Global Information Assurance Certification Paper

Walking the Perimeter: Strengthening the First Line of Defense

Introduction

This is a case study of the initial phase of a comprehensive review of the information security posture for a high tech manufacturing environment. The foundations of this review are fundamental precepts of information security practice; defense-in-depth and security as a process. A collection of activities have been identified to review, evaluate, and strengthen existing policies and system and/or network configurations to enhance protection of the company's information assets. This case study addresses one of the initial activities; securing the perimeter. This phase focuses on the Internet and WAN access points connected to the corporate network, the existing firewall implementation, dial-in access and a quick review of the inner perimeter implemented with dual-homed bastion hosts for common services.

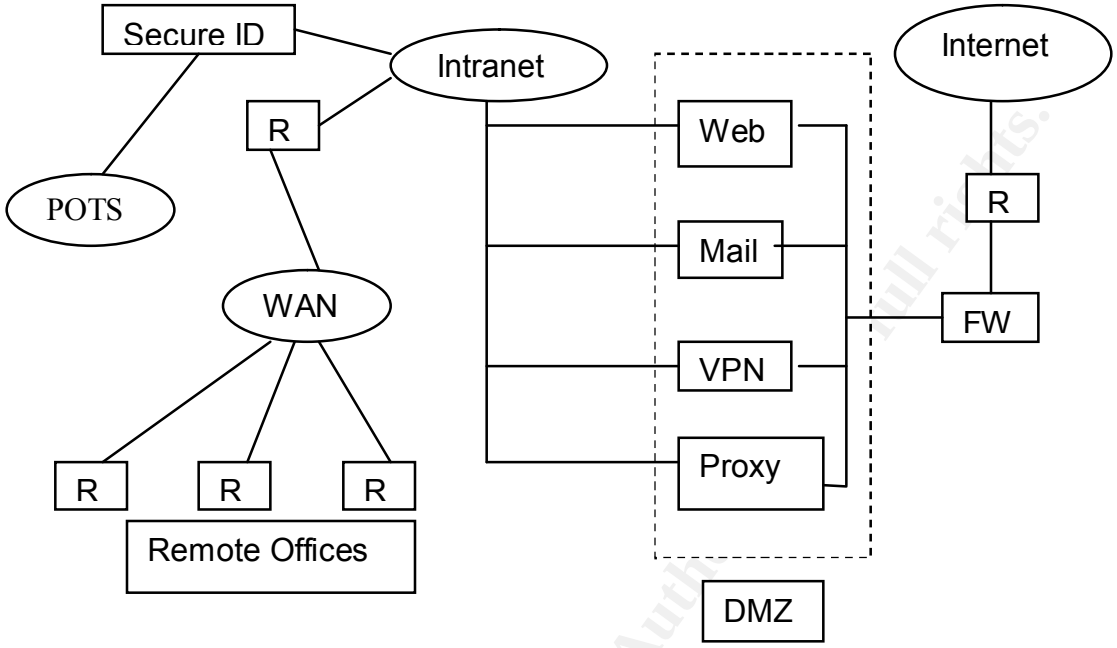
Walking the Perimeter – The "Before" Picture

The corporate network is interconnected with the wild at a number of points:

- WAN links implemented via Frame Relay interconnect the home network with three remote offices. These links are supported at each end by a Cisco router running IOS 11.x.
- The home network is connected to the Internet via two bonded T1 connections that converge at a specialized router used to support bandwidth aggregation and fault tolerance.
- A PIX firewall sits behind the Tiara router to provide stateful inspection of traffic.
- Dual-homed bastion hosts based on Windows 2000 provide a moat between the firewall and the inner sanctum containing the corporate computing and data assets.
- Dial-in is provided via Secure ID for company staff and management and authorized external individuals. A direct dial to a Lotus Notes server is provided for users to access their email directly.

The WAN routers and dial-in access are considered part of the perimeter due to their provision of connectivity between the internal network behind the Internet router, corporate firewall, and DMZ and the wild. Therefore, the concepts of filtering out unwanted traffic and providing a firewall to intrusion are just as critical here. Ignoring these would be like installing heavy armor on the front door of your house while the back door remains unlocked. A pictorial representation of the network and perimeter devices is shown

below.



Initial Assessment

Wide Area Network - Each of the field offices has only a few personnel and contains a two port router to connect its diminutive network to the corporate network at home. In addition, there is a small server at each field office to provide local services (domain login and printing primarily). Clients are typically laptops running Windows 2000 (or perhaps NT).

While there are some issues both with the local server and the laptop configurations those will have to wait until a future case study. Concentrating on the WAN routers, a review of their configuration confirmed my initial suspicions; they had been loaded with a basic configuration but no basic security. There were neither Access Control Lists loaded nor any filtering functions to provide basic protections. In addition, all passwords were stored in plain text in the configuration file (bad idea). Of particular concern is the relative insecurity of physical access – the router and other equipment are in an open office environment. In addition, the router management company providing services for all WAN locations uses dial-up access to manage the routers. A necessary evil in this case, but this makes attention to the issues of physical access and the necessary hardening of the configuration even more important.

Internet Connection - The Tiara router providing the bonded T1 connectivity to the Internet utilizes an operating system and command structure that is Cisco "work-alike". However, the configuration options are not as extensive. Options for protecting the router, its configuration, and the network connected to were not as

extensive. However, access control and protection against basic security issues are available. Since this is our screening router, availability of more extensive protections aren't critical here.

In reviewing the router's configuration, I was pleasantly surprised to see that passwords were not stored with the configuration (unlike Cisco). However, simple access lists to guard against spoofing and insure private addresses don't find their way to the Internet were not implemented. Nor were some simple protections against known issues; small services, ICMP, proxy ARP, etc. that should be part of any standard router configuration. On a good note, logging was enabled on this perimeter router but only captured locally (once the memory was full, events began to be overwritten). However, I don't think anyone had reviewed the logged events in some time and they weren't kept anywhere for historical purposes. In reviewing the router log there was very little to see except some previous logins from ISP tech support personnel as they set up and tested the router connectivity. It was interesting to note that the ftp server had been enabled for the router with a single user (only one is allowed) – presumably this was to facilitate configuration uploads and downloads.

Corporate Firewall – Unlike the Cisco routers used at the perimeter the PIX only stores passwords in their encrypted form – a good default. The firewall had an extensive filtering and access control configuration in place. Not surprising since this afforded a major portion of the protection for the corporate network. However, this configuration was also relatively standard and had not been examined to insure that it met all of our particular configuration and business needs. In addition, the configuration of the firewall (like the perimeter routers) had not been reviewed for some time so any additions and/or modifications that might be desirable or necessary based on new threats had not been incorporated.

In all cases, none of the perimeter routers or the firewall had logging turned on and monitoring was not performed. So far, I felt lucky that we had not had an incident. However, I was not totally convinced since low levels or activity or very good hackers could have penetrated the defenses without our knowing since no scrutiny of ongoing traffic was happening at all.

Dial-In Access - Most dial-in access to the network was provided via Secure ID. This relies on classic principles used to support solid access control; something you have, something you know, something you are. In our case you are issued a token generator, you select a PIN to use in conjunction with that token generator, and are authorized by a company official (member of management) to obtain access. Key practices for managing perimeter defense for this capability involves insuring that phone numbers to the system are not obvious or easily found, monitoring failed attempts to use the system, and removing access for individuals who no longer need it in a timely manner. As with many of the implemented functions and/or capabilities, regular monitoring and scrutiny was not as strong as it needed to be. Since there was only a single dial-in number rather than a

bank of numbers scanning would have to hit on this exactly (but this is not a hard thing to do for a war-dialing program given enough time). The final precaution was implemented already – insuring that the auto-answer did not pick up right away. In our case, there were three rings before the system picked up to make a connection. Determined hackers could still find this number but script kiddies doing fast scans would likely miss it most of the time. A final review of the actual banner provided during a connection revealed a simple message to login and then provide your PIN code. While not exactly a welcome, an updated banner regarding unauthorized access, legal penalties, and the expectation of monitoring and/or auditing would be an easy and useful addition.

Dual-homed Bastion Hosts (The DMZ) - While not covered in this phase at any detailed level, a couple of observations regarding the implementation of dual-homed hosts as part of the perimeter are appropriate. Two elements were reviewed as part of this initial "walk"; the hardening of the individual hosts and the opportunity to use this part of the perimeter as a monitoring point for host-based intrusion detection.

All of the bastion hosts are built on Windows 2000 operating systems. Individual servers provide corporate web, email, proxy, and VPN services. Each had dual NIC's with IP routing disabled. However, while they were hardened in the typical sense the opportunity to apply additional measures within the operating system were not taken (e.g., security templates and auditing/logging). No additional tools were installed on the systems to augment their monitoring/logging capability. If a new Windows 2000 attack became prevalent it would be impossible to know if we were protected. It was assumed that the precautions of the firewall and dual NIC's would provide the needed protection without further intervention.

I think that a healthy dose of paranoia is a good characteristic for an information security professional. Even though it appeared that the basics of securing the perimeter of the corporate network had been applied, there were many things that my paranoia was causing me to worry about. The details of how to address them come next.

Fence Repair – Fixing Holes and Shoring up Posts

Wide Area Network - There are a number of basic additions to a Cisco configuration that can help strengthen a perimeter router. These involve basic filters, access control lists (ACL's), access control, and logging. In general, the following features should be applied to virtually any perimeter router. The following modifications were made to the existing configuration for the routers at the corporate office and in each of the remote offices:

- Local and remote access control to the command subsystems
    - Telnet access – in most cases telnet access is desirable and/or needed to support remote management, etc. In our case, modem

based access is also required for the technical support staff charged with 24X7 monitoring of our WAN connections. In the existing configuration virtually any IP address could telnet to the router and try for access. Given the relative insecurity of the remote office locations I elected to insure that access via the console is restricted and network access limited to a subset of known static IP addresses with further restriction to authorized users where possible.

  - Console port access – there is a known issue with console access on a Cisco router, namely that the password reset feature can be used to obtain privileged access to the router. This is available, during a power cycle and reboot, a break signal is sent via the console port within the first 60 seconds of the reboot cycle. Given the possibility of obtaining physical access to the router in our remote offices I elected to disable this feature. This would eliminate a back door if we lost the password to the router but is preferable to waking up one morning to find that a break-in at the local office resulted in some nasty effects on the corporate network. However, the company providing our tech support had a modem connection into the console port so I moved this to the aux port to support continued remote management.
  - Aux port access – this is now the remote management port available via modem connection and has a line specific password configured for it
  - Passwords – a glaring problem in the existing configuration file related to the storing of the access and enable passwords for the router in clear text in the configuration file. Anyone working on the configuration of the router could inadvertently disclose critical passwords to unauthorized observers or if the router were hacked an attacker could learn the passwords and retain access without us ever knowing. In addition, these passwords were common among all the routers so if inadvertently disclosed or purposely hacked, an individual would have access to the entire set of WAN routers including the home office router directly connected to the corporate network. To strengthen the perimeter here I enabled the ability to store the enable password in its hashed representation. There is a second option that allows for the encryption of all passwords but the encryption algorithm used is weaker. Because of this I elected to provide maximum security to the enable password. In addition, I implemented sound password construction rules as part of the policy for managing access to the router. A further measure under consideration is to provide individual logins for access to the router. However, this will take more time to set up administratively and has not been put in place.

- Disable small TCP and UDP services – these services both provide the potential for giving away information and are popular targets for attacks

(e.g., buffer overflows). These should always be disabled out of hand for these reasons as well as avoiding the implementation of code that uses resources if it's not necessary. Remember the basic rule of thumb; if you don't explicitly need to run a service, make sure it's disabled since most of the time the default is to turn it on. This makes for a leaner and meaner runtime environment as well.

- Disable proxy ARP – proxy ARP was very nice when there were hosts that were not subnet-aware and needed help in everyday communications. That is rarely the case any more so this service isn't very useful. In addition, it can provide a nice way to help potential attackers engage in reconnaissance of your network by providing a simple way to map existing hosts behind a router. This is disabled in the updated configuration.
- Disable IP source routing – it is unlikely that source routing would be a problem for these particular routers since they are buried behind a filtering router, firewall, and dual-homed bastion hosts. However, in the spirit of disabling any useless capability that could potentially be misused, the command to disable this should be part of any standard router configuration. Certainly, this is much more of a problem if the router in question sits on the Internet or could be accessed via the Internet router since an attacker could spoof a legitimate address and specify a bogus return route to establish an unauthorized connection.
- Disable the Finger service – another potential for divulging more information than is desirable. In the same spirit as the source route capability this is disabled just as part of good practice.
- Disable Cisco Discovery Protocol (CDP) – this may be a useful protocol in the interior of a corporate network consisting of multiple routers.
- Disable ICMP redirects – maybe an issue but probably only for the home office router since it is functioning in a larger inter-network environment. However, if something like this gets through the Internet filter, firewall, dual-homed hosts, etc. then we probably have a bigger problem. This is another parameter included to maintain good practice in router configuration.
- SNMP configuration (or better yet, disabling) – if not necessary for network management Cisco recommends this be disabled on any router. SNMP read only access with a unique password is enabled on the WAN routers to aid in monitoring using tools on designated internal systems.
- Filtering
    - DHCP is used for client access in the remote offices but these are restricted to a specific address range. As a precaution, routing of traffic is restricted to/from these addresses only. This provides minimal protection but will at least preclude the attachment of any devices with hard-wired or static addresses without our knowledge. However, spoofing in the range of the allowed DHCP addresses could still happen if physical access to the remote office is compromised. (Actually it would be hard to call this spoofing since we give out the addresses via our own remote DCHP server but

this problem will more likely be solved by policy than technology, e.g., using static addresses on laptops when they are configured for use for the end user).

- Access Control Lists (ACL's)
  - Local addresses – since the remote offices rely on DHCP addresses these are restricted at the DHCP server to use a locally valid range. Access lists at each of the WAN routers are now used to restrict traffic to only these addresses. This will only stop attackers that attach to the local network and have static addresses so a future policy to allow only statically assigned addresses is being considered.
  - Remote access control – access lists to restrict telnet access to the routers in the remote offices have been included to insure that only authorized administrative connections are made from the home network to support remote monitoring and configuration changes. In addition, the remote routers are only allowed to connect to the home router interface to support monitoring and troubleshooting activities. This will reduce the potential for a compromised router in a remote location from getting access to assets either in one of the other remote offices or on the internal corporate network.
- Disable directed broadcast – this will remove the potential for smurf attacks (and is disabled by default beginning with Cisco IOS version 12.0).
- Disable ICMP "unreachable" messages – this will remove a key feature used by attackers to map a target network and will be disabled on the WAN router in the home office. It's less of a problem on the remote office routers and because it may be useful when troubleshooting those connections from the home location I chose to leave them enabled there.

Internet Connection - The Internet connection for the corporate network is through a Tiara router that supports the specialized function of bandwidth aggregation and link fault tolerance. This router has an operating system that is an IOS work-alike with similar commands but not identical. I applied the same precautions used to harden the perimeter routers for the WAN for the Internet router as available. In addition, tailored access control lists were installed at this access point to guard against known vulnerabilities and errant behavior:
Local and remote access control to the command subsystems

- Passwords – One advantage immediately apparent in the configuration of the Tiara is that the password to access the commands for controlling and configuring the router is not stored directly in the configuration file as on the Cisco.
  - Telnet access – privileged access is password protected. Telnet access will be terminated after three failed login attempts and a reconnect will be required before attempting access. While this does not provide a high level of security it can be logged for review later during regular monitoring to highlight multiple failed attempts.

    - Console port access – this router's physical security is higher and it does not support the same password reset mechanism as the Cisco so the console port is configured for use via password controlled access.

- The following are not explicitly disabled from the command line or within a configuration. Unfortunately, there is no documentation on how these are handled by default but given that this router is upstream of the firewall the vulnerabilities these represent are mitigated for internal hosts.
    - Small TCP and UDP services
    - Proxy ARP
    - IP source routing
    - Finger service
    - ICMP redirects
- Denial of Service - There is an interesting capability available on the Tiara that has been configured for extra protection; "denial of service". Although not well documented, this guards against denial of service attacks (presumably by timing out or limiting SYN flood attacks). I haven't investigated this thoroughly yet so this is still a "todo" for later.
- SNMP configuration (or better yet, disable) – if not necessary for network management this should be disabled on any router. While enabled for read-only access on the WAN routers to enable some management it has been disabled for the Internet router.
- Access Control Lists (ACL's) – some basic filtering via ACL's are desirable on this router as follows (incoming=from Internet; outgoing=to Internet):
    - Filter any incoming packets from the Internet with source addresses of the internal network to prevent spoofing
    - Filter any packets (incoming or outgoing) that are in the address ranges allocated to private networks (10.0.0.0 to 10.255.255.255/8, 172.16.0.0 to 172.31.255.255/16, and 192.168.0.0 to 192.168.255.255/16)
    - Filter incoming bootp, DHCP, TFTP protocols
    - Disable ICMP "unreachable" messages – this will remove a key feature used by attackers to map a target network and is disabled on the Internet side of the router. However, it is enabled on the interior Ethernet interface for diagnostics.

Corporate Firewall - The PIX firewall is an amazing machine loaded with capabilities for protecting networks. In a basic two interface PIX firewall there is an "inside" interface (i.e., the internal network connection) and an "outside" interface (i.e., the Internet connection). Normal behavior for a two interface firewall is to allow all outgoing connections and drop all incoming connections by default. Conduits are built to allow for certain types of incoming connections from the "outside" interface. In its default configuration it can do a respectable job at protecting assets and screening prying eyes (when I say default I mean standard and/or default options for filters, access lists, etc. set for the address spaces it is

connected to). However, the basic configuration must still be tailored initially and reviewed periodically to insure the best performance and protection. In this case, the basic setup provided good protection but there were still some weaknesses: Fixup (a Cisco term that allows special handling of certain protocols) included some settings from the default that were undesirable, namely h323, rsh, and sqlnet:

- H323 supports certain kinds of multimedia traffic, most notable VOIP. (Interestingly enough the rtsp protocol was not set for fixup which is more typically used since it supports Real Audio, etc.)
- rsh supports the "rsh" utility for UNIX
- sql for connection to databases

  There is no business reason for these connections to the Internet from internal addresses so they have been disabled.

- Logging was enabled but only locally. A free syslog-like logging utility for Windows NT is available from the Cisco website and will be implemented to allow for logging firewall status and messages to a remote system for review. This will provide another intrusion detection monitor for the DMZ and internal networks.
- ICMP – a conduit was configured to allow ICMP messages from any to any. Since ICMP is undesirable in general this needed to be changed. However, for diagnostic purposes, ICMP echo-reply is useful and, if originating from the inside, would be an acceptable behavior for the firewall. To support this, an access list applied to the outside interface allows echo-reply if the ping originates from an inside address but is expressly disallowed if attempted through the outside interface (the default behavior).

Dial-in Access - Dial-in access to the corporate network is through a Secure ID system on a single phone number. While this could be found by war dialing, an attacker would need to be diligent since the system is set to pick up only after three rings. This screens out the script kiddies and the more diligent types are greeted with the Secure ID login prompt. However, one improvement is to craft a short banner that contains the key elements of sound information policy; access is restricted to authorized individuals, unauthorized access can be prosecuted, and auditing/monitoring can be expected.

A second type of dial-in access has been provided directly to a Lotus Notes server for remote access to email. This was done to support better performance over phone lines than is available via the Web interface to the same environment. This access is problematic in that while access to other network resources aren't available it may be possible to compromise this connection and get access to the server. This risk of this is relatively low since an attacker would first have to find the phone number, successfully guess a username/password combination, and then compromise this access to get dumped into the operating

system or equivalent. However, as with most accessible systems there is also the possibility of a DoS attack even if slim. To improve our posture here the Secure ID system has been upgraded to utilize 56k modems (twice as fast as the direct dial) and these will be used for all dial-in access thereby allowing for the removal of this direct dial. Viola'! Problem solved.

Dual-Homed Bastion Hosts (The DMZ) - The perimeter configuration in this case study includes a set of dual-homed hosts that form the DMZ for the company's internal network. This works quite well with the fixup of mail and web protocols along with conduits for the proxy and VPN servers. Dual-homed servers provide a gap that is hard to traverse but do provide a concern in that once a server is compromised it is a great launching pad for attacks directly into the corporate network. In this case, each of the servers is running a single service that is allowed through the firewall in a specified manner. The most potent threat in this scenario is denial of service from an exploit that disables a server through the well-known service that it is supporting (not far-fetched these days). If this exploit provided a back channel that actually allowed for privileged login to the compromised server there would be real trouble. Since these servers are not on a separate screened subnet this means it is even more critical to insure that the servers themselves are hardened and monitored regularly. The process for this is beyond the scope of this case study. However, given the potential it was surprising to me that, again, no logging was being done at the servers and no rudimentary intrusion detection capability had been installed (especially given all the free tools readily available). For this exercise, I chose to implement a stealth monitor in parallel with these bastion hosts in order to begin watching the environment that they were operating in – more monitoring will be done on the servers themselves once their configurations are reviewed and appropriate hardening steps are taken.

New Perimeter Security Posture

In general, the perimeter was fairly secure with deficiencies in places that provided low level risks. However, with some simple changes, the company's security posture has been improved and our ability to "see" the operational threat environment has been improved. As discussed throughout the previous section, there have been a number of improvements to the existing perimeter. These are summarized below:

1. The WAN access has been tightened up both in terms of protocols allowed and the level of access provided.
2. Protection of the internal network from access by remote office routers that potentially become compromised is now guarded.
3. The lower level of physical security at the remote offices has been mitigated somewhat by protecting the console and telnet access to the routers.

4. The Internet access has been tightened through restriction of both protocols and addresses. Filters that provide for “good neighbor” behavior have also been implemented.
5. The firewall has been improved over its basic configuration through the restriction of unnecessary protocols and restriction of ICMP messages.
6. In all cases, logging has been enabled to help provide ongoing intrusion detection.
7. Dial-in access control is now improved by routing all through an existing Secure ID system.
8. A stealth monitor has been added to the DMZ to allow for further visibility into the threat environment and ongoing intrusion detection.

These improvements have promoted a better understanding of our current capabilities and threats. This allows us to provide a preliminary report to executive management that the perimeter has been evaluated and improved. This also buys us some additional comfort knowing that we need to spend some additional time on developing appropriate, up-to-date policies and hardening key systems. In addition, key technical staff are now more sensitized to the needs and opportunities in improving information security and are more in tune with an ongoing effort to develop comprehensive defense-in-depth and fine tune our practices that will support our information security needs as a process rather than just technology solutions.

References:

Pike, James. “Cisco Network Security”. Upper Saddle River, NJ: Prentice Hall, 2002.
Sedayao, Jeff. “Cisco IOS Access Lists”. Sebastopol, CA: O’Reilly and Associates, Inc., 2001.
Cheswick, William R. and Bellovin, Steven M. “Firewalls and Internet Security”. Reading, MA: Addison-Wesley, 1994.
Tasman Networks. “Command Reference Guide”. San Jose, CA: Tasman Networks, 2002.
Tasman Networks. “System Installation Guide”. San Jose, CA: Tasman Networks, 2002.