Global Information Assurance Certification Paper

SANS Network Security 2002
Darling Harbour, Sydney, Australia
19th - 23rd January, 2002

Firewalls, Perimeter Protection and VPNs

GCFW Practical Assignment Ver. 1.6a (revised October 26, 2001)

Section 1…… Security Architecture

Section 2…… Security Policy

Section 3…… Security Architecture Audit

Section 4…… Design Under Fire

Table of Contents

FIREWALLS, PERIMETER PROTECTION AND VPNS 1

ASSIGNMENT 1 - SECURITY ARCHITECTURE 4

Business Process Flow 4
Business Process 4
Customers 4
Suppliers 4
Partners 5
GIAC Enterprises Staff 5
GIAC Enterprises – Data Flow Diagram 6

Services, Applications and Protocols 6
Internet Access 6
Public Access. 6
Partner Access. 6
Corporate Access to the Internet. 7
E-Mail 7
DNS 7
HTTP Proxy 7

Network Architecture 7
Network Structure 7
Network Addressing 8
General Hardware and Software configuration rules 8
Perimeter Protection 9
Firewall 9
Intrusion Detection System 9
Proxy Server 9

ASSIGNMENT 2 - SECURITY POLICY 10

Perimeter Router 10
General Access Requirements and Restrictions 10
Configuration Rules 10
Access Lists 10
Logging and Debugging 12
Border Router Configuration 12

VPN 15
General Information 15
Server Configuration 16
Client Configuratio n 16

Firewall 16

General Information 16
Configuration Rules 17
Firewall Configuration 17

ASSIGNMENT 3 - SECURITY ARCHITECTU RE AUDIT 20

GIAC Enterprises Security Policy 20
Overview 20
Security Policy 20

Technical Audit 21
External Scan of GIAC Network 21
Scan of GIAC perimeter router 21
Perimeter Router Service Scan 21
Perimeter Router Network Address Filtering. 22
Perimeter Router Protocol Filtering. 22
Firewall Protection 23
Intrusion detection 23

Audit Evaluation 24

ASSIGNMENT 4 - DESIGN UNDER FIRE 26

Attack #1 26
Vulnerability #1 26
Vulnerability #2 27
Vulnerability #3 28
Selected attack design 29
Results 29

Attack #2 29
Compromise of an Internal system 29
Results 30

Summary 31

Assignment 1 - Security Architecture

Business Process Flow

Business Process

GIAC Enterprises is an e-business dealing in the online sale of Fortune Cookie sayings. The nature of the business is that the majority of business transactions are conducted electronically. These include financial transactions, the transmission of copyrighted material and personal details over external networks, order processing and remote access over external networks for the sales and marketing teams.

Customers

Potential customers are those individuals or businesses who make a product related request to GIAC Enterprises. Customers can be registered, in which case their bona fides have been verified by GIAC Enterprises, or un-registered. Un-registered customers are limited to viewing the GIAC Enterprises web site.
Valid registered customers' transactions are as follows

Login/Logout
Submit or cancel registration details
Submit, cancel or modify a product order
Query an order
Submit an enquiry or complaint

Access requirements

Registered customers require secure access (HTTPS) to the GIAC Enterprises web site
Un-registered customers require HTTP to access unrestricted non-secure areas of the site only.

Suppliers

The suppliers supply Fortune Cookie sayings to GIAC Enterprises. Fortune Cookie sayings are supplied electronically.
Valid supplier transactions are

LOGIN/LOGOUT

Update personal details
Change password
Upload a data file of Fortune Cookie Sayings

VIEW PERSONAL ACCOUNT

Access requirements

Suppliers require secure authenticated access to the GIAC application server to upload Fortune Cookie sayings.

Partners

GIAC Enterprises' partners are internationally based and translate and r esell fortunes. Partner transactions are:

- Login/Logout
- Update partner details
- Change password
- Download a date file of Fortune Cookie sayings
- View account details
- Submit an enquiry or complaint

Access requirements

- Partners require HTTPS to access restricted data on the GIAC Enterprises web site and to download Fortune Cookie sayings.

GIAC Enterprises Staff

GIAC Enterprises' staff perform all back office functions. The staff have been grouped into four general categories. Each category has different access re quirements to GIAC Enterprises' systems. The categories and access requirements are as follows.

Administration –

- Access internal systems only
- No remote access required
- No access to external entities.

Sales and Marketing –

- Access internal systems only
- Remote access to internal systems
- No access from internal hosts to external entities

Technology Operations –

- Access internal systems and external entities
- Require secure remote access to internal systems

Management -

- Access internal systems and external ent ities
- Require secure remote access to internal systems

GIAC Enterprises – Data Flow Diagram

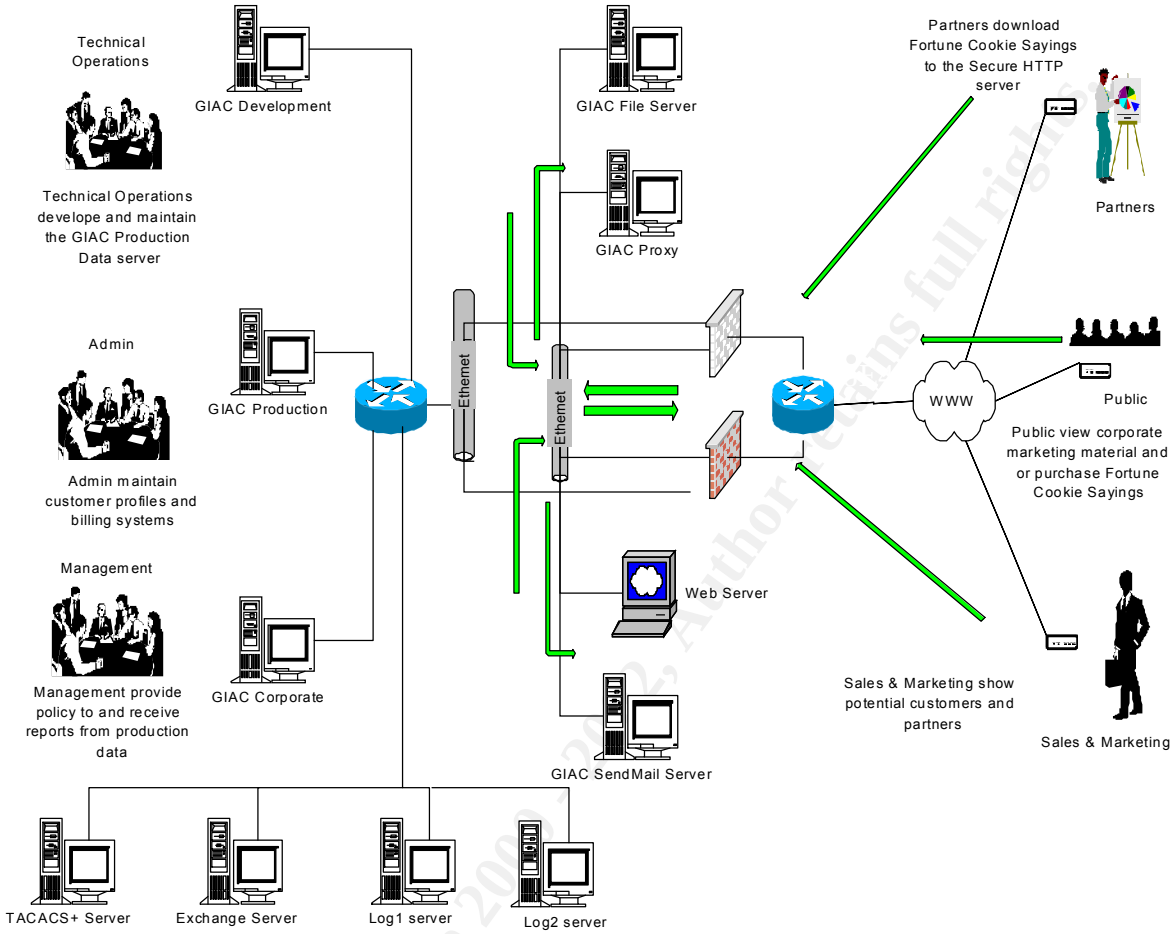


Figure 1.

Services, Applications and Protocols

Internet Access

The role of the GIAC Web site is to provide sales and marketing suppor t for Fortune Cookie Sayings. To enable this the following services, applications and protocols will be supported. Any services, applications and protocols not required to support the web site must be disabled. Refer to the Security Policy document in sect ion 2 for specific services that are allowed or disallowed.

Public Access.

The GIAC Web Server will only support the IP HTTP protocol (port 80) and HTTPS protocol to enable general browsing and e -commerce related transactions.

Partner Access.

Partner access to the GIAC Fortune Cookie Sayings (FCS) application server will be via a Virtual Private Network (VPN) to the FCS host located on the services domain of the GIAC Network. The

Partner host systems should run an IPSec compliant VPN client. Access for partners will be restricted to the FCS server. Client side communications use the HTTPS protocol.

Corporate Access to the Internet.

Staff of GIAC Enterprises will be able to access the Internet from the corporate network. Access to the Internet will be via a HTTP proxy server. Non-essential services from the gateway will be disabled.

E-Mail

GIAC Enterprises requires e-mail as part of their business communications strategy. The mail server will reside in the internal business network A Sendmail server should be deployed on the service network (DMZ). All inbound and outbound mail must pass through the Sendmail relay. The e-mail gateway uses the SMTP protocol.

DNS

DNS services are required to enable name resolution on the Internet. Zone transfers to the Internet should be disabled by blocking TCP port 54. A slave DNS server should be installed for redundancy.

HTTP Proxy

A proxy server has been selected to provide HTTP services to the Internet. This will enable GIAC Enterprises to provide address filtering and better management of what Internet services and sites are allowed from the corporate site.

Network Architecture

Network Structure

The network structure of GIAC Enterprises will be designed to provide flexibility while maintaining security internally and from malicious external attack. The network design incorporates three distinct layers, each layer providing security within itself and from the adjacent layer. The three layers have been defined as follows:

Layer 1 – The Corporate Domain. The internal network is segmented between the various business units of GIAC Enterprises by a Cisco 3640 router. This provides independent broadcast domains for each segment and security between the different business units. Each segment will have a registered private IP address domain. The business segments have been defined as follows.

- Corporate Management segment
- Administration segment
- Technology development segment
- Shared systems segment.

This router also provides the gateway to the Services Domain.

Layer 2 – The Services Domain. This layer provides the services that GIAC Enterprises requires for successful and secure access to and from the Internet. Hosts in this segment will employ registered public IP addresses.

Layer 3 - The Internet Domain. This layer provides physical access to and from the Internet. Services in this layer are restricted to specific addresses, protocols and services.

Figure 2 provides a pictorial representation of the network structure.

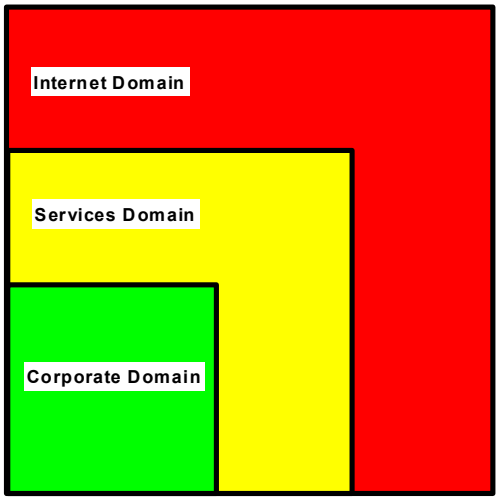


Figure 2.

Network Addressing

Comment	GIAC_CORP1	GIAC_PIX1	GIAC_PIX2	GIAC_PER1	GIAC_PER2
Management LAN	192.168.1.0/26				
Administration LAN	192.168.1.64/26				
Technology LAN	192.168.1.128/26				
Shared Systems LAN	192.168.1.192/26				
GIAC_CORP/ GIAC_PIX	192.168.2.248/29				
Shared Services LAN	208.10.2.0/25	208.10.2.2/25* 208.10.2.3/25	208.10.2.2/25* 208.10.2.4/25		
GIAC_PIX /GIAC_PER		208.10.2.129/29* 208.10.2.130/29	208.10.2.129/29* 208.10.2.131/29	208.10.2.132/29* 208.10.2.133	208.10.2.132/29* 208.10.2.134
GIAC_PER /Internet Proxy Server/DNS	208.10.2.4			208.10.2.137* 208.10.2.138	208.10.2.137* 208.10.2.139
File Server	208.10.2.5				
Web Server	208.10.2.3				
Sendmail Server	208.10.2.2				

* HSRP address

General Hardware and Software configuration rules

- Access to and from public networks must only occur via the perimeter router.

- Permissible traffic on the perimeter router is to be controlled by access lists on inbound and outbound ports.
- Only registered public Internet addresses can access the internal network from the Internet.
- Internal addresses accessing the Internet are to be translated to a registered public Internet address registered to GIAC Enterprises.

Perimeter Protection

Perimeter protection enables the business to establish protection against the most easily detected fraudulent network traffic. Examples are invalid or illegal network addresses and internal addresses being spoofed from the external network. It is recommended that dual Cisco 3620 series routers be installed to provide perimeter protection. This router provides the link from the World Wide Web to the GIAC Enterprises site via a Cisco PIX firewall. The Perimeter router provides static filtering on inbound and outbound interfaces and provides the first level of defense against malicious traffic.

Firewall

A Cisco PIX Firewall 515 running IOS version 5.2 should be installed to provide the firewall functionality for the GIAC Enterprises site. This product has been selected as it is designed for a small office yet provides the following features:

- VPN gateway function to enable secure access for GIAC Enterprises partners and support personnel.
- Intrusion Detection is available at release 5.2 of the software and the PIX includes some Denial of Service protection mechanisms
- Support for many popular authentication servers.
- Network Address Translation

The firewall provides a critical function for GIAC Enterprises. To ensure availability duplicate PIX 515s should be set up in a redundant configuration.

Intrusion Detection System

An Intrusion Detection System (IDS) complements the firewall by inspecting traffic that has been allowed through the firewall. It provides protection against a malicious payload that has legitimate packet headers and addressing. An IDS will not necessarily stop an attack, but it does provide the alarm for known attack patterns and can alert on suspicious traffic. Offending traffic can be logged for later analysis. This helps the business to improve the overall defense of the site by providing information necessary to update filtering and firewall rule-sets.

Proxy Server

The proxy server will be set up as the gateway for GIAC Enterprises to access the Internet. The primary purpose of the proxy is to avoid direct connection between GIAC desktop systems and WWW servers. Filtering on the proxy server will enable GIAC Enterprises to limit access to the Internet to authorized staff, block dangerous or undesirable web sites and filter any active code on the web servers such as Active X. The proxy server will have only those services enabled that allow it to provide the HTTP service only.

Assignment 2 - Security Policy
Perimeter Router

General Access Requirements and Restrictions

As an E-business, the perimeter router is critical to the GIAC Enterprises as it provides the channel for customers, business partners and the general public. For this reason the perimeter routing function needs to be secure and resilient. The recommended perimeter router is dual Cisco 3620 routers set up in redundant configuration (HSRP).
All access is based on the Internet protocol.
All transmissions of non-public information over public networks are to be encrypted using the SSL architecture with the highest-level cipher publicly available for the recipient's country. The site should be enabled with a 128 bit digital certificate to enable SSL communications and guarantee authentication, encryption and non-repudiation.
Where specific access is not defined in this policy it will be denied.
The guidelines for the configuration of these routers are taken from the Router Configuration Security Guide developed by the USA National Security Agency. This guide is available at the following URL - http://nsa2.www.conxion.com/cisco/index.html

Configuration Rules

- Generally, only permit required protocols and services on the external interface. Some of the well-known ports are listed below. This list should be expanded, as the requirements are known.

Port	Service
21	FTP
22	SSH (rlogin)
25	SMTP
53	DNS
80	HTTP
123	NTP
110	POP3
443	HTTPS
614	SSH Shell

- Shutdown unneeded servers on the router.
- Shutdown unneeded services on the router.
- Shutdown unused interfaces.
- Disallow directed-broadcasts and proxy-arp requests.
- Secure the console line, the auxiliary line and the virtual terminal lines on the router.
- Password access to the router should be protected via encryption and provide configure passwords for the console line, the auxiliary line and the virtual terminal lines.

Access Lists

Access lists should be implemented on the outside interface (Internet) and the inside interface (GIAC Service Domain). On the outside interface the following rules should be implemented.

- Deny private address space (RFC 1918) access to the perimeter router
- Deny IANA reserved add ress space from entering the GIAC network from the Internet
- Deny GIAC public address space from entering the GIAC network from the Internet
- Deny Loopback address
- Reject Risky Protocols and Services

The full list of assigned numbers and names is available f rom the IANA website at the following URL. http://www.iana.org/assignments/port -numbers
Known problem port numbers are listed below. This list should be updated as information becomes available.

Port	Service
1 (TCP & UDP)	Tcpmux
7 (TCP & UDP)	Echo
9 (TCP & UDP)	Discard
11 (TCP)	Systat
13 (TCP & UDP)	Daytime
15 (TCP)	Netstat
19 (TCP & UDP)	Chargen
37 (TCP & UDP) 43 (TCP)	Time Whois
67 (UDP)	Bootp
69 (UDP)	Tftp
93 (TCP)	Supdup
111 (TCP & UDP)	Sunrpc
135 (TCP & UDP)	Loc-srv
137 (TCP & UDP)	Netbios-ns
138 (TCP & UDP)	Netbios-dgm
139 (TCP & UDP)	Netbios-ssn
177 (UDP)	Xdmcp
445 (TCP)	Netbios (ds)
512 (TCP)	Rexec
513 (TCP & UDP)	rlogin, who
514 (TCP) 514 (UDP) on external inteface only	Rsh,rcp,rdist,rdump Syslog
517 (UDP)	Lpr
518 (UDP)	Ntalk
540 (TCP)	Uucp
550 (TCP & UDP)	New who
2049 (UDP	Nfs
6000-6009 (TCP)	X Window System
6667 (TCP)	Irc
12345 (TCP)	Netbus
12346 (TCP)	Netbus
31337 (TCP & UDP)	Back Orifice

Log access list port messages.

On Internal ports only allow only GIAC enterprises registered IP addresses to enter the router from the internal network On the external port define the following

- Allow DNS services inbound and outbound to/from DNS server
- Allow SMTP service inbound and outbound to/from Sendmail server
- Allow HTTP requests inbound to the Web server
- Block GIAC Enterprises registered addresses inbound to the port
- Block loopback addresses
- Block reserved addresses
- Block broadcast
- Block ICMP redirects
- Allow DNS, Mail, web access (HTTP) and secure web traffic (HTTPS)
- Allow SSH shell

Logging and Debugging

Turn on the router logging capability and use it to log errors and blocked packets to an internal (trusted) syslog host. Configure the router to include ti me information in the logging and get the time from an NTP server for accurate time tracking. This will allow the administrator to trace network attacks more accurately. Configure SNMP to remove the default community string and set a better read only commu nity string.

Border Router Configuration

The following configuration is designed for a Cisco model 3620 router running IOS version 12.0.5.

```
Press RETURN to get started!
User Access Verification
Password:
GIAC_PER1>en
Password:
GIAC_PER1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
    hostname GIAC_PER1
    !
    logging buffered 4096 warnings
    logging console critical
    aaa new-model
    aaa authentication login default tacacs+ enable
    aaa authentication login no_tacacs line
    enable secret 5 $1$a3YH $Hjj4B.b/AWyJVYzBIgI2R/
    enable password 7 04481F031924
!
! Disable Small services (echo, discard, chargen, etc.)
    no service tcp-small-servers
    no service udp-small-servers
    no ip bootp server
    no service finger
    no ip http server
```

```
    no snmp-server
!
! Shutdown unneeded services on the router
    no cdp run
    no service config
    no ip source-route
    no ip classless
!
! Line Commands
    interface Loopback0
    no ip address
    no ip directed-broadcast
!
! Outside link to ISP
    interface Serial0/0
    description Serial link to ISP
    ip address 208.10.2.137 255.255.255.248
    ip access-group 107 in
!
! Enable Access Lists
    ip access-group 107 in
    ip access-group 101 out
!
! Improve security against smurf attacks and ad -hoc routing
    no ip redirects
    no ip directed-broadcast
    no ip proxy-arp
    no cdp enable
    no mop enabled
!
    interface Ethernet0/0
    description Link to firewall hosts
    ip address 208.10.2.132 255.255.255.248
!
! Enable access list 101 for this interface
    ip access-group 101 in
!
! Improve security against smurf attacks and ad -hoc routing
    no ip redirects
    no ip directed-broadcast
    no ip proxy-arp
    no cdp enable
    no mop enabled
!
! Exit Line mode
    Exit
!
```

```
!Define network
    router eigrp 55555
    network 208.10.2.0
    no auto-summary
!
! Define outbound access to the internet
! Allow only GIAC registered addresses
    access-list 101 permit ip 208.10.2.0 0.0.0.255 any
    access-list 101 deny   ip any any log
    access-list 101 deny   udp any any log
!
! Define inbound access from the internet
! Deny GIAC registered addresses
    access-list 107 deny   ip 208.10.1.0 0.0.0.255 any l og
    access-list 107 deny   udp 208.10.1.0 0.0.0.255 any log
!
! Deny loopback addresses
    access-list 107 deny   ip 127.0.0.0 0.255.255.255 any log
    access-list 107 deny   udp 127.0.0.0 0.255.255.255 any log
!
! Deny private addresses
    access-list 107 deny   ip  10.0.0.0 0.255.255.255 any log
    access-list 107 deny   udp 10.0.0.0 0.255.255.255 any log
    access-list 107 deny   ip 172.16.0.0 0.15.255.255 any log
    access-list 107 deny   udp 172.16.0.0 0.15.255.255 any log
    access-list 107 deny   ip 192.168.0.0 0.0.255.255  any log
    access-list 107 deny   udp 192.168.0.0 0.0.255.255 any log
    access-list 107 deny   ip 224.0.0.0 0.255.255.255 any log
    access-list 107 deny   udp 224.0.0.0 0.255.255.255 any log
!
! Deny ICMP
    access-list 107 deny   icmp any any redirect log
!
! Allow DNS Access
    Access-list 107 permit tcp any any 53 reflect packets
    Access-list 107 permit tcp any host 208.10.2.4 eq 53
    Access-list 107 permit udp any host 208.10.2.4 eq 53
!
! Allow Mail traffic
    Access-list 107 permit tcp any host 208.10.2.2 eq 25
    Access-list 107 permit udp any host 208.10.2.2 eq 25
!
! Allow Web Traffic (HTTP) and secure web traffic (HTTPS)
    Access-list 107 permit tcp any host 208.10.2.3 eq 80
    Access-list 107 permit udp any host 208.10.2.3 eq 80
    Access-list 107 permit tcp any host 208.1 0.2.3 eq 443
    Access-list 107 permit udp any host 208.10.2.3 eq 443
```

```
!
! Allow Secure Shell
    Access-list 107 permit tcp any any eq 614
    Access-list 107 permit udp any any eq 614
!

! Use passwords for SNMP
    snmp-server community Hard2Guess1t RO
!
! Enable TACACS
    tacacs-server host 208.10.2.6
!
! Make the console line, the auxiliary line and the virtual terminal lines on the router secure
    line con 0
    Exec-timeout 5 0
    Login
    Transport input telnet
    line aux 0
    No exec
    Exec-timeout 0 10
    Transport input none
    line vty 0 4
    Exec-timeout 5 0
    Login
    Transport input telnet
!
! Configure the Enable Secret password, which is protected by the MD5 based algorithm.
    service password-encryption
!
! Enable debugging with time stamps
    Service timestamps log datetime localti me show-timezone
    Clock timezone EST –5
    Ntp source S0/0
!Enter the NTP server IP address in the following command
    Ntp server xxx.xxx.xxx.xxx
!
! Exit and save configuration
    Exit
    Copy running-config startup-config
    Quit
```

VPN

General Information

GIAC Enterprises has deployed a VPN to provide access to the GIAC systems for technical support and sales and marketing representatives. The VPN provides access to the corporate Intranet via dial,

ISDN, DSL and cable technologies. The VPN uses a client -initiated connection. With client-initiated access VPNs, users establish an encrypted IP tunnel from their clients across a service provider's shared network to the corporate network. Client -initiated VPNs ensure end -to-end security from the client to the host. With client-initiated VPN Access, the end user has IPSec client software installed at the remote site, which terminates on the PIX firewall for connection into the corporate network. The Cisco IPSec solution fully supports Internet key exchange (IKE) and certificate authority to generate the encryption, authentication, and certificate keys to be used to ensure secure transmission of data. IPSec provides a mechanism for secure data transmission over IP networks, ensuring confidentiality, integrity and authenticity of data communications over unprotected networks such as the Internet.

Server Configuration

IKE Policy.

Parameter	GIAC Pix VPN Server	Client
Encryption algorithm	3Des	3Des
Hash algorithm	SHA	SHA
Authentication method	Pre-share	Pre-share
Key exchange	768-bit D-H	768-bit D-H
IKE SA lifetime	86.400	86.400

Policy	GIAC Pix VPN Server	
Transform set	ESP-3DES tunnel	ESP-3DES tunnel
Peer Pix firewall hostname	GIAC_Pix	
Peer Pix firewall IP address	208.10.2.129	0.0.0.0
Encrypting hosts	208.10.2.0/25	0.0.0.0
Traffic (packet) type to be encrypted	IP	IP
SA establishment	Ipsec-isakmp	Ipsec-isakmp

Client Configuration

On the Cisco Client PC software create a new client connection

Connection entry - vpnpeer0
Host name or address of remote server - 208.10.2.129

In the properties section for vpnpeer0

Select group Access Information
Name - partner0
Password - ****

* this is the preshared key and matches the password in the PIX config

Confirm password - ****

Firewall

General Information

Dual Cisco PIX Firewall model 515 running software version 5.2 will provide the firewall functionality for the GIAC Enterprises site. This product provides the following features:

- Traffic filtering

- VPN gateway function
- Intrusion Detection
- Support for authentication servers.
- Network Address Translation

The firewall provides a critical function for GIAC Enterprises. To ensure availability duplicate PIX 515s will be installed in a fail-over configuration. In order for fail-over to work both units must have the same software version, activation key-type, flash memory and RAM.

Configuration Rules

- GIAC enterprises require that all access from the corporate network destined for the Internet have valid Internet addresses registered to GIAC Enterprises. To enable this the Network Address Translation feature should be configured.
- All messages from the Firewall should be logged to the logging server
- To hide the firewall from the external network disable ping responses but permit ICMP unreachable messages
- Enable the IP packet fragment guard. This secures against attacks such as teardrop.
- Configure Intrusion Detection
- To protect GIAC against a SYN attack, configure the SYN Flood Guard to limit the number of embryonic connections allowed.
- Allow access from the mail server to the exchange server
- Allow access from all servers to the log servers
- Allow access from the file server to the production server for https traffic
- Allow any host with a valid public address to access the web server for HTTP and HTTPS

Firewall Configuration

```
Pixfirewall>
Pixfirewall> enable
Password:
Pixfirewall# configure terminal
Pixfirewall(config)# hostname GIAC_PIX
!
!Configure Interfaces
        Nameif Ethernet1 outside security0
        Nameeif Ethernet0 dmz security50
        Nameeif Ethernet2 corp security100
        Nameeif Ethernet3 Failover
        ip address outside 208.10.2.129 255.255.255.248
        ip address dmz 208.10.2.2 255.255.255.128
        ip address corp 192.168.2.249 255.255.255.255.255.255.248
!
!Configure Routes
       route outside 208.10.2.129 0 208.10.2.132 1
        route dmz 208.10.2.2 255.255.255.128 208.10.2.1 1
        route corp 192.168.0.0 255.255.0.0 192.169.2.249 1
!
! Configure the logging to the logging server
```

```
            logging host corp 192.168.1.195
            logging host corp 192.168.1.196
            logging trap 7
            logging timestamp
            logging on
!
!Disable ping
            Icmp deny any echo -reply outside
!
!Maintain state tables on allowed protocols
          fixup protocol http 80
          fixup protocol ftp 21
!
!Turn on Mail Guard to allow only SNMP commands specified by RFC821
          fixup protocol smtp
!
!Provide network address translation for outbound internet access
          nat inside 1 192.168.1.0 255.255.255.0
          global outside 1 208.10.2.128 -208.10.2.254
!
!Permit ICMP unreachable messages
            Icmp permit any unreachable outside
!
!Enable the IP packet fragment guard. This secu res against attacks such as teardrop.
            Sysopt security fragguard
!
!Configure Intrusion Detection
            Ip audit name attackpolicy attack action alarm reset
            Ip audit interface outside attackpolicy
!
!SYN Flood Guard. Limit the number of embryonic connection s allowed
           Static (inside,outside) 208.10.2.129 208.10.2.0 255.255.255.128 0 1000
!
!Allow access from the mail server to the exchange server
           Access-list acl_dmz_corp permit tcp host 208.10.2.2 host 192.168.1.194
!
!Allow access from all servers to the log servers
          Access-list acl_dmz_corp permit tcp host 208.10.2.0 255.255.255.192 host 192.168.1.195
          Access-list acl_dmz_corp permit tcp host 208.10.2.0 255.255.255.192 host 192.168.1.196
!
!Allow access from the file server to the production server for htt ps traffic
          Access-list acl_dmz_corp permit tcp host 208.10.2.5 host 192.168.1.65 eq https
!
!Allow any host to access the web server
           Access-list acl_int_dmz permit tcp any host 208.10.2.3 eq www
!
!Apply the access lists to the ports on the firewall
```

```
        Access-group acl_dmz_corp in interface corp
        Access-group acl_int_dmz in interface outside
        Access-group acl_dmz_int out interface dmz
!
!Enable failover
        failover active
!
!Enable VPN Access
        Access-list 80 permit ip host 208.10.2.129 208.10.2.0 255.255.255.12  8
        Ip local pool partner 208.10.2.112 208.10.2.127
!
! No nat inside tunnel
        Nat 0 access-list 80
!
!Configure crypto Map
        Sysopt connection permit ipsec
        Crypto ipsec transform -set aaa-des esp-3des esp-md5-hmac
        Crypto dynamic -map dynomap 10 set transform -set aaades
        Crypto map vpnpeer 20 ipsec -isakmp dynamic dynomap
        Crypto map vpnpeer client authentication mytacacs
        Crypto map vpnpeer interface outside
!
!Configure the IKE parameters
        Isakmp enable outside
        Isakmp client configuration address -pool local partner  outside
        Isakmp policy 10 authentication pre -share
        Isakmp policy 10 encryption 3des
        Isakmp policy 10 hash md5
        Isakmp policy 10 group2
        Isakmp policy priority lifetime 86400
        Vpngroup internet address -pool partner
        Vpngroup internet idletime 1800
        Vpngroup partner password ********
        Access-group acl_dmz_int out interface dmz
!
!Enable TACACS
        Aaa-server mytacacs protocol tacacs+
        Aaa-server mytacacs host 208.10.2.5 tacacskey timeout 5
```

Assignment 3 - Security Architecture Audit
GIAC Enterprises Security Policy

Overview

A thorough security architecture audit requires both an on -site and off-site review of the infrastructure. The audit attempts to answer whether the site is secure both locally and remotely. Execution of the audit may disrupt the network traffic an d impact the GIAC systems therefore it is important to gain management approval for the structure of the audit, the scope and to highlight any implications from the execution of the audit and the audit results. The audit will be structured as follows.

On-site

The purpose of the onsite visit is to obtain management approval; the policy documents; view the infrastructure; and view the local physical security. While on -site, the auditor will discuss any issues or concerns that staff may have or any incidents they may be aware of regarding the physical and logical security of GIAC enterprises e -commerce site.

Off-site

The audit will review the GIAC Enterprises security policy and test the GIAC Enterprises site to see if policy designed to protect the site from inadvertent or malicious external access is effective. The audit will test the site against " The Twenty Most Critical Internet Security Vulnerabilities" as reported by the SANS institute. (SANS Resources - The Twenty Most Critical Internet Security Vulnerabilities (Updated) These threats have been identified as the most common threats to a site connected to public networks such as the Internet.

On-site

A return visit will be made to test the site against poli cies designed to protect the site internally.

The audit will be conducted at off -peak times during daytime and evening hours, as the business is a 24-hour site. While the audit will test for potential threats to the business, care will be taken to avoid pu tting the business in jeopardy during the testing. The tests will determine the potential of a threat, not create or threaten the business itself. The audit will take one person 40 hours to complete including the audit report to management. The fee for thi s service will be $8000.

*Note 1 – the majority of testing and the results in this section is hypothetical as I am unable to replicate the GIAC architecture to a sufficient degree to provide actual screen shots and other output displays.

Security Policy

GIAC Enterprises security policy consists of four broad areas of security implementation as follows:

- Perimeter protection – A set of design guidelines and rules to be applied to the GIAC enterprises Internet Gateway routers.
- Firewall protection for t he Web services – Specific rules governing access to and from each host in the services segment (DMZ) of the network.
- Remote access for customers and partners – Defines the methods of access for customers and staff and the allowed protocols and security m echanisms.

- Internet access for GIAC enterprises staff from the corporate network – Defines what addresses and protocols are allowed to access the Internet from within the corporate network.

Technical Audit

External Scan of GIAC Network

A typical attack scenario of the GIAC site would see an attacker doing a general scan of the GIAC subnet to see which addresses and applications are available for further investigation. To do this a tool such as NMAP or Superscan could be used. The command for NMAP is as follows:
Command: Nmap –sS –O GIAC.com/24
This command would launch a stealth scan against each machine in the subnet that corresponds to the GIAC.com subnet. It will try to determine what operating system is running on each host.
The expected response would be an ACK from those applications that GIAC supports over the web.

Scan of GIAC perimeter router

In order to test the security policy, the auditor will first test the border router that is the initial defence mechanism for the GIAC site. This test will be carried out with a network mapping tool such as NMAP and Superscan to determine what protocols and network addresses have access to the GIAC site. The router is not expected to support any services itself, therefore a scan of services is expected to return a nil result. The border router is expected to filter traffic based on either network address or protocol.

Testing will be in three passes.

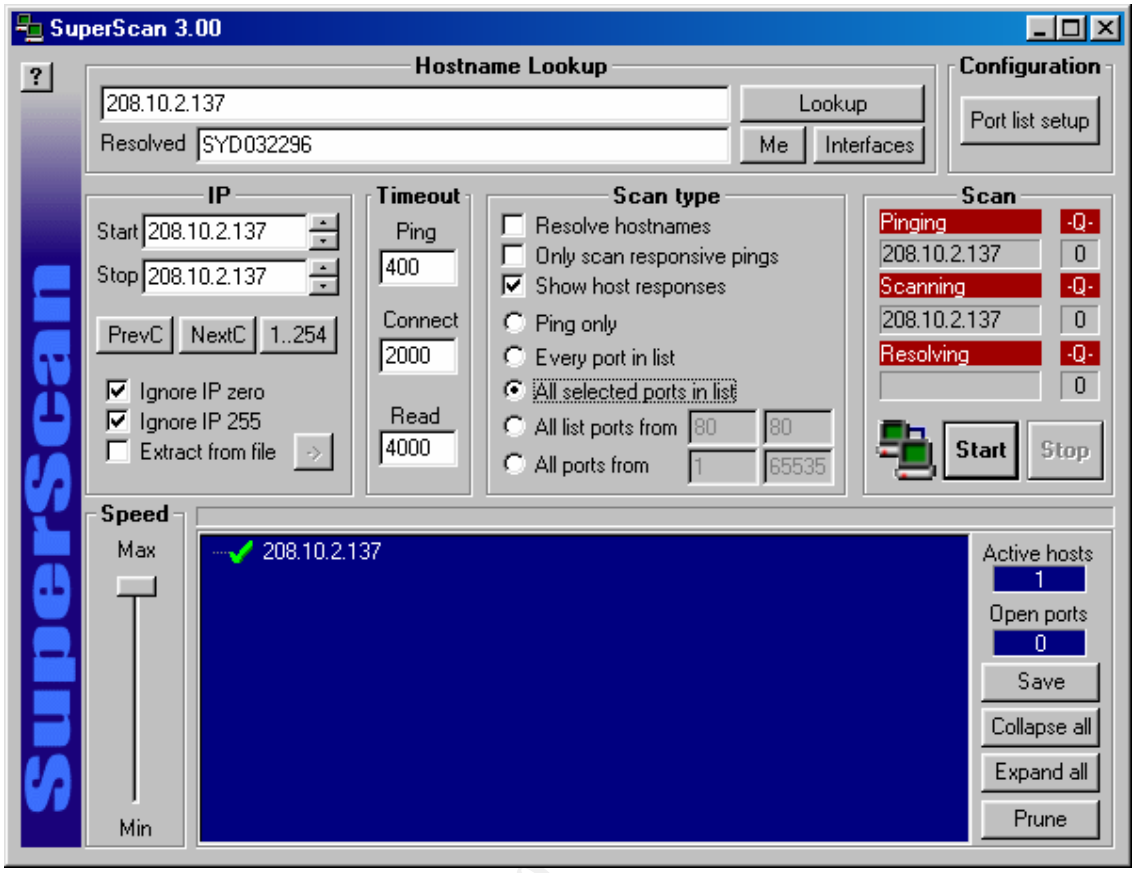
Pass 1 – Perimeter Router Service Testing.
Test for any services on the perimeter router. Services provide a tool for a hacker to further exploit the GIAC site.

Pass 2 – Perimeter Router Network Address Filtering.
Invalid addresses are used by a hacker to disguise the true identity of the attacking host. For example, if a hacker can appear as a legitimate internal user, they may gain additional access to the site.

Pass 3 – Perimeter Router Protocol Filtering.
Many applications have known weaknesses therefore a hacker will attempt to access these services first. Disrupting services on the perimeter router can cause enough impact to cause a denial of service. Typically services on the router should not be available from the Internet

Perimeter Router Service Scan

Using the network-mapping tool 'Superscan' the perimeter router was scanned from the external network to determine what services were available on the perimeter router itself. All recognized services were scanned for. No services were found on the perimeter router.



Perimeter Router Network Address Filtering.

Using the NMAP tool, an attempt was made to acces s the GIAC site using spoofed network addresses. To validate the attempts, the router logs are checked to see if the router has identified the illegal address. The router should indicate that the packet has been dropped. To further verify that the packed was dropped, the TCP Dump tool is used on the internal network to see if the packet passes through the perimeter router.*
To test this scenario, the NMAP command used will attempt to initiate a session with the GIAC web host on port 80

Command: nmap -sS -S192.168.1.15 -e0 –p80 208.10.2.3

Result: The perimeter router outputs the following message to the syslog server
"access list 107 denied TCP 192.168.1.15(33280) 208.10.2.3,m 1 packet "

* See Note 1

Perimeter Router Protocol Filtering.

An attempt was mad e with a valid IP address to access any host on the GIAC site on port 20. The source host was attempting to establish an FTP session. The FTP protocol should be disallowed according to the security policy. As in the previous test the router logs are checke d to see if the

router has identified the illegal packet. The router should indicate that the packet has been dropped. To further verify that the packed was dropped, the TCP Dump tool is used on the internal network to see if the packet passes through the perimeter router.*

The NMAP command used will attempt to initiate a session with any GIAC host on port 20 in the shared subnet 208.10.2.0/25

Command: nmap -sS –p20 208.10.2.1/25

Expected Result: The perimeter router outputs the following message to the syslog server
"access list 107 denied UDP xxx.xxx.xxx.xxx(21) 208.10.2.1,m 1 packet "
"access list 107 denied UDP xxx.xxx.xxx.xxx(21) 208.10.2.2,m 1 packet "
"access list 107 denied UDP xxx.xxx.xxx.xxx(21) 208.10.2.3,m 1 packet "
"access list 107 denied U DP xxx.xxx.xxx.xxx(21) 208.10.2.4,m 1 packet "
……
etc.

* See Note 1

Firewall Protection

The firewall is designed to provide protection against more sophisticated attacks where the perimeter router has allowed what would otherwise appear as legitimate pack ets to traverse the network. An example of this is a fragment attack where packets have legitimate IP and port addresses but are in fact disguised as a message fragment. The fragment payload can be the carrier of various types of attack such as buffer over -flow (ping o'death) and malformed packets such as a teardrop attack.

To determine that a packet with valid address and protocol id is legitimate, the PIX firewall maintains a state table. This table keeps a record of session states and can determine whet her a packet is a valid response to a request or just masquerading as such. The PIX will also re -assemble packets before sending them on to the destination server.

To test the firewall policy the NMAP program will be used to send an ACK scan to the h osts identified by the external scan of the GIAC network. This type of scan sends an ACK packet to the ports specified. If a RST comes back, the port is classified as 'un -filtered'. If nothing comes back (or if an ICMP Unreachable is returned), the port is classified as filtered.
Command: nmap -sA –p1-1024 GIAC.com/24
Result: The expected result would be to see an ICMP Unreachable returned indicating that the firewall has intercepted and dropped the packet. The Pix syslog should have an entry indicating the same. To verify this the syslog is checked. Also, a network sniffing tool like TCP Dump is used to monitor traffic between the from the firewall to the internal network.

Intrusion detection

The Intrusion Detection System is part of the PIX firewall. Intrusion detection is similar to virus detection in that the IDS uses a 'signature' file where known patterns of intrusion detection are

stored. This file needs to be kept up to date as intrusion detection patterns may change over time. It is important to regularly check this and should be part of standard operation procedures. The IDS system logs to the syslog server. The logs should be reviewed daily to determine any irregular activity and be used to identify the source addresses of suspect traffic. This information should be used to update firewall and router access lists.
To test that the IDS is working, we can attempt to ping any host behind the firewall.
Command: C:\>ping –l 65000 208.10.2.3
Result: Pinging 208.10.2.3 with 65000 bytes of data

Request timed out
Request timed out
Request timed out
Request timed out

The syslog has the following entry
<164> Feb 19 2002 08:10:15: %Pix -4-400025: IDS:2154 ICMP ping of death from 204.15.9.17 to 208.10.2.3 on interface outside
<164> Feb 19 2002 08:10:15: % Pix-4-400025: IDS:2154 ICMP ping of death from 204.15.9.17 to 208.10.2.3 on interface outside
<164> Feb 19 2002 08:10:15: %Pix -4-400025: IDS:2154 ICMP ping of death from 204.15.9.17 to 208.10.2.3 on interface outside
<164> Feb 19 2002 08:10:15: %Pix -4-400025: IDS:2154 ICMP ping of death from 204.15.9.17 to 208.10.2.3 on interface outside

Audit Evaluation

GIAC Enterprises has all the relevant tools in place to protect their network from known exploits. This however is not enough to say that GIAC Enterprises can rest assured that the network will always be safe.
It is noted that there is no internal firewall (between the service LAN and GIAC Enterprises corporate network). GIAC needs to consider the risk of compromise of data stored internally to the business and the impact compromise of this data would have to the business. At a minimum, the internal router should be hardened to a similar level as the perimeter router. NAT is used for web traffic from the internal to external network and no external traffic other than mail, log are expected on the internal network, filtering can be designed around these conditions.

To maintain ongoing security the following activities are recommenced

- When new versions of software are installed on GIAC hosts or changes are made to any components configuration then the audit should be carried out again.
- Logs should be reviewed daily to identify suspicious activity
- System security patches applied when available
- GIAC Enterprise staff monitor sites that provide network security information and alerting services such as CERT http://www.cert.org/ and SANS http://www.incidents.org/
- Review security policies and operating procedures regularly to ensure they are up to date.

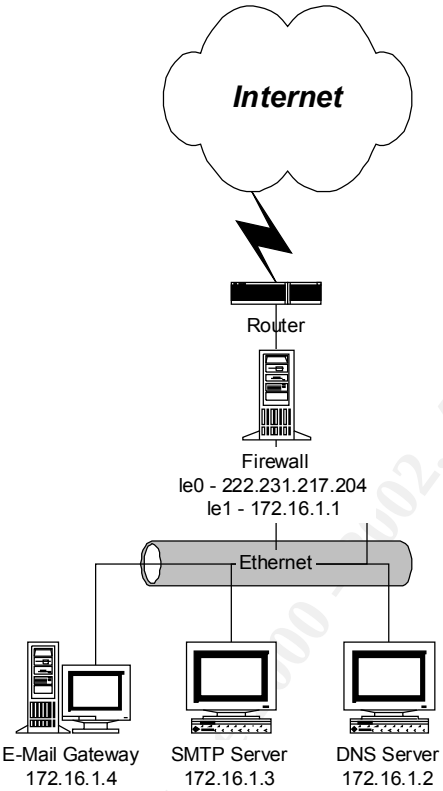
SANS Network Security 2002
Darling Harbour, Sydney, Australia
19th - 23rd January, 2002

To determine 'best practice' GIAC Enterprises policies and procedures should be compared regularly with recommendations from security organizations. These are available from several agencies and from the sites mentioned in this review.

SANS Network Security 2002
Darling Harbour, Sydney, Australia
19th - 23rd January, 2002

Assignment 4 - Design Under Fire

The following assignment was chosen
John_Folkerts.doc



Attack #1

The first attack chosen is an attack against the firewall itself. I have chosen this attac k as the site is using a device not specifically designed and built as a firewall platform. This allows the possibility of there being holes in other aspects of the host software besides the firewall itself.

John Folkerts elected to use IP Filter firewall software running on Sun Solaris V2.6 as the firewall for this site. The following vulnerabilities have been identified with the software and or hardware specified.

Vulnerability #1

The following comments were extracted from a posting to http://www.securepoint.com/
Ref: vulnerability reference

In versions of IP Firewall prior to V3.4.17
"In 10 words or less, fragment caching with can let through "any" packet.

Stephen_Monahan_GCFW.doc
SANS GIAC - Firewalls, Perimeter Protection, and VPNs
GCFW Practical Assignment version 1.6a (revised October 26, 2001)

SANS Network Security 2002
Darling Harbour, Sydney, Australia
19th - 23rd January, 2002

Ok, so that's 8."

Cause
=====
When matching a fragment, only srcip, dstip and IP ID# are checked and the fragment cache is checked *before* any rules are checked. It does not even need to be a fragment. Even if you block all fragments with a rule, fragment cache entries can be created by packets that match state information currently held.

Vulnerability #2

Sun Solaris DoS. CERT Advisory 2002 -01

Since CA-2001-31 was originally released last November, the CERT/CC has received reports of scanning for `dtspcd` (6112/tcp). Just recently, however, we have received credible reports of an exploit for Solaris systems. Using network traces provided by The Honeynet Project, we have confirmed that the `dtspcd` vulnerability identified in CA-2001-31 and discussed in VU#172583 is actively being exploited.
The Common Desktop Environment (CDE) is an integrated graphical user interface that runs on UNIX and Linux operating systems. The CDE Subprocess Control Service (`dtspcd`) is a network daemon that accepts requests from clients to execute commands and launch applications remotely. On systems running CDE, `dtspcd` is spawned by the Internet services daemon (typically `inetd` or `xinetd`) in response to a CDE client request. `dtspcd` is typically configured to run on port 6112/tcp with root privileges.
There is a remotely exploitable buffer overflow vulnerability in a shared library that is used by `dtspcd`. During client negotiation, `dtspcd` accepts a length value and subsequent data from the client without performing adequate input validation. As a result, a malicious client can manipulate data sent to `dtspcd` and cause a buffer overflow, potentially executing code with root privileges. The overflow occurs in a fixed-size 4K buffer that is exploited by the contents of one of the attack packets. The signature can be found at bytes 0x3e-0x41 in the following attack packet from a tcpdump log (lines may wrap):
Fix
VU#172583 contains information from vendors who have provided information for this advisory. We will update the vulnerability note as we receive more information. If a vendor's name does not appear, then the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Vendor information can be found in the "Systems Affected" section of VU#172583

http://www.kb.cert.org/vuls/id/172583#systems
Limit access to vulnerable service

Until patches are available and can be applied, you may wish to limit or block access to the Subprocess Control Service from untrusted networks such as the Internet. Using a firewall or other packet-filtering technology, block or restrict access to the port used by the Subprocess Control Service. As noted above, dtspcd is typically configured to listen on port 6112/tcp. It may be

possible to use TCP Wrapper or a similar technology to provide improved access control and logging functionality for dtspcd connections. Keep in mind that blocking ports at a network perimeter does not protect the vulnerable service from the internal network. It is important to understand your network configuration and service requirements before deciding what changes are appropriate.

TCP Wrapper is available from ftp://ftp.porcupine.org/pub/security/index.html

Disable vulnerable service

You may wish to consider disabling dtspcd by commenting out the appropriate entry in /etc/inetd.conf. As a best practice, the CERT/CC recommends disabling any services that are not explicitly required. As noted above, it is important to consider the consequences of such a change in your environment.

Ref:http://www.cert.org/advisories/CA-2002-01.html

Vulnerability #3

Ref: BUGTRAQ

The following comments were extracted from the BugTraq bulletin board at www.securepoint.com.

"Hi,
A while ago I noticed nmap V2.08 with OS fingerprinting (the -O option) could cause solaris kernel panic. The trick is this:

Select an active port to do an OS fingerprint. Kill the server after doing a fingerprint. Solaris will kernel panic. It doesn't matter what server you choose or whether or not it's on a priviledged port. However, it must be TCP.

The attack is troublesome because of the time differential between the fingerprint and the kernel panic. You probably won't think twice about the scan when the server dies and causes panic.

Tested on Solaris 2.6 using a simple listen/accept server, as well as with sendmail 8.9.3.

I worked with Sun a while ago on this problem, and they have released patch 105529-07 (for sparc) and 105530 (for x86). According to the patch readme, the problem is with a recursive mutex_enter on the TCP streams driver.

If you use nmap to scan your own network, use the -sT option to do vanilla connect()'s so you don't kill your own servers :)"

Selected attack design

In order to attack the design of John Folkerts I have selected vulnerability #3 as listed above. This attack could be mounted internally or externally of the network.

To implement the attack I would use the NMAP utility from a device on the external network (Internet). This enables me to better hide my identity and would less likely be noticed amongst other Internet traffic to the web site.

The following NMAP command would be used.

Nmap –sS –O –Sxxx.xxx.xxx.xxx 222.231.217.204

This command achieves the following
-sS – TCP SYN scan. This will scan for open ports with a SYN request only
-O - Remote host identification
-Sxxx.xxx.xxx.xxx – Spoof source address to a legitimate internet address
222.231.217.204 – IP address for the firewall
All well known ports will be tested.

Results

I am unable to test this in practice but a test would determine the following

- If relevant patches have not be applied the host may die thus achieving a denial of service
- Whether the host been updated with the relevant patches to fix the vulnerability.
- What ports are active. This would indicate other ports for opportunities for attack.

Attack #2

Compromise of an Internal system

For attack 2 I have chosen to attack the SMTP server behind the firewall. SMTP is considered weak in security terms and on the premise that I can compromise the firewall through attack #1 I then have access to all hosts behind the firewall. As the hosts behind the firewall are using private addresses this presents a problem.
To determine the addresses of the internal hosts I would run an NMAP scan from the firewall server and scan all private address ranges.
Nmap –sS –v -p25 –Sxxx.xxx.xxx.xxx 10.*.*.*
Nmap –sS -v –p25 –Sxxx.xxx.xxx.xxx 172.16.*.*
Nmap –sS-v –p25 –Sxxx.xxx.xxx.xxx 192.168.*.*
Nmap –sS v –p25 –Sxxx.xxx.xxx.xxx 224.*.*.*

A stealth SYN scan of port 25 on all private addresses using a spoofed network address. To avoid detection through log analysis, multiple spoofed source addresses can be used by creating a list file to contain the spoofed addresses. As we are past the firewall and are only scanning 1 port, it is unlikely that the SYN scan will be detected.
This scan should identify the active hosts and any active smtp ports on the GIAC site.

Once the SMTP server is identified (there is a mail gateway at 172.16.1.4 and the smtp server at 172.16.1.3) I could then attempt to compromise them.

The first task in compro mising the server is to determine the hardware and software the server is running on. To do this I would use NMAP to determine the platform.
Nmap –sS –O –Sxxx.xxx.xxx.xxx 172.16.1.3

This command achieves the following
-sS – TCP SYN scan. This will scan f or open ports with a SYN request only
-O - Remote host identification
-Sxxx.xxx.xxx.xxx – Spoof source address to a legitimate internet address
172.16.1.3 – IP address for the smtp server
All well known ports will be tested.

Results

There are many docume nted vulnerabilities for SMTP.
The following link provides a list of many of the vulnerabilities.
http://www.cve.mitre.org/cgi-bin/cvekey.cgi?keyword=smtp
Without knowing the exact platform in the example network I can only theorise on an exploit. Below are vulnerability references for two common platforms. The third example is a description of an exploit for an attack on the Cmail platform.

Windows 2000 SMTP vulnerability
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0504

Vulnerability in authentication process for SMTP service in Microsoft Windows 2000 allows remote attackers to use incor rect credentials to gain privileges and conduct activites such as mail relaying.

Lotus Domino
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1047

Buffer overflow in SMTP service of Lotus Domino 5.0.4 and earlier allows remote attackers to cause a denial of service and possibly execute arbitrary commands via a long ENVID keyword in the "MAIL FROM" command.

Below is an example exploit for Cmail. This vulnerability is posted at
http://lists.insecure.org/win2ksecadvice/1999/Oct/0028.html

To execute this exploit I first telnet to port 25

```
$ telnet 172.16.1.3 25
Trying 172.16.1.3...
Connected to 172.16.1.3
Escape character is '^]'.
220 SMTP services ready. Computalynx CMail Server Version: 2.4
```

I then connect to the server using the helo command

helo ussr
250 Hello ussr [yourip], how are you today?

I now create a mail header with a subject line greater than the buffer allows for.
MAIL FROM: cmail <[buffer]@cmaildotcom.com>

Where [buffer] is approximately 7090 characters. At his point the server overflows and crashes.

While the above are attacks specific to the SMTP software, a simpler attack would be a denial of service on the SMTP server itself. This can be easily achieved by bombarding the server with session requests or simply a ping of death attack.

This can be achieved using NMAP with TCP scans or via the ping command
'Ping 172.16.1.3 –l65000 172.16.1.3'

Summary

The weakness in the chosen network is clearly the firewall. To improve the protection on the site an Intrusion Detection System could be placed between the firewall and the services segment. This would (hopefully) pick up SYN and other type attacks. My personal preference is to not use a common platform such as a Unix host to run the firewall service. If Unix must be used, it should be stripped down as much as possible to remove any services not required. Even the kernel should be lean and mean.
A further option is to remove sensitive servers and information away onto another segment that is protected by another separate router. Further filtering and detection services on this router could prevent the scenario above .

---------- 000----------