Global Information Assurance Certification Paper

Security Architecture

The design of any security architecture should begin with a definition of a security policy which has been reviewed and signed off by (a) senior manager(s) within the organization. This is the basis on which requirements are defined and they run the gamut from the length and composition of passwords to encryption strength and Public Key Infrastructure.

This paper is based on the assumption that a good security policy is already in place. If not then there are adequate resources online at http://www.sans.org/newlook/resources/policies/policies.htm to help the professional to develop one in conjunction with the GIAC ENTERPRISES administrators.

Below is a diagram of the physical implementation of the security architecture. Following is a description of the components that make up the architecture.

INTERNET CONNECTIONS

Based on the expected volume of traffic that this site is going to handle, it was decide to use fractional DS3 (45Mbs maximum) circuits. Initially we will only commit to 15Mbs on each line but would be in a position to easily turn up the speed without any infrastructure change (hence a very short lead time) should our monitoring proves that it is necessary.

Each line will ideally be sourced from a different service provider running on separate SONET rings and entering GIAC through widely dispersed access points.

These measures are important to guard against failures in the ISP or tail circuits going back to the ISP - which may be caused by a backhoe inadvertently cutting through the line. In terms of physical security, it is easier to contain the damage from terrorist or other malicious activity with such a configuration.

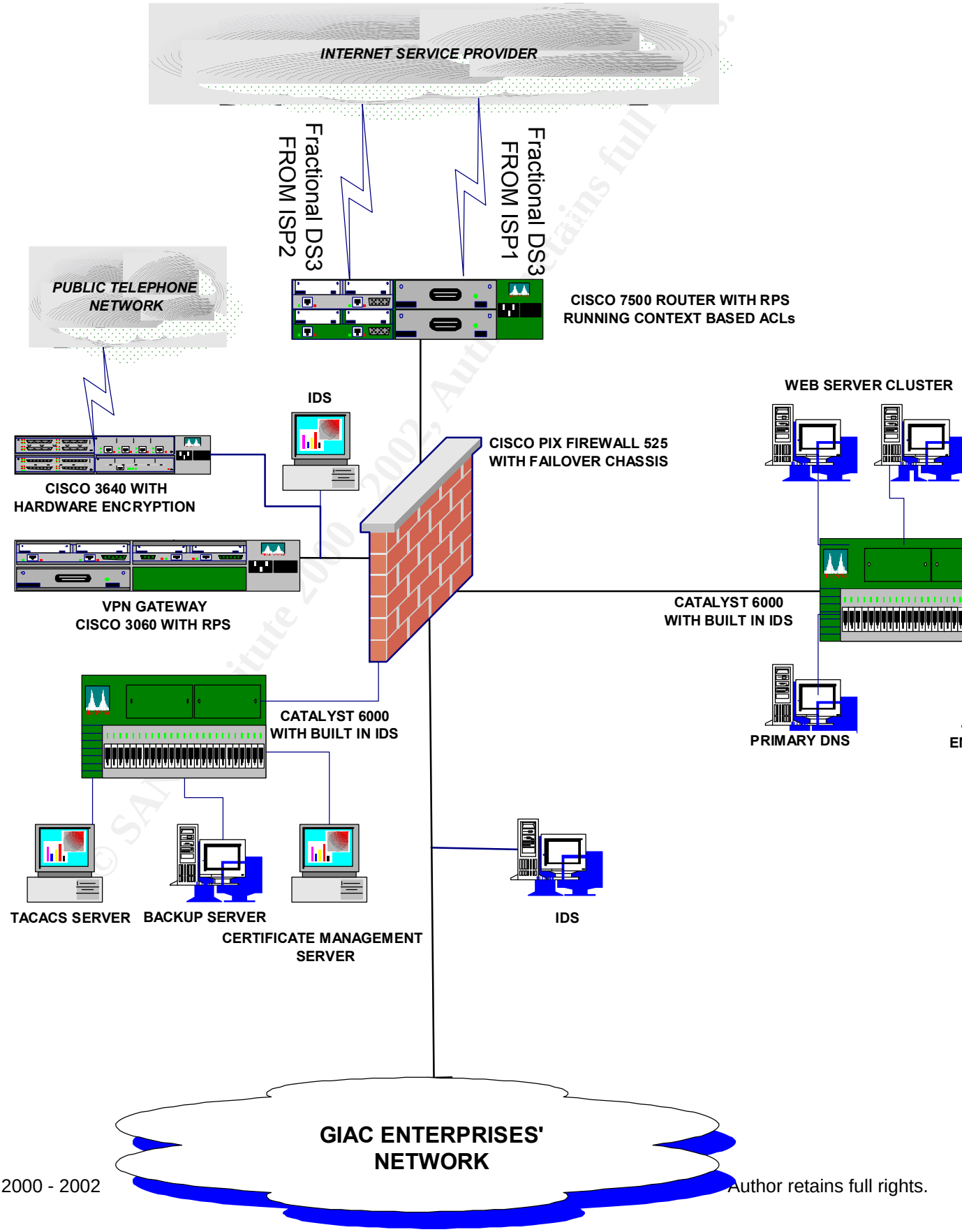
BORDER ROUTER

The border router used in this configuration is the first line of defense. It will be used to filter out most ICMP traffic (access from and responses to one or two supervisory workstations would be allowed to aid in troubleshooting), block spoofed addresses and other Internet noise etc. (i.e. many of the VISA top ten would be stopped here - with exceptions as required).

I have chosen to use a high end Cisco 7500 with redundant power supplies and running Context Based Access Control (CBAC) Lists. This was chosen because I intend to catch suspicious fragments here and also block much of the possible Denial of Service attacks by limiting the number of half open sessions, long SYN waits , TCP or UDP idle-timeouts, excessive opens per minute etc. Further information about CBAC can be found at http://www.cisco.com. Note, however that this router is only meant to augment the

firewall not replace it and care will be taken that it does not become a bottleneck by trying to do too much filtering.

GIAC ENTERPRISES INTERNET NETWORK



It will also be configured to only accept routing updates from known routers at the ISP. How this is achieved will depend on the routing protocols used e.g. with EIGRP will use access list on the ingress interfaces or distribute list entries on the router definition, OSPF will use encryption and passwords etc.The router itself needs to be secured and this is covered lower down in the document.

FIREWALL

The firewall chosen is a high performance Cisco PIX 525 with a fail-over chassis. A stateful inspection firewall was chosen because of its superior performance when compared to a proxy firewall. The primary difference being its ability to allow packets to cut-through the firewall once the session has been authenticated versus a proxy firewalls which have to open separate sessions to the inside and outside devices and pass packets from one to the other. This particular stateful inspection firewall is reputed to be built from the ground up as a firewall device so does not have the inherent weaknesses of firewalls which are built on general purpose operating systems. It also outperform any other of its type on the market, such as Firewall One, even though the latter has a much friendlier user interface. In this application it is run in parallel with a similar box, which act as a hot standby.

The rulebase used on the firewall, unlike the router, will begin with an implict deny everything and only allow through the services as needed. It will handle the protocols that the border router cannot handle (or handle efficiently).

Another reason for the selection of this particular firewall is the number of screened subnets that have been created. They are as follows

- A Web-server screened subnet which includes a web server cluster , an email relay an FTP sever, a primary and possibly a secondary external name server, and any other Web related devices that GIAC chose to put out there. It is a requirement to have at least two domain name servers to provide external name services about your domain. However, it is not required that you host both servers it is possible and sometimes desirable, to have your ISP host at least one of these and maybe a mail relay. GIAC have chosen not to do this because they want to control the security of these services.

  The GIAC name servers will be on bastion Solaris hosts with up-to-date versions of BIND i.e. 8.2.2 and later to protect against the known exploits in the earlier versions. The "named.conf" file on our primary name server will be configured to only allow zone transfers to known secondaries, the secondaries will not allow any zone transfers.

- The firewall will be used to strictly control access to the devices in this subnet, only allowing protocol and user access to them on an as-needed basis. Hence for example, domain name lookups will only be allowed from the outside to the name servers and only using UDP.

- Connection to the Web servers will be allowed through port 80 but any secure transaction will be done via SSLv3, or TLS where supported. To improve the quality of the security that GIAC Enterprises can offer its customers, it is GIAC Enterprises' intention to also use Secure Electronic Transaction (SET) once it has been ratified and adopted by financial institutions and incorporated into browsers.

- The mail relay will be used (in addition to the usual big brother mode) to scan incoming mail for any known viruses, trojans, etc., It will also quarantine any executables until the addressee can verify acceptance. It will also not allow itself to be used as an ongoing mailer to domains outside of GIAC. The antivirus software will come from a reputable company that is vigilant in releasing new DAT files as new threats are identified (McAfee is preferred).

- In addition to the screening done by the firewall and the hardening done on the servers, tools such as TCP wrappers will be used to further protect individual hosts and Tripwire (or similar) will be used to check the integrity of the data content). Connections from the internal network to the screened subnets will always be encrypted using tools such as Secure Shell (SSH).

- The connections in all the subnets are done on Catalyst 6000 switches with built in Intrusion Detection Systems (IDSes) so that even if a device within the subnet is compromised, it will not be possible for the cracker to run tools such as SNOOP to analyze the traffic going to other devices. This assumes that they have not been able to gain access to the switch and setup their port as a SPAN port. The IDS will record and shut down malevolent activity.

- The Web-server cluster and the FTP servers will run the Windows2000 operating system and will use that system's built in strong encryption. This is based on asymmetric keys tied to a user's logon ID. The administrator's user ID will encrypt proprietary company data left on these servers. Customers will be allocated an ID based on their credit card number and some secret only they will know which will be used to encrypt data that they may wish to leave on these servers. In later releases of this operating system customers and internal administrators will be able to use their own private keys to encrypt the data and publish their public keys to those whom they wish to give access to it. GIAC Enterprises will incorporate this into its service.

- The second subnet is GIAC's remote access subnet, which will include a VPN Gateway(s) and a modular router with modem cards inserted.

- The VPN gateway will be used to connect to remote offices, suppliers and remote employees via the Internet. This implementation will be IPSEC compliant and will use Encapsulating Security Payload (ESP) in tunneled mode. The options chosen within this standard, and where relevant, are X.509v3 digital certificates backed up by

the Cisco implementation of RADIUS (i.e. TACACS+ which is more secure) for authentication, authorizing (i.e. which host, networks the user is allowed to access) and auditing. Key exchange will be accomplished by the ISAKMP/OAKLEY procedure and bulk encryption will be 3DES (triple Data Encryption Standard). The digital certificates used here will be issued in two ways. GIAC's Public Key Infrastructure (PKI) will support digital certificates issued from GIAC's own Certificate Management Server (which will use the CMS built into Windows2000), or from trusted root and intermediate authorities such as Verisign, Entrust, Equifax, etc. GIAC employees and remote routers will generally use GIAC certificates while suppliers and partners will use public root authority certificates.

- Remote Offices will use an IPSEC compliant router (such as the Cisco 3640) to connect via a high quality local ISP terminated SDSL, to establish a VPN back to the corporate headquarters. Where performance or additional security demands, leased lines will be used. Access from these offices to the Internet will be through the corporate headquarters link except in cases where it is impractical in terms of volume or distance. Where there are exceptions, that access will be controlled by firewalls under headquarters' control.

- Remote employees will be supplied with digital certificates and VPN clients which they will use to connect via their Internet connection to headquarters. These clients will be shutdown so that the user cannot reconfigure them and they will employ split tunneling so that a user's PC will not form a pass-through conduit for hackers who have gained access to it from the Internet. They will also be encouraged to install a personal firewall such as ZoneAlarm on their computer to prevent such unauthorized access.

- When a user makes the VPN connection and logs in via the TACACS+ server, they will directed to a Terminal Server on that subnet (not shown) which will be configured so that no data can be uploaded to the remote users' PCs. This mean that the firewall can be configured to only allow the Terminal Server to access data on the internal network and no company proprietary will sit on relatively unprotected remote users' PCs.

- Partners and suppliers will also establish "router or client to VPN gateway" connections across the Internet, assuming that they can meet the required standards. Even so their access will be much more tightly controlled at the TACACS+ server.

- The 3640 router with the modem cards in this subnet is to be used for all dial-in access to GIAC. It will be used to terminate the VPN tunnel from dial-in users and partners who do not have Internet access instead of the VPN gateway. Except for that difference, the requirements for establishing a connection and they way that access is controlled will be the same as before.

- Only the ESP protocol (protocol 50) and the ports relevant to our implementation (only port 500 is expected) will be allowed in from the outside to this subnet. Only terminal server traffic will be allowed out from this subnet to the internal network and the other devices will be allowed to connect only via the required ports to the third subnet (TACACS+ and LDAP expected).

- The third subnet will host the TACACS+ and CMS server as mentioned before, and it will also host (a) backup server(s) and a syslog. Backups of all the servers in the various subnets will be initiated from these backup servers across an encrypted tunnel. No access will be allowed to this subnet from the outside and data stored here will be encrypted as before.

- The connection from the firewall to the internal network will be monitored by an Intrusion Detection System, which will log and alert the system administrators if an attack is identified.

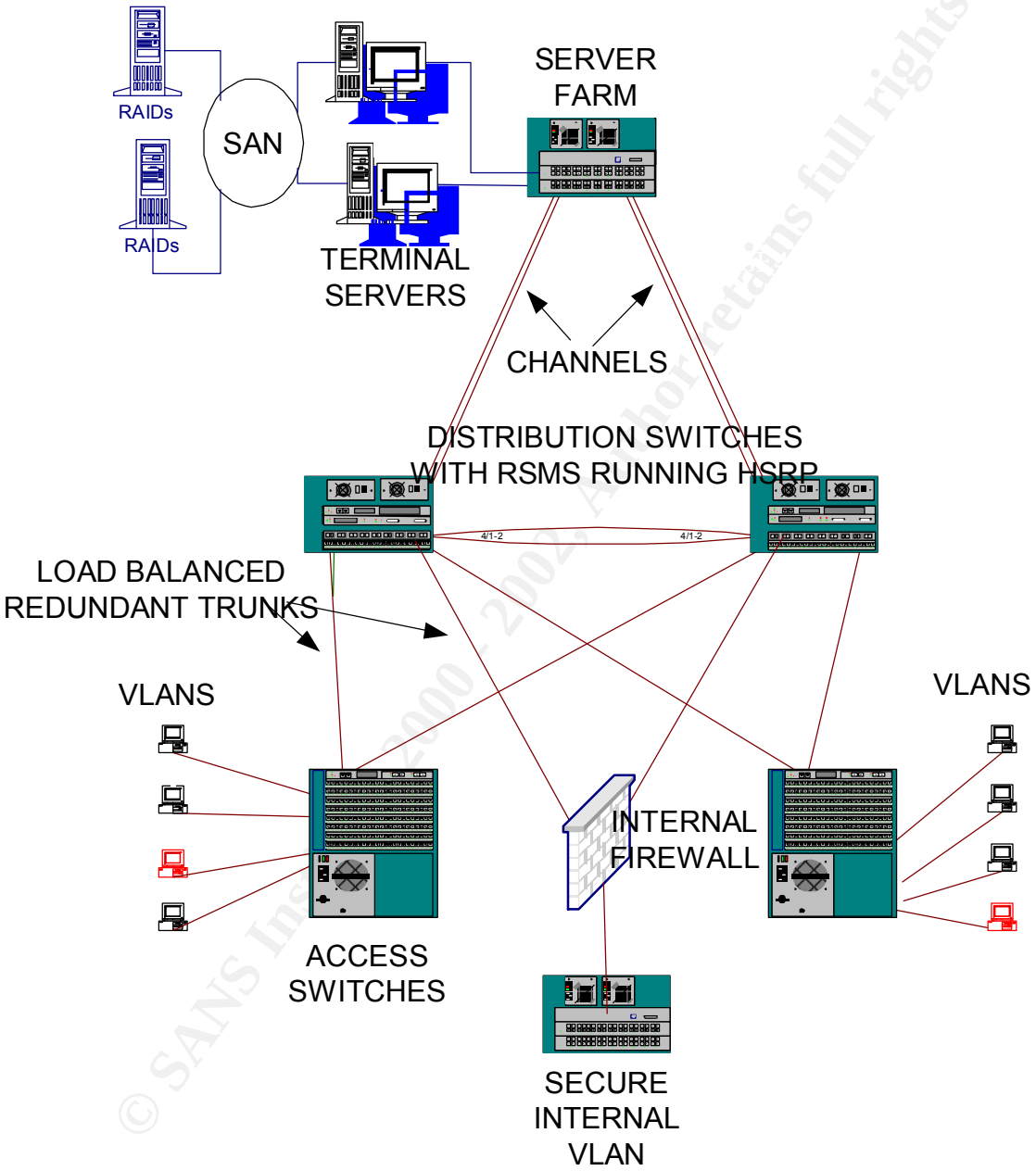
The internal network will share much of the principles of the screened subnets such as an infrastructure based on Catalyst 6000 switches with IDSes encrypted data, etc. The design (as shown) will be s based on a distribution layer fanning out to an Access layer over redundant links. The server farm will be concentrated on switches hanging off the distribution layer. All the connections to the desktop will be via 100Mbs links and all the trunks will be at least 1 Gbs. Where necessary these trunks will be combined into channels of up to 4 trunks (i.e. 8 Gbs full duplex). This design, apart from being efficient in terms of the number of routers needed will makes it easy to concentrate monitoring tools on important hosts and VLANs.

A firewall will also be redundantly connected to the distribution layer. The switch port on the connection to the firewall and all the ports to the devices on the switch behind the firewall will be configured to only make a connection to the small subset of hardware addresses on those devices. If an attempt is made to connect up a device not in the database then it will be rejected. This secure internal switch will hosts the sensitive VLANS such as Human Resources, Payroll etc.

Most users at GIAC with the exception of some power users and those developing or using special applications will run a thin client on their desktop. These will have a network interface and sufficient memory to run Citrix ICA client software. They will not have internal hard drives or any other connection for peripheral support. Even the power users will only run applications locally where it is not practical to do so on the terminal servers.

At the heart of the network will be a cluster of Citrix Terminal Servers to which all the clients will connect. All the ICA connections from the thin clients to the Terminal Servers will use DES encryption to further enhance security. The Terminal Servers will have SCSI connections across a Storage Area Network (SAN), which is separate from

GIAC ENTERPRISES'
INTERNAL NETWORK



the LAN, to RAID controllers and drives. On these users will be dynamically allocated up to 5 Gigabytes of personal hard drive space with more being available where it can be justified.

Weekly workstation inventories will be done on all the devices connected to the network using a tool called NetCensus. This will looks at, among other things, the type and version of applications loaded on these devices (only relevant for non-thin client devices).

This design has several advantages from a security point of view, some of which are,

Several instances but only a few copies of the email (Outlook) and other software will be actually run at GIAC Enterprises. Most of these will be on the terminal servers, hence when a new security patch becomes available it will quickly be patched on the terminal servers by the system administrators. Updates will be applied to one server and will propagate to the other servers in the cluster either immediately or when it is convenient depending on the threat.

Virus Scan software will be run on the terminal servers and will not depend upon individual users for installation and keeping up-to-date.

Users will only have access to data and to areas that are determined by their logon. Users will be generally assigned to a group to which rights have been allocated by the system administrators, but each ID within a domain will be unique. These will be further enforced from within the domain controllers which will not allow multiple logons from a single ID within a domain.

Because users will not generally load the applications that they run and because these applications will be concentrated on only a few servers, the system administrators will be able to devote time to ensuring that the applications are secured on these servers.

Data will always be properly virus scanned and backed up a few iterations deep so that the impact due to a failure or destructive virus will be minimized.

Security Policy

Assuming the top ten as listed at http://www.sans.org/topten.htm are already in place I will address a few other potential threats

1. **Sockets de Troie**
2. **Back Orifice**
3. **Hack-a-tack**
4. **Solaris rpcbind vulnerability**

Solaris rpcbind can be exploited to overwrite arbitrary files and gain root access.

Vulnerability

The first three is a group of trojans that allow someone to take control of your PC once you have inadvertently installed them. A fuller explanation is found at http://www.commodon.com/threat/threat-st.htm

How to block them

In the past few firewall filters would allow ports above 1023 to initiate a connection but because new applications are constantly being written these ephemeral ports are becoming less so. The following filters will not prevent the trojans from coming in on the back of emails etc. but it would stop them from communicating with the client should they be installed.

```
Access-list 101 deny tcp any any range 5000 5001 log
Access-list 101 deny tcp any any eq 30303 log
Access-list 101 deny tcp any any eq 50505 log
Access-list 101 deny udp any any range 5000 5001 log
Access-list 101 deny udp any any eq 30303 log
Access-list 101 deny udp any any eq 50505 log
Access-list 101 deny udp any any eq 31337 log
Access-list 101 deny udp any any eq 313789 log
Access-list 101 deny udp any any  eq 32771 log
```

A better approach to this would be to explicity allow the ports you want and deny all the rest. The access lists would then look like this.

```
Access-list  101 permit esp any host 188.8.10.12 fragments
Access-list 101 deny tcp any any gt 1023
Access-list 101 deny udp any any gt 1023
```

The order is important because the entries in the list are matched from the top down.

Testing
The best way to test this would be to have SARA do a scan and to see what gets through. I do not recommend getting a copy of the trojan and installing in on a sacrificial PC unless it can be properly quarantined as you may import other trojans of which you were unaware.

A more comprehensive list can be found at http://www.doshelp.com/trojanports.htm but the method of blocking them remains the same.

Another set of protocols that need looking at are the Netmeeting, streaming video, real audio etc. which are in common use and which are designed to deliver large payloads to vicitims in a short time.

These have already started to appear such as the so called Trinityv3 which use the IRC protocol. These are likely to be the next vehicles for DDoS attacks

Technically these can be blocked using the same format as above but obtaining the permission to do so my be more difficult.

Plan the Assessment

Determine the extent of the analysis required and agree on costs.

Ask the customer what private and public IP addresses he uses. You will be able to determine this once you start scanning but it is a good starting point in estimating the amount of time and resource you will need to do the job. Check the information by going to http://www.arin.net/whois

It is planned to do approach this assesment in five phases

1) A probe of the external network from (a) remote site(s). - 2 nights 2 days

2) A probe of the internal network from within the organization. - 2 nights 2 days

3) A review of the company's approach to security, namely how their users are educated about security, how often and what is checked, how are documents secured, where are logs kept, etc. This will involve a review of the company's security policy document, interviews with system and network administrators, security personnel and other support staff. - 1 week

4) The production and presentation of a report outlining weaknesses, strengths, etc. Avoid being personal, name bad practices not people. - 1 week

5) A final scan a month later to determine how well the fixes have been applied followed by a vulnerability report. - 1 day

Such a comprehensive analysis would require 2 people a month's work to complete with the break down as shown plus a few days for unexpected problems. GIAC Enterprises will be expected to pay about $25,000 for the analysis

Get permission to do the security check.

Snooping around and breaking into a company's network can get you into deep trouble. Be certain that you get written permission to do the assessment and have clearly defined the level of intrusion that they are willing to accept.

Obtain passes or clearances for the period that you expect to be on-site.

When analyzing perimeter defenses, it is a good idea to start on the outside but considering the large number of break-ins that come from the inside, it is important that you also probe the internal security.

Determine what the critical systems are

A company is not going to be pleased with you if during the course of your analysis you brought down their production system. A good analyst would identify potential vulnerabilities but an excellent one would want to exploit them. Some of these techniques such as generating buffer overflows to root a box is likely to cause some outage.

Find out the hours of operation

Find out the normal business hours of the company and the hours that Operations and Help Desk staff are on-site Find out if there are any shifts and when they change. This is usually a good time to gather intelligence from such staff as during the change the are usually busy and may not follow procedure or just after a change it is possible to convincingly allude to something that did not happen on the shift just completed.

Ask who the system and network administrators are, supposedly as contacts in case of trouble, but in reality because they are a worthwhile targets.

Find out which ISP(s) they use these can be good sources of information.

Find out (if possible) the stringency of your ISP.

Most ISPs will not react to a scan originating from one of its subscribers but some will shutdown your account if they notice such activity and some block most ports. If you are fortunate to have one of the latter types of ISP then you will have to find an alternative point from which to do your external scans.

Find out the company's telephone numbers (published and unpublished.

Keep vigilant for any mention of senior staff that might be out of town during the analysis period.

Select the tools that you wish to use.

Most companies (GIAC included) will only use IP in their external network but internally many may prefer to use IP and or IPX, Banyan Vines, AppleTalk, etc. depending on requirement, e,g, most publishing and newspaper networks have a great deal of MacIntoshes (which run best with Appletalk) because of their superior graphic handling. Fortunately, GIAC uses IP throughout the enterprise.

Define the rules of engagement

Agree what actions should be taken by GIAC Enterprises if they become aware of an attack against their system. It is advisable that they report any activity to you so that you can verify that it was a part of the analysis. They should not make assumptions as they may well ignore unauthorized scans during that period.

Implement the Assessment

External

The analysis is initiated by running HP's network node manager at GIAC Enterprises' address space. If ICMP or SNMP is allowed to penetrate the defenses, it returns a beautiful picture of the network complete with routers subnets, quantity and type of devices including servers, printers operating systems and release levels. It is a favorite tool because it does much of the discovery work for you. Unfortunately, those key protocols were blocked by GIAC Enterprises so nothing was returned.

The next test was to interrogate the Domain Name Server for any information that it might give out. This was one of the reasons that I wanted to find out the name of the ISP. Some ISPs are not very secure and will allow zone transfers. However GIAC did not use an ISP to host their name server, nonetheless, this is the information that GIAC's own name server returned

Get into the NSLOOKUP tool on my machine and using my ISP's name server as a start point.

nslookup
Default Server: myisp.nameserver.com
Address: 199.99.9.2

Tried do a zone transfer from GIAC's name server but it was refused.
> **ls -d giac.com**
[myisp.nameserver.com]
*** Can't list domain giac.com: Unspecified error

Found out what GIAC's name server was by
setting the query type to name server

> **set type=ns**

then asking about GIAC's domain.
> **www.giac.com**
Server: myisp.nameserver.com
Address: 199.9.9.2

giac.com
origin = giacns.com
mail addr = sysadm.giac.com
serial = 19990275
refresh = 7200 (2H)
retry = 3600 (1H)
expire = 604800 (1W)
minimum ttl = 43200 (12H)

Switched to using GIAC's name server as my default server
> **server giacns,com**
Default Server: giacns.com
Address: 188.8.8..215

Set the query type to SOA

> **set type=soa**

Ask giacns to return the SOA for GIAC's domain
> giac.com
Server: giacns.com
Address: 188.8.8.215

giac.com
origin = giacns.com
mail addr = sysadm.giac.com
serial = 19990187
refresh = 7200 (2H)
retry = 3600 (1H)
expire = 6048 (6048)
minimum ttl = 43200 (12H)
giac.com nameserver = GIACNS.COM
eia.doe.gov nameserver = GIACNSSEC.COM
GIACNS.COM internet address = 188.8.8.215
GIACSEC.COM internet address = 188.8.9.215
Ask giacns.com to tell me about its mail exchanger
> set type=mx
> giac.com
Server: giacns.com
Address: 188.8.8.215

```
giac.com     preference = 20, mail exchanger = giacrelay.com
giac.com     preference = 10, mail exchanger = giacrelaytwo.com
giac.com              nameserver = GIACNS.COM
giac.com              nameserver = GIACNSSEC.COM
giacrelay.com         internet address = 188.8.8.16
giacrelaytwo.com      internet address = 188.8.8.17
giacns.com            internet address = 188.8.8.8.215
giacnssec             internet address = 188.8.8.9.215
>
```

I continued querying the name service in this way trying different query types such as HINFO, reverse lookups on A(ddress) records, etc. and was able to build up a comprehensive view of the subnets including the border router.

```
> 188.8.8.230
Server:  giacns.com
Address:  188.8.8.215

Name:    giacwebserver.giac.com
Address:  188.8.8.230
```

I next looked up the version of BIND in use on the name server

```
> set type=txt
> set class=chaos
> version.bind
Server:  giacns,com
Address:  188.8.8.215

VERSION.BIND    text = "8.1.1"
```

I was now in a position to exploit the weaknesses present in this version see this URL http://www.cert.org/advisories/CA-99-14-bind.html for a description of the vulnerabilities.

I then used the information about the mail server to connect to the mailserver and get it information about its version

```
telnet giacrelay 25
Trying 188.8.8.16...
Connected to giacrelay.com.
Escape character is '^]'.
220 giacrelay.giac.com ESMTP Server (Microsoft Exchange Internet Mail Service 5.5
.2650.21) ready
```

This allowed me to then tailor my attacks to vulenrabilities as described in http://ciac.llnl.gov/ciac/bulletins/i-080.shtml
Armed with the IP addresses of the interesting servers in the external network I then trained the big guns unto them. The tools used here were Netsonar which has an NT and a UNIX version (available from Cisco and HP respectively both which you have to buy); and SARA which runs on UNIX and is available from http://www-arc.com/sara which you don't.

SARA is kept up-to-data with the latest CVE material and so is able to identify most vulnerabilites in a system. It can be run from the command line but I have used the browser interface as it is so easy to use. In appendix 1 is an example of the interrogation that SARA does on a system. As can be seen it also identifies the mail exchanger, default gateway and other servers known by the server. SARA can also be set to scan a range of addresses or a list of addresses.

Sara then produces attractive reports in HTML format, which list the services being run, the vulnerabilities identified by severity and advice on how to fix the problem.

Netsonar is very similar in appearance and performance.

The external scan was completed by running a war dial against the numbers identified during the planning stage, the tool used here was THC (The hacker's choice). This can be run either from the command line for one or a range of numbers or have the numbers to be dialed listed in a file. I chose the latter option. The file used was GIACNUM AND THE RESULTS ARE SHOWN IN Appendix B.

The following was done in the internal scan
An afterhours visit was made to GIAC Enterprises and several workstations were visited. Sure enough Ids and passwords were found next to keyboards. It so happened that GIAC in an effort to improve their security had taken to creating difficult 8 character alphanumeric passwords and issuing them to their users. The unfortunate result was that many users could not remember them so they wrote them down and kept them close to or under their keyboard.

They had made the effort to change the default SNMP community name but I found an unattended server running Compaq's Insight Manager. I put a minihub in line with it and using SnifferPro from Network Associates was able to learn the community strings being used (SNOOP on a UNIX platform or SMS on NT could just as easily have been used).

HP's NETWORK NODE MANAGER was next deployed using the IP address range and the RW community string discovered earlier. This as expected returned a picture of the

network with all the servers highlighted which were then easily targeted and exposed by SARA.

If you have any of the many OpenView implementations on your system and you are any good at writing UNIX shell scripts then the SNMPWALK command is useful. The example shown below and which is run from the `/usr/OV/bin` *directory takes a variable $I (normally a router's IP address) interrogates it and appends the content of its arp cache to the file as shown.*

```
./snmpwalk $i at.atTable.atEntry.atPhysAddress >> /apps/arpaddresses
```

I was also able to use the Cisco getconfig SNMP MIB to get the configuration of a router on which they had not bothered to use the "service password-encrytion" global command nor had they set an enable secret password. I used the passwords listed in clear text to gain entry to the routers and switches. Once into the switches I ran the command "set logging level all debug 6" on them, and located an unused drop on a switch for one of the system administrators that I had targeted. This port was then made a SPAN port using the command "set span <source port|source VLAN> myport" and the SnifferPro brought back into action. This Sniffer ran unattended all the next day with a trigger setup on it to start capturing once a new telnet or FTP session was started, stop 200 bytes later, then wait for the next session to open. This trigger proved to need some refinement but I was able to assemble some passwords from the capture log

I was also able to do a zone transfer to my laptop although it was irrelevant since I was already able to gather so much information.

I tried a couple phone calls to the Help Desk at different times hoping to get my password reset but was told that I had to go through the procedures. I was not able to get a Director out-of-office but the intent there was to call up his secretary posing as a Help Desk person and ask her for his password so that I could install some new software on his box. Many secretaries or personal assistants know their bosses passwords and many senior staff are give strong passwords with many privileges by default.

Recommendations

Use SNMP version 2 with encrypted password on all the network infrastructure equipment (upgrade the IOS level where necessary) and other servers where supported. Use a different community string on those servers that do not support SNMPv2.

Configure all devices to only accept SNMP requests from specific servers and make sure that these servers are secure.

Fix the hardware address of system administrators workstations and the above SNMP monitoring servers in the ARP cache of the distribution routers, "**arp** *ip-address hardware-address"* this prevents anyone from trying to spoof these addresses.

Put passwords on all console and auxiliary ports on routers and switches

Lock LAN cabinets, many were open during my surveillance.

Replace Telnet, FTP and the r-services on production servers with SSH version 1.2.22 or later.

Stop the practice of issuing passwords to users. Enforce the requirement for strong passwords on the servers but have the users choose these themselves.

Update the patch level on all domain name servers to BIND 8.2.2

Shut down named.conf in the primary internal DNS so that it only makes transfers to known secondaries.

Remove unnecessary services on internal servers in much they same way as they have done for the external servers. It would appear that GIAC does not think there is much of a threat on the inside of their network.

Appoint a full-time security person. That person should be responsible for making sure that all the possible and exploited vulnerabilities that were identified by SARA are patched and that any new threat is quickly identified and passed on to the system/network administrators for their attention. He will do well to get himself on the mailing list of SANS, McAfee and other incident alerting agencies. He should also be responsibel for running periodic scans and against any server before it is allowed to become a part of the network.

Start a user security education program and enforce the use of screen savers and session lockup (not timeout) from the terminal servers.

There is little wrong with the existing architecture of GIAC Enterprises the only variation might be the use of an inside and an outside firewall so that there is no direct route from the inside out and vice versa. However, this could be a bit counter productive since there is little point in using two Cisco 525s in this mode and a firewall from another manufacturer even one as good as Checkpoint's FW-1 on a Nokia I330 would slow the movement of data through the secure area.

Appendix A

```
<HTML>
<HEAD>
<TITLE>SARA data collection </TITLE>
<LINK REV="made" HREF="mailto:sara@fish.com">
</HEAD>
<BODY>
<H1><IMG SRC=http://myserver.myisp.com:19479/images/sara.gif> SARA data
collection</H1>
<hr>
<B>Data collection in progress...</B>

<P>
<PRE>

Adding a primary target
Add-primary: giacwebserver.giac.com
Add-target: giacwebserver.giac.com prox 0
policy: giacwebserver.giac.com prox 0 level 2
Check-pulse: giacwebserver.giac.com
==> running bin/timeout 180 bin/fping giacwebserver.giac.com
process_targets: probe giacwebserver.giac.com...
Prox: 0
AL  : 2
Add-todo: giacwebserver.giac.com|dns.sara|
Add-todo: giacwebserver.giac.com|rpc.sara|
Add-todo: giacwebserver.giac.com|finger.sara|
Add-todo: giacwebserver.giac.com|ddosscan.sara|
Add-todo: giacwebserver.giac.com|hosttype.sara|
Add-todo: giacwebserver.giac.com|tcpscan.sara 1-1525,1527-5404,5406-
5899,5901-7099,7101-8887,8889-
9999,12345,16600,20034,27374,27665,31337,31785,65000|
Add-todo: giacwebserver.giac.com|udpscan.sara 1-1760,1763-
2050,31335,31337,27444,32767-33500|
==> running bin/timeout 20 bin/dns.sara  giacwebserver.giac.com
Add-fact:
giacwebserver.giac.com|dns|a|||giacrelay.giac.com|giacrelay.giac.com|Ma
il exchanger
Add-fact:
giacwebserver.giac.com|dns|a|||giacwebserver.giac.com|giacwebserver.gia
c.com|Mail exchanger
Add-fact:
giacwebserver.giac.com|dns|a|host|giacwebserver.giac.com|giacns.giac.co
m||authoritative DNS host
Add-fact:
giacwebserver.giac.com|dns|a|host|giacwebserver.giac.com|giacns.giac.co
m||authoritative DNS host
==> running bin/timeout 20 bin/rpc.sara  giacwebserver.giac.com
Add-fact: giacwebserver.giac.com||a|||||rpcinfo error #256
==> running bin/timeout 180 bin/tcpscan.sara 1-1525,1527-5404,5406-
5899,5901-7099,7101-8887,8889-
9999,12345,16600,20034,27374,27665,31337,31785,65000
giacwebserver.giac.com
Add-fact: giacwebserver.giac.com|netbios-
ssn|a||||\131\000\000\001\143|offers netbios-ssn
```

```
Add-fact: giacwebserver.giac.com|https|a|||||offers https
Add-fact: giacwebserver.giac.com|http|a|||||offers http
Add-fact: giacwebserver.giac.com|epmap|a|||||offers epmap
Add-fact: giacwebserver.giac.com|shell|a|||||offers shell
Add-fact: giacwebserver.giac.com|1028:TCP|a|||||offers 1028:TCP
Add-fact: giacwebserver.giac.com|1041:TCP|a|||||offers 1041:TCP
Add-fact: giacwebserver.giac.com|1033:TCP|a|||||offers 1033:TCP
Add-fact: giacwebserver.giac.com|1037:TCP|a|||||offers 1037:TCP
Add-fact: giacwebserver.giac.com|1039:TCP|a|||||offers 1039:TCP
Add-fact: giacwebserver.giac.com|1046:TCP|a|||||offers 1046:TCP
Add-fact: giacwebserver.giac.com|neod2|a|||||offers neod2
Add-fact: giacwebserver.giac.com|nim|a|||||offers nim
Add-fact: giacwebserver.giac.com|cardax|a|||||offers cardax
Add-fact: giacwebserver.giac.com|asprovatalk|a|||||offers asprovatalk
Add-fact: giacwebserver.giac.com|ansoft-lm-1|a|||||offers ansoft-lm-1
Add-fact: giacwebserver.giac.com|cplscrambler-in|a|||||offers
cplscrambler-in
Add-fact: giacwebserver.giac.com|rootd|a|||||offers rootd
Add-fact: giacwebserver.giac.com|rmiregistry|a|||||offers rmiregistry
Add-fact: giacwebserver.giac.com|1113:TCP|a|||||offers 1113:TCP
Add-fact: giacwebserver.giac.com|1153:TCP|a|||||offers 1153:TCP
Add-fact: giacwebserver.giac.com|1157:TCP|a|||||offers 1157:TCP
Add-fact: giacwebserver.giac.com|1170:TCP|a|||||offers 1170:TCP
Add-fact: giacwebserver.giac.com|1179:TCP|a|||||offers 1179:TCP
Add-fact: giacwebserver.giac.com|1185:TCP|a|||||offers 1185:TCP
Add-fact: giacwebserver.giac.com|ms-sql-s|a|||||offers ms-sql-s
==> running bin/timeout 20 bin/ddosscan.sara  giacwebserver.giac.com
==> running bin/timeout 180 bin/hosttype.sara  giacwebserver.giac.com
==> running bin/timeout 180 bin/udpscan.sara 1-1760,1763-
2050,31335,31337,27444,32767-33500  giacwebserver.giac.com
Add-fact: giacwebserver.giac.com|tftp|a|x||||offers tftp
Add-fact: giacwebserver.giac.com|epmap|a|x||||offers epmap
Add-fact: giacwebserver.giac.com|netbios-ns|a|x||||offers netbios-ns
Add-fact: giacwebserver.giac.com|netbios-dgm|a|x||||offers netbios-dgm
Add-fact: giacwebserver.giac.com|snmp|a|x||||offers snmp
Add-fact: giacwebserver.giac.com|snmptrap|a|x||||offers snmptrap
Add-fact: giacwebserver.giac.com|syslog|a|x||||offers syslog
Add-fact: giacwebserver.giac.com|1027:UDP|a|x||||offers 1027:UDP
Add-fact: giacwebserver.giac.com|1029:UDP|a|x||||offers 1029:UDP
Add-fact: giacwebserver.giac.com|1038:UDP|a|x||||offers 1038:UDP
Add-fact: giacwebserver.giac.com|ansyslmd|a|x||||offers ansyslmd
Add-fact: giacwebserver.giac.com|vfo|a|x||||offers vfo
Add-fact: giacwebserver.giac.com|startron|a|x||||offers startron
Add-fact: giacwebserver.giac.com|bsquare-voip|a|x||||offers bsquare-
voip
Add-fact: giacwebserver.giac.com|bridgecontrol|a|x||||offers
bridgecontrol
Add-fact: giacwebserver.giac.com|emanagecstp|a|x||||offers emanagecstp
Add-fact: giacwebserver.giac.com|amt-esd-prot|a|x||||offers amt-esd-
prot
Add-fact: giacwebserver.giac.com|cplscrambler-lg|a|x||||offers
cplscrambler-lg
Add-fact: giacwebserver.giac.com|proofd|a|x||||offers proofd
Add-fact: giacwebserver.giac.com|nicelink|a|x||||offers nicelink
Add-fact: giacwebserver.giac.com|sunclustermgr|a|x||||offers
sunclustermgr
```

```
Add-fact: giacwebserver.giac.com|rmiactivation|a|x||||offers
rmiactivation
Add-fact: giacwebserver.giac.com|mctp|a|x||||offers mctp
Add-fact: giacwebserver.giac.com|pt2-discover|a|x||||offers pt2-
discover
Add-fact: giacwebserver.giac.com|adobeserver-1|a|x||||offers
adobeserver-1
Add-fact: giacwebserver.giac.com|isoipsigport-1|a|x||||offers
isoipsigport-1
Add-fact: giacwebserver.giac.com|icp|a|x||||offers icp
Add-fact: giacwebserver.giac.com|ardus-mtrns|a|x||||offers ardus-mtrns
Add-fact: giacwebserver.giac.com|1118:UDP|a|x||||offers 1118:UDP
Add-fact: giacwebserver.giac.com|1121:UDP|a|x||||offers 1121:UDP
Add-fact: giacwebserver.giac.com|murray|a|x||||offers murray
Add-fact: giacwebserver.giac.com|1124:UDP|a|x||||offers 1124:UDP
Add-fact: giacwebserver.giac.com|1139:UDP|a|x||||offers 1139:UDP
Add-fact: giacwebserver.giac.com|1140:UDP|a|x||||offers 1140:UDP
Add-fact: giacwebserver.giac.com|1142:UDP|a|x||||offers 1142:UDP
Add-fact: giacwebserver.giac.com|1151:UDP|a|x||||offers 1151:UDP
Add-fact: giacwebserver.giac.com|1156:UDP|a|x||||offers 1156:UDP
Add-fact: giacwebserver.giac.com|1160:UDP|a|x||||offers 1160:UDP
Add-fact: giacwebserver.giac.com|1166:UDP|a|x||||offers 1166:UDP
Add-fact: giacwebserver.giac.com|tripwire|a|x||||offers tripwire
Add-fact: giacwebserver.giac.com|1177:UDP|a|x||||offers 1177:UDP
Add-fact: giacwebserver.giac.com|1178:UDP|a|x||||offers 1178:UDP
Add-fact: giacwebserver.giac.com|1184:UDP|a|x||||offers 1184:UDP
Add-fact: giacwebserver.giac.com|1186:UDP|a|x||||offers 1186:UDP
Add-fact: giacwebserver.giac.com|qt-serveradmin|a|x||||offers qt-
serveradmin
Add-fact: giacwebserver.giac.com|1280:UDP|a|x||||offers 1280:UDP
Add-fact: giacwebserver.giac.com|xs-openstorage|a|x||||offers xs-
openstorage
Add-fact: giacwebserver.giac.com|globe|a|x||||offers globe
==> running bin/timeout 20 bin/finger.sara  giacwebserver.giac.com
Add-todo: giacwebserver.giac.com|http.sara|http
Add-todo: giacwebserver.giac.com|sample.sara.ext|http
Add-todo: giacwebserver.giac.com|http.sara|https
Add-todo: giacwebserver.giac.com|sample.sara.ext|https
Add-fact: giacwebserver.giac.com|https|a|g||||offers secure http
Add-todo: giacwebserver.giac.com|snmpscan.sara|
Add-todo: giacwebserver.giac.com|tftp.sara|
Add-todo: giacwebserver.giac.com|smb.sara|
==> running bin/timeout 20 bin/sample.sara.ext https
giacwebserver.giac.com
==> running bin/timeout 20 bin/tftp.sara  giacwebserver.giac.com
Add-fact: giacwebserver.giac.com|tftp|a|||||TFTP isn't running or is
restricted
==> running bin/timeout 180 bin/http.sara http giacwebserver.giac.com
Add-fact: giacwebserver.giac.com|http|a|us|ANY@ANY|ANY@ANY|http cgi
access|WWW: RDS is active and may be vulnerable
==> running bin/timeout 20 bin/sample.sara.ext http
giacwebserver.giac.com
==> running bin/timeout 700 bin/smb.sara  giacwebserver.giac.com
Add-fact: giacwebserver.giac.com|netbios-
ssn|a|zwoi|ANY@giacwebserver.giac.com|ANY@giacwebserver.giac.com|netbio
s over the internet|Is your Netbios secure
==> running bin/timeout 180 bin/http.sara https giacwebserver.giac.com
```

```
Add-fact: giacwebserver.giac.com|https|a|g||||offers http
==> running bin/timeout 180 bin/snmpscan.sara  giacwebserver.giac.com
</PRE>
<P>

<B>Data collection completed (1 host(s) visited).</B>
<hr> <a href=http://myserver.myisp.com:19479> Back to the SARA start
page </a> |
<a href=../reporting/analysis.pl>Continue with report and analysis</a>
| <a href="../reporting/sara_info_host.pl,borderrouter.giac.com,">
View primary target results</a>
</BODY>
</HTML>
```

APPENDIX B

```
12-09-2000 18:43:55 ___
12-09-2000 18:43:55 THC-SCAN v2.00 started
12-09-2000 18:43:57 Port  initialized
12-09-2000 18:43:59 Modem initialized
12-09-2000 18:43:59 ConfigFile : THC-SCAN.CFG
12-09-2000 18:43:59 TXT-Scanning Mode
12-09-2000 18:43:59 TXT-Scanf  : EIANUM~1.TXT
12-09-2000 18:43:59 Scan Mode: Carrier
12-09-2000 18:43:59 Dialing  : Textfile input
12-09-2000 18:43:59 Scan started
12-09-2000 18:43:59202 3060329 Carrier(0) 30sec
12-09-2000 18:44:30202 3068647 Timeout(0) 50sec
12-09-2000 18:45:22202 3067525 Timeout(0) 50sec
12-09-2000 18:46:14202 3061098 Timeout(0) 50sec
12-09-2000 18:47:06 202 3068342 Timeout(0) 50sec
12-09-2000 18:47:57 202 3068340 Timeout(0) 50sec
12-09-2000 18:48:49 202 3060715 Timeout(0) 50sec
12-09-2000 18:49:41 202 3066049 Timeout(0) 50sec
12-09-2000 18:50:32 202 3064941 Timeout(0) 50sec
12-09-2000 18:51:24 202 3060596 Timeout(0) 50sec


13-09-2000 02:38:49 202 3064838 Timeout(0) 50sec
13-09-2000 02:39:40 202 3061469 Timeout(0) 50sec
13-09-2000 02:40:32 202 3061344 Timeout(0) 50sec
13-09-2000 02:41:24 202 3061678 Timeout(0) 50sec
13-09-2000 02:42:15 202 3064791 Timeout(0) 50sec
13-09-2000 02:43:07 Exiting with Error Level 0
```

12-09-2000 18:59:38 Dialing... 202 3067382

CONNECT 33600 V42bis

OK

12-09-2000 19:01:11 Dialing... 202 3062509

CONNECT 33600 V42bis

OK

12-09-2000 19:01:53 Dialing... 202 3062509

CONNECT 33600 V42bis

OK

12-09-2000 19:02:36 Dialing... 202 3062509

CONNECT 31200 V42bis

OK

12-09-2000 19:03:17 Dialing... 202 3062509

CONNECT 33600 V42bis

OK

12-09-2000 19:04:00 Dialing... 202 3062509

CONNECT 33600 V42bis

OK

12-09-2000 19:04:41 Dialing... 202 3062509

CONNECT 33600 V42bis