Global Information Assurance Certification Paper

GIAC Enterprises

SANS GCFW Practical Assignment – Version 1.9

Prepared by: David Polano

April 2003

Table of Contents

Tables and Figures

Abstract

The purpose of this document is the following:

(1) Describe the newly implemented network security architecture of GIAC Enterprises.
(2) Detail the security policies of the border router, firewall and VPN.
(3) Audit the firewall policies to ensure that they are correctly implemented.
(4) Research and design a series of attacks against a rival company.

Company Summary

GIAC Enterprises is an e-business company that deals with the online sale of fortune cookie sayings. The company is based out of Vancouver, Canada and has been in existence since 2001. The company currently has 55 employees, of which 42 are based out of Vancouver. The remaining employees are part of the sales group and are strategically located in various locations around the world.

The last couple of years have not been kind to GIAC Enterprise. With the world gripped in fear as a result of the September 11 terrorism attacks, many people are afraid of what their future might hold and therefore are reluctant to read what their fortune cookies have to say. Also, the resulting world wide economic downturn has made things even worse as less people are eating out and therefore the demand for fortune cookies is down. As a result of these conditions, GIAC Enterprises was forced to reduce staffing levels so that the company could remain profitable. The reduction in staff has caused significant problems in certain departments. The IT department was hit particularly hard and as a result, there have been significant system outages due to virus and hacker attacks.

Due to the reduction in staffing levels, GIAC Enterprises is undertaking an initiative to streamline the business processes by deploying new technology. Also, understanding that the IT staff has difficulty managing the existing infrastructure, they have hired a consultant to redesign and implement a new network design that is better suited to the company's size. The intent is to keep the network design as simple and flexible as possible without compromising security or functionality.

Background

IT Staffing Levels

The IT staff is composed of 14 people with the following duties:

CIO

Responsible for setting the direction of the IT department and for reviewing new technologies that could further streamline business processes. Reports directly to the president of the company.

Network Support (4 employees)

Responsible for maintaining the network infrastructure. Includes monitoring, upgrading and deploying networking equipment (routers, switches, hubs), firewalls, infrastructure servers (mail, DNS, IIS, Domain controllers, etc).

Application Support (2 employees)

Responsible for assisting customers with e-business application related problems. Also maintain the content on the company's website.

Developer (2 employees)

Responsible for developing and maintaining the e-business applications.

PCSupport/Help Centre (3 employees)

Responsible for installing and maintaining the user workstations. These employees also man the Help Centre phone.

Production Support (2 employees)

Responsible for installing and maintaining application servers, performing system backups and monitoring server uptime.

Technology Platforms

GIAC Enterprises has standardized on the Windows platform. As per the direction of the CIO, non windows systems are to be used only when cost or security considerations justify their use. The primary reason for this policy is to ensure that the existing staff is capable of maintaining any new systems that should come on line. If there were no restrictions on the type of platforms that could be used, it could result in a complicated heterogeneous environment that would become difficult and expensive to manage. Also, since the IT staff has a good understanding of the Windows technology, they will be better equipped to ensure that the systems are deployed in a secure fashion.

Supported Software Packages

GIAC Enterprises has standardized on the following software packages:

Server OS – Windows 2000
Desktop OS – Windows XP
Office Software – Office XP
Mail Software – Exchange 2000
Database Software – SQL 2000
Data Interchange Software – BizTalk Server 2000
Antivirus Software – ETrust Antivirus 6.0
VPN Client Software – SecureClient NG FP3
Firewall Software – CheckPoint NG FP2
Host Based IDS Software – Tripwire 3.0
Exchange Antivirus: Antigen
Web Proxy: Microsoft ISA
URL Filtering: SmartFilter for MS Proxy

Hardware Platforms

All server hardware is standardized on the HP Proliant BL e-Class server. Desktop are generic Intel based systems that are provided by a local company (Seanix). Laptops are standardized on the IBM ThinkPad.

Backup Strategy

All production data is backed up daily to the central IBM TSM system. Backup tapes are relocated offsite daily. On Saturday evening, a full back up is done of all critical systems. Incremental backup are done for the remainder of the week. Users have been instructed not to store any documents on their local system and to keep files on the file server. Microsoft Office has been configured to locate the "My Documents" folder on the file server. End user systems are not backed up.

All servers use SCSI hard drives and all drives are mirrored for redundancy. Prod, QA and development servers use identical hardware and therefore parts between the systems can be swap in the event of hardware failure.

Physical Security

Access to the GIAC office is controlled via electronic card access. All non employees (excluding contractors) must be accompanied at all times by a GIAC employee. All access cards display a photo of the employee to whom the card has been issued to. Computer Room access is limited to select IT staff only.

Bandwidth Requirements

GIAC does not have a requirement for a high bandwidth Internet access. The data that is being transferred to and from GIAC is composed of small CSV files. Also, with the limited number of staff using VPN and the fact that only Terminal Services traffic (i.e. screen changes and mouse events) are being transferred back and forth, the bandwidth required for VPN is minimal.

Assignment 1 – Security Architecture

Business Process Overview

GIAC Enterprises is in the business of selling fortune cookie sayings online. GIAC Enterprises does not actually produce the fortune cookie sayings but instead purchases them from various suppliers located throughout the world. They "bulk purchase" the fortune cookie sayings from these suppliers and then turn around and sell them to a wide array of customers. GIAC has exclusive rights to their suppliers and their suppliers cannot sell their fortune cookie sayings to any other distributor. GIAC has also developed strategic partnerships with other fortune cookie sayings vendors. GIAC uses these partners to translate and resell their fortune cookie sayings in other language markets.

Standard Security Policies

(1) Deny everything by default. Explicitly add the ACL's to permit the required access.
(2) No direct access from the Internet to any internal system.

(3) Antivirus Policy – all systems on the GIAC network, with the exception of the firewall and routers must have the standard AV software installed (eTrust Antivirus). The Real-time monitor must be enabled and daily schedule scans must be performed.
(4) Unless explicitly authorized, modems are not permitted.
(5) Logging Policy – all servers in the DMZ are configured to push their log files at midnight to the SFTP/SSH server. The central logging server is scheduled to pull the log files from the SFTP/SSH server daily at 1:00am. The firewall logs are forwarded to the Checkpoint Management Server. Routers are configured to forward their logs to the central logging server.
(6) No remote management of border routers; all management must be done on the console.
(7) No remote terminal access (i.e. Remote Desktop/Terminal Services) to servers in the DMZ. All work must be performed while physically logged onto the system.
(8) All systems (end user desktops, servers, firewall, routers, etc.) are to be patched with the latest security patches for the operating system and applicable application software on a quarterly basis. Relevant security vulnerability deemed critical/high are to be installed within 48 hours of announcement unless there are other methods that can be used to mitigate the vulnerability.

Network Design

The network design that was implemented is as follows:

Figure 1 - Network Design

IP Address Scheme

GIAC Enterprises has acquired a single Class C address range for external access (120.0.0.0/24). NOTE: for the purposes of this paper, a reserved Class C address range was picked so as not to invite unwanted attention to an active Class C address range. The internal addressing scheme uses a private Class A (as defined by IANA). The class A was broken up as follows:

Address	Subnet Mask	Description
10.98.0.0	255.255.255.0	Infrastructure Services Network (DMZ #2)
10.99.0.0	255.255.255.0	Business Services Network (DMZ #1)
10.1.0.0	255.255.255.0	Subnet used by internal router and firewall
10.20.1.0	255.255.0.0	QA, DEV and User network
10.10.0.0	255.255.255.0	Production Server Network

Firewall Details

GIAC is running a CheckPoint VPN-1 Pro firewall. Checkpoint was chosen because the IT Manager has had prior success with this type of firewall and because the existing network administrators had previous experience using this firewall. The current version that is running is NG Feature Pack 2. Due to security and stability concerns, the underlying operating system is Checkpoint's SecurePlatform (Feature Pack 2, Edition 2). Since SecurePlatform is a hardened Linux kernel, it is much easier to keep secured than a Windows 2000 server. Also, the SecurePlatform installation process is very quick and therefore allows one to quickly build a firewall to where a backup of the firewall policies can be restored to. The firewall runs on an HP ProLiant DL360 server. The system has 1 GB of RAM and mirrored 18GB SCSI drives. A quad NIC card was installed on the unit to provide a total of 5 interfaces (at present, only four are required). There is an available PCI slot that will permit the installation of an additional quad NIC should there be future requirements to increase the number of interfaces. An identical DL360 server has been purchased for recovery purposes. The backup system is also used to test firewall upgrades and patches. A backup of the firewall configuration is taken anytime there are changes to the firewall. The Real-time monitor module has also been purchased to allow the monitoring of the firewall.

The placement of the firewall ensures that all traffic passing in to or out of the GIAC network must pass through the firewall. This ensures that the traffic can be tightly controlled to minimize the possibility of a successful attack.

VPN Details

The Checkpoint firewall that GIAC is running also serves as the VPN server. The VPN client is Checkpoint SecureClient. SecureClient allows one to secure the VPN client by enforcing a desktop policy.

Router Details

GIAC is using a Cisco 2611XM border router running IOS 12.2. The router comes with 16MB Flash Memory and 64MB of DRAM. It comes standard with 2 ethernet interfaces. This device is targeted towards the small to midsize companies in which GIAC easily falls into. The border router's placement in front of the Checkpoint firewall allows the filtering of unwanted traffic so that the firewall does not have to process it. Since GIAC's bandwidth requirements are not excessive (i.e. no more than a T1), the 2611XM will be able to easily handle the throughput. A spare router was also purchased to minimize

interruption in the event of hardware failure. Keeping both the internal and external routers the same means that only one spare had to be purchased. The internal router (and the spare) comes with an additional WIC module to provide the needed 3 interfaces. The router configuration is backed up so that it can be easily restored to the backup unit in the event of hardware failure.

Central Logging Server Details

The logging server is a Windows 2000 server running a Window's SYSLOG services from Kiwi Enterprises called Kiwi Syslog Daemon. It also has an SSH client to auto download log files from the external SFTP/SSH server.

Access Requirements

Business Service Network (DMZ#1) Access Requirements

GIAC has an existing security policy in place that states that no external party can have direct access to a system in the internal network. As a result of this policy, GIAC has opted to use "web services" to pass data to/from the DMZ to the internal network. The web services have been configured to communicate over SSL. Client and server side are certificates are used to verify the identity of the client and the server.

Source	Service	Port	Proto	Destination	Reason
DMZ #1 Servers	DNS	53	UPD	W2K DNS in DMZ#2	Allow DNS queries from servers in DMZ #1 to reach external DNS server in DMZ #2
IIS Application Server in DMZ #1 and SSH/SFTP Server	HTTPS	443	TCP	Internal BizTalk Server	Allows application web server and SFTP server to send data to internal BizTalk Server

Table 1 - Summary of Business Service Network Access Requirements

Infrastructure Services Network (DMZ #2) Access Requirements

GIAC has arranged for their ISP to provide an external backup DNS for the GIAC domain. As a result of this requirement, DNS zone transfers must be allowed to the ISP's DNS server. Also, the SMTP server must be able to forward mail to the internal Exchange 2000 server and inbound mail must be able to reach the SMTP server.

Source	Service	Port	Proto	Destination	Reason
Any	SMPT	25	TCP	External SMTP Server (DMZ #2)	Allow inbound mail to reach the SMTP server.
External SMTP Server (DMZ #2)	SMPT	25	TCP	Internal Exchange 2000 Server	Allow the SMTP server to deliver mail to the internal Exchange 2000 Server
ISP's DNS Server	DNS	53	TCP	External DNS in DMZ#2	Allow zone transfers to ISP's DNS server

Table 2 - Summary of Infrastructure Services Network Access Requirements

DMZ Backup Access Requirements

The Tivoli backup system must be able to backup the servers in the DMZ.

Source	Service	Port	Proto	Destination	Reason

Tivoli Backup Server	TSM backup	1500-1501	TCP	DMZ #1 and DMZ #2	Allow Tivoli server to backup DMZ servers

Table 3 - Summary of TSM Access Requirements

Customers Access Requirements

Customers purchase fortune cookie saying by accessing GIAC customer service web site. They logon to the website with the username/password that was created for them when they were issued accounts. All customers must register with GIAC prior to being issued a customer account. Customer must choose the type of fortune cookie sayings they want and the quantity they want to purchase. The type of fortune cookie saying indicates the subject to which the fortune cookie saying comments on (for example a fortune cookie saying regarding one's health or perhaps one's love life, etc). Customers can also choose to purchase a random selection of fortune cookie sayings. After the customer agrees to the total price, they will be redirected to a web page that will allow them to download a CSV (comma separated values file) file containing the fortune cookie saying(s) they requested. The customer services web application makes a call to the internal BizTalk server to obtain the necessary CSV file containing the fortune cookie sayings that were requested. Customers are then billed according to the information they provide during the registration process.

Source	Service	Port	Proto	Destination	Reason
Any valid IP	HTTP	80	TCP	External Static Content Web Server (DMZ #1)	Allow customers access to static information on GIAC web site.
Any valid IP	HTTPS	443	TCP	External IIS Application Web Server (DMZ #1)	Provide access to the Application Web Server.

Table 4 - Summary of Customer Access Requirements

Supplier Access Requirements

GIAC purchases their fortune cookie sayings from an assortment of suppliers. All suppliers must register with GIAC before fortune cookie sayings can purchase from them. All GIAC suppliers are issued an SSH username and password so that they can upload their fortune cookie saying to GIAC's secure SFTP/SSH server. GIAC has signed contracts with their suppliers stating that they must supply them with 250 fortune cookie sayings per month. Suppliers transfer their fortune cookie sayings in a single bulk SFTP transfer. All fortune cookie bulk transfers must be contained in a single CSV file. A process on the SFTP/SSH server monitors the Supplier's SFTP upload folders and when a new upload is detected, it makes a call to the web service on the internal BizTalk server. The upload is transferred to the BizTalk server which then processes the CSV file and stores the new fortune cookies saying in the central SQL database. The supplier must send an invoice to GIAC for payment. GIAC confirms that the fortune cookie sayings were in fact uploaded and then cuts a check to pay the supplier.

Source	Service	Port	Proto	Destination	Reason
Any valid IP	HTTP	80	TCP	External Static Content Web Server (DMZ #1)	Allow supplier access to static information on GIAC web site.
Any valid IP	SSH	22	TCP	SFTP/SSH Server	Provides supplier's access to the SFTP/SSH server.

Table 5 - Summary of Supplier Access Requirements

Partner Access Requirements

GIAC partners translate and re-sell fortune cookies saying in other language markets. GIAC has created a partner website which allows their partners to access their online fortune cookie sayings. When a partner wants to acquire new fortune cookie sayings for resale in a different language market, they must first logon into the GIAC partner website. All GIAC partners must register with GIAC prior to obtaining a username and password. From the website, the partners pick the type and quantity of fortune cookie sayings they want to download. The web application calls the internal web service and in turn receives a CSV file with the desired fortune cookie saying. The partner then downloads the CSV file to their system so that the fortune cookie sayings can be translated. The partner then attempts to sell the translated fortune cookie sayings in their respective markets. GIAC has signed a contract with each of their partners that guarantees that they are paid a minimum flat rate for each fortune cookie saying that the partner downloads plus a royalty fee each time the fortune cookie saying is sold to a customer.

Source	Service	Port	Proto	Destination	Reason
Any valid IP	HTTP	80	TCP	External Static Content Web Server (DMZ #1)	Allow partner access to static information on GIAC web site.
Any valid IP	HTTPS	443	TCP	External Application Web Server (DMZ #1)	Allow partner's access to the application web server.

Table 6 - Summary of Partner Access Requirements

Employee Access Requirements

All GIAC employees are issued Windows user accounts. These accounts are recorded in the W2K active directory. All employees have access to an Exchange mailbox in which they access via the standard Outlook XP application which is include on all GIAC user systems. All email attachments (inbound/outbound) are scanned for viruses with Antigen. Internet access is provided to those employees that require it for their job function. Internet access must be approved by the employee's supervisor. All employees, however, are able to access the GIAC external websites and external secure SFTP/SSH server. To control what protocols employees have access to, access is regulated via a MS ISA Proxy server. Internet Explorer has been configured to bypass the ISA proxy for GIAC's Internet web sites. The ISA server is configured to allow employees to use HTTP, HTTPS and FTP read only. If the employee requires additional access (for example, command line FTP access), the WinSock proxy client is installed on their system and they are explicitly granted access to the additional services they require. To ensure that employees are not viewing inappropriate or non business related materials on the web, all web access is filter through SmartFilter which is installed on the ISA Proxy server. The firewall only permits outbound user traffic via the ISA Proxy server.

Source	Service	Port	Proto	Destination	Reason
ISA Proxy Server	Any	Any	Any	Internet	Allow the ISA proxy server access to the Internet. Employee restrictions are enforced on the proxy server.
Employee Systems	SSH	22	TCP	SFTP/SSH Server	Allow employees to access external SFTP/SSH server.
Employee Systems	HTTPS	443	TCP	External Application Web Server	Allow employees to access external application web server
Employee	HTTP	80	TCP	External Web Servers	Allows employees to access the external web

systems					servers.

Table 7 - Summary of Internal Employee Network/Internet Access Requirements

Remote Employee Access Requirements

Most GIAC employees only require access to their email when not on site. Access to their Exchange mailbox is provided via OWA (Outlook Web Access). The connection to the OWA server is over a 128 bit SSL connection. Employees that require additional access (i.e. IT support, mobile sales force, etc), will be required to connect via VPN. Once connected via VPN they can then access the Terminal Services Server to access internal applications and systems. Mobile sales force employees are issued company laptops that are configured with VPN client software while other staff is permitted to install the VPN client software on their home system. The only protocol allowed to pass over the VPN tunnel is RDP (Remote Desktop Protocol). Also, a group policy has been applied on the Terminal Services Server that disabled the transferring of files from the VPN client to the Terminal Services Server. Remote Desktop has been disabled on all other desktop client systems for security reasons. There are no RAS facilities to allow employees to access the network directly. The use of modems is prohibited unless explicit permission is granted. Employees are required to obtain access to their own ISP so that they can either use OWA or VPN to access internal network resources.

Source	Service	Port	Proto	Destination	Reason
Any valid IP	HTTPS	443	TCP	Internal OWA Server	Allow employees to access their Exchange mailbox remotely.
Any VPN Connection	RDP	3389	TCP	Terminal Services Server	Allows authorized employees to access the Terminal Services Server over a VPN connection.
Any valid IP	IKE	500	UDP/ TCP	VPN/Firewall	Required for the VPN connection (IKE: Internet Key Exchange)
Any valid IP	ESP	50	ESP	VPN/Firewall	Required for the VPN connection (ESP: Encapsulated Security Payload)

Table 8 - Summary of Remote Employee Access Requirements

Production Server Network Access Requirements

Server systems located in the Production Server Network will have the following access requirements:

Source	Service	Port	Proto	Destination	Reason
Antivirus Server	FTP	21	TCP	Internet	Allow the Antivirus server to pull updated signature files from the vendor's ftp server
Exchange Server	FTP	21	TCP	Internet	Allow the Exchange Server to update signature files for Antigen
Internal DNS Servers	DNS	53	UDP	External DNS Server in DMZ	Allow internal DNS server to send recursive queries to external DNS server
Central Logging Server	SSH	22	TCP	Secure SFTP/SSH server in DMZ #1	Allows the Central Logging Server to pull log files from the Secure SFTP/SSH server
Exchange Server	SMTP	25	TCP	SMTP Server	Allow outbound mail to reach SMTP server
IBM TSM Server	TSM	1500 - 1501	TCP	DMZ Servers	Allow the TSM (Tivoli Storage Manager) to backup servers in the DMZ
Domain Controllers	NTP	123	TCP/ UDP	External NTP time server	Allow domain controllers to synchronize time with external NTP time server.
ISA Proxy Server	Any	Any	Any	Internet	Allow the ISA proxy server access to the Internet. Employee restrictions are enforced on the proxy server.

Table 9 - Summary of Partner Access Requirements

Network Cost Constraints

One of the primary constraints the new network design had to follow was that the cost of the implementation could not exceed CAN$250,000.00 (excluding the cost to purchase user desktops and laptops and the development of the software). An independent auditor estimated the replacement cost of GIAC Enterprises proprietary data to be valued CAN$750,000. GIAC has purchased insurance to protect its information assets and the deductible is set at CAN$150,000. Using more that $250,000.00 to protect this asset does not make financial sense and therefore a cap was set. Also, the design had to ensure that it could be managed by the existing IT staff. No significant budget increases were expected any time soon that could be used to hire additional IT staff. Annual software maintenance could not exceed CAN$50,000.

Assignment #2 – Security Policy and Tutorial

This section of document describes the specific security policies for the border router, firewall and VPN that need to be enforced according to the access requirements defined in the previous section.

The Ordering of the Rules

The order of the rules, whether on the router or firewall/VPN, is important both from a security perspective and a performance perspective. The first thing to note is that rules are applied from top to bottom. That is, it compares the packet with each rule in the rule list starting from the top until it finds a rule that matches. If the rules are configured such that you create an explicit permit rule before a deny rule, the traffic will be allowed to passed because it would hit the permit rule first. The opposite is also true. As a general principle, the rules at the beginning of the policy should be the deny rules. Below that, you should have the permit rules. The other thing to note about the rule order is that depending on the amount of traffic that is processed by the device, the order in which the rules are processed will affect the performance of the device. Therefore, if there are rules that get a lot of activity, they should be located somewhere near the top of the rule list.

Border Router Security Policy

The border router will be used to do some rudimentary filtering only; the majority of the work will be done by the Checkpoint firewall. All rejected traffic is logged by default so that analysis can be done in the event of a potential security breach. No remote configuration of the router is permitted. All changes must be made from the console.

General Router Configuration

To harden the router, the following configuration changes were made:

Due to the vulnerabilities of SNMP, it will be disabled.

```
no snmp
```

The services echo, discard, chargen and daytime are not required and will be disabled. Leaving these services enabled could potentially expose the router to an attack if future vulnerabilities are found.

```
no service udp-small-servers
no service tcp-small-servers
```

Loose source routing is disabled because it can be used to send traffic to a host that cannot normally be reached because of existing access lists.

```
no ip source-route
```

Bootp is not required.

```
no ip bootp server
```

All configuration changes are made from the console. HTTP access is not required and could be the target of attack.

```
no ip http server
```

Enable password encryption on the router.

service password-encryption

CDP (Cisco Discovery Protocol) is not needed and therefore disabled.

no cdp run

Disable the finger service as it can be used by hackers to find who is logged in.

no service finger

To prevent others from trying to use the router as an NTP server disable ntp master.

no ntp master

Protect the "enable" password (i.e. password used to access EXEC mode) with an MD5 hash.

enable secret ########

Configure a login banner to warn users that unauthorized access is not permitted

banner login/Unauthorized Access Prohibited!

Enable logging and configure to send logs to internal syslog server. No logging will be done to the console.

logging on
logging 10.10.0.51
no logging console

External Interface Configuration

The following settings were applied to the external interface:

To prevent Layer 3 to Layer 2 broadcast mapping and Smurf amplification, ip directed broadcast is disabled

no ip directed-broadcast

Disable proxy-arp so that the router only responds to ARP requests received for the GIAC address.

no ip proxy-arp

Prevent the router from giving out network information based on ICMP error messages by disabling ICMP unreachable messages.

no ip unreachables

NTP is not required on the external interface and therefore is disabled.

ntp disable

The following extended access list was applied inbound on the external interface:

Note: the rules are in the order as they would appear in the access list.

Reject traffic that has a source IP address reserved for private use (RFC 1918).

access-list 110 deny ip 192.168.0.0 0.0.255.255 any log
access-list 110 deny ip 172.16.0.0 0.15.255.255 anylog
access-list 110 deny ip 10.0.0.0 0.255.255.255 any log

Reject traffic that has a source IP address reserved for broadcast, local host and/or multicast addresses.

access-list 110 deny ip 127.0.0.0 0.255.255.255 any log
access-list 110 deny ip 255.0.0.0 0.255.255.255 any log
access-list 110 deny ip 224.0.0.0 7.255.255.255 any log

Reject traffic that does not have an IP address.

access-list 110 deny ip host 0.0.0.0 any log

Thwart spoofing attempts by rejecting traffic that has a source IP address set to GIAC's internal address.

access-list 110 deny ip 120.0.0.0 0.0.0.255 any log

Deny IDENT traffic due to future potential security risks.

access-list 110 deny tcp any any eq 113

Allow replies of connections initiated from the internal network to pass.

access-list 110 permit tcp any 120.0.0.0 0.0.0.255 gt 1023 established

Allow SMTP traffic to mail server.

access-list 110 permit tcp any 120.0.0.20 eq 25

Allow HTTP traffic to static content web server.

access-list 110 permit tcp any 120.0.0.30 eq 80

Allow HTTPS traffic to application web server.

access-list 110 permit tcp any 120.0.0.31 eq 443

Allow HTTPS traffic to OWA server.

access-list permit tcp any 120.0.0.20 eq 443

Allow SSH traffic to SSH server for sftp.

access-list permit tcp any 120.0.0.32 eq 22
access-list permit upd any 120.0.0.32 eq 22

Allow DNS queries to the external DNS server.

access-list 110 permit udp any 120.0.0.21 eq 53

Allow DNS Zone transfer to out backup DNS server

access-list 110 permit tcp 115.0.1.15 120.0.0.21 eq 53

**NOTE: 115.0.1.15 is the IP address of the backup DNS server on the ISP's network.*

Allow VPN traffic to firewall.

access-list 110 permit upd any 120.0.0.11 eq 500
access-list 110 permit esp any 120.0.0.11 eq 400

Deny anything that is not captured by any of the above rules and log.

access-list 101 deny ip any any log

Internal Interface Configuration

The follow extended access list is applied to the outbound traffic of the internal interface:

Reject outbound ICMP traffic.

access-list 120 deny icmp any any log

Reject outbound traffic where the source address is a non-routable private address (RFC 1918).

access-list 120 deny ip 192.168.0.0 0.0.255.255 any log
access-list 120 deny ip 172.16.0.0 0.15.255.255 any log
access-list 120 deny ip 10.0.0.0 0.255.255.255 any log

Reject outbound traffic where the destination address is a non-routeable private address (RFC 1918)

access-list 120 deny ip any 192.168.0.0 0.0.255.255 log
access-list 120 deny ip any 172.16.0.0 0.15.255.255 log
access-list 120 deny ip any 10.0.0.0 0.255.255.255 log

Permit outbound traffic from GIAC address.

access-list 102 permit ip 120.0.0.0 0.0.0.255 any

Deny anything that is not caught by the above rules and log.

access-list 102 deny ip any any log

Firewall Security Policy

Based on the defined access requirements, the following firewall policy was implemented:

Notation **--** The following notation is used when describing the rules that are defined on the Checkpoint firewall:

Source	Destination	Service	Action	Track

Source: Source IP address of the packet.
Destination: Destination IP address of the packet.
Service: The service which the packet is destined for. Note that Checkpoint comes with a list of defined services to choose from. A description of the service details (ports and protocols) will be included for each defined rule.

Action: The action to be performed when a match is found to the rule. Can be set to *Accept, Drop* or *Reject*. The difference between Drop and Reject is that Drop does not generate a reply where as Reject will reply with "packet rejected" or connection refused. Note: there are other options available for this setting but since they are not used, they have not been listed.
Track: Indicated how the event should be tracked (either *None* or *Log*). Note: there are other options available for this setting but since there are not used, they have not been listed.

Note: the rules are in the order as they would appear on the firewall.

Drop any NetBIOS traffic. Due to the amount of this type of traffic, it will not be tracked.

Source	Destination	Service	Action	Track
Any	Any	NBT	Drop	None

NBT Service includes:
nbdatagram: UDP, port 138
nbname: UDP, port 137
nbsession: UDP, port 139

Allow DNS queries to external DNS server.

Source	Destination	Service	Action	Track
Any	120.0.0.21	Domain-UDP	Permit	Log

Domain-UDP: UDP, port 53

Allow internal DNS servers to query external DNS server.

Source	Destination	Service	Action	Track
10.10.0.59	120.0.0.21	Domain-UDP	Permit	Log
10.10.0.58	120.0.0.21	Domain-UDP	Permit	Log

Allow ISA Proxy server to access the Internet

Source	Destination	Service	Action	Track
10.10.0.62	Any	Any	Permit	Log

Allow application web server to access web service on internal BizTalk server.

Source	Destination	Service	Action	Track
10.99.0.31	10.10.0.52	HTTPS	Permit	Log

HTTPS: TCP, port 443

Rule to allow web access to the external static content web server.

Source	Destination	Service	Action	Track
Any	120.0.0.31	HTTP	Permit	Log

HTTP: TCP, port 80

Rule to allow SSL access to the external application web server.

Source	Destination	Service	Action	Track

Any	120.0.0.31	HTTPS	Permit	Log

Rule to allow SSH access to the external SFTP/SSH server.

Source	Destination	Service	Action	Track
Any	120.0.0.32	SSH	Permit	Log

SSH: TCP, port 22

Allow SMTP server to forward mail to internal Exchange server.

Source	Destination	Service	Action	Track
10.98.0.20	10.10.0.56	SMTP	Permit	Log

SMTP: TCP, port 25

Allow Exchange server to send outbound email to external SMTP server.

Source	Destination	Service	Action	Track
10.10.0.56	10.98.0.20	SMTP	Permit	Log

Allow incoming mail to reach SMTP server

Source	Destination	Service	Action	Track
Any	120.0.0.20	SMTP	Permit	Log

Allow Domain controllers to synchronize time with external NTP time server.

Source	Destination	Service	Action	Track
10.10.0.56	Any	NTP	Permit	Log
10.10.0.57	Any	NTP	Permit	Log

NTP: TCP, port 123
UPD, port 123

Allow Zone transfers to the backup DNS server on the ISP's network.

Source	Destination	Service	Action	Track
*115.0.1.20	10.98.0.21	DNS	Permit	Log

**NOTE: 115.0.1.15 is the IP address of the backup DNS server on the ISP's network.*

Allow employees to access HTTP, HTTPS and SSH services in business services DMZ (i.e. DMZ #1)

Source	Destination	Service	Action	Track
10.20.0.0/16	10.99.0.0/24	TCP	Permit	Log
10.20.0.0/16	10.99.0.0/24	HTTPS	Permit	Log
10.20.0.0/16	10.99.0.0/24	SSH	Permit	Log

Allow eTrust Antivirus Server to access the Internet to update signature files.

Source	Destination	Service	Action	Track
10.10.0.51	Any	FTP	Permit	Log

FTP: TCP, port 21

Allow Exchange Server to access the Internet to update signature files for Antigen.

Source	Destination	Service	Action	Track
10.10.0.56	Any	FTP	Permit	Log

Allow Central Logging Server to access SFTP/SSH server.

Source	Destination	Service	Action	Track
10.10.0.51	10.99.0.32	SSH	Permit	Log

Allow TSM server to backup servers in the DMZ

Source	Destination	Service	Action	Track
10.10.0.53	10.99.0.0/24 10.98.0.0/24	TSM	Permit	Log

TSM: TCP, ports 1500-1501

Allow employees to access OWA server remotely

Source	Destination	Service	Action	Track
Any	10.10.0.64	SSL	Permit	Log

Rule to drop any packets sent to the firewall itself.

Source	Destination	Service	Action	Track
Any	120.0.0.11	Any	Drop	Log

Clean up rule. This rule is used to catch any traffic not caught by the above rules. Again we log these events.

Source	Destination	Service	Action	Track
Any	Any	Any	Drop	Log

VPN Security Policy

VPN functionality is included in the Checkpoint Firewall. Our VPN requirements are minimal as it is only being used to provide authorized employees access to the network.

VPN Client Security and Two Factor Authentication

We have opted to use SecureClient instead of SecureRemote so that we can enforce desktop security policies on the VPN client. This greatly reduces the possibility that a hacker can overtake a client machine and use it to gain access to the network. Also, to verify the identity of the VPN user, we are enforcing two factor authentication. In our case, we are using USB eTokens from Aladdin. The eTokens must be plugged into the VPN client system before access will be granted. The user must know the password of the eToken to unlock the credentials contained within it.

VPN Type

Of the available types of VPN's (SSH, SSL, PPTP and IPSec) we have chosen to use IPSec. IPSec is built into the Checkpoint firewall therefore was the easiest for us to configure.

User Authentication

Due to the limited number of VPN users (less than 20), we have opted to use Checkpoint's VPN-1 user authentication scheme. This requires that we create a username and password for each of our VPN users on the firewall. The password for the VPN account is encoded into the eToken and the user has no knowledge of the password. The password is randomly generated and stored on the eToken. The user must use their eToken password to unlock the VPN-1 credentials so that the logon credentials can be passed to SecureClient.

IPSec Details

IKE Settings

We have opted to use the public key authentication scheme instead of the pre-shared secret. Using the pre-shared secret method would be too difficult to manage compared to the public key method.

Security Association

Because we need to protect the confidentiality of the VPN traffic, we have opted to use the Encryption + Data Integrity Option (ESP). The "Data Integrity Only" (AH) option only ensures that the data in the packet has not been tampered with.

ESP Details

- Encryption Algorithm: 3DES
- Data Integrity: SHA1

VPN Firewall Rules

The following rule was added to the firewall policy to permit users to be able to use Terminal Services over a VPN connection:

Source	Destination	Service	Action	Track
*VPNUser	10.20.1.1	MS-TSClient	Permit	Log

MS-TSClient:TCP, port 3389
VPNUser – All VPN users are added to this Checkpoint VPN User group.

SecureClient Desktop Policies

To ensure that the VPN client is protected, the following desktop policies were defined:

Deny inbound connections when VPN is active:

Source	*Desktop	Service	Action	Track
Any	VPNUser@Any	Any	Block	Log

Allow inbound connections when VPN is not active

Source	Desktop	Service	Action	Track
Any	AllUsers@Any	Any	Permit	Log

Allow outbound connections when VPN is not active

Desktop	Destination	Service	Action	Track
AllUsers@Any	Any	**MS-TSClient	Permit	Log

***Desktop*:** We have two desktop security policies. The AllUsers@Any is the default desktop policy. It is in effect with or without the VPN connection. The VPNUser@Any is only in effect when the user is connected via VPN and logged into the policy server.

**MS-TSClient: TCP, port 3389

Additional Security Details

VPN users will only have Terminal Services access into internal network and they will only be able to Terminal Services into the dedicated terminal services server.

Firewall Policy Implementation Tutorial

The follow describes how to implement the firewall policy described above. You must have the Checkpoint Policy Editor NG FP2 installed on your system.

Step 1 – Define Hosts

Before we can start creating the firewall policy, we need to define the hosts that need access through the firewall. To create a new host, click on Manage → Network Object. You should see a screen similar to this one:

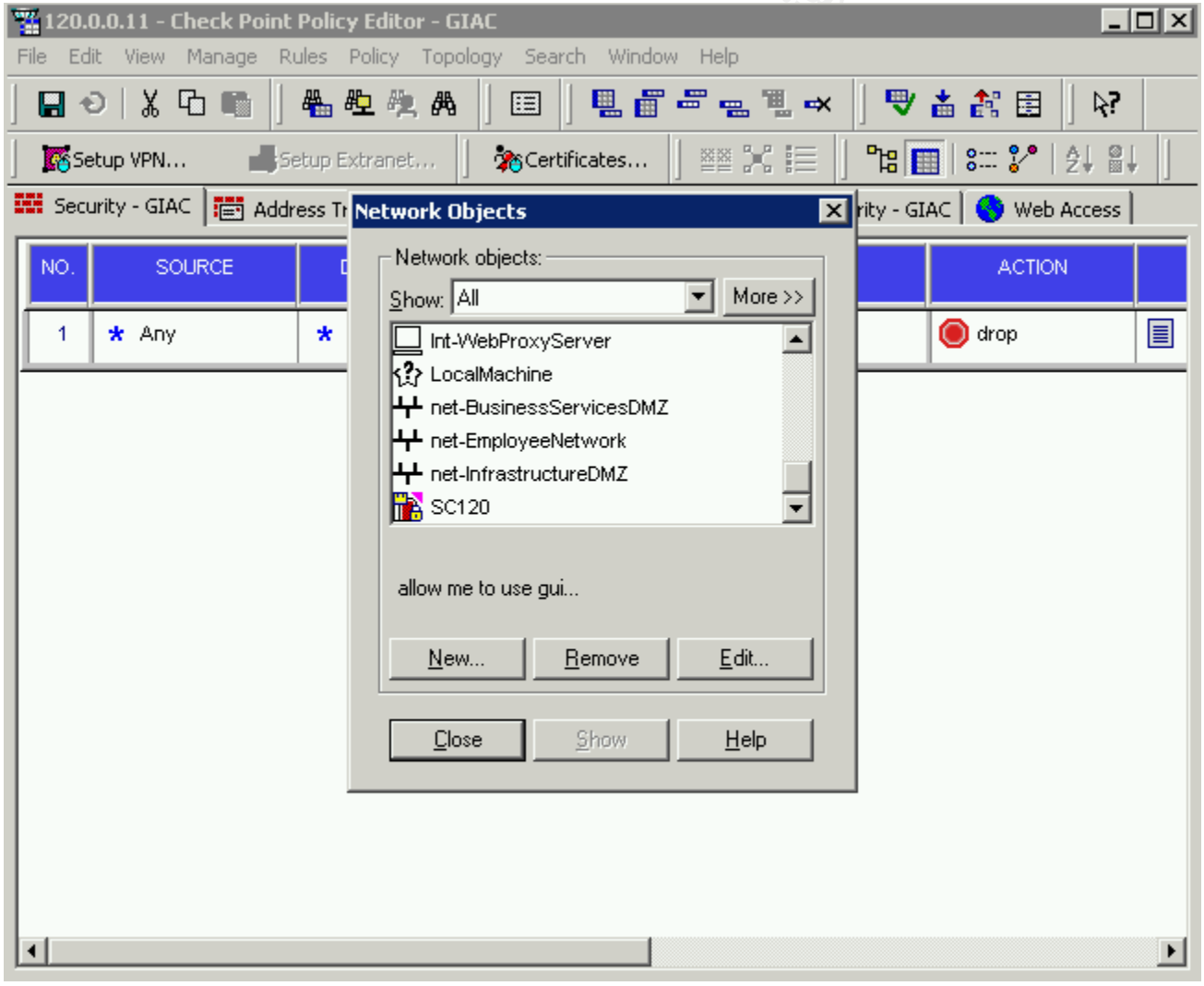


Figure 2 - Defining Hosts

Click on New →Node-Host. Enter in the Host name, IP address and description of the host (where appropriate, enable the NAT option). For those host that have an alias (refer to the network diagram, Figure 1), click on the Topology option and add the alias to the list. Note that the "name" of the alias refers to the interface on which the host can be found (i.e. eth0, eth1, eth2 or eth3). Repeat these steps for the following hosts:

Name	IP	Comment	Behind NAT
Ex-AppWebServer	10.99.0.31	External Application Web Server	Yes
Ex-SMTPServer	10.98.0.20	External SMTP and OWA server	Yes
Ex-StaticContWebServer	10.99.0.30	External Static Content Web Server	Yes
Ext-DNSServer	10.98.0.21	External DNS Server	Yes
Ext-FTPServer	10.99.0.32	External FTP Server	Yes
Int-AntivirusServer	10.10.0.51	Internal Antivirus Server	No
Int-BizTalkServer	10.10.0.52	Internal Production BizTalk Server	No
Int-CPMangServer	10.10.0.55	Internal Checkpoint Management Server	No
Int-DNS1Server	10.10.0.5	Internal DNS server #1	No
Int-DNS2Server	10.10.0.59	Internal DNS Server #2	No
Int-ExchangeServer	10.10.0.56	Internal Exchange 2K Server	No
Int-LogServer	10.10.0.51	Internal Central Logging Server	No
Int-TerminalServer	10.20.1.1	Internal Terminal Services Server	No
Int-TSMServer	10.10.0.53	Internal IBM TSM Backup Server	No
Int-WebProxyServer	10.10.0.62	Internal ISA Proxy Server used for outbound I...	Yes

When indicated above, enable the NAT option and select to hide behind their respective alias IP (refer to the network diagram, Figure 1). For the Int-WebProxy Server, it should be NATed behind the IP address of the firewalls external interface.

Step 2 – Define Networks

The next step is to define the networks. To create a network, click on Manage →Network Object. From the screen that is displayed, click on New→ Network. Enter in the network name, network address, and subnet mask of the network. In our case we need to define five networks with the following properties:

Name: **net-BusinessServicesDMZ**
Network Address: 10.99.0.0
Net Mask: 255.255.255.0

Name: **net-InternalNetwork**
Network Address: 10.1.0.0
NetMask: 255.255.255.0

Name: **net-InfrastructureDMZ**
Network Address 10.98.0.0
Net Mask: 225.255.255.0

Name: **net-EmployeeNetwork**
Network Address 10.20.0.0
Net Mask: 225.255.0.0

Name: **net-ProdServerNetwork**

Network Address 10.1.0.0
Net Mask: 225.255.255.0

Step 3 – Define Groups

The next step is to define the groups. Groups are collections of objects. To create a group, click on Manage → Network Object. From the screen that is displayed, click on New → Group → Simple Group. Enter in the Group Name and brief description of the group. Then proceed to add the objects that are members of the group. In our case, we need to define the following groups:

Name: **GRP-Int-DNSServers**
Hosts:
Int-DNS1Server ***(****defined in Step 1 above)*
Int-DNS2Server *(defined in Step 1 above)*
Purpose:

Name: **GRP-DMZ98**
Hosts:
Ext-SMTPServer *(defined in Step 1 above)*
Ext-DNSServer *(defined in Step 1 above)*

Name: **GRP-DMZ99**
Hosts:
Ext-AppWebServer *(defined in Step 1 above)*
Ext-StaticContWebServer *(defined in Step 1 above)*
Ext-FTPServer *(defined in Step 1 above)*

Name: **GRP-GIACNetworks**
Networks:
Net-BusinessServicesDMZ *(defined in Step 2 above)*
Net-EmployeeNework *(defined in Step 2 above)*
Net-InfrastuctureDMZ *(defined in Step 2 above)*
Net-InternalNetwork *(defined in Step 2 above)*
Net-ProdServerNetwork *(defined in Step 2 above)*

Name: **GRP-InternalNetworks**
Networks:
Net-EmployeeNetwork *(defined in Step 2 above)*
Net-InternalNetwork *(defined in Step 2 above)*
Net-ProdServerNetwork *(defined in Step 2 above)*

Step 4 – Configure Firewall Interfaces

The next step is to configure the firewall interfaces. Click on Manage → Network Object. Scroll down the list of available objects and select SC120 (name assigned to firewall). Click on Edit. From the

window that is displayed, click on Topology. In the window, you should now see the available interfaces. Highlight eth0 and click on edit. Click on the Topology tab and then select External (leads out to the Internet). The Antispoofing option should be enabled by default. Click on OK when done. Repeat these steps for the other 3 interfaces selecting the following options under the topology tab:

Eth1: Click on Internal (leads to local network). Select "Network defined by the interface IP and Net Mask.
Eth 2: Click on Internal (lead to local network). Select Specific and change to grp-DMZ99 (this is one of the groups we defined in Step 3 above).
Eth 3: Click on Internal (leads to local network). Select Specific and change to grp-DMZ98 (this is one of the groups we defined in Step 3 above).

Step 5 – Configuring Firewall Rules

We can finally start configuring the firewall rules. Creating a rule is easy. Simply click on Rules → Add Rule. Then select either Bottom, Top Below or Above depending on where you the rule to be located. The default rule appears as follows:

NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	* Any	* Any	* Any	* Any	drop	- None	* Policy Targets	*	

Right click in each of the cells and select the appropriate value. In our particular case, you will not need to make any changes to the "IF VIA" column or the TIME column.

Taking the details from above, you'll need to define the following rules:

NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	* Any	* Any	* Any	NBT	drop	Log	SC120	* Any	Block any NBT traffic. Do not log.
2	* Any	Ext-DNSServer	* Any	domain-udp	accept	Log	SC120	* Any	Allow DNS queries to reach external DNS server
3	Int-WebProxyServer	net-BusinessServicesDMZ Net-InfrastructureDMZ	* Any	* Any	accept	Log	SC120	* Any	Allow ISA proxy server to access the Internet. Deny access to DMZ's
4	Ex-AppWebServer	Int-BizTalkServer	* Any	https	accept	Log	SC120	* Any	Allow Application Web Server to access SSL encrypted web service on internal BizTalk server
5	* Any	Ex-StaticContWebServer	* Any	http	accept	Log	SC120	* Any	Allow global access to static content web server
6	* Any	Ex-AppWebServer	* Any	https	accept	Log	SC120	* Any	Allow global access to the application web server via SSL
7	* Any	Ext-FTPServer	* Any	ssh	accept	Log	SC120	* Any	Allow global access to the secure SFTP/SSH server
8	Ex-SMTPServer	Int-ExchangeServer	* Any	smtp	accept	Log	SC120	* Any	Allow external SMTP server to forward mail to internal Exchange server.
9	grp-GIACNetwork	Ex-SMTPServer	* Any	smtp	accept	Log	SC120	* Any	Allow inbound email to reach external SMTP server
10	Int-ExchangeServer	Ex-SMTPServer	* Any	smtp	accept	Log	SC120	* Any	Allow Exchange to send outbound email to external SMTP server
11	Ex-SMTPServer	grp-GIACNetwork	* Any	smtp	accept	Log	SC120	* Any	Allow external SMTP server to send outbound emails outside the GIAC network
12	Ext-DNSServer	grp-GIACNetwork	* Any	domain-udp	accept	- None	SC120	* Any	Allow external DNS server to query external DNS servers
13	grp-Int-DNSServer	grp-GIACNetwork	* Any	ntp	accept	Log	SC120	* Any	Allow internal DNS servers to synchronize time with external NTP servers
14	ISP-BCKUPDNS	Ext-DNSServer	* Any	domain-tcp	accept	Log	SC120	* Any	Allow DNS zone transfers to backup DNS server on ISP's network
15	Int-AntivirusServer Int-ExchangeServer	grp-GIACNetwork	* Any	ftp	accept	Log	SC120	* Any	Allow Antivirus and Exchange server (Antigen AV) to obtain virus signature updates via FTP
16	Int-TSMServer	grp-DMZ98 grp-DMZ99	* Any	TSM	accept	Log	SC120	* Any	Allow TSM backups of servers in the DMZ
17	* Any	Int-OWAServer	* Any	https	accept	Log	SC120	* Any	Allow global access access to the internal OWA server
18	* Any	SC120	* Any	* Any	drop	Log	SC120	* Any	Stealth firewall by dropping any packets sent directly to it.
19	* Any	* Any	* Any	* Any	drop	Log	SC120	* Any	Drop anything that falls through

Figure 3 -Firewall Rules

Note: In rule 16, the service is set to TSM. This service did not come with Checkpoint and was manually created using the following steps:

1. Click on Manage → Services
2. Click on the New → TCP
3. Set the following parameters:
   Name: TSM
   Comment: Tivoli Storage Manager
   Port: 1500-1501
4. Click on OK.

After you have entered in all the above rules click on File → Save to save the rule set. The last step is to apply the rules to the enforcement module. Click on Policy → Install. Confirm that the policy is going to be applied to the correct enforcement module (in our case SC120) and click on OK. Wait until you see a success message in the window before you close down the status window.

Assignment 3 – Verify the Firewall Policy

Overview

To ensure that we haven't made any errors in either the design or implementation of our firewall policy, we are going to perform an audit of the firewall. The intent of this audit is to ensure that the firewall policy we have defined has been properly implemented. This audit will not do a general vulnerability assessment of the firewall. For the purposes of this audit, the following tasks are out of scope:

- Verifying that physical security controls are in place to access the firewall.
- Ensuring that the underlying operating system has been secured.
- Verifying that any third party add-ons to the firewall (i.e. antivirus, IDS, etc) are functioning correctly.

In order to minimize costs, the audit will be performed by the senior Network Support Administrator. This employee has the most experience with the firewall and analysis tools.

Planning the Audit

Before performing an audit it is important to have a well documented plan. The goals of the audit must be clearly stated such that the task will remain on track. The plan will clearly document the time and place of the audit and list the resources required to perform the audit. The plan must also ensure that the audit is done within the allotted budget.

Before the audit can be performed, the following tasks must be completed:

- Advise the CIO of the pending audit. Since the tools that we are using may have a negative affect on the servers or the network, we must have written approval from the CIO prior to performing the audit.
- Advise Production and Network Support of the pending audit. Schedule a meeting to discuss the purpose of the audit. Ensure that the participants are aware that the audit to ensure that the firewall policy has been implemented properly and is not a means of checking how they are performing their jobs.
- Verify that system backups have been done on all critical systems. This is to ensure that the systems can be restored in the event of a catastrophic failure.
- Advise the ISP of the pending audit. Provide dates and time of the auditing and include what IP addresses will be involved.

Scheduling

Since we have a regular monthly maintenance window, we will schedule the audit for that time frame. Doing the audit during the maintenance window will mean that we won't have to coordinate the audit with our external customer, business partners or employees. The maintenance window is scheduled for the first Sunday of every month from 1:00am to3:00pm PST (14 hours). Email notices are sent out the Thursday prior to the maintenance window to remind customers, business partners and employees of the upcoming maintenance window.

The audit will start at 1:00am for the May maintenance window and must be completed by 6:00am. That gives Production and Network Support 9 hours to verify that none of the systems have been adversely affected.

Resource Requirements and Budget

The following resources will be required:

Resource	Time	Activity
1 Network Support	12 hours	Verify that systems come back online after the audit is completed; recover systems in the event of failure.
1 Prod Support	12 hours	Verify that systems come back online after the audit is completed; recover systems in the event of failure.
1 Application Support	3 hours	Test the web service functionality after the audit is completed to ensure that nothing has been broken.
1 Senior Prod Support	50 hours	Plan, coordinate and perform the audit. Analyze and document the results.
Contingency	20 hours	For the unexpected.

The audit will be broken down into the following activities:

Activity	Time (all resources)
Planning	20 hours
Meetings	9 hours
Performing Audit	25 hours
Analysis and Documentation	20 hours
Contingency	20
Total	**94 hours**

Assuming a blended rate of $60.00 per hour, the estimated labor budget for the audit is $5760. The blended rate includes the fact that some of the time will be charged at overtime rates.

Risks

One of the main risks we will face when performing this audit is the fact that a real attack on the network may be masked by our auditing activities. To mitigate this risk, the following will be done:

1. For the auditing tasks that do not require Internet access, the network cable from the border router to the firewall will be disconnected.
2. Upon completion of the audit, all systems will be scanned for viruses/trojans.
3. A detailed log analysis will be done after the audit is complete to verify that no unexpected traffic was detected on the network during the audit.

Technical Approach

The approach that will be used to verify the firewall policy will be as follows:

Phase 1: Scan the firewall itself from each of its interfaces.
Phase 2: From the Internet, scan the GIAC network to determine what services can be accessed.
Phase 3: From each subnet, scan the other subnets to determine what services can be accessed.
Phase 4: Take down specific production systems and replace them with one of our auditing systems to determine what resources are available to them.

We will have two laptops at our disposal during the audit, both running Windows XP. While one laptop is doing a scan, the other laptop will be configured to sniff the network traffic on the target network. The results from the scan, the firewall logs and the output from Ethereal will all be used to determine whether or not the firewall policy has been implemented properly.

Tools

NmapWin v1.3.1

To scan the firewall for open ports, we will be using Nmap. Nmap is a network exploration and security scanner tool.

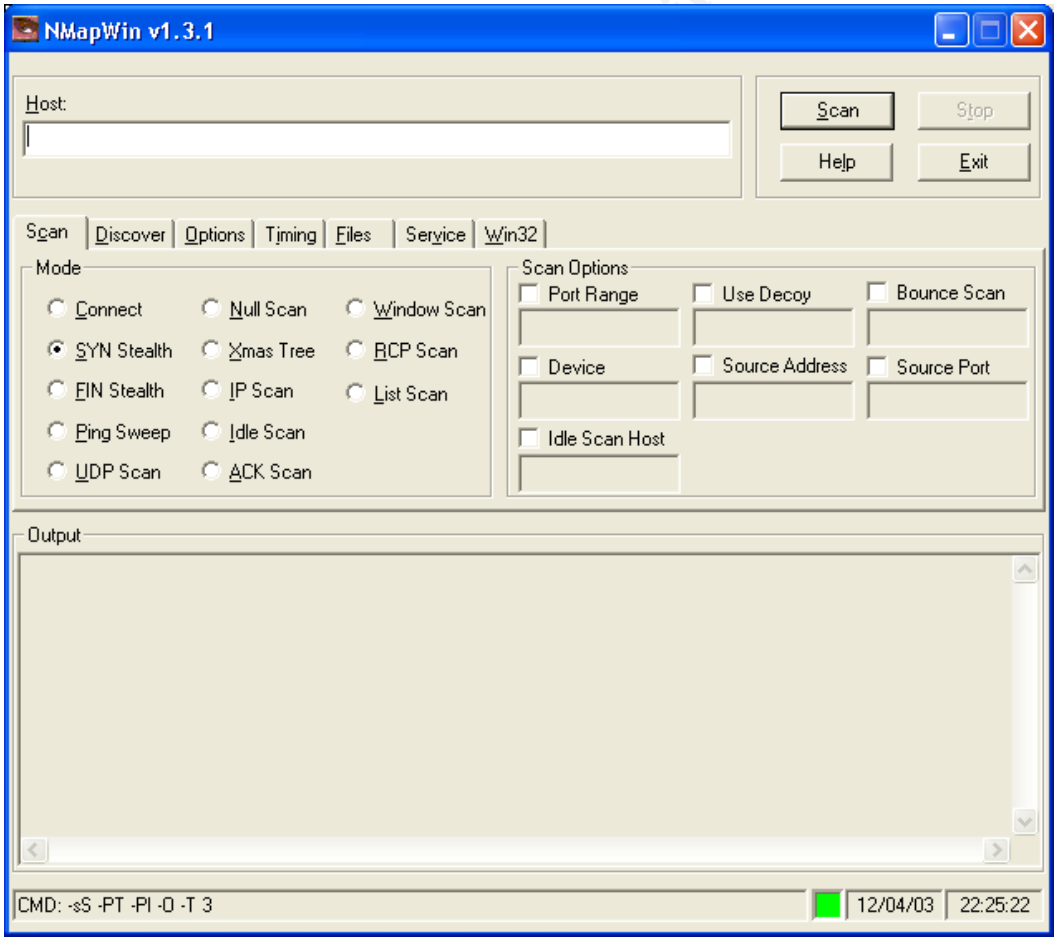


Figure 4 - Nmap

To start a scan, you simply indicate what host you want to scan and then click on the *Scan* button. The result of the scan will be displayed in the Output area of the window after the scan has been completed. Nmap has a wide range of scanning options that can be used. In our case, the following scans will be performed:

SYN Stealth Scan – This technique is also referred to as "half-open" scanning. A SYN packet is sent as if a connection were to be opened. A SYN|ACK response indicates that the port is open. A RST response typically means that the port is not listening.

UDP Scan – This scan will reveal what UDP ports are listening.

The following options also need to be set during the scan:

- Under the *Discover Tab*: Select Don't Ping
- Under the *Options Tab*: Unselect the *OS Detection* option
- Under the *Timing Tab*: Select the *Aggressive* option

Ethereal –v0.9.9 (Windows version)

Ethereal is a network protocol analyzer that can be used to determine what type of traffic can be seen on a network.

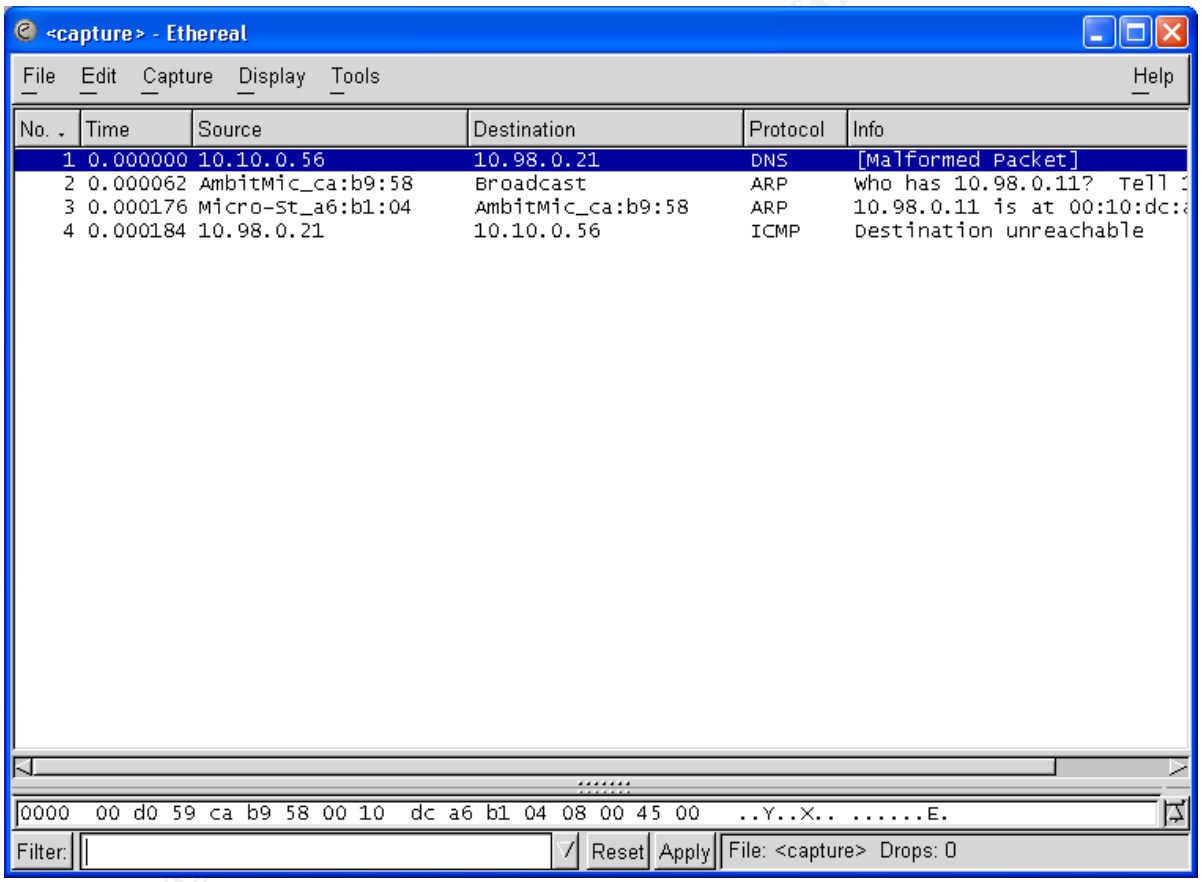


Figure 5 - Ethereal

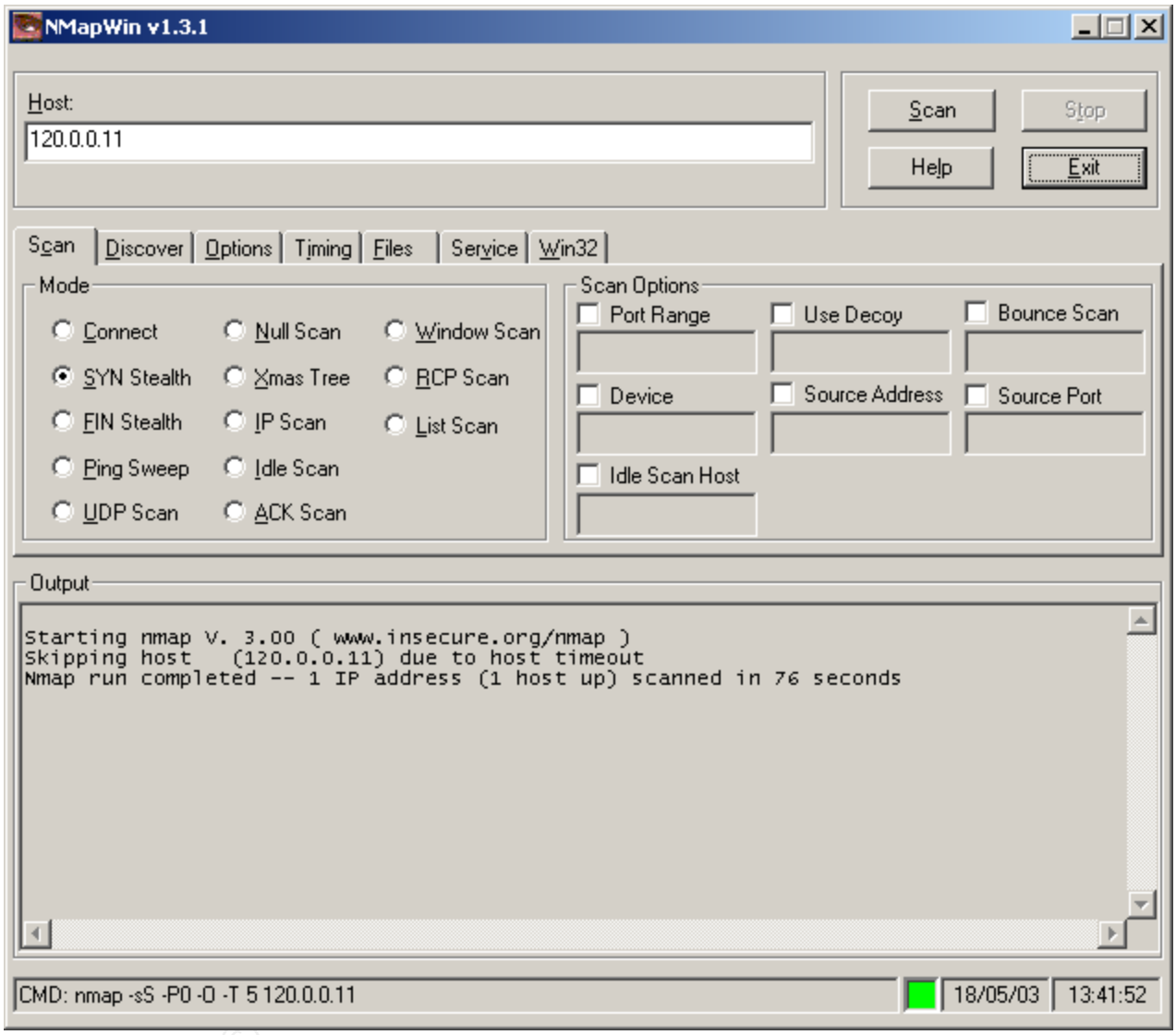
Ethereal has a very straight forward interface and is very easy to use. To start a scan, simply click on Capture → Start. If you want observe the traffic in real time in the capture window, enable the "update packets in real time" option. When you want to stop the scan, click on the Stop button.

NOTE: Both Ethereal and Nmap require that you install WinPcap.

The Audit

Phase 1 – Scanning the firewall

The first step in our audit is to scan the firewall itself for any listening ports. We start by disconnecting the cable from the firewall to the border router. We take one of our audit laptops and plug it into this interface (eth0) using a rolled CAT5 cable and launch NMap to scan the firewall at 120.0.0.11. The following is observed during the SYN scan:



As expected, we find no listening ports. We repeat the above but this time do a UDP scan and obtain the following results:

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Warning:  OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed  TCP port
Interesting ports on 120.0.0.11:
(The 1467 ports scanned but not shown below are in state: closed)
Port        State       Service
259/udp     open        firewall1-rdp
Nmap run completed -- 1 IP address (1 host up) scanned in 22 seconds
```

We do some research regarding UDP port 259 and determined that it is used by Checkpoint for FWZ Key Negotiations and is also used by SercureRemote and SecureClient to check for the availability of a VPN policy server. In our case, the port is available due to the fact that we are using a VPN Policy Server.

We repeat the above steps for the remaining three interfaces (eth1-10.1.0.11, eth2-10.99.0.11, eth3-10.98.0.11) and discover that no ports are listening.

Phase 2 – Scan from the Internet

The next phase of the audit is to scan the GIAC network from the Internet. We issue the following Nmap commands from our laptop that is currently configured with public Internet address:

```
nmap -sS -P0 -O -T 5 120.0.0.*
nmap -sU -P0 -O -T 5 120.0.0.*
```

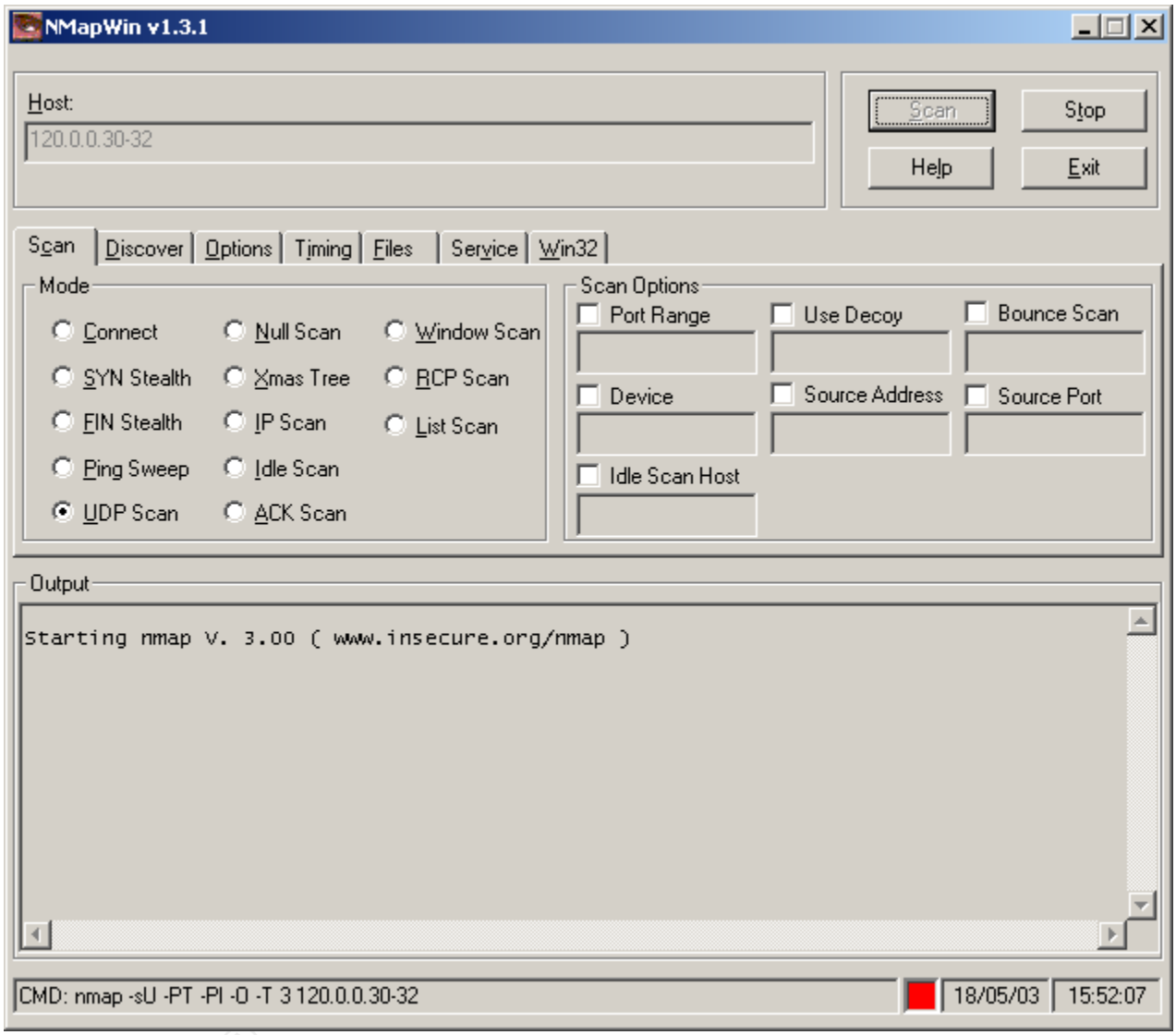
The above Nmap scans revealed the following listening ports:

Host	Protocol	Port	Description
120.0.0.30	TCP	80	Static Web Server
120.0.0.31	TCP	443	App. Web Server (SSL)
120.0.0.32	TCP	22	SSH/SFTP Server
120.0.0.20	TCP	25	SMTP Server
120.0.0.21	UDP	53	DNS Server
120.0.0.50	TCP	443	OWA Serve (SSL)

As part of this phase, we want to determine if any additional traffic is permitted into a particular subnet while we perform our scan from the Internet. We setup one of the laptops in one of the DMZ subnets and start capturing network traffic with Ethereal. We run the above two scans again and record the results. We then move the laptop to the other DMZ and repeat the scans. As a final step, we move the laptop with Ethereal to the Internal network and repeat the above scans. Upon reviewing all the output from Ethereal and the firewall logs, we determine that no traffic, other than what was identified above, was permitted into the GIAC network.

Phase 3 – Scan Between Subnets

In this phase, we will scan each subnet from the other subnets to determine what type of default traffic we are permitting between subnets. For the first scan, we will put one of the laptops in the DMZ #2 network and configure it to perform a SYN and UPD scan against the systems in DMZ#1 network. The second laptop is put in the DMZ#1 network and Ethereal is started to capture network traffic. Below is an example of the UPD scan:



Examine the output from NMap revealed the following listening ports:

Host	Protocol	Port	Description
120.0.0.30	TCP	80	Static Web Server
120.0.0.31	TCP	443	App. Web Server (SSL)
120.0.0.32	TCP	22	SSH/SFTP Server

The output from Ethereal and the firewall logs did not indicate that any traffic, other than what is listed above was permitted into the DMZ #1 network.

Using the same procedure described above, we continue our scan from the DMZ#1 network and scan the internal network and find the following listening port:

Host	Protocol	Port	Description
10.10.0.64	TCP	443	SSL connection to OWA server

The firewall and Ethereal output revealed that no additional traffic was permitted into the internal network.

Our next scan is from the DMZ#2 network. We start first by scanning of the DMZ#1 network using the same technique described above. The scan revealed the following listening ports:

Host	Protocol	Port	Description
120.0.0.20	TCP	25	SMTP Server
120.0.0.21	UDP	53	DNS Server

The output from Ethereal and the firewall logs did not reveal any additional traffic that was permitted to pass into the network. Next we scan the internal network from the DMZ#2 network. The scan identified the following listening ports:

Host	Protocol	Port	Description
10.10.0.64	TCP	443	SSL connection to OWA server

The firewall logs and Ethereal revealed that no additional traffic was permitted to pass into the internal network from the DMZ#2 network.

The last scan in this phase is to scan the two DMZ networks from the Internal network. We start by scanning the DMZ#1 network and find no listening ports. Analyzing the firewall logs and the output from Ethereal revealed no additional traffic permitted from the Internal network to DMZ#1. The final scan in this phase is to scan the DMZ#2 network from the Internal network. In this scan we find the following listening ports:

Host	Protocol	Port	Description
120.0.0.30	TCP	80	Static Web Server
120.0.0.31	TCP	443	App. Web Server (SSL)
120.0.0.32	TCP	22	SSH/SFTP Server

Analysis of the Ethereal output and the firewall logs revealed that no additional traffic was permitted to the DMZ#1 network during the scan.

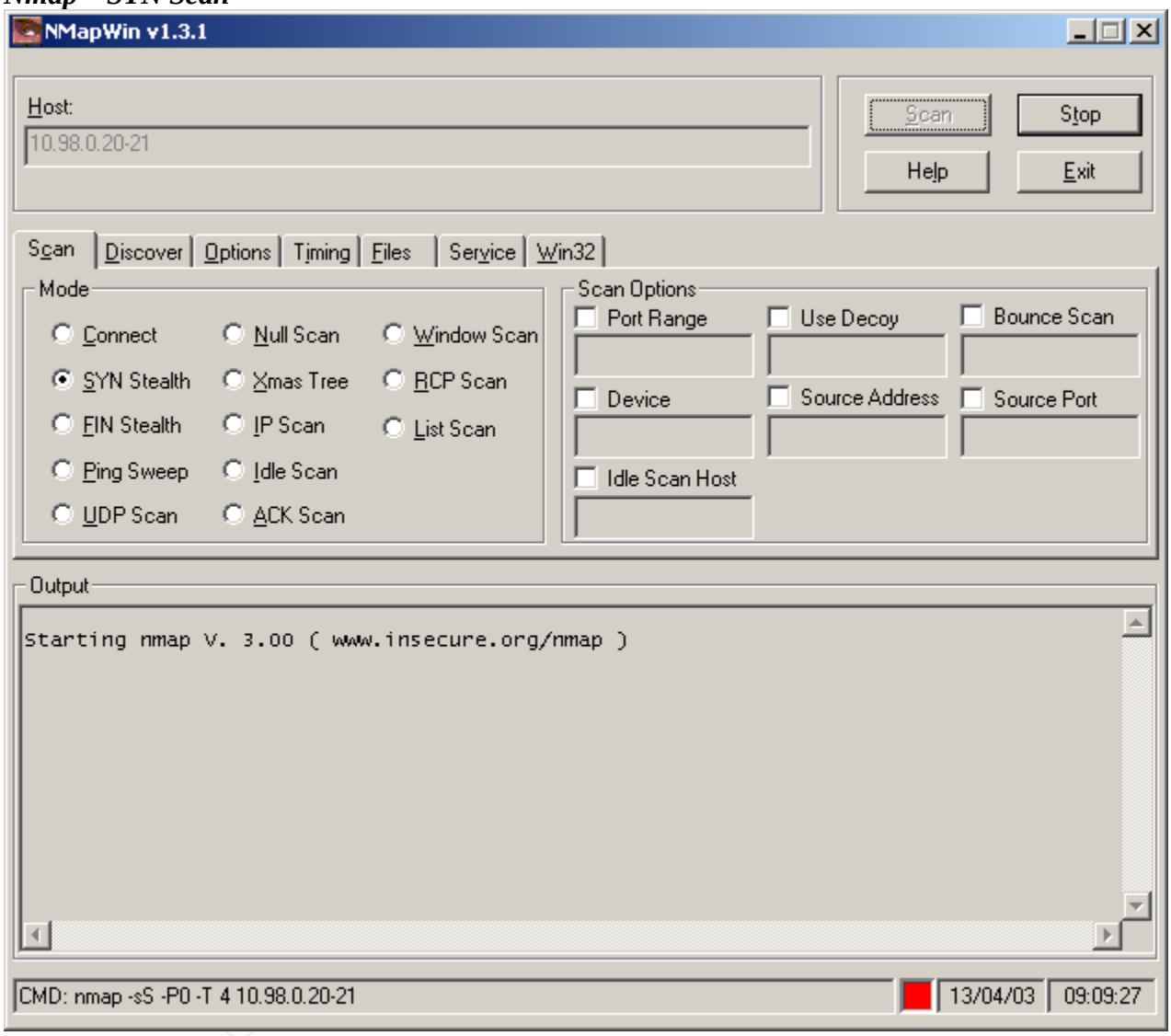
Phase 4 – Perform Scan of Subnets while Impersonating a Production Server

Next we configure one of the laptops with the same IP address as one of the servers we want to impersonate and start up Nmap. We configure Nmap for the type of scan we want to perform (SYN or UPD in our case) and fill in the address of the subnet that we want to scan. The second laptop is placed in the target subnet and assigned an appropriate address. Ethereal is started on this laptop so that it can capture the network traffic. We can now do a SYN scan and UDP scan of the target subnet. We

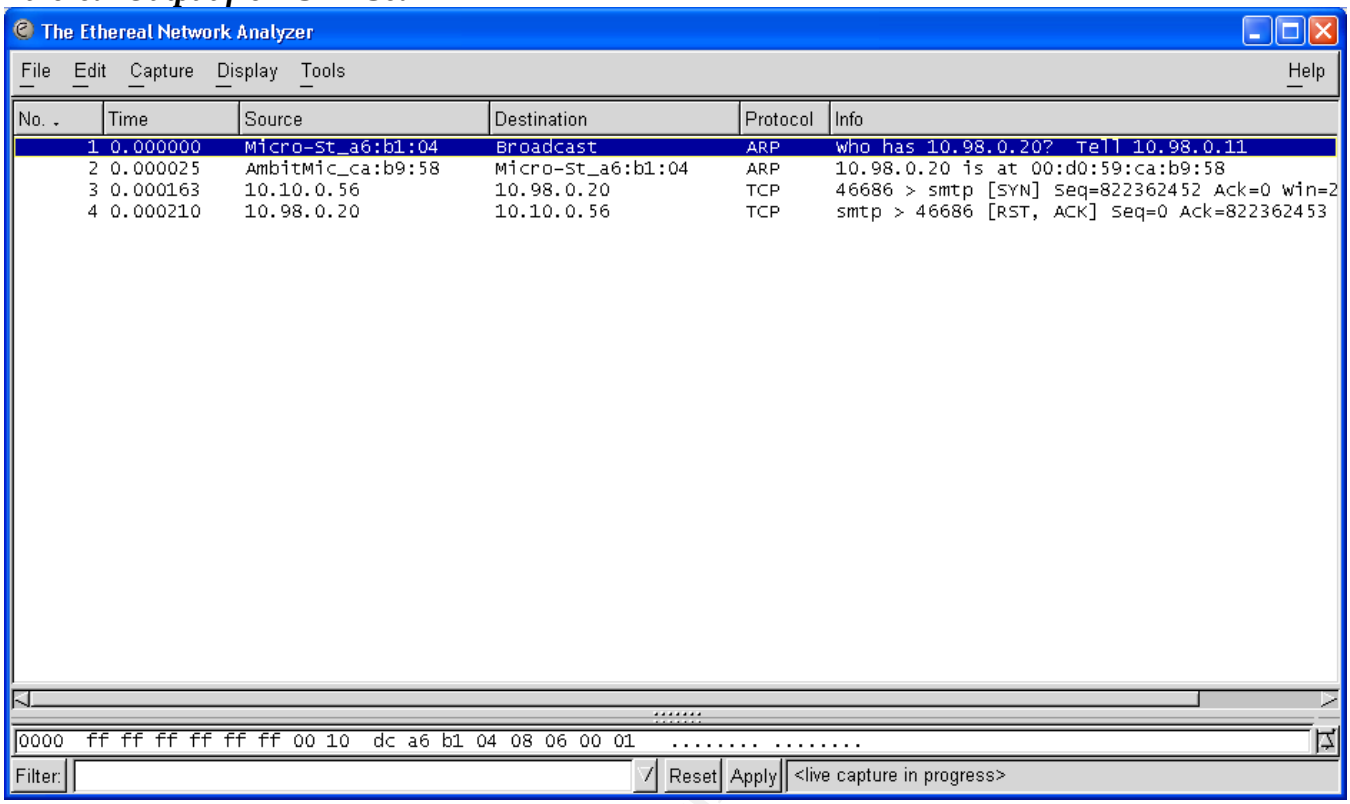
examine the output from Ethereal and the firewall logs to determine if the correct traffic was permitted thereby verifying if the firewall policy was correctly implemented.

The following is an example of a SYN scan from the internal network with the NMap scanning laptop impersonating the internal Exchange server and targeting the only two systems in the DMZ#2 network (10.98.0.20 and 10.98.0.21). The second laptop was put into the DMZ#2 network and captured the scan with Ethereal.

Nmap – SYN Scan

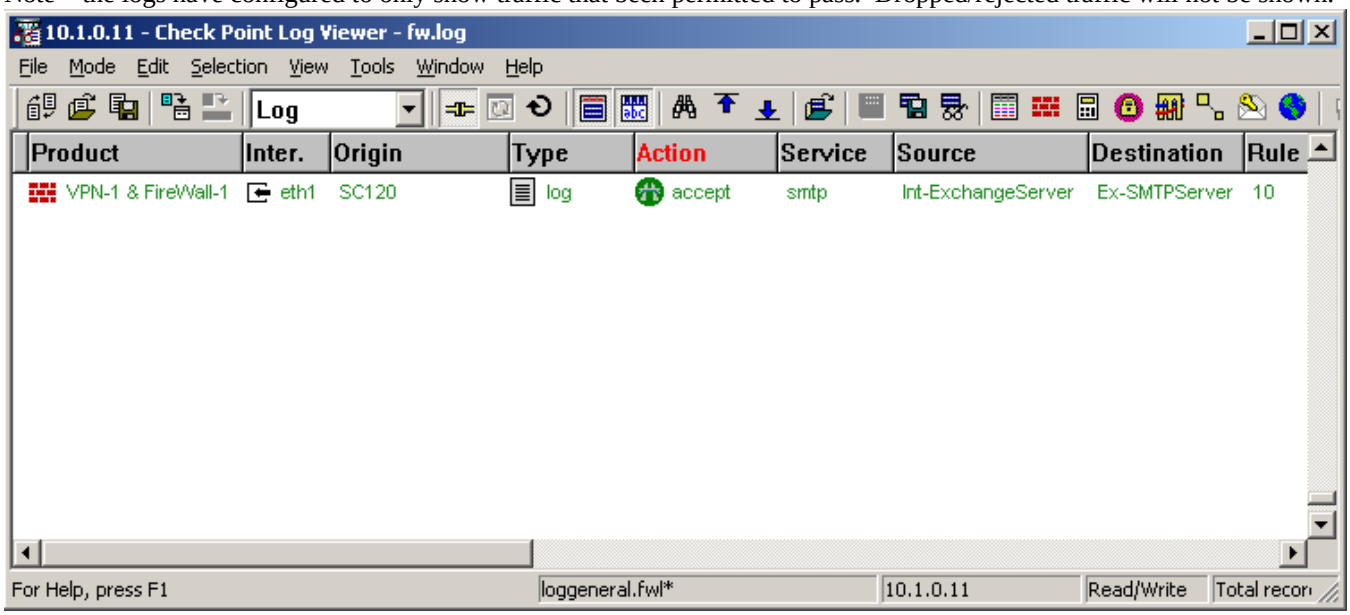


Ethereal Output from SYN Scan



Checkpoint Firewall Log Output from SYN Scan

Note – the logs have configured to only show traffic that been permitted to pass. Dropped/rejected traffic will not be shown.



As per our firewall policy, the internal Exchange server is permitted to communicate via SMTP to the SMTP server on the DMZ#2 network. It can be clearly seen by the output of Ethereal and the firewall logs that only SMTP was permitted to pass into the DMZ98 network from the internal Exchange server. The above process was used to perform SYN and UDP scans against all the source hosts/target network pairs and the results are summarized below.

Scanning from the Internal Network

From the **Exchange Server**, the scan revealed the following:

1. SMTP traffic permitted to SMTP server on DMZ#2
2. HTTP traffic permitted to static content web server on DMZ#1
3. HTTPS traffic permitted to application web server on DMZ#1
4. SSH traffic permitted to SSH server on DMZ#1
5. DNS traffic (UPD/53) permitted to DNS server on DMZ#2
6. FTP traffic permitted to the Internet
7. All other traffic dropped

From the **Domain Controllers**, the scan revealed the following:

1. DNS traffic (UPD/53) permitted to DNS server on DMZ#2
2. HTTP traffic permitted to static content web server on DMZ#1
3. HTTPS traffic permitted to application web server on DMZ#1
4. SSH traffic permitted to SSH server on DMZ#1
5. NTP traffic permitted to external NTP servers
6. All other traffic dropped

From the **DNS Servers,** the scan revealed the following:

1. DNS traffic (UPD/53) permitted to DNS server on DMZ#2
2. HTTP traffic permitted to static content web server on DMZ#1
3. HTTPS traffic permitted to application web server on DMZ#1
4. SSH traffic permitted to SSH server on DMZ#1
5. All other traffic dropped

From the **Proxy Server**, the scan revealed the following:

1. Full internet access permitted (UDP/TCP- all ports)
2. DNS traffic (UPD/53) permitted to DNS server on DMZ#2
3. All other traffic dropped

From the **Checkpoint Management Server**, the scan revealed the following:

1. DNS traffic (UPD/53) permitted to DNS server on DMZ#2
2. HTTP traffic permitted to static content web server on DMZ#1
3. HTTPS traffic permitted to application web server on DMZ#1
4. SSH traffic permitted to SSH server on DMZ#1
5. All other traffic dropped

From the **BizTalk Server**, the scan revealed the following:

1. DNS traffic (UPD/53) permitted to DNS server on DMZ#2
2. HTTP traffic permitted to static content web server on DMZ#1
3. HTTPS traffic permitted to application web server on DMZ#1
4. SSH traffic permitted to SSH server on DMZ#1
5. All other traffic dropped

From the **Antivirus/Logging Server**, the scan revealed the following:

1. DNS traffic (UPD/53) permitted to DNS server on DMZ#2
2. HTTP traffic permitted to static content web server on DMZ#1
3. HTTPS traffic permitted to application web server on DMZ#1
4. SSH traffic permitted to SSH server on DMZ#1

5. FTP traffic permitted to the Internet
6. All other traffic dropped

From the **IBM TSM Server**, the scan revealed the following:
1. DNS traffic (UPD/53) permitted to DNS server on DMZ#2
2. HTTP traffic permitted to static content web server on DMZ#1
3. HTTPS traffic permitted to application web server on DMZ#1
4. SSH traffic permitted to SSH server on DMZ#1
5. TCP/port 1500 permitted to servers in DMZ#2 and DMZ#2
6. TCP/port 1501 permitted to servers in DMZ#2 and DMZ#1
7. All other traffic dropped
8.

Scanning from DMZ#2

From the **SMTP Server**, the scan revealed the following:
1. HTTP traffic permitted to static content web server on DMZ#1
2. HTTPS traffic permitted to application web server on DMZ#1
3. SSH traffic permitted to SSH server on DMZ#1
4. SMTP traffic permitted to the Internet
5. SMTP traffic permitted to the internal Exchange server
6. HTTPS traffic permitted to the internal OWA server
7. All other traffic dropped

From the **DNS Server**, the scan revealed the following:
1. HTTP traffic permitted to static content web server on DMZ#1
2. HTTPS traffic permitted to application web server on DMZ#1
3. SSH traffic permitted to SSH server on DMZ#1
4. DNS traffic (UPD/53) permitted to the Internet
5. HTTPS traffic permitted to the internal OWA server
6. SMTP traffic permitted to the Internet
7. All other traffic dropped

Scanning from DMZ#1

From the **Static Content Web Server**, the scan revealed the following:
1. HTTPS traffic permitted to the internal OWA server
2. DNS traffic (UPD/53) permitted to DNS server on DMZ#2
3. All other traffic dropped

From the **Application Web Server**, the scan revealed the following:
1. HTTPS traffic permitted to the internal OWA server
2. HTTPS traffic permitted to the internal BizTalk server
3. DNS traffic (UPD/53) permitted to DNS server on DMZ#2
4. All other traffic dropped

From the **Secure FTP (SSH) Server**, the scan revealed the following:
1. HTTPS traffic permitted to the internal OWA server
2. DNS traffic (UPD/53) permitted to DNS server on DMZ#2
3. All other traffic dropped

Evaluating the Audit

The analysis of the audit revealed the following:

1. System in DMZ#2 and DMZ#1 could not update their antivirus signature files.
2. Systems in DMZ#2 and DMZ#1 had access to the internal OWA server.
3. Logs from the border router cannot reach the internal log server.
4. The border router is not configured to allow access to UDP/259 thereby preventing the SecureClient from communicating with the Policy Server.

As a result, the following recommendations were made:

1. Update the firewall policy and add the appropriate rule to permit the servers in DMZ#2 and DMZ#1 to update their antivirus signature files from the internal Antivirus server
2. Allowing HTTP access to the OWA server from the any of DMZ servers could result in an infected email attachment being downloaded to these servers. As a result, it is recommended that the firewall policy be updated to restrict access to the OWA server from servers in DMZ#2 and DMZ#1. Rule 17 on the firewall should be modified such that servers in DMZ#2 and DMZ#1 are not permitted HTTPS access to the OWA server.
3. Update the firewall policy and add the appropriate rule to permit the border router to send logs to the internal log server.
4. Add a new ACL on the router permitting UPD/259 traffic to the firewall.

During the audit, we also observed that a few changes in the our firewall rule order is probably necessary. The change in rule order is to improve the efficiency of the firewall and not to address any specific security concern. The stealth rule, (#18) should be moved up to into position #2. We want our firewall to drop traffic sent directly to it as quickly as possible. There may be other changes to the rule order but further traffic analysis is needed before we can make any conclusions.

Assignment 4 – Design Under Fire

In this exercise, we will be describing an attack against the network designed by (Analyst #: 0356), http://www.giac.org/practical/GCFW/Craig_Duerr_GCFW.pdf

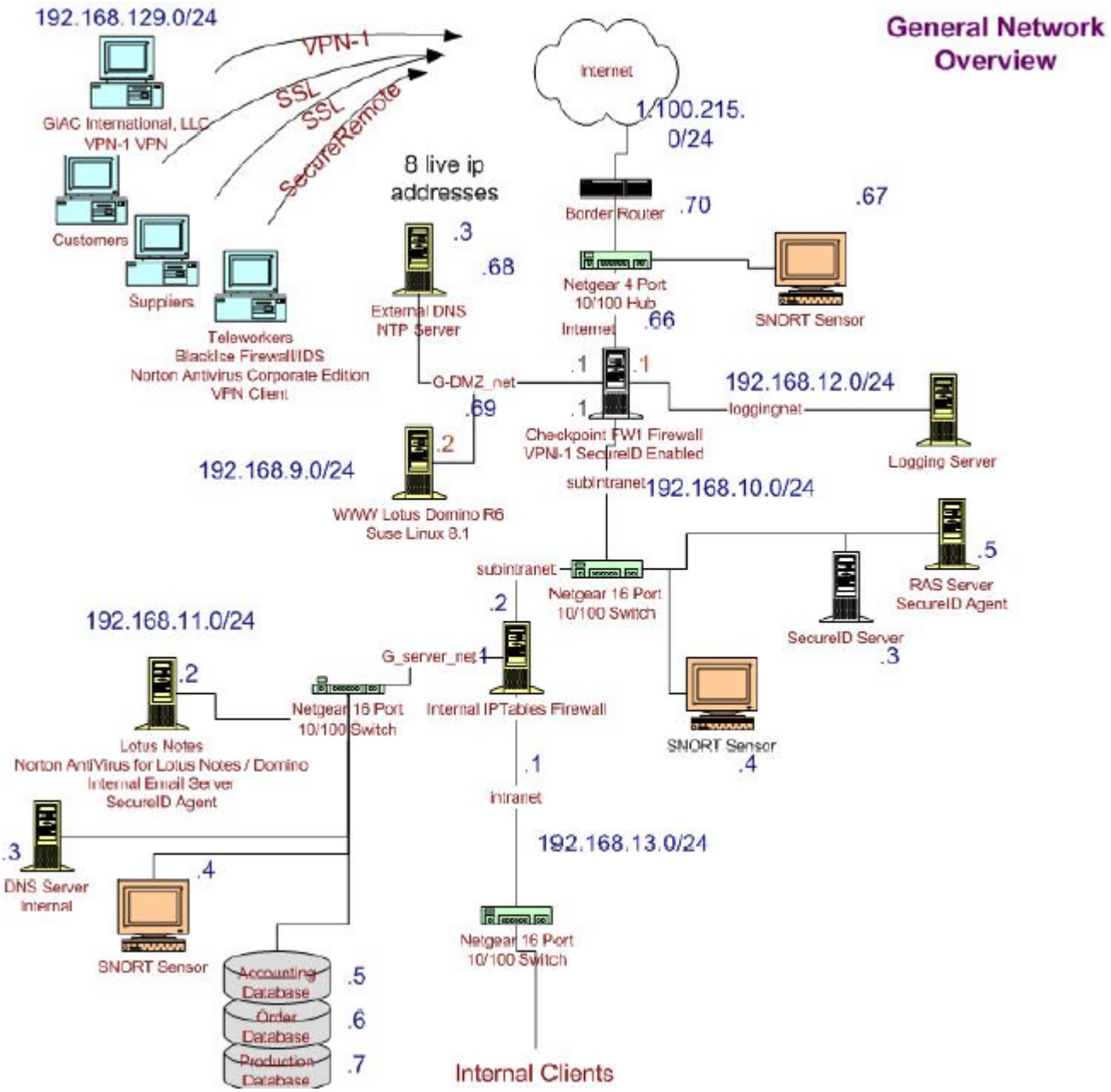


Figure 6 – Craig Duerr's Network Design

The two items to note in this diagram are the Checkpoint firewall and the Lotus Domino web server. It is these two items that we will be basing our attack on.

Attacking the Firewall

Any successful attack requires research and planning. Since we already have a copy of Craig's network diagram and description of his perimeter components, we already have a great deal of information about

his network. Typically, such information would have to be learned through OS or application fingerprinting. In this case we already know that Craig is running Checkpoint FW-1 SP6 on Windows 2000 (SP3) server. With this information in hand, the next step is to attempt to identify a vulnerability that we can exploit.

Identifying a Vulnerability

There are many sources of information that one can use to gather information regarding known vulnerabilities for a given piece of software. We start our research but doing a search through the Bugtraq database on the SecurityFocus website (http://www.securityfocus.com/cgi-bin/sfonline/vulns.pl). Our search for Checkpoint FW-1 SP6 revealed the following vulnerabilities:

2003-02-10: Multiple Vendor HTTP CONNECT TCP Tunnel Vulnerability
2002-09-19: Check Point Firewall-1 HTTP Proxy Server Unauthorized Protocol Access Vulnerability
2002-03-08: Check Point FW-1 SecuClient/SecuRemote Client Design Vulnerability
2001-09-19: Check Point Firewall-1 GUI Log Viewer Vulnerability
2001-09-10: Check Point Firewall-1 GUI Client Log Viewer Symbolic Link Vulnerability
2001-09-06: Check Point Firewall-1 Policyname Temporary File Creation Vulnerability
2001-07-18: Check Point Firewall-1 SecureRemote Network Information Leak Vulnerability
2001-07-12: Check Point Firewall-1/VPN-1 Management Station Format String Vulnerability
2001-01-23: Check Point Firewall-1 4.1 Denial of Service Vulnerability
2000-08-15: Check Point Firewall-1 Session Agent Dictionary Attack Vulnerability
2000-08-02: Check Point Firewall-1 Unauthorized RSH/REXEC Connection Vulnerability
2000-07-05: Check Point Firewall-1 Spoofed Source Denial of Service Vulnerability
2000-06-30: Check Point Firewall-1 SMTP Resource Exhaustion Vulnerability
2000-06-06: Check Point Firewall-1 Fragmented Packets DoS Vulnerability
2000-03-11: Check Point Firewall-1 Internal Address Leakage Vulnerability

As we can see, there are a number of vulnerabilities listed above that we could attempt to exploit. A quick review of these vulnerabilities didn't reveal any exploits that could be easily taken advantage of in this particular case. We continue our search by going to http://packetstorm.linuxsecurity.com and do another search for Checkpoint FW-1 SP6. The search revealed the following:

1) 0002-exploits/ftp-ozone.c.txt Exploit for recent FW-1 FTP problems - Demonstrate a basic layer violation in "stateful" firewall inspection of application data (ftp within IP packets). Checkpoint alert about this vulnerability here. Homepage here. By Dug Song

2) 0002-exploits/fw-13.htm Checkpoint-1 and other firewall vulnerability - The low-down of it is fooling a firewall into opening "a TCP port of your choice" against an FTP server. Or, if you're running an evil FTP server, having it open ports against clients accessing the server. Homepage here.

3) UNIX/firewall/firewall-1/fwlogsum-0.2.tar.gz fwlogsum summarizes and maintains a set of HTML reports, based on user-specified reports and Checkpoint FW-1 log entries. A few default reports are included, but users are invited to customize and create their own. Homepage: http://fwlogsum.sourceforge.net/ . By Rui Bernardino

4) 0007-exploits/cpd.c CheckPoint IP firewall crashes when it detects packets coming from a different MAC with the same IP address as itself. We simply send a few spoofed UDP packets to it. By Antipent

5) UNIX/firewall/firewall-1/fwsa.sh Fwsa.sh is a tool to penetration test Checkpoint Firewall-1 remotely which implements the recently published holes in session authentication. It attempts to recover user passwords, execute dos attacks, and brute force the firewall management password. Homepage: http://c3rb3r[at]hotmail.com.mailto:Gregory Duchemin

6) advisories/misc/checkpoint.ike.txt Checkpoint Firewall-1 SecuRemote IKE usernames can be guessed or sniffed using IKE exchange and can be guessed separately from the password. Firewall-1 versions 4.0 SP 7, 4.1 SP2, 4.1 SP6, NG Base, NG FP1 and NG FP2 allow username guessing using IKE aggressive mode. Homepage: http://www.nta-monitor.com. By Roy Hills

7) advisories/misc/checkpoint-fw1-proxy-auth.txt The Check Point VPN-1/FireWall-1 4.1 and NG HTTP Security Server (in.ahttpd) can be used to proxy all kinds of different protocols. Since it is not possible to select the allowed protocols, this is considered a security risk. By Mark van Gelder

Again, listed above are several vulnerabilities. As before we review each of the listed vulnerabilities and determine if they are applicable. In this case, the "Checkpoint Firewall-1 Internet Key Exchange (IKE)" bug seems like a good candidate to try and exploit. The version of Checkpoint that Craig is running is susceptible to this particular vulnerability. Also, from what little we were able to gather about Craig's VPN implementation, there is a good probability that we will have success with this exploit.

Understanding the Vulnerability

Now that we have chosen a vulnerability to exploit, we need to gather additional information regarding the details of this particular vulnerability. A detailed description of this vulnerability can be viewed at http://packetstormsecurity.nl/advisories/misc/checkpoint.ike.txt. and at http://www.securitytracker.com/alerts/2002/Sep/1005173.html

This vulnerability allows an attacker to determine whether or not a SecuRemote username is valid or not. SecuRemote is Checkpoint's VPN client that allows VPN connectivity to a Checkpoint VPN firewall. There are actually two different vulnerabilities described in the above articles. Both vulnerabilities are related to a problem with the implementation of the IPSec Internet Key Exchange (IKE) in Checkpoint. The vulnerability allows for the following exploits:

1. A remote user can query the system to determine valid usernames through a dictionary type attack.
2. A remote user that can sniff the network may be able to capture usernames during the IKE transaction.

To take advantage of this vulnerability, Checkpoint's "IKE Aggressive Mode" feature must be used. According to the testing that NTA Monitor (http://www.nta-monitor.com/news/checkpoint.htm) has done, they were able to perform 10,000 username guesses in 2 minutes and 30 seconds. According to their test results, the maximum guessing rate was primarily limited by the firewalls CPU resources rather than by the Internet speed. This means that companies with high performance firewalls are at an increased risk of attach since dictionary type of attack will be able to run that much faster. Checkpoint's response to the announcement of this vulnerability was that the flaw wasn't with their implementation of IKE but rather that there is flaw with the actual IKE protocol itself. Checkpoint recommends that for customers that must use "IKE Aggressive Mode", they use certificates instead of username for authentication.

In our case, we plan to take advantage of this vulnerability to perform a dictionary type attack against the firewall. We chose this attack since we can easily perform this attack from any remote station. The "sniffing" attack requires that we get an account with the same ISP that Craig is using and therefore it is not as appealing.

Attacking the Firewall

Now that we understand the details of the vulnerability, we can move forward to attacking the firewall. The details regarding the implementation of Craig's VPN are sketchy so there is no guarantee that this attack will work. However, we won't know until we try.

In order to attack the firewall, we need the ability to craft an IKE Phase-1 aggressive mode packet with the following payloads:

1. ISAKMP Header
2. SA – Containing one proposal with four transforms:
    a. 3DES encryption, SHA1 hash, Shared Secret Auth, DH group 2, Lifetime 86400 seconds
    b. 3DES encryption, MD5 hash, Shared Secret Auth, DH group 2, Lifetime 86400 seconds
    c. DES encryption, SHA1 hash, Shared Secret Auth, DH group 2, Lifetime 86400 seconds
    d. DES encryption, SHA1 hash, Shared Secret Auth, DH group 2, Lifetime 86400 seconds
3. Key Exchange – DH Group 2
4. Nonce
5. Identification – Type ID_User_FWDN (ie SecuRemote username guess)

Upon receiving the crafted packet, the firewall with reply with and IKE notification message indicating whether or not the username is valid. Also, with some versions of Checkpoint, the responses may contain the following additional information:

1. "User XXXX unknown" – User does not exist
2. "User XXXX cannot use IKE" – User exists but does not use IKE. May use FWZ or plain authentication
3. "Login expired on DDMMYYYY" – User exists but the account has expired
4. "IKE not properly defined for user XXXX" – User exists but IKE is not properly configured

Fortunately for us, a utility for crafting these packets has already been built by Roy Hills. After scouring the Internet, we were able to get a copy of **FW1-IKE-UserGuess.** This is a command line utility written in C that can be run a Linux system. Below is a summary of the options available with this command:

```
>fw1-ike-userguess --help
Usage: fw1-ike-userguess [options] <hostname>

<hostname> is name or IP address of Firewall.

Options:

--file=<fn> or -f <fn>  Read usernames from file <fn>, one per line.
--help or -h            Display this help message and exit.
--id=<id> or -i <id>    Use string <id> as SecuRemote username.
--sport=<p> or -s <p>   Set UDP source port to <p>.  Default 500.  0=random.
--dport=<p> or -d <p>   Set UDP dest. port to <p>.  Default 500.
--timeout=<n> or -t <n> Set timeout to <n> ms.  Default 2000.
--random=<n> or -r <n>  Set random seed to <n>.  Default is based on time
                         Used to generate key exchange and nonce data.
--version or -V         Display program version and exit.
--idtype=n or -y n      Use identification type <n>.  Default 3
(ID_USER_FQDN)
                         For Checkpoint SecuRemote VPN, this must be set to
3.
--dhgroup=n or -g n     Use Diffie Hellman Group <n>.  Default 2
                         Acceptable values are 1,2 and 5 (MODP only).

fw1-ike-userguess version 1.2 2002-08-30 <Roy.Hills@nta-monitor.com>
```

After downloading the utility to our laptop we run a few tests on a test firewall that we have built to make sure that we understand how it works. Realizing that our dictionary attack will probably generate significant log activity, we plan to launch our attack on Friday evening. It is unlikely that anyone will be monitoring the firewall logs over the weekend and that should provide ample time to launch a dictionary attack against the firewall. So that the attack cannot be easily traced back to us, we will launch our attack from a local Internet café that provides wireless connectivity.

With a Double Mocha Espresso in hand, we start our attack. A sample of the results obtained is as follows:

```
Script started on Fri May 2 22:01:30 2003
>fw1-ike-userguess --file=username-dict.txt --sport=0 1.100.215.1
apple     User apple unknown
ball      User ball unknown
marry     USER EXISTS
joe       User joe unknown
.
.
dog       User dog unknown
jack      Login expired 20-Mar-2003

Script done on Thu Aug 22 15:15:50 2002
```

A total of 4 active usernames were detected during the 39 minute dictionary attack. Not wanting to push our luck for this evening, we head home with the information we gleaned from the attack and will try another day to exploit the accounts. The next day, while reviewing Craig's network layout we realize that we missed one critical component of the infrastructure that will more than like render the information we gather from the attack useless. Craig has chosen to use RSA SecureID tokens to enforce strong authentication for his VPN users Therefore, launching a dictionary password attack using the accounts we learned of during the previous day's attack will more than likely not yield any positive results as it will be almost impossible to guess the password. Oh well, back to the drawing board.

Denial of Service Attack

In this attack we have compromised 50 cable/DSL systems and will use these systems to launch a denial of service attack against this network. We have opted to launch a TCP SYN Flood attack against the organization's external web server using Tribal Flood Network 2000. Tribal Flood Network 2000 (TFN2K) is a complex DDoS tool that can control any number of "agents" which are used to launch the actual attack. TFN can be used to generate multiple types of attacks and it can generate packets with spoofed source IP addresses. In our case, we will be using TFN2K to launch a SYN Flood attack against port 80 and 443 on the web server.

To initiate the attack we use the TFN2K "master" program to instruct our 50 compromised TFN2K Agents to attack the web server by sending SYN packets to port 80 and 443. The master program communicates with the agents using ICMP echo reply packets. The attack instructions (destination IP address, ports, attack pattern, etc) are embedded in the 16-bit ID field. When instructed, the agents will send a flood of SYN packets as if to initiate a normal three way handshake. However, the source IP addresses in these SYN packets are non existent IP addresses. Therefore, the SYN/ACK packet that is returned by the server will never actually get to a system. The server will continue to queue up the SYN

requests as it waits to receive the ACK response. Eventually the SYN request will time out but if we send SYN packets fast enough, the SYN requests will continue to take up resources on the machine until such a point that it severely affects the performance of the server.

Preparing the TFN2K Attack

There are three components that we will need to launch this attach. They are:

1. Master – a host to run the client software
2. Agents – hosts to run the daemon software
3. Target – a victim to run the attack against

We already know our target so can move forward with locating our Master. We will use our laptop as the Master but will launch the attack from the same Internet café that we used to launch the original attack against the firewall. This way if Craig is able to trace back the master, all he would get is the temporary address of the ISP we are using.

The next step is to build the install kit that we can use to create the agents. We download a copy of TFN2K from http://packetstorm.nl. In this case we are going to compile the kit for the Windows platform as we feel that there are many more exploitable Windows hosts to choose from. When compiling, we are prompted for a server password since we have enabled the REQUIRE_PASS option. Next we create a small program (ph.exe – "phonehome") that will be used to send an email to one of our Hotmail accounts with IP address of a client that has been compromised. This way we will be able to easily build up our list of compromised systems that will act as our agents. Finally we create an installation routine (setup.exe) that will be used to install both the above components and then zip everything into a single zip file. We name the zip file, freegame.zip and make it available on several P2P networks. We also download a webcrawler and use it to scour the Internet for email addresses. We then compose a "Spam" email claiming that the attachment can be used to protect your system against Spam. We rename our install kit to "SpamStopper.zip", attach it to the email and send it out using an improperly secured SMTP server that allows us to use it as a mail relay. We monitor our hotmail account for activity and as systems become infected, we receive emails with their IP address. After a week we are able to build up a list of 50 viable clients that have been compromised and are in a position to launch the attack.

As a final step, we compile a second copy of the TFN2K client for our Linux (RedHat) system that will act as the TFN2K master.

Launching the Attack

We are now ready to launch our attack. We've created an agents.txt file containing the IP address of our TFG2K agents. We head down to the Internet café and enter in the following command:

```
> tfn –f agents.txt –c5 -1 1.100.215.69 0
```

where:

tfn – tfn2k client application
-f agents.txt – use the ip address listed agents.txt as the tfn2k agents
-c5 – indicates to perform a SYN flood attack. Other available options are:
C0 – Status or stop command
C1 - Anti Spoof Level: The DoS attack commenced by the servers will always emanate from spoofed source IP addresses. With this command, you can control which part of the IP address will be spoofed, and which part will contain real bits of the actual IP.

C2 - Change Packet Size: The default ICMP/8, SMURF, and UDP attacks use packets of a minimal size by default. You can increase this size by changing the payload size of each packet in bytes.
C3 - Bind root shell: Starts a one-session server that drops you to a root shell when you connect to the specified port.
C4 - UDP flood attack. This attack can be used to exploit the fact that for every udp packet sent to a closed port, there will be an ICMP unreachable message sent back, multiplying the attacks potential.
C5 - SYN flood attack. This attack steadily sends bogus connection requests. Possible effects include denial of service on one or more targeted ports, filled up TCP connection tables and attack potential multiplication by TCP/RST responses to non-existent hosts.
C6 - ICMP echo reply (ping) attack. This attack sends ping requests from bogus source IPs, to which the victim replies with equally large response packets.
C7 - SMURF attack. Sends out ping requests with the source address of the victim to broadcast amplifiers, hosts that reply with a drastically multiplied bandwidth back to the source.
C8 - MIX attack. This sends UDP, SYN and ICMP packets interchanged on a 1:1:1 relation, which can specifically be hazard to routers and other packet forwarding devices or NIDS and sniffers.
C9 - TARGA3 attack. Uses random packets with IP based protocols and values that are known to be critical or bogus, and can cause some IP stack implementations to crash, fail, or show other undefined behavior.
C10 - Remote command execution. Gives the opportunity of one-way mass executing remote shell commands on the servers.

-1 – indicates that a spoof scan will be performed.
1.100.215.69 – the IP address of the web server
0 – indicates to use a random source port.

After initiating the attack, we monitor the website to see if we are having an affected. After a few minutes, we notice a significant degradation in performance of the website. After 10 minutes, we can no longer get access to the website. It appears that our attack was successful. After letting the attack run for an hour, we stop the attack by issuing the following command:

```
> tfn –f agents.txt –c0
```

We suspect that the Snort sensor in Craig has deployed in front of the firewall has detected the SYN attack. However, since the attack only lasted for an hour, it will be very difficult for him to trace the attack back to our Master TFN2K client. At best he would know the IP addresses of the TFN agents and could set up filters to block them from accessing his network.

Countermeasures

Denial of service attacks are difficult to defend against due to the fact that the attack is coming from multiple sources. Some firewalls can detect and thwart SYN attacks. However, a carefully planned attack can circumvent these built in security features. Also, if the firewall starts to drop SYN requests because it thinks it is under attack, that itself could result in the same denial of service that original SYN attack would have caused (with the exception that the target server would not actually crash).

Here are some steps that can be used to minimize the affects of an attack:

1. Examine the source IP addresses of the attacking systems. If you get lucky and find that the source IP addresses fall into a particular range, you can configure rules on the border router or firewall to filter out the range of IP address.
2. Increase the queue for the connection requests. This will take up more memory on the server but it may allow some legitimate traffic to get through.
3. Contact the ISP's from where the attack appears to be originating from and request that they do some egress filtering to stop SYN floods from originating from their networks.

The best way to prevent these attacks is to ensure that all clients on the Internet are properly protected. This, however, is far from what is actually

Compromising an Internal System

In this final attack, we will attempt to compromise the Lotus Domino web server. A search of http://www.securityfocus.com/cgi-bin/sfonline/vulns.pl revealed the following vulnerabilities:

> 2003-03-26: IBM Lotus Notes and Domino COM Object Control Handler Buffer Overflow Vulnerability
> 2003-03-26: IBM Lotus Domino HTTP Redirect Buffer Overflow Vulnerability
> 2003-03-26: IBM Lotus Domino Web Server HTTP POST Denial Of Service Vulnerability
> 2003-03-26: IBM Lotus Domino Web Server iNotes s_ViewName/Foldername Buffer Overflow Vulnerability

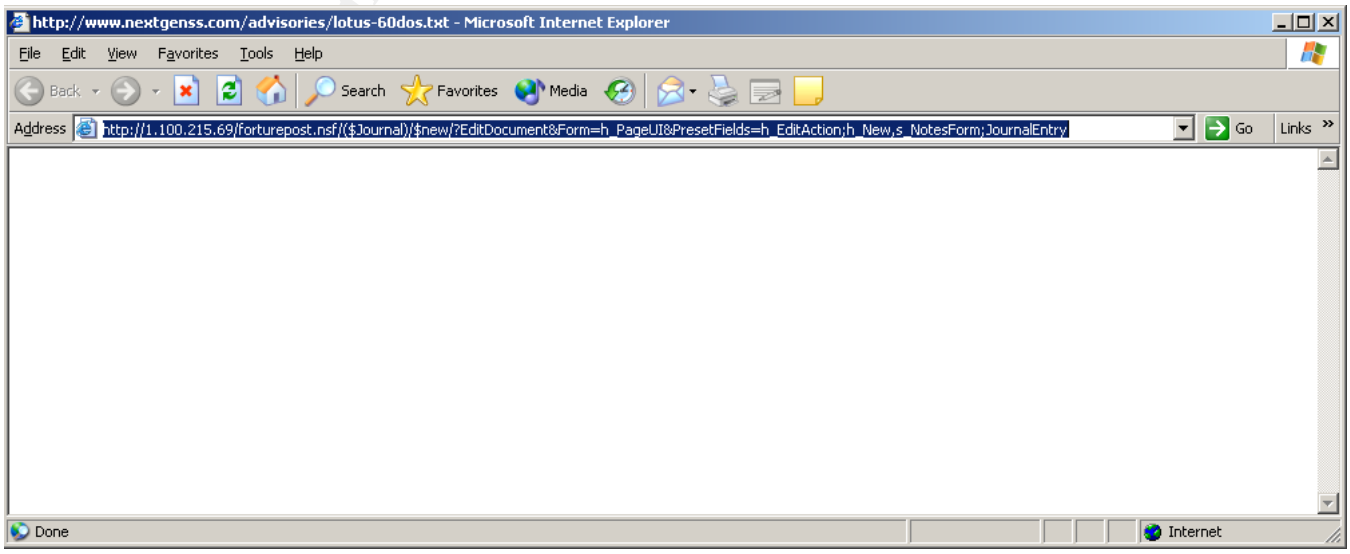
We will attack the Lotus Domino Web server by trying to exploit the HTTP POST Denial Of Service Vulnerability (http://www.securityfocus.com/bid/6951/info). According to information on this webpage, this vulnerability occurs when the web server process a specially malformed HTTP POST request. The specially crafted POST request will cause the Web server to behave in unpredictable fashion and could result in a denial of service condition. As long as Craig hasn't updated or patched his Lotus Domino server, we should have success with this exploit.

No special attack tools or exploit code are required to take advantage of this vulnerability. Simply using a web browser to send the malformed HTTP POST request is sufficient to disrupt the web server. From the research we did, we found that there are two types of condition that will have the affect of bringing down the server:

1. Submitting an incomplete POST request.
2. Submitting Fictionary Value Field POST request

After analyzing the structure of the website, we decide to try our first exploit by trying to issue an incomplete POST request by executing the following statement from our IE browser:

> http://1.100.215.69/fortunepost.nsf/($Journal)/$new/?EditDocument&Form=h_PageUI&PresetFields=h_EditAction;h_New,s_NotesForm;JournalEntry



After issuing the above command, the browser displayed a blank screen. It is unclear if this is the result that we expect to see. We attempt to access the web server to see if it has had any affect. Much to our disappointment, everything is still working. We execute the above statement several more times, each time making a slight modification in the structure of the statement. However, our efforts are not met with any success. We move onward and try to exploit the second type of POST request; a request with a fictionary value field. Again, after analyzing the website, we execute the following statement from the browser:

> http://1.100.215.69/fortunepost.nsf/iNotes/$new/?EditDocument&Form=h_PageUI&PresetFields=h_EditAction;h_New,s_NotesForm;ShimmerMailPref

Again, we check the web server to see if it is still available. Again, nothing seems to have happened. Several more attempts are made to execute variations of the above statement but with no success. We can only conclude that we are either not supplying the correct statement or Craig has updated his Lotus Domino web server to 6.0.1. Since this vulnerability we are trying to exploit is only a few months old, we feel that Craig has probably not gotten around to patching or upgrading his system. We suspect that we are not issuing the correct POST statements and this is why our attack is failing. Since we could not find any additional information on the Internet on how to make this exploit work, we abort our attack.

References

Bennett, Todd. "Auditing Firewalls: A Practical Guide."
URL: http://www.itsecurity.com/papers/p5.htm#II.A (5 April 2003).

Spitzner, Lance. "Auditing Your Firewall Setup." 26 March 2000
URL: http://www.rootprompt.org/article.php3?article=323 (5 April 2003).

Firewall.cx. "Firewall Topologies." URL: http://www.firewall.cx/index.php?c=firewall_topologies (29 March 2003).

Dekker, Marcel. "Security of the Internet." URL: http://www.cert.org/encyc_article/tocencyc.html (29 March 2003).

Tauer, Brad. "Practical Assignment v 1.8." March 2003.
URL: http://www.giac.org/practical/GCFW/Brad_Tauer.pdf (6 April 2003).

Gladsone, Emily. "Practical Assignment 1.6A." 30 April 2002
http://www.giac.org/practical/Emily_Gladstone_GCFW.zip 15 March 2003.

DeokJo, Jeon. "Understand DDOS Attack, Tools and Free Anti-tools with Recommendation." 7 April 2001. URL: http://www.sans.org/rr/threats/understanding_ddos.php (5 April 2003).

Stein, Lincon. "The World Wide Web Security FAQ – Securing against Denial of Service Attacks." 16 October 2002.
URL:http://www.windowsecurity.com/whitepapers/the_world_wide_web_security_faq__securing_against_denial_of_service_attacks.html (4 April 2003).

Cisco Systems Inc. "Conventions Used in Cisco Technical Tips."
URL: http://www.cisco.com/warp/public/459/techtip_conventions.html (15 March 2003).

Cisco Systems Inc. "Subnet Zero and the All-Ones Subnet."
URL: http://www.cisco.com/warp/public/105/40.html (15 March 2003).

Fadia, Ankit. "SYN Flooding Torn Apart." 16 October 2001
URL: http://www.ankitfadia.com/syn.htm (4 April 2003).

Curtin, Matt; Ranum, Marcus. "Internet Firewalls: Frequently Asked Questions." 1 December 2000
URL: http://www.interhack.net/pubs/fwfaq/ (20 March 2003).

Tanase, Mathew. "IP Spoofing: An Introduction." 11 March 2003.
URL: http://www.securityfocus.com/infocus/1674 (29 March 2003).

Keeney, Frank. "Here is my Cisco access list which is configured to prevent outside access." 1998
URL: http://pasadena.net/cisco/secure.html (21 March 2003).
Welch-Abernathy, Dameon D. "PhoneBoy's FireWall-1 FAQ." 23 March 2003.
URL: http://www.phoneboy.com/fom-serve/cache/1.html (25 March 2003).

Hills, Roy. "SecuRemote usernames can be guessed or sniffed using IKE exchange"

URL: http://packetstormsecurity.nl/advisories/misc/checkpoint.ike.txt (1 May 2003).

Litchfield, Mark. “Lotus Domino Denail of Service Attacks 1 & 2” 17 Februaby 2003
URL: http://www.nextgenss.com/advisories/lotus-60dos.txt (3 May 2003)