

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

SANS Global Incident Analysis Center

Firewall and Perimeter Protection Curriculum

Practical Assignment version 1.3

Network Security 2000
Monterey CA, October 15 - 19

© SANS Institute 2000 - 2002, Author retains full rights.

Submitted by:
Graham Bennett,

November 2000,

in partial fulfillment of the GCFW certification requirements.

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

Table of Contents

Overview 1
- Assignment 1
- Business Environment 1
- Enterprise Security Policies 2

Design 3
- Design (Assignment) Scope 4
- Business Interaction 4
  - Customers 4
  - Business Partners 4
  - Suppliers 4
  - Internal 4
  - Other 5
- Network 5
  - Perimeter 5
  - Firewalls 5
  - VPNs 5
  - Network Segmentation 5
  - Expansion and Growth 6
- Servers 6
  - OpenVMS Cluster 6
  - External Services 6
  - Internal Services 6
  - Console Consolidation 7
- Applications 7
  - Web Server 7
  - DNS Servers 7
  - Mail Servers 7
  - Maintenance 7
- Operations 8
  - Backups 8
  - Testing 8
  - Marketing & Training 8

Implementation 9
- Overview 9
- Network 9
- Hardware & Software 10
  - Router & Firewall 10
  - OpenVMS Servers 10
  - VPNs 11
  - Ethernet Connections 11
  - Home Systems 11
  - Business Partners 12
- Applications 12
  - Business Partner VPNs 12
  - Other Firewalls 12
  - Other considerations 12
- Network Implementation 12
  - 'Top Ten' exceptions 13
  - Enhancements 13
  - Configuration Tools 14

Audit 20
- Preparation & Planning 20

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

Process 20
Risks and considerations 21
Communication & Approvals 21
Construct & Collect Tools 21
Tool Choices 22
Data Collection & Reconnaissance 22
Timing 23
Cost Estimates 23
Security Assessment 24
Business Partners 24
Outer Perimeter 25
Back Doors 27
Windows 27
Doors 27
Inside 30
Analysis 31
General 31
Business Partners 31
Outer Perimeter 31
Back Doors 31
Router & Firewall 31
Servers 31
Inside 31
Recommendations 32
Business Partners 32
Outer Perimeter 32
Tools 32
Design 32
Appendices 33
Appendix A VISA Ten Commandments 33
Appendix B Base Security Policy 34
Appendix C References 35
Appendix D Resources 36
Appendix E OpenVMS Resources 37
Appendix F Firewall Script 38
Appendix H SARA Report 41

© SANS Institute 2000 - 2002, Author retains full rights.

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

Chapter

1

GIAC Enterprises
Security Architecture

Overview

Assignment

This research paper is written as one part of the SANS (System Administration, Networking, and Security Institute) GIAC (Global Incident Analysis Center) Firewall and Perimeter Protection Certification. The information contained herein represents a fictitious company "GIAC Enterprises" and a fictitious network implementation. The underlying business practices and methodologies are real and representative of some parts of the global IT community.

The design, site complexity and departmental interaction are representative of the experiences of the author, in managing a medium sized site within a medium to large organization. The intent has been to make this paper as realistic as possible, rather than the showing a 'shrink-wrapped' version that never applies directly to a real situation.

The intended audience for this paper is security and network professionals. Knowledge of networking and security terminology and theory is required. Knowledge of specific operating systems and network hardware is required for some parts of the discussion.

All network and site information is represented with the use of private IP addresses and fictitious domain names. This does make application of some of the security rules contradictory; just substitute your real addresses to make this apply within your target address space.

To reduce duplication of information, sources are referenced with hyperlinks or the resource material may be found in the appendices. The term DMZ is not used within this paper because no consistent definition is in common use.

The assignment is located on at: http://www.sans.org/NS2000/FPP_assignment.htm

All URLs were valid November 2000.

Business Environment

GIAC Enterprises was formed by the recent merger of two companies, both subsidiaries, of the umbrella multi-national corporation "Cards & Stuff International" (CSI).

The information systems within GIAC Enterprises consist of an OpenVMS Cluster for applications and server deployment with Microsoft desktops. The personnel use MS Windows, MS Office and MS Exchange as the office automation environment.

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

The parent, CSI, provides the network infrastructure, which consists of mostly Cisco equipment. The Internet connection consists of multiple high bandwidth links into an internal corporate network with a large address space. The corporate network provides a basic 'porous' filtering firewall at the Internet boundary and corporate VPN service. From a security perspective, parts of the corporate network are declared hostile. All business units are responsible for their own network security implementation with CSI providing the enterprise tools and analysis.

GIAC Enterprises is to function as a distinct Canadian business unit to allow the future expansion or sale as business markets dictate. The initial unit is small with the potential for rapid growth as regularly seen within E-Business enterprises.

Application Support, business-to-business links, and various consulting contracts are currently in place for the support of this enterprise.

Enterprise Security Policies

The following are extracts from the GIAC Enterprises' Security Policies and CSI Corporate Security Polices. The Security Architecture must implement these guidelines. They have been included here to provide a starting point for the assignment.

- As much as practical, within technology limitations, implement and maintain the VISA "Ten Commandments"[1] to ensure continued acceptance of customer credit cards and billing via VISA.
- Workstations and systems not within the protected network, if used for connections to systems within the protected network, are to install and maintain personal firewall software and virus scanning software.
- All hosts and servers are to display the standard user warning banner.
- Servers names may be based upon a theme or themes, they are not to be functional.
- Personal desktops are to be generically named.
- All electronic mail originating from, and destined to, users within the organization will be handled by corporate mail servers.
- All electronic mail may be subject to scanning.
- Network use policy applies to all employees and contractors using any GIAC Enterprises or CSI resources.
- OpenVMS password policy includes: minimum lengths, password history, dictionary of excluded words, and maximum period between changes.
- All network equipment installation requires prior approval. This includes routers, switches, firewalls, workstations, servers, modems, etc.

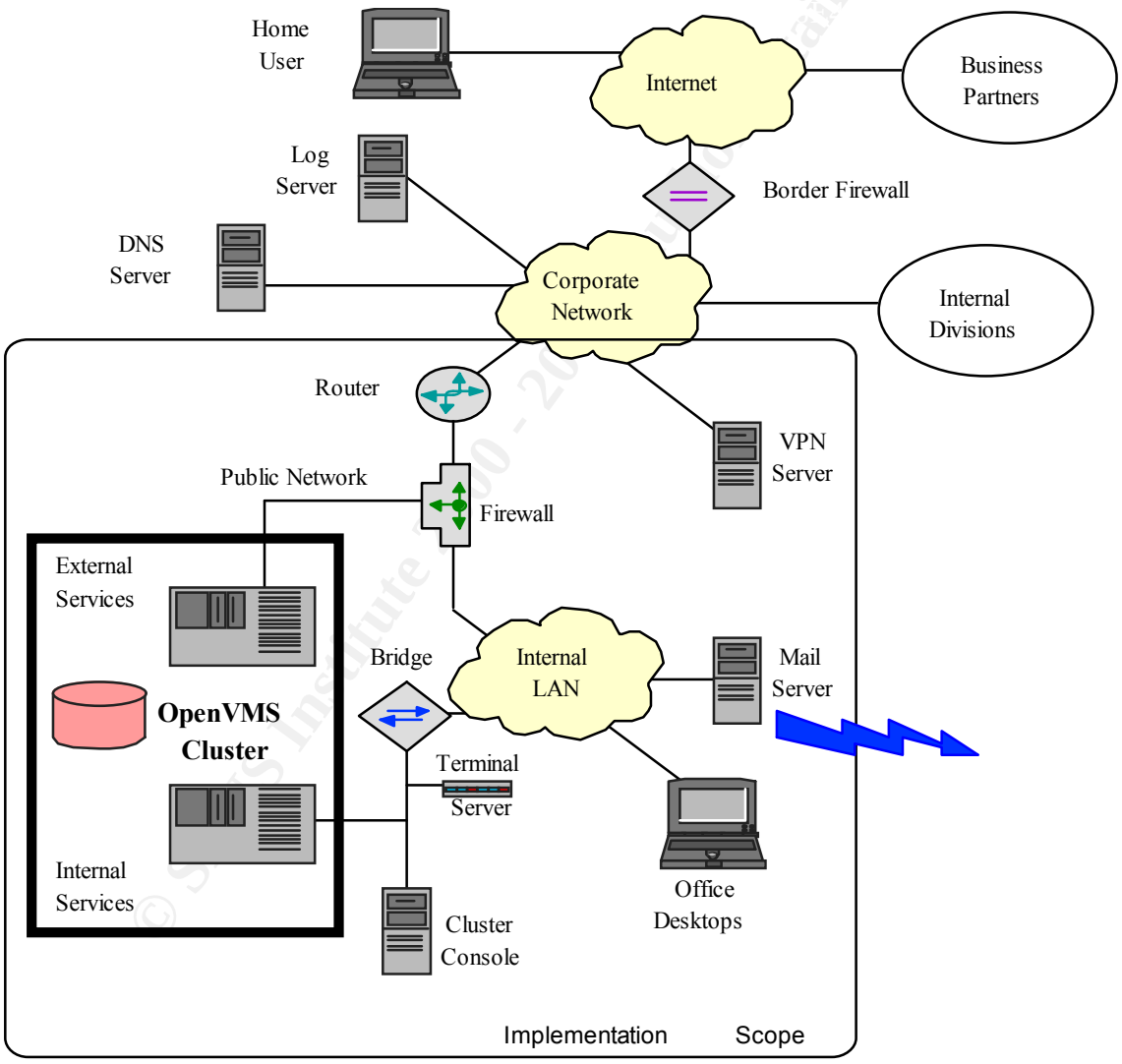
[1] Appendix A

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

Chapter
2

GIAC Enterprises
Security Architecture

Design



• Figure 1 Nework Overview

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

Design (Assignment) Scope

Figure 1 shows the context of the design described below. The description includes the design functionality required of the security architecture to implement the VISA "Ten Commandments"[2].

The emphasis is on the perimeter so does not go into application design specifics.

Provision is included for exception logging and forwarding to a central location. IDS design and sensor placement is not part of this paper.

Business Interaction

Customers

Customers have direct access via a single web interface for regular data polling and secure transactions for account actions. [HTTP (80/tcp) and SSL (443/tcp)] Names within the **giace.ca** domain are resolved by the GIAC Enterprises and CSI DNS Servers [DNS (53/udp)].

Electronic mail is provided by an external mail server.

Business Partners

An external contractor does application maintenance. They require interactive access to the OpenVMS Cluster to do database maintenance, software upgrades, file transfers of their new source, etc. [telnet (23/tcp), FTP (21/tcp), SSH (22/tcp)]

The corporate accounting systems (internal division) exchange data via a DECnet connection to their OpenVMS system. [DECnet-OSI over IP (ISO) (102,399/tcp)]

Suppliers

Static Company information and account status is available via the external web server. All other electronic interaction is via E-mail.

Internal

All of the Internal Divisions provide router data to the CSI Corporate log servers [syslog (514/udp)].

The CSI Corporate DNS Servers provide secondary domain server services [DNS (53/tcp,udp)] and maintain the VPN Server and services.

Contained within the CSI Corporate Network are labs and computer systems available to the public and educational groups. GIAC Enterprises considers these subnets hostile. Since they are within the corporate border firewall, the divisional implementation must take all precautions.

Within the Internal LAN, office functions are provided with Microsoft file servers, mail servers, management servers (SMS) and desktops. [NetBIOS (135/tcp,udp), (137/upd),

[2] Appendix A

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

(138/udp), (139/tcp), (445/tcp,udp); SMTP (25/tcp), SMS (1761/udp), (1762/upd), (7161/tcp)], MS Exchange Transport (135) then 2 random ports[3]]

For support of products and services internal desktops and the OpenVMS Cluster require FTP, Web, along with general access to external vendor sites.

Other

Some employees work from home. They require complete access to the Internal Services to do their day to day business.

Network

Perimeter

The router provides noise reduction and reduces the workload of the firewall.

The corporate policy explicitly restricts modems to only approved network requirements. No modems are to be connected to any desktops.

Firewalls

There are multiple firewall functions in use.

- Packet filter on the router as an initial line of defense;
- Stateful inspection firewall rules on the Firewall to restrict access to the public network as well as restrict access to the internal LAN;
- Packet filter on each host; and
- Personal Firewall on each system used by a home user that connects via the corporate VPN.

VPNs

- Dedicated VPN Server for multiple connections for home users and contractors. This provides Microsoft workstation to network secure sessions; and
- Host to Host SSH sessions for connections from business partners and systems that are unable to use the VPN Server implementation.

Network Segmentation

The internal LAN is implemented with switches to segment the local traffic and reduce the risk of data collection via sniffing.

A dedicated bridge creates a Trusted Local Network (TLN) specifically for the cluster, router, and firewall management traffic. This portion of the network is physically secured in the same room as the OpenVMS Cluster, router and firewall.

[3] http://support.microsoft.com/support/kb/articles/Q148/7/32.ASP

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

Expansion and Growth

The initial design and implementation must allow for rapid growth and 24x7 operation.

Using a subscription fee of $20/year, 1 connection per day per customer, and Marketing's estimate of $200 Million/annum gives us 10,000,000 connections per day. We are lucky our product is multi-lingual so that the connections are spread equally over the calendar day. The estimate yields an expected network load of 115 connections per second.

This design is intended as a starting point and will not be able to handle the complete growth. It is expected that the design can be easily migrated to a multi-router, multi-firewall load balancing configuration as the network load increases. There are a number of good GIAC papers covering this aspect of firewall and perimeter design[4] these can be used as a starting point when the migration is required.

Servers

OpenVMS Cluster

A two node OpenVMS CI Cluster provides the external services, internal services, and an application gateway in an environment that can grow to handle the expected loading without requiring a large increase in management effort.

The OpenVMS Cluster CI (computer interconnect) provides the communication between all nodes in the cluster on it's own wiring. The OpenVMS Cluster management environment allows applications to be maintained on one node and deployed by just placing the files in the location the application server is using on the other node. This environment also provides for direct application communication mechanisms outside of a network connection.

The CI Cluster was chosen over NI (network interconnect) because it provides better growth potential and doesn't put the LAVC protocol (Ethertype 0x6007) on the network wire. This way we don't have to deal with the bridging of LAVC.

For additional information on OpenVMS, a couple starting points are the Compaq OpenVMS home page[5] and the OpenVMS FAQ[6].

External Services

One OpenVMS Alpha host provides the external services (Mail, HTTP/HTTPS, DNS Master, DNS Forwarding). This server offers these services as four different addresses on the public network. This allows initial implementation on one node with additional nodes added only when the loading requires it. This node is limited to the server network processes only, no interactive logins are allowed.

Internal Services

The second OpenVMS Alpha host provides the internal services (Mail, DNS Internal lookups, FTP, telnet, SSH, DECnet/IP, Intranet WEB, Time, SMB).

General access to this host is provided as required for application maintenance, etc.

---

[4] http://www.sans.org/giactc/gcfw.htm
[5] http://www.openvms.compaq.com/
[6] http://www.openvms.compaq.com/wizard/openvms_faq.html

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

Console Consolidation

The OpenVMS Cluster Console provides monitoring, alarm and event notification, logging and access to the console of each node from one location. The serial console cables for the OpenVMS nodes, router and firewall are all connected to a LAT terminal server which then servers the ports to the cluster console application.

The LAT traffic is limited to the trusted local network.

Applications

Web Server

Provides customer product (the 'fortune cookies') via HTTP. Account access (via SSL or PKI) requires user specific accounts.

Customer data stored on-line is encrypted via a host based encryption product.

DNS Servers

The DNS External server provides the name and address resolution for the **giace.ca** sub-domain. A Secondary DNS server for this sub-domain is managed by the parent CSI network operations staff.

The split-split DNS configuration protects the internal DNS from poisoning and exploits. It is separate from the External server. The DNS Internal, caching only, server accepts requests from all of the Internal LAN and then forwards all unresolved (non-cached) requests to the DNS Forwarding (another caching only) server on the public network who does the resolution request.

This hides the internal DNS server because it never does any direct lookups.

Mail Servers

The External Mail server interacts with all external post offices. Any internal mail arrives here, is forwarded to the internal Mail server, which may re-write any addresses and then forwards to the mail server(s) on the Internal LAN.

There is no process communication between the two mail servers. The mail transfer is handled by a set of OpenVMS Batch Queues. Mail is sent through content and virus filters at this point.

The office mail server provides a FAX/E-Mail gateway for internal use. This removes the requirement for workstation attached modems to send FAXes. The office mail servers are running anti-virus software that matches their environment.

Maintenance

Product patch information is obtained via automated mechanisms (mailing lists, automated polling, etc.). The information is evaluated, tested and installed on a regular basis.

Workstation Anti-Virus software is configured to poll for updated virus signatures on a weekly basis and scan the local disks daily. If an active outbreak requires a new signature

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

file, e-mail notification is sent out to have the file manually down loaded. This configuration is required for home users as well.

Microsoft workstations run the Windows Critical Update Notification[7] program on a daily basis to ensure all critical patches are applied as they are released. This applies to home users as well.

Operations

Backups

The OpenVMS hosts are backed up to local tape drives with regular off site storage rotation.

The cluster console is backed up via DECnet to the internal OpenVMS host disk space, then to tape.

The internal LAN servers are backed up to the OpenVMS host using the host's SMB server, then to tape.

The firewall and router configurations are backed up to local media which is then secured with the off site storage rotation. The syslog entries are forwarded to the CSI Network Operations server for analysis and backup.

Testing

Software and configuration changes are implemented in a test environment not included in this design. (Separate from this network.)

This report includes the results of the first regular audit of the GEAC Enterprises' network security.

Marketing & Training

The security design will fail to be implemented if people using and maintaining the enterprise systems don't understand the design background and the need to keep their business secure.

With the many different groups conducting different types of business it is important to get agreement (buy in, etc.) on the basic principles and design. This is followed with training for technical staff and normal users about their use of the network and security tools (Virus Scanners, VPN Clients, Personal Firewalls, Router Upgrades & Maintenace, etc.). This aspect of the security design is not covered in this paper.

[7] http://windowsupdate.microsoft.com/

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

Chapter

3

GIAC Enterprises
Security Policy

Implementation

Overview

The base security policy[8] as recommended in **The Ten Most Critical Internet Security Threats[9] (Top Ten)** will require both additions and exceptions depending upon the network location and business functions required in our implementation.

Implementing the **Top Ten** has been covered by papers posted on the GIAC web site[10]. Additional specific instructions will be included here when they are specific to this design.

Creating firewall and router rule sets is technically difficult, hard to prove correct and error prone to maintain. Most companies do not have a network guru to rely on to do this, so it helps if we have tutorials and configuration tools. If we get the guru(s) to create a configuration tool and confirm that it functions correctly then we can trust the tool to do the basics we need.

I am an advocate of using configuration tools; they build in the dependencies, get the ordering right and don't create hard to troubleshoot typos the way I do. It is easier to proof the output script for functionality than try to find a miss-typed or placed rule. I've used a couple tools to ensure that my configurations do indeed implement what was intended by the design.

Network

Figure 2 provides the network addressing that is used in the implementation.

GIAC Enterprises uses real addresses in their implementation. All of the real names and addresses have been replaced by private addresses and dummy names for publishing of this assignment. I'm ignoring the inconsistency of applying Top Ten Rule #1 and having the packets actually get through.

As of November 2000 the domain **giace.ca** was not assigned. It is used in these examples for purely representational reasons.

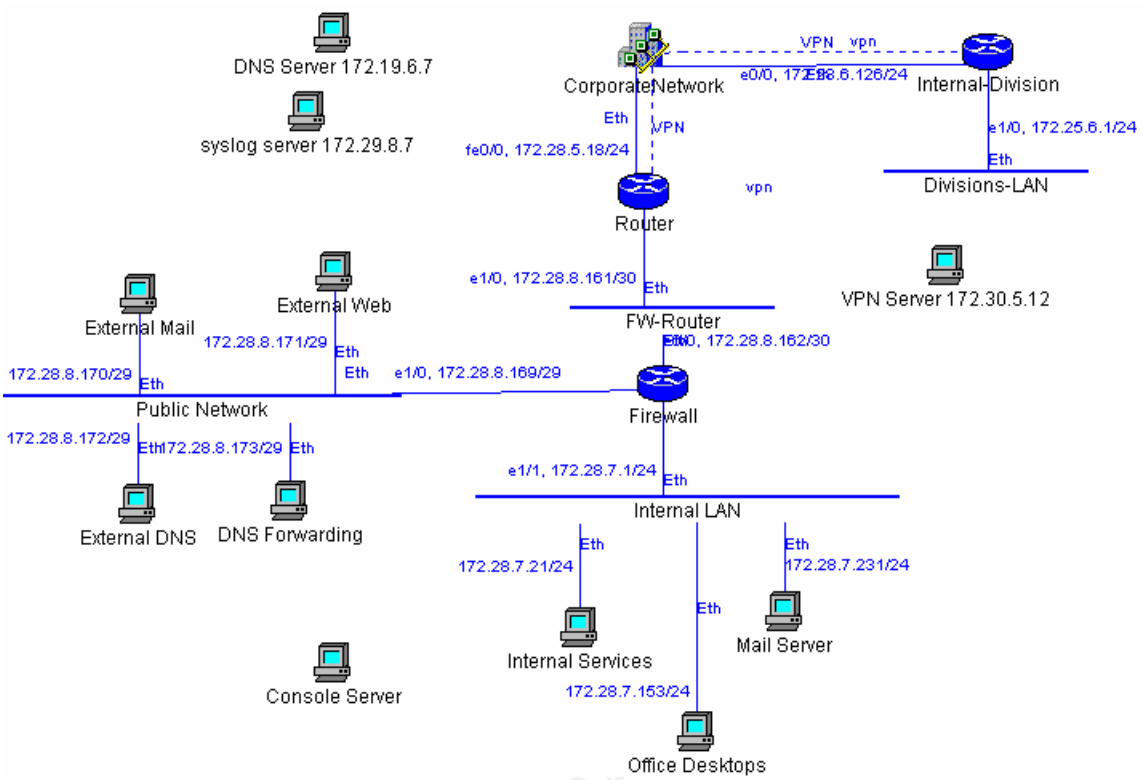
---

[8] Appendix B

[9] http://www.sans.org/topten.htm

[10] http://www.sans.org/giactc/gcfw.htm

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



• Figure 2 Network Addressing

Hardware & Software

Router & Firewall

- Router – Cisco 3620, IOS 12.1(3) T (minimum 12.1(1)T for SSH to router/firewall, if needed – we eliminated this need with a separate console system).

- Firewall – Cisco 2610, IOS 12.1(3) T (Minimum for 12.0(5)T for firewall feature set), IOS Firewall feature set[11].

This hardware provides component compatibility between the two models. The router is sized larger than necessary as the corporate network intends to share this between two divisions. The second connection is not currently scheduled, so we must implement this design and modify it later. The Cisco router line can grow to meet the load increases we expect.

The hardware matches that in use by the rest of the network and has a configuration tool that allows us to get this up and running in a short time.

OpenVMS Servers

- OpenVMS v7.2-1 on Alpha 2100 x2, E10/100 network, CI Adapters, disk controller, etc.

- Multinet v4.3a (Minimum for SSH and Bind 8.2.3 support)[12] or later. This includes Bind 8.2.3, SSHv1, Kerberos and Token Password systems.

[11] http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/index.shtml

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

- Compaq Secure Web Server v1.0 (Apache 1.3.12 with SSL)[13] or later
- PMDF v6.0 for OpenVMS[14] or later
- Console Server (Alpha DS10), DECnet only, no TCP/IP. So doesn't participate in the IP filtering rules. Uses a DECserver 200 (LAT Terminal Server) to consolidate the serial ports for all of the hosts, and network devices.

All of the OpenVMS applications will run without changes on faster, larger platforms as the growth dictates. Multinet supports interface pairing to allow multiple interfaces to use the same IP address – this will allow us to expand into multiple E100 interfaces for high bandwith and availability.

VPNs

- Cisco router to router VPN services.
- Nortel Contivity VPN[15] v2.6.1, managed by CSI Network Operations
- OpenVMS SSHv1 (included with MultiNet 4.3a)

Ethernet Connections

The Public Network and FW-Router Network both exist as a single cable. One direct cable between the Alpha 2100 and the Cisco 2610 Firewall and the other direct cable between the Cisco 2610 and Cisco 3620.

This makes it harder to add another device to each of these networks without being detected, even with physical access to the network devices. It also makes it harder for us to test from these segments.

Switches used within the Internal LAN must be chosen and tested for their resistance to exploitation. No switch model has been specified. Their management port for Out of Band (OOB) management would be included in the cluster console set of serial lines. The risks are well described in Aaron Turner's paper *Network Insecurity with Switches*.[16]

A dedicated bridge is used to separate the traffic from the OpenVMS Cluster-Console Server - Terminal Server from the rest of the Internal LAN. All of these components are co-located in the secure network cabinet within the OpenVMS Cluster area.

Home Systems

These aren't under our direct control. They do come under the overall policy, so need to be addressed within the evaluation because of the home user's VPN access to the network.

[12] http://www.process.com/tcpip/multinet.html
[13] http://www.openvms.compaq.com/openvms/products/ips/apache/csws.html
[14] http://www.process.com/tcpip/pmdf.html
[15] http://www.nortelnetworks.com/products/01/contivity/index.html
[16] http://www.sans.org/infosecFAQ/switch_security.htm

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

Business Partners

Again, not under our direct control. We must develop a policy that ensures that both sides maintain a minimum security level that matches our needs. This way neither one of us will be the point at which a break-in occurs and the launching point for an attack against the partner.

Applications

Business Partner VPNs

Cisco router to router VPN used to tunnel the DECnet/IP sessions to an internal division. This is required to secure the DECnet over IP traffic that would be in clear text otherwise. This can be used if external business partners have compatible HW & SW on their routers. This extends our perimeter out to the network on other end of the VPN. The business partner's security is now our own.

For workstation connections that require complete access to the Internal LAN the Contivity VPN clients are used and passed through without filters to the Internal LAN. This extends the perimeter we need to defend out to the home system. The home system must now have the same level of security protection we include for the Internal LAN.

The internal OpenVMS host accepts SSH sessions directly from external sources that are unable to use the other options implemented. This extends our perimeter out to the other host. The remote host's security is now part of our network at the level of access given to the user's account on our system.

Other Firewalls

Personal firewalls on each workstation such as Black Ice or AtGuard (no longer available, absorbed by another vendor's product line). Configured to deny by default and allow only those applications actually in use by the user.

Host packet filter (included as part of MultiNet) or ACLs on services. These are used to drop packets silently if they actually get through to the server or drop the packet and log the action to the server's logs for monitoring.

Other considerations

In addition to the normal parts of the design that we consider included in the network security there are application configuration issues that may have a direct impact on the network itself.

If the mail server is not configured to implement all of the recommendations of the e-mail community (relay, spam, etc.) then your server may be added to one or more of the mail black lists. Once your server is on these lists, other servers will reject connections from you. The mail service is down and there is nothing detectable within the network or IDS that will show this, other than the mail server logs.

Network Implementation

The SANS GIAC FW papers and reading room cover the implementation syntax and testing methodology for the Cisco routers and firewalls very well. Please read through some of these for the background.

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

The following configuration tools were used to implement the security policy. As with any tools they have their strengths and weaknesses. All of the initial source output was tested and validated to ensure the tool actually provided what we needed, then we could work with these in a maintenance phase.

- Cisco ConfigMaker v2.4[17]
- Linux Firewall Design Tool (ipchains or ipfw)[18]
- Personal Firewall (AtGuard v3.1)
- OpenVMS Utilities

'Top Ten' exceptions

1) SSH (22/tcp) will allowed through to the Internal OpenVMS host from all addresses. Some of the users of this service are on DHCP clients, we could manage a range of addresses or just allow all access and let the host security handle the connection. We have implemented the later choice.

2) Syslog (514/udp) is allowed through from the firewall and any routers on the internal network to the corporate server.

3) All connections are allowed from the VPN LAN (172.30.5.0/24) to the Internal LAN. We are trusting the management of the VPN LAN, it's security and the security of the intervening network routers.

4) Allow customers and network operations to ping and traceroute to the external servers as a 'nice' network neighbour. We explicitly remove ICMP replies returning to these systems to avoid a DoS attack.

Enhancements

1) SMS ports (1761/udp, 1762/udp, 7161/tcp) are blocked to protect our internal systems from scanning and possible DoS. The danger of a scan to these services is outlined in Robert Shimonski's article *SATAN: Dancing with the Devil and Wreaking Havoc in an NT Environment*.[19]

2) For the Public Network all connections are blocked except for connections destined to or coming from the four addresses and three services defined for this network. This locks down our services and will allow logging of any exceptions.

3) No DNS (53/udp) is allowed out of the Internal LAN other than the one connection from the DNSinternal to the DNSforwarding server. The removes the 53/udp scan and reduces the possibility of DNS poisoning causing problems with outbound connections.

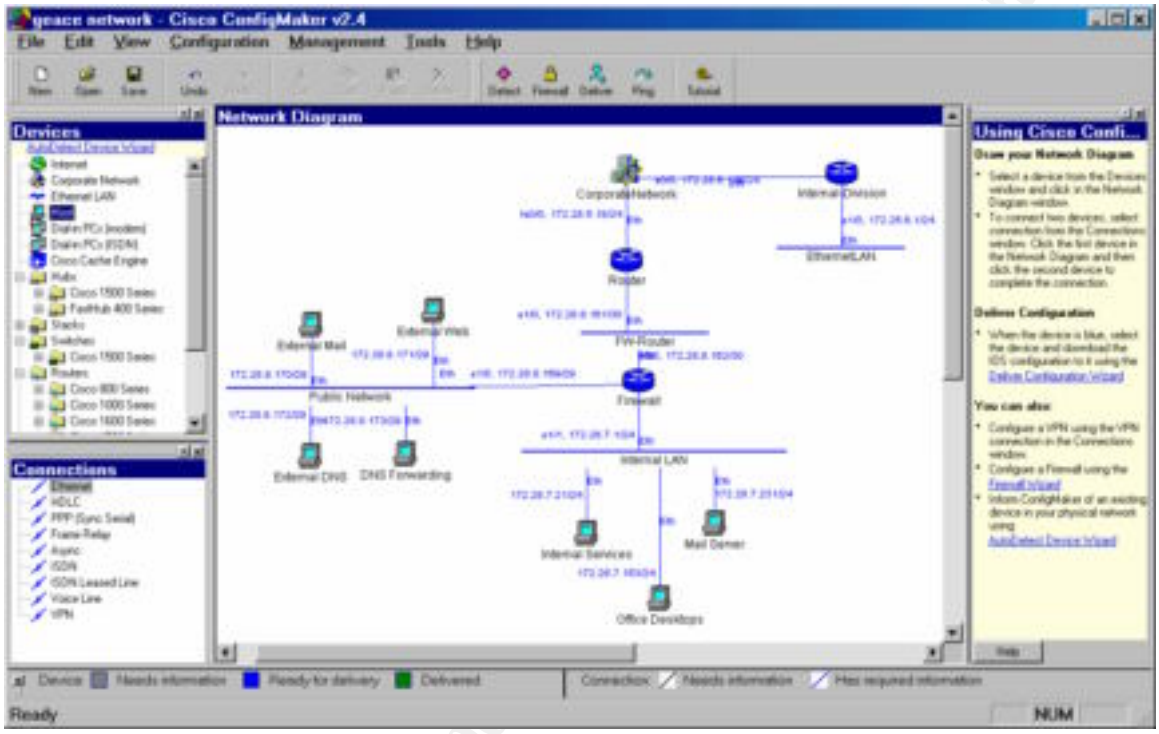
[17] http://www.cisco.com/warp/public/cc/pd/nemnsw/cm/index.shtml
[18] http://www.linux-firewall-tools.com/linux/firewall/index.html
[19] http://www.sans.org/infosecFAQ/SATAN.htm

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

Configuration Tools

Cisco ConfigMaker

Figure 2 was created with ConfigMaker. The application design window is shown in Figure 3



• Figure 3 ConfigMaker Design Window

The process used to create the network implementation scripts is:

1) Register and Download[20], install and go through the *Getting Started Tutorial*

2) Edit Network Properties to have all devices created with your policy defaults

- Create MOTD (message of the day) Banner (Standard Restricted Access wording for your organization).
- Change VTY devices = 0 to disable network access to the console
- change default passwords, remove SNMP or change defaults

3) Device wizards

- create device
- disable defaults (SNMP public – or disable)

[20] http://www.cisco.com/warp/public/cc/pd/nemnsw/cm/index.shtml

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

- Add location information for administration
- disable network access to console (Number of telnet sessions allowed = 0)

4) Add all other devices, network connections, and servers

5) Add Ethernet LANs WANs, etc.

- Connect devices
- Automatically goes through addressing wizard using an IP Subnet Calculator for VLSN (cool).

6) Run Firewall Wizard

- Once for router with VPN connection
- Remove router from diagram and run firewall wizard for the firewall

7) Modify scripts manually to include the basic Top Ten policy as described by Scott Winters' *Top Ten Blocking Recommendations Using Cisco ACLs*[21] article.

8) Change passwords prior to downloading to the device.

9) Secure the PC and any backups of the configurations! It would be really uncool to have this PC just walk out of the office.

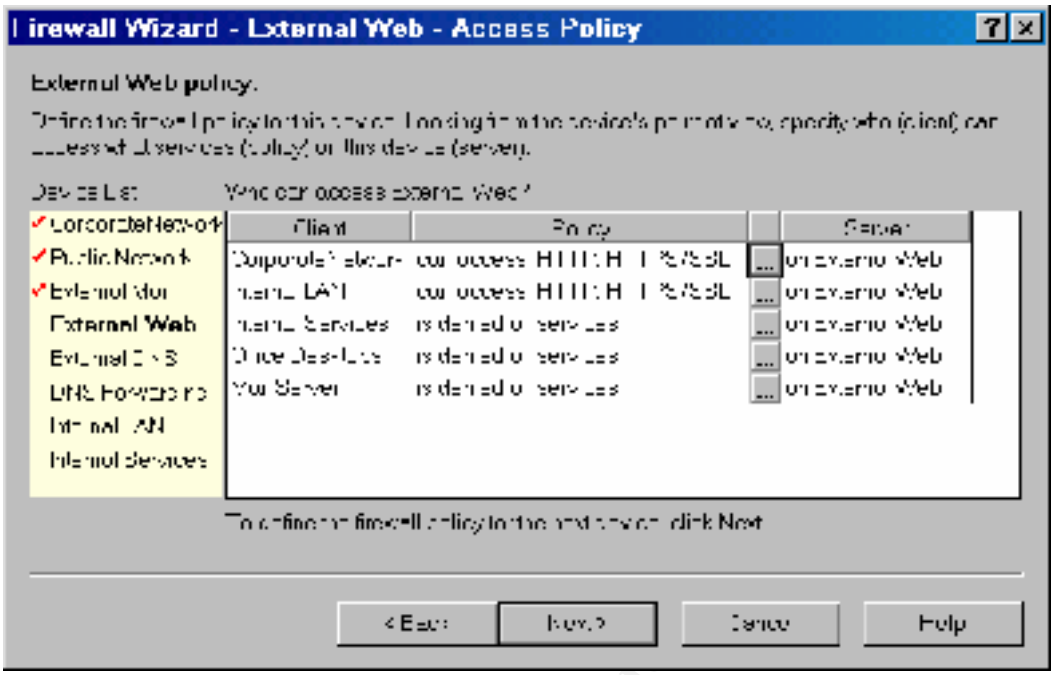
Comments:

- Go through all the tabs on each option. They handle the setup nicely, just don't miss something you may need.
- The password fields are blanked in one option and then in plain text in the script. I changed these just before sending them to the device (by pasting into a terminal session).
- The firewall wizard and VPN connection will only work on the device connected to the external network. This required use of two diagrams to get the multiple rules for our Defense In-Depth security policy.
- The configuration options match a view of firewall policy implementation that is overly restrictive when attempting to implement something outside of the tool.
- The configuration scripts produced are in Appendix F Firewall Script, these must be extensively modified to include the basic policy.

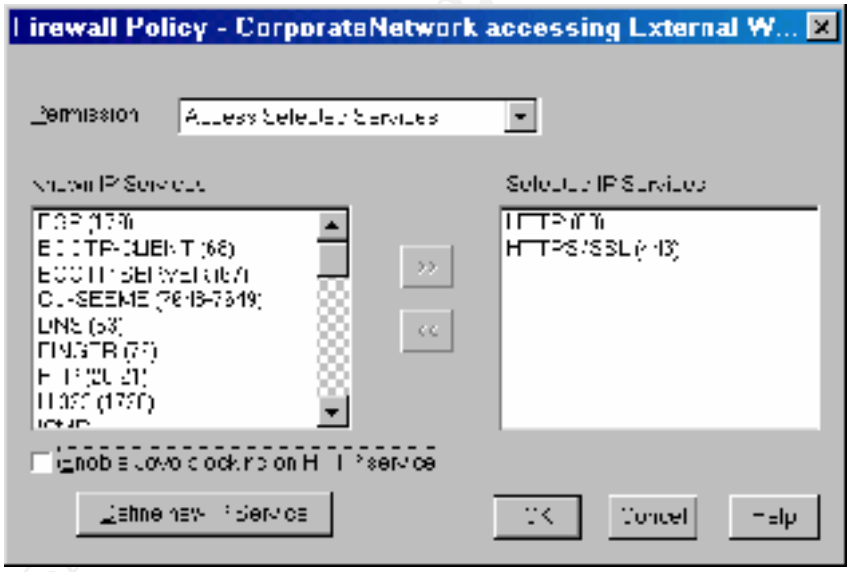
Samples of the Firewall Wizard configuration screens follow.

[21] http://www.sans.org/infosecFAQ/blocking_cisco.htm

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



- Figure 4 Firewall Wizard Example 1



- Figure 5 Firewall Wizard Example 2

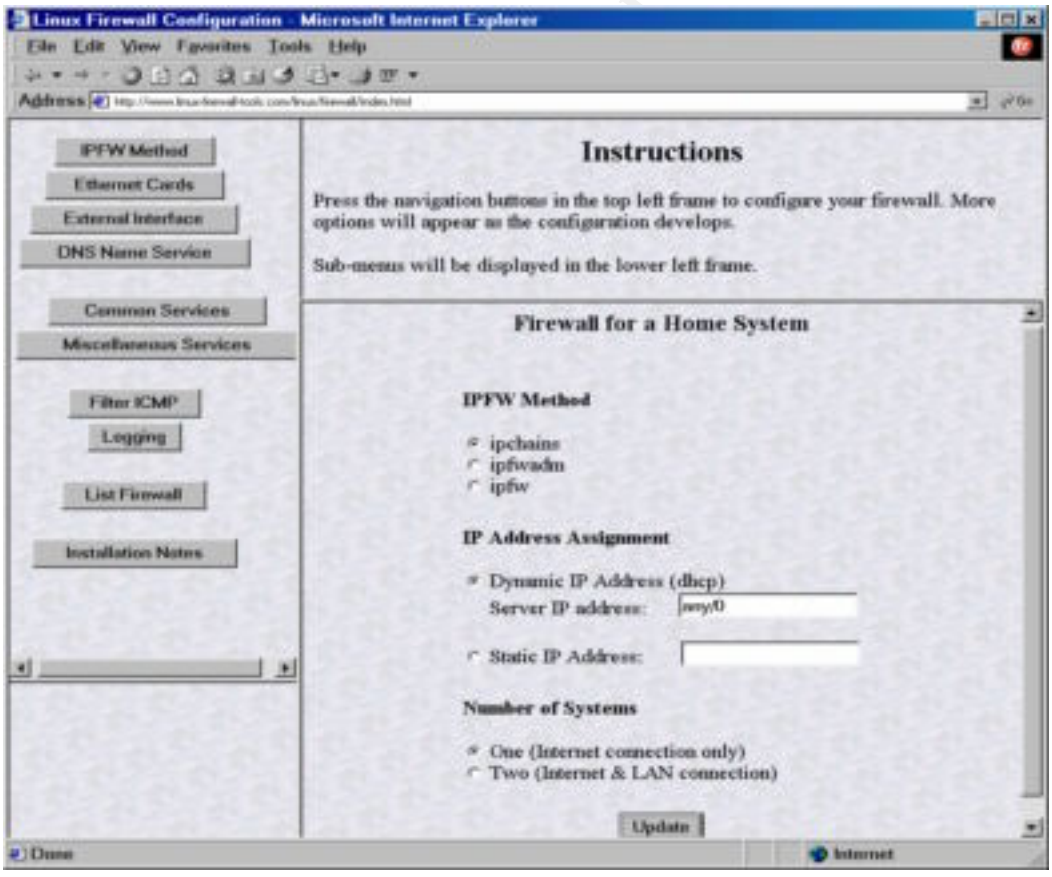
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Linux Firewall Design Tool (ipchains or ipfw)[22]

The design tool that Robert L. Ziegler has provided on his web site is the only reason I was comfortable attempting to work on a UNIX (Linux) scanner platform when my last UNIX command was typed in 18 years ago. This tool allowed the rapid creation of an ipchains ruleset that will protect the network scanner platform from attacks when it is being used to audit the network. It was also comforting to have this in place as the tools were being developed and evaluated using a system connected to a cable modem.

The tool is self-explanatory and includes installation information. Step through the configuration adding your network information along the way and you end up with a script that can be copied to the appropriate file on your Linux installation. They have included instructions on how the incorporate this on the system with a DHCP client or other options.

All of the basic SANS recommendations are included. They provide a well commented script that is customized based up your input into the web interface. This will provide both single user workstation and LAN Router configurations. I didn't include the 14 pages of script – create a copy for your use from the URL reference; it's worth trying the tool.



• Figure 6 Linux Firewall Configuration

[22] http://www.linux-firewall-tools.com/linux/firewall/index.html

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

Personal Firewalls

With the AtGuard v3.1 personal firewall, it was configured by using it's learn mode. Start it up, enter learn mode, and then attempt to use every application you have that uses the network interfaces.

This gets a set of rules in place, they aren't necessarily optimal, if you start with the deny everything first you get a useful set. This does have limitations, when you add a new application it will not work until you reconfigure the firewall for it (a normal FW management issue that workstation users aren't used to).

The VPN Client needs to be added to allow connection to the corporate resources only by way of the client.

OpenVMS Configuration

The MultiNet product includes options for:

- Psuedo Addresses – this puts more than one IP address on an interface and allows us to use one node to start and split the servers if we need to later.

```
$ multinet configure /network ! External Services
MultiNet Network Configuration Utility V4.3(103)
[Reading in MAXIMUM configuration from MULTINET:MULTINET.EXE]
[Reading in configuration from MULTINET:NETWORK_DEVICES.CONFIGURATION]
NET-CONFIG>show
Interface                              Adapter     CSR Address    Flags/Vector
---------                              -------     -----------    ------------
se0      (Shared VMS Ethernet/FDDI)       -NONE-        -NONE-       -NONE-
          [TCP/IP: 172.28.8.170, IP-SubNet: 255.255.255.248]
          [VMS Device: EWA0, Link Level: Ethernet]
pd0      (Secondary Ethernet Address)     -NONE-        -NONE-       -NONE-
          [TCP/IP: 172.28.8.171, IP-SubNet: 255.255.255.248]
          [Hardware-Device: se0]
pd1      (Secondary Ethernet Address)     -NONE-        -NONE-       -NONE-
          [TCP/IP: 172.28.8.172, IP-SubNet: 255.255.255.248]
          [Hardware-Device: se0]
pd2      (Secondary Ethernet Address)     -NONE-        -NONE-       -NONE-
          [TCP/IP: 172.28.8.173, IP-SubNet: 255.255.255.248]
          [Hardware-Device: se0]
```

© SANS Institute 2000 - 2002 Author retains full rights.

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

- Host based packet filter – to reinforce the filters on the routers. This will drop without logging.

```
! External Services multinet:filter-se0.dat
! implicit Deny at end
!
! format <action> <proto> <source ip> <mask> <dest ip> <mask> <rel op> ...
!
! allow access to mail server
permit tcp 0 0 172.28.8.170 255.255.255.248 eq 25
! allow access to web server
permit tcp 0 0 172.28.8.171 255.255.255.248 eq 80
permit tcp 0 0 172.28.8.171 255.255.255.248 eq 443
! allow access to DNS server for lookups
permit udp 0 0 172.28.8.172 255.255.255.248 eq 443
! allow zone transfers to secondary bind server
permit ip 172.19.6.7 255.255.255.0 172.28.8.173 255.255.255.248 eq 53
! allow forwarding access from internal bind server
permit udp 172.28.7.21 255.255.255.0 172.28.8.173 255.255.255.248 eq 53
!
! implicit deny 0 0 0 0
```

- ACLs on each service (port) – to reinforce the filters on the routers. We have the option to log the rejects or accepts based upon network or host specific addressing.

```
$ multinet configure /services ! Internal Services
MultiNet Server Configuration Utility V4.3(42)
[Reading in configuration from MULTINET:SERVICES.MASTER_SERVER]
SERVER-CONFIG>show telnet  /full
Service "TELNET":
        TCP socket (AF_INET,SOCK_STREAM), Port 23
        Socket Options = SO_KEEPALIVE
        INIT() = Merge_Image
        LISTEN() = TCP_Listen
        CONNECTED() = TCP_Connected
        SERVICE() = Internal_Telnet
        Program = "MULTINET:LOADABLE_KERBEROS_TELNET"
        Accept Nets = IP-172.28.7.0, IP-172.30.5.0, IP-172.25.6.0
        Log File for Accepts & Rejects = MULTINET_INCOMING_LOG
        Parameters = "include-authentication-indication"
                     "include-port-number"
```

© SANS Institute 2000 - 2002, Author retains full rights.

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

Chapter

4

GIAC Enterprises
Security Audit

Audit

Preparation & Planning

We must keep in mind that this is an audit and not a penetration test or attack against our network.

The advantage of this is that we can start with all the existing knowledge about our network. This saves us the 'dumpster diving', news searching and other reconnaissance that is done as a hacker's first step. The reconnaissance should be done to get a complete idea of how much information is being given away – this needs it's own set of tools, or a lot of manual effort and is not included in this paper. Eric Schultze and George Kurtz have a good set of ideas and areas to cover in their presentation *Hacking Exposed: LIVE!* given at the SANS Network Security 2000 Conference.

We are conducting an assessment against a network and working systems that are critical to our business functions. Any interruption or damage to systems would be very poorly received.

Process

1) Obtain approval for the audit

2) Plan the audit

3) Construct, collect and build the tools needed for the audit

4) Collect the configuration data needed to pre-configure the tools and evaluate the defenses

5) Update the audit plans

6) Communicate the audit intents, time line and obtain approvals as necessary

7) Conduct the security assessment

8) Analyze the findings

9) Communicate the results.

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

Risks and considerations

- Just scanning the network may cause problems with older versions of software. System crashes, CPU bound DoS (Windows), etc. would disrupt the service.
- Interrupting the network to add a scanner will cause the existing services to be disrupted causing loss of business.
- Ignoring activity while the assessment is being done may allow an intruder to piggyback their attack during your scans.
- You must be able to stop the assessment immediately and turn activity over the Incident Handling team if an attack is detected during the assessment.
- Publishing of this report is another source of information for an attacker to use.
- The assessment must stay within the approved boundaries for both political and potentially legal reasons.
- Legal requirements, such as regulations covering automated telephone dialing, may preclude the use of a tool or restrict it's use.
- All 'interested' parties need to be aware of and possibly approve the activity.
- Will a 'bad report' have career implications to anyone?
- The system and network administrators within this division have no recent UNIX skills.

Communication & Approvals

General approval to conduct the audit was received. Each division and external business partner replied that they would not support any assessment of their site or installations. They all did want a copy of the final report.

The network operations will permit the scanner to be connected on a segment adjacent to the Router (172.28.5.18).

The NT Server and Mail Server group would not permit complete assessment of Windows desktops, NT Servers or Mail servers. They were concerned that there were still vulnerable systems within the Internal LAN. A ping scan would be permitted and the mapping information would be appreciated.

The OpenVMS application developers would allow a vulnerability assessment and appreciate the report information. They would conduct their own application evaluation.

Construct & Collect Tools

A scanning platform constructed using a Portable PC configured as a dual boot (Windows/Linux), with built-in modem. The Linux installation was built from Red Hat v6.0, all of the patches applied, hardened using the SANS guide *Securing Linux: Step-By-Step*, ipchains rule set from the Linux Firewall Design Tool web interface. The Windows installation used a VPN client, the AtGuard personal firewall, with NetBIOS bindings removed from the ethernet NIC.

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

Scanning tools: including SARA, Firewalk, nmap, Sam Spade, THC-scan and the normal network tools included with the operating systems.

Tool Choices

The tool set for this assessment needs to address these functions:

- Gather general information about the environment.
- Evaluate the 'holes' or allowed and rejected paths through the defensive system.
- Evaluate the host vulnerability from external attacks.
- Evaluate the applications for attack from data corruption and manipulation.

For general gathering of DNS information, I've been using Sam Spade for Windows. It combines the DNS lookup and reference tools in a nice easy to use package.

For NEWS and web crawling there are a number of general tools for on-line and off-line searching including Sam Spade.

To check for back door modems by scanning blocks of telephone numbers; THC-scan provides a DOS based tool that works in Windows.

I went with the Security Auditor's Research Assistant (SARA) vulnerability scanner for this assessment. The tool was well received at a SANS BoF, has an easy to use web interface, CVEs for future incorporation in an IDS, and is approved by SANS to cover the Top Ten. I didn't have time to look at Nessus, which is very well received in the community.

To confirm the firewall configuration Firewalk was chosen for it's specific approach.

Nmap covers the basics, and is discussed in the referenced papers for it's use to evaluate the implementation of the base security policy.

Tools to use for evaluation of WEB applications (Achilles[23] and SSL-Proxy[24]) weren't explored. Information about them was passed to the application support personnel.

Data Collection & Reconnaissance

We obtain a current copy of the Security Policy to determine if it has been implemented.

The site configuration documentation provided the network diagrams, system configuration, and network addresses for the initial scanner configuration.

The office telephone list provided the block of telephone numbers that the division uses.

The application support group has provided the weekly server loading graphs and operational schedules.

[23] http://www.digizen-security.com/
[24] http://www.csnc.ch/index_e.html

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

Timing

For the telephone scan, we want to do this when it will least disturb the office. The workstations are managed with Microsoft SMS so are normally on overnight. This means that we can reasonably expect systems with modems to be on at night and calling each number in the office won't bother anyone at that time. Therefore, the telephone scan will be done after regular work hours.

For the network assessment we would like to do this when people are available, incase we do inadvertently create some problems, and when systems will be least affected. Conducting this on a long weekend would probably collide with increased hacker activity so a normal time is preferred. Based upon the weekly server loading, Tuesday afternoons are lightly loaded so any scans that create significant network or host loading would be done during this time. The added advantage is we have the server support team available without incurring overtime costs.

During the assessment, the scanning tools will be configured to reduce the host and network load to a reasonable amount. They don't need to be set at a 'stealth' level since that would increase the amount of time we need to do the work. This may also remove the connections from the host or router logs so we couldn't confirm all levels of the security.

Cost Estimates

- Construct scanning platform, collect tools, and learn them. For an OpenVMS analyst with no recent UNIX experience: 4 weeks ($10,500)

- Reconnaissance and external information evaluation. Manually over a week ($2,625). I would confirm this estimate with one of the security firms that conduct penetration testing on a regular basis. The time would be reduced when tools have been built, or collected, to automate as much of the process as possible.

- Conduct telephone scan. TCH-scan should handle about 100 #s/hour. 1 day ($525)

- Conduct perimeter assessment. For a small sized LAN, spread over 2 days ($1,050). This is an explicitly targeted scan, a general scan to blanket a large network could take weeks of running.

- Analyze data, administrative overhead, and document results. 3 days ($1,575).

Estimated total for first scan: $16,275. Estimated cost (excluding maintenance) for additional regular scan only assessments: (8 days) $3,675. This is based upon an analyst cost of $525/day.

© SANS Institute 2000 - 2002 Author retains full rights.

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

Security Assessment

Generally, I look at the assessment in the way that someone would approach breaking into a large building site. Walk around the fence to see if anything is open or unlocked. Look at other delivery vans, can I get a lift in with them. Look through the windows, is there another way in showing through? Knock on the windows and doors; give them a tug. Check the front door, can I walk in carrying a clipboard, listen at a door? Can I pay someone on the inside to do my work?

Therefore, what we will do is:

1) Check for other ways in – business partners

2) Check the outer fence – home users

3) Check for back doors – modem scan

4) Check the windows – find the paths through the firewall

5) Tap on the windows and touch the doors – scan each server, gently

6) Inside - Scan from the inside

7) Inside - Host and application check

Business Partners

They are excluded from an active assessment. The results of their past assessment(s) will need to be evaluated to determine what our risk may be.

© SANS Institute 2000 - 2002, Author retains full rights.

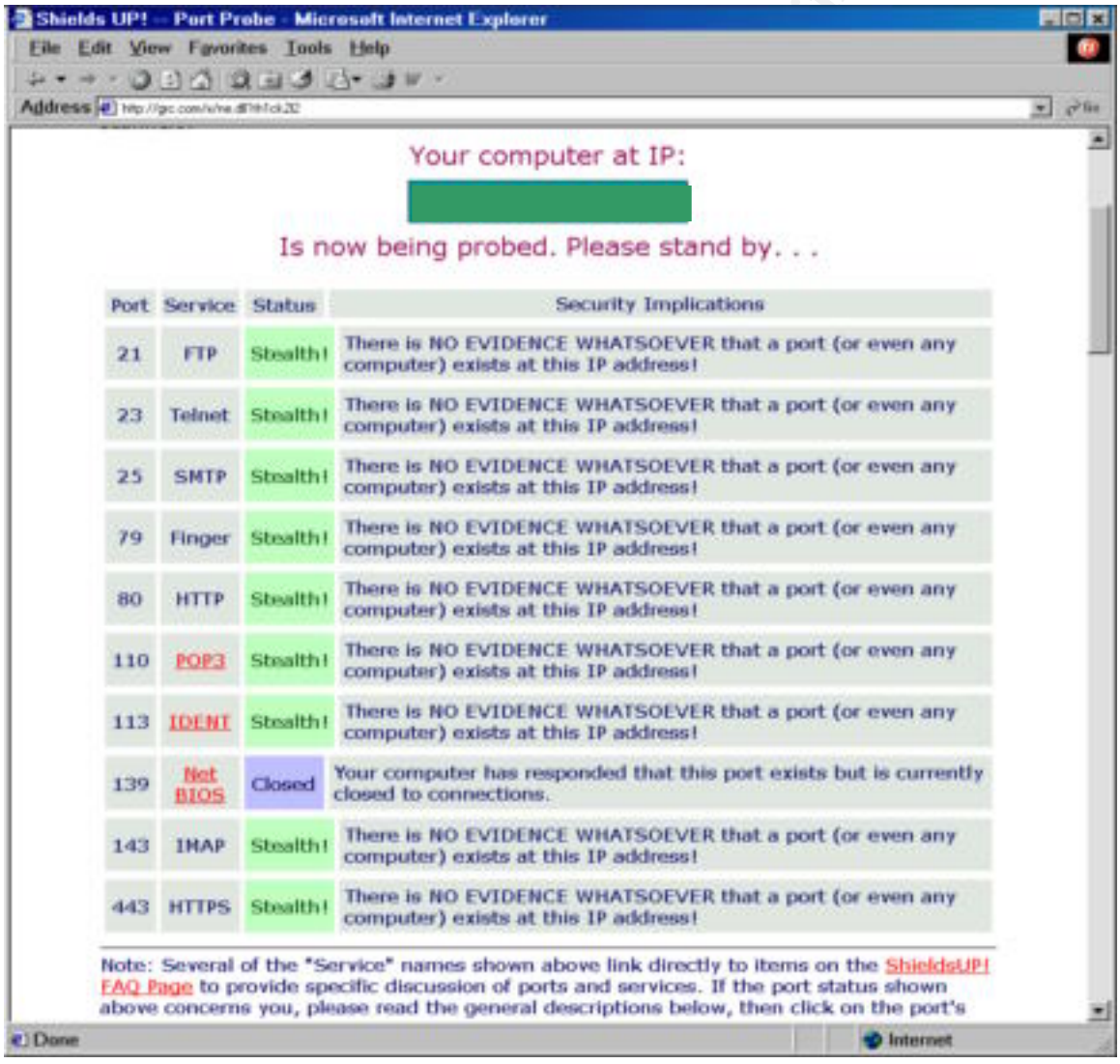
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Outer Perimeter

To check the home systems the use of the **Shields UP!** web site[25] to do the scan was adopted. The results were then forwarded via e-mail to the analyst. This allows each home user to see the results and read the background on the GRC site as a learning/training experience.

The Shields UP! scan needs to be done twice, once with the workstation in it's normal configuration and then once with the VPN in place using the DHCP address supplied from the VPN LAN. This tests the workstation defenses and the VPN defenses on our outer perimeter.

The Shields UP! web site loads a small Windows application (to confirm the local IP address) and does two types of scan – a Windows specific NetBIOS scan and a small port scan. The port scan results of one system are shown in Figure 7.



• Figure 7 Shields UP! Scan Results

[25] http://www.grc.com/

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

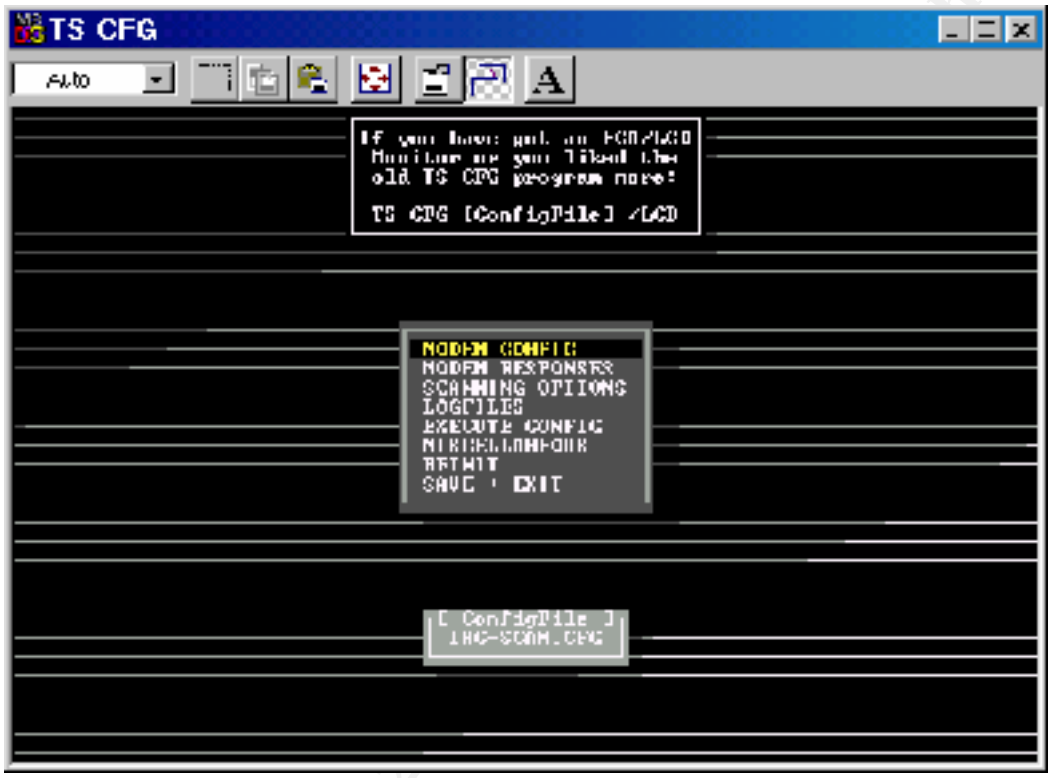
The AtGuard firewall log shows these entries during the port scan:

Firewall Event Log (Entries repeated x times are shown with *[x]* MM/DD/YY)
[4] 11/18/00 16:16:07.787 Rule "Implicit block rule" blocked (*scanner.cable.network*,https). Details:
Inbound TCP connection
Local address,service is (*scanner.cable.network*,https)
Remote address,service is (*xxx.grc.ip.xxx*,4553)
[4] 11/18/00 16:15:18.674 Rule "Implicit block rule" blocked (*scanner.cable.network*,imap). Details:
Inbound TCP connection
Local address,service is (*scanner.cable.network*,imap)
Remote address,service is (*xxx.grc.ip.xxx*,4325)
[4] 11/18/00 16:14:55.708 Rule "Default Inbound NetBIOS Sessions" blocked (*scanner.cable.network*,nbsession). Details:
Inbound TCP connection
Local address,service is (*scanner.cable.network*,nbsession)
Remote address,service is (*xxx.grc.ip.xxx*,4315)
[4] 11/18/00 16:14:27.812 Rule "Implicit block rule" blocked (*scanner.cable.network*,auth). Details:
Inbound TCP connection
Local address,service is (*scanner.cable.network*,auth)
Remote address,service is (*xxx.grc.ip.xxx*,4091)
[4] 11/18/00 16:13:38.589 Rule "Implicit block rule" blocked (*scanner.cable.network*,pop3). Details:
Inbound TCP connection
Local address,service is (*scanner.cable.network*,pop3)
Remote address,service is (*xxx.grc.ip.xxx*,3863)
11/18/00 16:12:49.367 Rule "Implicit block rule" blocked (*scanner.cable.network*,http). Details:
Inbound TCP connection
Local address,service is (*scanner.cable.network*,http)
Remote address,service is (*xxx.grc.ip.xxx*,3638)
[4] 11/18/00 16:12:37.658 Rule "Default Inbound NetBIOS" blocked (*scanner.cable.network*,nbname). Details:
Inbound UDP packet
Local address,service is (*scanner.cable.network*,nbname)
Remote address,service is (xxx.cable.address.xxx,1024)
11/18/00 16:12:36.239 Rule "Implicit block rule" blocked (*scanner.cable.network*,http). Details:
Inbound TCP connection
Local address,service is (*scanner.cable.network*,http)
Remote address,service is (*xxx.grc.ip.xxx*,3638)
[5] 11/18/00 16:12:35.239 Rule "Default Inbound NetBIOS" blocked (*scanner.cable.network*,nbname). Details:
Inbound UDP packet
Local address,service is (*scanner.cable.network*,nbname)
Remote address,service is (xxx.cable.address.xxx,1024)
[2] 11/18/00 16:12:29.680 Rule "Implicit block rule" blocked (*scanner.cable.network*,http). Details:
Inbound TCP connection
Local address,service is (*scanner.cable.network*,http)
Remote address,service is (*xxx.grc.ip.xxx*,3638)
[4] 11/18/00 16:12:00.144 Rule "Implicit block rule" blocked (*scanner.cable.network*,finger). Details:
Inbound TCP connection
Local address,service is (*scanner.cable.network*,finger)
Remote address,service is (*xxx.grc.ip.xxx*,3430)
[2] 11/18/00 16:11:10.922 Rule "Implicit block rule" blocked (*scanner.cable.network*,smtp). Details:
Inbound TCP connection
Local address,service is (*scanner.cable.network*,smtp)
Remote address,service is (*xxx.grc.ip.xxx*,3188)
[4] 11/18/00 16:09:32.476 Rule "Inbound TCP service: ftp" blocked (*scanner.cable.network*,ftp). Details:
Inbound TCP connection
Local address,service is (*scanner.cable.network*,ftp)
Remote address,service is (*xxx.grc.ip.xxx*,2820)

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

Back Doors

Configure THC-scan with TS-cfg to exclude the Support Hot Line telephone number, the block to use and then run THC-scan.exe in a DOS Window. The documentation with the kit shows the options available. This scan requires the operator running the utility to mark each number based upon what is heard on the line.



• Figure 8 TS-cfg Menu

The scan for modems within the telephone number block for the office got two hits. Both of these were on the telephone list: the office FAX machine and the mail server's FAX gateway number.

Windows

Use Firewalk to check what will pass through the multiple firewalls into the Public Network because we are allowing ICMP messages to be returned from that segment.

This utility needs the closed router's address to the firewall and an address on the other side of the firewall.

To test connections into the Public Network use each of the server addresses in turn and the router's external address 172.28.5.18 as the starting point.

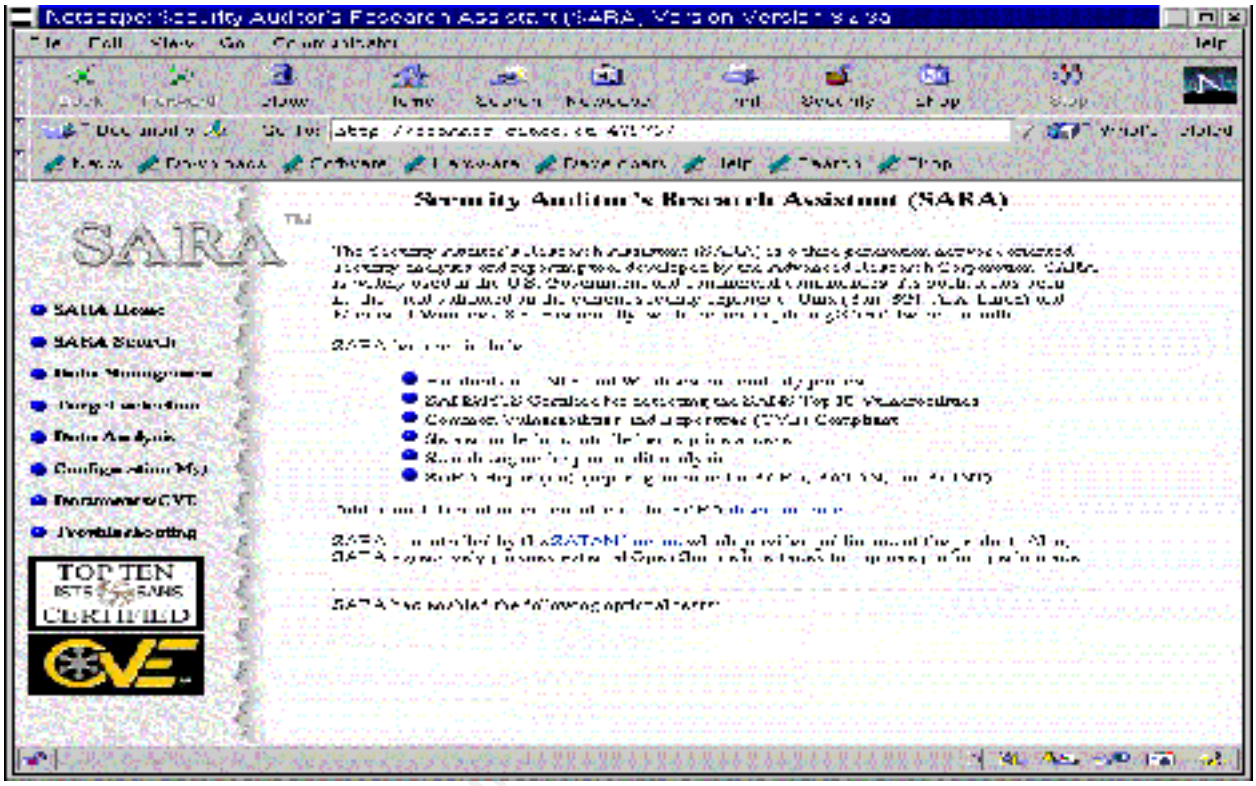
To test the lower numbered ports the scanner must as close to the starting point as possible.

Doors

Use SARA to evaluate each host for common vulnerabilities that are not yet patched.

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

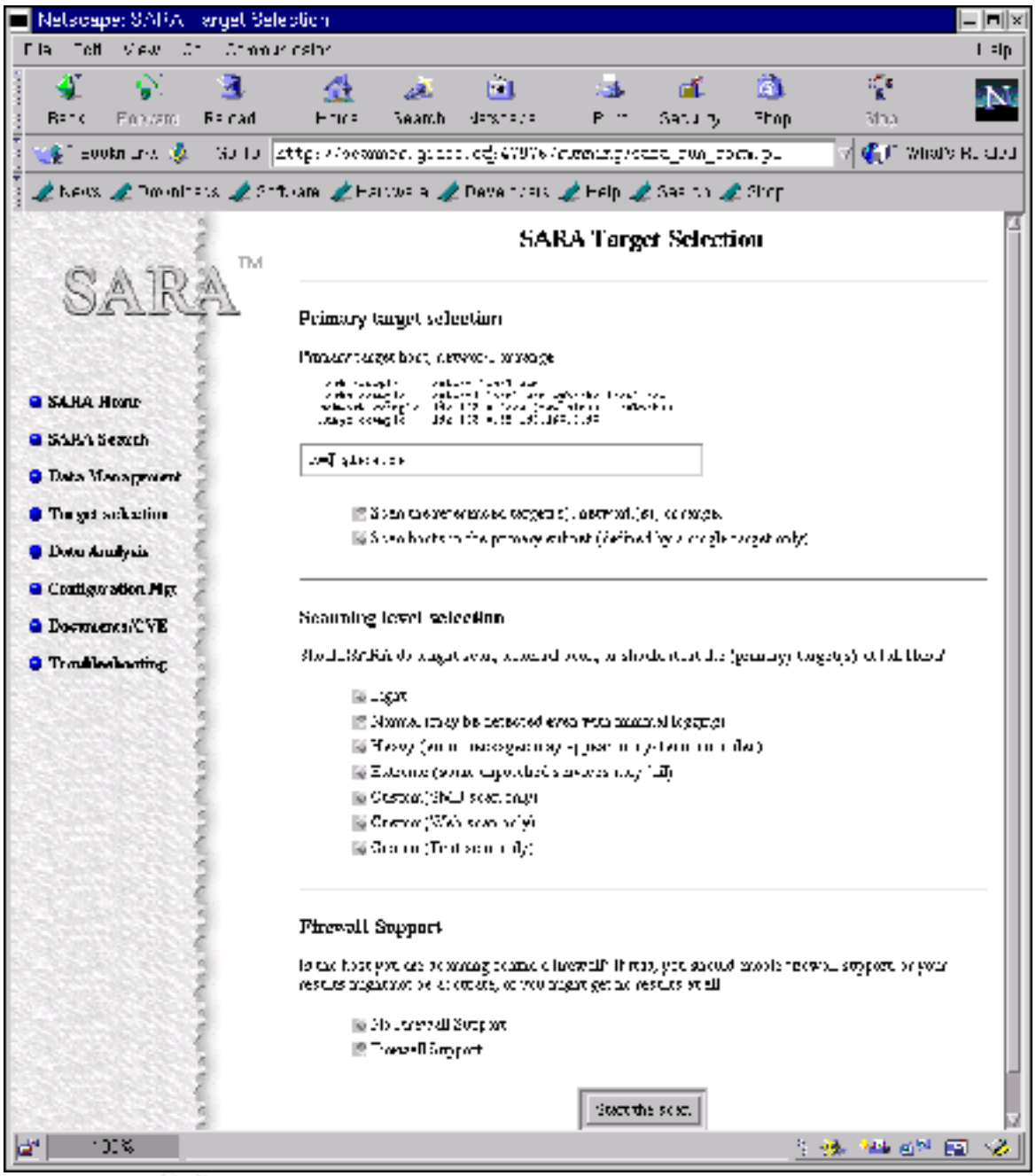
Configure and test a single host at a time; include each interface address of the Router [2] and Firewall [3]. Scan at the normal level for the initial evaluation with Firewall support selected for all the scans. For a complete scan use Heavy – this will cover a much larger range of ports with the corresponding greater network impact.



- Figure 9 SARA Initial Page

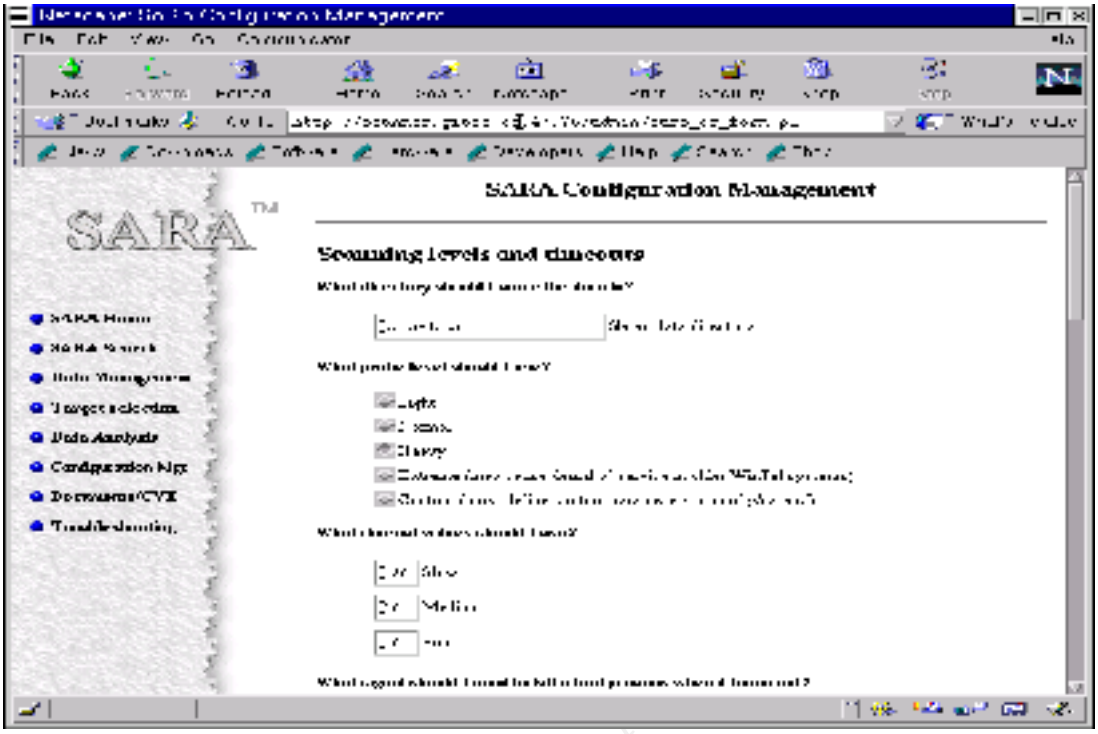
© SANS Institute 2000 - 2002

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



• Figure 10 SARA Target Selection

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



- Figure 11 SARA Configuration

SARA reported no vulnerabilities with the scans. See Appendix H SARA Report for the report.

Inside

Inspect the network room to ensure that it is kept locked and secure. Review the access list for the room.

Locate the scanner on the Internal LAN and conduct a basic ping sweep to map the network devices and confirm that each one is included on the network inventory.

Use the Network General Sniffer to listen on the wire on the Internal LAN and outside of the Router. Both the Public Network and FW-Router segments can't be sniffed on or tested from directly because the single cable can't be disturbed for the test.

Scan the Internal Services address with SARA for any host vulnerabilities that may be showing to the Internal LAN since these could impact the OpenVMS cluster as well.

Use the host based TCPdump utility to see if the data is being encrypted before going out on the wire via the SSH connections. (Use the remote host name or address).

```
$ multinet tcpdump /snap=1600 /hex host xxx.xxx.xxx.xxx
```

With administrator access to the customer database hex dump part of the data file to confirm that the important data is being encrypted.

```
$ dump <filename> /block=(start:1, end:10)
```


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

Analysis

General

For all of the data we have collected we need to compare it to the security policy see where entries are expected and where entries should be missing or are unexpected.

Match the time stamps for a scan across all of the available logs and then step through them to see if any anomalies show up.

Business Partners

The past assessments show everything from: don't have a security plan; through we've got it scheduled; to satisfactory. Needs work.

Outer Perimeter

Out of the entire office 30% responded with the results of their scan. All have active virus checking enabled with updates on a regular basis. The majority needs to install a firewall; the remainder have some rules in place.

The specific log we have as an example shows that during the test of the firewall the workstation got NetBIOS probe from a different address (cable network). Interesting coincidence that would help show the users why we are doing this work.

The other aspect of this log is what was missing. The web site shows a check of Telnet (23) and the log doesn't show any blocking for the probe of this port. The user's set of applications includes a terminal emulator used for telnet access to the OpenVMS cluster.

The final question is, are all of the home systems checked? There isn't an inventory of people who work from home so this can't be verified.

Back Doors

The number of modems matches the network inventory. Policy compliance.

Router & Firewall

No services enabled on either platform.

Configuration matches the intended policy.

Servers

No vulnerabilities reported. The report does seem to be strange, needs to be reviewed.

Inside

A sniffer on the Internal LAN between the OpenVMS host and the Firewall picked up DECnet traffic in the clear.

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

Recommendations

Business Partners

Each group needs to work together to educate and assist with the overall business security since in an E-business environment both sides may affect the other. The only recourse may be to work on the political level. If you are a bank, you may be able to specify the minimum requirements others must meet to conduct business with you.

Outer Perimeter

For this one workstation - add a rule to block inbound Telnet.

Use host logging to collect IP source addresses from the VPN LAN (172.30.5.0/24) along with the OpenVMS usernames so that a list of the home users can be created and testing verified.

Develop some sort of training program to assist the home users with their firewall configurations. Monitor the development of the **Shields UP!** testing tool.

Tools

There is significant risk in deploying a scanning platform that is UNIX based because the available skill level is very low within this group of OpenVMS system administrators. The value of the tools on the UNIX systems are currently higher than the other platforms so it is worth developing the minimum skills needed to maintain the audit tools in house.

Add the SMB tools to the Linux system and reconfigure SARA to include the SMB tests that weren't in the assessment. I didn't install SMB on Linux because it is a hardened workstation, and then one of the components SARA needed for testing was missing. The tools need to be kept in sync with the applications that are in use.

If the security policy permits, consider deployment of a permanent scanner as an enterprise tool that could be run on a regular basis. Nessus and SARA should both be evaluated in this context.

The SARA Reports are strange. They should be redone and possibly compared to another tool such as Nessus. Time limitations have precluded this additional analysis.

Design

Replace the router to router VPN by tunneling the DECnet link within a SSH session between the two OpenVMS systems. This way the DECnet traffic would not be in clear text for any part of the path.

With any sale of this business unit the VPN Server managed by the parent corporation would need to be replaced. The solution is to connect a similar product to the Firewall on one of it's unused ethernet interfaces.

The LAT Terminal Server should be replaced with one that would handle a secure session between itself and the Cluster Console system.

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

Appendices

Appendix A VISA Ten Commandments

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

9) Keep security patches up-to-date.

10) Encrypt stored data accessible from the Internet.

11) Encrypt data sent across networks.

12) Use and regularly update anti-virus software.

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

14) Assign unique IDs to each person with computer access to data.

15) Track access to data by unique ID.

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

17) Regularly test security systems and processes

© SANS Institute 2000 - 2002, Author retains full rights.

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

Appendix B Base Security Policy

This is a copy of 'Top Ten' Appendix B: *Perimeter Protection For An Added Layer of Defense In Depth* at http://www.sans.org/topten.htm#pp Please check the source document for updates.

In this section, we list 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, private (RFC1918 and network 127) and IANA reserved 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 destination unreachable messages **except** "packet too big" messages (type 3, code 4). (This item assumes that you are willing to forego the legitimate uses of ICMP echo request in order to block some known malicious uses.)

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

Appendix C References

Brenton, Chris. "*Network Design and Performance.*" *SANS Network Security 2000 Conference Proceedings*, Monterey, CA: October 2000.

Brenton, Chris and Elfering, Dave. "*VPNs and Remote Access.*" *SANS Network Security 2000 Conference Proceedings*, Monterey, CA: October 2000.

Deterding, Brent. *Nmap - The Tool, It's Author and It's Implications. SANS Institute.* Available at http://www.sans.org/infosecFAQ/nmap.htm

Kurtz, George and Schultze, Eric. "*Hacking Exposed: LIVE!" SANS Network Security 2000 Conference Proceedings*, Monterey, CA: October 2000.

Payne, Adam. SANS *GIAC Firewall and Perimeter Protection Practical Assignment v1.2, SANS Institute*. Available at: http://www.sans.org/y2k/practical/Adam_Payne.doc

Skoudis, Edward. "*Computer and Network Hacker Exploits: Step-by-Step" SANS Network Security 2000 Conference Proceedings*, Monterey, CA: October 2000.

Spitzner, Lance. "*Advanced Perimeter Protection and Defense In-Depth.*" *SANS Network Security 2000 Conference Proceedings*, Monterey, CA: October 2000.

Spitzner, Lance. *"Firewalls 101: Perimeter Defense with Firewalls." SANS Network Security 2000 Conference Proceedings*, Monterey, CA: October 2000.

SANS Institute. *How To Eliminate The Ten Most Critical Internet Security Threats - The Experts' Consensus*. Available at http://www.sans.org/topten.htm

SANS Institute. *Securing Linux: Step-by-Step*. Version 1.0, ISBN 0-9672992-0-9. Available at http://www.sansstore.org/

Shimonski, Robert. *SATAN: Dancing with the Devil and Wreaking Havoc in an NT Environment. SANS Institute.* Available at http://www.sans.org/infosecFAQ/SATAN.htm

Stark, Vernon. *Nessus - A Very Capable Security Auditing Tool. SANS Institute.* Available at http://www.sans.org/infosecFAQ/nessus.htm

Turner, Aaron. *Network Insecurity with Switches. SANS Institute.* Available at http://www.sans.org/infosecFAQ/switch_security.htm

Winters, Scott. *Top Ten Blocking Recommendations Using Cisco ACLs: Securing the Perimeter with Cisco IOS 12 Routers. SANS Institute.* Available at http://www.sans.org/infosecFAQ/blocking_cisco.htm

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

Appendix D Resources

SANS Institute. Information Security Reading Room: http://www.sans.org/infosecFAQ/index.htm

Achilles: http://www.digizen-security.com/

Cisco ConfigMaker: http://www.cisco.com/warp/public/cc/pd/nemnsw/cm/index.shtml

Cisco Secure Product Literature: http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/prodlit/index.shtml

Cisco IOS Firewall: http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/index.shtml

Q&A Cisco IOS Firewall 12.0(5)T and Later Releases: http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/prodlit/fw12t_qp.htm

Firewalk: http://www.packetfactory.net/firewalk/

FAQ: Firewall Forensics (What am I seeing?): http://www.robertgraham.com/pubs/firewall-seen.html

Linux Firewall Design Tool: http://www.linux-firewall-tools.com/linux/firewall/index.html

Microsoft Knowledge Base: http://support.microsoft.com/support/kb/articles

Microsoft Windows Update: http://windowsupdate.microsoft.com/

NmapNT Location: http://www.eeye.com/html/Databases/Software/nmapnt.html

Nortel Contivity VPN: http://www.nortelnetworks.com/products/01/contivity/index.html

Sam Spade for Windows: http://samspade.org/ssw/

Security Auditor's Research Assistant (SARA): http://www-arc.com/sara/

Shields UP! by Gibson Research Corporation: http://www.grc.com/

SSL-Proxy: http://www.csnc.ch/index_e.html

THC-scan: from CD supplied as part of Edward Skoudis' "*Computer and Network Hacker Exploits: Step-by-Step"* session at SANS NS 2000.

© SANS Institute 2000 - 2002, Author retains full rights.

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

Appendix E OpenVMS Resources

OpenVMS FAQ http://www.openvms.compaq.com/wizard/openvms_faq.html

DSNlink – available with any support contract, installation kit on Consolidated Software Distribution CD (Condist) set.

DSNlink New – scans for new articles in DSNlink, installation kit on the Freeware CD (Condist, or below OpenVMS Home Page)

Each of the home pages has the product patch location and support links somewhere below.

Compaq OpenVMS Home Page http://www.openvms.compaq.com/

Compaq Secure Web Server (Apache):
http://www.openvms.compaq.com/openvms/products/ips/apache/csws.html

MultiNet Product Home Page http://www.process.com/tcpip/multinet.html

PMDF Product Home Page http://www.process.com/tcpip/pmdf.html

© SANS Institute 2000 - 2002, Author retains full rights.

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

Appendix F Firewall Script

I've included one of the two original scripts produced by ConfigMaker. This is an example of where the configuration tool left off and the hand modifications started. Modifications were made to the scripts to match the policy as described by Scott Winters' *Top Ten Blocking Recommendations Using Cisco ACLs*[26] article.

```
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname Firewall
!
enable password changethis
!
ip source-route
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
! Context-Based Access Control
!
no ip inspect audit-trail
ip inspect tcp synwait-time 30
ip inspect tcp finwait-time 5
ip inspect tcp idle-time 3600
ip inspect udp idle-time 30
ip inspect dns-timeout 5
ip inspect one-minute low 900
ip inspect one-minute high 1100
ip inspect max-incomplete low 900
ip inspect max-incomplete high 1100
ip inspect tcp max-incomplete host 50 block-time 0
!
! IP inspect Ethernet_1_1
!
no ip inspect name Ethernet_1_1
ip inspect name Ethernet_1_1 tcp
ip inspect name Ethernet_1_1 udp
ip inspect name Ethernet_1_1 cuseeme
ip inspect name Ethernet_1_1 ftp
ip inspect name Ethernet_1_1 h323
ip inspect name Ethernet_1_1 rcmd
ip inspect name Ethernet_1_1 realaudio
ip inspect name Ethernet_1_1 smtp
ip inspect name Ethernet_1_1 streamworks
ip inspect name Ethernet_1_1 vdolive
ip inspect name Ethernet_1_1 sqlnet
ip inspect name Ethernet_1_1 tftp
!
! IP inspect Ethernet_0_0
!
no ip inspect name Ethernet_0_0
ip inspect name Ethernet_0_0 smtp
ip inspect name Ethernet_0_0 tcp
ip inspect name Ethernet_0_0 udp
!
interface Ethernet 0/0
 no shutdown
 description connected to FW-Router
 ip address 172.28.8.162 255.255.255.252
```

[26] http://www.sans.org/infosecFAQ/blocking_cisco.htm

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

```
 ip inspect Ethernet_0_0 in
 ip access-group 102 in
 keepalive 10
!
interface Ethernet 1/0
 no shutdown
 description connected to Public Network
 ip address 172.28.8.169 255.255.255.248
 ip access-group 100 in
 keepalive 10
!
interface Ethernet 1/1
 no shutdown
 description connected to Internal LAN
 ip address 172.28.7.1 255.255.255.0
 ip inspect Ethernet_1_1 in
 ip access-group 101 in
 keepalive 10
!
interface Ethernet 1/2
 no description
 no ip address
 shutdown
!
interface Ethernet 1/3
 no description
 no ip address
 shutdown
!
! Access Control List 100
!
no access-list 100
access-list 100 deny ip any any
!
! Access Control List 101
!
no access-list 101
access-list 101 deny ip 172.28.8.0 0.0.0.7 any
access-list 101 permit eigrp any any
access-list 101 deny ip host 172.28.7.231 host 172.28.8.170
access-list 101 deny ip host 172.28.7.231 host 172.28.8.171
access-list 101 deny ip host 172.28.7.231 host 172.28.8.172
access-list 101 deny ip host 172.28.7.231 host 172.28.8.173
access-list 101 deny ip host 172.28.7.231 172.28.8.0 0.0.0.7
access-list 101 permit ip host 172.28.7.231 any
access-list 101 deny ip host 172.28.7.21 host 172.28.8.170
access-list 101 deny ip host 172.28.7.21 host 172.28.8.171
access-list 101 deny ip host 172.28.7.21 host 172.28.8.172
access-list 101 permit udp host 172.28.7.21 host 172.28.8.173 eq domain
access-list 101 deny ip host 172.28.7.21 host 172.28.8.173
access-list 101 permit udp host 172.28.7.21 172.28.8.0 0.0.0.7 eq domain
access-list 101 deny ip host 172.28.7.21 172.28.8.0 0.0.0.7
access-list 101 permit ip host 172.28.7.21 any
access-list 101 deny ip host 172.28.7.153 host 172.28.8.170
access-list 101 deny ip host 172.28.7.153 host 172.28.8.171
access-list 101 deny ip host 172.28.7.153 host 172.28.8.172
access-list 101 deny ip host 172.28.7.153 host 172.28.8.173
access-list 101 deny ip host 172.28.7.153 172.28.8.0 0.0.0.7
access-list 101 permit ip host 172.28.7.153 any
access-list 101 deny ip any host 172.28.8.170
access-list 101 permit tcp any host 172.28.8.171 eq 80
access-list 101 permit tcp any host 172.28.8.171 eq 443
access-list 101 deny ip any host 172.28.8.171
access-list 101 deny ip any host 172.28.8.172
access-list 101 deny ip any host 172.28.8.173
access-list 101 permit tcp any 172.28.8.0 0.0.0.7 eq 80
access-list 101 permit tcp any 172.28.8.0 0.0.0.7 eq 443
access-list 101 deny ip any 172.28.8.0 0.0.0.7
access-list 101 permit ip any any
!
! Access Control List 102
```


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

```
!
no access-list 102
access-list 102 deny ip 172.28.8.0 0.0.0.7 any
access-list 102 deny ip 172.28.7.0 0.0.0.255 any
access-list 102 permit tcp any host 172.28.8.170 eq 25
access-list 102 deny ip any host 172.28.8.170
access-list 102 deny ip any host 172.28.8.171
access-list 102 permit tcp any host 172.28.8.171 eq 443
access-list 102 permit tcp any host 172.28.8.171 eq 80
access-list 102 deny ip any host 172.28.8.172
access-list 102 permit udp any host 172.28.8.172 eq domain
access-list 102 deny ip any host 172.28.8.173
access-list 102 permit tcp any host 172.28.7.21 eq 22
access-list 102 deny ip any host 172.28.7.21
access-list 102 deny ip any host 172.28.7.231
access-list 102 deny ip any host 172.28.7.153
access-list 102 permit tcp any 172.28.8.0 0.0.0.7 eq 25
access-list 102 permit tcp any 172.28.8.0 0.0.0.7 eq 443
access-list 102 permit udp any 172.28.8.0 0.0.0.7 eq domain
access-list 102 permit tcp any 172.28.8.0 0.0.0.7 eq 80
access-list 102 deny ip any 172.28.8.0 0.0.0.7
access-list 102 permit tcp any 172.28.7.0 0.0.0.255 eq 22
!
router eigrp 7373
 network 172.28.0.0
 passive-interface Ethernet 0/0
 no auto-summary
!
!
ip classless
!
! IP Static Routes
ip route 0.0.0.0 0.0.0.0 Ethernet 0/0
no ip http server
snmp-server location 42 River Road, VMS Room
snmp-server contact Graham Bennett,555-555-1234,graham.bennett@geace.ca
banner motd #Authorized access only. All activity logged.#
!
line console 0
 exec-timeout 0 0
 password changethis
 login
!
end
```

© SANS Institute 2000 - 2002, Author retains full rights.

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

Appendix H SARA Report

Security Auditor's Research Assistant (SARA) Professional (PRO) Report Writer

Back to the SARA start page | Back to SARA Reporting and Analysis

place date here
place document number here

SARA Scan Results of *Customer Name*

INTRODUCTION

Advanced Research Corporation ® was tasked to perform a Security Auditor's Research Assistant (SARA) security scan on hosts on the *Customer Name* sub-nets. The SARA scan was performed to identify potential security vulnerabilities in the *Customer Name* sub-domain.

DISCUSSION

SARA is a third generation security analysis tool that analyzes network-based services on the target computers. SARA classifies a detected service in one of four categories:

- Green: Services found that were not exploitable
- None: No services or vulnerabilities
- Red: Services with potentially severe exploits (account compromise)
- Yellow: Services with potentially serious exploits found (data compromise)
- Brown: Possible security problems.

Figure 1 summarizes this scan by color where the *Green* bar indicates hosts with no detected vulnerabilities. *None* indicates hosts with no services. The *Red* bar indicates hosts that have one or more red vulnerabilities. The *Yellow* bar indicates hosts that have one or more yellow vulnerabilities (but no red). And the *Brown* bar indicates hosts that have one or more brown problems (but no red or yellow)



Figure 1 Host Summary by Color

The SARA scan results are distributed as three appendices to this paper:

- Appendix A: Sub-net tables depicting hosts, host-types, and vulnerability counts.
- Appendix B: Details on the hosts reported <truncated>
- Appendix C: Description of the vulnerabilities <not included because it was empty>

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

Appendices A through C are hyper-linked to assist the reader in navigating through this report. The report includes information on all non-Windows hosts that have one or more vulnerabilities. In addition, Windows hosts that have Red and/or Yellow vulnerabilities are also included.

RECOMMENDATION

The identified hosts should be analyzed immediately.

Appendix A
SARA Scan Summary

Host Name	IP Address	Host Type	Green	Red	Yellow	Brown
www.geace.ca	172.28.8.171	unknown type	0	0	0	0
mail.geace.ca	172.28.8.170	unknown type	0	0	0	0
dns.geace.ca	172.28.8.172	unknown type	0	0	0	0
dnsf.geace.ca	172.28.8.173	unknown type	0	0	0	0

Table 1 Hosts on Sub-net 172.28.8

Host Name	IP Address	Host Type	Green	Red	Yellow	Brown
babylon.geace.ca	172.28.7.21	unknown type	0	0	0	0

Table 2 Hosts on Sub-net 172.28.7

Host Name	IP Address	Host Type	Green	Red	Yellow	Brown
router.geace.ca	172.28.5.18		0	0	0	0

Table 3 Hosts on Sub-net 172.28.5

Appendix B
SARA Scan Details

Host: www.geace.ca

General host information:

- Host type: unknown type
- Subnet 172.28.8.171

Vulnerability information:

<remainder of report similarly blank, not included>

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