GCFW 1.7 Assignment

Sans Parliament Square, London
April, 2002

Author: Mark Hillick
Company: GIAC

Table of Contents

1. Assignment 1

1.1 The GIAC Story so far

GIAC Enterprises, a successful e-business company selling fortune cookie sayings online, was founded in 1997, at the height of the dot-com craze. However, it, unlike the other fledgling dot-coms had a well-thought business plan (YES a dot-com company with a plan). As a result, it has been able to survive and prosper. GIAC has its headquarters in Clearbridge, a small town about 15 miles outside Cork, Ireland.

1999 saw GIAC launch on the NASDAQ and despite its share price dropping by 50% in the first twelve months, it was able to record a $4 million profit for the year 2000. Inevitably the share price soon recovered and profits ($150 million) rose further in 2001. With such good results and the fall of the majority of the other fledgling technology companies, GIAC was able to buy some very cheap hardware and recruit some new highly qualified staff. As one of these new staff members, I was lucky enough to join the Internet Infrastructure team, whose main responsibility for the next six months is to design and install an upgrade of the existing GIAC Internet Network.

1.2 Objectives

With profits continuing to increase and an international presence, the GIAC directors realise that they must improve their technology infrastructure so that GIAC can continue to grow and prosper. Their customers, suppliers and partners not only receive a more efficient, reliable service but also in a secure method.
With Code Red 2 ringing up nearly $2 billion on its way to becoming one of the most expensive security threats to hit the Internet, e-businesses everywhere, including GIAC, received their wake-up call that Internet security has a direct impact on their prosperity. Having had numerous discussions, not all constructive, with the directors and senior management, I am aware that Code Red 2 impacted on GIAC but I have bot been privy to exact figures. Therefore, we, i.e. the Internet Infrastructure team, have the following objectives –

- To design a highly available, reliable, secure network, though which customers, suppliers and partners will all be able to use the GIAC services as before but now more efficiently, while not losing any trust in the security of their respective services. GIAC Internet Services must be secure.
- GIAC internal staff must be able to access the Internet securely.
- Ensure the scalability of the network with its suitability for future growth and expansion.

1.3 The GIAC Internet Team

The Internet Infrastructure staff have a strong background in Unix, particularly Sun Solaris, while there is also substantial knowledge of the Windows platform. Consequently, Solaris is the preferred platform but all staff members are also comfortable with Windows 2000.

In designing, building and supporting the GIAC Internet Network, the team works closely with the Network Design, Unix and Windows teams. There is a dedicated Security section in GIAC, however, we (in II) are responsible for the security of the GIAC Internet Network. We do liase with the Security team to ensure we are following best practice and to do this, we follow the "defence-in-depth" philosophy. Furthermore, we tried to design the network in such a way that we did have a single point of failure

Moreover, we receive the regular security advisories and updates from CERT (www.cert.org) , Bugtraq, SANS, Sun (www.sun.com), CVE (Common Vulnerabilities and Exposures) database. The "Sans Top 20" living document, http://www.sans.org/top20.htm, has been used as a basis in securing our network and where we may have to open a service that can possibly be considered insecure, we ensure the service is truly locked down.

1.4 Users and their Access Requirements

1.4.1 Mobile Workers

- Access to GIAC through the VPN tunnel.
- SMTP services – incoming and outgoing email.
- FTP services – ftp browsing access to the Internet through the internal web proxy.
- HTTP & HTTPS services – access to the Internet through the internal web proxy.
- DNS services – access to the Internal DNS server to resolve domain names to IP addresses for web browsing and sending emails.

1.4.2 Partners & Suppliers

- Access to the GIAC database vlan through the VPN link
- Read and write access on the database server.

1.4.3 Internal GIAC Staff

- SMTP services – incoming and outgoing email.
- FTP services – ftp browsing access to the Internet through the internal web proxy.
- HTTP/HTTPS services – access to the Internet through the internal web proxy.
- DNS services – access to the Internal DNS server to resolve domain names to IP addresses for web browsing and sending emails.

1.4.4 External Customers

- SMTP services - Sending emails into GIAC.
- DNS services - access to the Primary giac.com Name Server to resolve domain names to IP addresses for browsing GIAC web-sites and sending emails into GIAC.
- HTTP & HTTPS services - access to the GIAC web-server.

1.5 What do we have to work with?

Below is a description of what GIAC Internet Infrastructure Team has to work with – in terms of financial constraints, present technology, available IP addressing.

1.5.1 Budget

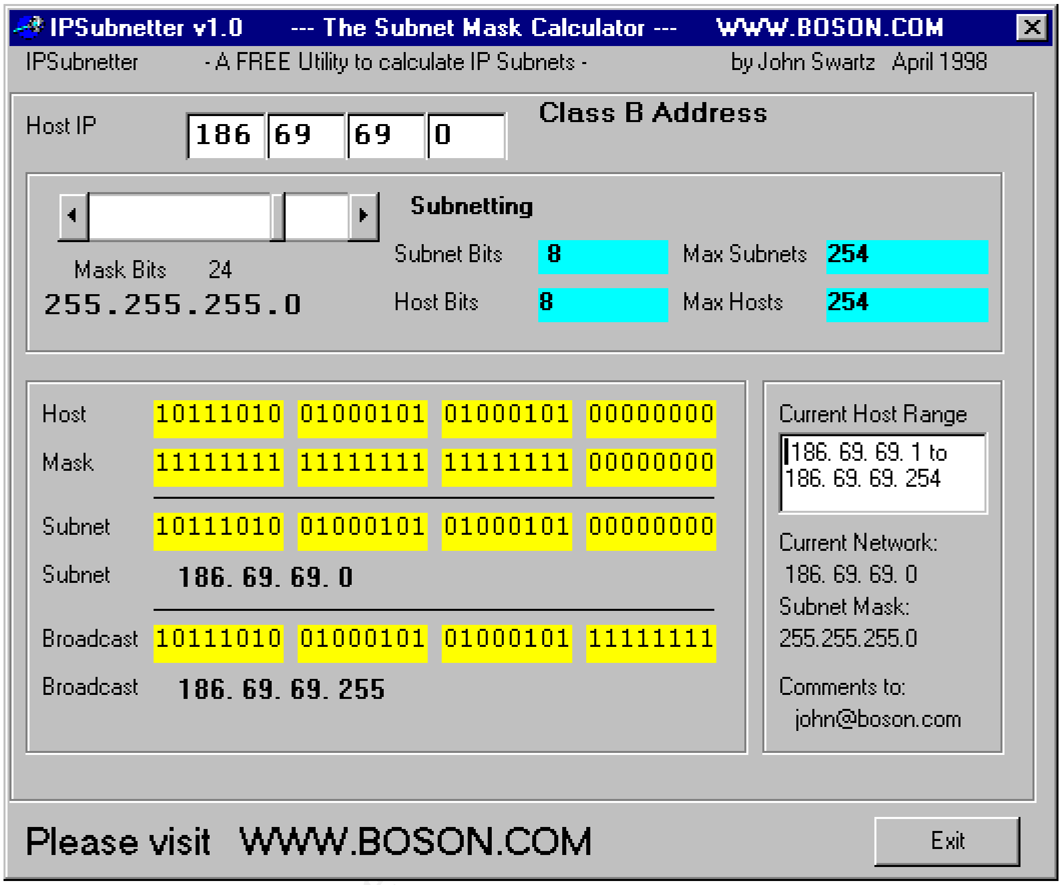
Realising the security vulnerabilities and disappointing reliability of the GIAC Internet Infrastructure, GIAC Enterprises have provided us with $2 million to satisfy the requirements stated in 1.2. This $2 million includes –

- the initial costs of buying the hardware and software
- the hiring of external consultants (Senior Management have a thing about hiring external consultants, it gives them some reassurance and yes, they do have deep pockets!!!)
- the set-up costs for the initial audit and the running of subsequent audits
- the support contracts with the software and hardware vendors for the next 2 years
- the successful set-up of a second computer room, thus providing the GIAC Internet Infrastructure with BRP (Business Resumption Plan) options as problems will inevitably arise with parts of the infrastructure despite our best efforts. Consequently, with BRP we will be able to invoke fail-over during the day, suffering practically no service outage, and then work on the problem area.

1.5.2 IP addressing

- GIAC already has one legal Class C Network of IP addresses, 186.69.69.0/24. There is no need to get more Provider Independent addresses, as we will not come close to using this whole Class C range.
- For the internal network, i.e. everything from the internal interfaces of the external firewalls and in, we will be using the allowed private addresses, as stated in RFC 1918 (RFC 1918 – http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1918.html):
  - ❑ 10.0.0.0/8
  - ❑ 172.16.0.0/12
  - ❑ 192.168.0.0/16

We will use the subnet10.exe tool, available from www.boson.com, to verify our subnetting.



IPSubnetter v1.0 --- The Subnet Mask Calculator --- WWW.BOSON.COM

IPSubnetter - A FREE Utility to calculate IP Subnets - by John Swartz April 1998

Host IP 186 69 69 0 Class B Address

Subnetting

Mask Bits 24

255.255.255.0

Subnet Bits 8 Max Subnets 254

Host Bits 8 Max Hosts 254

Host 10111010 01000101 01000101 00000000

Mask 11111111 11111111 11111111 00000000

Subnet 10111010 01000101 01000101 00000000

Subnet 186. 69. 69. 0

Broadcast 10111010 01000101 01000101 11111111

Broadcast 186. 69. 69. 255

Current Host Range

186. 69. 69. 1 to
186. 69. 69. 254

Current Network:
186. 69. 69. 0

Subnet Mask:
255.255.255.0

Comments to:
john@boson.com

Please visit WWW.BOSON.COM

Figure 1: screenshot of BOSON's handy subnet10.exe subnet tool.

1.5.3 Present Network Infrastructure

- 1MB link to the Internet through the local ISP, MerdeNET.
- Two computer rooms, 2 miles apart, with dark fibre running between them yet there is no high-availability or solution presently in place for the firewalls or the web-servers. It is hoped that this project will take advantage of the empty second computer-room and use it constructively for load balancing of services and as a viable BRP solution.

1.6 GIAC Internet Infrastructure Schematic

In designing the GIAC Internet Infrastructure, we have followed the "defence in depth" philosophy. Being in the online cookie-fortune business and with a worldwide image to protect, it is critical that GIAC enable access to critical applications and data while maintaining the confidentiality, integrity and availability of these resources. One of the first steps to completing it is to use network segmentation and access-control methodologies (http://www.networkcomputing.com/1214/1214ws1.html).

No network will ever be 100% full proof, though layering our defences will provide added protection and places multiple barriers between the attacker and our business-critical information resources. As a result, we use a combination of

- router ACLs (access control lists)
- DMZ's
- vlan segmentation
- virus-vetting
- firewall rulesets
- employing two firewall layers, each layer using different software and firewall-type

Furthermore, with the increasing visibility of service-outages as the GIAC customer-base grows, both in numbers and in geography a BRP site with dynamic-failover capabilities is essential.

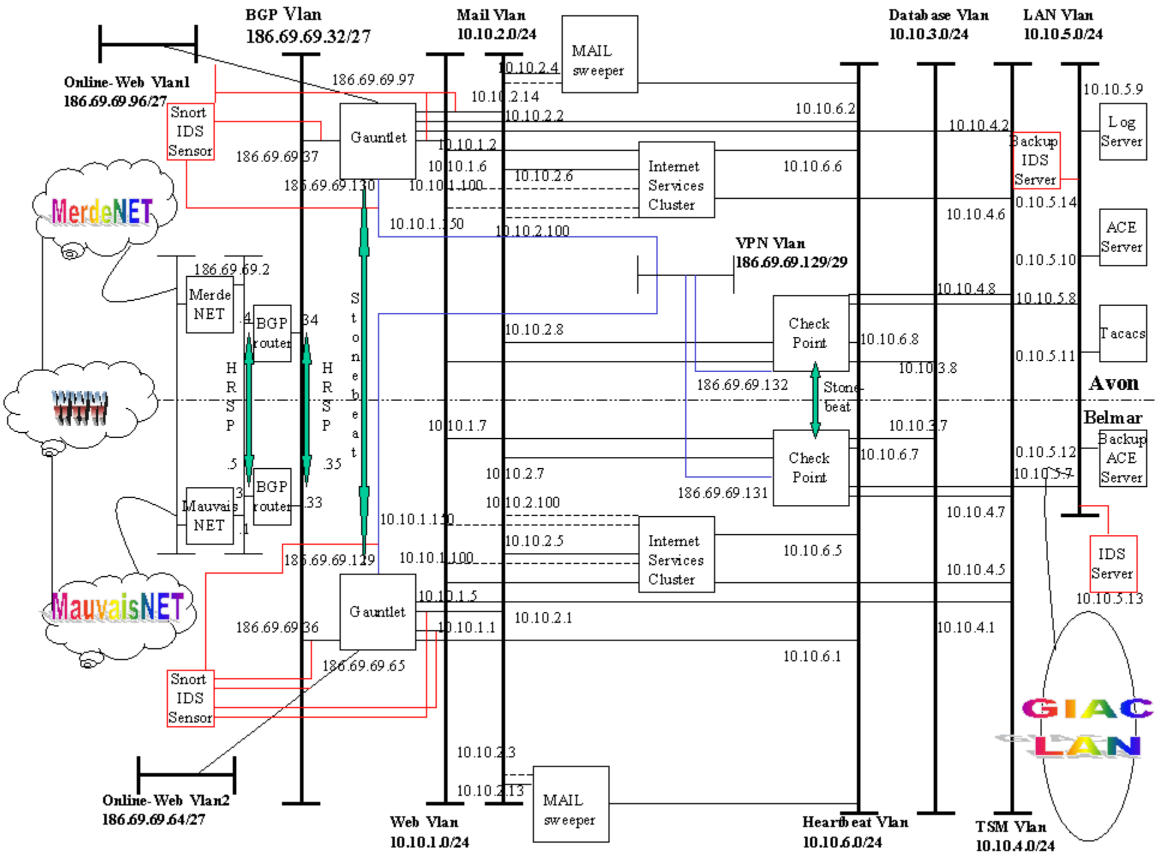


Figure 2: schematic showing the layout of the GIAC Internet Infrastructure. Note that we have not included the virtual addressing scheme for Stonebeat on either the internal or external firewalls.

Therefore, in description the GIAC Internet Infrastructure it makes sense to split the analysis into layers.

1.7 The Internet Infrastructure

1.7.1 The **www** Layer

Essentially, anything goes out here, some would say it's like the old "Wild Wild West" as opposed to the "World Wide Web". GIAC Enterprises have no control of what traffic leaves this layer and tries to enter GIAC's network. With the new infrastructure, we now have a two 4M links, one to MerdeNET and one to MauvaisNET. We will not need 4M on either link, or even close to it, but there is an aggressive expansion plan plus, with the telcos doing so bad, it was going ridiculously cheap. Additionally, this increased bandwidth will reduce the likelihood of a DOS attack being successful.

1.7.2 BGP Layer

Components: Four routers (one belonging to ISP MauvaisNET, one to MerdeNET and two to GIAC)
Software: IOS 12.1 (16)
Hardware: Cisco 7206VXR

The router has 128 MB of DRAM, as this is the recommended amount of memory to carry the full Internet BGP routing table.

The BGP layer is the GIAC's gateway to the Internet and so is the first line of defence. With GIAC business increasingly coming from all four corners of the globe and markets such as China opening up, the GIAC senior management asked us to improve the accessibility and reliability of GIAC Internet services to users in distant locations, as well as our traditional users across Europe. Therefore, the Network Design team and ourselves felt that we needed to implement a BGP design for the external routers. With MauvaisNET being a local, regional ISP and MerdeNET, the 2nd biggest global ISP, both our local and global users will be better served. Furthermore, this BGP design gives us the ability to invoke a dynamic BRP fail-over between ISPs and provides us with an excellent load-balancing solution.

1.7.2.1 What is BGP? How does it work?

Our BGP (version 4) is set-up to comply with RFC 1771 (http://www.ietf.org/rfc/rfc1771.txt). A good introduction to BGP can be found at http://www.academ.com/nanog/feb1997/BGPTutorial/sld001.htm.

"BGP (Border Gateway Protocol) is a protocol for exchanging routing information between gateway hosts (each with its own router) in a network of autonomous systems. BGP is often the protocol used between gateway hosts on the Internet. The routing

table contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen.

Hosts using BGP communicate using the Transmission Control Protocol (TCP) and send updated router table information only when one host has detected a change. Only the affected part of the routing table is sent. BGP-4, the latest version, lets administrators configure cost metrics based on policy statements. (BGP-4 is sometimes called BGP4, without the hyphen.)

BGP communicates with autonomous (local) networks using Internal BGP (IBGP) since it doesn't work well with IGP. The routers inside the autonomous network thus maintain two routing tables: one for the interior gateway protocol and one for IBGP.

BGP-4 makes it easy to use Classless Inter-Domain Routing (CIDR), which is a way to have more addresses within the network than with the current IP address assignment scheme."[1]

GIAC have their BGP design configured in such a way, that the GIAC 7200 BGP routers are running in a "Passive-Active" set-up. As a result, the router located in the Belmar site is the secondary, with the router in the Avon site, being the primary. To enable dynamic failover between the GIAC BGP routers, we use HSRP (Hot Standby Router Protocol). A more detailed description on BGP would be out of scope for this project, though this Cisco link, http://www.cisco.com/warp/public/619/3.html should answer any questions on HSRP and http://cisco.com/warp/public/459/18.html for BGP configuration.

The two GIAC routers and the two ISP routers are within the same AS. As such they have IBGP peers between them to allow routing updates to be learned by the GIAC routers from both providers. This allows the GIAC routers to pick the provider with the best path to a destination and to allow dynamic failover between providers.

Both routers have identical routing tables and if the primary fails, HSRP will fail all traffic over to the secondary in about 7 seconds. If one of the ISP routers fail, it will take the primary GIAC BGP router approximately 4 minutes to age out routing entries from that provider. This is based on standard BGP timers.

[1] http://whatis.techtarget.com/definition/0,,sid9_gci213813,00.html

We now have some diagrams of the BGP set-up – the first diagram giving a high-level view of the BGP set-up and the second showing the addressing schema.

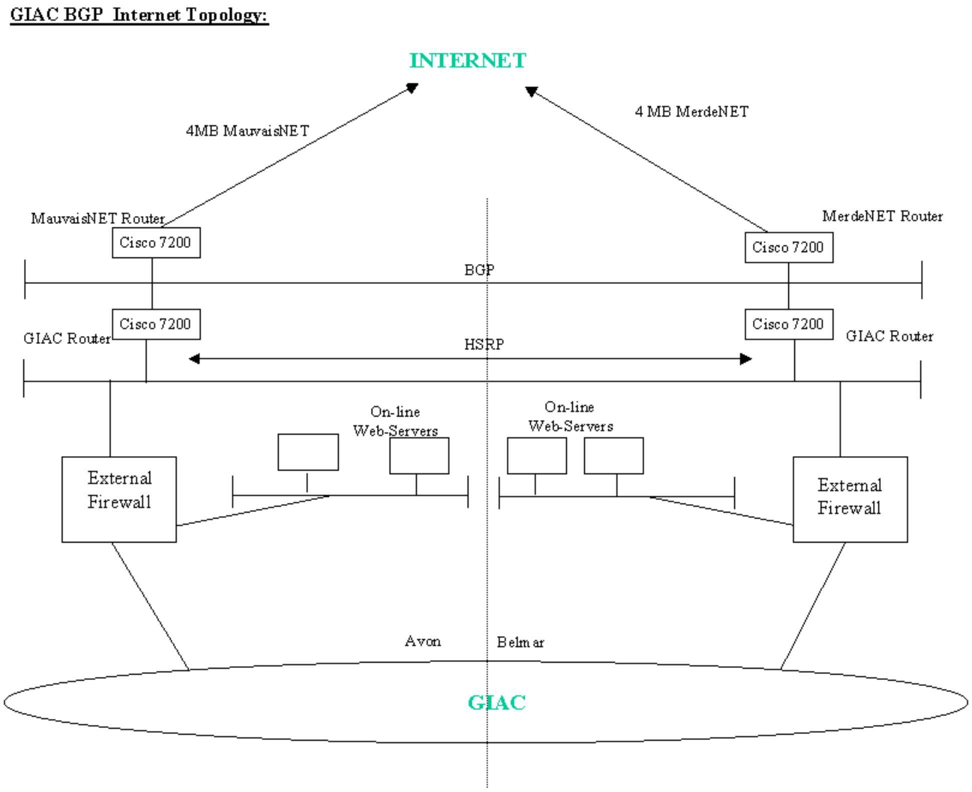


Figure 3: High-level diagram of the GIAC BGP Internet Topology.

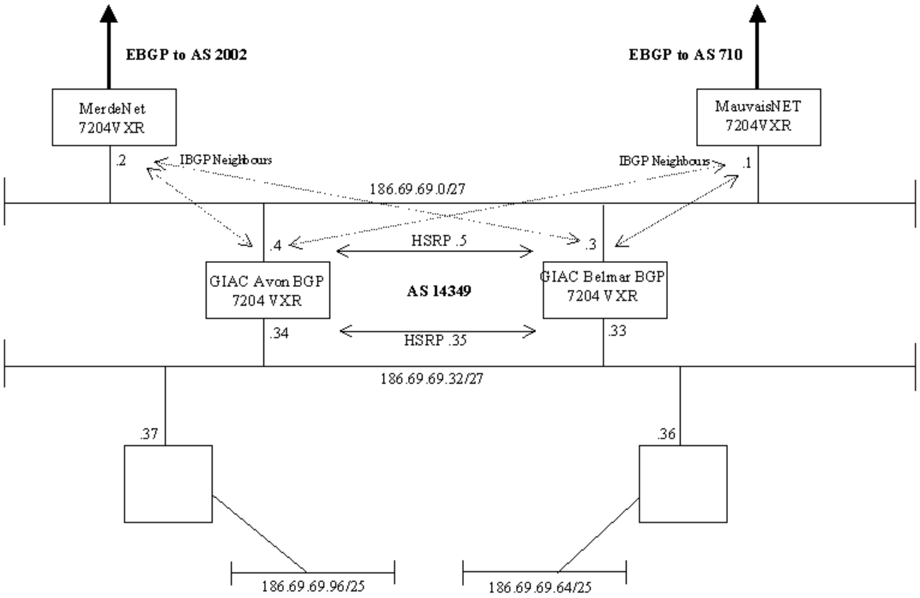


Figure 4: Diagram of the addressing schema of the GIAC BGP Internet Topology.

GIAC security policy dictates that all ports and services, that are not required for GIAC to conduct business, must be closed. This policy is implemented via access-control lists (see Section 2.1) on the routers.

There are two mini-zones to the BGP layer, “Zone 1”, representing the ISP routers, and “Zone 2”, the GIAC routers.

1.7.2.2 Zone 1

Obviously GIAC will have more control over their own routers, though they do insist on only those ports and services required for GIAC business be left open and they have received written confirmation on the ISP router configurations. Furthermore, the contract with the ISPs requires all changes on the routers and their respective networks to be change-controlled (using the agreed SLA) with written verification of any change given to GIAC. Moreover, there is monthly testing of the BGP links (with one ISP down at a time) to verify the configuration of both BGP routers. This may seem strange but there are various reasons behind this fail-over testing –

- GIAC need to be confident that in the event of issues at one of the ISPs (not unknown) that normal business can be conducted without any service degradation.

- ISPs have been known to ignore dynamic routing such as BGP or OSPF, in favour of creating static routers back to a customers network. By failing connections to each ISP bi-monthly, GIAC will be testing that their ISPs can pick up the new routes almost immediately.
- Finally, GIAC want to regularly test the monitoring and responses of the ISPs network teams, i.e. are they actively monitoring our links and is their follow-up procedure sufficient?

1.7.2.3 Zone 2

Zone 2 consists of the two GIAC BGP routers, with router 1 being the primary and router 2, the secondary. These routers operate using the HRSP protocol, with each router identically configured and with the same external and internal routes. There is further packet filtering of traffic at this zone and only allows in smtp, http, ssl, dns and vpn traffic.

1.7.3 External Firewall Layer

Components : 2 * external firewalls
Software: Gauntlet 6.0 (http://www.securecomputing.com/gauntletkb.cfm)
Hardware: Sun E450
O/S: Solaris 8

The Gauntlet Firewall was chosen because of its obvious security advantage, as application-based firewalls are considered to be more secure (Gauntlet receives prestigious certification – http://www.securecomputing.com/archive/press/2002/apr24,02.htm). The firewall proxies prevent applications on outside networks from talking directly with applications on your inside network, and vice-versa. No IP packets pass from one side of the firewall to the other and all data is passed at the application level.

Although NAI sold Gauntlet to Secure Computing midway through this "Infrastructure Upgrade" we were too advanced in our plan to review the firewall choice. Yet, more importantly, this is where the firewall experience lay and we actually felt more comfortable with Secure Computing's vision for Gauntlet than NAI's (the roadmap and other useful information is on the site – *http://www.securecomputing.com/archive/press/2002/june25,02.htm* and *http://www.securecomputing.com/index.cfm?sKey=974).*

The routers will have filtered any external traffic hitting this layer and so we should only see smtp, dns, http (internal http and ftp browsing traffic via a web proxy), ssl and vpn traffic hitting this layer.

Any http, ssl and ftp traffic hitting these firewalls from internally will originate from the internal web proxy. The internal dns server will forward dns requests to the dns server on the external firewall, while all smtp traffic will come from the Mimesweepers.

Moreover, the Gauntlet firewalls connect to http://relays.ordb.org to do reverse-dns lookups so that they block spam mail. Inevitably this does have an overhead on the firewall, though the business are prepared to put up with a slight delay, while we block spam at the first available point. According to our capacity planning scripts, 30% of our incoming email is spam – this block will undoubtedly improve on the overall performance of the Internet Infrastructure, while also pleasing our internal customers and greatly reducing the load on the IT helpdesk.

The external firewalls run in a shared environment but if one drops out the other is able to take up the load. We use the Stonebeat HA solution to enable this HA solution (http://www.stonesoft.com/products/StoneBeat/FullCluster_for_Gauntlet)

1.7.4 Internet Services Layer

The external firewall rulebase obviously dictates what traffic is allowed in and out of this layer. Again a more detailed explanation is available in Section 2.2.

1.7.5 Internal Firewalls

Software: Checkpoint NG
Hardware: Sun E450
O/S: Solaris 8

These firewalls are an integral part of our "defence-in-depth" philosophy. We have decided to use Checkpoint NG firewalls at this point for several reasons.

With an application-based firewall at our external perimeter, it is recommended that we have a stateful packet-filtering firewall at our internal firewall layer, as it won't have the same vulnerabilities. In addition, it provides another but different obstacle to a hacker who manages to compromise our external firewall layer. Besides, Checkpoint NG is the number 1 leading firewall choice across the world with over 60% market share, though that also means that it is most likely to be hacked. However, with sites such as http://www.phoneboy.com, http://www.cisecucurity.org and http://www.checkpoint.com we keep on top of patching and all security alerts for Checkpoint.

1.7.6 VPN Zone

Software: Checkpoint NG (http://www.checkpoint.com)
Hardware: Sun E450
O/S: Solaris 8

Dial-up connectivity will be handled with Secure Client

http://www.checkpoint.com/products/vpn1/secureclient.htm

The VPN zone is defined by a vlan hanging off the two Checkpoint NG firewalls. The IP address of the VPN interface on the firewall will be a real, private-independent address, however, the firewall rulebase protects this zone and only permits access to the supplier, mobile user and partner groups. This access is restricted by an ACE server, which contains the login, password and key-fob code of each user. The firewall in turn has each user in specific groups, which contain their access rights. Mobile users can access their mail and use ftp and http browsing like they can when they are working at their desk in GIAC. The partners and suppliers on the other hand, are only permitted to access the database server. A more detailed description of the GIAC VPN solution is available in Section 2.3.

1.7.7 GIAC LAN

This zone is where the user desktop PCs, the development servers, all GIAC HR information and financial data are located. Our “defence in depth” philosophy will have ensured (as much as possible) that a security breach from the Internet to the GIAC LAN is unlikely. With our various rulesets we can restrict internal staff from accessing the Internet Infrastructure, but we cannot prevent “social engineering” amongst internal staff from causing a security breach on our infrastructure. Yet we hope that the other IT teams in GIAC have their servers properly secured and that Security has ensured all staff have read and signed the necessary HR and Security documentation.

1.7.8 Web Servers

Software: Apache 1.3.24 (www.apache.org)
Hardware: Sun E250
O/S: Solaris 8

There are four web-servers, two on each DMZ of each firewall. The GIAC web servers only listen for traffic on port 443 (ssl).

The web-servers have dynamic fail-over using Cisco distributed directors in MerdeNET. This is an old set-up from the first two years of GIAC, where MerdeNET first set-up a load-balancing solution for us when we moved from one web-server to two. Though it was worth noting that back then it was two web-servers on the same hub hanging off the firewall (a packet-filtering router)! When a user requests www1.giac.com, he/she is directed to web-server 1, on the Belmar DMZ (https://www2.giac.com goes to web-server 2, on the Avon DMZ). Both web-servers have a back up on the opposite DMZ for dynamic fail-over

Slightly out-of-scope, but the MerdeNET Cisco directors provide us with a dynamic fail-over of the web-servers. Forward-filter rules have been set up on the firewall (see section 2.2) so that the distributed directors can poll the web-server, ensuring that it is up. If the distributed director cannot poll the web-server for a two-minute period, it changes its DNS record to point to the IP address of the relevant back-up web-server. (The hosts file on the firewall points DNS for www1 and www2 out to the dd01.merde.net and back up, dd02.merde.net).

We looked at replacing the distributed directors with more modern Content Switches (installed in GIAC and managed by GIAC) but the price ($350,000 for four, which would also enable us to load-balance the firewalls) meant we would run over budget. Moreover, no one in GIAC had any experience of working with content switches (so we still had to add in training and Cisco consultancy days). We felt that we would wait six-nine months before considering deploying content switches, especially considering we had enough new technology to learn and support, in our new Infrastructure. Additionally, a H/A solution using Stonebeat or maybe Cisco local redirectors was considered, however, there were problems over maintaining concurrency for the ssl sessions (ssl sticky). These content switches will be installed further down the line, when the infrastructure has successfully bedded-down and will give us much more functionality, such as high availability and load-balancing across both the firewalls and web-servers.

The web-server is hardened using TITAN (www.fish.com), which is explained in greater detail in Appendix A.

1.7.9 IDS

The importance of an Intrusion Detection System cannot be understated these days. It will not stop an attack, but it does track all traffic (in real-time) alerts on known attacks and can also distinguish between suspicious and legitimate traffic. It inevitably provides the administrators with a better understanding of the how the firewalls and their rulesets work. As a result, vulnerabilities, incorrect rulesets etc. will hopefully be noticed before any real damage is done.

The testing done so far in GIAC has shown that only the “compromise” alerts, i.e. where a web-server, firewall etc. has been successfully attacked, will be sent to the Operations Bridge. These alerts will be sent using SNMP and will be rendered readable through GIACs Management Monitoring tools.

We are using Snort (together with tcp dump) as our IDS solution, http://www.snort.org. Snort (version 1.8_7). Snort, running on FreeBSD (http://www.freebsd.org) version 4.6, fulfils all the requirements in GIAC and is now available with commercial support.

1.7.10 DNS in GIAC

GIAC will be providing a “split-brain” DNS service using two separate “internal” and “external” content DNS servers, each with different databases.

Securing DNS in the GIAC Internet Infrastructure without compromising functionality.

For the giac.com domain, our dns set-up is as follows –

Primary Name Server: fermet.giac.com, which is one of the external firewalls.
Secondary Name Server: sec01.ns.merde.net, which is a name server in MerdeNET. MerdeNET have configured and secured this name server in accordance with our best practices, under an agreed SLA.

1.7.10.1 Configuration[2]

1. Run all external DNS services on BIND version 9.1.2.
   - Domains hosted on external firewall 1 – fermat.giac.com.
   - All Internal Services that require external DNS services should forward queries onto the second external firewall – galileo.giac.com.
   - fermat.giac.com will only service dns queries from attached web-servers and local processes such as sendmail.
   - The following fields will be set for the giac.com domain:

     TTL: 30mins
     Refresh: 15mins
     Retry: 60 mins
     Expire: 1 week
     Negative TTL: 15 mins

     where –

     TTL - Sets the default time-to-live for subsequent records with undefined TTL settings. A TTL directive is used to tell resolvers, i.e. other name servers, how long they should cache the information for this zone.

     Refresh - How often secondary DNS servers should check if changes are made to the zone.

     Retry - How often secondary DNS server should retry checking if changes are made – if the first refresh fails.

     Expire – the length of time the zone will be valid after a refresh. Secondary name servers will discard the zone if no refresh could be made within this interval.

     Negative TTL: Negative caching is the ability of a name server to cache so-called negative results from other name servers. For example, if a request for

[2] Information about BIND was gathered from http://www.nominum.com/resources/faqs/bind-faqs.html.

information about a domain returns an NXDOMAIN reply (domain does not exist), the name server will cache these negative results.

2. Restrict Zone Transfers
   - Restricting Zone transfers prevents hackers from listing the contents of hosted zones and identifying targets such as internal mail servers and name servers.
   - We will ensure that zone transfers can only be performed on our master name server (fermat.giac.com) by our slave name servers.

     Our backup secondary name server is:
     Name: sec01.ns.merde.net
     Address: 186.69.144.11

     and the other backup name server, or the tertiary name server, is:
     Name: auth01.ns.mauvais.net
     Address: 63.69.145.11

     For example,

```
Zone "giac.com" {
                Type master;
                File "db.giac.com";
                Allow-transfer {186.69.144.11; 63.69.145.11};
}
```

     This would instruct the name server only to allow transfers of the giac.com zone to the slave servers in MerdeNET and MauvaisNET. To do this globally (i.e. to restrict for all hosted zones), you would use something like:

```
Options {
                Allow-transfer {186.69.144.11; 63.69.145.11};
};
```

3. Restrict Dynamic Updates
   - By default Bind 9 does not accept dynamic updates.
   - Dynamic updates are used in practice by DHCP servers. These servers assign IP addresses automatically to computers and then need to register the resulting name-to-address and address-to-name mappings.

4. Restrict Queries
   - The queries that the name servers accept should be restricted to the addresses they should come from and the zone they should ask about.
   - Queries for records in authoritative zones can come from anywhere because the zones are delegated to the name server.

- Queries for records outside authoritative zones should only come from internal addresses..

5. Do not advertise BIND versions.
   - The "version" statement will be used with bogus version information.

6. Bind should only listen on necessary interfaces
   - The "listen-on" statement should be used to specify the interfaces that expect dns queries.

7. Bind will run as a non-root user.

1.7.10.2 Split-Brain DNS

Split-Brain DNS is configured as follows in GIAC,

- The first DNS server will listen on an IP address that is reachable by the Internet and is listed in the public DNS database as being that of your domain's content DNS server. This server's database contains the DNS that GIAC wish to be published to the rest of the Internet.[3]

- The second server (inside the firewall) listens on an IP address that is only reachable and known by GIAC's own resolving proxy DNS servers (in our case, this is the loopback IP address on the scrodinger.giac.com, i.e. one of the E450 Internet Cluster boxes). This server is not listed in the public DNS database and contains data that GIAC only wish to be published within GIAC. All internal GIAC hosts will use the internal DNS server.

Please see Appendix A for further information on GIAC's network.

[3] Both http://homepages.tesco.net/~J.deBoynePollard/FGA/dns-split-horizon.html http://www.phoneboy.com/faq/0241.html were used for help in defining GIAC split-brain DNS policy

2. Assignment 2

Through describing the security architectures of our border router, external firewall and VPN we will explain how we have implemented the "defence in depth" philosophy described in Section 1.6.

2.1 Border Router

Although we have two external routers, due to our BGP configuration, (router pythagros.giac.com is primary and newton.giac.com is secondary) both routers have identical configurations. A router's number one priority is the routing of packets (SANS Track Two, Day Three), yet the GIAC BGP routers can also contribute to the overall defence of our network. Inevitably they will be nowhere near as good as the firewalls, yet we can use it to block the "absolutes", i.e. do traffic filtering.

We used the NSA security document (http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf), http://www.cisco.com/warp/public/0707/21.html, the SANS Track Two, Day Three module and the SANS anti-spoofing recommendations (www.sans.org/dosstop/cisco_spoof.htm) as guidelines in configuring the GIAC BGP routers. To achieve the aims set out in Assignment 1 and successfully implement meaningful ingress and egress filtering, it was felt that we must –

- Permit only those services required, i.e. disable any unnecessary service and close any port that is not needed
- Use the ACLs to successfully filter traffic in and out of GIAC
- Enable the routers for secure (and only secure) access for the system administrators

To resolve any legal issues that may arise in the future, as a result of the GIAC network being compromised, we have been advised to put the following login banner on the two GIAC BGP routers –

```
######################################################################
#       This system is for the use of authorised users only.
#
#       Individuals using this computer system without authority, or in
#       excess of their authority, are subject to having all of their
#       activities on this system monitored and recorded by system
#       personnel.
#
#       In the course of monitoring individuals improperly using this
#       system, or in the course of system maintenance, the activities
#       of authorised users may also be monitored.
#
#       Anyone using this system expressly consents to such monitoring
#       and is advised that if such monitoring reveals possible
#       evidence of criminal activity, system personnel may provide the
#       evidence of such monitoring to law enforcement officials.
######################################################################
```

This logon banner is actually on all GIAC Internet machines.

2.1.1 Basic Services and Configuration

We firstly need to create our hostname –

```
hostname pythagros.giac.com
```

All of the machines in the GIAC Infrastructure have been named after famous mathematicians, thus ensuring that the GIAC System Administrators can easily remember the machines but that those on the outside cannot easily work out whether its router, firewall, web-server etc.

We drop source routing as this can be used (by a hacker) to deliver harmful packets to destinations that cannot normally be reached.

```
no ip source-route
```

Additionally, we will store the password in MD5 hash as opposed to plain text so we use

```
service password encryption
```

to encrypt our password.

We want to timestamp our debug and log messages to simplify our logs analysis and auditing

```
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

Following our philosophy of disabling any service we do need, we disable non-essential UDP and TCP services.

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

As "Sans Track Two, Module Three, page 55" points out these are TCP and UDP services used for echo, character generation and discarding data that are hardly ever used. Disabling these services prevents some undiscovered vulnerability from being able to penetrate the router.

The finger server is also disable as it can aid a hacker by telling him/her who is logged in and from where –

```
no service finger
```

The PAD service is also disabled –

```
no service PAD
```

Furthermore, we do not want the router to listen for SNMP, which, although useful for informing the administrators about the status of the routers, would leave us vulnerable for attack.

```
no snmp
```

All server services should also be disabled as we have no servers that use "bootp" and as we use the command-line to administer the router, we do not need the web interface open

```
no ip bootp
no ip http
```

The router does not need to resolve domain names, so we disable that service

```
no ip domain-lookup
```

nor do we require the identification service, so it too is disabled –

```
no ip identd
```

Lastly, we allow the use of subnet zero (WHY) and classless routing (which is needed by BGP) -

```
ip subnet-zero

ip classless
```

Finally, we need to provide administrative access to our routers and we obviously want to restrict this to only the GIAC administrators –

```
access-list 5 permit 172.16.1.0 0.0.0.255
line vty 0 4
access-class 5
login
```

2.1.2 Access-Lists

By default, routers allow all traffic. The moment an ACL is added, all traffic is dropped except that which is specifically added. Each ACL must be attached to a specific interface and that interface is the only interface affected by that ACL.[4]

[4] Sans Track Two, Day Three, Page 21

Page 30 on Sans Track Two, Day Three, describes the extended ACL format that we will be using –

```
Access-list number action protocol source [wild card] [src-port] destination [wild-card] [dest-port] [other-options]
```

[5]

- Number:must be 100-199 for EXTENDED list
  - ➢ Extended access lists can also be named
- Action: must be **permit** or **deny**
- Type: name or number of protocol – ip, tcp, udp
- Spurce: source IP address to compare
- Source Options: TCP or UDP source port

We will have two separate access-lists, one for incoming traffic – access list 101 – and one for outgoing traffic, access list 102.

In setting up these access-lists, the GIAC Internet Infrastructure team have followed a 3-point approach –

- Block unwanted IP ranges and unnecessary services
- Permit protocols required for GIAC to successfully conduct business
- Lastly, put in the "Implicit Deny" rule so that any unspecified packets are denied

Moreover, before installing a new ACL, we use the "show interface" command to see if the router is dropping any packets. This may sound trivial, but

"there have been cases when an overloaded router has started ignoring ACLs and passing traffic unchecked." SANS Track Two, Day Three

2.1.2.1 External Internet-facing Interface

Hackers can use redirects, unreachables, broadcast and proxy arp to gain information about the GIAC network. They are not required and so are disabled. The "no ip direct-broadcast" command prevents malicious directed broadcasts from causing denial of service problems, while "no ip unreachables" prevents the router from giving out network information based on ICMP error messages (SANS Track Two, Day Three Page 56).

```
Interface FastEthernet  F0/0

no ip redirects
no ip unreachables
no ip direct-broadcast
no ip proxy-arp
```

[5] Page 30 on Sans Track Two, Day Three

Our time-servers are on the GIAC LAN and so we have no need to use NTP on the Internet-facing interface, so port 123 does not listen for traffic from the Internet.

The GIAC Infrastructure does not need the Cisco Discover Protocol and so it is disabled.

```
no cdp enable
```

Configuring HSRP –

```
standby Priority 10
                     5
standby authentication internet
standby IP 186.69.69.5
standby preempt
Ip access-group 101 in
```

Anti-Spoofing Measures:

We will block the non-routable private internet address ranges and log all traffic hitting us with that source address as stated in RFC 2827 -http://www.faqs.org/rfcs/rfc2827.html.

```
access-list 101 deny ip 10.0.0.0       255.255.255.255 any log
access-list 101 deny ip 172.0.0.0      0.240.255.255    any log
access-list 101 deny ip 192.168.0.0   0.0.255.255       any log
```

We also deny any loopback traffic,

```
access-list 101 deny ip 127.0.0.0      0.255.255.255    any log
```

The "log" at the end of the deny statement in the access list, will log any packet that is sent with a source address other than the ones permitted by the previous statement (SANS anti-spoof document).

Similarly we block any traffic hitting the external interfaces of the GIAC BGP routers with a source address of 186.69.69.0, i.e. we are denying the GIAC routable address space –

```
access-list 101 deny ip 186.69.69.0 0.0.0.255 any log
```

We also block the IANA reserved address space, www.iana.org/assignments/ipv4-address-space

```
access-list 101 deny ip 0.0.0.0        255.255.255.255 any log
```

```
access-list 101 deny ip 1.0.0.0        255.255.255.255 any log
access-list 101 deny ip 2.0.0.0        255.255.255.255 any log
access-list 101 deny ip 5.0.0.0        255.255.255.255 any log
access-list 101 deny ip 7.0.0.0        255.255.255.255 any log
access-list 101 deny ip 100.0.0.0        255.255.255.255 any log
```

There are quite a few well-known ports, which are frequently scanned by hackers. As we do not listen for traffic on these and definitely do not want to be receiving this traffic from the Internet, we will deny access on these ports:

```
access-list 101 deny tcp any any range 21 23 log                ftp, ssh, telnet
access-list  101 deny tcp any any eq 37 log
access-list  101 deny udp any any eq 37 log
access-list  101 deny tcp any any eq 69 log
access-list  101 deny udp any any eq 79 log
access-list  101 deny tcp any any range 123 log                        NTP
access-list  101 deny tcp any any range 135 139 log             Netbios
access-list  101 deny udp any any range 135 139 log             Netbios
access-list  101 deny tcp any any range 161 162 log             SNMP
access-list  101 deny udp any any range 161 162 log             SNMP
access-list  101 deny tcp any any range 6000 139 log            X-Windows
```

Services allowed:

Not only do routers deny and filter the "bad" traffic, but they also enable GIAC to conduct business with its various customers and partners. What services are we allowing?

- http
- ssl
- smtp
- dns
- checkpoint topology upgrades (port 264)
- esp
- ike

Therefore, to enable external customers to access our web-servers –

```
access-list 101 permit tcp any 186.69.69.33 eq 80
access-list 101 permit tcp any 186.69.69.34 eq 80
access-list 101 permit tcp any 186.69.69.65 eq 80
access-list 101 permit tcp any 186.69.69.66 eq 80
access-list 101 permit tcp any 186.69.69.33 eq 443
access-list 101 permit tcp any 186.69.69.34 eq 443
access-list 101 permit tcp any 186.69.69.65 eq 443
```

```
access-list 101 permit tcp any 186.69.69.66 eq 443
```

and likewise so they can resolve our giac.com domain names –

```
access-list 101 permit tcp any 186.69.69.8 eq 53
access-list 101 permit udp any 186.69.69.8 eq 53
```

Our GIAC internal staff need to be able to receive emails so we have to permit smtp access through the router –

```
access-list 101 permit tcp any 186.69.69.8 eq 25
access-list 101 permit tcp any 186.69.69.9 eq 25
```

Allowing HSRP,

```
access-list permit  ip host 186.69.69.3 host 224.0.0.2
```

Our last requirement is enabling VPN access for our mobile staff, partners and suppliers so that their requirements (as stated in Section 1) are fulfilled –

```
access-list 101 permit tcp any host 186.69.69.97 eq 264
access-list 101 permit udp any host 186.69.69.97eq isakmp
access-list 101 permit esp any host 186.69.69.97
```

ISKAMP, i.e. Internet Key Exchange, uses UDP port 500, while the Checkpoint Topology Upgrades uses ports 264. The “esp” service is the VPN tunnel itself.

As recommended we have the “implicit deny” to stop any other packets that we may have missed and we clearly want these to be logged.

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

2.1.2.2 Internal GIAC-facing Interface

As we did on the Internet-facing interface –

```
no ip redirects
no ip unreachables
no ip direct-broadcast
no ip proxy-arp
```

Configuring HSRP –

```
standby Priority 10
                     5
standby authentication internet
standby IP 186.69.69.35
standby Preempt
Ip access-group 102 in
```

Enabling the GIAC Network to securely log on and administer the routers, while increasing the difficulty for an attacker to log onto our routers.

TACACS + authentication/authorisation & Accounting:

aaa new-model	New model definition
aaa authentication login default tacacs+ local	Authenticate login via TACACS then Local
aaa authorization console	Enable Authorisation on console port
aaa authorization exec default tacacs+ local	Authorise exec level access
aaa authorization commands 15 default tacacs+ local	Authorise level 15 Commands
aaa accounting exec default start-stop tacacs+	Log start & stop time of Session
aaa accounting commands 15 default start-stop tacacs+	Log level 15 commands
tacacs-server host 10.252.10.10	TACACS Primary server
tacacs-server host 10.252.10.11	TACACS Secondary server
tacacs-server key netdeslan	TACACS key shared with server
ip tacacs source-interface fastethernet 0/0	Use FE0/0 as the source of TACACS frames

Although NTP is denied at the external interface of the router, like all other machines in the GIAC Internet Infrastructure, the external BGP routers are time-synchronised with time-servers on the GIAC LAN. Time-synchronisation of the Internet Infrastructure makes it easier to manage and audit the network.

REMEMBER we have blocked NTP on the internet-facing interface of the router.

Timezone & NTP:

clock timezone GMT 0 **Define timezone**

clock summer-time IRL recurring last Sun Mar 2:00 last Sun Oct 2:00 **Define summertime hour change**

ntp server 10.36.1.2 **Secondary NTP server**

ntp server 10.36.1.1 prefer **Primary NTP server**
ntp source Fastethernet 0/0 **Use lo0 as a source of NTP frames**

The GIAC Operations team receive alerts concerning the BGP routers via a combination of maxm and HP Openview to analyse. These commands below are for logging and management purposes and enable the NOC to successfully manage the routers.

Logging & SNMP Management:

snmp-server trap-source fastethernet0/0	Use lo0 as source of SNMP Trap Frames
Logging source-interface fastethernet0/0	Use lo0 as source of SYSLOG Frames
Logging 10.10.5.9	Define SYSLOG server
snmp-server enable traps	Enable sending of SNMP Traps
snmp-server host 10.52.52.7 traps public	Define Trap destination
snmp-server host 10.52.52.8 traps public	Define Trap destination

Allowing HSRP,

access-list permit ip host 186.69.69.33 host 224.0.0.2

There are a few things we can do on the internal-facing interface to increase security for GIAC. Hackers often use ping queries when trying to map a network so we block outgoing ping replies

access-list 102 deny icmp any any echo-reply

When an ICMP packet's TTL (time to live) has expired, the sender of the packet receives a ICMP time-exceeded message. This would be very helpful to a hacker trying to map our network and we will disable it

access-list 102 deny icmp any any time-exceeded

Lastly, we need to permit the GIAC internal staff out to the Internet and then we follow that with the "Implicit Deny" –

access-list 102 permit ip 186.69.69.0 0.255.255.255 any

access-list 102 deny any any

2.1.2.3 Tidying up

Below we ensure that any session opened on the router, which is idle for five minutes is successfully closed.

```
line con 0
exec-timeout 5 0                    Set idle timeout to 5 minutes
line aux 0
exec-timeout 5 0
line vty 0 4
exec-timeout 5 0
```

The final step in configuring the router is applying the ACLs to the interfaces and writing the configuration to memory -

- Internet-facing

```
ip access-group 101 in
```

- GIAC-facing

```
ip access-group 102 in
```

```
write memory
```

We reboot the router to ensure that the router runs the correct configuration on reboot.

2.2 Primary Firewall

2.2.1 Gauntlet 6.0

There are many improvements in 6.0 such as an easier-to-use management interface, integrity checker, adaptive proxying, new scripts that assist in the actual upgrade from 5.5, creating backups and other administrative tasks. Section 1.7.3 has already explained why Gauntlet 6.0 was chosen as the external firewall. Administering the Gauntlet firewall, we remember the Gauntlet philosophy:

> ***"That which is not expressly permitted is prohibited."***[6]

2.2.2 Firewall Rulebase

"Building a solid rulebase is a critical, if not the most critical, step in implementing a successful and secure firewall."[7]

[6] Gauntlet Philosophy – Gauntlet Administration Guide, which comes with the Gauntlet software.
[7] Lance Spitzner http://www.enteract.com/~lspitz/rules.html

With this in mind, the GIAC Internet Infrastructure team was very conscious in implementing their policy, following documents such as Lance's and the best practice document, http://www.roble.com/docs/firewall_best_practices.html. We decided to keep our rulebase simple and short, thus decreasing the possibility of mis-configurations and ensuring that we understood all the rules. In addition, we believed that this provided us with a more secure firewall – I guess we'll have to see about that. Furthermore, most firewalls (and Gauntlet 6 is no different) try to match the packet against each rule in order until it does. As a result, to ensure that the firewall is efficient it is ideal to put the most frequently used rules towards the top and the lesser used at the bottom.

"***It is critical to understand that the first rule that matches is applied to the packet, not the rule that best matches. Based on this, I like to keep the more specific rules first, the more general rules last. This prevents a general rule being matched before hitting a more specific rule. This helps protect your firewall from mis-configurations***."
http://www.enteract.com/~lspitz/rules.html

The ordering of the firewall rules is something that may be changed quite frequently, as new services are added, old ones taken away and others becoming more or less popular. As we are using Webtrends (http://www.webtrends.com) on our log server, we will easily be able to see what rules are used most frequently and adjust the rulebase accordingly.

The firewall ruleset is best described in two sections –

- Filter Rules
- Proxy Rules

The default state of the Gauntlet firewall is to deny any traffic that is not expressly permitted by firewall rules. If a rule is not created to allow a type of traffic, that traffic will be denied and dropped at the firewall. As a result, we do not need to create a tidy-up "deny" rule for the external firewalls.

2.2.2.1 Filter Rules

We use the forward-filter rules to deny traffic such as icmp (rule 05) and rpc (rules 6& 7), X-Windows (rule 8) while they also enable us to drop any "Gauntlet GUI" traffic on the external interface (rule 9). Gauntlet applies the filter rules, before going to the proxy rules. Rules 1-4 allow the ONLY distributed directors to complete a 3-way handshake on port 443 to verify that the web-server is up and then the director sends a "reset" to kill the connection.

Source	**Service**	**Action**	**Destination**	**Attribute**
dd01.merde.net	dd-in	Forward	www1	Log
www1	dd-out	Forward	dd01.merde.net	Log

dd02.merde.net	dd-in	Forward	www2	Log
www2	dd-out	Forward	dd02.merde.net	Log
Any	ICMP	Deny	Any	Log
Any	RPC (tcp)	Deny	Any	Log
Any	RPC (udp)	Deny	Any	Log
Any	ESPMD	Deny	Any	Log
Any	X-Windows (tcp)	Deny	Any	Log

2.2.2.2 Proxy Rules

Source	**Protocol**	**Action**	**Destination**	**Attribute**
Firewall Admins	ESPMD SSH	Permit	Fermat.giac.com	Connection
Untrusted	DNS	Permit	Fermat.giac.com	Connection
Untrusted	HTTP & SSL	Permit	GIAC web-servers	Connection
VPN user	VPN	Permit	VPN Host	Connection
Untrusted	SMTP	Permit	Fermat.giac.com	Connection
Network Admin	Tacacs	Permit	GIAC BGP routers	Connection
Internal Web Proxy	HTTP-internal	Permit	Any	Connection
Internal MAILsweepers	SMTP	Permit	any	Connection
Internal DNS	DNS	Permit	Fermat.giac.com	Connection
Firewalls	TSM-fire	Permit	Back up Servers	Connection
GIAC web-servers	TSM-web	Permit	Back up Servers	Connection
GIAC web-servers	SNMP-web	Permit	Management Server	Connection
Routers	SNMP-router	Permit	Management Server	Connection
Firewalls	NTP-fire	Permit	Time Servers	Connection
GIAC web-servers	NTP-web	Permit	Time Servers	Connection
BGP routers	NTP-router	Permit	Time Servers	Connection

Definitions:

Source – origin of the traffic
Service / Protocol – includes information such as port that the traffic uses, is the traffic tcp or udp, how many connections, processes can be open/run etc.
Action – permits or denies the traffic
Destination – destination of the traffic
Attributes – what type of logging is done of the packet – e.g. connection, alert, log etc.

As Gauntlet is a proxy-based firewall, the external world only sees the IP address of the external firewall interface. Therefore, for example, for someone responding to an email or a web-server sending a page down, they will both be talking to 186.69.69.36.

In Gauntlet (shown in more detail in section 2.5) the proxies can be bound to the interfaces. As a result, the external customers use a different instance of the http and ssl proxies compared to internal GIAC users. We also use this to add additional security to NTP, SNMP and TSM, where these services are bound to specific interfaces when defining a separate instance of them.

Proxy Ruleset

Rule 01: Enables the firewall administrators to manage the firewall using the gui and connect to the firewall, using SSH.
Rule 02: Anyone on the Internet is permitted to send DNS requests to fermat.giac.com so that they can resolve the giac.com domain. This would also enable our secondary DNS name server to do zone transfers.
Rule 03: Likewise anyone can talk to the giac.com web-servers on the DMZ, using http and ssl.
Rule 04: Allows the VPN traffic, only from the specified IP pool of the various VPN users, into the VPN host on the Checkpoint firewalls.
Rule 05: External people are allowed to send emails into GIAC (to fermat.giac.com specifically).
Rule 06: allows the Network Administrators to administer the GIAC BGP routers.
Rule 07: The Internal web proxy (a group including the virtual IP addresses of the web proxy and trend) is allowed to talk out to the Internet, using the “http-gw” proxy on the Gauntlet Firewalls.
Rule 08: The GIAC Mimesweepers are able to send mails to the Internet.
Rule 09: As we use split-brain dns, we need the internal dns server to be allowed to send DNS requests to the external DNS server, fermat.giac.com, which may answer them or forward them on to one of the root name servers on the Internet
Rule 10: Allows the firewall to be backed-up via TSM
Rule 11: The back-up of the GIAC web-servers, using TSM (Tivoli Service Management) on port 1500, is conducted through the firewall dmz interface and the internal web-interface of the Gauntlet firewall. Although a separate logging network would be desirable, to keep with our defence-in-depth philosophy it would involve buying more firewalls on the internal layer, an expense not within our budget. Moreover, our back-ups are done at 3am daily, when there is no traffic in the GIAC Internet Infrastructure.

Rule 12: the web-servers send snmp-traps to the management server on the LAN. The traffic is bound as in Rule 10.
Rule 13: Only the IP addresses of the internal interfaces of the BGP routers are permitted to talk back to the snmp-server on the LAN. The traffic is bound to the external and internal web-interface.
Rule 14: As rule 09, except this time for NTP.
Rules 15 & 16: As rules 11and 12, except this time we are using NTP.

2.2.3 Firewall Hardening

The default GIAC install of Solaris does not support IP packet forwarding, source routed packets, or ICMP redirects. These services would be extremely useful to a hacker as they change the directions in which packets flow and, consequently, could direct networks to circumvent the firewall. Services such as NFS, NIS and RPC cannot easily be made secure, so they are disabled.

As previously described in Section 1, the Gauntlet firewalls are hardened (after we have installed the all rulesets) with the free TITAN program (www.fish.com). We use Version 4.0.

"TITAN is a collection of programs, each of which either fixes or tightens one or more potential security problems."[8]

While TITAN is very useful, we are well aware that it does not provide us with 100% security or replace other tools. However, when used in combination with other tools it improves the security of the system it is running on. It is recommended in SANS Track Two, Day Four that you run TITAN on your Solaris systems.

2.3 VPN

The Checkpoint NG Firewall & VPN solution is used in GIAC (in a client-site VPN design). It is the market leader with a 25% share of the market (2001) Sans Track 2, Day 4, and page 197. Using the "secureclient" http://www.checkpoint.com/products/vpn1/secureclient.htm application (that comes with NG), we are able to ensure that the remote users PC and connection is secure, such that a hacker would not be able to piggyback on the remote users VPN connection/tunnel.

The VPN traffic on port 500 is allowed into GIAC via the external firewall and the tunnel terminates at the firewall vpn interface. The firewall then queries the ace server, on the LAN, when it receives a login request from a user. The user must match its userid, password and pin number (which changes every 60 seconds). The pin number is given by the RSA Secure ID key fob, which only the ACE server has a record of.

- Mobile GIAC users (i.e. internal GIAC staff dialling in from the Internet – come from a restricted IP range (186.69.70.0/27, belonging to MerdeNET), which we were able

[8] www.fish.com/titan/TITAN_documentation.html

ascertain when MerdeNET were only starting up and as we are their biggest customer, they have allowed us to keep it.

- Partners & Suppliers – are all large regional or national companies, whose traffic can only originate from two IP addresses at most.

The rulebase on NG will allow the following –

Mobile Users	SMTP	Mail Server	Permit
Mobile Users	FTP & HTTP on port 8080	Proxy Server	Permit
Partners & Suppliers	MySQL	Database	Permit

As a result, the router, external and internal firewalls all only permit traffic from IP recognised addresses for VPN traffic. Added to the key fob, user id and users password, this gives us a fourth layer of security.

Before accessing their data on the database server, the partners and suppliers have a logon and password to enter. Similarly, the remote users need an additional logon and password to access their email or browse the Internet.

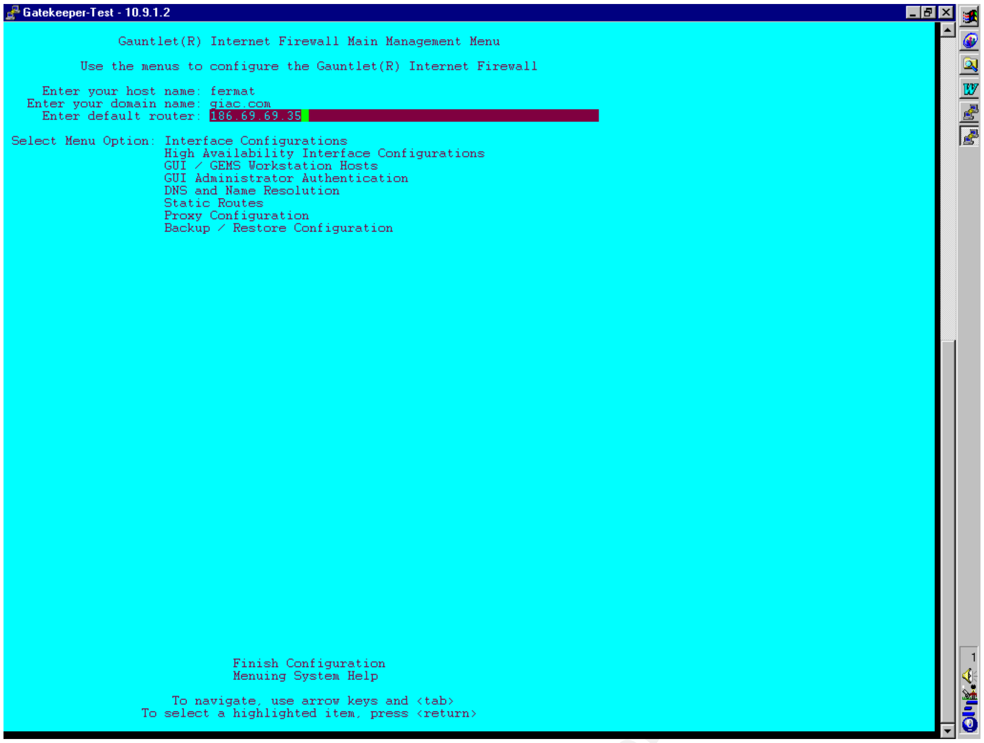
2.4 *Tutorial*

In this final section[9] of Assignment 2, we describe in greater detail how we implement the security policy described in Section 2.2. In compiling this tutorial, extensive use was made of the various Gauntlet Administration guides, which come with the Gauntlet software.

2.4.1.1 Applying rules in Gauntlet

There are two types of Management-GUIs with Gauntlet 6.0. The first GUI is text-based (type gauntlet-admin at the prompt), see figure 5, and is generally only used at the initial install when you are configuring the interfaces, enabling the administrators and adding routes before returning to the PC to complete the install and configuration with the Java-based Firewall Manager. It is used for everything from now on, other than adding static routes, which the text-based GUI is still required for. In the Gauntlet 6.0 Firewall Manager we can actually see the source and destination in the same rule on the same visual!

[9] Gauntlet Administration Guides were used in writing this section



```
               Gauntlet(R) Internet Firewall Main Management Menu

          Use the menus to configure the Gauntlet(R) Internet Firewall

     Enter your host name: fermat
   Enter your domain name: giac.com
     Enter default router: 186.69.69.35

Select Menu Option: Interface Configurations
                    High Availability Interface Configurations
                    GUI / GEMS Workstation Hosts
                    GUI Administrator Authentication
                    DNS and Name Resolution
                    Static Routes
                    Proxy Configuration
                    Backup / Restore Configuration





                             Finish Configuration
                             Menuing System Help

                     To navigate, use arrow keys and <tab>
                 To select a highlighted item, press <return>
```

Figure 5: the Gauntlet-Admin text based gui.

2.4.1.2 Firewall Rules

2.4.1.2.1 How does Gauntlet treat each packet it receives?

Step 1: Receive the packet
Step 2: Check (packet filter) its source and destination
Step 3: Check (packet filter) the request type.
Step 4: Process (proxy filter) the request.

2.4.1.2.2 Firewall Processing – Packet Filtering versus Proxy

There are two main types of firewall rules that can be applied, packet filtering rules and proxy rules. There is one list for each type of rule. The rules are applied in the order of their listing and when a rule that applies to a packet is found, the action in the rule is taken and no more rules of that type are processed for that packet.

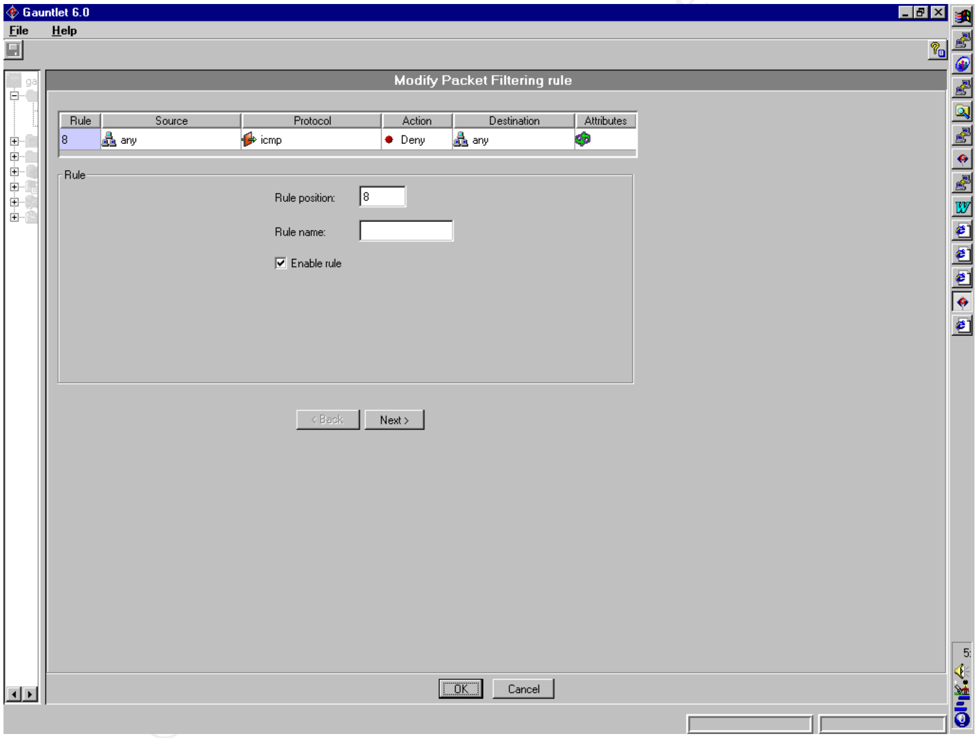
Figure 6, in the next section, is a screenshot of the forward filter ruleset, as described in section 2.2.1.2. These rules ensure that protocols such as sun rpc, icmp, espmd (the gauntlet-firewall GUI) cannot go through the firewall. These services could potentially be a security risk and these rules ensure traffic using these services, is dropped on the external interface. From Figure 6, you can notice the improvement in the Gauntlet 6 GUI, as you can see the source, protocol, action destination etc. all on the one site – may not seem significant, but makes Gauntlet much easier to manage! Furthermore, we can look at the forward filter and the proxy rules (which here have been scrolled down) at the same time – again a great help.

Using filter rules means not passing everything up to a proxy, thus gaining significant throughput. However, for the extra speed you are sacrificing security as the packet screening only checks the IP address, protocol and port numbers. In GIAC, we only have "deny" filter rules as there is nothing we need or want to packet filter through, though we do employ an adaptive proxy at times, which makes a speed versus security trade-off for us.

We will use the forward filter rules to explain setting-up a rule in Gauntlet – the process is identical for the proxy and local filter rules, so there is no point repeating ourselves.

2.4.1.2.3 Setting up a Firewall Rule

Figure 6: showing a sample packet forward filer rule



Rule	Source	Protocol	Action	Destination	Attributes
8	any	icmp	● Deny	any	

Rule

Rule position: 8

Rule name:

☑ Enable rule

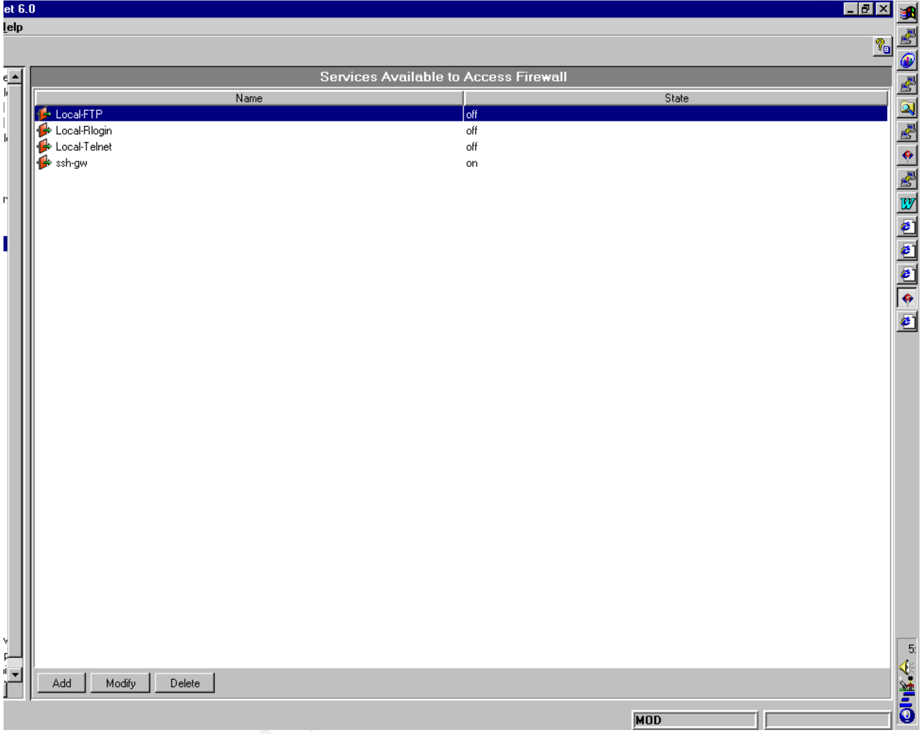
1. Open the rules folder and click rules
2. Click add and select "Packet Filter"
3. Enter a name for the rule in the "Name field" and click "Next"
4. Select a "network object" and then click Next or the Protocol field
5. Select a protocol and then click Next or the Action field
6. Select "Absorb" to allow the packet in or "Deny" to drop the packet and then click Next or the Destination field (for packet filter rules, there is also "forward", "forward with reply")

7. Select a network object for the destination and then click Next or the Attributes field
8. Select the logging level and confirm that the rule is ok
9. Click OK

Note: for proxy rules, "Permit" would be selected instead of "absorb".

2.4.1.3 Accessing the Firewall

As Figure 7 shows, we have turned off telnet, ftp and rlogin as means for accessing the firewall. These protocols are all unsecure and a hacker sniffing the traffic can easily gain an immediate advantage. We will use ssh (as mentioned in Section 2.2) We enable the service as below, before adding a proxy rule for the administrators to ssh to the firewall.



Name	State
Local-FTP	off
Local-Rlogin	off
Local-Telnet	off
ssh-gw	on

Figure 7: methods of accessing the firewall.

2.4.1.4 Adaptive Proxy

A new feature in Gauntlet is the "adaptive proxy", which combines the strengths of packet filtering, stateful inspection, and application gateways for enforcing firewall security.

Adaptive proxying works by proxy-processing the packets for a connection and verifying that the source, port and destination are permitted. Thereafter, all packets for that connection are packet-filtered only. This substantially speeds up the firewall processing for the connection.

There are four services that can be enabled to use the “adaptive proxy” option –

- http and ftp, unless you using an antivirus, URL filter or anything that requires analysis of the protocol
- Oracle
- Some TCP-plug proxies, one of which is ssl

GIAC have enabled the adaptive proxy on the ssl plug proxy (incoming and outgoing ssl) and the http proxy (outgoing http and ftp traffic, which has originated from the proxy server. (Ref. Gauntlet Admin guide).

2.4.1.5 Plug Proxy versus Service-Specific Proxy

2.4.1.5.1 Service-Specific Proxies

As I have said earlier, Gauntlet 6.0 proxies prevent applications on outside networks from talking directly with applications on your inside network, and vice-versa. No IP packets pass from one side of the firewall to the other and all data is passed at the application level. Typical service-specific proxies include –

- HTTP
- FTP
- Oracle

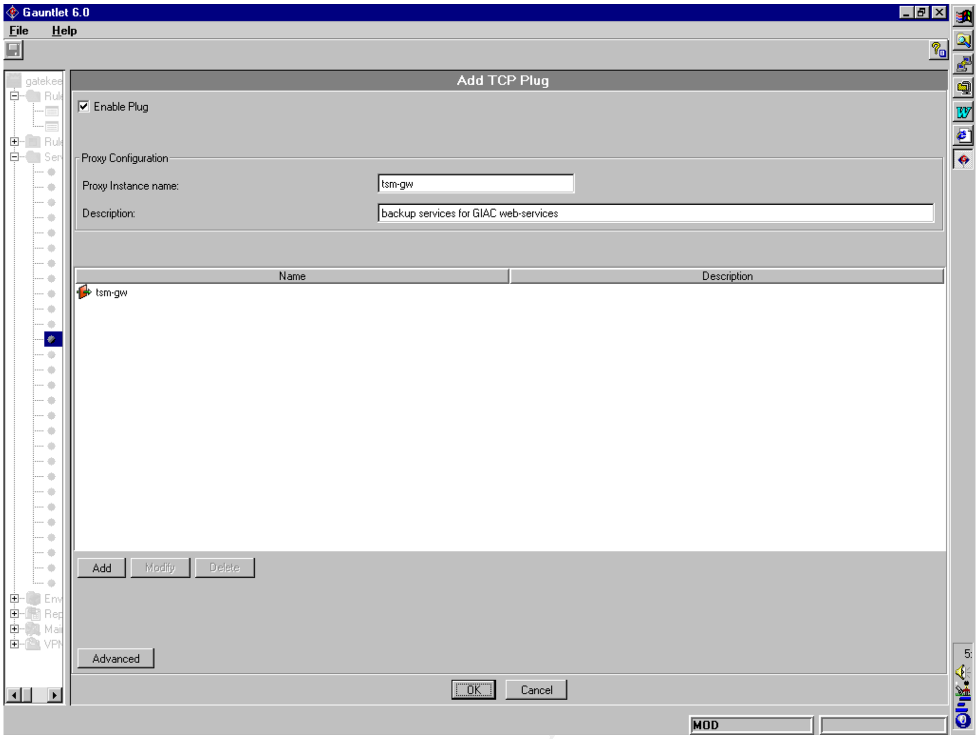
2.4.1.5.2 TCP & UDP Plug Proxies

With Gauntlet 6.0, we have a generic “TCP/UDP plug” proxy. This proxy passes (plugs) TCP/UDP traffic from a particular port on one side of the firewall to a particular port on another system on the other side of the firewall. As with the service-specific proxies, no ip packets pass directly from one side of the firewall to the other. If no proxy has been installed for a service, that traffic type will not pass through the firewall.
Below are some of the Gauntlet 6.0 pre-configured plug proxies for:

TCP	**UDP**
• AOL	DNS
• Secure Web Services (SSL)	IKE
• X.500	NTP

2.4.1.5.3 Creating a Plug Proxy

In configuring the ssl gateway on the Gauntlet firewall, we create two separate ssl proxies – one for internal GIAC staff, the other for external GIAC customers connecting to GIAC on ssl. The internal ssl proxy does not forward the originating IP address (as we do not what the external world to know our internal addresses) and the external ssl proxy does forward the source IP address because we DO want to know who is connecting to us. Other proxies, such as the “http-gw” can be set up similarly (in regard to the originating IP). The ssl proxy is a “plug proxy”, whereas the “http-gw” is an actual proxy.



☑ Enable Plug

Proxy Configuration

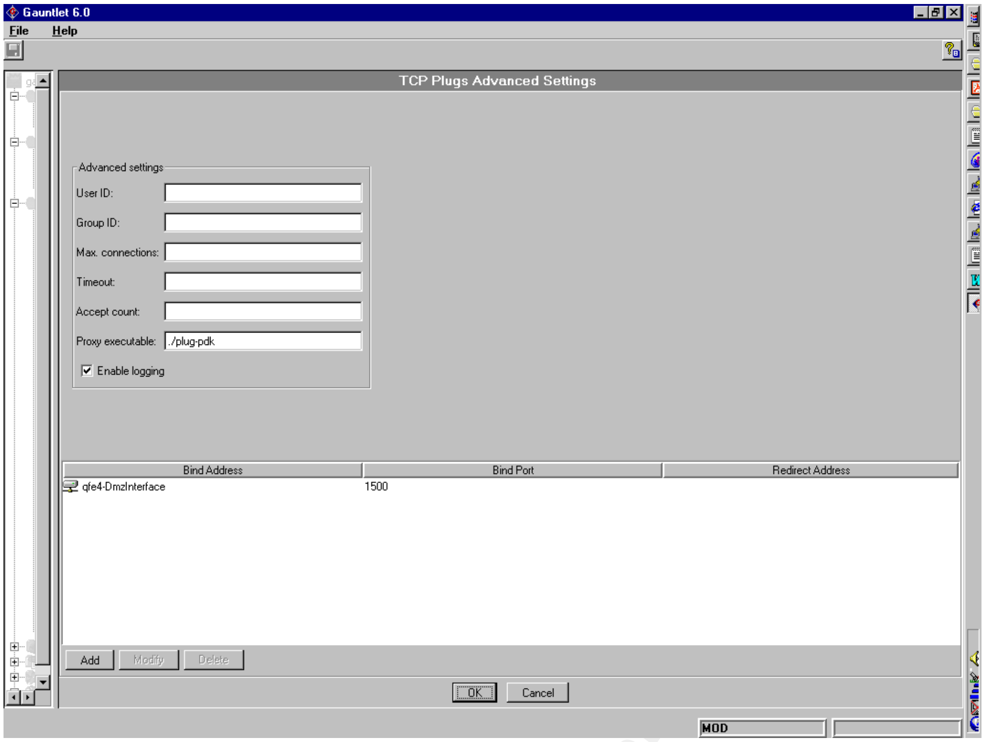
Proxy Instance name: tsm-gw

Description: backup services for GIAC web-services

Name	Description
tsm-gw	

Figure 8: screenshot of setting up the tsm plug proxy.

As you can see from the screenshot below, we have bound the tsm traffic to the DMZ interface. At this stage, only the DMZ interface will allow tsm traffic from whatever IP addresses the proxy rule for tsm states. Our next step is to permit the traffic through the internal web interface, so that the back-ups can successfully reach the tsm servers on the LAN. Figure 7 shows us defining that traffic on port 1500 is bound to the web interface.
Figure 9: the TSM gateway runs as the plug-pdk process and is bound to the DMZ interface



Gauntlet 6.0

TCP Plugs Advanced Settings

Advanced settings

User ID:

Group ID:

Max. connections:

Timeout:

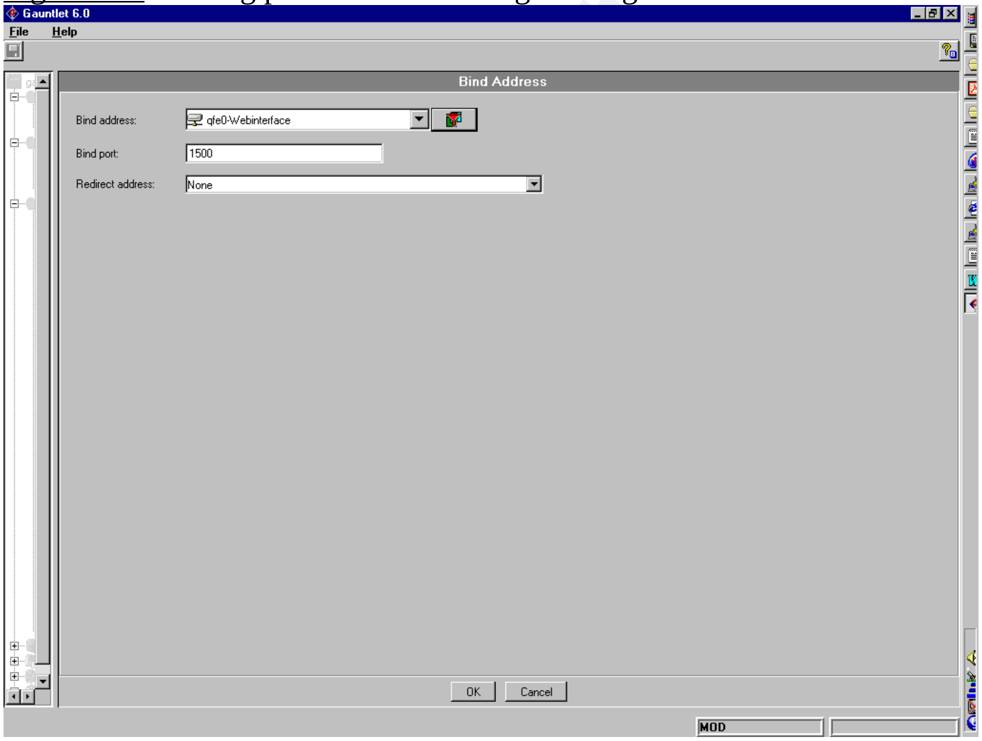
Accept count:

Proxy executable: ./plug-pdk

☑ Enable logging

Bind Address	Bind Port	Redirect Address
qfe4-DmzInterface	1500	

Figure 10: allowing port 1500 traffic to go through the web interface



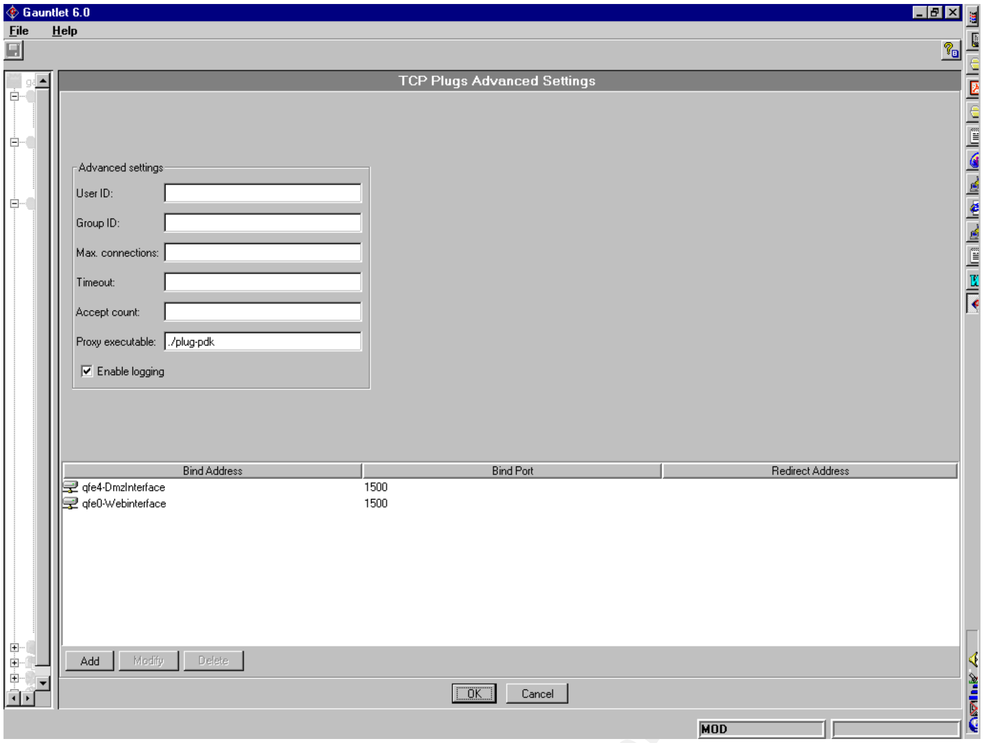
Gauntlet 6.0

Bind Address

Bind address: qfe0-Webinterface

Bind port: 1500

Redirect address: None



Advanced settings

User ID:

Group ID:

Max. connections:

Timeout:

Accept count:

Proxy executable: ./plug-pdk

☑ Enable logging

Bind Address	Bind Port	Redirect Address
qfe4-DmzInterface	1500	
qfe0-WebInterface	1500	

Figure 11: we now have the complete picture, where traffic on port 1500 is bound to the DMZ and web interfaces. If the TSM traffic hits another interface, it will be dropped (the sender will not receive an error message or a deny, but will simply know their traffic has been dropped somewhere along its path to its destination. This applies to all traffic (and all protocols) hitting the firewall where it should not be. Below is a sample security log of TSM traffic hitting the wrong interface (external) and being dropped-

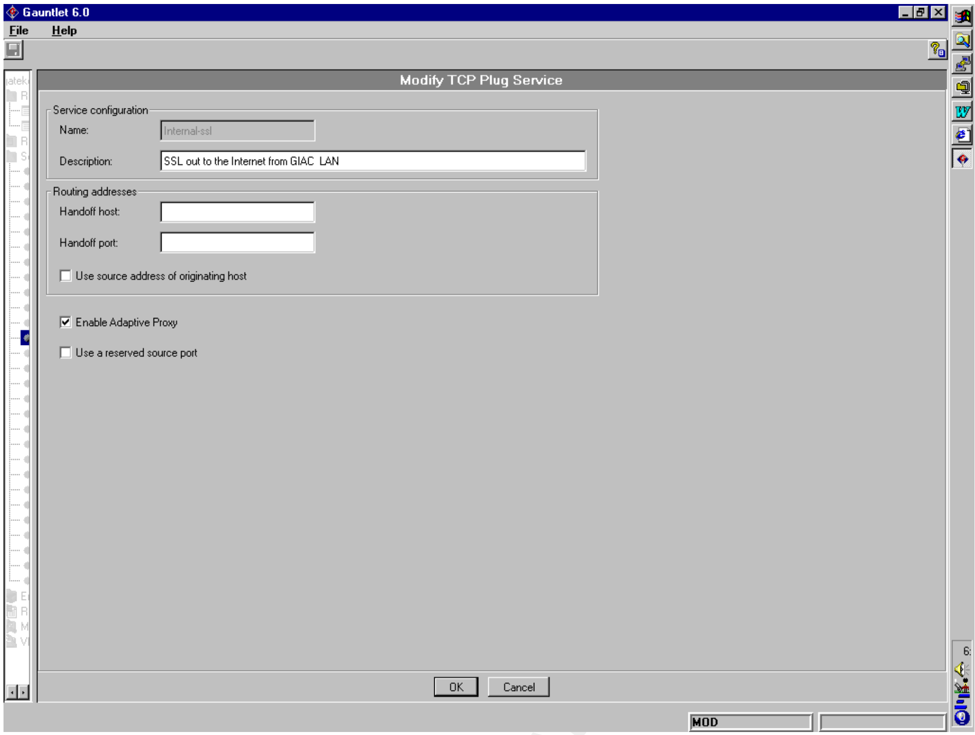
```
Sep 17 16:24:09 fermat.giac.com gfw: [ID 702911 kern.info] securityalert
: packet denied by local screen: TCP(12) if=qfe0 srcaddr=186.69.69.66 srcport=1500
 dstaddr=186.69.69.36 dstport=32771
```

2.4.1.6 Internal versus External Proxy Use

With external users connecting to GIAC services (for VPN, ssl, smtp etc.) we want to know their source/originating IP address, whereas for GIAC users connecting out to the Internet we do not want their GIAC source address to be transferred out. We, therefore, set up separate proxies (and, consequently, separate rules) for internal and external users. Using ssl as an example,

Figure 12: setting up the ssl proxy for internal users. To ensure that the source IP address (from the GIAC LAN) has not been forwarded we leave the box for "Use source address of originating host" clear. Additionally, this is one of the examples where we would run the "adaptive proxy", thus enabling ssl to run better on the firewall and connect more efficiently to the web-servers. Sometimes, though, system administrators may have to be

careful as the proxy may be behaving too efficiently for the web-server, causing erratic responses for users browsing the GIAC web-site.



Modify TCP Plug Service

Service configuration

Name: Internal-ssl

Description: SSL out to the Internet from GIAC LAN

Routing addresses

Handoff host:

Handoff port:

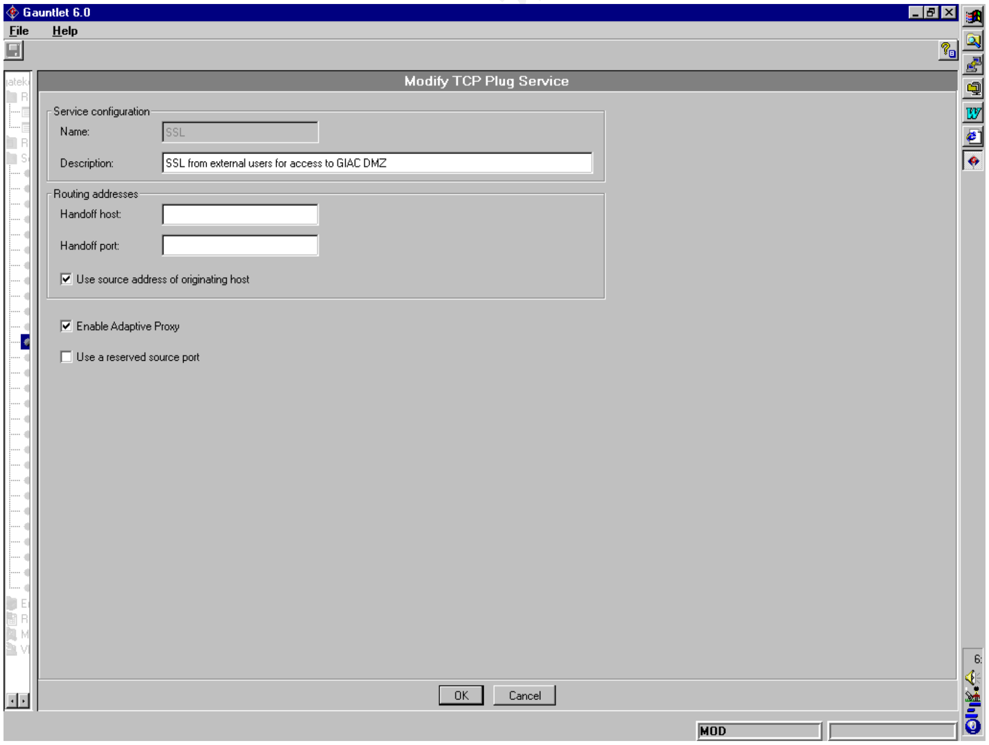
☐ Use source address of originating host

☑ Enable Adaptive Proxy

☐ Use a reserved source port

Figure 12

Figure 13: below, external SSL users (who will connect to the giac.com webserver) with their source IP



Modify TCP Plug Service

Service configuration

Name: SSL

Description: SSL from external users for access to GIAC DMZ

Routing addresses

Handoff host:

Handoff port:

☑ Use source address of originating host

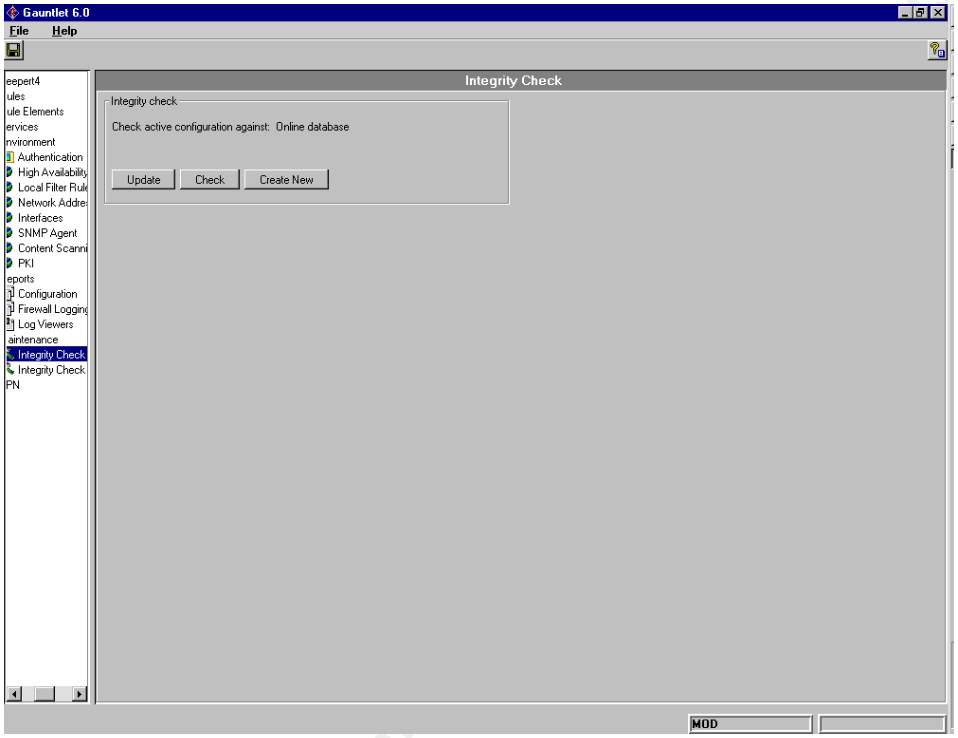
☑ Enable Adaptive Proxy

☐ Use a reserved source port

2.4.1.7 IP screening

The IP screening facility is an additional security piece of Gauntlet 6.0. It processes or rejects packets based on criteria such as address and protocol, thus enabling it to detect spoofed packets. The firewall can be configured, using IP screening, so that it is transparent to the user for most activities.

2.4.1.8 Integrity Checker



Check active configuration against: Online database

Figure 14: the Integrity Checker would set up using the Gauntlet Management gui. The set-up process is well detailed in the Gauntlet administration notes that come with the Gauntlet software.

The Integrity Checker enables administrators to verify the integrity of their firewall (e.g. have files been modified), by serving as a baseline against which configuration data can be checked. Integrity Checker will be run monthly to verify the firewall.

The integrity database, an ASCII file, contains a checksum for each file, including information such as file owner, group etc. It does not contain information about files that can change often, such as the mail spool.

The firewall runs a scan program (**scan**) that walks the directory tree and creates MD5 messages digest checksums for each file, writing the checksum to the integrity database. The Integrity Check Status item is then used to review any changes that have been made and that they are acceptable.

Now that you ensured that nothing on your firewall has been modified, the integrity database itself must be protected. This should be done by copying the database to disk or tape or both. Keep this offline, and stored according to security policy. To review the system status, copy the previous database (from offline) back to the /usr/local/etc/checksums directory and then run the integrity checker.

2.4.1.9 Testing Firewall Rules

We then test a selection of firewall rules, with at least one from each of possible location:

- Proxy Rule 01

We test "rule 01" by resolving http://www1.giac.com from a dial-up.

```
 #nslookup
Default Server: localhost
Address: 127.0.0.1
> server ns23.merde.net
Default Server: ns23.merde.net
Address: 186.69.71.1
> www1.giac.com
Name: www1.giac.com
186.69.69.66
```

- Filter Rule 1

We try to ping the firewall from the Internet but we get no answer as expected since the packet filter rules deny icmp.

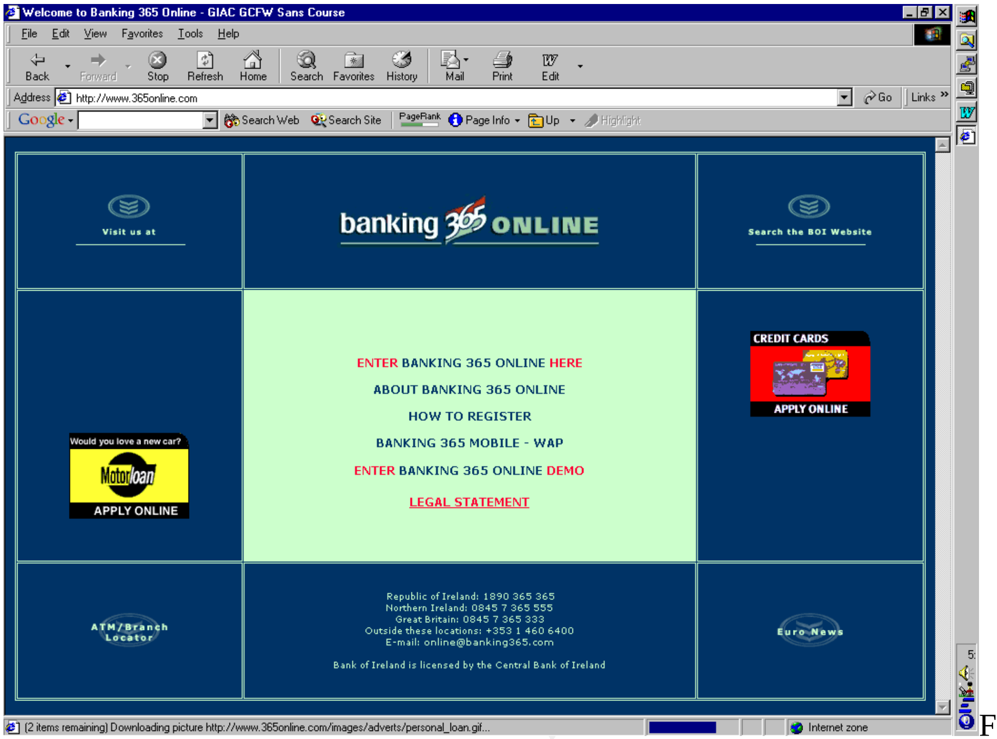
```
#ping 186.69.69.36
no answer from 186.69.69.36
```

- Proxy Rule 02

Using a laptop with a dial-up account, we test whether external customers can browse successfully to the giac.com web-sites, though only using the IP address. We successfully access the www1.giac.com web site, receiving the pop-up ssl certificate also. We try to access the site on port 80 but we are unsuccessful, as expected.

- Proxy Rules 7 and 9

We test that the internal GIAC staff can successfully browse the Internet. Therefore, we simply use one of the desktop PCs on the LAN to connect to a web-site. The DNS cache on the internal and external DNS servers has been cleared in order that the internal dns server queries the external DNS server, which will in turn send a query to a root name server. As the screenshot below shows, we were able to connect first to the "home page" of the http://www.365online.com site before connecting then to the secure section of the site. At this point, we are satisfied that these rules on the external firewall are behaving as they should and allowing users to access their required http, ssl and dns services. Remember if users cannot access this, we're in trouble on payday – this is a crucial service.

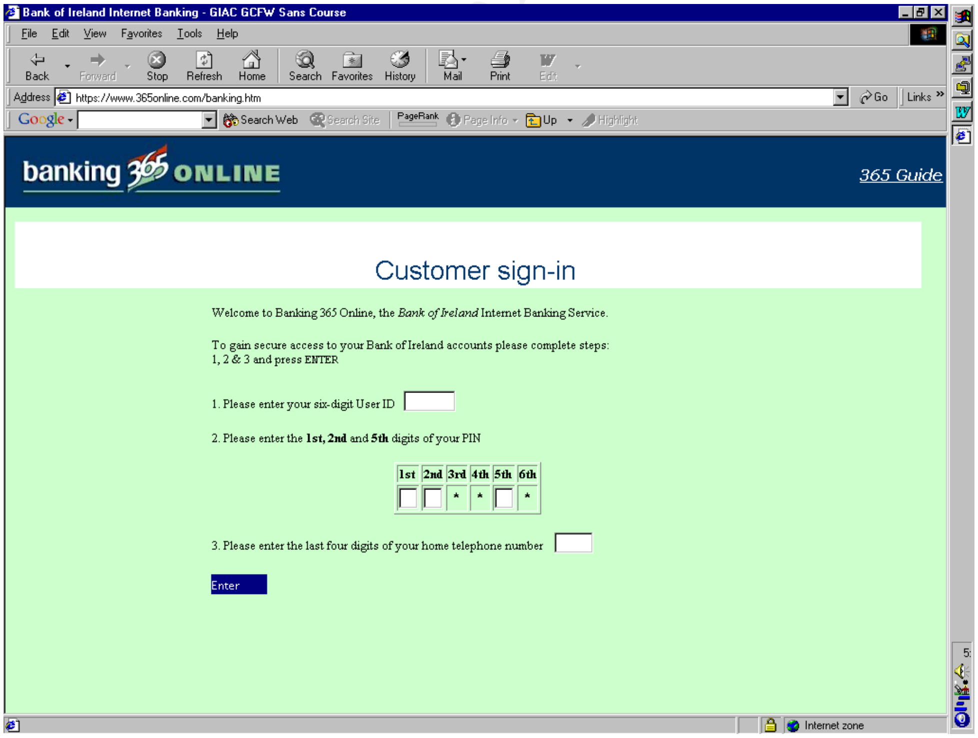

Welcome to Banking 365 Online - GIAC GCFW Sans Course
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit
Address http://www.365online.com
Go Links
Google Search Web Search Site PageRank Page Info Up Highlight
Visit us at
banking 365 ONLINE
Search the BOI Website
CREDIT CARDS
APPLY ONLINE
Would you love a new car?
Motorloan
APPLY ONLINE
ENTER BANKING 365 ONLINE HERE
ABOUT BANKING 365 ONLINE
HOW TO REGISTER
BANKING 365 MOBILE - WAP
ENTER BANKING 365 ONLINE DEMO
LEGAL STATEMENT
ATM/Branch Locator
Euro News
Internet zone

Republic of Ireland: 1890 365 365
Northern Ireland: 0845 7 365 555
Great Britain: 0845 7 365 333
Outside these locations: +353 1 460 6400
E-mail: online@banking365.com

Bank of Ireland is licensed by the Central Bank of Ireland

(2 items remaining) Downloading picture http://www.365online.com/images/adverts/personal_loan.gif...

Figure 15


Bank of Ireland Internet Banking - GIAC GCFW Sans Course
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit
Address https://www.365online.com/banking.htm
Go Links
Google Search Web Search Site PageRank Page Info Up Highlight
banking 365 ONLINE
365 Guide
Enter
Internet zone

Customer sign-in

Welcome to Banking 365 Online, the *Bank of Ireland* Internet Banking Service.

To gain secure access to your Bank of Ireland accounts please complete steps: 1, 2 & 3 and press ENTER

1. Please enter your six-digit User ID

2. Please enter the **1st, 2nd** and **5th** digits of your PIN

1st	2nd	3rd	4th	5th	6th
□	□	*	*	□	*

3. Please enter the last four digits of your home telephone number

Figure 16: showing a successful https (ssl) connection to the registration page www.365online.com. The lock at the bottom of the screen confirms that this page is using ssl.

3. Assignment 3

3.1 Introduction

As mentioned in Section 1, senior management has become very concerned at recent security breaches at top companies and state organisations across the world. With hackers such as Kevin Mitnick (http://www.kevinmitnick.com) gaining such a notoriety and popularity, attempts at compromising GIAC's security will become more frequent and without doubt more intelligent. Consequently, as part of the "Internet Upgrade Project" the Internet Infrastructure team have been commissioned to audit their external firewalls.

3.2 Audit Plan

3.2.1 The Audit

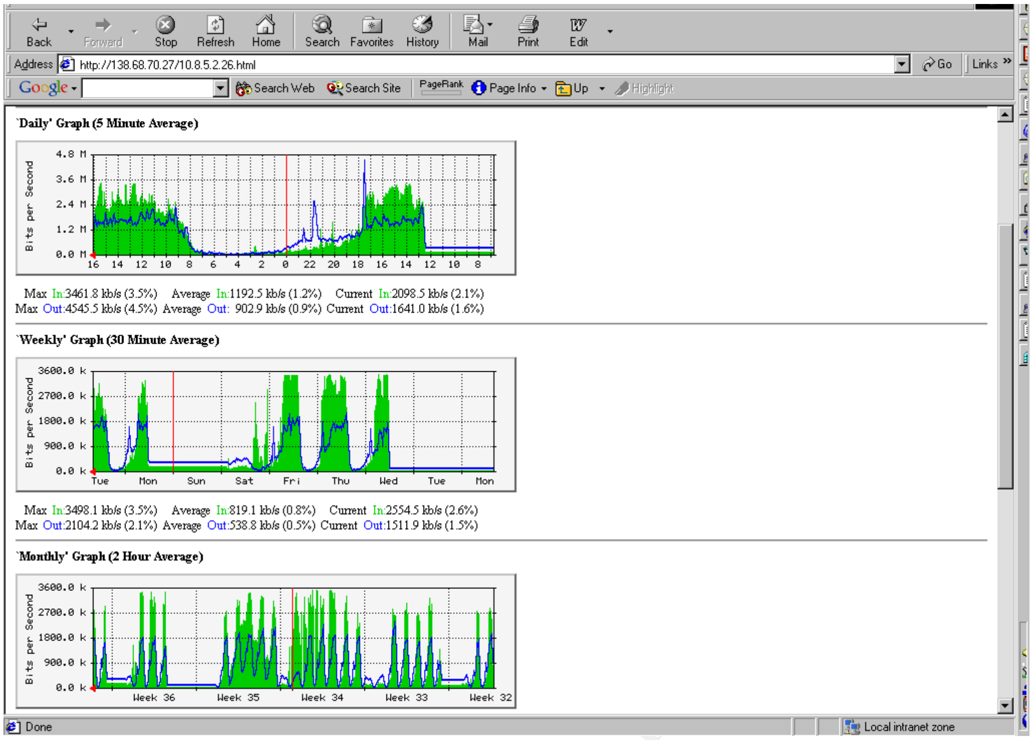
It is intended that this audit will ensure that if any holes have been left in the configuration of the new external firewalls they will be found and rectified. As a result, GIAC will have very secure firewalls at its external perimeter, providing reassurance to senior management that their substantial financial investment has not been in vain and that everything that is possible has been done to prevent an internet security breach at GIAC. We again look to documentation done by Lance Spitzner[10], for advice in planning our audit.

We want to ensure that the firewall itself is secure, but also we want to verify what traffic can pass through the firewall. With this in mind, we have chosen to audit the firewall from three vantagepoints –

- DMZ
- LAN
- EXTERNAL

The Snort IDS servers and sensors will be monitored throughout the audit. Snort should alert on all of the scanning and hacking attempts. The Operations team is aware (and has received extensive documentation) of the internal audit and so has been instructed to follow normal procedure for alerts, except that we (the audit team) are the first contact-point. Indeed, documentation has been provided to the operators. There will be communication with the Operations team throughout the audit.

[10] http://www.enteract.com/~lspitz/audit.html – Lance Spitzner's "how to audit a firewall" paper.



`Daily' Graph (5 Minute Average)

Max In:3461.8 kb/s (3.5%) Average In:1192.5 kb/s (1.2%) Current In:2098.5 kb/s (2.1%)
Max Out:4545.5 kb/s (4.5%) Average Out: 902.9 kb/s (0.9%) Current Out:1641.0 kb/s (1.6%)

`Weekly' Graph (30 Minute Average)

Max In:3498.1 kb/s (3.5%) Average In:819.1 kb/s (0.8%) Current In:2554.5 kb/s (2.6%)
Max Out:2104.2 kb/s (2.1%) Average Out:538.8 kb/s (0.5%) Current Out:1511.9 kb/s (1.5%)

`Monthly' Graph (2 Hour Average)

Figure 17: showing the typical traffic profile for the link between the MerdeNET BGP router and the primary GIAC BGP router.

3.2.2 Timing

Using MRTG on the external GIAC BGP routers (see Figure 17), we have been able to analyse the traffic profiles from the Internet to GIAC and vice-versa. It is clearly evident that there is very little traffic between the hours of 2am-6am (Sunday) and, as a result, it has been decided to run the audit between those hours. All back-ups will run have been finished at 1am, slightly earlier than normal but this will ensure that if any problems arise we will be able to revert back to our old configurations very quickly.

A message (see below) will be posted on the web-site to inform customers that service is only temporarily affected. All suppliers, partners and internal staff will be made aware that the service will be unavailable for those 4 hours.

> **"Unfortunately due to necessary maintenance and testing, the www.giac.com will be unavailable from 2am to 6am, 13/10/2002. If you have any questions, please do not hesitate to contact the GIAC Helpdesk on 0035391-549834 or helpdesk@giac.com."**

Senior Management has signed off on the change. Additionally, a non-waiver clause has been added so that if the "audit team" cause a prolonged outage of service the "audit team" will not suffer any consequences.

3.2.3 Audit Team & Costs

The audit team is made up of individuals from various GIAC infrastructure teams, as there will be a need for knowledge of all parts of the infrastructure during this audit (especially if there are any problems).

Department	No. of representatives	Responsibilities	Cost
Network Design	1	All of GIAC Network (audit – switches, routers)	60 euro p/h + lunch
IT Security	1	Secuirty of GIAC Network	60 euro p/h + lunch
Internet Infrastructure	1	GIAC Internet Network	60 euro p/h + lunch
NT Server Support	1	All NT servers in GIAC (audit - GIAC webservers)	60 euro p/h + lunch
Unix Support	1	All Unix servers in GIAC (audit – o/s of firewalls and most of Internet Intfrastructure)	60 euro p/h + lunch

Cost for staff to scan the firewall = (60*7^)*5 + 20*7=2140 euro

^ the figure 7 comes from the 1.5 hours testing of network and servers before the audit; the four hours of the audit; and the 1.5 hours of auditing and testing afterwards.

It is estimated that the planning process involved 3 man-hours per person, i.e. 15hours in total.

Moreover, the process of collating the data, analysing the results and making recommendations is estimated to require 4 man-hours each, which is a total of 20 hours (again 30-euro p/h).

Although this audit will incur substantial financial costs and also result members of the "audit team" being unable to do their normal work the following day, senior management feels that if they pay up now and follow the correct security procedures, they are preventing pain further down the line.

3.3 Modus operandi

3.3.1 The Audit

Having verified that all GIAC Internet services are working, the team will begin to audit the firewall using the various tools – all team members will be actively involved. With such diversity in skills and knowledge, we believe that all security vulnerabilities will be covered and understood, thus making the audit more thorough and reliable. We

> ***"want to test the firewall itself…"***[11]

and

> ***"secondly…what traffic can pass through the firewall."***[12]

We will audit the firewall from inside GIAC, the GIAC DMZ, from the Internet, firstly as a VPN user and secondly, as a user from a dial-up ISP. We have two laptops, each with a dual boot of Red Hat Linux or Windows 2000 and various security tools (see below) installed.

3.3.1.1 Tools

3.3.1.1.1 ISS Scanner (http://www.iss.net)

ISS (version 6.2.1) is a scanner, which although free itself requires a licence that costs $1000 but is very good at identifying o/s vulnerabilities. We felt this was small amount of money in the grand-scheme of the GIAC upgrade and this tool will help us ensure our network is correctly configured and secure. Although slightly duplicating Nessus and Nmap to a degree, we felt it would complement them well and help us ensure those existing vulnerabilities and as many potential ones as possible are tested.

On the next page, is a screen shot of us setting up the ISS scanner. We put the IP addresses of the external firewall interfaces and the web-servers in the scanner's hosts file so that we not scan the firewall itself but also through the firewall. We, therefore, ran a "Unix and Firewall" scan, see Figure 19.

[11] http://www.enteract.com/~lspitz/audit.html – Lance Spitzner's "how to audit a firewall" paper.
[12] http://www.enteract.com/~lspitz/audit.html – Lance Spitzner's "how to audit a firewall" paper.

Figure 19: configuring the full Unix and Firewall scan.

3.3.1.1.2 Nessus (http://www.nessus.org)

Nessus is constantly receiving praise as an excellent vulnerability scanner. Plus, it is FREE. For those new to Nessus, there is introduction documentation at http://linuxsecurity.com/feature_stories/nessusintro-part1-2.html and http://www.linuxsecurity.com/feature_stories/nessusintro-printer.html, both by Banchong Harangsri.

The “audit team” ran the Nessus server on a Unix o/s (located externally on the Internet), while the client was on the laptop. Although Nessus uses nmap to find open ports, it also lists potential vulnerabilities that the host could be subject to, while nmap only reports if the ports are open.

3.3.1.1.3 Nmap (http://www.insecure.org/nmap)

The following documentation was used as a guide in configuring and using nmap –
http://www.insecure.org/nmap/lamont-nmap-guide.txt
http://www.insecure.org/nmap/nmap.usage.txt

Below are some of the common nmap scan types -

Nmap Option	Description
-sU	UDP port scan
-sX	TCP FIN URG PUSH scan
-sS	TCP SYN scan (reported to be the best all-around TCP scan)
-F	Only scans ports listed in nmap-services
-sP	PING scan
-sF	Stealth TCP FIN scan
-sT	Basic TCP Connect scan (default)
-O	Guessing the operating system of the target, using TCP/IP fingerprinting
-p <range>	Telling nmap what ports to scan
-v	Verbose – its use is recommended. (-vv for very verbose)
-p0	Don’t ping ho
-Ddecoy_host1_decoy2[,..]	Hide scan using many decoys
-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane>	General timing policy
-n/-R	Never do DNS resolution/Always resolve
-S <your_IP>/-e <devicename>	Specify source address or network interface
--interactive	Go into interactive mode
-ON <filename>	Converting the nmap output to a more readable format

3.3.1.1.4 CIScan (http://www.cisecurity.org)

GIAC used the "Solaris Benchmark" v1.0.1b software tool for scoring and monitoring the status of benchmark settings at the network and system level of the Gauntlet Firewalls. These tools are available freely as part of the CIS Solaris Download package. The CIS scan tool will enable us to verify the security and configuration of our Solaris 8 operating system.

3.3.1.2 Patches

With the majority of staff on the Cert (www.cert.org), Bugtraq (www.bugtraq.com), SANS (www.sans.com) and individual vendor mailing lists, the "Audit Team" are well aware of the present vulnerabilities. In preparation for the audit, we have thoroughly researched the present Gauntlet vulnerabilities and we try to exploit them. At this stage, we have all latest Gauntlet 6.0 and Solaris 8 patches installed.

3.4 The Audit

3.4.1 Verification

We have verified that all of GIAC's internal and external Internet services are working, as they should be. Additionally, all back-ups have been successfully completed. The Operations team has given sign-off.

3.4.2 BGP

As part of the external audit, we verified our BGP configuration by testing its failover and alerting capabilities. We simply dropped the interface on the switches connecting the GIAC routers with the firewalls, firstly, and secondly, with the ISP routers. When dropping the interfaces on the ISP side, we received calls (within ten minutes) from both MerdeNET and MauvaisNET's NOCs as our link had dropped.

3.4.3 SMTP

Having Gauntlet as the external firewall, we must connect to it for smtp, as it prevents us from connecting directly to the mail server. We have installed all the latest csmap patches on Gauntlet (downloadable from www.securecomputing.com/index.cfm, using your company's grant number) and set up extensive anti-spam and anti-relay measures, through both the ordb.org site and the Gauntlet-Firewall Manager anti-spam and anti-relay settings. We are verifying csmap because there have been known recent numerous vulnerabilities. For example, the latest patch dealt with a message truncation issues caused by premature session termination and fixed the child spawning issue (April, 2002).

Using ordb.org we sent several spam-emails and saw that Gauntlet dropped the mail immediately. Additionally, we telneted on port 25 to the firewall and tried to use as a relay agent for hotmail, yahoo email accounts and were immediately rejected.

Finally, we attempted to use “expn” and “vrfy” commands on Gauntlet but it did not permit us, as we hoped. Using these commands, a hacker or spammer could easily find out valid giac.com email addresses. The vrfy command allows an attacker to keep trying email addresses until he/she finds a valid one, which is not too difficult considering that email addresses follow well-known patterns. The expn command can be used to get the names of the users of a machine – even more dangerous (http://www.burningvoid.com/iaq/expn-vrf.html). As a side-note, we also verified these commands on both the Mimesweepers and the internal mail server, which also rejected us.

3.4.4 DNS

Using nslookup we can attempt to transfer a whole giac.com zone file using the **ls** command, we can attempt to carry out a zone transfer of the giac.com domain. We have already asked the IP team in MerdeNET to verify they can do a zone transfer from sec01.ns.merde.net and they have confirmed a successful pull. Mauvais have confirmed likewise for the tertiary, auth01.ns.mauvais.net.We then try to pull the giac.com zone file from several locations on the Internet and we fail every time. For example,

```
>nslookup
Default Server ns.exter.net
Address: 69.63.69.34
> ls giac.com
*** Can’t list domain giac.com.
```

Running Nessus we attempt to do a zone transfer and find out information regarding BIND, however, we are again unsuccessful.

3.4.5 VPN

We try to log on from several IP addresses, that don’t belong to a partner, or the MerdeNET IP pool, however, the Gauntlet firewall drops our connection each time. We then run tcpdump, on the laptop, sniffing for VPN traffic intended for giac.com and try to piggyback on the connection, but SecureClient never allows us to do this. We are satisfied with our the security for our VPN and database servers.

3.4.6 From Dial-up

Running a nmap TCP Syn scan, while also trying to guess the O/S, we have discovered that we only have five ports open. This is what we expected to see, as these are the five ports we have decided on opening on the external interface.

```
hillickm@giac$ sudo nmap -sS -O 186.69.69.36

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
```

```
Interesting ports on  (186.69.69.36):
(The 1021 ports scanned but not shown below are in state: filtered)
Port       State       Service
25/tcp     open        smtp
53/tcp     open        domain
80/tcp     open        http

443/tcp    open        https
500/udp   open            ike
1024/tcp   closed      kdm
1025/tcp   closed      NFS-or-IIS
1026/tcp   closed      LSA-or-nterm
1027/tcp   closed      IIS
……………………
 …………………..
65301/tcp  closed      pcanywhere
Remote operating system guess: Solaris 8 early access beta through
actual release
Uptime 2.075 days (since Thu Aug 22 01:37:51 2002)

Nmap run completed -- 1 IP address (1 host up) scanned in 809 seconds
```

As you can see we were able to guess the o/s version on the firewall, however, when we ran nmap against the whole 186.69.69.0/24 subnet the firewall blocked us from guessing the o/s version of the web-servers or anything-else behind the firewall, such as our mail server.

In keeping with the “testing not only the firewall but also through the firewall” policy we send traffic for a slightly incorrect giac.com URL, though to the web-server. Apache has been known to return its web-server version to users when a user types in a slightly incorrect URL. We to our amazement find that giac.com does this. This change is carried out immediately and is detailed in Section 3.5.7.

Unsurprisingly, Nessus agrees with Nmap in that we have seven ports open for service and it warns us about snmp vulnerabilities. However, taking into account our strict rules, based on IP restrictions and bound interfaces and the business accept the risk because given recent events on the Internet they want all logs, including those from the routers. Moreover, we are denying both snmp and ntp at the external router interface.

3.4.7 From DMZ

By auditing the firewall ruleset from the DMZ we are replicating a hacker’s attack on a web-server whereby they get control of the web-server and from there try to do further damage across the whole network. By restricting what the web-servers are permitted to do, via the firewall rulesets, we reducing the options a hacker has.

Running nmap to see what ports the firewall is listening to on its DMZ interface – we see that the firewall dmz interface is listening on ports 80, 443, 123 and 1500. However, when we try to initiate a connection out to the Internet from the DMZ (on any port) we are blocked by the firewall rules. The Gauntlet logs confirm this by showing that it dropped the traffic and complaining about “a security alert on the unserved DMZ interface”.

The only connections out that something on the DMZ subnet can make is for NTP and TSM back to the NTP and TSM servers on the LAN. We tried to send NTP and TSM traffic to the Internet but Gauntlet dropped the traffic and logged it as a security alert on the external interface.

3.4.8 From Inside GIAC

A substantial number of hacks are initiated by company-insider, usually a disgruntled employee. As a result, we wanted to test what a normal user could access from the PC on the LAN.

The Audit Team attempted to connect directly from the LAN (using subnets other than that of the firewall administrators, including those of the TSM and NTP servers) to the firewall using a variety of protocols such as http, ssl, telnet, ssh *et al.*. Thankfully all these attempts were denied by the Checkpoint Firewall first. Changing the default route off the LAN from the Internal Firewalls to the external firewalls, we repeated our tests but this time our packets were dropped by the Gauntlet firewall. The TSM and NTP servers could not initiate a connection to the firewalls or other Internet servers, only respond to a Syn.

3.4.9 Further Audits

It has been decided that this audit should be conducted on a monthly basis. This new schedule has been agreed between the various teams and received approval from GIAC senior management. Additionally, with GIAC about to embark on a major marketing and expansion plan worldwide, Internet Security will become more important. As a result, GIAC have agreed to employ an external IT security firm to conduct independent scans and attempted hacks of the GIAC Infrastructure on a quarterly basis. In these further audits, as we become more experienced we will invoke BRP failover procedure so that the GIAC customers, who are becoming increasingly diversified in their geographical location, will not be affected.

3.5 Recommendations & Changes

3.5.1 IDS Sensors

The IDS sensors, as evidenced in the audit, have proved to be very effective and GIAC are happy that the Snort detection system provides the:

- Ability to perform at traffic rates experienced at real-world traffic rates
- Ability to identify known exploits and detect potential vulnerabilities
- Ability to correlate and understand typical GIAC network traffic

However, we feel that host IDS is essential to completely benefit from installing IDS. For instance, we know the firewall will allow port 443 attacks through to the web-server because it sees it just as port 443 traffic and we know the web-servers are hardened, though we cannot be completely sure the attack has been thwarted. Therefore, we are installing the host version of Snort on the web-servers, external and internal firewalls.

In addition, we need to fully ensure that we are only receiving authorised vpn traffic. As a result, we will place network snort on the external connections to the vpn/internal firewall for the database, web and mail vlans.

3.5.2 Closing Port 80

Closing of port 80 as it simply gives the hacker another option of attack and as we do not need port 80 to be open for incoming traffic (that has been initiated on the Internet) we will close it on both the BGP routers and external firewalls. We have received crucial sign-off after showing them the costs caused by the Nimda virus (done over port 80) and the Snort IDS logs, which indicated out we, are being bombarded by Nimda-like attacks every day.

The business section in GIAC had wanted port 80 left open so that external customers, who typed “http” as opposed to “https”, would be re-directed by the web-server to the correct page. We, therefore, remove the “http” service from proxy rule 3, disable the http proxy altogether.

3.5.3 Gauntlet GUI

It is a well-known fact that Gauntlet listens on TCP port 8004 (on all interfaces) for the GUI. Why should we make a hacker’s life easier? We are using the filter rules to deny it externally.We will, therefore, change the Gauntlet configuration so that it listens on a different high port.

3.5.4 Apache

We have made the Apache configuration change so the Apache server returns minimal information about itself, which does not include its version number. We run the “incorrect URL” test again and we did not receive any information about Apache.

3.5.5 TCP wrappers

Although it is free piece of third-party software, we are following the CIS recommendations and installing this key security tool. We will build the wrappers on a box on the LAN as there needs to be a C compiler on the box, which we don't want on the firewall, as it would make it easier for attackers to import software onto the system. We will copy the tool onto the firewalls and other target machines via ssh over the network. These TCP wrappers will enable us, as administrators, to control who has access to various network services based on the IP address of the remote end of the connection. The TCP wrappers are generally triggered out of /etc/inet/inetd.conf.

3.5.6 Gauntlet Patches

During the audit a new patch for BIND on Solaris 8 came out – http://sunsolve.com/pub-cgi/show.pltarget=patchpage. We, therefore, install this patch in test first, where it goes through extensive testing – including trying to exploit the vulnerability it is supposed to fix. When we are happy, we change-control the patch, install it and then try to exploit the vulnerability on the production firewalls. The patch (as all firewall patches are) will be installed out of working-hours.

Additionally, we have to be particularly wary of keeping our Gauntlet firewalls up-to-date with "csmap" patches as this has been a well-known vulnerability on Gauntlet and been subject to successful denial of service attacks.

3.5.7 Qualys Free Sans Top 20 Scanner

Just after the audit was finished, Qualys introduced a scanner, https://sans20.qualys.com/index.php?lsid=340, which scans for the "San/FBI Top 20 Vulnerabilities" list published on 27th September (version 2.6), http://www.sans.org/top20. Although these vulnerabilities are known, they are still frequently used and many networks are still vulnerable to them.

You can run the scan from your desktop, through your browser, where the results will be published within 10 minutes.
This will be an invaluable tool and will be included this tool in all further audits.

4. Assignment 4

4.1 Chosen Practical

I have chosen Stephen Monahan's practical[13], for my test attack. Stephen has designed a pretty secure network and as he is GIAC certified, the network will be secure and keep up-to-date with patches so we have a stern test ahead but we'll see what we can find out.

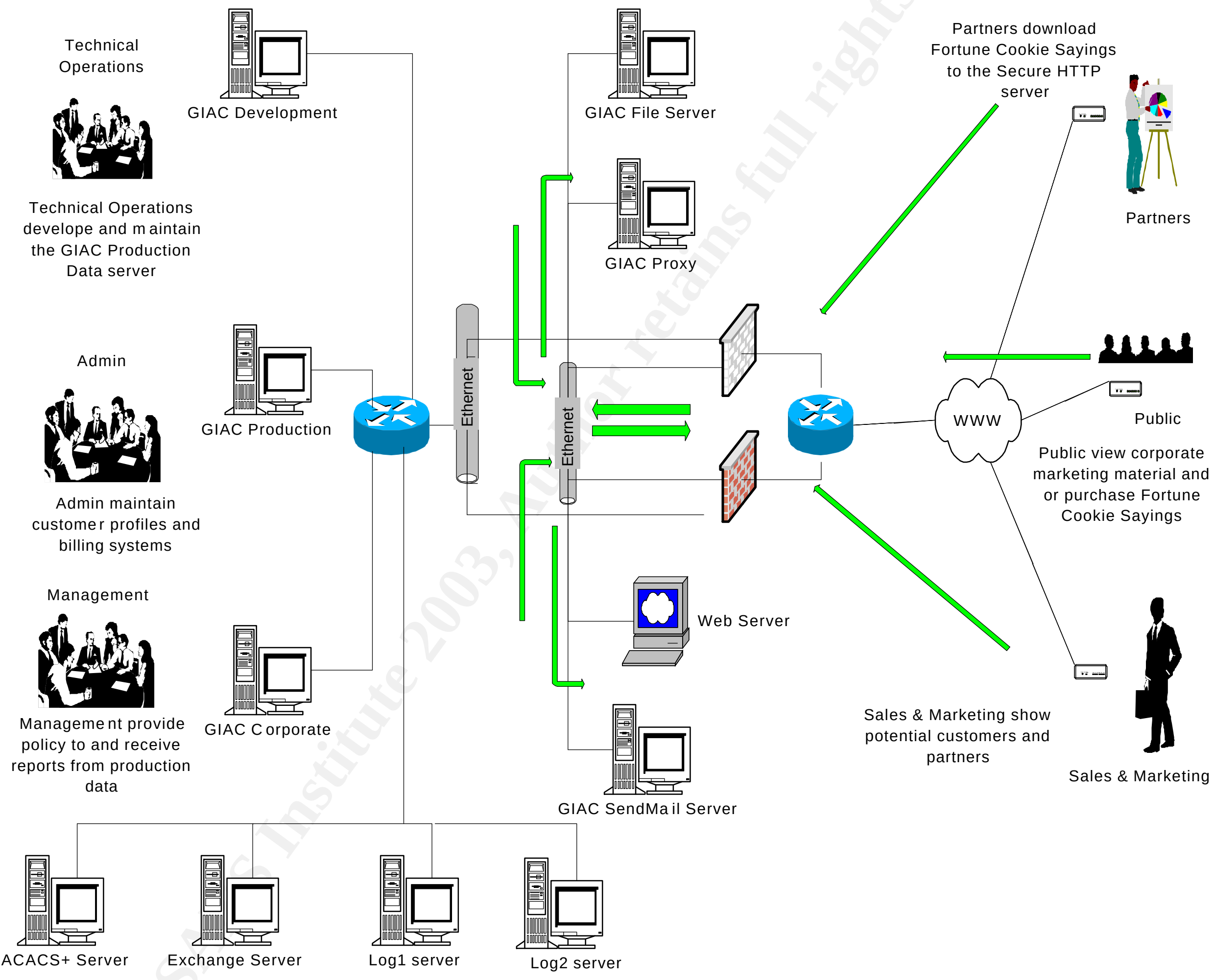

Technical Operations
GIAC Development
Technical Operations develope and maintain the GIAC Production Data server
Admin
GIAC Production
Admin maintain customer profiles and billing systems
Management
GIAC Corporate
Management provide policy to and receive reports from production data
GIAC File Server
GIAC Proxy
Ethernet
Ethernet
Web Server
GIAC SendMail Server
Partners download Fortune Cookie Sayings to the Secure HTTP server
Partners
WWW
Public
Public view corporate marketing material and or purchase Fortune Cookie Sayings
Sales & Marketing show potential customers and partners
Sales & Marketing
TACACS+ Server
Exchange Server
Log1 server
Log2 server

Figure 20: Stephen Monahan's practical.

Throughout our attempted-hack we will be using several dial-up accounts, while also relaying off a compromised intermediate system so as not to arouse suspicion.

As part of the GIAC.com research, the Economist, Fortune, Bloomberg, Reuters and CNN have been read regularly. I now have a good profile of GIAC and where they

[13] http://www.giac.org/practical/Stephen_Monahan_GCFW.doc

conduct business. As a result, I reckon their busiest hours are 10am-3pm and the least, 12am – 6am. Therefore, most of information gathering will be carried out between 12am and 6am. Additionally, it is unlikely that GIAC, being a small fortune cookie company, have a 24hour NOC actively monitoring the alerts.

4.2 Firewall Attack

We have discovered the following vulnerabilities for the Cisco PIX firewall.

Reference Website	**Vulnerability Description**
http://www.kb.cert.org/vuls/id/6733	A problem that was first discovered in 1998 and has again returned. This time a common configuration in PIX could allow a hacker to bypass the firewall.

We are assuming that Stephen (as he is GIAC qualified) has the latest patches on his Cisco firewalls. However, as this vulnerabilities has been first around since 1998, I believe that it may not be fruitless at all to try to exploit some of these vulnerabilities since Cisco may not have fully resolved this issue.

We want to find out as much information as possible about GIAC.com before going for a fully-fledged attack. Therefore, we run "nslookup" to retrieve information GIAC's domain.

```
#nslookup
>www.giac.com
Server: ns202.merde.net
Address: 186.69.56.56
208.10.2.3
>set q=ns
>giac.com
Server: ns202.merde.net
Address: 186.69.56.56
>set type=MX
Server: ns202.merde.net
Address: 186.69.56.56

Non-authoritative answer:
entropy.ie      preference = 15, mail exchanger = smtpstore.esat.net
entropy.ie      preference = 25, mail exchanger = mxbackup.esat.net
entropy.ie      preference = 10, mail exchanger = mail.giac.com

Authoritative answers can be found from:
rte.ie  nameserver = ns2.giac.com
rte.ie  nameserver = ns1.giac.com
mx.rte.ie       internet address = 208.10.2.2


Non-authoritative answer:
giac.com nameserver=ns.giac.com
ns.giac.com internet address= 208.10.2.4
```

```
Now we try to do a zone transfer
> ls giac.com
*** Can't list domain giac.com.
```

Unfortunately (but as expected) it did not work, as the firewall is blocking all zone transfers. At least, we know the IP address of his dns server and web-server. We, therefore, now know more about his addressing schema. This can great help us in mapping the GIAC network.

Running nmap against the external interface of Stephen's router, we see the following ports are open –

21	FTP
22	SSH
25	SMTP
53	DNS
80	HTTP
123	NTP
110	POP3
443	HTTPS
614	SSH Shell

With the above ports being open, I can make a connection to the web-server on port 80 or 443, mail server on port 25, dns server on port 53 (udp) and more. If we have a legitimate connection to any machine on Stephens's network, we can then connect from our outside host to the inside host on any port. So far, we are unlikely to have attracted any attention as we have only been running 2 nmap scans and perfectly legal DNS lookups.

We, therefore, make a legitimate connection on http and ssl to the web-server. We then try connecting to the web-server for other services, such as netbios or snmp, which if successful would enable us to do some serious damage. It appears Stephen's firewall is vulnerable and we bypass the firewall as the "**established**" command allows these connections through, however, the web-server rejects us as it is only listening on ports 80 and 443. We fare no better with the sendmail server, which has been locked down to port 25 only.

We leave our attack for a couple of days and do some more research on the vulnerability and how best to exploit it. Remembering that GIAC is listening for ftp on the external side, we realise the possibilities if we can establish an ftp connection to an ftp server behind the firewall. However, when we try to exploit the firewall vulnerability (from a different dial-up account, in case our previous attacks were noticed and that the IP address is blocked) we find that the firewall is denying our attempts to open up a second connection. It appears that GIAC has detected our attacks and implemented Cisco's fix, using the **permitto** and **permittfrom** keys.[14]

[14] http://www.kb.cert.org/vuls/id/6733

From our research though, we remember that this still allows us to make a second connection, over the established connection, on open ports such as http, ssl etc. Consequently, we decide to note this down and consider a new attack, using solely port 80.

4.3 Denial of Service Attack

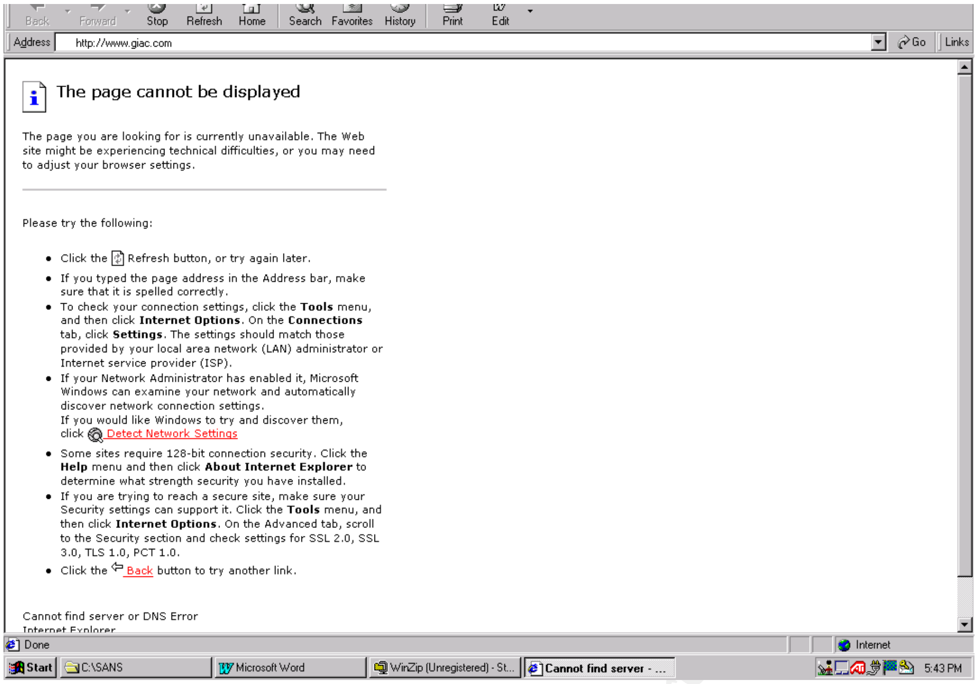
4.3.1 The Attack itself

The Tribal Flood Network tool (TFN2K) is a very useful Distributed Denial of Service (DDOS) tool (by Mixster), which we will use in designing an attack from 50 compromised cable modems. We downloaded TFN2K from http://packetstorm.security.com/distributed, which has a substantial number of DDOS tools. Stephen Carroll's SANS project, - http://www.giac.org/practical/Stephen_Carroll_GCFW.doc, was used as research in using TFN2K to carry out the DDOS attack, though the excellent http://staff.washington.edu/dittrich/misc/ftn.analysis formed the basis for configuring and running TFN2K.

Communication between TFN clients, handlers and agents is done using ICMP ECHO and ICMP ECHO REPLY packets.

From researching GIAC's business, it is felt that they most probably have a T1 link to the Internet. With a 1.55MB link we reckon we can successfully run a denial of service. From our earlier nmap scans, there are quite a few ports open on the external router. Having been sniffing traffic entering and leaving GIAC, their traffic appears to peak around 1pm. We are going to run the actually DDOS attack around 1pm since it will be easier to flood the network at this time with so much traffic already hitting and leaving GIAC. More importantly, an attack at this time will have the biggest effect as most business is being conducted now. Although the GIAC NOC will be better manned at 1pm than say 12am, we felt that with the additional traffic already there it will be easier to crash the GIAC service. Furthermore, at 1pm, people are usually breaking for lunch and vice-versa and, as a result, there are slightly fewer people there, while the people there are other thinking about lunch or distracted because they are just back from lunch.

We begin our attacks from the 50 cable modems. After about 30 minutes, we quickly notice that the GIAC.com is not resolving (see figure 22). We have either knocked the web-site off the air by fully utilising the bandwidth or causing the firewall CPU to reach its maximum. Either way we have succeeded in our DDOS attack.



http://www.giac.com

The page cannot be displayed

The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.

Please try the following:

- Click the Refresh button, or try again later.
- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- To check your connection settings, click the **Tools** menu, and then click **Internet Options**. On the **Connections** tab, click **Settings**. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
- If your Network Administrator has enabled it, Microsoft Windows can examine your network and automatically discover network connection settings.
  If you would like Windows to try and discover them, click Detect Network Settings
- Some sites require 128-bit connection security. Click the **Help** menu and then click **About Internet Explorer** to determine what strength security you have installed.
- If you are trying to reach a secure site, make sure your Security settings can support it. Click the **Tools** menu, and then click **Internet Options**. On the Advanced tab, scroll to the Security section and check settings for SSL 2.0, SSL 3.0, TLS 1.0, PCT 1.0.
- Click the Back button to try another link.

Cannot find server or DNS Error
Internet Explorer

Figure 22: showing the giac.com web-site off the air.

We cannot connect to GIAC mail server either on port 25 –

```
# telnet 208.10.2.2 25
Trying 208.10.2.2...
telnet: Unable to connect to remote host: Connection timed out
```

4.3.2 Countermeasures

Although not a direct measure to a DOS attack, but it will undoubtedly help, it must not be forgotten that staff must

- Thoroughly document all configurations, changes and be proactive about their systems as opposed to reactive.
- Receive substantial training, such as SANS (GIAC Certification), CCISP (Certified Information Systems Security Professional), but also vendor-specific training for Checkpoint NG, Cisco PIX, Gauntlet etc.
- Enrol on both the vendor (Sun, Gauntlet and Cisco) and independent security mailing lists (SANS, Cert and Bugtraq).

This will reduce the likelihood in incorrectly configuring rulesets, ACLs etc. but will also keep the system administrators/engineers up-to-date with new attacks and vulnerabilities.

- Ensure that both the O/S and the software on the box have the latest patches.
- Using the Stonebeat (www.stonesoft.com) that we have used in our GIAC environment will enable a dynamic fail-over. Additionally, a BGP solution with two

separate ISPs greatly counters a DDOS attack. There should be no single point of failure.

- As we have been saying throughout this document, only allow those services needed for business – close all ports that are not needed.

This subsequent information will seem very familiar, as it is essentially in Section 2.1. Some measures include the ingress and egress filtering, which we implemented in Section 2.1 such as,

- Block the non-routable private internet address ranges
- Deny any loopback traffic
- Disable ICMP on the external routers and deny ICMP on the external firewalls
- Deny GIAC routable address space – 186.69.69.0/24
- Deny (IANA) reserved address space

Although these are valid anti-DDOS measures, it has to remembered that any decent hacker will not use these addresses as its source, but is more likely to use an IP address of at least one, probably more, innocent internet-user.

- With spam becoming so prominent and wasting so much bandwidth, employing an anti-spam solution such as relays.ordb.org would be very useful against a DOS attack. It would also be wise to put a block on all emails above 5MB (such a scenario on MAILsweeper can be easily configured).

Using the *"Rate Limit"* command (on the BGP routers) we can limit the traffic on our links. For example, with a 2M link one can *rate limit* SMTP so that it never uses more than 1M. As a result, one could *rate limit* ICMP or anything else that is non-critical and could be used in DOS attacks.

4.4 IIS Attack

4.4.1 Why have we chosen the web-server?

The vast majority of websites are accessed using http, non-secure traffic. It can leave quite a few security holes that can be exploited by a hacker. One only needs to think of Trojans and Worms, such as Nimda and Code Red, to see the damage that can be caused by port 80 attacks. Nimda and Code Red are still bombarding companies across the world.

In his practical Stephen does not state the version of his web-server, however, if we were a hacker we reckon that it is either an Apache or Microsoft IIS web-server as almost 90% of web-servers are either Apache or IIS servers (see figure 22). Using the Netcraft site, we are told that the web-server is Windows 2000/IIS 5.0.

4.4.2 The Attack

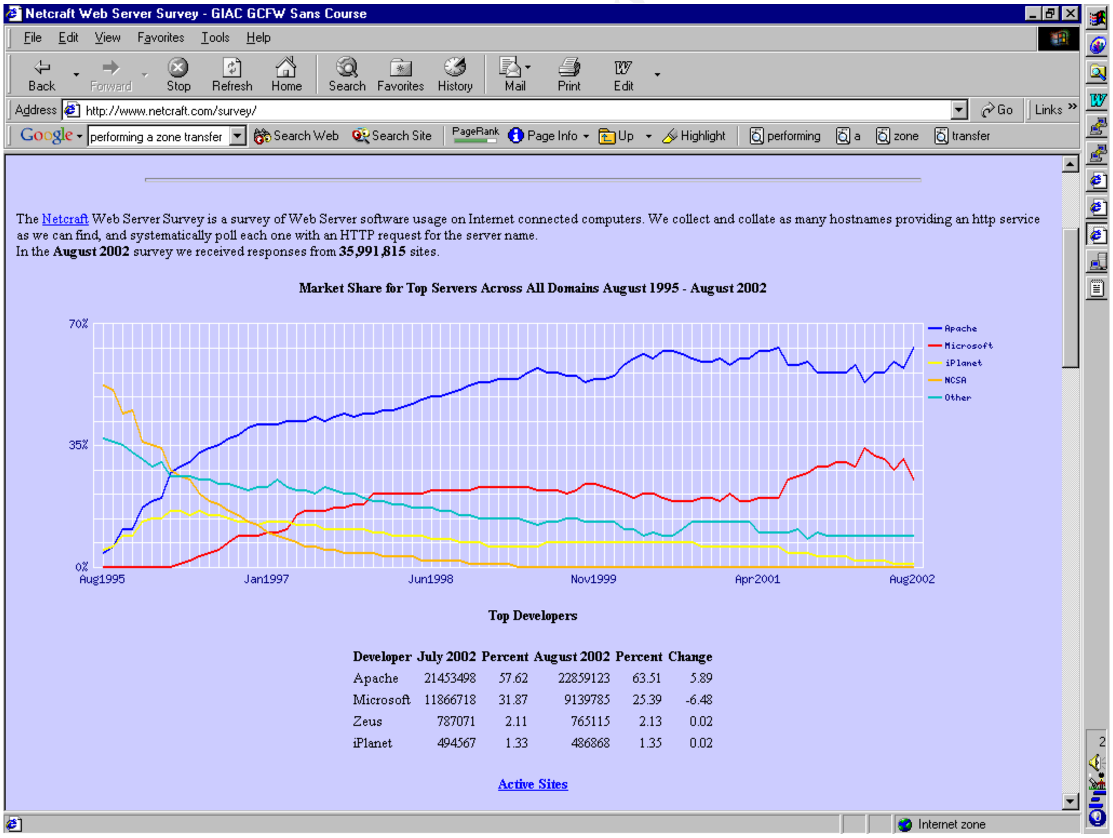
Running nmap against the web-server (know the IP address from our earlier nslookup commands), which we are sure is listening on ports 80 and 443, from a dial-up –

- nmap –v –xX –P0 –p80 208.10.2.3
- nmap –v –xX –P0 –p443 208.10.2.3

We verify that GIAC.com firewalls are listening on port 80 and port 443 and nmap says that his o/s is Windows 2000. We did not want to arouse suspicion so we only scanned ports 80 and 443. At present, our goal is to gather information. As we only needed to run the above nmap commands once, they should not arouse suspicion and will not alert on IDS as an attack as this is normal (port 80 and 443) traffic allowed in.

So far, our attacks have been infrequent and varied, while we have been carrying out innocuous scans as we are merely seeking information.

Before running a full scan with Nessus and IIS, we want to get more information while we are still unnoticed because a scan is more likely to be noticed.



The Netcraft Web Server Survey is a survey of Web Server software usage on Internet connected computers. We collect and collate as many hostnames providing an http service as we can find, and systematically poll each one with an HTTP request for the server name.
In the **August 2002** survey we received responses from **35,991,815** sites.

Market Share for Top Servers Across All Domains August 1995 - August 2002

Top Developers

Developer	July 2002	Percent	August 2002	Percent	Change
Apache	21453498	57.62	22859123	63.51	5.89
Microsoft	11866718	31.87	9139785	25.39	-6.48
Zeus	787071	2.11	765115	2.13	0.02
iPlanet	494567	1.33	486868	1.35	0.02

Active Sites

Figure 22: screen shot from www.netcraft.com/survey showing the web-server market share.

Knowing that only ports 80 and 443 are open on this web-server, we carry out some port 80 fingerprinting attacks.[15]

We begin with a common fingerprint and try to gather a list of the log files with
http://www.giac.com/index.asp?something=..\..\..\..\WINNT\system32\cmd.exe?\c+DIR+E:\WINNT\*.txtp

We get some .txt files back but they are essentially useless, all the important logs seem to be denied to us or transferred off the box. Moving on, we expect the box is hardened against Nimda or Code Red, though we try to access the root.exe backdoor
http://www.giac.com/scripts/root.exe?/c+dir+c:\

Again we are unsuccessful, though we try to get retrieve the SAM file from the box utilising the following attack.
http://www.giac.com/index.asp?something=..\..\..\..\WINNT\system32\cmd.exe?\c+DIR+E:\WINNT\system32\config\

If we get this file, we will use L0phtcrack http://www.atstake.com/research/lc/ to do a brute-force attack to obtain user logins and passwords. As the file will be on our box and off the Internet, no one will detect us – GIAC will not notice our cracking attempts.

Again we are permitted through the firewall, as it is port 80 traffic, however, the patched web-server again denies us. Not disheartened we move on to some more advanced techniques. These may not succeed but they will fill up the logs quickly. Below is an example–

*http://www.giac.com///

Here we are looking for the autoexec.bat, so that we can clear logs etc. so that no one knows we were ever on the web-server. At this point, we notice our traffic appearing to be denied. Wondering what happened, we try to access the giac.com web-site via a browser, we notice that the site is down. It seems we successfully knocked the box over, most probably by filling the logs up so quickly. We try to telnet to the web-server on port 80 but are rejected –

```
# telnet 208.10.2.3 80
Trying 208.10.2.3...
telnet: Unable to connect to remote host: Connection timed out
```

Grasping the chance that the GIAC team will be concentrating on their web-server we now run Nessus and IIS, against the sendmail-server (we figure it out from earlier information garnered through nslookup). We try all our various dial-up accounts, but it appears that these are all being blocked by the GIAC router – we have definitely been spotted and GIAC have checked their firewall logs, noted all our IP addresses from our various attacks, and blocked them. A fellow hacker later confirms that the GIAC web-site suffered a 40-minute outage. Although we were unable to retrieve sensitive information

[15] http://cgisecurity.com/papers/fingerprinting-2.html

such as passwords or gain control of the web-server, we did show how the firewall can be compromised so-to-speak and we did knock out the web-service by filling the logs.

With GIAC seeming to be on high alert, we decide to lie low for a while and hit the beach! We are disappointed as our attack was cut short and we didn't have much success but we have to cut our losses at this point. We decide to pick an easier target next time and not someone who is GIAC certified. In the meantime, we head back to the drawing board to improve our scripting and hacking skills.

4.4.3 Countermeasures

To ensure that an attack does not succeed on the web-server, the system administrators should firstly, ensure that the web-server is kept up-to-date with patches by being on the relevant vendor and security bulletins. With proper training as well, the web-server will be correctly configured and more secure.

Not only should an IDS solution be installed, but also a proper Incident Response team should be created to manage IDS. They should understand the alerts and know how to react and who to contact (i.e. are extensively trained). A hacker will be less likely to succeed as his traffic will have been monitored and tracked. Consequently, more obstacles will have been placed in his/her path to discourage him/her further.

With a BRP solution for the web-servers, if the attack succeeds, dynamic fail-over to the backup server can be carried out and all traffic from the hacker's IP address blocked, while further analysis is carried out. Therefore, although the attack has succeeded, its effects have been limited as service outage has been limited and there has been no pr disaster.

References

Assignment 1

1. Split-Brain DNS - http://homepages.tesco.net/~J.deBoynePollard/FGA/dns-split-horizon.html
2. Split-Brain DNS - http://www.phoneboy.com/faq/0241.html
3. Hardening – http://www.fish.com
4. RFC 1918 – http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1918.html
5. Network Segmentation - http://www.networkcomputing.com/1214/1214ws1.html
6. RFC 1771 - http://www.ietf.org/rfc/rfc1771.txt
7. Introduction to BGP - http://www.academ.com/nanog/feb1997/BGPTutorial/sld001.htm
8. What is BGP - http://whatis.techtarget.com/definition/0,,sid9_gci213813,00.html
9. HSRP - http://www.cisco.com/warp/public/619/3.html
10. BGP - http://cisco.com/warp/public/459/18.html
11. http://www.securecomputing.com/gauntletkb.cfm
12. Prestigious Certification – http://www.securecomputing.com/archive/press/2002/apr24,02.htm
13. Secure Client - http://www.checkpoint.com/products/vpn1/secureclient.htm
14. IDS – http://www.snort.org
15. BIND - http://www.nominum.com/resources/faqs/bind-faqs.html

Assignment 2

1. Firewall Security Architecture - http://www.enteract.com/~lspitz/rules.html
2. Firewall Best Practice - http://www.roble.com/docs/firewall_best_practices.html
3. Section 2.5 Tutorial – Gauntlet Admin. Guide
4. Anti-spoofing - http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf
5. Anti-spoofing - http://www.cisco.com/warp/public/0707/21.html
6. Anti-spoofing - SANS Track Two, Day Three module
7. Anti-spoofing - www.sans.org/dosstop/cisco_spoof.htm
8. RFC 2827 - http://www.faqs.org/rfcs/rfc2827.html

Assignment 3

1. Auditing Your Firewall Setup – http://www.enteract.com/~lspitz/audit.html
2. Port Listings – http://www.good-stuff.co.uk/useful/portfull.html
3. ISS – http://www.iss.net
4. Nessus – http://www.nessus.org
5. Nessus Guide - http://linuxsecurity.com/feature_stories/nessusintro-part1-2.html
6. Nessus Guide - http://www.linuxsecurity.com/feature_stories/nessusintro-printer.html
7. Nmap - http://www.insecure.org/nmap
8. Using nmap – http://www.insecure.org/nmap/lamont-nmap-guide.txt
9. Using nmap - http://www.insecure.org/nmap/nmap.usage.txt

10. CIScan - http://www.cissecurity.org
11. Expn & Vrfy - http://www.burningvoid.com/iaq/expn-vrf.html
12. BIND patch - http://sunsolve.com/pub-cgi/show.pltarget=patchpage

Assignment 4

1. Stephen Monahan's practical - http://www.giac.org/practical/Stephen_Monahan_GCFW.doc
2. Web Server Attacks - http://cgisecurity.com/papers/fingerprinting-2.html
3. Web Server Market Share - www.netcraft.com/survey
4. TFN2K - http://packetstorm.security.com/distributed
5. Port 80 Fingerprinting - http://cgisecurity.com/papers/fingerprinting-2.html
6. Stephen's Carroll's practical – http://www.giac.org/practical/Stephen_Carroll_GCFW.zip
7. TFN analysis – http://staff.washington.edu/dittrich/misc/ftn.analysis

Sites Frequently Used

(For information gathering, research etc.)

1. http://www.cisecurity.org
2. http://www.phoneboy.com
3. http://www.sans.org
4. http://www.cert.org
5. http://www.sans.org/top20.htm
6. http://www.cve.mitre.org

Appendix A

Remaining Information about the Internet Infrastructure

In this final section of Assignment 1, we detail other parts of the GIAC Internet Infrastructure. These details are for informational purposes and most of this information is out of scope for this particular project, though I feel it is useful and relevant to include it.

NTP - there are two time-servers on the LAN, which all machines on the Internet Infrastructure are allowed to talk to on NTP. The external firewalls will only allow NTP through them from the HSRP IP address of the GIAC BRP routers to the time servers, while the internal firewalls will have a rule allowing NTP traffic through to these time servers, see sections 2.2 and 2.4.

HTTP & FTP – http and ftp access permitted is through the FTP proxy. The IPlanet 3.6 (www.iplanet.com) proxy enables the user to access sites on the Internet, and authenticates the user password, login and access permissions against the users account on the IPlanet 5 LDAP (www.iplanet.com). This http and ftp traffic is virus-vetted on the way into GIAC by Trend 3.7 Interscan Viruswall (www.antivirus.com).

SSH – firewall/unix/router administrators must all use ssh to administer their relevant machines. All administrators use the putty Ssh client to access their various machines.

SNMP – is blocked on the internal and external interfaces of the router and the external firewall interface. The web-servers are permitted to send snmp traps to an SNMP management machine on the LAN to aid the Windows Administrators in managing the web-servers. We know hackers can exploit SNMP, however, we have bound this SNMP traffic to the DMZ interface and the web-interface of Gauntlet, while the rules ensure it is only from the web-servers to the management machine. No other firewall interface will accept SNMP traffic.

SMTP –

Incoming SMTP: the csmap process on the external Gauntlet firewalls listen (on port 25) for all smtp traffic intended for the giac.com domain. After csmap has received the full smtp packet, the sendmail process takes the packet and sends it on to the MAILsweeper, which in turn forwards the email onto the mail server, EXIM.

Note: the EXIM mail server is configured only to accept and relay email for user@giac.com.

Outgoing SMTP: the users mail client connects to the EXIM (www.exim.org) mail server, through the Checkpoint Firewall, using SMTP. The mail server relays the mail onto the MAILsweeper, which after content-vetting the email relays onto the Gauntlet Firewall. The csmap process listens on port 25 for the email, before transferring it to the sendmail process, which sends it to the GIAC BGP router and on to the Internet.

MAILsweeper – the incoming MAILsweeper (www.clearswift.com/products/msw/smtp/default.asp), relay1, has a physical address of 10.9.2.10 and a virtual one of 10.9.2.12. The outgoing MAILsweeper, relay2, has a physical address of 10.9.2.11 and a virtual one of 10.9.2.13. The Gauntlet firewall is configured to relay all incoming mail to the virtual address, 10.9.2.12, and EXIM, sends all outgoing mail to 10.9.2.13. These virtual addresses fail-over dynamically between each MAILsweeper, using Lifekeeper V2.04 (www.steeleye.com) . GIAC also use the textual analysis scenarios (on the subject) on the MAILsweepers to block any spam mail that may bypass the external firewalls.

H/A on the Internet Cluster - We use Veritas (www.veritas.com) as our HA solution, for dynamic fail-over of all services on the cluster, i.e. the web proxy, ldap, mail server and trend.

EXIM – the EXIM (http://www.exim.org) mail server is installed on a SUN E450 cluster. It runs on the virtual IP 10.9.2.100. It has some nice features and directly supports abuse lists.

Virus-Vetting

- All outgoing and incoming SMTP traffic is virus-vetted by the MAILsweeper machines, using the Sophos Anti-Virus Solution Version 3.61 (www.sophos.com). The Sophos AV receives automatic updates, using a free utility on the Internet sophosupdate.exe (www.gsfax.com).
- HTTP and FTP traffic is virus-vetted by Trend Interscan Viruswall V3.7 (www.antivirus.com) before it reaches the IPlanet proxy on its way back into GIAC. The latest pattern files are automatically downloaded from the Trend web-site. Trend listens on port 1898, on the virtual address – 10.10.1.150.
- Network Associates Solomons Anti-Virus Solution is installed on all desktop PCs. The automated update occurs at logon - a script checks the current version of the AV software based on the file size of the scan.dat file. Based on this comparison, if there is an update it copies the new superdat/datfiles update to the PC, stopping and starting the McShield services before and after the update.
- Additionally, GIAC use the Websense Version 4.4 (www.websense.com) URL database, which is updated daily, as a plug-in to the proxy server. Web-sites are blocked based on the categories they fall under – porn, games, web-based email, information technology - hacking etc.

Monitoring of Servers and Network

The Operations team receives alerts on their screens, through a combination of HP Openview (http://www.openview.hp.com) and Maxm (http://www.bmc.com).

Additionally, under the SLA agreements with our ISPs, GIAC receive weekly traffic-analysis from both MerdeNET and MauvaisNET.

Vlan Segmentation

Vlan Segmentation is achieved using Cisco Catalyst switches (2948), where each port will be configured only to allow traffic for a specific vlan. The IDS network sensors will be connected into appropriate ports on these switches to analyse the traffic on each vlan.

Log Server

The routers log back to the syslog servers on the LAN - 10.10.5.9. Each night, after the back-ups have been done, the logging server connects (using ssh) to the TSM server on the LAN to pull down the various log files. Using a mixture of Webtrends (www.webtrends.com) and perl scripts, the logs are analysed for user, company and machine statistics. The results are published on the local Intranet on a selection of sites, which have varying degrees of access and security based upon what the graphs are about.

Hardening of Servers

After being configured, all UNIX servers (including the firewalls) are hardening using the TITAN script (www.fish.com). For a description of what each module (in the TITAN script) does, see www.fish.com/titan/TITAN_Solaris.html. Any anomalies (e.g. rules, file permissions etc.) that arise are then resolved.

Back-ups and Check-ins

All boxes on the Internet Infrastructure are backed-up using Tivoli Service Management (TSM). These back-ups occur between 3 and 5am daily, when we have little or no traffic going to our web-servers. All boxes use RCS (Revision Control Software – see Appendix B) so that we can keep track of changes made to the configurations on all systems. Additionally, on all Unix boxes sudo (see Appendix A) is strictly enforced, again ensuring that all commands, changes etc. are logged.

Dual-site Redundancy

The second data centre bought cheaply off one of the recent dot.com failures, newco.com, gives GIAC more scope for load-balancing and an excellent BRP functionality. The two data centres are 1.5 miles apart, and with the telecos in such a dire state with no business, GIAC were able to connect their two data centres very cheaply with fibre.

As a result, GIAC will now have a real viable BRP option, which cannot fail to improve the services GIAC provides.

Each network component has a replicate machine in the other data centre – some are primary – back-up scenario and others are load balancing. As a result, we have no "single point of failure".

Physical Security

As part of the audit, we examined the physical security employed by GIAC in relation to their data centres and we were shocked.

- Doors – alarm-based
- All data-centres have a security guard at the entrance to the centre, but to be let into the actual "computer room" access can only be allowed by ringing the Operations Bridge using your ID card, which can (via cameras) see who you are before they let you in.

Additionally, any external contractor allowed into the data centres MUST be accompanied by an internal GIAC system administrator.

Appendix B

GIAC Sudo Policy

Assumed Knowledge

Basic UNIX User Knowledge, including:

- Understanding implications of running commands as another user – especially as the “root” user.

Purpose for use

sudo - *execute a command as another user (“root” by default)*

sudo *allows a permitted user to execute a command as the superuser (root) or another user, as specified in the* sudoers *file. The real and effective uid and gid are set to match those of the target user as specified in the passwd file (the group vector is also initialised when the target user is not root). By default,* sudo *requires that users authenticate themselves with a password (NOTE: this is the user's password, not the root password). Once a user has been authenticated, a timestamp is updated and the user may then use* sudo *without a password for a short period of time (five minutes by default).*

User Base

System and application administrators.

User Guide/How to use

Usage of the *sudo* command is exactly the same, as you would normally type, except that you include the word *sudo* at the beginning. This tells the operating system that the command you are about to run should be run with the privileges of another user, such as root.

All commands run with sudo are logged using SYSLOG. This includes successful as well as unsuccessful attempts to use the command.

sudo access can be given on a "per host", "per command" or "per user" basis; or a combination of the above. This allows a system administrator to provide customised distributed administration access to users, while still retaining full control over the system

Example:
Old Command – run as root:

```
/usr/sbin/tcpdump –i fxp1
```

New Command – run as “normal” user with root privileges:

```
sudo /usr/sbin/tcpdump –i fxp1
```

To run a command as another user:

```
sudo -u <username> <command>
```

For detailed usage instructions on using *sudo*, please type in “man sudo” at the Unix command prompt.

Vendor Documentation

The main site for *sudo* is:

http://www.courtesan.com/sudo/

Note: This policy has been adapted from http://www.andrew.mosina.com.au/content/doco.html

Appendix C

RCS in GIAC

Overview

Revision Control System (RCS) allows for management of files, in particular configuration files. It is especially useful in the management of version control for files. It allows for logging of changes, comparison between versions, and rolling back and forward between versions.

Use of RCS also helps ensure that there is no "critical race" between users trying to edit files.

Requirements

Software

1. GNU Diff Utilities – http://www.sunfreeware.com – installed as part of this installation process
2. sudo package installed - optional

Hardware (Servers)

- No specific server is required, however it will need the above packages installed

Assumed Knowledge of System Administrator

Sun Solaris System Administration experience (1-2 years minimum preferred)

- Ability to use and understand implications of using “sudo”
- Appropriate access for using sudo (ie. in the “*/etc/sudoers*” file)
- Knowledge of implications and requirements in using RCS - including training

Assumptions

- That Packages will not be compiled, rather they will be downloaded from SunFreeware – http://www.sunfreeware.com Packages should be downloaded and installed for the version of Operating System you are running.
- WGET is installed for downloading source files
    - WGET is an application that can be installed onto a unix server for downloading source files where the server requires proxy server access to the internet

  - WGET is NOT required for this installation, however Step #1 below will need to be done manually (eg. ftp file to local workstation, then ftp file to server)
- GZIP is installed – GZIP is required for extracting the pre-compiled Solaris binary packages from SunFreeware
- Solaris 8 is the version of Solaris used in the installation documentation in this example

Vendor Documentation

There is limited vendor documentation, however the source files also contain limited documentation. Usage instrucations are installed after installing the RCS package. Use `man rcs` after installation for information
RCS - http://www.gnu.org/software/rcs/

Simple Usage Instructions

Below are instructions that ***must*** *be used when modifying files that are being controlled by RCS*

Editing a file with RCS for the FIRST TIME

Important - ALWAYS make sure you have a backup of a file before performing the steps below

1. Make the RCS sub-directory - this sub-directory is used to store all the RCS version information for all files in the directory that are controlled by RCS. Eg. For all files */etc* the RCS version information is stored in */etc/RCS*

```
cd /<path>/<to>/<directory file is in>
sudo mkdir RCS   # If the directory doesn't already
exist
```

2. Check in the file to be edited for the first time. You will be prompted to enter a description of the file about to be controlled by RCS

```
sudo /usr/local/bin/ci <filename>
<enter description>
```

3. Check Out the file and lock it for you explicit control

```
sudo /usr/local/bin/co -l <filename>
```

4. Edit the file (this example presumes you use "*vi*" to edit files)

```
sudo vi <filename>
```

5. Check In the file and unlock it from you explicit control . Remember to enter a description of the modifications made to the file

   ```
   sudo /usr/local/bin/ci -u <filename>
   ```

Editing a file already under the control of RCS

1. Check Out the file and lock it for you explicit control

   ```
   sudo /usr/local/bin/co -l <filename>
   ```

2. Edit the file (this example presumes you use "*vi*" to edit files)

   ```
   sudo /usr/local/bin/vi <filename>
   ```

3. Check In the file and unlock it from you explicit control . Remember to enter a description of the modifications made to the file

   ```
   sudo /usr/local/bin/ci -u <filename>
   ```

Sample "Header Information" for a file under RCS Control

Below is a recommended "Header" file to add to the beginning of a file that is under RCS control.

The various flags are:

```
$Source$ = The full pathname of the RCS file
$Revision$ = The revision number assigned to the
revision/version
$Date$ = Time and Date the revision was checked in. Time is
in GMT (UTC)
$Author$ = Login ID of the user who checked in the revision
$Locker$ = Login ID of user who locked the revision (empty
if revision not locked) – Handy if you want to know who has
the file locked
```

A Recommended header for configuration files is:

```
#-#
#-# WARNING - This file is under RCS Control
#-#

#-#
#-# $Source$
#-# $Revision$
#-# $Date$
```

```
#-# $Author$
#-# $Locker$
#-#
```

Please note that after the file has been checked in and out a few times, the above example will change and you will see the latest information being updated. Eg:

```
#-#
#-# WARNING - This file is under RCS Control
#-#

#-#
#-# $Source: /opt/IBMHTTPD/conf/RCS/httpd.conf,v $
#-# $Revision: 1.14 $
#-# $Date: 2002/06/28 10:41:12 $
#-# $Author: root $
#-# $Locker:  $
#-#
```

Viewing RCS Log History of a file

To view the RCS log history of a file that is under RCS control, use the command syntax of:

```
/usr/local/bin/rlog <filename>
```

An example of this use is below (including output):

```
crmbc02t/root# /usr/local/bin/rlog httpd.conf

RCS file: RCS/httpd.conf,v
Working file: httpd.conf
head: 1.16
branch:
locks: strict
access list:
symbolic names:
keyword substitution: kv
total revisions: 16;    selected revisions: 16
description:
IBM Apache Web Server Configuration file
----------------------------
revision 1.16
date: 2002/07/02 14:24:45;  author: root;  state: Exp;
lines: +3 -2
```

```
Copied the WAS Plugin Config Bootfile line in preperation
for SSH Tunnels
.
.
.
<and so-on until revision 1.1>
```

Note: This policy has been adapted from http://www.andrew.mosina.com.au/content/doco.html