Global Information Assurance Certification Paper

Securing an Exchange 2000 Front End Outlook Web Access Server

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b
Option 2 – Case Study in Information Security

SANS Network Security 2002
San Francisco, CA
December 2002

Prepared by:
Eric Logeson

Summary

Catapulted by business needs and the necessity for easily obtaining and exchanging information, email has emerged as the preferred method to electronically exchange information. Additionally, web technologies have made email accessible from any Internet connected computer. Unfortunately, the ease at which information is obtained and how well information is secured are typically inversely related. Many companies depend on Microsoft Exchange email suite of products, and in particular Outlook Web Access (OWA). OWA enables email capabilities from any web browser making information exchange easy for the end user. This document will strive to balance the "ease of use" vs. "information security" inverse relationship regarding OWA. Securely installing and operating OWA is the end result of this document.

Assumptions

The following procedures assume the following:

1. Exchange 2000 server is installed and operating
2. Firewall with DMZ
3. Windows 2000 system administration skills

Required Exchange Server 2000 Concepts

Exchange 2000 is the latest retail email server from Microsoft. Exchange 2000 is a collection of services requiring communications with and existence of active directory, global catalog, and IIS. Exchange 2000 is comprised of the following services:

Service	Function
Microsoft Exchange POP3	Post Office Protocol 3 (POP3) is a read-only protocol that allows a POP3 client to connect to an Exchange Server computer from anywhere on the Internet and download messages locally for reading.
Microsoft Exchange IMAP4	Internet Message Access Protocol 4 (IMAP4) another read-only protocol similar to POP3, allows users to access any of their folders, not just their Inbox.
Microsoft Exchange Information Store	Accesses the mailbox and public folder stores
Microsoft Exchange search	Searches mailbox and public folder stores
Microsoft Exchange event	Backwards compatibility with version 5.5, used in version 5.5 to monitor events that occur in folders.
Microsoft Exchange Site Replication Service	Backwards compatibility with version 5.5
Microsoft Exchange Management	Introduced in Exchange SP2, the Directory Access display is new and the Message Tracking Center functionality is updated.

Microsoft Exchange MTA	Message Transfer Agent (MTA) provides the engine for sending messages and distributing information between Microsoft Exchange Server systems or between Microsoft Exchange Server and a foreign system. Each MTA is associated with one information store. The MTA conforms to the 1988 X.400 specification.
Microsoft Exchange Routing Engine	The routing engine determines the appropriate gateway to use for messages, based on the address type of the recipient.

Table 1

Front-end / Back-end Architecture

Exchange 2000 Server can distribute server tasks to front-end (FE) and back-end (BE) servers. FE servers proxy client requests to the BE server. In the procedures that follow a FE server will be used for OWA functionality and will be dedicated to accept Hypertext Transfer Protocol (HTTP) traffic. In this configuration no user data is stored on the FE server. While it is possible to use FE servers to proxy Simple Mail Transfer Protocol (SMTP), Post office Protocol version 3 (POP3), and Internet Message Access Protocol (IMAP) we will focus on HTTP. In the FE and BE server architecture, the processing required to encrypt and decrypt Secure Sockets Layer (SSL) can be offloaded to the FE server. Additionally SSL processing can be offloaded to a SSL hardware accelerator device. Exchange 2000 servers are BE servers by default while FE servers are configured to operate as FE servers.

Authentication methods

Exchange supports different authentication methods depending on the topology. FE servers can *only* authenticate using basic authentication or by anonymously forwarding the request to a back end server. BE servers support both basic and Integrated Windows Authentication. In Dual Authentication, both the FE and BE servers authenticate users using HTTP basic authentication. In Pass through Authentication, FE servers anonymously forward authentication requests to a BE server.

Patching Exchange Servers

Patching FE-BE exchange server configurations require special consideration. Outlook Web Access clients download script files from the front-end server to which they connect. These script files are not compatible with back-end servers that are running a later version of Exchange than the front-end server. When you upgrade a server running Exchange 2000 to a later service pack, you must upgrade all front-end servers before you upgrade Exchange on any back-end servers. The script files on an upgraded front-end server are backwards compatible with any back-end server running a down level Exchange 2000 service pack.

Current OWA configuration

The current topology consists of:

1. Back-end Exchange 2000 server
2. Front-end Exchange 2000 server
3. Cisco PIX 515 firewall with 3 interfaces
4. Active Directory and Global Catalog servers

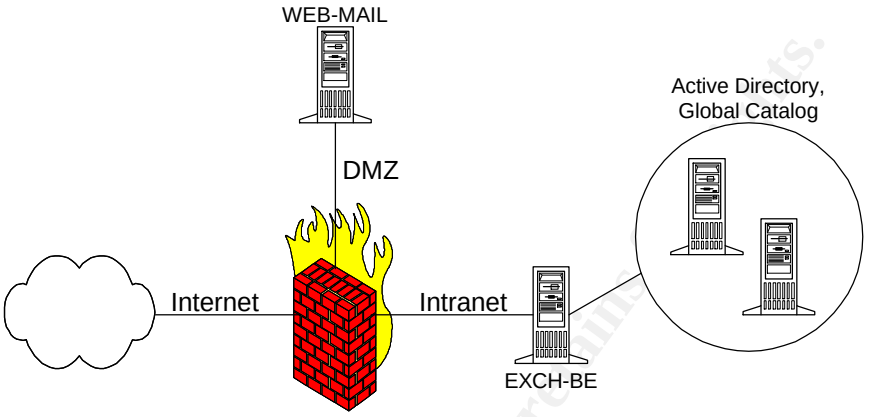

Diagram 1

The FE Exchange Server (WEB-MAIL) is configured to operate as a front-end server; however, no additional steps were taken to secure WEB-MAIL. Furthermore, users connect to their mailboxes using basic authentication on http port 80. Exchange service pack 1 is installed on both exchange servers and service pack 3 is installed on all Windows 2000 servers.

Summary of Current Exchange Configuration:

Machine	OS	Role	Hardware
EXCH-BE	Windows 2000 Server SP3	Exchange 2000 SP1 Back End Server	Dell PowerEdge 2550
WEB-MAIL	Windows 2000 Server SP3	Exchange 2000 SP1 Front End Server	Dell Optiplex GX110
DC1	Windows 2000 Server SP3	Domain Controller	Dell PowerEdge 1650
DC2	Windows 2000 Server SP3	Domain Controller	Dell PowerEdge 1650

Table 2

Summary of Firewall Configuration:

Source	Destination	Port
Internet	WEB-MAIL (192.168.20.50)	80

Table 3

WEB-MAIL was a proof of concept server that *became* a production server and the current configuration has several security vulnerabilities. As the planner and

implementer of this project I have identified, by studying the SANS coursework and observations made during the conference, the following vulnerabilities:

1. The absence of a web based email security and configuration policy. This document will serve as the configuration and security policy for the FE exchange server. This requirement was identified in SANS Security Essentials II page 2-4.
2. LANMan Authentication is enabled. Only NTLMv2 should be allowed and strong passwords should be enforced. This requirement was identified in SANS Security Essentials II page 3-43, 3-43.
3. Currently HTTP 1.1 basic authentication between clients and front-end servers is enabled which lightly encodes the user's name and password before sending it to the server. To achieve password and email security SSL encryption should be used between the client and front-end server. This requirement was identified in SANS Security Essentials II page 6-11.
4. Much of SANS Security Essentials V: Windows Security is germane and the current WEB-MAIL fails to address. Following are the highlights:
    a. Currently the "Principle of Least Privilege" isn't being observed.
    b. Service Packs, Patches, and hot fixes historically have not been a priority, in spite of an existing patch policy.
    c. The items listed on pages 2-10 through 2-24, dealing with specific Windows 2000 Server operating system security, currently is not implemented. The security policy in Appendix A will address these deficiencies.
    d. The current WEB-EMAIL server is a default installation of Windows 2000 server with all accessories installed, violating the minimal install mantra, on page 3-30.

Securing OWA

Instead of retrofitting security on WEB-MAIL in diagram 1, a new front-end exchange server (EXCH-FE) will replace WEB-MAIL. Running these front-end servers in parallel temporarily allows for the new sever to be thoroughly tested and minimizes disruption of services. Once the security model on EXCH-FE is vetted and operational, WEB-MAIL can be decommissioned with little or no impact to the end user. This case study will use a dual authentication scheme for the exchange architecture, which requires RPC communications between the FE server in the DMZ and the directory servers (domain controllers) in the Intranet. The decision to use Dual Authentication is three fold:

1. The alternative, Pass Through Authentication, would require an explicit logon request of the form http://mailname.mydomain.com/exchange/username
2. The alternative, Pass Through Authentication, would expose the BE server to any request including malformed requests.
3. The alternative to use Microsoft's Internet and Security Acceleration (ISA) Server is cost prohibitive and isn't considered as robust as the current firewall implementation.

This case study focuses on the specifics involved in securely installing and operating OWA. Details regarding Windows 2000 Server security and the steps involved in achieving other non-OWA security requirements are included in the appendices and will be referenced through out the procedures that follow.

Windows 2000 Server and IIS 5.0 installation and configuration

1. Install and secure Windows 2000 Server according to the security policy defined in ***Appendix A***. This very restrictive security policy will have to be tempered as application requirements dictate.
2. Install and secure Internet Information Server 5.0 (IIS) according to the security policy defined in ***Appendix B***.
3. Patch the server with the latest security patches according the patch deployment policy defined in ***Appendix C***.

Start the following services so EXCH-FE can join the domain and Exchange can be installed. These services are currently disabled due to implementing the security policy in Appendix A. Change the start up type to manual and start the following services.

1. TCP/IP NetBIOS Helper Service
2. IPSEC Policy Agent
3. Remote Procedure Call (RPC) Locator
4. Remote Registry Service
5. Windows Installer
6. NT LM Security Support Provider

Exchange Server 2000 installation and configuration

1. Insert the installation media and run setup. Choose custom and install to a non-system partition, such as E:
2. Install only the "Exchange messaging a collaboration tools". Note: choose yes to the "Digital Signature Not Found" errors, this is a result of the security policy defined in Appendix A. Note: choose cancel on any errors regarding "Unable to set registry settings for Miscellaneous Atom", the installation will continue safely.
3. Configure EXCH-FE to operate as a FE server. Start the Exchange System Manager on any Backend server->Administrative Groups->First Administrative Group->Servers->EXCH-FE right click properties. Check "this is a front end server" on the general tab and choose the OK button. Reboot EXCH-FE
4. Install the latest Exchange Service Pack (service pack 3 as of this writing) and any Exchange hot-fixes using Appendix C as a guideline.
5. Hide the Change Password button, this registry change must occur on all FE and BE exchange servers.
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeWEB
   Keyname = OWA
   Value name: DisablePassword
   Type: REG_DWORD
   Data :1

6. Dismount the “Mailbox Store”. Start the Exchange System Manager on any backend server ->Servers->EXCH-FE->First Storage Group right click on the “Mailbox Store” and select “Dismount Store”. Right click on the Mailbox Store->properties->database tab check “Do not mount this store at start-up”, press OK.
7. Dismount and delete the public folder store. Start the Exchange System Manager on any backend server ->Servers->EXCH-FE->First Storage Group right click on the “Public Folder Store” and select “Dismount Store”. Right click “Public Folder Store” and select “Delete”. Choose a backend sever for system objects and press Yes.
8. Since EXCH-FE is a front-end exchange server and only supports web-based email, disable the following services and reboot.
    a. Microsoft Exchange Event
    b. Microsoft Exchange IMAP4
    c. Microsoft Exchange Information Store
    d. Microsoft Exchange MTA Stacks
    e. Microsoft Exchange POP3
    f. Microsoft Exchange Site Replication Service
    g. Microsoft Search

    Table 4 lists the minimal set of services required for a stable FE Exchange server configuration; all other services should be disabled.
9. Add Authenticated users with RX NTFS permissions on %systemroot%\system32\inetsrv\asp.dll. The Security policy defined in Appendix A would prevent users from being able to use the LogOff option in OWA.

Service	Status	Startup Type	Required by
IIS Admin Service	Started	Automatic	Exchange 2000
IPSEC Policy Agent	Started	Automatic	Exchange 2000
Microsoft Exchange Routing Engine	Started	Automatic	Exchange 2000
Net Logon	Started	Automatic	Exchange 2000
Remote Procedure Call (RPC) Locator	Started	Automatic	Exchange 2000
Workstation	Started	Automatic	Exchange 2000
World Wide Web Publishing Service	Started	Automatic	Exchange 2000
Application Management	Started	Automatic	Windows 2000
Event Log	Started	Automatic	Windows 2000
Locks Floppy for Admin use only	Started	Automatic	Windows 2000
Logical Disk Manager	Started	Automatic	Windows 2000
Network Connections	Started	Automatic	Windows 2000
Plug and Play	Started	Automatic	Windows 2000
Protected Storage	Started	Automatic	Windows 2000
Remote Procedure Call (RPC)	Started	Automatic	Windows 2000
Security Accounts Manager	Started	Automatic	Windows 2000
Task Scheduler	Started	Automatic	Windows 2000
Windows Management Instrumentation	Started	Automatic	Windows 2000

Windows Management Instrumentation Driver Ext	Started	Automatic	Windows 2000
Windows Time	Started	Automatic	Windows 2000

Table 4

SSL Configuration

SSL will encrypt communications between the client (Web browser) and the FE server.

1. Using the Internet Services Manager, right click on the "Default web site" and choose properties. Select the "Directory Security" tab and choose "Server certificate".
2. Press "Next" when the certificate wizard initializes.
3. Choose "Create a new Certificate" and click "Next".
4. Choose "Prepare the request now, but send it later" and click "Next".
5. Enter a name for the certificate in the name field, such as "OWA SSL". Choose a bit length of 1024 and click "Next". Note: Key bit lengths greater than 1024 are not recommended.
6. Enter the Organization information such as company name and/or department and click "Next".
7. Enter the common name for the server. This is the Fully Qualified Domain Name (FQDN) that users will use to access the OWA server from the internet, such as *mailname.mydomain.com* and press "Next"
8. Enter the County, State, and City. Click "Next".
9. Enter a location to save the certificate request such as c:\certreq.txt and press "Next".

The certificate request is ready to be submitted to a certificate authority. Geotrust (www.geotrust.com) will be used for this case study. A 3-year certificate costs $327 dollars and the request was fulfilled in less than 10 minutes. Note: knowing the administrative and/or technical contact for the DNS domain of the OWA server greatly speeds up this process.

1. The certificate is typically emailed to the administrative contact for the Domain and resembles:

```
-----BEGIN CERTIFICATE-----
MIIDCjCCAnMCAQAwdTEZMBcGA1UEAxMQaG9zdC5kb21haw4ubmFtZTEVM
BMGA1UECxMMT3JnYW5pemF0aW9uMRUwEwYDVQQKEwxPcmdhbml6YXRpb2
4xDTALBgNVBAcTBENpdHkxDjAMBgNVBAgTBVN0YXRlMQswCQYDVQQGEwJ
VUzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyZ1dYomQ4jhSr6f/
G3GYxjS4B837+y3A6xIM9OVXV4ZnSIe9nOLHgdksQJpwaQeOZwWeqifte
hrJ/s55PvPxok+Tqq0t7BfMkkUSuiYnFdUo1OpDPdw3cEaP9WWSrduouI
Vnq2AWTDw2ykyxKg6neb2vYTZRvbot7M578Vvh6P8CAwEAAaCCAVMwGgY
KKwYBBAGCNw0CAzEMFgo1LjAuMjE5NS4yMDUGCisGAQQBgjcCAQ4xJzAl
MA4GA1UdDwEB/wQEAwIE8DATBgNVHSUEDDAKBggrBgEFBQcDATCB/QYKK
wYBBAGCNw0CAjGB7jCB6wIBAR5aAE0AaQBjAHIAbwBzAG8AZgB0ACAAUg
BTAEEAIABTAEMAaABhAG4AbgBlAGwAIABDAHIAeQBwAHQAbwBnAHIAYQB
wAGgAaQBjACAAUAByAG8AdgBpAGQAZQByA4GJACB3C0g9psK0+V+N/Me1
JsG39vonCPQBdOwNp6zHJSPCU3FwQ0SgFpEQNy6HEn79IOCMrU93q9Hh1
TQtd2YU6lWHQunXrIcytmAFVjhibNX6Dp1e41Wjc2N4ilJyy1GFss686c
dZt2GP6y04I74/OvkW2Wf9nezUrMrESM2PP4B1AAAAAAAAAAAwDQYJKoZ
IhvcNAQEFBQADgYEAg4+QHTvkP5CG+WcGnrhKiMkJnMP6QEsds4OobUDS
dGtEupQz8C+4xoMd1aM68q9Ri6Va+JTeuhKHxLz9hT/KUJhNBy0sRfnx+
JkQdrKG69UanTwvLqXINh9xChw9ErIto/2kZI5kl2KYQdiOqTv6p0GEUP
Rq/MD52Zy3bOzSRF0=
-----END CERTIFICATE-----
```

2. Copy the certificate into a text editor and save as c:\certreq.cer Note: be sure to copy all lines including the "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" lines.

3. Using the Internet Services Manager, right click on the “Default web site” and choose properties. Select the “Directory Security” tab and choose “Server certificate”.
4. Choose “Process the pending request and install the certificate”, and click “Next”.
5. Enter the location (c:\certreq.cer) of the certificate, and click “Next”
6. Click “Next” on the summary screen.
7. Right click on the “Exchange” virtual directory under the “Default Web Site” and choose properties.
8. Select the “Directory Security” tab and the click on the “Edit”. Check the box “Require Secure Channel (SSL)” and click “OK”.
9. Configure the DMZ to allow https traffic, port 443.
10. Setup a redirection URL and bind it to the startup.htm document that was created in Appendix B. Right click on starthere.htm and select properties. On the file tab choose “A redirection to a URL” and type in the FQDN of the OWA server, e.g. https://mailname.mydomain.com/exchange. Special note: do not remove the Exchange or Public virtual directories in IIS, the “Stop” signs on these virtual directories are normal.
11. Test the server, http://mailname.mydomain.com, you should be automatically redirected to the secure site.

Final Tasks

After EXCH-FE has been thoroughly tested, shutdown WEB-MAIL for a month to flush out any problems and to ensure the new server is properly providing all OWA functions. After the month burn-in, uninstall Exchange on WEB-MAIL. Since Exchange is a schema modifying application uninstalling will undo the LDAP changes in active directory made during the original installation.

Verify Configuration

Using SSL has significantly improved the security posture. A complex password policy is feckless if transmitted passwords are easily decoded. To demonstrate how easily basic authentication can be exploited, the following packet was captured using ethereal while accessing WEB-MAIL:

```
GET /exchange HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel,
application/msword, application/x-shockwave-flash, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Host: web-mail.mydomain.com
Connection: Keep-Alive
Authorization: Basic bXlkb21haW5cdXNlcnRlc3Q6QzhtcGwzeDIz==
```

A two-line perl script can decode http 1.1 basic authentications:

```
use MIME::Base64;
print decode_base64("bXlkb21haW5cdXNlcnRlc3Q6QzhtcGwzeDIz==");
```

Which reveals the domain, username and password.

```
mydomain\usertest:C8mpl3x2^3
```

Since EXCH-FE is protected by SSL all application data, after the SSL tunnel has been established, is encrypted. Using ethereal to capture traffic between a client browser and the OWA server doesn't reveal intelligible data.

```
-c#+™™:ƒ‘  œÅa k^E ª f7ÁXƒ °óa i  0>ûérÛ£ šÖ #3ÐÍžt^  ‘ ¬Â‹Uj    r  o
 l0, h0, Ñ        Æ 0*†H†÷     0N10 U  US1 0 U  Equifax1-0+ U $Equifax Secure Certificate
Authority0030422190350Z06042219035OZ0 é10 U  US10  Umailname.mydomain.com1S0Q U JBusiness
Registration: https://services.choicepoint.net/get.jsp?2583102333100. U'See
www.geotrust.com/quickssl/cps (c)031!0 U  Domain Control
Validated10  U mailname.mydomain.com0 Ÿ0*†H†÷         0 ‰
`÷Ü^ÙÍ `0BšS¹îè ä UF ¹Ü (&ÎšÑHÔ½(RbV  dò ˜¤”² N¸-`=Þ fB:ƒè[SJSYìÁÐV'{J» ·×µ ØB^"j+i!
 £ ·0 ´0`†H†øB@0 U    ÿ  ð0  U   Õ8 Òwê/ÑÒ‰F'Ø÷ÆÐÕ D0: U 3010/ -
 +†)http://crl.geotrust.com/crls/secureca.crl0 U # 0 € Hæhù+Ò²•×GØ#
 O3˜ ŸÔÔ  U %0 +      †H†÷         ö ^œ1ðíÅ& JuÛFMàæ›Ý~¡½„d½yÈ Š®ôCGjBPÿ_
ùOC¿Ÿ˜UÑ»ËÌ™-ÛJµ î* D à$þL¯ÓúöåRÓÿs SÖ™aZ:M°n,û¹ d°èKoÛ1T-ÿlèÚO,ÿšØNôÿ 'p"ÉošTC0¾+Ô?°øFj¿
=   =Þ€¦;°]^\Åª Î:ö~ÝT9âÆ ÎÐƒRM¸Z ›p0 ^¨É]€4°3PÿGßÁ8ÊÌ«lÈ5D ^½Û~Þä|ÃP‘ôÞ °,¾¶Ä
```

Securing Windows 2000 server and Internet information according to the appendices has improved the security posture. Specifically, adopting a least access as possible policy will prevent internal users from changing the configuration of IIS. Vulnerability tools such as GFI LanGuard Network Security Scanner didn't find operating system or web server vulnerabilities. Further more since null sessions are disabled the LanGuard Network Security Scanner could not enumerate any NetBios shares, the NetBios computer name, or garner user account information.

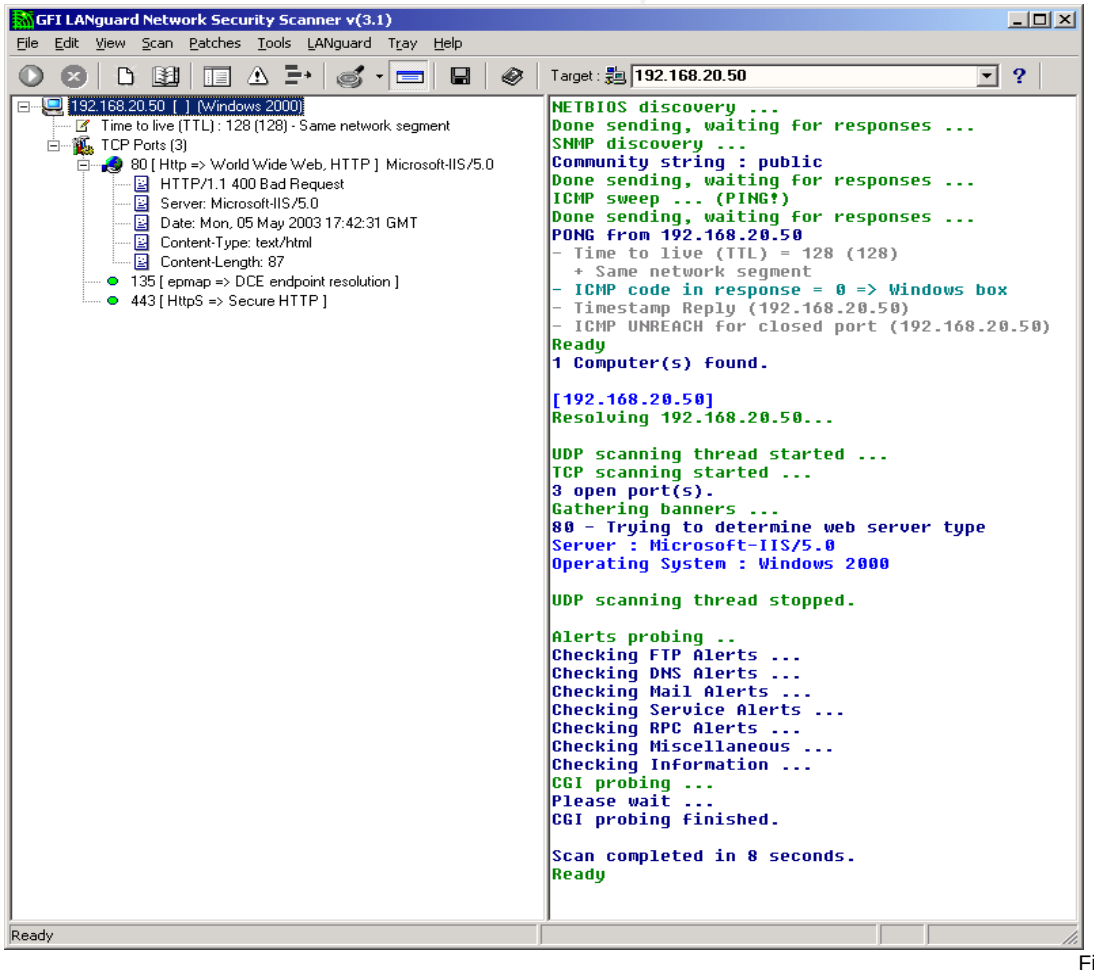

Figure 1

Impact Assessment

Impact assessment falls into three categories performance, availability and usability.

Performance

A benefit of the front-end back-end architecture is off loading SSL to the front-end server. If SSL is used to encrypt all sessions between clients and the front-end server, CPU requirements can increase up to three times and the amount of memory used by the InetInfo process increases by a factor of approximately 1.6 times[1]. Since EXCH-FE (a server class machine with two processors and a gigabyte of memory) replaced WEB-MAIL (a desktop with a single celeron with 256 megabytes of memory) performance has increased in lieu of implementing SSL.

Availability

WEB-MAIL and EXCH-FE operated in parallel during the migration; consequently end users never experienced downtime. Furthermore, since EXCH-FE and WEB-MAIL are network address translated behind a firewall the migration was instantaneous and most users never knew the switch occurred. Migrating to a server class machine with redundant power supplies and hard disks has increased our hardware failure tolerance.

Usability

The only issue to date occurs email messages link to external web sites. When a message links to external web sites or images a warning message appears indicating that the page contains both secure and non secure items, see figure 2. An interesting behavior occurs when auto preview is enabled in OWA. When a message links to an external web site the warning in figure 2 displays and the lock in Internet Explorer indicating that the site is implementing SSL disappears. The disappearing lock is misleading and may be confuse users that notice. Although the site is still implementing SSL users should be educated that auto preview is in general dangerous and should be avoided.

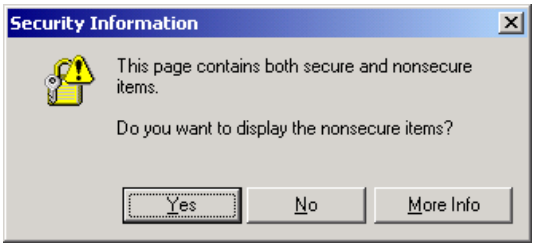

Figure 2

[1] "Microsoft Exchange 2000 Front-End Server and SMTP Gateway Hardware Scalability Guide." Page 11. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/exchange/exchange2000/deploy/depovg/exchsmpt.asp

References

1. Fugatt, Mark. “Securing Outlook Web Access using SSL.” August 6, 2002. http://www.msexchange.org/tutorials/MF004.html
2. “Microsoft Exchange 2000 Server Service Pack 3.” July 18, 2002. http://www.microsoft.com/exchange/downloads/2000/sp3/Rnotes_US.htm
3. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wss/wss/sgw_overview.asp
4. “5-minute Security Advisor - Configuring Outlook Web Access.” http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/5min/5min-301.asp
5. “Configuration and Security Update Recommendations for Exchange 2000.” http://www.microsoft.com/exchange/techinfo/security/bestconfig.asp
6. Lemson, KC. Martin, Michele. “Using Microsoft Exchange 2000 Front-End Servers.” October 2002. http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=AFAD8426-572E-40F8-99DA-EB7198F374C4
7. “Security Operations Guide for Exchange 2000 Server.” http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/mailexch/opsguide/default.asp
8. “OWA 2000 Security and Scalability.” http://www.exchangeadmin.com/Articles/Index.cfm?ArticleID=23139&pg=1
9. “Microsoft Exchange 2000 Front-End Server and SMTP Gateway Hardware Scalability Guide.” http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/exchange/exchange2000/deploy/depovg/exchsmpt.asp

Appendix A
Windows 2000 Bastion Host Security Policy

Operating System Installation Guidelines:

1. Disconnect machine from network.
2. Perform a clean installation of Windows 2000 Server (format all drives, if using RAID recreate and format all volumes).
3. Install minimal components (for example, uncheck *all* options such as accessories and IIS).
4. Install minimal networking components (TCP/IP only).
5. Configure as a stand-alone server (do not add to a domain).
6. Install the high encryption pack.
7. Install the latest service pack (SP3 at the time of this writing).
8. Install the latest version of Internet Explorer.

Local Security Policy Settings:

1. Password Policies
    a. Enforce password history, should be set to 24 passwords.
    b. Maximum password age should be set to 90 days.
    c. Minimum password age should be set to 1 day.
    d. Minimum password length: set to twelve characters.
    e. Passwords must meet complexity requirements. (Must contain three of four classes; uppercase letters, lowercase letters, numbers, and special characters).
    f. Do not store passwords using reversible encryption. (Used for certain applications tantamount to storing passwords in clear text format).
2. Account Lockout Polices
    a. Account lockout duration should be set to zero minutes (Administrator has to unlock a locked account).
    b. Account lockout threshold set to three invalid logon attempts.
    c. Reset account lockout counter after 1440 minutes (1 day).
3. Auditing Policy

a.	Audit account logon events	Success, Failure
b.	Audit account management	Success, Failure
c.	Audit directory service access	No auditing
d.	Audit logon events	Success, Failure
e.	Audit object access	Failure
f.	Audit policy change	Success, Failure
g.	Audit privilege use	Success, Failure
h.	Audit process tracking	No auditing
i.	Audit system events	Success, Failure

4. User Rights

a.	Access this computer from the network	Administrators
b.	Act as part of the operating system	
c.	Add workstations to domain	
d.	Back up files and directories	Administrators, Backup Operators
e.	Bypass traverse checking	Administrators, Backup Operators
f.	Change the system time	Administrators
g.	Create a pagefile	Administrators
h.	Create a token object	
i.	Create permanent shared objects	
j.	Debug programs	Administrators
k.	Deny access to this computer from the network	
l.	Deny logon as a batch job	
m.	Deny logon as a service	
n.	Deny logon locally	
o.	Enable computer and user accounts to be trusted for delegation	
p.	Force shutdown from a remote system	Administrators
q.	Generate security audits	
r.	Increase quotas	Administrators
s.	Increase scheduling priority	Administrators
t.	Load and unload device drivers	Administrators
u.	Lock pages in memory	
v.	Log on as a batch job	SYSTEM, Administrators
w.	Log on as a service	SYSTEM, Administrators
x.	Log on locally	Administrators
y.	Manage auditing and security log	Administrators
z.	Modify firmware environment values	Administrators
aa.	Profile single process	Administrators
bb.	Profile system performance	Administrators
cc.	Remove computer from docking station	

dd. Replace a process level token
ee. Restore files and directories — Backup Operators, Administrators
ff. Shut down the system — Administrators
gg. Synchronize directory service data
hh. Take ownership of files or other objects — Administrators

5. Security Options
   a. Additional restrictions for anonymous connections — No access without explicit anonymous permissions
   b. Allow server operators to schedule tasks (domain controllers only) — Not defined
   c. Allow system to be shut down without having to log on — Disabled
   d. Allowed to eject removable NTFS media — Administrators
   e. Amount of idle time required before disconnecting session — 15 minutes
   f. Audit the access of global system objects — Enabled
   g. Audit use of Backup and Restore privilege — Disabled
   h. Automatically log off users when logon time expires (local) — Enabled
   i. Clear virtual memory pagefile when system shuts down — Disabled
   j. Digitally sign client communication (always) — Disabled
   k. Digitally sign client communication (when possible) — Enabled
   l. Digitally sign server communication (always) — Disabled
   m. Digitally sign server communication (when possible) — Enabled
   n. Disable CTRL+ALT+DEL requirement for logon — Disabled
   o. Do not display last user name in logon screen — Enabled
   p. LAN Manager Authentication Level — Send NTLMv2 response only\refuse LM & NTLM
   q. Message text for users attempting to log on — legal message
   r. Message title for users attempting to log on — legal message
   s. Number of previous logons to cache — 0 logons
   t. Prevent system maintenance of computer account password — Disabled
   u. Prevent users from installing printer drivers — Enabled
   v. Prompt user to change password before expiration — 14 days
   w. Recovery Console: Allow automatic administrative logon — Disabled
   x. Recovery Console: Allow floppy copy and access to all drives and all folders — Disabled
   y. Rename administrator account — yes
   z. Rename guest account — yes
   aa. Restrict CD-ROM access to locally logged-on user only — Enabled
   bb. Restrict floppy access to locally logged-on user only — Enabled
   cc. Secure channel: Digitally encrypt or sign secure channel data (always) — Disabled
   dd. Secure channel: Digitally encrypt secure channel data (when possible) — Enabled
   ee. Secure channel: Digitally sign secure channel data (when possible) — Enabled
   ff. Secure channel: Require strong (Windows 2000 or later) session key — Disabled
   gg. Send unencrypted password to connect to third-party SMB servers — Disabled
   hh. Shut down system immediately if unable to log security audits — Enabled
   ii. Smart card removal behavior — No Action
   jj. Strengthen default permissions of global system objects (e.g. Symbolic Links) — Enabled
   kk. Unsigned driver installation behavior — Warn but allow installation
   ll. Unsigned non-driver installation behavior — Warn but allow installation

Event Log Settings:

1. System 30720 KB Do not overwrite events
2. Security 61440 KB Do not overwrite events
3. Application 30720 KB Do not overwrite events
4. Secure event log viewing.
   Access logs can often reveal significant details relating to user usage patterns, and application installations.
   Restrict Guest access to the audit logs for Application and System
   Add the following information into the registry using regedit.exe:
   Hive: HKEY_LOCAL_MACHINE
   Key: SYSTEM\CurrentControlSet\Services\EventLog\Application, Security, System
   Value Name: RestrictGuestAccess
   Type: REG_DWORD
   Value: 1
5. Dump, clear, and backup event logs weekly to the data partition.
6. Install a time-server for log and event correlation.

Registry Configuration:

1. Registry Settings
   a. **Avoid Netware DLL Trojan horse**.
   The Local Security Authority (LSA) collects passwords for further authentication to a Netware server. Users with write access to %systemroot%/system32 could install a Trojan DLL in place of FPNWCLNT and collect passwords. Remove this DLL only if Netware Clients are NOT being used.

Remove the following information from the registry using regedit.exe:
Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Control\Lsa
Value Name: Notification Packages
Type: REG_MULTI_SZ
Value: REMOVE FPNWCLNT (ONLY if MS Netware Client is NOT used.

b. **Remove OS/2 and POSIX subsystems.**
The OS/2 and POSIX subsystems allow for unnecessary vulnerabilities.
Add the following information into the registry using regedit.exe:
Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Control\Session Manager\Subsystems
Value Name: Optional
Value: **REMOVE** OS2 and POSIX
Note: Also delete the files os2ss.exe and psxss.exe (located in %systemroot%\System32)

c. **Remove OS/2 and POSIX subsystems.**
The OS/2 and POSIX subsystems allow for unnecessary vulnerabilities.
Add the following information into the registry using regedit.exe:
Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Control\Session Manager\Subsystems
Action: **REMOVE** the Os2 and Posix keys

d. **Disable CD Autorun**
The CD Autorun feature enables the capability to launch an application from CDs, if the autorun.exe program exists on the CD. This can potentially allow arbitrary programs to be executed without the knowledge or approval of the system administrator or the user.
Add the following information into the registry using regedit.exe:
Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Services\Cdrom
Value Name: AutoRun
Type: REG_DWORD
Value: 0

e. **Confirm Blocking of null session access.**
Blocks null session access to the system except for shares with “Everyone” permissions. Removing “Everyone” permissions from shares will block null sessions completely.
Add the following information into the registry using regedit.exe:
Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Services\LanManServer\Parameters
Value Name: RestrictNullSessAccess
Type: REG_DWORD
Value: 1

f. **Disable Auto Generation of 8.3 Filenames**
Windows 2000 supports 8.3 file name formats for backward compatibility with 16-bit applications. This means that an attacker only needs 8 characters to refer to a file that may be 20 characters long.
Change the following information into the registry using regedt32.exe:
Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrrentControlSet\Control\FileSystem\
Value Name: NtfsDisable8dot3NameCreation
Type: REG_DWORD
Value: 1

g. **Removing Administrative Shares**
By default if you delete the c$, d$, etc administrative shares, they will be recreated when after a reboot.
Change the following information into the registry using regedt32.exe:
Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrrentControlSet\Services\LanmanServer\Parameters\
Value Name: AutoShareServer
Type: REG_DWORD
Value: 0

h. **Associate common script extension with innocuous program**
Scripting languages are configured to execute by default, by associating these with notepad no unwanted scripts will execute. See Appendix A.

2. **Registry Permissions**

i. **Restrict Remote Access to the Performance Monitor**

Remote access to the performance monitor software could potentially allow users to query the processes and process priorities on the local machine.
Change the following information into the registry using regedt32.exe:

Hive: HKEY_LOCAL_MACHINE
Key: SOFTWARE\Microsoft\Windows NT\Current Version\Perflib
Change ACL (click on Security, then Permissions)
Administrators: **Full Control**
SYSTEM: **Full Control**
REMOVE ALL other groups/users

j. **Control who may submit jobs to the schedule service.**

The ability to submit jobs for scheduling should only be allowed by Administrators
Add the following information into the registry using regedit.exe:

Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Services\Schedule
Change ACL (click on Security, then Permissions)
Administrators: **Full Control**
SYSTEM: **Full Control**
REMOVE all other groups/users

k. **Restrict network share creation**

Network shares provide the ability to distribute access to local server or workstation files to others on the network. There is a significant risk when providing shares. Restricting the ability to create shares should be granted to Administrators only.
Change the following information into the registry using regedt32.exe:

Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Services\LanManServer\Shares
Change ACL (click on Security, then Permissions)
Administrators: **Full Control**
SYSTEM: **Full Control**
Everyone group: **Read**
REMOVE all other groups/users

l. **Restrict Ability to Add Services**

Windows 2000 can be configured to run any number of services at boot time. To ensure only administrators have the capability to install services, modify the registry as follows:
Add the following information into the registry using regedt32.exe:

Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Services
Change ACL (click on Security, then Permissions)
Administrators: **Full Control**
SYSTEM: **Full Control**
Everyone: **Read**
REMOVE ALL other groups/users

m. **Control remote access to the registry.**

By default, Windows 2000 allows remote users some access to the system registry. To disable remote access, set the following registry key permissions
Add the following information into the registry using regedt32.exe:

Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
(add key if winreg is absent)
Change ACL (click on Security, then Permissions)
Administrators: **Full control**
SYSTEM: **Full Control**

n. **Restrict Access to the WinLogon Key**

The winlogon key controls processes relating to the Windows NT logon sequence, and could be used to raise a user's access level to Administrator.
Change the following information into the registry using regedt32.exe:

Hive: HKEY_LOCAL_MACHINE
Key: SOFTWARE\Microsoft\Windows NT\Current Version\WinLogon
Change ACL (click on Security, then Permissions)
Administrators: **Full Control**
SYSTEM: **Full Control**
REMOVE ALL other groups/users

o. **Restrict Access to the Command Key Modifications**

By default, users can change the file association of .reg files. The ability to modify such file associations should be restricted to administrators and system only.
Change the following information into the registry using regedt32.exe:
Hive: HKEY_LOCAL_MACHINE
Key: SOFTWARE\Classes\regfile\shell\open\command
Change ACL (click on Security, then Permissions)
Administrators: **Full Control**
SYSTEM: **Full Control**
REMOVE ALL other groups/users

File System (NTFS) Permissions

Directory	Guidelines	Comments
\Documents and Settings\	Administrators: **Full Control** System: **Full Control** Backup Operators: **Modify** Everyone: **Read**	DO NOT replace Permissions on Subdirectories or files. Do not allow inheritable Permissions From parent propagate to this object
\Documents and Settings\ Administrator	Administrators: **Full Control** System: **Full Control** Backup Operators: **Modify**	Replace Permissions on Subdirectories and files
\Documents and Settings\ All Users\Documents\ DrWatson	Administrators: **Full Control** System: **Full Control** Creator Owner: **Full Control** Backup Operators: **Modify** Everyone: **Read**	Replace Permissions on Subdirectories and files
%systemroot%	Administrators: **Full Control** System: **Full Control** Creator Owner: **Full Control** Backup Operators: **Modify** Everyone: **Read**	Replace existing permissions on all subfolders and files Do not allow inheritable Permissions From parent propagate to this object
%systemroot%\config	REMOVE **Everyone Group**	
%systemroot%\repair	REMOVE **Everyone Group**	
%systemroot%\system32\ config	REMOVE **Everyone Group**	
%systemroot%\system32\ spool	Modify Everyone: **Modify**	
%systemroot%\temp	Modify Everyone: **Modify**	
%systemroot%\security	REMOVE **Everyone Group**	
%systemroot%\system32\ dllcache	REMOVE **Everyone Group**	
%systemroot%\Offline web pages	Modify Everyone: **Full Control**	
C:\boot.ini C:\ntdectect.com C:\ntldr	REMOVE **Everyone Group** Administrators: **Full Control** System: **Full Control** Backup Operators: **Modify**	Apply to each individual file. Do not allow inheritable permissions from parent to propagate to these objects
All Data partitions	REMOVE **Everyone Group** Administrators: **Full Control** System: **Full Control** Authenticated Users: **Read**	Replace permissions
cmd.exe, ftp.exe, telnet.exe, ntbackup.exe, rcp.exe, rsh.exe, regedit.exe, regedt32.exe, rexec.exe, secedit.exe, nbtstat.exe, tracert.exe, tftp.exe, finger.exe, netstat.exe, runas.exe, xcopy.exe, arp.exe, cacls.exe, debug.exe, nslookup.exe, cscript.exe, wscript.exe, edlin.exe, ipconfig.exe, ping.exe, at.exe, net.exe, route.exe, edit.com, runonce.exe, ntbackup.exe, syskey.exe	Administrators: **Full Control** System: **Full Control** Backup Operations: **Modify**	Replace existing permissions on all subfolders and files Do not allow inheritable Permissions From parent propagate to this object

Service Configuration:
Configure the following services to start automatically:
1. Event Log
2. Locks Floppy for Admin use only
3. Logical Disk Manager

4. Network Connections
5. Plug and Play
6. Protected Storage
7. Remote Procedure Call
8. Security Account Manager
9. Task Scheduler
10. Windows Management Instrumentation
11. Windows Management Instrumentation Driver Extensions

Configure the following service to start manually:

1. Logical Disk Manager Administrative Service

Disable all remaining services

Disabling NetBIOS:

1. Open Computer Management Console | System Tools | Device Manager | View and select show hidden devices.
    a. In the results expand non-plug and play drivers.
    b. Right click "NetBIOS over TCP/IP" and select disable.

Remap Extensions

The following file types; *.vbs, *.vbe, *.jse, *.js, *.wsh, *.wsf, and *.shs are associated with the windows scripting host and execute automatically. Remapping these extensions to an innocuous program will prevent inadvertent execution of dangerous files.

Appendix B
Security Policy for a Internet Information Server 5.0

Install Internet Information Server 5.0

1. Add/Remove Windows Components
2. Highlight IIS and choose details
3. Choose "World Wide Web Server", "NNTP Service", and "SMTP Service". Additional required components will automatically populate for installation. Note: NNTP and SMTP are required for an Exchange 2000 installation and will be disabled post install.
4. Press "OK", Press Next
5. The install continues without prompting you to select where to place the wwwroot, it will be moved post install.

Configure IIS

1. Start | Programs | Administrative Tools | Internet Service Manager
2. Expand Internet Information Server, Expand computer icon
3. Right click Default Web Site | Properties
   6. Change the Default Web Site Local Path to E:\Inetpub\wwwroot
4. Select Home Directory Tab, Configuration button
5. Under the "App mappings" tab, remove all Application mappings, **except** for .asp. Double click .asp mapping and select "Check that file exists". Press OK
6. Under the "App Options" tab uncheck "Enable parent paths"
7. Under the "Directory Security" tab choose "Edit", uncheck "Windows NT Challenge/Response, uncheck "Anonymous access" and check "Basic authentication". Note: OWA only supports anonymous and basic authentication.
8. Under the "Documents" add a "starthere.htm" file reference and remove all others.
9. Delete all virtual directories under "Default Web Site"
10. Create E:\logfiles
11. Right click web site | properties | Web Site tab | Check Enable Logging | Choose properties and change the "Log file directory" to E:\Logfiles, under the Extended Properties tab check all. Do the same for the SMTP service.
12. Set permissions on E Drive, Administrators Full, System Full, Authenticated Users RX, and Remove Everyone. Check "Replace Permissions on Subdirectories".
13. Delete C:\inetpub, C:\winnt\System32\inetsrv\adminsamples, C:\winnt\system32\issadmin, C:\winnt\system32\inetsrv\issadmpwd, C:\winnt\system32\inetsrv\MetaBack, c:\winnt\help\iishelp, c:\wint\web\printers, c:\program files\common files\system\msadc
14. Disable NetBIOS over TCP/IP Change the following TCP/IP parameter SYN Flood attacks, HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters SynAttackProtect REG_DWORD=1
15. Disable Internet Printing: HKLM\Software\Policies\Microsoft\Windows NT\Printers\DisableWebPrinting DisableWebPrinting REG_DWORD=1
16. Since anonymous access isn't required, disable the IUSR_*Computername* account

Appendix C
Patch Deployment Policy for
Windows Server Operating Systems
And Applications

Introduction

This document details the patch deployment policy for Windows server operating systems and applications. A combination of the Microsoft Security Notification Service and the Shavlik patch management tool *Hfnetchkpro* to report the status of, manage and install patches for the following:

- Windows NT 4.0
- Windows 2000
- .NET Server
- Internet Explorer 5.0 and later
- Internet Information Server 4.0
- Internet Information Services 5.0 and 5.1
- Windows Media Player 6.4, 7.0, 7.1, 8.0, 9.0
- Java Virtual Machine
- SQL Server 7.0 and 2000
- Exchange 2000

Patch Installation Process

1. The security team receives an E-mail notification from the Microsoft Security Service regarding the release of an update[1].
2. The update is evaluated.
3. The update is installed on the staging environment and tested.
4. If successfully tested in staging, the update is installed on the production environment during the next available maintenance window. **Note:** Critical security updates may require immediate installation during an emergency maintenance window.
5. Patch status and installations are verified weekly using Hfnetchkpro.

Patch Verification Process

Machines are scanned weekly using. Hfnetchkpro is an application that performs Microsoft security patch assessment. The HFNetChk engine uses an Extensible Markup Language (XML) file that contains information about which Microsoft security hotfixes are available for each product. The XML file contains security bulletin name and title, and detailed data about product-specific security hotfixes, including:

- Files in each hotfix package and their file versions and checksums.
- Registry keys that were applied by the hotfix installation package.
- Information about which patches supersede which other patches.
- Related Microsoft Knowledge Base article numbers.

For Hfnetchkpro to determine if a specific patch is or is not installed on a given computer, three items are evaluated:

- Registry key that is installed by the patch.
- File versions for all files installed by the patch.
- Checksums for each file installed by the patch.

[1] An update can be hotfix(s), service pack(s), cumulative security updates, and manual configuration instructions.