Global Information Assurance Certification Paper

GIAC level two – Firewalls , perimeter protection and VPNs.

Practical assignment for captiol SANS

December 10 -15 2000.

Giac Enterprises
Security Plan

SUBMITTED BY - AVI SARFATI

This Document is an assignment written for the GIAC level two perimeter protection Course – for a GCFW certification.

Practical assignment for capitol sans – December 10 – 15 2000.

Giac Enterprises
Security Plan

Table of Contents

List of Tables

List of Figures

1. Scope

GIAC Enterprises is a new Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings. This document is to provide A security plan for the enterprise.

GIAC must allow access for:

- Customers (the companies that purchase bulk online fortunes).
- Suppliers (the authors of fortune cookie sayings that connect to supply fortunes).
- Partners (the international partners that translate and resell fortunes).

The assumption is that , as a start up , GIAC's security budget is limite d, Hence Security Architecture must not be overloaded.

The security plan outlined in this document specifies Perimeter protection measures only.

The document will continue to describe to auditing measures for the selected architecture.

In addition, the doc ument will include a "Underfire" examination of a previous posted SANS GIAC assignment.

2. Guidelines

Security guidelines are derived from the technical aspects. Both are in derived from the business needs. (Numbering in sections corresponds). The security plan is formed based on the following guidelines.

2.1. BUSSINESS REQUIERMEN TS

[B.1] Giac Enterprises should provide, Non-interruptible, service to it's customers.

[B.2] Customers personal info, collected and processed by Giac Enterpr ises, should be available to the individual customer only, and should in no way be accessible to others.

[B.3] Connectivity should be provided to partners (Suppliers and Partners will be dealt in the same manner and will here after will be regarded as Part ners).

[B.4] Full connectivity should be provided to traveling company employees.

2.2. TECHNICAL REQUIERMEN TS

[T.1.a] All system components should include high availability and should be covered in a disaster recovery plan.

[T.1.b] The Internet c onnection should not be a single point of failure.

[T.2.a] Customers will access their data by web browsing (HTTP).

[T.2.b] As the application in use requires ASP support, web servers will be IIS.

[T.3.a] At current state, there is only one partner abroa d. It is estimated that one or two may be added. Connectivity would be provided through the Internet. Connectivity is needed for partners to access an internal Development Lab. Connectivity will be provided through the Internet.

[T.4.a] Estimated traveler s 5-15. Connectivity will be provided through the Internet.

2.3. SECURITY REQUIERMENT S

[S.1.a] Security mechanisms should ensure the systems "resistance" to attacks, and especially D.O.S attacks. On line alerting should be provided by the mechanisms in every case of an attempted attack or a successful one in order provide ASAP human intervention.

Intruder detection systems will be deployed. "Tripwire" technologies will be used in order to track changes.

[S.1.b] In order to thwart Flooding D.O.S attacks, "dual home"ing mechanism should be deployed.

[S.2.a] As customers will access by HTTP and they will access private data, SSL should be used to secure the confidentiality of the session. SSL will not include two way authentication (through the us e of client certificates) as there is currently no distribution method, and will rely on user authentication (by password) on the application level.

Aside of HTTP and HTTPS, there are no other protocols that should be used by the customers. Hence, Perimete r filtering should drop all other protocols.

[S.2.b] As IIS is regarded as a vulnerable component (as holes are discovered periodically), Buffering mechanisms should secure their access. NT/Win2k OS for the servers would be strictly armored. Strict procedu res for their security will be implemented including frequent security audits and on -line alerting.

[S.3.a] VPN should be used in order to secure Parteners connections. As the number of partners is small, VPN should be integrated with the FW (and not a separate system). Access should be allowed for the internal Development lab only.

[S.3.b] External parties that will need access to the company network will have to use a VPN connection. External developers will be allowed access only to components on a "mus t" basis. Network architecture should segment these components in order to confine access to a specific area.

[S.4.a] Remote access to the company for travelers would be provided by the use of VPNs. VPNs will be handled by the FW component (due to the smal l number of travelers). Access will be authenticated both on the client level and on the user level.

2.3.1. General security guidelines

[GS.1] A multi-layered approach for security will be deployed. Security will be configured at every level – network, host and application level. Security configurations will be, in some cases, overlapping in order to thwart attacks that might be successful in one of the layers.

[GS.2] The "Deny all but specifically allowed" approach for security/flittering mechanisms will be preferd.

[GS.3] Every kind of access will be based on the "need to know" rule.

[GS.4] Internal network compartmentalization will also be based on the "need to know rule", Through the use of network segmentation, filtering and access controls and permissions.

[GS.5] All system components will be categorized by the following classification scale:

Table 1: Classification scale.

Classification	Explanation
No	Holds no security aspect what so ever. May be freely accessed.
Medium	Holds data that is sensitive in a non -crucial manner (one that does not threatens the company's existent). Allowed for all company employees only.
High	Holds data that is very sensitive in a manner that, if revealed, threatens the company's existents . Access control mechanisms should insure it's limited distribution.

[GS.6] "Good Internet neighbor" principals will be applied.

3. Classification of components.

Table 2 below describes the components needed in the compan y's architecture. It also describes their needs for classification and access control. Classification of components will allow segmentation analysis for the architecture design.

Table 2: Components. Classification and access contro l.

Component	Classification	Access control
Customer related Components		
Web server (accessible directly)	**No**. Server by itself does not hold any data. Data is retrieved from the dB by ASP during session.	Every customer may only see his private data. Authen tication is processed by application. Authentication credentials must be protected in transit
DB (Serves as backoffice for the system)	**High** .Holds private customer data including financial.	Should not be accessible by customers (only the web server is allowed to retrieve after authentication). Should not be accessible by internal employees – Only by accounting.
DNS -external (To allow internet accessibility).	**No**. The server must not hold DNS data for internal purposes only general.	Should be protected fro m vandalizing/poisoning in order to allow business continuity.
Company external interface related components		
Mail server	**Medium** . Privacy issues of employees. (Not secret –"**High**" material would be encrypted at the application level - PGP).	Users may acc ess the mailbox only. Administrative access will be provided to Sys admins only.
Ftp server (Exchanging files between subsideries).	**Medium .** "**High**" data will not be allowed through by procedure.	All company employees , travelers and subsidiaries. Private folder will be supplied.
Internal company components		
WS + file and print servers.	**Medium**. Users that will hold "**High**" material will secure them by using local tools (encrypted disks).	All local data should be accessible for the user only. Administrative access is allowed.
Laptops (for travelers)	Will be regarded as **High** due to the nature of exposure due to missing physical security.	User access only.

Component	Classification	Access control
Lab servers	**Medium.**	Fully accessible for company employees. May be accessed by subsideries.
DNS – internal	**Medium.**	For internal uses only.

Conclusions:

The architecture should include 5 zones –

1. **No** - accessible to all (Web servers). – Zone A2
2. **No** – external. – Zone A3
3. **Medium** – accessible to employees only (General Network). - Zone A4
4. **Medium** – accessible to employees and Partners (Lab). - Zone A5
5. **High** – Access per need (Db). – Zone A6

4. Architecture

4.1. CONCEPTUAL ARCHITECT URE

Figure 1 below describes the conceptual security architecture.

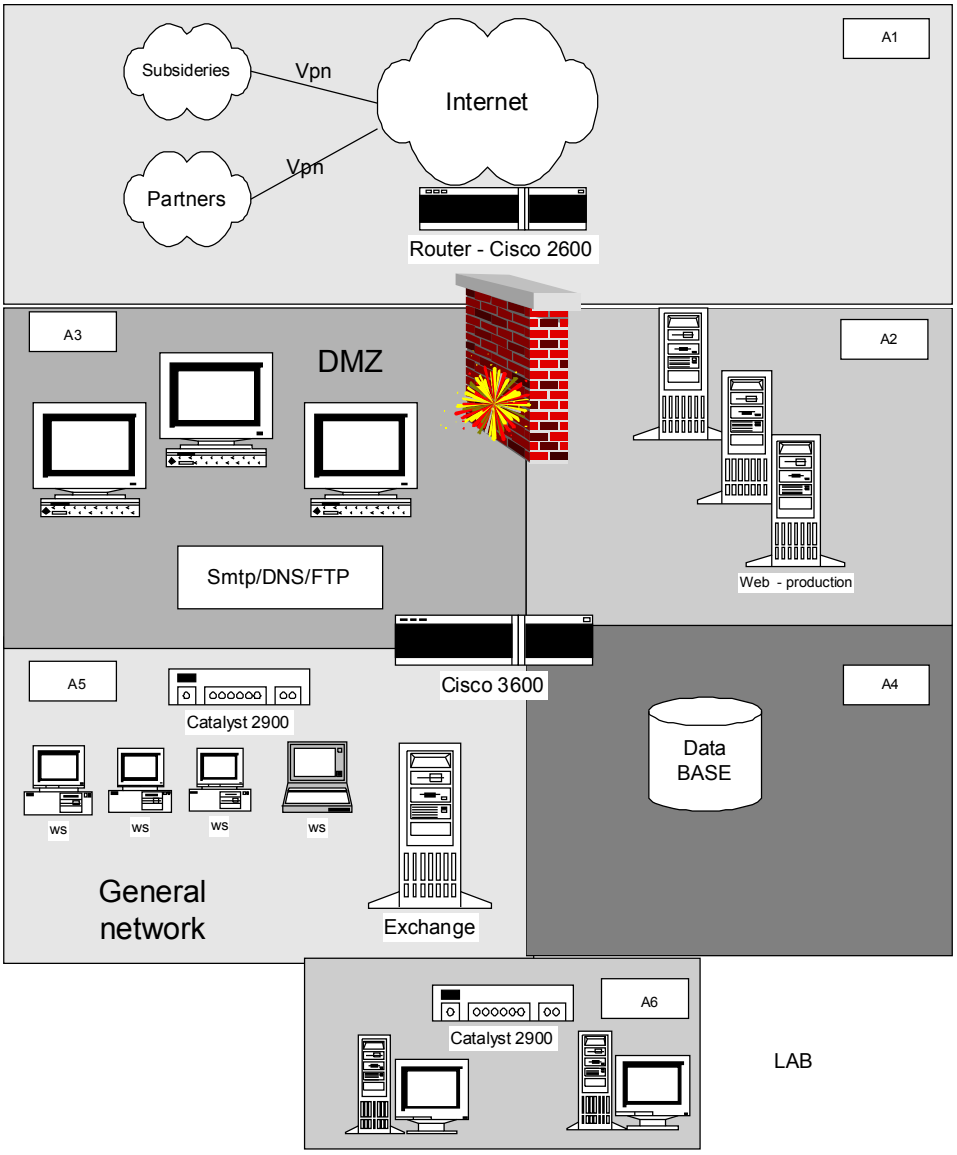


Figure 1: Security architecture.

4.2. NETWORK ARCHITECTURE

Figure 2 below describes the network architecture.

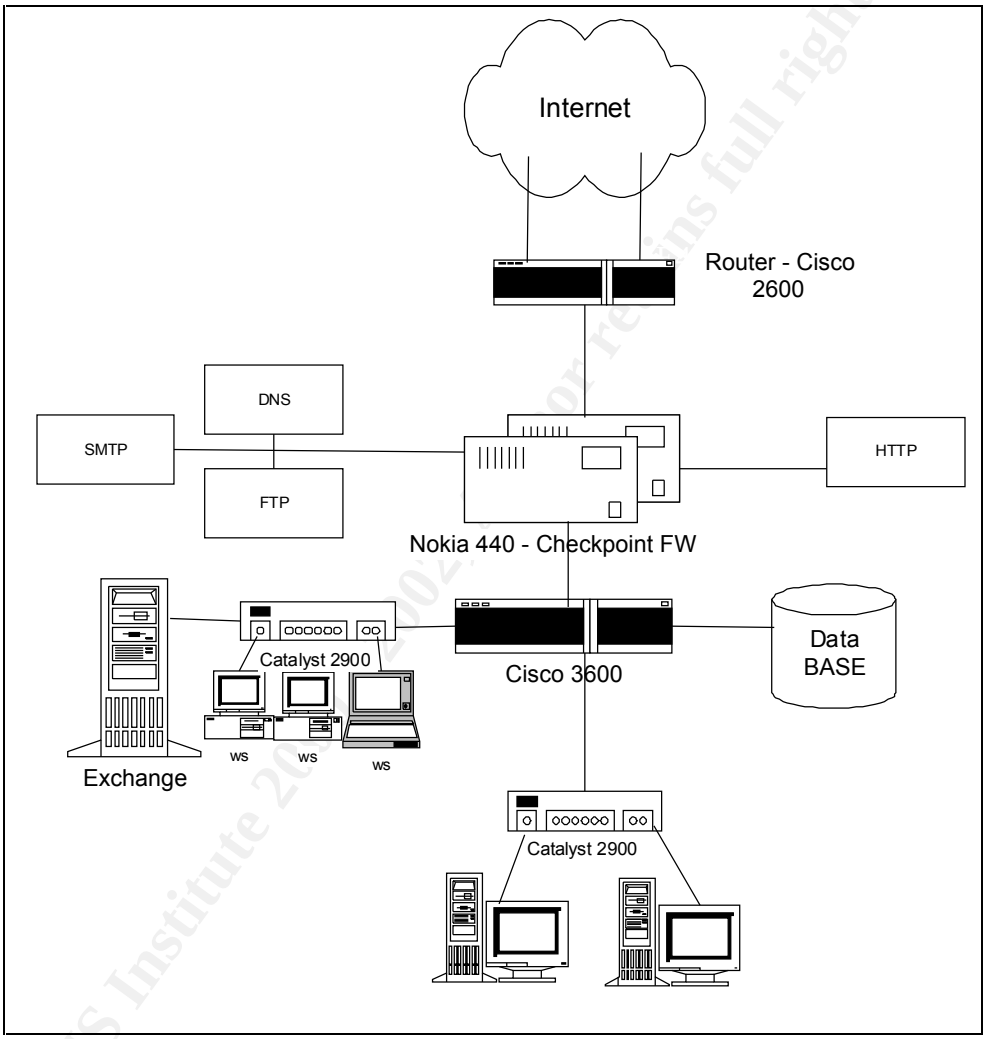


Figure 2: network architecture

5. Security Policy

This section will detail the security policy for every com ponent mentioned above. Policy will be presented by zone segregation as in figure 1.

Every section will also include the rulebases/ACLs for the interfaces relating to that zone.

Note: In the following "Outbound" will be used into specify access going out from Giac Enterprises's network; were as "Inbound" will specify access entering it.

5.1. ZONE A1

The zone includes the Internet connection through a Cisco 2600 router.

As a border GW the router will be configured to act as the first line of defens e.

The router will provide dual ISP connection in order to thwart D.O.S attacks.

The router will be configured to provide NAT.

5.1.1. Armoring the router

The following will be used to armor the Router:

- Service password-encryption
- Enable secret.
- No service tcp-small services.
- No service udp-small_services.
- No service finger.
- No ip unreachables.
- No ip direct-broadcast.
- No ip bootp server.
- No ip http server.
- No ip source route.
- No snmp.
- Banner / Warning: Authurized Acees Only – Giac Enterprises/.

5.1.2. Thwarting D.O.S attacks.

In order to thwart D.O.S attacks Cisco's strategy will be deploye d as found at - http://www.cisco.com/warp/public/707/newsflash.html.

5.1.3. Interface A1.1 (Inbound – external interface)

The Access list at the border router will be designed as deny explicit.

The ACLs are designed based on SANS top ten threats.

Block spoofed address + local host + multicast addresses +invalid.

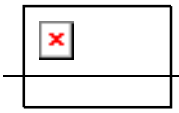
Access-list 1xx	Deny	10.0.0.0	0.255.255.255
Access-list 1xx	Deny	127.0.0.0	0.255.255.255
Access-list 1xx	Deny	172.16.0.0	0.15.255.255
Access-list 1xx	Deny	192.168.0.0	0.255.255.255
Access-list 1xx	Deny	224.0.0.0	0.31.255.255
Access-list 1xx	Deny	host	0.0.0.0

Block login services – telnet, exec, lpd, r-services, netbios and ssh.

Access-list 1xx	Deny	tcp any any range telnet exec lpd log
Access-list 1xx	Deny	tcp any any range 512 514
Access-list 1xx	Deny	tcp any any range telnet exec lpd log
Access-list 1xx	Deny	tcp any any eq 139 log
Access-list 1xx	Deny	tcp any any eq 22

Block RPC and NFS – sunrpc, NFS, lockd

Access-list 1xx	Deny	tcp any any eq sunrpc log
Access-list 1xx	Deny	udp any any eq sunrpc log
Access-list 1xx	Deny	tcp any any eq 2049 log
Access-list 1xx	Deny	udp any any eq 2049 log
Access-list 1xx	Deny	tcp any any eq 4045 log
Access-list 1xx	Deny	udp any any eq 2049 log



NetBios

Access-list 1xx Deny tcp any any eq 135 log
Access-list 1xx Deny udp any any eq 135 log
Access-list 1xx Deny udp any any eq 137 log
Access-list 1xx Deny udp any any eq 138 log
Access-list 1xx Deny tcp any any eq 139 log
Access-list 1xx Deny tcp any any eq 445 log
Access-list 1xx Deny udp any any eq 445 log

Xwindows

Access-list 1xx Deny tcp any any range 6000 6255 log.

Naming Services – DNS, ldap (Allow DNS for external use).

Access-list 1xx Permit tcp any 'DNS-ext' eq 53 .
Access-list 1xx Permit udp any 'DNS-ext' eq 53 .
Access-list 1xx Deny tcp any any eq 53 lo g.
Access-list 1xx Deny udp any any eq 53 log.
Access-list 1xx Deny tcp any any eq 389 log.
Access-list 1xx Deny udp any any eq 389 log.

Mail – smtp, pop, imap (allow to ext. mail -relay)

Access-list 1xx Permit tcp any 'mail-relay' eq 25 .
Access-list 1xx Permit tcp any 'mail-relay' eq 109 .
Access-list 1xx Permit tcp any 'mail-relay' eq 110 .
Access-list 1xx Permit tcp any 'mail-relay' eq 143 .
Access-list 1xx Deny host 'mail relay'.

Web Access –HTTP ,SSL.

Access-list 1xx Permit tcp any 'Web-servers' eq 80 .
Access-list 1xx Permit tcp any 'Web-servers' eq 443 .
Access-list 1xx Deny host 'web servers'.

Small services -

Access-list 1xx Deny tcp any any range 0 20 log.
Access-list 1xx Deny udp any any range 0 20 log.
Access-list 1xx Deny tcp any any eq 37 log.
Access-list 1xx Deny udp any any eq 37 log.

Miscellaneous -

Access-list 1xx Deny udp any any eq 69 log.
Access-list 1xx Deny tcp any any eq 79 log.
Access-list 1xx Deny tcp any any eq 119 log.
Access-list 1xx Deny tcp any any eq 123 log.
Access-list 1xx Deny tcp any any eq 515 log.
Access-list 1xx Deny udp any any eq 514 log.
Access-list 1xx Deny tcp any any eq 161 log.
Access-list 1xx Deny udp any any eq 161 lo g.
Access-list 1xx Deny tcp any any eq 162 log.
Access-list 1xx Deny udp any any eq 162 log.
Access-list 1xx Deny tcp any any eq 179 log.
Access-list 1xx Deny tcp any any eq 1080 log.

Permit -

Access-list 1xx Permit ip any any.

5.1.4. Interface A1.2 (outbound – internal interface)

Egress -

Access-list 1xx Permit 10.0.0.0 0.255.255.255.

Access-list 1xx Deny any log.

5.2. FW1 VPN CONFIGURATIO NS

Subsidiaries, Road warriors and partners netw orks will be granted access through configuration of VPNs - subsidiaries to A5 and A6, Partners to A6 only.

- The Vpn will be configured as follows:
- Vpn will use Ipsec.
- Vpn will implement ESP (as full encryption is needed to secure the data transfers).
- Vpn will use this SA – 3DES, MD5.
- Users access will be permitted through the use of secure -remote VPN agent.

Source	Destination.	Service	Action	Track	Inst. on	Time
Subsidiaries	Int-net	Any	ClientEncrypt	Short	FW	Any
Partners	Lab	Any	ClientEncrypt	Short	FW	Any
All-users@any	Int-net	Any	ClientEncrypt	Short	FW	Any

5.3. ZONE A2

This zone includes the FW-1 interfaces relating to access to the web servers.

5.3.1. Interface A2.1 (Inbound from A1)

This interface defines what access will be permitted from the Internet to the web servers. It allows web access for customers (Web service is defined to include SSL).

Source	Destination.	Service	Action	Track	Inst. on	Time
Any	Web-ser	Web	Accept	No	FW	Any

5.3.2. Interface A2.2 (Outbound to all interfaces)

- No sessions allowed, aside of access to the dB.(next section).

5.3.3. Interface A2.3 (Outbound to A4)

Allow dB query by the web-servers.

Source	Destination.	Service	Action	Track	Inst. on	Time
Web-ser	dB	SQL	Accept	No	FW	Any

5.3.4. Web servers

The web servers will be NT based and as such will be armore d as sepcified with the "Windows NT security guidelines" (http://www.trustedsystems.com).

The IIS 5 web server will be configured using the "Internet server security tool". (http://www.microsoft.com/WINDOWS2000/news/bulletins/iistool.asp) .

In addition application security will be provided through the use of Sanctum's AppSheild (http://www.sanctuminc.com).

5.4. ZONE A3

5.4.1. Interface A3.1 (Inbound fr om A1)

Source	Destination.	Service	Action	Track	Inst. on	Time
Any	Ext-Dns	DNS	Accept	short	FW	Any
Any	Ext-Mail	SMTP	Accept	No	FW	Any
Any	Ext-FTP	FTP	Accept	short	FW	Any

5.4.2. Interface A3.3 (Outbound to A5)

Allow mail relaying to internal netw ork.

Source	Destination.	Service	Action	Track	Inst. on	Time
Ext-mail	Int-Mail	X400	Accept	No	FW	Any

5.5. FW-1 OUTBOUND RULEBASE AND GENERAL SECURITY

In order to complete the FW -1 rulebase there's a need to define the general outbound rules.

Source	Destination.	Service	Action	Track	Inst. on	Time
Int-net	ANY	SQL	Drop	Long	FW	Any
Int-net	ANY	Any	Accept	Long	FW	Any

* the first rule is another precaution in case circumstance will change and somehow allow access to the dB.

The FW will include th e RealSecure Intruder detection option and will allow traffic analysis for intrusion attempts.

The Syn defender option will be used in order to thwart Syn attacks.

5.6. ZONE A4

Zone A4 is protected (In addition to the FW -1) by the internal r outer ACLs.

5.6.1. Interface A4.1 (Inbound to A4)

Allow Db query only

Access-list 1xx Permit tcp 'web-serv' 'dB' eq 1433 log

Access-list 1xx Permit tcp 'Accounting' 'dB' eq 1433 log.

5.7. OTHER COMPONENETS

Other components security requirements are wider than to be included in this doc. They will be covered in separate docum ents.

6. Combined FW -1 Rule Base.

For the logic flow – Rulebase was developed above as separated interfaces. Below is an aggregation of these rulebases into one (as will actually be deployed at the FW).

Table 3: FW-1. Rule base.

Source	Destination.	Service	Action	Track	Inst. on	Time
Subsidiaries	Int-net	Any	ClientEncrypt	Short	FW	Any
Partners	Lab	Any	ClientEncrypt	Short	FW	Any
All-users@any	Int-net	Any	ClientEncrypt	Short	FW	Any
All-users@any	Dev-serv	Web	User auth	Long	FW	Any
Any	Web-ser	Web	Accept	No	FW	Any
Any	Ext-Dns	DNS	Accept	Short	FW	Any
Any	Ext-Mail	SMTP	Accept	No	FW	Any
Any	Ext-FTP	FTP	Accept	Short	FW	Any
Web-ser	dB	SQL	Accept	No	FW	Any
Ext-mail	Int-Mail	X400	Accept	No	FW	Any
Int-net	ANY	SQL	Drop	Long	FW	Any
Int-net	ANY	Any	Accept	Long	FW	Any
ANY	ANY	ANY	Drop	Short	FW	Any

7. Auditing of security policy

This section describes the action needed in order to test the strength (and proper deployment) of the security policy.

A network sniffer will be used in order to check that the VPNs are adequately configured (check that sessions are encrypted).

Nmap tool would be used in order to port scan the external interfaces of the border router and the FW. Results will be compared to the ACLs and RuleBase. (Checks will be onducted several time at different time of day)

Vulnerability scanners will launched from outside. Tools will include SARA, SATAN and ISS's Internet Scanner. The check will also be run on all DMZ components.

The intruder detection engine will be tested to detect the above tests.

Internal Router ACLs will be tested by trying to access/open sessions, which are not SQL and thus denied.

The armored servers will also be checked through the use of vulnerability scanners.

The Db security will be tested by using ISS's Db Scanner.

Sanctum's APPscan will test the Web servers application layer.

Tools:

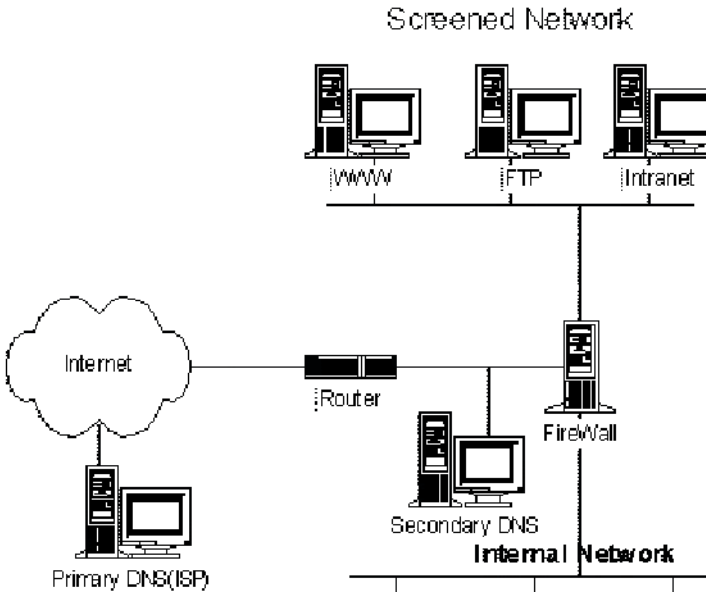
Nmap http://www.insecure.org

ISS http://www.iss.net

SATAN http://www.porcupine.org/satan/

Sanctum http://www.sanctuminc.com .

8. Design Under fire



- DNS 53/UDP is allowed from the screened network (DMZ) & from the Internet Network to the secondary DNS which is as shown above is outside the firewall, while DNS 53TCP/UDP are allowed from the Secondary DNS to the World.
- HTTP & HTTPS are allowed from the internal networks to the DMZ (Mail & Web, intranet) servers and to the universe.
- HTTP & HTTPS are allowed from the universe to the (WWW& Mail) in the DMZ.
- POP, POP3, SMTP are Allowed from the universe to the DMZ mail.
- POP, POP3, SMTP are allowed from the internal to the Mail server in the DMZ& from the internal to the universe through the application gateway proxy since some internal users have personal mail accounts on other internet servers.

http://www.sans.org/y2k/practical/Hussam_Hamdy_Hanafy.doc

8.1. ATTACK AGAINST THE F W ITSELF:

The FW is a Raptor V.6 – the vulnerability I chose to exploit is of a D.O.S type.

A denial of service attack was discovered against the Axe nt Raptor firewall that can cause the system to freeze. When the firewall's IP option parsing code tries to skip a 'benign' option, it forgets to check if it is of zero length. This error can cause the code to enter an irrecoverable infinite loop. The IP o ptions that can lock up the firewall are the Timestamp and Security options.

Such formed packet can be easily formed through the use of "Sniffer" programs.

Running such an attack will cause the FW to freeze – thus denying any service.

The remedy is to app ly Axent's Hotfix.

See full details at - http://www.securityfocus.com/frames/?content=/templ ates/archive.pike%3Flist%3D1%26date%3D1999 -10-15%26msg%3D199910202245.RAA28104@expert.cc.purdue.edu

8.2. A D.D.O.S ATTACK

The first thing to do is to make sure your ISP has D.O.S countermeasures - to detect and thwart massive attacks such as this. This should insure that the connection will not be clogged.

At the border GW I would apply Cisco's D.O.S advisories - http://www.cisco.com/warp/public/707/newsflash.html .

These specifically include the "IP verify unicast reverse -path" command and "rate limiting" both ICMP and SYN packets.

Either than that I would apply an IDS system at the GW in order to be acknowledged when an attack occurs. The system can also be used for automatic response.

I would also consider a redundant Internet connection, if the services I am offering are time sensitive.

8.3. INTERNAL SYSTEM COMP ROMISE

The system I would select is the web server due to the following reasons - The system must be acces sible (Http). By nature, web servers are a vulnerable system. The aim is to get a "foot hold" within the internal network, which can later be expanded.

As the architecture places the Intranet server in the same DMZ segment, once the Web server is accessibl e, so would the intranet. Siting on the DMZ I would be able to sniff the POP,IMAP passwords as they are passing in clear text.

I would later place malicious code with the intranet server (Since I can rely that internal users have little security measures, if any, for local zones).this trojanized code (server) will be then installed by users – allowing (hopefully) full access.

B.T.W – It would be easy to map the internal network, due to the lack of internal DNS. (The external can be interrogated – if not compromised).