Case 1 Network Design
Abstract

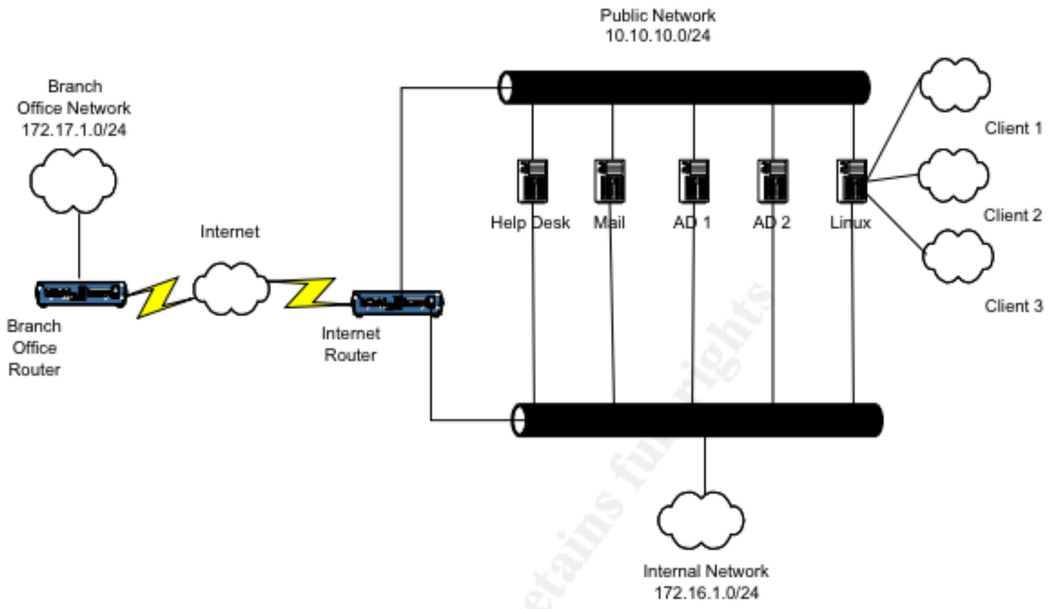
The company in this case is a small consulting firm whose specialty is providing their customers with Microsoft Windows and Citrix networked business solutions.
They believed their internal servers are secure due to their diligence in keeping the Operating Systems up to date with the latest service packs,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

Examination of the perimeter infrastructure showed the network to be virtually defenseless. There is 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. Your proposal is to completely redesign the network perimeter to provide a layered Defense in Depth.

Current 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 is 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.



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 is 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 is permitted.

Branch Office Router

The Branch office router is configured to provide NAT for outgoing Internet traffic, in addition to a VPN tunnel to the corporate router. An inbound access list is applied to the serial interface making it somewhat more secure. The access list is 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 2003 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 2003 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 is forwarded to the internal Exchange mail server, storing it if the internal server is unavailable. This server also acted as a public NFuse front end to the internal Citrix server.

Linux Server

The Linux server runs the Redhat 9.2 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 host 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 is to provide Active Directory services to the PCs in the branch office over the VPN. Without the internal interface, the branch office is 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. Compromised resources on our network could be used to unknowingly participate in a Distributed Denial of Service (DDOS) attack 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.

Logs are not kept of the types or frequency of Internet traffic. Without logs there is no way to determine if the network is being probed or attacked.

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 is built and is maintained by one of the consulting engineers. Patches, bugfixes and other administrative tasks were performed whenever his schedule allowed. There is no one else in the company familiar enough with Linux to assume this responsibility.

There are no written policies concerning the frequency or responsibility for maintaining the security levels of hardware and software.