Global Information Assurance Certification Paper

SANS GIAC Firewall and Perimeter Protection Practical Assignment

SANS Monterey 2000

Submitted by: Chap Wong
11/20/2000

Assignment 1: Security Architecture - 25 Points

Define a security archtecture. The goal of your policy is to use filtering routers, firewalls, VPNs and internal firewalls to rapidly implement the VISA "Ten Commandments" to the extent possible at GIAC Enterprises, a new Internet Startup that expects to earn 200 million per year in sales of online fortune cookie sayings. The "Ten Commandments" are listed below:

1. Install and maintain a working network firewall to protect data accessible via the Internet.
2. Keep security patches up-to-date.
3. Encrypt stored data accessible from the Internet.
4. Encrypt data sent across networks.
5. Use and regularly update anti-virus software.
6. Restrict access to data by business "need to know."
7. Assign unique IDs to each person with computer access to data.
8. Track access to data by unique ID.
9. Don't use vendor-supplied defaults for system passwords and other security parameters.
10. Regularly test security systems and processes

The student assignment is to produce a diagram, or set of diagrams with explanatory text defining how to use perimeter technologies to implement as many of the requirements above as possible. For this assignment you are a large and growing E-business that just completed a merger/acquisition you must consider the need for customers, suppliers, and partners.

For this assignment, I used a CISCO 4500 router with IOS 11.2 as filtering firewall, a CISCO PIX as the main firewall, VPN is Nortel BayStack instant Internet 400 router. The PIX box is the main firewall for GIAC Enterprises. GIAC has small offices in many locations, and I use Nortel VPN to support those location. Web, Email and Ftp servers are located in the Screen Service network, . I also installed two PC Redhat Linux 6.2 with Snort (www.snort.org) as network intrusion detection system. I monitor all system with Big Brother (bb4.com), I also use Big Brother to scan the log and log any problems. Strict security policies are applying in the GIAC Enterprises, the base Policies are:

1) Firewall must be deployed is all Internet entrance point. CISCO PIX and Nortel VPN are used. All firewall configurations should be reviewed by at least two administrators. All logs will be kept at least one year. Log should be reviewed daily. Access to firewall will strictly limit to few authorized employee only. Backup firewall configuration file should be kept in a secure place.

2) Subscript to Cert-advisory (www.cert.org) Email list. Email from Cert-advisory will be reviewed within 24 hours, and implemented if applied within 48 hours, otherwise reasons for not applying the patches should be documented. Check CERT, SUN, SGI , HP, CISCO, RedHAT, Nortel site for security patch and security information daily. Also check SANS sites for security information.

3) All Internet Web data identified by owner as critical data should only be accessible by SSL and digital certificate by Entrust.

4) SSH is used to access all servers included X window (ssh tunnel).

5) World Secure Email Firewall is used to anti virus and spam on mail server. Also Snort is used to do intrusion detection, logs are reviewed daily. We run Snort under Redhat 6.2 PC. (snort rpm can be downloaded from www.redhat.com/swr/i386/snort-1.6.3-0.i386.html)

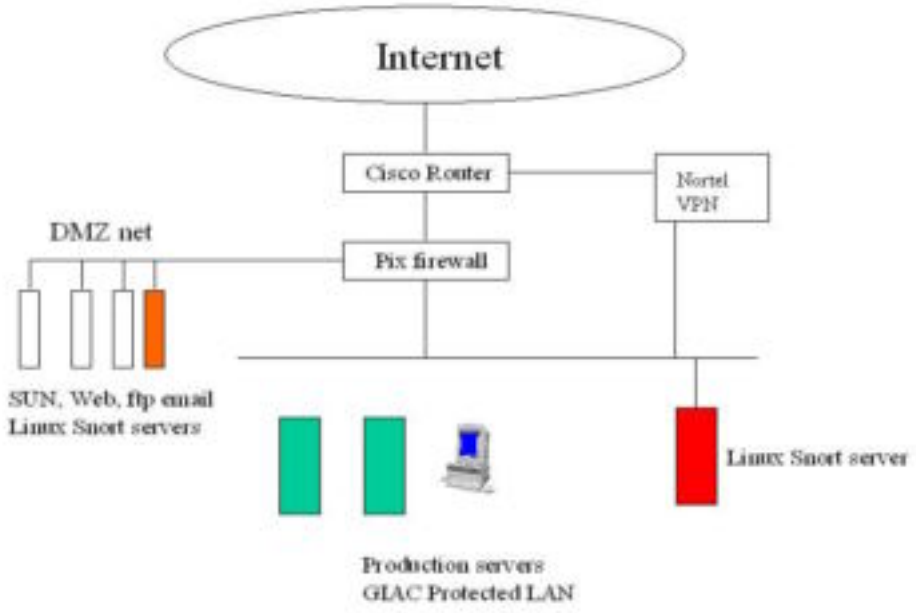
6) Data access is based on "need to know" bases. NT and UNIX groups are utilized to control data accessibility. UNIX netgroup is used to restrict access to machine. TCP wrapper is also implemented to restrict access. User are group to access only the data and machine they are authorized to. User access list is audit regularly to make the access list is kept current.

7) Every user has his/her own password. No group ID sharing is allowed. All password should be at least 8 characters and Crack is run nightly to check all password. Password should be changed every 30 days. At GIAC we maintain a data base of encrypted password to make sure password is changed every 30 days, and not to be reused not all. All users must sign computer usage agreement to make sure all usage is legal and business related. Legal warning banner messages is displayed when user logs on to any computer system.

8) All user logins are logged included fail logins. Session will be reset after three fail attempts.

9) TCP wrappers are implemented to limit machines access.

10) Security internal audit are performed regularly (at least once a quarter). Security external audit is performed once a year. (see assignment 3)



GIAC Network design

Assignment 2: Security Policy - 25 Points
For the purposes of this assignment, your security policy should be focused on implementation of requirement number 1 above "Install and maintain a working network firewall to protect data accessible via the Internet." For a baseline policy, use the filtering recommendations located at www.sans.org/topten.htm. You DO NOT need to repeat that information. Instead, focus on ADDITIONAL filtering you would recommend and why. Keep in mind you are an E-Business with customers, suppliers, and partners, you MAY NOT simply block everything! Your policy should implement your design above. Write a tutorial on how to implement each additional recommended action in the filtering policy below on your firewall or perimeter defense solution. Be explicit about the brand and version of perimeter defense. The base policy is taken from the recommended perimeter defense actions in the "Top Ten" document. Screenshots, network traffic traces, firewall log information and URLs to find further information should all be used. Be certain to include the following:
1. The reason these services might be considered a vulnerability
2. Relevant information about the behavior of the protocol or service on the network
3. Syntax of the filter
4. Description of each of the parts of the filter
5. Explain how to apply the filter
6. If this filter is order dependant, what other rules should this filter precede and follow**
7. Explain how to test the filter
8. Be certain to point out any tips, tricks, or gotcha's.
** You may find it easier to create a section of your practical that describes the order you would apply all of the rules rather than trying to do it with each policy cluster. Be certain to explain your reasons for the order you choose, we cannot read your mind.

Base Security Policy
Please note, we are not asking you to repeat the blocking instructions for the "top ten" security vulnerabilities. You may wish to reference one of the later practicals in your work since they were focused on blocking the "top ten" they can be found: http://www.sans.org/giactc/gcfw.htm
In this section, we list the base security policy so you know what additional services to recommend blocking. These are ports that are commonly probed and attacked.
Blocking these ports is a minimum requirement for perimeter security, not a comprehensive firewall specification list. A far better rule is to block all unused ports. And even if you believe these ports are blocked, you should still actively monitor them to detect intrusion attempts. A warning is also in order. Blocking some of the ports in the following list may disable needed services. Please consider the potential effects of these recommendations before implementing them.
1) Block "spoofed" addresses-- packets coming from outside your company sourced from internal addresses or private (RFC1918 and network 127) addresses. Also block source routed packets.
2) Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)
3) RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)
4) NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 - earlier ports plus 445(tcp and udp)
5) X Windows -- 6000/tcp through 6255/tcp
6) Naming services-- DNS (53/udp) to all machines which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp)
7) Mail-- SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)
8) Web-- HTTP (80/tcp) and SSL (443/tcp) except to external Web servers, may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.)
9) "Small Services"-- ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)

10) Miscellaneous-- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/tcp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp)

1) ICMP-- block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded, and unreachable messages

Following are GIAC IP addresses for GIAC servers.

ISP provider address for Cisco router outside 100.1.1.50
Cisco Router to PIX port 1.1.1.1
PIX to Cisco PIX port 1.1.1.2
PIX to DMZ net port 2.2.2.1
DMZ zone Web (http, https) 2.2.2.2
FTP 2.2.2.3
Email 2.2.2.4
PC LINUX 2.2.2.5
Citrix server 2.2.2.6
DNS server 2.2.2.7
PIX to Production network 3.3.3.1

For this assignment we will discuss the VPN set up. In additional to block the Top Ten services we are monitoring CERT current activity daily included any new Virus Activity , Scans and Probes. As of 11/20/2000, Liuxconf (98/tcp), Klogind (542/tcp) and SGI Objectserver (5135/tcp) shows up on Scan and Probes list in additional to some of the ten top services in the SANS lists. All our SGI boxes are running 6.5.7 and above, so we are not concern about Objectserver. We also scan our network to make sure any services can be exploited will be blocked. We used nmap (www.nmap.org) to do the scanning. We also review Snort log to look for irregular service activity. Currently we are checking the following service port in additional to the ten top list of SANS.

Citrix ICA 1494/TCP allow for Citirx thin clients.
Citirx ICA 1604/TCP allow for Citrix publish applications
IMAP 3 220/TCP block
SQL-net 1521/TCP block
Shell 514/TCP block
BootP 67 TCP/UDP block
Talk 517 TCP block
Ntalk 518 TCP block
Printer 515 TCP block
SGI cluster discovery 5450, 5451, 5452, 5453, 5454 /TCP block.

Now, let us look at some of the Cisco filter router configuration statement and some PIX firewall statement to address this assignment. We are running CISCO IOS 11.2 and PIX versions 5.0(3). I configured Cisco to block the services list above.

1) Linux is a fast growing OS in today's computer environment. Many Linux distributions ship with linuxconf, a program which listens on TCP port 98. According to

Cert, There are no reports of intruders actively exploiting vulnerabilities in linuxconf (11/20/2000), however, these probes may be used to identify linux machines that other vulnerabilities.

access-list 100 deny tcp any eq 98

2) In CA-2000-06, Klogind, a Kerberos authentication daemon buffer overflow is reported.

Access-list 100 deny tcp any eq 543

3) Citrix ICA is using by Citirx Metaframe for thin client technology, GIAC runs both Citirx NT and Citrix UNIX servers, we are migrating to VPN for all remote client. When our migration is done, we will block Citrix ICA port 1494 and publish application port 1604. But for now, we need to allow Citrix ports to come into GIAC network. These entries are reminder for us to change when migration is done.

access-list 100 permit tcp any eq 1494
aceess-list 100 permit tcp any eq 1604

4) I also want to block IMAP 3 port 220/TCP in additional to POP (109/tcp and 110/tcp) and IMAP(143/tcp). IMAP 3 is a superset of POP2 is to allow a (possible unreliable) workstation to access electronic mail from a reliable mailbox.

access-list 100 deny tcp any eq 220

5) SQL-NET is used to access our Oracle data base. We will deny any attempt to access oracle from outside.

access-list 100 deny tcp any eq 1521

6) We also want to block shell 514 tcp.

Access-list 100 deny tcp any eq 514

7) bootpc 67 and 68 will be blocked. It is used by bootp and dhcp. They should not coming into GIAC network.

acess-list 100 deny tcp any eq 67
acess-list 100 deny udp any eq 67
acess-list 100 deny tcp any eq 68
accss-list 100 deny udp any eq 68

8) Ntalk and Talk are message daemons, we have no reason to use it so they are blocked.

```
access-list 100 deny udp any eq 517
access-list 100 deny tcp any eq 517
access-list 100 deny udp any eq 518
access-list 100 deny tcp any eq 518
```

9) GIAC has SGI cluster installed, so we don't want to see any cluster discovery to come in. Port 5450, 5451, 5452, 5453 and 5454 TCP are used by SGI to do SGI cluster discovery. Any discovery command can be used to probe our environment and allows future exploit. So we have to examine and block any discovery commands that we don't see a business need to come in.

```
access-list  100 deny tcp any eq 5450
access-list 100 deny tcp any eq 5451
access-list 100 deny tcp any eq 5452
access-list 100 deny tcp any eq 5453
access-list 100 deny tcp any eq 5454.
```

Now we have to allow all other traffic to come in, the default ACL for Cisco router is to block all.

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

Then we apply it to the external interface

```
interface serial 0/0
ip address 100.1.1.50 255.255.255.0
ip access-group 100 in
```

For PIX firewall configuration, we will name the outside interface to Cisco router "ouside", the production network "inside" and the screened network "dmz"

```
: Name interfaces and assign security level, most secure 100 for inside, 10 for dmz and
0 for outside
: interface

nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security10

;Identify network interface speed and duplex
interface ethernet0 100Full
interface ethernet1 100Full
```

```
interface ethernet2 100Full
:
ip address outside 1.1.1.2 255.255.255.0
ip address inside 3.3.3.1 255.255.255.0
ip address dmz 2.2.2.1 255.255.255.0

: PIX fixup protocol are enable for default, I list them as reminder for ftp http and smtp.
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25


: Disable Network address Translation for our network.
nat (inside) 0 0.0.0.0 0.0.0.0

static (dmz,outside)  2.2.2.2 netmask 255.255.255.255 0 0
conduit permit tcp host 2.2.2.2 eq http any
conduit permit tcp host 2.2.2.2 eq 443 any

static (dmz,outside)  2.2.2.3 netmask 255.255.255.255 0 0
conduit permit tcp host 2.2.2.3 eq ftp any

static (dmz,outside)  2.2.2.4 netmask 255.255.255.255 0 0
conduit permit tcp 2.2.2.4 eq smtp any

static (dmz,outside)  2.2.2.6 netmask 255.255.255.255 0 0
conduit permit tcp 2.2.2.6 eq 1494 any
conduit permit tcp 2.2.2.6 eq 1604 any


static (dmz,outside)  2.2.2.7 netmask 255.255.255.255 0 0
conduit permit tcp 2.2.2.7 eq 53 any
```

Other PIX security related PIX configuration statement I use:

```
: Specifies SNMP information may be accessed by internal hoss that knows the
community string, but
: PIX Firewall does not send trap information to any host
no snmp-server location
no snmp-server contact
snmp-server community helloyoucantguessthis
no snmp-server enable traps

:  My workstatoin can telnet to PIX firewall
telnet 3.3.3.10 255.255.255.255 inside
```

Assignment 3: Audit your security architecture - 50 Points
For the purposes of this assignment please assume that you have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises, a electronic commerce facility that is the largest supplier of electronic fortune cookie sayings in the world. The firewall analyst has set their firewall up according to their base + recommended enhancements security policy that happens to mirror your assignment 1 security policy exactly. Your assignment is:

- Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.
- Implement the assessment. Validate that the firewall or perimeter router is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Screenshots when possible should be included in your report.
- Perimeter analysis. Based on your assessment and referring to data from your assessment, analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

GIAC audit has three parts, the most important opponent is an audit documentation. The documentation is the base for the security audit and it is the minimum-security procedure for GIAC Enterprise. The second part is the system administrator will perform their own audit quarterly and provide audit report to GIAC management. The third part will be outside auditor who will audit the administrator activity and ongoing maintenance/update of the audit documentation.

Audit document:

System logs:

Important system event is tracked and evaluates. Firewall logs, sulog, acct log, wtmp, loginlog and shutdown log should be scanned daily. All logs will be kept for one year. Bib Brother is a tool we use to monitor system: system activity, disk usage, network usage and we also use it to scan the system log.

Change Control

Review the change control procedure, critical configuration change should be documented and reviewed by more than one person. Backup plan will be provided for critical system function changes.

Backup and Recovery

GIAC is electronic commerce facility, firewall route and server are critical opponent for the company. Backup and Recovery plan will be documented and backup up plan should be exercised at least once a year.

Physical Security

Firewalls, routers and servers should maintain in physically secure area. We should review all personal who has the authority to enter the secure area quarterly

Intrusion detection

Nmap should be run nightly in the dmz and screen network to make sure we filter all no necessary ports in our Cisco router and PIX firewall.
Snort log will be reviewed daily to check any intrusion activity.

User administration

Review user list, group list to make sure our user list is up to date. User password must be at least 8 charters. All user account is kept in a database and all users can't reuse old password. All passwords should be expired at 30 days. No default password is allowed. Crack is run nightly.

Access to machine

Review all netgroup and tcp wrapper information to make sure only authorize personal can access to the resource they need. We also need to test our CISCO ACL and PIX firewall at least once a quarter. We can use "telnet address portnumber" to test the connection.

From Internet to test whether we can access mail to our production network

telnet 3.3.3.10 25

We should have a connection time-out.

We will test common service, ftp, nfs, smtp, http with the simple telnet address port regularly.

Access to data

Review all critical data attribute. Data should only be accessed by authorize user. Data owner should review the access list regularly. The list should be cleaned up regularly (once a month).

OS Patches

All security patches listed in Cert should be reviewed within 24 hours and implemented within 48 hours. If there is reason not to install the patched, it should be documented. In additional to security patches, OS level should not be older than 6 months, otherwise reasons should be documented.

Internal and External audit

During internal and external audit, we should review the security policy as stated in assignment number 1, review these items. Develop a checklist, list who is responsible for each item list in the policy. Also we have to go over the audit document, develop action item, assign people to check each item. For the staff to test the network, testing should be done in the weekend, so it will not impact our system performance.

Internal audit should be done at least quarterly. External audit should be done once a year. External audit should also include a review and update of the audit document. Internal audit should take abut three days, and external audit should take five days. Security checking, included log scan, security patch watching, implementation, monitoring vendor, Cert and SANS sites should be a half full time job. GIAC will delicate half of a administrator's time for that activity.

Known Weaknesses and Suggested Improvements to the Physical Network Architecture.

The followings are know weakness and suggested to improve to the assignment.

1) Both Cisco router and PIX are Cisco product and might have the same software or hardware problem. We can replace the PIX firewall with a Firewall 1 firewall. In this Monterey SANs conference, more than half of the people in the class is using Firewall 1, so I suggest to replace the PIX with Firewall 1.
2) In our production network, we don't have additional firewall to protect any critical data, so we might put the FIX firewall inside our product network and use it to further protect our data.