# Global Information Assurance Certification Paper

# Sourcefire Intrusion Detection System Deployment
# An Auditor's Perspective

Don C. Weber
GSNA Practical Assignment v2.1
September 24, 2003

List of Tables



List of Figures

# 1 Research in Audit, Measurement Practice, and Control

## 1.1 Identify the system to be audited

### 1.1.1 What is Being Accomplished

This is an internal audit of the Sourcefire Intrusion Detection System (IDS) from an auditor's point of view. The purpose of this audit is to determine if the IDS is deployed correctly according to internal policies/procedures and the current best practices of the security community. This audit will concentrate on the Sourcefire IDS as a "commercial, off the self" (COTS) product. The Sourcefire system is currently made up of two primary components, the network sensor (sensor) and the management console (MC). Both of these components are separate devices that combine into an integrated system. The following table touches on the key pieces of these devices. This information was taken from the Sourcefire documentation[1] and/or by querying the processes on each device.

| ***Sourcefire Intrusion Detection System Devices*** | |
|---|---|
| ***Network Sensor 3020f*** | |
| Chassis | Intel SR2300 Server Chassis |
| Processor | Dual Intel Xeon |
| RAM | 2 GB |
| Command and Control Interfaces | 2 10/100/1000 Base T (RJ-45) Ethernet |
| Monitoring Interface | Dual port fiber 1000SX (LC) Ethernet |
| OS Version | Sourcefire Linux OS 2.0.2 [2] |
| Sourcefire Version | Network Sensor 3000 v2.6.0 (build 65)[3] |
| Kernel Version | 2.4 |
| Apache | Server version: Apache/1.3.26 (Unix) |
| MySQL | Ver 11.18 Distrib 3.23.51, for slackware-linux-gnu (i386) |
| Snort | Version 2.0.0 (Build 71) |
| Barnyard | Version 0.3 (Build 13) |
| | |
| ***Management Console*** | |
| Chassis | Intel SR2200 2U |
| Processor | Dual Pentium 3 |
| RAM | 1 GB |
| Command and Control Interfaces | 2 10/100 Base T (RJ-45) Ethernet |
| OS Version | Sourcefire Linux OS 2.0.2[2] |
| Sourcefire Version | Management Console v2.6.0 (build 65)[3] |
| Kernel Version | 2.4 |

[1] "Sourcefire Products" – URL: http://www.sourcefire.com/products/products.htm – 07/08/2003
[2] The command "cat /proc/version" returns "Linux version 2.4.18sf (mbrannig@ender.Sourcefire.com) (gcc version 2.96 20000731 (Red Hat Linus 7.3 2.96-112)) #3 SMP Wed Nov 13 15:12:49 EST 2002"
[3] This version was taken from the information from the MOTD display when logging in via SSH. The network sensor, although listed as 3000, is considered a 3020f because of its dual port fiber interface.

| Sourcefire Intrusion Detection System Devices | |
|---|---|
| Apache | Server version: Apache/1.3.26 (Unix) |
| MySQL | Ver 11.18 Distrib 3.23.51, for slackware-linux-gnu (i386) |
| Snort | Version 2.0.0 (Build 71) |

**Table 1 Sourcefire IDS Device Configuration**

### 1.1.2 Sourcefire IDS Research

As one can tell from analyzing Table 1, the Sourcefire IDS is a commercial version of the freely available Snort intrusion detection software. The sensors' primary responsibilities are to watch their specific portion of the network for suspicious activity and log it. The MC is a central management, auditing, and data storage point for a large number of sensors (30 to 50 depending on traffic).

Administrative actions are controlled, primarily, through the secure web interface. These configurations are stored within the database on each system. Networking is configured separately on each box. Users can be created and limited to specific functions. Access can be limited from specific hosts. The number of specific events stored within the database is configurable. Sensors can be remotely activated and deactivated and their data configured for storage locally or centrally. When utilized, the MC is designed to provide the following for its sensors:

- Manage the snort configurations
- Create, tune, build, and push rule sets
- Place sensors with similar tasks into groups
- Provide a central location to store, view, analyze, and produce detailed reports on alerts
- Monitor processes, system logs, and disk usage

The sensors have the ability to log alerts directly to a separate central log server via SYSLOG and SNMP. Sensors are also configured to report on performance issues.

### 1.1.3 Network Research

The network in which this IDS is deployed has several functions. Information flows from the outside network through the border routers. These routers, through a series of access control lists (ACL), are configured to only allow known hosts to perform allowed tasks. The traffic is then passed to one of two load balancers, configured as a fail-over pair, to the firewalls where the traffic is again screened and allowed, denied, or proxied. Once through the firewalls, the web traffic is sent to another load balancer. This load balancer performs the additional function of decrypting the web traffic to reduce the load on the web servers. Thus the traffic comes into the load balancer on port 443 (encrypted) and is passed on to the web servers via port 80 (unencrypted). Information then travels in the opposite direction in the same manner, reversed. All other traffic,

from the interior network to the web servers, is passed through the load balancer to the web servers normally.

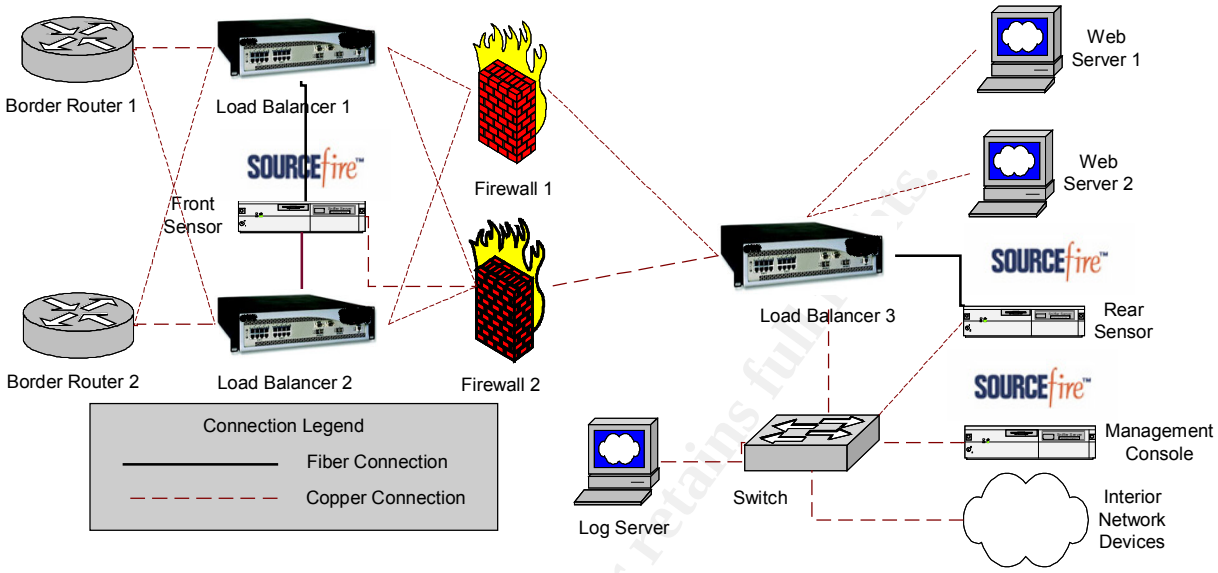



**Figure 1 Network Setup**

A typical IDS system is set up so that the sensors are placed in strategic locations throughout the network according to specific policy and procedure. These sensors are managed, when possible, by a centralized management console. The Sourcefire IDS setup within this network is no different. Although the network configuration must be accomplished on the actual sensor, the MC controls the snort configuration, the rules, and is the central alert and reporting mechanism for the IDS.

Within this network, the key locations are the load balancers and the sensors are set up to monitor traffic mirrored by these devices. More specifically, the load balancers between the border routers and the firewall are set up so that all traffic, to and from anywhere, is mirrored to the sensor (Front Sensor). The load balancer that is deployed between the firewall and the web servers is set up to decrypt the web traffic and then mirror this decrypted traffic, and all other traffic destined for the web servers, to the sensor (Rear Sensor) connected to it. The Front Sensor is configured to utilize both of its fiber ports, in stealth mode[4], to receive all network traffic mirrored by the load balancers. Only one load balancer will be processing network traffic at any one time, as they are set as a fail-over pair. This is also connected to the inside network by passing traffic through the firewall and back to the MC via one of its RJ-45 ports. The Rear Sensor is connected to Load Balancer 3 on one of its fiber ports and it will connect to the switch with one of its RJ-45 ports. Load Balancer 3 is configured to mirror the

[4] Stealth mode a setting for an interface that allows it to monitor network traffic in promiscuous mode without being assigned an IP address. This interface is virtually invisible to the rest of the network. This is the default setting for Sourcefire Network Sensors.

decrypted and regular traffic, going to and from the web servers, to the sensor. Both sensors are connected to the MC, technically, through the switch. The MC is connected to the switch through one of its RJ-45 ports.

In order for the Front Sensor to contact the MC, the firewall and Load Balancer 2 must be configured to allow traffic to travel between the two. The only connections that are needed are HTTPS (TCP/port 443), SSH (TCP/port 22), SYSLOG (UDP/port 514), NTP (UDP/port 123) and a Sourcefire management connection (TCP/port 5555). Connections from the interior network will originate only from the MC and the log server. The MC must connect to the sensor for obvious management reasons but the log server acts as an auditing, NTP, and configuration host where the administrators can access, via SSH and HTTPS, the sensor directly for maintenance or to conduct research on the Front Sensor itself.

One other important item for this network: management specifically denied the use of scanning and vulnerability assessment tools. The importance of these tools to the auditing process was explained but unfortunately approval for these tools was not available at the time the audit was performed.

## Documentation Research

Locating company documentation can be a challenge for any administrator. Fortunately, this was not the case and, with administrative help, this information was fairly easy to find. The following represents the most important company policies and procedures that pertain to the implementation of the IDS within this environment. This information will be the basis for the checklists.

- All documentation will be controlled according to company policies.
- Changes, updates, and corrections to documents will be logged at the beginning of each document.
- Installation and configuration will be completely documented in a highly granular, step-by-step, format.
- Specific system maintenance and operating procedures will be documented.
- An incident response plan will be devised and documented.
- The official company security banner must be display prior to any system access.
- User and administrator passwords will adhere to the company strong password policy.
- All system events and alerts will be centrally logged.
- All encrypted web traffic must be decrypted before reaching the web servers and monitored for intrusions.
- Physical access to the environment must be controlled and audited.
- Physical access to systems must be controlled and audited.
- Software and hardware licenses will be monitored and stored when necessary.
- Software and hardware upgrades and patches will only be accepted from authorized sources.
- The use of any security tools is not authorized by company security.

Although not specifically covered within the company documentation, the network security team manager stated that the IDS would be utilized according a combination of the industry best practices and company policy for the environment in which it is being deployed.

**Evaluate the risk to the system**

In the following table we will evaluate inherent risks within this system within the company infrastructure. These will be determined according to company policies and procedures as well as industry current practices.

| Category | Vulnerability | Consequence[5] | Likelihood[4] | System Threat[4] | Risk Risk | Audit Strategy |
|---|---|---|---|---|---|---|
| Documentation | Badly written, unimplemented, and missing documentation. | High | Medium | Medium | Documentation problems can lead to some very serious problems. These include, but are not limited to:<br>• Poorly configured systems<br>• Missed attacks and/or reconnaissance efforts<br>• Damaged evidence<br>• Vulnerable systems<br>• Late or no incident response<br>• Legal repercussions | • Obtain and read documentation to determine current company policies and procedures and involve the IDS.<br>• Interview key personnel responsible for writing, maintaining, and utilizing these documents. |
| Physical | Physical access to systems. | High | Medium | Medium | Unauthorized physical access to network and individual systems could lead to compromise that may or may not be detected. | • Physically observe all techniques used to limit access to the network and individual systems. |
| | Lack of safety devices. | High | Medium | Medium | Buildings that lack required by law are in violation of safety standards and can be closed until the building is brought up to code. | • Physically observe safety devices present within the working area. |
| Network | Security system with auditing and performance tools. | Medium | Low | Low | Administrators generally have at least one system that contains tools that are utilized to analyze and test a network or system. Unauthorized access to this system could lead to the compromise of the entire network. | • Interview system and security administrators to determine location and security of this system(s). |
| | Poorly configured network devices. | Medium | High | Medium | Network devices that are not configured to account for the IDS can, in effect, blind the monitoring system by not passing it the network traffic or by blocking traffic altogether. | • Check Spans and/or Mirrors, on the network devices, to ensure that the proper information is getting passed to the sensor.<br>• Insure that devices not intended to filter traffic are, in fact, not filtering traffic<br>• Check firewall proxies and filtering rules related to the IDS system |

[5] "GSNA Study Guide" by SANS personnel and associates – URL: http://www.giac.org/gsna_study_guide_v11.pdf, 08/13/2003

| Category | Vulnerability | Consequence[5] | Likelihood[4] | System Threat[4] | Risk | Audit Strategy |
|---|---|---|---|---|---|---|
| | Unauthorized access to host capable of accessing the IDS devices | High | Medium | Medium | Any unauthorized access to the IDS devices means that the whole system is not trusted and could ultimately result in the redeployment of the whole system. This would lead to down time of the monitoring system and possibly undetected attacks and/or reconnaissance efforts. | • Insure that access to systems capable of communicating with the IDS is controlled according to company policies and procedures.<br>• Check IDS for strong password implementation. |
| | Poorly configured central logging host | High | Medium | Medium | Central logging hosts that are required to perform extra actions for alerts that are considered priority may not function properly if they are not configured properly. | • Determine which alerts are considered priority and determine if predetermined extra actions are followed for each of these alerts. |
| Sourcefire IDS | Sensor or MC is incorrectly configured. | High | High | High | If a sensor or the management console is not configured correctly it can lead to several problems:<br>• Missed attacks and/or reconnaissance efforts<br>• Damaged evidence<br>• Vulnerable systems<br>• Legal repercussions | • Insure that the MC and Sensor are configured according to manufacturer instructions, community best practices, and company policy and procedure by manually checking configurable settings on each device. |
| | Unchanged default user id and password for access to the sensor or MC. | High | Medium | Medium | "Some systems come with software installed that has password protection, but with passwords that are set at the factory. These default passwords are widely available online; if you leave a service running with a password which was set by the vendor, you may be leaving yourself open to the first attacker who comes along with a default password list."[6] | • Check that the default user id and password has been changed. |

[6] "UW Security Site--Protect your file server" – URL: http://www.washington.edu/computing/security/servers.html, 07/15/2003

| Category | Vulnerability | Consequence[5] | Likelihood[4] | System Threat[4] | Risk Risk | Audit Strategy |
|---|---|---|---|---|---|---|
| | User connections do not display company approved login banner before logging in | Medium | Low | Low | Company banners are used as a preventive measure to inform would-be intruders and everyday users that legal action can and will be taken if there is unauthorized or malicious activity on that system. | • Check that each machine has the company login banner displayed according to policy and procedure. |
| | Operating systems and software with vulnerabilities. | High | Medium | Medium | Operating systems and software that have not been upgraded are possible targets for malicious activity. A machine that has not been upgraded or patched has the potential to be denied, exploited, controlled, and/or used by malicious hackers to compromise other systems and company information. | • Check that each machine has been updated to the latest vender version. |
| | Poorly configured and undocumented local rules | High | High | High | Rules that have not been properly constructed can lead to the generation of a large quantity of false positive or negative alerts. These rules can hamper the systems ability to monitor network traffic efficiently. | • Check the local rules are properly constructed and documented according to company policies and procedures. |
| | Improper IDS tuning | High | High | High | Sourcefire, via snort, has many configurable variable and network settings that, if set incorrectly, can lead to missed attacks and/or reconnaissance efforts. | • Check that all variables are set correctly according to the network and application configurations. |
| | Improper system and alert logging | High | Medium | Medium | If system and snort alerts are not centrally logged correctly then incident investigation and reporting can become difficult or impossible. Additionally, valuable evidence of attacks and/or reconnaissance could be lost. | • Check the logging settings on the sensors and the MC. Also check that the central log system is receiving alert and reporting them according to company policies and procedures. |

| Category | Vulnerability | Consequence[5] | Likelihood[4] | System Threat[4] | Risk Risk | Audit Strategy |
|---|---|---|---|---|---|---|
| | Undocumented changes to system configurations and/or rule sets | High | High | High | Undocumented changes to any system can lead to confusion and, ultimately, cause the device to be configured incorrectly and thereby allow attacks and/or reconnaissance to pass without alerting. System changes can also lead to vulnerable systems that can possibly be exploited. | • Insure that there is a change log for each system and that system changes are noted according to company policies and procedures. |
| | Insider malicious activity | High | Medium | Medium | Malicious insiders that have access to highly sensitive machines will definitely be interested in compromising the IDS for information purposes. Since the actual IDS devices are generally not directly logged into, these systems make great places to hide just about anything. | • Check that all logins to the IDS devices are audited and centrally logged according to company policies and procedure. |
| General | Remote access that displays user names and passwords | High | Medium | Medium | Certain applications allow users to traverse the network by logging into machines over an unencrypted channel. This exposes user names and passwords to anybody that is monitoring the network. Malicious users can use this information to attempt to gain access to different hosts with this information. | • Insure that only secure services will accept connections to the IDS device by checking running processes and attempting to connect with well-known services such as TELNET and rlogin. |
| | A malicious intruder changes files on a system to cover any changes that have been implemented and to insure access to the controlled device | High | Low | Low | When a skilled malicious intruder has compromised a system, one of the first tasks that is usually performed is the replacement of key process, files, and applications. These changes cover the intruder's tracks and can insure that access to the system remains open and covert. | • Check that file integrity software has been deployed and configured to monitor the IDS system. |

| Category | Vulnerability | Consequence[5] | Likelihood[4] | System Risk Threat[4] | Risk | Audit Strategy |
|---|---|---|---|---|---|---|
| | Weak passwords and improper password practices | High | High | High | Human beings are notoriously lazy. Everyday processes quickly become mundane and even annoying. Passwords and password policies are no exception. When strong passwords are not utilized and password policies are not adhered to it becomes more probable that this system of protection can be compromised. | • Insure that proper password policies are employed and verify they are utilized. |

**Table 2 System Risk**

## 1.2 What is the current state of practice

### 1.2.1 Documentation

Process documentation is an important aspect of any project, and intrusion detection is no exception. Most of the research into documentation produced similar results. These can be narrowed down to specific categories.

- Product Configuration – Everything about the configuration of a specific product should be documented. This insures that group configurations are consistent and individual configurations are known. Configuration documentation also insures that systems can be reinstalled, upgraded, or replaced entirely, properly, by any individual authorized to do so. [7]
- Vendor Documentation – Nobody knows the product better than the manufacturer (in most cases). This document is necessary to troubleshoot any problems that arise or for personnel to brush up on the product.[4]
- Other Product and Application Documentation – Very few products are deployed alone. They interoperate with other systems and applications within the company environment. How these products act can directly influence other products configuration and usability. Some of the most important documentation concerns system administration in general. [4]
- Network Configuration – All networks are planned (hopefully) and there should be documentation explaining this plan. Computer hardware, wiring, and application deployment should all be described in the network diagram. An up to date version of this diagram should be available to all system administrators.[8]

### 1.2.2 Physical Security

Common sense and general industry standards dictate that all systems must take into consideration the physical security of these systems. Access control to all aspects of a device must be taken into consideration if that device is to be trusted within the company infrastructure.

- Access to computer buildings or rooms, by company personnel or visitors, should be monitored, logged, and audited.[9]
- Server security features (rack and servers locks) should be utilized and device access controlled, logged, and audited.[10]
- Physical safety considerations should be examined and implemented accordingly.[11]

---

[7] "National Institute of Standards and Technology: Computer Security Plans References for High-Risk Review" – URL: http://csrc.nist.gov/cseat/cseat_computer_security_plans_ref_hr.html, 07/08/2003

[8] "Virginia Alliance Standard Compliance Checklist" – URL: http://www.vascan.org/checklist/physical_security_check.html, 07/08/2003

[9] "National Institute of Standards and Technology: Physical Security References for High-Risk Review" – URL: http://csrc.nist.gov/cseat/cseat_physical_security_ref_hr.html, 07/08/2003

[10] Personal experience.

[11] "System Security Plan Development Assistance Guide" by SANS Institute 2003 - URL: http://www.sans.org/rr/special/NIALV/kessler.pdf, 07/08/2003

- Mobile and portable systems should be controlled and protected from unauthorized access.[6]

The Occupational and Safety Health Act[12] (OSHA) describes employer requirements within a working environment. Local, county, and state laws describe other safety considerations.

### 1.2.3 Sourcefire Configuration

The Sourcefire IDS is configured through a secure html-based graphical user interface (GUI) on the sensor and the MC. The basic configuration for networking, access, rules, and database control is described within the documentation, supplied by the vendor, located on each box in PDF format. Rules are fine tuned in the same manner that regular snort configurations except, within Sourcefire's system, it is all configured through the GUI. Additional information on tuning snort can be found at the documentation center of the website.[13] Much of the tuning information will come from company policies and procedures as well as the network configuration.

### 1.2.4 Network Devices

Certain devices within this network are considered security devices. These include firewalls, routers, and IDS. The load balancers and switches, however, are not security devices and should not be configured as such. The specific job of these devices should be to pass all traffic in the manner that it receives it. If the device is configured to drop or deny certain traffic then it is possible that the IDS will not detect, and alert on, certain reconnaissance efforts.[7] As these devices will also be supplying the network traffic to the sensors they must be configure correctly according to manufacturer specifics.
Another network consideration is a centralized logging structure. Logging plays an important role in prevention and detection throughout the system. Several key issues that the industry considers important in this area include:

- Perform system access auditing[14]
- Distribute log files to a centralized log server[10]
- Synchronize network systems[7]
- Employ log monitoring and alerting software[10]

### 1.2.5 General Security Considerations

Every system should take into consideration several, general, security issues. These can be gleaned from just about any security checklist and applying common sense. Unless otherwise noted the following are considerations taken from the well known security document, "*UNIX Security Checklist v2.0*"[13] published by the Australian Computer Emergency Response Team (AusCERT) and the CERT® Coordination Center (CERT/CC).

---

[12] "U.S. Department of Labor: Occupational Safety & Health Administration" – URL: http://www.osha.gov/oshinfo/mission.html, 08/13/2003
[13] Snort Documentation – URL: http://www.snort.org/docs/, 07/08/2003
[14] "The Australian Computer Emergency Response Team (AusCERT) and the CERT® Coordination Center (CERT/CC): UNIX Security Checklist v2.0" – URL: http://www.cert.org/tech_tips/usc20_full.html#1.0, 07/09/2003

- Insure that the product is up to date with current vender versions and patches
- Strong password implementation and proper password practices
- Utilize secure remote login applications
- Deploy file integrity systems

## 2 Create an Audit Checklist

The following explain the purpose of each field in the checklists.

- The “List” column is an identifier within the testing category.
- The “Objective/Test Steps” column describes the objective of the test and lists the actual steps that will be performed.
- The “Expected Results” column demonstrates the proper results, from the test steps, in order to prove compliance.
- The “Type” column describes the testing methods that will be utilized for a particular test case. The following table describes the different testing methods that will be used during this audit.

| Testing Methods | | |
|---|---|---|
| ***Name*** | ***Description*** | ***Symbol*** |
| Subjective | Subjective evaluation refers to opinions obtained through inquiry and observation.[15] | S |
| Objective | Objective evaluation relieves on opinions and observations that are also augmented by supporting facts and evidence. | O |

**Table 3 Checklist Testing Methods**

- The description within the “Risk” column demonstrates the possible results of noncompliance to the test steps.
- The numbers within the “Reference” column of each checklist refer to the list number of the reference in Section 8.

The following checklists were created while considering the company’s policies and procedures and the community best practices. The most extensive checklist will be the Sourcefire Configuration Checklist due to the fact that this is the major focus of this audit. However, there are always other considerations for any IDS deployment. The extra checklists identify the important subjects but they have been limited to the most important for this company while staying as close as possible to the best practices within the IDS community.

[15] “GSNA Study Guide” by SANS.org – URL: http://www.giac.org/gsna_study_guide_v11.pdf

## 2.1 Documentation Checklist

| Documentation Checklist | | | | | |
|---|---|---|---|---|---|
| **List** | **Objective/Test Steps** | **Expected Results/Success Criteria** | **Type** | **Risk** | **Reference** |
| 1. | Objective: Insure that the IDS has configuration and change log documentation associated with each sensor and the MC.<br><br>Test Steps:<br>• Obtain a copy of the IDS configuration document.<br>• Compare the documentation with the company policies and procedures.<br>• Obtain a copy of the change logs for each IDS sensor and MC. | The configuration documentation should cover the complete installation and configuration procedures for all IDS devices. These documents should adhere to company policies and procedures. Each device should have a corresponding change log.<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | IDS devices that are not configured correctly can potentially not alert on suspicious traffic. | 6 |
| 2. | Objective: Insure that vendor supplied documentation for IDS devices are current, available, and stored<br>Test Steps:<br>• Determine where the documentation should be located.<br>• Check for the documentation and note versions.<br>• Verify that versions are current with device type and current manufacturer version of documentation. | There should be documentation present and controlled for each different IDS sensor and MC. The documentation should be concurrent with the device and it should be the latest documentation available from the manufacturer.<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | Correct implementation of any device is necessary so that the device can function properly. Not all devices handle procedures by the same methods. Manufacturer information should be available for reference during configuration and administration. | 6 |
| 3. | Objective: Insure that there is documentation that outlines the incident response procedures.<br><br>Test Steps:<br>• Obtain and review the documentation that outlines the incident response procedures.<br>• Interview the administrators that are responsible for monitoring the network for suspicious activity. | The incident response document should fully and clearly outline the steps that should be taken to identify a possible threat. Each administrator should be familiar with this document and know its location for quick reference.<br><br>☐ Pass<br>☐ Fail<br>Notes: | S | Without a documented incident response plan the complete intrusion detection system is worthless. Administrators that are not able to act upon suspicious activity in a timely and methodical manner put the whole network at risk. Audit trails and evidence could be lost in this situation and malicious intruders will either not be detected or they might not be prosecutable. | 8 |
| 4. | Objective: Insure application documentation is present and accessible. | There should be documentation present for each different application running within the network. The | S | Understanding the applications within a network will help the | 6 |

| Documentation Checklist | | | | | |
|---|---|---|---|---|---|
| **List** | **Objective/Test Steps** | **Expected Results/Success Criteria** | **Type** | **Risk** | **Reference** |
| | Test Steps:<br>• Determine common applications utilized on the network.<br>• Determine where the documentation should be located.<br>• Check for the documentation and note versions.<br>• Verify that versions are current with device type and current manufacturer version of documentation. | documentation should be concurrent with the application and it should be the latest documentation available from the manufacturer.<br><br>☐ Pass<br>☐ Fail<br>Notes: | | administrator determine the proper settings and location for the IDS. It will also help during traffic analysis to know and be able to research how certain applications act within the network. This in turn will help separate normal traffic from suspicious traffic so that the administrator can tune the IDS efficiently. | |
| 5. | Objective: Insure that there is an up-to-date and controlled network diagram.<br>Test Steps:<br>• Determine where the network diagram should be located<br>• Check for the diagram.<br>• Confirm that the diagram is current by checking it against the physical layout of the network. | The document should be controlled, easy to find, and up-to-date with the current network configuration.<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | Networks are dynamic environments by nature. If the layout is not accurate then the IDS sensors may be deployed in poor locations. This could cause rules to fail, which, in turn, would mean that the sensor would not alert to suspicious traffic. | 6, 7 |

**Table 4 Documentation Checklist**

## 2.2 Physical Security Checklist

| Physical Security Checklist | | | | | |
|---|---|---|---|---|---|
| **List** | **Objective/Test Steps** | **Expected Results/Success Criteria** | **Type** | **Risk** | **Reference** |
| 1. | Objective: Confirm that access to the facilities housing the intrusion detection system is controlled.<br><br>Test Steps:<br>Start outside the building and walk to the location of note security measures for | • Outside building<br>❑ Building access monitored.<br>❑ Access limited by key card.<br>❑ Key cards are centrally controlled.<br>• Outside server room<br>❑ Server room access monitored.<br>❑ All entrances are locked. | O | Uncontrolled access to servers and their storage areas can potentially lead to compromised servers. These types of compromises can go undetected for long periods of time. Intruders can install modems, unplug or | 7, 14 |

| List | Objective/Test Steps | Physical Security Checklist<br>Expected Results/Success Criteria | Type | Risk | Reference |
|---|---|---|---|---|---|
| | outside the building, outside the server room, outside the server rack, and inside the server rack. | ❑ Access limited by key card.<br>• Outside server rack<br>❑ Server rack monitored by access logbook that is located with the server rack.<br>❑ Access limited by rack key.<br>❑ Rack keys are centrally controlled.<br>• Inside server rack<br>❑ Server access monitored by access logbook that is located with the server.<br>❑ Access to drives, control buttons, and hardware is limited by server key.<br>❑ Rack keys are centrally controlled.<br><br>☐ Pass<br>☐ Fail<br>Notes: | | damage servers/devices, or login as an administrator locally (no documented user logins to trace). | |
| 2. | Objective: Confirm that proper safety precautions have been considered within the server room.<br><br>Test Steps:<br>Insure that the items in the checklist are available, accessible, and in working condition. | ❑ Smoke/Fire detectors<br>❑ Fire alarms<br>❑ Fire extinguishers<br>❑ Exit maps<br>❑ Fire exits<br>❑ Overhead exit signs<br>❑ First aid kit<br>❑ Telephone<br>❑ Power shutdown switch<br>❑ Grounding straps<br>❑ Hearing protection<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | The following is one federal law on the subject of workplace safety.<br><br>Occupational and Safety Health Act (OSHA)[16]<br>Sec. 654. - Duties of employers and employees<br>(a) Each employer -<br>(1) Shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees;<br>(2) Shall comply with occupational safety and health standards promulgated under this chapter.<br>(b) Each employee shall comply | 13, 14 |

[16] "US Code Collection" supplied by Legal Information Institute – URL: http://www4.law.cornell.edu/uscode/29/654.html, 07/14/2003

| Physical Security Checklist | | | | | |
|---|---|---|---|---|---|
| **List** | **Objective/Test Steps** | **Expected Results/Success Criteria** | **Type** | **Risk** | **Reference** |
| | | | | with occupational safety and health standards and all rules, regulations, and orders issued pursuant to this chapter which are applicable to his own actions and conduct | |

**Table 5 Physical Security Checklist**

## 2.3 Network Devices Checklist

| Network Devices Checklist | | | | | |
|---|---|---|---|---|---|
| **List** | **Objective/Test Steps** | **Expected Results/Success Criteria** | **Type** | **Risk** | **Reference** |
| 1. | Objective: Determine if the IDS sensors are properly deployed within the environment.<br><br>Test Steps:<br>• Note each network segment that needs to be monitored according to company policy and procedure.<br>• Note the location of the IDS sensor within the network. | One or more sensors should be located on each segment of the network that needs to be monitored.<br><br>☐ Pass<br>☐ Fail<br>Notes: | S | If there is no sensor on a portion of the network, malicious activity will go undetected within that portion of the network. | 16, 17 |
| 2. | Objective: To determine if the IDS sensors and MC are physically located in the proper locations and wired correctly.<br><br>Test Steps:<br>• Obtain the network diagram.<br>• Locate the IDS sensors and the MC within the diagram and note their wiring configuration.<br>• Locate the actual sensors and the MC and insure that the IDS sensors are | The sensors and the MC should be placed in the location notated by the company documentation. Each device should be connected to the correct host.<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | Human mistakes in configuration can happen. Persons with malicious intent could also unplug or purposely plug cables into the wrong locations. When this happens malicious activity can go undetected. | 16, 17 |

| List | Objective/Test Steps | Expected Results/Success Criteria | Type | Risk | Reference |
|---|---|---|---|---|---|
| | **Network Devices Checklist** | | | | |
| | connected to the network as depicted in the network diagram. | | | | |
| 3. | Objective: Insure that the load balancers are configured to mirror all traffic to the IDS sensor that is assigned that portion of the network.<br><br>Test Steps: Have the administrator perform the following steps.<br>• Note from the network diagram the port that the IDS sensor should be connected to.<br>• Note from the network diagram all ports on the load balancer that should be mirrored to the IDS sensor<br>• Log into the load balancer with an account with privileged status on the load balancer.<br>• Have the administrator list all mirrors or SPANs on the load balancer according to the manufacturer. Note the configuration of these mirrors or SPANs. | This configuration should be consistent with the network diagram and the physical layout. All ports to be monitored my the IDS sensor must be mirrored or SPANed.<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | If the load balancers are not configured correctly then the traffic passing through the device might not get passed to the IDS sensor and thus reconnaissance and malicious activity will not be detected. | 17 |
| 4. | Objective: Insure that the load balancers are not configured to block any traffic.<br><br>Test Steps: Have the administrator perform the following steps.<br>• Log into the load balancer with an account with privileged status on the load balancer.<br>• Have the administrator list all of the filtering rules utilized by the load balancer according to the manufacturer. | The load balancer should not be configured to block or filter any traffic flowing through it.<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | If the load balancers are configured to drop traffic then it is possible for reconnaissance efforts and attempted malicious activity to be dropped undetected by the IDS sensor. | Personal Experience |
| 5. | Objective: Insure that access to all mobile and portable systems is controlled and documented.<br><br>Test Steps: | These systems should be controlled and there should be an access log. Systems may or may not have been used recently, or if the log was just created there might not be any entries. If systems are on floor the responsible individual should have | O | Portable stations enable personnel to directly access systems. Mobile systems may contain security tools that will aid a malicious intruder's reconnaissance or destructive | 14 |

| Network Devices Checklist | | | | | |
|---|---|---|---|---|---|
| **List** | **Objective/Test Steps** | **Expected Results/Success Criteria** | **Type** | **Risk** | **Reference** |
| | • Locate the list of all mobile and portable systems.<br>• Locate storage space for the systems.<br>• Locate the access roster and insure that all mobile and portable systems are listed.<br>• Check server room for any mobile or portable systems and check logs for entries. | line of site with the device..<br><br>☐ Pass<br>☐ Fail<br>Notes: | | intentions. | |
| 6. | Objective: Insure that administration host, capable of accessing the IDS devices, is controlled and secure.<br><br>Test Steps:<br>• Locate administration server in network diagram.<br>• Have the administrator log into this server as root via:<br>❑ telnet<br>❑ rlogin<br>❑ ssh<br>• Have the administrator log into this server with a user account that has access to this server via:<br>❑ telnet<br>❑ rlogin<br>❑ ssh | Access to the server should only be allowed over ssh as a non-root user. All other attempts should fail or time out.<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | Root logins make audit trails more difficult to follow. Configuration changes that can only be performed by root cannot be tracked back to a specific user account if they are allowed to login with a root account.<br>Additionally, if telnet or rlogin is used to access the administration server, all information is passed in the clear. If a user logins into the administration server over telnet and then makes a secure connection to the IDS, a portion of this traffic will still appear on the network in plain text and can be utilized to gain access to the IDS or other network devices. | Personal Experience |

**Table 6 Network Devices Checklist**

## 2.4 Sourcefire Configuration Checklist

| Sourcefire Configuration Checklist |
|---|

| List | Objective/Test Steps | Expected Results/Success Criteria | Type | Risk | Reference |
|---|---|---|---|---|---|
| 1. | Objective: Insure that the Sourcefire device is up-to-date with all upgrades, patches, and rule sets.<br><br>Test Steps:<br>• Log into the Sourcefire Support site[17] and record the version numbers for the latest Sourcefire OS for the MC and the versions of the sensors. Download the latest rules updates.<br>• Have the administrator connect to the IDS device via ssh.<br>• Check OS version<br>❑ Have the administrator log into the device via SSH.<br>❑ Run 'cat /etc/sf/sf-version'<br>❑ Note returned string<br>• Have the administrator connect to the IDS device via the secure web interface (GUI).<br>❑ Select RULES.<br>❑ Select Search.(Figure 27 Select Rules - Search)<br>❑ Pick several of the new rules Snort ID (listed as "sid:#" with the rule) numbers and enter them as a comma separated list in the text box. (Figure 28 Select Multiple Rules)<br>❑ Compare the rules that are returned to the new rules.<br>• Check the change log for all updates.<br>• Repeat for each device.<br>• If versions are not current check to see if the new version are in the evaluation process.<br>• Have the administrator explain any differences. | The versions available from the vendor (Sourcefire) should be the same as the versions deployed on the IDS devices. If versions are not current then they should be in the evaluation process. If the current versions are not in the evaluation process then it must be documented as to why the current versions are not being utilized within the environment.<br><br>☐ Pass<br>☐ Fail<br>Notes: | S | Systems that are not updated can be vulnerable to attack. Venders often post vulnerabilities on the support sites along with the patches to fix them. There are many tools created to check for and exploit vulnerable systems. Snort rules are also updated to detected attempts to exploit systems. Not updating the rule sets could lead to missed reconnaissance and malicious attacks. | 10 |
| 2. | Objective: Determine if the company legal login banner is displayed prior to | Banner should be displayed before the user is prompted to enter a user name or password. Each | O | "Network banners are electronic messages that provide notice of | 19 |

[17] "Sourcefire Support Login" – URL: https://support.sourcefire.com, 07/16/2003

| List | Objective/Test Steps | Expected Results/Success Criteria | Type | Risk | Reference |
|---|---|---|---|---|---|
| | attempted login.<br><br>Test Steps:<br>• Obtain a copy of the company legal login banner.<br>• Have the administrator connect to the MC via the GUI.<br>❑ Note when the banner appears.<br>❑ Compare banner to the copy.<br>• Have the administrator connect to the MC via the SSH interface.<br>❑ Note when the banner appears.<br>❑ Compare banner to the copy.<br>• Repeat for each sensor. | banner should be worded exactly the same as the company copy.<br><br>☐ Pass<br>☐ Fail<br>Notes: | | legal rights to users of computer networks. From a legal standpoint, banners have four primary functions. First, banners may be used to generate consent to real-time monitoring under Title III. Second, banners may be used to generate consent to the retrieval of stored files and records pursuant to ECPA. Third, in the case of government networks, banners may eliminate any Fourth Amendment "reasonable expectation of privacy" that government employees or other users might otherwise retain in their use of the government's network under O'Connor v. Ortega, 480 U.S. 709 (1987). Fourth, in the case of a non-government network, banners may establish a system administrator's "common authority" to consent to a law enforcement search pursuant to United States v. Matlock, 415 U.S. 164 (1974)."[18] | |
| 3. | Objective: Insure that the default root password was changed after installation.<br><br>Test Steps:<br>• Have the administrator connect a mobile station directly to the MC.<br>• Enter the password "Opensnort".<br>• Repeat for ssh.<br>• Repeat for GUI.<br>• Repeat for each IDS device. | Logging should fail on all sensors and the MC.<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | Malicious intruders usually attempt default passwords as they are widely known, easy to find with minimal research, and often times not changed. If an intruder can gain access to an IDS sensor or MC they will be able to monitor the entire network. The intruder can also configure the system with backdoors to provide access and/or distribute information remotely. | 3, 18 |

[18] "APPENDIX A: Sample Network Banner Language" by U.S. Department of Justice - Criminal Division, (Computer Crime & Intellectual Property Section) – URL: http://www.usdoj.gov/criminal/cybercrime/s&sappendix2002.htm, 07/17/2003

| List | Objective/Test Steps | Expected Results/Success Criteria | Type | Risk | Reference |
|---|---|---|---|---|---|
| | | **Sourcefire Configuration Checklist** | | | |
| 4. | Objective: Check that the Sourcefire license has been copied and stored in a secure location.<br>Test Steps:<br>• Have the administrator print out a copy of the stored license for each IDS device.<br>• Have the administrator log into the MC via the GUI.<br>❑ Select ADMIN.<br>❑ Select License.<br>• Compare the licenses to insure that they are consistent with the documented licenses. | The licenses for each IDS device should be stored in a location that is accessible by an administrator. These licenses should be identical to the licenses that are stored locally on the IDS device.<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | If an IDS device has to be restored and the license for that device is lost then the administrator must contact the vendor for a new license. This will increase down time for the device that could result in missed reconnaissance and malicious attack detection. | Personal Experience |
| 5. | Objective: Insure that only authorized users have accounts on the IDS devices.[19]<br><br>Test Steps:<br>• Have the administrator connect to the MC via the GUI.<br>❑ Select ADMIN<br>❑ Select Users<br>❑ Note each user displayed and not that user's permissions.<br>• Have the administrator connect to the MC via the ssh.<br>❑ cat /etc/passwd<br>❑ Note all users that do not have a shell (last item of the colon delimited list) of /bin/nologin. | There should be no extra user accounts on any of the devices. All passwords should adhere to the company policy.<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | Most malicious activity is a product of disgruntled employees or employees that are no longer with the specific company. Old, undeleted, accounts provide easy access to devices that these individuals should no longer be allowed access. | 21 |
| 6. | Objective: Insure that all user passwords adhere to the strong password company policy.<br><br>Test Steps: | As this company does not allow password-cracking utilities within the environment the password application process must be evaluated instead of the actual use passwords. The password received should match the strong password criteria listed in | O | Weak passwords also provide easy access to malicious intruders. When left uncontrolled, employees will often use names, birth dates, and/or dictionary words as their | 20 |

[19] Sourcefire does not, currently, support the ability to change or delete the default "admin" account and therefore, changing this account, will not be enforced by this checklist. Sourcefire support has been notified of this security flaw.

| List | Objective/Test Steps | Expected Results/Success Criteria | Type | Risk | Reference |
|---|---|---|---|---|---|
| | • Have administrator fill out, and turn in, the forms necessary to obtain a new user id and password for the auditor.<br>• Obtain password.<br>• Insure that the password adheres to the following criteria[20].<br>❑ Seven + characters in length.<br>❑ Does not contain all or a portion of the user name.<br>❑ Does not contain a complete common word.<br>❑ Contains at least one uppercase letter.<br>❑ Contains at least one lowercase letter.<br>❑ Contains at least one digit (0-9)<br>❑ Contains at least one special character.<br>• Have the administrator fill out, and turn in, the forms necessary to delete the account. | the test steps.<br><br>☐ Pass<br>☐ Fail<br>Notes: | | passwords. Fast password cracking utilities are readily available on the internet and can be used to compromise a system or network. | |
| 7. | Objective: Insure that root login has been disabled for ssh.<br><br>Test Steps:<br>• Have the administrator try to log into the MC as root.<br>• Have the administrator log into the MC.<br>• Have the administrator run the following commands.<br>❑ more /etc/ssh/ssh_config<br>❑ Search for "PermitRootLogin"<br>❑ Note the value that this variable is set to.<br>• Repeat for each IDS device. | The administrator should not be able to log in as the root user.<br>The "PermitRootLogin" should be set to "no".<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | When users are allowed to log into a device as the root user there is no accountability for the changes that are made during that session. Any changes that are made are made as the root user and cannot easily be track back to a specific individual. | 33 |

[20] "Strong passwords" – URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/windows_password_tips.asp, 08/01/2003

| List | Objective/Test Steps | Expected Results/Success Criteria | Type | Risk | Reference |
|---|---|---|---|---|---|
| | | **Sourcefire Configuration Checklist** | | | |
| 8. | Objective: Insure that the devices have been installed according to the configuration documentation. Also, check that configuration changes are documented in the change log.<br><br>Test Steps:<br>• Locate the configuration and change log documentation for each device.<br>• With an administrator, follow the instructions step by step without making any actual changes.<br>• Repeat for each IDS device. | The devices should all be configured according to the configuration documentation. Any changes must be noted in the change log along with the reason that the configuration document was not changed to reflect the change.<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | Poorly configured IDS devices could lead to missed reconnaissance and malicious attacks. Undocumented changes could mean that a device has been compromised. | Company Policy |
| 9. | Objective: Insure that the network interfaces are configured correctly on each device.<br><br>Test Steps:<br>• Have the administrator log into the MC via the GUI.<br>❑ Select ADMIN.<br>❑ Select Network.<br>• Compare all text boxes against the network diagram and insure that the information displayed is correct.<br>• If the device is a network sensor (See Figure 29 Network Sensor Interfaces)<br>❑ Insure that the monitoring interface is in stealth mode.<br>❑ Insure that the MC manages the sensor. | All information should be consistent with the provided network diagram.<br>The "Sensing Interface" for each sensor must be in "Stealth Mode."<br>The MC should manage each sensor, if it does not then the administrator should explain why and show where this is noted in the documentation.<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | IDS devices that are not configured correctly could lead to missed reconnaissance and malicious attacks. Additionally, if the sensor interface is not set to stealth mode, the sensor has a greater possibility of being detected and attacked. | "Sourcefire Network Sensor Configuration & Management Guide"[21], "Management Console User Guide"[22] |
| 10. | Objective: Insure that the sensors are active and configured for "Remote Data Share." | Each sensor that is listed should be activated on the MC. If a sensor is not active then the administrator should be able to explain why it is not in the active state. | O | IDS devices that are not active will lead to missed reconnaissance and malicious attacks. Not configuring a Sourcefire sensor for | "Management Console User Guide" |

[21] Provided on the Sourcefire Network Sensor
[22] Provided on the Sourcefire Management Console

| List | Objective/Test Steps | Expected Results/Success Criteria | Type | Risk | Reference |
|---|---|---|---|---|---|
| | Test Steps:<br>• Have the administrator log into the MC via the GUI.<br>❑ Select ADMIN.<br>❑ Select Sensors.<br>• Check the following for all sensors on the network. (See Figure 30 Management Console Sensor Configuration)<br>❑ Active status.<br>❑ Are configured for "Remote Datashare." | "Remote Datashare" increases the sensor performance on a gigabit network and therefore should be enabled for all sensors that the MC administers.<br><br>☐ Pass<br>☐ Fail<br>Notes: | | "Remote Datashare" could lead to decreased performance and therefore missed reconnaissance and malicious attacks. | |
| 11. | Objective: Insure that access via ssh and the GUI is limited to specific hosts.<br><br>Test Steps:<br>• Have the administrator log into the MC via the GUI.<br>❑ Select ADMIN.<br>❑ Select Access<br>• Note the allowed ports for each IP address present in the text box. (See Figure 31 Access Configuration)<br>• Repeat for each sensor. | Each sensor and the MC should only be accessible from the management host. In this configuration that host is the Log Server. Therefore there should only be on IP address and both port 22 and port 443 should be allowed for this host.<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | By not limiting the access to a device from specific host we are exposing it to attack from multiple avenues. Access via unencrypted protocols can lead to the exposure of user ids and passwords that can be used to access these, and potentially other, devices. | "Sourcefire Network Sensor Configuration & Management Guide", "Management Console User Guide" |
| 12. | Objective: Insure that the sensor groups are configured correctly.<br><br>Test Steps:<br>• Have the administrator log into the MC via the GUI.<br>❑ Select RULES.<br>❑ Select Groups.<br>• Note the groups that are present. | There should be a group present for each sensor.[23]<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | If groups are configured incorrectly then it is possible that the rules for one or more of the sensors in that group will be configured improperly for its particular portion of the network. This could lead to missed reconnaissance and malicious attacks. | Personal Experience |

[23] Sourcefire v2.6.0 has a known bug involving sensors and groupings. When building and applying new rule sets only the first sensor in a group will receive the command to updates its configuration. Therefore, when utilizing this version of the software, all sensors must be configured in its own group. This bug has been fixed with the release of v2.7.0.

| List | Objective/Test Steps | Expected Results/Success Criteria | Type | Risk | Reference |
|---|---|---|---|---|---|
| | | **Sourcefire Configuration Checklist** | | | |
| 13. | Objective: Check the configuration of the snort preprocessors.<br><br>Test Steps:<br>• Have the administrator log into the Sensors via the GUI.<br>❑ Select RULES.<br>❑ Select Sensors.<br>• Compare the configuration to the configuration shown in Figure 32 Sensor Subsystem Configuration<br>Select the "Advanced" button and then compare the configuration to that shown in Figure 33 Sensor Subsystem Advanced Configuration. | The system installation defaults to with all the preprocessors running. This configuration should be left alone. If it is not then the administrator should be able to explain why and show where this is documented.<br><br>☐ Pass<br>☐ Fail<br>Notes: | S | The sensors, in this situation, should be configured to monitor everything. If any of the preprocessor settings are turned off then there is the potential that malicious activity or reconnaissance efforts are missed. | 34 |
| 14. | Objective: Check if the sensors are dropping packets.<br><br>Test Steps:<br>• Have the administrator log into one of the sensors via the GUI.<br>❑ Select STATUS.<br>❑ Select Perf Stats.<br>• In the "Select Graph" combo box select "Percent Packets Dropped." (See Figure 34 Dropped Packets)<br>• In the "Select Time Range combo box select "last month" then click the "Select" button.<br>• Repeat for "last week" then "last day."<br>• Repeat for each sensor. | When the graph returns there should be no line. This indicates that there have been no dropped packets.<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | Dropped packets could cause a sensor to fail to report a reconnaissance effort or a malicious attack. If sensors are dropping packets then the system is not working correctly and must be reconfigured. | 35 |
| 15. | Objective: Check that the snort variables are configured correctly.<br><br>Test Steps: | There should be a variable for each group of servers that handle a specific protocol. (I.E. $HTTP_SERVERS ).<br>There should also be a variable for each group of | O/S | The IDS sensor will not alert to network traffic unless a specific signature is matched. If a protocol is not allowed but the traffic does | "Sourcefire Network Sensor Configuration & Management |

[24] When the rule sets are build (pushed out to the sensors) only the configuration files are updated on the sensor. This means that the database on that sensor is not updated. Therefore, in order to verify that a sensor has been updated to the current configuration, the snort.conf file must be checked for the existence of specific variables and the local.rules file must be checked for specific rules.

| List | Objective/Test Steps | Expected Results/Success Criteria | Type | Risk | Reference |
|---|---|---|---|---|---|
| | • Locate the network diagram.<br>• Have the administrator log into the MC via the GUI.<br>❑ Select RULES.<br>❑ Select Vars.<br>❑ Click the "Change Group" button and pick a group. (See Figure 35 Variable Configuration Table)<br>• Compare all of the variables to the network diagram.<br>• Have the administrator describe all the locally configured rules.<br>• Check the change log, for the device, for entries describing new variables.<br>• Check the configuration documentation for all the variables.<br>• Have the administrator log into the sensor via ssh.<br>❑ more /etc/sf/snort.conf<br>❑ Note all of the variables present.<br>• Repeat for each group | servers that should not handle a specific protocol (I.E. !$HTTP_SERVERS ).<br>The administrator should be able to describe all the variables on the system.<br>All variables should be documented within the change log and/or the configuration documentation.<br>Each variable should be present on the sensor for which it was configured.[24]<br><br>☐ Pass<br>☐ Fail<br>Notes: | | not match one of the signatures then an alert will not be produced. This could allow compromised systems to go unnoticed.<br>If a malicious intruder were to compromise one of the IDS devices it would be possible for that individual to change the variables. These variable changes will allow the IDS to continue functioning but in a manner that does not alert on traffic initiated by the intruder. | Guide", "Management Console User Guide", 36 |
| 16. | Objective: Check that local rules contain rules that alert on traffic that should not be seen on the network.[25]<br><br>Test Steps:<br>• Make a list of all the protocols that are not allowed within the network environment.<br>• Have the administrator log into a sensor via ssh.[26]<br>❑ cat /var/sf/rules/local.rules<br>❑ Note all of the rules present. | There should be a rule, for each unexpected protocol, that will alert on any traffic. An example of such a rule for TELNET is "alert tcp any any -> any 23 stateless: msg: "TELNET Traffic" sid: 1000000 rev:1".<br>Each active rule should be present on the sensor for which it was configured.[21]<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | The IDS sensor will not alert to network traffic unless a specific signature is matched. If a protocol is not allowed but the traffic does not match one of the signatures then an alert will not be produced. This could allow compromised systems to go unnoticed.<br>If a malicious intruder were to compromise one of the IDS devices it would be possible for that individual to change the rules. These rule changes will allow the | "Sourcefire Network Sensor Configuration & Management Guide", "Management Console User Guide", 36, Sourcefire support |

[25] A unique feature to the Snort build within the Sourcefire configuration allows for a type of "DENY ALL" rule. More complex rules are evaluated first within this system. Therefore, a rule that merely specifies any->any will get evaluated last. This creates the unique opportunity for the administrator to still allow the IDS to evaluate the type of malicious activity that was attempted. An alert will be generated if there is suspicious traffic for the protocol or, if the traffic does not appear suspicious, it will be alerted on because of the any->any rule.

[26] When a sensor is controlled by a MC the rule sets that have been pushed to the sensor, from the MC, will not appear within the GUI. The MC actually copies the specified rules set to the proper file on the sensor and the database, which the GUI displays, is not updated. Therefore, it is necessary to view the actual rules file, not the GUI, to insure that a sensor has been updated correctly.

| List | Objective/Test Steps | Expected Results/Success Criteria | Type | Risk | Reference |
|---|---|---|---|---|---|
| | | **Sourcefire Configuration Checklist** | | | |
| | • Repeat for each sensor. | | | IDS to continue functioning but in a manner that does not alert on traffic initiated by the intruder. | |
| 17. | Objective: Check that each device has been configured for alerting.<br><br>Test Steps:<br>• Locate the network diagram.<br>• Have the administrator log into one of the Sensors via the GUI.<br>❑ Select EVENTS.<br>❑ Select Alerting.<br>• Note the settings for SYSLOG, E-MAIL, and SNMP. (See Figure 37 System Alerting Configuration)<br>• Repeat for each Sensor.<br>• Have the administrator log into the MC via ssh and execute the following commands and note the values returned. [27]<br>❑ more /etc/syslog.conf<br>• Search for the following line.<br>❑ *.* @<IP ADDR LOG SERVER><br>• Have the administrator log into the MC via the GUI.<br>❑ Select EVENTS.<br>❑ Select Alerting.<br>• Note the settings for SYSLOG and E-MAIL. | Network Sensors -<br>• Because this network does not utilize E-MAIL or SNMP the "Off" radio box, for both of these, should be marked.<br>• The SYSLOG "On" radio box should be marked.<br>❑ The "Facility" dropdown list should be set to "LOG_AUTH".<br>❑ The "Priority" dropdown list should be set to "LOG_DEBUG".<br>❑ The IP address for the central logging server should be in the "Logging Host" text box.<br><br>Management Console -<br>• The line "*.* @<IP ADDR LOG SERVER>" should be present in the /etc/syslog.conf.<br>• In the GUI, EMAIL should be turned off and the SYSLOG settings should match the settings for the sensors above.<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | Malicious intruders are known for deleting evidence of their intrusions. If a device is not configured for central logging then all of the devices logs are stored locally. Intruders that have compromised a system can delete all traceable evidence if they are able to obtain the proper permissions. | "Sourcefire Network Sensor Configuration & Management Guide", "Management Console User Guide" |
| 18. | Objective: Check that the database has been configured to contain a sufficient amount of events.<br><br>Test Steps:<br>• Have the administrator log into the MC via the GUI.<br>❑ Select ADMIN. | The database should be set to a reasonable amount. This figure, however, is totally up to the administrator. Ask the administrator to explain the logic behind this setting.<br><br>☐ Pass<br>☐ Fail<br>Notes: | S | A database with too many records will take longer to search. A database with too few records means that older information will be removed. The latter could lead to missed reconnaissance and malicious attacks. It could also mean the destruction of evidence. | "Management Console User Guide" |

[27] The SYSLOG feature on the MC is broken in Sourcefire v2.6.0. Therefore central logging must be initiated by modifying the SYSLOG configuration file manually. This feature is fixed in Sourcefire v2.7.

| List | Objective/Test Steps | Expected Results/Success Criteria | Type | Risk | Reference |
|---|---|---|---|---|---|
| | ❑ Select Database.<br>• Note the settings for "Max Events in Database." | | | | |
| 19. | Objective: Insure that logins are centrally logged.<br><br>Test Steps:<br>• Have the administrator log into the central logging host and search the log files.<br>❑ grep Accepted /var/log/messages | There should be log entries showing user login for all IDS devices.<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | If access to systems is not monitored then there is no accountability for any configuration changes to a system. Employees with access and malicious intent can make changes with impunity by deleting the local log files. | 16, 28 |
| 20. | Objective: Insure that the devices are configured to the network time.<br><br>Test Steps:<br>• Have the administrator log into the MC via ssh and execute the following commands and note the values returned.<br>❑ ntpdate –q <NTP SERVER IP ADDR> \| awk '{ print $9" "$10" "$11 }'<br>• Have the administrator locate demonstrate how the device updates its system time with the central timeserver.<br>• Repeat for each IDS device. | The ntpdate command will return a value "offset <TIME> sec".<br>The offset time should be less than a tenth of a second.<br>The system should be configured to update its time, at least, every hour.<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | If the timing of a network is not controlled then it is possible for central logging to become very convoluted. One sensor might alert and log traffic now where as another sensor will alert and log the same traffic with a difference of minutes, hour, days, or even years. This can affect reporting and the use of the saved information as evidence. | 32 |
| 21. | Objective: Insure that the sensors are monitoring network traffic and detecting events.<br><br>Test Steps:<br>• Have the administrator log into a host that is allowed to connect to the web servers and, using a web browser, enter the following command. [28] | Alerts for the web attack and the telnet attack should be present within the IDS logs on the MC.<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | If the IDS sensors are not configured correctly then they will not alert on suspicious traffic, malicious or reconnaissance. | "Management Console User Guide" |

[28] Company policy will not allow vulnerability tools or scanners within the working environment. Therefore, alternate ways to generate alerts must be used in this step. Showing that the IDS will alert on any traffic should be enough to show that the system is monitoring network traffic.

| List | Objective/Test Steps | Sourcefire Configuration Checklist<br>Expected Results/Success Criteria | Type | Risk | Reference |
|---|---|---|---|---|---|
| | ❑ https://<target address>/cgi-bin/windmail.exe?%20-n%20c:\boot.ini%20test@bsw.com<br>• Have the administrator log into a host that attempt to telnet to any host in the network.[29]<br>• Have the administrator log into the MC via the GUI.<br>❑ Select EVENTS.<br>❑ Select View. (See Figure 38 MC Alerting Information Leak Attempt)<br>• Have the administrator point out all alerts associated with the traffic generated by these attempts. | | | | |
| 22. | Objective: Insure that alerts are centrally logged.<br><br>Test Steps:<br>• Have the administrator log onto the central log server and show that the alerts generated in Step 21 (above) present within the logs.<br>• Repeat for each IDS sensor. | There should be an entry for each of the alerts generated by the actions in Step 21 (above).<br><br>☐ Pass<br>☐ Fail<br>Notes: | O | If the IDS sensor or MC is the only location that data is stored then a malicious intruder only has to worry about destroying the data at this one source to cover his/her tracks. | 16, 28 |
| 23. | Objective: Insure that reports are created and alerts are investigated.<br><br>Test Steps:<br>• Have the administrator locate and open a few reports that were generated by the IDS. (See Figure 39 MC Generated Alert Reports)<br>• Have the administrator locate where the reporting procedure is documented. | The administrator should be able to display several IDS reports. He/she should be able to explain the importance of these reports and walk the auditor through the information provided by it.<br>The reporting procedure should be documented.<br><br>☐ Pass<br>☐ Fail<br>Notes: | S | If the administrators are not monitoring, on a routine bases, the activity that an IDS sensor has alerted on then the whole usefulness of the system has been undermined. Without alert reporting network reconnaissance and malicious activity could be missed entirely.<br>Monitoring is also required to "tune" an IDS properly. This could lead to missed network reconnaissance and malicious activity. | 36 |

[29] This traffic will alert because of a local rule that should be present in this system.

| List | Objective/Test Steps | Expected Results/Success Criteria | Type | Risk | Reference |
|---|---|---|---|---|---|
| | | **Sourcefire Configuration Checklist** | | | |
| 24. | Objective: Insure that each device is configured with file integrity software<br><br>Test Steps:<br>• Have the administrator demonstrate how file integrity is accomplished on the MC.<br>• Repeat for each device. | The administrator should be able to demonstrate that there is the capability to determine if critical files have been changed on a system.<br><br>☐ Pass<br>☐ Fail<br>Notes: | S | When a skilled malicious intruder has compromised a system, one of the first tasks that is usually performed is the replacement of key process, files, and applications. These changes cover the intruder's tracks and can insure that access to the system remains open and covert. | 10, 16 |

**Table 7 Sourcefire Configuration Checklist**

## 3 Audit Evidence[30]

Twelve items have been selected from the complete system audit. These items represent some of the more important items within the audit. Because the auditor is one of the administrators for this system, during the initial meeting with management it was insured that one of the other administrators was assigned to help perform the audit. One important test case that was not included with in this audit report is test case number one of the Sourcefire Configuration Checklist. Most audit reports cover the issue of checking system versioning. Therefore, the results of this test case were not chosen for inclusion in the selected audit test cases. This allowed the auditor to include several other important test cases. The test case for incident response documentation, although it is an extremely important part of an IDS, was not included in this audit report do to the very size and subjectivity of this subject matter. Incident Response could, very easily, require a full audit of its own.

Please note that management specifically denied the use of scanning and vulnerability assessment tools. After evaluating the situation it was the conclusion of the auditor that suspicious traffic could be reproduced manually and that the test, although limited, could be completed.

| Selected Audit Test Cases | | | |
|---|---|---|---|
| **Checklist** | **Number** | **Audit Item** | **Pass/Fail** |
| Documentation | 1 | Configuration and change log documentation. | Fail |
| Network Devices | 5 | Security of mobile computers and portable systems. | Fail |
| Sourcefire Configuration | 2 | Company security banner | Pass |
| | 3 | Default user and root password. | Pass |
| | 14 | Sensor dropping packets. | Pass |
| | 16 | Local rules that alert on unwanted traffic. | Pass |
| | 17 | Sensors are configured to centrally log alerts. | Pass |
| | 19 | User logins are centrally logged. | Pass |
| | 20 | Devices are configured to network time. | Pass |
| | 21 | Sensors are generating alerts. | Pass |
| | 22 | Alerts are logged to a central log server | Pass |
| | 23 | File Integrity Configuration | Fail |

[30] Due to security considerations, the information displayed in the following test cases are not actual screenshots from the working environment. The screenshots displayed here are representations of the audit results. The only alterations have been to mask actual system and environment information.

**Table 8 Selected Audit Test Cases**

## 3.1 Documentation Test #1

| Documentation Checklist | |
|---|---|
| ***Objective/Test Steps*** | ***Expected Results/Success Criteria*** |
| **Objective:** Insure that the IDS has configuration and change log documentation associated with each sensor and the MC.<br><br>**Test Steps:**<br>• Obtain a copy of the IDS configuration document.<br>• Compare the documentation with the company policies and procedures.<br>• Obtain a copy of the change logs for each IDS sensor and MC. | The configuration documentation should cover the complete installation and configuration procedures for all IDS devices. These documents should adhere to company policies and procedures.<br>Each device should have a corresponding change log.<br><br>☐ Pass<br>☒ Fail<br>Notes:<br>The configuration documentation was acceptable. However, there were no change log documents associated with any of the devices. |

The configuration documentation for the intrusion detection system was stored in the company documentation repository in a document that contains the configuration information for all the other security devices. The document was easy to find as the administrator had the location bookmark on his desktop. When asked to find the document without the bookmark it took a while but he was able to locate it. Unfortunately, the document was not approved for inclusion within this audit report. However, upon inspection, this document appeared very straightforward and granular in its nature. This adheres to the company policy for configuration documentation. This document also called for the use of scripts during the initial configuration of the IDS. When reviewed, these scripts were well commented and stored in the local repository.

When asked about change log documentation the administrator was unable to produce any documentation. He did, however, inform the auditor that considerations for change log documentation were underway.

## 3.2 Physical Security Test #1

| Network Security Checklist | |
|---|---|
| ***Objective/Test Steps*** | ***Expected Results/Success Criteria*** |
| **Objective:** Insure that access to all mobile and portable systems is controlled and documented.<br><br>**Test Steps:**<br>• Locate the list of all mobile and portable systems.<br>• Locate storage space for the systems.<br>• Locate the access roster and insure that all mobile and portable systems are listed.<br>• Check server room for any mobile or portable systems and check logs for entries. | These systems should be controlled and there should be an access log. Systems may or may not have been used recently, or if the log was just created there might not be any entries. If systems are on floor the responsible individual should have line of site with the device.<br><br>☐ Pass<br>☒ Fail<br>Notes: |

| Network Security Checklist | |
|---|---|
| **Objective/Test Steps** | **Expected Results/Success Criteria** |
| | When walking the server room floor with an administrator several devices were found that could access the sensors and the management console directly. There were no access control logs for these devices. |

The administrator and the auditor walked down to the server room and gained entry. Walking around for a few minutes turned up several monitor, keyboard, and mouse setups as well as several computer stations on carts with wheels. These devices were not being monitored by anybody on the floor at that time. When asked about access logs it was determined that there were no documents to control them. When asked about portable systems, such as laptops, the administrator stated that there were no systems of this time.

### 3.3 Sourcefire Configuration Test #2

| Sourcefire Configuration Checklist | |
|---|---|
| **Objective/Test Steps** | **Expected Results/Success Criteria** |
| Objective: Determine if the company legal login banner is displayed prior to attempted login.<br><br>Test Steps:<br>• Obtain a copy of the company legal login banner.<br>• Have the administrator connect to the MC via the GUI.<br>❑ Note when the banner appears.<br>❑ Compare banner to the copy.<br>• Have the administrator connect to the MC via the SSH interface.<br>❑ Note when the banner appears.<br>❑ Compare banner to the copy.<br>• Repeat for each sensor. | Banner should be displayed before the user is prompted to enter a user name or password. Each banner should be worded exactly the same as the company copy.<br><br>☒ Pass<br>☐ Fail<br>Notes:<br>None |

The security administrator obtained a copy of the security banner from the security documentation for the IDS. The following is a copy of this banner.

**********

NOTICE TO USERS

This computer system is the private property of Some Young Security Company, whether individual, corporate or government. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to your employer, to authorized site, government, and law enforcement personnel, as well as authorized officials of government agencies, both domestic and foreign.

By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of such personnel or officials. Unauthorized or improper use of this system may result in

civil and criminal penalties and administrative or disciplinary action, as appropriate. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

**********

Next the administrator connected to each device via SSH and via the web browser from the log host. The following are screen captures from these log in attempts that demonstrate the security banner being displayed prior to prompting the user for a password.

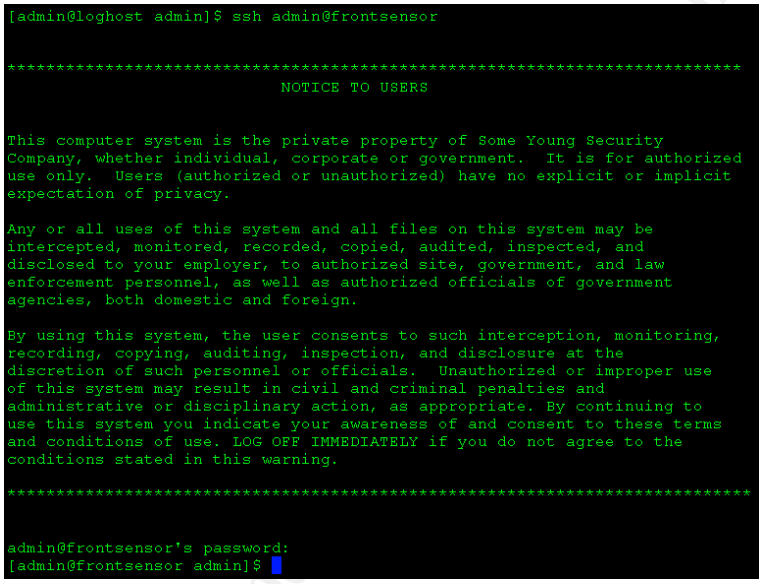



**Figure 2 Front End Sensor SSH Login**

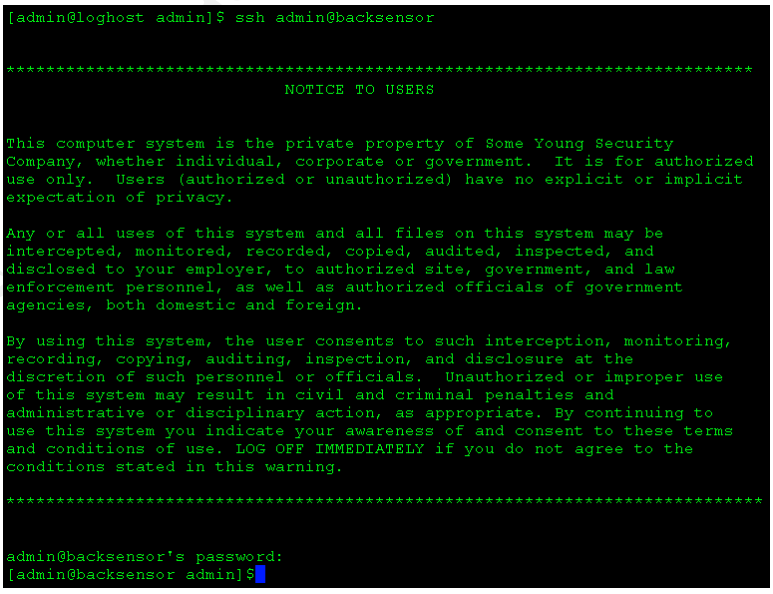



**Figure 3 Back End Sensor SSH Login**

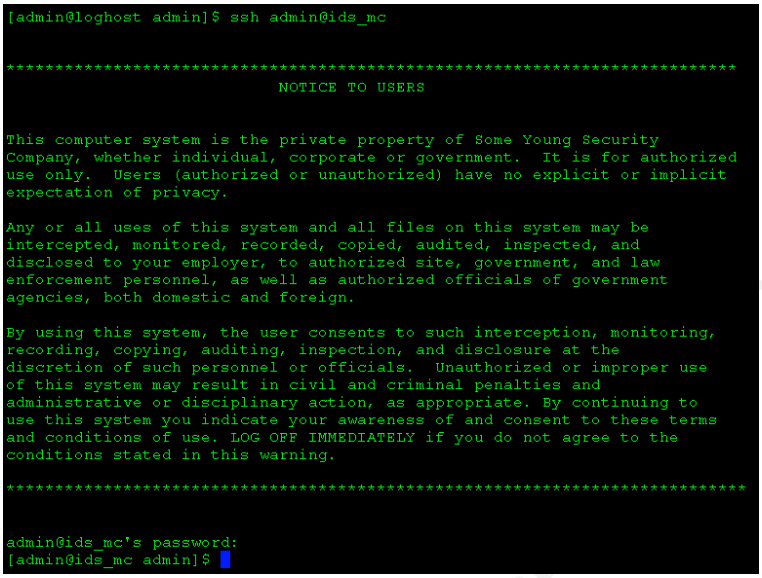



**Figure 4 Management Console SSH Login**


**Figure 5 Front End Sensor GUI Login**


**Figure 6 Back End Sensor GUI Login**

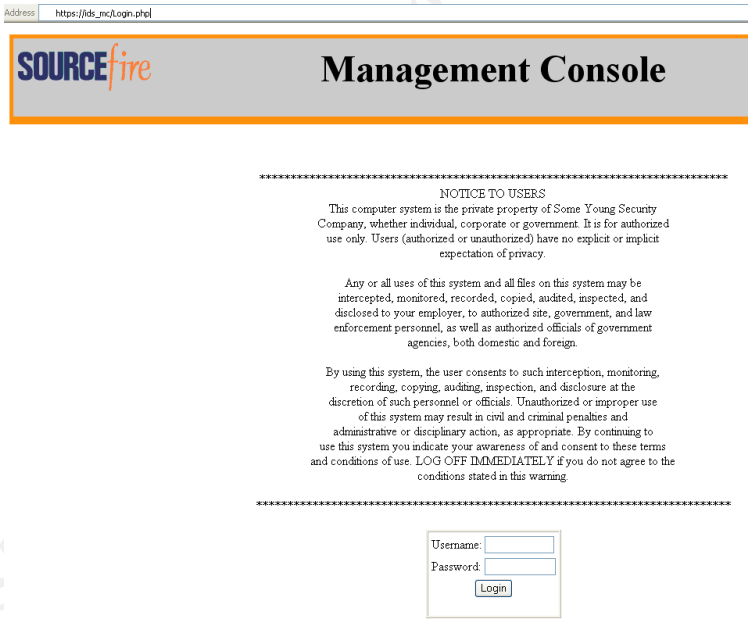



**Figure 7 Management Console GUI Login**

## 3.4 Sourcefire Configuration Test #3

| *Sourcefire Configuration Checklist* | |
|---|---|
| ***Objective/Test Steps*** | ***Expected Results/Success Criteria*** |
| Objective: Insure that the default root password was changed after installation. | Logging should fail on all sensors and the MC. |

| Sourcefire Configuration Checklist | |
|---|---|
| **Objective/Test Steps** | **Expected Results/Success Criteria** |
| Test Steps:<br>• Have the administrator connect a mobile station directly to the MC.<br>• Enter the password "Opensnort".<br>• Repeat for ssh.<br>• Repeat for GUI.<br>• Repeat for each IDS device. | ☒ Pass<br>☐ Fail<br>Notes:<br>None |

The administrator initiated the login attempts to each device but the auditor entered the default password of "Opensnort" at each login prompt. The screenshots demonstrate that the login attempts failed on each attempt.

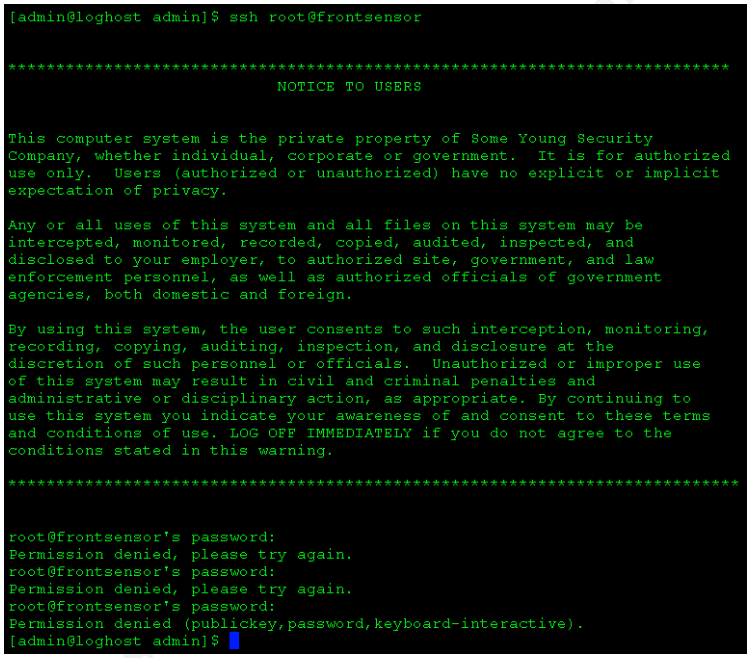



**Figure 8 Front Sensor Default Password Attempt**

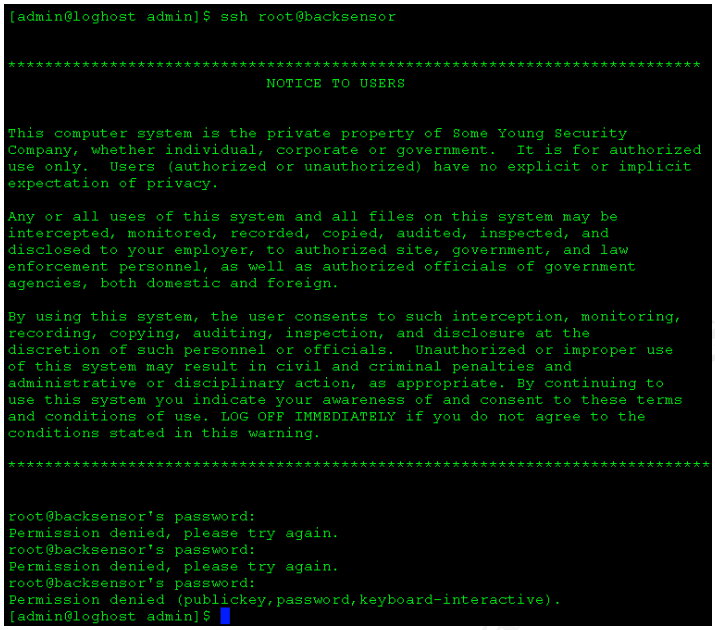



**Figure 9 Back Sensor Default Password Attempt**

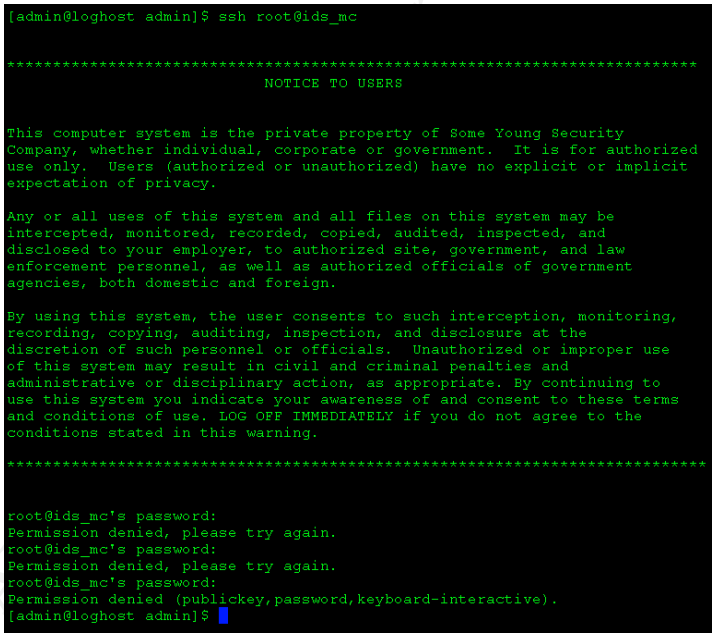



**Figure 10 Management Console Default Password Attempt**

## 3.5 Sourcefire Configuration Test #14

| *Sourcefire Configuration Checklist* | |
|---|---|
| ***Objective/Test Steps*** | ***Expected Results/Success Criteria*** |

| Sourcefire Configuration Checklist | |
|---|---|
| **Objective/Test Steps** | **Expected Results/Success Criteria** |
| Objective: Check if the sensors are dropping packets.<br><br>Test Steps:<br>• Have the administrator log into one of the sensors via the GUI.<br>❑ Select STATUS.<br>❑ Select Perf Stats.<br>• In the "Select Graph" combo box select "Percent Packets Dropped." (See Figure 34 Dropped Packets)<br>• In the "Select Time Range combo box select "last month" then click the "Select" button.<br>• Repeat for "last week" then "last day."<br>• Repeat for each sensor. | When the graph returns there should be no line. This indicates that there have been no dropped packets.<br><br>☒ Pass<br>☐ Fail<br>Notes:<br>None |

The administrator logged into the each sensor and checked if the sensor was dropping any packet with the current configuration and network traffic load. The screenshots prove that the sensors are not currently dropping packets.

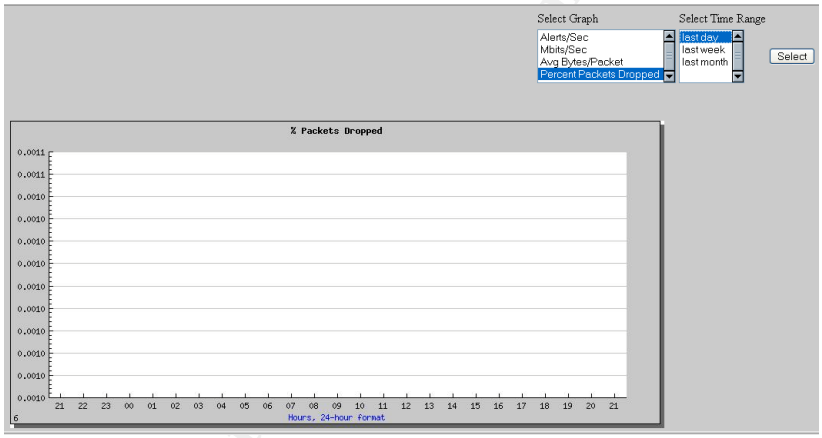



**Figure 11Front Sensor Percent Packages Dropped**

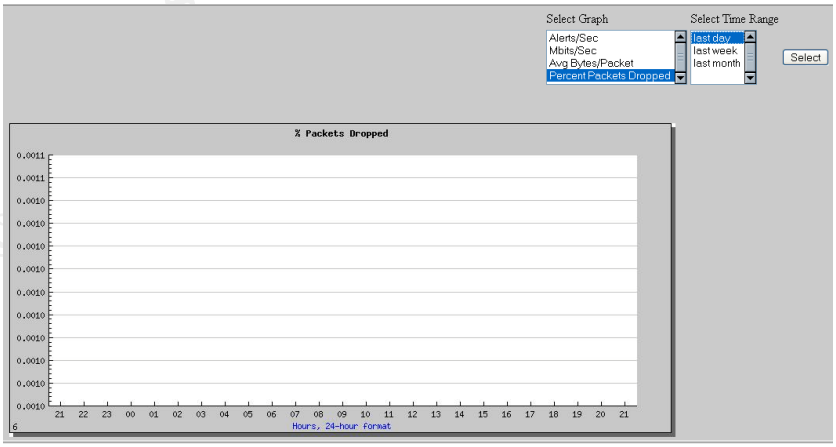



**Figure 12 Back Sensor Percent Packages Dropped**

### 3.6 Sourcefire Configuration Test #16

| Sourcefire Configuration Checklist | |
|---|---|
| **Objective/Test Steps** | **Expected Results/Success Criteria** |
| Objective: Check that local rules contain rules that alert on traffic that should not be seen on the network.[31]<br><br>Test Steps:<br>• Make a list of all the protocols that are not allowed within the network environment.<br>• Have the administrator log into a sensor via ssh.[32]<br>❑ cat /var/sf/rules/local.rules<br>❑ Note all of the rules present.<br>• Repeat for each sensor. | There should be a rule, for each unexpected protocol, that will alert on any traffic. An example of such a rule for TELNET is "alert tcp any any -> any 23 stateless: msg: "TELNET Traffic" sid: 1000000 rev:1".<br>Each active rule should be present on the sensor for which it was configured.[21]<br><br>☒ Pass<br>☐ Fail<br>Notes:<br>None |

The administrator provided the following list of protocols that should not be seen within the network during normal activity. This list came from the configuration documentation. The screenshots are the output of the local rules files on each sensor. They confirm that the rules have been created and are deployed to each sensor. It should also be noted that the configuration is different for each sensor. The front sensor has a rule that alerts on any HTTP traffic whereas the back sensor does not sense HTTP traffic is normal for the back end of the network.

| Abnormal Network Traffic | |
|---|---|
| **Protocol** | **Port Numbers** |
| finger | 79 |
| telnet | 23 |
| smtp | 25 |
| rservices | 513, 514(TCP) |
| tftp | 69 |
| x11 | 6000 |
| netbios | 137, 138, 139, 445 |
| imap | 143 |

[31] A unique feature to the Snort build within the Sourcefire configuration allows for a type of "DENY ALL" rule. More complex rules are evaluated first within this system. Therefore, a rule that merely specifies any->any will get evaluated last. This creates the unique opportunity for the administrator to still allow the IDS to evaluate the type of malicious activity that was attempted. An alert will be generated if there is suspicious traffic for the protocol or, if the traffic does not appear suspicious, it will be alerted on because of the any->any rule.

[32] When a sensor is controlled by a MC the rule sets that have been pushed to the sensor, from the MC, will not appear within the GUI. The MC actually copies the specified rules set to the proper file on the sensor and the database, which the GUI displays, is not updated. Therefore, it is necessary to view the actual rules file, not the GUI, to insure that a sensor has been updated correctly.

| Abnormal Network Traffic | |
|---|---|
| **Protocol** | **Port Numbers** |
| pop3 | 109, 110 |
| dns | 53(TCP/UDP) |
| rpc | 111, 32770-32789 |
| snmp | 161,162 |
| http | 80 (Front Sensor ONLY) |

**Table 9 Abnormal Network Traffic**

```
[root@frontsensor root]$ cat /var/sf/rules/local.rules
alert tcp any any -> any 23 (msg:"TELNET Activity Detected"; stateless:; sid:1000000; rev:1;)
alert tcp any any -> any 79 (msg:"FINGER Activity Detected"; stateless:; sid:1000001; rev:1;)
alert tcp any any -> any 25 (msg:"SMTP Activity Detected"; stateless:; sid:1000002; rev:1;)
alert tcp any any -> any $RSERVICES_PORTS (msg:"RSERVICES Activity Detected"; stateless:; sid:1000
003; rev:1;)
alert tcp any any -> any 69 (msg:"TFTP Activity Detected"; stateless:; sid:1000004; rev:1;)
alert tcp any any -> any 6000 (msg:"X11 Activity Detected"; stateless:; sid:1000005; rev:1;)
alert tcp any any -> any $NETBIOS_PORTS (msg:"NETBIOS Activity Detected"; stateless:; sid:1000006;
 rev:1;)
alert tcp any any -> any 143 (msg:"IMAP Activity Detected"; stateless:; sid:1000007; rev:1;)
alert tcp any any -> any $POP3_PORTS (msg:"POP3 Activity Detected"; stateless:; sid:1000008; rev:1
;)
alert tcp any any -> any 53 (msg:"DNS Activity Detected"; stateless:; sid:1000009; rev:1;)
alert udp any any -> any 53 (msg:"DNS Activity Detected"; stateless:; sid:1000010; rev:1;)
alert tcp any any -> any $SNMP_PORTS (msg:"SNMP Activity Detected"; stateless:; sid:1000011; rev:1
;)
alert tcp any any -> any 80 (msg:"Front End HTTP Activity Detected"; stateless:; sid:1000009; rev:
1;)
[root@frontsensor root]$
```

**Figure 13 Front End Local Rules**

```
[root@backsensor root]$ cat /var/sf/rules/local.rules
alert tcp any any -> any 23 (msg:"TELNET Activity Detected"; stateless:; sid:1000000; rev:1;)
alert tcp any any -> any 79 (msg:"FINGER Activity Detected"; stateless:; sid:1000001; rev:1;)
alert tcp any any -> any 25 (msg:"SMTP Activity Detected"; stateless:; sid:1000002; rev:1;)
alert tcp any any -> any $RSERVICES_PORTS (msg:"RSERVICES Activity Detected"; stateless:; sid:1000
003; rev:1;)
alert tcp any any -> any 69 (msg:"TFTP Activity Detected"; stateless:; sid:1000004; rev:1;)
alert tcp any any -> any 6000 (msg:"X11 Activity Detected"; stateless:; sid:1000005; rev:1;)
alert tcp any any -> any $NETBIOS_PORTS (msg:"NETBIOS Activity Detected"; stateless:; sid:1000006;
 rev:1;)
alert tcp any any -> any 143 (msg:"IMAP Activity Detected"; stateless:; sid:1000007; rev:1;)
alert tcp any any -> any $POP3_PORTS (msg:"POP3 Activity Detected"; stateless:; sid:1000008; rev:1
;)
alert tcp any any -> any 53 (msg:"DNS Activity Detected"; stateless:; sid:1000009; rev:1;)
alert udp any any -> any 53 (msg:"DNS Activity Detected"; stateless:; sid:1000010; rev:1;)
alert tcp any any -> any $SNMP_PORTS (msg:"SNMP Activity Detected"; stateless:; sid:1000011; rev:1
;)
[root@backsensor root]$
```

**Figure 14 Back End Local Rules**

## 3.7 Sourcefire Configuration Test #17

| Sourcefire Configuration Checklist | |
|---|---|
| **Objective/Test Steps** | **Expected Results/Success Criteria** |

| Sourcefire Configuration Checklist | |
|---|---|
| **Objective/Test Steps** | **Expected Results/Success Criteria** |
| Objective: Check that each device has been configured for alerting.<br><br>Test Steps:<br>• Locate the network diagram.<br>• Have the administrator log into one of the Sensors via the GUI.<br>❑ Select EVENTS.<br>❑ Select Alerting.<br>• Note the settings for SYSLOG, E-MAIL, and SNMP. (See Figure 37 System Alerting Configuration)<br>• Repeat for each Sensor.<br>• Have the administrator log into the MC via ssh and execute the following commands and note the values returned. [33]<br>❑ more /etc/syslog.conf<br>• Search for the following line.<br>❑ *.* @<IP ADDR LOG SERVER><br>• Have the administrator log into the MC via the GUI.<br>❑ Select EVENTS.<br>❑ Select Alerting.<br>• Note the settings for SYSLOG and E-MAIL. | Network Sensors -<br>• Because this network does not utilize E-MAIL or SNMP the "Off" radio box, for both of these, should be marked.<br>• The SYSLOG "On" radio box should be marked.<br>❑ The "Facility" dropdown list should be set to "LOG_AUTH".<br>❑ The "Priority" dropdown list should be set to "LOG_DEBUG".<br>❑ The IP address for the central logging server should be in the "Logging Host" text box.<br><br>Management Console -<br>• The line "*.* @<IP ADDR LOG SERVER>" should be present in the /etc/syslog.conf.<br>• In the GUI, EMAIL should be turned off and the SYSLOG settings should match the settings for the sensors above.<br><br>☒ Pass<br>☐ Fail<br>Notes: |

The following screenshots are the results of the logging configuration for each device. Note that, even though the MC's has no ability to configure SYSLOG (in v2.6), the system is still configured through the GUI to avoid confusion as to the systems actual settings.

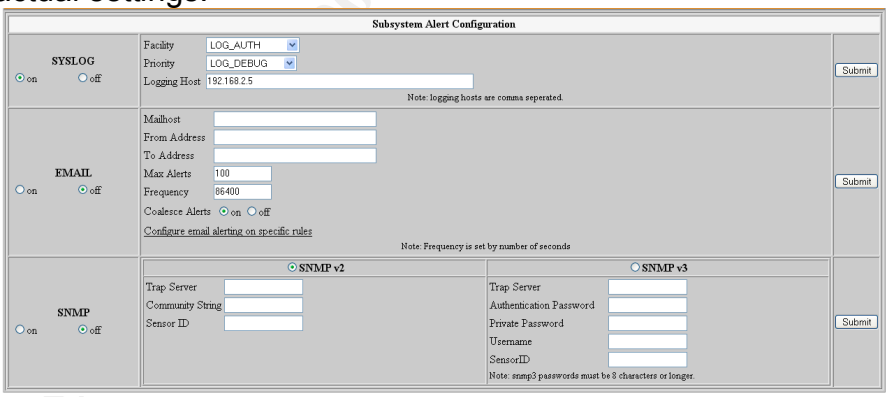



**Figure 15 Back Sensor Alerting Configurations**

[33] The SYSLOG feature on the MC is broken in Sourcefire v2.6.0. Therefore central logging must be initiated by modifying the SYSLOG configuration file manually. This feature is fixed in Sourcefire v2.7.

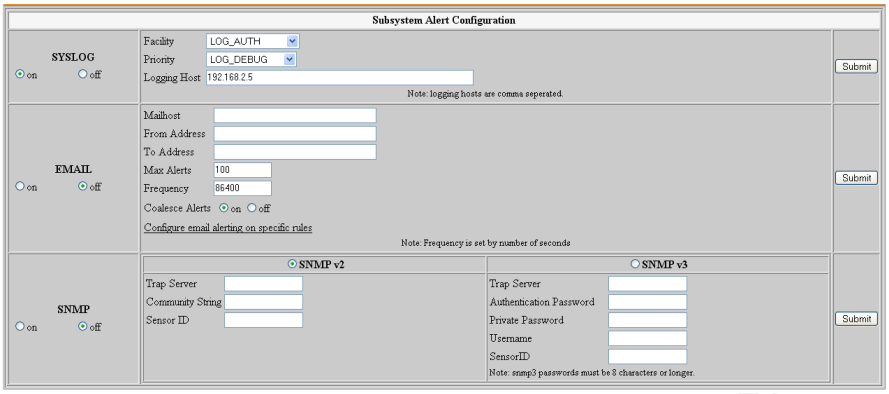



**Figure 16 Front Sensor Alerting Configurations**

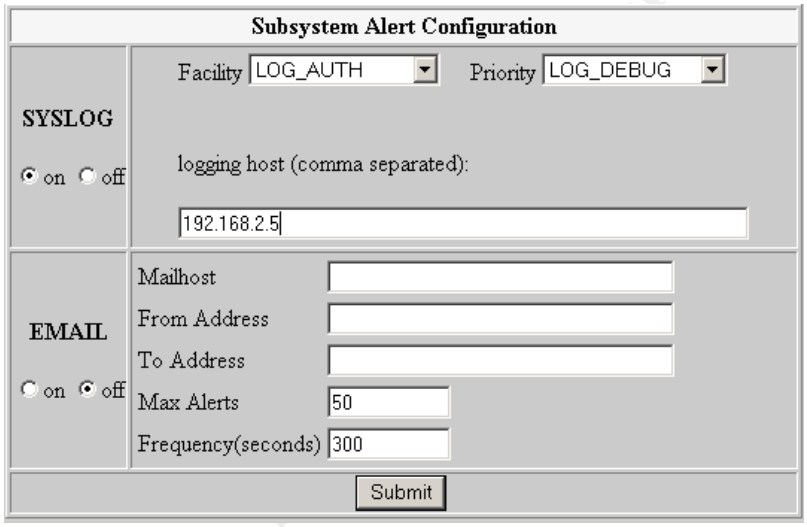



**Figure 17 Management Console Alerting Configurations**

```
[root@ids_MC root]$ cat /etc/syslog.conf
#/etc/syslog.conf
# For info about the format of this file, see "man syslog.conf"
# and /usr/doc/sysklogd/README.linux.

# Uncomment this to see kernel messages on the console.
kern.*                                                  /var/log/messages

# Log anythingm 'info' or higher, but lower than 'warn'.
# Exclude authpriv, cron, mail, and news.  These are logged elsewhere.
*.info;*.!warn;\
        authpriv.none;cron.none;mail.none;news.none     /var/log/messages

# Log anything 'warn' or higher.
# Exclude authpriv, cron, mail and news.  These are logged elsewhere.
*.warn;\
        authpriv.none;cron.none;mail.none;news.none     /var/log/messages

# Debugging information is logged here.
*.=debug                                                /var/log/messages

# Private authentication message logging:
authpriv.*                                              /var/log/messages

# Cron related logs:
cron.*                                                  /var/log/messages

# Mail related logs:
mail.*                                                  /var/log/messages

# Emergency level messages go to all users:
*.emerg                                                 *

*.crit                                                  /var/log/messages

# This log is for news and uucp errors:
uucp,news.crit                                          /var/log/messages

# Uncomment these if you'd like INN to keep logs on everything.
# You won't need this if you don't run INN (the InterNetNews daemon).
#news.=crit                                             /var/log/news/news.crit
#news.=err                                              /var/log/news/news.err
#news.=notice                                           /var/log/news/news.notice

*.*                             @192.168.2.5

[root@ids_MC root]$
```

**Figure 18 Management Console /etc/syslog.conf**

## 3.8 Sourcefire Configuration Test #19

| ***Sourcefire Configuration Checklist*** | |
|---|---|
| ***Objective/Test Steps*** | ***Expected Results/Success Criteria*** |
| Objective: Insure that logins are centrally logged.<br><br>Test Steps:<br>• Have the administrator log into the central logging host and search the log files.<br>❑ grep ids_MC /var/log/messages<br>❑ grep backsensor /var/log/messages<br>❑ grep frontsensor /var/log/messages | There should be log entries showing user login for all IDS devices.<br><br>☒ Pass<br>☐ Fail<br>Notes:<br>None |

The following log entries represent the values returned to the administrator during his query. The return values were confirmed that the devices were centrally logged.

```
[admin@loghost admin]$ grep ids_MC /var/adm/messages | more
Aug 11 02:24:53 ids_MC sshd[21158]: Failed password for admin from 192.168.2.5 port 25517 ssh2
Aug 11 02:25:16 ids_MC last message repeated 2 times
Aug 11 02:27:07 ids_MC sshd[21169]: Accepted password for admin from 192.168.2.5 port 28112 ssh2
Aug 11 02:34:53 ids_MC sshd[21253]: Failed password for root from 192.168.2.5 port 31427 ssh2
Aug 11 02:35:32 ids_MC last message repeated 2 times
Aug 11 02:36:14 ids_MC sshd[21311]: Accepted password for admin from 192.168.2.5 port 32852 ssh2
[admin@loghost admin]$
```

**Figure 19 Management Console Syslog'ed Login Attempts and Failures**

```
[admin@loghost admin]$ grep backsensor /var/adm/messages | more
Aug 11 03:11:56 backsensor sshd[15238]: Failed password for admin from 192.168.2.5 port 3539 ssh2
Aug 11 03:12:16 backsensor last message repeated 2 times
Aug 11 03:13:07 backsensor sshd[15249]: Accepted password for admin from 192.168.2.5 port 4987 ssh
2
Aug 11 03:22:58 backsensor sshd[15271]: Failed password for root from 192.168.2.5 port 5221 ssh2
Aug 11 03:23:22 backsensor last message repeated 2 times
Aug 11 03:24:38 backsensor sshd[15318]: Accepted password for admin from 192.168.2.5 port 6791 ssh
2
[admin@loghost admin]$
```

**Figure 20 Back Sensor Syslog'ed Login Attempts and Failures**

```
[admin@loghost admin]$ grep frontsensor /var/adm/messages | more
Aug 11 03:25:32 frontsensor sshd[421]: Failed password for admin from 192.168.2.5 port 26139 ssh2
Aug 11 03:26:06 frontsensor last message repeated 2 times
Aug 11 03:27:09 frontsensor sshd[445]: Accepted password for admin from 192.168.2.5 port 25791 ssh
2
Aug 11 03:33:28 frontsensor sshd[515]: Failed password for root from 192.168.2.5 port 26900 ssh2
Aug 11 03:34:12 frontsensor last message repeated 2 times
Aug 11 03:35:11 frontsensor sshd[589]: Accepted password for admin from 192.168.2.5 port 32213 ssh
2
[admin@loghost admin]$
```

**Figure 21 Front Sensor Syslog'ed Login Attempts and Failures**

## 3.9 Sourcefire Configuration Test #20

| ***Sourcefire Configuration Checklist*** | |
|---|---|
| ***Objective/Test Steps*** | ***Expected Results/Success Criteria*** |
| Objective: Insure that the devices are configured to the network time.<br><br>Test Steps:<br>• Have the administrator log into the MC via ssh and execute the following commands and note the values returned.<br>❑ ntpdate –q <NTP SERVER IP ADDR> \| awk '{ print $9" "$10" "$11 }'<br>• Have the administrator locate demonstrate how the device updates its system time with the central timeserver.<br>• Repeat for each IDS device. | The ntpdate command will return a value "offset <TIME> sec".<br>The offset time should be less than a tenth of a second.<br>The system should be configured to update its time, at least, every hour.<br><br>☒ Pass<br>☐ Fail<br>Notes:<br>The inclusion of the –s option for the ntpdate command is a good touch. This sends the output of the time update to SYSLOG for auditing. |

The screenshot below show that each device is configured to update its time to the network standard. The auditor noted, with approval, the inclusion of the –s

option in the ntpdate command that sends the time update information to the SYSLOG

```
[root@ids_MC root]$ /usr/sbin/ntpdate -q 192.168.2.5 | awk '{  print $9" "$10" "$11 }'

offset 0.000556 seec
[root@ids_MC root]$ /usr/sbin/ntpdate -s 192.168.2.5
[root@ids_MC root]$ cat /etc/cron.hourly/local.ntpdate
#!/bin/bash
/usr/sbin/ntpdate -s 192.168.2.5
[root@ids_MC root]$
```

**Figure 22 Management Console Network Time Configuration**

```
[root@backsensor root]$ /usr/sbin/ntpdate -q 192.168.2.5 | awk '{  print $9" "$10" "$11 }'

offset 0.000556 seec
[root@backsensor root]$ /usr/sbin/ntpdate -s 192.168.2.5
[root@backsensor root]$ cat /etc/cron.hourly/local.ntpdate
#!/bin/bash
/usr/sbin/ntpdate -s 192.168.2.5
[root@backsensor root]$
```

**Figure 23 Back Sensor Network Time Configuration**

```
[root@frontsensor root]$ /usr/sbin/ntpdate -q 192.168.2.5 | awk '{  print $9" "$10" "$11 }'

offset 0.000556 seec
[root@frontsensor root]$ /usr/sbin/ntpdate -s 192.168.2.5
[root@frontsensor root]$ cat /etc/cron.hourly/local.ntpdate
#!/bin/bash
/usr/sbin/ntpdate -s 192.168.2.5
[root@frontsensor root]$
```

**Figure 24 Front Sensor Network Time Configuration**

## 3.10 Sourcefire Configuration Test #21

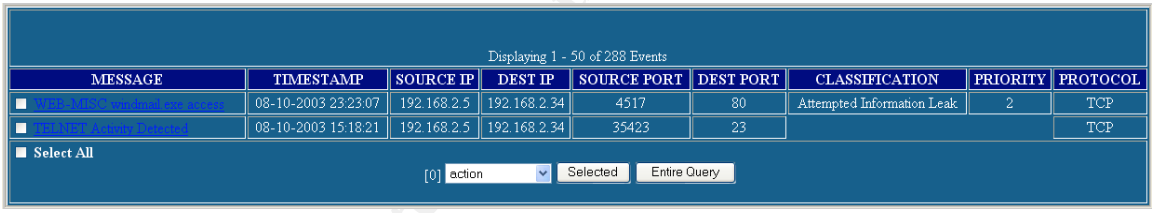
| ***Sourcefire Configuration Checklist*** | |
|---|---|
| ***Objective/Test Steps*** | ***Expected Results/Success Criteria*** |
| Objective: Insure that the sensors are monitoring network traffic and detecting events.<br><br>Test Steps:<br>• Have the administrator log into a host that is allowed to connect to the web servers and, using a web browser, enter the following command. [34]<br>❑ https://<target address>/cgi-bin/windmail.exe?%20-n%20c:\boot.ini%20test@bsw.com<br>• Have the administrator log into a host then attempt to telnet to any host in the network.[35]<br>• Have the administrator log into the MC via the GUI.<br>❑ Select EVENTS. | Alerts for the web attack and the telnet attack should be present within the IDS logs on the MC.<br><br>☒ Pass<br>☐ Fail<br>Notes:<br>The inability to utilize vulnerability assessment tools limited the scope of this test. It is the suggestion of the auditor that these tools be made available to network security administrators for future auditing and testing. |

[34] Company policy will not allow vulnerability tools or scanners within the working environment. Therefore, alternate ways to generate alerts must be used in this step. Showing that the IDS will alert on any traffic should be enough to show that the system is monitoring network traffic.

[35] This traffic will alert because of a local rule that should be present in this system.

| Sourcefire Configuration Checklist | |
|---|---|
| **Objective/Test Steps** | **Expected Results/Success Criteria** |
| ❑ Select View. (See Figure 38 MC Alerting Information Leak Attempt)<br>• Have the administrator point out all alerts associated with the traffic generated by these attempts. | These tools and the devices on which they are stored can be properly maintained and controlled to limit the risk of malicious use within the network.<br>The network security administrators cannot fully protect against the common hacker tools of the trade if they are unable to test their configurations with the very tools that are available to the community. Maintaining these tools are, in this auditor's opinion, worth the risk if they are tightly controlled. |

This test was, unfortunately, very limited in scope. The inability to utilize vulnerability assessment tools makes it very difficult to fully test the configuration of the IDS. However, the main goal of this test step is to insure that the sensors are seeing network traffic and that they will alert accordingly to suspicious traffic. The following screenshot shows that the sensors are, indeed alerting to this type of traffic.



Displaying 1 - 50 of 288 Events

| MESSAGE | TIMESTAMP | SOURCE IP | DEST IP | SOURCE PORT | DEST PORT | CLASSIFICATION | PRIORITY | PROTOCOL |
|---|---|---|---|---|---|---|---|---|
| WEB-MISC sendmail.cgi access | 08-10-2003 23:23:07 | 192.168.2.5 | 192.168.2.34 | 4517 | 80 | Attempted Information Leak | 2 | TCP |
| TELNET Activity Detected | 08-10-2003 15:18:21 | 192.168.2.5 | 192.168.2.34 | 35423 | 23 | | | TCP |

Select All

[0] action Selected Entire Query

**Figure 25 MC Consolidated Alerts**

## 3.11 Sourcefire Configuration Test #22

| Sourcefire Configuration Checklist | |
|---|---|
| **Objective/Test Steps** | **Expected Results/Success Criteria** |
| Objective: Insure that alerts are centrally logged.<br><br>Test Steps:<br>• Have the administrator log onto the central log server and show that the alerts generated in Step 21 (above) present within the logs.<br>• Repeat for each IDS sensor. | There should be an entry for each of the alerts generated by the actions in Step 21 (above).<br><br>☒ Pass<br>☐ Fail<br>Notes:<br>Although the alerts are centrally logged there should be a mechanism to provide real time alerting to priority alerts. Normally this system would be configured with the ability for email alerting, but as this environment does not allow for such activity then a system should be developed to provide this missing capability. |

| Sourcefire Configuration Checklist | |
|---|---|
| **Objective/Test Steps** | **Expected Results/Success Criteria** |

The following screenshot demonstrators that the alerts generated by the sensors are centrally logged and controlled.

```
[admin@loghost admin]$ grep snort /var/adm/messages | more
Aug 11 02:14:03 backsensor snort: [1:1158:4] WEB-MISC windmail.exe access [Classification: attempt
ed-recon] [Priority: 2]: {TCP} 192.168.2.5:4517 -> 192.168.2.34:80
Aug 11 02:16:03 backsensor snort: [1:1000000:1] TELNET Activity Detected {TCP} 192.168.2.5:35423 -
> 192.168.2.34:23
Aug 11 02:23:46 frontsensor snort: [1:1000000:1] TELNET Activity Detected {TCP} 192.168.1.5:13293
-> 192.168.2.34:23
[admin@loghost admin]$
```

**Figure 26 Syslog'ed Snort Alerts**

### 3.12 Sourcefire Configuration Test #24

| Sourcefire Configuration Checklist | |
|---|---|
| **Objective/Test Steps** | **Expected Results/Success Criteria** |
| Objective: Insure that each device is configured with file integrity software<br><br>Test Steps:<br>• Have the administrator demonstrate how file integrity is accomplished on the MC.<br>• Repeat for each device. | The administrator should be able to demonstrate that there is the capability to determine if critical files have been changed on a system.<br>There should be a system that performs automated file integrity checking on each IDS device.<br><br>☐ Pass<br>☒ Fail<br>Notes:<br>There is no method to insure file integrity on any of the IDS devices. However, there is also no way to currently configure this feature that is supported by the manufacturer.<br>This matter should be discussed with the Sourcefire support. |

The administrator was unable to demonstrate any method of file integrity checking. However, the vendor had been contacted about the issue and stated that any internal configuration changes not validated by the Sourcefire development team or software additions violates the support contract of the device.[36]

[36] Sourcefire support did state that this issue would be addressed in up-coming versions of the software.

# 4 Audit Findings

## 4.1 Results

The following table is contains the overall findings of the complete audit.

| Complete Audit Results | | | |
|---|---|---|---|
| **Checklist** | **Number** | **Audit Item** | **Pass/Fail** |
| Documentation | 1 | Configuration and change log documentation. | Fail |
| | 2 | Vendor document availability. | Pass |
| | 3 | Incident response documentation. | Pass |
| | 4 | Application documentation availability. | Pass |
| | 5 | Network diagram availability and correctness. | Pass |
| Physical Security | 1 | Access to facility. | Fail |
| | 2 | Safety precautions within the server room. | Pass |
| Network Devices | 1 | Proper deployment of IDS. | Pass |
| | 2 | Proper installation of IDS devices. | Pass |
| | 3 | Load balancer port mirror configuration. | Pass |
| | 4 | Load balancer traffic configuration. | Fail |
| | 5 | Security of mobile computers and portable systems. | Fail |
| | 6 | Administrative host access. | Pass |
| Sourcefire Configuration | 1 | Software and rule set versions. | Pass – comments |
| | 2 | Company security banner. | Pass |
| | 3 | Default user and root password. | Pass |
| | 4 | Device license storage. | Pass |
| | 5 | User account management. | Pass |
| | 6 | Strong password enforcement. | Pass |
| | 7 | Disable SSH root login. | Pass |
| | 8 | Device configuration documentation. | Pass |
| | 9 | Network interface configuration. | Pass |
| | 10 | Sensor set to remote datashare. | Pass |
| | 11 | Device network access limited. | Pass |
| | 12 | Sensor group configuration. | Pass |
| | 13 | Snort preprocessor configuration. | Pass |
| | 14 | Sensor dropping packets. | Pass |
| | 15 | Snort variable configuration. | Pass |
| | 16 | Local rules that alert on unwanted traffic. | Pass |

| Complete Audit Results | | | |
|---|---|---|---|
| **Checklist** | **Number** | **Audit Item** | **Pass/Fail** |
| | 17 | Sensors are configured to centrally log alerts. | Pass |
| | 18 | Database configuration. | Pass |
| | 19 | User logins are centrally logged. | Pass |
| | 20 | Devices are configured to network time. | Pass |
| | 21 | Sensors are generating alerts. | Pass |
| | 22 | Alerts are logged to a central log server | Pass |
| | 23 | Report creation and investigation. | Pass |
| | 24 | File Integrity Configuration | Fail |

**Table 10 Complete Audit Results**

### 4.1.1 Documentation

Documentation for the overall system was exceptional. However, the lack of change logs for any of the devices is a concern. Change logs are very important documents that give administrators and managers more control over the entire system. A change log lets these individuals know what has or has not been done to a system as well as providing a way to track changes and the reasoning behind them.

Cost - Implementing a change log system should not take an administrator more than two days. Training personnel on the use of the change logs should take about an hour.

### 4.1.2 Physical Security

Physical security was very tight from the outside of the facility up until the inside of the server room. The systems and the racks that they are stored in are not controlled in any way. There is no access accountability and the keys to the racks and servers are not maintained or monitored.
Cost – Implementing access control over the entire server room will be an undertaking. A system will have to be devised and accountability assigned. Overall, a small team should be able to complete this task in about a week's time.

### 4.1.3 Network Devices

There are two major points to be noted in this section.

The configuration of the load balancers in this network needs to be reconsidered. These devices are currently configured to block all echo and echo-reply ICMP traffic. The load balancers should not be configured to act as security devices. The firewalls and routers are in place to proved this function. The load balancers

should be configured to pass all traffic from point to point regardless of what that traffic represents.
Cost – Reconfiguring the load balancers and changing the configuration documentation should not take one person more than three hours.

Secondly, the presence of uncontrolled mobile devices on the server room floor is very disturbing. These devices can be used to access any device on within the server room. Coupled with the fact that access to the racks and devices are not controlled, this leaves direct access by malicious insiders uncontrollable. This practice needs to be reevaluated.
Cost – This task can be assigned to the team that is implementing physical access control and should not create a significant amount of extra work.

### 4.1.4 Sourcefire Configuration

There is an issue of the current state of the systems version and rule sets. The current configuration of the systems is at a state that is two versions behind the manufacturer. However, the system is not is this state because of poor administration but rather because the newer versions have not been completely evaluated in a test environment. Rule sets are a particular concern as the vender version starts falling behind. With each new version the vendor generally implements improvements to the core software. Newly developed rules might utilize some of these improvements and therefore may not be configurable to an older version of the vendor software. A system needs to be implemented that allows the network security administrator to set aside more time to review new rules that apply to major software and network vulnerabilities so that the intrusion detection system is capable of alerting to this traffic when it appears within the network.
Cost – An extra two to five hours a week should give an administrator ample time to research, reconfigure (if necessary), and implement any new rule sets.

File integrity is a major issue when it comes to system security. However, it may not be possible to implement this type of security software because of support issues. This makes this a management issue instead of an administrative issue.
Cost – A decision about this subject should not take more than an hour in a conference call. Picking, evaluating it, and implementing a file integrity product will take a two-person team about a two to three weeks.

## 4.2 Is the system auditable?

The main purpose of this audit is to determine if the Sourcefire intrusion detection system has been securely deployed and properly maintained. The Sourcefire Configuration Checklist does just that by going into detail about known issues with this system. The other checklists, documentation, physical security, network devices, are very dependent on the company situation. The checklists, within this audit, provide a good starting point to the development of more personalized checklists. However, these types of checklists should be created after the initial research has been conducted for the specific environment in which the intrusion

detection system will be deployed. It is the opinion of the auditor that the entire audit objectives have been addressed and discussed within the checklists provided.

# 5 Risk Assessment

## 5.1 Summary

An audit of the Sourcefire Intrusion Detection System was conducted to determine the if the system was being deployed, configured, and utilized according to company policies, procedures, and industry best practices. Overall the audit was successful and demonstrated that the Sourcefire system is, for the most part, configured correctly. Major issues that should be address came more from the environment that the system is deployed in rather than the actual system itself. The following findings are several key issues, taken from the results of the audit, which should be addressed by management and/or the administrators.

## 5.2 Audit Findings

### 5.2.1 Documentation

**Observation:**
**TEST CASE #1:** There are no change logs on the IDS devices.

**Risk:** Change logs provide a system of accountability as well as show a current state of configuration for a device. Without such a document, changes can be made to a system that can cause the sensors to miss reconnaissance efforts or malicious attacks. An example of this would be test changes that are made to a system but are not changed back. If there were a requirement that all changes are documented in a change log then during a daily or weekly review it can be noticed that this configuration was never changed back. Without a change log the failure to change the system back to its proper configuration could go unnoticed indefinitely.

**Recommendation:** Change log documents should be provided for each IDS device. A policy needs to be created, documentation written, and training needs to be conducted.

**Cost:** Implementing a change log system should not take an administrator more than two days. Training personnel on the use of the change logs should take about an hour.

### 5.2.2 Physical Security

**Observation:**
**TEST CASE #1:** Physical security at the server racks and on the servers themselves was nonexistent.

**Risk:** Unauthorized physical access to the network and individual systems could lead to a compromise that may or may not be detected. Systems can be changed, pilfered, unplugged, or even destroyed under these circumstances.

**Recommendation:** Servers and server racks should be locked at all times. The keys to these devices should be controlled and access limited to a single point. All access to any device should be documented by recording the accessing individual, time of key checkout and return, and purpose for accessing the device.

**Cost:** A small team should be able to complete this task in about a week's time.

### 5.2.3 Network Devices

**Observation:**
**TEST CASE #4:** Load balancers are configured to deny all ping (echo and echo-reply) traffic within the network.

**Risk:** The IDS sensors will miss reconnaissance efforts by malicious intruders or insiders.

**Recommendation:** Simply reconfigure the load balancers to allow all traffic from anywhere to anywhere.

**Cost:** Reconfiguring the load balancers and changing the configuration documentation should not take one person more than three hours.

**Observation:**
**TEST CASE #5:** Workstations on wheeled carts and mobile monitor/keyboard/mouse setups were present and uncontrolled on the server room floor.

**Risk:** These devices can be used to access any device on within the server room. Coupled with the fact that access to the racks and devices are not controlled, this leaves direct access by malicious insiders uncontrollable. This insider would have the capability of logging into almost any device in the server room directly, bypassing the audit log trail provided by remotely accessing machines.

**Recommendation:** This task can be assigned to the team that is implementing physical access control and should not create a significant amount of extra work.

**Cost:** No extra cost if assigned to the team developing physical access control. If implemented separately then a small team should be able to complete this task in three to four days.

### 5.2.4 Sourcefire Configuration

**Observation:**
**TEST CASE #1:** The current Sourcefire system is not the latest version that is available by the manufacturer due to the amount of time that it takes to evaluate a new product or version. Leaving the system in this state limits the installation

of new rule sets due to the fact that some of the new rules might require changes made to the new version of the software.

**Risk:** If new rule sets are not installed into the sensors, new malicious activity can go unnoticed. A system could be compromised by a new vulnerability and the IDS will never be the wiser.

**Recommendation:** Rules can do not have to be entered as downloaded by the manufacturer (although this is recommended). An administrator can pick and choose the rules that need to be implemented. This means that a rule for a new vulnerability can be inspected, reconfigured (if necessary), and installed into the system.

**Cost:** An extra two to five hours a week should give an administrator ample time to research, reconfigure (if necessary), and implement any new rule sets.

**Observation:**
**TEST CASE #21:** The non-availability of network scanning and vulnerability assessment tools.

**Risk:** Tools are abundantly available throughout the internet. Every time a new vulnerability is discovered somebody is creating a tool that can detect that vulnerability. Most of the time these tools are created for system administrator so that they can detect vulnerability within their networks. However, malicious intruders use these same tools to detect open avenues of approach. If an administrator is not performing periodic scans of the environment then that administrator is completely unaware as to the security holes that infect the network.

**Recommendation:** Have a team of administrators develop a tool kit that can be evaluated an approved for use within the network. This tool kit should be deployed on a laptop because of its mobility and controllability. A policy for the use of this laptop should be developed and access strictly controlled and audited.

**Cost:** Most tools are freeware and readily available for download off of the internet. Commercial tool kits are available but tend to get fairly expensive. A dual boot laptop will fall in the price range of $900-$1500 depending on the features required. A small team of administrator can research the required tools in about one week. Approving these tools will take about three to four hours worth of meetings. Setting up the laptop and downloading the approved tools should only take one administrator one or two days.

**Observation:**
**TEST CASE #23:** File integrity software is used to “fingerprint” a system so no changes can be made to the system without changing the fingerprint. Most of

these systems are automated so that a check is run on a regular basis and the results are sent to an administrator. This allows the administrator to determine if a system has been compromised and to what extent.

**Risk:** Skilled malicious intruders often replace key processes, files, and applications within a system that they have compromised. This, in effect, covers the intruder's tracks and makes it much more difficult to track the individual. Additionally, if the intruder has compromised the intrusion detection system, that intruder now has access to all the information passed to the device, which is everything.

**Recommendation:** File integrity is a major issue when it comes to system security. However, Sourcefire does not support the use of file integrity software on any of their devices. This makes the decision to implement any file integrity software a management issue instead of an administrative issue.

**Cost:** A decision about this subject should not take more than an hour in a conference call. Picking, evaluating it, and implementing a file integrity product will take a two-person team about a two to three weeks.

# 6 Conclusion

On a whole the implementation of the Sourcefire Intrusion Detection System, within this environment is secure and is functioning according to plan. The issues about physical security are the most pressing of all issues and should be addressed first and with haste. Additionally, company management should reconsider the policy of not allowing any scanning or vulnerability assessment tools within the environment. These tools are necessary equipment to any network or network security administrator. With careful consideration safe tools can be found and when controlled on a device with which there is limited access the risk can be minimized significantly.

# 7 Instructional Images

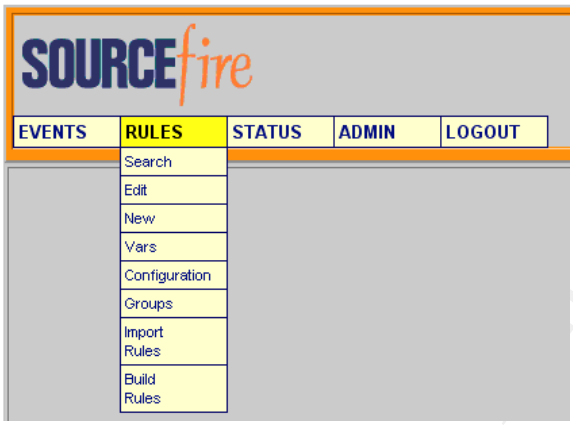



**Figure 27 Select Rules - Search**

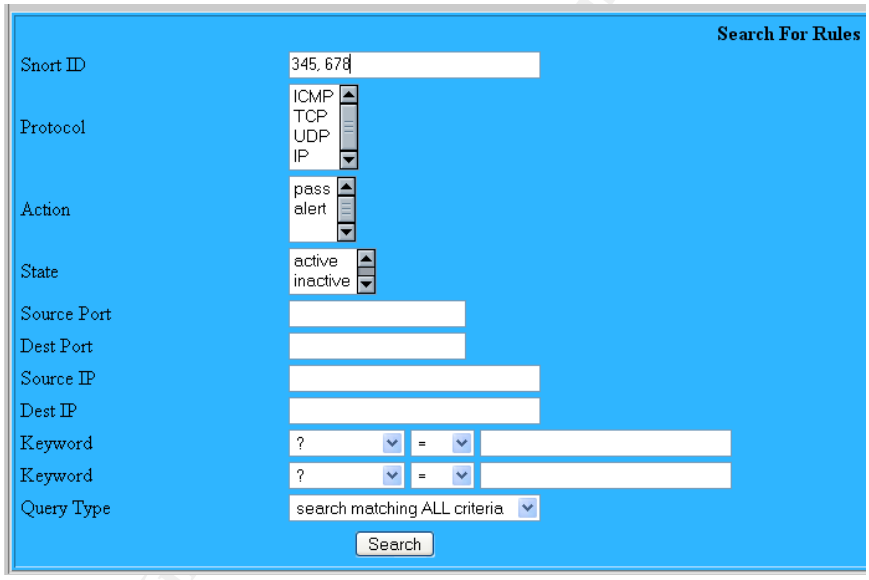



Figure 28 Select Multiple Rules

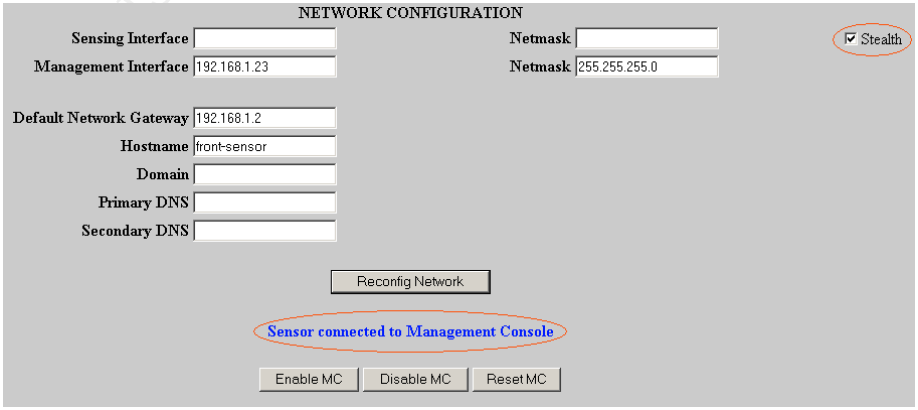



**Figure 29 Network Sensor Interfaces**

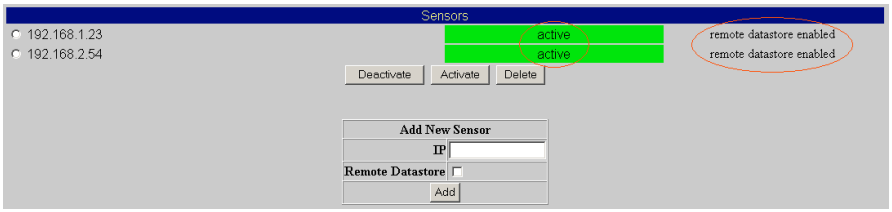



**Figure 30 Management Console Sensor Configuration**

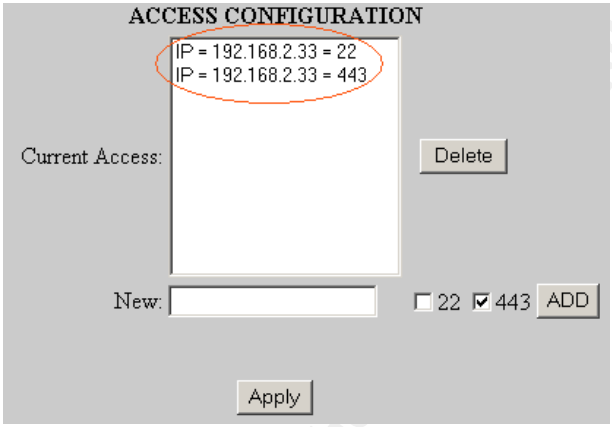



**Figure 31 Access Configuration**

| Subsystem Configuration | Advanced |
|---|---|
| Back Orifice Detection | on off |
| Checksum Verification | Turn off checksums Turn on all checksums No IP checksums<br>No TCP checksums No UDP checksums No ICMP checksums |
| IP Defragmentation | on off |
| HTTP Normalization | on off |
| RPC Normalization | on off |
| Stateful Inspection and Stream Reassembly | on off |
| Telnet Normalization | on off |
| | Submit |

**Figure 32 Sensor Subsystem Configuration**

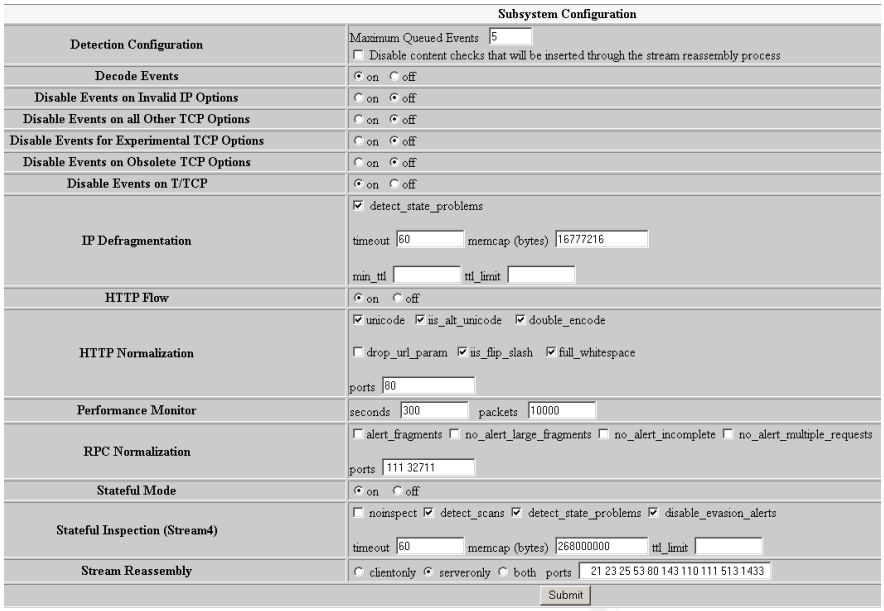



**Figure 33 Sensor Subsystem Advanced Configuration**

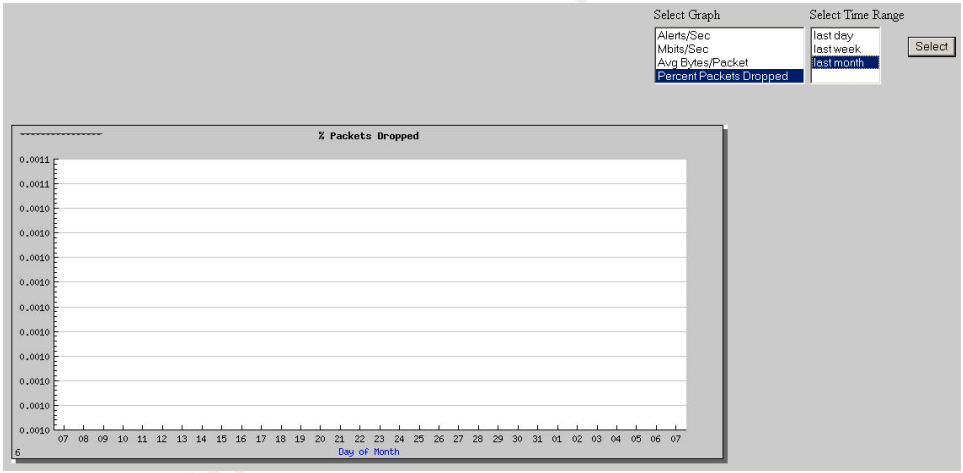



**Figure 34 Dropped Packets**

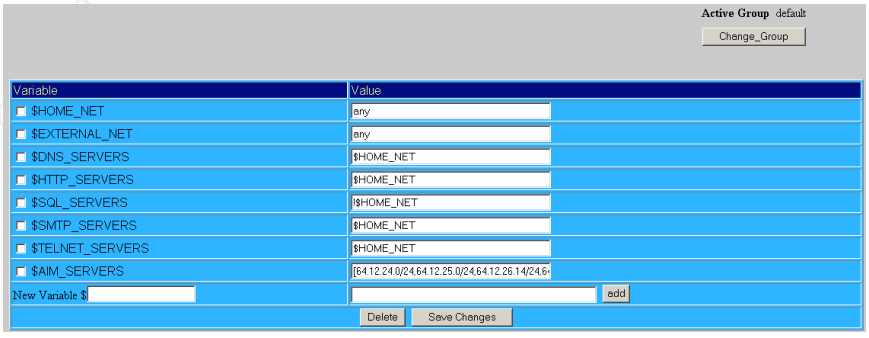
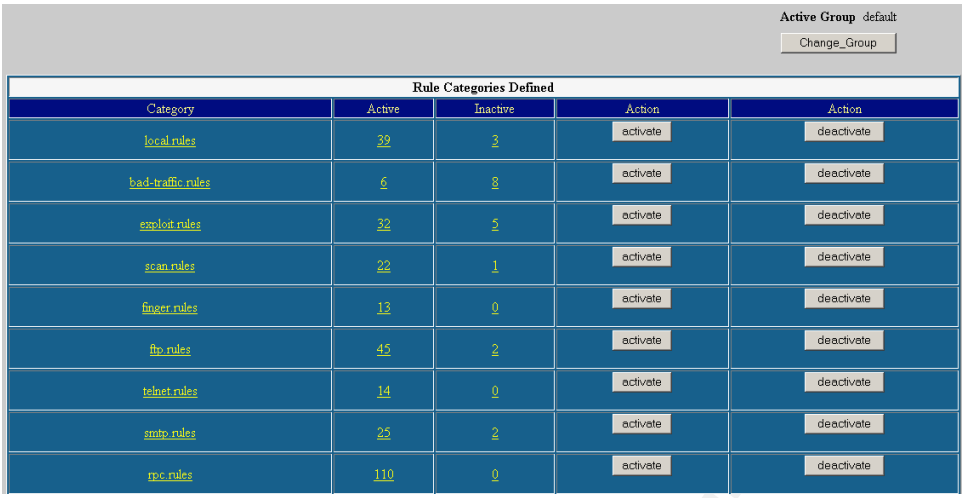



**Figure 35 Variable Configuration Table**



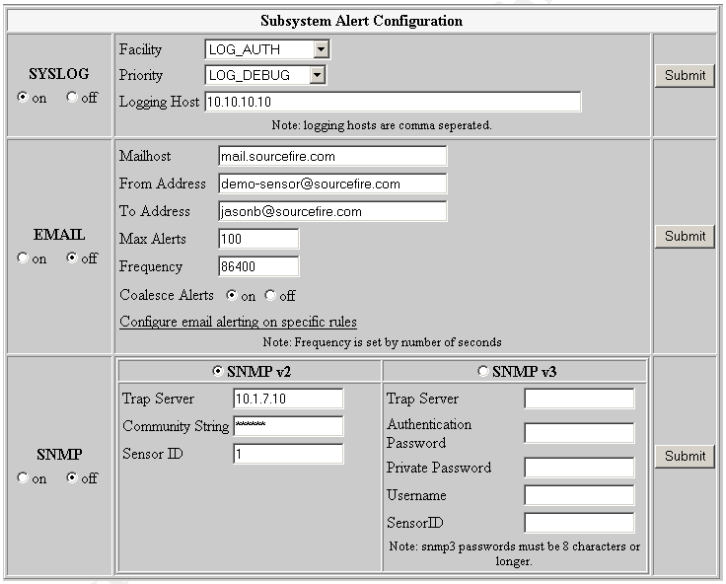
Active Group default

Change_Group

Rule Categories Defined

| Category | Active | Inactive | Action | Action |
|---|---|---|---|---|
| local.rules | 39 | 3 | activate | deactivate |
| bad-traffic.rules | 6 | 8 | activate | deactivate |
| exploit.rules | 32 | 5 | activate | deactivate |
| scan.rules | 22 | 1 | activate | deactivate |
| finger.rules | 13 | 0 | activate | deactivate |
| ftp.rules | 45 | 2 | activate | deactivate |
| telnet.rules | 14 | 0 | activate | deactivate |
| smtp.rules | 25 | 2 | activate | deactivate |
| rpc.rules | 110 | 0 | activate | deactivate |

**Figure 36 Edit Rules Table**



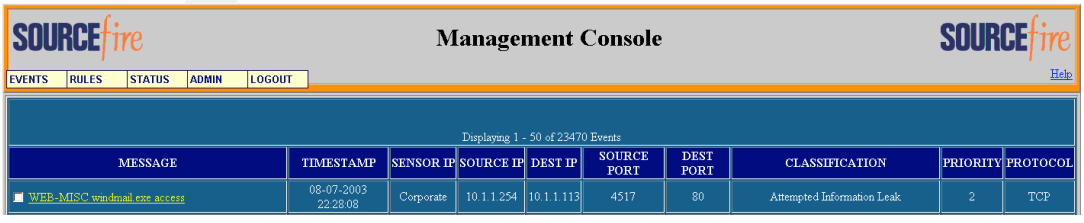
Subsystem Alert Configuration

SYSLOG — on / off
Facility: LOG_AUTH
Priority: LOG_DEBUG
Logging Host: 10.10.10.10
Note: logging hosts are comma seperated.
Submit

EMAIL — on / off
Mailhost: mail.sourcefire.com
From Address: demo-sensor@sourcefire.com
To Address: jasonb@sourcefire.com
Max Alerts: 100
Frequency: 86400
Coalesce Alerts: on / off
Configure email alerting on specific rules
Note: Frequency is set by number of seconds
Submit

SNMP — on / off
SNMP v2: Trap Server 10.1.7.10; Community String; Sensor ID 1
SNMP v3: Trap Server; Authentication Password; Private Password; Username; SensorID
Note: snmp3 passwords must be 8 characters or longer.
Submit

**Figure 37 System Alerting Configuration**



SOURCEfire Management Console SOURCEfire

EVENTS | RULES | STATUS | ADMIN | LOGOUT

Help

Displaying 1 - 50 of 23470 Events

| MESSAGE | TIMESTAMP | SENSOR IP | SOURCE IP | DEST IP | SOURCE PORT | DEST PORT | CLASSIFICATION | PRIORITY | PROTOCOL |
|---|---|---|---|---|---|---|---|---|---|
| WEB-MISC windmail.exe access | 08-07-2003 22:28:08 | Corporate | 10.1.1.254 | 10.1.1.113 | 4517 | 80 | Attempted Information Leak | 2 | TCP |

**Figure 38 MC Alerting Information Leak Attempt**

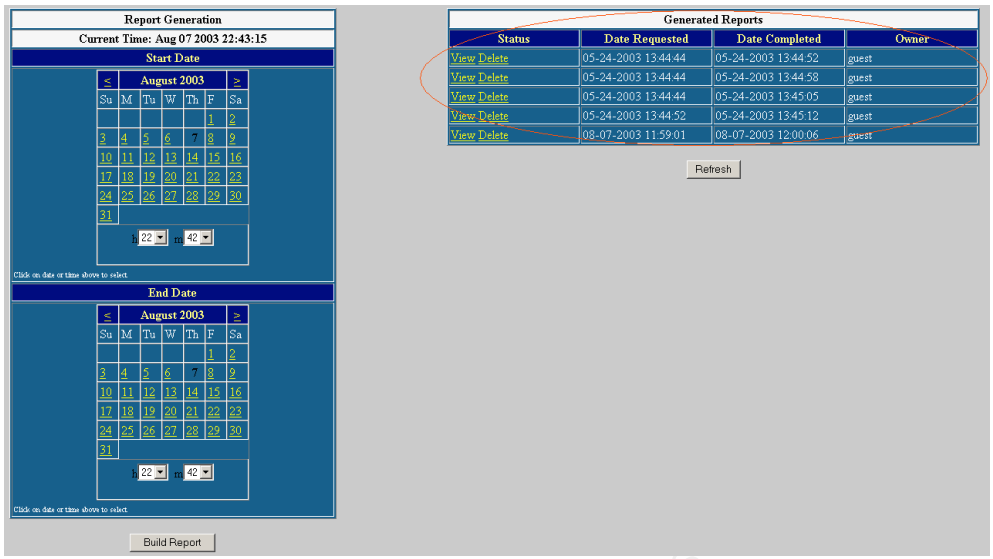



**Figure 39 MC Generated Alert Reports**

# 8 Glossary

| Glossary of Terms | |
|---|---|
| ***Term***[37] | ***Definition*** |
| ACL* | Short for access control list, a set of data that informs a computer's operating system which permissions, or access rights, that each user or group has to a specific system object, such as a directory or file. Each object has a unique security attribute that identifies which users have access to it, and the ACL is a list of each object and user access privileges such as read, write or execute. |
| APACHE* | a public-domain open source Web server developed by a loosely-knit group of programmers. |
| BARNYARD[38] | Output spool reader for Snort! This program decouples output overhead from the Snort network intrusion detection system and allows Snort to run at full speed. It takes input and output plugins and can therefore be used to convert almost any spooled fil |
| best practices[39] | A Best Practice is comprised of policies, principles, standards, guidelines, and procedures that contribute to the highest, most resource-effective performance of a discipline. Best Practices are based upon a broad range of experience, knowledge, and extensive work with industry leading clients. |
| COTS* | Short for commercial off-the-shelf, an adjective that describes software or hardware products that are ready-made and available for sale to the general public |
| fiber optics* | A technology that uses glass (or plastic) threads (fibers) to transmit data. A fiber optic cable consists of a bundle of glass threads, each of which is capable of transmitting messages modulated onto light waves. |
| file integrity software[40] | [A]… program monitors key attributes of files that should not change, including binary signature, size, expected change of size, etc. The hard part is doing it the right way, balancing security, maintenance, and functionality. |
| firewall* | A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. |
| GUI* | A program interface that takes advantage of the computer's graphics capabilities to make the program easier to use. |
| HTTPS* | Short for Secure Sockets Layer, a protocol developed by Netscape for transmitting private documents via the Internet. |
| IDS* | An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. |
| incident response | A reaction to a particular set of events. |
| load balancer | A device that distributes incoming traffic across multiple servers to |

[37] The definition of all terms that are followed by are * have been provided by "Webopedia: Online Dictionary for Computer and Internet Terms" – URL: http://www.webopedia.com, 08/13/2003
[38] "Barnyard at Sourceforge" – URL: http://sourceforge.net/projects/barnyard/, 08/13/2003
[39] "A Best Practices Assessment: A white paper prepared by Tom Finneran, Principal Consultant, CIBER, Inc" – URL: http://www.ciber.com/downloads/whitepapers/bestpractices/, 08/13/2003
[40] "What is tripwire?" – URL: http://www.tripwire.org/qanda/index.php#1, 08/13/2003

| Glossary of Terms | |
|---|---|
| **Term**[37] | **Definition** |
| | increase performance. |
| log_auth[41] | The authorization system: login(1), su(1M), getty(1M), etc. ftpd(1M), and rshd(1M) also use LOG_AUTH. |
| log_debug[39] | Messages that contain information normally of use only when debugging a program. |
| IP address* | An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. |
| MC | Sourcefire Management Console, a device that manages the Sourcefire Network Sensors |
| MYSQL* | MySQL is an open source RDBMS that relies on SQL for processing the data in the database. |
| network diagram | An illustration that demonstrates the configuration of an entire network in a logical view. |
| NTP* | Short for Network Time Protocol, an Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network of computers. |
| NTPDATE[42] | set the date and time via NTP |
| OSHA[43] | The mission of the Occupational Safety and Health Administration (OSHA) is to save lives, prevent injuries and protect the health of America's workers. To accomplish this, federal and state governments must work in partnership with the more than 100 million working men and women and their six and a half million employers who are covered by the Occupational Safety and Health Act of 1970. |
| PDF* | Short for Portable Document Format, a file format developed by Adobe Systems. |
| proxy* | A server that sits between a client application, such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server. |
| RJ-45* | Short for Registered Jack-45, an eight-wire connector used commonly to connect computers onto a local-area networks (LAN), especially Ethernets. RJ-45 connectors look similar to the ubiquitous RJ-11 connectors used for connecting telephone equipment, but they are somewhat wider. |
| rlogin[44] | Rlogin starts a terminal session on a remote host host. |
| router* | A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect. |
| sensor | A device that monitors network traffic. |
| SNMP* | Short for Simple Network Management Protocol, a set of protocols for managing complex networks. |
| SNORT[45] | Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be |

[41] "Syslog notes" by Jack Suess – URL: http://userpages.umbc.edu/~jack/ifsm498d/syslog.html, 08/13/2003
[42] "man ntpdate" – URL: http://linux.ctyme.com/userdoc/ntp-4.1.1/ntpdate.htm, 08/13/2003
[43] "U.S. Department of Labor: Occupational Safety & Health Administration" – URL: http://www.osha.gov/oshinfo/mission.html, 08/13/2003
[44] "man rlogin" – URL: http://linux.ctyme.com/man/man2824.htm, 08/13/2003

| Glossary of Terms | |
|---|---|
| **Term**[37] | **Definition** |
| | used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. |
| SSH* | Developed by SSH Communications Security Ltd., Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist. |
| stealth mode | A setting for an interface that allows it to monitor network traffic in promiscuous mode without being assigned an IP address. This interface is virtually invisible to the rest of the network. |
| SYSLOG[39] | Syslog allows you to encode messages by level and by facility. Levels can be considered various levels of a problem (e.g. warning, error, emergency) whereas facilities are considered to be service areas (e.g. printing, email, network ). Syslog also allows you to forward log entries to another machine for processing, in this way syslog functions as a distributed error manager. |
| TELNET* | A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. |
| tuning | An ongoing effort to distinguish between normal network traffic and traffic that should generate an alert. "Tuning" helps minimize false positives and false negatives. |

**Table 11 Glossary of Terms**



[45] "Snort" – URL: http://www.snort.org/about.html, 08/13/2003

## 9 References

1. Sourcefire Products" – URL: http://www.sourcefire.com/products/products.htm – 07/08/2003
2. "Sourcefire Support Login" – URL: https://support.sourcefire.com, 07/16/2003
3. "Sourcefire Network Sensor" – URL: http://www.sourcefire.com/products/ntwrk_sensor/SF_sensor_flyer_0403.pdf – 07/08/2003
4. "Sourcefire Management Console" – URL: http://www.sourcefire.com/products/mgmt_csle/SF_mgmt_console_0403.pdf – 07/08/2003
5. "National Institute of Standards and Technology" – URL: http://www.nist.gov – 07/08/2003
6. "National Institute of Standards and Technology: Computer Security Plans References for High-Risk Review" – URL: http://csrc.nist.gov/cseat/cseat_computer_security_plans_ref_hr.html, 07/08/2003
7. "Virginia Alliance Standard Compliance Checklist" – URL: http://www.vascan.org/checklist/physical_security_check.html, 07/08/2003
8. "System Security Plan Development Assistance Guide" by SANS Institute 2003 - URL: http://www.sans.org/rr/special/NIALV/kessler.pdf, 07/08/2003
9. Snort Documentation – URL: http://www.snort.org/docs/, 07/08/2003
10. "The Australian Computer Emergency Response Team (AusCERT) and the CERT® Coordination Center (CERT/CC): UNIX Security Checklist v2.0" – URL: http://www.cert.org/tech_tips/usc20_full.html, 07/09/2003
11. "GSNA Study Guide" by SANS personnel and associates – URL: http://www.giac.org/gsna_study_guide_v11.pdf, 08/13/2003

12. “BUILDING SAFETY CHECKLIST” by the New Zealand Fire Service - URL: http://www.fire.org.nz/building/evac_proc/step3/build_check.PDF, 07/14/2003
13. “Occupational Health and Safety Checklist” by University of Washington - College of Engineering – URL: http://www.engr.washington.edu/facilities/Checklist_C.html, 07/14/2003
14. “National Institute of Standards and Technology: Physical Security References for High-Risk Review” – URL: http://csrc.nist.gov/cseat/cseat_physical_security_ref_hr.html, 07/08/2003
15. “US Code Collection” supplied by Legal Information Institute – URL: http://www4.law.cornell.edu/uscode/29/654.html, 07/15/2003
16. “Emerging Technology: Deploying an Effective Intrusion Detection System” by Ram??n J. Honta????n” – URL: http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=8702894&pgno=1, 07/15/2003
17. “How do you implement IDS (network based) in a heavily switched environment?” by Brian W Laing – URL: http://www.sans.org/resources/idfaq/switched.php, 07/15/2003
18. “UW Security Site--Protect your file server” – URL: http://www.washington.edu/computing/security/servers.html, 07/15/2003
19. “APPENDIX A: Sample Network Banner Language” by U.S. Department of Justice - Criminal Division, (Computer Crime & Intellectual Property Section) – URL: http://www.usdoj.gov/criminal/cybercrime/s&sappendix2002.htm, 07/17/2003
20. “Strong passwords” – URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/windows_password_tips.asp, 08/01/2003

21. “National Institute of Standards and Technology: http://csrc.nist.gov/cseat/cseat_it_security_controls_ref_hr.html” – URL: http://csrc.nist.gov/cseat/cseat_it_security_controls_ref_hr.html, 08/01/2003
22. “Webopedia: Online Dictionary for Computer and Internet Terms” – URL: http://www.webopedia.com, 08/13/2003
23. “U.S. Department of Labor: Occupational Safety & Health Administration” – URL: http://www.osha.gov/oshinfo/mission.html, 08/13/2003
24. “Webopedia: Online Dictionary for Computer and Internet Terms” – URL: http://www.webopedia.com, 08/13/2003
25. “Barnyard at Sourceforge” – URL: http://sourceforge.net/projects/barnyard/, 08/13/2003
26. “A Best Practices Assessment: A white paper prepared by Tom Finneran, Principal Consultant, CIBER, Inc” – URL: http://www.ciber.com/downloads/whitepapers/bestpractices/, 08/13/2003
27. “What is tripwire?” – URL: http://www.tripwire.org/qanda/index.php#1, 08/13/2003
28. “Syslog notes” by Jack Suess – URL: http://userpages.umbc.edu/~jack/ifsm498d/syslog.html, 08/13/2003
29. “U.S. Department of Labor: Occupational Safety & Health Administration” – URL: http://www.osha.gov/oshinfo/mission.html, 08/13/2003
30. “Snort” – URL: http://www.snort.org/about.html, 08/13/2003
31. “man rlogin” – URL: http://linux.ctyme.com/man/man2824.htm, 08/13/2003
32. “man ntpdate” – URL: http://linux.ctyme.com/userdoc/ntp-4.1.1/ntpdate.htm, 08/13/2003
33. “Locking Down Your Linux Box - A Checklist Approach” – URL: http://georgetoft.com/linux/security/locking/checklist.shtml, 08/13/2003
34. “Auditing a Distributed Intrusion Detection System: An Auditors Perspective” by Darrin Wassom – URL: http://www.giac.org/practical/Darrin_Wassom_GSNA.doc, 08/13/2003

35. “Snort Intrusion Detection System Audit: An Auditor's Perspective” by Jason Trudel – URL: http://www.giac.org/practical/GSNA/Jason_Trudel.pdf, 08/13/2003
36. Brian Caswell, Jay Beale, James C. Foster, Jeremy Faircloth, “Snort 2.0 Intrusion Detection,” Syngress, 2003

Last Updated: August 17th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| **SANS Network Security 2017** | **Las Vegas, NV** | **Sep 10, 2017 - Sep 17, 2017** | **Live Event** |
| **SANS AUD507 (GSNA) @ Canberra 2017** | **Canberra, Australia** | **Oct 09, 2017 - Oct 14, 2017** | **Live Event** |
| **SANS 2018** | **Orlando, FL** | **Apr 03, 2018 - Apr 10, 2018** | **Live Event** |
| **SANS OnDemand** | **Online** | **Anytime** | **Self Paced** |
| **SANS SelfStudy** | **Books & MP3s Only** | **Anytime** | **Self Paced** |