

Securing Exchange 2000, Part 2

Chris Weber 2002-05-08

Securing Exchange 2000, Part Two

by *Chris Weber*

last updated May 8, 2002

This is the second installment in the two-part series on securing Exchange 2000. The first article offered a brief overview of implementing Exchange 2000, along with some exploits that systems administrators need to be aware of. This installment will focus on secure configuration and administration of Exchange 2000, including locking down Exchange, and an analysis of some publicized vulnerabilities.

Secure Administration

Now that we have covered some of the basics of implanting Exchange 2000, let's step away from the assessment side, and get into securing it.

Some Security related changes from 5.5 to 2000

There are quite a few key differences between Exchange 5.5 and 2000. Among these differences are that SMTP relay is disabled, rights to the Mailbox are different, and there is no more Service Account. I will go into greater detail about these changes in the section that follows.

SMTP

SMTP relay was a big problem for earlier versions of Exchange. Because SMTP relay came enabled by default, mail servers could be exploited by spammers unless the administrator was aware and disabled the relay functionality. A relay server will happily send mail to any Internet e-mail address, by any sender creating the mail message. The sender doesn't need to have an account on the mail server, and there is no authentication requirement.

Needless to say, if anybody on the Internet can use your mail server to send SMTP based e-mail to anybody else on the Internet, your server will quickly gain popularity in the spammer community and you will wonder why your tracking logs keep growing so fast.

Microsoft made a good move by shipping Exchange 2000 with SMTP relay disabled by default. If you need it, you have to enable it. However, this includes a big caveat: as you may have seen with the February security alert from Microsoft ([MS02-011](#)), there is a vulnerability that still allows for mail relay even when it has been disabled. As BindView's Razor team discovered, the SMTP service bundled with IIS supports NTLM authentication, and [will allow for null credentials to be used for authentication](#). Once authenticated, the default behavior of the SMTP service is to allow mail relay.

Rights to the Mailbox

Exchange 2000 user rights are much more granular than earlier versions. Your administrator accounts can no longer read other user's e-mail (at least not by default), and you will notice that there are a couple of new User groups setup in your domain and forest. The following summarizes the key differences in user rights between Exchange 5.5 and 2000:

- Admin is DENIED access to mailboxes (by default), but is easily changed;
- "Exchange Domain Servers" group full access; and,
- %COMPUTERNAME%\$ full access.

Service Account

Exchange 2000 now uses the LocalSystem account to run its services. Your LSA secrets are safe now because this service account has been removed, and replaced with the LocalSystem account. You should know by now that using administratively privileged accounts to run Window's services provides one of the most common means for an entire domain to be compromised. Whenever you run a SERVICE in the context of a USER account, that user's password is stored in a protected part of the registry (called LSA Secrets) in almost clear text. Tools like LSADUMP2.EXE will dump these contents so that you can see the password in plain clear text. You can easily conclude that when a system is compromised, even a basic user's workstation, the password for a domain administrator account running some backup software service can be a very useful find.

Locking Down Exchange 2000

Some of the things to put on your lockdown checklist, mostly related to the Windows OS instead of the Exchange application, include the following:

- [Windows 2000 Server Baseline Security Checklist](#), which includes
 - Disable unnecessary services and ports
 - Enable Auditing
 - Rename local Admin account and enable a strong password
- ACL and monitor critical Registry keys - This is basic good practice for secure administration.

Just a note, it's good to know if your WinReg key changes to allow the EVERYONE group READ access. That permission allows any user to remotely connect to the REGISTRY of the Exchange server. This is NOT a good thing! This is actually part of a known Exchange vulnerability that will be discussed later in this article. You should also watch your event logs for failed log-in attempts on the administrator account. This is a sure way of knowing that someone is trying to get your keys.

Administrative Roles

Administrative roles can be applied at the Organizational level within Exchange, as well as the Administrative Groups level. Exchange 2000's three built-in roles are:

- Exchange Administrator
- Exchange Full Administrator
- Exchange View Only Administrator

By default the OU "domain admin" is given Full Admin rights at the Exchange Organization level. This can be easily changed, and should be controlled in organizations that do not want administrators reading other's e-mail. Not that the admin can by default, but as mentioned, this is trivial to set.

With Exchange 2000, you can completely control delegation of responsibilities through granular admin rights. The help desk folks can view and add mailboxes, and change passwords with the "View Only Administrator" role. The "Exchange Full Administrator" can manage the Exchange Organization as well as change permissions on Exchange configuration objects. And the "Exchange Administrator" can manage the Organization, but cannot modify permissions on objects.

Keep the following things in mind when you plan and setup your Admin accounts:

- Create individual admin accounts and make use of the built-in roles to audit who does what in your Exchange Organization.
- Exercise the principle of least privilege: don't make anyone an admin unless they don't need to be!
- Make sure to use the Delegation Wizard whenever adding or editing user administrative roles in Exchange. This tool sets the proper rights in Active Directory and Exchange.

The article [XADM: How to Get Service Account Access to All Mailboxes in Exchange 2000 \(Q262054\)](#) describes how you can set it up so an Admin has access to all Mailboxes.

Exchange Domain Servers

There is a potential weakness in multiple server environments. It is really just another case of "trusting the trusted." Because the "EXCHANGE DOMAIN SERVERS" Global group is Full Admin on each Exchange computer, and this Global group contains all the exchange SERVER computer accounts, then every Exchange SERVER account in your organization has full control over the other servers. Since you may not want servers accessing each other's information stores, Microsoft has made a script that addresses this default setting. Check out the article [XADM: Enhancing the Security of Exchange 2000 for the Exchange Domain Servers Group](#). The lockdown script tightens security by allowing access to the mailbox and public stores on only the local server.

Security Permissions Pages

You may want to enable the security pages within the System Manager. This will give you a view and control of Security ACLs in all relevant parts of the Organization. To show the security tab in System Manager, set this registry key:

```
HKCU\Software\Microsoft\Exchange\ExAdmin  
Value: ShowSecurityPage  
Date: 1 (REG_DWORD)
```

For more details, read the article [XADM: Security Tab Not Available on All Objects in System Manager](#)

Note: it is important that you do not remove permissions without verifying that Exchange still

functions as expected! To be safe, you should use the Delegation Wizard when assigning permissions, which will set permissions correctly in all relevant parts of the configuration.

Share Security

I talked a little bit about how the Tracking Logs can expose some information useful to an attacker. The tracking logs contain e-mail addresses that typically correspond directly to usernames. Once an attacker has a list of usernames, they have won half the battle! Now all they need is to guess passwords. The tracking logs are available to EVERYONE "Read only" by default. Remove this permission from the share for added security. Add

The path to the tracking logs is \Exchsrvr\%COMPUTERNAME%.log and the files are named according to the date.

Turn Off What You Don't Need

This point cannot be emphasized enough! Disable any unused protocols and services from your Windows OS and Exchange. Do not run IPX/SPX if you are only using TCP/IP. Do not run the DHCP client if you are configuring static IP addresses. If your Exchange server is only doing SMTP relay, then turn off HTTP, POP, and IMAP.

Exchange comes with many options turned on. If you don't take the time to tone it down a bit, you will most likely end up wishing you did!

System Policies

Built-in System Policies in Exchange 2000 include:

- Server policy
- Mailbox policy
- Public Folder policy

System Policies provide a way to maintain settings and apply them to multiple servers, mailboxes, or public folders. Under your Administrative Group in System Manager, right click System Policies and select **New** followed by **Server**, **Public Store**, or **Mailbox Store** policy. Create a new policy container for each item this way. Then configure each policy. For Server, you can enable/disable message tracking. For Mailbox Store you can set Storage Limits, deleted

item retention time, and other options. The same is true for the Public Folder store.

Malware

Your malware protection strategy should be a multi-layered one. For incoming and outgoing SMTP mail, you start filtering at the gateway with an SMTP content filter. Make this a separate host from the Exchange server, if possible. Filter for attachments you don't want entering, such as: .VBS, .EXE, .BAT, .CMD, .WSF, and others. If your users really want to get such attachments, they should use PGP or some other form of encryption to get by this restriction. The main purpose of this restriction is to safeguard against those folks who don't know any better than to open up such attachments, even when they come from some random, unknown sender!

Then load up your Exchange server itself with good anti-virus software that will protect the Information Store and the file system. Finally, stagger it all by enabling anti-virus software on your file servers and client workstations. Keep updated virus signatures on all of these systems and you should be in good shape. Remember, the best way to defend against future attacks similar to the worms of last year like Nimda, is to filter on attachments at your gateway.

Outlook Client

The client is the most important piece in this malware puzzle. After all, Exchange server itself is just a delivery service, and does a fine job of getting mail from point A to point B - don't blame the messenger right?. The client is where the real threat is, and where the core threat lies. The client software is usually where the malicious code is actually launched from, when a user opens an email or attachment that they shouldn't have. I don't get into Internet Explorer and Outlook too much here, but they are perhaps more important to consider than the server itself. I don't get into Internet Explorer and Outlook too much here, but they are equally important. Because Outlook uses the IE engine for reading HTML based e-mail, you need to set it to use the Restricted Sites setting. This will make Outlook treat all HTML mail as untrusted, preventing the execution of active content and scripts (provided you haven't adjusted these zone settings in IE).

Outlook Web Access

When setting up OWA, you have several things to consider. Remember to lock down IIS and

the Web Publishing Service. Decide if you are going to use the front-end/back-end model and plan your design around it, considering your firewall rule-sets. Plan on using SSL for protection between your Internet clients and the OWA front-end. Also, look into setting up static RPC ports for communication between the OWA front-end and back-end AD servers.

Lockdown IIS

In addition to locking down the Windows OS, you have to tighten up the IIS configuration. For this, you can follow the Microsoft checklist of [security tools](#). Install IIS on a non-system partition, remove those default virtual directories, the sample directories, AND perhaps most important, the script MAPPINGS you are not using, such as ".printer". Check out the iislock.exe tool from Microsoft, it can save you some time in hardening your IIS configuration.

Use SSL

Definitely use SSL between the front end Web server and clients. This will encrypt messages sent across the network, as well as encrypting your usernames and passwords. Basic Auth is required for an OWA front-end server! Realize that the user name and password is sent in practically clear text: that is, they are Base64 encoded, which provides almost no protection - another reason you should use SSL! You can also explore the use of secure tokens such as RSA SecurID for maximum protection. And look for smart card and S/MIME support in upcoming versions of OWA.

To configure SSL support for HTTP, open up the *Internet Services Manager* for the Exchange virtual server, and right-click the Default Web Site, then click Properties. Open the Directory Security tab, and select Server Certificate. Go through the certificate wizard to set up your server's SSL certificate.

Front-end/Back-end Mode

When designing your OWA network, be sure to check out the Microsoft white paper [Exchange 2000 Front-end and Back-end Topology](#), which describes how to design your front-end/back-end topology. This paper describes the different scenarios you will probably consider in your OWA design, and details the firewall configurations for each set-up. Consider isolating your OWA front-end in a protected DMZ, where it can only communicate with the back-end Exchange server and an Active Directory DC or Global Catalog server.

Set Static RPC Ports

Remember that Windows uses RPCs to do much of its Active Directory service discovery and client authentication. On your Domain Controller and Global Catalog server, set this RPC port to a static TCP port instead of dynamic, so you don't have to open up TCP ports 1024+ on your firewall. If you set the static RPC port to 1025, for instance, you will only need to open up ports 135, 445, and 1025 on your DMZ firewall. This will enable you to use features provided via RPC, such as implicit log-in. Details for setting up static RPC ports can be found at Microsoft's Website: [Restricting Active Directory Replication Traffic to a Specific Port](#)

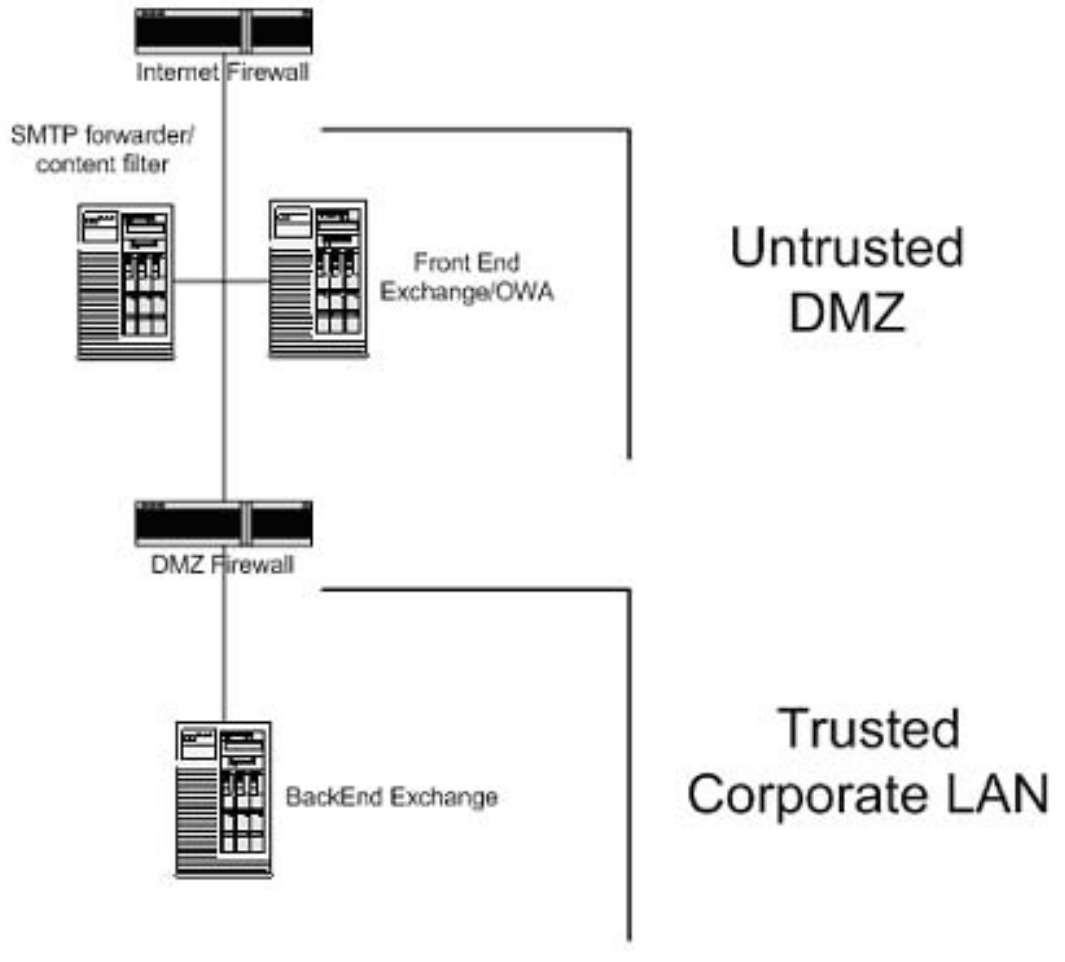
Front-End/Back-End Network Design

In the following diagram, I illustrate a common Exchange/OWA network configuration, in which the front-end OWA server is sandwiched in a DMZ between two firewalls. The traffic you let pass through the firewalls will depend on your organization; however, in general, this diagram shows the holes you will need for a basic Exchange/OWA design.

Internet Firewall:

DENY ALL by default
Incoming from Internet Allow
TCP port 25 (SMTP)
TCP/UDP port 53 (DNS)
TCP port 443 (HTTPS)

Outgoing Allow:
Only established connections
TCP/UDP port 53 (DNS)
TCP port 25 (SMTP)



DMZ Firewall:

DENY ALL by default
Incoming from DMZ Allow
TCP/UDP port 53
TCP port 80 (HTTP)
TCP/UDP port 88 (Kerberos)
TCP port 135 (endpoint mapper)
TCP/UDP port 389 (LDAP)
TCP port 445 (SMB/CIFS)
TCP port 1025 (optional RPC static port - hey, it's either this or 1024+)
TCP port 3268 (GC)

Outgoing Allow:
Only established connections

Vulnerabilities

The following is a list of Exchange 2000 vulnerabilities (as of the time of publication of this article). These bullets take a look at some of the publicized vulnerabilities for Exchange 2000 listed at [Microsoft's security search Web site](#).

- February 2002 *
 - [MS02-012: Malformed Data Transfer Request can Cause Windows SMTP Service to Fail](#)
 - [MS02-011 : Authentication Flaw Could Allow Unauthorized Users To Authenticate To SMTP Service](#)
 - [MS02-003 : Exchange 2000 System Attendant Incorrectly Sets Remote Registry Permissions](#)
- September 2001
 - [MS01-049 : Deeply-nested OWA Request Can Consume Server CPU Availability](#)

- August 2001
[MS01-043 : NNTP Service in Windows NT 4.0 and Windows 2000 Contains Memory Leak](#)
- July 2001
[MS01-041 : Malformed RPC Request Can Cause Service Failure](#)
- June 2001
[MS01-030 : Incorrect Attachment Handling in Exchange OWA Can Execute Script](#)
- March 2001
[MS01-014 : Malformed URL Can Cause Service Failure in IIS 5.0 and Exchange 2000](#)
- November 2000
[MS00-088 : Exchange User Account Vulnerability](#)

Of most interest are the three most recent one, announced in February of this year.

MS02-012 describes a denial of service vulnerability in the SMTP service. By sending a specially crafted SMTP packet, the SMTP service will fail, and possibly the other services which IIS provides (Web, NNTP, and FTP).

MS02-011 describes the fact that an anonymous user can send e-mail via IIS's SMTP service. This is equivalent to saying that a null session can be used to relay mail off your SMTP server. The fact is that the SMTP service doesn't perform any extra, necessary steps during authentication, to prevent this attack. This vulnerability was discovered and reported by BindView's RAZOR team, and actually does not apply to Exchange 2000. It only affects IIS 5.0 and Exchange 5.5, but not to systems with Exchange 2000 installed.

MS02-003 the System Attendant inappropriately gives the EVERYONE group access to the WinReg key for remote registry access. The System Attendant does this in order to facilitate remote Exchange management; however, it is an inappropriate setting. Check out the [link and article](#) for more info. You will definitely want to fix this. With this setting, any authenticated, and in some cases ANONYMOUS, user can remotely connect to the server's registry, and read through a ton of useful information. And worse, depending on how your registry key permissions are set up, they may be able to modify values.

Also, the last one on the slide, **MS00-088**, is important to those EARLY Exchange 2000 adopters out there. If you installed one of the early Exchange releases, I believe it was Revision A, then you might have the EUSR_COMPUTERNAME account installed on your server. This account has Full Admin rights to Exchange, and has a known password. Watch out!

Some Final Notes

SMTP replication in clear text! Use *IPSec with encryption parameters to protect this traffic. SMTP replication is an option for Exchange server connectivity. You can opt to use SMTP as the transport protocol between two Exchange servers, instead of RPC. By doing this you are losing out of several of RPC's security defenses, the most important of which may be encryption. If you are using an SMTP connector across an insecure network, such as the Internet (or maybe even your intranet), you should definitely use IPSec to protect the traffic.

*IPSec Reference Articles

[Using IPSec in Windows 2000 and XP](#)

[Using IPSec in Windows and XP, Part Two](#)

[Using IPSec in Windows 2000 and XP: Part Three](#)

Public folders Remember that by default, the EVERYONE group can add new public folders. If you have been running Exchange for a while, you have most likely already dealt with this.

Event sinks Finally, if you have installed and enabled the Event Sinks, which come with the installation files, take a look at the article [XCCC: Script Host Sink Is Not Registered on Exchange 2000 Server by Default \(Q264995\)](#) by Glen Scales to understand the security implications. With the event sinks installed, it is possible to run vbscript code through plain e-mail messages. Of course, with VBscript much is possible, including modifying user accounts and controlling the file system.

Relevant Links

[Securing Exchange 2000, Part One](#)

Chris Weber, SecurityFocus

[Privacy Statement](#)

Copyright 2006, SecurityFocus