Global Information Assurance Certification Paper

Security Assessment at a Bank Holding Company – A Second Look

Tony Hartanto
GIAC Security Essentials Certification (GSEC)
Practical Version 1.4b – Option 2
May 2003

Abstract

I work for a Banking Holding company that is very supportive of securing the company's network infrastructure. I manage the Information Systems department and I am responsible for the Network Security for the company. For the past two years, we have installed Cisco PIX Firewall, Micro Trend's Virus Protection Systems, and Internet Security Systems' Real Secure Network Intrusion Detection Systems. We used Microsoft's Windows as our standard desktops and servers operating systems.

After attending the GIAC Security Essentials classes, I realized that I could apply what I learned from these classes to further improve the security of the company's network. I decided to take a second look at the security of our network infrastructure. With help from outside consultants, we found a number of issues and decided to correct the issues that we determined to be important.

1. The Cisco PIX firewall IOS version 4.2 is out of date and no longer supported.
2. The Outlook Web Access and the Windows NT system being utilized for this has a number of security issues.
3. The Intrusion Detection Systems (IDS) Enterprise database files are corrupted.
4. Apply the appropriate security improvements found in the Windows NT Security Step-by-Step, a survival guide for Windows NT security [1] to improve the security of the Windows NT systems.

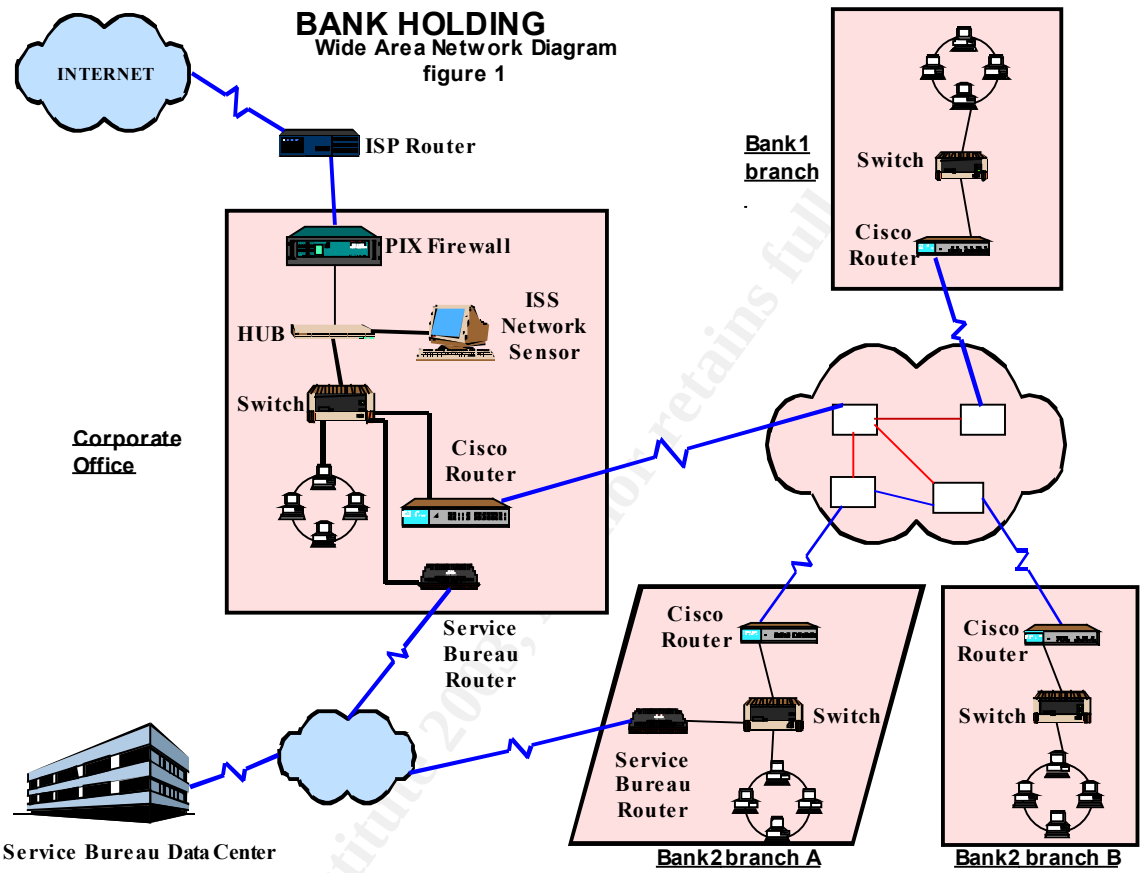
Before

Wide Area Network Design (figure 1)

The holding consists of two commercial banks. The banks are connected through a private frame relay data lines. Cisco routers are installed at the corporate office and each of the banks' branches. We configured all network devices using the 10.x.x.x private network ID. All outbound Internet traffic is routed through the PIX firewall and the ISP router. A Service Bureau router is installed at each bank (bank 1 and bank 2) to route traffic from each bank to the Service Bureau data center. The Service Bureau hosts each bank's clients' database files.

Cisco PIX 520 Firewall

The PIX firewall is installed between the corporate office Cisco router and the ISP router. All inbound and outbound Internet requests from the internal network users are routed through the PIX firewall. The firewall was installed three years ago and due to the lack of personnel and lack of 'Security Essentials' awareness, we have not upgraded its IOS as well as reviewed the event logs.



Outlook Web Access (OWA)

Due to the growing demand from users to access their emails from remote locations (outside the bank's premises) and from users that wish to work-from-home, we installed the Outlook Web Access for Exchange 5.5 on the Windows NT system located at the corporate office. We deployed OWA without considering the potential security risk associated with it.

Internet Security Systems Network based Intrusion Detection System (IDS)

The IDS network sensor is installed to monitor the network traffic from the Internet. A HUB is placed between the firewall and the corporate office Switch and the IDS is connected to this HUB to monitor the network traffic.

Assessment

- No maintenance was ever done to the PIX 520 firewall. During the assessment I found that the IOS software release 4.2 is at "End of Life" status with the Last Support date of June 9, 2003 [2]. Without the latest IOS software release level, the firewall will be ineffective to protect the company's network. Firewall event logs were not reviewed.

- The Cisco PIX Firewall Manager (PFM) program version 4.3 installed on the management workstation could allow an attacker to gain full access to the PIX firewall. The PFM is a program that provides a Web-based configuration interface for Cisco PIC firewalls. PFM stores the enable password for the managed device in plain text in the C:\Program Files\Cisco\PIX Firewall Manager\protect\PFM.LOG file located on the management station. An attacker with access to the management station can recover the password to gain full access to the PIX firewall [3].

- We engaged the services of the outside consultant to conduct the External Network Security Review. The result of the review revealed the following notable security issues specific to the Windows NT system being utilized for Outlook Web Access: [4]

    i. Microsoft Index Server could expose the source code of Active Server Pages (ASP) and other server-side Web files to a remote attacker that has sent specially crafted URL.
    ii. Microsoft Internet Information Server (IIS) version 4.0 is running on this system in what appears to be the default configuration, including FrontPage Extensions.
    iii. HTTP TRACE support is enabled on this system and is typically used for network debugging and troubleshooting. An attacker could use this support to gain information to help launch focused attacks against this server.

- Microsoft Exchange servers that offer the Outlook Web Access service are vulnerable to an information disclosure vulnerability that can reveal any email address stored in the Global Address List. Attackers can exploit this vulnerability to perform unauthenticated searches on sensitive contact information. For example, an attacker could obtain a user's email address by searching on their name [5].

- Even though the OWA user has logged off, a hacker can gain access to the user's Outlook email box if the user fails to close the browser after using the OWA [6]. This is because when a user logs off of OWA, their session does not automatically end. Their credentials are cached in the browser and remain available. If the user uses OWA from publicly shared computers, it can lead to potential security breach if they do not close the

browser after they log off from OWA session. In some situations, browsers on these publicly shared computers are configured so that they cannot be closed.

- The OWA server is deployed behind the firewall. In order to allow the OWA server to communicate with the Exchange server, port 80 was opened in the existing firewall configuration. If the OWA server were compromised, the entire network would be at risk because there is nothing to hinder an attacker once they have gained access to the OWA server [7].

- Due to the 2 GB limit of the MSDE database file size, the Intrusion Detection Systems (IDS) Enterprise database files that include the transaction logs file are corrupted. We were not diligent in reviewing and archiving these logs. Without a working IDS logs, we would have no clues to determine if any intrusion occurred. We would not be able to identify possible points of entry, intrusion or outbound points of traffic and, attack patterns. IDS logs is the type of information that helps to support the company's Computer Incident Response Plan, and its Information Security program. Furthermore, the Comptroller of the Currency Administrator of National Banks in their OCC Bulletin OCC 2000-14 states that the senior management and the board of directors are responsible for overseeing the development and implementation of their bank's security strategy and plan. Key elements to be included in those strategies and plans are an intrusion risk assessment plan, risk mitigation controls, intrusion response policies and procedures, and testing processes [8]. Without a working IDS the company would not be able to effectively implement the security strategy and plan.

- Using the GSEC Security Essentials Windows Security course book (Windows NT Security Step-by-Step, a survival guide for Windows NT security), we assessed our existing Windows NT security policy. We compared our policy with phases of the implementation and operation of an NT system mentioned in the course book. There were some phases that we have implemented and we will implement the phases that would improve our Windows NT security.

During

After completing and reviewing my assessment, I presented my finding to our Information Steering committee. I recommended the changes that need to be done immediately and obtained the budget that is required to implement the changes.

PIX 520 Firewall

We decided to replace the firewall with the Cisco PIX 515E. The difference in cost between purchasing the new PIX 515E and upgrading the IOS and renewing the hardware maintenance contract for the PIX 520 is minimal. We were able to make the following improvement to the new firewall:

- Enable encrypted password for telnet access with the following command: (passwd *password* [encrypted]). The 'passwd' command sets a password for Telnet access to the PIX firewall console [9]. We also assign our own password.
- At the time of implementation (March 2003), we were able to load the latest version of the IOS (version 6.2(2)135. The version 6.0 or later of IOS will resolve the issue with the PIX Firewall Manager (PFM) program vulnerability.
- Remove PIX Firewall Manager program from the NT workstation.
- Enable Cisco PIX Device Manager (PDM). PDM provides administrators with graphical reporting and monitoring tools for both real-time and historical network activity, utilization, and event logs [10].
- Enable the Virtual Private Networking (VPN) features of this new firewall and upgrade from the standard 56-bit Data Encryption Standard (DES) to 168-bit Triple DES (3DES). We are beta-testing the 168-bit 3DES VPN remote access using the Microsoft Terminal Access services. We do not feel comfortable implementing VPN with 56-bit DES. Cracking the 56-bit DES encryption algorithm no longer takes a number of years to achieve; it can now be done in one day, as was demonstrated by a hacking group participating in RSA Data Security's yearly DES Challenge contest [11]. My GSEC class instructor also mentioned that DES is not considered secured in today's environment.

Corrective Actions taken to the result of the External Network Review

- We obtain and apply the appropriate patch as listed in the Microsoft Security Bulletin MS00-006 to resolve the Microsoft Index Server vulnerability [3]. The download location is at: http://www.microsoft.com/downloads/release.asp?ReleaseID=17727
- We obtain and apply the latest service release for FrontPage Server Extensions which can be found on the Microsoft Web site at: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnservext/html/fpovrw.asp
- We will disable the HTTP TRACE support using the Microsoft URLscan Security Tool as recommended by the consultant.

Outlook Web Access

The result of the assessment on the existing Outlook Web Access (OWA) deployment and the report of the External Network Security review pointed out a

number of security concerns with OWA. I will propose two possible solutions to replace the OWA server. I will point out what is involved in implementing these solutions:

1. Install e-Gap Webmail Appliance from Whale Communications [12].

   The e-Gap Webmail Appliance provides a secure front end to Exchange 5.5 enabling Outlook Web Access from any browser anywhere. It is a cost-effective, rapidly deployable alternative to traditional VPNs. How does this appliance address the security concerns of OWA?

   - Web server vulnerabilities - The e-Gap Webmail Appliance addresses these vulnerabilities by performing application-level inspection, and checking that only proper, correct, and expected URLs and associated parameters are allowed to reach the webmail server.
   - Insecure log-off - e-gap Webmail has a Secure Logoff feature to ensure that when a user clicks Logoff he/she is really logged out, that credentials are not cached on the local machine and that subsequent attempts to access the webmail system require authentication.
   - Open port 80 - The e-Gap Webmail Appliance allows only application-level information to flow into an organization's internal network -- without requiring the opening of any ports from the Internet or DMZ to the back office.

   This option will involve the approval of additional budget to purchase the required hardware and software. However, there will be little if any user training. User will be able to check their emails from any computer terminal.

2. Remove Outlook Web Access capabilities and required users who wish to access their email from remote location using the newly installed Cisco PIX 515E firewall's VPN and Microsoft's Terminal Access Services. There will be no additional cost to purchase hardware or software if we select this option. The VPN is part of the Cisco PIX 515E firewall. However, if the user does not have a computer with at least Windows 2000 Professional operating system, additional Terminal Access Client software is needed. The drawback for this option is that VPN client software must be installed on user's computer. The user will not be able to access their emails from any public terminal if the terminal does not have the VPN client software.

Which solution we will implement will depend on whether our users have a business need to access their email anytime, anywhere and from any public terminal. My observation is that most of our OWA users access their emails from

their personal home computer or the company's assigned portable computer. All the users that make business trip have company assigned portable computer. I will recommend implementing the VPN solution to our committee.

Intrusion Detection System (IDS)

- Use the osql utility [13] command interpreter to delete even data (transaction logs) from the Enterprise database. (Author's Note: Not only that we refer to the osql utility document from Microsoft to maintain the database, we also used our SAFESuite Deployment document from ISS Consulting Group which describes how to maintain the Enterprise database).

- Assign responsible personnel making sure that:

    i. The IDS Management Console is reviewed periodically throughout each workday to identify important security events and to ensure that sensors are still active.
    ii. The 'text' only reports, which display in detail every event that has been logged for the specific period, are run at least weekly.
    iii. The graphical reports, which often are effective at viewing trend information or obtaining an overview of the threat traffic, are run at least weekly.
    iv. Updates from ISS are installed and applied as they become available.
    v. The Enterprise Database files are archived before they reach the 2GB file size limit.

Windows NT Security

At the time of this Security Assessment project, we were completing the project to upgrade all desktop computers' operating system to Windows 2000 Professional. We implemented the following to improve our Windows NT systems:

- Use the logon message to warn uninvited users that they are not allowed and to warn authorized users that they must use the system only for approved purposes.

    For Windows NT, we made the following change to the Registry key.

    Hive: HKEY_LOCAL_MACHINE
    Key: \Software\Microsoft\Windows NT\Current Version\Winlogon
    Name: LegalNoticeText
    Type: REG_SZ
    Value: <text message that we used>

- Install the passprop.exe utility that will lock out the Administrator account after repeated failed access attempts over the network, but never locks the account out at the console.
- Rename the Administrator account to some other name and create a new user and make them a member of the Administrator group.
- Create a bogus account called Administrator without administrative privileges.
- Enforce the Strong passwords policy using the passfilt.dll password filter. The dll implements the following restrictions: [14]

    - Passwords must be at least 6 characters long.
    - Passwords may not contain your user name or any part of your full name.
    - Passwords must meet at least 3 of the following criteria

        i. Include uppercase letters (A-Z)
        ii. Include lowercase letters (a-z)
        iii. Include numbers (0-9)
        iv. Include non-alphanumeric characters (ex: !, #, etc.)

- Enforce password protected screensaver policy.

After

The changes that were implemented have made our network to be more secured and less likely to be compromised.

We have a new firewall with the latest release of IOS. Known vulnerabilities to the previous firewall have been removed. We require Telnet user to the firewall console to enter the Telnet access password.

We conducted the Independent External Network Review that pointed out the vulnerabilities of our existing network. This review provides the management with reasonable assurance that assets are safeguard against loss and unauthorized use or disposition.

The proposed solutions to the Outlook Web Access security concerns gives the management the understanding of why the current OWA deployment is not secured and why we must deploy the recommendation that was presented.

We now have an Intrusion Detection System that is working. It will help support our Incident Response Plan. It gives us additional way to know when our network is compromised.

With the addition of the Windows NT security tools and policy, our Windows NT system is much more secured.

Conclusion

Security is an on-going process that needs to be continually improved and refined. Security is extremely dynamic in nature. The effectiveness of the controls and security measures that we put in place do not provide total assurance that our network will not be compromise. Additional work needs to be done to improve our network security. For example, we need to effectively capture and archive the Windows NT servers' event logs and the Cisco routers logs to support the Incident Response plan. We are implementing the email filter for SMTP to prevent sensitive information from being sent out of the company and to prevent malicious code from entering our network through email attachment.

I am glad that I took a 'second look' at our network security infrastructure. This process has significantly improved our network security.

References

1. SANS INSTITUTE Track 1 - SANS Security Essentials + CISSP CBK Manual. 1.5 SANS Security Essentials V: Windows Security.
2. “End of Life for PIX Firewall Release 4.2, No. 1119” July 12, 2000. URL: http://www.cisco.com/en/US/products/sw/secursw/ps2120/prod_bulletin09186a0080091b37.html
3. "Cisco PIX Firewall Manager plaintext password". October 11, 2001. URL: http://www.iss.net/security_center/static/7265.php
4. RSM McGladrey, "XXX Holding Company - External Network Review". May 2003. (External Network Review Report)
5. “Microsoft Exchange Outlook Web Access fails to authenticate users when searching the Global Address List.” September 12, 2001. URL: http://www.kb.cert.org/vuls/id/111947
6. “See how easy it is to hack a CEO’s mailbox (java viewlet).” URL: http://www.whalecommunications.com/site/SFunctions/Viewlets/2282.EN.ver1/webmailfinal_viewlet.html
7. "Options for Securely Deploying Outlook Web Access" page 4, April 6, 2003. URL: http://www.sans.org/rr/paper.php?id=873.
8. "OCC 2000-14 Infrastructure Threats-Intrusion Risks---Message to Bankers and Examiners". May 15, 2000. URL: http://www.occ.treas.gov/ftp/bulletin/2000-14.doc
9. Cisco PIX Firewall Command Reference Version 6.1.
10. “Cisco Secure PIX Firewall – Dedicated Firewall Appliances With Built in IPSec Encryption”. February 14, 2002. URL: http://www.products.datamation.com/networking/vpn/916161236.html
11. "Cracking DES code all in a day's work for security experts". January 21, 1999. URL: http://www.cnn.com/TECH/computing/9901/21/descrack.idg/
12. "Secure browser-based access to MS Exchange data...anytime, anywhere". URL: http://www.whalecommunications.com/site/Whale/Corporate/Whale.asp?pi=32
13. "osql Utility" URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/coprompt/cp_osql_1wxl.asp
14. "How to Enable Strong Password Functionality in Windows NT [Q161990]" June11, 2002. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;161990