Auditing a Symantec VelociRaptor Firewall
An Independent Auditor's Perspective

GIAC System and Network Auditor (GSNA)
Practical Assignment v2.1

Jeff Horne
November, 2003

Abstract:

While businesses can not solely rely on firewalls to protect their computing assets, securing the network perimeter with a firewall is still a critical piece of overall security architecture. Defense in depth, or multi-layered protection is comprised of various tools that must work together to provide the desired level of security. The perimeter firewall is only one piece of this defensive strategy but it is a key piece that must be maintained as securely as possible since a firewall that is not kept secure only gives a false sense of safety. One way to make sure that an adequate level of security is maintained is by periodic audits. This paper documents the audit of a corporation's perimeter firewall as part of the requirements for the GIAC Systems and Network Auditor (GSNA) certification.

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

1.1 Identify the system to be audited.

The subject of this audit is a VelociRaptor firewall appliance. The firewall is part of the security architecture designed to protect the computing resources of an imaginary company known as GIAC Enterprises, Inc., described in an earlier paper by this author. [1] GIAC Enterprises uses the Internet extensively in its day-to-day business: selling fortune cookie fortunes. Customers view GIAC's product line and download the fortunes using the company's web server; they also contact sales people and receive bills by electronic mail. Employees use the Internet to exchange mail with potential or current customers and research new fortune cookie sayings. The company also has an internal, corporate network used to transfer information between employees and facilitate access to data resources. The firewall prevents unauthorized access to GIAC Enterprises' systems and data, thereby maintaining the confidentiality, availability and integrity of that data.

1.1.1 System Specifications:

Operating System: Linux
Hardware: VelociRaptor 1300

- 1GB main memory
- 1 1GB hard drive & 1 26 GB hard drive
- 110v AC power (no special power requirement)
- 1.0 GHz processor
- 3 Network Interfaces: Internal, External and Service Net

The service network is connected to the third NIC on the firewall and it is where the company's external web, mail and DNS servers are connected.

1.1.2 Firewall Specifications:

The firewall is Symantec's VelociRaptor Firewall, an integrated hardware and software appliance that runs on a hardened Linux kernel. The VelociRaptor uses vendor-supplied application proxies to provide transparent network connectivity between corporate users and remote, Internet resources. An application proxy, also known as a proxy daemon, is an application that runs on the firewall and acts as both a server and a client, accepting connections from a client and making requests on behalf of the client to the destination server.

An important security feature of the firewall is that, by default, all connections not specifically permitted by a rule are denied. For specific uses where proxies are

[1] GIAC Firewall and Perimeter Protection Curriculum; SANS Network Security 2000 Practical Assignment; Author: Jeff Horne

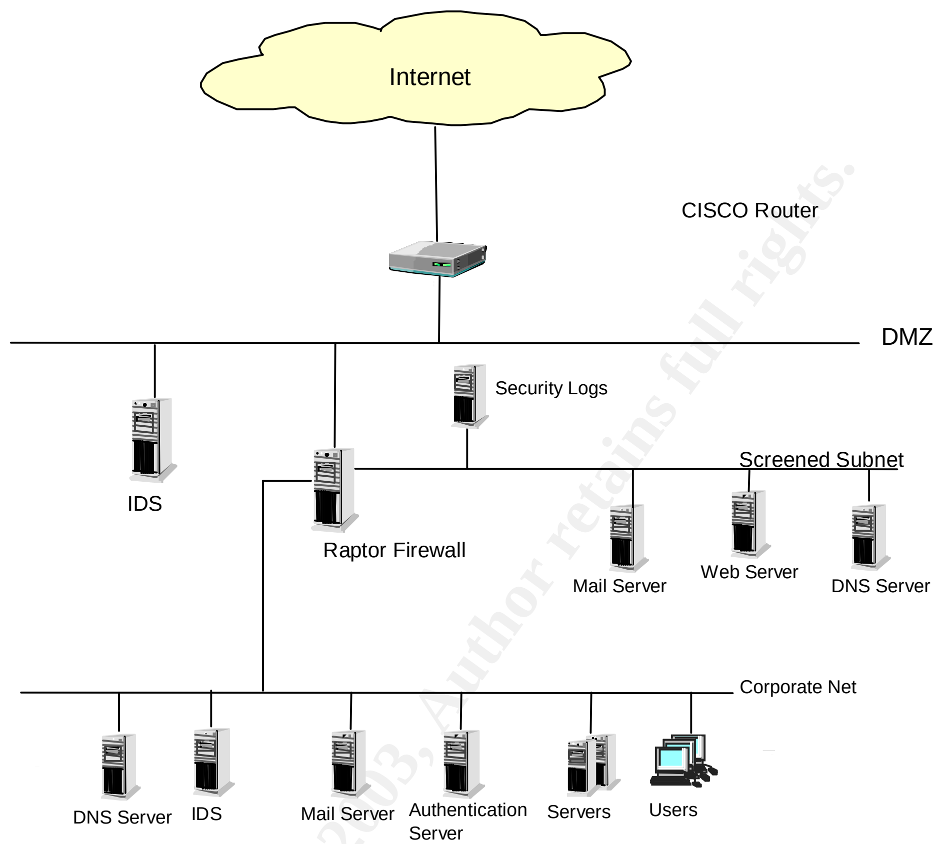
not supplied, packet filtering rules can be developed. The application proxies shown below are supplied with the system:

- FTP
- HTTP/HTTPS
- NetBIOS Datagram Proxy
- Common Internet File System (CIFS)
- DNS
- H.323
- NNTP
- NTP
- Ping
- Real-Time Streaming Protocol
- SMTP
- SQL*Net
- Telnet

1.1.3 Firewall Management Console:

The VelociRaptor firewall is managed using a GUI client, called the Symantec Raptor Management Console (SRMC). The SRMC is designed to work on Windows 2000 and NT 4.0 platforms and provides 3DES-AES encryption between the client and the firewall. There is also a tool called "Secure Remote Login", (SRL) which allows an administrator to login to the system over an encrypted link.

1.1.4 Network Topology:



Network Diagram for GIAC Enterprises

1.2 Evaluate the risk to the system.

In order to evaluate the risk associated with any computer system, especially a firewall, it is important to know what the system is used for, i.e. what it is protecting. GIAC Enterprises uses the Internet extensively in its day-to-day business workings and it is essential for the company to do business. The company also has an internal, corporate network used to transfer information between employees and facilitate access to data resources. The firewall is the main defensive mechanism for GIAC Enterprises' systems and data.

GIAC depends on the Internet to facilitate customers' access to the company's products and employees' access to the customers and research materials. Since the firewall plays a crucial role in the company's ability to function it is important to carefully evaluate potential risks to the system. The overriding objective is to keep the firewall functioning as designed so it protects GIAC's valuable information assets and allows both customers and employees to access the information they need.

When assessing risk to an IT system it is valuable to use existing standards or guidelines so subjective differences are minimized. The National Institute of Standards and Technology (NIST), has developed publication 800-30, entitled "Risk Management Guide for Information Technology Systems"[2] describing a methodology for assessing risks. That methodology is used as the basis for the following risk assessment.

The following steps are used in the risk assessment process:

1. Identify or characterize the system
2. Identify possible threats to the system
3. Identify vulnerabilities of the system
4. List current and planned controls
5. Rate the likelihood of threats being realized
6. Analyze the impact of realized threats
7. Weigh the likelihood of various threats being realized, controls that might mitigate those possibilities and the potential impact of compromise to determine risk.

1.2.1 System Characterization

The system was identified in Section 1.1 above so that information will not be repeated here.

1.2.2 Threat Identification

[2] NIST Publication 800-30; Risk Management Guide for Information Technology Systems; Gary Stoneburner, Alice Goguen, Alexis Feringa

Threats to the firewall can be natural or human. Human threats can be further classified as accidental or deliberate. Natural threat sources consist of the following:

- Flood
- Fire
- Hurricanes
- Tornados
- Earthquakes

Any of these events could be catastrophic to a company's ability to carry on their business but these threats can be fairly easily identified and evaluated. All the above threats essentially constitute a physical threat to the system. Human threats are difficult to defend because of the wide variety of motivations and tools available to the evil-doer.

Potential human threat-sources are described below. Where the threat-source is identified as malicious, possible motivations and the actions they might employ are also listed.

Threat Source	Motivation	Actions
Computer Hackers/Crackers	The challenge of breaking into a system or network, the thrill of evading detection, ego	Unauthorized access to proprietary information, denial-of-service, compromise of information, loss of data.
Industrial Espionage	Economic advantage, competitive edge	Information theft, denial-of-service, modification of data.
Insiders (malicious)	Economic gain, anger, curiosity	Corrupted data, information theft, unauthorized access to information, denial-of-service
Insiders (non-malicious)		Accident, inattention, not following procedures

1.2.3 Vulnerability Identification

The following are *potential* vulnerabilities. The company's security and contingency plans will be reviewed during the actual audit fieldwork.

Vulnerability	Threat-Source	Threat Action
No Disaster-Recovery (DR) plan for the firewall	Natural disasters, malicious or non-malicious insiders	Physical destruction of the firewall.
Inadequate protection and archiving of backups	Natural disasters, malicious or non-malicious insiders	Impede the ability to recover the firewall configuration in case of a major failure.
Inadequate physical security	Malicious or non-malicious insiders	Physical damage to the firewall, unauthorized access to the firewall console.
Inadequate patch level for the Raptor firewall	Hackers, Industrial Espionage, Insiders	Compromise of the firewall or some protected resource behind the firewall using published vulnerabilities.
Inadequate operating system or security patches	Hackers, Industrial Espionage, Insiders	Compromise of the firewall or some protected resource behind the firewall using published vulnerabilities.
Inadequate protection of firewall logs.	Hackers, Industrial Espionage, Insiders	Cover-up of a compromise of the firewall or some other protected resource.

1.2.4 Control Analysis

The following controls reduce the possibility that the identified threats may exploit one or more of the listed vulnerabilities:

- Installation of the firewall in a dedicated, secure computing facility minimizes the opportunity for accidental or intentional damage to the firewall by insiders.
- Having a written policy that includes guidelines for performing backups and installing patches. The policy should require all pertinent patches to be downloaded and tested prior to installation on production systems. Security patches should be given high priority for installation.

1.2.5 Likelihood Determination

The following definitions describe the likelihood that a particular vulnerability will be exploited by one of the identified threat-sources.

Likelihood Level	Likelihood Determination
High	The threat-source is highly motivated and capable and defensive controls to prevent exploitation of the vulnerability are ineffective.
Medium	The threat-source is highly motivated and capable but effective controls are in place that may inhibit exploit of the vulnerability.
Low	The threat-source lacks motivation or capability OR controls exist to significantly inhibit exploit of the vulnerability.

Vulnerability	Threat-Source	Threat-Action	Likelihood
No Disaster-Recovery (DR) plan for the firewall	Natural disasters, equipment failure, malicious or non-malicious insiders	Physical destruction of the firewall.	Medium*
Inadequate archiving of backups	Natural disasters, malicious or non-malicious insiders	Impede the ability to recover the firewall configuration in case of a major failure.	Medium
Lack of control of the Raptor console software: Raptor Management Console (SRMC)	Malicious insiders	Gain unauthorized access to the firewall. Modify rules install back-door software.	High
Inadequate physical security	Malicious or non-malicious insiders	Physical damage to the firewall, unauthorized access to the firewall console.	Medium
Inadequate patch level for the Raptor firewall	Hackers, Industrial Espionage, Insiders	Compromise of the firewall or some protected resource behind the firewall using published vulnerabilities.	Low

Vulnerability	Threat-Source	Threat-Action	Likelihood
Inadequate operating system or security patches	Hackers, Industrial Espionage, Insiders	Compromise of the firewall or some protected resource behind the firewall using published vulnerabilities.	Low
Inadequate protection of firewall logs.	Hackers, Industrial Espionage, Insiders	Cover-up of a compromise of the firewall or some other protected resource.	Low

Although natural disasters can not be predicted, GIAC Enterprises is geographically located were hurricanes are not a problem and the incidence of tornados and earthquakes is very low. Additionally, GIAC's computer facility does not use water for fire suppression but does have an inert-gas system in place. The likelihood of this vulnerability is rated as "medium" because it is poor practice to not have a DR plan in place.

1.2.6 Impact Analysis

Since GIAC Enterprises is an Internet-based company, anything that adversely affects the firewall has potential to be very damaging to the business. Denial of customers' ability to access the web server prevents the company from completing sales and having potential customers view their web page. Defacement of the web page would be an embarrassment to the company and also deny legitimate use. Similarly, compromise of the corporate mail server could cause loss of customer confidence and potential revenue. Theft or destruction of data from a server on the corporate network could compromise customer information and potentially lose billing data. The potential impact of the above listed vulnerabilities being realized is defined in the following terms:

Magnitude of Impact	Definition of Impact
• High	The result may be an *extremely* costly loss of assets or *significantly* damage to the organization's mission.
• Medium	The result may be a costly loss of assets or damage to the organization's mission or reputation.
• Low	The result may be some loss of assets or noticeable damage to the organization's mission or reputation.

Vulnerability	Threat-Action	Likelihood	Impact
Inadequate or non-existent Disaster-Recovery (DR) plan for the firewall.	Catastrophic failure of the firewall.	Medium	High
Inadequate archiving of backups.	Impede the ability to recover the firewall configuration in case of a major failure.	Medium	High
Inadequate physical security	Physical damage to the firewall, unauthorized access to the firewall console.	Medium	High
Lack of control of the Raptor console software: RMC	This console client is used to remotely manage the firewall.	Low	High
Misconfiguration of the firewall rulebase	Unauthorized access to company information, compromise of a protected resource on the corporate network or the service net.	Low	High
Inadequate patch level for the Raptor firewall	Compromise of the firewall or some protected resource behind the firewall using published vulnerabilities.	Low	High
Inadequate operating system or security patches	Compromise of the firewall or some protected resource behind the firewall using published vulnerabilities.	Low	High
Inadequate protection of firewall logs.	Cover-up of a compromise of the firewall or some other protected resource.	Low	High

1.2.7 Risk Determination

Once the threats, vulnerabilities, likelihoods and impacts have been considered we can develop a determination of overall risk to the system. First, we show the formulas used, factoring in all the above information.

Threat Likelihood	Impact Low (10)	Medium (50)	High(100)
High (1.0)	Low 10 x 1.0 = 10	Medium 50 x 1.0 = 50	High 100 x 1.0 = 100
Medium (0.5)	Low 10 x 0.5 = 5	Medium 50 x 0.5 = 25	Medium 100 x 0.5 = 50
Low (0.1)	Low 10 x 0.1 = 1	Low 50 x 0.1 = 5	Low 100 x 0.1 = 10

Finally, we calculate the risk level for each of the identified vulnerabilities:

Vulnerability	Likelihood	Impact	Risk Level
No Disaster-Recovery (DR) plan for the firewall	Medium	High	Medium (50)
Inadequate archiving of backups	Medium	High	Medium (50)
Lack of control of the Raptor console software: Raptor Management Console (RMC)	Low	High	Low (10)
Inadequate physical security	Medium	High	Medium (50)
Inadequate patch level for the Raptor firewall	Low	High	Low (10)
Inadequate operating system or security patches	Low	High	Low (10)
Inadequate protection of firewall logs.	Low	High	Low (10)

1.3 Describe the current state of practice.

When auditing any computer system, particularly a security device, there are several areas that must be considered to provide a comprehensive picture of the system's security. The most obvious area is the technical, i.e. how the system is configured, patched etc. Other aspects, such as change management, disaster recovery plans and access controls are also very important and must not be overlooked if a complete overall picture is to be developed. Failure to adequately audit all these areas can lead management to a false sense of security. The scope of this audit is the firewall itself; therefore the other areas will be covered only as they relate to the overall security of the firewall.

Numerous articles, white papers and books are available to assist anyone wanting to do a technical audit of firewalls and other perimeter security devices. No resources were found that specifically detail checks for a Raptor firewall but there are numerous lists for auditing firewalls in general. Personal experience of the auditor, Internet searches and various security books were used in researching this topic. The following resources were used to develop the audit checklist for this firewall:

General Resources:

Author	Link/Title
Shon Harris	CISSP Certification All-In-One Exam Guide McGraw-Hill/Osborne, 2002
Gary Stoneburner, Alice Goguen, Alexis Feringa	Risk Management Guide for Information Technology Systems www.nist.org
Various Authors	SANS Auditing Firewalls Perimeters and Systems
Colin Rose	Computer Security Audit Checklist http://www.itsecurity.com/papers/iomart2.htm

Firewall Resources:

Author	Link/Title
Lance Spitzner	Auditing Your Firewall Setup http://www.spitzner.net/audit.html
Bennett Todd	Auditing Firewalls: A Practical Guide http://www.itsecurity.com/papers/p5.htm
Symantec Knowledgebase	http://www.symantec.com/techsupp/enterprise/products/sym_velociraptor/sym_vr_15_1200_1300/hot_topics_ts.html
FireTower FAQ for Raptor firewalls	http://www.firetower.com/faqs/index.html

Assignment 2: Create an Audit Checklist

The steps in the audit checklist are divided into general categories:

- Physical/Access
- Documentation/Procedures
- Technical

2.1 Physical/Access Controls

2.1.1 Verify that physical access to the firewall is restricted.

- Reference: 1, 3, 9, 10, 13
- Control Objective: Limit access to the firewall system to authorized security and sysadmin personnel.
- Risk: Physical access to the firewall can provide the means for an attacker to shutdown, damage or compromise the security of the system.
  Likelihood: Low. This type of threat would have to come from an insider with both the desire and technical know-how to compromise the firewall
  Severity: High. Although unlikely, if this situation were to occur, such an insider could cause an outage to the firewall or compromise its security.
- Compliance: The firewall should be in a locked room with access given to a specified list of personnel. The list should be available for review. Compliance is measured within an acceptable range: there can be some physical security
- Testing: Perform and on-site inspection of the data center and observe the security measures in place to restrict access. Controls should include cipher or card-reader locks. Review the access list for those authorized to access the firewall.
- Objective/Subjective: Objective

2.1.2 Verify that environmental controls are adequate to protect the firewall.

- Reference: 1, 9
- Control Objective: Ensure that the physical environment is designed to keep the firewall functioning as designed.
- Risk: Lack of adequate environmental controls can result in damage to the firewall from water, temperature, dust, fire or electricity. This could cause increased failure rates or complete outages.

Likelihood: High. Poor environmental control carries a high probability of allowing, or causing, damage to the system or its data.

Severity: High. An outage to the firewall would prevent the company from carrying on business over the Internet and cause loss of revenue.

- Compliance: The firewall should be in a protected environment where there is electrical power control, dry fire suppression, temperature, dust and humidity control. Compliance is measured on a sliding scale since some of the protective measures can be in place without all of them being present.
- Testing: Perform and on-site inspection of the data center and observe the environmental control features in place to protect the computer equipment.
- Objective/Subjective: Subjective.

2.1.3 Verify that access to the SRMC software is controlled.

- Reference: 1, 13
- Control Objective: Limit access to the SRMC client software to authorized security personnel. This means controlling the distribution of the client and access to the workstations where it is legitimately installed.
- Risk: Access to the SRMC client increases the opportunity for an unauthorized insider to gain access to the firewall. Although the SRMC client is necessary to access the firewall, possession of the software alone is not sufficient to enable access. Access to a PC running the client and connected to the firewall would allow total control of the firewall.

Likelihood: Medium. The SRMC software is distributed with the firewall software therefore installation media is usually in the hands of the security staff. Access to a security administrator's workstation depends on controls in the software and the awareness and diligence of the staff.

Severity: Medium. Access to the client software alone is not sufficient to gain access the firewall. The firewall allows management connections from systems identified in its configuration files only. If an authorized workstation is used, the user can perform all actions on the firewall.

- Compliance: 1. A list should be available of all those to whom the SRMC client is distributed along with the criteria for distributing the software.
2. Security administrators should receive instruction to never leave their SRMC workstation connected to the firewall when they are not present.
3. The SRMC should automatically break the management connection after a defined idle period.
- Testing: 1. Review the firewall logs for attempts to connect to the firewall on TCP ports: 416, 418 and 423. These are used by the SRMC to connect to the firewall.
2. Interviews should be done with firewall administrators to determine whether they have been made aware of their responsibility.
3. Research on the software should be done to determine if there is some automatic timeout feature.
- Objective/Subjective: Objective

2.2 Documentation/Procedures

2.2.1 Verify the existence of a written security policy for the firewall.

- Reference: 2, 5, 13
- Control Objective: Document how the firewall fits into the company's security objectives.
- Risk: Lack of a written security policy can cause confusion among staff and management and inability to enforce corporate direction.
- Compliance: There should be a written document, signed by management. This is a binary measure since we are only considering whether the document exists.

  Likelihood: High. In a medium/large company there would be many opportunities for employees and management to apply their individual interpretation to what they think the company wants for security.

  Severity: High. Lack of cohesive direction can result in security configurations that allow a successful exploit of the firewall or a resource that it is protecting.

- Testing: Manually examine the document.
- Objective/Subjective: Objective

2.2.2 Determine whether there is written guidance for performing backups on the firewall.

- Reference: 4, 9, 10, 11
- Control Objective: Make sure the firewall itself is being backed up regularly, according to written procedure.
- Risk: Rebuilding the firewall, with all its rules, network objects, etc. from scratch would be very time consuming, error prone and costly. Backups should be well-defined and performed regularly.
- Compliance: Backup procedures should be available in writing for review and should specify the drives or files being backed-up and the frequency of backups.
  Likelihood: High. Disk drive failures could happen at any time, even on new hardware.
  Severity: High. For a business that depends on the Internet, even a brief outage can be costly in terms of lost orders and loss of customer confidence.
- Testing: Manually examine the backup plan or disaster recovery plan.
- Objective/Subjective: Objective

2.2.3 Verify the existence of a Disaster Recovery plan for the firewall.

- Reference: 9, 10, 11
- Control Objective: Ensure there is a plan in case of an extended outage of the firewall. Determine how the company will keep their business processes running.
- Risk: Lack of a disaster recovery plan can result in extended down time if there is a severe failure of the firewall.
- Compliance: Disaster recovery for the firewall should be part of a larger-scale plan for the computing center in general. If there is no overriding document, there should still be a written plan for what to do in case the firewall is unavailable for any reason.
  Likelihood: Low. The firewall is located in a dedicated computer facility which does not allow unrestricted access.
  Severity: High.
- Objective/Subjective: Objective

2.2.4 Verify that there is a written procedure for controlling changes to the firewall.

- Reference: 9, 10
- Control Objective: Ensure that the process for making changes to the operating system and firewall software is clearly defined.
- Risk: Lack of change control can lead to compromise of the firewall's availability or security by mistake or intent. Multiple firewall security and/or system admins can make changes that the others were unaware of were not approved.
- Compliance: A change management procedure should be available in writing.
  Likelihood: Low. The firewall is located in a dedicated computer facility which does not allow unrestricted access.
  Severity: High. Misconfiguration of the firewall or disruption of service could impact the company's business.
- Testing: Manually inspect the change control documentation.
- Objective/Subjective: Objective

2.3 Technical Controls

2.3.1 Review the operating system configuration to make sure that unnecessary services have been disabled.

- Reference: 3, 10, 13
- Control Objective: Verify that the operating system has been configured with the minimum required services.
- Risk: Many services that come with a default operating system installation contain potential vulnerabilities. These vulnerabilities may be exploited and allow compromise of the firewall or systems that it is protecting.
- Compliance: Only network services required to operate the firewall should be enabled, others should be commented out or disabled. This measure is really on a sliding scale since some services could be disabled while some un-necessary services remain enabled.
  Likelihood: Medium. The firewall software should prevent most exploits of the underlying operating system; however, there are some network services that are considered undesirable on any system.

Severity: High. Many default services are very vulnerable to exploit. If this were to occur, the firewall's integrity and that of the systems behind it could be compromised.

- Testing: Manually review the /etc/inetd.conf file and note any services that are not commented out.
- Objective/Subjective: Objective

2.3.2 Ensure that the Raptor firewall and RMC software are patched up to the most current levels.

- Reference: 5, 6, 7, 8, 10, 11, 13
- Control Objective: Verify that the Raptor firewall and the SRMC management stations have been configured with the latest patches available from the vendor.
- Risk: Un-patched vulnerabilities could allow an attacker to compromise the firewall or a resource that it is protecting.
- Compliance: All vendor patches for the VelociRaptor firewall should have been addressed and either installed or non-compliance documented. This is a binary, yes-or-no action.

  Likelihood: High. There is a continuous, high volume of network scanning on the Internet. It is likely that an un-patched system will be discovered and compromised.

  Severity: High. Security patches to the firewall software should be considered of the highest priority. A successful exploit of one of these vulnerabilities could allow an attacker unlimited access to the firewall or the company's network behind the firewall.
- Testing: Look up the latest patches for the VelociRaptor firewall appliance at the following URL: http://www.symantec.com/techsupp/enterprise/products/sym_velociraptor/sym_vr_15_1200_1300/files.html
- Objective/Subjective: Objective

2.3.3 Ensure that all unused proxies are disabled.

- Reference: 1, 3, 13
- Control Objective: Configure the firewall with the minimum set of proxy daemons required to fulfill its mission.
- Risk: Previously undiscovered security flaws in any of the proxy software could allow an attacker to

compromise the firewall or a resource that it is protecting. Also, proxy daemons actively listen for connections and can be detected by port scanners.

- Compliance: Proxies that are not used should be marked as "disabled" in the configuration as viewed with the SRMC. Ports for these proxies should not show up on port scans for the inside, outside or service net interfaces. This is a binary measure since the necessary proxies should be defined by the security policy and in the rulebase.
  Likelihood: Low. The existence of a proxy does not allow traffic to pass through the firewall; a rule is still required.
  Severity: Low. The appearance of a port on a port scan report does not mean there is an actual vulnerability present.
- Testing: Review the list of proxies using the SRMC and verify that the ones that are enabled are actually required by the firewall security policy. Perform an Nmap scan on each interface and identify the ports shown as open.
- Objective/Subjective: Objective

2.3.4 Verify that Network Address Translation (NAT) is in use for all outbound network traffic.

- Reference: 10, 11, 13
- Control Objective: Minimize information leaks about GIAC's internal network.
- Risk: Exposure of internal addresses provides information to potential attackers.
- Compliance: Controls to enable NAT should be enabled on the firewall and no GIAC internal IP addresses should be visible on the Internet.
  Likelihood: Low. NAT is used by default with all preconfigured proxies.
  Severity: Medium. Leaking private address information is not a particular vulnerability but it does provide intelligence about the internal network.
- Testing: Use the SRMC to verify that the NAT feature is enabled. Use tcpdump to observe network traffic at the external firewall interface and see if any inside or service net addresses are seen.
- Objective/Subjective: Objective

2.3.5 Review the rulebase to verify that all rules are current according to the defined security policy.

- Reference: 2, 5, 10, 11, 13
- Control Objective: Verify that the rules enforce the security policy.
- Risk: Having rules that are no longer necessary makes the rulebase more cluttered and confusing for the staff to manage. It also might allow an external or internal user a greater than desired level of access.
- Compliance: All rules on the firewall should correspond to a requirement in the security policy. This measure is binary: each rule either is or is not described by a corresponding policy requirement.
  Likelihood: Medium. Over time rules are added to meet evolving business need and, occasionally, the original need for the rule no longer exists. Keeping the rulebase up-to-date is sometimes overlooked.
  Severity: Medium. Rules that do not reflect the security policy do not necessarily pose a threat.
- Testing: Manually review the security policy and compare it with the defined rules on the firewall.
- Objective/Subjective: Objective

2.3.6 Verify that there are no known vulnerabilities detected on the external (Internet) interface.

- Reference: 1, 3, 5, 10, 11
- Control Objective: Vulnerability and port scans should only show recognized ports listening and no vulnerabilities.
- Risk: The presence of open ports or especially known vulnerabilities indicates the firewall could be successfully attacked by an outside entity. This could lead to a denial of service or compromise of systems behind the firewall.
- Compliance: Scans of the firewall should reveal no high risk vulnerabilities and all ports identified as listening should be identified and documented. This is a binary measure.
  Likelihood: High. Hacking and scanning activities have continued to increase dramatically over the past several years. A firewall that contains exploitable vulnerabilities will be detected and attacked.
  Severity: High. Vulnerabilities on the firewall could compromise the basic function of the firewall, its

ability to protect GIAC's corporate network from unauthorized access.

- Testing: Perform vulnerability and port scans on the external interface of the firewall. Use ISS and Nessus as the scanning tools and compare results.
- Objective/Subjective: Objective

2.3.7 Verify that the firewall is not susceptible to Denial of Service (DoS) attacks.

- Reference: 1, 3, 5
- Control Objective: Ensure the firewall is able to withstand attempts to disrupt its normal function, either by crashing it or rendering it unusable due to high processing load.
- Risk: A successful DoS attack that disrupts the firewall also disrupts access to the web and mail systems behind it on the service network.
- Compliance: The firewall should be able to withstand concerted DoS attacks by common software tools. Compliance is determined by whether the firewall can function properly while under DoS attack.

  Likelihood: Medium. DoS attacks are common on the Internet and can come from various sources, such as anonymous hackers or industry competitors.

  Severity: Medium. This would prevent users from accessing the company's website and potentially lead to loss of customer confidence and revenue.
- Testing: Use ISS Internet Scanner and Nessus to scan the external firewall interface, enabling all DoS attacks.
- Objective/Subjective: Objective

2.3.8 Verify that Anti-Spoofing controls are enabled on the internal and external firewall interfaces and that the firewall detects logs and drops these packets.

- Reference: 5, 10, 11
- Control Objective: Prevent IP spoofed packets from entering or leaving the corporate network.
- Risk: Anti-spoofing helps defend the firewall against spoofed-packet attacks and keeps systems on

GIAC's network from being used in attacks on other networks.

- Compliance: Each network interface configuration has anti-spoofing enabled. Spoofed packets directed at some interface are not passed through the firewall to the destination network.
  Likelihood: Medium. This control is sometimes overlooked during firewall installation.
  Severity: Medium.
- Testing: 1. Verify that spoofed packets are dropped by the firewall by using hping2 to generate some spoofed packets
  2. Review the firewall log for evidence of the spoofed packet activity.
  3. Use "tcpdump" on the firewall to observe the packet traffic on the inside and outside interfaces and verify that it is being dropped.
- Objective/Subjective: Objective

2.3.9 Verify that NTP is being used to synchronize the firewall's time.

- Reference: 10, 11, 13
- Control Objective: Make sure the firewall is synchronized to a standard time for accurate record keeping and event correlation.
- Risk: If the internal clock on the firewall drifts without being corrected it could cause confusion when trying to track some event in the system or firewall log files. Inaccurate time on the firewall could inhibit successful prosecution of computer criminals if that ever became necessary.
- Compliance: The firewall is configured to use NTP to synchronize its system clock with a public NTP server.
  Likelihood: Medium. The amount of suspicious network traffic that must be manually reviewed means it is likely that some event will need to be investigated.
  Severity: Medium. System clocks do not usually drift a large amount in a short period of time. The system clock can be set manually by the firewall administrator.
- Testing: Using the SRMC, select the Proxy Services icon and double-click NTPD. This will display the NTPD Properties page which should show an external NTP server, such as: "ntp2.usno.navy.mil" or "tock.usno.navy.mil".
- Objective/Subjective: Objective

2.3.10 Verify that the firewall's ability to log activity is not degraded by high-volume scans or attacks.

- Reference: 1, 5
- Control Objective: Ensure that the firewall is always able to log activity that it detects, even in the face of intense network scans or DoS attacks.
- Risk: Disruption of normal firewall logging might allow an attacker to perform unwelcome activities while the firewall is "blind".
- Compliance: Firewall logs should show normal logging activity during high-volume vulnerability scans and DoS attacks.

  Likelihood: Medium. If the firewall is undergoing some type of attack that is overwhelming its ability to log traffic, it is possible that some secondary attack is going on concurrently.

  Severity: High. Disabling the firewall's ability to log anomalous network activity cripples an important piece of the firewall's defensive mechanism.
- Testing: Perform high-intensity vulnerability and port scans on the external interface of the firewall. Review the log and verify that all the scanning activity is recorded.
- Objective/Subjective: Objective

2.3.11 Determine whether modifications to critical files are monitored and logged.

- Reference: 1, 9, 10, 11
- Control Objective: Make sure that changes to firewall configuration and system files are tracked for accountability.
- Risk: Files can be modified by multiple firewall administrators or possibly by someone who has compromised the security of the system. No logging of these modifications could allow an outsider or malicious insider to make subtle changes undetected.
- Compliance: The system should be running some software to make a baseline checksum of critical files and regularly compare current checksums to the baseline. This is a binary measure.

  Likelihood: High. Without monitoring files for changes it is very likely that accidental or malicious changes to the configuration that compromise the security of the firewall would go unnoticed.

  Severity: High. Undetected firewall changes could compromise the security of the firewall.

- Testing: Determine whether any type of file-checksum software is present on the system by interviewing the firewall administrator(s).
- Objective/Subjective: Objective

2.3.12 Verify that the firewall's logs are protected off the system.

- Reference: 1, 9, 10, 11
- Control Objective: Ensure that the firewall logs are kept safe from accidental or intentional compromise.
- Risk: A successful attacker would immediately seek to cover their tracks by modifying the logs. If there are no remote copies, all traces of the activity might be lost.
- Compliance: Firewall logs should be either copied to a remote system or concurrently logged to a remote system. Compliance is a binary measure.

  Likelihood: High. The first thing an attacker would try to do is erase evidence of their activity by deleting or modifying the log files.

  Severity: High. If the authenticity of the log files is compromised a penetration of the firewall might continue unnoticed while passwords are recorded and other machines are compromised.
- Testing: Interview the firewall administrators to determine whether the logs are being duplicated on a remote machine.
- Objective/Subjective: Objective

2.3.13 Verify that that firewall management traffic is encrypted.

- Reference: 9, 10, 11
- Control Objective: Ensure that network traffic between the management station running SRMC and the firewall is safe from "eavesdropping".
- Risk: A malicious insider might be able to pick up an administrator's password by using any number of commonly available network "sniffing" tools.
- Compliance: Monitoring the link between the firewall and some SRMC client should show no clear-text. This is a binary measure.

  Likelihood: Medium. A potential hacker would have to be on the internal network and know something about the communication between the firewall and the management client. This would imply not just an insider but a knowledgeable insider.

Severity: High. If someone were knowledgeable and motivated enough to attempt this kind of compromise they would also be able to compromise the security of the firewall.

- Testing: Use tcpdump on the inside interface of the firewall to record traffic from a selected SRMC client to a file. Examine the data to determine whether any of the communication between firewall and client is clear-text.
- Objective/Subjective: Objective

Assignment 3: Audit Evidence

The previous exercise compiled a list of items to be included in the audit. The following pages describe the actual audit field work and detail the results of each step. As directed in the assignment, ten items from the previous list have been selected for this phase. A list of the tools used for the audit is included below:

Hardware:	2 IBM laptop computers running Windows 2000
	2, 4-port10/100 Ethernet hubs
Software:	Nessus, version 2.0.8
	ISS RealSecure Internet Scanner, version 7
	hping2
	tcpdump

Note: Written permission was obtained from GIAC's management prior to commencing the audit.

The ten items chosen for verification from the previous list are:

Task 1: Physical access to the firewall is restricted.
Task 2: Access to the SRMC software is controlled.
Task 3: Unnecessary services have been disabled.
Task 4: The SEF and SRMC software have current patches.
Task 5: Unused proxies are disabled.
Task 6: Network Address Translation is enabled.
Task 7: The rulebase is current with the defined security policy.
Task 8: No known vulnerabilities are detected.
Task 9: The firewall is not susceptible to DoS attacks.
Task 10: Anti-spoofing is enabled.

3.1 Conduct the audit.

3.1.1 Task 1: Verify that physical access to the firewall is restricted.

Procedure:

Perform and on-site inspection of the data center and observe the security measures in place to restrict access. Controls should include cipher or card-reader locks. Review the access list for those authorized to access the firewall.

Results:

This information is based on an on-site inspection and interview with data center personnel. GIAC has a dedicated data-center manned 24 x 7 and access to the data center is controlled by proximity cards and card readers. Assigning of cards is done through the data center manager and is reviewed annually for cards that have not been used. The manager receives notice of employee terminations so cards can be revoked on an ad-hoc basis.

Assessment:

No finding noted.

3.1.2 Task 2: Verify that access to the SRMC software is controlled.

Procedure:

1. Review the firewall logs for attempts to connect to the firewall on TCP ports: 416, 418 and 423. These are used by the SRMC to connect to the firewall. Scripts can be used to search the log files for the most recent quarter. The command "egrep" can be used to check for these ports, for example:
   # egrep –l port=416
2. Interview the firewall administrators to determine whether they have been made aware of their responsibility regarding protection of the SRMC console.
3. Research on the software should be done to determine if there is some automatic timeout feature.

Results:

1. Review of firewall logs for the period July 1, 2003 through September 30, 2003 do not reveal any access attempts on these ports.
2. Interviews of the 4 current firewall administrators revealed that they all knew access to the SRMC had to be protected. Additionally, it was discovered that SRMC software is not loaded on individual administrators' workstations; instead it is installed on two workstations used only for firewall administration in a nearby, controlled-access area.

3. Research showed that the SRMC does not include an automated mechanism to disconnect the control connection with the firewall after a certain amount of time. This is due to the fact that closing the connection when the firewall configuration has been changed but the change has not been committed might cause corruption of some configuration files.

Assessment:

No finding noted. Although the SRMC software does not have an automatic disconnect feature, other controls are in place to prevent misuse of the SRMC.

3.1.3 Task 3: Verify that unnecessary services have been disabled on the firewall.

Procedure:

Manually review the /etc/inetd.conf file and record any services that are not commented out.

Results:

All services in the file were commented out as shown below:

```
[root@GIACfw /root]# more /etc/inetd.conf
#
# inetd.conf    This file describes the services that will be available
#               through the INETD TCP/IP super server.  To re-configure
#               the running INETD process, edit this file, then send the
#               INETD process a SIGHUP signal.
# Version:      @(#)/etc/inetd.conf     3.10    05/27/93
# Authors:      Original taken from BSD UNIX 4.3/TAHOE.
#               Fred N. van Kempen, <waltje@uwalt.nl.mugnet.org>
# Modified for Debian Linux by Ian A. Murdock <imurdock@shell.portal.com>
# Modified for RHS Linux by Marc Ewing <marc@redhat.com>
#
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
#
# Echo, discard, daytime, and chargen are used primarily for testing.
#
# To re-read this file after changes, just do a 'killall -HUP inetd'
#
#echo   stream  tcp     nowait  root    internal
#echo   dgram   udp     wait    root    internal
#discard        stream  tcp     nowait  root    internal
#discard        dgram   udp     wait    root    internal
#daytime        stream  tcp     nowait  root    internal
#daytime        dgram   udp     wait    root    internal
```

```
#chargen        stream  tcp     nowait  root    internal
#chargen        dgram   udp     wait    root    internal
#time   stream  tcp     nowait  root    internal
#time   dgram   udp     wait    root    internal
#
# These are standard services.
#
#ftp    stream  tcp     nowait  root    /usr/sbin/tcpd  in.proftpd
#telnet stream  tcp     nowait  root    /usr/sbin/tcpd  in.telnetd
#
# Shell, login, exec, comsat and talk are BSD protocols.
#
#shell  stream  tcp     nowait  root    /usr/sbin/tcpd  in.rshd
#login  stream  tcp     nowait  root    /usr/sbin/tcpd  in.rlogind
#exec   stream  tcp     nowait  root    /usr/sbin/tcpd  in.rexecd
#comsat dgram   udp     wait    root    /usr/sbin/tcpd  in.comsat
#talk   dgram   udp     wait    root    /usr/sbin/tcpd  in.talkd
#ntalk  dgram   udp     wait    root    /usr/sbin/tcpd  in.ntalkd
#dtalk  stream  tcp     waut    nobody  /usr/sbin/tcpd  in.dtalkd
#
# Pop and imap mail services et al
#
#pop-2   stream  tcp     nowait  root    /usr/sbin/tcpd ipop2d
#pop-3   stream  tcp     nowait  root    /usr/sbin/tcpd in.qpopper
#imap    stream  tcp     nowait  root    /usr/sbin/tcpd imapd
#
# The Internet UUCP service.
#
#uucp   stream  tcp     nowait  uucp    /usr/sbin/tcpd  /usr/lib/uucp/uucico    -l
#
# Tftp service is provided primarily for booting.  Most sites
# run this only on machines acting as "boot servers." Do not uncomment
# this unless you *need* it.
#
#tftp   dgram   udp     wait    root    /usr/sbin/tcpd  in.tftpd
#bootps dgram   udp     wait    root    /usr/sbin/tcpd  bootpd
#
# Finger, systat and netstat give out user information which may be
# valuable to potential "system crackers."  Many sites choose to disable
# some or all of these services to improve security.
#
#finger stream  tcp     nowait  root    /usr/sbin/tcpd  in.fingerd
#cfinger stream tcp     nowait  root    /usr/sbin/tcpd  in.cfingerd
#systat stream  tcp     nowait  guest   /usr/sbin/tcpd  /bin/ps -auwwx
#netstat        stream  tcp     nowait  guest   /usr/sbin/tcpd  /bin/netstat    -f inet
#
```

```
# Authentication
#
#auth   stream  tcp     nowait    nobody    /usr/sbin/in.identd in.identd -l -e -o
#
# End of inetd.conf
#swat      stream  tcp     nowait.400      root /usr/sbin/swat swat
#
# Raptor secure service daemons (none)
#
```

Assessment:

No finding noted.

3.1.4 Task 4: Verify that the SEF and SRMC software patch levels are up-to-date.

Procedure:

All vendor patches for the VelociRaptor and the SRMC should have been reviewed and either installed or non-compliance documented.

1. Get a list of the most current patches and hotfixes from the vendor at the following URL: http://www.symantec.com/techsupp/enterprise/products/sym_ent_firewall/sym_ent_firewall_7_solaris/files.html

2. The patches consist of replacements for specific executables in the SEF configuration directory so the auditor must look at the date and of the patch file and compare it to the creation date of the executable(s) to be replaced to determine whether the newest version is running. For example, in the patch: SG7000-20030605-00, listed below the release date is June 2003. When the patch is downloaded and unzipped you can see that all the files have a creation date of 6/5/03. Compare the files in the SEF configuration directory, /usr/adm/sg and determine their creation date. If the files in the patch are later, they have not been installed.

Results:

Available patches: SG7000-20030605-00 - June 2003 patch
MC7000-20030417-00 - modules for SRMC 7.0

The files updated by the patch are listed below:

(From the URL: ftp://ftp.symantec.com/public/updates/patch-70s-readme.txt)

apache
cifsd
changelog

fetcher
filter
ftpd
gopherd
gwcontrol
httpd
isakmpd
nntpd
notifyd
nsetupd
pgate
pingd
rad
rmcimport
rtspd
saveconfig
setrts
smtpd
statsd
telnetd
tcp_gsp
tcpap_gsp
udp_gsp
vpn
config_files

/kernel/strmod:
vpn driver

After comparing the dates of the existing files in the /var/adm/sg directory, it was determined that the patch had already been installed. The file creation date for files modified by the SRMC patch show they are current as well.

Assessment:

No findings recorded.

3.1.5 Task 5: Verify that unnecessary proxies are disabled.

Procedure:

Review the list of proxies and verify that the ones that are enabled are actually required by the firewall security policy. The file /var/adm/sg/config.cf is the main configuration file used by the Raptor firewall. The list of proxies and their status can be seen in the config.cf file as follows:

The various enable flags
httpd=Enable
gopherd=Disable
telnetd=Disable
ftpd=Enable
srld=Enable # SRL is the Secure Remote Login tool for managing the firewall
dnsd=Enable
notifyd=Enable
nsetupd=Disable
smtpd=Enable
nntpd=Disable
cifsd=Disable
vpnd=Disable
xntpd=Enable
readhawk=Enable # These daemons are used by the SRMC remote management.
gwcontrol=Enable
tacacsd=Enable
realaudio=Disable
visualizer=Disable
eagleslave=Enable
fetcher=Disable
# The sqlnet flag below is ignored on VelociRaptor because sqlnet is not
# a supported component on that platform.
sqlnet=Enable
statsd=Enable
h323d=Disable
pingd=Disable
remlogd=Enable

tcp-gsp=Enable # Auditor's note: the GSPs enable user-defined proxies.
tcpap-gsp=Enable
ip-gsp=Enable
udp-gsp=Enable

nbdgramd=Disable
oobauthd=Disable
rcmd=Disable
rtsp=Disable
wapdgram=Disable
sipd=Disable

Results:

The proxies listed as "enabled" are either required to implement specific items in the security plan or they are required by the SRMC for remote management.

Assessment:

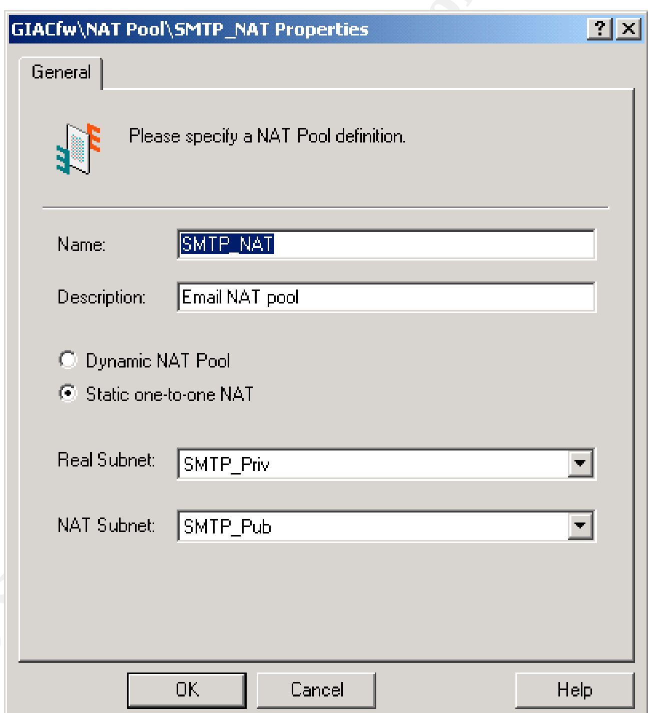
No finding noted.

Task 6: Verify that NAT is enabled.

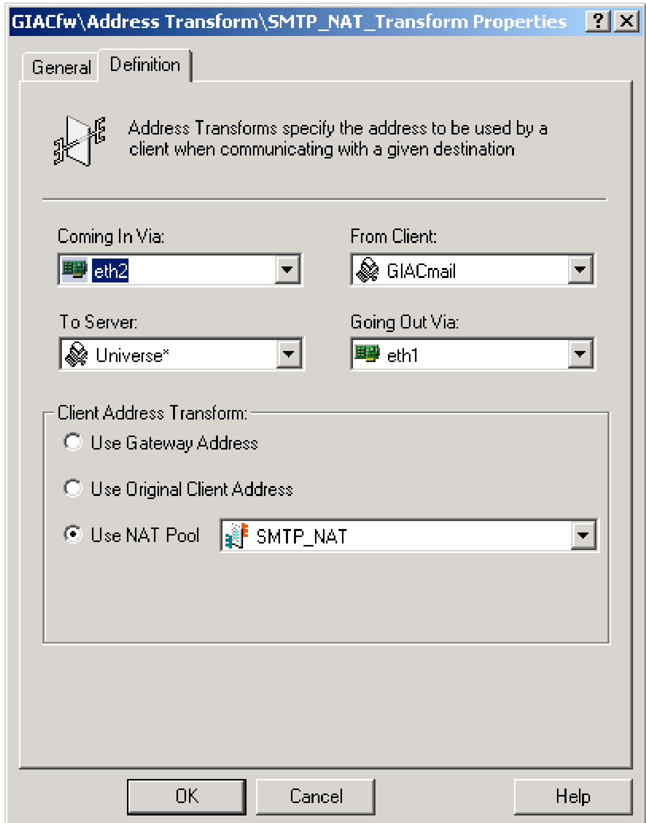
Procedure:

Controls to enable NAT should be enabled on the firewall and no GIAC internal IP addresses should be visible on the Internet. Use the SRMC to verify that NAT is enabled on all interfaces and use tcpdump to check for address leakage.

Results:



Each NAT pool requires a corresponding Address Transform



The following tcpdump command configures the external interface of the firewall to listen for and display any traffic to or from the internal network (192.168.100.0) *OR* the service network (192.168.50.0). The command is set to write its output to a file named /root/addr_leak.tcp.

[root@GIACfw]# *tcpdump -i eth1 -n –v net –w /root/addr_leak.tcp 192.168.100 or net 192.168.50*
tcpdump: listening on eth1

<u>Assessment</u>:

The firewall configuration is correct for setting up NAT for the email server and the http proxy automatically NATs the address of any internal web (http) user to the outside IP address of the firewall. The tcpdump command did not detect any packets although routine email and web traffic were going on during the time it was run.

No finding noted.

3.1.6 Task 7: The rulebase is current with the defined security policy.

Procedure:

All rules on the firewall should correspond to a requirement in the security policy. Obtain printed copies of the rulebase and the security policy and compare the two documents. All rules should have a corresponding requirement in the policy.

Results:

An excerpt is included of GIAC Enterprises' Security policy as it pertains to the firewall:

1. Allow any source to access the external web server using HTTP (Port 80) or Secure HTTP (Port 443). These services allow customers to access our fortune cookie data.
2. E-mail. Allow any source to send SMTP to the external mail server, external mail server to send SMTP out and the internal server to get mail from the external server. E-mail is a big target but we allow SMTP traffic only between the outside world and our external mail server. The internal server forwards outgoing mail to the external server and retrieves inbound mail.
3. The Ident protocol (Port 113/TCP) can be used to gather information about our corporate network by potential attackers and it is not necessary to allow it through the firewall. We choose to drop this traffic at the internal interface. The logging level will be turned down for this rule because of the amount of this kind of traffic.
4. NetBIOS traffic should not leave the corporate network and is also dropped at the internal firewall interface. Logging will be turned down on this rule because it will generate a lot of entries.
5. Allow any source to query the external DNS server using UDP only. The external DNS server contains no information about our inside network. Also, allow the external web server to use both TCP and UDP port 53 to request information from other DNS servers.
6. Allow system administrators to access a group of systems on the screened subnet using SSH.
7. Allow security administrators access to the syslog server on the screened subnet using Secure Shell (SSH). Also allow them to connect to the router using telnet after authenticating on the firewall. SSH is not available for the router.
8. Allow GIAC Enterprises' employees access to the World Wide Web
9. Allow GIAC Enterprises' employees access to FTP resources on remote servers.

Following is a copy of the rulebase extracted from the VelociRaptor firewall:

Rul e	Description	In Via	Sourc e	Dest.	Out Via	Perm s	Services	Time	Auth
#1	Allow external access to web	eth1	Univer se*	ServN et	eth2	ALLO W	http*	<ANYTIM E>	<NON E>
#2:	Allow SMTP from internet to mail server	eth1	Univer se*	GIAC mail	eth2	ALLO W	smtp*	<ANYTIM E>	<NON E>
#3:	Allow SMTP outbound from external mail server	eth2	GIAC mail	Univer se*	eth1	ALLO W	smtp*	<ANYTIM E>	<NON E>
#4:	Allow SMTP bound from internal mail server to external mail server	eth0	IntMail	GIAC mail	eth2	ALLO W	smtp*	<ANYTIM E>	<NON E>
#5:	Allow SMTP inbound from external mail server to internal mail server	eth2	GIAC mail	IntMail	eth0	ALLO W	smtp*	<ANYTIM E>	<NON E>
#6	Reject Ident TCP 113 packets	eth2	GIAC mail	Univer se*	eth1	DEN Y	Ident	<ANYTIM E>	<NON E>
#7	Deny NetBIOS outbound	eth0	GIACn et	Univer se*	<ANY >	DEN Y	netbios_137 _tcp netbios_137 _udp netbios_138 _tcp netbios_138 _udp netbios_139 _tcp netbios_139 _udp	<ANYTIM E>	<NON E>

#8:	Allow DNS inbound from internet to external server	eth1	Universe*	GIACdns	eth2	ALLOW	dns_udp dns_udp_rev	<ANYTIME>	<NONE>
#9:	Allow DNS outbound from external dns server to internet	eth2	GIACdns	Universe*	eth1	ALLOW	dns_udp dns_udp_rev dns_udp_s2s	<ANYTIME>	<NONE>
#10	Allow internal DNS sever to query external DNS server	eth0	IntDNS	GIACdns	eth2	ALLOW	dns_udp dns_udp_rev dns_udp_s2s	<ANYTIME>	<NONE>
#11:	Allow SSH for Admins to access systems on screened net	eth0	GIACnet	ServNet	eth2	ALLOW	ssh_tcp ssh_udp	<ANYTIME>	<NONE>
#12:	Allow HTTP outbound from internal network	eth0	GIACnet	Universe*	eth1	ALLOW	http*	<ANYTIME>	<NONE>

Assessment:

The rulebase accurately reflects the security policy.

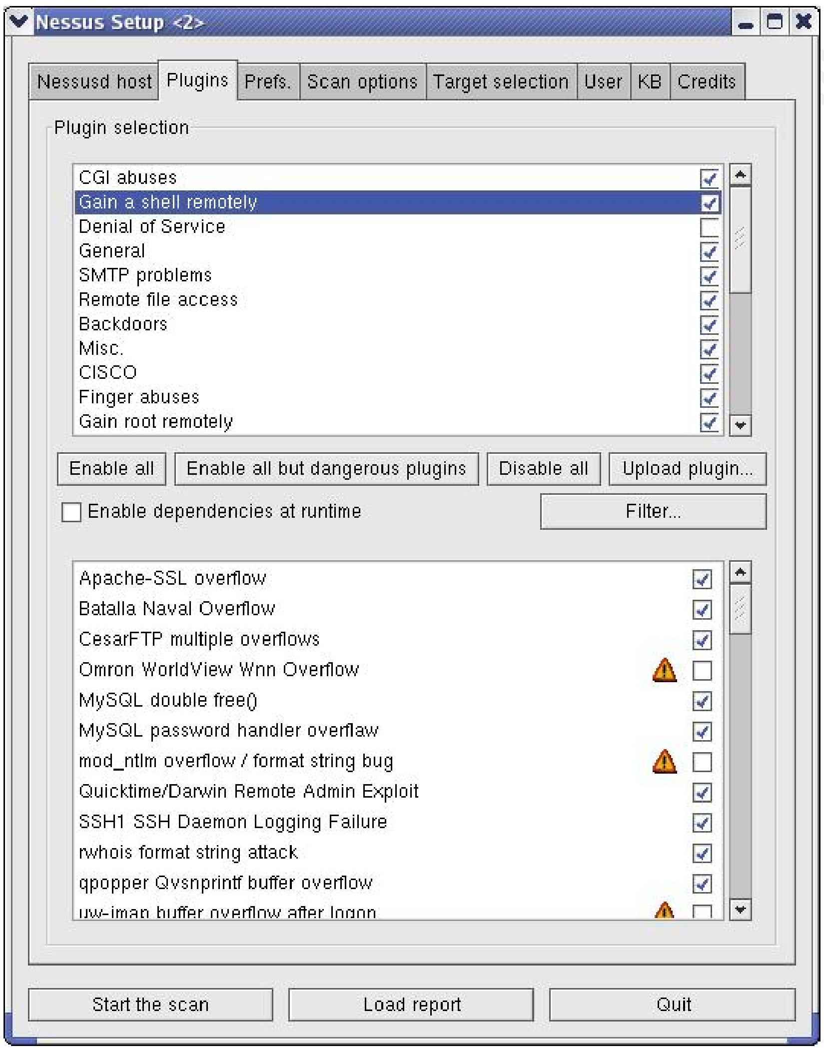
No finding noted.

3.1.7 Task 8: No known vulnerabilities are detected by vulnerability scanning the external (Internet) interface.

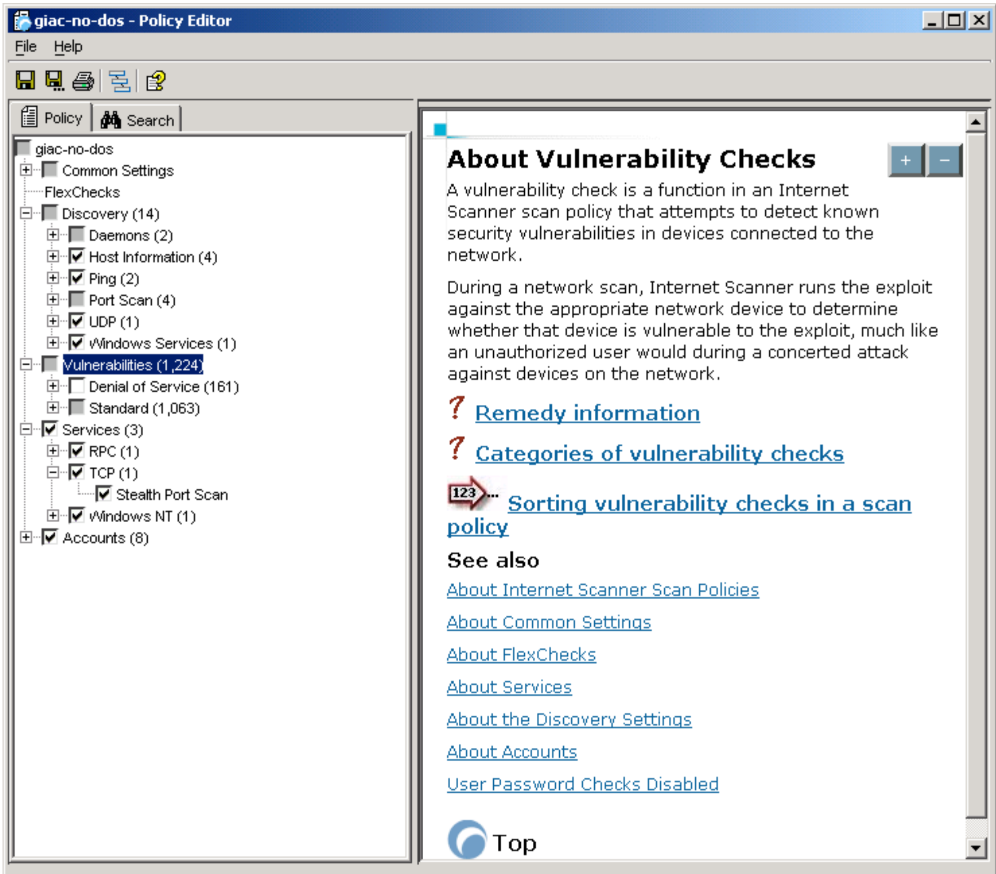
Procedure:

Perform vulnerability and port scans on the external interface of the firewall. Use ISS and Nessus as the scanning tools and compare results. Disable all Denial-of-Service tests since these will be used in a later assessment.

A: Nessus



B: ISS Internet Scanner



<u>Results</u>:

A: Nessus

Nessus Scan Report

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

Scan Details

Hosts which were alive and responding during test
1

Number of security holes found
0

Number of security warnings found
2

Host List

Host(s)
Possible Issue

X.Y.250.10
Security warning(s) found

[return to top]

Analysis of Host

Address of Host
Port/Service
Issue regarding Port

X.Y.250.10
smtp (25/tcp)
Security notes found

X.Y.250.10
ssh (22/tcp)
Security notes found

X.Y.250.10
ftp (21/tcp)
Security notes found

X.Y.250.10
domain (53/tcp)
Security notes found

X.Y.250.10
tacacs (49/tcp)
No Information

X.Y.250.10

http (80/tcp)
Security warning(s) found

X.Y.250.10
gopher (70/tcp)
Security notes found

X.Y.250.10
auth (113/tcp)
Security notes found

X.Y.250.10
netbios-ssn (139/tcp)
No Information

X.Y.250.10
netbios-dgm (138/tcp)
No Information

X.Y.250.10
netbios-ns (137/tcp)
Security notes found

X.Y.250.10
icad-el (425/tcp)
Security notes found

X.Y.250.10
opc-job-start (423/tcp)
No Information

X.Y.250.10
hyper-g (418/tcp)
No Information

X.Y.250.10
onmux (417/tcp)
Security notes found

X.Y.250.10
silverplatter (416/tcp)
Security notes found

X.Y.250.10
https (443/tcp)
Security notes found

X.Y.250.10

dvs (481/tcp)
No Information

X.Y.250.10
shell (514/tcp)
No Information

X.Y.250.10
login (513/tcp)
Security warning(s) found

X.Y.250.10
exec (512/tcp)
Security notes found

X.Y.250.10
realserver (7070/tcp)
Security notes found

X.Y.250.10
domain (53/udp)
Security notes found

X.Y.250.10
general/udp
Security notes found

Security Issues and Fixes: X.Y.250.10

Type
Port
Issue and Fix

Informational
smtp (25/tcp)
An unknown service is running on this port.
It is usually reserved for SMTP
Nessus ID : 10330

Informational
smtp (25/tcp)
smtpscan was not able to reliably identify this server. It might be:
Lotus SMTP MTA Service
The fingerprint differs from these known signatures on 6 point(s)

Nessus ID : 11421

Informational
smtp (25/tcp)
An unknown server is running on this port.
If you know what it is, please send this banner to the Nessus team:
00: 35 35 34 20 35 2e 37 2e 31 20 47 49 41 43 66 77 554 5.7.1 GIACfw
10: 2e 67 69 61 63 2e 63 6f 6d 20 4e 6f 20 6d 61 69 .giac.com No mai
20: 6c 20 73 65 72 76 69 63 65 0d 0a l service..

Nessus ID : 11154

Informational
ssh (22/tcp)
An unknown service is running on this port.
It is usually reserved for SSH
Nessus ID : 10330

Informational
ftp (21/tcp)
An FTP server is running on this port.
Here is its banner :
220 Secure Gateway FTP server ready.
Nessus ID : 10330

Informational
ftp (21/tcp)
Remote FTP server banner :
220 Secure Gateway FTP server ready.
Nessus ID : 10092

Informational
domain (53/tcp)

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

Risk factor : Low
Nessus ID : 11002

Warning
http (80/tcp)

Your webserver supports the TRACE and/or TRACK methods. It has been

shown that servers supporting this method are subject
to cross-site-scripting attacks, dubbed XST for
'Cross-Site-Tracing', when used in conjunction with
various weaknesses in browsers.

An attacker may use this flaw to trick your
legitimate web users to give him their
credentials.

Solution: Disable these methods.

If you are using Apache, add the following lines for each virtual
host in your configuration file :

RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]

If you are using Microsoft IIS, use the URLScan tool to deny HTTP TRACE
requests or to permit only the methods needed to meet site requirements
and policy.

See http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf
http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html

Risk factor : Medium
Nessus ID : 11213

Informational
http (80/tcp)
An unknown service is running on this port.
It is usually reserved for HTTP
Nessus ID : 10330

Informational
http (80/tcp)
The remote web server type is :

Simple, Secure Web Server 1.1

Solution : We recommend that you configure (if possible) your web server to
return
a bogus Server header in order to not leak information.

Nessus ID : 10107

Informational
http (80/tcp)
A web server seems to be running on this port
Nessus ID : 11153

Informational
gopher (70/tcp)
An unknown service is running on this port.
It is usually reserved for Gopher
Nessus ID : 10330

Informational
gopher (70/tcp)
An unknown server is running on this port.
If you know what it is, please send this banner to the Nessus team:
00: 33 54 68 61 74 20 69 74 65 6d 20 69 73 20 6e 6f 3That item is no
10: 74 20 63 75 72 72 65 6e 74 6c 79 20 61 76 61 69 t currently avai
20: 6c 61 62 6c 65 2e 0d 0a lable...

Nessus ID : 11154

Informational
auth (113/tcp)
The service closed the connection after 0 seconds without sending any data
It might be protected by some TCP wrapper

Nessus ID : 10330

Informational
netbios-ns (137/tcp)
The service closed the connection after 0 seconds without sending any data
It might be protected by some TCP wrapper

Nessus ID : 10330

Informational
icad-el (425/tcp)
The service closed the connection after 0 seconds without sending any data
It might be protected by some TCP wrapper

Nessus ID : 10330

Informational
onmux (417/tcp)
The service closed the connection after 0 seconds without sending any data
It might be protected by some TCP wrapper

Nessus ID : 10330

Informational
silverplatter (416/tcp)
The service closed the connection after 0 seconds without sending any data
It might be protected by some TCP wrapper

Nessus ID : 10330

Informational
https (443/tcp)
An unknown service is running on this port.
It is usually reserved for HTTPS
Nessus ID : 10330

Warning
login (513/tcp)

The remote host is running the 'rlogin' service, a remote login
daemon which allows people to log in this host and obtain an
interactive shell.

This service is dangerous in the sense thatit is not ciphered - that is,
everyone can sniff the data that passes between the rlogin client
and the rlogin server, which includes logins and passwords as well
as the commands executed by the remote host.

You should disable this service and use openssh instead (www.openssh.com)

Solution : Comment out the 'login' line in /etc/inetd.conf and restart the
inetd process.

Risk factor : Low
CVE : CAN-1999-0651
Nessus ID : 10205

Informational
exec (512/tcp)
The service closed the connection after 0 seconds without sending any data
It might be protected by some TCP wrapper

Nessus ID : [10330]

Informational
realserver (7070/tcp)
The service closed the connection after 0 seconds without sending any data
It might be protected by some TCP wrapper

Nessus ID : [10330]

Informational
domain (53/udp)

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

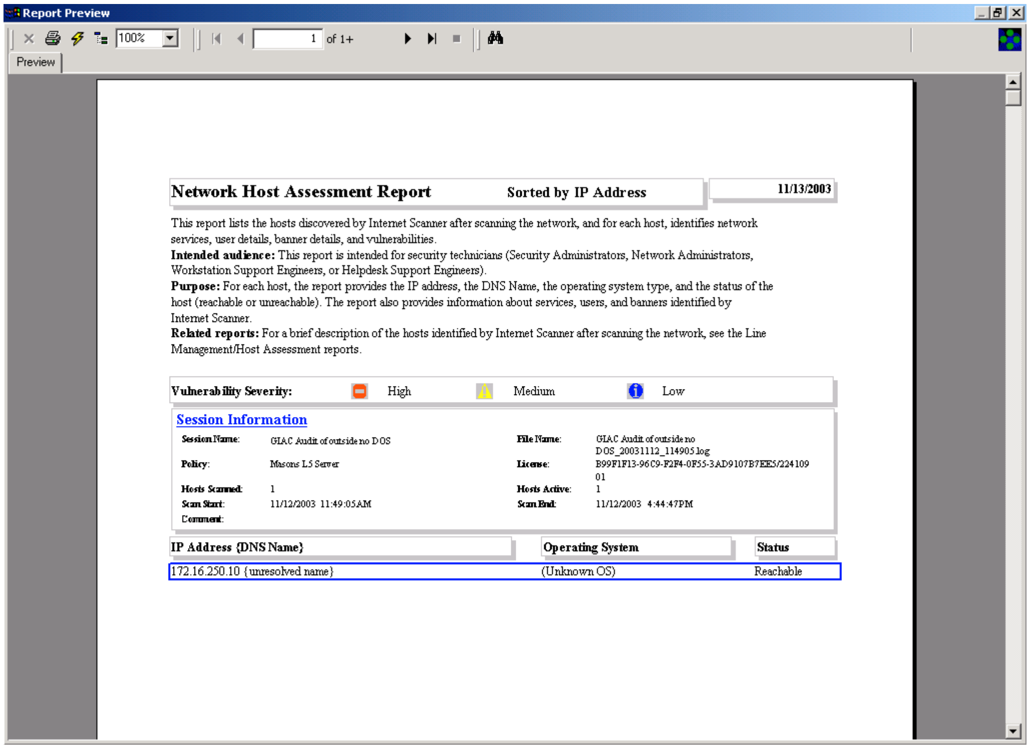
Risk factor : Low
Nessus ID : [11002]

Informational
general/udp
For your information, here is the traceroute to X.Y.250.10 :
X.Y.250.10

Nessus ID : [10287]

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

B: ISS Internet Scanner



Report Preview

Preview

Network Host Assessment Report **Sorted by IP Address** **11/13/2003**

This report lists the hosts discovered by Internet Scanner after scanning the network, and for each host, identifies network services, user details, banner details, and vulnerabilities.
Intended audience: This report is intended for security technicians (Security Administrators, Network Administrators, Workstation Support Engineers, or Helpdesk Support Engineers).
Purpose: For each host, the report provides the IP address, the DNS Name, the operating system type, and the status of the host (reachable or unreachable). The report also provides information about services, users, and banners identified by Internet Scanner.
Related reports: For a brief description of the hosts identified by Internet Scanner after scanning the network, see the Line Management/Host Assessment reports.

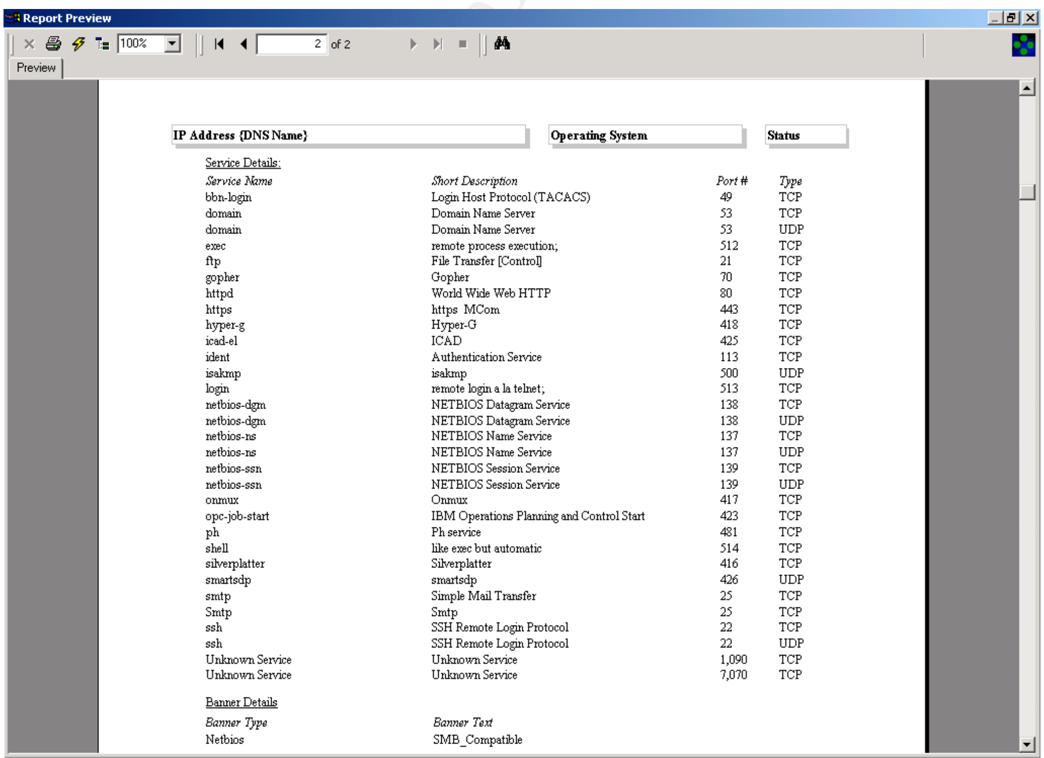
Vulnerability Severity: High Medium Low

Session Information

Session Name:	GIAC Audit of outside no DOS	**File Name:**	GIAC Audit of outside no DOS_20031112_114905.log
Policy:	Masons L5 Server	**License:**	B99F1F13-96C9-F2F4-0F55-3AD9107B7EE5/22410901
Hosts Scanned:	1	**Hosts Active:**	1
Scan Start:	11/12/2003 11:49:05AM	**Scan End:**	11/12/2003 4:44:47PM
Comment:			

IP Address {DNS Name}	Operating System	Status
172.16.250.10 {unresolved name}	(Unknown OS)	Reachable

Open ports detected by ISS:



Report Preview

Preview

IP Address {DNS Name}	Operating System	Status

Service Details:

Service Name	*Short Description*	*Port #*	*Type*
bbn-login	Login Host Protocol (TACACS)	49	TCP
domain	Domain Name Server	53	TCP
domain	Domain Name Server	53	UDP
exec	remote process execution;	512	TCP
ftp	File Transfer [Control]	21	TCP
gopher	Gopher	70	TCP
httpd	World Wide Web HTTP	80	TCP
https	https MCom	443	TCP
hyper-g	Hyper-G	418	TCP
icad-el	ICAD	425	TCP
ident	Authentication Service	113	TCP
isakmp	isakmp	500	UDP
login	remote login a la telnet;	513	TCP
netbios-dgm	NETBIOS Datagram Service	138	TCP
netbios-dgm	NETBIOS Datagram Service	138	UDP
netbios-ns	NETBIOS Name Service	137	TCP
netbios-ns	NETBIOS Name Service	137	UDP
netbios-ssn	NETBIOS Session Service	139	TCP
netbios-ssn	NETBIOS Session Service	139	UDP
onmux	Onmux	417	TCP
opc-job-start	IBM Operations Planning and Control Start	423	TCP
ph	Ph service	481	TCP
shell	like exec but automatic	514	TCP
silverplatter	Silverplatter	416	TCP
smartsdp	smartsdp	426	UDP
smtp	Simple Mail Transfer	25	TCP
Smtp	Smtp	25	TCP
ssh	SSH Remote Login Protocol	22	TCP
ssh	SSH Remote Login Protocol	22	UDP
Unknown Service	Unknown Service	1,090	TCP
Unknown Service	Unknown Service	7,070	TCP

Banner Details

Banner Type	*Banner Text*
Netbios	SMB_Compatible

<u>Assessment</u>:

Although neither assessment tool listed any major vulnerabilities, both of them list a fairly large number of ports that appear to be open from the Internet-side. Research on the Symantec website and discussion with Symantec engineers discovered that there are certain ports that the Raptor firewall shows as open, although they are supposedly not "really" open. The explanation given verbally was that the firewall will log attempts to connect to these ports and gather intelligence on the attacks in a honeypot-like behavior.

Although this is considered normal behavior for this firewall, the auditor considers it undesirable to have these ports show up on port scans.

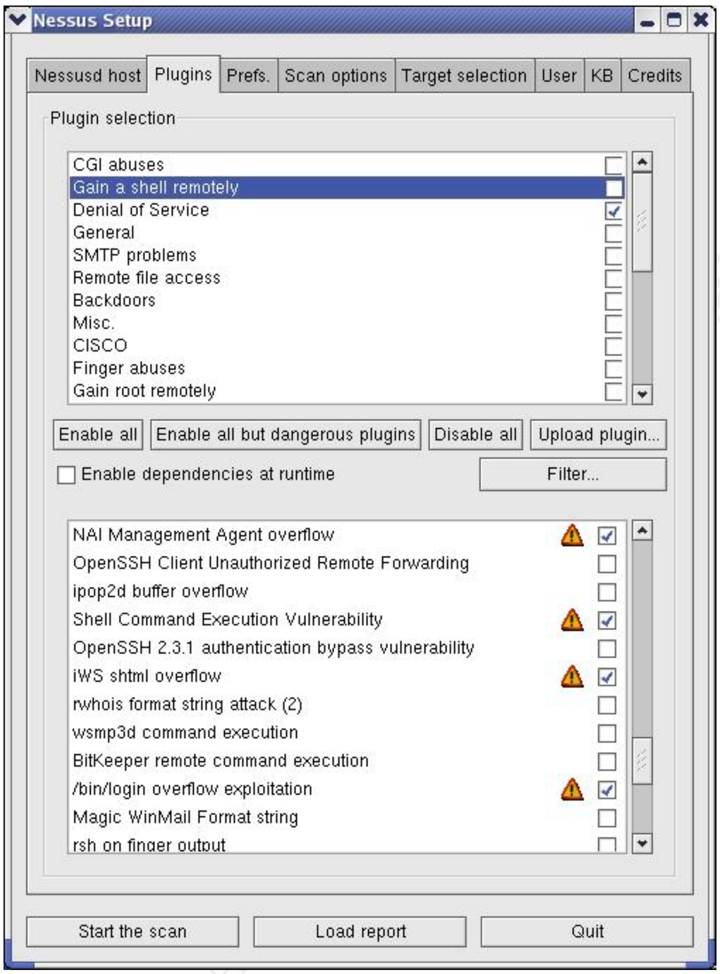
A negative finding is noted for these scan results.

3.1.8 Task 9: Verify the firewall is not susceptible to DoS attacks.

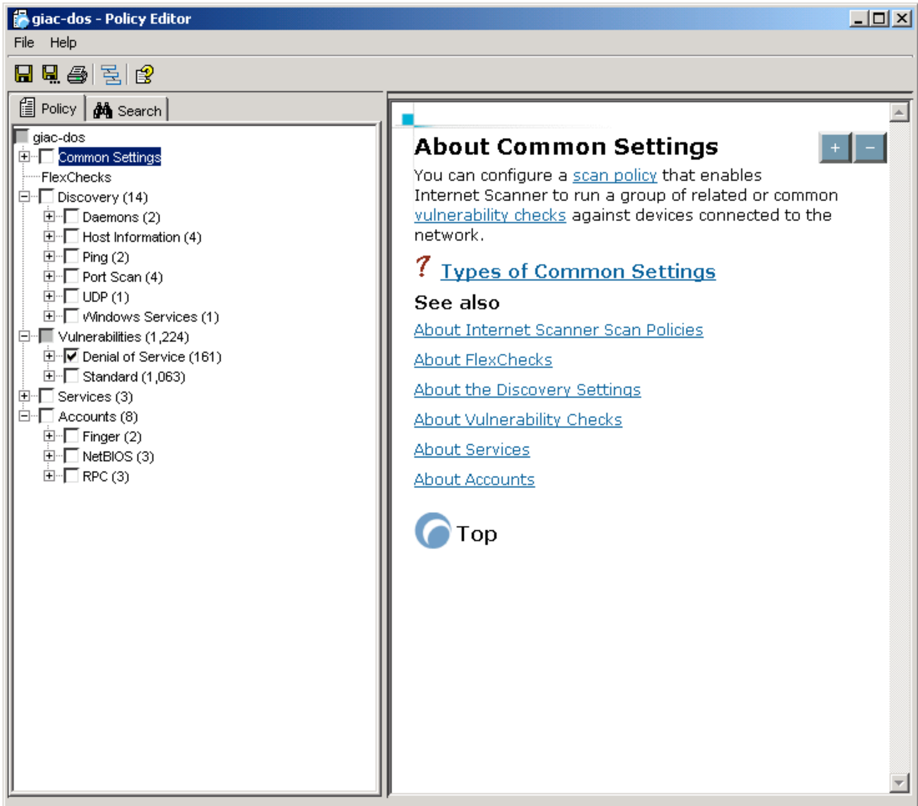
Procedure:

Use ISS Internet Scanner and Nessus to scan the external firewall interface, enabling all DoS attacks.

1. Nessus using Denial of Service



2. ISS Internet Scanner using Denial of Service:



<u>Results</u>:

The firewall was not affected by the DoS attacks from either ISS or Nessus. The firewall was observed to process normal traffic during these attacks.

1. Nessus:

Nessus Scan Report

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

Scan Details

Hosts which were alive and responding during test
1

Number of security holes found
0

Number of security warnings found
0

Host List

Host(s)
Possible Issue

X.Y.250.10
No noticeable information found

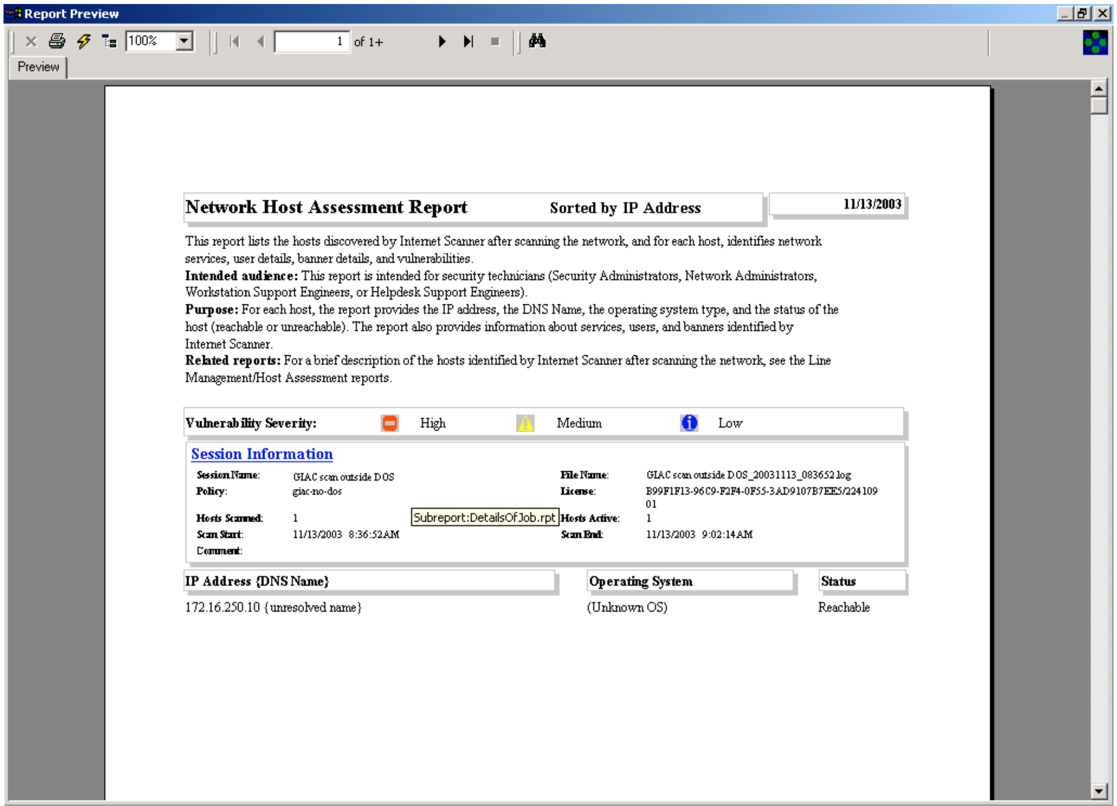
[return to top]

Security Issues and Fixes: X.Y.250.10

Type
Port
Issue and Fix

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

2. ISS Internet Scanner



Assessment:

No finding noted.

3.1.9 Task 10: Anti-spoofing is enabled on all network interfaces.

Procedure:

1. Verify that spoofed packets are detected and dropped by the firewall by using hping2 to generate some spoofed packets from inside each interface.
2. Use "tcpdump" on the firewall to observe the packet traffic on the inside and outside interfaces and verify that it is being dropped.
3. Review the firewall log for evidence of the spoofed packet activity.

Results:

1. Using hping2 against the outside interface
   [root@localhost root]# *hping2 -a 192.168.100.77 -1 X.Y.250.10*
   HPING X.Y.250.10 (eth0 X.Y.250.10): icmp mode set, 28 headers + 0 data bytes
   --- X.Y.250.10 hping statistic ---
   19 packets tramitted, 0 packets received, 100% packet loss

   round-trip min/avg/max = 0.0/0.0/0.0

   Using hping2 against the inside interface
   [root@localhost root]# *hping2 -a X.Y.250.90 -1 192.168.100.10*
   HPING 192.168.100.10 (eth1 192.168.100.10): icmp mode set, 28 headers + 0 data bytes
   --- 192.168.100.10 hping statistic ---
   29 packets transmitted, 0 packets received, 100% packet loss

   round-trip min/avg/max = 0.0/0.0/0.0

2. Use tcpdump to check for traffic on the other interfaces
   [root@GIACfw /etc]# *tcpdump -i eth0 -n -v*
   tcpdump: listening on eth0

   0 packets received by filter
   0 packets dropped by kernel
   [root@GIACfw /etc]#

   [root@GIACfw /etc]# *tcpdump -i eth1 -n -v*
   tcpdump: listening on eth1

   0 packets received by filter
   0 packets dropped by kernel
   [root@GIACfw /etc]#

root@GIACfw /etc]# *tcpdump -i eth2 -n -v*
tcpdump: listening on eth2

0 packets received by filter
0 packets dropped by kernel
[root@GIACfw /etc]#

3. Firewall Log showing detection and action on spoofed packets:

```
Nov 12 10:58:01.609 GIACfw kernel[0]: 225 Possible spoofed IP packet (192.168.100.77->X.Y.250.10: Protocol=ICMP[Echo request id=28985]) dropped on interface X.Y.250.10
Nov 12 10:58:02.604 GIACfw kernel[0]: 225 Possible spoofed IP packet (192.168.100.77->X.Y.250.10: Protocol=ICMP[Echo request id=28985]) dropped on interface X.Y.250.10
Nov 12 10:58:03.604 GIACfw kernel[0]: 225 Possible spoofed IP packet (192.168.100.77->X.Y.250.10: Protocol=ICMP[Echo request id=28985]) dropped on interface X.Y.250.10
Nov 12 10:58:04.605 GIACfw kernel[0]: 225 Possible spoofed IP packet (192.168.100.77->X.Y.250.10: Protocol=ICMP[Echo request id=28985]) dropped on interface X.Y.250.10
Nov 12 10:58:05.604 GIACfw kernel[0]: 225 Possible spoofed IP packet (192.168.100.77->X.Y.250.10: Protocol=ICMP[Echo request id=28985]) dropped on interface X.Y.250.10
Nov 12 10:58:06.604 GIACfw kernel[0]: 225 Possible spoofed IP packet (192.168.100.77->X.Y.250.10: Protocol=ICMP[Echo request id=28985]) dropped on interface X.Y.250.10
Nov 12 10:58:07.604 GIACfw kernel[0]: 225 Possible spoofed IP packet (192.168.100.77->X.Y.250.10: Protocol=ICMP[Echo request id=28985]) dropped on interface X.Y.250.10
Nov 12 10:58:08.604 GIACfw kernel[0]: 225 Possible spoofed IP packet (192.168.100.77->X.Y.250.10: Protocol=ICMP[Echo request id=28985]) dropped on interface X.Y.250.10
Nov 12 10:58:09.604 GIACfw kernel[0]: 225 Possible spoofed IP packet (192.168.100.77->X.Y.250.10: Protocol=ICMP[Echo request id=28985]) dropped on interface X.Y.250.10
Nov 12 10:58:10.604 GIACfw kernel[0]: 225 Possible spoofed IP packet (192.168.100.77->X.Y.250.10: Protocol=ICMP[Echo request id=28985]) dropped on interface X.Y.250.10
```

Note: The corresponding log entries for the other interfaces: eth0 and eth2 are the same and will not be included here.

<u>Assessment</u>:

The firewall correctly identified the spoofed packets, logged them and dropped them.

No finding noted.

3.2 Measure Residual Risk

Even the most meticulously maintained firewall is only one part of the overall security picture for GIAC Enterprises. There are many components that must work together to achieve a desired level of protection. A perimeter firewall is part of a strategy to mitigate risk but all risk can not be eliminated as long as the company depends on the Internet to perform business. The level of controls implemented depends on the value of the assets being protected, in this case the assets are the company's computing systems and data. Residual risk is what you have left when you consider the original risk and factor in the controls that exist to mitigate it.

One area of residual risk is in the physical protection of the firewall. Although the system is in a physically protected in the computer room, there is no failover device in case the system experiences a catastrophic failure. For a business that depends so much on access to the Internet and thereby on their firewall, some type of automated failover system would be indicated.

Another residual risk is that, although apparently well-configured and managed, the firewall makes itself an enticing target because it shows so many open ports when scanned by commonly-used tools. In the current Internet environment the random scanning activity is constantly at a high level. Common practice is for a potential hacker to scan hundreds of IP addresses to determine possible weak systems and then focus more intense activity on those systems. Even if the ports do not actually represent a vulnerability, they invite further unwelcome attention.

Finally, GIAC users have unrestricted access to web and ftp servers on the Internet. This should be addressed at least in an acceptable use policy that each employee would be required to sign. Employee abuse of the Internet, to download and store pornography for example, could pose liability issues for the company.

3.3 Evaluate the audit (Is the system auditable?)

The Symantec VelociRaptor firewall appliance is certainly an auditable system. The majority of the items on the checklist are objective so there should be little room for interpretation as to whether the system meets its objective. The manufacturers' stance on the ports issue is a judgment call but this auditor feels that "quiet" is better than "tricky" when it comes to firewalls. The objectives chosen for audit were intended to show that the system is sufficiently protected against internal and external threats and the results seem to indicate that is the case.

Assignment 4: Audit Report or Risk Assessment

4.1 Executive Summary

An audit was requested by GIAC Enterprises' management to evaluate the security of GIAC's perimeter firewall. The purpose of the audit was to determine whether the firewall was adequately fulfilling the objective of protecting the company's computing assets and data. Because GIAC depends on the Internet to conduct business the firewall is seen as a critical component of the network infrastructure. The audit consisted of interviews with GIAC personnel, review of pertinent documentation and technical analysis using free and commercial software tools. The results of the audit indicate the firewall is protected adequately against internal threats and it does its job of protecting the company's assets. While areas for improvement exist the audit finds that the firewall receives a satisfactory grade.

4.2 Audit Findings

The audit resulted in only one finding, in Section 3.1.8 Task 8, and that concerns the numerous ports that show as "open" or "listening" when the firewall is port and vulnerability scanned from the Internet. Network monitoring that was done concurrently with the scanning did not detect any network traffic that penetrated the firewall.

4.3 Background / risk

As stated above, the firewall was not seen to actually pass any unauthorized traffic during any of these scans and the vendor acknowledges that these ports will be seen on such a scan. The risk of having a large number of ports identified on these scans is that a potential hacker using a similar tool would see this firewall as a potentially vulnerable system and possibly focus more attention on compromising it. If they were to post the system on a hacker's bulletin board the result would be hundreds more hackers attempting to compromise the system.

4.4 Audit Recommendations

The firewall has the ability to block the ports that are listening for network connections by using custom "filters". These can be implemented by the security staff with the result of eliminating the majority of the ports that show up on vulnerability scans.

Although not presented as a finding, it is recommended that management consider implementing failover capability for the firewall because of the role it plays in the success of the business. Hardware and software failover options are available and these should be researched to find the right solution for GIAC.

4.5 Costs

The cost of implementing filters to reduce open ports is negligible. A firewall administrator could research the open ports, determine which are not actually in use and configure filters in four to six hours. Firewall changes are generally handled by two admins to minimize errors and to provide oversight so the total would be 1 – 1.5 FTE for one day to make this change.

The cost of implementing failover depends on the level of redundancy pursued. Solutions that provide almost instant, automated failover will cost correspondingly more than lower-tech solutions. Research should be done with Symantec for further information on automated hardware and software failover solutions.

4.1 Compensating Controls

Since there is no external cost for implementing filters to restrict open ports there should be no need for further compensating controls in this case. If, for some reason, it is determined to be impractical to implement these filters they could be implemented at the screening router. The cost for personnel to do the job would be approximately the same.

If the cost of implementing an automated failover system is determined to be too high, a manual failover could be implemented by purchasing an additional VelociRaptor firewall. This system would be configured identically to the production system and kept ready in case of a failure to the primary system.

References:

1. Contribution based on personal knowledge and experience.
2. Auditing Firewalls: A Practical Guide; Bennett Todd; www.ITsecurity.com
3. Auditing Your Firewall Setup; Lance Spitzner; www.spitzner.net; 2000
4. Computer Security Audit Checklist; Colin Rose; Posted in ITsecurity.com, April 2002; http://www.itsecurity.com/papers/iomart2.htm
5. Firewall Checklist; Krishni Naidu; SANS Security Consensus Operational Readiness Evaluation (S.C.O.R.E.) http://www.sans.org/score/firewallchecklist.php
6. Symantec Tech Support Download Page; http://www.symantec.com/techsupp/enterprise/select_product_updates.html
7. FireTower FAQ for Raptor Firewalls; http://www.firetower.com/faqs/index.html
8. BugTraq; www.securityfocus.com;
9. CISSP Certification All-In-One Exam Guide; Shon Harris; McGraw Hill/Osborne 2002
10. SANS – Auditing Networks, Perimeters and Systems; 2003
11. SANS – Firewalls, Perimeter Protection and VPNs; 2002
12. Symantec Enterprise Firewall and Symantec Enterprise VPN Reference Guide; Symantec Corporation ©1998-2001
13. Guidelines on Firewalls and Firewall Policy; NIST Special Publication 800-41; 2002

Last Updated: September 24th, 2017

Upcoming Training

Community SANS Virginia Beach AUD507~	**Virginia Beach, VA**	**Nov 27, 2017 - Dec 01, 2017**	**Community SANS**
SANS London February 2018	**London, United Kingdom**	**Feb 05, 2018 - Feb 10, 2018**	**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**