Global Information Assurance Certification Paper

Author: Frank Meylan

Date: 11/18/00

Firewall and Perimeter Protection

Assignment #1: Security Architecture

Introduction

With the objective of assisting the security requirements of a new Internet Startup that expects to earn through the electronic commerce about 200 million dollars per year, it is presented and commented the diagram of Figure 1.

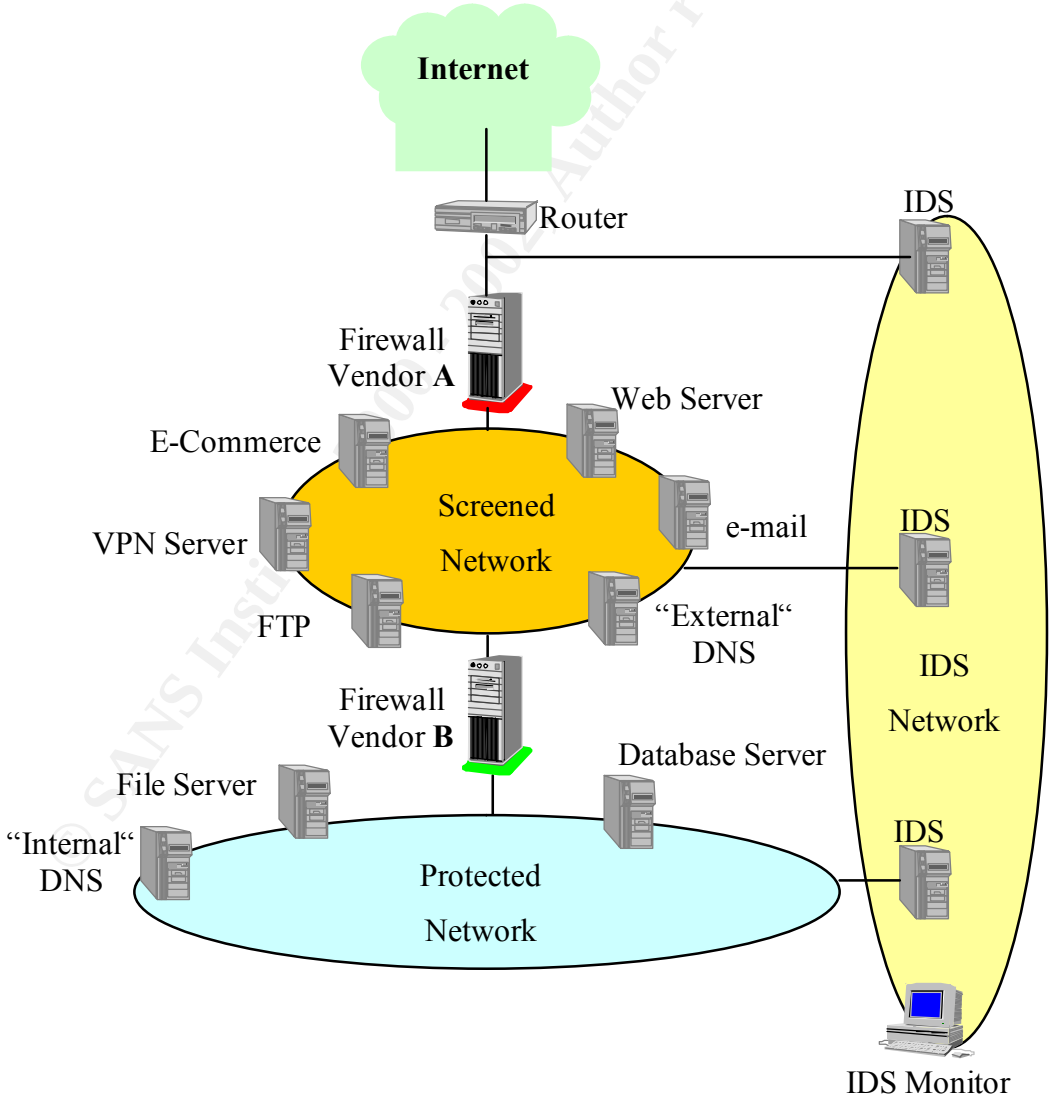
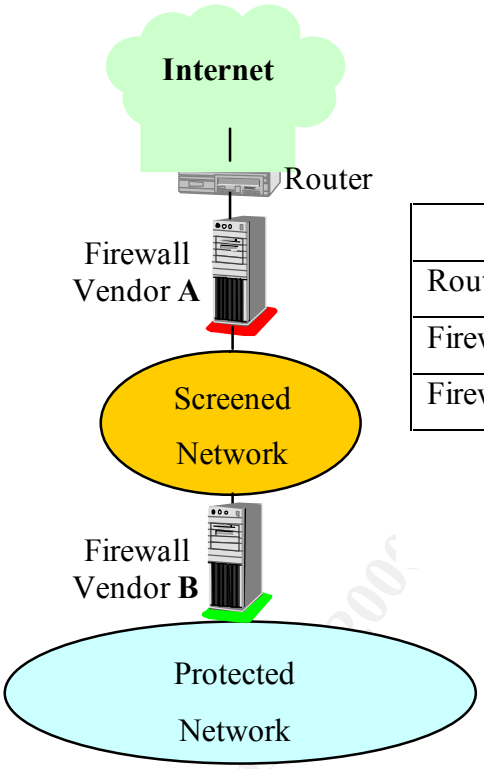


Figure 1 – Security Architecture Diagram

Firewall Infrastructure

As it can be observed in Figure 2, two firewalls compose the security system of the company. This way, two independent sub-networks were created:

- Screened Network: or service network, destined to host servers that provide services for Internet;
- Protected Network: hosts only internal servers and workstations.



Sample Configuration	
Router	Cisco 7000
Firewall Vendor **A**	Checkpoint Firewall -1
Firewall Vendor **B**	NAI Gauntlet

Figure 2 – Firewall Infrastructure

It is recommended to use firewalls from to different suppliers, so in case of a specific vulnerability discovery that commits the safety of certain firewall, the "Protected Network" remains safe.

The two firewalls should be configured to just allow external access to certain servers and specifically for the provided services. Depending on the requested service a user's authentication mechanism should be required to restrict access. For the accesses coming from the "Protected Network", the firewalls will be configured according to the company Security Policy.

Besides the use of the firewalls, the configuration of filters is also specified in the Internet access router. The router filters will reduce the possibility to overload the firewall when through DDoS attacks and will block the entrance of badly formed packets (IP fragmentation, source route, etc.).

All communication that goes through the firewalls and through the router should be logged to allow subsequent audit.

Immediately after the installation of the firewalls, router and servers, the default passwords should be changed. All passwords should be changed periodically according to the security policy of the company.

Commandment	Status
1. Install and maintain a working network firewall to protect data accessible via the Internet.	✓
9. Don't use vendor-supplied defaults for system passwords and other security parameters.	✓

Security Systems Maintenance

With the security system running and the administrators' network team well trained, the company should implement a periodic verification of the new updatings lists of security systems. This policy intends to maintain the security systems updated and the team in constant contact with the suppliers.

Commandment	Status
2. Keep security patches up-to-date.	✓

Proxy Firewall

The firewalls should be configured to act as proxies (application firewall) for certain services. Specifically in the cases of the e-mail, ftp and HTTP, the firewalls should verify the content of the transmissions trying to identify and block virus, trojans, or malicious JAVA/JavaScript code [SANS2.2].

This technique together with virus detection programs installed in servers and workstations will minimize the possibility of virus dissemination over the corporate network.

Commandment	Status
5. Use and regularly update anti-virus software.	✓

VPN's Configuration

The communication between the company and commercial partners should be made through the configuration of VPN's (Virtual Private Network) [Doraswamy1999]. VPN's will allow the mutual authentication between the participants and the secure information exchange through Internet, once the content of the communication is encrypted.

As this project is destined to a company that expects high amount of transactions through VPN's, it is recommended the use of a hardware VPN's server instead of a software one. Software VPN's cannot handle a large number of simultaneous VPN's with the expected performance.

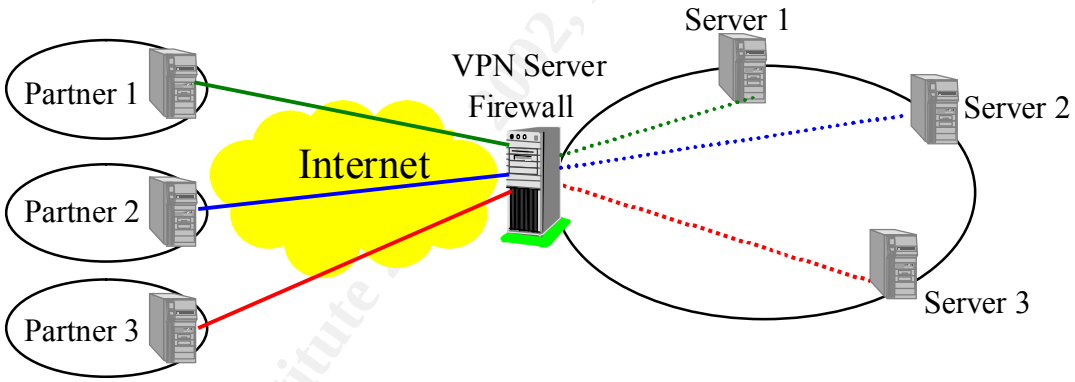


Figure 3 – VPN Configuration: specific servers for specific partners

As VPN's connections will be unique for each commercial partner, it is recommended to define dedicated servers for each connection, disallowing resources sharing among different companies. This way, the rule 6 "Restrict access to data by business "need to know" " is assisted. The Figure 3 illustrates a possible example of VPN's configuration among commercial partners.

Commandment	Status
4. Encrypt data sent across networks.	✓
6. Restrict access to data by business "need to know"	✓

Intrusion Detection System (IDS)

Firewalls don't guarantee completely the security of the network. This way, it is necessary to introduce in the network systems that can detect possible intrusion attempts.

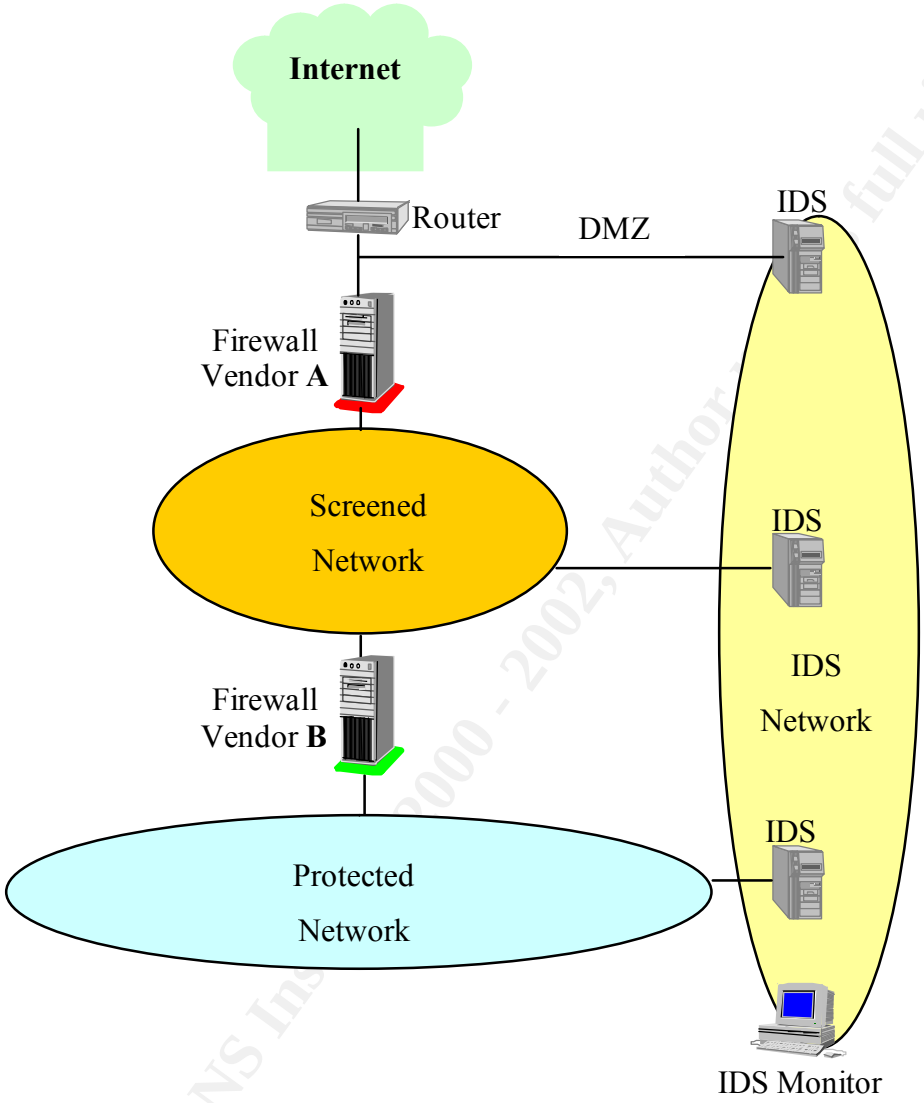


Figure 4 – IDS Architecture

According to Figure 4, IDS [Northcutt2000] will monitor three different points of the network with the following objectives:

Network	Monitoring Objective
DMZ	Identify and alarm scanning and attack preparation
Screened Network	Identify and block intrusions well succeeded
Protected Network	Identify users' suspicious actions or communication not allowed

It is interesting to notice that the communication between the IDS agents and the monitoring workstation is made through a dedicated network.

Besides continually monitor the network, IDS can be used to aid in the verification of the router filters and firewalls security policy. It is recommended to run periodically vulnerabilities evaluation tools like ISS, nmap, nessus, etc. from several points of the network intending to certify the policy adopted in each security equipments and to verify on each test if IDS was capable to recognize the attack attempt. Figure 5 illustrates how IDS can aid the verification of security systems.

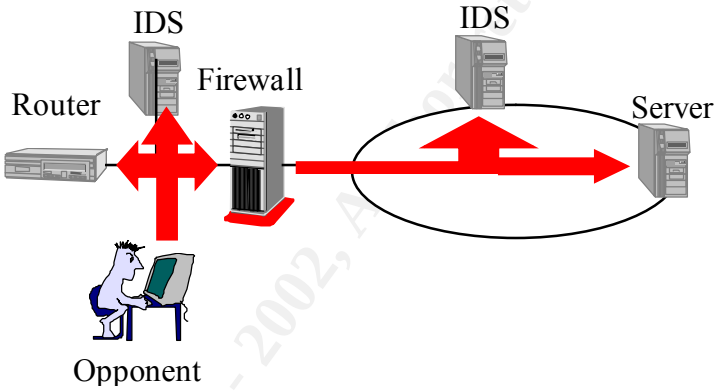


Figure 5 – IDS used to aid the test of security systems

Commandment	Status
10. Regularly test security systems and processes	✓

Some examples of IDS are:

- Snort (www.snort.org)
- RealSecure (www.iss.net)
- Shadow (www.nswc.navy.mil/ISSEC/CID)

Split DNS

The DNS were configured using the Split DNS scheme [SANS2.2]. This way, the company actually has at least two DNS servers:

- **External DNS:** List only what you want the world to see like Web, VPN, FTP servers.
- **Internal DNS:** Hold all internal server and host information.

This configuration will reduce the possibility for an opponent to obtain information about the internal hosts.

Complementary Systems

With network security systems proposed in this work, the following requirements could not be assisted:

Commandment	Status
3. Encrypt stored data accessible from the Internet.	X
7. Assign unique IDs to each person with computer access to data.	X
8. Track access to data by unique ID.	X

To implement these commandments it ‘s necessary additional security systems.

To encrypt the stored data on servers accessible from Internet, it is necessary to install a cryptography file system manager. Several commercial solutions implement this functionality. Among them are: Windows 2000 EFS, PGP Disk, etc.

The commandments 7 and 8 can be assisted using a centralized user authentication system in the network like Kerberos or NIS. LDAP also can be configured to implement this functionality.

Assignment 2: Security Policy

Introduction

This assignment consists in define an additional security policy to the recommendations proposed in *www.sans.org/topten.htm* to combat the top ten most frequent vulnerabilities. For the definition of the filters to be implemented in the firewalls, it is necessary to specify the addresses of the involved sub-nets. Figure 6 illustrates a possible configuration of sub-nets addresses.

For the proposed rules it will be used as example IPCHAINS [Mitchell2000] syntax on Linux.

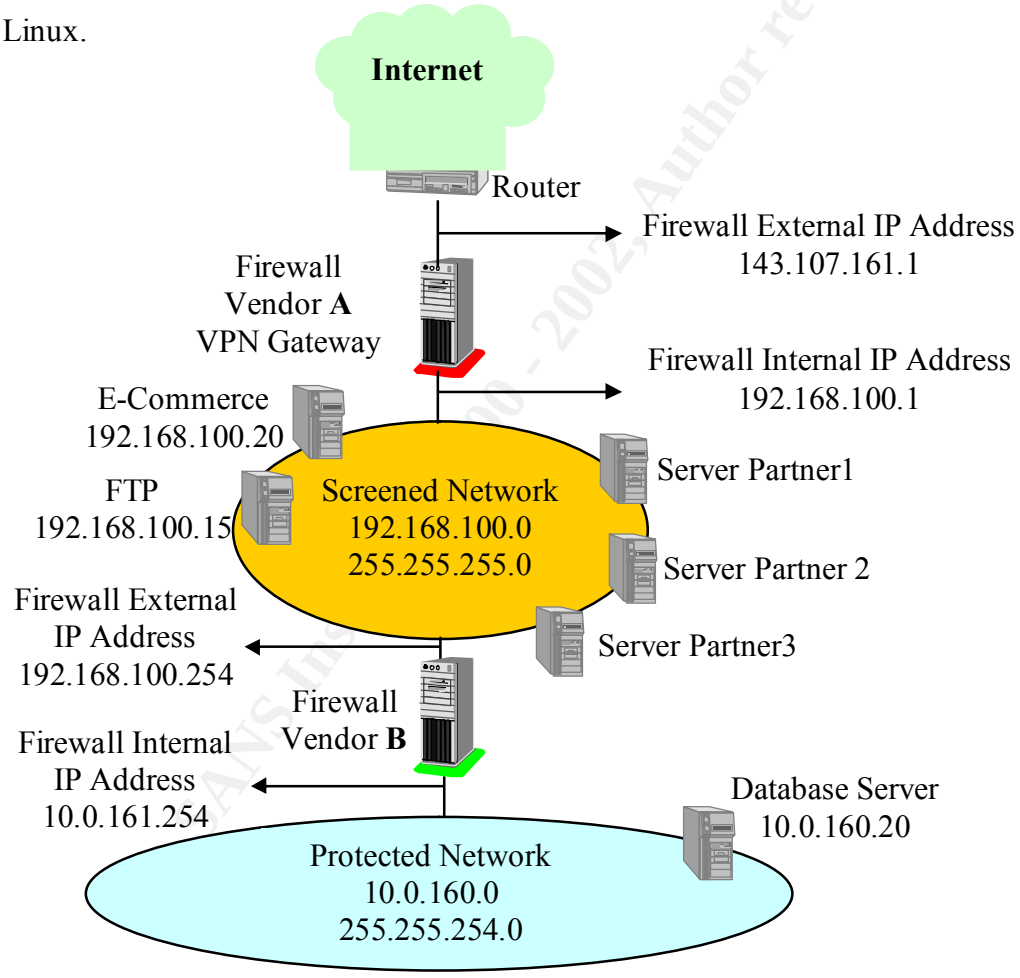


Figure 6 – Network addresses specification

For all configurations used in this work the default policies will be REJECT, implemented as showed:

#Default policies

ipchains -P input REJECT

ipchains -P output REJECT

ipchains -P forward REJECT

Additional Rules 1–Egress Filters

As discussed by [Anders2000], the implementation of egress filters blocks the use of the company network in a DdoS attack with spoofed source address. Therefore, the filter only allows the transmission of packets to the Internet with source address belonging to the company network address space.

To avoid the firewall overload, this rule will be implemented in the router. Even for the router the IPCHAINS syntax will be used.

ipchains -A output –i eth1 –s 143.107.161.0/24 –j ACCEPT

ipchains -A output -i eth1 –s 0.0.0.0/0 –j DENY

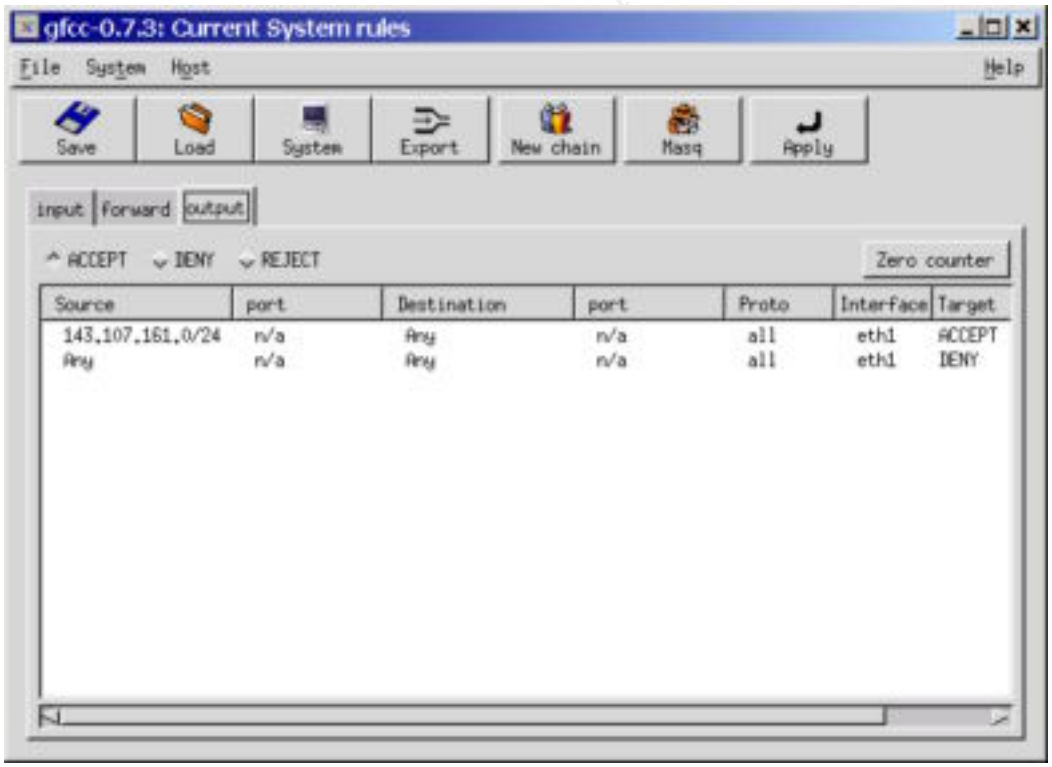


Figure 7 – GFCC configured with the egress filter

The first rule allows packets whose source address belongs to the sub-net 143.107.161.0 go out from router through the external interface “eth1”. The second rule discards all the

packets. Figure 7 illustrates the graphical interface of the GFCC, program used to verify the IPCHAINS configuration.

So, only packets with source address belonging to the company network address space will be routed to the Internet.

Additional Rule 2 - VPN Support

As part of the project elaborated in the assignment 1, it is foreseen VPN's support. So, it is necessary to configure "Firewall Vendor A" to allow the traffic of VPN packets.

Vulnerability: As VPN encapsulates other protocols, allowing VPN packets to enter in the network, will allow access to services blocked by the firewall. So the VPN Server configuration should restrict the access to a certain number of dedicated servers.

In this project it is being assumed that VPN will only be used for the transport of NetBios protocol, allowing connection with Windows NT servers. As all servers to each commercial partner are in the Screened Network, Firewall Vendor B should block the transmission of NetBios protocol, and Firewall Vendor A should only accept and transmit Netbios packets through internal interface "eth0", the encrypted tunnel entrance/exit.

Filter syntax implemented in "Firewall Vendor A"

#VPN (IPSEC) packets can enter and leave the Firewall only on external interface (eth1)
ipchains –A input –i eth1 –p 47 –s 0.0.0.0/0 –d 143.107.161.1/32 –l –j ACCEPT
ipchains –A output –i eth1 –p 47 –s 143.107.161.1/32 –d 0.0.0.0/0 135:139 –l –j ACCEPT

#NetBios packets can enter and leave the Firewall only on internal interface (eth0)
ipchains –A input –i eth0 –p tcp –s 0.0.0.0/0 –d 0.0.0.0/0 135:139 –l –j ACCEPT
ipchains –A output –i eth0 –p tcp –s 0.0.0.0/0 –d 0.0.0.0/0 135:139 –l –j ACCEPT
ipchains –A input –i eth0 –p udp –s 0.0.0.0/0 –d 0.0.0.0/0 135:139 –l –j ACCEPT
ipchains –A output –i eth0 –p udp –s 0.0.0.0/0 –d 0.0.0.0/0 135:139 –l –j ACCEPT

#NetBios packets can't enter or leave the Firewall on external interface (eth1)
ipchains –A input –i eth1 –p tcp –s 0.0.0.0/0 –d 0.0.0.0/0 135:139 –l –j DENY

ipchains –A output –i eth1 –p tcp –s 0.0.0.0/0 –d 0.0.0.0/0 135:139 –l –j DENY
ipchains –A input –i eth1 –p udp –s 0.0.0.0/0 –d 0.0.0.0/0 137:138 –l –j DENY
ipchains –A output –i eth1 –p udp –s 0.0.0.0/0 –d 0.0.0.0/0 137:138 –l –j DENY

Filter syntax implemented in "Firewall Vendor B"

NetBios packets are blocked
ipchains –A input –i eth0 –p tcp –s 0.0.0.0/0 –d 0.0.0.0/0 135:139 –l –j DENY
ipchains –A input –i eth1 –p tcp –s 0.0.0.0/0 –d 0.0.0.0/0 135:139 –l –j DENY
ipchains –A input –i eth0 –p udp –s 0.0.0.0/0 –d 0.0.0.0/0 137:138 –l –j DENY
ipchains –A input –i eth1 –p udp –s 0.0.0.0/0 –d 0.0.0.0/0 137:138 –l –j DENY

Additional Rule 3 – E-Commerce Server access Database Server

For the operation of the E-commerce server it is necessary to allow access to the database server. This is the only server in the Screened Network that needs this access, so any other requisition should be filtered. It is being assumed that the database server is Oracle and the connections to that server will use port 1521. The communication will happen following the steps:

1. E-commerce server sends the connection requisition to Firewall B (192.168.100.254) on port 1521
2. Firewall B forwards the requisition to Oracle server (10.0.160.20) using ipmasqadm port forward facility
3. Oracle server receives the request and responds to Firewall B (10.0.160.254)
4. Firewall B transmits the answer to E-commerce server using IP masquerading

"Firewall Vendor A"

rule for blocking inbound and outbound Oracle Database queries
ipchains –A input –i eth0 –p tcp –s 0.0.0.0/0 –d 0.0.0.0/0 1521 –l –j DENY
ipchains –A input –i eth1 –p tcp –s 0.0.0.0/0 –d 0.0.0.0/0 1521 –l –j DENY

"Firewall Vendor B"

#rule for port forwarding from Firewall B to Database Server on port 1521

ipmasqadm portfw -a -P tcp -L 192.168.100.254 1521 -R 10.0.160.20 1521

#rule for masquerading from Protected Network to outside

ipchains -A forward -s 10.0.160.0/255.255.254.0 -d 0.0.0.0/0.0.0.0 -i eth1 -j MASQ

rule for allow Oracle Database queries only from E-Commerce Server

ipchains –A input –i eth1 –p tcp –s 192.168.100.20/32 –d 192.168.100.254/32 1521 –j ACCEPT

ipchains –A output –i eth0 –p tcp –s 192.168.100.20/32 –d 10.0.160.20/32 1521 –l –j ACCEPT

ipchains –A input –i eth0 –p tcp –s 10.0.160.20/32 1521 –d 192.168.100.20/32 –l –j ACCEPT

ipchains –A output –i eth1 –p tcp –s 192.168.100.254/32 1521 –d 192.168.100.20/32 –l –j ACCEPT

rule for blocking inbound and outbound Oracle Database queries

ipchains –A input –i eth0 –p tcp –s 0.0.0.0/0 –d 0.0.0.0/0 1521 –l –j DENY

ipchains –A input –i eth1 –p tcp –s 0.0.0.0/0 –d 0.0.0.0/0 1521 –l –j DENY

Additional Rule 4 –FTP access from Internet

In this project it is being considered that the company needs the FTP server accessible from the Internet. To provide this service we must open the ports 20 and 21 only for the FTP server (192.168.100.15). A port forward for that server will be necessary also.

#Port Forward to FTP server on port 20 and 21

ipmasqadm portfw -a -P tcp -L 143.107.161.1 20 -R 192.168.100.15 20

ipmasqadm portfw -a -P tcp -L 143.107.161.1 21 -R 192.168.100.15 21

#rule for masquerading from Screened Network to outside

ipchains -A forward -s 192.168.100.0/255.255.255.0 -d 0.0.0.0/0.0.0.0 -i eth1 -j MASQ

rule for allow FTP connections from Internet

ipchains –A input –i eth1 –p tcp –s 0.0.0.0/0 –d 143.107.161.1/32 20 –j ACCEPT

ipchains –A output –i eth0 –p tcp –s 0.0.0.0/0 –d 192.168.100.15/32 20 –l –j ACCEPT

ipchains –A input –i eth0 –p tcp –s 192.168.100.15/32 20 –d 0.0.0.0/0 –l –j ACCEPT

ipchains –A output –i eth1 –p tcp –s 143.107.161.1/32 20 –d 0.0.0.0/0 –l –j ACCEPT

ipchains –A input –i eth1 –p tcp –s 0.0.0.0/0 –d 143.107.161.1/32 21 –j ACCEPT

ipchains –A output –i eth0 –p tcp –s 0.0.0.0/0 –d 192.168.100.15/32 21 –l –j ACCEPT

ipchains –A input –i eth0 –p tcp –s 192.168.100.15/32 20 –d 0.0.0.0/0 –l –j ACCEPT

ipchains –A output –i eth1 –p tcp –s 143.107.161.1/32 20 –d 0.0.0.0/0 –l –j ACCEPT

Additional Rule 5 – What internal users can do

The next rules will define what users can do from "Protected Network"

Web access (ports 80 and 443)

#Firewall B

#Port 80

ipchains -A input -i eth0 -p tcp -s 0.0.0.0 -d 0.0.0./0 80 –j ACCEPT

ipchains -A output -i eth1 -p tcp -s 192.168.100.254/32 1024:65535 -d 0.0.0.0/0 80 -j ACCEPT

ipchains -A input -i eth1 -p tcp -s 0.0.0.0/0 80 -d 192.168.100.254/32 1024:65535 -j ACCEPT ! -y

ipchains -A output -i eth0 -p tcp -s 0.0.0.0/0 80 -d 10.0.160.0/23 1024:65535 -j ACCEPT

#Port 443

ipchains -A input -i eth0 -p tcp -s 0.0.0.0 -d 0.0.0./0 443 –j ACCEPT

ipchains -A output -i eth1 -p tcp -s 192.168.100.254/32 1024:65535 -d 0.0.0.0/0 443 -j ACCEPT

ipchains -A input -i eth1 -p tcp -s 0.0.0.0/0 443 -d 192.168.100.254/32 1024:65535 -j ACCEPT ! -y

ipchains -A output -i eth0 -p tcp -s 0.0.0.0/0 443 -d 10.0.160.0/23 1024:65535 -j ACCEPT

#Firewall A

#port 80

ipchains -A input -i eth0 -p tcp -s 0.0.0.0 -d 0.0.0./0 80 –j ACCEPT

ipchains -A output -i eth1 -p tcp -s 143.107.161.1/32 1024:65535 -d 0.0.0.0/0 80 -j ACCEPT

ipchains -A input -i eth1 -p tcp -s 0.0.0.0/0 80 -d 143.107.161.1/32 1024:65535 -j ACCEPT ! -y

ipchains -A output -i eth0 -p tcp -s 0.0.0.0/0 80 -d 192.168.100.0/24 1024:65535 -j ACCEPT

#port 443

ipchains -A input -i eth0 -p tcp -s 0.0.0.0 -d 0.0.0./0 443 –j ACCEPT

ipchains -A output -i eth1 -p tcp -s 143.107.161.1/32 1024:65535 -d 0.0.0.0/0 443 -j ACCEPT

ipchains -A input -i eth1 -p tcp -s 0.0.0.0/0 443 -d 143.107.161.1/32 1024:65535 -j ACCEPT ! -y

ipchains -A output -i eth0 -p tcp -s 0.0.0.0/0 443 -d 192.168.100.0/24 1024:65535 -j ACCEPT

e-mail (SMTP + POP) IP: 192.168.100.16

Firewall A – already covered by topten

#Firewall B

#SMTP

ipchains -A input -i eth0 -p tcp -s 10.0.160.0/23 -d 192.168.100.16/32 25 -j ACCEPT

ipchains -A output -i eth1 -p tcp -s 192.168.100.254/32 -d 192.168.100.16/32 25 -j ACCEPT

ipchains -A input -i eth1 -p tcp -s 192.168.100.16/32 25 -d 192.168.100.254/32 -j ACCEPT

ipchains -A outut -i eth0 -p tcp -s 192.168.100.16/32 25 -d 10.0.160.0/23 -j ACCEPT

#POP

ipchains -A input -i eth0 -p tcp -s 10.0.160.0/23 -d 192.168.100.16/32 110 -j ACCEPT

ipchains -A output -i eth1 -p tcp -s 192.168.100.254/32 -d 192.168.100.16/32 110 -j ACCEPT

ipchains -A input -i eth1 -p tcp -s 192.168.100.16/32 110 -d 192.168.100.254/32 -j ACCEPT

ipchains -A outut -i eth0 -p tcp -s 192.168.100.16/32 110 -d 10.0.160.0/23 -j ACCEPT

Internal DNS (10.0.161.17)

#Firewall A

ipchains -A input -i eth0 -p udp -s 192.168.100.254/32 -d 0.0.0.0/0 53 -j ACCEPT

ipchains -A output -i eth1 -p udp -s 143.107.161.1/32 -d 0.0.0.0/0 53 -j ACCEPT

ipchains -A input -i eth1 -p udp -s 0.0.0.0/0 53 -d 143.107.161.1/32 -j ACCEPT

ipchains -A output -i eth0 -p udp -s 0.0.0.0/0 53 -d 192.168.100.254/32 -j ACCEPT

#Firewall B

ipchains -A input -i eth0 -p udp -s 10.0.161.17/32 -d 0.0.0.0/0 53 -j ACCEPT

ipchains -A output -i eth1 -p udp -s 192.168.100.254/32 -d 0.0.0.0/0 53 -j ACCEPT

ipchains -A input -i eth1 -p udp -s 0.0.0.0/0 53 -d 192.168.100.254/32 -j ACCEPT

ipchains -A output -i eth0 -p udp -s 0.0.0.0/0 53 -d 10.0.161.17/32 -j ACCEPT

Assignment 3: Audit your Security Architecture

Introduction

The installation of proposed security system doesn't guarantee that the network is completely safe. New vulnerabilidades of operating systems, services and even of firewalls are frequently discovered. So, the maintenance of the network security depends fundamentally of periodic audits of all the system components.

Two different types of evaluations will accomplish auditing the proposed security system:

- External Evaluation: executed from Internet. This evaluation intends to identify the company services available for Internet and the associated vulnerabilities.
- Internal Evaluation: executed in each internal sub-network of the company. This evaluation intends to verify the vulnerabilities in the internal servers and the method of resources utilization by the users (authentication, rights, logs, etc).

The audit execution costs should take into account the number of hours foreseen for the accomplishment of the work and the use of vulnerability analysis commercial tools. As minor is the amount of information given to the auditor, more time he will spend to obtain them, consequently the cost of the project will increase. However, giving a great amount of information, the auditor can achieve access to confidential information without a lot of effort, which an attacker would not get accomplishing the attack from the Internet without any information of the company. The conclusion is to supply the minimum possible of information to the auditor, however that allows the execution of the work in a reasonable period of time.

A vulnerability analysis of a company can be faced as an attack or preparation for an attack, so before the execution of any test, an authorization from the company allowing such evaluation is required. Such authorization should specify the schedule destined for the execution of the tests, the type of the tests that can be executed (port scanning, denial of service testes, password guessing, etc). A confidentiality term about the results obtained from the analysis is also recommended.

Evaluation Methodology

The evaluation methodology defines the steps taken to obtain and analyze the information about the security of computational systems. The methodology proposed can be used for the internal and external evaluation of a company.

1. **IP Addresses Verification. C**onsists in scanning all the sub-network addresses of the company. This scanning can be made through the use of the ICMP protocol or port verification in each specific address. As in this work it is being assumed that ICMP is being filtered in the router, for the external analysis, the port verification technique is recommended.
2. **O.S. (Operating Systems) Identification.** Once the active workstations and servers were mapped, the next step consists of O.S. identification. This information will be very important in the verification of specific vulnerabilities associated with a certain O.S. type and version.
3. **Services Available.** For each address identified in step 1, should be tried to map all the ports open for connection (in state LISTEN). The enumeration of these ports will aid in the discovery of the available services for each server or station.
4. **Identification of Vulnerabilities.** With the type and version of O.S installed in the stations and the respective available services, the auditor should focus on discovering the vulnerabilities. To do that he can use vulnerability analysis tool, or try to look for new vulnerabilities at security sites. Some important lists of vulnerabilidades are:
    - **SANS www.sans.org**
    - **CERT www.cert.org**
    - **Security Focus www.securityfocus.com**
    - **Insecure.Org www.insecure.org**
    - **NTSecurity www.ntsecurity.com**
    - **Windows IT Security www.ntsecurity.net**

Vulnerability Analysis Tools

The implementation of the previously described methodology depends on the use of network analysis tools. Nowadays several types of tools exist, some are of public domain and others are commercial. Among the commercial ones are:

- Internet Security Scanner (www.iss.net)
- HackerShield (www.bindview.com)
- CyberCop Scanner (www.nai.com)

Some public domain tools are:

- NMAP (www.insecure.org)
- Nessus (www.nessus.org)

The utilization of different tools is highly recommended in an evaluation, because the results can be complementary once the tools may implement each test in different way.
The commercial tools usually have a user friendly graphic interface and are easy to use. They also generate reports containing graphs, recommendations for correcting the problems found, etc. The public domain tools are distributed at no cost for acquisition or use, allowing small and medium companies to have access to this technology.
The use of network sniffers can also be quite useful in the identification and evaluation of the protocols that runs over the network. Some sniffers examples are:

- TCPDump (Unix)
- X-Ray (Windows)
- Ethereal (Linux)
- Sniffit (Linux)
- Iris (Windows)

Testes execution and Results Analysis

Following the previously specified methodology, NMAP and ISS were used for internal and external network evaluation, as shown in Figure 8.

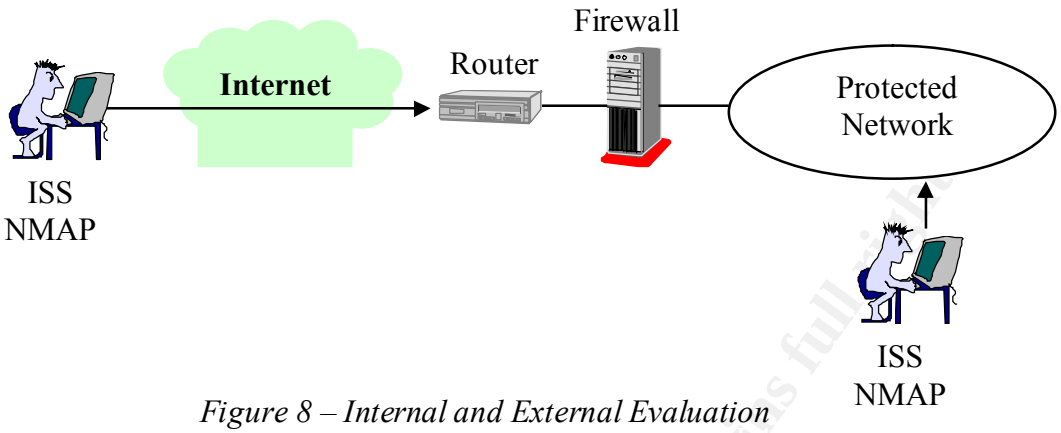


Figure 8 – Internal and External Evaluation

The external audit showed that only the services specified by security policy were available from Internet. This is due mostly by the fact that the internal sub-networks adopted private addresses scheme. The servers that provide services for the Internet are visible through the use of NAT (Network Address Translation) in the firewall. The firewall, however, showed efficient in blocking the NetBios protocol, as it can be seen below through Figure 9.

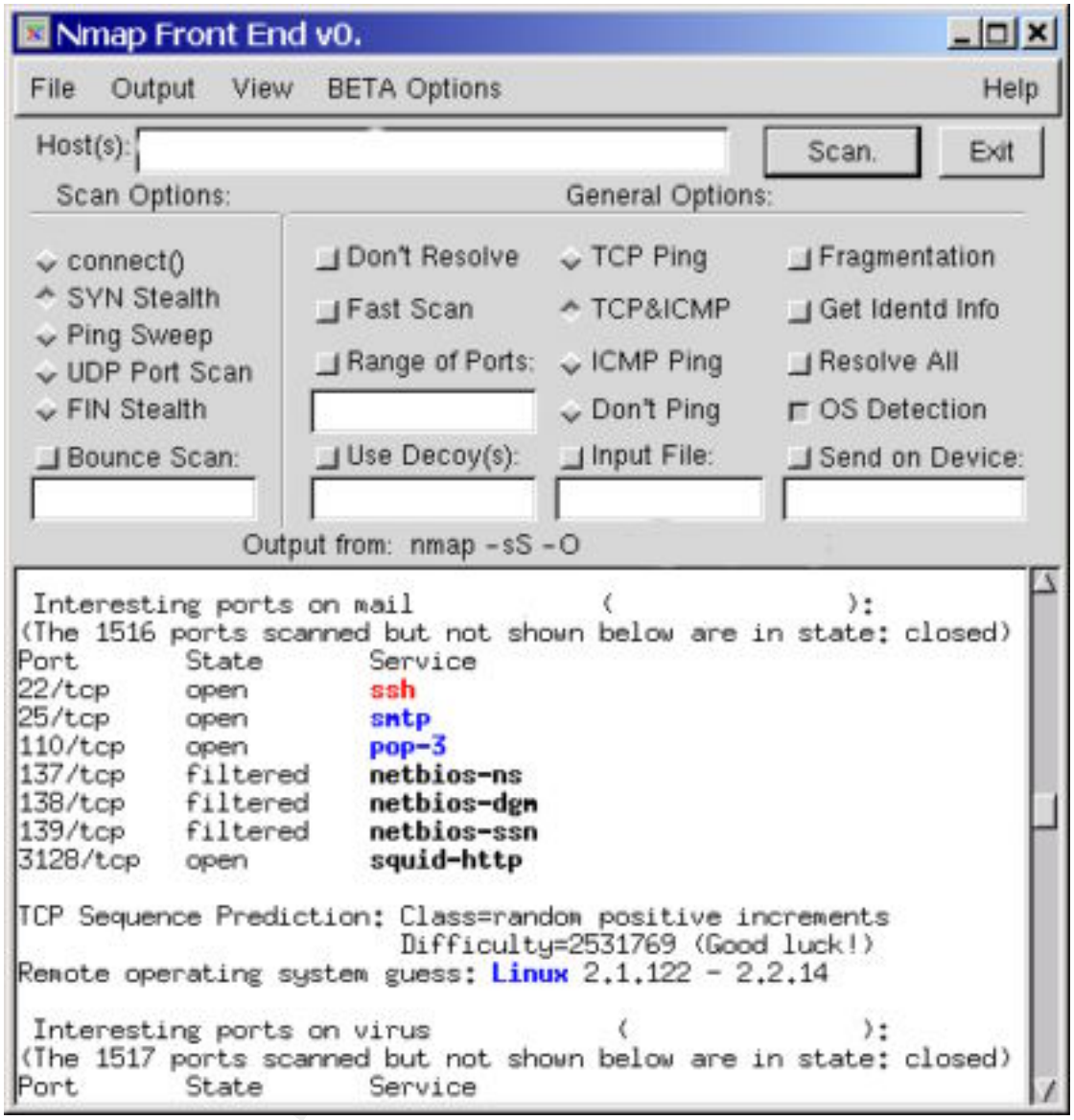


Figure 9 - External evaluation. NMAP output without ip addresses scanned

Observing the illustration above, it is noticed that external connections are allowed to the e-mail server through the POP protocol. As the POP protocol transmits passwords unencrypted, the substitution of this service by a Webmail with SSL (Secure Sockets Layer) is highly recommended.

The internal audit demonstrated several vulnerabilidades of high medium and low risks, according to the classification of ISS. Figure 10 illustrates ISS in operation during the scanning process of the internal network 10.0.161.0.

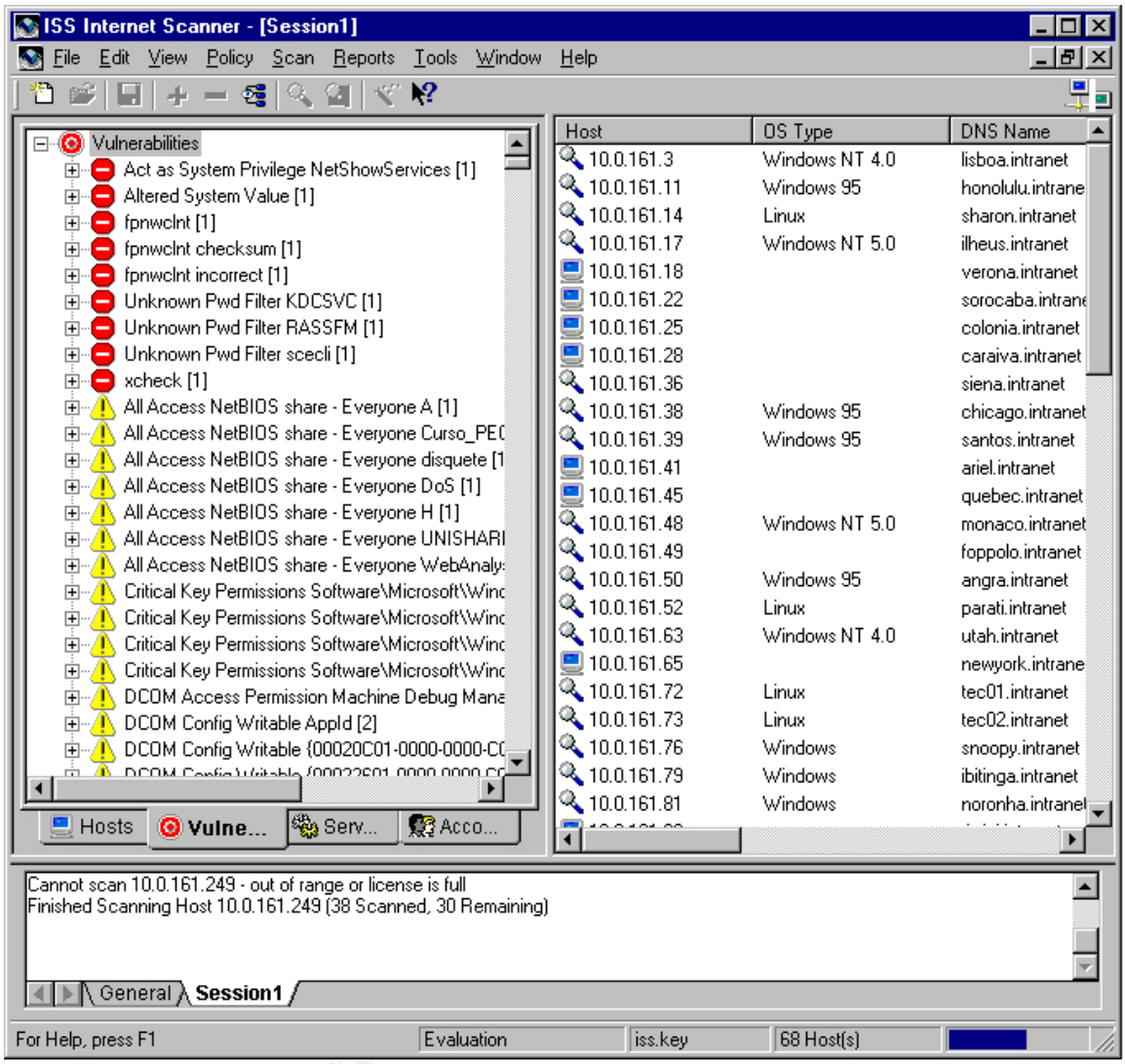


Figure 10 – ISS scanner auditing internal network

It is easy to notice that because of the vulnerabilidades found through ISS, the internal network would not implement the VISA "Ten Commandments". Some of the vulnerabilities found are:

- File or folder sharing open for all users
- Weak passwords
- Old or unpatched operating systems
- Unnecessary services available
- etc.

Besides the use of scanners, it was also used a sniffer (Tcpdump on a RedHat Linux) as evaluation tool. This test aimed to verify which protocols are used in the internal network. This test demonstrated the existence of the POP protocol used for the reception of e-mails. The vulnerability of the POP resides in the fact of transmitting the login and the user's password unencrypted. Figure 11 illustrates tcpdump in execution.

```
# tcpdump dst port 110
User level filter, protocol ALL, datagram packet socket
tcpdump: listening on all devices
10:49:45.477148 eth0 < luana.intranet.2822 > galaxy2.intranet.pop3: S 1525942367:1525942367(0) win
16384 <mss 1460,nop,nop,sackOK> (DF)
10:49:45.477971 eth0 < luana.intranet.2822 > galaxy2.intranet.pop3: . 1525942368:1525942368(0) ack
3093963980 win 17520 (DF)
10:49:45.507039 eth0 < luana.intranet.2822 > galaxy2.intranet.pop3: P 0:13(13) ack 41 win 17480 (DF)
10:49:45.519895 eth0 < luana.intranet.2822 > galaxy2.intranet.pop3: P 13:28(15) ack 47 win 17474 (DF)
10:49:45.544144 eth0 < luana.intranet.2822 > galaxy2.intranet.pop3: P 28:34(6) ack 53 win 17468 (DF)
10:49:45.548246 eth0 < luana.intranet.2822 > galaxy2.intranet.pop3: P 34:40(6) ack 62 win 17459 (DF)
10:49:45.550380 eth0 < luana.intranet.2822 > galaxy2.intranet.pop3: . 40:40(0) ack 69 win 17453 (DF)
10:49:45.552154 eth0 < luana.intranet.2822 > galaxy2.intranet.pop3: F 40:40(0) ack 69 win 17453 (DF)
10:49:47.937537 eth0 < ledzepp.spm.univ-rennes1.fr.1370 > galaxy2.intranet.pop3: P
14878120:14878126(6) ack 2643824873 win 8699 (DF)
10:49:48.773184 eth0 < ledzepp.spm.univ-rennes1.fr.1370 > galaxy2.intranet.pop3: . 6:6(0) ack 8 win 8693
(DF)
10:49:48.942751 eth0 < ledzepp.spm.univ-rennes1.fr.1370 > galaxy2.intranet.pop3: F 6:6(0) ack 8 win
8693 (DF)
```

Figure 11 – Tcpdump sniffing the internal network

For the evaluation of the **Egress Filter** recommended in assignment 2, it was used the program HPING2. This program permits the generation and transmission of packets according to the user's need. The test was accomplished generating packets with spoofed source address (1.2.3.4) and transmitting to some address on Internet (DEST_IP). The HPING2 syntax used was:

 # hping2 DEST_IP -a 1.2.3.4

The analysis of the Firewall A log presented below demonstrates that Egress Filter acted accordingly to the expected.

```
Nov 22 00:55:16 gateway kernel: Packet log: output DENY eth1 PROTO=6 1.2.3.4:1777
    DEST_IP:0 L=40 S=0x00 I=1220 F=0x0000 T=64 (#2)
Nov 22 00:55:37 gateway kernel: Packet log: output DENY eth1 PROTO=6 1.2.3.4:1785
    DEST_IP:0 L=40 S=0x00 I=9265 F=0x0000 T=64 (#2)
```

Figure 12 – Log containing Egress Filter execution

Conclusions and Recommendations

From the external network point of view, the proposed security infrastructure showed quite efficient, assisting the VISA recommendation #1 integrally "Install and maintain the working network firewall to protect data accessible through the Internet."

The problems appeared in the analysis of the internal sub-networks. Due the fact of inexistence of security policy that defines how should be installed the operating systems, how and who can share files and folders, anti-virus standardization, etc, several vulnerabilities were detected compromising the company security. Besides, it was possible to capture e-mail user passwords through the POP protocol, once some network segments were shared (based on Hubs).

To combat the problems found in the internal network, first of all, it is recommended to elaborate and implement a security policy appropriate with business of the company. Basically, the security policy should reflect the value of the information transmitted or stored by the computational systems. All the employees of the company, independently of position, salary or time of work, should accomplish this policy.

To minimize the sniffing problem in the internal network, it is recommended the substitution of all Hub's by Switches and implementation of VLAN's whenever possible.

To accomplish the defined rules by security policy, should be installed access control on all servers and services provided. The access control is usually based on passwords, so these must be changed periodically. When changing passwords it is required to have a system that verifies if the new password isn't "weak".

Periodic internal audits should be executed with the objective of verifying the adoption of the security policy. Audits together with the inventory software have as goals:

- Verify and maintain O.S updated;
- Verify and maintain anti-virus systems updated;
- To verify the "quality" of the passwords;
- To verify the storage conditions of sensitive data and the respective back-up's policy;
- To reformulate the company's security policy.

It is clear that the company's security is not summarized in firewalls, IDS, proxies, etc. configuration, but consists in the continuous evaluation of the interaction process among servers, services and users.

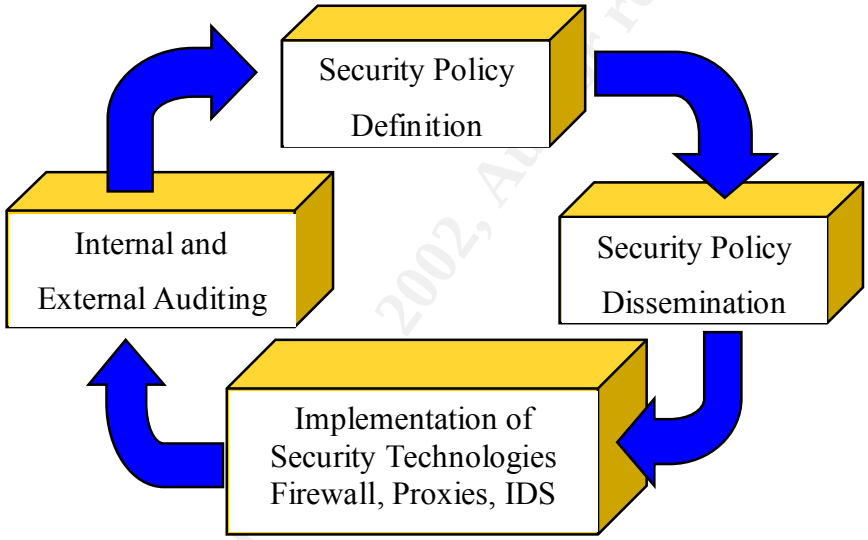


Figure 13 – The continuous process of security evaluation

References

[Anders2000] Anders, D., "Firewall and Perimeter Protection Practical Assignment", May, 2000.
URL: http://www.sans.org/y2k/practical/Dustin_Anders_gcfa.doc

[SANS2.2] Spitzner, Lance, "Firewalls 101: Perimeter Protection with Firewalls", SANS Network Security 2000, October 2000.

[Mitchell2000] Mitchell E., Mann S., "Linux System Security The Administrator's Guide to Open Source Security Tools", Prentice Hall, NJ 2000

[Doraswamy1999] Doraswamy N., Harkins D., "IPSec The New Security Standard for the Internet, Intranets, and Virtual Private Networks", Prentice Hall, NJ 1999.

[Northcutt2000] Northcutt S., Novak J., "Network Intrusion Detection – An Analyst's Handbook", New Riders Publishing, September 2000