Global Information Assurance Certification Paper

GIAC Firewall And Perimeter Protection Curriculum Practical Assignment
Network Security 2000 – Monterey, CA
Version 1.3
By Timothy W. Foreman
22-Nov-00

Assignment 1: Security Architecture

Scope: Define a security architecture based on the VISA "Ten Commandments" by developing a set of network diagrams for an E-Commerce business. More information on the VISA "Ten Commandments" can be found on the VISA web site at: http://www.visabrc.com/doc.phtml?2,64,932,932_cisp_download.html

The VISA "Ten Commandments" are as follows:

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

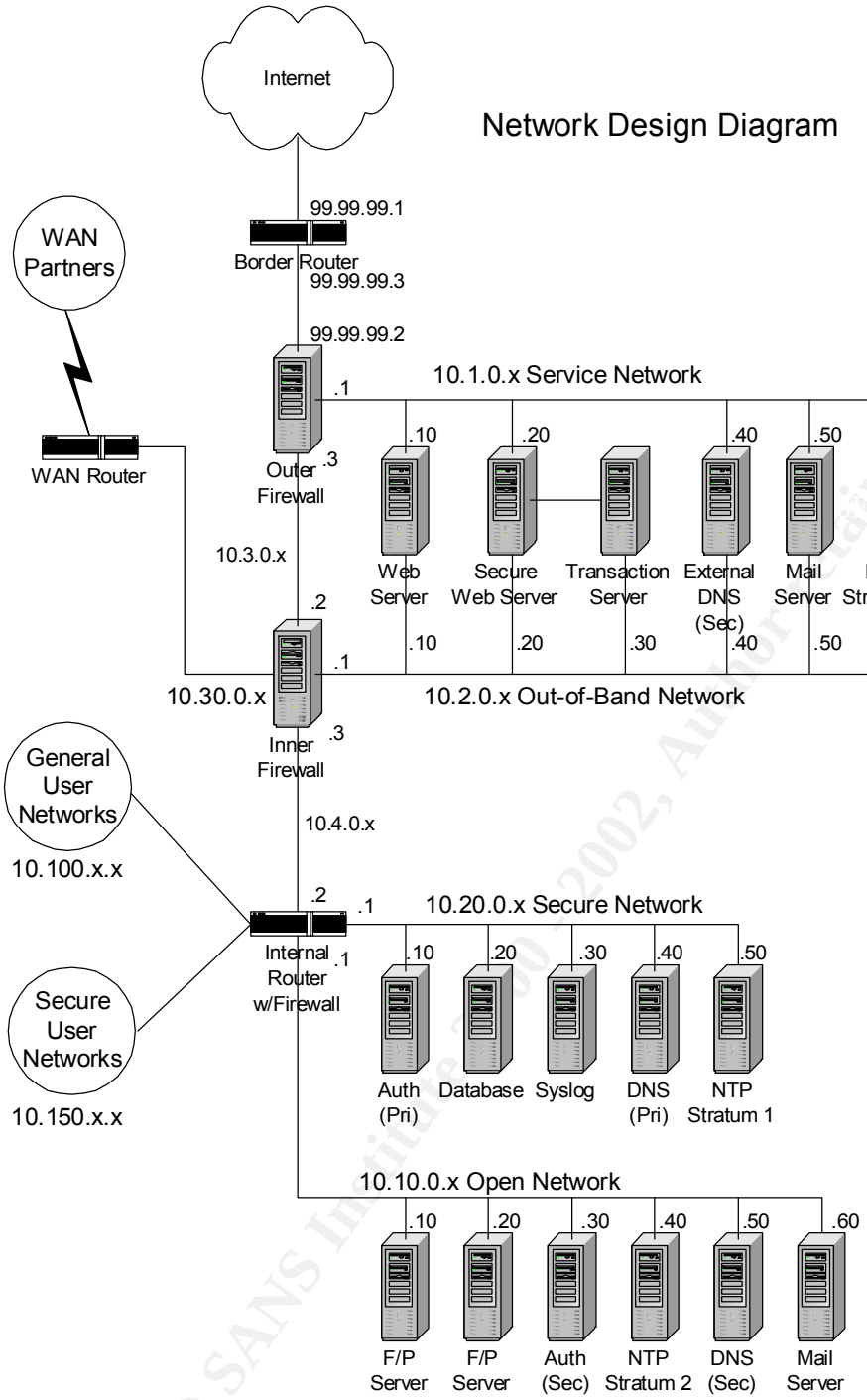
The network design diagram and explanations will be aimed mainly at implementing numbers 1, 3, 4 and 6. The rest of the rules are implemented by the policy and procedures outlined after the network design. This document is not meant to be a complete network design, but more an overview to aid in determining how to implement the security features required.

Network design rules:

1. All internal networks will use the 10.x address pool. The first firewall will be running NAT to allow access to the Service network and allow internal user machines to access the Internet.
2. Access to the Internet from servers and workstations must be limited to specific services.
3. Access from the Internet to servers on the Service network must be limited to required services.
4. Access from the Internet to servers not on the Service network must be blocked.

5. All primary servers will be located on the internal Secure network with strictly limited access. Primary servers include: Primary DNS, Primary Authentication server, Network Time server – Stratum 1 and the Syslog server.
6. All servers will log to a centrally located Syslog server.
7. A Stratum 1 Network Time server will be set up on the Secure network and Stratum 2 servers installed on the Service network and the Open network. All servers and workstations will sync to the Stratum 2 servers. Only the Stratum 2 servers will sync to the Stratum 1 server.
8. All user authentication will occur to secondary authentication servers on the Open network. These secondary servers will sync with the primary authentication server on the secure network.
9. All servers will be hardened by removing all unnecessary services and software. All default accounts and passwords will be removed or changed. All current patches will be applied and future patches evaluated.
10. The 10.x address pool will be sub-netted based on security demarcations as follows:
    a. The 10.1.0.x subnet will be used for the public servers. These servers are on the Service network connected to the first firewall.
    b. The 10.2.0.x network will be created to enable Out-of-Band management of the servers on the 10.1.0.x (Service) network. This network will be connected to the second firewall to limit access to authorized personnel and limit damage in case of a breach.
    c. The 10.10.0.x network will be used for general purpose file and print servers that can be accessed by anyone in the company for day to day usage.
    d. The 10.20.0.x network will contain all the administration servers that have limited user access. These servers include the Syslog server, the Primary DNS server, the Authentication server and the Accounting servers.
    e. The 10.100.x.x networks will contain all the general users in the company.
    f. The 10.150.x.x networks will contain the secure users in the company. These are users that require access to the servers on the Secure network and have access to the Out-of-Band network.
    g. WAN access for the partners who require access to the internal network will be allowed using a router on the 10.30.x.x network. This router will be filtered through the second firewall.

The main reasoning behind this design is to limit which servers are allowed to have connections coming from the Internet. The only servers that the public should be allowed to access are the ones in the service network. Additionally, no server in the service network should be allowed to make connections to any internal servers except those expressly permitted.



Implementing the relevant "Ten Commandments" using this design

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

This requirement is fulfilled by the Border Router, which is configured with ACLs to perform primary filtering and eliminate address spoofing, and the Outer and Inner Firewalls configured with rule sets to limit traffic.

2. Keep security patches up-to-date.

The Security Policy and Procedures documents clearly define that we monitor security mailing lists and vendor sites in order to be aware of any new vulnerabilities that arise in all the products that we run. It also states that we install all patches on a test system before deploying them in order to assure that we don't break something else with the patch.

3. Encrypt stored data accessible from the Internet.

This is requirement is met by encrypting all data on the Transaction server. Also, the Transaction server is not directly accessible via the Internet, but only from the Secure Web Server and the Out-of-Band network.

4. Encrypt data sent across networks.

This primarily refers to encrypting cardholder information sent across the Internet during sales transactions. We are doing this by using a Secure Web server and SSL for order processing. In addition, we will encrypt all data transferred from the Transaction server to the Database server located on the Secure network.

5. Use and regularly update anti-virus software.

The Security Policy and Procedures documents clearly define installing Anti-Virus software on all servers and desktops in the organization. It also states that we must keep all virus definition files up to date.

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

This means that we need to restrict the access to data by both internal and external people. We are doing this by blocking all access to the secure network from the Internet and only allowing specific machines and users access from the internal networks.

7. Assign unique IDs to each person with computer access to data.

We are running a mixed environment of various flavors of Unix and Windows NT on the servers. All desktops are Windows NT. Each user has their own domain login account with appropriate permissions assigned.

8. Track access to data by unique ID.

Auditing will be turned on for all NT servers and set to monitor access to sensitive data. In addition, all System Administrators on Unix boxes will use SUDO to do all work requiring root privileges. All Unix boxes will log to a central Syslog server in the Service network.

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

All default passwords will be changed or removed on all servers and installed software packages.

All Administrator accounts on NT servers will be given a difficult password which will then be sealed and stored away. The Administrator accounts will then be renamed and disabled and dummy accounts created. All administration work will be carried out using accounts with appropriate privileges.

All root accounts on Unix servers will be given difficult passwords which will then be sealed and stored away. All administration will take place using SUDO.

10. Regularly test security systems and processes

IDS systems placed on each network section monitor for suspicious traffic. All logs are reviewed daily. An audit process is defined to periodically test systems and processes.

Assignment 2: Security Policy

It is assumed that the base security policy including anti-spoofing has been implemented on all firewall devices and routers.

NAT Table

The following NAT entries have been implemented

System/Network	IP Address	NAT Address(es)
Service Web Server	10.1.0.10	99.99.99.10
Service Secure Web Server	10.1.0.20	99.99.99.20
Service DNS Server	10.1.0.40	99.99.99.40
Service Mail Server	10.1.0.50	99.99.99.50
Secure Syslog Server	10.20.0.30	99.99.99.30
General User Networks	10.100.x.x	99.99.99.100, 110
Secure User Networks	10.150.x.x	99.99.99.150, 160

Router Security

Border, Internal and WAN routers have been configured. Logging has been enabled to the internal Syslog server and the banner changed. All unnecessary services have been disabled.

```
banner /Authorized Personnel Only/
logging 99.99.99.30
no service finger
no service tcp-small-servers
no service udp-small-servers
no snmp
no ip bootp server
no ip unreachables
no ip direct-broadcast
no ip http server
no ip source-route
```

All routes on the border router are static. No routing protocols are enabled.

Firewall Configurations

Configuring the Outer (PIX) firewall

The interfaces are named and assigned a 'Security Level.' The security levels define the way that access is handled from interface to interface. The 'inside' is always 100 and the 'outside' is always 0.

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 service security50
```

Create ACLs for each interface and apply them to the inbound side.

```
access-group acl_outside in interface outside
access-group acl_inside in interface inside
access-group acl_service in interface service
```

To make configuration easier to understand, we will assign names to the IP addresses. This does introduce another layer of administration, in that when hosts are added and removed to the network they need to be added and removed here. In addition, mapping these names to DNS entries can be a hassle.

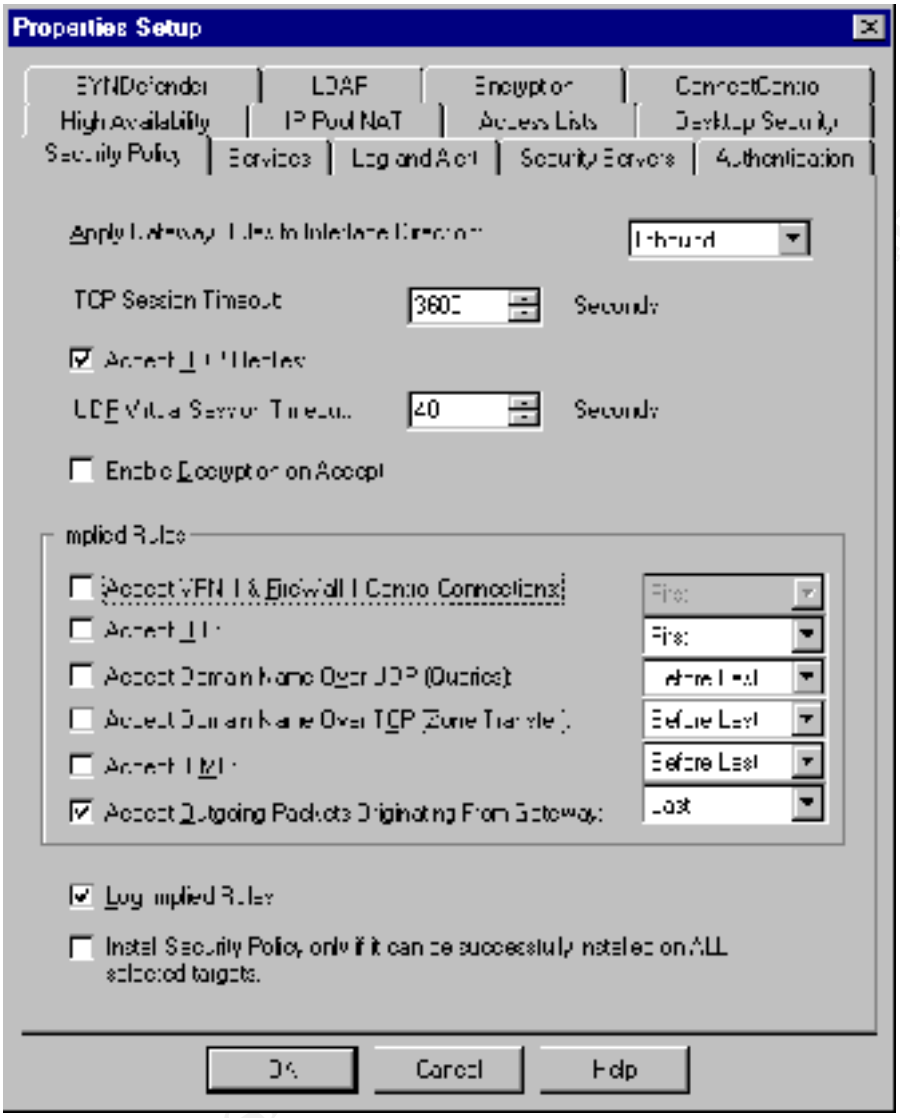
```
name 99.99.99.3  border_router
name 99.99.99.10 web_server
name 99.99.99.20 secure_web_server
name 99.99.99.40 dns_server
name 99.99.99.50 mail_server
name 99.99.99.100 workstation_nat1
name 99.99.99.110 workstation_nat2
name 99.99.99.150 workstation_nat3
name 99.99.99.160 workstation_nat4
name 10.3.0.2 inner_firewall
name 10.20.0.30 syslog_private
```

We need to tell the firewall where to log

```
logging on
logging level informational
logging host syslog_private udp 514
```

Configuring the Inner (Firewall-1) firewall

The default settings for Firewall-1 leave it quite open and can allow DNS and ICMP traffic to pass through without logging. It is recommended that the following configuration changes be made:



Firewall Rule Sets

The PIX ACL format is as follows:

```
access-list "Name" "Action" "Protocol" "Source Address & Mask" \
"Source Port" "Destination Address & Mask" "Destination Port"
```

Name	Name of the access-control-list this filter applies to
Action	Permit - pass traffic Deny - do not pass traffic
Protocol	IP protocol – UDP, TCP, ICMP or an IP protocol number
Source Address & Mask	Source IP address & subnet mask, or 'any' or 'host' & IP address
Source Port	Optional source port for TCP or UDP
Destination Address & Mask	Destination IP address & subnet mask, or 'any' or 'host' & IP address
Destination Port	Optional destination port for TCP or UDP protocols

The Firewall-1 format is as follows:

No.	Ordered rule number
Source	Source objects - IP addresses/Networks/Groups, may also be negated
Destination	Destination objects - IP addresses/Networks/Groups, may also be negated
Service	Protocol objects - individual protocols (TCP/UDP ports) or groups
Action	Accept - pass traffic Drop - do not pass traffic Reject - do not pass traffic and reply with RST Encrypt - encrypt VPN traffic Client Encrypt - authenticate user and encrypt VPN traffic
Track	Type of logging
Install On	Firewall this rule is applied to
Time	Times this rule is active
Comment	Description of rule

Rule: Allow Web (HTTP and HTTPS) access from the Internet to the Web servers on the Service Network *only*.

Why? Prevents access to internal servers that may be running web services, i.e. Intranet servers, mis-configured servers or "unauthorized" servers.

Test: Attempt to browse to allowed servers from the Internet. Perform a port scan of all addresses on the 99.99.99.x network to determine if the web ports are open.

Note: This rule only applies to the Outer (PIX) firewall as the Inner firewall is not in the path to these servers.

PIX

```
access-list acl_outside permit tcp any host www_server eq http
access-list acl_outside permit tcp any host secure_www_server eq 443
```

Firewall-1

```
n/a
```

Rule: Allow outbound Web and FTP access from Internal user networks *only*.

Why: No servers should be allowed to browse the Internet. This prevents browsing to malicious web pages from servers. Although it makes tech support a little more difficult, it's worth it from a security standpoint.

Test: Attempt to browse the Internet from the servers.

PIX

```
access-list acl_inside permit tcp host workstation_nat1 any eq http
access-list acl_inside permit tcp host workstation_nat1 any eq 443
access-list acl_inside permit tcp host workstation_nat1 any eq ftp
access-list acl_inside permit tcp host workstation_nat2 any eq http
access-list acl_inside permit tcp host workstation_nat2 any eq 443
access-list acl_inside permit tcp host workstation_nat2 any eq ftp
access-list acl_inside permit tcp host workstation_nat3 any eq http
access-list acl_inside permit tcp host workstation_nat3 any eq 443
access-list acl_inside permit tcp host workstation_nat3 any eq ftp
access-list acl_inside permit tcp host workstation_nat4 any eq http
access-list acl_inside permit tcp host workstation_nat4 any eq 443
access-list acl_inside permit tcp host workstation_nat4 any eq ftp
```

Firewall-1

Rule: Only allow UDP DNS queries from the Internet to the DNS server on Service network. Allow the DNS server on Service network to make Zone Transfers from the Primary DNS server on Secure network.

Why? Preventing TCP DNS queries restricts people from performing Zone Transfers and learning about the network. The Secondary DNS server on the Service network needs to be able to get new Zone records from the Primary DNS server on the Secure network.

Notes: The Internal DNS server runs split DNS for internal networks. The DNS server on the Service network does not allow recursion for inquiries from the Internet. The DNS server on the Service network performs Zone Transfers through the Out-of-Band network. The User network machines can use ISP DNS servers as backups if the server on the Open network is unavailable.

PIX

```
access-list acl_outside permit udp any host dns_server eq 53

access-list acl_inside permit udp host workstation_nat1 host isp_dns1 eq 53
access-list acl_inside permit udp host workstation_nat2 host isp_dns1 eq 53
access-list acl_inside permit udp host workstation_nat3 host isp_dns1 eq 53
access-list acl_inside permit udp host workstation_nat4 host isp_dns1 eq 53
```

Firewall-1

Rule: Allow SMTP connections from Internet to Mail server on Service network *only*. Allow Mail server on Secure network to poll Mail server on Out-of-Band network. All User network machines relay mail through Mail server on Secure network.

Why? Protects Mail server on Secure network from DOS attacks. Having the Secure Mail server poll the Service Mail server instead of allowing the Service Mail server to initiate connections to the Secure Mail server prevents further security breeches in the event the Service Mail server is compromised.

Test: Try sending mail to internal machines.

PIX

```
access-list acl_outside permit tcp any host service_mail eq smtp
access-list acl_service permit tcp host service_mail any host eq smtp
```

Firewall-1

Rule: Allow Syslog connections only from specified locations to the Secure Syslog server

Why? Prevents possible Syslog exploits. Placing the log files on an internal host prevents hackers from modifying the log files to cover their tracks.

Test: Trigger syslog events to assure that logging occurs. Attempt to log from invalid IP addresses.

Notes: The Service network servers will send their Syslog data through the Out-of-Band network.

PIX

```
access-list acl_outside permit udp host border_router host secure_syslog \
eq 514
```

Firewall-1

Rule: Only allow administrative access to security devices from authorized users.

Why? To prevent unauthorized access and prevent tampering.

Test: Try to access devices from unauthorized workstations.

Notes: The Outer (PIX) firewall only needs to grant access to the Border Router. All administration for the servers on the Service network takes place on the Out-of-Band network.

PIX

```
access-list acl_inside permit tcp host secure_admin host border_router \
eq telnet
access-list acl_inside permit tcp host secure_admin host border_router \
eq tftp
```

Firewall-1

Rule: Allow the Transaction to connect to the Database server on the Secure network.

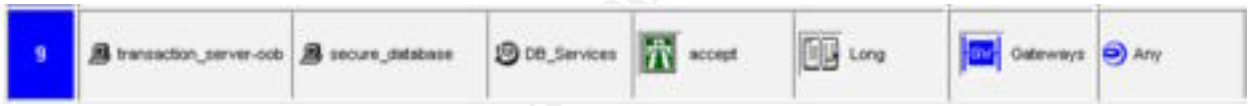
Why? To transfer transactions to the database server.

Notes: This traffic occurs on the Out-of-Band network.

PIX

```
n/a
```

Firewall-1



Rule: Allow Service networks to connect to Open Authentication server.

Why? To allow Secure users to authenticate and log into the servers.

Notes: This traffic passes over the Out-of-Band network.

PIX

```
n/a
```

Firewall-1

Rule: Allow WAN partners to access the internal networks, but not the Out-of-Band network, nor use our Internet connection.

Why? WAN partners need to access internal resources but should have their own Internet connection.

Test: If possible, have a WAN user try to browse the Internet through a route into our network.

Notes: Since the WAN connection is into the Internal firewall, it can do all the filtering.

PIX

n/a

Firewall-1

Rule: Block and log everything else except normal NetBIOS noise.

Why? We block all non-required services and ports. We filter out the NetBIOS noise to keep from filling up the logs.

Test: Monitor NetBIOS traffic on the network and make sure it is not getting into the logs. Generate traffic that is not allowed in the rules and make sure it is dropped and logged.

PIX

```
access-list acl_outside deny ip any any
access-list acl_service deny ip any any
access-list acl_inside deny ip any any
```

Firewall-1

Complete Rule Sets for each Firewall

Outer (PIX) Firewall

```
access-list acl_outside permit tcp any host www_server eq http
access-list acl_outside permit tcp any host secure_www_server eq 443
access-list acl_outside permit udp any host dns_server eq 53
access-list acl_outside permit tcp any host service_mail eq smtp
access-list acl_outside permit udp host border_router host secure_syslog \
eq 514
access-list acl_outside deny ip any any


access-list acl_inside permit tcp host workstation_nat1 any eq http
access-list acl_inside permit tcp host workstation_nat1 any eq 443
access-list acl_inside permit tcp host workstation_nat1 any eq ftp
access-list acl_inside permit tcp host workstation_nat2 any eq http
access-list acl_inside permit tcp host workstation_nat2 any eq 443
access-list acl_inside permit tcp host workstation_nat2 any eq ftp
access-list acl_inside permit tcp host workstation_nat3 any eq http
access-list acl_inside permit tcp host workstation_nat3 any eq 443
access-list acl_inside permit tcp host workstation_nat3 any eq ftp
access-list acl_inside permit tcp host workstation_nat4 any eq http
access-list acl_inside permit tcp host workstation_nat4 any eq 443
access-list acl_inside permit tcp host workstation_nat4 any eq ftp
access-list acl_inside permit udp host workstation_nat1 host isp_dns1 eq 53
access-list acl_inside permit udp host workstation_nat2 host isp_dns1 eq 53
access-list acl_inside permit udp host workstation_nat3 host isp_dns1 eq 53
access-list acl_inside permit udp host workstation_nat4 host isp_dns1 eq 53
access-list acl_inside permit tcp host secure_admin host border_router \
eq telnet
access-list acl_inside permit tcp host secure_admin host border_router \
eq tftp
access-list acl_inside deny ip any any

access-list acl_service permit tcp host service_mail any host eq smtp
access-list acl_service deny ip any any
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Inner (Firewall-1) Firewall

No.	Source	Destination	Service	Action	Track	Install On	Time
1	secure_int_users	outer_firewall inner_firewall border_router WAN_router	telnet tftp ftp	accept	Long	Gateways	Any
2	Any	border_router inner_firewall outer_firewall WAN_router	Any	drop	Long	Gateways	Any
3	secure_int_users	out-of-band_network	Any	accept	Long	Gateways	Any
4	internal_users secure_int_users	WAN_Partners out-of-band_network	http ftp https	accept	Long	Gateways	Any
5	service_dns-oob	secure_dns	dns	accept	Long	Gateways	Any
6	open_dns_server	external_network	domain-udp	accept	Long	Gateways	Any
7	open_mail	service_mail-oob	smtp	accept	Long	Gateways	Any
8	out-of-band_network border_router outer_firewall WAN_router inner_firewall	secure_syslog	syslog	accept	Long	Gateways	Any
9	transaction_server-oob	secure_database	DB_Services	accept	Long	Gateways	Any
10	service_ntp-oob	secure_ntp	ntp	accept	Long	Gateways	Any
11	out-of-band_network	open_auth_server	ldap-ssl	accept	Long	Gateways	Any
12	WAN_Partners	out-of-band_network external_network	Any	accept	Long	Gateways	Any
13	Any	Any	NBT	drop		Gateways	Any
14	Any	Any	Any	drop	Long	Gateways	Any

Assignment 3: Auditing

Planning Phase

1. Discuss with IT Management the scope of project and possible ramifications of the auditing.
   a. Determine if password cracking falls under the scope of this project.
   b. Make sure that it is understood that some of the tools to be used may inadvertently create a DoS or some other problem.
   c. Obtain a written authorization signed by someone in the company with the appropriate authority. (Vice Presidents are good.)
   d. It is probably a good idea to inform all ISPs involved that port scanning and other types of probing will be occurring to avoid causing a DoS to the client (or yourself) due to an over-protective ISP.
   e. These steps needs to be performed during business hours
   f. Time required: one to three hours.
2. Collect as much information as possible from IT staff regarding network topology and security configurations. This information may take several days to collect and collate depending on the state of the existing documentation and which employees need to be contacted.
   a. This research needs to be performed during office hours.
   b. Time required: Varied. Could range from one to five days.
3. Perform DNS server checking using 'dig' to probe the DNS server for the domain.
   a. This research can be performed anytime.
   b. Time required: one hour
4. IP Address scanning to find hosts for further probing.
   a. This research can be performed anytime, but it would probably make the most sense to do it during business hours when most workstations are powered on.
   b. Time required: Varies by number of addresses to be scanned. A full class C address will probably take around an hour.
5. Scanning of discovered hosts for vulnerabilities.
   a. This process should probably be performed during non-business hours but with IT staff on hand. There is a chance that the testing will crash a machine or cause it to stop responding. Any workstations that are to be scanned will need to be left running. Scans should be scheduled around business-critical processes the should not be interrupted and may need to be spread over several days.
   b. Time required: Varied. Could range from one to five days.

6. Modem discovery/scanning. Modems can create a huge security hole in a network. Anytime that a user is connected to the Internet via a dialup connection they have done a complete end-run around the firewall. In addition, they have created a backdoor into the network for hackers.
   a. This research can be done by walking around and looking at all the workstations or by 'war dialing' the phone exchange associated with the company. Both types of information gathering should probably be done after hours or on the weekend to minimize disruption to the work force.
   b. Time required: Varies. The walk around inspection would take a couple of hours for 50 users. The 'war dialing' takes about 10 minutes per 50 numbers.

As you can see, coming up with a fixed cost and time estimate for a security audit is difficult. If the work is being performed on a consulting basis, it may be best to break this audit into phases and give an estimate for each phase based on the results of the previous one.

Implementation Phase

1. Discuss with IT Management the scope of project and possible ramifications of the auditing.
   a. It was determined that password cracking was not going to be under the scope of this project.
   b. Management is fully cognizant of the fact that some of the tools used may take services (or even servers) down.
   c. Written authorization was obtained from the V.P. of Technology.
   d. I have informed my ISP of my intent and the company has informed theirs.
2. Collect as much information as possible from IT staff regarding network topology and security configurations.
   a. As expected, the network maps and host lists are out of date. No matter how good the intentions are, this stuff always seems to end up on the bottom of the pile.
   b. The Security Policy looks pretty good and the rule sets from the Firewalls seem to match it.
3. Perform DNS server checking using 'dig' to probe the DNS server for the domain.
   a. 'dig' is a tool that comes with BIND 8, available at: http://www.isc.org/products/BIND/

First, we will find the authoritative name servers for the domain. There are at least two ways to do this. We can run 'whois' and see what we get, or we can use 'dig'. I'm going to show the output from both.

```
# whois somedomain.com
[whois.internic.net]

Whois Server Version 1.3

Domain names in the .com, .net, and .org domains can now be registered
```

```
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: SOMEDOMAIN.COM
   Registrar: NETWORK SOLUTIONS, INC.
   Whois Server: whois.networksolutions.com
   Referral URL: www.networksolutions.com
   Name Server: NS1.SOMEDOMAIN.COM
   Name Server: NS2.SOMEISP.NET
   Updated Date: 11-oct-2000


>>> Last update of whois database: Tue, 21 Nov 2000 09:31:36 EST <<<

The Registry database contains ONLY .COM, .NET, .ORG, .EDU domains and
Registrars.
```

So, there are two name servers we can try, one on site and one at the ISP. Let's see what 'dig' tells us.

```
# dig somedomain.com

; <<>> DiG 8.2 <<>> somedomain.com
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
;; QUERY SECTION:
;;      somedomain.com, type = A, class = IN

;; ANSWER SECTION:
somedomain.com.             1h32m3s IN A    99.99.99.10

;; AUTHORITY SECTION:
somedomain.com.             21h31m46s IN NS  NS1.somedomain.com.
somedomain.com.             21h31m46s IN NS  NS2.SOMEISP.NET.

;; ADDITIONAL SECTION:
NS1.somedomain.com.         2h21m42s IN A   99.99.99.40
NS2.SOMEISP.NET.            2m10s IN A      222.111.111.111

;; Total query time: 42 msec
;; FROM: host to SERVER: default - 111.111.111.111
;; WHEN: Tue Nov 21 22:10:53 2000
;; MSG SIZE  sent: 27  rcvd: 154
```

A little more information with a different format. With 'dig', we get the IP addresses of the name servers on the first shot, so it's a little easier to continue on. If we use the info from 'whois' we might have to do an additional 'nslookup' to get the IP addresses of the name servers.

Lets go a little deeper and see what we can find. We will use 'dig' to probe the name servers and see if they allow zone transfers. First we'll see if the ISP knows what they are doing.

```
# dig @222.111.111.111 somedomain.com

; <<>> DiG 8.2 <<>> @222.111.111.111 somedomain.com axfr
; (1 server found)
;; Received 0 answers (0 records).
;; FROM: host to SERVER: 222.111.111.111
;; WHEN: Tue Nov 21 22:20:15 2000
```

Well, looks like someone is on the ball anyway. Let's see if the client's DNS server is setup right.

```
# dig @99.99.99.40 somedomain.com axfr

; <<>> DiG 8.2 <<>> @99.99.99.40 somedomain.com axfr
; (1 server found)
$ORIGIN somedomain.com.
@                       12H IN SOA      ns.somedomain.com.
postmaster.somedomain.com. (
                                        2000102801      ; serial
                                        1D              ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        12H )           ; minimum

                        1D IN NS        ns.somedomain.com.
                        1D IN NS        ns2.someisp.com.
                        1D IN A         99.99.99.10
                        1D IN MX        10 mail
                        1D IN MX        100 mx1.someisp.com.
mail                    1D IN A         99.99.99.50
www                     1D IN A         99.99.99.10
www2                    1D IN A         99.99.99.20
ns                      1D IN A         99.99.99.40
bonzo                   1D IN A         99.99.99.37
bozo                    1D IN A         99.99.99.42
devbox1                 1D IN A         201.111.221.111
workstation1            1D IN A         99.99.99.100
workstation2            1D IN A         99.99.99.101
workstation3            1D IN A         99.99.99.102
workstation4            1D IN A         99.99.99.103
.
.
workstation99           1D IN A         99.99.99.199
@                       12H IN SOA      ns.somedomain.com.
postmaster.somedomain.com. (
                                        2000102801      ; serial
                                        1D              ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        12H )           ; minimum

;; Received xx answers (xx records).
;; FROM: host to SERVER: 99.99.99.40
;; WHEN: Tue Nov 21 22:24:40 2000
```

Wow. That's pretty impressive. We got a huge list of hosts to try and access. It looks like they added entries for all the NATed user machines and a host that is not on their network. Looks like we should aim our scanning at the 99.99.99.x network and make sure to hit the hosts named bonzo, bozo and devbox1 extra hard. This host should restrict zone transfers to stop this kind of information from being handed out.

If 'dig' had not given us this information, it is still possible to do some more mining by setting the type=any option and querying for common host names such as 'www', 'ftp', 'mail', etc.

4. IP Address scanning to find hosts for further probing.

The entire external network (99.99.99.0/24) should be scanned from a host positioned on the external network (or the Internet.) One tool for this is 'nmap' which can be downloaded from http://www.insecure.org/nmap/. This tool has many features for port scanning including a feature to try and determine the operating system and version.

The command to run a basic TCP and UDP scan on all well-known ports on the entire network is:

```
nmap -sTU 99.99.99.0/24
```

What is returned by this scan is a voluminous list of machines and ports. The ports will be marked with one of the following states:

- Open – This port is open and accepting connections.
- Filtered – This port is protected by a firewall and nmap can't determine if it is open or not.
- Unfiltered - Unfiltered means that the port is known by nmap to be closed and no firewall/filter seems to be interfering with nmap's attempts to determine this. Unfiltered ports are the common case and are only shown when most of the scanned ports are in the filtered state.

Here is a sample of an 'nmap' scan on a single host:

```
# nmap -sTU 99.99.99.2

Interesting ports on  (99.99.99.2):
(The 1535 ports scanned but not shown below are in state: closed)
Port       State       Service
1/udp      filtered    tcpmux
2/udp      filtered    compressnet
3/udp      filtered    compressnet
4/udp      filtered    unknown
5/udp      filtered    rje
6/udp      filtered    unknown
7/udp      filtered    echo
8/udp      filtered    unknown
9/udp      filtered    discard
10/udp     filtered    unknown
11/udp     filtered    systat
12/udp     filtered    unknown
```

```
13/tcp     open        daytime
.
.
5800/tcp   open        vnc
5800/udp   filtered    unknown
5801/udp   filtered    unknown
5900/tcp   open        vnc
.
.
27444/udp  filtered    Trinoo_Bcast
27665/udp  filtered    unknown
27960/udp  filtered    Quake3Server
31335/udp  filtered    Trinoo_Register
31337/udp  filtered    BackOrifice
.
.
Nmap run completed -- 1 IP address (1 host up) scanned in 406 seconds
```

Note that most of the ports are filtered by a firewall. 'nmap' still lists the interesting ports it knows about, like 27444 for Trinoo or 31337 for BackOrifice, but it can't tell if these services are running. At least it indicates that the ports are blocked by a firewall, so even if the services are running, they are not accessable from the Internet.

One thing that might need to be checked is that this host is running VNC on a couple of open ports. VNC is a remote control program like PCAnywhere and should be a security concern. More information on VNC can be gathered from: http://www.uk.research.att.com/vnc/

Additionally, port 13 (daytime) is open. There is really no need to have this port open and this could actually be the basis for a DoS attack. If a hacker sends a packet that is spoofed to come from the 'echo' port on one machine to the 'daytime' port on another machine, they will continue to bounce packets back and forth ad infinitum. This can cause the two machines to flood the network or become unresponsive.

Additional scans should be made of each internal network to determine if any services or programs are running that shouldn't be. Our main focus is determining if these systems are vulnerable to attack from the Internet, but a good audit should include scans of all hosts on the internal networks too.

5. Scanning of discovered hosts for vulnerabilities.

Once we have generated a list of all the hosts that are accessible from the Internet, there are a few tools that we can run to determine if the services on open ports are vulnerable to known attacks.

Keep in mind that new vulnerabilities are discovered daily. No tool can tell you that you are invulnerable, just that you are not vulnerable to the attacks that it knows about today.

There are a couple of easy tests that we can do to start off with. First, let's determine what version of BIND the DNS server is running. We can use the 'nslookup' command to do this from any host on the Internet.

```
# nslookup
Default Server:  ns.someisp.com
Address:  111.111.111.111

> server ns1.somedomain.com
Default Server:  ns1.somedomain.com
Address:  99.99.99.40

> set class=chaos
> set type=txt
> version.bind
Server:  ns1.somedomain.com
Address:  99.99.99.40

VERSION.BIND    text = "4.9.7-REL"
>
```

This does not always work. It is possible to tell the DNS server to lie about it's version, but most people don't. This server is running version 4.9.7 which is an older version of BIND, but it is the latest version and should be pretty secure.

We can also telnet into the mail server on port 25 and determine what software and version it is running.

```
# telnet mail.somedomain.com 25
Trying 99.99.99.20...
Connected to mail.somedomain.com.
Escape character is '^]'.
220 www.somedomain.com ESMTP Sendmail 8.9.3/8.9.3; Wed, 22 Nov 2000 14:02:27
-0600
```

Well, that server was certainly helpful. Now we know that its running sendmail 8.9.3 and we can go look up any known vulnerabilities for that version.

Let's try another server:

```
# telnet mail.someotherdomain.com 25
Trying 99.99.99.20...
Connected to mail.someotherdomain.com.
Escape character is '^]'.
220 mail.someotherdomain.com ESMTP Sendmail Pro-8.9.2.Beta1/Pro-8.9.2.Beta1;
Wed, 22 Nov 2000 15:00:15 -0600 (CST)
```

Sendmail Pro-8.9.2.**Beta1** – If I were a hacker, I'd be really interested in a sendmail server running a **beta** version. Better check this one out further.

Here is third server:

```
# telnet mail.somedomain3.com 25
Trying 99.99.191.99...
Connected to mail.somedomain3.com.
Escape character is '^]'.
```

```
220 mail.somedomain3.com ESMTP Server (Microsoft Exchange Internet Mail
Service 5.5.2650.21) ready
```

A Microsoft Exchange server.

Note: Sendmail can be configured to lie or to not return version information just like BIND, so this doesn't always work. But you would be surprised how helpful most servers can be.

Lets take a look at that web server next. It's pretty easy to get a web server to tell you what software and version it's running.

```
telnet 111.111.111.111 80
Trying 111.111.111.111...
Connected to 111.111.111.111.
Escape character is '^]'.
get http/1.0
HTTP/1.0 404 Not found
Server: Netscape-Enterprise/2.01
```

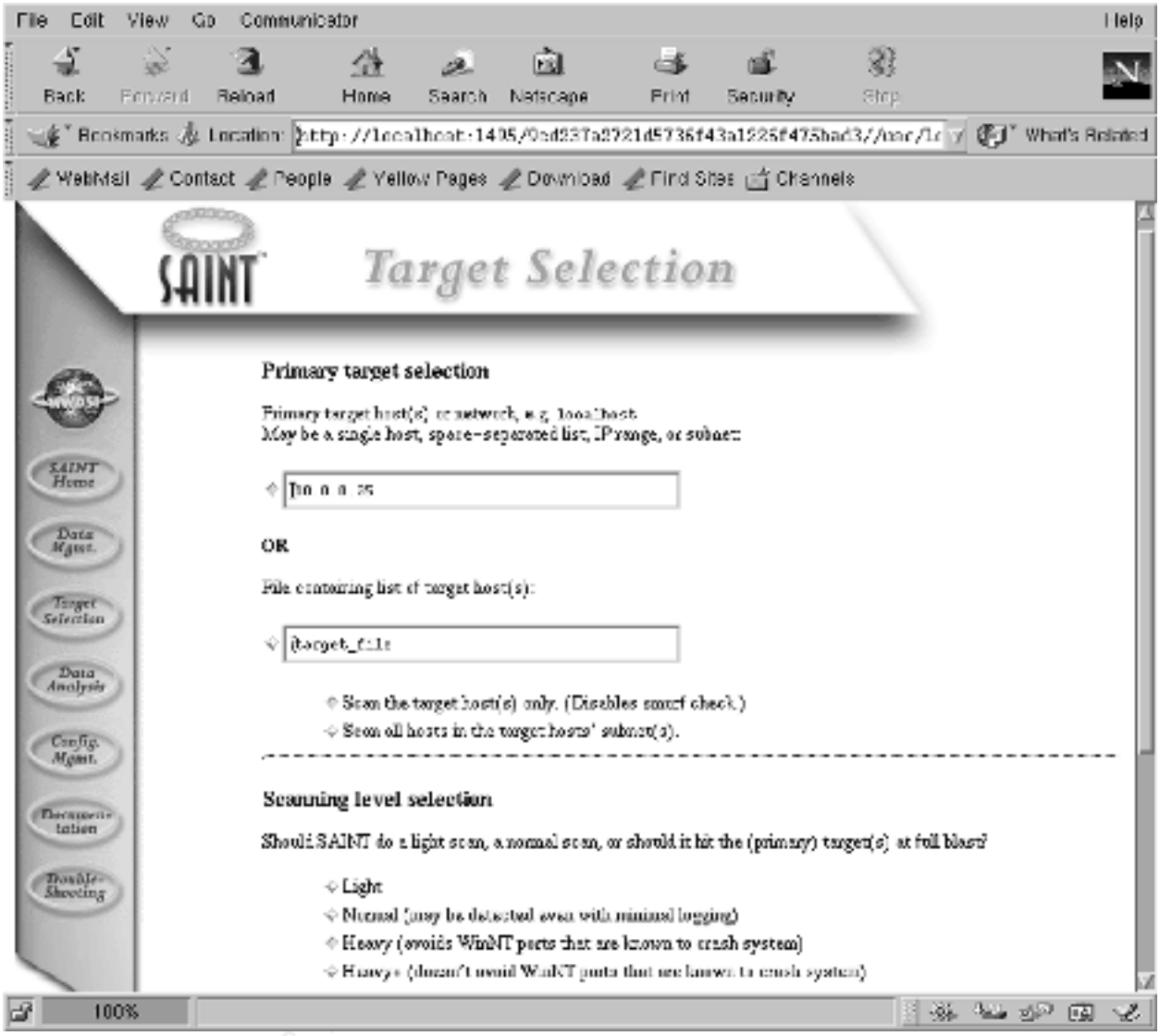
Let's try that again on another server.

```
telnet 111.111.111.112 80
Trying 111.111.111.112...
Connected to 111.111.111.112.
Escape character is '^]'.
get http/1.0
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/4.0
```

So, it's as easy as telneting to port 80 and doing a GET command and the server will be happy to tell you what software and version it's running. Note: As with Sendmail and BIND, the server can be told to lie, but out of the box it will hand out all kinds of information.

Okay, now we will pull out the big guns. We will now attach a host to the external network and run SAINT or SARA against our list of hosts with open ports.

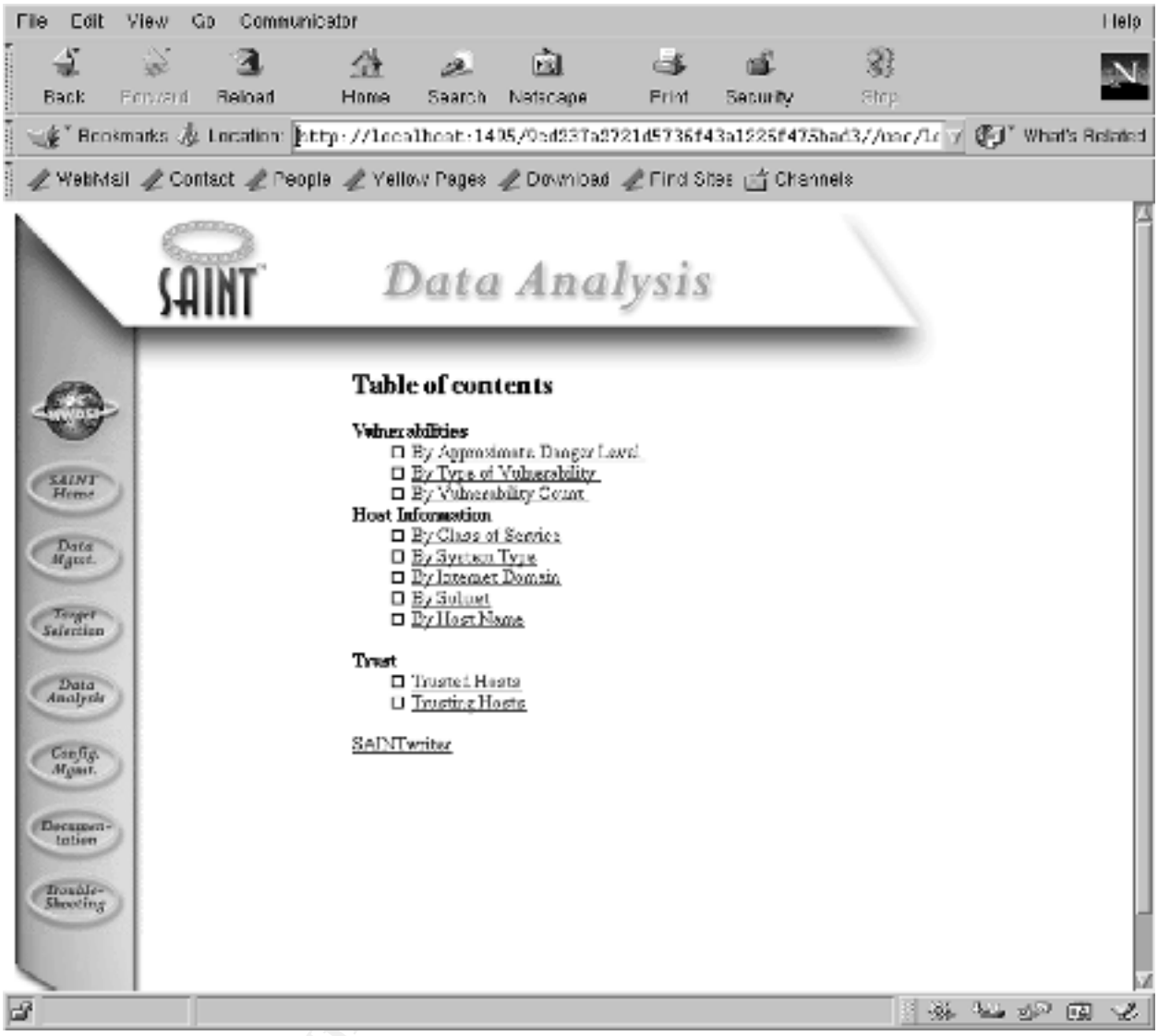
SAINT is the next generation of SATAN, a port scanning and vulnerability detection tool. SAINT stands for "The Security Administrator's Integrated Network Tool." It can be obtained from: http://www.wwdsi.com/saint/



This is the target selection screen for SAINT. Notice that we can define a single host, an IP address range, a subnet or use a list of hosts in a file. We also get to select a scanning level. Use caution in selecting the Heavy+ scan. There are ports on an NT machine that can crash the box when scanned with this option.

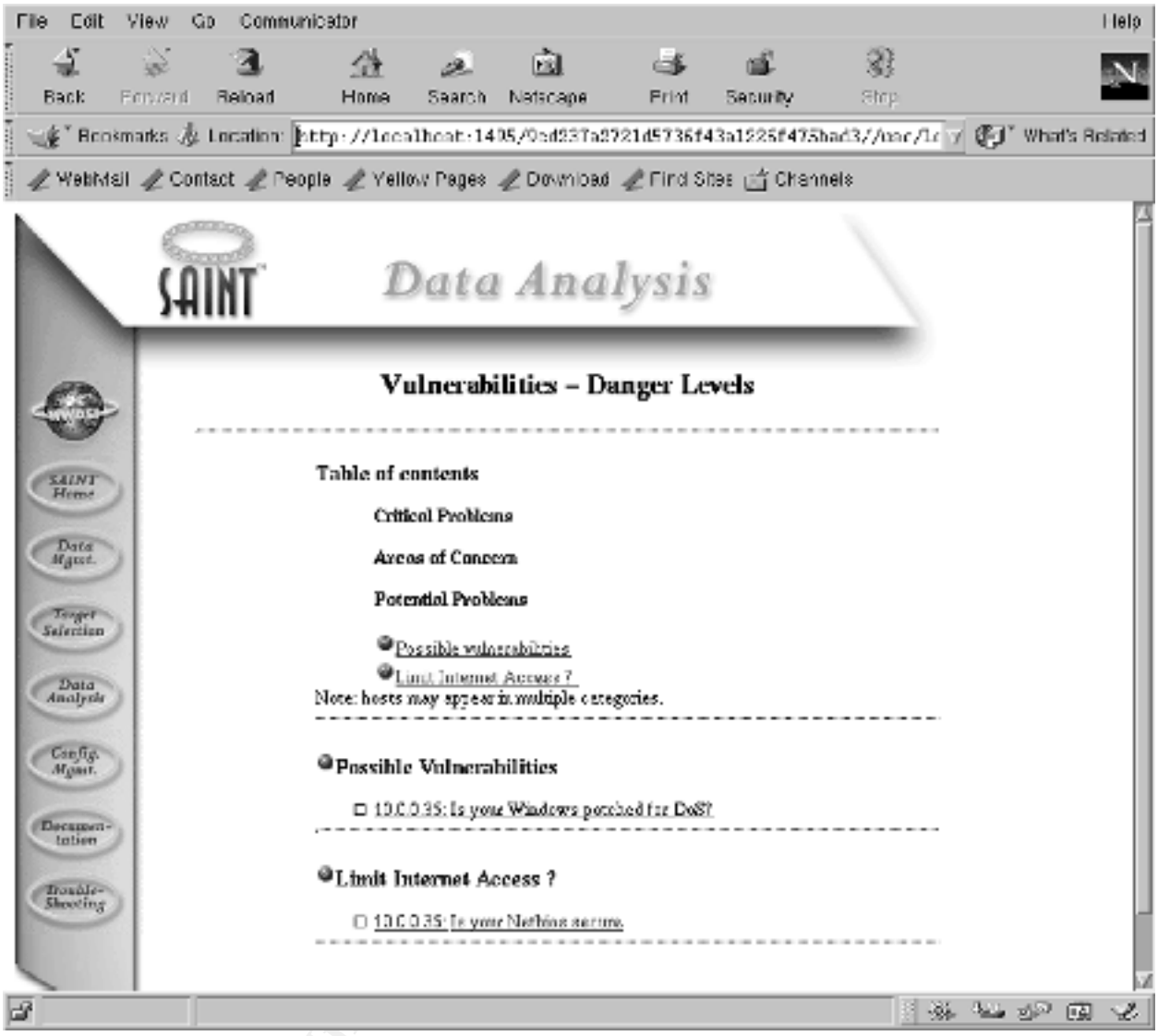
There is also an option for using SAINT behind a firewall and a Start Scan button that you press when you are ready to go.

After you are done scanning you go to the Data Analysis page. This is the front page for all the findings that SAINT has made.



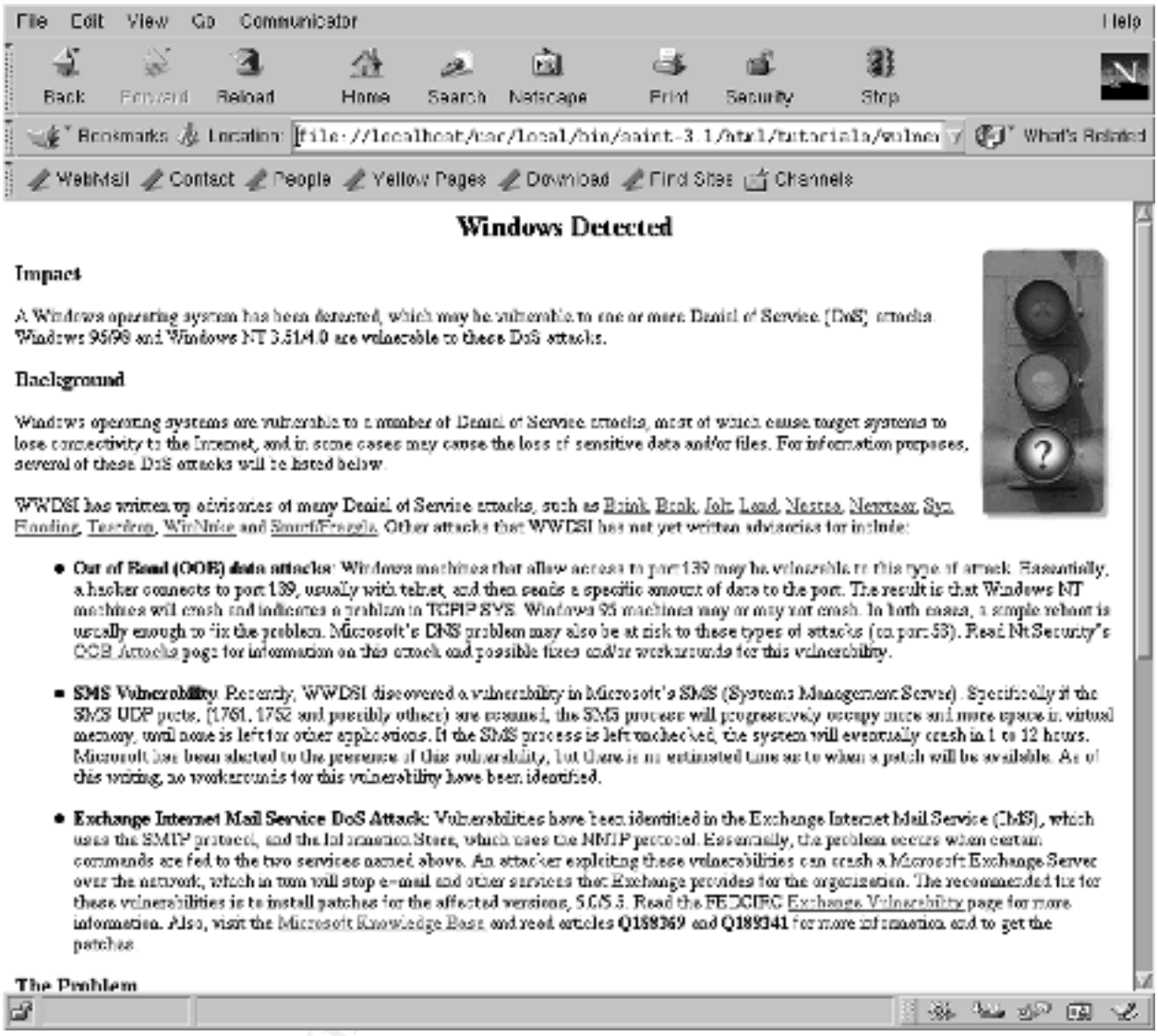
Notice all the different ways you can sort the collected information.

This is the vulnerabilities page. Notice that it has correctly identified the host as a Windows machine.



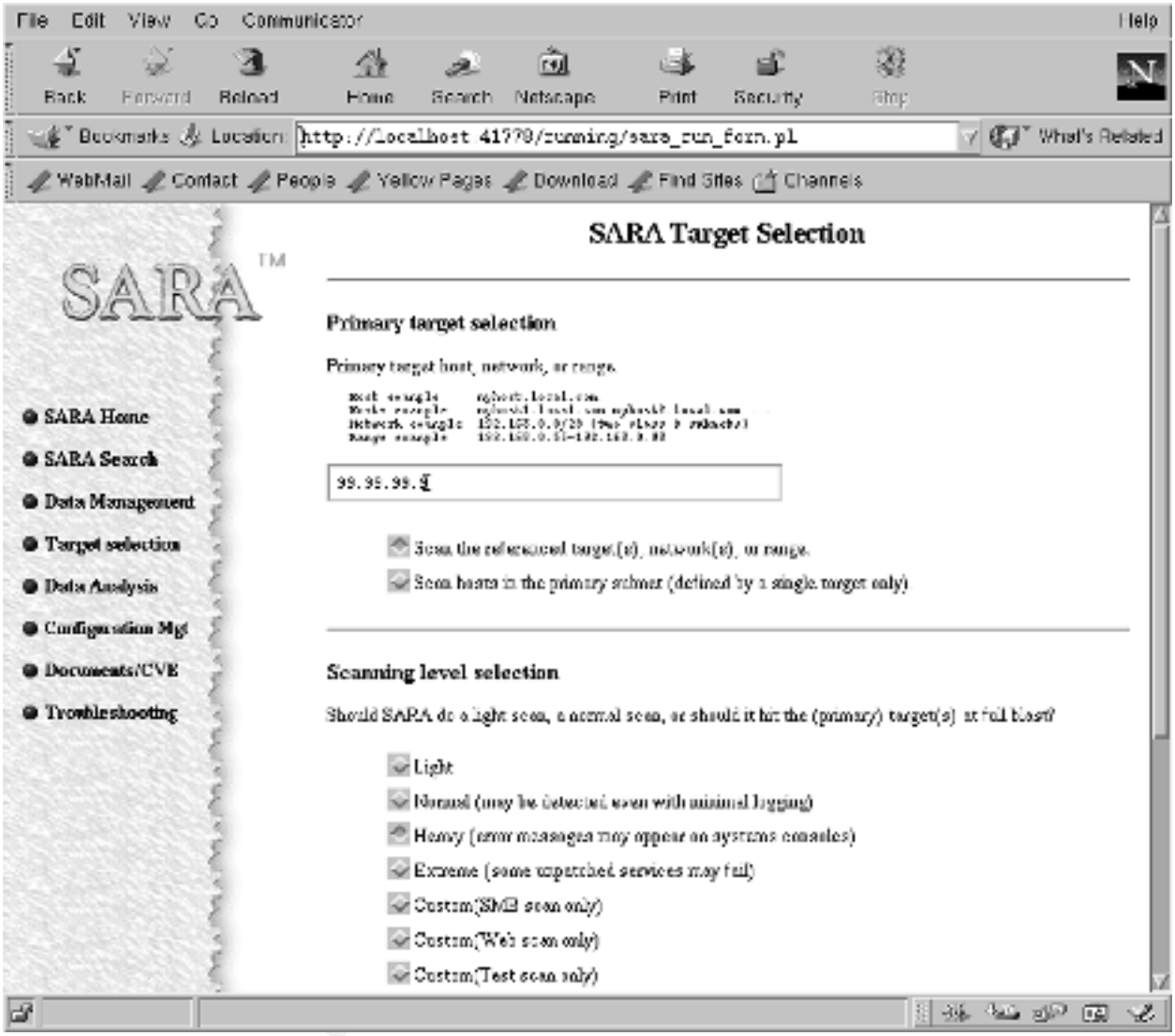
There are only Possible Vulnerabilities shown, so there are no gaping holes with this host, but SAINT does have a few suggestions for us anyway.

This is what SAINT shows you when you click on the link labeled 'Is your Windows patched for DoS?'



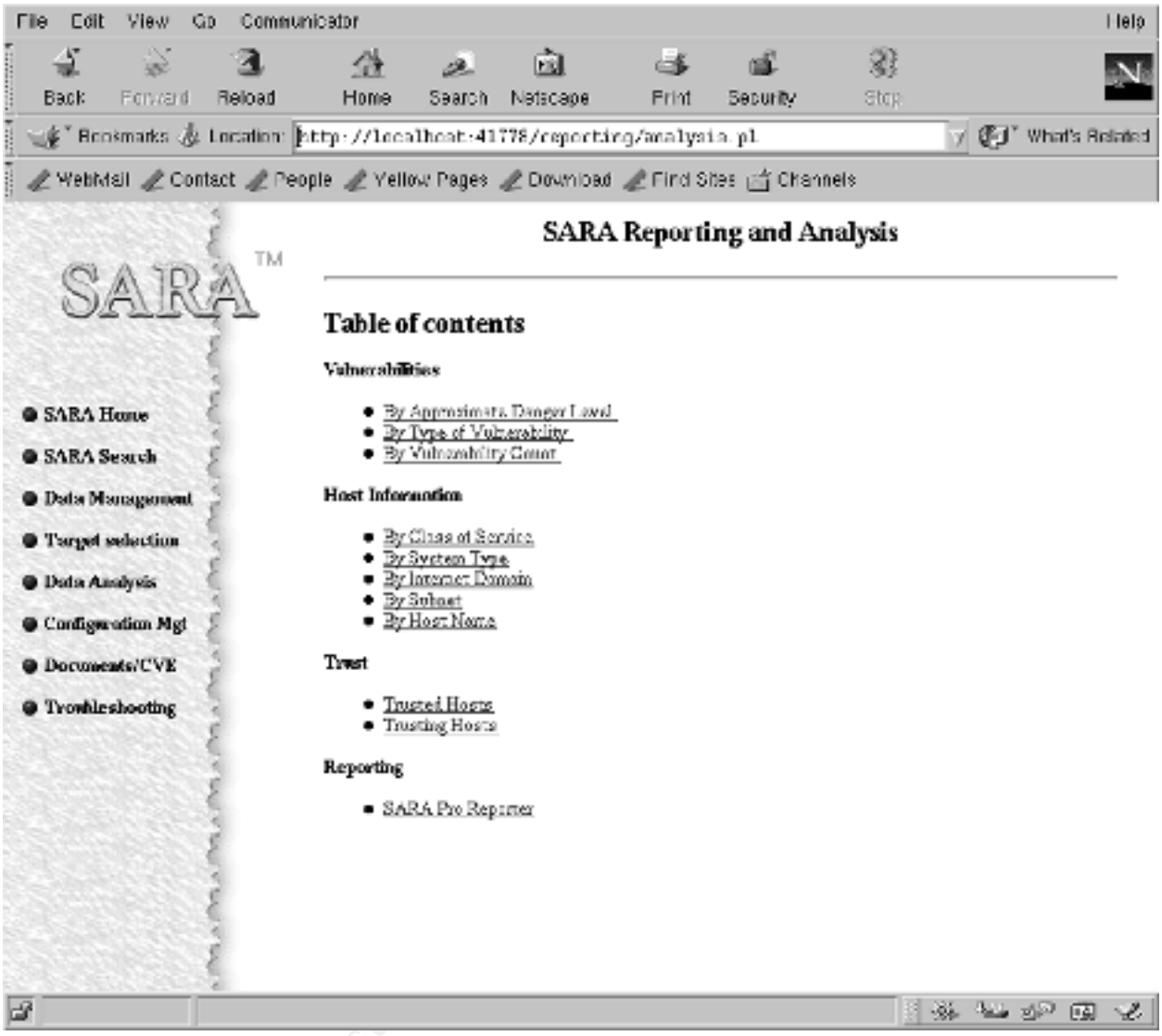
Notice the nice collection of information about Windows vulnerabilities that SAINT provides us with. This would make a great page to print out and give to a client for educational purposes (not to mention it makes great reading material for consultants.)

This is the target selection screen for SARA. The Security Auditor's Research Assistant, SARA bills itself as a third generation security analysis tool that is based on the SATAN model. More information about SARA is available at: http://www-arc.com/sara/

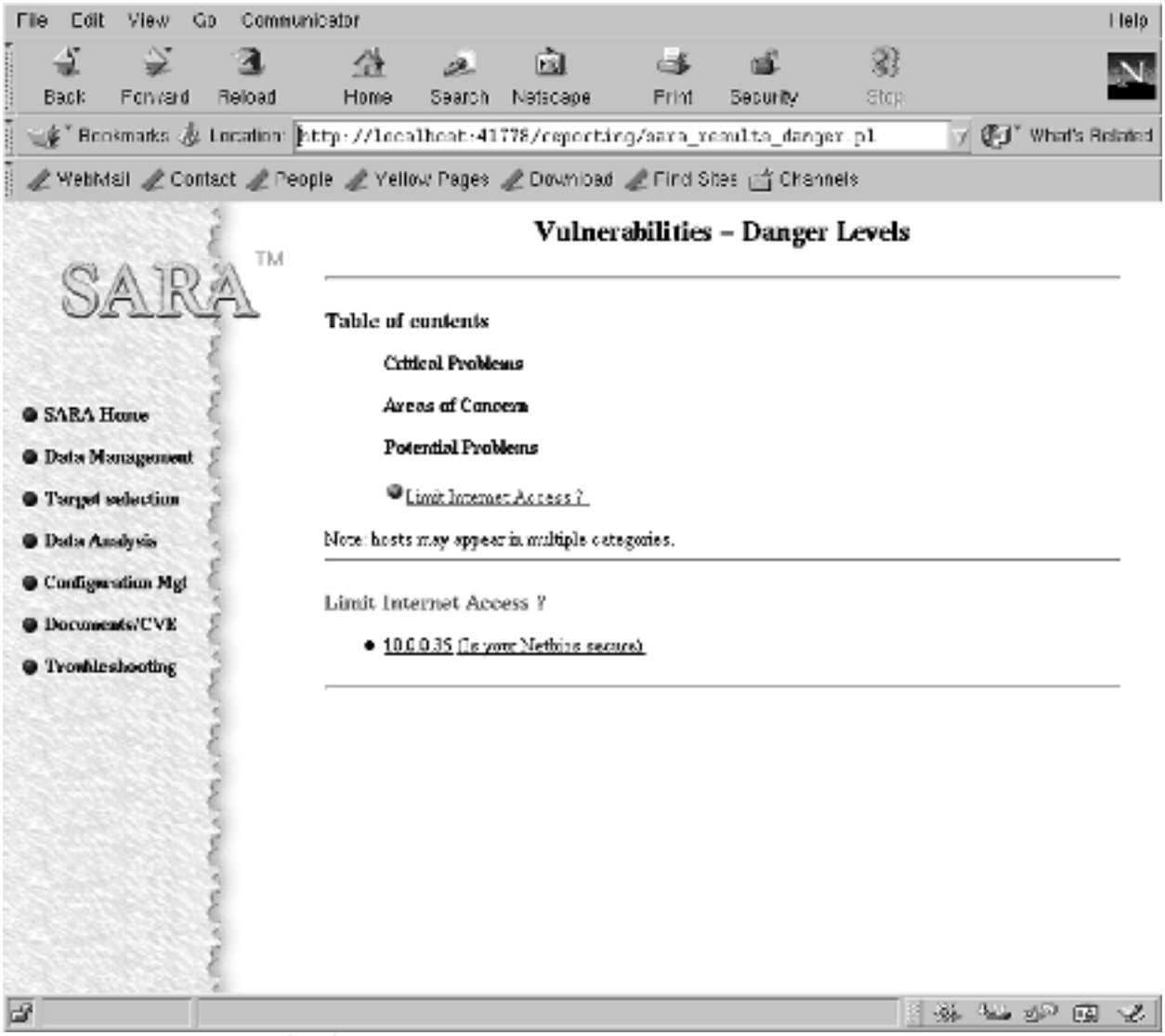


Notice that like SAINT, we can scan a single host, a range of hosts or a subnet. But we can't scan a list of hosts from a file. We are going to scan the same host that we scanned with SAINT and look at the information that we get.

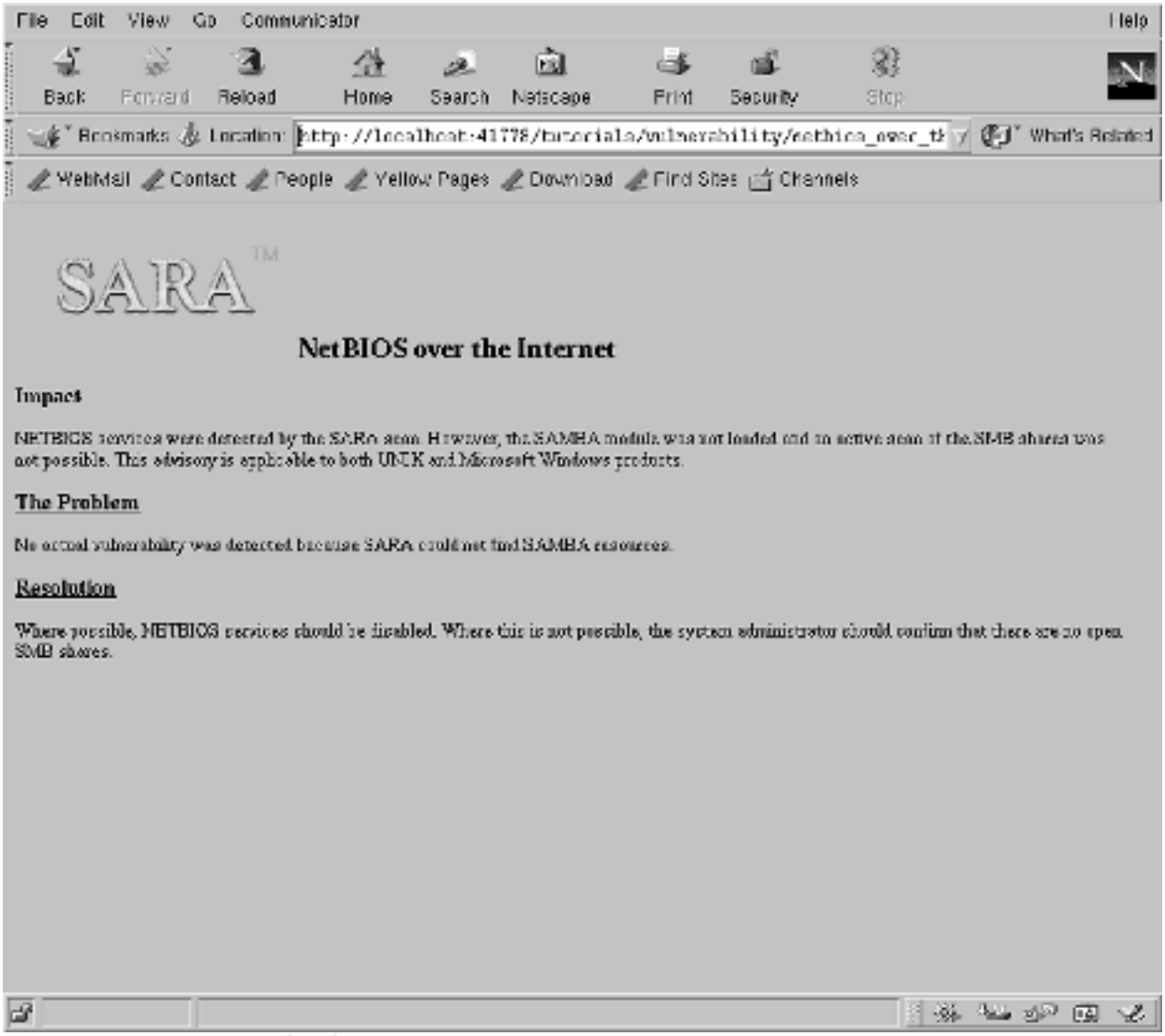
This is the Reporting and Analysis page. Note that it looks a lot like the page from SAINT.



Here is the Vulnerabilities page. Notice that SARA doesn't seem to have picked up as much as SAINT did. This is why I run scans with more than one tool. Some tools will pick up things that others will miss.



This is the page that SARA gives us about the NetBIOS vulnerabilities it is warning us about. It's not quite as glitzy as the page from SAINT, but it does point out that it can be a security issue.



6. Modem discovery/scanning.

It was decided that the IT staff would perform a walk around inspection of all workstations to look for modems. The staff was advised to work in pairs so as to avoid any claims of theft or tampering.

Analysis

After analyzing the network, I would recommend the following changes:

1. Implement a VPN solution.

Why? The fact that VNC was discovered on several hosts coupled with the fact that there are holes in the firewall for it seem indicate a need to be able to remotely access the network. It would be far more secure to remove the VNC application and setup a VPN solution for access. Special care should be taken not to create more security holes due to the 'split horizon' vulnerability inherent in many VPN solutions.

2. Make sure all patches are up to date.

That **Beta1** versioning on the Sendmail server puts up a big red flag for me. I would also ensure that the DNS server is running the latest version and the Exchange and Web servers are fully patched.

3. Turn off all banners/version information.

There is no need to advertise the version of Sendmail, BIND or Web server you are running. I would advise either turning off the information or changing it to something that doesn't give any information away. Sure, it's security by obscurity, but why hand out information? Make the bad guys work for it.

4. Turn off Zone transfers in BIND.

If it is required to get the Zone information to a Secondary DNS server, only allow that server to request Zone transfers. DNS servers don't change IP addresses that often, so it would be worth adding another rule to the firewall for that specific server to do TCP DNS connections.

5. Double check the firewall rule sets.

Make sure that there are no extra holes in the firewall.

References

Cisco (Routers and PIX Firewall)..... www.cisco.com

Checkpoint (Firewall-1) ..... www.checkpoint.com

SANS..... www.sans.org

VISA Ten Commandments

http://www.visabrc.com/doc.phtml?2,64,932,932_cisp_download.html

Insecure.org..... www.insecure.org

tcpdump..... www.tcpdump.org

BIND and dig..... www.isc.org/products/BIND/

nmap ..... www.insecure.org/nmap/

SAINT ..... www.wwdsi.com/saint/

SARA ..... www.www-arc.com/sara/

sendmail (freeware) ..... www.sendmail.org

sendmail (commercial) ..... www.sendmail.com

VNC..... www.uk.research.att.com/vnc/