Global Information Assurance Certification Paper

SANS GIAC Certification
Level 2 GCFW
Firewall and Perimeter Protection Curriculum

Practical Assignment for SANS Network Security 2000
Monterey CA, October 15–19, 2000

Written by:
Alexander Usenko

10/22/2000

Assignment #1: Security Architecture

Define a security architecture. 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.

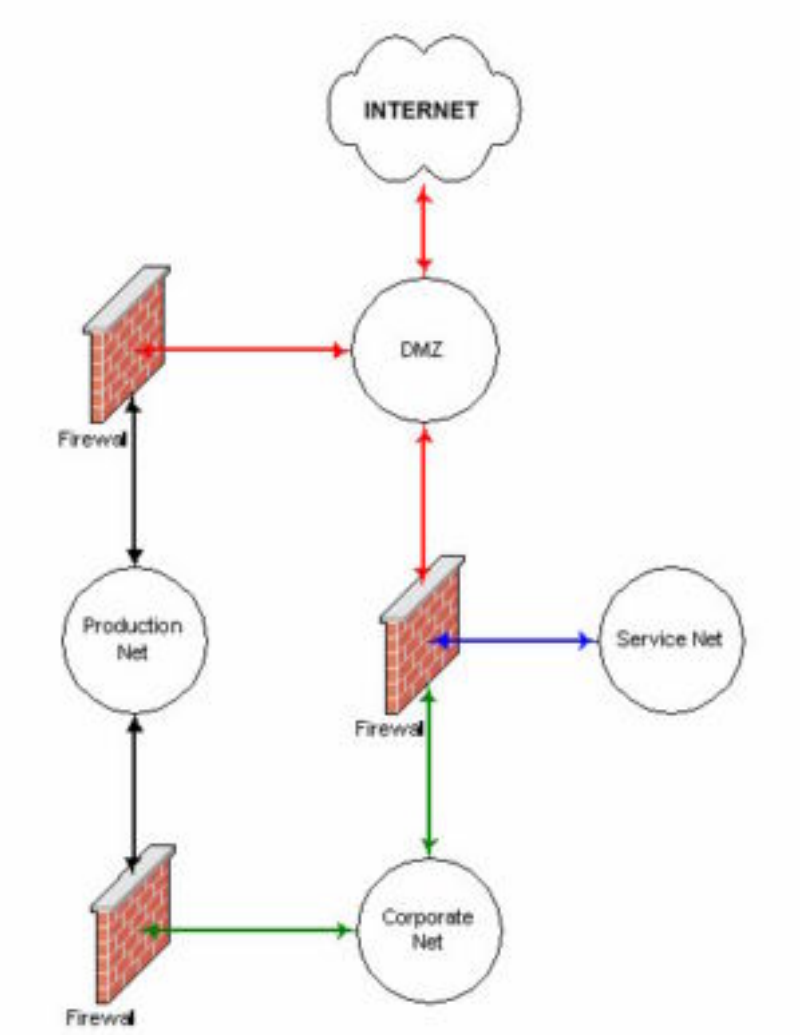
1. Physical Network Architecture

Please note that proposed network architecture is of a modular type, with independent and logically separate Corporate and Production Networks. In real life very often these networks are also physically separated, e.g.: Production Network is situated somewhere at a Co-location facility and Corporate Net is located in the Corporate office and has its separate connection(s) to ISP. In such a case it is highly recommended to have a dedicated private point-to-point line between Production and Corporate.

This design approach has several advantages especially important for rapidly growing and highly mobile E-Commerce Startup Companies: not every Company can afford to have a "state-of-the-art" Data Center with redundant multi-path network connections, redundant power, raised floor, sufficient air-conditioning, the adequate level of physical security, etc., etc.; the bandwidth requirements are different for Production and Corporate and it is usually significantly less expensive and much faster to get an additional bandwidth at Co-location then to bring something like DS3 into your office; you do not need to move your Data Center every time your office has to move.

The physical network is divided into several security zones. Each zone has it's own function and/or a different level of security. Each of these zones is separated from the other zones and protected by means of a firewall, filtering router or similar device.

The following main security zones were defined (the Diagram #1: Principal Networking Diagram):



A. The Untrusted Network (The Internet) - it mainly includes the connection(s) to Internet Service Provider.

B. DMZ (or Unprotected DMZ) - a subnet with minimal protection from potential attackers/intruders. This minimal protection is provided by our first line of defense - border screening router.

C. The Service Network (or Protected DMZ) - a subnet protected by the external corporate firewall with limited access from and to Internet. We will use this subnet for all the public Internet services we need to provide to Internet users, e.g.: corporate website, external DNS, mail relays, etc.

D. The Internal Corporate Network - a subnet behind the Corporate firewall which is not accessible from Internet unless via secure VPN tunnels; the Internal Corporate Network may be further "compartmentalized" and have a developed and complex structure where each part of it could be also isolated and protected by firewalling devices;

E. Production Network (or E-Commerce Network) - highly protected and multi-layered "compartmentalized" network

Border Router

The screening border router is located between the Internet and the DMZ. This router has basic ingress/egress filters to block spoofed addresses and some other unwanted traffic. The router shall not be considered as a substitution for a firewall. Although it has some filtering capabilities those are limited and CPU intensive and you do not want to put a complex ACLs on your router, especially when that is just an underpowered low-end device like Cisco 2500 series router.

The screening border router must be "hardened": all unnecessary services and features should be disabled; SNMP should be disabled or blocked on external interface; ICMP should be blocked. IP source-routed packets should be blocked since they could be exploited to have a device or host return packets using selected routes thus bypassing firewalls and/or router filters. IP directed-broadcasts should be turned off on all interfaces in the router to prevent smurf attacks from our network (for details check Craig Huegen's white paper on smurf and DOS attacks available at http://www.pentics.net/denial-of-service/white-papers/smurf.html). To protect the router itself and to complicate the fingerprinting of our network we will also block specific TCP/UDP services directed at the router such as echo, chargen, finger and ICMP-Redirects.

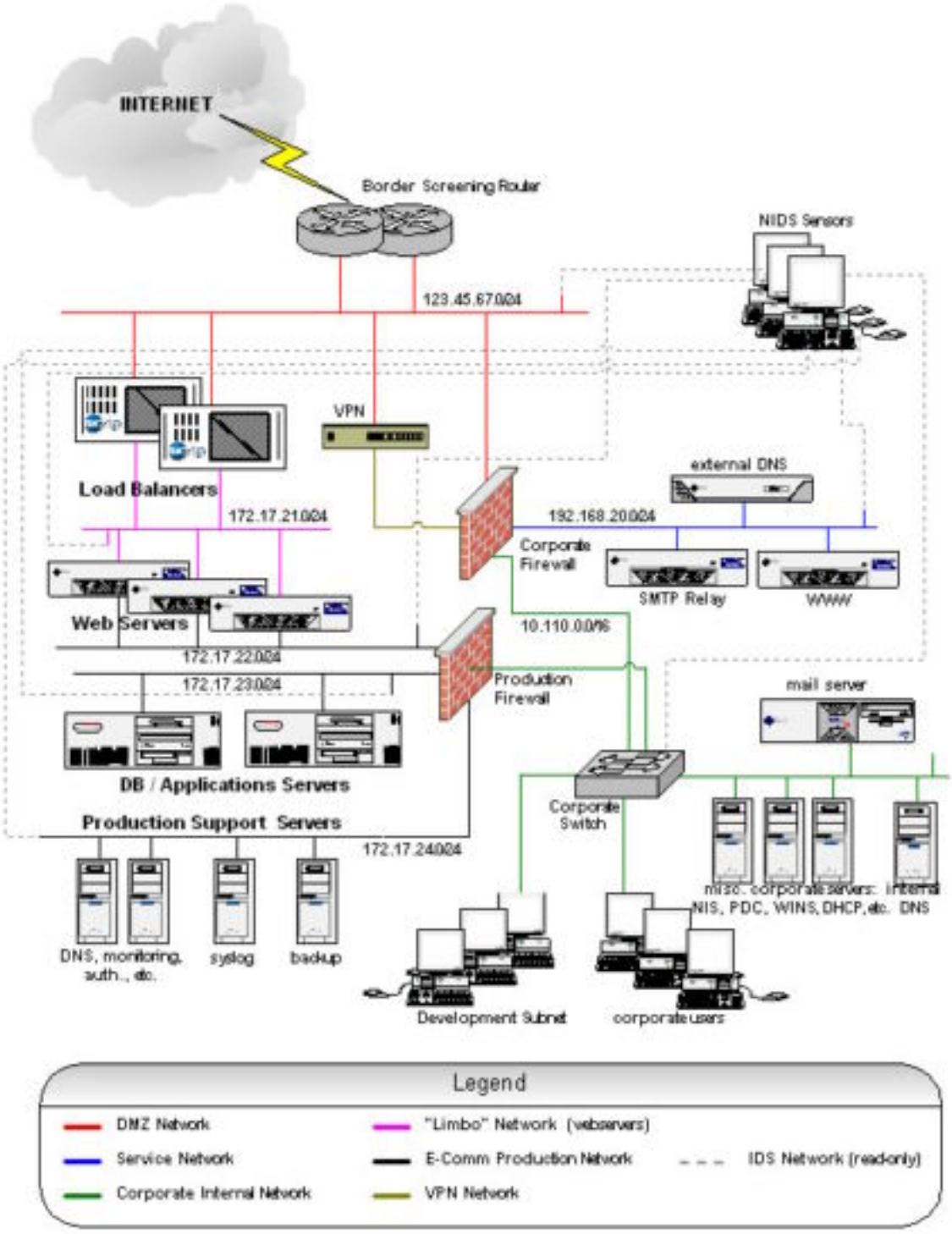
Management of the router should be done via either SSH (where applicable) or telnet, with access restricted to a limited number of addresses and only from the corporate network side of the router. Egress traffic filters may be implemented to ensure no spoofed traffic is forwarded from the corporate network to the Internet. All the passwords should be changed frequently and according to the corporate security policy (i.e. monthly). For more information on securing Cisco routers please check the appropriate document at: http://www.cisco.com/warp/public/707/21.html

Corporate Firewall

Between the DMZ, the Service and the Internal networks we have placed an application gateway firewall such as a Checkpoint Firewall-1 system or similar. The platform (hardware, firmware and operating system) hosting the firewall should be hardened by applying the latest vendor supplied/recommended patches/service packs and disabling all non-required services. Management of the firewall machine shall be done via console or if remotely then SSH only, with access restricted to a limited number of addresses and only from the internal network interface of the firewall. All administrative and other passwords should be changed frequently and accordingly to corporate security policy, all non-required accounts and features should be disabled on the firewall.

Diagram #2

GIAC Enterprises Network Diagram



Incoming firewall policies are implemented to ensure that legitimate traffic: web, mail, dns (you may want to limit it to UDP only except from secondary DNS server(s), although this could be considered as an extra precaution as the appropriate access lists for zone transfers should be implemented on our primary DNS server) and VPN traffic is forwarded only to the servers that are supposed to accept that traffic and all other traffic is blocked. All filters output and denials should be logged. Outgoing policies from the Service network should permit outgoing mail and DNS queries; all other outgoing connections should be blocked and logged. Outgoing policies from the Internal network to Service network should allow connections from authorized systems via SSH/VPN to servers for administrative purposes and between internal and external mail servers for mail exchange. Depending on decision of the corporate Management, an outgoing policy may also be implemented to allow outgoing web or any other connections from the Internal network and department subnets to the Internet. For the purposes of this assignment an assumption is made that GIAC Enterprises Management has decided to completely trust its employees and that anything outgoing Corporate to Internet is allowed.

VPN server

The VPN server will be used to allow secure connections with remote offices and users, business partners and suppliers. The VPN could be the firewall itself, or it could be a separate dedicated box. The detailed network diagram (Diagram #2) shows the VPN server as a separate device in case if we decide not to use firewall for this purposes of if we choose a firewall that does not have the VPN functionality. IPSec suit of protocols is the most common/standard and therefore recommended for compatibility with different vendors.

Network Intrusion Detection System (NIDS)

This is a very important integral part of our Network Security Architecture. NIDS sensors should be strategically placed on all the networks you want to monitor. Should any of these networks be breached, the NIDS should detect the intruder before significant damage can occur. All the communications between sensors and central collection station should be encrypted and done via separate "of-the-bandwidth" network.

Corporate network / Internal Firewalls

Depending on specific client requirements you may want to further "compartmentalize" the corporate Internal network. Additional internal firewalls may be implemented between critical Department subnets within Internal network to isolate them from each other and to restrict access to corporate informational resources and/or to Internet. Although be reasonable: it is usually difficult to justify the purchase of something powerful and expensive (e.g. Nokia IP 650 with an unlimited license) for the purpose of isolating internally HR Department from Legal and Engineering. A small firewall appliance (e.g.: Netscreen-5, SonicWALL or similar) or any other IP-filtering device/software could easily do the job.

Servers

All the servers located on the corporate Internal and Service networks should have all the current patches installed, unnecessary services disabled and should be configured to allow management access only from a restricted group of addresses. Unnecessary tools and programs should be removed from the server. A checksums (cryptographic hashes) database should be created of all programs at the time of initial server installation and stored in a secure place (not locally) and on read-only media to be used to assess whether the server has been compromised or any of the sensitive files altered (Tripwire or similar could be used for the purpose). All management should be performed via either SSH or directly at the server's console (in case if you have a central console server this machine/device should be considered as very sensitive and secured appropriately).

E-commerce Production databases or any sensitive or personally identifiable information should never be stored unencrypted. If you are using public key encryption make sure that only the public key located on the server.

Mail servers should have virus-scanning software installed to scan email and attachments, signature files should be updated regularly from trusted sources. DNS servers should be configured to allow zone transfers only to secondaries. Services supplied by default with the operating system should be carefully scrutinized and if necessary replaced with more secure versions of these tools/services from respected 3rd party sources.

Production (E-Commerce) Network

If you look at block-schema (diagram #1) you can see a typical "classical" approach when any network has firewall in front of it and in between. Now, if you check the actual implementation (see more detailed networking diagram #2) you will notice that in front of our Production Network there is no firewall per se. That's because we use our load-balancers as effective firewalling devices.

All modern load-balancers (Alteon, F5, etc.) have pretty powerful built-in IP-filtering mechanisms that should be used to protect load-balancers themselves and servers behind them. Although it is not really required, in addition we can also protect load-balancers by installing ACLs on the border router to permit incoming http and https traffic only.

In cases where web-traffic is substantial and you need to utilize load-balancers we do not think that firewall will add any security/functionality. Moreover, traditional firewall will sooner or later become a bottleneck. And to deal with it you will have to increase the complexity of your design.

And we've seen already a lot of bulky, difficult to implement and manage and very expensive designs where first line of load-balancers used to "load-balance" the line of firewalls what in turn will "protect" next line of load-balancers and only those are finally used to spread the load on web-servers. It is not a really effective approach.

In real life when you permit only http/https to your webservers the traditional firewall does not really add a protection. If your webservers will be ever hacked – then they will hacked through legitimate open ports (80, 443 or any others your webservers are listening to) and your application firewall won't protect the servers.

That's why we suggest for an implementation of the following design:

a) use border router and load-balancers to protect your webservers on Production Network from outside and block everything but required services only;
b) since webservers are the only servers accessible from Internet consider these as "high-risk" group (expendable/replaceable) and put them on a separate subnet – "Limbo";
c) implement the "internal" firewall to strictly control all the connections between the webservers and other components of our "fortune cookies" applications/servers/databases;
d) do not allow any outgoing connections from web/applications/DB/servers and implement a special "service" subnet to consolidate all the facilitating services and servers which may require such connections.

Corporate Security Procedures:

To fully address all the 'Ten Commandments' and to complete the Assignment #1 of this Practical we would use the following checklist:

"Ten Commandments" checklist:

1) *Install and maintain a working network firewall to protect data accessible via the Internet.*

   The installation was addressed under the first part of this assignment. Maintenance of our networked security systems should also include regular monitoring and analyzing the log files from all the components: firewalls, routers, servers and IDS (Intrusion Detection Systems). Regular reviews and tests of existing firewall policies and filters should be done on a periodical basis to ensure the correctness and full compliance with corporate security policy.

2) *Keep security patches up-to-date.*

   The systems and security administrator should be assigned to monitor respected information sources such as Bugtraq, CERT, GIAC, vendor mailing lists / websites and other alternative sources of information for system vulnerabilities and security updates/patches. Log files should be checked to determine if any breaches listed in the advisories have occurred. Updates/patches should be obtained and tested to ensure sanity prior to installation. After installation on the live network, an audit should be run to determine if vulnerabilities are patched and no new problems were created, if there are, these should be immediately addressed. Intrusion detection systems should have their attack signature databases updated frequently.

3) Encrypt stored data accessible from the Internet.

It should be addressed by corporate security policy that no critical data should be stored on any server that is exposed to the Internet. A multi-layered approach and tiered architecture is the standard model for Internet web applications, with a firewall between the web/application servers and the database servers. In case if third party web applications require the users registration database stored within its own architecture then passwords shall be stored in an encrypted format. Production databases with any personally identifiable or sensitive information should be stored encrypted. If you are using public key encryption methods make sure that only the public key located on the server.
All the tapes with backups for off-site storage should be encrypted as well.

4) *Encrypt data sent across network.*

A) E-commerce web traffic to clients will be encrypted using SSL.
B) All communications between remote offices, business partners and suppliers should be encrypted via VPN solution (in our case it could be the same firewall box with an additional software license (Checkpoint's VPN-1 Gateway) or could be also a standalone VPN box such as Compatible Systems, Altiga or RedCreek.
C) Remote access traffic is encrypted by means of VPN server/client (again: could be Checkpoint VPN-1 Gateway / SecureClient or just a standalone VPN box with a software client).
D) Email traffic is encrypted using PGP or similar.

5) Use and regularly update anti-virus software.

Anti-virus software should be installed on all firewalls (where applicable), mail servers, and every and each employee workstation. New viruses signatures should be regularly downloaded from contracted vendors and distributed internally. Some of the vendors have "auto-updating" feature which should be used with a caution or better yet reconfigured to pick-up updates from internal corporate server

6) Restrict access to data by business "need to know."

This commandment is usually addressed by strong authentication and encryption of the data. According to our standard procedures approval by the respective data owner shall be required for access authorization. Access to networks, servers, applications and data should be based upon the user's profile and his/her role(s) within the organization. Access to internal sensitive informational resources (payroll, sales, customer information, etc.) should be audited, and the data owners should review the audit reports for compliance. It could be also addressed in the Physical Network Architecture and facilitated by implementing internal firewalls between Departments.

7) Assign unique IDs to each person with computer access to data.
8) Track access to data by unique ID.

These two commandments should be addressed by Corporate Security Policy. Each employee should be issued a unique user ID with the profile / appropriate level of access that their job requires, and that each user is responsible for all activities under this user identity on any of the

corporate systems. Shared IDs are not acceptable and shall not be issued.. Third parties who require access to extranet applications/systems (partners, vendors, etc.) will be issued unique IDs as well. These third parties should be required to sign a legal access agreement before the IDs are issued. No anonymous/general purpose/role-user/guest accounts shall be used for any kind of access to the systems, networks or data. For accountability and tracking purposes System Administrators should also log into the servers with their personal user IDs and then escalate to the root or system administrator's account/privilege level as required (e.g. using the "su", "sudo" or "runas" utilities on unix, which also provides control, tracking and logging capabilities).

9) *Don't use vendor-supplied defaults for system passwords and other security parameters.*

Standard procedures / best practices for secure configuration of different systems, network gear and applications should be developed, maintained and implemented by the responsible team. Default passwords should be changed, and any unnecessary default accounts should be either removed or disabled. Sample scripts and programs should be removed. Default parameters should be also modified to reflect the corporate security policy

10) *Regularly test security systems and processes*

The corporate Internal Audit team should conduct periodic audits of network, operating systems and applications security. These audits should be scheduled regularly using security assesment tools such as network and vulnerabilities scanners (nmap, Nessus, etc.). Independent security audits of corporate perimeter security and external web applications should be also performed periodically by contracted third parties to validate findings of the internal audits. Password cracking programs such as John the Ripper or Crack could be run periodically to test compliance with password policies.

The security group should have access to an external Internet connection separate from the primary Internet connection for the purposes of performing audits and scans of the GIAC Enterprises network. This separate Internet connection should only be accessible from a host secured and isolated from the corporate network.

We will also address these points in details in the first part of Assignment #3 of this document.

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

There is no need to explain the well-known statement that the rule of thumb for creating good security policy is to keep it as simple as possible. The more rules you have the more opportunities

exist to inadvertently misconfigure your firewall or router and potentially expose your network to outside world.

The best base security policy should be to permit the minimum access to hosts with explicitly defined ports/protocols to provide the required services. So, despite the encouraging statement in the SANS definition for this very assignment that *"...you are an E-Business with customers, suppliers, and partners, you MAY NOT simply block everything!*" we will take a risk not to agree with them and we WILL simply block everything but explicitly permitted services what absolutely required to run the business. By permitting the services required and finishing our policy with deny "any-any", we effectively implement the "top ten" recommendation to the greatest extent possible while blocking all other traffic. And obviously if business needs will be changed we will review and modify this security policy as all security policies are driven by those business needs.

We've been trying to be vendor-neutral in our Assignment #1 - Physical Network Architecture but for the purpose of Assignment #2 we will need to make our assumptions on the platforms for our perimeter protection devices. And for the purpose of this assignment that will be Cisco (perhaps 2600 series) as the border router and Nokia IP (440 or 650; 330 is too small and has not enough interfaces) with CheckPoint FW-1 ver. 4.1. After all: no one was fired for buying from: first IBM, then Cisco and now CheckPoint. Although, to be honest: if customer will not insist on something different and if they won't have specific technical requirements to support their choice of vendor and finally if money is not an issue I would strongly recommend Cisco and FW-1 (my personal favorite flavor is Nokia appliances; Sun boxes are next).

We can obviously adjust and implement our security architecture on any platform if necessary but Cisco and CheckPoint would be the "reference" platform.

For the purpose of this assignment we will implement the security policy for one of our networks only, namely Corporate Network, since this one has most of the network components we may need to protect (DMZ, Service Net and Protected Net), most of the features and also because the architecture is standard and clear.

2.1 Border Router Configuration and Rules (Best Practices)

The border router should be set up with ACLs to prevent spoofing and drop selected ICMP. The router will forward all other traffic to the firewall or VPN.

Ingress ACLs should be added to the routers outside interface to block packets with spoofed source addresses. These rules drop all packets that have source addresses in the private address space.

```
! Deny RFC 1918 addresses
!
access-list 17 deny 10.0.0.0 0.255.255.255 log
access-list 17 deny 172.16.0.0 0.15.255.255 log
access-list 17 deny 192.168.0.0 0.0.255.255 log
!
```

```
!Deny loopback and other illegal addresses
!
access-list 17 deny 127.0.0.0 0.255.255.255 log
access-list 17 deny 0.0.0.0 0.255.255.255 log
access-list 17 deny 255.255.255.255 0.0.0.0 log
!
!Deny spoofing of our registered addresses (This includes the firewall and service network
servers)
access-list 17 deny xxx.yyy.zzz.0 0.0.0.255 log
!Allow everything else
access-list 17 permit any
!
! (outside interface of router)
!
interface serial 0
ip access-group 17 in
```

Egress ACLs may also be set up on the inside interface of the router to prevent our networks from sending spoofed packets.

```
!Allow only packets from our network  addresses.
access-list 22 permit 123.45.67.0 0.0.0.255
! Deny and log  everything else
access-list 22 deny any log
!
! (inside interface of router)
interface ethernet 0
ip access-group 22 in
```

The following will prevent ICMP broadcasts, ICMP unreachable messages, and IP source routing. Also, we want to disable SNMP, all unused tcp/udp services, and CDP (Cisco discovery protocol).

```
!(apply this in gobal config mode)
service password-encryption
no ip source-route
no snmp.
no service tcp-small-servers
no service udp-small-servers
no service finger
no ip http service
no ip bootp service
!
!(apply this on external interface)
no ip proxy-arp
no ip directed-broadcast
```

no ip unreachables
no cdp enable
ntp disable

All the logs should be written on the syslog server and keep it also locally (useful for debugging).

logging <syslog server address>
logging buffered

Place an access list defining the IP addresses that can connect to the router. Only IP addresses listed in the access list will be allowed to make a telnet connection to the router. The connection will appear to come from the firewall since NAT is used. If your router does not have SSH support then remove the line in red in the following:

access-list 3 permit <firewall-address>
line vty 0 4
transport input ssh
access-class 3
login

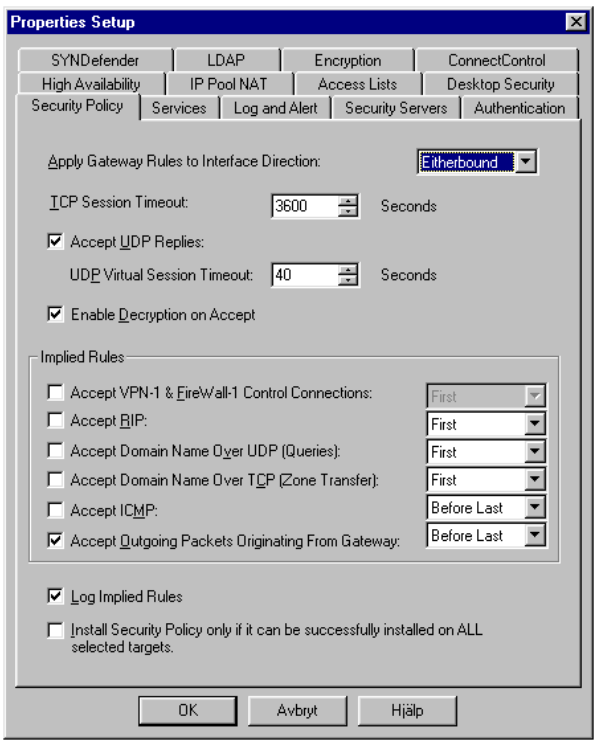
For additional information on securing Cisco routers see:
http://pasadena.net/cisco/secure.html
http://www.cisco.com/warp/public/707/21.html
http://www.attrition.org/~modify/texts/phrack/Phrack55/P55-10

2.2 Firewall Configuration

The following firewall policy assumes for the purpose of this exercise that the base policy referenced in the assignment instructions has been implemented via a combination of filters on the border router and firewall rules on the Corporate firewall. In addition to the blocking of these ports, ingress and egress filtering has been implemented on the Cisco border router.

The first step in setting up a secure rulebase on the CheckPoint Firewall-1 4.1 firewall is to review the default properties page and turn off the default properties. For more details, please read a whitepaper, "Building Your Firewall Rulebase" by Lance Spitzer, at http://www.enteract.com/~spitz/rules.html.

If you want to see a screenshots here they are:



Also, we would like to mention for the purpose of this assignment we assume that readers are familiar with a product and we will not go into great details on configuring and tuning the FW-1. Since numerous papers and tutorials were already written by SANS students with great attention to details and with nice illustrations and screenshots we suggest you may wish to check some of those tutorials at http://www.sans.org/giactc/gcfw.htm . Check Patric Sternudd's practical – it is one of the best tutorials on FW-1.

As with many firewalls and other packet-filtering devices, rule order for Firewall-1 policy is critical. When a packet is received, the firewall compares it against the rulebase and when it finds the first match, it applies that rule. Therefore it is important to keep the more specific rules first and the more general rules last.

Rule 1: Firewall administration access to the firewall.

This rule allows firewall administrators to access the firewall, and limits them to only the predefined Firewall-1 services. Access is limited to group of IP addresses. The rule must appear in order above the firewall lockdown rule (Rule 3).

Rule 2: Reject ident protocol from any source

The ident protocol may be used by many services/servers (ssh, pop, smtp, ftp, http) to identify the user who wants to establish a connection. This rule is designed to reject ident for security and performance reasons. Ident may allow an informational leakage, such as user information, objects, or processes considered private. The initial delays, sometimes quite substantial (up to a minute),

depending on specific default configurations may occur when the connection is initiated. It is often misinterpreted as "poor performance". This rule rejects the packet so that a RST is issued to quickly close the connection instead of waiting for a default timeout, thus greatly improving response.

Rule 3: Firewall lockdown rule

The lockdown rule is placed at the beginning of the rule base with the purpose of protecting the firewall itself. Placing it on top insures that regardless of what rules may be added later, the firewall is still protected. It ensures that the firewall isn't accidentally exposed to unauthorized users.

Rule 6: Allow access to the webserver for any source any destination

This rule allows both http and https access to the webserver from inside and outside our network. It is placed in the upper section of the rulebase due to the frequency that this traffic will occur.

For more details please check: "How to Eliminate the Ten Most Critical Internet Security Threats" http://www.sans.org/topten.htm

EMAIL ISSUES

The next four rules (7-10) should address the requirements for email system at GIAC Enterprises. For these rules, we have established network objects for the internal and external mail servers. To permit email without giving the Internet direct access to the corporate email server, a relay or "split horizon" approach (much more fancy term) should be used. The external mail server has no even slightest idea about actual user accounts and will merely function as a temporary store and forward device for the internal corporate mail server. It will calmly accept everything for "e-cookies.com" and forward it to the real mail server located on Internal Corporate Network.

What actually surprised me while reading other people Policy Implementation is that how many people do not really understand how mail is functioning and how MTAs (and SMTP as a common protocol in particular) work. Most of the students have no rules for email delivery to internal servers. Some students even try to permit outbound connections on 25/tcp from Internal to Service Network "to pick-up" the mail from relay!

It should be absolutely clear: any SMTP connections/exchanges will be always initiated by the sender, and not the recipient. Therefore we have to drill a hole in our firewall (as an exception to a common practice) from our Service Net to Internal Net. Although, the rule is pretty strict: host-to-host and only 25/tcp.

For ultimately paranoid types (could I be one of them?) who do not want ANY connection from the untrusted networks to protected internal ones I would suggest to implement UUCP (over IP) for mail exchange. It is very reliable and absolutely suitable for the purpose protocol, although "old-

fashioned" and already slightly forgotten. UUCP will permit you to pickup e-mail from your external relays (you will initiate the connection from inside).

Rule 7: Allow smtp traffic to the external mail relay

Smtp traffic is allowed from the Internet to external mailserver on the Service Network.

Additional Security Measures:
Make sure that VRFY and EXPN commans are disabled to prevent enumeration. Anti-spamming rules should be enforced on the mailserver, prohibiting third-parties relaying. Banner information may also be changed to make enumeration more difficult. Keep up to date all the patches and upgrades.

Rule 8: Allow outgoing smtp traffic to the Internet

Smtp traffic is allowed from the external mail server on the Service Network out to the Internet.

Rule 9: Allow smtp traffic from the external to the internal mail relays
Rule 10: Allow smtp traffic from the internal to the external mail relays

Smtp exchange is allowed between the internal and external mail servers.

Rule 11: Allow the external DNS server access to initiate name resolution for the hosts in the screened network.

The external DNS server is allowed to initiate name resolution for the screened network hosts. The server is not, however, allowed a connection to the corporate network. This DNS server should only have entries for publicly available servers. The rule is placed with the cluster of screened network rules.

Additional Measures:
There have been a large number of security related problems with BIND recently. BIND is number one on the SANS list of the ten most exploited security flaws. The basics to securing BIND include updating to the latest version and patch level; run bind as a non-privileged user or in a chroot-ed environment.

For more details check:
How to Eliminate the Ten Most Critical Internet Security Threats http://www.sans.org/topten.htm
Foiling DNS Attacks http://www.securityportal.com/cover/coverstory20001113.html

Rule 12: Allow Internet access to external DNS server for DNS lookups

This rule allows Internet access to the external DNS server. Access from the corporate network is denied; they will use the internal DNS server. This traffic will not be logged; otherwise the logs will fill up in a short time. The rule is placed in the cluster of rules that have sources including the Internet.

Rule 13: Allow internal and external smtp access to the mailserver

This rule allows internal and external smtp access to the mailserver. The rule is placed in the cluster of rules that have sources including the Internet.

Rule 14: Unlimited Internet access for the corporate network, excluding access to the screened network

This rule allows unlimited Internet access for corporate users, with the exception of denied access to the Service Network. It is an untrusted network, and no access will be allowed from the trusted network. This will prevent the users from accidentally bringing in something from the Service Network, which could be compromised by design.

Rule 15: Deny access from the screened network

In general the DMZ / Service Network should never initiate traffic to the Internal corporate network. Evidence of such traffic may suggest a compromise within the screened network. The only exception to this is the access allowed from the external mailserver to the internal one. Any other traffic should be considered suspicious. Alerting for this rule is turned on for quick notification. By the way: Lance Spitzner advise how to use this thing as a "free" honey-pot and it could be done quite successfully.

For more details check:
"Building Your Firewall Rulebase" http://www.enteract.com/~lspitz/rules.html

Rule 16: Deny everything else

Although Firewall-1 will drop all the packets that do not match any rule but by default the traffic will not be logged. This rule is finishing our rulebase in order to log all the events that are denied.

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.*

NOTE: Assignment 3 should be primarily focused on VISA requirement number 1, "Install and maintain a working network firewall to protect data accessible via the Internet." and your base + recommended security policy. Credit towards honors status will be given to students that are able to design an audit that can test all or a good deal of the VISA requirements.

3.1 Perimeter Penetration Testing and Firewall Audit

Perimeter penetration testing allows us to evaluate how security policy in organization is implemented and whether the actual security level is appropriate and sufficient for the organization.

For the purpose of this assignment we will provide you with a brief overview of common methodology used for such penetration testing and some of the possible issues which auditor may have.

It is also strongly recommended that the preparation stage mentioned below be carefully executed.

Preparation

Obtain management approval (or Client request) and prepare a test plan outlining the following important items:

- *Objectives of the Test:*
  a) the overall implementation of the security policy (report on weaknesses, errors);
  b) the effectiveness and sufficiency of firewall policy / rules;
  c) organizational effectiveness/response

- *Scope of Engagement*
  a) what will and especially what will not be tested: e.g., alternative network entry points or bypasses such as remote access (e.g.: modem attached to user's desktop PC);
  b) possible weaknesses in the firewall services / operating systems / configuration, logging levels and analysis;
  c) whether intrusion detection systems and policy exist and how effective these are? whether the network and system administrators notice an attempt or successful break-in

and how do they react?

- *Rules of Engagement (how far can we go):*
  a) whether the firewall operation may be disruptive, strength of attack and whether attacks should be attempted from both inside and outside;
  b) whether Denial of Services (DoS) attacks are allowed against perimeter security devices and/or protected by them servers (it is very unlikely though, on practice clients strongly avoid such an option, especially on "holy cow" - Production Network);
  c) whether social engineering tricks are allowed (this methods usually are underestimated. Although it could be really effective and is relatively easy to implement – just one call to the helpful IT support person: "Hi, it is the same John Smith again, Big VP of Something. I am really sorry but I forgot my SecurID card at home and I am on the road. Can you ple-e-ease set me with a fixed password just for 2 days only? I promise I will never forget it again… Thank you VERY MUCH!");
  d) whether the IT personnel and firewall/network administrators should be informed about perimeter testing in advance (this is important decision that requires management approval);
  e) whether the source code should be examined (it is labor intensive process and could be really expensive);
  f) whether physical security of the premises and equipment (routers, firewalls, servers, switches, wiring, etc.) will be examined

- *Project plan with deadlines, costs, description of deliverable (report) and responsibilities.*

Now, get this plan signed along with permission to start the test on a particular day.

Legal Issues

Do not forget to obtain an official letter on Company letterhead signed by Senior Executive / VP and stating that such and such will be engaged in authorized security audit of Company systems and networks on a particular date. It should also have the emergency contacts listed if this statement will need to be verified.

Such a letter may get you out of trouble with Law Enforcement if by any chance the ISP or some zealous and uninitiated junior sysadmins will notice your "malicious" activities and will report on you directly to LE.

Phases of Engagement

Phase 1: Indirect information collection or Footprint Analysis

At this stage, no perimeter protection device is approached, so no attack attempt can be detected.

- Use all available and publicly accessible informational sources: DNS (e.g. nslookup/dig, whois, ARIN) to see what information is published about the network, try to map it.
- Search public archives for postings from employees of this domain (different network/OS/security related newsgroups, mail-lists archives etc.).
- Examine the target's Internet WWW, ftp servers for possible informational leakage. Examine sites that may provide information about the company (e.g. SEC).

Phase 2: Direct information collection

Now the firewall/network administrators may detect us, but no disruption to services should occur.

- Check email gateway what software it is running and what particular version. Try to interrogate loosely configured systems for users enumeration.
- Check DNS server for version of the software and attempt to get all the dns information it can provide.
- Check webservers what software they are running and what particular version.
- Check bounced email headers (send email to non-existent users), to see if the internal machines names/structure will be provided.
- Scan address space for additional available hosts (do it gently, i.e. with ping or better yet with "nmap –sP")
- then perform a stealth scan to enumerate available ports/services, i.e. use a tool which can provide TCP FIN and SYN scan capabilities, e.g. nmap.
- at this stage you can attempt to perform IP stack fingerprinting to identify what platforms/OS those services are running on (there are several tools out there, nmap is on of them).
- If this is defined in Scope of Engagement you will need to scan phone lines for modems (e.g. with ToneLoc, PhoneSweep or THC)

Phase 3: General attack from outside

The steps from here on in can make a lot of noise and trigger a lot of alarms...

- Check for obvious, primitive and easy to attack holes first, e.g.: "showmount –e", rpcinfo, NT/Win95 Shares, etc.
- Vulnerabilities scanners (tools like ISS/Sara/Nessus) will most probably trigger the alarms on the firewall/NIDS and warn the administrators.
- If there are obvious holes at this stage and the holes allow access to machines inside the firewall, then you may skip the advanced techniques.

Phase 4: Advanced techniques from outside

At this phase the firewall configuration needs to be understood to launch an attack on particular services that are available.

- webserver attack: try to exploit common webserver vulnerabilities (use the information obtained on previous phases: OS/platform and type/version of the webserver; it is silly to run IIS exploit against Apache webserver; and the shell-code for SPARC would not work on x86 platform and so on).
- DNS server attack: check and test for bind vulnerabilities.
- Blind IP spoofing: try to spoof the firewall into believing to are an internal host (which is trusted by the firewall), possibly while blocking the internal host with a SYN flood attack. This will not work if the firewall has a filter that rejects packets from the outside that contain "from" addresses from internal hosts.
- If any server on protected network can be compromised you can try non-blind IP spoofing in order to exploit some additional trusts (e.g.: in most of network designs the external mailserver is allowed to talk to internal one and so on).
- If a simple packet filter is used to allow incoming connection according to port number, then the source of telnet can be modified to come from another port and possible be allowed to connect because it is coming from an allowed port (typical example will be the use of 53/tcp: old implementations assumed that clients make DNS requests and if anything is coming with a source port 53 it is a response from DNS servers and will be allowed to go trough).
- Source routing: Most border routers and firewalls will discard source routed packets, but it can be tried anyway.
- The high port numbers on Cisco routers can be tried.

Phase 5: Attack from the inside

Basically all of the methods in Phases 3 and 4 are possible, but they are much easier, since the trust of the internal network is generally much higher. This will check the firewall inbound and outbound rules between all of these network segments. This audit may reveal the presence of active ports or services which should not be running which could also indicate the presence of trojan horses.

Phase 6: Firewall configuration review

Now the auditor comes onsite and completes an on-site audit of the firewall and the network connections.

Organizational procedures review:

- How are changes made, alerts raised and handled? Does an incident response procedure/policy exist?
- How many people are responsible? Is responsibility clearly defined?
- Is Policy clear and correctly implemented? Who defines policy?
- Are inter-network connection audited? How often? Does a general policy for inter-network connection exist? How is it enforced?
- If new networks are connected, is the security reviewed on the other side? Is the connection justified business-wise? Who approves connections? Who controls routers and VPNs?

- How many people are allowed to configure (have passwords) interface routers, firewalls and VPN boxes?

Technical review:

- Using the knowledge of what exactly the perimeter protection consists of, one can use experience and expert knowledge to analyze what additional weaknesses to those discovered in the previous stages may exist.
- Checking of all network access points, protocols
- Network device checking: hardware and software (OS network services, network applications)
- Host checking: OS, applications, hidden files, open/changed/modified files (use checksums/cryptographic hashes, e.g. Tripwire), unusual SUID/SGID files, world/group writeable files/directories, hidden/unknown processes, installed compilers/debuggers, logins from unknown hosts or at invalid or unusual times, etc., etc.
- Network vulnerability checking: remote access points, weaknesses, check for strange packets (incomplete, invalid addresses, source routed etc.)

Report findings

List findings ordered by risk level and propose the corrective action (if required).

3.2 Some practical steps, suggestions and considerations on how to perform a security audit

Internet footprinting.

The purpose of network footprint analysis is to identify all the pieces of information and technologies related to GIAC Enterprises network presence: domain names; network blocks; specific IP addresses of systems reachable via the Internet; TCP/UDP services running on each system identified; Operating Systems and underlying architecture (e.g.: NT vs. Linux; SPARC vs. x86, etc.); access control mechanisms and related ACLs; intrusion detection systems (IDS); system enumeration (usernames, group names, system banners, routing tables, SNMP information, etc.) .

If GIAC Enterprises is publicly traded company we can start our initial reconnaissance with queries to Securities and Exchange Commission (SEC) EDGAR database at http://www.sec.gov . We all know that the biggest problem organizations have is managing and integrating their Internet connections, especially when they are in the process of active mergers and acquisitions (which is a crazy "standard" these days). The easiest target for a perimeter penetration usually would be newly acquired small company which has poor/obsolete infrastructure and had no recent security audit but was swiftly "integrated" with. While we are at EDGAR we will also check for "maiden" names of acquired entities - this information will be very useful to "pin-point" all the networks what belong to GIAC.

Next step would be the WHOIS database at whois.networksolutions.com what will give us the complete information about registrant or will tell us who is their registrar and who can provide us with an information required. The output should look something like this:

```
linux# whois e-cookies.com@whois.networksolutions

or

solaris# whois -h whois.networksolutions e-cookies.com

Registrant:
         GIAC Enterprises Ltd. (E-COOKIES-DOM)
            12300 N.First Street
            San Jose, CA 12345
            US

            Domain Name: E-COOKIES.COM

            Administrative Contact, Technical Contact, Billing Contact:
               Smith, John  (JS1111)  jsmith@E-COOKIES.COM
               Giac Enterprises Ltd.
               12300 N.First Street
            San Jose, CA 12345
            US

               408-555-5555 (FAX) 408-555-5555

            Record last updated on 01-Jan-1998.
            Record expires on 01-Jan-2001.
            Record created on 01-Jan-1998.
```

```
Database last updated on 29-Nov-2000 10:24:05 EST.

Domain servers in listed order:

NS.E-COOKIES.COM        123.45.67.4
DNS.ISP.NET             123.45.89.2
```

Next step will be DNS interrogation and to simplify it we will attempt to transfer the whole zone file from GIAC authoritative server. The practice shows that these days a lot of companies prohibit zone transfers to unauthorized parties at their servers but the secondary servers at ISPs almost always will nicely provide you with such a possibility. Then if you are lucky the results will look similar to this:

```
linux# dig @ns2.isp.net e-cookies.com axfr

; <<>> DiG 2.0 <<>> @ns2.isp.net e-cookies.com axfr
;; QUESTIONS:
;;      e-cookies.com, type = AXFR, class = IN

e-cookies.com.  3600    SOA     ns1.e-cookies.com.  hostmaster.ns1.e-
cookies.com. (
                        2000122701      ;serial
                        3600    ;refresh
                        1200    ;retry
                        3456000 ;expire
                        3600 )  ;minim

e-cookies.com.  3600    NS      ns1.e-cookies.com.
e-cookies.com.  3600    NS      ns2.isp.net.
e-cookies.com.  3600    MX      20 relay2.isp.com.
e-cookies.com.  3600    MX      40 relay1.isp.com.
e-cookies.com.  3600    MX      10 smtp.e-cookies.com.
e-cookies.com.  3600    A       123.45.67.2
smtp.e-cookies.com.     3600    A       123.45.67.3
pop.e-cookies.com.      3600    A       123.45.67.4
www.e-cookies.com.      3600    A       123.45.67.5
gateway.e-cookies.com.  3600    A       123.45.67.6
vpn.e-cookies.com.      3600    A       123.45.67.7
db1.e-cookies.com.      3600    A       123.45.67.8
```

We can continue with traceroute to determine the route packets take between our auditing host and some GIAC Enterprises addresses. The actual trace might look similar to this:

```
linux# traceroute ns1.e-cookies.com
 1  testhost.someisp.net (100.100.100.100)  2.285 ms  2.234 ms  2.303 ms
 2  gw.someisp.net (101.101.101.1)  7.743 ms  4.929 ms  4.871 ms
 3  ge-2-0.a05.mtvwca01.us.ra.verio.net (129.250.122.193)  4.888 ms  5.058 ms  5.414 ms
 4  p4-0-0.a03.plalca01.us.ra.verio.net (129.250.122.69)  6.068 ms  5.745 ms  5.734 ms
 5  ge-6-0.r05.plalca01.us.bb.verio.net (129.250.29.62)  5.867 ms  5.766 ms  5.757 ms
 6  ibr02-p0-0.sntc04.exodus.net (209.185.9.29)  6.974 ms  6.982 ms  7.052 ms
 7  bbr01-g3-0.sntc04.exodus.net (216.34.2.19)  7.063 ms  7.020 ms  7.200 ms
 8  bbr01-p0-0.sntc05.exodus.net (209.1.169.138)  7.149 ms  7.090 ms  7.041 ms
 9  gw.isp.net (123.45.89.1) 7.246 ms  7.123 ms  7.137 ms
10  ns1.e-cookies.com (123.45.67.3) 7.546 ms  7.323 ms  7.337 ms
```

The port scanning will help us to determine which ports and services are active from the internet on the GIAC Enterprises internet address space. The tool of choice will be nmap by Fyodor (

www.insecure.org/nmap) - the most comprehensive and versatile scanning tool available (there is also a version for windows at www.eeye.com).

The sample of nmap output:

```
linux# nmap -sS -P0 -O 10.1.1.2

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on somehost.somecompany.com (10.1.1.2):
(The 1511 ports scanned but not shown below are in state: closed)
Port       State       Service
7/tcp      open        echo
9/tcp      open        discard
21/tcp     open        ftp
22/tcp     open        ssh
23/tcp     open        telnet
25/tcp     open        smtp
53/tcp     open        domain
79/tcp     open        finger
80/tcp     open        http
143/tcp    open        imap2
443/tcp    open        https
540/tcp    open        uucp

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=24307 (Worthy challenge)
Remote OS guesses: Solaris 2.6 - 2.7, Solaris 7

Nmap run completed -- 1 IP address (1 host up) scanned in 4 seconds
```

Please note that we've used fingerprinting capabilities to facilitate the identification of remote OS. In cases if NAT devices are used and different services/servers mapped the same external IP address such "fingerprinting" will be difficult or not possible at all. We would recommend different methods of OS identification, such as banners, services interrogation and specific their behavior.

Based on the security policy, we should expect to see the following ports to be detected:

Host	**Port**	**Service**
Web Server	80/tcp	http
Secure Web Server	443/tcp	https
SMTP Server	25/tcp	Smtp
Primary DNS Server	53/udp (53/tcp)	domain-udp (domain-tcp)

If you see something different it means that firewall rules and/or router filters do not reflect the current security policy and would need to be corrected.

Next step would be to check these active services for known vulnerabilities. Obviously, you can use any "of the shelf" commercial or free vulnerability scanners for this purpose (e.g.: ISS, Nessus, SARA, Retina, etc.) but to make it more educational and for the purpose of this assignment we will show you how to do it using just your bare hands (and may be few standard tools coming with virtually any unix or even NT system).

Web Server

To identify the version/platform of the webserver running (assuming that you already have some of information about underlying OS from previous fingerprinting) you just make a telnet connection to port 80.

```
telnet www.e-cookies.com 80
```

then type:

```
GET index.htl HTTP/1.0
```

and hit return twice. If webserver is up and running and there are no problems with networking connection you should expect to see something like this:

```
HTTP/1.1 400 Bad Request
Date: Tue, 29 Nov 2000 09:04:13 GMT
Server: Apache/1.3.14 (Unix) mod_ssl/2.7.1 OpenSSL/0.9.6
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>400 Bad Request</TITLE>
</HEAD><BODY>
<H1>Bad Request</H1>
Your browser sent a request that this server could not understand.<P>
Invalid URI in request GET index.htl HTTP/1.0<P>
<HR>
<ADDRESS>Apache/1.3.14 Server at www.e-cookies.com Port 80</ADDRESS>
</BODY></HTML>
Connection closed by foreign host.
```

In this particular example we've intentionally misspelled the URL to get much shorter response and less garbage from the server and not to raise a suspicion of webmasters with a strange request if they are by any chance checking those log files.

Now all we need is to check this particular version of webserver for any known vulnerabilities and if check is positive then we can run the exploit to gain an unauthorized access to the server (in those cases if gaining access / collecting trophies is required by our perimeter penetration plan).

Secure Web Server

There is a popular believe that using HTTPS only (e.g.: often implemented for a "secure" remote access to internal corporate mail systems) would make the webserver itself much more secure. I regret to disappoint those naïve people but I've done numerous field tests and have to admit that absolutely same methods, tools and exploits what could be used against plain HTTP server you can use against HTTPS enabled servers.

All we would need is to add an additional layer – encryption. Any ssl-aware proxy will do the job: sslproxy, stunnel, etc.

On your favorite unix box compile sslproxy and run it with the appropriate parameters/ports:

```
sslproxy –L <local address> -l <local port> -R <remote address of webserver we
are testing> -r <remote port, usually 443> -s –p <protocol: ssl2, ssl3, tls1>
```

Now you can proceed as usual and run things against you local proxy address/port. And if your webserver has any unpatched holes it will be hacked, and ironically enough it will be hacked "securely" via encrypted channel (as a side effect it will also defeat any Network IDS watching for known exploits/attacks on your webservers).

SMTP Server

Inappropriately configured smtp server can leak out important information. You can interrogate such server by simply making a telnet connection on port 25.

```
telnet smtp.e-cookies.com 25
```

then you should see something like this:

```
Trying 123.45.67.4...
Connected to smtp.e-cookies.com.
Escape character is '^]'.
220 smtp.e-cookies.com ESMTP Sendmail 8.9.3/8.9.3; Tue, 29 Nov 2000 01:50:50 -
0800 (PST)
```

If this information is sufficient for your test purposes you may simply close the connection and go check for known vulnerabilities/exploits for this particular version of smtp server (tip: do not go, this one is not vulnerable).

You may also want to interrogate mail server a little bit longer in order to get additional information on existing accounts (especially with administrative privileges, e.g. root), naming conventions, any misconfigurations (e.g.: allowing third-party relaying, a.k.a. SPAM), etc.

```
ehlo your.hostname.com

250-smtp.e-cookies.com Hello your.hostname.com [your_IP_address], pleased to
meet you
250-EXPN
250-VRFY
250-8BITMIME
250-SIZE
250-DSN
250-ONEX
250-ETRN
250-XUSR
250 HELP
```

```
expn root
250 Petr Ivanov <ivanov@e-cookies.com>
expn webmaster
250 John Smith <jsmith@isp.net>
expn postmaster
250 Tak Chen <tchen@e-cookies.com>
expn hostmaster
550 hostmaster… User unknown
```

now, when we already learned who is who at e-cookies.com we can check if SPAM is allowed:

```
mail from: spammer@spammer.net
250 Ok
rcpt to: whoever@other-company.com
554 < whoever@other-company.com >: Recipient address rejected: Relay access
denied
```

The mail system does not allow foreign relaying. It is configured right. However, it does leak out the information on accounts. And this could be easily fixed by simply disabling commands like EXPN and VRFY.

Also, to make the life harder for those curious banner-grabbing types, you may want to change the banner to something neutral and anonymous like "Generic MTA" or may be "Who cares?"

DNS servers

The DNS is a really important part of the system. Should it fall victim into hands of an attacker, the DNS information could be altered to divert customers to attacker's sites, tricking them to give away passwords or credit card numbers. Therefore we have to check several things just to make sure everything is properly configured.

Zone Transfers

We want to check that our DNS servers do not permit zone transfers to unauthorized parties.

The convenient tool I would suggest to use for this purpose could be "dig" (free, comes with the ISC BIND) or just your standard "nslookup". In case if you decided that the firewalls should be blocking port 53/tcp from everyone but our secondary DNS try first to perform this from outside then place your test machine on the same network segment as the DNS server and do it again.

```
linux# dig @ns1.e-cookies.com e-cookies.com axfr

; <<>> DiG 2.0 <<>> @ns2.isp.net e-cookies.com axfr
linux# dig @ns1.isp.net e-cookies.com axfr
; (1 server found)
;; Received 0 answers (0 records).
;; FROM: your_test_machine to SERVER: ns1.e-cookies.com
;; WHEN: Tue Nov 29 20:01:10 2000
```

You may want to repeat the command several times as sometimes the server could be busy and will not answer your request. If anyway you received no answers and zero records back, then DNS Server may be configured right and presumably would not permit the zone transfer to anyone else but to authorized addresses (to be absolutely sure you will need to check configs files and log files on that DNS server).

Also, as we've mentioned already there are those secondary DNS servers at ISP, and those usually will give you anything you ask them.

```
linux# dig @ns2.isp.net e-cookies.com axfr

; <<>> DiG 2.0 <<>> @ns2.isp.net e-cookies.com axfr
;; QUESTIONS:
;;      e-cookies.com, type = AXFR, class = IN

e-cookies.com.  3600    SOA     ns1.e-cookies.com.  hostmaster.ns1.e-
cookies.com. (
                        2000122701      ;serial
                        3600    ;refresh
                        1200    ;retry
                        3456000 ;expire
                        3600 )  ;minim

e-cookies.com.  3600    NS      ns1.e-cookies.com.
e-cookies.com.  3600    NS      ns2.isp.net.
e-cookies.com.  3600    MX      20 relay2.isp.com.
e-cookies.com.  3600    MX      40 relay1.isp.com.
e-cookies.com.  3600    MX      10 smtp.e-cookies.com.
e-cookies.com.  3600    A       123.45.67.2
smtp.e-cookies.com.     3600    A       123.45.67.3
pop.e-cookies.com.      3600    A       123.45.67.4
www.e-cookies.com.      3600    A       123.45.67.5
gateway.e-cookies.com.  3600    A       123.45.67.6
vpn.e-cookies.com.      3600    A       123.45.67.7
db1.e-cookies.com.      3600    A       123.45.67.8
```

To fix this you will need to contact the ISP and request them to prohibit zone transfers (could be difficult though).

Also, never keep any unnecessary records in your zone file – only absolutely required. Do not assign informative names to machines (e.g.: sun10, firewall, ssh-gateway), do not use HINFO fields, etc.

Version of DNS Server

Since bind is well known for numerous vulnerabilities leading to root access we should be really interested in what version of bind (or other DNS software) our server is running. Again, we can use "dig" for the purpose. And command line would look neat and simple:

```
linux# dig -t txt -c chaos VERSION.BIND @ns1.e-cookies.com
```

or we can use more common tool available on any platform – nslookup.

```
linux# nslookup
Default Server: localhost
Address: 127.0.0.1

server ns1.e-cookies.com
Default Server: ns1.e-cookies.com
Address: 123.45.67.4

> set q=txt
> set class=chaos
> version.bind
Server:  ns1.e-cookies.com
Address:  123.45.67.4

VERSION.BIND    text = "8.2.2-P5"
```

The DNS Server claims it is running BIND version 8.2.2-P5 (patch level 5). This should be checked by login on that machine or contacting system or network admin responsible for dns servers since this information could be easily spoofed, although the probability of this is low. The latest version is 8.2.2-P7 and we would strongly recommend the upgrade to the latest. It is also advisable to change the version field in "named.conf" to something neutral and anonymous, giving the potential attackers a harder time to figure out what system it is.

Recursive queries

There is perhaps one more thing we want to check: whether recursive queries are allowed. If so then there is a probability of DNS cache poisoning, and furthermore, there is no really good reason why your primary DNS server should serve for something or somebody else. Once again, we can use "nslookup"

```
linux# nslookup
Default Server: localhost
Address: 127.0.0.1

server ns1.e-cookies.com
Default Server: ns1.e-cookies.com
Address: 123.45.67.4


> www.yahoo.com
Server:  ns1.e-cookies.com
Address:  123.45.67.4

Name:    www.yahoo.com
Served by:
- M.ROOT-SERVERS.NET
          202.12.27.33
```

```
- I.ROOT-SERVERS.NET
          192.36.148.17

- E.ROOT-SERVERS.NET
          192.203.230.10

- D.ROOT-SERVERS.NET
          128.8.10.90

- A.ROOT-SERVERS.NET
          198.41.0.4

- H.ROOT-SERVERS.NET
          128.63.2.53

- C.ROOT-SERVERS.NET
          192.33.4.12

- G.ROOT-SERVERS.NET
          192.112.36.4

- F.ROOT-SERVERS.NET
          192.5.5.241

- B.ROOT-SERVERS.NET
          128.9.0.107
```

If you get an answer like above that means that DNS server does not allow recursion, otherwise you would receive an address you requested.

Some DNS Implementation suggestions

Never put internal addresses on external DNS. Implement "split DNS": internal DNS server serves only for internal machines and users. An external one provides an information on your domain to customers. Better yet, implement "split–split DNS". In this case you will have to have two DNS servers on the Service Net. The first one will serve as a primary authoritative name server for our domain and will not provide recursive queries at all (although it is just an issue of giving away some of your CPU cycles and is not really required: it is not possible to poison zones for which the server is authoritative). It will be used ONLY for external customers. The second server will not be accessible from any place but Service Network and will serve (with recursive queries) for the servers on Service Network.

3.3 Perimeter Analysis and Recommendations

And for the purpose of this last assignment we will consider that an audit did not find any design flaws or implementation errors in GIAC Perimeter Design.

* * * * * * * * * * * * * * * * * * *

Although, to tell you the truth… the whole this last sub-chapter of Assignment #3 does not really serve the purpose: if you are the author of the Security Network Design and corresponding Policy Implementation (Assignments #1 and #2 respectively) then all of your "analysis" and "recommendations" will be nothing but… cheating!

You will completely "unintentionally" omit some serious and important parts and details in your initial network design just to be able to make some "smart" suggestions and recommendations to "improve" the design later (should I remove the whole my NIDS network in Chapter 1 and then "recommend" it here, in this Chapter? Will it look as a significant improvement?).

You will also absolutely "inadvertently" forget to close some of known holes or leave vulnerable versions of the software - just to "discover" those surprisingly enough and eagerly "patch" them in this very Chapter (by the way, it seems that I did it already! I've used a previous "stable" version of bind in one of my examples several pages back, although it was a real (not updated) machine on one of my internal networks, but nevertheless…)

So, instead of doing this sort of "Potemkin's village" / "dog-and-pony-show" I would suggest to improve and modify the practical assignment for this track itself.

The easiest way could be to split the whole work in half: Assignment #1 and #2 will go first. Then the student would receive one of the several standard "pre-built" security designs from SANS for an analysis and recommendations on improvement . And that will be Assignment #3.

The alternative and perhaps more fun solution could be to exchange the security design proposals between students for cross-evaluation and analysis. But from organizational point of view it could also be more difficult to manage.

References

Brenton, Chris, Introduction to VPNs, SANS Security 2000, Monterey CA

Brenton, Chris, VPNs and Remote Access, SANS Security 2000, Monterey CA

Brenton, Chris, Network Design and Performance, SANS Security 2000, Monterey CA

Haeni, Reto, Firewall Penetration Testing, http://www.seas.gwu.edu/~reto/firewall/

Mcclure, Scambray & Kurtz, Hacking Exposed: Network Security and Solutions, Osborne/McGraw-Hill

Northcutt, Stephen, TCP/IP for Intrusion Detection and Firewalls, SANS Security 2000, Monterey CA

Stevens, W. Richard, TCP/IP Illustrated, Volume 1, Addison-Wesley Publishing

Spitzner, Lance, Advanced Perimeter Protection and Defense In-Depth, SANS Security 2000, Monterey CA

Spitzner, Lance, Firewalls 101: Perimeter Protection with Firewalls, SANS Security 2000, Monterey CA

Spitzner, Lance, Auditing Your Firewall Setup, http://www.enteract.com/~lspitz/audit.html