:00 p.m. PDT, Barnyard converts the timestamps on all log entries to UTC/GMT. Therefore, any scan traffic should be identified between 2345 and 0100 GMT. I used the `tail` command to monitor the `fast.alert` file for any entries that matches the IP address of my Nessus server; I executed this command prior to launching my nmap scan. The output of the command is included below.

```
# clear; tail -f fast.alert
#
```

No nmap traffic was detected by Snort.

Assessment

The firewall clearly controls application and infrastructure management flows from the untrusted interface to the DMZ interface. It denies by default any services not explicitly authorized. Moreover, the network-based intrusion detection system did not detect any network traffic on unauthorized ports. Therefore, the firewall is compliant with item C4 regarding untrusted to DMZ traffic.

Scan of Trust from Untrust: PASS

Nmap Output

```
# /usr/local/bin/nmap -v -sP -T Aggressive -iL trust-hosts.txt -oN untrust-  
to-trust-icmp.txt
```

Reading target specifications from FILE: trust-hosts.txt

Starting nmap 3.20 (www.insecure.org/nmap/) at 2003-07-23 18:02 PDT

Host <ip address censored> appears to be down.

Host <ip address censored> appears to be down.

Host <ip address censored> appears to be down.

Host <ip address censored> appears to be down.

Nmap run completed -- 4 IP addresses (0 hosts up) scanned in 1.995 seconds

```
# /usr/local/bin/nmap -v -g53 -P0 -sS -T Aggressive -iL trust-hosts.txt -oN  
untrust-to-trust-tcp-syn.txt
```

Reading target specifications from FILE: trust-hosts.txt

Starting nmap 3.20 (www.insecure.org/nmap/) at 2003-07-23 18:04 PDT
Host host13.foo.com (<IP address censored>) appears to be up ... good.
Initiating SYN Stealth Scan against host13.foo.com (<IP address censored>) at 18:4

The SYN Stealth Scan took 117 seconds to scan 1611 ports.
All 1611 scanned ports on host13.foo.com (<IP address censored>) are:
filtered

Host host14.foo.com (<IP address censored>) appears to be up ... good.
Initiating SYN Stealth Scan against host14.foo.com (<IP address censored>) at 18:6

The SYN Stealth Scan took 117 seconds to scan 1611 ports.
All 1611 scanned ports on host14.foo.com (<IP address censored>) are:
filtered

Host host15.foo.com (<IP address censored>) appears to be up ... good.
Initiating SYN Stealth Scan against host15.foo.com (<IP address censored>) at 18:7

The SYN Stealth Scan took 119 seconds to scan 1611 ports.
All 1611 scanned ports on host15.foo.com (<IP address censored>) are:
filtered

Host host12.foo.com (<IP address censored>) appears to be up ... good.
Initiating SYN Stealth Scan against host12.foo.com (<IP address censored>) at 18:9

The SYN Stealth Scan took 115 seconds to scan 1611 ports.
All 1611 scanned ports on host12.foo.com (<IP address censored>) are:
filtered

Nmap run completed -- 4 IP addresses (4 hosts up) scanned in 468.070 seconds
/usr/local/bin/nmap -v -g53 -P0 -sU -T Aggressive -iL trust-hosts.txt -oN untrust-to-trust-udp.txt

Reading target specifications from FILE: trust-hosts.txt

Starting nmap 3.20 (www.insecure.org/nmap/) at 2003-07-23 18:16 PDT
Host host13.foo.com (<IP address censored>) appears to be up ... good.
Initiating UDP Scan against host13.foo.com (<IP address censored>) at 18:16
(no udp responses received -- assuming all ports filtered)
All 1470 scanned ports on host13.foo.com (<IP address censored>) are:
filtered

Host host14.foo.com (<IP address censored>) appears to be up ... good.
Initiating UDP Scan against host14.foo.com (<IP address censored>) at 18:22
(no udp responses received -- assuming all ports filtered)
All 1470 scanned ports on host14.foo.com (<IP address censored>) are:
filtered

Host host15.foo.com (<IP address censored>) appears to be up ... good.
Initiating UDP Scan against host15.foo.com (<IP address censored>) at 18:28
(no udp responses received -- assuming all ports filtered)
All 1470 scanned ports on host15.foo.com (<IP address censored>) are:
filtered

Host host12.foo.com (<IP address censored>) appears to be up ... good.
Initiating UDP Scan against host12.foo.com (<IP address censored>) at 18:34
(no udp responses received -- assuming all ports filtered)

All 1470 scanned ports on host12.foo.com (<IP address censored>) are:
filtered

Nmap run completed -- 4 IP addresses (4 hosts up) scanned in 1511.200 seconds

Results of the Nmap Scan Recorded with the Sniffer Snort

```
# clear; tail -f fast.alert
#
```

No nmap traffic was detected by Snort.

Assessment

The firewall clearly controls application and infrastructure management flows from the untrusted interface to the trusted interface. It denies by default any services not explicitly authorized. Moreover, the network-based intrusion detection system did not detect any network traffic on unauthorized ports. Therefore, the firewall is compliant with item C4 regarding untrusted to trusted traffic.

Scan of Untrust from DMZ: PASS

Nmap Output

```
# /usr/local/bin/nmap -v -sP -T Aggressive -iL untrust-hosts.txt -oN dmz-to-untrust-icmp.txt
```

Reading target specifications from FILE: untrust-hosts.txt

Starting nmap 3.30 (<http://www.insecure.org/nmap/>) at 2003-07-28 17:19 PDT

Host host6.foo.com (<IP address censored>) appears to be up.

Host host7.foo.com (<IP address censored>) appears to be up.

Nmap run completed -- 2 IP addresses (2 hosts up) scanned in 0.481 seconds

```
# /usr/local/bin/nmap -v -g22 -P0 -sS -T Aggressive -iL untrust-hosts.txt -oN dmz-to-untrust-tcp-syn.txt
```

Reading target specifications from FILE: untrust-hosts.txt

Starting nmap 3.30 (<http://www.insecure.org/nmap/>) at 2003-07-28 17:21 PDT

Host host6.foo.com (<IP address censored>) appears to be up ... good.

Initiating SYN Stealth Scan against host6.foo.com (<IP address censored>) at 17:21

Adding open port 135/tcp

Adding open port 813/tcp

Adding open port 683/tcp

Adding open port 703/tcp

Adding open port 111/tcp

Adding open port 32770/tcp

Adding open port 22/tcp

The SYN Stealth Scan took 1 second to scan 1644 ports.

Interesting ports on host6.foo.com (<IP address censored>):

(The 1637 ports scanned but not shown below are in state: closed)

Port	State	Service
------	-------	---------

22/tcp	open	ssh
111/tcp	open	sunrpc
135/tcp	open	loc-srv
683/tcp	open	unknown
703/tcp	open	unknown
813/tcp	open	unknown
32770/tcp	open	sometimes-rpc3

Host host7.foo.com (<IP address censored>) appears to be up ... good.
Initiating SYN Stealth Scan against host7.foo.com (<IP address censored>) at 17:21

Adding open port 53/tcp
Adding open port 32772/tcp
Adding open port 111/tcp
Adding open port 22/tcp
Adding open port 32771/tcp
Adding open port 32777/tcp
Adding open port 4045/tcp

The SYN Stealth Scan took 0 seconds to scan 1644 ports.

Interesting ports on host7.foo.com (<IP address censored>):

(The 1637 ports scanned but not shown below are in state: closed)

Port	State	Service
22/tcp	open	ssh
53/tcp	open	domain
111/tcp	open	sunrpc
4045/tcp	open	lockd
32771/tcp	open	sometimes-rpc5
32772/tcp	open	sometimes-rpc7
32777/tcp	open	sometimes-rpc17

Nmap run completed -- 2 IP addresses (2 hosts up) scanned in 1.387 seconds

/usr/local/bin/nmap -v -g53 -P0 -sU -T Aggressive -iL untrust-hosts.txt -oN dmz-to-untrust-udp.txt

Reading target specifications from FILE: untrust-hosts.txt

Starting nmap 3.30 (<http://www.insecure.org/nmap/>) at 2003-07-29 08:32 PDT

Host host6.foo.com (<IP address censored>) appears to be up ... good.

Initiating UDP Scan against host6.foo.com (<IP address censored>) at 08:32

The UDP Scan took 8872 seconds to scan 1471 ports.

Interesting ports on host6.foo.com (<IP address censored>):

(The 1452 ports scanned but not shown below are in state: closed)

Port	State	Service
111/udp	open	sunrpc
135/udp	open	loc-srv
655/udp	open	unknown
680/udp	open	unknown
700/udp	open	unknown
798/udp	open	unknown
799/udp	open	unknown
800/udp	open	mdbs_daemon
814/udp	open	unknown
1022/udp	open	unknown
1023/udp	open	unknown
32770/udp	open	sometimes-rpc4
32771/udp	open	sometimes-rpc6
32772/udp	open	sometimes-rpc8
32773/udp	open	sometimes-rpc10

```
32774/udp  open      sometimes-rpc12
32776/udp  open      sometimes-rpc16
32777/udp  open      sometimes-rpc18
32778/udp  open      sometimes-rpc20
```

Host host7.foo.com (<IP address censored>) appears to be up ... good.
Initiating UDP Scan against host7.foo.com (<IP address censored>) at 11:00
The UDP Scan took 26120 seconds to scan 1471 ports.
Interesting ports on host7.foo.com (<IP address censored>):
(The 1448 ports scanned but not shown below are in state: closed)

Port	State	Service
53/udp	open	domain
111/udp	open	sunrpc
123/udp	open	ntp
161/udp	open	snmp
514/udp	open	syslog
742/udp	open	netrcs
1015/udp	open	unknown
1016/udp	open	unknown
1017/udp	open	unknown
1018/udp	open	unknown
1019/udp	open	unknown
1020/udp	open	unknown
1021/udp	open	unknown
1022/udp	open	unknown
1023/udp	open	unknown
4045/udp	open	lockd
32771/udp	open	sometimes-rpc6
32773/udp	open	sometimes-rpc10
32774/udp	open	sometimes-rpc12
32777/udp	open	sometimes-rpc18
32778/udp	open	sometimes-rpc20
32780/udp	open	sometimes-rpc24
32787/udp	open	sometimes-rpc28

Nmap run completed at Tue Jul 29 18:15:22 2003 -- 2 IP addresses (2 hosts up) scanned in 34992.678 seconds

Results of the Nmap Scan Recorded with the Sniffer Snort

```
# clear; tail -f fast.alert
#
```

No nmap traffic was detected by Snort.

Assessment

The firewall clearly controls application and infrastructure management flows from the DMZ interface to the untrusted interface. It denies by default any services not explicitly authorized. Moreover, the network-based intrusion detection system did not detect any network traffic on unauthorized ports. Therefore, the firewall is compliant with item C4 regarding DMZ to untrusted traffic.

Scan of Trust from DMZ: PASS

Nmap Output

```
# /usr/local/bin/nmap -v -sP -T Aggressive -iL trust-hosts.txt -oN dmz-to-trust-icmp.txt
```

Reading target specifications from FILE: trust-hosts.txt

Starting nmap 3.30 (<http://www.insecure.org/nmap/>) at 2003-07-28 17:22 PDT

Host host13.foo.com (<IP address censored>) appears to be up.

Host host12.foo.com (<IP address censored>) appears to be up.

Host host14.foo.com (<IP address censored>) appears to be up.

Host host15.foo.com (<IP address censored>) appears to be up.

Nmap run completed -- 4 IP addresses (4 hosts up) scanned in 0.370 seconds

```
# /usr/local/bin/nmap -v -g22 -P0 -sS -T Aggressive -iL trust-hosts.txt -oN dmz-to-trust-tcp-syn.txt
```

Reading target specifications from FILE: trust-hosts.txt

Starting nmap 3.30 (<http://www.insecure.org/nmap/>) at 2003-07-28 17:22 PDT

Host host13.foo.com (<IP address censored>) appears to be up ... good.

Initiating SYN Stealth Scan against host13.foo.com (<IP address censored>) at 17:22

Adding open port 22/tcp

The SYN Stealth Scan took 102 seconds to scan 1644 ports.

Interesting ports on host13.foo.com (<IP address censored>):

(The 1643 ports scanned but not shown below are in state: filtered)

Port	State	Service
22/tcp	open	ssh

Host host12.foo.com (<IP address censored>) appears to be up ... good.

Initiating SYN Stealth Scan against host12.foo.com (<IP address censored>) at 17:24

Adding open port 22/tcp

The SYN Stealth Scan took 100 seconds to scan 1644 ports.

Interesting ports on host12.foo.com (<IP address censored>):

(The 1643 ports scanned but not shown below are in state: filtered)

Port	State	Service
22/tcp	open	ssh

Host host14.foo.com (<IP address censored>) appears to be up ... good.

Initiating SYN Stealth Scan against host14.foo.com (<IP address censored>) at 17:25

Adding open port 22/tcp

The SYN Stealth Scan took 99 seconds to scan 1644 ports.

Interesting ports on host14.foo.com (<IP address censored>):

(The 1643 ports scanned but not shown below are in state: filtered)

Port	State	Service
22/tcp	open	ssh

Host host15.foo.com (<IP address censored>) appears to be up ... good.

Initiating SYN Stealth Scan against host15.foo.com (<IP address censored>) at 17:27

Adding open port 22/tcp

The SYN Stealth Scan took 103 seconds to scan 1644 ports.

Interesting ports on host15.foo.com (<IP address censored>):

(The 1643 ports scanned but not shown below are in state: filtered)

Port	State	Service
22/tcp	open	ssh

Nmap run completed -- 4 IP addresses (4 hosts up) scanned in 404.719 seconds

```
# /usr/local/bin/nmap -v -g53 -P0 -sU -T Aggressive -iL trust-hosts.txt -oN dmz-to-trust-udp.txt
```

Reading target specifications from FILE: trust-hosts.txt

Starting nmap 3.30 (<http://www.insecure.org/nmap/>) at 2003-07-28 14:13 PDT

Host host13.foo.com (<IP address censored>) appears to be up ... good.

Initiating UDP Scan against host13.foo.com (<IP address censored>) at 14:13

The UDP Scan took 5608 seconds to scan 1471 ports.

(no udp responses received -- assuming all ports filtered)

All 1471 scanned ports on host13.foo.com (<IP address censored>) are:
filtered

Host host12.foo.com (<IP address censored>) appears to be up ... good.

Initiating UDP Scan against host12.foo.com (<IP address censored>) at 19:08

The UDP Scan took 10508 seconds to scan 1471 ports.

(no udp responses received -- assuming all ports filtered)

All 1471 scanned ports on host12.foo.com (<IP address censored>) are:
filtered

Host host14.foo.com (<IP address censored>) appears to be up ... good.

Initiating UDP Scan against host14.foo.com (<IP address censored>) at 20:42

The UDP Scan took 10508 seconds to scan 1471 ports.

(no udp responses received -- assuming all ports filtered)

All 1471 scanned ports on host14.foo.com (<IP address censored>) are:
filtered

Host host15.foo.com (<IP address censored>) appears to be up ... good.

Initiating UDP Scan against host15.foo.com (<IP address censored>) at 23:31

The UDP Scan took 10508 seconds to scan 1471 ports.

(no udp responses received -- assuming all ports filtered)

All 1471 scanned ports on host15.foo.com (<IP address censored>) are:
filtered

Nmap run completed -- 5 IP addresses (5 hosts up) scanned in 45038.287 seconds

Results of the Nmap Scan Recorded with the Sniffer Snort

```
# clear; tail -f fast.alert
```

```
-----  
07/28/03-23:17:26.466667 {ICMP} <host1.foo.com IP address censored> ->  
<host14.foo.com IP address censored>
```

```
[**] [1:402:4] ICMP Destination Unreachable (Port Unreachable) [**]
```

```
[Classification: Misc activity] [Priority: 3]  
-----
```

```
07/28/03-23:17:26.466675 {ICMP} <host1.foo.com IP address censored> ->  
<host14.foo.com IP address censored>
```

```
[**] [1:402:4] ICMP Destination Unreachable (Port Unreachable) [**]
```

```
[Classification: Misc activity] [Priority: 3]  
-----
```

```
07/28/03-23:17:26.466689 {ICMP} <host1.foo.com IP address censored> ->
<host14.foo.com IP address censored>
[**] [1:402:4] ICMP Destination Unreachable (Port Unreachable) [**]
[Classification: Misc activity] [Priority: 3]
-----
```

```
07/28/03-23:17:26.466703 {ICMP} <host1.foo.com IP address censored> ->
<host14.foo.com IP address censored>
[**] [1:402:4] ICMP Destination Unreachable (Port Unreachable) [**]
[Classification: Misc activity] [Priority: 3]
-----
```

```
07/28/03-23:17:26.466738 {ICMP} <host1.foo.com IP address censored> ->
<host14.foo.com IP address censored>
[**] [1:402:4] ICMP Destination Unreachable (Port Unreachable) [**]
[Classification: Misc activity] [Priority: 3]
-----
```

(output truncated)

#

Snort recorded a tremendous number of these ICMP alerts. No other traffic was recorded by Snort.

Assessment

The firewall clearly controls application and infrastructure management flows from the DMZ interface to the trusted interface. It denies by default any services not explicitly authorized. Moreover, the network-based intrusion detection system did not detect any network traffic on unauthorized ports. Therefore, the firewall is compliant with item C4 regarding DMZ to trusted traffic.

Scan of Untrust from Trust: PASS

Nmap Output

```
# nmap -v -sP -T Aggressive -iL untrust-hosts.txt -oN trust-to-untrust-icmp.txt
```

Reading target specifications from FILE: untrust-hosts.txt

```
Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-07-28 17:03 PDT
Host host6.foo.com (<IP address censored>) appears to be up.
Host host7.foo.com (<IP address censored>) appears to be up.
Nmap run completed -- 2 IP addresses (2 hosts up) scanned in 0.385 seconds
```

```
# nmap -v -g22 -P0 -sS -T Aggressive -iL untrust-hosts.txt -oN trust-to-untrust-tcp.txt
```

Reading target specifications from FILE: untrust-hosts.txt

```
Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-07-28 17:04 PDT
Host host6.foo.com (<IP address censored>) appears to be up ... good.
Initiating SYN Stealth Scan against host6.foo.com (<IP address censored>) at 17:04
```

```
Adding open port 703/tcp
Adding open port 32770/tcp
Adding open port 135/tcp
Adding open port 22/tcp
```

Adding open port 111/tcp
Adding open port 683/tcp
Adding open port 813/tcp
The SYN Stealth Scan took 1 second to scan 1644 ports.
Interesting ports on host6.foo.com (<IP address censored>):
(The 1637 ports scanned but not shown below are in state: closed)

Port	State	Service
22/tcp	open	ssh
111/tcp	open	sunrpc
135/tcp	open	loc-srv
683/tcp	open	unknown
703/tcp	open	unknown
813/tcp	open	unknown
32770/tcp	open	sometimes-rpc3

Host host7.foo.com (<IP address censored>) appears to be up ... good.
Initiating SYN Stealth Scan against host7.foo.com (<IP address censored>) at 17:04

Adding open port 32777/tcp
Adding open port 4045/tcp
Adding open port 32772/tcp
Adding open port 22/tcp
Adding open port 111/tcp
Adding open port 53/tcp
Adding open port 32771/tcp

The SYN Stealth Scan took 0 seconds to scan 1644 ports.
Interesting ports on host7.foo.com (<IP address censored>):
(The 1637 ports scanned but not shown below are in state: closed)

Port	State	Service
22/tcp	open	ssh
53/tcp	open	domain
111/tcp	open	sunrpc
4045/tcp	open	lockd
32771/tcp	open	sometimes-rpc5
32772/tcp	open	sometimes-rpc7
32777/tcp	open	sometimes-rpc17

Nmap run completed -- 2 IP addresses (2 hosts up) scanned in 0.683 seconds

nmap -v -g53 -P0 -sU -T Aggressive -iL untrust-hosts.txt -oN trust-to-untrust-udp.txt

Reading target specifications from FILE: untrust-hosts.txt

Starting nmap 3.30 (<http://www.insecure.org/nmap/>) at 2003-07-28 17:16 PDT
Host host6.foo.com (<IP address censored>) appears to be up ... good.
Initiating UDP Scan against host6.foo.com (<IP address censored>) at 17:16
The UDP Scan took 1452 seconds to scan 1471 ports.

Adding open port 32771/udp
Adding open port 1023/udp
Adding open port 32778/udp
Adding open port 680/udp
Adding open port 32773/udp
Adding open port 655/udp
Adding open port 798/udp
Adding open port 111/udp
Adding open port 32776/udp
Adding open port 799/udp
Adding open port 135/udp

```
Adding open port 800/udp
Adding open port 814/udp
Adding open port 32774/udp
Adding open port 32777/udp
Adding open port 1022/udp
Adding open port 700/udp
Adding open port 32770/udp
Adding open port 32772/udp
Interesting ports on host6.foo.com (<IP address censored>):
(The 1452 ports scanned but not shown below are in state: closed)
Port      State      Service
111/udp   open       sunrpc
135/udp   open       loc-srv
655/udp   open       unknown
680/udp   open       unknown
700/udp   open       unknown
798/udp   open       unknown
799/udp   open       unknown
800/udp   open       mdbus_daemon
814/udp   open       unknown
1022/udp  open       unknown
1023/udp  open       unknown
32770/udp open       sometimes-rpc4
32771/udp open       sometimes-rpc6
32772/udp open       sometimes-rpc8
32773/udp open       sometimes-rpc10
32774/udp open       sometimes-rpc12
32776/udp open       sometimes-rpc16
32777/udp open       sometimes-rpc18
32778/udp open       sometimes-rpc20
```

Host host7.foo.com (<IP address censored>) appears to be up ... good.
Initiating UDP Scan against host7.foo.com (<IP address censored>) at 17:41
The UDP Scan took 831 seconds to scan 1471 ports.

```
Adding open port 1646/udp
Adding open port 1022/udp
Adding open port 32787/udp
Adding open port 32777/udp
Adding open port 1016/udp
Adding open port 32774/udp
Adding open port 514/udp
Adding open port 1021/udp
Adding open port 161/udp
Adding open port 1017/udp
Adding open port 4045/udp
Adding open port 1020/udp
Adding open port 1019/udp
Adding open port 742/udp
Adding open port 123/udp
Adding open port 111/udp
Adding open port 32773/udp
Adding open port 1018/udp
Adding open port 32780/udp
Adding open port 1015/udp
Adding open port 32778/udp
Adding open port 1023/udp
Adding open port 32771/udp
```

Adding open port 53/udp

Interesting ports on host7.foo.com (<IP address censored>):

(The 1447 ports scanned but not shown below are in state: closed)

Port	State	Service
53/udp	open	domain
111/udp	open	sunrpc
123/udp	open	ntp
161/udp	open	snmp
514/udp	open	syslog
742/udp	open	netrcs
1015/udp	open	unknown
1016/udp	open	unknown
1017/udp	open	unknown
1018/udp	open	unknown
1019/udp	open	unknown
1020/udp	open	unknown
1021/udp	open	unknown
1022/udp	open	unknown
1023/udp	open	unknown
1646/udp	open	radacct
4045/udp	open	lockd
32771/udp	open	sometimes-rpc6
32773/udp	open	sometimes-rpc10
32774/udp	open	sometimes-rpc12
32777/udp	open	sometimes-rpc18
32778/udp	open	sometimes-rpc20
32780/udp	open	sometimes-rpc24
32787/udp	open	sometimes-rpc28

Nmap run completed -- 2 IP addresses (2 hosts up) scanned in 2283.721 seconds
#

Results of the Nmap Scan Recorded with the Sniffer Snort

```
# clear; tail -f fast.alert
```

```
07/29/03-00:17:00.292903 {ICMP} <host6.foo.com IP address censored> ->  
<host14.foo.com IP address censored>  
[**] [1:402:4] ICMP Destination Unreachable (Port Unreachable) [**]  
[Classification: Misc activity] [Priority: 3]  
-----
```

The above entry repeated hundreds of times; I am quoting only an excerpt of the output.
Then the following entry repeated hundreds of times.

```
-----  
07/29/03-00:41:12.710627 {ICMP} <host7.foo.com IP address censored> ->  
<host14.foo.com IP address censored>  
[**] [1:402:4] ICMP Destination Unreachable (Port Unreachable) [**]  
[Classification: Misc activity] [Priority: 3]  
#
```

Assessment

The firewall clearly controls application and infrastructure management flows from the trusted interface to the untrusted interface. It denies by default any services not

explicitly authorized. Moreover, the network-based intrusion detection system did not detect any network traffic on unauthorized ports. Therefore, the firewall is compliant with item C4 regarding trusted to untrusted traffic.

Scan of DMZ from Trust: PASS

Nmap Output

```
# nmap -v -sP -T Aggressive -iL dmz-hosts.txt -oN trust-to-dmz-icmp.txt
```

Reading target specifications from FILE: dmz-hosts.txt

```
Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-07-28 16:11 PDT
Host host1.foo.com (<IP address censored>) appears to be up.
Host host2.foo.com (<IP address censored>) appears to be up.
Host host3.foo.com (<IP address censored>) appears to be up.
Host host4.foo.com (<IP address censored>) appears to be up.
Host host5.foo.com (<IP address censored>) appears to be up.
Nmap run completed -- 5 IP addresses (5 hosts up) scanned in 0.428 seconds
```

```
# nmap -v -g22 -P0 -sS -T Aggressive -iL dmz-hosts.txt -oN trust-to-dmz-tcp-syn.txt
```

Reading target specifications from FILE: dmz-hosts.txt

```
Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-07-28 16:15 PDT
Host host1.foo.com (<IP address censored>) appears to be up ... good.
Initiating SYN Stealth Scan against host1.foo.com (<IP address censored>) at 16:15
```

Adding open port 898/tcp

Adding open port 22/tcp

The SYN Stealth Scan took 35 seconds to scan 1644 ports.

Interesting ports on host1.foo.com (<IP address censored>):

(The 1087 ports scanned but not shown below are in state: closed)

Port	State	Service
1/tcp	filtered	tcpmux
2/tcp	filtered	compressnet
4/tcp	filtered	unknown
12/tcp	filtered	unknown
15/tcp	filtered	netstat
16/tcp	filtered	unknown
17/tcp	filtered	qotd
21/tcp	filtered	ftp
22/tcp	open	ssh
23/tcp	filtered	telnet
31/tcp	filtered	msg-auth
33/tcp	filtered	dsp
44/tcp	filtered	mpm-flags
50/tcp	filtered	re-mail-ck
52/tcp	filtered	xns-time
53/tcp	filtered	domain
54/tcp	filtered	xns-ch
56/tcp	filtered	xns-auth
57/tcp	filtered	priv-term
58/tcp	filtered	xns-mail
62/tcp	filtered	acas
70/tcp	filtered	gopher
74/tcp	filtered	netrjs-4

76/tcp	filtered	deos
79/tcp	filtered	finger
82/tcp	filtered	xfer
83/tcp	filtered	mit-ml-dev
87/tcp	filtered	priv-term-1
88/tcp	filtered	kerberos-sec
89/tcp	filtered	su-mit-tg
90/tcp	filtered	dnsix
92/tcp	filtered	npp
95/tcp	filtered	supdup
97/tcp	filtered	swift-rvf
99/tcp	filtered	metagram
106/tcp	filtered	pop3pw
108/tcp	filtered	snagas
109/tcp	filtered	pop-2
112/tcp	filtered	mcidas
115/tcp	filtered	sftp
117/tcp	filtered	uucp-path
118/tcp	filtered	sqlserv
119/tcp	filtered	nntp
120/tcp	filtered	cfdpkt
124/tcp	filtered	ansatrader
128/tcp	filtered	gss-xlicen
133/tcp	filtered	statsrv
135/tcp	filtered	loc-srv
136/tcp	filtered	profile
139/tcp	filtered	netbios-ssn
144/tcp	filtered	news
147/tcp	filtered	iso-ip
150/tcp	filtered	sql-net
151/tcp	filtered	hems
155/tcp	filtered	netsc-dev
160/tcp	filtered	sgmp-traps
162/tcp	filtered	snmptrap
169/tcp	filtered	send
172/tcp	filtered	cl-1
174/tcp	filtered	mailq
176/tcp	filtered	genrad-mux
177/tcp	filtered	xdmcp
185/tcp	filtered	remote-kis
189/tcp	filtered	qft
192/tcp	filtered	osu-nms
195/tcp	filtered	dn6-nlm-aud
202/tcp	filtered	at-nbp
204/tcp	filtered	at-echo
206/tcp	filtered	at-zis
217/tcp	filtered	dbase
218/tcp	filtered	mpp
220/tcp	filtered	imap3
222/tcp	filtered	rsh-spx
224/tcp	filtered	unknown
227/tcp	filtered	unknown
232/tcp	filtered	unknown
233/tcp	filtered	unknown
236/tcp	filtered	unknown
239/tcp	filtered	unknown
242/tcp	filtered	direct

244/tcp	filtered	dayna
246/tcp	filtered	dsp3270
247/tcp	filtered	subntbcst_tftp
254/tcp	filtered	unknown
255/tcp	filtered	unknown
258/tcp	filtered	Fwl-mc-gui
262/tcp	filtered	arcisdms
266/tcp	filtered	unknown
267/tcp	filtered	unknown
268/tcp	filtered	unknown
274/tcp	filtered	unknown
278/tcp	filtered	unknown
279/tcp	filtered	unknown
280/tcp	filtered	http-mgmt
282/tcp	filtered	cableport-ax
283/tcp	filtered	unknown
284/tcp	filtered	unknown
285/tcp	filtered	unknown
294/tcp	filtered	unknown
301/tcp	filtered	unknown
302/tcp	filtered	unknown
304/tcp	filtered	unknown
305/tcp	filtered	unknown
306/tcp	filtered	unknown
313/tcp	filtered	magenta-logic
314/tcp	filtered	opalis-robot
316/tcp	filtered	decauth
318/tcp	filtered	unknown
320/tcp	filtered	unknown
323/tcp	filtered	unknown
324/tcp	filtered	unknown
331/tcp	filtered	unknown
334/tcp	filtered	unknown
338/tcp	filtered	unknown
344/tcp	filtered	pdap
346/tcp	filtered	zserv
354/tcp	filtered	bh611
355/tcp	filtered	datex-asn
359/tcp	filtered	tenebris_nts
360/tcp	filtered	scoi2odialog
361/tcp	filtered	semantix
364/tcp	filtered	aurora-cmgr
371/tcp	filtered	clearcase
372/tcp	filtered	ulistserv
374/tcp	filtered	legent-2
375/tcp	filtered	hassle
379/tcp	filtered	is99c
380/tcp	filtered	is99s
383/tcp	filtered	hp-alarm-mgr
384/tcp	filtered	arns
387/tcp	filtered	aurp
391/tcp	filtered	synotics-relay
396/tcp	filtered	netware-ip
403/tcp	filtered	decap
405/tcp	filtered	ncld
415/tcp	filtered	bnet
419/tcp	filtered	ariell

422/tcp	filtered	ariel3
425/tcp	filtered	icad-el
427/tcp	filtered	svrloc
428/tcp	filtered	ocs_cmu
429/tcp	filtered	ocs_amu
434/tcp	filtered	mobileip-agent
435/tcp	filtered	mobilip-mn
436/tcp	filtered	dna-cml
442/tcp	filtered	cvc_hostd
444/tcp	filtered	snpp
451/tcp	filtered	sfs-smp-net
453/tcp	filtered	creativeserver
462/tcp	filtered	datasurfsrvsec
466/tcp	filtered	digital-vrc
471/tcp	filtered	mondex
472/tcp	filtered	ljk-login
473/tcp	filtered	hybrid-pop
474/tcp	filtered	tn-tl-w1
475/tcp	filtered	tcpnethaspsrv
477/tcp	filtered	ss7ns
479/tcp	filtered	iafserver
484/tcp	filtered	integra-sme
486/tcp	filtered	sstats
488/tcp	filtered	gss-http
489/tcp	filtered	nest-protocol
490/tcp	filtered	micom-pfs
492/tcp	filtered	ticf-1
495/tcp	filtered	intecourier
499/tcp	filtered	iso-ill
500/tcp	filtered	isakmp
501/tcp	filtered	stmf
504/tcp	filtered	citadel
505/tcp	filtered	mailbox-lm
507/tcp	filtered	crs
509/tcp	filtered	snare
510/tcp	filtered	fcp
520/tcp	filtered	efs
521/tcp	filtered	ripng
522/tcp	filtered	ulp
523/tcp	filtered	ibm-db2
528/tcp	filtered	custix
534/tcp	filtered	mm-admin
539/tcp	filtered	apertus-ldp
541/tcp	filtered	uucp-rlogin
545/tcp	filtered	ekshell
549/tcp	filtered	idfp
558/tcp	filtered	sdnskmp
560/tcp	filtered	rmonitor
563/tcp	filtered	snews
569/tcp	filtered	ms-rome
570/tcp	filtered	meter
580/tcp	filtered	sntp-heartbeat
581/tcp	filtered	bdp
582/tcp	filtered	scc-security
583/tcp	filtered	philips-vc
585/tcp	filtered	imap4-ssl
587/tcp	filtered	submission

592/tcp	filtered	eudora-set
593/tcp	filtered	http-rpc-epmap
594/tcp	filtered	tpip
599/tcp	filtered	acp
601/tcp	filtered	unknown
603/tcp	filtered	unknown
606/tcp	filtered	urm
607/tcp	filtered	nqs
608/tcp	filtered	sift-uft
609/tcp	filtered	npmp-trap
614/tcp	filtered	unknown
617/tcp	filtered	sco-dtmgr
622/tcp	filtered	unknown
623/tcp	filtered	unknown
624/tcp	filtered	unknown
630/tcp	filtered	unknown
631/tcp	filtered	ipp
632/tcp	filtered	unknown
633/tcp	filtered	unknown
635/tcp	filtered	unknown
642/tcp	filtered	unknown
643/tcp	filtered	unknown
652/tcp	filtered	unknown
653/tcp	filtered	unknown
657/tcp	filtered	unknown
661/tcp	filtered	unknown
662/tcp	filtered	unknown
665/tcp	filtered	unknown
667/tcp	filtered	unknown
668/tcp	filtered	unknown
671/tcp	filtered	unknown
673/tcp	filtered	unknown
674/tcp	filtered	acap
677/tcp	filtered	unknown
686/tcp	filtered	unknown
687/tcp	filtered	unknown
691/tcp	filtered	resvc
692/tcp	filtered	unknown
695/tcp	filtered	unknown
697/tcp	filtered	unknown
698/tcp	filtered	unknown
700/tcp	filtered	unknown
706/tcp	filtered	silc
710/tcp	filtered	unknown
711/tcp	filtered	unknown
712/tcp	filtered	unknown
713/tcp	filtered	unknown
717/tcp	filtered	unknown
720/tcp	filtered	unknown
721/tcp	filtered	unknown
722/tcp	filtered	unknown
723/tcp	filtered	unknown
728/tcp	filtered	unknown
734/tcp	filtered	unknown
738/tcp	filtered	unknown
740/tcp	filtered	netcp
746/tcp	filtered	unknown

751/tcp	filtered	kerberos_master
753/tcp	filtered	rrh
754/tcp	filtered	krb_prop
755/tcp	filtered	unknown
756/tcp	filtered	unknown
759/tcp	filtered	con
761/tcp	filtered	kpasswd
762/tcp	filtered	quotad
770/tcp	filtered	cadlock
772/tcp	filtered	cycleserv2
773/tcp	filtered	submit
774/tcp	filtered	rpaswd
782/tcp	filtered	hp-managed-node
783/tcp	filtered	hp-alarm-mgr
786/tcp	filtered	concert
787/tcp	filtered	unknown
791/tcp	filtered	unknown
798/tcp	filtered	unknown
800/tcp	filtered	mdbd_daemon
803/tcp	filtered	unknown
805/tcp	filtered	unknown
806/tcp	filtered	unknown
808/tcp	filtered	unknown
815/tcp	filtered	unknown
816/tcp	filtered	unknown
817/tcp	filtered	unknown
820/tcp	filtered	unknown
822/tcp	filtered	unknown
827/tcp	filtered	unknown
834/tcp	filtered	unknown
837/tcp	filtered	unknown
838/tcp	filtered	unknown
842/tcp	filtered	unknown
844/tcp	filtered	unknown
849/tcp	filtered	unknown
854/tcp	filtered	unknown
856/tcp	filtered	unknown
860/tcp	filtered	unknown
861/tcp	filtered	unknown
863/tcp	filtered	unknown
867/tcp	filtered	unknown
868/tcp	filtered	unknown
872/tcp	filtered	unknown
878/tcp	filtered	unknown
882/tcp	filtered	unknown
883/tcp	filtered	unknown
889/tcp	filtered	unknown
890/tcp	filtered	unknown
891/tcp	filtered	unknown
892/tcp	filtered	unknown
893/tcp	filtered	unknown
895/tcp	filtered	unknown
896/tcp	filtered	unknown
898/tcp	open	sun-manageconsole
903/tcp	filtered	unknown
905/tcp	filtered	unknown
908/tcp	filtered	unknown

916/tcp	filtered	unknown
918/tcp	filtered	unknown
920/tcp	filtered	unknown
922/tcp	filtered	unknown
923/tcp	filtered	unknown
926/tcp	filtered	unknown
932/tcp	filtered	unknown
933/tcp	filtered	unknown
940/tcp	filtered	unknown
942/tcp	filtered	unknown
943/tcp	filtered	unknown
951/tcp	filtered	unknown
953/tcp	filtered	rndc
955/tcp	filtered	unknown
959/tcp	filtered	unknown
960/tcp	filtered	unknown
963/tcp	filtered	unknown
968/tcp	filtered	unknown
975/tcp	filtered	securenetpro-sensor
976/tcp	filtered	unknown
983/tcp	filtered	unknown
994/tcp	filtered	ircs
995/tcp	filtered	pop3s
996/tcp	filtered	xtreelic
1006/tcp	filtered	unknown
1014/tcp	filtered	unknown
1016/tcp	filtered	unknown
1021/tcp	filtered	unknown
1022/tcp	filtered	unknown
1024/tcp	filtered	kdm
1025/tcp	filtered	NFS-or-IIS
1026/tcp	filtered	LSA-or-nterm
1029/tcp	filtered	ms-lsa
1030/tcp	filtered	iad1
1031/tcp	filtered	iad2
1032/tcp	filtered	iad3
1033/tcp	filtered	netinfo
1050/tcp	filtered	java-or-OTGfileshare
1084/tcp	filtered	ansoft-lm-2
1109/tcp	filtered	kpop
1110/tcp	filtered	nfsd-status
1112/tcp	filtered	mysql
1127/tcp	filtered	supfiledbg
1212/tcp	filtered	lupa
1337/tcp	filtered	waste
1351/tcp	filtered	equationbuilder
1361/tcp	filtered	linx
1364/tcp	filtered	ndm-server
1369/tcp	filtered	gv-us
1372/tcp	filtered	fc-ser
1373/tcp	filtered	chromagrafx
1374/tcp	filtered	molly
1376/tcp	filtered	ibm-pps
1377/tcp	filtered	cichlid
1378/tcp	filtered	elan
1383/tcp	filtered	gwha
1385/tcp	filtered	atex_elmd

1388/tcp	filtered	objective-dbc
1393/tcp	filtered	iclpv-nls
1396/tcp	filtered	dvl-activemail
1398/tcp	filtered	video-activmail
1399/tcp	filtered	cadkey-licman
1400/tcp	filtered	cadkey-tablet
1401/tcp	filtered	goldleaf-licman
1404/tcp	filtered	igi-lm
1412/tcp	filtered	innosys
1424/tcp	filtered	hybrid
1425/tcp	filtered	zion-lm
1427/tcp	filtered	mload
1428/tcp	filtered	informatik-lm
1429/tcp	filtered	nms
1430/tcp	filtered	tpdu
1431/tcp	filtered	rgtp
1432/tcp	filtered	blueberry-lm
1433/tcp	filtered	ms-sql-s
1437/tcp	filtered	tabula
1438/tcp	filtered	eicon-server
1448/tcp	filtered	oc-lm
1456/tcp	filtered	dca
1458/tcp	filtered	nrcabq-lm
1461/tcp	filtered	ibm_wrless_lan
1462/tcp	filtered	world-lm
1463/tcp	filtered	nucleus
1464/tcp	filtered	msl_lmd
1466/tcp	filtered	oceansoft-lm
1472/tcp	filtered	csdm
1473/tcp	filtered	openmath
1476/tcp	filtered	clvm-cfg
1478/tcp	filtered	ms-sna-base
1479/tcp	filtered	dberegister
1483/tcp	filtered	afs
1486/tcp	filtered	nms_topo_serv
1490/tcp	filtered	insitu-conf
1493/tcp	filtered	netmap_lm
1496/tcp	filtered	liberty-lm
1500/tcp	filtered	vlsi-lm
1501/tcp	filtered	sas-3
1503/tcp	filtered	imtc-mcs
1504/tcp	filtered	evb-elm
1506/tcp	filtered	utcd
1507/tcp	filtered	symplex
1511/tcp	filtered	3l-l1
1515/tcp	filtered	ifor-protocol
1520/tcp	filtered	atm-zip-office
1523/tcp	filtered	cichild-lm
1526/tcp	filtered	pdap-np
1529/tcp	filtered	support
1535/tcp	filtered	ampr-info
1538/tcp	filtered	3ds-lm
1545/tcp	filtered	vistium-share
1548/tcp	filtered	axon-lm
1552/tcp	filtered	pciarray
1600/tcp	filtered	issd
1652/tcp	filtered	xnmp

1663/tcp	filtered	netview-aix-3
1665/tcp	filtered	netview-aix-5
1671/tcp	filtered	netview-aix-11
1680/tcp	filtered	CarbonCopy
1720/tcp	filtered	H.323/Q.931
1827/tcp	filtered	pcm
1900/tcp	filtered	UPnP
1984/tcp	filtered	bigbrother
1989/tcp	filtered	tr-rsrb-p3
1991/tcp	filtered	stun-p2
1992/tcp	filtered	stun-p3
1994/tcp	filtered	stun-port
1999/tcp	filtered	tcp-id-port
2002/tcp	filtered	globe
2003/tcp	filtered	cfingerd
2007/tcp	filtered	dectalk
2008/tcp	filtered	conf
2009/tcp	filtered	news
2011/tcp	filtered	raid-cc
2013/tcp	filtered	raid-am
2016/tcp	filtered	bootserver
2017/tcp	filtered	cypress-stat
2021/tcp	filtered	servexec
2023/tcp	filtered	xinuexpansion3
2027/tcp	filtered	shadowserver
2028/tcp	filtered	submitserver
2032/tcp	filtered	blackboard
2038/tcp	filtered	objectmanager
2040/tcp	filtered	lam
2048/tcp	filtered	dls-monitor
2068/tcp	filtered	advocentkvm
2106/tcp	filtered	ekshell
2201/tcp	filtered	ats
2307/tcp	filtered	pehelp
2401/tcp	filtered	cvspserver
2500/tcp	filtered	rtsserv
2564/tcp	filtered	hp-3000-telnet
2603/tcp	filtered	ripngd
2604/tcp	filtered	ospfd
2605/tcp	filtered	bgpd
2627/tcp	filtered	webster
2638/tcp	filtered	sybase
2784/tcp	filtered	www-dev
2998/tcp	filtered	iss-realsec
3006/tcp	filtered	deslogind
3052/tcp	filtered	PowerChute
3141/tcp	filtered	vmodem
3292/tcp	filtered	meetingmaker
3372/tcp	filtered	msdtc
3455/tcp	filtered	prsvp
3456/tcp	filtered	vat
3457/tcp	filtered	vat-control
3462/tcp	filtered	track
3689/tcp	filtered	rendezvous
3984/tcp	filtered	mapper-nodemgr
3985/tcp	filtered	mapper-mapethd
3986/tcp	filtered	mapper-ws_ethd

3999/tcp	filtered	remoteanything
4000/tcp	filtered	remoteanything
4008/tcp	filtered	netcheque
4045/tcp	filtered	lockd
4132/tcp	filtered	nuts_dem
4144/tcp	filtered	wincim
4321/tcp	filtered	rwhois
4343/tcp	filtered	unicall
4444/tcp	filtered	krb524
4899/tcp	filtered	radmin
5000/tcp	filtered	UPnP
5001/tcp	filtered	complex-link
5003/tcp	filtered	filemaker
5010/tcp	filtered	telepathstart
5011/tcp	filtered	telepathattack
5101/tcp	filtered	admdog
5190/tcp	filtered	aol
5191/tcp	filtered	aol-1
5236/tcp	filtered	padl2sim
5304/tcp	filtered	hacl-local
5308/tcp	filtered	cfengine
5405/tcp	filtered	pcduo
5550/tcp	filtered	sdadmind
5631/tcp	filtered	pcanywheredata
5717/tcp	filtered	prosharenotify
5803/tcp	filtered	vnc-http-3
5901/tcp	filtered	vnc-1
5902/tcp	filtered	vnc-2
6001/tcp	filtered	X11:1
6007/tcp	filtered	X11:7
6009/tcp	filtered	X11:9
6101/tcp	filtered	VeritasBackupExec
6105/tcp	filtered	isdninfo
6110/tcp	filtered	softcm
6143/tcp	filtered	watershed-lm
6144/tcp	filtered	statscil-lm
6146/tcp	filtered	lonewolf-lm
6148/tcp	filtered	ricardo-lm
6699/tcp	filtered	napster
6969/tcp	filtered	acmsoda
7005/tcp	filtered	afs3-volser
7007/tcp	filtered	afs3-bos
7201/tcp	filtered	dlip
7326/tcp	filtered	icb
7597/tcp	filtered	qaz
8000/tcp	filtered	http-alt
8888/tcp	filtered	sun-answerbook
9152/tcp	filtered	ms-sql2000
9876/tcp	filtered	sd
9991/tcp	filtered	issa
9992/tcp	filtered	issc
10000/tcp	filtered	snet-sensor-mgmt
11371/tcp	filtered	pktd
12346/tcp	filtered	NetBus
13701/tcp	filtered	VeritasNetbackup
13708/tcp	filtered	VeritasNetbackup
13713/tcp	filtered	VeritasNetbackup

13717/tcp	filtered	VeritasNetbackup
13718/tcp	filtered	VeritasNetbackup
13721/tcp	filtered	VeritasNetbackup
15126/tcp	filtered	swgps
17007/tcp	filtered	isode-dua
18181/tcp	filtered	opsec_cvp
18187/tcp	filtered	opsec_ela
22370/tcp	filtered	hpnpd
27004/tcp	filtered	flexlm4
27009/tcp	filtered	flexlm9
27665/tcp	filtered	Trinoo_Master
31337/tcp	filtered	Elite
32770/tcp	filtered	sometimes-rpc3
32772/tcp	filtered	sometimes-rpc7
32774/tcp	filtered	sometimes-rpc11
32776/tcp	filtered	sometimes-rpc15
32777/tcp	filtered	sometimes-rpc17
32779/tcp	filtered	sometimes-rpc21
44442/tcp	filtered	coldfusion-auth
54320/tcp	filtered	bo2k
65301/tcp	filtered	pcanywhere

Host host2.foo.com (<IP address censored>) appears to be up ... good.
Initiating SYN Stealth Scan against host2.foo.com (<IP address censored>) at 16:16

Adding open port 111/tcp
Adding open port 22/tcp
Adding open port 13722/tcp
Adding open port 53/tcp
Adding open port 32772/tcp
Adding open port 32771/tcp
Adding open port 4045/tcp
Adding open port 13783/tcp
Adding open port 13782/tcp
Adding open port 32776/tcp

The SYN Stealth Scan took 2 seconds to scan 1644 ports.

Interesting ports on host2.foo.com (<IP address censored>):

(The 1634 ports scanned but not shown below are in state: closed)

Port	State	Service
22/tcp	open	ssh
53/tcp	open	domain
111/tcp	open	sunrpc
4045/tcp	open	lockd
13722/tcp	open	VeritasNetbackup
13782/tcp	open	VeritasNetbackup
13783/tcp	open	VeritasNetbackup
32771/tcp	open	sometimes-rpc5
32772/tcp	open	sometimes-rpc7
32776/tcp	open	sometimes-rpc15

Host host3.foo.com (<IP address censored>) appears to be up ... good.
Initiating SYN Stealth Scan against host3.foo.com (<IP address censored>) at 16:16

Adding open port 111/tcp
Adding open port 22/tcp
Adding open port 13722/tcp
Adding open port 53/tcp

Adding open port 32772/tcp

Adding open port 32771/tcp

Adding open port 4045/tcp

Adding open port 13783/tcp

Adding open port 13782/tcp

Adding open port 32773/tcp

The SYN Stealth Scan took 2 seconds to scan 1644 ports.

Interesting ports on host3.foo.com (<IP address censored>):

(The 1634 ports scanned but not shown below are in state: closed)

Port	State	Service
22/tcp	open	ssh
53/tcp	open	domain
111/tcp	open	sunrpc
4045/tcp	open	lockd
13722/tcp	open	VeritasNetbackup
13782/tcp	open	VeritasNetbackup
13783/tcp	open	VeritasNetbackup
32771/tcp	open	sometimes-rpc5
32772/tcp	open	sometimes-rpc7
32773/tcp	open	sometimes-rpc9

Host host4.foo.com (<IP address censored>) appears to be up ... good.

Initiating SYN Stealth Scan against host4.foo.com (<IP address censored>) at 16:16

Adding open port 111/tcp

Adding open port 22/tcp

Adding open port 927/tcp

Adding open port 820/tcp

Adding open port 800/tcp

The SYN Stealth Scan took 3 seconds to scan 1644 ports.

Interesting ports on host5.foo.com (<IP address censored>):

(The 1639 ports scanned but not shown below are in state: closed)

Port	State	Service
22/tcp	open	ssh
111/tcp	open	sunrpc
800/tcp	open	mdbs_daemon
820/tcp	open	unknown
927/tcp	open	unknown

Host host5.foo.com (<IP address censored>) appears to be up ... good.

Initiating SYN Stealth Scan against host5.foo.com (<IP address censored>) at 16:16

Adding open port 111/tcp

Adding open port 1521/tcp

Adding open port 22/tcp

Adding open port 13722/tcp

Adding open port 53/tcp

Adding open port 32772/tcp

Adding open port 80/tcp

Adding open port 32771/tcp

Adding open port 4045/tcp

Adding open port 13783/tcp

Adding open port 13782/tcp

The SYN Stealth Scan took 3 seconds to scan 1644 ports.

Interesting ports on host5.foo.com (<IP address censored>):

(The 1633 ports scanned but not shown below are in state: closed)

Port	State	Service
------	-------	---------

22/tcp	open	ssh
53/tcp	open	domain
80/tcp	open	http
111/tcp	open	sunrpc
1521/tcp	open	oracle
4045/tcp	open	lockd
13722/tcp	open	VeritasNetbackup
13782/tcp	open	VeritasNetbackup
13783/tcp	open	VeritasNetbackup
32771/tcp	open	sometimes-rpc5
32772/tcp	open	sometimes-rpc7

Nmap run completed -- 5 IP addresses (5 hosts up) scanned in 44.387 seconds

```
# nmap -v -g53 -P0 -sU -T Aggressive -iL dmz-hosts.txt -oN trust-to-dmz-udp.txt
```

Reading target specifications from FILE: dmz-hosts.txt

Starting nmap 3.30 (<http://www.insecure.org/nmap/>) at 2003-07-28 16:17 PDT
Host host1.foo.com (<IP address censored>) appears to be up ... good.
Initiating UDP Scan against host1.foo.com (<IP address censored>) at 16:17
The UDP Scan took 147 seconds to scan 1471 ports.
All 1471 scanned ports on host1.foo.com (<IP address censored>) are: closed

Host host2.foo.com (<IP address censored>) appears to be up ... good.
Initiating UDP Scan against host2.foo.com (<IP address censored>) at 16:19
The UDP Scan took 821 seconds to scan 1471 ports.

Adding open port 743/udp
Adding open port 4045/udp
Adding open port 111/udp
Adding open port 1019/udp
Adding open port 1021/udp
Adding open port 53/udp
Adding open port 514/udp
Adding open port 1020/udp
Adding open port 123/udp
Adding open port 1018/udp
Adding open port 161/udp

Interesting ports on host2.foo.com (<IP address censored>):
(The 1460 ports scanned but not shown below are in state: closed)

Port	State	Service
53/udp	open	domain
111/udp	open	sunrpc
123/udp	open	ntp
161/udp	open	snmp
514/udp	open	syslog
743/udp	open	unknown
1018/udp	open	unknown
1019/udp	open	unknown
1020/udp	open	unknown
1021/udp	open	unknown
4045/udp	open	lockd

Host host3.foo.com (<IP address censored>) appears to be up ... good.
Initiating UDP Scan against host3.foo.com (<IP address censored>) at 16:33
The UDP Scan took 824 seconds to scan 1471 ports.
Adding open port 765/udp

Adding open port 161/udp
Adding open port 123/udp
Adding open port 32776/udp
Adding open port 32778/udp
Adding open port 32777/udp
Adding open port 514/udp
Adding open port 53/udp
Adding open port 111/udp
Adding open port 4045/udp
Interesting ports on host3.foo.com (<IP address censored>):
(The 1461 ports scanned but not shown below are in state: closed)

Port	State	Service
53/udp	open	domain
111/udp	open	sunrpc
123/udp	open	ntp
161/udp	open	snmp
514/udp	open	syslog
765/udp	open	webster
4045/udp	open	lockd
32776/udp	open	sometimes-rpc16
32777/udp	open	sometimes-rpc18
32778/udp	open	sometimes-rpc20

Host host4.foo.com (<IP address censored>) appears to be up ... good.
Initiating UDP Scan against host4.foo.com (<IP address censored>) at 16:47
The UDP Scan took 1456 seconds to scan 1471 ports.
Adding open port 1022/udp
Adding open port 797/udp
Adding open port 607/udp
Adding open port 800/udp
Adding open port 1023/udp
Adding open port 514/udp
Adding open port 733/udp
Adding open port 928/udp
Adding open port 817/udp
Adding open port 799/udp
Adding open port 111/udp
Adding open port 796/udp

Interesting ports on host5.foo.com (<IP address censored>):
(The 1459 ports scanned but not shown below are in state: closed)

Port	State	Service
111/udp	open	sunrpc
514/udp	open	syslog
607/udp	open	nqs
733/udp	open	unknown
796/udp	open	unknown
797/udp	open	unknown
799/udp	open	unknown
800/udp	open	mdbs_daemon
817/udp	open	unknown
928/udp	open	unknown
1022/udp	open	unknown
1023/udp	open	unknown

Host host5.foo.com (<IP address censored>) appears to be up ... good.
Initiating UDP Scan against host5.foo.com (<IP address censored>) at 17:11
The UDP Scan took 148 seconds to scan 1471 ports.

```
Adding open port 161/udp
Adding open port 32780/udp
Adding open port 1022/udp
Adding open port 123/udp
Adding open port 1023/udp
Adding open port 32776/udp
Adding open port 514/udp
Adding open port 53/udp
Adding open port 32775/udp
Adding open port 1021/udp
Adding open port 111/udp
Adding open port 4045/udp
Adding open port 32774/udp
Interesting ports on host5.foo.com (<IP address censored>):
(The 1458 ports scanned but not shown below are in state: closed)
Port      State      Service
53/udp    open       domain
111/udp   open       sunrpc
123/udp   open       ntp
161/udp   open       snmp
514/udp   open       syslog
1021/udp  open       unknown
1022/udp  open       unknown
1023/udp  open       unknown
4045/udp  open       lockd
32774/udp open       sometimes-rpc12
32775/udp open       sometimes-rpc14
32776/udp open       sometimes-rpc16
32780/udp open       sometimes-rpc24
```

Nmap run completed -- 5 IP addresses (5 hosts up) scanned in 3396.284 seconds

Results of the Nmap Scan Recorded with the Sniffer Snort

```
# clear; tail -f fast.alert
07/28/03-23:11:28.029164 {ICMP} <host14.foo.com IP address censored> ->
<host1.foo.com IP address censored>
[**] [1:469:1] ICMP PING NMAP [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://www.whitehats.com/info/IDS162]
-----
07/28/03-23:11:28.029235 {ICMP} <host14.foo.com IP address censored> ->
<host2.foo.com IP address censored>
[**] [1:469:1] ICMP PING NMAP [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://www.whitehats.com/info/IDS162]
-----
07/28/03-23:11:28.029288 {ICMP} <host14.foo.com IP address censored> ->
<host3.foo.com IP address censored>
[**] [1:469:1] ICMP PING NMAP [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://www.whitehats.com/info/IDS162]
-----
07/28/03-23:11:28.029341 {ICMP} <host14.foo.com IP address censored> ->
<host5.foo.com IP address censored>
[**] [1:469:1] ICMP PING NMAP [**]
```

```
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://www.whitehats.com/info/IDS162]
-----
07/28/03-23:11:28.029392 {ICMP} <host14.foo.com IP address censored> ->
<host4.foo.com IP address censored>
[**] [1:469:1] ICMP PING NMAP [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://www.whitehats.com/info/IDS162]
-----
07/28/03-23:12:26.564249 {TCP} <host14.foo.com IP address censored>:22 ->
<host1.foo.com IP address censored>:705
[**] [1:1421:2] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:12:26.971569 {TCP} <host14.foo.com IP address censored>:22 ->
<host1.foo.com IP address censored>:705
[**] [1:1421:2] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:12:27.291976 {TCP} <host14.foo.com IP address censored>:22 ->
<host1.foo.com IP address censored>:705
[**] [1:1421:2] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:12:38.820943 {TCP} <host14.foo.com IP address censored>:22 ->
<host1.foo.com IP address censored>:161
[**] [1:1418:2] SNMP request tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:12:39.140195 {TCP} <host14.foo.com IP address censored>:22 ->
<host1.foo.com IP address censored>:161
[**] [1:1418:2] SNMP request tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:12:49.059590 {TCP} <host14.foo.com IP address censored>:22 ->
<host1.foo.com IP address censored>:162
[**] [1:1420:2] SNMP trap tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:12:49.379395 {TCP} <host14.foo.com IP address censored>:22 ->
<host1.foo.com IP address censored>:162
[**] [1:1420:2] SNMP trap tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
```

```
-----
07/28/03-23:12:52.932743 {TCP} <host14.foo.com IP address censored>:22 ->
<host2.foo.com IP address censored>:705
[**] [1:1421:2] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:12:54.630246 {TCP} <host14.foo.com IP address censored>:22 ->
<host2.foo.com IP address censored>:161
[**] [1:1418:2] SNMP request tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:12:56.940293 {TCP} <host14.foo.com IP address censored>:22 ->
<host2.foo.com IP address censored>:162
[**] [1:1420:2] SNMP trap tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:12:57.941317 {TCP} <host14.foo.com IP address censored>:22 ->
<host3.foo.com IP address censored>:705
[**] [1:1421:2] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:12:59.958001 {TCP} <host14.foo.com IP address censored>:22 ->
<host3.foo.com IP address censored>:161
[**] [1:1418:2] SNMP request tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:13:01.939996 {TCP} <host14.foo.com IP address censored>:22 ->
<host3.foo.com IP address censored>:162
[**] [1:1420:2] SNMP trap tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:13:02.940395 {TCP} <host14.foo.com IP address censored>:22 ->
<host5.foo.com IP address censored>:705
[**] [1:1421:2] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:13:04.629135 {TCP} <host14.foo.com IP address censored>:22 ->
<host5.foo.com IP address censored>:161
[**] [1:1418:2] SNMP request tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
```

```
07/28/03-23:13:06.939169 {TCP} <host14.foo.com IP address censored>:22 ->
<host5.foo.com IP address censored>:162
[**] [1:1420:2] SNMP trap tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:13:07.939544 {TCP} <host14.foo.com IP address censored>:22 ->
<host4.foo.com IP address censored>:705
[**] [1:1421:2] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:13:09.948585 {TCP} <host14.foo.com IP address censored>:22 ->
<host4.foo.com IP address censored>:161
[**] [1:1418:2] SNMP request tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:13:12.258474 {TCP} <host14.foo.com IP address censored>:22 ->
<host4.foo.com IP address censored>:162
[**] [1:1420:2] SNMP trap tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:15:35.443196 {TCP} <host14.foo.com IP address censored>:22 ->
<host1.foo.com IP address censored>:705
[**] [1:1421:2] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:15:36.414854 {TCP} <host14.foo.com IP address censored>:22 ->
<host1.foo.com IP address censored>:3128
[**] [1:618:4] SCAN Squid Proxy attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
-----
07/28/03-23:15:36.731527 {TCP} <host14.foo.com IP address censored>:22 ->
<host1.foo.com IP address censored>:3128
[**] [1:618:4] SCAN Squid Proxy attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
-----
07/28/03-23:15:49.413463 {TCP} <host14.foo.com IP address censored>:22 ->
<host1.foo.com IP address censored>:162
[**] [1:1420:2] SNMP trap tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:15:49.729944 {TCP} <host14.foo.com IP address censored>:22 ->
<host1.foo.com IP address censored>:162
[**] [1:1420:2] SNMP trap tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
```



```
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:15:50.049933 {TCP} <host14.foo.com IP address censored>:22 ->
<host1.foo.com IP address censored>:162
[**] [1:1420:2] SNMP trap tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:16:02.210363 {TCP} <host14.foo.com IP address censored>:22 ->
<host1.foo.com IP address censored>:8080
[**] [1:620:3] SCAN Proxy \ (8080\ ) attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
-----
07/28/03-23:16:05.728365 {TCP} <host14.foo.com IP address censored>:22 ->
<host1.foo.com IP address censored>:1080
[**] [1:615:4] SCAN SOCKS Proxy attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://help.undernet.org/proxyscan/]
-----
07/28/03-23:16:06.048084 {TCP} <host14.foo.com IP address censored>:22 ->
<host1.foo.com IP address censored>:1080
[**] [1:615:4] SCAN SOCKS Proxy attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://help.undernet.org/proxyscan/]
-----
07/28/03-23:16:08.609797 {TCP} <host14.foo.com IP address censored>:22 ->
<host1.foo.com IP address censored>:161
[**] [1:1418:2] SNMP request tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:16:09.915404 {TCP} <host14.foo.com IP address censored>:22 ->
<host2.foo.com IP address censored>:705
[**] [1:1421:2] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:16:09.928745 {TCP} <host14.foo.com IP address censored>:22 ->
<host2.foo.com IP address censored>:3128
[**] [1:618:4] SCAN Squid Proxy attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
-----
07/28/03-23:16:10.651215 {TCP} <host14.foo.com IP address censored>:22 ->
<host2.foo.com IP address censored>:162
[**] [1:1420:2] SNMP trap tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:16:11.693424 {TCP} <host14.foo.com IP address censored>:22 ->
<host2.foo.com IP address censored>:8080
[**] [1:620:3] SCAN Proxy \ (8080\ ) attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
-----
```

```
07/28/03-23:16:12.036551 {TCP} <host14.foo.com IP address censored>:22 ->
<host2.foo.com IP address censored>:1080
[**] [1:615:4] SCAN SOCKS Proxy attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://help.undernet.org/proxyscan/]
-----
07/28/03-23:16:12.058734 {TCP} <host14.foo.com IP address censored>:22 ->
<host2.foo.com IP address censored>:161
[**] [1:1418:2] SNMP request tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:16:12.074729 {TCP} <host14.foo.com IP address censored>:22 ->
<host3.foo.com IP address censored>:705
[**] [1:1421:2] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:16:12.084489 {TCP} <host14.foo.com IP address censored>:22 ->
<host3.foo.com IP address censored>:3128
[**] [1:618:4] SCAN Squid Proxy attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
-----
07/28/03-23:16:12.803403 {TCP} <host14.foo.com IP address censored>:22 ->
<host3.foo.com IP address censored>:162
[**] [1:1420:2] SNMP trap tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:16:13.843441 {TCP} <host14.foo.com IP address censored>:22 ->
<host3.foo.com IP address censored>:8080
[**] [1:620:3] SCAN Proxy \ (8080\ ) attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
-----
07/28/03-23:16:14.497766 {TCP} <host14.foo.com IP address censored>:22 ->
<host3.foo.com IP address censored>:1080
[**] [1:615:4] SCAN SOCKS Proxy attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://help.undernet.org/proxyscan/]
-----
07/28/03-23:16:14.518513 {TCP} <host14.foo.com IP address censored>:22 ->
<host3.foo.com IP address censored>:161
[**] [1:1418:2] SNMP request tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:16:14.539966 {TCP} <host14.foo.com IP address censored>:22 ->
<host5.foo.com IP address censored>:705
[**] [1:1421:2] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
```

```
07/28/03-23:16:14.550344 {TCP} <host14.foo.com IP address censored>:22 ->
<host5.foo.com IP address censored>:3128
[**] [1:618:4] SCAN Squid Proxy attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
-----
07/28/03-23:16:15.271454 {TCP} <host14.foo.com IP address censored>:22 ->
<host5.foo.com IP address censored>:162
[**] [1:1420:2] SNMP trap tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:16:16.628518 {TCP} <host14.foo.com IP address censored>:22 ->
<host5.foo.com IP address censored>:8080
[**] [1:620:3] SCAN Proxy \ (8080\ ) attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
-----
07/28/03-23:16:16.651389 {TCP} <host14.foo.com IP address censored>:22 ->
<host5.foo.com IP address censored>:1080
[**] [1:615:4] SCAN SOCKS Proxy attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://help.undernet.org/proxyscan/]
-----
07/28/03-23:16:16.994190 {TCP} <host14.foo.com IP address censored>:22 ->
<host5.foo.com IP address censored>:161
[**] [1:1418:2] SNMP request tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:16:17.010825 {TCP} <host14.foo.com IP address censored>:22 ->
<host4.foo.com IP address censored>:705
[**] [1:1421:2] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:16:17.020663 {TCP} <host14.foo.com IP address censored>:22 ->
<host4.foo.com IP address censored>:3128
[**] [1:618:4] SCAN Squid Proxy attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
-----
07/28/03-23:16:17.741299 {TCP} <host14.foo.com IP address censored>:22 ->
<host4.foo.com IP address censored>:162
[**] [1:1420:2] SNMP trap tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
07/28/03-23:16:19.098429 {TCP} <host14.foo.com IP address censored>:22 ->
<host4.foo.com IP address censored>:8080
[**] [1:620:3] SCAN Proxy \ (8080\ ) attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
-----
07/28/03-23:16:19.120798 {TCP} <host14.foo.com IP address censored>:22 ->
<host4.foo.com IP address censored>:1080
[**] [1:615:4] SCAN SOCKS Proxy attempt [**]
```

```
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://help.undernet.org/proxyscan/]
-----
07/28/03-23:16:19.776737 {TCP} <host14.foo.com IP address censored>:22 ->
<host4.foo.com IP address censored>:161
[**] [1:1418:2] SNMP request tcp [**]
[Classification: Attempted Information Leak] [Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
-----
#
```

Assessment

The firewall clearly controls application and infrastructure management flows from the trusted interface to the DMZ interface. It denies by default any services not explicitly authorized. Moreover, the network-based intrusion detection system did not detect any network traffic on unauthorized ports. Therefore, the firewall is compliant with item C4 regarding trusted to DMZ traffic.

Overall Assessment for Checklist Item C4

Since clearly all ports have been disabled by default in both directions and only authorized ports have been opened, the firewall is compliant with checklist item C4.

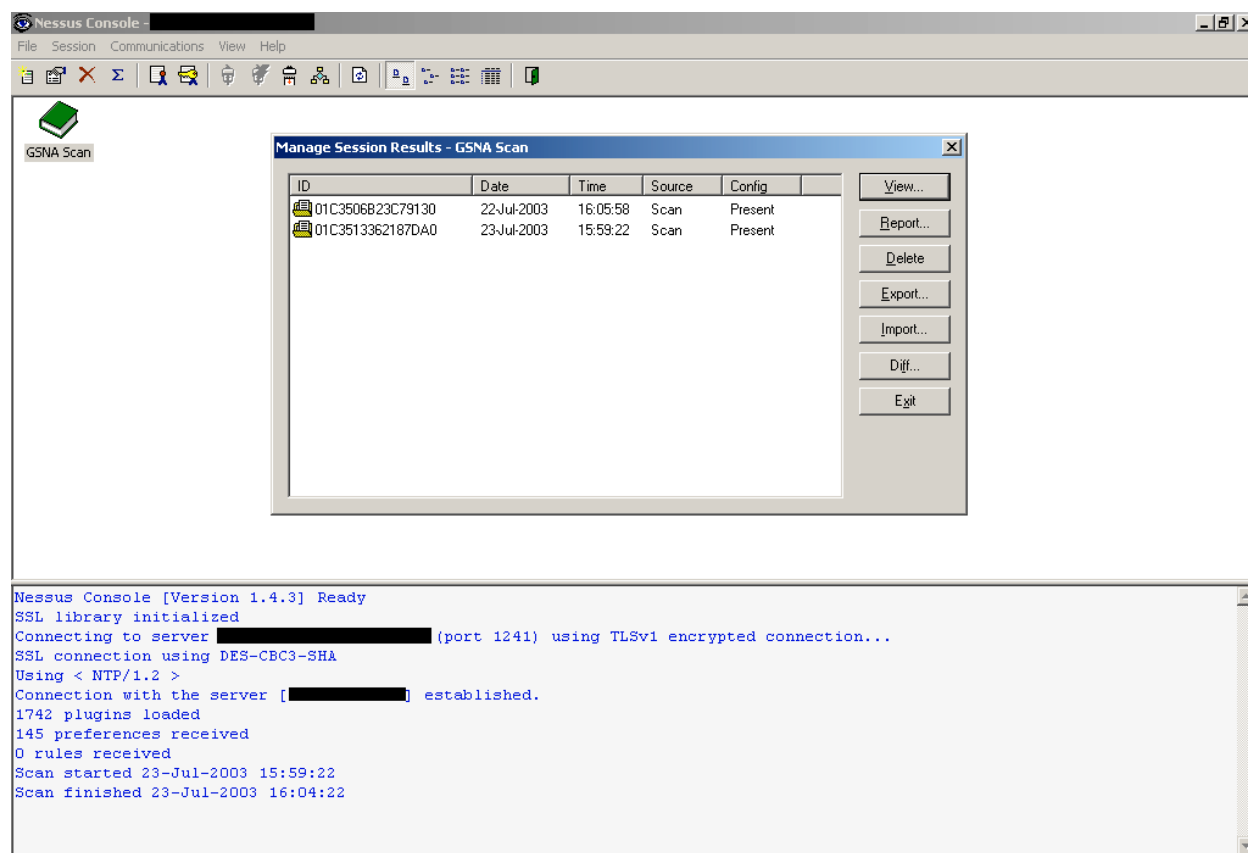
Checklist Item C9: FAIL

Objective: No vulnerable services should be accessible through the perimeter's countermeasures.

In order to determine if vulnerable services were accessible through the perimeter's countermeasures, I performed a vulnerability assessment using Nessus. I deliberately launched the scan from outside the firewall, since I wanted to identify vulnerable services *accessible through the perimeter's countermeasures*. Unfortunately, it is difficult to fully capture the Nessus configuration through a series of screen snapshots. Instead, I have provided a snapshot of the Nessus Console window after the scan, followed by a report on the scan results. The report includes a summary of the scan configuration.

Figure 4 shows the Nessus console window after completing the vulnerability scan.

Figure 4 – Nessus Console Window After Scan



Nessus Vulnerability Scan: Configuration and Results

For the Nessus Vulnerability Scan, I enabled the following plug-ins: Backdoors, RPC, NIS, "Gain a shell remotely", "Remote file access", "Gain root remotely," and a handful of individual items from other plugins. Detailed configuration settings are provided below.

NESSUS SECURITY SCAN REPORT

Created 23.07.2003 Sorted by vulnerabilities

Session Name : GSNA Scan
 Start Time : 23.07.2003 15:59:22
 Finish Time : 23.07.2003 16:04:22
 Elapsed Time : 0 day(s) 00:04:59

Plugins used in this scan:

Id	Name
10794	PC Anywhere TCP
11198	BitKeeper remote command execution
10996	JRun Sample Files
10141	MetaInfo servers

11412 IIS : WebDAV Overflow (MS03-007)
10827 SysV /bin/login buffer overflow (telnet)
10727 Buffer overflow in Solaris in.lpd
11691 Desktop Orbiter Server Detection
10640 Kerberos PingPong attack
11356 Mountable NFS shares
10747 3Com Superstack II switch with default password
10221 nsd service
10787 tooltalk format string
10549 BIND vulnerable to ZXFR bug
11077 HTTP Cookie overflow
11114 Canna Overflow
10228 rusersd service
10918 Apache-SSL overflow
11032 Directory Scanner
10213 cmsd service
11645 wsmp3d command execution
10093 GateCrasher
10232 showfhd service
10054 Delegate overflow
11754 List of printers is available through CUPS
10463 vpopmail input validation bug
11418 Sun rpc.cmsd overflow
11028 IIS .HTR overflow
10169 OpenLink web config buffer overflow
10132 Kuang2 the Virus
11339 scp File Create/Overwrite
10229 sadmin service
10677 Apache /server-status accessible
10517 pam_smb / pam_ntdom overflow
11250 Unpassworded backdoor account
11241 Unpassworded EZsetup account
11535 SheerDNS directory traversal
11715 Header overflow against HTTP proxy
11113 Samba Buffer Overflow
10714 Default password router Zyxel
11254 Unpassworded friday account
10274 SyGate Backdoor
11390 rsync array overflow
10238 tfds service
11386 Lotus Domino 6.0 vulnerabilities
10184 Various pop3 overflows
10961 AirConnect Default Password
10235 statd service
11244 Unpassworded OutOfBox account
11585 Sambar Transmits Passwords in PlainText
10883 OpenSSH Channel Code Off by 1
10917 SMB Scope
11054 fakeidentd overflow
11654 ShareMailPro Username Identification
10208 3270 mapper service
10522 LPRng malformed input
11246 Unpassworded lp account
11195 SSH Multiple Vulns
10088 Writeable FTP root
10325 Xtramail pop3 overflow
10680 Test Microsoft IIS Source Fragment Disclosure

10989 Nortel/Bay Networks default password
10322 Xitami Web Server buffer overflow
11121 xtel detection
10802 OpenSSH < 3.0.1
10237 sunlink mapper service
10536 Anaconda remote file retrieval
11058 rusersd output
10234 sprayd service
10217 keyserve service
10146 Tektronix /ncl_items.html
10316 WinSATAN
10024 BackOrifice
10223 RPC portmapper
11707 Bugbear.B web backdoor
10374 uw-imap buffer overflow after login
11220 Netscape /.perf accessible
10683 iPlanet Certificate Management Traversal
11030 Apache chunked encoding
10622 PPTP detection and versioning
10045 Cisco 675 passwordless router
11245 Unpassworded root account
11586 FileMakerPro Detection
11120 xtelw detection
11243 Unpassworded 4Dgifts account
11510 BIND 4.x resolver overflow
11061 HTTP version number overflow
11167 Webserver4everyone too long URL
11523 Samba trans2open buffer overflow
10607 SSH1 CRC-32 compensation attack
10994 IPSwitch IMail SMTP Buffer Overflow
11408 Apache < 2.0.43
11251 Unpassworded tutor account
10954 OpenSSH AFS/Kerberos ticket/token passing
11136 /bin/login overflow exploitation
11755 CesarFTP multiple overflows
10438 Netwin's DMail ETRN overflow
11118 alya.cgi
11396 hp jetdirect vulnerabilities
10323 XTramail control denial
10029 BIND vulnerable
10472 SSH Kerberos issue
11353 NFS fsirand
11188 X Font Service Buffer Overflow
10752 Apache Auth Module SQL Insertion Attack
11060 OpenSSL overflow (generic test)
10685 IIS ISAPI Overflow
11263 Default password (lrkr0x) for gamez
10881 SSH protocol versions supported
10343 MySQLs accepts any password
10341 Pocsag password
10625 IMAP4rev1 buffer overflow after login
10006 PC Anywhere
11403 iPlanet Application Server Buffer Overflow
11164 SOCKS4 username overflow
11704 icmp leak
10828 SysV /bin/login buffer overflow (rlogin)
10962 Cabletron Web View Administrative Access

10243 ypupdated service
11081 Oracle9iAS too long URL
11299 MySQL double free()
11192 multiple MySQL flaws
11369 irix performance copilot
11170 Alcatel OmniSwitch 7700/7800 switches backdoor
11138 Citrix published applications
11196 Cyrus IMAP pre-login buffer overrun
10998 Shiva LanRover Blank Password
10220 nlockmgr service
10879 Shell Command Execution Vulnerability
11742 Magic WinMail Format string
10350 Shaft Detect
11126 SOCKS4A hostname overflow
10320 Too long URL
10257 SmartServer pop3 overflow
10713 CodeRed version X detection
11340 SSH Secure-RPC Weak Encrypted Authentication
11312 DHCP server overflow / format string bug
10678 Apache /server-info accessible
11420 Sun portmap xdrmem_getbytes() overflow
11153 Identifies unknown services with 'HELP'
10031 bootparamd service
10116 IIS buffer overflow
10424 NAI Management Agent leaks info
10654 Oracle Application Server Overflow
11265 Default password (satori) for rewt
11210 Apache < 2.0.44 file reading on Win32
10355 vqServer web traversal vulnerability
10722 LDAP allows null bases
11612 PXE server overflow
10036 CDK Detect
11259 Unpassworded StoogR account
10407 X Server
11354 Buffer overflow in FreeBSD 2.x lpd
11204 Apache Tomcat Default Accounts
10501 Trinity v3 Detect
10242 yppasswd service
10066 FakeBO buffer overflow
10882 SSH protocol version 1 enabled
11733 Bugbear.B worm
10425 NAI Management Agent overflow
10381 Piranha's RH6.2 default password
10421 Rockliffe's MailSite overflow
11031 OpenSSH <= 3.3
11260 Default password (wank) for wank
10200 RealServer G2 buffer overrun
10214 database service
10241 ypbind service
10439 OpenSSH < 2.1.1 UseLogin feature
11544 MonkeyWeb POST with too much data
11279 Webmin Session ID Spoofing
10580 netscape imap buffer overflow after logon
10351 The ACC router shows configuration without authentication
11338 Lotus Domino Vulnerabilities
11005 LocalWeb2000 remote read
10698 WebLogic Server /%00/ bug

11607 Apache < 2.0.46 on OS/2
10158 NIS server
11187 4553 Parasite Mothership Detect
10269 SSH Overflow
11327 Nortel Baystack switch password test
11151 Webserver 4D Cleartext Passwords
10219 nfsd service
11592 12Planet Chat Server Path Disclosure
11540 PPTP overflow
11314 Buffer overflow in Microsoft Telnet
10215 etherstatd service
10684 yppasswdd overflow
10708 SSH 3.0.0
11130 BrowseGate HTTP headers overflows
10240 walld service
11665 Apache < 2.0.46
10529 Nortel Networks passwordless router (user level)
10786 Samba Remote Arbitrary File Creation
10212 automountd service
10454 sawmill password
11567 CommunicatePro Hijacking
10307 Trin00 for Windows Detect
10230 sched service
11137 Apache < 1.3.27
10596 Tinyproxy heap overflow
11409 ePolicy orchestrator format string
11634 Proxy Web Server Cross Site Scripting
10646 Lion worm
11783 Multiple IRC daemons format string attack
11235 Too long OPTIONS parameter
11003 IIS Possible Compromise
10544 format string attack against statd
10288 Trin00 Detect
10226 rquotad service
10283 TFN Detect
11563 Oracle LINK overflow
11341 SSH1 SSH Daemon Logging Failure
11266 Unpassworded jill account
11481 mod_auth_any command execution
11357 NFS cd ..
11075 dwhttpd format string
10440 Check for Apache Multiple / vulnerability
10411 klogind overflow
11484 apcupsd overflows
11716 Misconfigured Gnutella
10109 SCO i2odialogd buffer overrun
10559 XMail APOP Overflow
10699 IIS FrontPage DoS II
11633 lovgate virus is installed
10342 Check for VNC
11000 MPEi/X Default Accounts
11242 Unpassworded demos account
11201 Nortel/Bay Networks/Xylogics Annex default password
10008 WebSite 1.0 buffer overflow
10172 Passwordless HP LaserJet
10626 MySQL various flaws
10538 iWS shtml overflow

11262 Default password (D13hh[]) for root
11311 shtml.exe overflow
11554 BadBlue Administrative Actions Vulnerability
11419 Office files list
10149 NetBeans Java IDE
10225 rje mapper service
10605 BIND vulnerable to overflows
10244 ypxfrd service
10063 Eserv traversal
11268 OS fingerprint
10705 SimpleServer remote execution
10515 Too long authorization
10453 sawmill allows the reading of the first line of any file
11123 radmin detection
11006 RedHat 6.2 inetd
11261 Default password (D13HH[]) for root
10423 qpopper euidl problem
11197 Etherleak
10523 thttpd ssi file retrieval
11598 MailMax IMAP overflows
10832 Kcms Profile Server
10186 Portal of Doom
10554 RealServer Memory Content Disclosure
10233 snmp service
10498 Test HTTP dangerous methods
11152 BIND vulnerable to cached RR overflow
11337 mountd overflow
10687 Too long POST command
11480 3com RAS 1500 configuration disclosure
11552 mod_ntlm overflow / format string bug
10211 amd service
10659 snmpXdmid overflow
11651 Batalla Naval Overflow
11134 QMTP
11442 Samba TNG multiple flaws
11218 Tomcat /status information disclosure
11257 Default password (manager) for system
10224 rexd service
10760 Alcatel ADSL modem with firewalling off
11111 rpcinfo -p
11264 Default password (wh00t!) for root
10469 ipop2d reads arbitrary files
10420 Gauntlet overflow
10333 Linux TFTP get file
11240 Unpassworded guest account
11514 Netgear ProSafe Router password disclosure
10481 Unpassworded MySQL
10123 Imail's imap buffer overflow
11023 lpd, dvips and remote command execution
11127 HTTP 1.0 header overflow
11082 Boozt index.cgi overflow
10657 NT IIS 5.0 Malformed HTTP Printer Request Header Buffer Overflow
Vulnerability
11736 gnocatan multiple buffer overflows
10527 Boa file retrieval
11388 l2tpd < 0.68 overflow
10057 Lotus Domino ?open Vulnerability

11157 Trojan horses
10410 ICEcap default password
10379 LCDproc server detection
10231 selection service
10697 WebLogic Server DoS
10125 Imap buffer overflow
10790 rwhois format string attack
11203 Motorola Vanguard with No Password
10530 Passwordless Alcatel ADSL Modem
10380 rsh on finger output
10161 rlogin -froot
10330 Services
10239 tooltalk service
10950 rpc.walld format string
11699 URLScan Detection
11228 Unreal Engine flaws
11628 WebLogic Certificates Spoofing
10251 rpc.nisd overflow
11267 OpenSSL password interception
11642 Helix RealServer Buffer Overrun
11019 Alcatel PABX 4400 detection
11435 ActiveSync packet overflow
10812 libgtop_daemon format string
10378 LCDproc buffer overflow
10647 ntpd overflow
10436 INN version check (2)
10012 Alibaba 2.0 buffer overflow
10709 TESO in.telnetd buffer overflow
10010 AliBaba path climbing
10329 BIND iquery overflow
10437 NFS export
11406 Buffer overflow in BSD in.lpd
10723 LDAP allows anonymous binds
10833 dtspcd overflow
11376 qpopper Qvsprintf buffer overflow
10600 ICECast Format String
11456 PostgreSQL multiple flaws
10222 nsemntd service
10104 HP LaserJet direct print
11389 rsync modules
10965 SSH 3 AllowedAuthentication
10345 Passwordless Cayman DSL router
10540 NSM format strings vulnerability
10368 Dansie Shopping Cart backdoor
10339 TFTP get file
11591 12Planet Chat Server ClearText Password
10287 Traceroute
10920 RemotelyAnywhere WWW detection
11504 MultiTech Proxy Server Default Password
11606 WebLogic Server hostname disclosure
10578 Oops buffer overflow
10382 Atrium Mercur Mailserver
11318 BIND 9 overflow
10815 Web Server Cross Site Scripting
11278 Quicktime/Darwin Remote Admin Exploit
10124 Imail's imonitor buffer overflow
10532 eXtropia Web Store remote file retrieval

10094 Girlfriend
10053 DeepThroat
10005 NetSphere Backdoor
10218 llockmgr service
10070 Finger backdoor
10390 mstream agent Detect
10909 Brute force login (Hydra)
10209 X25 service
11355 Buffer overflow in AIX lpd
11252 Unpassworded toor account
10691 Netscape Enterprise INDEX request problem
11513 Solaris lpd remote command execution
10129 INN version check
11358 The remote portmapper forwards NFS requests
11256 Default password (guest) for guest
10771 OpenSSH 2.5.x -> 2.9.x adv.option
11637 MailMax IMAP overflows (2)
10608 OpenSSH 2.3.1 authentication bypass vulnerability
10210 alis service
10206 Rover pop3 overflow
11656 Eserv Directory Index
11763 Kerio WebMail interface flaws
10681 Netscape Messaging Server User List
10292 uw-imap buffer overflow
11108 Omron WorldView Wnn Overflow
10502 Axis Camera Default Password
11405 dmsd service
11576 tthttpd directory traversal thru Host:
11154 Unknown services banners
10018 Knox Arkeia buffer overflow
10286 tthttpd flaw
11168 Samba Unicode Buffer Overflow
10110 iChat
10666 AppleShare IP Server status query
10409 SubSeven
10091 FTPGate traversal
10935 IIS ASP ISAPI filter Overflow
10103 HP LaserJet display hack
10951 cachefs overflow
11673 Remote PC Access Server Detection
10197 qpopper LIST buffer overflow
10196 qpopper buffer overflow
11133 Generic format string
11135 Bugbear worm
10384 IRIX Objectserver
10268 SSH Insertion Attack
10391 mstream handler Detect
10422 MDBMS overflow
10889 NIDS evasion
10048 Communigate Pro overflow
10966 IMAP4buffer overflow in the BODY command
10823 OpenSSH UseLogin Environment Variables
10483 Unpassworded PostgreSQL
11574 Portable OpenSSH PAM timing attack
11169 SSH setsid() vulnerability
11342 PKCS #1 Version 1.5 Session Key Retrieval
11343 OpenSSH Client Unauthorized Remote Forwarding

10724 Cayman DSL router one char login
10227 rstatd service
11712 OpenSSH Reverse DNS Lookup bypass
10202 remwatch
11199 Multiple vulnerabilities in CUPS
11378 MySQL mysqld Privilege Escalation Vulnerability
11313 MCMS : Buffer overflow in Profile Service
10216 fam service
11248 Unpassworded date account
11249 Unpassworded jack account
10804 rwhois format string attack (2)
10658 Oracle tnslnr version query
10766 Apache UserDir Sensitive Information Disclosure
10928 EFTP buffer overflow
10130 ipop2d buffer overflow
11069 HTTP User-Agent overflow
11493 Sambar Default Accounts
10758 Check for VNC HTTP
10919 Check open ports
11255 Default password (root) for root
10660 Oracle tnslnr security
11577 MDAemon IMAP CREATE overflow
11183 HTTP negative Content-Length buffer overflow
11253 Unpassworded hax0r account
11620 Airport Administrative Port
11258 Default password (glftpd) for glftpd
11021 irix rpc.passwd overflow
11209 Apache < 2.0.44 DOS device name
10270 Stacheldraht Detect
11247 Unpassworded sync account
10096 rsh with null username
11078 HTTP header overflow
10236 statmon service
10151 NetBus 1.x
11784 Abyss httpd overflow
11068 iPlanet chunked encoding
10285 thttpd 2.04 buffer overflow
11522 Linksys Router default password
10500 Shiva Integrator Default Password
11495 tanned format string vulnerability
10276 TCP Chorusing
10816 Webalizer Cross Site Scripting Vulnerability
10923 Squid overflows
11280 Usermin Session ID Spoofing
10921 RemotelyAnywhere SSH detection
10528 Nortel Networks passwordless router (manager level)
10152 NetBus 2.x
11335 mibiisa overflow
11641 BadBlue Remote Administrative Interface Access
11507 Apache < 2.0.45
10805 Informix traversal
11096 Avirt gateway insecure telnet proxy
10389 Cart32 ChangeAdminPassword
11129 HTTP 1.1 header overflow
10267 SSH Server type and version
10408 Insecure Napster clone
10154 Netscape Enterprise 'Accept' buffer overflow

10533 Web Shopper remote file retrieval
 11398 Samba Fragment Reassembly Overflow
 10706 McAfee myCIO Directory Traversal
 10948 qpopper options buffer overflow

Preferences settings for this scan:

```

max_hosts                = 16
max_checks               = 10
log_whole_attack         = yes
cgi_path                 = /cgi-bin
port_range               = 1-65535
optimize_test           = yes
language                 = english
checks_read_timeout      = 5
non_simult_ports         = 139, 445
plugins_timeout          = 320
safe_checks              = yes
auto_enable_dependencies = yes
use_mac_addr             = no
save_knowledge_base      = yes
kb_restore               = no
only_test_hosts_whose_kb_we_dont_have = no
only_test_hosts_whose_kb_we_have   = no
kb_dont_replay_scanners  = no
kb_dont_replay_info_gathering = no
kb_dont_replay_attacks   = no
kb_dont_replay_denials   = no
kb_max_age               = 864000
plugin_upload            = no
plugin_upload_suffixes   = .nasl, .inc
slice_network_addresses  = no
ntp_save_sessions        = yes
ntp_detached_sessions    = yes
server_info_nessusd_version = 2.0.7
server_info_libnasl_version = 2.0.7
server_info_libnessus_version = 2.0.7
server_info_thread_manager = fork
server_info_os            = SunOS
server_info_os_version    = 5.7
reverse_lookup           = no
ntp_keep_communication_alive = yes
ntp_opt_show_end         = yes
save_session             = yes
detached_scan            = no
continuous_scan          = no

```

```

Total security holes found : 55
      high severity : 16
      low severity  : 39
      informational : 0

```

Scanned hosts:

Name	High	Low	Info
------	------	-----	------

host12.foo.com	0	0	0
host4.foo.com	4	13	0
host5.foo.com	3	5	0
host13.foo.com	0	0	0
host2.foo.com	3	8	0
host15.foo.com	0	0	0
host14.foo.com	0	0	0
host3.foo.com	3	8	0
host1.foo.com	3	5	0

Service: oracle (1521/tcp)

Severity: High

The remote Oracle Database, according to its version number, is vulnerable to a buffer overflow in the query CREATE DATABASE LINK.

An attacker with a database account may use this flaw to gain the control on the whole database, or even to obtain a shell on this host.

Solution : See <http://otn.oracle.com/deploy/security/pdf/2003alert54.pdf>

Risk Factor : High

BID : 7453

Vulnerable hosts:

host4.foo.com

Service: ssh (22/tcp)

Severity: High

You are running a version of OpenSSH older than OpenSSH 3.2.1

A buffer overflow exists in the daemon if AFS is enabled on your system, or if the options KerberosTgtPassing or AFSTokenPassing are enabled. Even in this scenario, the vulnerability may be avoided by enabling UsePrivilegeSeparation.

Versions prior to 2.9.9 are vulnerable to a remote root exploit. Versions prior to 3.2.1 are vulnerable to a local root exploit.

Solution :

Upgrade to the latest version of OpenSSH

Risk factor : High

CVE : CVE-2002-0575

BID : 4560

Vulnerable hosts:

```
host2.foo.com
host1.foo.com
host3.foo.com
host4.foo.com
host5.foo.com
```

Service: ssh (22/tcp)
Severity: High

You are running a version of OpenSSH which is older than 3.1.

Versions prior than 3.1 are vulnerable to an off by one error that allows local users to gain root access, and it may be possible for remote users to similarly compromise the daemon for remote access.

In addition, a vulnerable SSH client may be compromised by connecting to a malicious SSH daemon that exploits this vulnerability in the client code, thus compromising the client system.

Solution : Upgrade to OpenSSH 3.1 or apply the patch for prior versions. (See: <http://www.openssh.org>)

Risk factor : High
CVE : CVE-2002-0083
BID : 4241

Vulnerable hosts:

```
host5.foo.com
host4.foo.com
host3.foo.com
host1.foo.com
host2.foo.com
```

Service: ssh (22/tcp)
Severity: High

You are running a version of OpenSSH which is older than 3.4

There is a flaw in this version that can be exploited remotely to give an attacker a shell on this host.

Note that several distribution patched this hole without changing the version number of OpenSSH. Since Nessus solely relied on the banner of the remote SSH server to perform this check, this might be a false positive.

If you are running a RedHat host, make sure that the command :
rpm -q openssh-server

Returns :
openssh-server-3.1p1-6

Solution : Upgrade to OpenSSH 3.4 or contact your vendor for a patch
Risk factor : High
CVE : CVE-2002-0639, CVE-2002-0640
BID : 5093

Vulnerable hosts:
host4.foo.com
host5.foo.com
host1.foo.com
host3.foo.com
host2.foo.com

Service: domain (53/tcp)
Severity: Low

A DNS server is running on this port. If you
do not use it, disable it.

Risk factor : Low

Vulnerable hosts:
host3.foo.com
host2.foo.com
host4.foo.com

Service: domain (53/tcp)
Severity: Low

The remote bind version is : 12.1.1-udbd

Vulnerable hosts:
host4.foo.com
host2.foo.com
host3.foo.com

Service: domain (53/udp)
Severity: Low

A DNS server is running on this port. If you do not use it, disable it.

Risk factor : Low

Vulnerable hosts:

host2.foo.com
host4.foo.com
host3.foo.com

Service: general/udp

Severity: Low

For your information, here is the traceroute to <host4 IP> :

?

<host4 IP>

Vulnerable hosts:

host4.foo.com

Service: http (80/tcp)

Severity: Low

The remote web servers is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map or search page instead.

Nessus enabled some counter measures for that, however they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate

Vulnerable hosts:

host4.foo.com

Service: http (80/tcp)

Severity: Low

The remote host appears to be running a version of Apache which is older than 1.3.27

There are several flaws in this version, you should upgrade to 1.3.27 or newer.

*** Note that Nessus solely relied on the version number
*** of the remote server to issue this warning. This might
*** be a false positive

Solution : Upgrade to version 1.3.27

See also : <http://www.apache.org/dist/httpd/Announcement.html>

Risk factor : Medium

CVE : CAN-2002-0839, CAN-2002-0840, CAN-2002-0843

BID : 5847, 5884, 5995, 5996

Vulnerable hosts:

host4.foo.com

Service: http (80/tcp)

Severity: Low

The remote web server type is :

Apache/1.3.26 (Unix) PHP/4.2.1

Solution : You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Vulnerable hosts:

host4.foo.com

Service: oracle (1521/tcp)

Severity: Low

This host is running the Oracle tnslnsr: TNSLSNR for Solaris: Version 8.1.7.4.0 - Production

CVE : CVE-2000-0818

BID : 1853

Vulnerable hosts:

host4.foo.com

Service: ssh (22/tcp)

Severity: Low

The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol.

These protocols are not completely cryptographically safe so they should not be used.

Solution :

If you use OpenSSH, set the option 'Protocol' to '2'

If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'

Risk factor : Low

Vulnerable hosts:

host2.foo.com
host3.foo.com
host5.foo.com
host1.foo.com
host4.foo.com

Service: ssh (22/tcp)

Severity: Low

You are running OpenSSH-portable 3.6.1 or older.

There is a flaw in this version which may allow an attacker to bypass the access controls set by the administrator of this server.

OpenSSH features a mechanism which can restrict the list of hosts a given user can log from by specifying a pattern in the user key file (ie: *.mynetwork.com would let a user connect only from the local network).

However there is a flaw in the way OpenSSH does reverse DNS lookups. If an attacker configures his DNS server to send a numeric IP address when a reverse lookup is performed, he may be able to circumvent this mechanism.

Solution : Upgrade to OpenSSH 3.6.2 when it comes out

Risk Factor : Low

CVE : CAN-2003-0386

BID : 7831

Vulnerable hosts:

host3.foo.com
host5.foo.com
host1.foo.com
host2.foo.com
host4.foo.com

Service: ssh (22/tcp)
Severity: Low

You are running OpenSSH-portable 3.6.1p1 or older.

If PAM support is enabled, an attacker may use a flaw in this version to determine the existence of a given login name by comparing the times the remote sshd daemon takes to refuse a bad password for a non-existent login compared to the time it takes to refuse a bad password for an existent login.

An attacker may use this flaw to set up a brute force attack against the remote host.

*** Nessus did not check whether the remote SSH daemon is actually using PAM or not, so this might be a false positive

Solution : Upgrade to OpenSSH-portable 3.6.1p2 or newer
Risk Factor : Low
CVE : CAN-2003-0190
BID : 7482

Vulnerable hosts:
host2.foo.com
host1.foo.com
host4.foo.com
host3.foo.com
host5.foo.com

Service: ssh (22/tcp)
Severity: Low

Remote SSH version : SSH-1.5-OpenSSH_3.0.2p1

Vulnerable hosts:
host4.foo.com
host5.foo.com
host3.foo.com
host2.foo.com

Service: ssh (22/tcp)
Severity: Low

Remote SSH version : SSH-1.99-OpenSSH_3.0.2p1

Vulnerable hosts:
host1.foo.com

Service: ssh (22/tcp)
Severity: Low

The remote SSH daemon supports the following versions of the SSH protocol :

- . 1.33
- . 1.5

Vulnerable hosts:
host2.foo.com
host3.foo.com
host5.foo.com
host4.foo.com

Service: ssh (22/tcp)
Severity: Low

The remote SSH daemon supports the following versions of the SSH protocol :

- . 1.33
- . 1.5
- . 1.99
- . 2.0

Vulnerable hosts:
host1.foo.com

Results of the Nessus Scan Recorded with the Sniffer Snort

Since we are running the Snort Intrusion Detection System in the e-commerce system, I checked the Snort logs to learn how much of my Nessus scan was detected by Snort. Snort monitors network traffic on both the DMZ and Trust interfaces of the Netscreen-100 firewall. When it detects traffic that matches an enabled signature, it writes data in a binary format into the appropriate directory tree: dmz for DMZ interface traffic and trust for Trust interface traffic. Barnyard is a separate Snort process that converts the raw,

binary data into a human-readable text format. Barnyard creates two files: `fast.alert` and `dump.log`. The `fast.alert` file is an executive summary of the day's alerts, while the `dump.log` file contains both the alerts and the raw data dump of that alert.

Although my Nessus scan ran between approximately 4:00 and 4:05 p.m. PDT, Barnyard converts the timestamps on all log entries to UTC/GMT. Therefore, any scan traffic should be identified between 2300 and 2305 GMT. I used the `grep` the `fast.alert` file for any entries that matches the IP address of my Nessus server. Since there are separate logs for each network interface, I had to run the command twice, once for each interface. The output of each command is included below.

DMZ Interface

```
[root@<censored> 072303]# zcat dump.log.072303.gz | more
```

(snip)

```
[**] [1:1852:3] WEB-MISC robots.txt access [**]  
[Classification: access to a potentially vulnerable web application]  
[Priority: 2]  
[Xref => http://cgi.nessus.org/plugins/dump.php3?id=10302]  
Event ID: 292      Event Reference: 292  
07/22/03-23:07:10.609717 <scanner IP>:51849 -> <host4 IP>:80  
TCP TTL:253 TOS:0x0 ID:37914 IpLen:20 DgmLen:68 DF  
***AP*** Seq: 0x8C4637FB Ack: 0xF534B610 Win: 0x2238 TcpLen: 20  
47 45 54 20 2F 72 6F 62 6F 74 73 2E 74 78 74 20  GET /robots.txt  
48 54 54 50 2F 31 2E 30 0D 0A 0D 0A  HTTP/1.0....
```

=====

```
[**] [1:1551:3] WEB-MISC /CVS/Entries access [**]  
[Classification: access to a potentially vulnerable web application]  
[Priority: 2]  
Event ID: 294      Event Reference: 294  
07/22/03-23:07:10.651137 <scanner IP>:51850 -> <host4 IP>:80  
TCP TTL:253 TOS:0x0 ID:37920 IpLen:20 DgmLen:69 DF  
***AP*** Seq: 0x8C467E49 Ack: 0xDA59CA7B Win: 0x2238 TcpLen: 20  
47 45 54 20 2F 43 56 53 2F 45 6E 74 72 69 65 73  GET /CVS/Entries  
20 48 54 54 50 2F 31 2E 30 0D 0A 0D 0A          HTTP/1.0....
```

[illegible]

```
[**] [1:1212:4] WEB-MISC Admin_files access [**]  
[Classification: Attempted Information Leak] [Priority: 2]  
Event ID: 296      Event Reference: 296  
07/22/03-23:07:11.214516 <scanner IP>:51867 -> <host4 IP>:80  
TCP TTL:253 TOS:0x0 ID:38012 IpLen:20 DgmLen:70 DF  
***AP*** Seq: 0x8C599C9E Ack: 0xAF5AE621 Win: 0x2238 TcpLen: 20  
47 45 54 20 2F 41 64 6D 69 6E 5F 66 69 6C 65 73  GET /Admin_files  
2F 20 48 54 54 50 2F 31 2E 30 0D 0A 0D 0A      / HTTP/1.0....
```

[illegible]


```
6D 69 6E 50 61 73 73 77 6F 72 64 20 48 54 54 50 minPassword HTTP
2F 31 2E 30 0D 0A 0D 0A /1.0....
```

[illegible]

```
[**] [1:1553:4] WEB-CGI /cart/cart.cgi access [**]
[Classification: access to a potentially vulnerable web application]
[Priority: 2]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0252]
Event ID: 334      Event Reference: 334
07/22/03-23:07:41.481522 <scanner IP>:52716 -> <host4 IP>:80
TCP TTL:253 TOS:0x0 ID:42228 IpLen:20 DgmLen:71 DF
***AP*** Seq: 0x8FEE987D Ack: 0x353156FF Win: 0x2238 TcpLen: 20
47 45 54 20 2F 63 61 72 74 2F 63 61 72 74 2E 63 GET /cart/cart.c
67 69 20 48 54 54 50 2F 31 2E 30 0D 0A 0D 0A      qi HTTP/1.0....
```

[illegible]

```
[**] [1:1995:1] WEB-CGI alya.cgi access [**]
[Classification: access to a potentially vulnerable web application]
[Priority: 2]
[Xref => http://cgi.nessus.org/plugins/dump.php3?id=11118]
Event ID: 336      Event Reference: 336
07/22/03-23:07:50.925621 <scanner IP>:52800 -> <host4 IP>:80
TCP TTL:253 TOS:0x0 ID:42326 IpLen:20 DgmLen:74 DF
***AP*** Seq: 0x905CB492 Ack: 0x76F4791E Win: 0x2238 TcpLen: 20
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 61 6C 79 GET /cgi-bin/aly
61 2E 63 67 69 20 48 54 54 50 2F 31 2E 30 0D 0A a.cgi HTTP/1.0..
0D 0A
```

=====

```
[**] [1:590:8] RPC portmap yperv request UDP [**]
[Classification: Decode of an RPC Query] [Priority: 2]
[Xref => http://www.whitehats.com/info/IDS12]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1043]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1042]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1232]
[Xref => http://www.securityfocus.com/bid/5914]
[Xref => http://www.securityfocus.com/bid/6016]
Event ID: 338          Event Reference: 338
07/23/03-02:40:13.784431 <host8.foo.com IP address censored>:48831 ->
<host3.foo.com IP address censored>:111
UDP TTL:250 TOS:0x0 ID:38945 IpLen:20 DgmLen:84 DF
Len: 64
3F 1F AE 2D 00 00 00 00 00 00 02 00 01 86 A0    ?...-.....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00    .....
00 00 00 00 00 00 00 00 00 01 86 A4 00 00 00 02    .....
00 00 00 11 00 00 00 00    .....
```

=====

```
[**] [1:590:8] RPC portmap ypsserv request UDP [**]  
[Classification: Decode of an RPC Query] [Priority: 2]  
[Xref => http://www.whitehats.com/info/IDS12]  
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1043]  
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1042]
```

```
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1232]
[Xref => http://www.securityfocus.com/bid/5914]
[Xref => http://www.securityfocus.com/bid/6016]
Event ID: 340      Event Reference: 340
07/23/03-02:40:30.437302 <host8.foo.com IP address censored>:49586 -> <host4
IP>:111
UDP TTL:250 TOS:0x0 ID:55595 IpLen:20 DgmLen:84 DF
Len: 64
3F 11 D0 27 00 00 00 00 00 00 02 00 01 86 A0  ?...'.....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 01 86 A4 00 00 00 02  .....
00 00 00 11 00 00 00 00  .....
=====
```

```
[**] [1:590:8] RPC portmap yperv request UDP [**]
[Classification: Decode of an RPC Query] [Priority: 2]
[Xref => http://www.whitehats.com/info/IDS12]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1043]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1042]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1232]
[Xref => http://www.securityfocus.com/bid/5914]
[Xref => http://www.securityfocus.com/bid/6016]
Event ID: 342      Event Reference: 342
07/23/03-02:40:38.531858 <host8.foo.com IP address censored>:49914 ->
<host2.foo.com IP address censored>:111
UDP TTL:250 TOS:0x0 ID:63695 IpLen:20 DgmLen:84 DF
Len: 64
3F 10 6E C5 00 00 00 00 00 00 02 00 01 86 A0  ?.n.....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 01 86 A4 00 00 00 02  .....
00 00 00 11 00 00 00 00  .....
=====
```

```
[**] [1:590:8] RPC portmap yperv request UDP [**]
[Classification: Decode of an RPC Query] [Priority: 2]
[Xref => http://www.whitehats.com/info/IDS12]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1043]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1042]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1232]
[Xref => http://www.securityfocus.com/bid/5914]
[Xref => http://www.securityfocus.com/bid/6016]
Event ID: 344      Event Reference: 344
07/23/03-02:41:54.546151 <host8.foo.com IP address censored>:52587 ->
<host3.foo.com IP address censored>:111
UDP TTL:250 TOS:0x0 ID:8653 IpLen:20 DgmLen:84 DF
Len: 64
3F 13 F7 5F 00 00 00 00 00 00 02 00 01 86 A0  ?.._.....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 01 86 A4 00 00 00 02  .....
00 00 00 11 00 00 00 00  .....
=====
```

```
[**] [1:590:8] RPC portmap yperv request UDP [**]
[Classification: Decode of an RPC Query] [Priority: 2]
```

```
[Xref => http://www.whitehats.com/info/IDS12]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1043]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1042]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1232]
[Xref => http://www.securityfocus.com/bid/5914]
[Xref => http://www.securityfocus.com/bid/6016]
Event ID: 346      Event Reference: 346
07/23/03-02:42:16.526793 <host8.foo.com IP address censored>:53385 -> <host4
IP>:111
UDP TTL:250 TOS:0x0 ID:30633 IpLen:20 DgmLen:84 DF
Len: 64
3F 13 BE D9 00 00 00 00 00 00 00 02 00 01 86 A0  ?.....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 01 86 A4 00 00 00 02  .....
00 00 00 11 00 00 00 00  .....
=====
```

```
[**] [1:590:8] RPC portmap yperv request UDP [**]
[Classification: Decode of an RPC Query] [Priority: 2]
[Xref => http://www.whitehats.com/info/IDS12]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1043]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1042]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1232]
[Xref => http://www.securityfocus.com/bid/5914]
[Xref => http://www.securityfocus.com/bid/6016]
Event ID: 348      Event Reference: 348
07/23/03-02:42:26.438000 <host8.foo.com IP address censored>:53743 ->
<host2.foo.com IP address censored>:111
UDP TTL:250 TOS:0x0 ID:40553 IpLen:20 DgmLen:84 DF
Len: 64
3F 11 0B 60 00 00 00 00 00 00 02 00 01 86 A0  ?..`.....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 01 86 A4 00 00 00 02  .....
00 00 00 11 00 00 00 00  .....
=====
```

```
[**] [1:590:8] RPC portmap yperv request UDP [**]
[Classification: Decode of an RPC Query] [Priority: 2]
[Xref => http://www.whitehats.com/info/IDS12]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1043]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1042]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1232]
[Xref => http://www.securityfocus.com/bid/5914]
[Xref => http://www.securityfocus.com/bid/6016]
Event ID: 350      Event Reference: 350
07/23/03-02:43:20.395914 <host8.foo.com IP address censored>:56369 ->
<host3.foo.com IP address censored>:111
UDP TTL:250 TOS:0x0 ID:28977 IpLen:20 DgmLen:84 DF
Len: 64
3F 11 84 0F 00 00 00 00 00 00 02 00 01 86 A0  ?.....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 01 86 A4 00 00 00 02  .....
00 00 00 11 00 00 00 00  .....
=====
```

```
[**] [1:590:8] RPC portmap yperv request UDP [**]
[Classification: Decode of an RPC Query] [Priority: 2]
[Xref => http://www.whitehats.com/info/IDS12]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1043]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1042]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1232]
[Xref => http://www.securityfocus.com/bid/5914]
[Xref => http://www.securityfocus.com/bid/6016]
Event ID: 352      Event Reference: 352
07/23/03-02:43:33.817934 <host8.foo.com IP address censored>:57047 -> <host4
IP>:111
UDP TTL:250 TOS:0x0 ID:42407 IpLen:20 DgmLen:84 DF
Len: 64
3F 1E CF 5E 00 00 00 00 00 00 00 02 00 01 86 A0  ?...^.....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 01 86 A4 00 00 00 02  .....
00 00 00 11 00 00 00 00  .....
=====
```

```
[**] [1:590:8] RPC portmap yperv request UDP [**]
[Classification: Decode of an RPC Query] [Priority: 2]
[Xref => http://www.whitehats.com/info/IDS12]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1043]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1042]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1232]
[Xref => http://www.securityfocus.com/bid/5914]
[Xref => http://www.securityfocus.com/bid/6016]
Event ID: 354      Event Reference: 354
07/23/03-02:43:39.915872 <host8.foo.com IP address censored>:57422 ->
<host2.foo.com IP address censored>:111
UDP TTL:250 TOS:0x0 ID:48507 IpLen:20 DgmLen:84 DF
Len: 64
3F 19 49 D9 00 00 00 00 00 00 02 00 01 86 A0  ?.I.....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 01 86 A4 00 00 00 02  .....
00 00 00 11 00 00 00 00  .....
=====
```

```
[**] [1:590:8] RPC portmap yperv request UDP [**]
[Classification: Decode of an RPC Query] [Priority: 2]
[Xref => http://www.whitehats.com/info/IDS12]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1043]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1042]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1232]
[Xref => http://www.securityfocus.com/bid/5914]
[Xref => http://www.securityfocus.com/bid/6016]
Event ID: 356      Event Reference: 356
07/23/03-02:45:47.973584 <host8.foo.com IP address censored>:60687 ->
<host3.foo.com IP address censored>:111
UDP TTL:250 TOS:0x0 ID:45515 IpLen:20 DgmLen:84 DF
Len: 64
3F 1B 8B FC 00 00 00 00 00 00 02 00 01 86 A0  ?.....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 01 86 A4 00 00 00 02  .....
```

• • • • •

=====

```
[**] [1:590:8P] RPC portmap yperv request UDP [**]
[Classification: Decode of an RPC Query] [Priority: 2]
[Xref => http://www.whitehats.com/info/IDS12]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1043]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1042]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1232]
[Xref => http://www.securityfocus.com/bid/5914]
[Xref => http://www.securityfocus.com/bid/6016]
Event ID: 358          Event Reference: 358
07/23/03-02:46:22.743378 <host8.foo.com IP address censored>:61624 -> <host4
IP>:111
UDP TTL:250 TOS:0x0 ID:14749 IpLen:20 DgmLen:84 DF
Len: 64
3F 1F 62 9C 00 00 00 00 00 00 02 00 01 86 A0  ?.b.....
00 00 00 02 00 00 00 00 03 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 01 86 A4 00 00 00 02  .....
00 00 00 11 00 00 00 00  .....
.....
```

[illegible]

```
[**] [1:590:8] RPC portmap ypserve request UDP [**]
[Classification: Decode of an RPC Query] [Priority: 2]
[Xref => http://www.whitehats.com/info/IDS12]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1043]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1042]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1232]
[Xref => http://www.securityfocus.com/bid/5914]
[Xref => http://www.securityfocus.com/bid/6016]
Event ID: 360      Event Reference: 360
07/23/03-02:46:41.975698 <host8.foo.com IP address censored>:62074 ->
<host2.foo.com IP address censored>:111
UDP TTL:250 TOS:0x0 ID:33989 IpLen:20 DgmLen:84 DF
Len: 64
3F 1B F9 4A 00 00 00 00 00 00 00 02 00 01 86 A0    ?...J.....
00 00 00 02 00 00 00 00 03 00 00 00 00 00 00 00    .....
00 00 00 00 00 00 00 00 00 00 01 86 A4 00 00 00 02    .....
[Xref => http://www.securityfocus.com/bid/6016]
Event ID: 356      Event Reference: 356
07/23/03-02:45:47.973584 <host8.foo.com IP address censored>:60687 ->
<host3.foo.com IP address censored>:111
UDP TTL:250 TOS:0x0 ID:45515 IpLen:20 DgmLen:84 DF
Len: 64
3F 1B 8B FC 00 00 00 00 00 00 00 02 00 01 86 A0    ?.....
00 00 00 02 00 00 00 00 03 00 00 00 00 00 00 00    .....
00 00 00 00 00 00 00 00 00 00 01 86 A4 00 00 00 02    .....
00 00 00 11 00 00 00 00                                .....
```

=====

```
[**] [1:590:8] RPC portmap ypserve request UDP [**]  
[Classification: Decode of an RPC Query] [Priority: 2]  
[Xref => http://www.whitehats.com/info/IDS12]  
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-10431]
```


Remote Management Console

```
ns100(M)-> get ha
version:1.2.2
state: master(0.0.62)
group id:1 priority:1 ha interface:DMZ/trust
ha mac: <censored> virtual mac: <censored>
encryption: enable password: <censored>
authentication: enable password: <censored>
arp count: 5 time ratio: 8
monitor ports: Trust Untrust
ha mode: normal
session sync: on
slave linkup: on
ns100(M)->
```

Checklist Item F1: PASS

Objective: The firewall(s) must provide an audit trail or log of all attempted and successful network connections.

```
ns100(M)-> get policy
total policies 44, default deny
pid  direction  source      destination  service  action  state  stlc
18  todmz      <censored>  <censored>  <censored> <censored> enabled --X-
23  todmz      <censored>  <censored>  <censored> <censored> enabled --X-
63  todmz      <censored>  <censored>  <censored> <censored> enabled --XX
2   todmz      <censored>  <censored>  <censored> <censored> enabled --X-
17  fromdmz    <censored>  <censored>  <censored> <censored> enabled --X-
72  fromdmz    <censored>  <censored>  <censored> <censored> enabled --XX
57  fromdmz    <censored>  <censored>  <censored> <censored> enabled --XX
76  fromdmz    <censored>  <censored>  <censored> <censored> enabled --XX
80  fromdmz    <censored>  <censored>  <censored> <censored> enabled --XX
58  fromdmz    <censored>  <censored>  <censored> <censored> enabled --XX
54  fromdmz    <censored>  <censored>  <censored> <censored> enabled --XX
71  fromdmz    <censored>  <censored>  <censored> <censored> enabled --XX
88  fromdmz    <censored>  <censored>  <censored> <censored> enabled --XX
90  fromdmz    <censored>  <censored>  <censored> <censored> enabled --XX
46  fromdmz    <censored>  <censored>  <censored> <censored> enabled --XX
51  fromdmz    <censored>  <censored>  <censored> <censored> enabled --XX
70  fromdmz    <censored>  <censored>  <censored> <censored> enabled --XX
87  fromdmz    <censored>  <censored>  <censored> <censored> enabled --XX
62  fromdmz    <censored>  <censored>  <censored> <censored> enabled --XX
42  fromdmz    <censored>  <censored>  <censored> <censored> enabled --XX
44  fromdmz    <censored>  <censored>  <censored> <censored> enabled --XX
85  fromdmz    <censored>  <censored>  <censored> <censored> enabled --XX
89  fromdmz    <censored>  <censored>  <censored> <censored> enabled --XX
61  fromdmz    <censored>  <censored>  <censored> <censored> enabled --XX
86  fromdmz    <censored>  <censored>  <censored> <censored> enabled --XX
19  outgoing   <censored>  <censored>  <censored> <censored> enabled --XX
25  outgoing   <censored>  <censored>  <censored> <censored> enabled --XX
91  outgoing   <censored>  <censored>  <censored> <censored> enabled --XX
65  outgoing   <censored>  <censored>  <censored> <censored> enabled --XX
20  incoming   <censored>  <censored>  <censored> <censored> enabled --XX
74  incoming   <censored>  <censored>  <censored> <censored> enabled --XX
67  incoming   <censored>  <censored>  <censored> <censored> enabled --XX
78  incoming   <censored>  <censored>  <censored> <censored> enabled --XX
82  incoming   <censored>  <censored>  <censored> <censored> enabled --XX
84  incoming   <censored>  <censored>  <censored> <censored> enabled --XX
```

```
48 todmz      <censored> <censored> <censored> <censored> enabled --XX
43 todmz      <censored> <censored> <censored> <censored> enabled --XX
66 todmz      <censored> <censored> <censored> <censored> enabled --XX
39 todmz      <censored> <censored> <censored> <censored> enabled --XX
55 todmz      <censored> <censored> <censored> <censored> enabled --XX
59 todmz      <censored> <censored> <censored> <censored> enabled --XX
47 todmz      <censored> <censored> <censored> <censored> enabled --XX
21 todmz      <censored> <censored> <censored> <censored> enabled --X-
45 incoming   <censored> <censored> <censored> <censored> enabled --XX
ns100 (M) ->
```

Checklist Item F2: PASS

Objective: The audit trail or log must include action taken by administrators, including user IDs; login date/time; log-out date/time; changes to policies; changes or additions to user privileges; and system start-ups and shut-downs.

```
ns100 (M) -> get log event
2003-07-17 00:21:01 system warn 00515 Admin <backup> has logged out via SCS
from <IP address censored>:49547
2003-07-17 00:21:01 system warn 00515 Admin <backup> has logged on via SCS
from <IP address censored>:49547
2003-07-17 00:21:00 system notif 00528 SCS: SSH user <backup> has been
authenticated using password from <IP address censored>:49547.
2003-07-16 14:32:07 system info 00767 <user1>: System Config saved from host
<IP address censored>
2003-07-16 14:32:17 system notif 00018 <user1>: Policy 91 has been moved
before 65
2003-07-16 14:32:07 system notif 00018 <user1>: Policy (91, <censored>) has
been added from host <IP address censored>
2003-07-16 14:29:24 system warn 00515 <user1>: Admin "<user1>" has logged on
via the WebUI(http) to port 80 from <IP address censored>:23751.
```

Checklist Item F3: PASS

Objective: Firewall logs must be stored on a dedicated syslog server.

Remote Management Console

```
ns100 (M) -> get syslog config
Syslog Configuration:
  Host Name: syslog.foo.com
  Security Facility: local5
  Facility: local5
  Max Send Level: debug
  module=system: emer, alert, crit, error, warn, notif, info, debug
  Host Port: 514
  VPN Encryption: disabled
Syslog is enabled
ns100 (M) ->
```

Checklist Item G1: FAIL

Objective: Procedures for backing up and restoring the firewall configuration must be documented.

As the firewall administrator, I was not aware of a documented procedure for backing up and restoring the firewall configuration. Moreover, I interviewed other members of my company's security team, who were equally unaware of such documentation. Therefore, we are out of compliance with checklist item G1.

© SANS Institute 2003, Author retains full rights.

Measure Residual Risk

In Assignment 1, I conducted a pre-audit risk assessment. In that risk-assessment, I compiled a list of assets, a list of threats (events) to each asset, and a list of potential vulnerabilities (conditions) that could allow each threat to be exploited. Because the audit had not yet been conducted, I had to use my background knowledge as a system administrator to determine the degree of risk for each of the vulnerabilities. Now that I have completed the audit, however, I have much more complete knowledge of the effectiveness of the controls. In other words, I am in a position to measure the residual risk. Table 5 summarizes my post-audit or residual risk analysis. Much of the table is copied from Table 3, Pre-Audit Risk Analysis. There are two important differences, though. First, I have deleted the rows corresponding to the Netscreen-100 physical appliance, since physical security controls were outside the scope of my audit. Second, I have added two new columns to the table: mitigating controls and residual risk. Mitigating controls is a brief summary of the controls that decrease the asset's vulnerability, along with a brief reference to the relevant audit results. Residual risk is a qualitative assessment of the risk, in light of the mitigating controls.

Table 5. Post-Audit Residual Risk Analysis

Asset	Threat	Vulnerability	Degree of Risk	Impact	Mitigating Controls	Residual Risk
Access to SSN or Internal Network	Unauthorized network access to SSN (Screened Service Network) or internal network	Existing (authorized) firewall policy allows an attacker to gain access to resources on either the SSN or internal network.	High	Greater probability of an attacker successfully compromising the security of servers in the SSN or internal network.	The firewall controls application flows in both directions. It denies by default any services not explicitly authorized.	Low

Asset	Threat	Vulnerability	Degree of Risk	Impact	Mitigating Controls	Residual Risk
Access to SSN or Internal Network	Denial of Service attack	Denial of Service attacks are a well-known problem. Given the lack of an approved security policy, it seemed likely that security vulnerabilities were not being updated in a timely manner, if at all.	High	A prolonged disruption of firewall availability would be a customer-visible outage and have a direct impact on revenue.	The firewall is kept current with the latest vendor upgrades, security patches, and security problem fix software.	Low
Details of our internal network architecture.	Unauthorized disclosure of internal network architecture	Although controls are in place to prevent the unauthorized disclosure of the architecture by an employee, it is not known if an outsider would be able to gain knowledge of our internal architecture.	Unknown	Greater probability of an attacker successfully compromising the security of the network.	The current firewall configuration allows an attacker to discover hosts in the SSN ("DMZ" interface), but not hosts on the back-end network segment ("trust" interface).	Medium

Asset	Threat	Vulnerability	Degree of Risk	Impact	Mitigating Controls	Residual Risk
Netscreen 100 Policies and Configuration	Unauthorized access to policies or configuration	Netscreen 100s offer two methods of administrative access: command-line (via SSH) and web-based (via SSL). An exploit in the Netscreen's implementation of either service could result in an intruder gaining unauthorized access.	Unknown	An intruder with unauthorized administrative access could deliberately bring the firewall down, disrupting network availability. The intruder could also modify the firewall configuration to make it easier to compromise the other machines on the network. A compromise of the e-commerce server could lead to theft of sensitive customer data, which would be a disaster for the business.	1. Command-line interface (CLI) management sessions are encrypted using Secure Shell (SSH). Nevertheless, web-based management sessions are not encrypted using Secure Sockets Layer (SSL). Instead, web-based sessions use unencrypted HTTP. 2. There are multiple layers of firewalls before the firewall that is the subject of this audit,	Low

Asset	Threat	Vulnerability	Degree of Risk	Impact	Mitigating Controls	Residual Risk
	Unauthorized modification of policies or configuration	An attacker with unauthorized access could make unauthorized changes to the firewall policies or configuration.	Unknown	Greater probability of an attacker successfully compromising the security of the network. Disruption or degradation of service.	1. CLI management sessions use SSH, not Telnet. 2. Multiple layers of firewalls.	Low
	Unauthorized disclosure of policies or configuration	An attacker with unauthorized access would be able to view the firewall policies and configuration, which would be an unauthorized disclosure of sensitive information.	Unknown	Greater probability of an attacker successfully compromising the security of the network.	1. CLI management sessions use SSH, not Telnet. 2. Multiple layers of firewalls.	Low
	Destruction of policies or configuration	An attacker with unauthorized access could delete the policies or configuration.	Unknown	Partial or total disruption of service.	1. CLI management sessions use SSH, not Telnet. 2. Multiple layers of firewalls.	Low
Financial information	Unauthorized access to (confidential) corporate financial data	Given that the firewall sees all connections between the batch processing server and the e-commerce database, it might be	Unknown	Using that information, the intruder could make educated guesses about some of the company's financial	While theoretically possible, it is unlikely that an intruder could	Low

Asset	Threat	Vulnerability	Degree of Risk	Impact	Mitigating Controls	Residual Risk
		possible for an intruder with access to the firewall to determine aggregate information about the number of transactions between the two systems.		data. This could be useful to a competitor.	aggregate financial information from the firewall logs. My audit revealed that the logs provide no <i>contextual</i> information about e-commerce transactions. For example, it is unclear how many transactions correspond to one network connection.	

Asset	Threat	Vulnerability	Degree of Risk	Impact	Mitigating Controls	Residual Risk
Potential forensic data	Unauthorized access to forensic data	Unauthorized access to forensic data might allow an intruder to learn confidential information about the company's financial condition, internal network architecture, usernames of authorized firewall administrators, as well as the contents of the forensic data.	Medium	The knowledge gained from this information could help an attacker compromise the SSN or internal networks.	The lack of encryption of web-based management sessions makes it possible for an attacker to eavesdrop an administrator's username and password, gain access to the system, and read the logs.	Medium
	Unauthorized modification of forensic data	An attacker with administrative access on the firewall might be able to modify the firewall logs.	Medium	Unauthorized modifications to forensic data might hamper investigations into security incidents. It would also disrupt the chain of custody of evidence. The data might not be usable in court.	My audit did not identify any way for an attacker to <u>modify</u> firewall logs. (I assess the risk of log <u>deletion</u> below.)	Low

Asset	Threat	Vulnerability	Degree of Risk	Impact	Mitigating Controls	Residual Risk
	Unauthorized disclosure of forensic data	Unauthorized access to forensic data might allow an intruder to learn confidential information about the company's financial condition, internal network architecture, usernames of authorized firewall administrators, as well as the contents of the forensic data.	Medium	The knowledge gained from this information could help an attacker successfully compromise security.	The lack of encryption of web-based management sessions makes it possible for an attacker to eavesdrop an administrator's username and password, gain access to the system, and read the logs.	Medium

Asset	Threat	Vulnerability	Degree of Risk	Impact	Mitigating Controls	Residual Risk
	Unauthorized destruction of forensic data	An attacker with administrative access on the firewall might be able to delete the firewall logs.	Medium	Destruction of the firewall logs could hamper security incident investigations.	The lack of encryption of web-based management sessions makes it possible for an attacker to eavesdrop an administrator's username and password, gain access to the system, and delete the logs.	Medium
Company reputation	Damage to reputation	A security compromise could lead to public embarrassment.	Medium	Public embarrassment can cause loss of customer and shareholder confidence.	Overall, the firewall appears to be a well-maintained and reasonable secure system.	Low

Overall, the residual risk is well within acceptable limits. Moreover, it would be very inexpensive to implement additional controls, which would further decrease the risk. These controls include the following:

- *Encrypt all administrative management sessions.* The organization can choose to either disable web-based management sessions or use SSL to encrypt them. Either option is very inexpensive to implement.
- *Document procedures for backup and restoration of firewall configuration and policies.* Only a very small amount of employee time would be needed to create the documentation.

The system successfully achieved most, but not all, of the control objectives. The unachieved control objectives are listed below.

Table 6. Unfulfilled Control Objectives

No.	Control Objective
CO7	All ports on the firewall itself should be disabled by default; only ports that have been specifically authorized should be open.
CO9	No vulnerable services should be accessible through the perimeter's countermeasures.
CO14	Firewall management sessions are extremely sensitive and must be encrypted.
CO22	Firewall configuration back up and restore procedures must be documented.

Is the system auditable?

I was unable to audit one portion of the firewall: the HA link failure detection. In order to audit that feature of the firewall, one would have to unplug interface cables from a production system. The owner of the e-commerce system that sits behind the firewall was rightfully concerned about the potential for disruption. Unfortunately, I had to delay this test until well after the timeframe for this audit.

Assignment 4 – Risk Assessment

Executive Summary

The e-commerce system owner recently requested an audit of the Netscreen-100 firewalls that protect the e-commerce environment. As the administrator of those firewalls, I set out to measure their compliance with organizational policies and procedures. The audit was conducted from July 7 to July 25, 2003.

Unfortunately, no approved security policy was in place at the time of my audit, so I was forced to audit the system against recognized best practices instead. Audit activity included interviews of network personnel, review of existing documentation, network mapping, vulnerability analysis, and development of high-level procedural and operational recommendations. However, I did not review physical security controls or the designs of future network security improvements.

As of July 25, 2003, it appears that the firewall does not meet all of its control objectives. While no high-risk vulnerabilities were discovered during the course of this audit, a few control objectives are not currently being met. The primary conclusions of the audit follow.

- Web-based firewall management sessions are not encrypted.
- An unauthorized service was running on the firewall's management interface.
- The firewall allowed access to vulnerable services running on internal hosts.
- Firewall configuration back up and restore procedures are not documented.

FINDINGS

After compiling my list of findings, I presented my recommendations to management for fixing the vulnerabilities. For some of the findings, I was actually able to correct the problem and then re-audit the system. For completed changes, I will summarize the corrective actions taken and then repeat the relevant item from the audit checklist to demonstrate that the vulnerability has been corrected. For some other findings, however, I was not able to correct the problem prior to the completion of this practical. While management agreed with me about the need to fix these "other" findings, management decided that other operational projects were a higher priority than the pending system changes. For pending system changes, I will simply indicate the implementation plan for removing vulnerabilities.

B8: Web-based firewall management sessions are not encrypted.

C2: An unauthorized service was running on the firewall's management interface.

Background / Risk

When a Netscreen-100 administrator wishes to administer the firewall using the web interface, the administrator must authenticate with his or her username and password. If the web session is not encrypted, then the administrator's username and password, along with all of the sensitive information contained within the firewall's configuration and policies, are transmitted as clear text. An attacker running a sniffer on the local network segment could capture and analyze any traffic that passes through that network segment. Moreover, since sniffers are passive by their very nature, they are difficult to detect. Because of eavesdropping on a firewall management session, an attacker would learn the administrator's username and password, making it possible for the attacker to create, modify, or delete firewall policies. That, in turn, places at risk the confidentiality, integrity, and availability of the systems behind the firewall. The attacker could disrupt network connectivity to the internal machines. The attacker could also expose the internal machines to attacks by opening ports that are currently closed.

Since the lack of encryption meant that the firewall management interface was running unencrypted HTTP and not HTTPS/SSL, which is encrypted, I have grouped together finding B8 with finding C2.

System Changes and Further Testing

To correct these related findings, I generated and downloaded to my PC an SSL certificate. I also downloaded to my PC a Certificate Authority (CA) certificate. (The details of how to generate and download a digital certificate are beyond the scope of this paper.) Once both certificates were downloaded to my PC, I then uploaded them to the firewall. (See Figure 5.) I next opened a web-based firewall management session and clicked on "Admin" and then "Web." I kept the default value of 443 for the "HTTPS (SSL) Port:" setting. I then clicked on the drop-down list next to "Certificate:" and selected the new SSL certificate I just uploaded, along with the correct Cipher. I clicked "Apply." (See Figure 6.) I then logged out and logged back in to verify that my implementation of SSL was effective. I then disabled unencrypted HTTP by clicking on "Interface," selecting the untrust interface, clicking "edit," and then unchecking the "Web equals HTTP" box. (See Figure 7.)

Figure 5 – Local Certificates Configuration on Netscreen-100

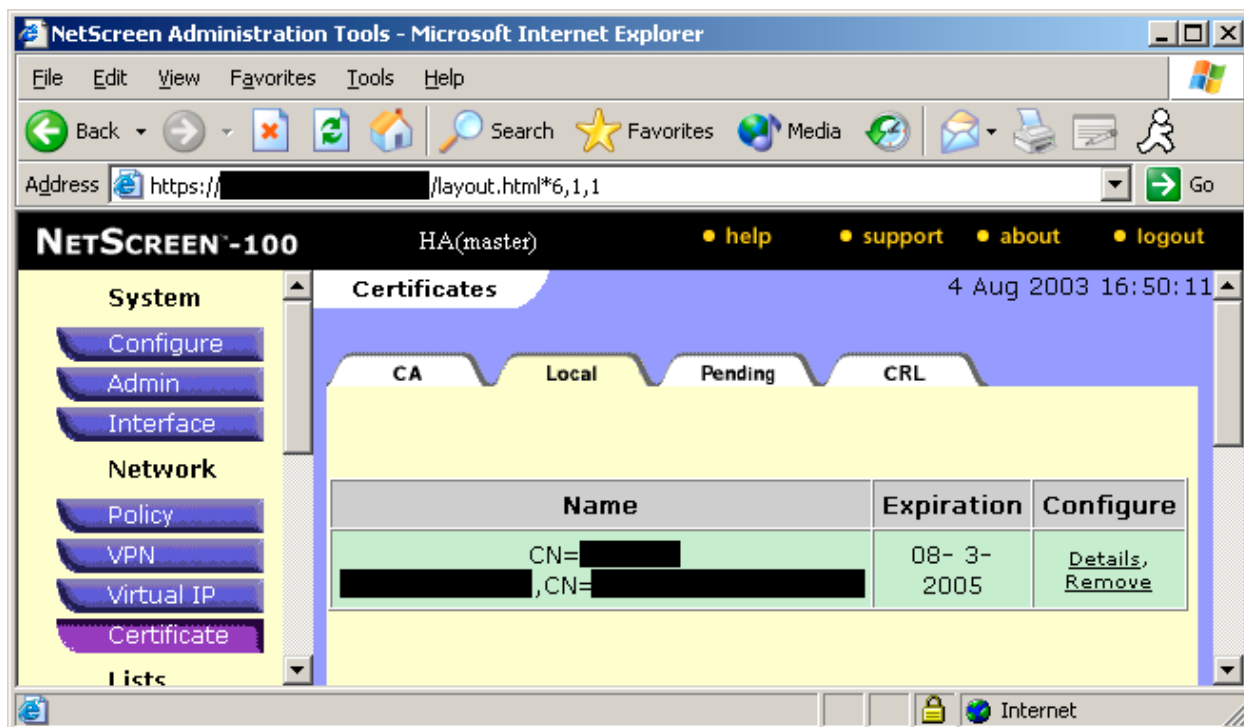


Figure 6 – Web Administration Settings on Netscreen-100

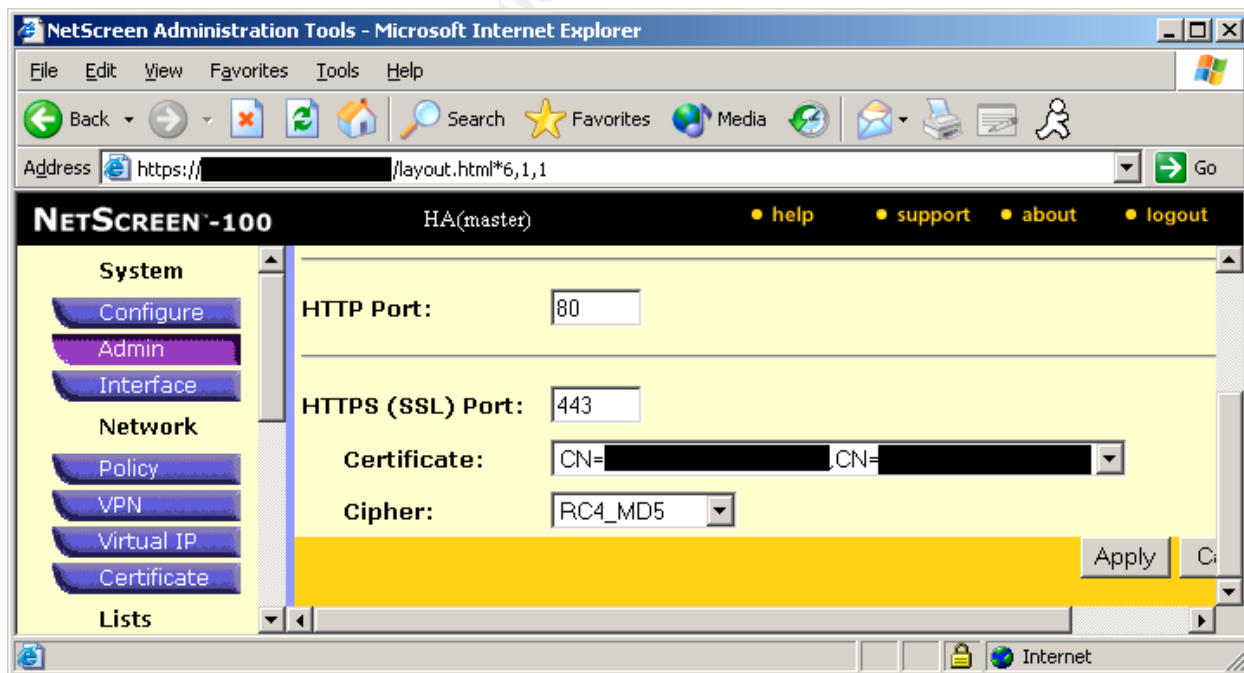


Figure 7 – Interface Configuration for Untrust Interface

The screenshot shows the NetScreen Administration Tools web interface in Microsoft Internet Explorer. The browser address bar shows a URL ending in /layout.html*6,1,1. The page title is "NETSCREEN-100 HA(master)". The left sidebar contains a navigation menu with categories: System (Configure, Admin, Interface), Network (Policy, VPN, Virtual IP, Certificate), Lists (Address, Service, Schedule, Users), and Monitor (Traffic, Counters, Alarm, Log). The main content area is titled "INTERFACE CONFIGURATION" and shows the configuration for the "untrust" interface (Up/100Mb). The "Obtain IP using PPPoE" option is selected, with "Connect" and "Disconnect" buttons and a "Status: Disabled" message. Below this are input fields for "User Name" and "Password". The "Static IP" option is also visible. Under "Static IP", there are input fields for "IP Address", "Netmask", "Default Gateway", and "Manage IP". A "Traffic Bandwidth" field is set to 0 Kbps. Under "Management Services", there are checkboxes for "Web UI", "Telnet", and "SNMP". Under "Other Services", there are checkboxes for "Web UI", "SCS", "SSL", "NS-GlobalPRO", "Ping", and "Ident-reset". At the bottom of the configuration area are "Save", "Cancel", and "Save and Reset" buttons. The footer of the page includes copyright information: "Copyright © 1998-2002 NetScreen Technologies Inc. All rights reserved." and a link to "Go to the Untrusted Interface".

C9: The firewall allowed access to vulnerable services running on internal hosts.

If it is possible to access vulnerable services running on internal hosts, then an attacker who knows how to exploit a vulnerable service will be able to successfully attack the system. A successful attack may allow the attacker to view sensitive data, modify data, or make the system unavailable to users.

Since this finding consists of multiple specific vulnerabilities, I provide below a brief summary of the risk posed by each of the vulnerabilities. In order to correlate each vulnerability with the Nessus output, whenever possible I will cross-reference each

vulnerability with the Nessus "plug-in ID" responsible for discovering the vulnerability. Also whenever possible, I will list the Common Vulnerabilities and Exposures (CVE) or Bugtraq ID (BID) number associated with each vulnerability.

The vulnerabilities may be divided into two groups: true positives and false positives. True positives are accurate findings; the vulnerabilities really do exist in the audited systems. False positives are inaccurate; the vulnerabilities are not applicable. Of the eleven specific vulnerabilities reported by Nessus, five turned out to be true positives. All of the true positives present a low degree of risk. The remaining six vulnerabilities reported by Nessus were false positives. After investigating all of the false positives, it appears that most of the false positives were due to the implementation of patches or fix-actions that Nessus is unable to detect. For example, in at least one instance, Nessus relied on the version number reported by the OpenSSH software. Unknown to Nessus, however, the vulnerability had been patched in a way that did not change the version number of the software. Thus, the false positives are understandable, even if inaccurate.

Web Server Advertising Version Number

Nessus plug-in ID: none provided in report
CVE: none

BACKGROUND / RISK

Knowing the version number of any software package running on a server, including web server software, can be very helpful to an attacker. Such information can allow the attacker to identify specific exploits that will provide unauthorized access. While the 'security-through-obscurity' approach is unwise when it is one's *only* layer of security, it can be useful as an *extra* layer of security since it can slow an attacker down.¹⁴

SYSTEM JUSTIFICATION

This vulnerability is accurate; the web server on host4.foo.com does advertise the version number of the Apache web server software. On the other hand, as I will show below, there are no other known vulnerabilities in our Apache implementation. Moreover, the Apache web server is not accessible from the Internet. Therefore, I recommended to management that this should be addressed, but be viewed as a low priority. Management agreed with me. Unfortunately, this prevents me from demonstrating the effectiveness of the recommended change prior to the completion of this practical.

Oracle Net Services Link Buffer Overflow Vulnerability

Nessus plug-in ID: 11563
BID: 7453

BACKGROUND / RISK

A buffer overflow vulnerability is a special kind of bug or defect in computer software. A buffer overflow vulnerability exists whenever computer software allocates and uses a "buffer" or section of computer memory, but the software fails to verify that the amount of information it wants to store in that buffer actually fits. If the stored information exceeds the buffer size, then the software may behave in unexpected ways. If a sophisticated attacker learns that a particular software application has a buffer overflow vulnerability, the attacker can send specially crafted packets to the application that exceed the buffer size. Since the specially crafted packets include instructions for the machine to follow, the attacker can actually trick the victim machine into executing virtually any instructions, including a set of instructions that gives the attacker access to the machine.

The Oracle Net Services Link Buffer Overflow Vulnerability is a perfect example of a buffer overflow vulnerability. This particular buffer overflow vulnerability requires that the attacker already have a valid account on the Oracle database. If the attacker sends a special type of query to the database (CREATE DATABASE LINK) and overflows the buffer with specially crafted packets, the attacker may be able to gain complete control over the database or even get a Unix account on the database machine.¹⁵

SYSTEM JUSTIFICATION

Nessus reported that this vulnerability was applicable to host4.foo.com. Upon further investigation, however, I learned that this item was a "false positive." This vulnerability had been removed by removing users' privilege to execute the "create database link" command.

```
setenv ORACLE_HOME /censored/oracle/product/8.1.7
setenv ORACLE_SID <censored>
$ORACLE_HOME/bin/sqlplus /NOLOG
>connect / as sysdba
>select * from dba_sys_privs
where privilege = 'CREATE DATABASE LINK'
```

GRANTEE	PRIVILEGE	ADMIN_OPTION
<censored>	CREATE DATABASE LINK	NO
DBA	CREATE DATABASE LINK	YES
<censored>	DATABASE LINK	NO
<censored>	CREATE DATABASE LINK	NO

Thus, the only Oracle user with privileges to execute the "create database link" command is the "dba" user. The "connect" role, which is assigned to every user in Oracle, is not listed as a grantee of the "create database link" privilege. Therefore, the only user who could successfully exploit the Oracle Net Services Link Buffer Overflow Vulnerability is the "dba" user. Since the "dba" user is a privileged account, an attacker with control of the "dba" user wouldn't need to exploit that vulnerability. The attacker would already "own" the database and could do whatever he or she pleased.¹⁶

Therefore, there is no compelling business reason to apply a patch to fix this vulnerability.

Buffer Overflow in OpenSSH

Nessus plug-in ID: 10954

CVE: CVE-2002-0575

BACKGROUND / RISK

OpenSSH is an application that is designed to provide authorized users with secure access to an interactive command prompt on a remote machine. Unfortunately, certain versions of the OpenSSH have a buffer overflow vulnerability. If an attacker successfully exploits this vulnerability, the attacker can gain privileges on the target system.¹⁷ Moreover, the attacker need not have pre-existing access on the target system in order to exploit this vulnerability; the vulnerability is remotely exploitable.

SYSTEM JUSTIFICATION

This vulnerability only applies to OpenSSH versions before 2.9.9 and versions 3.x before 3.2.1, if either Kerberos or AFS is supported. If those conditions are met, then the vulnerability applies.¹⁸

SecurityFocus.com clarifies the risk posed by this vulnerability. The degree of risk posed by this vulnerability depends upon the version of OpenSSH. For OpenSSH versions prior to 2.9.9, an attacker does not even "require valid user credentials" in order to exploit the vulnerability, whereas valid user credentials are required for versions 2.9.9 and higher.¹⁹

Since all of the Unix machines in my environment are running OpenSSH 3.0.2p1, this vulnerability is not remotely exploitable. An attacker must already have valid user credentials in order to exploit this vulnerability. Even with valid user credentials, however, the attacker still cannot exploit this vulnerability unless two conditions apply:

- (a) Kerberos/AFS is supported, and
- (b) KerberosTgtPassing or AFSTokenPassing is enabled²⁰

Nevertheless, neither condition applies. Regarding (a), we did not configure OpenSSH with Kerberos support enabled. As for (b), that condition does not apply to hosts1-5, as demonstrated by the following command line output.

```
host1$ grep AFSTokenPassing /usr/local/etc/sshd_config
#AFSTokenPassing no
host1$ grep KerberosTgtPassing /usr/local/etc/sshd_config
#KerberosTgtPassing yes
```

```
host2$ grep AFSTokenPassing /etc/sshd_config
```

```
host2$ grep KerberosTgtPassing /etc/sshd_config
host2$

host3$ grep AFSTokenPassing /etc/sshd_config
host3$ grep KerberosTgtPassing /etc/sshd_config
host3$

host4$ grep AFSTokenPassing /etc/sshd_config
host4$ grep KerberosTgtPassing /etc/sshd_config
host4$

host5$ grep AFSTokenPassing /usr/local/etc/sshd_config
#AFSTokenPassing no
host5$ grep KerberosTgtPassing sshd_config
#KerberosTgtPassing yes
```

Since both lines had been commented out on both host1 and host5, this means that OpenSSH resorts to defaults. Likewise, on hosts2-4, since there were no entries in `sshd_config` for `AFSTokenPassing` or `KerberosTgtPassing`, those machines also operate according to defaults. As the OpenSSH.com security advisory states, "Ticket and token passing is not enabled by default."²¹ Thus, this vulnerability was a false positive.

Off-by-One Error in the Channel Code of OpenSSH 2.0 through 3.0.2

Nessus plug-in ID: 10883
CVE: CVE-2002-0083

BACKGROUND / RISK

OpenSSH uses channels "to segregate differing traffic between the client and the server."²² OpenSSH versions 2.0 through 3.0.2 have an overflow vulnerability "in the code that handles channels."²³ This vulnerability makes two different kinds of attacks possible: (1) attacks against the OpenSSH server; and (2) attacks against the client.²⁴ I will briefly summarize each attack in turn.

Regarding (1), in order to successfully attack an OpenSSH server using this vulnerability, the attacker must have valid authentication credentials (e.g., username and password).²⁵ If successful, the attacker may be able to get the victim server to execute arbitrary code, which in turn may allow the attacker to take control of the victim machine. The attacker could view sensitive information, disrupt service to authorized users, or modify important files.

As for (2), this attack method requires that a client initiate a connection to an OpenSSH server. If successful, the malicious server is able to execute arbitrary code on the vulnerable client's machine with the privileges of the current user.²⁶ This means, for example, that an attacker could gain access on employee PCs used to run the SSH client software.

Thus, the off-by-one vulnerability is a serious vulnerability that may allow remote compromise of the root account.

SYSTEM JUSTIFICATION

According to the advisory at www.openbsd.org,²⁷ the solution for this vulnerability is to either upgrade to OpenSSH 3.1 or apply a patch to the source code. I checked the source code repository on the machine that was used to compile the OpenSSH binary. I confirmed that the source code had been patched.

```
$ more channels.c
```

```
[snip]
```

```
channel_lookup(int id)
{
    Channel *c;

    if (id < 0 || id >= channels_alloc) {
        log("channel_lookup: %d: bad id", id);
        return NULL;
    }
    c = channels[id];
```

```
[snip]
```

Thus, this was a false positive. Nessus reported the item as a vulnerability since there is no way to determine from the OpenSSH version number if the source code has been patched.

OpenSSH Challenge-Response Buffer Overflow Vulnerabilities

Nessus plug-in ID: 11031

CVE: CVE-2002-0639 and CVE-2002-0640

BACKGROUND / RISK

There are multiple vulnerabilities in OpenSSH's authentication process, specifically how OpenSSH handles challenge-response. After receiving the authentication challenge from a vulnerable OpenSSH server, an attacker could exploit a buffer overflow condition and trick the target machine into executing specially crafted instructions. Those instructions could allow the attacker to gain "root" privileges and effectively take over the machine.

SYSTEM JUSTIFICATION

As the SecurityFocus advisory points out, this vulnerability only applies to instances of OpenSSH that have been "configured at compile-time to support BSD_AUTH or SKEY."²⁸ Since I am the firewall administrator but not the Unix system administrator, I interviewed the Unix system administrator. He stated that my organization did not compile OpenSSH with either BSD_AUTH or SKEY support enabled. I confirmed his remarks by consulting the script used to compile OpenSSH. The following is an excerpt of that script.

```
cd openssh-3.0.2p1
./configure --sysconfdir=/etc
make
make install
```

Since the `--with-bsd-auth` option was not used at compile time, this vulnerability does not apply to our systems.

Domain Name Server (DNS) is Running

Nessus plug-in ID: none provided in report
CVE: none

BACKGROUND / RISK

DNS software is the software that helps translate web site "domain names" or address (e.g., `www.microsoft.com`) into numerical addresses the machine understands (e.g., `10.1.1.25`). When I ran Nessus it did not complain about any bugs in the version of DNS software that we run on our machines. Instead, the Nessus report simply stated, "A DNS server is running on this port. If you do not use it, disable it." Thus this warning seems to be an application of the general principle that software and services should not be run by default; only those software packages and services that are actually necessary should be run. Although no specific vulnerability is known at this time, there is always the possibility that a vulnerability could be identified in the future, increasing the organization's exposure. Clearly, this is a low-risk finding.

SYSTEM JUSTIFICATION

"named" is the name of the DNS server software that we use. Although it is not necessary that named run on each server, we run named on each server for three reasons. First, we get better load balancing on each server by running DNS locally. Second, running DNS on each host provides better resiliency, which is critical for many of our applications. Third, named provides more intelligent caching than what was built into Solaris by default.

Web Server does not return '404 Not Found' Error Code for Non-Existent Files

Nessus plug-in ID: 10386

CVE: none

BACKGROUND / RISK

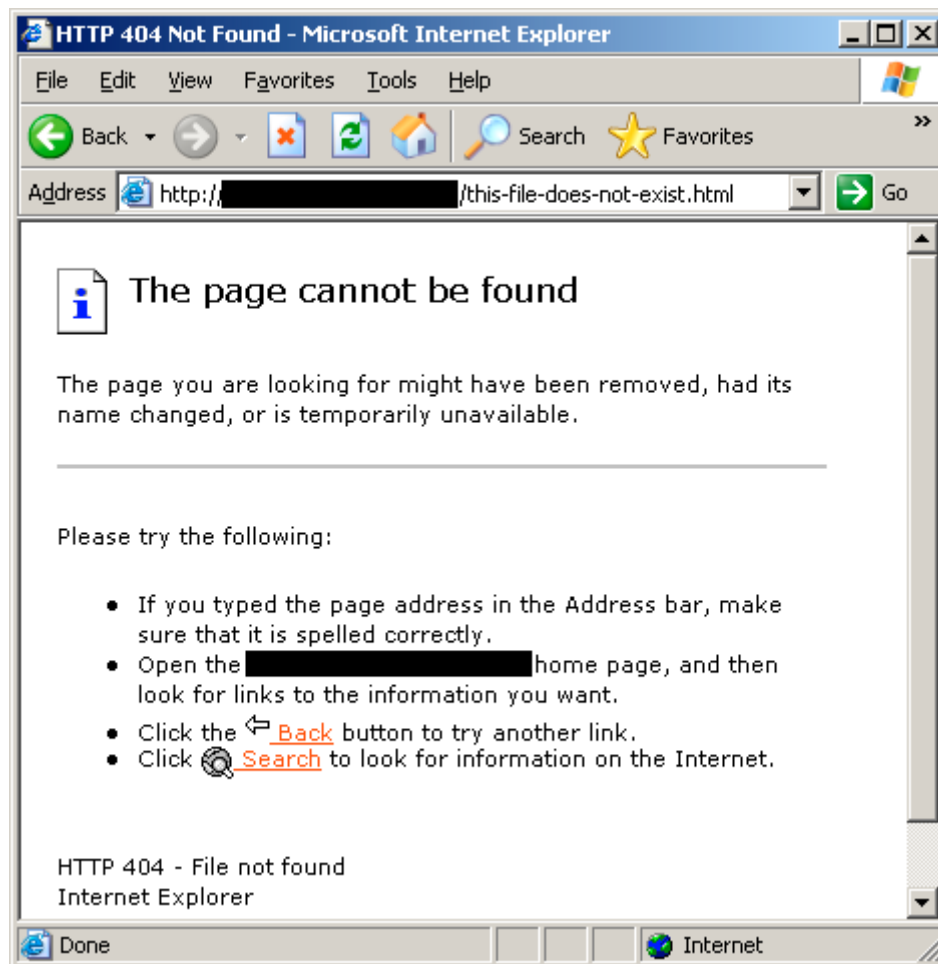
Normally, when one requests a non-existent "page" or file from a web site, the remote web server will return a "404 Not Found" error message. Nessus claims that our web server fails to do this; that is, Nessus claims that our web server fails to return a "404 Not Found" error message for non-existent pages. Yet it is unclear why Nessus considers this item a low-risk security vulnerability. The Nessus report states that this item may indicate a misconfiguration. Even if that were true, however, the misconfiguration would not be a threat to the confidentiality, integrity, or availability of the web server. Therefore, I do not consider this item to be a security vulnerability (even if it is a misconfiguration).

SYSTEM JUSTIFICATION

This vulnerability also turned out to be a false positive. I tried accessing multiple pages that do not exist on the web server; each time I received a page with the title "HTTP 404 Not Found". The snapshot below provides an example.

Figure 8 – Attempt to Download a Non-Existent HTML Page

© SANS Institute 2003, Author retains full rights.



Running Version of Apache Older than 1.3.27

Nessus plug-in ID: 11137

We use Apache as our web server software. Nessus reported that we are running an older version of the software, a version that has multiple security vulnerabilities. The Nessus output listed three specific vulnerabilities that applied to host4.foo.com since that host is running a version of Apache older than 1.3.27. I explain the vulnerabilities below.

*(1) APACHE WEB SERVER SCOREBOARD MEMORY SEGMENT OVERWRITING SIGUSR1S
ENDING VULNERABILITY*

CVE: CAN-2002-0839

BACKGROUND / RISK

Apache web servers with this vulnerability are susceptible to a local exploit allowing an authorized user to escalate privileges and possibly take over the system by gaining access to the "root" account.

SYSTEM JUSTIFICATION

The vulnerability only affects apache servers that are started as root. (Most apache servers are started as the root user because they need to bind a privileged port.) The Apache server on host4.foo.com, however, is started with only the credentials of the 'web' user. Thus, host4 is not vulnerable.

(2) APACHE SERVER SIDE INCLUDE CROSS SITE SCRIPTING VULNERABILITY

CVE: CAN-2002-0840

BACKGROUND / RISK

Attacks that exploit this vulnerability target *users*, not web servers. This vulnerability allows an attacker to execute arbitrary code in the web browser of the victim user. As a result, attackers may be able to display content in the victim user's web browser that differs from the content you intend for them to see. (For example, the attacker could display pornography or a form that asks users for their credit card numbers and sends the information to the attacker.) This vulnerability may also allow an attacker to steal the user's "cookie" or credentials, and gain access to whatever restricted web page the victim user had been authorized to access.²⁹

SYSTEM JUSTIFICATION

This vulnerability only affects Apache web servers that support Server Side Include (SSI). According to the Apache Tutorial on SSI,³⁰ even if Apache is compiled with SSI support, it is not active unless the following directive appears either in the httpd.conf file or in a .htaccess file:

```
Options +Includes
```

The following grep command verified that the directive does not appear in the httpd.conf file:

```
host4$ grep "Options \+Includes" /var/httpd/conf/httpd.conf
host4$
```

I next verified that the directive does not appear in any .htaccess files on host4.foo.com. To do so, I first identified the document root directory from the httpd.conf file:

```
host4$ grep DocumentRoot httpd.conf
```

```
DocumentRoot /censored/htdocs
```

I then searched all subdirectories under /censored/htdocs for .htaccess files:

```
host4$ cd /censored/htdocs
host4$ find . -name ".htaccess" -print
./censored1/.htaccess
./censored2/.htaccess
```

Finally, I confirmed that the directive does not appear in either .htaccess file:

```
host4$ grep "Options \+Includes" ./censored1/.htaccess
host4$ grep "Options \+Includes" ./censored2/.htaccess
host4$
```

Since neither .htaccess file contained the "Options +Includes" directive, I conclude that host4.foo.com is not affected by this vulnerability.

(3) APACHE AB.C WEB BENCHMARKING BUFFER OVERFLOW VULNERABILITY

CVE: CAN-2002-0843

BACKGROUND / RISK

As the Apache HTTP Server Project explains, "ab is a tool for benchmarking your Apache Hypertext Transfer Protocol (HTTP) server."³¹ Attackers can cause vulnerable Apache web servers running this tool to possibly execute arbitrary code and gain control of the machine. Attackers may also be able to cause denial-of-service, making the web server unavailable to legitimate users.³²

SYSTEM JUSTIFICATION

I interviewed the system administrator of the Apache web server, who informed me that we do not use the ab benchmarking tool. I also checked the list of current processes to see if ab was running.

```
$ ps -ef | grep ab
jlowder 26255 24340 0 01:16:06 pts/3 0:00 grep ab
```

I conclude that we are not affected by this vulnerability.

Remote SSH Daemon Supports Connections using Versions 1.33 or 1.5 of SSH Protocol

Nessus plug-in ID: 10881 and 10882

BACKGROUND / RISK

Recall that OpenSSH is an application that is designed to provide authorized users with secure access to an interactive command prompt on a remote machine. OpenSSH sends encrypted packets over a network using a special communications protocol, the SSH protocol. There are different versions of the SSH protocol; our machines support version 1.5 of the protocol. Unfortunately, there are multiple security vulnerabilities in that version.³³ These vulnerabilities include the following.

(1) SSH CRC32 COMPENSATION ATTACK DETECTOR VULNERABILITY

CVE: CAN-2001-0144

The first vulnerability is yet another example of a buffer overflow vulnerability.³⁴ By attacking vulnerable instances of the SSH software, sophisticated attackers can remotely execute arbitrary code on the system. Although such an attack is difficult to execute,³⁵ successful execution of the attack could allow an attacker to gain control of the victim machine.

(2) SSH PROTOCOL 1.5 UNAUTHORIZED SESSION KEY RECOVERY

CVE: CVE-2001-0361

This vulnerability is both complicated to explain and complicated to exploit. Without going into complex details of cryptography that are outside the scope of this paper, the vulnerability may be summarized as follows. SSH communications are encrypted. Nevertheless, a sophisticated attacker may be able to decrypt SSH connections involving vulnerable servers.³⁶ If an attacker is able to decrypt SSH connections, the attacker will be able to learn sensitive information, including the logon credentials of legitimate users, which in turn could allow the attacker to gain unauthorized access to the system.

SYSTEM JUSTIFICATION

This vulnerability finding is, in fact, accurate. Nevertheless, an upgrade will be an ambitious and time-consuming project; management decided that other current and pending projects are a higher priority. This decision was based upon several factors, including (a) other projects were deemed more critical; (b) the affected servers are not Internet-facing; (c) the affected servers are segmented from the rest of the production network; (d) the difficulty of successfully exploiting the vulnerabilities in the protocol; and (e) management has dictated that the system support version 1.5 of the SSH protocol.

OpenSSH Reverse DNS Lookup Access Control Bypass Vulnerability

CVE: CAN-2003-0386

BACKGROUND / RISK

An optional feature of the OpenSSH software is the ability to limit SSH connections to authorized source addresses. If a person tries to initiate an SSH connection from an

unauthorized address, the SSH server will block the connection. Regrettably, there is a vulnerability in this feature of OpenSSH. This vulnerability could allow an attacker to establish an SSH connection with a company server, in spite of any restrictions placed by the server on the source address of incoming connections.³⁷

SYSTEM JUSTIFICATION

This is a false positive. The vulnerability only applies to older versions of OpenSSH servers that restrict access to specific hosts based on certain hostnames or IP addresses.³⁸ Nevertheless, the `sshd_config` file has not been configured to restrict certain users to logging from certain hosts.

```
host1$ grep \@ sshd_config
host1$
```

(The command output was the same on all five hosts. I have omitted the output from the other four hosts for the sake of brevity.)

OpenSSH-portable Enabled PAM Delay Information Disclosure Vulnerability

CVE: CAN-2003-0190

BACKGROUND / RISK

The OpenSSH software authenticates users before granting them access to the system. As part of the authentication process, all users are required to identify themselves by supplying their username. Unfortunately, some versions of OpenSSH send "an error message when a user does not exist, which allows remote attackers to determine valid usernames."³⁹ Once an attacker learns valid usernames, he could then try a brute-force password guessing attack against those accounts until he successfully guesses a password and gains access to an account on the system.

SYSTEM JUSTIFICATION

While we are undeniably vulnerable to this, we do not plan to upgrade OpenSSH just to fix this vulnerability. The affected servers are internal machines that are not connected to the Internet. Indeed, they are located behind multiple layers of firewalls. Moreover, the affected servers use RSA key authentication, not password authentication. One of the primary benefits of using RSA key authentication is protection against brute-force password guessing attacks. RSA key authentication provides this protection by requiring that users *both* know a passphrase *and* have the correct RSA private key on the client machine.⁴⁰ Even if an attacker were to learn valid usernames by exploiting this vulnerability, and even if the attacker were then able to guess the passphrase through brute force, the attacker would still lack the user's private key and thus be unable to log into the user's account.

G1: Firewall configuration back up and restore procedures are not documented.**Background / Risk**

If the procedures for backing up and restoring firewall configuration are not documented, the configuration may not be properly backed up or restored. A change in personnel could mean that a firewall administrator might be unfamiliar with the procedure. Alternatively, in a crisis, even the regular administrator might skip steps because of the urgency or excitement of the situation. Having documented procedures available increases the likelihood that the backup or restoration is done correctly.

System Changes and Further Testing

Because of this audit, I ensured that these procedures were documented. Both procedures are quite simple and are summarized below.

1. Backup Procedure

From the Command Line Interface (CLI), type, "get config." Copy the output, paste to a text editor, and then save as a text file. Upload the file to <machine name and file path censored>.

2. Restore Procedure

From the CLI, copy and paste the contents of the text file into the command prompt.

© SANS Institute 2003. Author retains full rights.

List of References

"ab – Apache HTTP Server Benchmarking Tool." N.d. URL: <http://httpd.apache.org/docs-2.1/programs/ab.html> (25 July 2003).

"Apache Server Side Include Cross Site Scripting Vulnerability." 4 June 2003. URL: <http://www.securityfocus.com/bid/5847/discussion/> (25 July 2003).

"Apache Tutorial: Introduction to Server Side Includes." N.d. URL: <http://httpd.apache.org/docs/howto/ssi.html#configuringyourservertopermitssi> (25 July 2003).

"CAN-2002-0843 (under review)." Common Vulnerabilities and Exposures. 8 August 2002. URL: <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0843> (25 July 2003).

"CAN-2003-0190 (under review)." Common Vulnerabilities and Exposures. 1 April 2003. URL: <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0190> (25 July 2003).

"CAN-2003-0386 (under review)." Common Vulnerabilities and Exposures. 9 June 2003. URL: <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0386> (25 July 2003).

Cavendar, Terry. "Checkpoint Firewall Audit Work Program." January 2000. URL: <http://www.auditnet.org/docs/CheckpointFirewall.PDF> (8 July 2003).

Cheswick, William R., Steven M. Bellovin, and Aviel D. Rubin. Firewalls and Internet Security: Repelling the Wily Hacker. Second ed. Boston: Addison-Wesley, 2003.

COBIT Steering Committee and the IT Governance Institute, COBIT 3rd Edition: Control Objectives. July 2000. URL: <http://www.isaca.org/control.pdf> (5 July 2003).

Computer Incident Advisory Capability. "M-017: Multiple SSH Version 1 Vulnerabilities." 16 November 2001. URL: <http://www.ciac.org/ciac/bulletins/m-017.shtml> (25 July 2003).

"CVE-2002-0083." Common Vulnerabilities and Exposures. 25 June 2002. URL: <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0083> (25 July 2003).

"CVE-2002-0575." Common Vulnerabilities and Exposures. 2 April 2003. URL: <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0575> (25 July 2003).

Drakos, Nikos and Ross Moore. "RSA Key Authentication." 30 November 2001. URL: <http://runlinux.net/tech/ssh/node5.html> (25 July 2003).

"Firewall Review." 28 May 2002. URL: <http://www.auditnet.org/docs/Firewall%20Review%20May%2028,%202004.pdf> (8 July 2003).

Garfinkel, Simson and Gene Spafford. Practical Unix and Internet Security. Second ed. Cambridge, MA: O'Reilly & Associates, 1996.

Gill, Stephen. "Application Note: Hardening Netscreen Firewalls." Version 1.2. 18 July 2002. URL: <http://www.qorbit.net/documents/screenos-hardening-appnote.pdf> (8 July 2003).

Green, John. 7.4 Network Auditing Essentials. Version 4.1. N.p.: The SANS Institute, 2003.

Harding, Mike. "OpenSSH Remote Client Address Restriction Circumvention." Bugtraq Archive. 5 June 2003. URL: <http://www.securityfocus.com/archive/1/324016/2003-06-03/2003-06-09/0> (25 July 2003).

International Standards Organization. ISO 17799: Information Technology—Code of Practice for Information Security Management. London: BSI, 2000.

Lowder, Jeffery J. "Firewall Management and Internet Attacks." Handbook of Information Security Management 1999. Ed. Mi[k]ki Krause and Harold F. Tipton. Boca Raton, Florida: Auerbach, 1999. 199-215. Rpt. in Information Security Management Handbook. Ed. Harold F. Tipton and Mikki Krause. 4th ed. Vol. 1. Boca Raton, Florida: Auerbach, 2000. 115-131. Rpt. in Architectures for E-Business Systems: Building the Foundation for Tomorrow's Success. Ed. Sanjiv Purba. Boca Raton, Florida: Auerbach, 2001. 681-697. All citations of this source refer to the article in Tipton and Krause, 2000.

Netscreen Technologies. "Download Software." 24 July 2003. URL: http://www.netscreen.com/services/download_soft/current_releases.jsp (25 July 2003).

Harding, Mike. "OpenSSH Remote Client Address Restriction Circumvention." Bugtraq Archive. 5 June 2003. URL: <http://www.securityfocus.com/archive/1/324016/2003-06-03/2003-06-09/0> (25 July 2003).

Northcutt, Stephen. 7.2 Auditing the Perimeter. N.p.: The SANS Institute, 2003.

Northcutt, Stephen. Mark Cooper, Matt Fearnow, and Karen Frederick. Intrusion Signatures and Analysis. Boston: New Riders, 2001.

Northcutt, Stephen, Lenny Zeltser, Scott Winters, Karen Kent Frederick, and Ronald W. Ritchey. Inside Network Perimeter Security. Boston: New Riders, 2003.

"OpenSSH Challenge-Response Buffer Overflow Vulnerabilities." SecurityFocus. 27 June 2003. URL: <http://www.securityfocus.com/bid/5093/discussion/> (25 July 2003).

"OpenSSH Channel Code Off-by-One Vulnerability." SecurityFocus. 10 June 2003. URL: <http://www.securityfocus.com/bid/4241> (25 July 2003).

"OpenSSH Channel Code Off-By-One Vulnerability." Symantec DeepSight Alert Services. 10 June 2003. URL: https://alerts.symantec.com/ep/alerts-users/vuln_db.epl (spotted 24 July 24 2003).

"OpenSSH Kerberos 4 TGT/AFS Token Buffer Overflow Vulnerability." SecurityFocus. 26 April 2002. URL: <http://www.securityfocus.com/bid/4560/> (25 July 2003).

"OpenSSH Security Advisory (adv.channelalloc)." OpenBSD. 8 March 2002. URL: http://www.openbsd.org/advisories/ssh_channelalloc.txt (25 July 2003).

"OpenSSH Security Advisory (adv.token2)." OpenBSD. 21 April 2002. URL: http://www.openbsd.org/advisories/ssh_afstoken.txt (25 July 2003).

Oracle Corporation. "Buffer Overflow in Oracle Net Services for Oracle Database Server." Oracle Security Alert 54 (30 April 2003). URL: <http://otn.oracle.com/deploy/security/pdf/2003alert54.pdf> (28 July 2003).

Peltier, Thomas R. Information Security Risk Analysis. Boca Raton, Florida: Auerbach, 2001.

"PKCS #1 Version 1.5 Session Key Vulnerability." SecurityFocus. 20 September 2001. URL: <http://www.securityfocus.com/bid/2344> (25 July 2003).

Rafail, Jason. "Vulnerabilty Note VU#408419." 2 April 2002. URL: <http://www.kb.cert.org/vuls/id/408419> (26 July 2003).

"Revised OpenSSH Security Advisory." OpenBSD. 26 June 2002. URL: <http://www.openssh.com/txt/preauth.adv> (25 July 2003).

Spitzner, Lance. "Auditing Your Firewall Setup." December 12, 2000. URL: <http://www.spitzner.net/audit.html> (8 July 2003).

Strom, Dan. "Auditing the Netscreen-5 Firewall Used as a VPN Gateway." 16 August 2001. URL: http://www.giac.org/practical/Dan_Strom_GSNA.zip (8 July 2003).

Wood, Charles Cresson. Information Security Policies Made Easy. 8th ed. Houston: Pentasafe, 2001.

Zalewski, Michal. "Remote Vulnerability in SSH Daemon CRC32 Compensation Attack Detector." 8 February 2001. URL: http://razor.bindview.com/publish/advisories/adv_ssh1crc.html (25 July 2003).