# Global Information Assurance Certification Paper

# SANS GIAC 2001
# (Sydney)

# Firewall and Perimeter Protection

## Practical Assignment

*By*


## Gordon Crease

# Firewall and Perimeter Protection

*by*

**Gordon Crease**

**1.1 Introduction to the GIAC Business** 3

**1.2 Access to the Network and Applications** 4

**2.1 Password Policy** 7

**2.2 Information Policy** 7

**2.3 IPSec Policy** 7

**2.4 The Border Router** 8

**2.4.1 Access Control Lists** 8

**2.4.2. Internet facing interface** 9

**2.4.3 Internal Network facing interface** 10

**2.4.4. VPN router facing interface** 10

**2.4.5 Rule ordering** 11

**2.4.6 ACL Rule Testing** 11

**2.4.7 Router Armoring** 11

**2.5 Firewall Policy** 12

**3.2 The Network Assessment** 17

**3.2.1 Gathering the information** 17

**3.2.2 Scanning the System** 18

**4.1 Introduction** 21

**4.2 Firewall Attack** 22

**4.3 Denial of Service Attack** 22

**4.4 Internal System Attack** 24

**References** **26**

***Assignment 1 – Security Architecture***

*Define a security architecture for GIAC Enterprises, a growing Internet start-up 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, VPN's to partners, secure remote access and internal firewalls. Be explicit about the brand and version of each perimeter defence component. Produce a diagram 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 saying that connect to supply fortunes)*
- *Partners (the international partners that translate and resell fortunes)*

## 1.1 Introduction to the GIAC Business

The nature of the GIAC business is to sell fortune cookie sayings to two categories; general customers, and resellers (partners). Both groups will have developed a trust relationship with GIAC before transactions can take place.

Sales and queries are dealt with via Web generated forms. For the receipt (from suppliers) and distribution (to customers) of the bulk cookie product, an FTP server is used. One of the most important aspects of the operation is to ensure that the 'sayings' can not be seen by anyone other than members of the GIAC family therefore, no content other than samples will be stored on the Web server. Customers and Partners who buy complete packages relating to specific subjects will obtain their product from the FTP server. To keep costs to a minimum in the initial stages of the business deployment, Web and Internet technologies will be adopted wherever possible.

Even though an annual return of hundreds of millions of dollars is anticipated, costs will be kept to a minimum by the use of some open source software (of a high quality). Redundancy of network elements and applications will be addressed in the second year when finances permit.

A partnership has been formed with an advertising agency that will need to have access to customer details to promote upcoming products. They will also be instrumental in increasing the customer base by promoting the latest GIAC fortune cookie saying products to the world market. Therefore, they will be provided with access to the Customer records.

## 1.2 Access to the Network and Applications

The four primary groups needing access to various areas within the corporation are;

- Customers – who will need access to the Web server(s) to view company details and advertising, along with a product listing of fortune cookie saying packages that are available for purchase (no actual product is shown, only classifications and samples). Access to the FTP server will also be necessary for acquisition of the selected fortuned cookie packages once an order has been submitted and processed.
- Partners – who will need restricted access to the internal company network elements where customer details are stored.
- Suppliers – who will need access to the Web server(s) to check existing product lines, and will need to upload their product to the FTP server.
- External Staff – Depending upon the level of authorisation, will need access to most of the Internal network for out-of-band support purposes.
- Internal Staff – Access to the Internal network for administrative and support duties (depending upon authorisation levels) along with Internet access.

Customers and Supply companies that wish to deal with GIAC are provided with an IPSec Client (Nortel) compatible with the IPSec switch/router (Nortel 2500 CES) used by GIAC. They also receive username/password pairs that will provide identification, authentication and authorisation. Each customer and supplier will also have an account number that will be used for administrative purposes. Web server access can be achieved via a standard Internet browser and standard TCP/IP traffic over the Internet.

Partner(s) have a compatible IPSec router at the access point to their network(s). This VPN will allow GIAC and Partners to share network functionality. Username/Password pairs are used for identification, authentication and authorisation. The IPSec tunnel is to provide encryption for the communications traffic and therefore Encryption Security Payload (ESP) is used. This

External Staff have IPSec Clients that will allow them secure access to the network. Identification and Authentication is provided by username and password respectively.

## 1.3 The Network

See Figure 1 below for the network architecture

The GIAC network is divided into several areas that are 'protected' and isolated by the use of firewalls A and B. All external traffic is first passed and filtered by the border router. All ESP IPSec traffic is passed to the VPN router for decryption and initial filtering.
Acceptable TCP/IP Internet traffic (Web and mail) is passed from the border router to firewall A where a second set of filtering rules is applied. This particular traffic will pass to and from the Service Network only

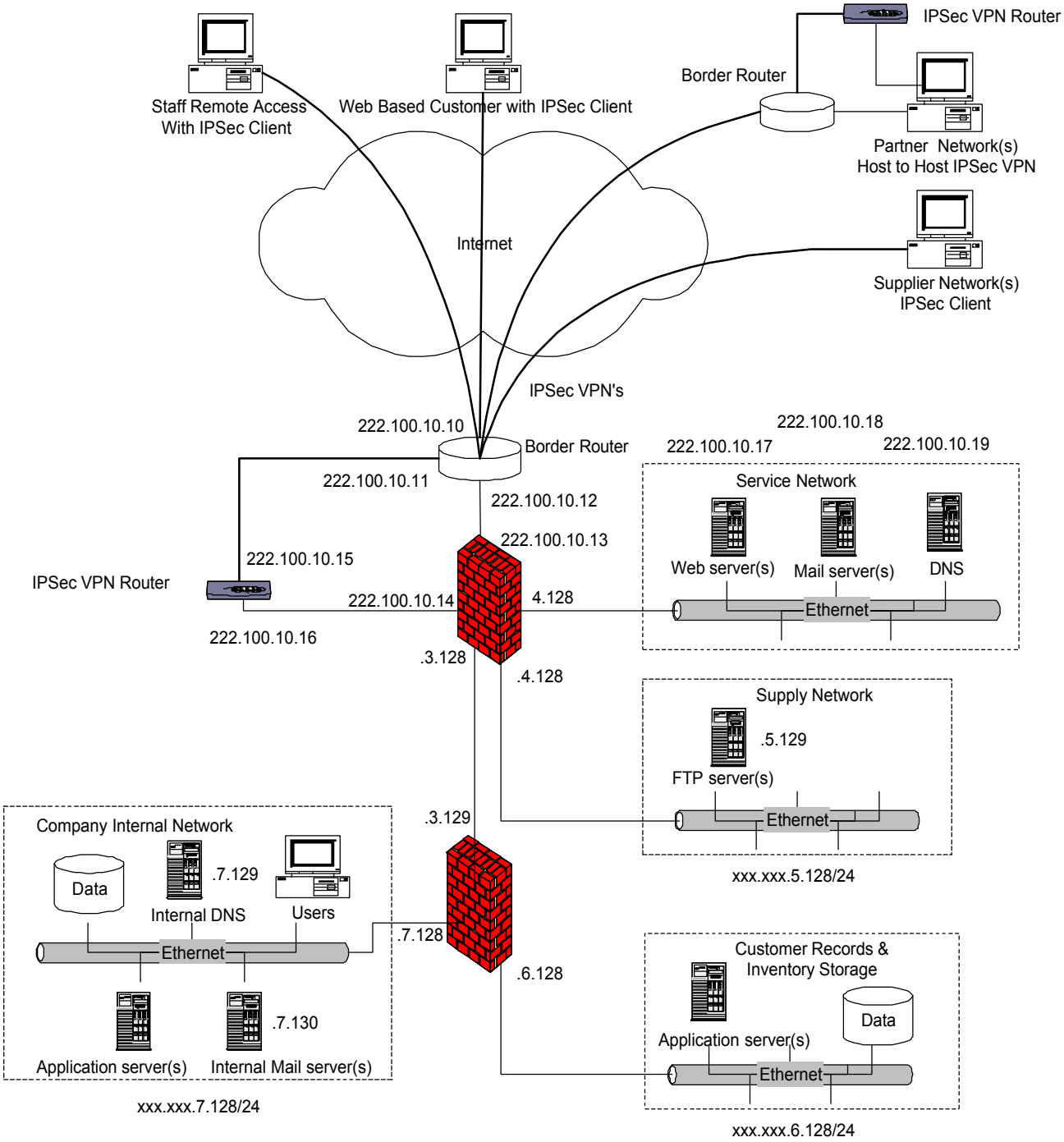
The Contivity Extranet Switch terminates the VPN's, authenticates the users, and decodes the IPSec packets. It then passes packets to Firewall A, which filters all traffic through its interfaces, and protects the necessary parts of the GIAC network. IPSec VPN users will be Customers and Suppliers who access the FTP server, Partners connecting to the application server in the Records area (where they will need to log on), and External staff to all parts of the Internal network.

Firewall B is used to partition the internal network functionality, and allows for the logging of actions. This Firewall will filter traffic from Partners to the Records area where customer records are kept, and the External Staff to any part of the internal network. No other external soured traffic will pass this firewall.

Although it is often preferred that different firewalls be used within an organisation so that possible configuration errors may be caught at different levels, the GIAC organisation is using a single firewall vendor for ease of management. Firewalls A and B are Gauntlet firewalls, version 5.5 from Network Associates running on greater than 'recommended requirements (For Sun Solaris 8 1/01 operating system, UltraSPARC with 256 MB of RAM, 2x10 GB of disk space).

The border router is a Cisco 3600 series which is a mid-range device that lies within the present company requirements for size and price. The device runs Cisco's Internet Operating System (IOS) 12.0(7). This version of IOS has a vulnerable to crashing if scanned for vulnerabilities. However, this is not known to happen on the 3600 series (http://www.para-protect.com/advisories/2000/Para-Cert-00-06-08.pdf, Para-CERT Advisory 00-06-08).

**Figure 1**. *GIAC Enterprise Network Architecture*



***Assignment 2 – Security Policy***

*Based on the security architecture that you defined in Assignment 1, provide a security policy for AT LEAST the following three components:*

- *Border Router*
- *Primary Firewall*
- *VPN*

## 2.1 Password Policy

Passwords have been selected that have the following format:

- 8 characters long
- consist of alphanumeric characters (including at least one capital letter and two numeric characters)
- Do not use dictionary words.
- Passwords are to be changed regularly (at least every 90 days)
- Passwords were sent to the mail address of the applicant after a prescribed check was performed on the application data.
- Applications have password lock-out to limit the possibility of password guessing attacks

A set of policies and procedures have been developed by the IT team to ensure that username/password management is kept current.

## 2.2 Information Policy

- All data stored on the Customer Records and Information Storage database will be encrypted. Only GIAC staff and Partners will have access to this data. This will provide a level of protection and privacy.
- Data stored on the FTP server will be encrypted (from suppliers and to customers). [This is due to the possible vulnerability of FTP protocols]
- Tape backups of all data will be performed routinely as part of daily business functions.
- Checks on the ability to restore data (and the storage medium) will be performed at regular intervals.
- Logs from Web server(s) and Mail server(s) will be checked periodically
- Logs from the FTP server will be checked daily

## 2.3 IPSec Policy

IPSec will be used to add a level of security to the majority of the trusted

communications by adding encryption to the traffic. Therefore, Encapsulation Security Payload (ESP) IPSec will be used with 56 bit DES symmetric encryption. This will allow acceptable protection of the data being transmitted while also allowing for the international restrictions.

Since the majority of the GIAC important communications will be done over IPSec tunnels, the Nortel Contivity Extranet Switch (CES) series 2600 will be used to support up to 1000 consecutive sessions. This is expected to be more than enough connectivity, and will allow for growth. Username/Password authentication will be used until a suitable public key policy can be determined. [The use of digital certificates is envisioned for future use. This will require the development of an internal Certificate Authority and associated management policies. The certificates can then be issued to trusted users]. The CES can be configured to accept passwords originally, and then certificates later.

Although the Firewall chosen as the primary protection for the company network has IPSec VPN capabilities, it was believed that the use of a separate, dedicated VPN connector would be preferable. Filtering rules can be applied in detail at the CES that will add to the security of the communications processes, and authentication can be achieved using the internal LDAP of the unit. The CES also responds to VPN and ping traffic only. Similarly there will be no added loading placed on the firewall due to encryption requirements. Access to internal systems can be limited to particular network addressess, individual user, and the packet type. This will be necessary since external staff will need radically different needs than will customers and suppliers, or even partners.

## 2.4 The Border Router

All traffic will be implicitly denied since an access control list is being applied to each of the router interfaces. Therefore, it will be necessary to explicitly permit the communications traffic that is allowed into the network. The GIAC company communications are deliberately restricted and therefore it is more effective to explicitly specify the acceptable protocols. All unacceptable packets are dropped at the each of the interfaces as they enter the router so that no unnecessary processing need be done.

### ***2.4.1 Access Control Lists***

Only logging of unwanted traffic will be done at the router (not to overtax the system). The firewall will be used to log **all** events.

All unnecessary services have been disabled as part of the original configuration of the unit.

An extended ACL is being used so that protocols and port numbers can be

specified.

**[Note**: The established extension is not being used due to its possible opening of risks to the network]

### ***2.4.2. Internet facing interface***

```
Interface Serial 0
        ip address 222.100.10.10
        ip access-group 101 in

# Stop the possibility of address spoofing of known private addresses
# (including the GIAC internal address ranges)

        access-list 101 deny IP 10.0.0.0 0.255.255.255 any log
        access-list 101 deny IP 172.16.0.0 0.0.255.255 any log
        access-list 101 deny IP 192.168.0.0 0.0.255.255 any log

# Stop the possibility of broadcast, multicast and inappropriate addresses
# usage such as loopback and the zero address range

        access-list 101 deny IP 255.255.255.255 0.255.255.255 any log
        access-list 101 deny IP 0.0.0.0 0.255.255.255 any log
        access-list 101 deny IP 127.0.0.1 0.0.0.0 any log
        access-list 101 deny IP 224.0.0.0 15.255.255.255.255 any log

# ESP IPSec (protocol number 50) must be allowed through the router. This
# could come from any external address as support staff and customers will
# most probably have dynamically assigned addresses supplied by ISP's
#Partner public addresses will be known and used by the firewalls for
filtering.

        access-list 101 permit 50 any 222.100.10.16 gt 1023

# Allow Web (HTTP – port 80 and 443 only) and mail (SMTP – port 25 only)
# access from anywhere to the Service Network

        access-list 101 permit TCP any gt 1023 host 222.100.10.17 eq 80
        access-list 101 permit TCP any gt 1023 host 222.100.10.17 eq 443
        access-list 101 permit TCP any gt 1023 host 222.100.10.18 eq 25


# Permit return Web requests from the Internal Company Network

        access-list 101 permit TCP any 80 1023 192.168.0.0 0.0.255.255 gt
        1023
        access-list 101 permit TCP any 443 1023 192.168.0.0 0.0.255.255 gt
        1023
```

*# Permit DNS (UDP on port 53) queries to the primary nameserver resident in*
*# in the GIAC service network and responses from external servers*

```
access-list 101 permit UDP any gt 1023 host 222.100.10.19 eq 53
access-list 101 permit UDP any 53 host 222.100.10.19 gt 1023
```

*# Enable the IPSec data channel (UDP on port 500)*

```
access-list 101 permit UDP any host 222.100.10.15 eq 500
```

*# Block all other traffic, and log – this must be the last entry in ACL 101*
*# otherwise no packets will pass the router.*

```
access-list 101 deny IP any any log
```

### *2.4.3 Internal Network facing interface*

The access control lists for this interface will determine what traffic is allowed to leave the GIAC network

```
Interface Ethernet 0
    ip address 222.100.10.12
    ip access-group 102 in
```

*# Allow outgoing mail, and Web enquiries from the Company Internal Network*

```
access-list 102 permit TCP 192.168.7.128 0.0.0.255 gt 1023 any eq 80
access-list 102 permit TCP 192.168.7.128 0.0.0.255 gt 1023 any eq 443
access-list 102 permit TCP 192.168.7.128 0.0.0.255 gt 1023 any eq 25
```

*# Allow outgoing DNS replies from the Service Network*

```
access-list 102 permit UDP host 222.100.10.19 eq 53 any
```

*# Stop all other traffic, and log*

```
access-list 102 deny IP any any log
```

### *2.4.4. VPN router facing interface*

There should only be IPSec traffic passing across this interface.

```
Interface Ethernet 1
        ip address 222.100.10.11
        ip access-group 103 in

# Allow IPSec packets from the VPN switch to any external address

        access-list 103 permit 50 host 222.100.10.15 any
        access-list 103 permit UDP host 222.100.10.15 eq 500 any
        access-list 103 deny IP any any log

Interface Ethernet 1
        ip address 222.100.10.11
        ip access-group 104 out

# Allow IPSec packets to the VPN switch from anywhere

        access-list 104 permit 50 any host 222.100.10.15
        access-list 104 permit UDP any host 222.100.10.15 eq 500
        access-list 104 deny IP any any log
```

### *2.4.5 Rule ordering*

The precise nature of the access control lists, in terms of the packets that are passed, has limited the need for ordering. However, it is sensible to immediately drop unwanted packets that come from unacceptable IP addresses. Also, the ACL command “deny all IP from any to any” must be the last entry for each interfaced. If this is not done, then some important communication packets may be lost.

### *2.4.6 ACL Rule Testing*

The best way to test if the ACL’s are performing the expected tasks is to place a source on each of the interfaces in turn, and then perform a scan of a host placed on the other side of the router. The host would ‘sniff’ all received packets and the logs could be examined for correctness.
For this test if would be best to try all types of packets (UDP, TCP, ICMP) and all unacceptable address ranges.

### *2.4.7 Router Armoring*

There is a need to armor the router. This is done by applying routing rules that drop all source routing, adding rules that disable services such as echo, discard, chargen, and disabling servers. Thus the following rules are globally applied to the router so that they affect all interfaces.

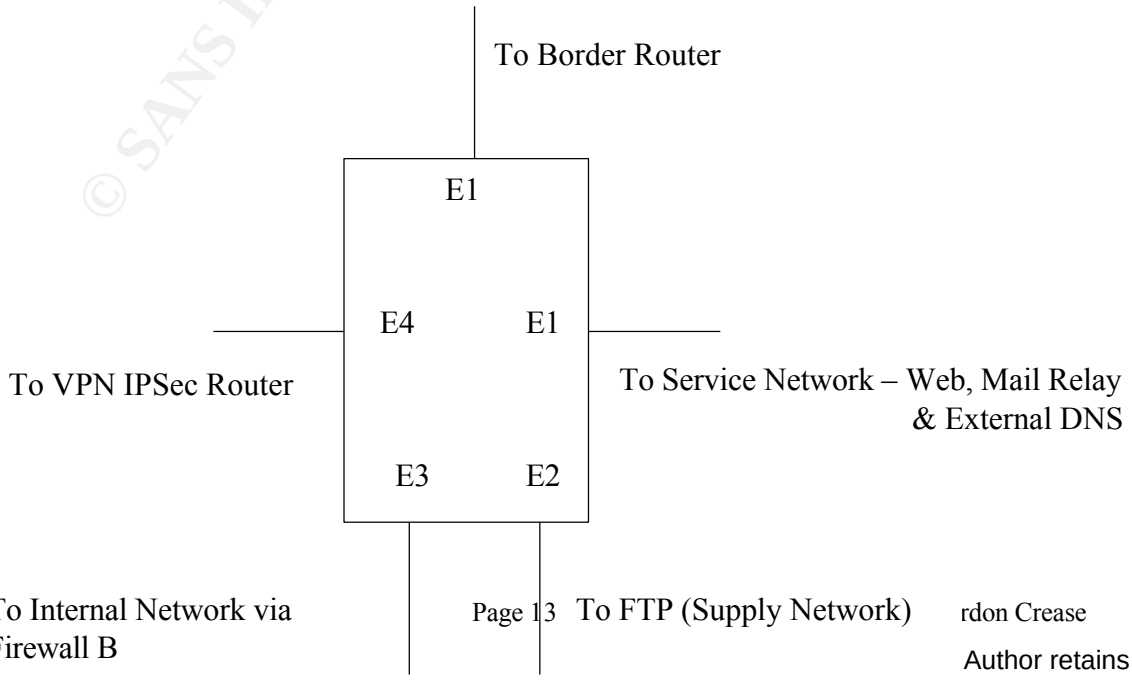
No ip source routing
No service tcp-small-servers
No service udp-small-servers
No service finger
No ip http
No ip bootp
No ip direct broadcast # limits 'smurf' amplification
No ip unreachables # stops ICMP 'unreachable messages'

## 2.5 Firewall Policy

The company policy regarding the firewall has the following directives

- Firewall will reside on 'hardened' operating platforms that have been cleansed of default userid/passwords.
- Images of all configurations and policies will be kept in the possibility that a swift rebuild is required.
- Copies of all software will be kept on site and in a remote location.
- Logs will be checked regular and frequently. Logs will be sufficiently complete allow them to be used as an adjunct to improving security through out the GIAC network.
- Track all access attempts.
- The application of patches for the operating system will be applied as early as is feasible within the business requirements.
- Anti-virus software will be applied to all relevant traffic, and will be updated regularly.
- Management of the firewall will be by authorised staff only.
- Firewall rules will be reviewed regularly in relation to the changing business environment.
- All firewall configuration changes will be done via the local console, except in an emergency.

**Figure 2**. *Interfaces on the Primary Gauntlet Firewall*



The Gauntlet firewall allows for the filtering of packets entering each interface. These are 'named' at the install process. The premise used in determining firewall rules is that any packet not expressly permitted is denied.
The interfaces are as per the Figure 2, and the rules are applied as shown in the table below.

The Action options are:

'FWR' – Forward with reply (this sets up an automatic return rule)
'FWTR' – Forward packet without reply (no return rule)
'ABS' – Absorb traffic (the packet is processed at the firewall proxy)
'DNY' – Drops the packet without notifying the sender (logs the action)

NOTE: (a) '*' denotes a wildcard that matches all possible entries.
(b) logging will be performed on all applied rules.

| No | Int | Protocol | Action | Source | Port | Destination | Port |
|---|---|---|---|---|---|---|---|
| 1 | E0 | HTTP | FWR | * | * | 222.100.10.17 255.255.255.255 | 80 |
| 2 | E0 | HTTPS | FWR | * | * | 222.100.10.17 255.255.255.255 | 443 |
| 3 | E0 | SMTP | FWR | * | * | 222.100.10.18 255.255.255.255 | 25 |
| 4 | E0 | UDP | FWR | * | * | 222.100.10.19 255.255.255.255 | 53 |
| 5 | E0 | * | DNY | * | * | 222.100.10.13 255.255.255.255 | * |
| 6 | E0 | * | DNY | * | * | * | * |
| | | | | | | | |
| 7 | E1 | HTTP | FWR | 222.100.10.17 255.255.255.255 | * | * | 80 |
| 8 | E1 | HTTPS | FWR | 222.100.10.17 255.255.255.255 | * | * | 443 |
| 9 | E1 | SMTP | FWR | 222.100.10.18 255.255.255.255 | * | * | 25 |
| 10 | E1 | UDP | FWR | 222.100.10.19 255.255.255.255 | * | * | 53 |
| 11 | E1 | ICMP | FWR | Service Network | * | Company Internal Network | * |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 12 | E1 | * | DNY | * | * | 192.168.4.128 255.255.255.255 | * |
| 13 | E1 | * | DNY | * | * | * | * |
| | | | | | | | |
| 14 | E2 | FTP | FWR | Supply Network | Gt 1023 | * | 22 |
| 15 | E2 | ICMP | FWTR | Supply Network | * | Company Internal Network | * |
| 16 | E2 | * | DNY | * | * | 192.168.4.128 255.255.255.255 | * |
| 17 | E2 | * | DNY | * | * | * | * |
| | | | | | | | |
| 18 | E3 | HTTP | FWR | Company Internal Network | Gt 1023 | * | 80 |
| 19 | E3 | HTTPS | FWR | Company Internal Network | Gt 1023 | * | 443 |
| 20 | E3 | UDP | FWR | 192.168.7.129 255.255.255.255 | Gt 1023 | 222.100.10.19 255.255.255.255 | 53 |
| 21 | E3 | ICMP | FWR | Company Internal Network | * | Service Network | * |
| 22 | E3 | ICMP | FWR | Company Internal Network | * | Supply Network | * |
| 23 | E3 | ICMP | FWR | Company Internal Network | * | Customer Records Network | * |
| 24 | E3 | ICMP | FWR | Company Internal Network | * | 222.100.10.16 255.255.255.255 | * |
| 25 | E3 | ICMP | FWR | Company Internal Network | * | 222.100.10.12 255.255.255.255 | * |
| 26 | E3 | SMTP | FWR | 192.168.7.130 255.255.255.255 | Gt 1023 | 222.100.10.18 255.255.255.255 | 25 |
| 27 | E3 | FTP | FWR | Company Internal Network | Gt 1023 | Supply Network | 21 |
| 28 | E3 | * | DNY | * | * | 192.168.3.128 255.255.255.255 | * |
| 29 | E3 | * | DNY | * | * | * | * |
| | | | | | | | |
| 30 | E4 | HTTP | FWR | * | * | 222.100.10.17 255.255.255.255 | 80 |
| 31 | E4 | HTTPS | FWR | * | * | 222.100.10.17 255.255.255.255 | 443 |
| 32 | E4 | SMTP | FWR | * | * | 222.100.10.18 255.255.255.255 | 25 |
| 33 | E4 | UDP | FWR | * | * | 222.100.10.19 255.255.255.255 | 53 |
| 34 | E4 | FTP | FWR | * | Gt 1023 | Supply Network | 21 |
| 35 | E4 | ICMP | FWR | * | * | Service Network | * |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 36 | E4 | ICMP | FWR | * | * | Supply Network | * |
| 37 | E4 | ICMP | FWR | * | * | Customer Records Network | * |
| 38 | E4 | ICMP | FWR | * | * | Company Internal Network | * |
| 39 | E4 | TCP | FWR | * | * | Customer Records Network | * |
| 40 | E4 | TCP | FWR | * | * | Company Internal Network | * |
| 41 | E4 | * | DNY | * | * | 222.100.10.14 255.255.255.255 | * |
| 42 | E4 | * | DNY | * | * | * | * |
| | | | | | | | |

The firewall rules are designed to permit only the acceptable traffic through each of the five interfaces. Interface E0 allows packets to pass to the Service Network only, but from any Internet address. The protocols for Web access (HTTP and HTTPS are enabled to pass to the Web server address on the relative ports (80 and 443). Mail (SMTP) is enabled if the packets are going to the Mail server address only, on port 25. There is also the enabling of DNS requests to the GIAC's External DNS server, on port 53 using the UDP protocol.

Interface E1 has rules applied to only allow the return traffic from the Web server, Mail server and DNS server in the Service Network. However, destination addresses can be anywhere on the Internet, as well as the Company Internal Network.

The FTP protocol is the only application protocol needed to pass through the E2 Interface. This will consist of the reverse data channel request once the user client has established a connection. Thus, the destination port number can be determined to be 22. [If client software supports Passive FTP, then a new rule will need to be created, or GIAC may require customers and suppliers to use standard FTP]

E3 must allow outbound traffic from the Company Internal Network and from the Customer Records Network. This traffic includes access to the Internet, access to the Internal Web server, the Mail relay, and the DNS External Mail server. There is also a need to be able to upload and download files to the FTP server as a core function of the organisation.
This interface must also allow support staff access to the ping utility as a tool for checking the state of the network. Therefore, ICMP traffic is permitted to the Service Network, Supply Network, the Customer Records Network, the VPN router and Bourder router interfaces.
The final need is to allow DNS UDP requests from the Company Internal Network to the External DNS in the Service Network.

The final firewall interface is E4 which filters the VPN traffic passed from the Contivity Extranet Switch. The rules allow access to the Service Network elements, the Supply Network for the uploading and downloading of files at the FTP server, and ICMP packets for remote management needs by support staff. There is also TCP traffic allowed into the Company Internal Network and Customer Records Network, and filtering of this traffic is performed by Firewall 2. At this point, separation of Staff and Partner needs is achieved.

All interfaces have an explicit deny added that drops packets directed at the interface address, along with an explicit deny for all other packets. These rules are placed at the end of each interface list so that incoming packets are initially checked against permit actions, and if they are not acceptable, then they are dropped.

***Assignment 3- Audit Your Security Architecture***

*You have been assigned to provide technical support for a comprehensive information system audit for GIAC Enterprises. You are required to audit the primary Firewall described in Assignments 1 and 2. Your assignment is to:*

1. *Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.*
2. *Implement the assessment. Validate that the Primary Firewall is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.*
3. *Conduct a perimeter analysis. Based on your assessment (and referring to data from you r assessment), analyse the perimeter defence and make recommendation for improvements or alternative architectures. Diagrams are strongly recommended for this part of the assignment.*

## 3.1 Introduction

The aim of the audit is to collect information relating to the state of the network and to determine if the results lie within the policies dictated by the organisation. A first step is to obtain copies of the anticipated policies that are being applied (in this case, they will refer to parts of Assignment I and 2 in this document).. The audit is looking for compliance to stated rules and is not a penetration test where an attempt is made to 'hack' the system.

When performing an external security audit of a system it is essential to obtain written permission from all responsible parties. This will mitigate any problems that may arise from the processes undertaken in the audit, and will ensure some level of support from administrators or managers of the network. Poor configuration of network elements can have unexpected outcomes when scanning tools are used. It is important to ensure that the

resources are available (backups, images, staff) for rapid restoration of critical systems.

There are steps that can be followed in order to assess the network perimeter. These should be performed in an order suitable to the situation and availability of staff and equipment.

- Determine the security policies that apply to the organisation.
  - Firewall(s) and Router(s) rule-sets and management methodologies
  - Access permissions and management – password policies and authorisation levels
  - Information Security
  - Staff requirements – zonin
- Gather information that will indicate the layout of the network to be assessed
  - Determine IP addresses and interconnectivity
  - All network elements – host names
- Prepare a detailed “plan-of-attack”
    - Examine documented rule-sets and compare to security policies
    - Determine what tools will be used and in what format
    - Determine at which hosts the scanning tools be directed?
- Ensure that the necessary tools and resources are available when and where required
  - Provide for access to all available logs
  - Find the most acceptable access points
  - Check the source tools are correctly configured
- Ensure the cooperation of strategic members of the organisation
  - Make everyone aware that an assessment is to take place
  - Determine with the organisation the most acceptable time to perform the assessment.
    - Recommended times would be outside business hours for invasive or bandwidth intensive tests, or where security elements are accessed.
    - Assessment times must be flexible and work around daily business activities.
  - Ensure that there is an understanding of the conclusions and recommendations that may come about from the assessment
- Prepare for contingencies that may arise out of the assessment
  - Check for the existence of backups and configuration images
  - Ensure that accidental damage can be swiftly repaired
  - Have insurance
- Perform the physical assessment
  - Check the physical security of all network elements.
  - Access routers and Firewall(s) and gain a copy of configurations and rule sets – compare these to expected.
  - Perform planned scans
  - Examine Operating Platform configurations

Perimeter Assessment costs can run from a few thousand dollars to many tens of thousands. For an assessment of the GIAC perimeter, the audit team (two people) is charging $3000 per day. It is expected to take approximately two days to determine the requirements and collect and understand network details; one day to confirm a mapping of the network, perform scans and collect data; and two days to complete the assessment. A final day is allocated to presenting the findings and consulting with the key people. This totals to seven days, with a price tag of $21000.

## 3.2 The Network Assessment

### ***3.2.1 Gathering the information***

If the audit team is taking on the role of an *informed insider*, then the network administrators will most probably supply network diagrams and host information. However if they are *uninformed outsiders*, then some network mapping will be necessary. Taking on the role of the outsider can help determine how simply any would-be hacker could map the organisations network and from there, develop an attack strategy.

Any supplied network information can be verified using 'traceroute" (or tracert) and "ping" utilities. Ping will verify that a host is present, and various tracerout switches can be employed to determine the number of hops to the specified hosts, and also do reverse lookups and supply host names.

Another source of information on the system is the InterNIC which can be queried using the 'whois' command. This will provide the registered domain name of the organisation as well as organisational specific information such as administrative contacts (this can be useful to socially engineer more information if a penetration test was anticipated). An IP address for a subnet on the domain plus the domain name servers is also supplied.

Armed with this information, the nslookup (or DIG – domain name groper) command can be used to query the organisations nameserver. If zone transfers are possible, the 'ls –d' command and switch for the hosts.lst file will provide the names and addresses of the listed hosts.
[If this is possible, then there is an immediate breach of oraganisational policy as zone transfers should be limited to specific hosts].

Email sources can also be a wealth of information. Headers can be examined to elicit information on possible mail gateways within the organisation. With the organisations domain name know (or through educated guessing), bogus email addresses can be sent that return a 'mail undelivered' message. This may contain useful information.

### ***3.2.2 Scanning the System***

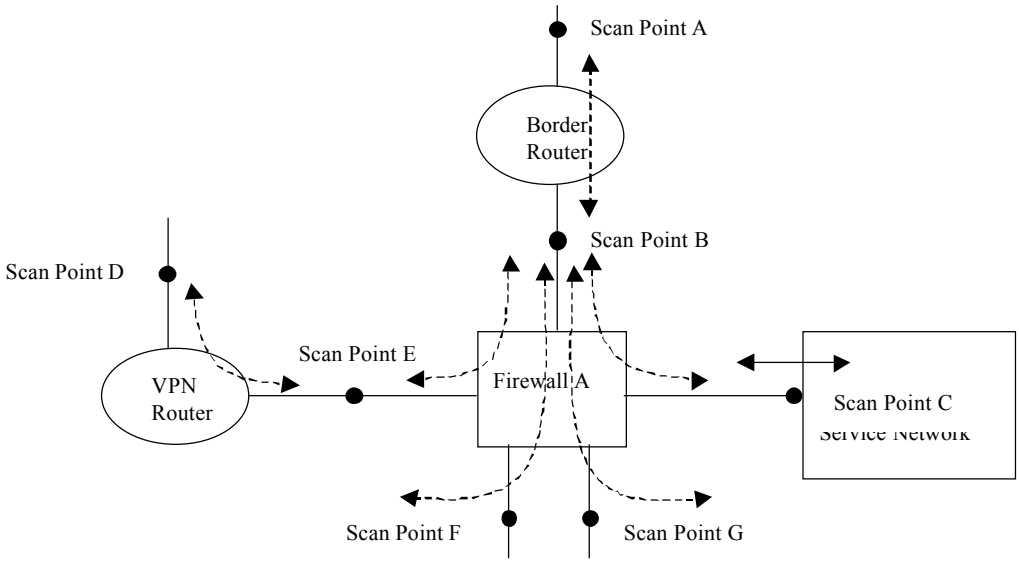
Once a network map has been acquired and verified (by whatever means), it will then be necessary to scan the hosts with the chosen toolset. There are a plethora of commercial and freeware tools available for the job. A simple and easily accessible tool is Nmap. Nevertheless, whatever tool is chosen, the aim behind its use is to search for open (or listening) ports, which will indicate the services that are running. Additional, useful information will come in the form of operation system fingerprinting. Information sources should be examined later to see if the information output could be limited as it can aid possible attackers.

For this assignment, we only need to assess the perimeter. This is effectively the Screening router (or border router), the Primary firewall, and the VPN router. Together, these units form the hard shell around the network, and if any of these are penetrated then some of the soft core is exposed.

For these units, there are two primary factors that must be checked, the Operating System and its configuration, and the actual rule-sets that have been activated. The aim must then be to discover if there are vulnerabilities that can be exploited, and then to 'fix' them.

There are many points within and external to the GIAC network that should be sourced in order to test all security rules. The places the audit team will investigate for possible Scan Points are shown in Figure 2 below.

**Figure 2**. *Possible Scanning Points for the GIAC Organisation Audit*



Unfortunately, not all points will have connectivity for the team's portable toolset. Thus full auditing of the system will be more difficult. It would require the network to be unused to be able to add hubs for Scan Points B, D,E, and possibly F. For this audit there is only the external Scanning Point A, C and F from where the our tools can be directed at the known addresses. With all the scans, the team is aiming to find the open ports on the target systems and thus an indication of the probable services that might be running.

The audit team will first run tests from Scanning Point A. From this point, Nmap scans were aimed at the IP addresses 222.100.10.10, 222.100.10.11 and 222.100.10.12 which are the Border Router interfaces.

Stealth is not a requirement in these tests. In fact, the team wants to check the logs to make certain that the packets permitted or denied match expectations.

nmap –sT <all valid IP addresses>

```
# this command will attempt a full TCP 'connect ( )' to any
# listening ports. The resulting nmap will be a complete list of
# open ports.
```

nmap –sU <all valid IP addresses>

```
# It is worthwhile doing a complete UDP port scan as well since
# the audit team is looking for any possible vulnerabilities
```

The next step is to attempt to telnet to each of the addresses.
Any connections may provide more information regarding the type of operating system through 'banner grabbing'. Information gleaned at this point should be noted, to be used in tightening the overall security of the site.

This process will be repeated for each of the firewall interface IP addresses to determine if the rule to drop all packets directed at the interface are working. By scanning a host on the other side of the firewall the team can also see if the rules pertaining to the network are working correctly.

If time and costs permit, it is worth using another tool along with Nmap. A very useful scanning tool is Nessus. It is also relatively simple to use and has Nmap as an optional part of its scanning possiblities. It can determine if there are known vulnerabilities existing on any on the platforms. By using the two tools as part of the audit, there is a greater chance of ensuring that any weaknesses in the network design are found, and can then be mitigated.

**Note**: The nmap program tries to check that a system is alive before it will continue a scan. It does this by sending an echo request packet to the host. If the rules do not allow for the reply to be sent then nmap will not continue the scan. Thus, it may be necessary to add a rule that allows for the echo reply to be sent. If this is done, great care must be taken, as it may open up the system to an unwanted scan while the audit is being undertaken.

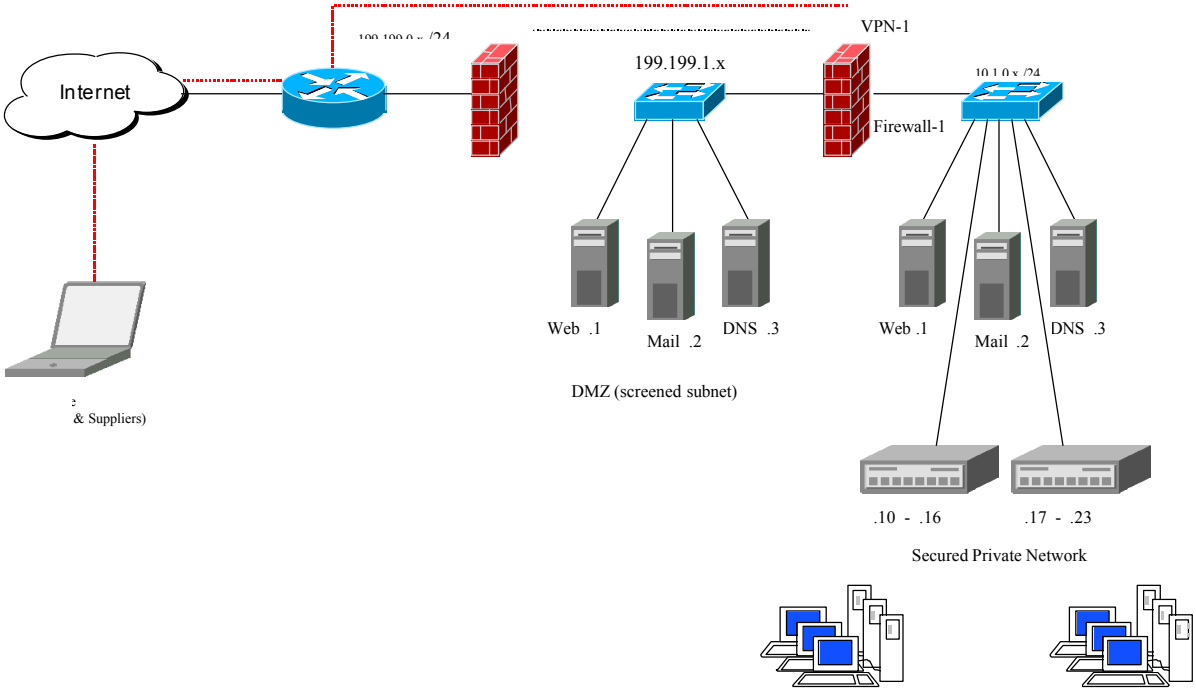
***Assignment 4 – Design Under Fire***

*Select a network design from any previously posted GCFW practical and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture.*

1. *An attack against the Firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.*
2. *A denial of service attack. 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 choose.*
3. *An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.*

## 4.1 Introduction

The Design Under Fire has been provided by Bob Hockensmith (http://www.sans.org/y2k/practical/Bob_Hockensmith_GCFW.doc). This design has some admirable features, and may be invulnerable to the attacks mentioned since not all network details can be supplied in so short a document. However, for this exercise some assumptions will have to be made.



**1.** The attacks described in this section are based on the belief that the border router rules have not effectively filtered all packets. Bob has added the following rules to the serial interface (Internet facing);

```
access-list 100 permit tcp any any
access-list 100 permit tcp any any
```

These rules were added so that all traffic not explicitly denied by earlier rules will be routed to the internal network. Added to this is the probability that no logging has been enabled. Thus, forensic information will be minimal.

**2.** An inspection of the PIX firewall rule also suggests that there are no deny rules applied to the actual interface addresses. An assumption will be made that the same methodology was applied to the Firewall-1 ruleset.

The two 'weaknesses' mentioned will allow packets to be sent directly to the Internet facing interfaces of the two firewalls with whatever purpose is desired by the attacker.

## 4.2 Firewall Attack

A first attack is to be directed at the firewall itself. The primary firewall for Bob's design is considered to be the VPN-1/Firewall-1 combination that protects the core elements of the network. According to a Black Hat security briefing in September 2000, one of the many security holes found in Firewall-1 is "S/Key Password Authentication Brute Force Vulnerability". As yet, this is not know to have been exploited due to the need to intelligently guess the original password length. It can not be considered a finessed attack since it requires the attacker to use a form of dictionary attack to guess the original password.

S/key is a one-time-password system that can be used by VPN-1 as an authentication method (the assumption here is that FWA1 has been disabled by the administrator). The process relies on the use of a seed and a sequence number, sent by the firewall, to be used in a set of hashes of and a resulting string that is finally exchanged. The exploit has been developed on with the expectation that only 86400 possible secrets can be generated in one day. There is a 'brute forcing' program called fw1bf that can make up to 50 guesses per second, and using the captured DSL modems in parallel, a powerful attack can be developed. Once the authentication secret is discovered, there is an fw1skey program that will unload the filter module, effectively disabling the firewall functionality.

## 4.3 Denial of Service Attack

The primary aim behind a denial of service attack is, as expected, to prevent

the user of a system from having access to the functionality normally provided by that system. It is a spiteful attack that in most cases will return the attacker nothing more than the satisfaction of knowing that they have caused damage. There are other possibilities, such as using the attack as a diversion away from other activities. Or the denial may give one company a short-lived competitive edge. However, whatever the reason, the attack is meant to bring operations to a close.

With this in mind, a denial of service attack on Bob's network should try to deny as much as possible. Therefore, an attack on the Checkpoint Firewall would effectively block all incoming traffic as Bob is using the Firewall-1 proxies along with the VPN capabilities. The operating system chosen for the firewall is NT4. This product has a variety of denials of service attacks that can be mounted against it. Therefore, it would be worthwhile to separate the 50 DSL modems into groups of around 10 or so and direct the five separate attacks at the firewall.

The attacks that will be tried are:

- **Bonk -** Aliases/variants: boink, newtear, teardrop2

  In this attack, corrupt UDP that cause the host system to attempt a reconstruction of a packet with an offset designed to make the final packet larger than acceptable. The Bonk attack is aimed at port 53. However, the Boink variation allows for port ranges to be attacked.

  Symptoms**:** Blue screen freeze and crash.

- **Land (TCP SYN)**

  This attack sets the source and destination IP address and port numbers to be identical, and which are that of the victim's machine. The SYN flag is set.

  Symptoms: Freeze and crash.

- **Land UDP** – Aliases/variants: snork

  As with Land above, except that UDP packets are sent instead of TCP.

  Symptoms: Freeze and crash.

- **Teardrop -** Aliases/variants: tear, TCP/IP fragment bug, overlapfrag bug

  This is the revers of the Bonk attack in that the fragmentation offset is such that undersized packets result.

  Symptoms: Immediate crash or reboot.

- **Fraggle -**Aliases/variants: smurf (but using UDP instead of ICMP)

For this attack, there will be a need to send the UDP echo request to the compromised systems' IP broadcast addresses with Bob's firewall address as the source. UDP echo reply packets will be sent on mass to the firewall.

Symptoms: Blue Screen (virtual device driver) error or computer to lock up.

With this variety of attacks directed at the firewall, there is a good possibility that at least one will succeed. Each is intended to 'kill' the system at which it is directed. However, the chances that Bob has not patched NT4 to a level that will resist any of the attacks mentioned is doubtful. These particular attacks are relatively old and should be well catered by the latest patches.

Dropping packets that have identical source and destination addresses can mitigate the land attack. This is accomplished by adding suitable rules at the border router or firewall.

An additional action can be taken. Adding a 'deny' rule to each of the firewall interfaces could strengthen Bob's system. This would make the firewall seem transparent to the outside world. Adding specific rules for administration purposes will be necessary. In this way, packets directed at the any of the interface IP address would be dropped (and should be logged).

Denial-of-Service attacks are difficult to defeat if a determined and persistent attacker uses them. It would be possible to set up the compromised sources to rotate source addresses as the continue to flood Bob's, or any system with either SYN, ACK, FIN, RST packets.

Many security professionals would prefer that the Firewall be placed on a Unix-like system that can be more easily 'hardened' against attacks. But even this defense would most probably be useless against a simple SYN flood directed at one interface and originating from the 50 DSL modems with an automated script. Under normal circumstances the logs of the system would provide the IP addresses of the 50 rogue devices. Since Bob does not appear to have added logging to the ruleset then the assumption is that denying the SYN packets from the known source would be difficult even after a re-boot of the system (assuming no IP spoofing has taken place). Logging should always be performed at the highest level possible. Too much information is better than too little when it comes to discovering the cause of a denial of service attack.

## 4.4 Internal System Attack

The most likely system to attack is the Web server in the DMZ. Web servers are particularly open to a number of different attacks.

Since Web servers in the DMZ are by their very nature open to the world, it will be simple to make this the point of attack. Also, since the attack on Bob's network has been based on denial of service, the exploit will be aimed at continuing the harassment of the system administrator.

To choose between of one of the many possible variety of Web server attacks, there is a need to determine which type of server is being used. The HEAD command is used by telneting to the Web server on port 80. The system will then return the required information, unless the system administrtator has taken steps to limit the amount of information broadcast to the world.

In this instance, the Web server turns out to be a OmniHTTPd Web server. Now that the identity is known, the Whisker CGI scanner is used to look for a particular file in the cgi-bin directory. Fortunately, the results are positive, and the visadmin.exe file has been left on the system as part of the default install. All that is needed is to send the following URL to the server:

http://omni.server/cgi-bin/visadmin.exe?user=guest

The Omni Web server will now continue to make 'temp' files until the hard disk is full. Then, the system will be unusable, and the denial of service is completed.

The system administrator can easily stop the attack happening again by removing the visadmin.exe file from the cgi-bin directory.

The system has been attacked, denied services, and the attacker is satisfied with their efforts.

## References


*More Nuke Information and Patches*

http://www.irchelp.org/irchelp/nuke/info.html#land

Nmap

http://www.insecure.org/nmap

*Remote Exploit (Bug) in OmniHTTPd Web Server*

http://cert.uni-stuttgart.de/archive/bugtraq/1999/06/msg00041.html

Network Defense, *System Fingerprinting*, Rik Farrow

http://www.spirit.com/Network/net0900.txt

@stake Research Labs

http://atstake.com/research/advisories

Gnac, *Firewalls – Re:S/Key Holes*

http://lists.gnac.net/firewalls/mhonarc/firewalls.199609/msg00819.html

FAQ: *Firewalls: What am I seeing?*

http://www.ussrback.com/docs/papers/firewall/firewal-seen.htm

Crackers and Commercial Vulnerability Scanners, Nomad Mobile Research Centre,m 1999

http://www.ussrback.com/docs/papers/IDS/scanners.txt

*Common Vulnerabilities and Exploits*

http://www.cve.mitre.org

*Hacking Exposded: Network Security Secrets & Solutions*, Stuart McClure & Joel Scambray

*Validating Your Security Plan Using Penetration Testing*, Andrew T Robinson

*Gauntlet for Windows NT Version 5.5 Administrators Guide,* Configuring Packet Screening