Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

How to Secure Exchange 2000 against internet threats

Tamer Hassan
MCSE, MCNE, CCNA
Version 1.4b

Abstract

Microsoft Exchange 2000 is one of the leaders in messaging and collaboration. Because of its new enhanced features such as mail, instant messaging, conferencing and XML Web services; Exchange 2000 became an essential critical application for many organizations. Connecting Exchange 2000 and windows 2000 environment to the internet means that many threats will target your email system. Threats result from vulnerabilities found in Exchange 2000 and Windows 2000 and misconfiguration. Leaving the email system defenseless means disaster to your organization's e-business.

To protect against internet threats, this paper will outline the importance of applying the latest patches, how to configure the Exchange 2000, how to secure outlook web access, what to do to protect against viruses and worms and what to do when your budget expands.

Assumptions:

The following has been assumed:
-Firewall has been configured to enable HTTP (port 80), HTTPS (port 443) and SMTP (port 25) traffic between the internet and your network.
-Windows 2000 has been hardened and latest service pack 3 and hot fixes applied.
-You know how to use Exchange System Manager, Registry, and Windows 2000 Administrator tools.

Service Packs and Hot fixes:

Microsoft constantly releases updates for Windows 2000 and Exchange 2000. As an administrator you must keep up with the latest service packs and hot fixes for both Exchange 2000 and Windows 2000.

Service packs and hot fixes will fix the vulnerabilities and solve your system stability problems that may lead to threats target your email server. Missing a hot fix for vulnerability maybe makes your system open to an attack from the internet and your system will be controlled remotely.

SMTP Banner:

Banner grabbing is the first step the attacker will take to identify the version of your email server. Banner Grabbing will help the attacker to tailor later attacks.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Using telnet application to connect to SMTP Port (25), you will see the following banner:

> 220 host.domain.com Microsoft ESMTP MAIL Service, Version: 5.0.2195.5329 ready at Thu, 26 Sep 2002 08:39:08 +0200

To Protect against SMTP Banner Grabbing and confuse the attacker:

1. Download the IIS metabase editor and install it
   Note: IIS Metabase editor can be downloaded from: http://support.microsoft.com/support/kb/articles/Q232/0/68.ASP.
2. Run the Metabase editor.
3. Locate the following key LM\Smtpsvc\1, right click, select New, and then click String.
4. Make sure that the entry in the ID box is 'other', and then type '36907' on the right side of the ID box.
5. In the Data text box, enter the banner that you want to be displayed.
6. Stop the SMTP service and then restart it.

Note: stopping SMTP services will also stop other Exchange services. Make sure that all the Exchange services are running after restarting the SMTP services.

To confirm that the banner has been changed, telnet to port 25 of and you will see the new banner. The section “ESMTP MAIL Service, Version: 5.0.2195.5329” of the old banner has been changed to what you entered. The fully qualified domain name and the date and time will remain the same.

SPAM

Spam is unsolicited commercial email, also called "junk mail"; it consists of advertisements. It is extremely annoying.

SPAM wastes your network bandwidth, and fills your users' mailboxes with useless emails which result in running out of the server’s disk space and down your Exchange 2000 by stopping the ‘Exchange Information Store’ service.

Exchange 2000 does not provide a built in content filtering to protect against SPAM. You can only filter emails based on the email address, domain name, or by an automated junk e-mail script that delivers messages that have a blank address in the 'From' field.
Note: Most spammers do not use real email addresses and that these addresses are randomly changed.

To filter spam, we must first create a message filter list then enable message filtering on the SMTP virtual server:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

A- Create a message filter:

1. Run Exchange System Manager.
2. Expand the Global Settings container, right-click 'Message Delivery', and then click 'Properties'.
3. Click the 'Filtering' tab.
4. Click 'Add', type the name of the sender whose messages you want to filter in the in the Recipient box.

    Note: You can filter by:
    - Display name; for example, “FirstName LastName”.
    - Email address of the sender; for example, “email@domain.com.
    - Group of users in the same domain; for example “*@domain.com.

5. To Archive the filtered messages; Select the 'Archive filtered messages' check box.

    Note: Archived messages will be Archived to the "Exchsrvr\Mailroot\ vsi#\filter". Archived messages will not be removed automatically; you have to plan removing them.

6. Select "Filter messages with blank sender" check box, to filter of messages in which the "From:" box is blank.
7. To prevent the sender from receiving a message informing him that his message was not delivered, select 'Accept messages without notifying sender'

B-Enable Message Filtering on an SMTP Virtual Server:

1. Run Exchange System Manager.
2. Locate the SMTP virtual server, right click and then click 'Properties'.
3. Click 'Advanced', select the 'IP address' to which you want to enable message filtering, and then click 'Edit'.
4. Select the 'Apply Filter' check box, and then click 'OK' three times.

Running Out of Disk Space

An attacker can take your Exchange 2000 down by sending you several emails until the Exchange 2000 server runs out of disk space and stop the ‘Exchange Information Store’ service.

To prevent against such an attack you have to specify the ‘Mailbox Store’ limit:

1. Run System Manager.
2. Locate the mailbox store that you want to configure, right click then select ‘Properties’.

© SANS Institute 2003, Author retains full rights.

3. Click the ‘Limits’ tab to set storage limits according to your server storage capacity.
4. To stop receiving emails more than the required mailbox size. Click ‘Prohibit send and receive at’ then specify the mailbox size limit.

Denial of Service Attack (DoS)

An attacker can take your server down or prevent it from servicing the users by sending more data than your server can handle.

In Exchange 2000 you can reduce the effect of the DoS by specifying message delivery options:

1. Run Exchange System Manager.
2. Locate your SMTP virtual server, and then click ‘properties’.
3. Click on the ‘Messages’ tab.
4. To set the maximum individual message size select **‘**Limit message size to (KB)’ and type the value in KB. The Exchange server will not accept email messages larger than the maximum size which will help limit network traffic, save disk space and improve overall network performance.
5. To set the maximum amount of data that will be accepted during each e-mail session, click the ‘Limit session size to (KB)’ box and enter the value in KB.

SMTP Relay

SMTP Relay is transferring emails through your Exchange 2000 server to other servers. SMTP Relay hides the real email address of the sender and the relayed server address will appear in the header of the message. Your users may use SMTP Relay to send emails when they are on the internet.

SMTP Relay can be used to send emails for spam purposes. One of the anti-spam organizations can detect your server as SMTP Open Relay and include your server’s ip address in their databases-Blacklists. These Blacklists can be used by other email servers’ administrators to stop receiving messages from SMTP Open Relay servers. You will find your server unable to send emails to certain email servers.

To remove your server from the blacklists you have to configure your server to prevent it from being Open relay. Then submit your server ip address to the anti-spam organizations that blacklisted you server to remove your server’s ip address from their blacklists.

By sending many emails through your Exchange 2000 server, an attacker can

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

take your server down and consume your internet link bandwidth

By default Microsoft Exchange 2000 allows authorized Relaying; to relay through an Exchange 2000 server you must provide a valid user name and password.

You have to make sure that the default settings have not been changed by doing the following:

1. Run the Exchange 2000 System Manager, locate your SMTP Virtual Server, right click on it and then click properties.
2. Click on “Access” Tab, then click on the “Relay” button.
3. In the “Relay Restrictions” Dialog box; make sure that “Allow all computers which successfully authenticate to relay, regardless of the list above” is selected.

Address Spoofing:

An attacker can send you an email using any internal user email address. The email will appear as if the message has been sent from that internal user. It could be used as some sort of social engineering. For example, an attacker can send an email using one of the IT personnel email addresses asking the CEO about his password.

By default, Exchange 2000 resolves addresses in the header to addresses in the Global Address List whether the email is from internal user or from the internet.

To ensure that the emails from outside the Exchange organization remain unresolved:

1. Locate the following key in the registry:

   HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/ MsExchangeTransport/Parameters/ 1

2. Right click on the right panel, click 'Add Value', and then add the following registry value:

   Value name: ResolveP2
   Data type: REG_DWORD

3. Set the value of the 'ResolveP2' to '48'.
4. Exit the Registry editor.
5. Restart the SMTP Virtual Server to apply the changes.

Securing OWA

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Outlook Web Access is an Application that works in conjunction with IIS to enable Exchange 2000 Users to access their mailboxes using any standard web browser like Internet Explorer or Netscape.

IIS is more vulnerable to attack than any other Web server. The default installation of the IIS contains several security holes and exploits that lead into compromising your server.

We will discuss locking down the IIS to protect against web attacks, hiding the Internal private IP address of the server, using SSL to protect the communication between your Internet users and the OWA Server and Password Defense.

IIS Lockdown Tool:

Microsoft has released a security tool known as the IIS Lockdown Tool. You can use this tool to protect against security threats that target the IIS by removing and disabling settings and services not related to the Exchange 2000 OWA.

The IIS Lockdown wizard tool can be downloaded from:
http://www.microsoft.com/downloads/release.asp?ReleaseID=43955&area=search&ordinal=1

To lockdown IIS for Exchange 2000:

1. Run the IIS Lockdown wizard “iislockd.exe”.
2. Once the Internet Information Services Lockdown Wizard begins, click ‘Next‘
3. Click ‘I agree’ to agree to the licensing agreement and then click ‘Next’
4. In the Select Server Template window, select ‘Exchange Server 2000 (OWA, PF Management, IM, SMTP, and NNTP)’
5. Click ‘View Template Settings checkbox’ and then click ‘Next’
6. Review the Internet Services settings and then click ‘Next’
7. Review the Script Maps settings and then click ‘Next’
8. Review the Additional Security settings and then click ‘Next’
9. Review the important note for the URLScan settings and then click ‘Next’
10. Click next to acknowledge the settings you have chosen to apply to the IIS sever then click next.
11. Once the wizard completes the configuration, click ‘View Report’
12. Review changes made by the wizard then close the log
13. Click ‘Next’ and then click ‘Finish’.

IIS Lockdown wizard performed the following:

- Disabled ‘Index Server Web Interface (.idq, .htw, .ida)' script map.
- Disabled ‘Internet Data Connector (.idc)’ script map.
- Disabled 'Server side includes (.shtml, .shtm, .stm)' script map.

© SANS Institute 2003, Author retains full rights.

- Disabled '.HTR scripting (.htr)' script map.
- Disabled 'Internet printing (.printer)' script map.
- removed the printer virtual directory.
- Set file permissions to prevent anonymous IIS users from writing to content directories.
- Set file permissions to prevent anonymous IIS users from running system utilities.
- Installed URLScan filter on the server.
- Removed 'Scripts' virtual directory.
- Removed 'MSADC' virtual directory.
- Removed 'IIS Samples' virtual directory.
- Removed 'IISAdmin' virtual directory.
- Removed 'IISHelp' virtual directory.

URLScan Tool:

"URLScan screens all incoming requests to the server, and filters them based on rules set by the administrator. This secures the server by ensuring that only valid requests are processed"[1]. Microsoft released URLScan 2.5 which allows you to filter requests based on length, character set, content and other factors.

URLScan 2.5 can be downloaded from:
http://microsoft.com/downloads/release.asp?ReleaseID=38020&area=search&ordinal=5

Note: Before installing URLScan 2.5 you must install URLScan 2.0 which is part of IIS Lockdown tool.

You can customize URLScan by editing 'urlscan.ini'. You can find 'urlscan.ini' in the folder 'c: \winnt\system32\inetsrv\urlscan'.

To protect against buffer overflow you can limit the length of the requests by editing the 'urlscan.ini' and setting the value of 'MaxUrl' option under 'Request Limits' section.

To protect against figuring out what web server you use, you can remove the server header on all responses by editing the 'urlscan.ini' and changing the value of 'IISRemoveServerHeader' to 1.

Note: whenever you edit urlscan.ini restart IIS to apply the changes.

[1] "URLScan Security Tool". Microsoft. 27 November 2001. URL:http://www.microsoft.com/windows2000/downloads/recommended/urlscan/default.asp

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

IIS IP Address disclosure

By sending an HTTP request with an empty host name to the IIS; The IIS will reveal its private IP address. IP Address disclosure will help the attacker to map your internal network.

To prevent Internal IP Address disclosure you can modify a value in the IIS Metabase:
1- Open a command prompt and change the current directory to 'c:\inetpub\adminscripts' or to where the adminscripts can be found.
2- Run the command: 'c:\inetpub\adminscripts>adsutil set w3svc/UseHostName True' [enter].
This value will cause the IIS server to send the server's host name instead of its private IP address.
3- Restart the 'IISAdmin' to apply the changes.

SSL

By default all communications between the OWA and the end-user browser are not encrypted. This may lead into the Man-In-the-Middle Attack. The attacker will be able to capture the traffic between the server and client and extract the important data such as username and password.

Using SSL will encrypt the traffic between the OWA and the end-user browser. To enable SSL on your IIS server you have to obtain an SSL certificate or you can use Microsoft Certificate Server to install your own certification authorities.

To configure SSL for OWA:

1. Start Internet Services Manager.
2. Locate the Default web site that contains the Exchange 2000 virtual roots, and then Right click and select 'Properties'.
3. In the 'Web Site' tab, enter the SSL port number, default is 443, then click 'apply'.
4. Click the 'Directory Security' tab.
5. Under 'Secure communications', click 'Server Certificate' to start the Web Server Certificate Wizard. You can use the Web Server Certificate Wizard to configure the certificate, based on the information that your certification authority provided.
6. Confirm that SSL is enabled by browsing to: https://servername/Exchange.

If you want to enforce the use of SSL, you can enable the 'require secure channel' option on each Exchange 2000 virtual root:

1. Start Internet Services Manager.

© SANS Institute 2003, Author retains full rights.

2. Locate the Exchange 2000 virtual root that you want to secure, then Right click and select 'Properties'.
3. Click the 'Directory Security' tab.
4. Under 'Secure communications', click 'Edit'.
5. Check the 'Require secure channel (SSL)' check box.

Password Defense

If your users access the Exchange 2000 using the Outlook Web Access you must enforce a strong password policy to protect their passwords. An attacker can use one of the password cracking methods to crack one of the users password.

You should educate users when they change their passwords they have to consider the following:

- Password must be at least six characters.
- Password should be at least three of these four character types: uppercase letters, lowercase letters, numerals, and non-alphanumeric characters (e.g. *, %, &,!).
- Password must not be identical to the user's login name or full name.

Viruses and Worms

Most of viruses and worms spread using emails. Viruses and worms can result in a lot of damage to your system. They can replicate themselves to all the Exchange 2000 mailboxes and consume your storage.

Exchange 2000 provides a new virus scanning API that is implemented at a very low-level in the Exchange store. The virus scanning API provides improved support for scanning streaming content and reporting on the sender and receiver of the virus.

The most efficient way to protect against viruses and worms is to install a server based antivirus. Server based Antivirus will be your first line of defense against viruses and worms.

When you buy a server based antivirus consider the following key features:
- Seamless integration with the Microsoft Exchange 2000 virus scanning API.
- Support of multiple virus engines.
- Real-time protection of multiple storage groups and their databases.
- Full protection of the Exchange 2000 web storage system, including support for messages sent via Outlook Web Access.
- Memory scanning and multi-threaded scanning process.
- Protection against new virus threats and blocking of attachments based on wildcards.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Blocking and removal of mass mailed emails during virus outbreaks, thus preventing unproductive content from entering the Exchange server.
- Content filtering and anti-spamming.

When your budget expands

According to your IT budget you can do the following to protect your Exchange 2000:
1- Implement Front-End and Back-End Servers. The Front-End will act as a proxy for the Back-End and will provide protection against attacks. Attacking the Front-End will not compromising the Back-End.
2- Implement a DMZ and place the Front-End Server between two Firewalls.
3- Implement antivirus and content solution on the Firewall.
4- Implement Network Intrusion Detection System and Host Intrusion Detection System.
5- Implement Patch management software to help you keep up to date and deploy the latest Microsoft software updates.

Conclusion

Exchange 2000 is a critical and vital application for your business. The most important task for the Exchange 2000 administrator is to keep the Exchange 2000 secure and available. Any leakage of information or system failures can be disastrous. Keep in your mind that Implementing Firewall will not fully protect your Exchange 2000. Extreme measures must be taken to make sure that the server is protected against threats that might have a negative impact on your business. The IT department should always remain up-to-date on all security and update issues concerning Exchange 2000 and Windows 2000.

References

Weber, Chris, "Securing Exchange 2000, Part One". 23 April 2002. URL:http://online.securityfocus.com/infocus/1572

Weber, Chris, "Securing Exchange 2000, Part Two".8 May 2002.

URL:http://online.securityfocus.com/infocus/1578

“Turning on SSL for Exchange 2000 Server Outlook Web Access", Microsoft Support.6 August 2002.

URL:http://support.microsoft.com/default.aspx?scid=kb;en-us;Q320291

“How to Enable or Disable Message Filtering on a Simple Mail Transfer Protocol Virtual Server", Microsoft Support. 22 October 2000. URL:http://support.microsoft.com/default.aspx?scid=kb;en-us;Q261087

“Internet Information Server Returns IP Address in HTTP Header", Microsoft Support. 11 June 2002.

URL:http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q218180&

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Litchfield David, "IIS Internal IP Address Disclosure". 6 March 2002.

URL:http://www.securiteam.com/windowsntfocus/5VP021P6KY.html

“Security Operations Guide for Exchange 2000 Server”, Microsoft Support. 14 October 2002.

URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/mailexch/opsguide/default.asp

"ResolveP2 Functionality in Exchange 2000 Server", Microsoft Support. 6 August 2002.

URL:http://support.microsoft.com/default.aspx?scid=kb;en-us;Q288635

"Configuration and Security Update Recommendations for Exchange 2000", Microsoft Support. June 2002.

URL:http://www.microsoft.com/exchange/techinfo/deployment/2000/BestConfig.asp

English, Bill, "Securing Exchange 2000 Server E-mail". 14 March 2002.

URL:http://rr.sans.org/email/sec_exchange.php

"Email Security", GFI Security.

URL:http://rr.sans.org/email/GFI_email_sec.php

“IIS Lockdown and URLscan Configurations in an Exchange Environment”. Microsoft Support. 14 October 2002.

URL:http://support.microsoft.com/default.aspx?scid=kb;en-us;Q309508

“Prevent Unsolicited Commercial E-Mail in Exchange 2000 Server”.

Microsoft Support. 26 October 2002.

URL:http://support.microsoft.com/default.aspx?scid=kb;en-us;319356

© SANS Institute 2003, Author retains full rights.