



International Bank

Remote Penetration Test Assessment and Results 2003

By: Mederick Jones
Sr. Security Engineer

Table of Contents

Table of Contents.....	2
1. Introduction.....	3
1.1. Overview	3
1.2. Objectives	3
1.3. Current Situation.....	4
1.4. Problems / Needs	4
2. Status of Environment	4
3. Engagement	9
3.1. POP3	9
3.2. SMTP	10
3.3. FTP.....	11
3.4. DoS.....	12
3.5. FrontPage / Sambar ISAPI	13
3.6. IIS.....	14
3.7. DNS	17
3.8. Firewall	18
4. Conclusion	19
4.1. Summary of Objectives.....	19
4.2. Conclusion.....	20
4.3. Special Notes.....	20

1. Introduction

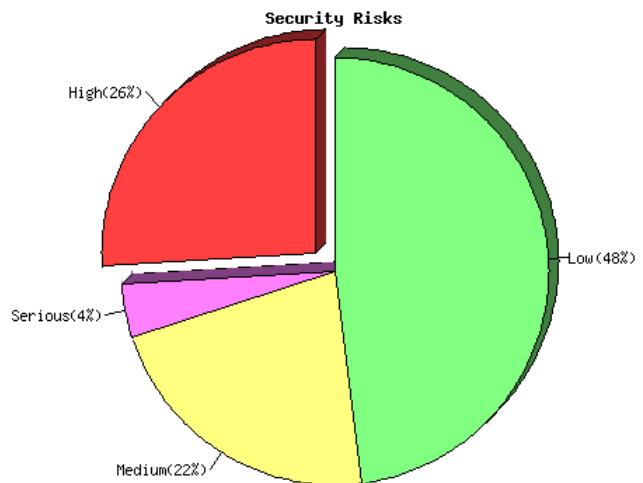
NetMD is a collective of Internet Network Security Engineers (INSE) and network security gurus that have advanced backgrounds in networking, application development, web programming and Internet security. Our elite group of engineers and developers are continually working with and developing advanced network and security technologies. By continually doing research and development on emerging network and security technologies, we are able to enhance our technical skills to meet the most intensive network and security issues.

Each of our people has years of experience in developing and implementing secured Internet network architectures. Our documentation and security auditing skills is unsurpassed in detail and insight. Combining this with our extensive knowledge of Black-hat hacker techniques and exploits makes our NetMD staff of White-hat network security experts, the best in the network security industry.

NetMD combines all this with our professional and experienced management team to provide you with the highest level of secure network and Internet security solutions for your business network, E-commerce application or Internet services.

1.1.Overview

The International bank requires remote internet penetration testing to confirm the overall security of there Branch Office communication systems as well the home banking and Corporate Head Quarters. The Name of the organization to be assessed was provided via third party to NetMD. At no time did NetMD have any internal information communicated from the International Bank. These steps insured the integrity of the assessment.



1.2.Objectives

Due to government regulations and commitments to their customers to provide secure transactions, The International Bank contracted \$\$\$\$\$ to perform a remote penetration test against their internal network and their Internet point of presence.

The overall scope of the engagement was to provide International Bank with a snapshot of their security, as it presently exists. The objective of the test was to identify any serious vulnerability in their Internet and network infrastructure. Additionally the engagement will provide International Bank with recommended solutions for fixing any vulnerabilities or security risks to their network or Internet point of presence.

1.3.Current Situation

Because of the growing risk of internet fraud and identity theft International Bank elected to under go a complete remote penetration test to verify it's current network and home banking security levels. This audit has completely assessed the current state of the network and identified the needs of the organization to better protect and serve it's customers.

1.4.Problems / Needs

- Identify risk exposure to Denial of Service attacks.
- Identify risk exposure to remote attacks against network services.
- Identify risk exposure to remote attacks against operating systems vulnerabilities.
- Identify risk exposure to remote attacks against the Internet point of presence and associated Internet services.
- Identify all other vulnerabilities that may compromise banking data.

2. Status of Environment

The environment this document outlines is based on our recognizance of the network. We were provided no prior information from the International Bank or it's agents. All data was obtained solely by our own means. By gathering involuntary information from Palau National Communication Corporation and through remote mapping of the network, we were able to arrive at this model, which is perceived as follows from a remote point of view.

The environment of the International Bank is based on common internetworking designs. We Identified 3 separate networks that constituted the entire Internet Infrastructure of the organization. The International Bank currently has a peering Agreement with UUNET and derives ISP and Hosting Services from IT&E Overseas, Inc or (ite.net) whose upstream provider is Alter.net. UUNET also provides address space to IT&E Overseas. We have identified these Net blocks as significant to the organization.

ARIN <http://www.arin.net>

UUNET Technologies, Inc. UUNET1996B (NET-0.0.0.0 – 0.0.0.01)

0.0.0.0 – 0.0.0.0

IT&E Overseas, Inc. UU-208-0-0 (NET-208-0-0-0-1)

0.0.0.0 – 0.0.0.0

UUNET Technologies, Inc. UUNETCBLK228 (NET-0.0.0.0 – 0.0.0.0)

0.0.0.0 – 0.0.0.0

IT&E Overseas, Inc. UU-205-0-0 (0.0.0.0 – 0.0.0.0)

0.0.0.0 – 0.0.0.0

APNIC <http://www.apnic.net>

BANK UUNET ***** Non-Portable Customer Assignment
0.0.0.0 – 0.0.0.0

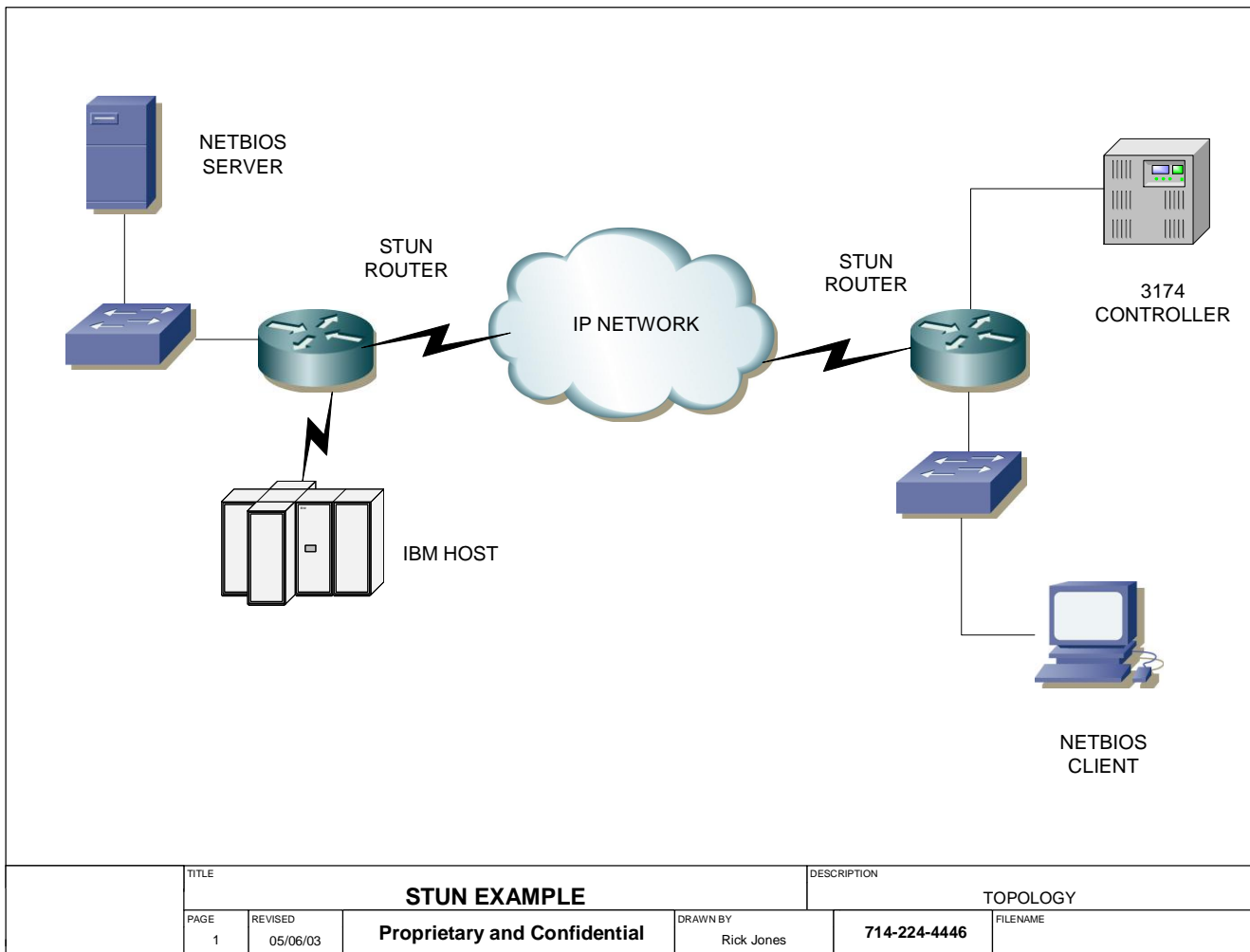
TALAYA2000 IT&E OVERSEAS, INC.
0.0.0.0 – 0.0.0.0

Current Internet Traffic is passed through a router to a firewall and then split into two sections: a Demilitarized Zone (DMZ) and a Private Network. This design is considered to be amongst the most secure. It makes servers easily accessible in the DMZ while it protects workstations belonging to the company from outside users. All traffic must be passed through the firewall, as it is the single point of entry on the network. This allows for inspection of packets and use of firewall rules to allow and deny certain connections. The design theory implemented here is sound however the actual implementation is flawed.

The first point of entry onto the network is router. The router has an IP address 0.0.0.0. This is the router that provides all access to the Internet from the ISP. It is unclear if the router is owned by International Bank or the ISP.

The firewall shielding the entire network is Reported as a Novell 5.1 SP3 Box which we believe is running Boarder Manger 3.5 or above. The outside Interface IP address of the firewall is 0.0.0.0. This firewall is improperly configured.

There is a second Router that is acting as a firewall located at IP address 0.0.0.0. This Router is a Cisco 3600 running IOS Version 12.2 and possibly the Firewall Feature Set is Enabled. This device is configured for STUN or Serial Tunneling Protocol. STUN permits you to use IP as a transport for Synchronous Data Link Control (SDLC) frames across a WAN or other media network. This eliminates the need to have an additional leased line or POTS. We assume this point of access to be a link between branches or a provision for remote access. We were able to penetrate the Cisco Router to some degree. Here is an example network using STUN.



We identified several hosts to attack using a common port scanning tool. The First was the Mail server with IP Address 0.0.0.0 This Server is running Windows NT 4.0 and SLmail 5.5.0. The Second host of note was the IBM AS/400 running a Web Server for Home Banking. The AS/400's IP address is 0.0.0.0. We also noted an IIS Server with a modified banner page running on IP address 0.0.0.0. The STUN router IP was provided and the Development Website was discovered during our scans. A listing of the hosts scanned open ports and banner pages are below.

HOSTS

- 200.0.0.0 Firewall
- * + 0.0.0.0
- |___ 25 Simple Mail Transfer

```

|___ 220 *****.com SMTP Server SLmail 5.5.0.4433 Ready ESMTP spoken here..
|___ 110 Post Office Protocol - Version 3
|___ +OK POP3 server bogina01.bank.com ready
<04112.685059765@*****.com>..
|___ 180 Intergraph
* + 0.0.0.0
|___ 22 SSH Remote Login Protocol

+ 0.0.0.0
|___ 80 World Wide Web HTTP
|___ HTTP/1.0 200 Document follows..Server: IBM-Secure-ICS-AS400/4.1..Date:
Fri, 02 May 2003 10:37:33 GMT..Content-Type: text/html..
+ 0.0.0.0
|___ 80 World Wide Web HTTP
|___ HTTP/1.1 200 OK..Server: apache ver 2.0.35..Content-Location:
http://172.16.0.30/homebank.htm..Date: Fri, 02 May 2003 00:39:09

* + 0.0.0.0
|___ 21 File Transfer Protocol [Control]
|___ 220 baracuda Microsoft FTP Service (Version 4.0)...
|___ 25 Simple Mail Transfer
|___ 37 Time
|___ .JT.
|___ 80 World Wide Web HTTP
|___ HTTP/1.1 200 OK..Server: Microsoft-IIS/4.0..Content-Location: http:// 0.0.0.0
/index.htm..Date: Fri, 02 May 2003 20:31:13
|___ 135 DCE endpoint resolution
|___ 443 https MCom
|___ 465 ssmtp
|___ 1027 ICQ?
|___ 8080 Standard HTTP Proxy

* + 0.0.0.0
|___ 1720 h323hostcall
|___ 1990 cisco STUN Priority 1 port
|___ 1991 cisco STUN Priority 2 port
|___ 1992 cisco STUN Priority 3 port
|___ 1994 cisco serial tunnel port

```

Perhaps the most vulnerable server and common service used on the Internet is the webserver. Through WHOIS and DNS lookups we found this machine to be at IP address 0.0.0.0. This machine is a Windows NT 4.0 computer using the IIS 4.0 package for providing web services. A trace route verified this server is hosted at a separate facility operated by IT&E Overseas, Inc. The NT 4.0 webserver hosts the main Internet website for the Bank of www.^^^^.com

Registrant:
International Bank (#####-DOM)

#####

Domain Name: ??????????.COM

Administrative Contact:

#####

Technical Contact:

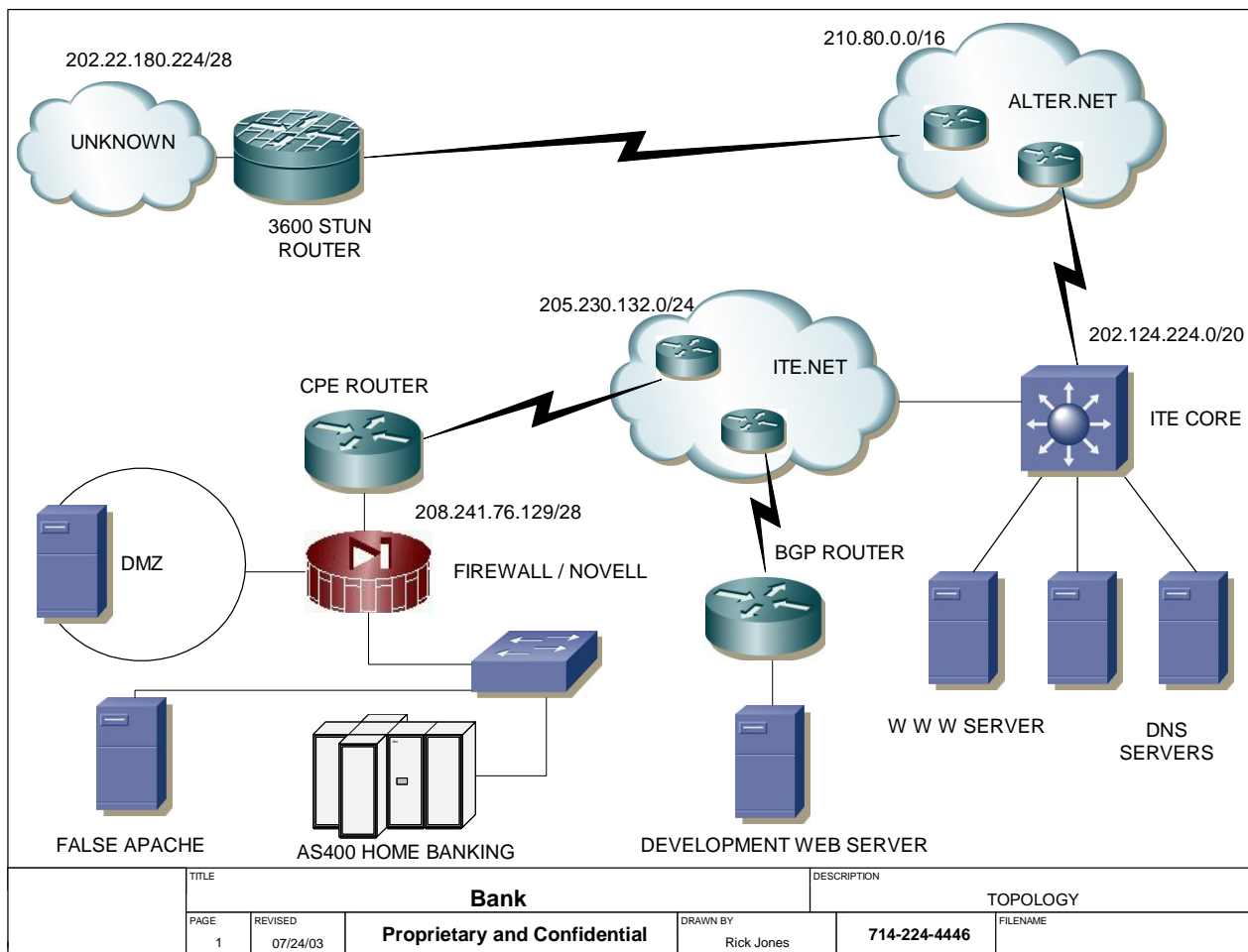
#####

Record expires on 24-Jul-2004.
Record created on 23-Jul-1.997.
Database last updated on 6-May-2003 13:42:33 EDT.

Domain servers in listed order:

NS1.BADISP.NET 0.0.0.0
NS2.BADISP.NET 0.0.0.0

We were able to locate the rest of the network by transferring the International Bank Zones from the ITE.NET DNS servers listed above. These servers provided us with the locations and IP addresses of any other servers we were not aware of. Here is the network map we were able to derive from the information we gathered unobtrusively.



3. Engagement

The audit involved conducting a remote penetration test targeting various services running on the International Bank’s Internet Infrastructure. Here we address each service noted running and its compromise or vulnerability.

3.1.POP3

3.1.1 Definition

POP3, or Post Office Protocol Version 3, is designed to allow remote users to easily retrieve e-mail from any POP3 compatible e-mail client. POP3 is used by most ISP’s for mail retrieval and is not of form of secure data delivery.

3.1.2 Approach

Our goal was to identify buffer overflows for Denial of Services and gain POP mail account access to the server to send and receive mail or view another email users mail on the system.

3.1.3 Positive Results

SL Mail is a strong mail server product it support many security features such as message tracking and management, content and virus filters, pop relay authentication and anti-

spam capabilities. The server is located behind a firewall providing it's OS some level of protection. Note that **POP3 Passwords are always sent in clear text.**

3.1.4 Negative Results

The mail server at IP address 0.0.0.0 was an easy target based on the Personal information about the Branch Managers listed on the International Bank website. http://www.^^^^^^.com/about_bog/branch_managers/ and senior Management http://www.^^^^^^.com/about_bog/senior_management/. This information provided us with the usernames or 1/2 of the mail server account information we needed to break into the mail server. We created a username list using the first letter of the first name and last name of these real people and visa versa.

Example: cynthiaq & cqueball

We were able to authenticate to the pop mail server using a list of 27 usernames and a password list of 125,000 common passwords. Of the 27 usernames we positively authenticated 12 within 3 hours. These speed at which this was done is due to the information provided by the website and the fact that the mail server is not configured to rate limit or drop sessions that fail to authenticate.

The remote POP3 server also leaks information about the software it is running, through the login banner. This may assist an attacker in choosing an attack strategy. We found a number of Buffer overflow vulnerabilities specific to this product.

<http://www.google.com/search?q=Smmail+buffer&hl=en&lr=&ie=UTF-8&oe=UTF-8>

3.1.5 Recommendation

If POP3 access is to be allowed at the firewall, we recommend dropping all incoming packets to the POP3 server that are not specifically allowed. The bank should authorize external access to the POP3 Server by IP address. Dropping the packets will show an attacker that there is no service running at all, thereby protecting network configuration information. Also all POP3 mail account passwords should be more complex and should not be the same passwords used to access other more sensitive systems. We noted a number of accounts with common first names for passwords.

3.2.SMTP

3.2.1 Definition

SMTP, Simple Mail Transfer Protocol, is a protocol for sending e-mail messages between servers. Most email systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an email client using either POP or IMAP. In addition, SMTP is generally used to send messages from a mail client to a mail server. This is why you need to specify both the POP or IMAP server and the SMTP server when you configure your e-mail application

3.2.2 Approach

SMTP is almost impossible of all internet super applications to secure properly. It can be used as a relaying point for spammers or hackers wishing to hide their identity while sending e-mail. SMTP can be used to demoralize the organization as a whole by accepting and delivering email with false credentials.

3.2.3 Positive Results

SL Mail is a full featured MTA (Mail Transfer Agent) that is well supported and Flexible. This mail server is a strong alternative to Lotus Notes and Exchange. The mail service is running behind a firewall that affords the Servers OS some level of protection.

3.2.4 Negative Results

The mail server advertises its type and version in the banner page. This page should be modified to reduce the information given about the server. The server is configured to accept email from any email address for any valid user. This a common configuration and a large problem with mail servers today. Here is an example of us exploiting this configuration issue.

```
220 host.bank.com SMTP Server SLmail 5.5.0.4433 Ready ESMTP spoken here
helo
250 host.bank.com
mail from:aGuerrero@ host.bank.com
rcpt to:tBernardo@ host.bank.com
250 OK
data
354 Start mail input; end with <CRLF>.<CRLF>
test
.
250 OK, submitted and queued. (822A8B8D7F0F11D7821F00A0C9311BDC.SKM)
```

There server is configured to prevent open relay access from unauthorized users see below however allows you to relay to with valid accounts on the system. This vulnerability specifically relates to fraudulent emails being created by any one from anyone to actual mail server users.

```
220 host.bank.com SMTP Server SLmail 5.5.0.4433 Ready ESMTP spoken here
helo
250 host.bank.com
mail from:aGuerrero@ host.bank.com
250 OK
rcpt to:mjones@net-md.net
571 mail relay is not allowed
```

3.2.5 Recommendations

Although it may affect performance of the mail system we suggest that the MTA only accept email for servers with valid MX or Mail Exchanger records. This will prevent the MTA from delivering messages with invalid domain names. Enable message tracking to ensure properly logging of email message origin for reference when dealing with inappropriate interoffice email or fraudulent email situations. Good logging and message tracking is you only defense against email fraud.

3.3.FTP

3.3.1 Definition

FTP (File Transfer Protocol) is a protocol on the Internet to allow the easy transfer of files from one machine to another. FTP was designed early in the days of the Internet when there was little threat from hackers and security was not built into most applications by design. FTP daemons are still designed with many inherent flaws which make them easily

susceptible to attacks such as Denial of Service and buffer overflows which can lead to a root compromise or a system crash. FTP servers can also be used to attack each other. This is referred to as a bounce attack.

3.3.2 Approach

FTP is an often-misconfigured service that allows anonymous users to upload and download files with no authentication mechanism in place. We check for this service, which is frequently, abused by hackers for free storage, or root compromise. FTP Usernames and passwords are transmitted in Clear Text.

3.3.3 Positive Results

0.0.0.0 was configured to block anonymous ftp access and allow only privileged users, which provides good security.

3.3.4 Negative Results

0.0.0.0 server is running the barracuda Microsoft FTP Service (Version 4.0) which comes with IIS4. The patch level of the FTP server is below the current patches provided by Microsoft. We confirmed a well known buffer overflow attack on the FTP server. Please refer to CVE : [CAN-2002-0073](#). We also noted that we were able to connect to the server and continually attempt to authenticate with out our connection be dropped or rate limited. This presents the opportunity to perform brute force and dictionary password cracking attacks against the server at high speeds.

3.3.5 Recommendations

Recommendation for 0.0.0.0

This server is hosted at IT&E Overseas, Inc. The server itself has many security issues associated with it. We would recommend that your website be relocated onto a different server that has been properly hardened. The FTP service on the webserver may not even be needed by the Bank , in such case removing the FTP access to bank resources all together is a recommended. Should the bank need FTP on Windows we recommend staying away from Microsoft FTP and using a FTP server product that provides better control like Bullet Proof FTP Server located at <http://www.bpftpserver.com/index.php>. If the bank transmits and stores sensitive data using FTP we recommend migrating to SFTP for encrypted data transfers.

3.4.DoS

3.4.1 Definition

A DoS (Denial of Service) disallows use of network or computer resources. DoS attacks are based on flooding service with multiple valid and/or invalid requests. DoS attacks are not necessarily hacks; computers are not broken into. They can however be just as dangerous when they deny access to your web site or other internet services over extended periods of time.

3.4.2 Approach

During the penetration test, we noted DoS vulnerabilities on the network and identified the types of attacks that could be used to paralyze critical information flow. These types of attacks varied from buffer overflow attacks to DNS denial of service attacks.

3.4.3 Positive Results

The AS/400 we found to be properly configured and we were unable to perform any type of denial of service attack against this system at base levels.

3.4.4 Negative Results

The Windows NT 4.0 server with IP address 0.0.0.0 was host to many of the vulnerabilities associated to DoS attacks. This server we believe is not under the direct responsibility of the International Bank and is subject to the jurisdiction of the ISP. The other denial of service vulnerability of note again falls under the responsibility of the ISP. This vulnerability lies in the insecure configuration of the DNS servers hosting the bank.com domain. (see 3.7 DNS) One highly exploitable software package running on the Windows NT 4.0 web server was SAMBAR. Sambar is a web development application. This port was open to the internet. We were able to access it's administration pages as well as browse it file system. Please refer to: <http://0.0.0.0:8080> and <http://packetstormsecurity.nl/0009-exploits/sambar-http.txt>

3.4.4 Recommendations

We recommend migrating DNS to a more secure hosting provider. We also recommend hosting the www.bank.com website internally where the organization will have more control over the patch levels and web server configuration.

3.5.FrontPage / Sambar ISAPI

3.5.1 Definition

FrontPage, as explained by Microsoft, is a web site creation utility. It allows a user to create dynamic content quickly and with little knowledge how web site programming works.

3.5.2 Approach

Web Site Defacement

A dangerous feature of the FrontPage product is an automatic update. Files will synchronize with the computer they are being created from to ensure the most recent files are on the web site. However the authentication method is stored on the webserver itself in a DES encrypted file. This was the first easy target in mind to quickly deface the webserver. Surprisingly, the file did not exist. With the current updates from Microsoft, the authentication method was changed or moved. The quick defacement issues with FrontPage are not a problem with the current state of the network.

File Browsing

Many FPSE Vulnerabilities lie in the sample files found on the server after a default installation of IIS. Some of these vulnerabilities include the browsing of files that normally you would not public access to=. With FrontPage and Sambar, files are kept on the webserver that list files and directories managed by FrontPage and Sambar.

File Execution

FrontPage operates through a translation-based scripting language. A single binary takes a file and translates actions based upon the contents of the file. The binary that does this is called shtml.dll or shtml.exe. This is a required file for the FrontPage Extension to work properly. Based on the configuration and patch level of the server, files are capable of being executed remotely.

3.5.3 Positive Results

None

3.5.4 Negative Results

From our findings, the FrontPage extensions of IIS are insecure. Since the site itself is comprised primarily of ASP and HTML code there is no reason to have FPSE installed on the server. We used ISAPI to exploit the server by listing drive contents and website structure. This attack provided the ability to view the file system and execute files.

<http://www.bank.com:8080/search.dll?search?query=/&logic=AND>

3.5.5 Recommendations

Remove Sambar and Front Page Server Extensions. Upgrade Web Server and harden system. Disable unneeded services. You can use this tool to remove unneeded services. <http://www.microsoft.com/windows2000/downloads/recommended/iislockdown/default.asp>

3.6.IIS

3.6.1 Definition

Internet Information Services (IIS) is the Microsoft solution to enterprise grade web serving. IIS is interfaced through a Management Control Console that allows graphical configuration of the services. IIS controls the web site, ftp, and FrontPage extensions, as well as any other ISAPI extensions used. These extensions are for ease-of-use. They make creating and implementing web sites much easier. However, these extensions can become security flaws very quickly.

3.6.2 Approach

The first test for IIS is a common vulnerability in extra files. The files come by default with all IIS installations. This was going to be the first attempt to enter the system. IIS creates a folder called scripts, located in the root directory of the Inetpub folder. The scripts are nothing more than files that make certain tasks easier. Attempting to access the scripts folder failed, it had either been hidden or removed. The scripts files are not necessary for WebPages. A similar folder is the cgi-bin. Many times a poor webserver will allow read/write/execute of this folder to all users, which allows anyone to execute the scripts. These scripts once again commonly have security vulnerabilities. This folder did not allow us access to even view its contents.

The next common vulnerability lies in a method called directory traversing. A poorly configured webserver will allow a user to execute files in different folders on the computer. Again, this did not work, the webserver has been properly configured to disallow directory browsing which leads to directory traversing. The two methods commonly used for fixing this are disable directory browsing or, move the root directory of the webserver to a different drive that is not the C drive.

The last test was a check against the common running ISAPI extensions. As stated before these extensions make working with the webserver much easier. A recently vulnerable extension is the ISAPI printer extension, which allows printing through the web. A buffer overflow in this file allows any user to run commands on the system.

3.6.3 Positive Results

The only IIS server we noted to be secured was the server with IP address 0.0.0.0. This server had been locked down and even the Banner page was modified to display HTTP/1.1 200 OK..Server: apache ver 2.0.35.

3.6.4 Negative Results

While it was nice to see the changed banner of this IIS server to match that of an apache server, the banner was incorrect, and gave away the server as a non-apache server immediately. We also noted other differences that you can improve upon if deception is the goal. Keep in mind that even the "ETag" header gives away the web server in use. Also note that the INTERNAL address of this server was disclosed by only sending it an HTTP header, this could be considered a miss-configuration or a network design problem.

Simulated Apache Banner	Real Apache Banner
HTTP/1.1 200 OK Server: apache ver 2.0.35 Content-Location: http://172.16.0.30/homebank.htm Date: Fri, 02 May 2003 03:37:53 GMT Content-Type: text/html Accept-Ranges: bytes Last-Modified: Tue, 18 Feb 2003 00:39:22 GMT ETag: "5c72362ee6d6c21:2988" Content-Length: 14146	HTTP/1.1 200 OK Date: Fri, 02 May 2003 04:24:00 GMT Server: Apache/2.0.35 (Unix) Content-Location: index.html.en Vary: negotiate,accept,accept- language,accept-charset TCN: choice Last-Modified: Fri, 04 May 2001 00:01:18 GMT ETag: "10876-5b0-40446f80;10891-94f- d3574dc0" Accept-Ranges: bytes Content-Length: 1456 Connection: close Content-Type: text/html; charset=ISO-8859- 1 Content-Language: en Expires: Fri, 02 May 2003 04:24:00 GMT

Some Web Servers use a file called /robot(s).txt to make search engines and any other indexing tools visit their WebPages more frequently and more efficiently. By connecting to the server and requesting the /robot(s).txt file, an attacker may gain additional information about the system they are attacking.

We were also able to locate and identify a development IIS 5.0 server with IP address 0.0.0.0. This server was not firewalled and we were able to establish a null IPC\$ connection as well as take note of the default installation of IIS 5.0 that is highly vulnerable to attack.

Null Session Information Leak

```
server: 0.0.0.0
setting up session... success.
password policy:
  min length: none
  min age: none
  max age: 42 days
  lockout threshold: none
  lockout duration: 30 mins
  lockout reset: 30 mins
opening lsa policy... success.
server role: 3 [primary (unknown)]
names:
  netbios: QNETWEB
  domain: WORKGROUP
quota:
  paged pool limit: 33554432
  non paged pool limit: 1048576
  min work set size: 65536
  max work set size: 251658240
  pagefile limit: 0
  time limit: 0
trusted domains:
  indeterminate
netlogon done by a PDC server
getting namelist (pass 1)... got 5, 0 left:
  Administrator Guest IUSR_QNETWEB IWAM_QNETWEB TsInternetUser
getting user list (pass 1, index 0)... success, got 5.
  Administrator Guest IUSR_QNETWEB IWAM_QNETWEB TsInternetUser
enumerating shares (pass 1)... got 3 shares, 0 left:
  IPC$ ADMIN$ C$
getting machine list (pass 1, index 0)... success, got 0.
Group: Administrators
QNETWEB\Administrator
Group: Backup Operators
Group: Guests
QNETWEB\Guest
QNETWEB\TsInternetUser
QNETWEB\IUSR_QNETWEB
QNETWEB\IWAM_QNETWEB
Group: Power Users
Group: Replicator
Group: Users
NT AUTHORITY\INTERACTIVE
NT AUTHORITY\Authenticated Users
```

Web Site Posted on Server

the time is 3:41:56 PM, Friday, May 02, 2003

Pacific Express Online

USER ID:
PASSWORD:
sign on

counts
Sign On here

Local Weather

mostly sunny
currently: 58°
3-day forecast

Local News

NEWS 8
Governor explains his plan to shave \$100 million off Gov/Guam budget
Tax Conversion Commission unable to prepare report

Investor Relations
Bank Demos
Press Releases

Personal
Business
About the Bank
Other Services
Contact

Branch Info
ATM Locations
Apply Online

Career Opportunity
Community Relations

check
Check, Remit, Express

Homeland pride. Values. Tradition. Family.

30 Years of Service

When [redacted] set out to create Bank [redacted], these were the principles that guided him. His hardwork, determination, values, and ideals epitomized Guam's spirit and helped him found a bank that has served the banking needs of our local families since 1972.

Thirty years later, these same standards will make up the foundation upon which Bank [redacted] continues to grow. Our tradition of service, and helping our people reach for and attain opportunities are the driving force behind Bank [redacted] success.

Online Banking

Why stand in line when you can Bank online? The Bank of [redacted] Online offers you services from anywhere at anytime.

3.7.DNS

3.7.1. Definition

Domain Name Service (DNS) is an Internet service that translates *domain names* into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name *www.example.com* might translate to *198.105.232.4*.

3.7.2. Approach

To begin testing we had to locate host to attack and map out the network we would be testing. This process is called network discovery or recon. Our primary tool of discovery was the DNS servers that host the bank.com domain.

3.7.3. Positive Results

The name servers are functional, resolve names to IP Addresses and we were able to connect to the www.bank.com web site by using a common URL or Universal resource locator. Here is the lookup we pulled off the DNS servers. The name servers are not under the direct configuration control of the Bank IT Staff.

;; QUESTION SECTION:

www.bank.com. IN ANY

;; ANSWER SECTION:

www.bank.com. 86400 IN CNAME bank.com.

```

;; AUTHORITY SECTION:
bank.com.      86400  IN      NS      badisp.net.
bank.com.      86400  IN      NS      stealth. badisp.net..
bank.com.      86400  IN      NS      badisp.net..

;; ADDITIONAL SECTION:
badisp.net.    172795 IN      A       0.0.0.0
badisp.net.    172795 IN      A       0.0.0.0

```

3.7.4. Negative Results

These DNS servers are vulnerable to a DoS DNS attack that would render their domain unavailable for an indefinite amount of time. This attack is simple in nature and highly disruptive. The attack is performed by sending connection requests to the DNS server over TCP port 53 from spoofed addresses.

DNS cache Poisoning is possible on the authoritative DNS servers. DNS Cache poisoning would allow us to redirect all IP traffic to a rouge server acting as a man in the middle allowing us to intercept all sensitive communications. This attack is particularly dangerous since most victims are unaware this being done for extended periods of time.

The DNS servers will e transfers Zones. The authoritative name servers allow zone transfers to the world, this should be disabled, as it leaks information about your network structure.

The Bind version is disclosed when performing remote version queries. The authoritative name server provides the version of software it is running. This is valuable information for would-be attackers because Bind has a host of vulnerabilities that are version specific.

3.7.5. Recommendations

You may choose to change DNS servers to a more secure service provider. Ask the service provider to disable recursive lookups on the authoritative DNS servers. Request ITE.NET to disable zone transfers within the bind servers configuration or restrict its use with acls. You can edit the bind source to return fictitious or X.X.X version banners, or restrict this sort of query with an acl to eliminate version queries.

3.8.Firewall

3.8.1. Definition

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

3.8.2. Positive Results

We identified a firewall in use on the network located at IP address 0.0.0.0. The firewall was effective in its filtering configuration. We were unable to positively identify its type to attempt specific exploits. No external management services were identified on this firewall. A second firewall was noted on IP Address 0.0.0.0. This firewall is actually a Cisco Router utilizing ACL's or the Cisco CBAC IOS Firewall Feature Set.

3.8.3. Negative Results

The firewalls we scanned on this network disclosed their firewall rule sets by non-uniform behavior to "firewalled" packets. For example "blocked" ports would not return a "connection" teardown response for the scanning host, but open ports did. This provides valuable information to attackers about what protocols might be in use within the "trusted area" of the network. We also encountered several inconsistencies that disclosed ingress filtering and other information about the network (See Below results).

Firewall	0.0.0.0		Firewall	0.0.0.0	
Port	State	Service	Port	State	Service
7/tcp	filtered	echo	23/tcp	filtered	telnet
19/tcp	filtered	chargen	134/tcp	filtered	ingres-net
23/tcp	filtered	telnet	135/tcp	filtered	loc-srv
57/tcp	filtered	priv-term	136/tcp	filtered	profile
79/tcp	filtered	finger	137/tcp	filtered	netbios-ns
135/tcp	filtered	loc-srv	138/tcp	filtered	netbios-dgm
136/tcp	filtered	profile	139/tcp	filtered	netbios-ssn
2001/tcp	filtered	dc	445/tcp	filtered	microsoft-ds
6001/tcp	filtered	X11:1	1720/tcp	open	H.323/Q.931
Remote operating system guess: Novell NetWare 3.12 - 5.00			1990/tcp	open	stun-p1
			1991/tcp	open	stun-p2
			1992/tcp	open	stun-p3
			1994/tcp	open	stun-port
			Remote operating system guess: Cisco 3600 running IOS 12.2(6c)		

The Cisco firewall had remote administration enabled from specified IP Addresses. Unfortunately the form of remote administration is insecure as it is telnet which uses plain text authentication mechanism.

3.8.4. Recommendations

Modify firewall rulesets to return an ICMP error code for closed ports with the source address of the IP in question. Audit every IP address in use, and don't return any ICMP errors for non-existent hosts.

Example Solution: (for linux 2.4 with iptables)

```
iptables -A DUMP -p tcp -j REJECT --reject-with tcp-reset
iptables -A DUMP -p udp -j REJECT --reject-with icmp-port-unreachable
iptables -A FORWARD -i eth0 -p TCP --dport 6346 -j DUMP
```

4. Conclusion

4.1. Summary of Objectives

- Retrieve as much information possible about the internal working of the network
- Gain unauthorized accesses to Critical systems
- Determine Remote Denial of Service Capabilities
- Test verify Authentication and encryption remote access methods
- Document results

4.2.Conclusion

Like all penetration tests, this one provides a snapshot of the state of security. In the case of the public network, it was apparent that many of the security concerns were a direct result of the choice of Internet service providers. This test was limited by the actual time allocated and network instabilities noted during the test. Had we been malicious attackers we would have been able to obtain customer account information and probably transfer or with draw funds from the home banking system by redirecting banking customers to a fake home banking authentication page.

Because of the Microsoft IIS Servers plagued with vulnerabilities in use on the same subnet as the AS/400 Home Banking system had we the time was would have been able to execute shell code on the IIS web server that would have allowed us to sniff all the clear text traffic to the AS/400 including account names and passwords. As a Bank you must pay special attention to this matter by performing regular audits and vulnerability assessments, as well as assigning a dedicated network administrator versed in security. Security patches and software upgrades are coming out on a daily basis, and it will not be sufficient to have a part-time Security administrator in this kind of environment.

4.3.Special Notes

During our testing procedure, we determined The International Bank or it affiliates made changes to the Firewall configuration. We are afraid we cannot give you an accurate picture of the security of that machine as it was prior to its modification. We also lost important assessment data because the changes happened during our testing. We have a number of examples to verify these changes. Note a report was generated on 11/1/2003 at approximately 5:12:23 PM that identified Host 0.0.0.0 to have telnet world accessible (User Access Verification Password:). This host was no longer accessible on port 23 on the same day at approximately 6:13:40 PM

During our testing on Monday the 5th our upstream provider was served a warrant by the US Marshals service to terminate our Internet connection. We were not informed by the FBI or Marshals service who had initiated the warrant but were informed that IBM was a complainant party. We did identify the relationship between IBM and The Bank. IBM is the Managed Security Service Provider.