Global Information Assurance Certification Paper

Securing the Perimeter: A Case Study

George Kelschenbach
GIAC Security Essentials Certification (GSEC)
Practical Version 1.4b option 2
March 2003

Abstract

My employer is a small consulting firm whose specialty is providing their customers with Microsoft Windows and Citrix networked business solutions. They believed their internal servers were secure due to their diligence in keeping the Operating Systems up to date with the latest service packs, hotfixes and patches. Virus signatures and scanning software was also kept current. I was given the task of evaluating the security of the network perimeter and to make recommendations for securing our Internet connection.

Examination of the perimeter infrastructure showed the network to be virtually defenseless. There was no Firewall installed and very little filtering of inbound or outbound Internet traffic on either the router at the corporate office or the router at the branch office. The Linux, Help Desk, Mail server and the two Active Directory servers had direct network links to both the internal network and the Internet making them prime targets for intruders. We decided to completely redesign the network perimeter to provide a layered Defense in Depth.

Before

Network design

The original perimeter network design included two Cisco routers and five publicly addressed servers, four of which were Windows based and the fifth, RedHat Linux. As stated, the network did not have a Firewall device and the perimeter routers performed extremely limited inbound packet filtering. The corporate router was configured with a serial interface for connection to the Internet, an Ethernet interface for the public network, and an Ethernet interface for the internal (private) network. The branch office router had a serial interface to the Internet and an Ethernet interface to their internal network (*diagram 1*). The branch and corporate routers were connected by VPN tunnel over the Internet. The various network devices at the corporate office, both internal and external, were connected via three cascaded switches. Each of the external (public) servers had a direct link to the internal network and represented a significant danger if they were compromised. The branch office network consisted of four PCs on a hub connected to the router. A brief description of each network device follows.

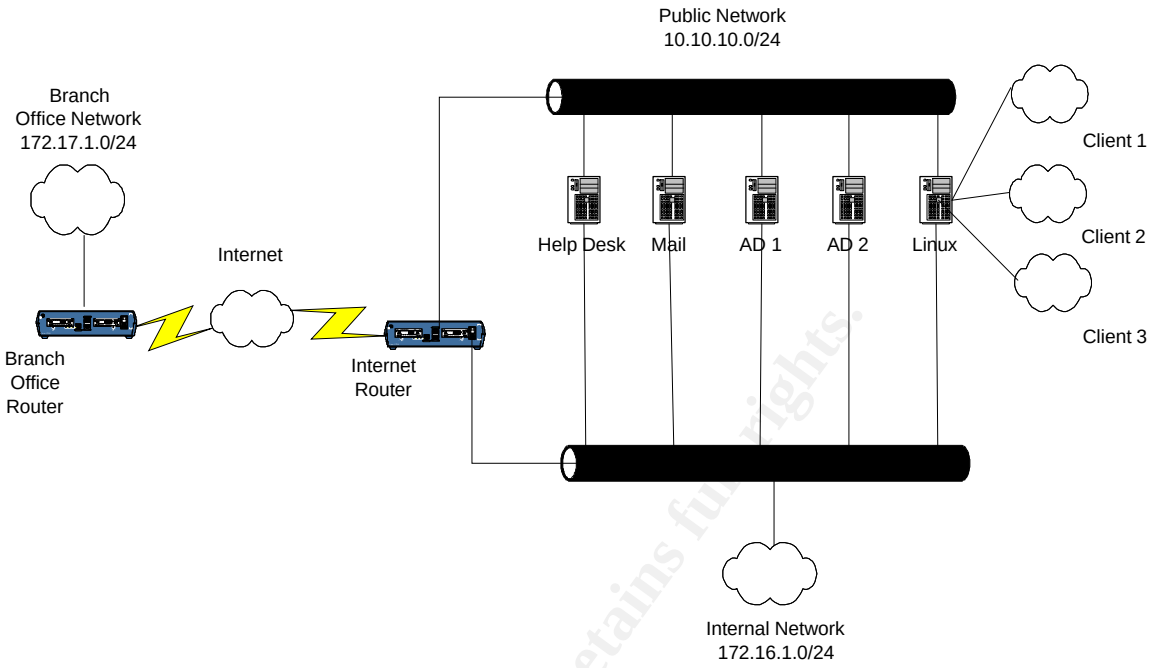

Diagram 1

Routers

Corporate Router

The Cisco router at the corporate office provided Network Address Translation (NAT) for outbound Internet connections. The five public servers were assigned static NAT addresses. All other traffic was given the public address of the serial interface by the NAT "overload" feature of the Cisco Internetwork Operating System (IOS). The router also acted as one end of a point-to-point VPN tunnel to the branch office router. This provided secure access to the corporate Microsoft Active Directory servers and other network resources. The serial interface had an inbound access list to block port 1433 (SQL Server) traffic to a single internal server. All other traffic, inbound and outbound was permitted.

Branch Office Router

The Branch office router was configured to provide NAT for outgoing Internet traffic, in addition to a VPN tunnel to the corporate router. An inbound access list was applied to the serial interface making it somewhat more secure. The access list was designed to block packets with spoofed private network addresses. No other security measures were in place.

Public Servers

Help Desk Server.

This is a Windows 2000 server providing web based Help Desk services to clients and staff. It runs Microsoft Internet Information Server (IIS) and Microsoft SQL to support the Help Desk application. There were two network interfaces installed, one connected to the public network, the other connected to the private network. The patch levels and virus signatures on this server were kept up to date.

Mail Server

The second server is also Windows 2000 based. It acts as a mail server using Microsoft Exchange and provides file and print services to the internal network through a second network interface. Mail sent to this server was forwarded to the internal Exchange mail server, storing it if the internal server was unavailable. This server also acted as a public NFuse front end to the internal Citrix server.

Linux Server

The Linux server runs the Redhat 7.2 operating system and Apache web server software. This server has a total of five network interfaces. One public, one private, and three others used to provide routing and Internet gateway services to other companies in our building for a monthly fee. There is a minimal Ipchains firewall in place, allowing the three companies to access the Internet, but preventing them from accessing the other networks in the building. All Internet traffic inbound or outbound is permitted to their networks with no additional filtering. Our service agreement with these clients does not require us to provide any additional type of security services. The Linux machine also acts as a web server providing portal access to our internal servers. Clients and staff can access each portal service by providing their name and password. Credentials are passed to the internal Active Directory server for validation using LDAP.

Active Directory Servers

The Primary and Secondary Active Directory Servers had two interfaces each, one connected to the internal network and the other to the Internet. The reason for the dual attachment was to provide Active Directory services to the PCs in the branch office over the VPN. Without the internal interface, the branch office was unable to browse the corporate network.

Vulnerability Assessment

- The network does not have a Firewall installed for protection against outside probes or attacks. This is a critical weakness because even the

most well patched, up to date operating system is vulnerable to a determined attack. The same is true of web services and other applications. A Firewall can protect a network against some types of address spoofing, SYN flooding [1] and many types of port scanning. Network performance can also be improved by blocking unwanted traffic at the firewall. Without a Firewall or other type of basic protocol filtering, the entire network is open to compromise. An example of this would be a TCP sequence number guessing attack like the Mitnick attack against Ken Shimomura [2] in 1994. Our lack of network security not only puts our internal network at risk, it also presents a threat to the rest of the Internet community. Compromised resources on our network could be used to unknowingly participate in a Distributed Denial of Service (DDOS) attack [3] launched against another network.

- There is insufficient filtering on the routers. As with the lack of firewall, this leaves the network wide open to attack and exploitation. Perimeter routers should be configured with ingress and egress filters, based on the company security policy, to protect the internal network. An ingress filter should be configured to block any incoming packets with inappropriate source addresses. Examples would be internal network addresses, public addresses as defined in RFC1918 [4], and networks 127 and 224. Egress filters should block any outgoing packets that do not have source addresses originating on the internal network.

- Logs were not kept of the types or frequency of Internet traffic. Without logs there was no way to determine if the network was being probed or attacked. Collection and analysis of daily logs can be used as a means of intrusion detection and is one of the best ways to determine what traffic is normal and what should be investigated. Logs also provide an audit trail of suspected criminal activity and can be used as evidence in court.

- Each of the public servers also had links to the company's internal network. If any of these machines were compromised, they could act as gateways to the rest of the company's data and servers.

- The Linux server was built and maintained by one of the consulting engineers. Patches, bugfixes and other administrative tasks were performed whenever his schedule allowed. There was no one else in the company familiar enough with Linux to assume this responsibility. At least one backup Linux administrator is needed to maintain the security and availability of this server.

- There are no written policies concerning the frequency or responsibility for maintaining the security levels of hardware and software. Written policies have to be developed specifying who is responsible for maintaining the security and patch levels [5] of each network device.

During

After reviewing my assessment of the perimeter network, it was decided that our first task was acquiring and installing a Firewall. Three different Firewall products were considered based on functionality and price: Checkpoint Firewall-1, the Cisco Pix 515e, and the Sonicwall 300. Each platform was capable of supporting a separate DMZ segment and providing the VPN and NAT features we required. I have several years experience with the Checkpoint and Cisco firewall products and know they perform well. The Sonicwall 300 has received excellent reviews in various publications. My GSEC course instructors also spoke highly of this product. Since all three products were capable of the required functionality, the deciding factor was one of cost. The Sonicwall 300 was selected because it provided the desired features at an acceptable price.

With the selection of the Firewall decided, the next step was to redesign the perimeter architecture to incorporate the Firewall. This would provide a simplified network design capable of providing Defense in Depth *(Diagram2)*. In the first phase of the project, the Firewall was placed between the internal network and the Internet router. The Sonicwall 300 model has a LAN, WAN and DMZ port as its standard configuration. The new DMZ segment will be used to host the Linux, Mail and Help Desk servers. The Sonicwall 300 can be configured to permit NetBIOS traffic through the VPN tunnel eliminating the need for public interfaces on the Active Directory servers. The interfaces to the internal network on the Linux, Help Desk, and Mail servers will also be shutdown. This will reduce the threat to the internal network in the event these servers are compromised. The new design shifts NAT and VPN functions from the Internet router to the Sonicwall 300. This will free the router to perform packet filtering and logging functions without overtaxing the CPU. Any required patches or updates will be applied to the three public servers on the DMZ.

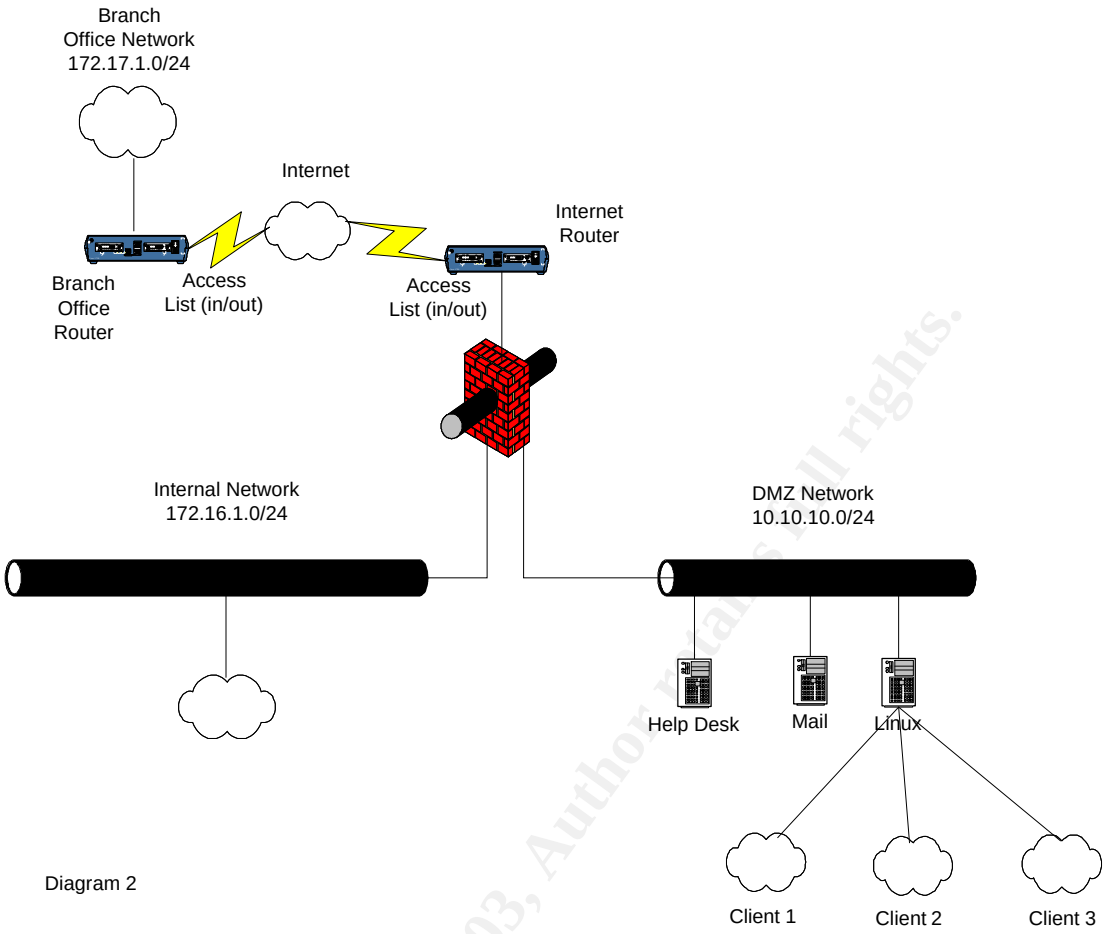

Diagram 2

The second phase of the project includes designing and implementing the router access lists and building a Syslog server to collect logs from the routers and firewall. The work was completed as a two-phase process in order to minimize the impact on the network and is described below.

Phase 1

Design the Network Security Policy

The company security policy defines which services are allowed to access the internal and DMZ networks. The policy will be used as the basis for the Firewall rule set and router access lists. The Sonicwall 300 protects against Syn Flood, Ping of Death, IP Spoofing, Land Attack, Smurf amplification, and sequence number prediction by default. The rest of the security policy has to be defined in a series of sequential rules. Our security policy allows the following traffic:

Internal network

All outbound traffic to the DMZ or Internet is allowed. The only outbound restriction will be to prevent illegal traffic from leaving the network. Any outbound packet not having a legitimate internal or DMZ source address will be blocked and logged to the Syslog server. Traffic blocked will include RFC1918 private addresses, multicast, 127 network addresses and most ICMP packets.

DMZ

Traffic from the DMZ to the internal network is allowed. The Linux server is permitted to receive http (80), https (443), ftp (21), ssh (22), and dns (53) packets from the Internet. LDAP (389) is used between the Linux server and the internal Active Directory server for user authentication. The mail server is allowed to receive Citrix (1494), pop3 (110) and mail (25) services. The help desk server receives http (80), https (443) from the Internet and SQL (1433) traffic from the internal network. Syslog (514) and TFTP (69) services are allowed inbound from the routers and Sonicwall 300 to the internal Syslog server.

Internet

Unless explicitly allowed, all inbound traffic from the Internet is blocked and logged.

Reconfigure the Corporate Router

The following configuration changes are designed to be the first layer in our Defense in Depth:

- Backup the current router configuration so we can fall back if necessary.
- This router has two Ethernet interfaces. We will disconnect and shutdown the Ethernet interface directly connected to the internal network. The second Ethernet port will be used to connect the router to the Sonicwall 300. This eliminates the possibility traffic getting to the internal network without going through the firewall.
- Remove configurations statements for NAT and VPN. This functionality is no longer required and will free CPU cycles for other processes.
- Configure Secure Shell for remote access to the router. We will also block Telnet and the "r" services (rsh, rlogin and rcp) through access lists.
- Harden the router to improve the security of the router itself [6] by making the following configuration changes:
    - Enable password encryption with the "service password-encryption" command. This encryption can be broken but will provide a minimal level of protection. Configuration files with this level of

encryption should be treated as if they were clear text and only be available to authorized administrators.
    - Use the “enable secret” command instead of “enable password”. This encrypts the enable password using MD5 hashing, which is far more secure than the “service password-encryption” used on other passwords in the router’s configuration.
    - Use an access list to control remote login to the router. Use the “transport input ssh” and “access-class” commands to allow only Secure Shell access to Virtual Terminal (VTY) connections.
    - Enable AAA Authentication and define users and passwords for use with ssh.
    - Eliminate unnecessary services such as finger, bootp and Cisco Discovery Protocol (CDP).
    - Disable the http server to prevent web access to the router.
    - Disable IP source-route, and directed broadcasts. These are unnecessary and dangerous services.
    - Use the “scheduler allocate” command to protect the router from the effects of flooding. This command forces the router to stop packet switching at configurable intervals to perform other necessary processing.
- Write a script to back up the router configuration and send it to the Syslog server twice weekly.

Reconfigure the Branch Office Router

The router at the branch office provides a VPN tunnel to the corporate office and local access to the Internet. We will perform the same hardening procedures as outlined for the Internet router. Again, this will act as the first layer of our Defense in Depth. This router will continue to perform its current NAT functions, but the VPN tunnel will be temporarily shutdown. The script we use to backup the corporate router configuration will also backup the configuration of this router.

Install Sonicwall 300 Firewall Appliance

This is the second layer of our Defense in Depth. A brief description of the configuration process follows:

- Configure LAN, DMZ and WAN interfaces. Assign IP address and mask to each interface.
- Define each of the company’s networks.
- Configure NAT. The Sonicwall supports dynamic and static NAT (One-to One NAT). Outgoing source addresses in the dynamic range are changed to the public address of the Sonicwall. Static or One-to-One addresses are assigned to servers available to the Internet and the pairings do not change.

- Configure the security policy rule set.
    - Identify services and ports to be used in the rule set.
    - Create custom service (port) definitions for those services not in the Sonicwall 300 default list.
    - Re-address internal servers to fit the Sonicwall 300 One-to-One Nat address range.
    - Create the rule set. Add the rules needed to enforce our security policy. The Sonicwall OS automatically places the rules in optimum order. The most specific rules are listed first, followed by more general rules.
    - Allow NetBIOS traffic between the internal network and DMZ, and internal network and remote office.
    - Configure to run in stealth mode (traffic dropped with no message to source).

Help Desk and Mail Server.

- Apply any patches or fixes required to bring the servers up to date.
- User and group policies have been defined according to the principle of least privilege. Each User or Group can access only the files or applications required for them to perform their jobs.
- User and Group policies have been defined in Active Directory
- Most of the Users have thin client machines running a Citrix client providing a desktop tailored for that particular individual.
- All the Windows 2000 servers use the NTFS file system for its stability and security capabilities.

Linux Server

- Disconnect and shutdown the internal network interface. This will eliminate a possible backdoor to the internal network.
- Update the Linux OS using the RedHat "up2date" service.
- Apply any patches required for the Apache web server software.
- Enable kernel security [7] options using parameters in the /proc/sys/net/ipv4 directory. Set the values to 1 to enable, or 0 to disable. The parameters are:
    - Enable "icmp_echo_ignore_broadcasts" to prevent response to multicast ping requests.
    - Enable "tcp_syncookies" to protect against SYN flooding attacks.
    - Enable "rp_filter" to help prevent spoofing attacks. This is enabled on systems acting as routers.
    - Enable "secure_redirects" to allow icmp redirects from default gateways.
    - Enable "log_martians" to log invalid addresses to the kernel log.
    - Disable "accept_source_route" to decline source routed packets. This parameter is disabled by default in Redhat Linux 7.2.

- Disable as many unnecessary services as possible. Use the "/sbin/chkconfig –list" command to list the services on Redhat Linux. Most of the services we considered unnecessary were already disabled with the exception of telnet, nfs and lpd. Since these services are not required, they have been disabled.
- Enable Secure Shell to replace telnet access to the server.
- Configure the "syslogd" daemon to send log information to the Syslog server.

Active Directory Servers

- Disconnect and shutdown their public network interfaces.
- Apply any required security patches.

DNS. Update internal and external DNS servers to reflect new addressing.

Test new network architecture.

- Add a rule to the Sonicwall to allow ICMP (ping) for testing purposes. Disable when testing complete.
- Verify connectivity between LAN and DMZ (one-to-one NAT servers).
- Verify connectivity between LAN and Internet.
- Verify Internet connectivity to our public services (web, citrix, mail, ssh, etc.).
- Verify remote office's ability to access and browse the corporate network.

Phase 2

Now that we have determined that the new network design is working properly, we can now add router access lists and activate VPN functionality.

Reconfigure Internet Router.

- Develop inbound and outbound access lists and apply them to the Serial connection to the Internet. Include the "log-input" keyword on each deny statement to enable logging.
- Test access lists to verify they work and do not block any required traffic.
- Specify the address of the Syslog server and set logging level to 3 (errors).

Reconfigure Remote Router.

- Reconfigure the VPN tunnel to the corporate office using the Sonicwall as the endpoint.

- Develop reflexive ingress and egress access lists based on the network security policy. A reflective access list [8] is a named, extended access list, which creates dynamic packet filters based on statements containing the "reflect" keyword. These types of access lists are configured in pairs, one to filter outgoing packets (egress) and one to filter incoming packets (ingress). The outgoing filter keeps track of all the "reflected" packets. The incoming filter checks packets against the dynamically created filters using the "evaluate" keyword, permitting or blocking the packets accordingly. All blocked packets are logged for later analysis. Reflexive access lists are more CPU intensive than standard or extended access lists. Monitoring CPU utilization is important to determine if the access lists are degrading the router's performance.
- Set the logging level to 3 (errors) and specify the Syslog server address.
- Test the access lists to verify they are working without blocking any required traffic.

Reconfigure Sonicwall 300 Firewall Appliance.

- Configure site-to-site VPN to the branch office router. Ensure the router has the appropriate Cisco IOS level to allow creation of the tunnel. Set up group key, hash, and encryption level, and allowed networks. Test the connectivity to and from the remote office.
- Use a packet sniffer to verify encryption is taking place.
- Install the Sonicwall remote VPN client on a notebook computer and test connectivity. Document the client install procedure and create a zip file containing everything needed for client installation.
- Configure the Sonicwall 300 to send its logs to the Syslog server.
- Configure the Sonicwall 300 to e-mail event notifications to the Network Administrator. Events are reports of blocked probes or attacks.

Set up a Syslog Server

A surplus PC will be re-deployed for use as the Syslog server.

- Install and patch RedHat Linux 7.2.
- Configure the "syslogd" daemon to accept Syslog traffic from the network.
- Turn off unnecessary services.
- Write scripts to move each log file to an archive directory every night at midnight. This creates daily logs making it easier to analyze trends or events.
- Write a script to backup the configuration of both routers.

Define Policies

Write and publish policies designed to enhance and maintain the security of the network and its resources. Management is supporting this effort and we are currently developing policies for the following topics:

- Define the responsible personnel for maintaining the routers, Sonicwall and network servers.
- Define the responsible personnel for maintaining virus engine and signature updates on network servers and PCs.
- Define the personnel responsible for receiving and disseminating security alerts from the various security organizations (SANS, CERT, Bugtraq, etc).

After

The new design of our network reflects a physical and logical separation of network areas and functions. This clear separation makes it easier to incorporate Defense in Depth strategies. The creation of a separate DMZ network isolates our public servers from the internal network. By removing unneeded servers from the DMZ and eliminating unnecessary connections to the internal network we have reduced our vulnerability to attack.

The two added layers of filtering provided by the routers and firewall further enhance our defensive posture. The two routers perform packet filtering on the Internet perimeter and log all blocked traffic. The separate Firewall device provides a second layer of protection against a variety of probes and attacks and further enforces the company security policy. The Firewall e-mails alerts to the network administrator and saves its logs on the central Syslog server. Maintaining patch levels and virus signature files on servers and workstations and hardening the OS adds a third level of defense.

The log information received from the Firewall and routers provides a form of Intrusion Detection. An examination of the logs saved on the Syslog server has shown the effectiveness of our defenses. The Sonicwall logs, in particular, show a variety of probes and attacks previously undetected. The corporate router has blocked and logged packets using port 1434 which could be part of a "SQL slammer" [9] attack as shown below:

"Mar 21 04:32:58 router 449: Mar 21 04:32:00: %SEC-6-IPACCESSLOGP: list 120 denied udp 10.230.214.164(8059) (Serial0 *PPP*) -> 172.16.1.38**(1434)**, 1 packet".

The Sonicwall 300 has blocked and logged address spoofing, port scans and Sub Seven attacks as shown by the alerts below:

03/15/2003 11:25:33.752 - **IP spoof detected** - Source:172.16.10.208, 20392, DMZ - Destination:10.58.4.106, 25, WAN - MAC address: 00.60.08.37.B8.4E -

03/14/2003 15:34:42.192 - **Sub Seven Attack Dropped** - Source:10.37.66.237, 36707, WAN - Destination:10.8.1.130, 27374, WAN - -

03/14/2003 11:56:00.112 - **Possible Port Scan** - Source:10.208.0.15, 11797, WAN - Destination:10.8.1.130, 4480, WAN - TCP scanned port list, 1080, 1180, 1080, 1180, 80 -

03/14/2003 11:56:00.128 - **Probable Port Scan** - Source:10.208.0.15, 11805, WAN - Destination:10.8.1.130, 8095, WAN - TCP scanned port list, 1080, 1180, 1080, 1180, 80, 81, 1182, 3128, 4480, 6588 -.

The policies we are developing to both enhance security awareness and to assign specific security responsibilities acts as an additional layer of defense. Maintenance and security updates are now scheduled events and are performed by assigned personnel. Performance of these duties is now a part of their yearly performance appraisal.

Conclusion

Security is an on-going process, which needs to be continually improved and refined. Our initial security focus was on the perimeter network and our Internet connections. While this has been a good first step, there is still much to be done to improve our overall security. Additional work needs to be done to lock down our public and private servers. Network and host based intrusion detection measures need to be evaluated as well as the addition of a TACACS or Radius authentication server. We are also implementing Microsoft Operations Manager providing us with a central platform to monitor the event logs on our internal Microsoft servers. The implementation of layered defenses has significantly improved network security and contributed to our Defense in Depth.

References

1. CERT. "CERT® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks". 29 November 2000. URL: http://www.cert.org/advisories/CA-1996-21.html

2. Farrow, Rik. "Sequence Number Attacks" URL: http://packetstormsecurity.nl/spoof/ip-spoof-guides/001.txt

3. Cisco Systems. "Strategies to Protect Against Distributed Denial of Service (DDoS) attacks". 17 February 2000. URL: http://www.cisco.com/warp/public/707/newsflash.pdf

4. Rekhter, Y., et el. "RFC 1918". February 1996. URL: http://www.faqs.org/rfcs/rfc1918.html

5. CERT. "Keep operating systems and applications software up to date". URL: http://www.cert.org/security-improvement/practices/p067.html

6. Cisco Systems. "Improving Security on Cisco Routers". URL: http://www.cisco.com/warp/public/707/21.pdf

7. Guardian Digital Inc. "Linux Security Quick Reference Guide". URL: http://www.linuxsecurity.com/docs/REF/ls_quickref/QuickRefCard.pdf

8. Winters, Scott. "Securing the Perimeter with Cisco IOS 12 Routers". 15 August 2000. URL: http://www.sans.org/rr/firewall/blocking_cisco.php

9. Cisco Systems. "SAFE SQL Slammer Worm Attack Mitigation". URL: http://www.cisco.com/warp/public/cc/so/neso/sqso/worm_wp.pdf.