Global Information Assurance Certification Paper

Level 2: Firewalls, Perimeter Protection and VPN's

Practical Assignment
Version 1.5e

By John Kahanek
Date: August 31, 2001

Table of Contents

1 ASSIGNMENT 1—SECURITY ARCHITECTURE 5

1.1 Assignment Requirements 5

1.2 Architecture Requirements 5

1.3 GIAC Enterprises Network Components 8

2 ASSIGNMENT 2—SECURITY POLICY 10

2.1 Overview of Security Process 10

2.2 Border Router Policies 10
2.2.1 General Router Configs 10
2.2.2 Ingress Filter 12
2.2.3 Egress Filter 14

2.3 Primary Firewall Policies 14

2.4 VPN Policies 17

2.5 Testing the Policy 18

3 ASSIGNMENT 3—AUDIT YOUR SECURITY ARCHITECTURE 19

3.1 Plan the Assessment 19
3.1.1 Memo to the President of GIAC 19
3.1.2 Our Understanding of Your Needs 20
3.1.3 Our Approach to This Project 20
3.1.4 Limitation on Liability 21
3.1.5 Management's Response to the Proposal 22

3.2 Implement the Assessment 22
3.2.1 Speak with Management 22
3.2.2 Border Router Review 23
3.2.2.1 ISS Internet Scanner 23
3.2.2.1.1 Change the policy 23
3.2.2.1.2 Run the Scan 24
3.2.2.2 NMAP Implementation 26
3.2.2.2.1 External Scan 26
3.2.2.2.2 Internal Scan reviewing primary firewall and router review 27

3.3 Recommendations on Improvement 28

4 ASSIGNMENT 4—DESIGN UNDER FIRE 28

4.1 Network to Attack 28

4.2 Attack Against Firewall Itself 29

4.3 Denial of Service Attack 29
4.3.1 Define Scenario 29
4.3.2 Tool used to Initiate Attack 30
4.3.3 The Attack 30
4.3.4 Immediate Countermeasures 31
4.3.5 Other Countermeasures 31

4.4 Attack Methodology to Compromise an Internal System 32
4.4.1 Define Target 32
4.4.2 Casing the Environment 32
4.4.3 Options for Obtaining the Targeted Database 32
4.4.3.1 Option 1 33
4.4.3.1.1 Attack Method and Result 33
4.4.3.1.2 Controls to Mitigate this Risk and Enhance Perimeter Defense 33
4.4.3.2 Option 2 34
4.4.3.2.1 Attack Method and Result 34
4.4.3.2.2 Controls to Mitigate this Risk and Enhance Perimeter Defense 34
4.4.3.3 Option 3—Attack Against the Firewall 34
4.4.3.3.1 Case the Environment before Performing an Exploit 34
4.4.3.3.2 Exploit #1 35
4.4.3.3.2.1 Impact 35
4.4.3.3.2.2 Result 36
4.4.3.3.2.3 Controls to Mitigate this Risk and Enhance Perimeter Defense 36
4.4.3.3.3 Exploit #2 36
4.4.3.3.3.1 Impact 37
4.4.3.3.3.2 Result 37
4.4.3.3.3.3 Controls to Mitigate this Risk and Enhance Perimeter Defense 37
4.4.3.4 Which option should be implemented? 37

Table of Figures

FIGURE 1: GIAC ENTERPRISE'S NETWORK DIAGRAM (PHASE II WITH FAILOVER) 6
FIGURE 2: GIAC ENTERPRISE'S NETWORK DIAGRAM (PHASE I) 7
FIGURE 3: SELECT A POLICY 23
FIGURE 4: EDIT A POLICY IN POLICY EDITOR 24
FIGURE 5: SELECT THE ROUTER OR SWITCH TO SCAN 25
FIGURE 6: AVOID USING EXPLOITS 26

Tables

TABLE 1: TEST RULES WITH NMAP 19
TABLE 2: TASK AND DURATION OF AUDIT FOR INITIAL PROPOSAL 21
TABLE 3: TASK AND DURATION OF AUDIT FOR REVISED PROPOSAL 22

1 Assignment 1—Security Architecture

1.1 Assignment Requirements

Define a security architecture for GIAC Enterprises, a growing Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings, and which has just completed a merger/acquisition. Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component. Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture.
You must consider and define access for:

- Customers (the companies that purchase bulk online fortunes);
- Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);
- Partners (the international partners that translate and resell fortunes).

1.2 Architecture Requirements

The architecture must satisfy confidentiality, integrity and availability requirements. In addition to security other business characteristics are required including reliability, scalability, redundancy, speed, and client value. A secure architecture requires creating a solid outside perimeter with one entry point. Factors affecting the outside perimeter include:

- Configure securely the border routers, internal & external firewalls, switches, proxy servers, split DNS, VPN's, etc.
- Provide security awareness seminars to prevent cases of circumventing the firewall such as social engineering.
- Remove internal modems or disable the auto answer feature. Wardialing will ensure that this is in fact secure.
- Erect solid physical security restricting access of unauthorized individuals who could easily visit at lunchtime with a computer and run scans.
- Ensure offsite backups are indeed stored securely.
- Shred paper media before disposing to provide dumpster divers little information.
- Utilize the appropriate level of encryption and ensure that the key is stored, distributed, and destroyed securely.

The emphasis of this paper may appear to be the first bullet; however, as infosecurity personnel we should not ignore other domains requiring security on the outside perimeter. Paper media, backups, phone calls, and personnel do not pass through a router or firewall, and could just as easily circumvent the firewall to acquire corporate resources as illustrated in "Attack Methodology to Compromise an Internal System" beginning on p. 32.

After attending the senior management meeting for GIAC Enterprises the focus was on the availability, client value, speed, redundancy, and scalability of the system. Security was mentioned briefly, and the topic did receive well-deserved attention with the recessionary trends in the economy. Based on the given requirements, the following network diagram surfaced labeled "Figure 1: GIAC Enterprise's Network Diagram (Phase II with Failover)". However, due to expenses this diagram received heavy criticism and the diagram on p. 7 labeled "Figure 2: GIAC Enterprise's Network Diagram (Phase I)" prevailed until the enterprise proves profitable.

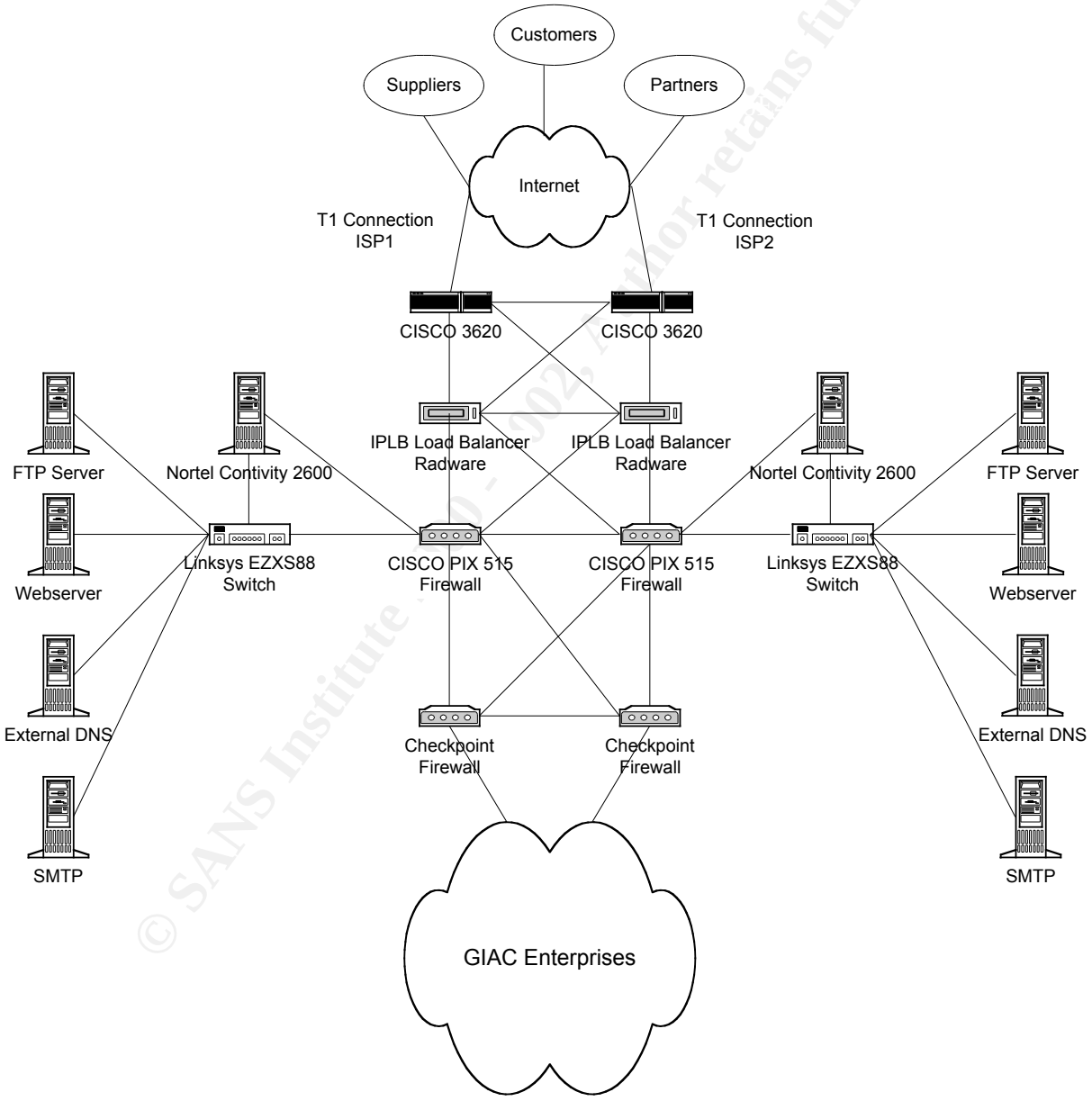


Figure 1: GIAC Enterprise's Network Diagram (Phase II with Failover)

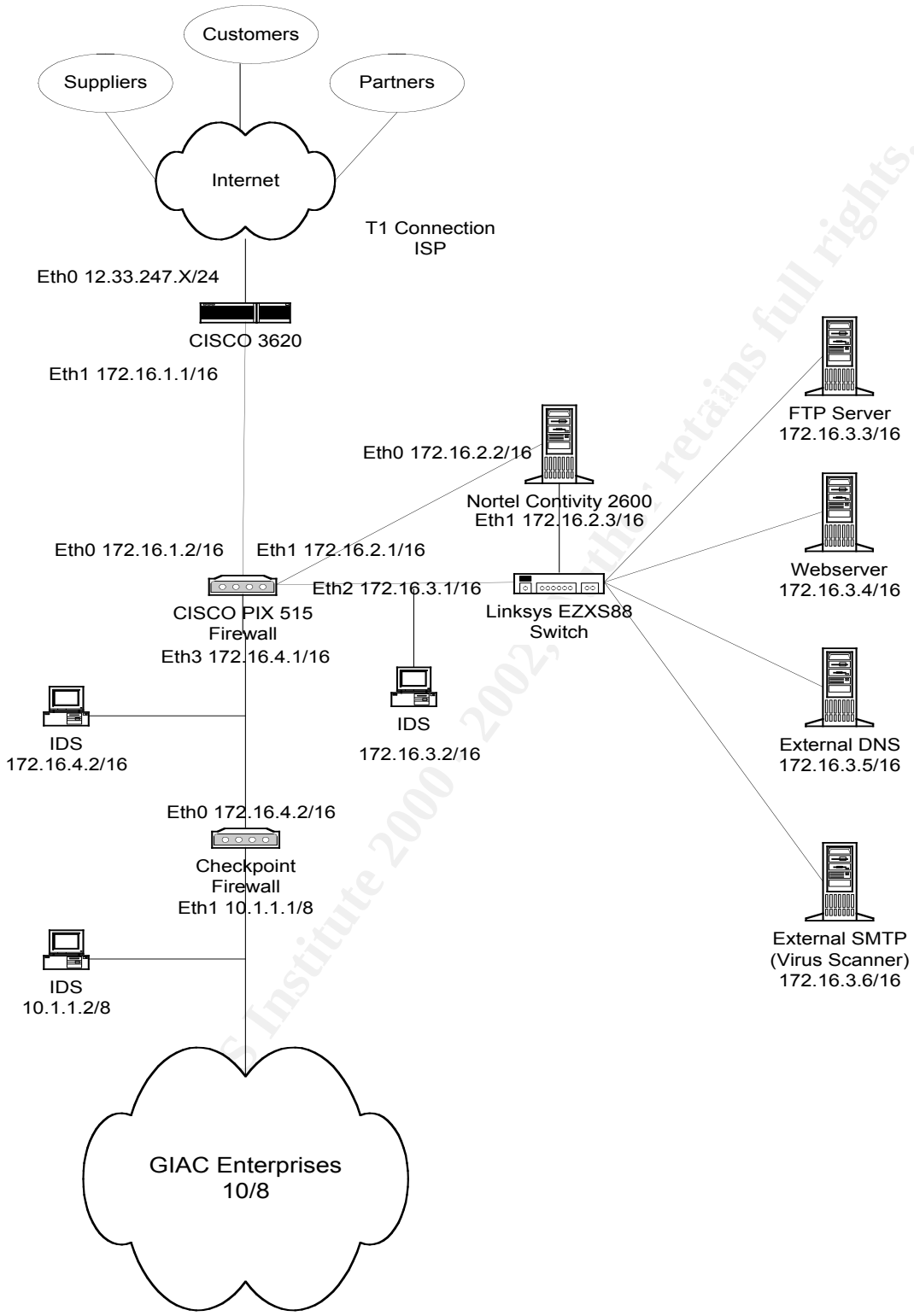


Figure 2: GIAC Enterprise's Network Diagram (Phase I)

1.3 GIAC Enterprises Network Components

The desired network focuses on redundancy and availability removing a single point of failure as listed in Phase II. Aside from hardware configurations with additional processors, drives and memory for each platform, the network diagram for Phase II illustrates that if any one component fails the identical component is prepared to take the load. When management reviewed the costs, they decided that initially Phase I would require less resources until revenues post in the black.

DR may require that another location is required for added availability. In case of a natural disaster, an additional site could provide the necessary support. The same design structure would suffice for the second site and connectivity with the other site would occur through a lease line.

The border routers include a CISCO 3620 connect to an ISP. The border router filters most of the noise alleviating the load on the CISCO PIX Firewalls. Additionally, the router performs a Network Address Translation (NAT) for the routable Internet addresses to nonroutables (RFC 1918). Router configurations are listed in "Border Router Policies**"** on p. 10.

The border routers significantly screen the amount of anomalous traffic, and the CISCO PIX 515 UR firewalls will further filter the traffic based on configurations. The configuration between the firewalls and the router is critical. I have read books that place too much emphasis on the firewall alone. Additionally, I view the outside perimeter as not only firewalls, routers, and VPN's. As mentioned in "Architecture Requirements" on p. 5, the corporate culture must shift through awareness presentations thwarting social engineering attacks, dumpster diving, phreaking, etc. The firewall complements the router, and configurations are defined based on the defined security policy.

The PIX firewall forwards packets to the Nortel Contivity VPN, webserver, external dns, smtp server and ftp server. The Nortel Contivity VPN provides connectivity for the suppliers and partners. Additionally, remote employees access the site through the VPN to access the internal network. Any unencrypted packets are dropped immediately by the VPN. The website, ftp servers, and external dns servers are accessible by the Internet users, primarily customers. However, suppliers, partners, and other Internet viewers may view portions of this site. Business needs of the suppliers and partners are satisfied via Nortel's Contivity.

A split-split DNS implementation is preferred. If funds do not permit then preference leans towards a split DNS as diagramed in "Figure 2: GIAC Enterprise's Network Diagram". The internal DNS is located in GIAC Enterprises' Intranet. The external DNS records are configured to contain only a small zone file, listing Web, Mail and FTP server addresses published to the world. Internal DNS records are configured for only internal networks, so GIAC Enterprise employees only have access to internal records. When internal users look up host names on the Internet, the query is answered by the

internal external DNS server for resolution. Internet users who look up host names in GIAC's domain are answered by external DNS servers that only know about the publicly accessible resources. Employee users are directed to the internal DNS for GIAC intranet queries and to the internal external for Internet-based queries. This setup reduces misdirects for internal employees if the cache is poisoned in the external DNS. Additionally, privately held nonroutable addresses are less likely to be poisoned or worse obtained by an unauthorized party.[1]

The location of the RealSecure IDS devices should be in three places:

- between the CISCO PIX firewall and the Linksys switch
- between CISCO PIX firewall and the CheckPoint firewall and
- between the Checkpoint firewall and GIAC Enterprises internal network.

Other less expensive devices will suffice; however, GIAC Enterprises has already licensed the ISS Suite from ISS to utilize specifically the DBScanner 4.1 and the ISS Internet Scanner 6.1 for internal wellness checks. RealSecure was an add-on in the negotiation process.

The Checkpoint firewall was pushed by management because of name recognition despite a push for Nokia or Gauntlet to provide additional security. Checkpoint is a great product, especially based on ease of use; however, I am concerned about continually hardening Win2000 and maintaining the security CERTs. This firewall provides an additional line of defense for the intranet. If the PIX firewall is compromised because of an exploit specific to the PIX OS, the probability of both firewalls succumbing to the exploit is minimized.

A discussion of the hardening of the applications, databases and operating systems internally in GIAC Enterprises is out of scope; however, this additional line of defense is critical. Additionally, various zones protecting critical assets within GIAC Enterprises is out of scope. The most critical assets should be zoned deep internally with very limited access based on internal firewall and switch or router configuration. Some other key components for the organization are also not listed for simplicity's sake such as a mail server with proxy supporting masquerade so cyber stalking is minimized. These additional network components are important for an organization; however, this paper would creep to a large number of pages quickly possibly losing focus on securing the outside perimeter, with the basics for this practical focusing on the border router, primary firewall, and VPN.

[1] Blass, Steve. "What is Split DNS". 15 Jan 2001. URL: http://www.nwfusion.com/columnists/2001/00288013.html. (22 Aug 2001).

2 Assignment 2—Security Policy

2.1 Overview of Security Process

GIAC's Information Security Program Committee (ISPC) approves all security policies. The committee is responsible for final approval of security baselines for information media including digital, paper, phone, physical, personnel, etc. Standards include vendor controls, various platforms (i.e. UNIX, NT, AS/400, OS390, etc.), firewalls, routers, encryption, and other technologies. Each security baseline must be reviewed and approved by the ISPC consisting of senior management, technical owners, administrators and consultants. Administrators and consultants are engaged for very technical circumstances requiring specialized advice. Any standards, which cannot be implemented, based on a business or technical justification requires that the implementer draft a waiver and forward to the committee for approval. Only the committee can accept or deny the risk representing the organization.

2.2 Border Router Policies

The router ACL rules will take the following order: 1) specific denies, 2) general allows, and 3) deny rest.

Ideally, logging should occur at the router but the "show proc CPU" may reveal that the CPU is heavily affected when logging occurs. To reduce the strain on the router, balancing more logging features between the RealSecure IDS devices and primary firewall should assist. However, GIAC will use logs as often as possible until a resource constraint occurs. Another tip to increasing the performance of the router is to place the ACL's on the outbound side of the router instead of the inbound. Also, consider using a standard access list rather than extended if i.e. "eq" won't be utilized because of use at firewall.

2.2.1 General Router Configs

View Cisco IOS v12 commands at http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/rbkixol.htm#xtocid267960. Cisco has also written a paper titled "CISCO—Improving Security on CISCO Routers", which assisted greatly. Additionally, SANS material from Rocky Mountain SANS aided.

A tip before beginning is to avoid using "service password—encryption" with the enable password command, because the algorithm is proprietary and is a simple Vigenere, easily cracked by L0PHT's palm Cisco router cracker. Use the "enable secret" feature instead, which utilizes MD5 for password hashing, which has passed more cryptographic review.

Another tip is to not use http for management, which is a clear text transfer. Use SSH.

!

```
!  Enable encrypted passwords for the router using MD5 algorithm and avoid
!  “enable password” command using CISCO proprietary algorithm.
!
enable secret
!
!  This first warning banner, motd (message of the day) banner, prompts first.
!
banner motd d You are entering an authorized area!!!! d
!
!  The warning banner before a login follows
!
banner login d WARNING: Only authorized access is permitted; all others will be prosecuted.
All activity is logged and monitored d
!
!  Enable TACACS+ (enabled through aaa) instead of TACACS or Extended TACACS.
!  Review a variety of logging features reviewing v12 commands at Cisco (url listed
above).
!
aaa accounting system start-stop tacacs+
aaa accounting network start-stop tacacs+
aaa accounting connection start-stop tacacs+
aaa accounting exec stop-only tacacs+
aaa accounting command 1 stop-only tacacs+
aaa accounting command 15 wait-start tacacs+
!
!  Logging is forwarded to a syslog server where backups can occur to retain logs up to
!  2 MB and 10 subfiles under screenrter directory
!
logging internal_syslog_server 2000 10 screenrter
!
!  Set your local logging buffer to a minimal size unless mem is available (Use “show
!  memory” to review this.).  Keep setting between 16384 and 262144 bytes.
!
logging buffered 16384
!
!  Enable time stamp log entries based on Greenwich time for forensics analysis.
!
service timestamps log datetime msecs
!
!  All communication with routers should utilize SSH or another option is IPSec
!  or kerberized telnet
!
transport input telnet SSH
!
!  After a period of 5 minutes the exec interpreter command times out.
!
```

```
exec-timeout 5
!
!  Disable fingering services so added information regarding user accounts are
!  inaccessible
!
no service finger
!
!  Time servers are internal and set to Greenwich time to provide ease of use in forensic
!  analysis.  No Internet servers are needed for synchronization.
!
no ntp enable
!
!  This command halts broadcasted traffic
!
no ip directed-broadcast
!
!  All packets with the source route flag set will be denied or dropped.  Helps prevent
! spoofing.
!
no ip source-route
!
!  Small services are disabled by default in IOS v. 12, but earlier versions require this.
!
no services tcp-small-servers
no service udp-small-servers
!
!  Disable routers advertising that they are a router with CDP protocol
!
no cdp running
```

2.2.2 Ingress Filter

```
interface Ethernet 0
        ip address 12.33.247.0 255.255.255.0
        ip access-group 110 out

! Ingress ACL [2]
!
! Specific denies are listed first
!
! Deny loopback, broadcast and 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
```

[2] SANS Institute. "2.2 Firewalls 101: Perimeter Protection with Firewalls". Unknown date. pp. 83-87.

```
access-list 110 deny ip 224.0.0.0 7.255.255.255 any log
!
! Deny private addresses (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 any log
access-list 110 deny ip 10.0.0.0 0.255.255.255 any log
!
! Deny packets without ip address.
!
access-list 110 deny ip host 0.0.0.0 any
!
! Deny all ICMP packets
!
access-list 110 deny icmp any any redirect
!
!Deny inbound packets using source address
!
access-list 110 deny ip 12.33.247.0 0.0.0.255 any log
!
! Block Login Services—log this—shift control to firewall if router processing affected
!
access-list 110 deny tcp any any range ftp telnet log
access-list 110 deny tcp any any range exec lpd log
!
!Sunrpc and nfs—log this—shift control to firewall if router processing affected
!
access-list 110 deny udp any any eq sunrpc log
access-list 110 deny tcp any any eq sunrpc log
access-list 110 deny udp any any eq 2049 log
access-list 110 deny tcp any any eq 2049 log
access-list 110 deny udp any any eq 4045 log
access-list 110 deny tcp any any eq 4045 log
!
! Netbios—log this—shift control to firewall if router processing affected
!
access-list 110 deny udp any any eq 135 log
access-list 110 deny tcp any any eq 135 log
access-list 110 deny udp any any range 137 138 log
access-list 110 deny tcp any any eq 139 log
access-list 110 deny udp any any eq 445 log
access-list 110 deny tcp any any eq 445 log
!
! Xwindows—log this; additionally increase range based on n/w size—shift control to
! firewall if router processing affected
!
```

```
access-list 110 deny tcp any any range 6000 6255 log
!
!General Allows
!
! Perform rest of filtering at firewall
!
access-list 110 permit ip any any
!
!  Implicit deny at the end
```

2.2.3 Egress Filter

For an effective egress filter the following example applies.

```
interface ethernet 1
ip address 172.16.1.0 255.255.255.0
ip access-group 120 out


!  Egress ACL[3]
!
access-list 120 permit ip 172.16.1.0 0.0.0.255
any access-list 120 deny ip any any log
```

I log this because I would like to know when my site is used for a potential DDOS.

2.3 Primary Firewall Policies

The border router focused on specific denies and then a general allow. The primary firewall will drop everything unless a business justified reason for accessing the network exist. In other words, the firewall focuses on specific allows and then a general deny.

View PIX 6.0 commands at
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_60/config/commands.htm
for additional clarification.

The following connections should be allowed at a minimum:

- HTTP (80) traffic to the web servers
- HTTPS (443) traffic to the web servers
- Port 514 UDP traffic from the router to the Syslog server
- FTP (21) traffic from the Internet to the FTP server
- DNS (53) to external DNS

[3] SANS Institute. "CISCO Anti-Spoof Egress Filtering". 15 Jan 2001. URL: http://www.nwfusion.com/columnists/2001/00288013.html. (22 Aug 2001).

- SMTP (25) traffic to the mail server from the Internet
- Port 500 UDP traffic for VPN key negotiation.
- SSH (22) TCP traffic to the border router and other devices for secure remote login.

```
!  PIX Version 6.0(1)
!Enable a password
enable password {password}
! Enter the host name and domain name for the firewall but do not name it after the
firewall
hostname 1XF
domain-name 1xf.giac.com
!  Assign the security levels to the interfaces.
nameif ethernet0 outside security0
nameif ethernet1 VPN security60
nameif ethernet2 web security20
nameif ethernet3 inside security100
! Identify speed & duplex mode.
interface ethernet0 100basetx
interface ethernet1 100basetx
interface ethernet2 100basetx
interface ethernet3 100basetx
! Assign Maximum Transmission Units
mtu outside 1500
mtu inside 1500
mtu VPN 1500
mtu web 1500
! Assign addresses to interfaces.
ip address outside 172.16.1.2  255.255.0.0
ip address inside 172.16.4.1  255.255.0.0
ip address VPN 172.16.2.1  255.255.0.0
ip address web 172.16.3.1  255.255.0.0
! Enable an adaptive security algorithm for selected application protocols.  "'Strict' for ftp
! prevents web browsers from sending embedded commands in FTP requests. Each
! FTP command must be acknowledged before a new command is allowed.
Connections
!  sending embedded commands are dropped." [4]
fixup protocol ftp strict 21
fixup protocol http 80
fixup protocol https 443
fixup protocol smtp 25
```

[4] CISCO. "Command Reference". Unknown Date. URL: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/commands.pdf. (2 Sept 2001).

```
! Disable failover feature but it will be enabled if phase II of Architecture implemented.
no failover
! Enable Flood Defender will reclaim PIX firewall resources if user authentication
! subsystem run out of resources reclaiming in the follow order:  1) Timewait 2) FIN wait
! 3) Embryonic, and 4) Idle
floodguard enable
! Disable RIP (Routing Information Protocol) enabled by default. Dynamic routing
!  has some security issues.
no rip inside passive
no rip inside default
no rip outside passive
no rip outside default
no rip VPN passive
no rip VPN default
no rip web passive
no rip web default
! Set the outside default route to the border router
route outside 0.0.0.0 0.0.0.0.0 172.16.1.1 1
! The IP address of the security administrator computer and syslog.
Name secadm 10.10.2.6
Name syslog 10.10.2.6
! Enable logging
logging on
logging timestamps
logging console critical
logging trap notifications
logging host inside logserver
! Allow SSH access from the security administrator's computer and timeout after 5
!  minutes of inactivity
ssh secadm 255.0.0.0 inside
! Define for outside access list according to policy and deny everything else.
access-list acl_out permit tcp any host 172.16.3.4 eq http
access-list acl_out permit tcp any host 172.16.3.4 eq https
access-list acl_out permit udp host 172.16.1.1 host syslog eq 514
access-list acl_out permit tcp any host 172.16.3.3 eq ftp
access-list acl_out permit tcp any host 172.16.3.5 eq 53
access-list acl_out permit tcp any host 172.16.3.6 smtp
access-list acl_out permit udp any host 172.16.2.2 eq 500
access-list acl_out deny ip any any
!Apply acl_out access list to outside interface
access-group acl_out in interface outside
! Define an inside access list according to policy and deny everything else.
access-list acl-in permit ip 172.16.4.2 any
access-list acl-in deny any any
!Apply acl_in access list to inside interface
access-group acl_in in interface inside
```

```
! Define a vpn access list according to policy and deny everything else.
access-list acl-vpn permit tcp 172.16.2.2 any
access-list acl-vpn deny any any
!Apply acl_vpn access list to vpn interface
access-group acl_vpn in interface vpn
! Define a web access list according to policy and deny everything else.
access-list acl-web permit tcp 172.16.3.0 255.255.255.0 any
access-list acl-web deny any any
!Apply acl_web access list to web interface
access-group acl_web in interface web
```

2.4 VPN Policies

The Nortel Contivity 2600 will handle 1,000 tunnels. [5] A layer 3 protocol utilizing IPSec is preferred over a layer 2 protocol using PPTP and L2TP because a tunnel for layer 2 requires maintenance including creation, maintaining and termination.

RFC 1827 elaborates on ESP (Encapsulating Security Payload) and AH (Authentication Header) used in IPSec. IPSec should not be confused with IP v6. IP v6 focuses on the addressing scheme and increasing it; this will potentially replace IP v4. IPSec, focuses on added security, which can be used with IP v4 or IP v6. With IPSec one must choose between ESP and AH. ESP provides added integrity and confidentiality for IP packets encrypting the TCP header and the data portion of the packet. AH provides nonrepudiation with the correct key setup. Based on this information, I choose to implement IPSec with ESP for added protection of IP packets. As for a key arrangement, ISAKMP will be utilized.

Some issues can occur when using IPSec with ESP tunnel mode through a NAT and "Trouble with a NAT" at http://www.cisco.com/warp/public/759/ipj_3-4/ipj_3-4_nat.html mentions this in detail.

Contivity can use 3 different encryptions including 3DES, DES and RC4. Encryption analysis follows based on John Kahanek's paper on encryption. [6] Comparing the 3 encryption algorithms, 3DES wins by a landslide for having the strongest encryption tested over time. Unfortunately, due to the high number of rounds in the encryption, it is very inefficient compared to the newer encryption standards like AES (Rijndael). However, the 3DES encryption algorithm has withstood the test of time, and algorithms like Rijndael may come into play after more years of testing by the cryptographic community.

[5] Nortel Networks. "Contivity VPN Switches". 03 Feb 2001. URL: http://www.nortelnetworks.com/products/library/collateral/55129.02-03-01.pdf (25 Aug 2001).

[6] Kahanek, John. "Protecting Business Applications with Encryption". 31 Dec 2000. http://www2.csc.com/lef/programs/grants/finalpapers/kahanek_encryption.pdf. (25 Aug 2001). pp. 16-31.

3DES has 168 bit effective key length, a 64 bit block length with 48 rounds of encryption, with the 8X8 S-Boxes designed by the NSA adding significant strength. This algorithm's key is not 192 bits as sometimes marketed because 24 bits is used towards parity. DES has a 56 bit effective key length, a 64 bit block length with 16 rounds of encryption and the 8X8 S-Boxes. This algorithm may eventually be replaced by AES which needs more time to substantiate its level of security in the marketplace. RC4 has 40 bit effective key length and is definitely the weakest among the 3.

Additionally, Split horizon with poisoned reverse will be implemented ending an infinite loop by advertising a metric of 16. "'Split horizon' is a scheme for avoiding problems caused by including routes in updates sent to the gateway from which they were learned. The 'simple split horizon' scheme omits routes learned from one neighbor in updates sent to that neighbor. 'Split horizon with poisoned reverse' includes such routes in updates, but sets their metrics to infinity." [7]

2.5 Testing the Policy

After implementing the policies on the routers, VPN's, and firewalls, testing is required to ensure that each feature has been implemented.

Testing the CISCO Router's egress ACL requires generating packets using i.e. NMAP on an internal device with source address spoofing utilizing any address outside of 172.16.1.0 255.255.255.0

nmap –sS –D 65.1.148.226 172.16.1.1

Testing the ingress filter requires performing a similar test from the outside; however, more requirements must pass. Just test each rule one at a time and determine if the packet(s) are dropped at the router by reviewing router logs.

Test Specific Rule	Nmap
access-list 110 deny ip 127.0.0.0 0.255.255.255 any log	Nmap *–sS –D 127.15.16.285 12.33.247.x*
access-list 110 deny ip 255.0.0.0 0.255.255.255 any log	Nmap *–sS –D 255.224.224.255 12.33.247.x*
access-list 110 deny ip 224.0.0.0 7.255.255.255 any log	Nmap *–sS –D 224.234.28.54 12.33.247.x*
access-list 110 deny ip 192.168.0.0 0.0.255.255 any log	Nmap *–sS –D 192.168.2.2 12.33.247.x*
access-list 110 deny ip 172.16.0.0 0.15.255.255 any log	Nmap *–sS –D 172.16.24.38 12.33.247.x*
access-list 110 deny ip 10.0.0.0 0.255.255.255 any log	Nmap *–sS –D 10.1.1.1 12.33.247.x*

[7] Internet Encyclopedia. "2.2.1. Split Horizon". Unknown Date. http://www.freesoft.org/CIE/RFC/1058/9.htm. (26 Aug 2001).

access-list 110 deny ip host 0.0.0.0 any	Nmap *–sS –D 0.0.0.0 12.33.247.x*
Etc.	

Table 1: Test Rules with NMAP

Before testing a router from the Internet, receive approval from senior management for the activity. Don't trust your immediate manager's approval as final decision, or you could both be out the door.

Sniffers placed after the tested device will provide the best source of information regarding a device's configuration as well as the logs of the tested device. The check and balance that I use requires utilizing the IDS devices and if specific activity, normally blocked by the router, is detected then I know the router's ACL is ineffective.

Testing the PIX and Checkpoint firewall would take a similar approach as the router. I would utilize the IDS devices to determine if traffic produced in the test passes the tested device. Tools to utilize include nmap, other vulnerability scanners (Nessus, ISS Internet Scanner, Cybercops, etc.), and packet generators (Ballista, SPAK, NTO Max, UDP Flood, etc.). The current IDS configuration may require a short-term adjustment to place the IDS in the most optimal location utilizing hubs.

Management should be informed of these testing activities and any testing from the Internet should require senior management written approval. I have seen and heard of circumstances where a manager and the assigned staff are both dismissed due to inappropriate scanning.

3 Assignment 3—Audit Your Security Architecture

3.1 Plan the Assessment

3.1.1 Memo to the President of GIAC

August 26, 2001

Mr. Stephen Northcutt
President of Global Incident Analysis Center

SANS Institute
5401 Westbard Ave. Suite 1501
Bethesda, MD 20816

Dear Stephen:

We appreciate the opportunity to propose on performing an independent evaluation of GIAC's perimeter. As a starting point for the review, we have summarized our understanding of your situation based upon our previous meetings and documentation provided. As indicated during our last meeting, you explained that GIAC has effectively secured its outside perimeter. To ensure an added level of comfort, we will investigate the current level of security for your current outside perimeter and provide suggestions on enhancing your architecture or configurations to further harden your environment. The nature of the projects selected for audit will require varied EDP audit skills ranging from client server platform knowledge to routers, firewalls, and dial-in access. We have included our proposed involvement and level of technical proficiency required for each project within this engagement. To this end, we have organized this letter as follows: Our Understanding of Your Needs, Project Approach, Our Experience & Credentials, Project Staffing, and Fees. This letter will clearly define our methodology in performing the various projects within the overall GIAC engagement.

We are convinced Infosec Solutions has the experience to provide the assistance you require and is dedicated to serving you with the highest level of professional competence and capability. We are enthusiastic about working with you on these critical projects and in cultivating a professional relationship with GIAC that will extend many years into the future.

Regards,
John Kahanek
Infosec Solutions Inc.
www.infosecsolutions.com

3.1.2 Our Understanding of Your Needs

GIAC is seeking an independent outside security assessment of major components within the client server/network environment. As a result of our conversations, GIAC has identified a review of the outside perimeter of most importance to protecting critical assets on the internal network.

3.1.3 Our Approach to This Project

Our high level approach to this project is listed in the attached timeline.

Approach	Duration
Speak with management to determine security policies and procedures.	4 hours
Speak with technical owners to understand the perimeter. This process will include documentation gathering and interpreting (i.e. network diagram)	16 hours
Confirm network diagram with Microsoft Visio 2000 Enterprise Edition.	2 hours
Review border router including performing scans with ISS Internet Scanner and using nmap. We will review IDS logs and screening router log to determine results of the scan. Additionally, we will review the ACL's and procedures around the router.	40 hours

Review PIX firewall. We will review IDS logs and firewall to determine results of the scan. Additionally, we will review the rule set and procedures around the external firewall.	32 hours
Review Firewall-1 firewall. We will review IDS logs and firewall to determine results of the scan. Additionally, we will review the rule set and procedures around the internal firewall. Additionally, the Win2000 operating system will require an assessment utilizing ISS Internet Scanner and a review of CERT update procedures and other hardening according to established security baselines by the GIAC Information Security Committee.	32 hours for firewall review 32 hours for Win2000 review.
Review the IIS web server on an NT4 operating system. Use AppScan to review the IIS web server configurations. Use ISS Internet Scanner to review NT4 vulnerabilities.	32 hours for IIS web server review 32 hours for NT4 review
Perform wardial scan of corporation.	16 hours
Summarizing Report	16 hours
Total hours for engagement	**254 hours**

Table 2: Task and Duration of Audit for Initial Proposal

We understand the importance of this project to GIAC and accordingly, we are prepared to start work on September 17, 2001 and anticipate having a draft of our deliverables to management for review by October 12, 2001. We expect to commit 254 hours over this period, with our professional service fees estimated to be between $38,000 to $41,000, plus out-of-pocket expenses.

3.1.4 Limitation on Liability

Without covering too much legalize, one portion of the assignment requires covering the risks of audit implementation, and this is usually covered in a Limitation of Liability Statement as follows. Notice the number of risks entailed in the following documentation and consider how much risk GIAC management should accept.

Client cooperation for obtaining necessary information is pertinent for project completion on time and on budget. Additionally, any issues should be communicated immediately by both the client personnel and InfosecSolutions personnel to ensure an ontime and ontrack deliverable. Other considerations include an appropriate work environment for InfosecSolutions personnel to perform in, and also access to the appropriate client personnel to expedite retrieval of information.

Before initiating any scripts or automated processes the client has the right to review the developed action plan and scripts to ensure that no issues will occur. All network activities will occur at a time chosen by the client to ensure minimal impact in case of an unusual event to the network. Infosecsolutions does not anticipate an issue to the

network; however, if unusual circumstances occur, Infosecsolutions will not be held liable.

3.1.5 Management's Response to the Proposal

GIAC Management for the time-being is only interested in the review of the primary firewall (PIX) and nothing else. InfosecSolutions convinces GIAC management to also include the screening router. Based on this situation, the negotiations of pricing and specific deliverables begin. Without boring the reader with details regarding negotiations, we should accept that the final decision is to review the primary firewall and the screening router, which will entail the following work.

Approach	Duration
Speak with management to determine security policies and procedures around the screening router and firewall.	2 hours
Review border router including performing scans with ISS Internet Scanner and using nmap. We will review IDS logs and screening router log to determine results of the scan. Additionally, we will review the ACL's and procedures around the router.	40 hours
Review PIX firewall. We will review IDS logs and firewall to determine results of the scan. Additionally, we will review the rule set and procedures around the external firewall.	32 hours
Summarizing Report	12 hours
Total hours for engagement	**86 hours**

Table 3: Task and Duration of Audit for Revised Proposal

With the revised hours discussed between GIAC and InfosecSolutions management, we expect to commit 86 hours over this period, with our professional service fees estimated to be between $13,000 to $14,000, plus out-of-pocket expenses. We are prepared to start work on September 17, 2001 and anticipate having a draft of our deliverables to management for review by September 28, 2001.

3.2 Implement the Assessment

3.2.1 Speak with Management

On September 17th, morning meetings were scheduled between GIAC management and senior consultants. Based on these discussions, very few weaknesses surfaced regarding the router and firewall except that no documented procedures exist. Management primarily touted how great the firewall is. All personnel updating router ACL's and PIX filters have been well certified. The senior consultant requested a print out of the router ACL and the PIX filter policy. Management has asked for the consultant to perform the scans, and then the documentation will be provided. Management also presented a network diagram to assist the consultant (as noted in "Figure 2: GIAC Enterprise's Network Diagram"). A program Cheops was ran by technical staff to assist consultants in verifying the outside perimeter.

3.2.2 Border Router Review

3.2.2.1 ISS Internet Scanner

ISS scans will occur from the internal network. This scan will focus on router vulnerabilities.

3.2.2.1.1 Change the policy

1. Select “Policy” from the top drop down menu.
2. The select “New…” The “New Policy” dialog box is displayed. Click on “Next”.
3. The “Select a Policy” dialog box appears. Select “L3 Router & Switch”. Click on “Next”.

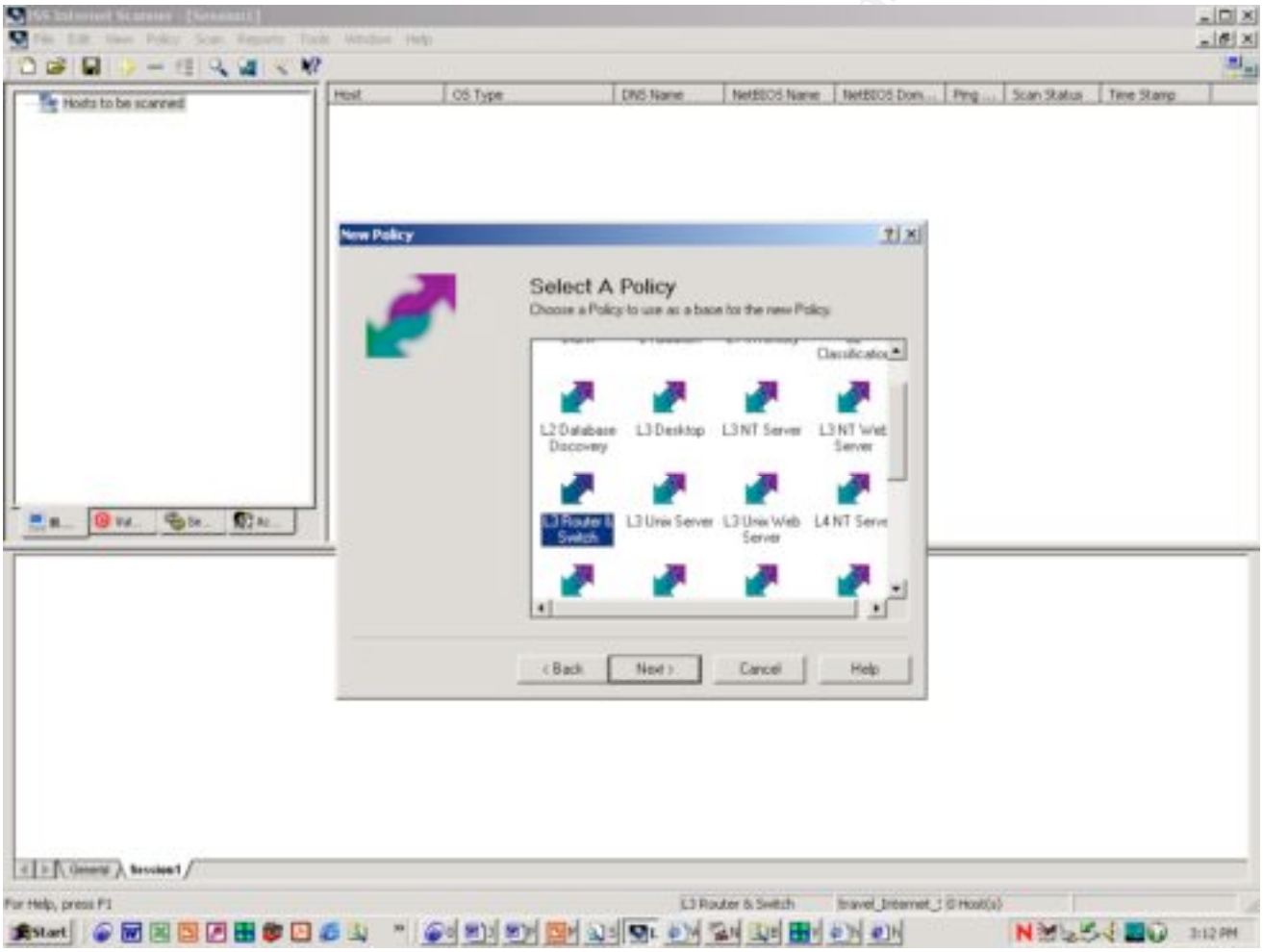


Figure 3: Select a Policy

4. The “Name the New Policy” box appears. Name it based on the new policy parameters like “Router Vulnerabilities for the CISCO 3620”. Click on “Finish”.
5. The “Building a View” dialog box appears for a few seconds. The policy editor should now appear.

6. Expand the “Vulnerabilities” folder in the left windowpane. Expand the “Router/Switch” folder and select all vulnerabilities, which are not already selected.

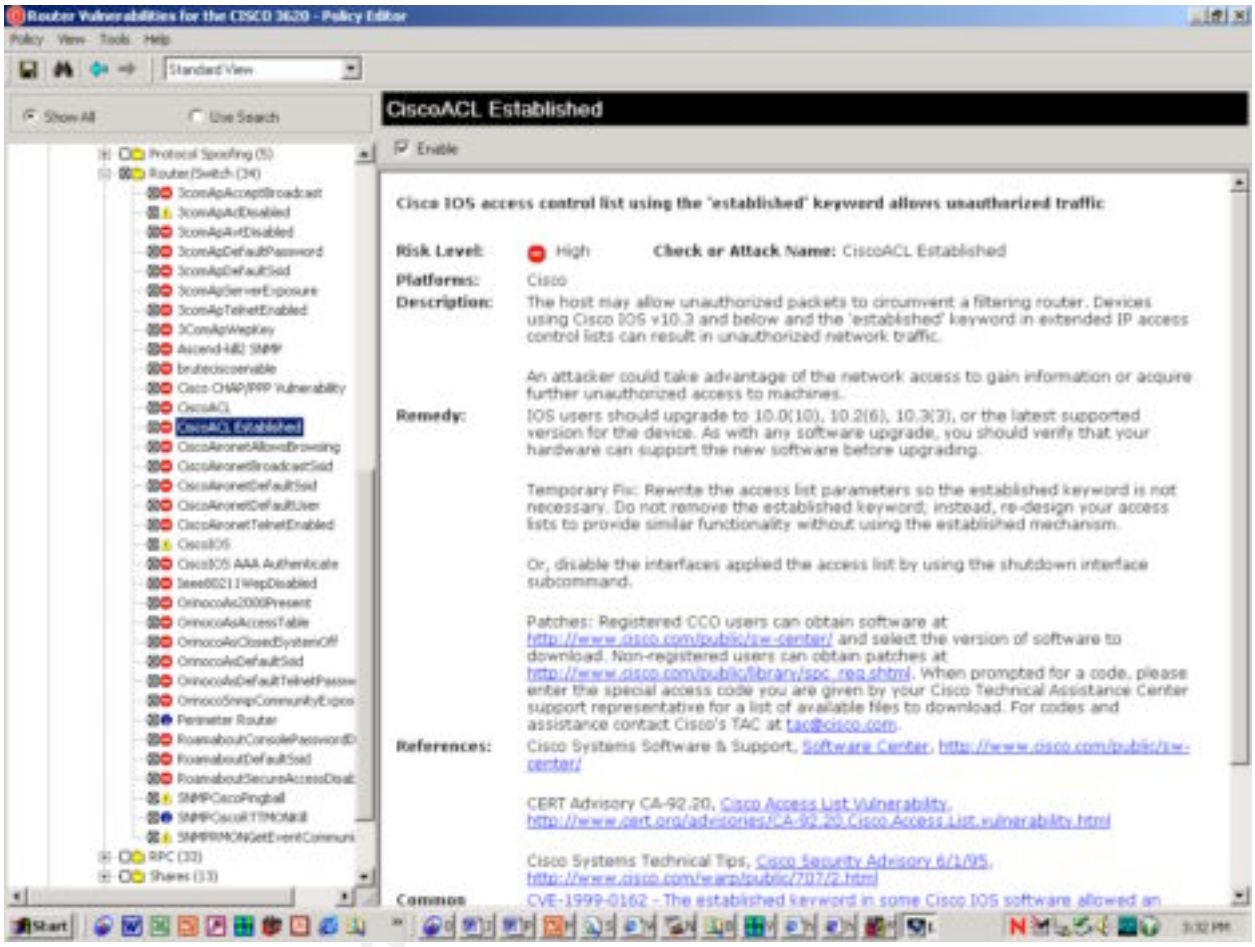


Figure 4: Edit a Policy in Policy Editor

7. Save and close the policy editor.

3.2.2.1.2 Run the Scan

Warning: Do not initiate a scan until GIAC management approves of scans at a specific time. My rule of thumb is 2 hours after business hours. I do this even if I know for a fact that the scan will not affect a production server. Before I initiate a scan in production I follow change control procedures. If a test, development, and/or a QA environment exist, test the scans in this area first to avoid costly mistakes. If scanning UNIX or NT then review logs in syslog or eventviewer for unusual activities that could bring the server down.

The following steps lead to a successful scan after selecting and testing a policy.

1. Select “File” and “New Session…” in the top drop down menu.

2. In the “New Session Wizard-Key Select” dialog box select the appropriate license key, which should be located in c:program files/ISS/Scanner 6 directory. Click on “Next”.
3. The “Select a Policy” dialog box will appear. Select “Router Vulnerabilities for the CISCO 3620”. Click on “Next”.
4. The “Add a Session Comment” dialog box will appear. Type an appropriate comment for the specific scan.
5. The “Specify Hosts” dialog box will appear. Select “Ping valid hosts in your key”.
6. The “Set Host Ping” dialog box will appear. Select a ping range that focuses on your scan and do not ping the entire organization. Select “Edit Range…” Enter the targeted addresses for the scan and select “OK”.

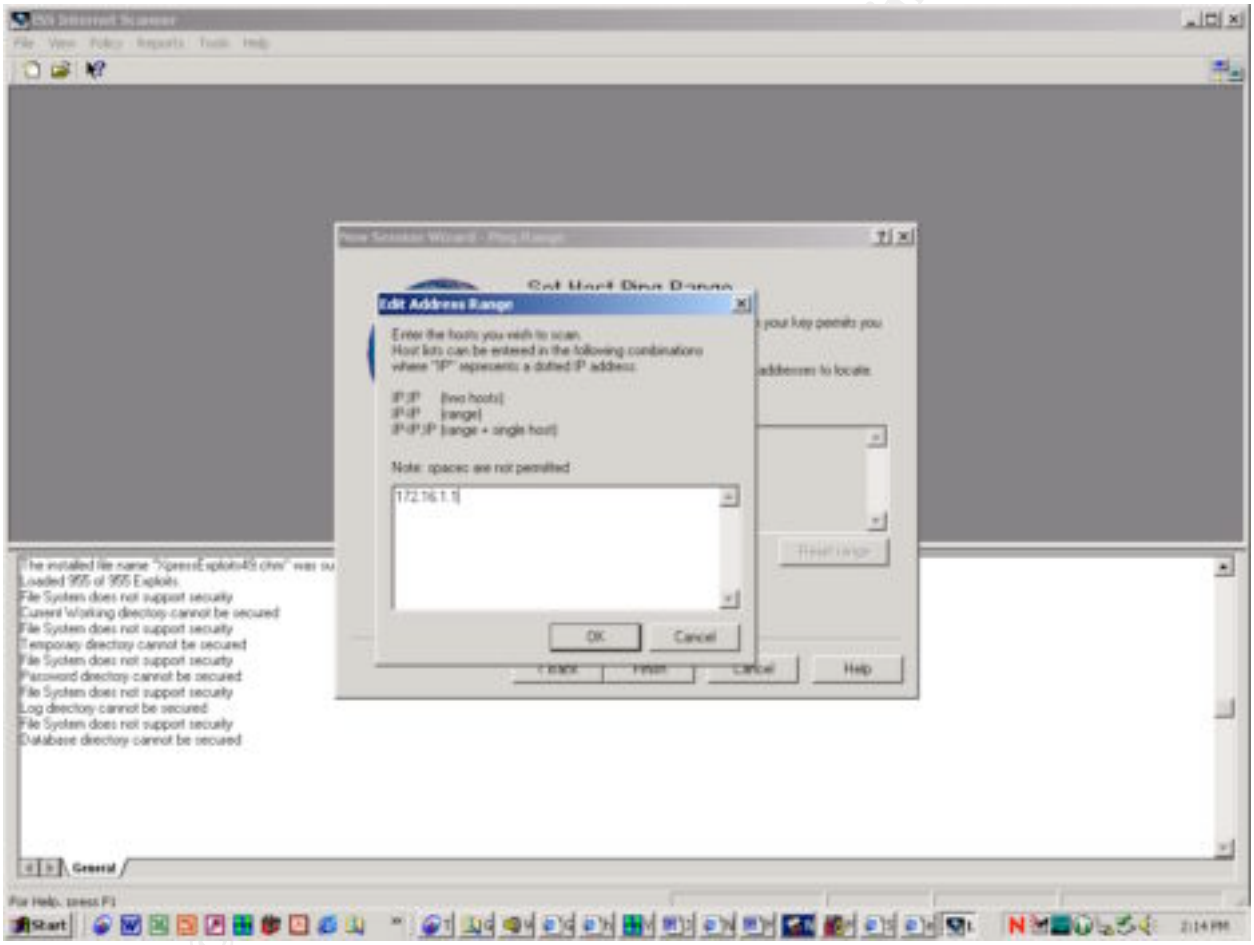


Figure 5: Select the Router or Switch to Scan

7. Select “Scan” from the top drop down menu and then select “Scan Now”. If a “Denial of Service Warning” dialog box appears as displayed in the snapshot on the following page, select “Cancel” and confirm with management if these settings should be ran. Otherwise, be conservative and deselect these items within the dialog box because the targeted system could fail if not appropriately protected by the vulnerability.

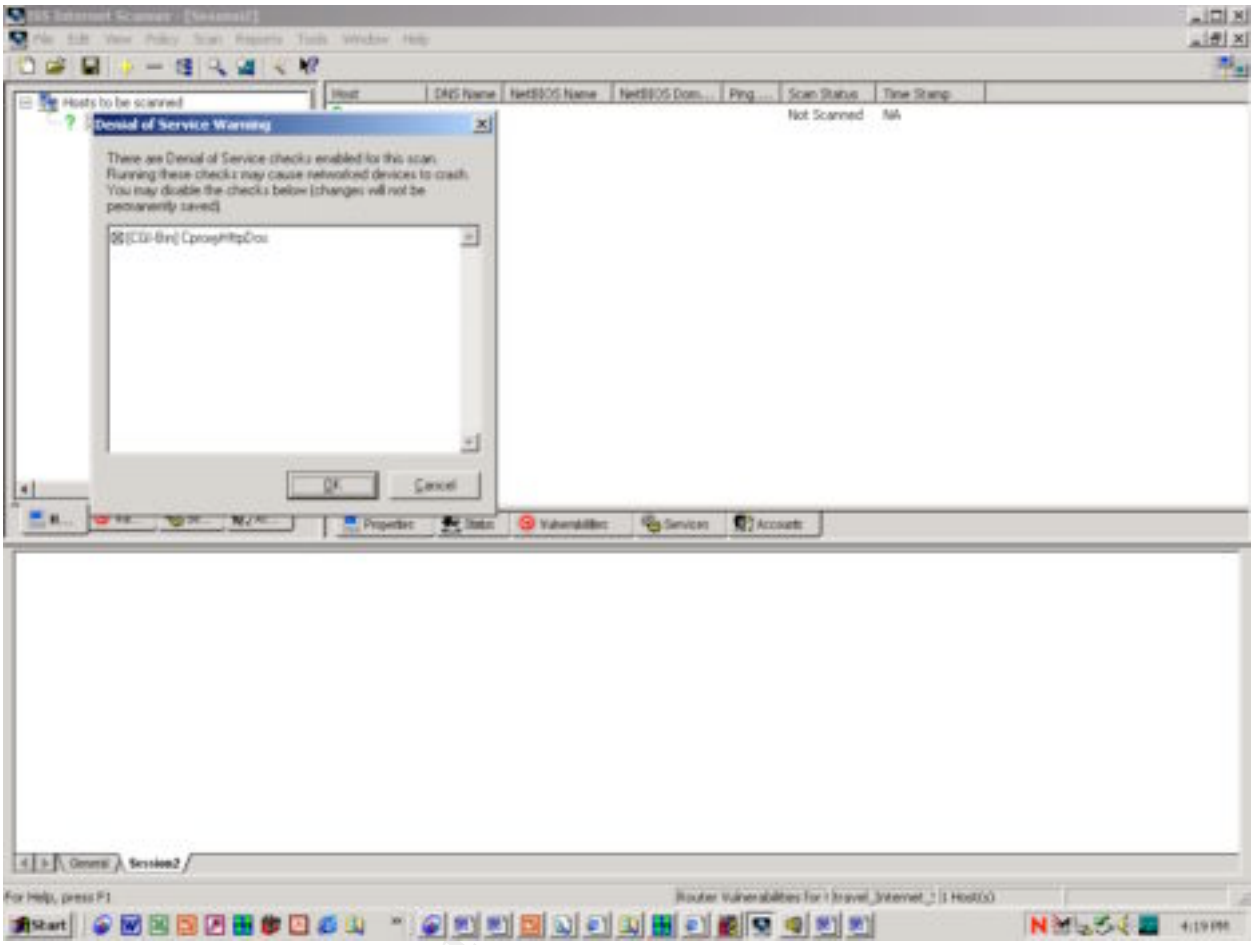


Figure 6: Avoid Using Exploits

Reports generation will not be covered.

3.2.2.2 NMAP Implementation

3.2.2.2.1 External Scan

The external scan utilizing NMAP will audit the router ingress filters and the primary firewall.

Run a stealthy port scan with the following setting. After each scan review the router logs, IDS, and/or primary firewall for results. Additionally, the auditor should nmap for the same issues that you tested earlier.

Test variable or description	Nmap command
This is a stealthy port scan forwarding only syn flagged tcp packets.	nmap -sS 12.33.247.x
This is a stealthy port scan forwarding only fin flagged tcp packets.	nmap -sF 12.33.247.x
This is a stealthy port scan forwarding fin, psh, and urg flagged tcp packets with a sequence number of 0.	nmap -sX 12.33.247.x
This is a stealthy port scan forwarding no flagged tcp packets with a sequence number of 0.	nmap -sN 12.33.247.x
access-list 110 deny ip 127.0.0.0 0.255.255.255 any log	Nmap *–sS –D 127.15.16.285 12.33.247.x*
access-list 110 deny ip 255.0.0.0 0.255.255.255 any log	Nmap *–sS –D 255.224.224.255 12.33.247.x*
access-list 110 deny ip 224.0.0.0 0.255.255.255 any log	Nmap *–sS –D 224.234.28.54 12.33.247.x*
access-list 110 deny ip 192.168.0.0 0.0.255.255 any log	Nmap *–sS –D 192.168.2.2 12.33.247.x*
access-list 110 deny ip 172.16.0.0 0.15.255.255 any log	Nmap *–sS –D 172.16.24.38 12.33.247.x*
access-list 110 deny ip 10.0.0.0 0.255.255.255 any log	Nmap *–sS –D 10.1.1.1 12.33.247.x*
access-list 110 deny ip host 0.0.0.0 any	Nmap *–sS –D 0.0.0.0 12.33.247.x*
Etc.	

3.2.2.2.2 Internal Scan reviewing primary firewall and router review

The internal scan will audit the router egress filters and the firewall egress rule set to ensure that this site's servers are Internet friendly. Do not use a scanner to test the firewall and router internally. If the router and firewall are misconfigured then it is possible that you could inadvertently scan Internet sites unless only the IP address is the target.

Test variable or description	Nmap command
access-list 120 permit ip 172.16.1.0 0.0.0.255 any access-list 120 deny ip any any log	Nmap *–sS –D 10.0.0.1 12.33.247.X*
access-list acl-web permit tcp 172.16.3.0 255.255.255.0 any access-list acl-web deny any any	Nmap *–sS –D 10.0.1.2 12.33.247.X*
etc.	

3.3 Recommendations on Improvement

Based on audit activities the following issues and recommendations were drafted for management review.

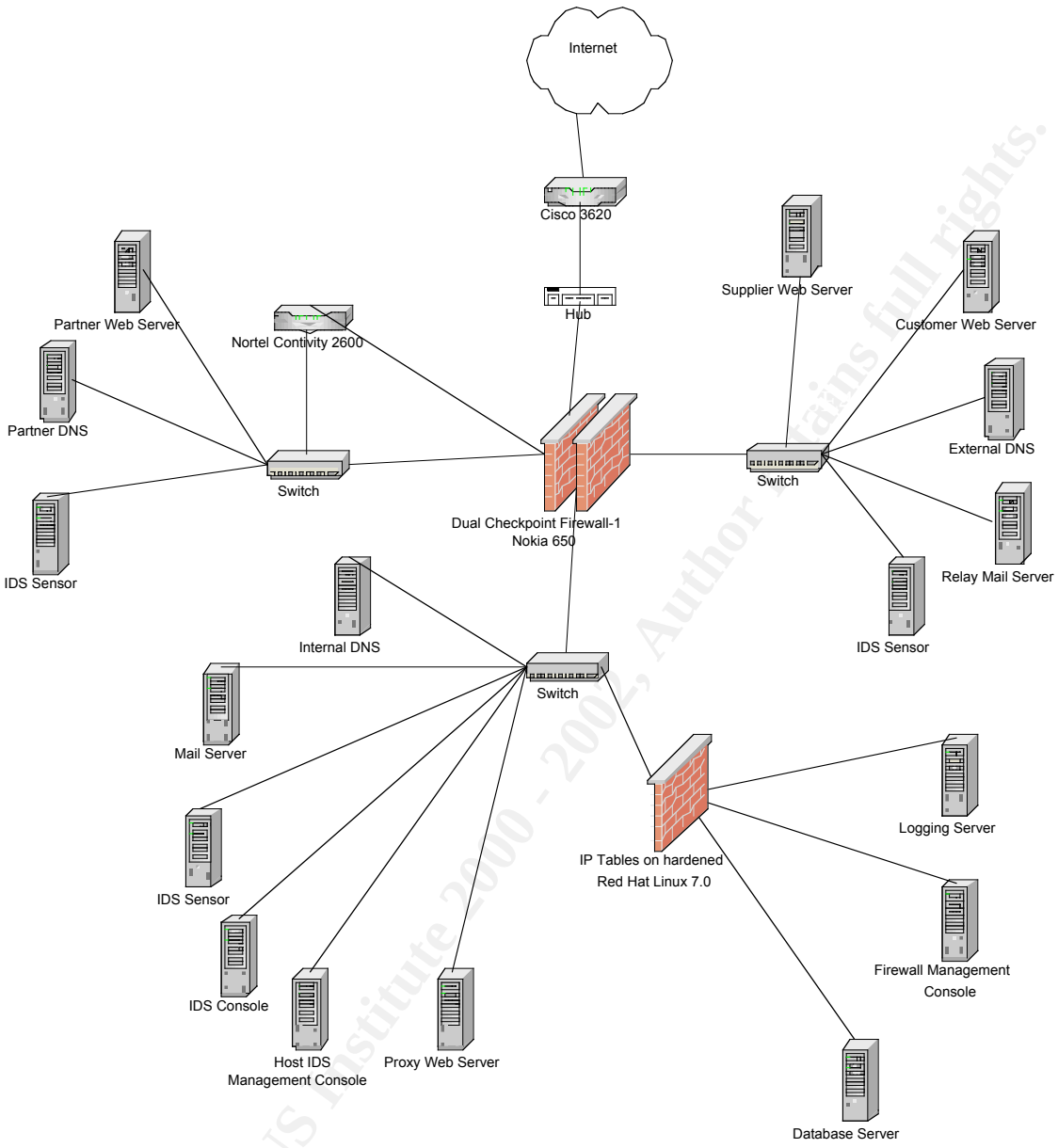
Audit Issue	Recommendation	Task Performed Revealing Vulnerability	Risk Ranking
Some undetected issues were noted in the firewall and router logs.	Review router and firewall logs daily. Develop security incident procedures to expedite security related response initiatives.	Review of router logs.	High
Written procedures have not been drafted.	Document procedures around the outside perimeter devices.	Interviews with personnel	Medium
SSH sessions are not timed out in the PIX firewall due to inactivity	Include “ssh timeout 5” in the firewall ruleset	Review of firewall rules	Medium
NMAP scans detect that users are allowed to use any services to direct at the Internet though the range has been restricted.	Restricting the services and ports available to Internet Users is highly recommended.	NMAP Scan	Medium
If ISS Scanner or other vulnerability scanners detect something then add this here.	Implement the suggested control to mitigate the vulnerability	ISS Internet Scanner	Varies
Etc.			

More issues could have surfaced; however, testing performed earlier reflects the audit points. Management probably wants the auditors to confirm as a third party that the firewall is in fact secure for interested stakeholders to GIAC Corporation. This does not imply that the outside perimeter is actually secure as the “Design Under Fire” section will reflect because hackers think outside of the box and are not restricted by time and resources (to an extent). All audits are constrained by time, money and resources.

4 Assignment 4—Design Under Fire

4.1 Network to Attack

I chose Matthew Brown’s design at http://www.sans.org/giactc/gcfw.htm. Similar tools used to audit a system could be used to attack a system. The only difference between auditors and hackers (actually crackers) are ethics and intent.



4.2 Attack Against Firewall Itself

I included this with the ”4.4.3.3 Option 3—Attack Against the Firewall” on p. 34. The topic ties in better in this section. Please continue with “4.2 Denial of Service Attack”.

4.3 Denial of Service Attack

4.3.1 Define Scenario

“Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.”

4.3.2 Tool used to Initiate Attack

Which tool could a hacker use?

Trinoo would support our need for a UDP flood attack; it will not support a TCP SYN and ICMP flood attack. [8]

"TFN [Tribe Flood Network] supports ICMP flood, UDP flood, SYN flood, and Smurf style attacks, and is controlled via commands sent as ICMP_ECHOREPLY (ICMP Type 0) packets." [9]

Stacheldraht (barbed-wire in German) takes TFN to new levels adding encrypted communication between the attacker machine and the slave machines. Additionally, it uses tcp on port 16660 and ICMP. [10]

After reviewing Trinoo, TFN, tfn2k, Stacheldraht, shaft and mstream, my tool of choice is tfn2k.

TFN2K can attack targets utilizing *TCP/SYN, UDP, ICMP/PING, or BROADCAST PING (SMURF) packet flood. "*All control communications are unidirectional, making TFN2K extremely problematic to detect by active means. Because it uses TCP, UDP, and ICMP packets that are randomized and encrypted, packet filtering and other passive countermeasures become impractical and inefficient. Decoy packets also complicate attempts to track down other agents participating in the denial-of-service network." [11]

This tool can not only perform all 3 floods mentioned in the requirements for this portion of the assignment, but the communication channel is random, encrypted and covert making this my tool of choice.

4.3.3 The Attack

It's 2AM and the pager goes off. In my incoherent state I come to realize that the IDS is reporting that the network is under a severe attack. I stumble to the computer to login through the VPN, but I have absolutely no access. Since no dialup modem has been established based on security policies, which may need reconsideration, I must drive to work to assess damage and gain control of the incident. There have been talks of a 24X7X365 attack analysis guru on site, but the costs and business justification has been difficult to substantiate, and I wish that it had been. When I arrive to the office, I

---

[8] Dittrich, David. "The DoS Project's "trinoo" distributed denial of service attack tool". 21 Oct 1999. URL: http://staff.washington.edu/dittrich/misc/trinoo.analysis (30 Aug 2001).

[9] Dittrich, David. "The "Tribe Flood Network" distributed denial of service attack tool". 21 Oct 1999. URL: http://staff.washington.edu/dittrich/misc/tfn.analysis (30 Aug 2001).

[10] [10] Dittrich, David. "The "stacheldraht" distributed denial of service attack tool". 31 Dec 1999. URL: http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt (30 Aug 2001).

[11] Barlow, Jason and Thrower, Woody. "TFN2K—An Analysis". 10 Feb 2000. URL: http://security.royans.net/info/posts/bugtraq_ddos2.shtml. (30 Aug 2001).

login to the syslog server, centralizing IDS and log results, and I determine that the network is flooded with SYN flagged TCP packets.

4.3.4 Immediate Countermeasures

Based on the attack scenario, I contemplate some countermeasures. First, I contact my ISP so traffic can be filtered at the source, and I also encourage my ISP to contact any second-tier Internet provider that they use to block this traffic as well. This procedure will free up bandwidth.

Blocking each IP on the router will require 50 rules, so I avoid this action because of the amount of added processing taken from the firewall. Reviewing a range of tcp packets utilizing the command "TCP Intercept" on the border router appears to be a more reasonable approach after a more thorough review. "TCP Intercept" will intercept the range of TCP packets from the client to servers. As stated in CISCO documentation, "For each SYN, the software responds on behalf of the server with an ACK and SYN, and waits for an ACK of the SYN from the client. When that ACK is received, the original SYN is sent to the server, and the code then performs a three-way handshake with the server. Then the two half-connections are joined." [12]

However, this solution is just short term because I am loosing bandwidth, and the attacker is still sending packets my way. At least my screening router is dropping the packets in the address range. The new rules significantly degrade processing power on the router requiring that logging is disabled for some rules. Occasionally, I review the activity to review any change of status based on ISP actions.

4.3.5 Other Countermeasures

Some other countermeasures that could assist follow:

- Contact the administrators of the attacking sites and inform them of the attack scenario. This option appears more reasonable with 50 slaves, but what if TFN2K had infected 1000+ nodes. It's a slow process and not as effective in the short term.
- Ensure CEF (CISCO Express Forwarding) switching mode is utilized when available.
- Depending on the attack, it is possible to send return packets (i.e. zombie_zapper program) to shut down the activity without shutting down the other site. Be cautious with this kind of initiative because some slave sites will consider you to be the attacker.
- Review the ingress filter thoroughly to determine if any adjustments would reduce your risk.
- Patch O/S platforms with latest patches or service packs.

[12] CISCO. CISCO IOS v. 12 Commands. Unknown date. URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_r/srprt3/srdenial.htm#3971. (5 SEPT 2001).

4.4 Attack Methodology to Compromise an Internal System

4.4.1 Define Target

GIAC Enterprises has an intense competitor, Anti-GIAC, willing to do anything to obtain information situated on a critical database, labeled "Database Server" in Matthew's diagram. This information is extremely critical as an ongoing concern for the business. Hence, GIAC has spent a lot of time and money to secure the network's outside perimeter. The optimal set of circumstances is to go in and out without notice. No devices should be compromised; only critical information is desired.

4.4.2 Casing the Environment

Since GIAC Enterprises has not had any security awareness seminars for its employees the following information has been obtained.

- GIAC Enterprises has allowed security vendors and other product vendors to use its name in advertising. Based on the search, I have determined that the company is pro-ISS Suite and prefers Oracle, Linux and UNIX Solaris.
- GIAC Enterprise employees have posted in news groups inquiring on router and firewall configurations. So you know that their outside perimeter comprises of a dual firewall with Checkpoint and Nokia 650. The screening firewall is a CISCO 3620.
- I, Anti-GIAC, gained access to the employee handbook providing names for system administrators and all other employees. With this information, a few disguised calls as GIAC employees grant Anti-GIAC further access to the system. I would like to gain access to the internal network guised as an employee; however, the administrator states that I must bring in my computer to gain internal access via the VPN. Of course, I can't just walk in, or maybe I can. Regardless, I still have the necessary access to formulate an attack.
- One of the employees listed in the GIAC handbook is Matthew Brown. He is listed as the firewall administrator. When I see his design posted at SANS, I know that he probably knows what he's doing. Additionally, I search the net for any other postings on Matthew Brown. I discovered the following:

    - He has also posted at http://cthulhu.ale.org/ale-archive/ale-1999-01/msg00070.html (showing a preference in ISDN's).
    - He was hacked via identd and imap http://cthulhu.ale.org/ale-archive/ale-1999-01/msg00087.html. (These 2 areas could be open but he probably secured it.)
    - He has posted regarding emacs (RHL 5.2). http://cthulhu.ale.org/ale-archive/ale-1999-01/msg00240.html
    - Matt runs backups across the firewall using Amanda (http://groups.yahoo.com/group/amanda-users/message/18510)
    - The list goes on.

4.4.3 Options for Obtaining the Targeted Database

At this time AntiGIAC can now determine the best way to infiltrate and obtain the information from the database. The following options are considered.

Before I continue please note that one must think like a thief in order to catch a thief.

4.4.3.1 Option 1

4.4.3.1.1 Attack Method and Result

Pass through the physical security at lunchtime wearing casual business attire, which is much easier than it sounds. If asked any questions state that you are new. Take the following steps:

1. Find an empty desk with a computer running and use it to determine what the address range and basic configuration is. The screen saver is on, but no one uses a password.
2. Go find an empty cubicle and log into the network with the id and password supplied a few days ago.
3. Stay focused on the target. Ask personnel for their assistance in locating the desired information on the database. Don't be shy; people are very helpful, especially with newcomers. Download the necessary information or preferably the entire database. Do not set off any alarms by using scanning tools. Once you have the targeted information get out.
4. Quietly walk out and no one will ever expect anything. If management determines that information has leaked then they will blame the firewall administrator.
5. Interpret the data at home.

This scenario still has some exposure. Another approach would be to stay with the firm for 1 week as a new hire. Take the information that you need then leave.

Remember: "The most serious financial losses occurred through unauthorized access by insiders (18 respondents reported a total of $50,565,000 in losses), theft of proprietary information (20 respondents reported a total of $33,545,000 in losses), telecommunications fraud (32 respondents reported a total of $17,256,000 in losses) and financial fraud (29 respondents reported a total of $11,239,000 in losses)." [13] The 2000 and 2001 reports do not mention insider vs. outsider losses.

4.4.3.1.2 Controls to Mitigate this Risk and Enhance Perimeter Defense

- Provide a security awareness program catered to general users, administrators, technical owners, project managers, and senior management. This training will include how to identify unauthorized personnel and how to respond, tips for the security novice, media handling from computers to faxes to paper documents, etc.
- Ensure that all personnel have name badges to enter facilities and use turnstiles requiring a badge for entry per person. Most organizations require a badge to enter a door, and of course, the 3 individuals exiting the elevator also spoof their way in.
- Monitor new personnel closely on the network for the first month logging their activity.

[13] Rapulus, Patrice. "Annual cost of computer crime rise alarmingly Organizations report $136 million in losses." 4 MAR 1998. URL: http://www.gocsi.com/prelea11.htm. (6 SEPT 2001).

- Ensure that all computers use a password-protected screensaver activated after 5 minutes of inactivity.

4.4.3.2 Option 2

4.4.3.2.1 Attack Method and Result

After reviewing the employee handbooks, I noticed that there are 3 GIAC Enterprise locations. Location #1's phone number begins with 555-XXXX. Location #2's phone number begins with 254-XXXX. Location #3's phone number begins with 835-XXXX. Using a wardialer (http://members.tripod.com/cusika/phreak/phrack2.htm), a phreaker or hacker could dial the 30,000 possibilities over a period of time and attempt breaking in through this backdoor via i.e. PCAnywhere. Although the Information Security Program Committee may have standards prohibiting the use of modems on equipment, administrators will still install these tools for business reasons from their point of view. After all, if an administrator receives a late night page then dialing into a server is a convenient option if the VPN is not user friendly under attack. If the remote control software (i.e. PCAnywhere) is set on default without a password then GIAC is opening the server for an outside attack. Once the hacker gains access to the system via remote control software, then access to other systems is fairly easy in most organizations using default passwords. Some administrators are not even aware that accounts with default passwords exist. Approximately, 900 default passwords can be retrieved at http://www.securityparadigm.com/ as a primer.

4.4.3.2.2 Controls to Mitigate this Risk and Enhance Perimeter Defense

- Provide a security awareness program catered to general users, administrators, technical owners, project managers, and senior management. This training will include how to identify unauthorized personnel and how to respond, tips for the security novice, media handling from computers to faxes to paper documents, etc.
- Ensure that personnel are made aware that all remote activity must pass through the VPN or VPN dialer if Internet Access is not readily available. Stress this fact to administrators and state that dismissal is appropriate for those circumventing the controls.
- Implement a wardial scan/audit of the environment before the hacker does.
- Program the PBX to only allow outgoing calls for all analog lines. All incoming calls should be disabled, except for identified fax machines.
- Program all company modems to initiate outgoing calls, and disable autoanswer for incoming calls.

4.4.3.3 Option 3—Attack Against the Firewall

4.4.3.3.1 Case the Environment before Performing an Exploit

Though less preferred, hacking at a border router and a firewall is a requirement for passing this section. In Matthew's case, he has defined an effective setup with the dual firewall combination with Checkpoint and Nokia, which I may consider in the future. Additionally, to protect the critical data at the database, he has this located behind a firewall running on a hardened Linux platform.

We need a tool to scan the outside server. Insecure.org polled its nmap-hackers mailing list to select the top 50 security tools listed at (http://www.insecure.org/tools.html). This site provides a good overview of the tools of the trade.

First, run a scan in stealth mode using nmap to determine the open ports; these options are already listed in the audit and testing section for "Testing the Policy" on p. 5. Before initiating, I should telnet quite a few times to hide tracks and initiate from another machine in the arsenal. Next, review open services and determine the best course of action. The following open services are based on the actions taken during Matthew's audit.

 # Nmap (V. nmap) scan initiated 2.53 as: nmap -v -g53 -sS -sR -P0 -p 1-65000 -o realfw1.out 115.50.25.14
(The 64991 ports scanned but not shown below are in state: filtered)

Port	*State*	*Service (RPC)*
25/tcp	*open*	*smtp*
53/tcp	*open*	*domain*
80/tcp	*open*	*http*
138/tcp	*closed*	*netbios-dgm*
443/tcp	*open*	*https*
1010/tcp	*closed*	*unknown*
1017/tcp	*closed*	*unknown*

Only 4 ports are open including 25, 53, 80, and 443. This is what I expected to see. All other services are closed.

Based on these 4 ports and the type of firewall and router I should research exploits to attack this environment head on. This angle of attack is the area of most resistance, and I would not necessarily choose this. In spite of this, the following exploits could be utilized.

4.4.3.3.2 Exploit #1

4.4.3.3.2.1 Impact

Cert.org issued a vulnerability as follows "Vulnerability Note VU#35958 IP Fragmentation Denial-of-Service Vulnerability in FireWall-1". The impact of this vulnerability follows: "An attacker who exploits this vulnerability can monopolize the CPU of a FireWall-1 firewall, rendering it incapable of processing any incoming or outgoing traffic. Attackers are not able to pass packets or fragments that would be filtered out under normal circumstances, nor are they able to gain privileged access to the firewall or its host system." [14]

[14] CERT Coordination Center. "Vulnerability Note VU#35958 ". 11 Jan 2001. URL: http://www.kb.cert.org/vuls/id/35958. (25 Aug 2001).

4.4.3.3.2.2 Result

Was target obtained? No. I am not any closer to obtaining the information from the database server. I have let the opponent know that I exist. I have effectively shut down a firewall. This is the equivalent of a teenager spraying graffiti on public walls. Absolutely nothing tangible was accomplished except upsetting a firewall administrator who will possibly hack at me later from her/his home computer if s/he has correctly identified me.

4.4.3.3.2.3 Controls to Mitigate this Risk and Enhance Perimeter Defense

The cert.org lists a solution as follows to mitigate this risk.

From Checkpoint:
"Check Point is in the process of building new kernel binaries that will modify the mechanism by which fragment events are written to the host system console, as well as providing configurable options as to how often to log. In addition and independent of the console message writing, with the new binaries FireWall-1 administrators will be able use the Check Point log file method for reporting fragmentation events. These binaries will be released shortly in Service Pack 2 of FireWall-1 version 4.1, for 4.1 users, and as a Service Pack 6 Hot Fix for FireWall-1 version 4.0 users."

Workaround:
As an interim workaround, customers can disable the console logging, thereby mitigating this issue by using the following command line on their Fire-Wall 1 module(s):

$FWDIR/bin/fw ctl debug -buf

For further information regarding this vulnerability and the above solution, please visit:
http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html

Quite a few exploits can be found on various sites:

- ISS X-Force http://www.iss.net/xforce
- RootShell http://www.rootshell.com
- TechnoTronic http://www.technotronic.com
- Packet Storm Security Site http://www.Genocide2600.com/~tattooman/index.shtml
- Bugtraq archives: http://www.netspace.org/lsv-archive/bugtraq.html
- NTBugTraq http://www.ntbugtraq.com Aelita Software http://www.ntsecurity.com
- Comprehensive listing of CERTs http://home.flash.net/~kahanek/certs.htm

Most of the exploits don't appear to assist me with the goal of obtaining critical data from the database. There are many piece meal solutions, which get me closer to the target each time, but they create so much noise that the art of surprise is lost.

4.4.3.3.3 Exploit #2

Hacker sites may provide a clearer picture of new exploits attacking the network, but are not yet reported by CERTs. It appears that most CERTs or organizations hesitate issuing a CERT unless there is a fix. For this reason, hacker sites can provide more input into potential exploits. Also, a large percentage could be "magical 'hand-waving' attacks" as noted in the GIAC practical test instructions.

4.4.3.3.3.1 Impact

"A very serious bug in IIS4 has been found, that lets anybody in the world get a DOS prompt in the server, even if it is behind the best firewall." [15] Assuming that the web server is IIS, an exploit using an ncx.exe allows a hacker to telnet to an IIS4 web server via port 80 going unnoticed by the Checkpoint firewall. At this point the hacker can install her/his favorite utilities (Trojans) as the site explains (http://www.megasecurity.org/trojans/iishack/IisHack.htm). It is difficult to tell if this would work since I cannot test it. I'm unsure if the ftp session that is initiated from the IIS server would run through port 80 or attempt to pass through 21 which is blocked. This type of exploit would be preferred because telneting would give me enough control to identify the DMZ, and I could determine what my next step should be to attack the internal firewall launching the attack from the DMZ.

In case this exploit is not real, I will stop at this point. To summarize, between the 2 mentioned exploits, I prefer using tools that could allow remote access through identified ports provided by the nmap scan.

4.4.3.3.3.2 Result

Was target obtained? No. However, if the exploit is real, I am one step closer to the internal network.

4.4.3.3.3.3 Controls to Mitigate this Risk and Enhance Perimeter Defense

- Configure IDS devices to monitor for this specific activity when reviewing packets on port 80.
- Monitor logs on NT Event Viewer for unusual activity.
- Review hacker boards to follow current trends and activity targeting GIAC's environment. A CERT function within the organization could be responsible for this.

4.4.3.4 Which option should be implemented?

Based on the design displayed at SANS and some information posted on the web, I would decide not to risk detection via the Internet. An inside attack is much easier. Therefore, option 1 & then 2 take preference.

[15] Unknown author. "Welcome to NT Bugs ". uncertain of date. URL: http://www.megasecurity.org/trojans/iishack/IisHack.htm (25 Aug 2001).

List of References

Anonymous. "Welcome to NT Bugs ". uncertain of date. URL: http://www.megasecurity.org/trojans/iishack/IisHack.htm. (25 Aug 2001).

Barlow, Jason and Thrower, Woody. "TFN2K—An Analysis". 10 Feb 2000. URL: http://security.royans.net/info/posts/bugtraq_ddos2.shtml. (30 Aug 2001).

Blass, Steve. "What is Split DNS". 15 Jan 2001. URL: http://www.nwfusion.com/columnists/2001/00288013.html (22 Aug 2001).

CERT Coordination Center. "Vulnerability Note VU#35958 ". 11 Jan 2001. URL: http://www.kb.cert.org/vuls/id/35958. (25 Aug 2001).

CISCO. CISCO IOS v. 12 Commands. Unknown date. URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_r/srprt3/srdenial.htm#3971. (5 SEPT 2001).

CISCO. "Command Reference". Unknown Date. URL: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/commands.pdf. (2 Sept 2001).

Dittrich, David. "The DoS Project's "trinoo" distributed denial of service attack tool". 21 Oct 1999. URL: http://staff.washington.edu/dittrich/misc/trinoo.analysis (30 Aug 2001).

Dittrich, David. "The "Tribe Flood Network" distributed denial of service attack tool". 21 Oct 1999. URL: http://staff.washington.edu/dittrich/misc/tfn.analysis (30 Aug 2001).

Dittrich, David. "The "stacheldraht" distributed denial of service attack tool". 31 Dec 1999. URL: http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt (30 Aug 2001).

Internet Encyclopedia. "2.2.1. Split Horizon". Unknown Date. http://www.freesoft.org/CIE/RFC/1058/9.htm. (26 Aug 2001).

Kahanek, John. "Protecting Business Applications with Encryption". 31 Dec 2000. http://www2.csc.com/lef/programs/grants/finalpapers/kahanek_encryption.pdf. (25 Aug 2001). pp. 16-31.

Nortel Networks. "Contivity VPN Switches". 03 Feb 2001. URL: http://www.nortelnetworks.com/products/library/collateral/55129.02-03-01.pdf (25 Aug 2001).

Rapulus, Patrice. "Annual cost of computer crime rise alarmingly Organizations report $136 million in losses." 4 MAR 1998. URL: http://www.gocsi.com/prelea11.htm. (6 SEPT 2001).

SANS Institute. “2.2 Firewalls 101: Perimeter Protection with Firewalls”. Unknown date. pp. 83-87.

SANS Institute. “CISCO Anti-Spoof Egress Filtering”. 15 Jan 2001. URL: http://www.nwfusion.com/columnists/2001/00288013.html. (22 Aug 2001).