Global Information Assurance Certification Paper

Securing Exchange 2000 Server E-mail.

Bill English

Abstract:

The focus of this paper is on how to secure Exchange 2000 Server e-mail. Attack types are presented and solutions are offered in the hopes that many will find new methods of securing their inbound and outbound e-mail. Specific vulnerabilities with Exchange 2000 Server are discussed as well. This paper outlines two common topologies and explains how to use current technologies to ensure e-mail sent to and from an Exchange 2000 Server is both secured and free of malicious code or attachments.

Introduction

> "The bill to 50,000 US firms this year for viruses and computer hacking will amount to $266 billion, or 2.5 percent of USA's GDP."
>
> -Information Week, July 2000

The old phrase "a chain is only as strong as its weakest link" is one that we've all heard before. Some have taken this phrase and applied it to security: "a network is only as secure as its least secured link". E-mail should always be considered a "weak link" on your network because it is an obvious entry-point into your network. Attackers like to use e-mail to wreak havoc because it's easy: no matter how well you secure your network, chances are good that you'll have port 25 open on your firewall and have an SMTP server ready to work with e-mail when it comes in.

This paper will outline four different actions you can take to secure your Exchange 2000 Server deployment. The focus of the paper will be on security both at the product level, and at the larger network level too. And we'll see that the larger part of securing Exchange 2000 Server is securing the e-mail before it arrives at your Exchange 2000 Server.

Whenever we secure anything, we should, at some point, ask the question, "Secure it from what?" Since Exchange 2000 Server can't protect your data or itself from all types of attacks, we need to outline the specific attack types that we have in mind, and they are:

- Attacks against the Exchange platform
- E-Mail attacks
- Attacks against Internet Information Services (IIS) that affect Exchange 2000 Server

There's much to discuss on this topic. We will start by discussing content and virus scanning, then we'll discuss certificates and encryption. We'll also discuss router placement and the current vulnerabilities of Exchange itself. We will present all these issues using two different, but common topologies as a backdrop to learning how to secure Exchange 2000 Server.

Securing Exchange 2000 Server with a Single Firewall

In our first topology, Exchange 2000 Server is placed behind a single firewall. Port 25 is opened to allow e-mail to pass in and out of the organization. In many environments, this is the sum total of their network security measures for e-mail. Figure 1 illustrates this single-firewall configuration.

Figure 1

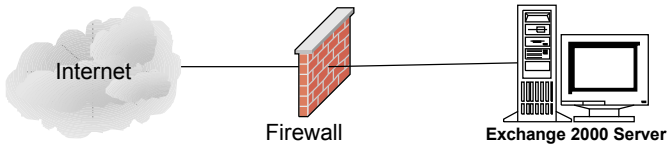

Figure 1

The problem with this approach is not that port 25 is open, but that there is little to account for the known vulnerabilities with e-mail and Exchange 2000 Server that operate over port 25. And given that port 25 and e-mail in general is one of the most often attacked ports by hackers[2], it is rather unwise to ignore these potential threats.

How Hackers Work

Hackers start by learning that a mail server exists. Generic scanning tools can tell them this. Coupled with the public information of your DNS records, they can quickly know much about your network.

If they are unsure as to the exact platform of your SMTP (Simple Mail Transport Protocol) server, they can do one of two things to learn which mail system is being run. First, the hacker can send a bogus e-mail to your server, such as blah@yourdomain.com and then read the header that comes back to determine what mail server your running. Your server's platform information is in the header. Secondly, the hacker can use telnet to open a session to your server over port 25 and read the banner, which by default, includes the version of Exchange 2000 server you're running.

Now that they know which e-mail server software you're running, the hacker will

then check known databases to find vulnerabilities they can exploit. The known vulnerabilities (at the time of this writing) for Exchange 2000 Server are listed in Microsoft's Security Bulletins MS00-088[3], MS01-014[4], MS01-030[5] and MS01-049[6]. A short description of each vulnerability is listed in Table 1.

Table 1
Vulnerability Descriptions for Exchange 2000 Server

Microsoft ID	Description	Vulnerability Fix
MS00-088	During the initial setup of Exchange 2000 Server, a default user account, EUSR_EXSTOREEVENT was created to facilitate the processing of workflow and event scripts. If Exchange 2000 Server is installed on a domain controller, then this account will have domain rights. A malicious user could use this account to gain access to other domain resources.	Exchange 2000 Server Service Pack 1
MS01-014	A malformed URL could cause IIS (Internet Information Services) to cease functioning. This affects Exchange 2000 Outlook Web Access (OWA) clients. MAPI (Message Application Programming Interface) clients are not affected by this vulnerability and this is not a direct attack on Exchange 2000 Server. The flaw exists in two different code modules, on one that installs with IIS and the other that installs with the OWA pages for Exchange 2000 Server.	Patches have existed since March, 2001 for both platforms
MS01-030	When a user receives e-mail using OWA, there is the possibility that an attachment which contains HTML code that includes malicious scripts could be programmed to execute when the attachment is opened, regardless of the attachment type. Because OWA requires that scripting be enabled in the zone where the OWA server is located, this script could take action against the user's Exchange mailbox, including the manipulation of messages or folders.	A security patch exists for this vulnerability.

MS01-049	This security vulnerability relates to Outlook Web Access. OWA will accept and process a request for an item in an authenticated user's mailbox without verifying first that the folder structure is valid. A malicious attack could be mounted by repeatedly levying a request for a non-existent but deeply nested folder in the user's own mailbox. The effect of this vulnerability is to cause the process servicing the attacker's mailbox to consume most or all of the CPU availability on the server it was running on.	A security patch exists for this vulnerability.

Notice that in three out of the four vulnerabilities, OWA is involved. This is not surprising, since OWA requires IIS, and IIS is a favorite target for many hackers. In addition, note that none of these vulnerabilities exposes the Exchange stores directly to the internet. Instead, these vulnerabilities nip at the edges of Exchange 2000 Server.

Flying at the 50,000 foot level, here are, generally speaking, the kinds of attacks an e-mail administrator can rightfully anticipate:

Here are the more common types of vulnerabilities[7]:

1. Buffer overflows: sends a larger quantity of data to the server than was anticipated. Depending on how the overflow is executed, this could cause the server to stop working or it might run malicious code from the attacker.
2. Data processing errors: not as common now, but the concept is that a small program is sent directly to the server and the server will run it. What is more common today is to send such programs to a network though e-mail as attachments. Depending on their function and purpose, these programs can be called worms, viruses or Trojans.
3. HTML viruses that do not require user intervention that run unattended scripts[8]

Notice that the first attack type depends on a server that has not been patched for a known vulnerability. The second type of attack usually depends on a user's intervention. The third type of attack is the most sinister, not requiring any user intervention or lack of a patch on the server in order for it to be effective. The e-mail arrives at the Exchange 2000 Server and the code simply fires. There is little, if any warning, that you are under attack – until it is too late.

In a single firewall topology, with no content or virus scanning, what can a hacker do in such a situation? Well, quite a bit, actually. Here are some things that an attacker can do to an Exchange 2000 Server[9] in this first scenario:

- Send you a Trojan.

- Send you a worm.
- Attempt a Denial of Service (DoS) attack
- Use specialized tools that will run programs intended for a different port, such as port 80, over any port selected, in this case, port 25.
- Exploit Outlook Web Access (OWA) over port 80

How do we protect against these kinds of attacks? By starting with the use of dual firewalls.

Dual Firewall Topology

In this scenario, you can place the Exchange 2000 Server that hosts your mission-critical data behind *two* firewalls, as illustrated in Figure 2.

Figure 2
Dual Firewall Topology

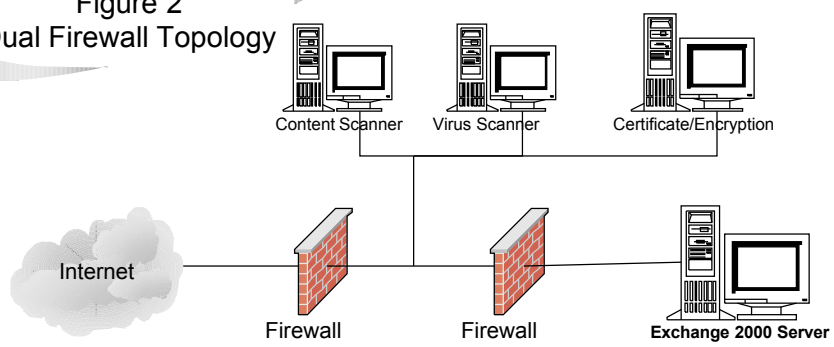

Figure 2

You have obviously noticed the addition of three servers between the two firewalls. These servers offer specific functions that provide additional protections. In this scenario, mail from the internet will pass through port 25 on the outside firewall, then be routed to the Content Scanning server where the e-mail will be scanned for attachments and HTML code embedded in the e-mail itself. Then, any mail after that is passed through the virus scanner to clean out any attached, known viruses. Thirdly, the e-mail is forwarded to another Exchange 2000 Server that will re-send the e-mail to the internal Exchange 2000 Server encrypted and signed. The internal Exchange 2000 Server is configured to accept inbound mail *only* from the third Exchange 2000 Server. Now, no system is fool-proof, but this logical topology is has several advantages. You'll recall that I promised four actions you could take to secure your e-mail in Exchange 2000 Server. I've just outlined what those four actions are:

1. Content scanning of e-mail
2. Virus scanning of e-mail
3. Encryption of e-mail to the internal Exchange 2000 Server
4. Digital Signature of e-mail from the third, perimeter Exchange 2000 Server to the internal Exchange 2000 Server

Let's discuss how each function serves to secure your intern Exchange 2000 Server.

First, you'll want to pass incoming e-mail through a good content scanning tool. These tools look for code types that virus scanners don't. For instance, a good content scanning tool will block VB script, macros, Windows Scripting scripts, Java Scripts, executables and HTML scripts. Now, you might be thinking that Outlook does this already. But why depend on the client to perform this function and *why allow potentially malicious code into your network in the first place?*

The reason that you pass your e-mail through a content scanner first is because content scanners can catch new viruses. Virus scanners are rarely updated in time to catch the latest virus and they do not protect the body of the e-mail, which is where malicious HTML code can reside. Think back to the LoveLetter virus or the Code Red worm. These attacks spread world-wide in a matter of hours. There is really no practical way that any anti-virus company can respond faster than a few hours to a new virus or worm. Content scanning is *pro-active* in that it can be configured to clean all e-mail of all known script types before they enter your network. This affords you an excellent chance to ensure that your e-mail is cleaned of all malicious code even before it is send to the virus scanner, whether that code is brand new or years old. And because a content scanner is looking for content type, not simply a signature or pattern, it can catch the newest of new viruses even before your anti-virus company has a chance to push out an updated virus definition.

Secondly, you'll want to pass your e-mail through a virus scanner to ensure that all known viruses are cleaned out. Not passing your e-mail through an updated anti-virus server after running it through a scanner is unwise because some older viruses may not be caught by the content scanner. So, after scanning the e-mail content, be sure to let your anti-virus server have a shot at finding and disabling any viruses in attachments that it might find.

Thirdly, the e-mail is then sent to another Exchange 2000 Server that will encrypt it and digitally sign it before sending the mail to the internal Exchange 2000 Server. This provides you with several types of protections. First, the IP address of the internal Exchange 2000 server does not need to be published in the public DNS records. This means that an attacker attempting to telnet into your server will never be able to reach it directly. Secondly, if you configure the internal Exchange 2000 Server to accept e-mail only from the encrypting Exchange server over a port number above 1024, then any attempts to make port 25 connections to the internal Exchange server from any other IP address will be rejected.

Now, you might be thinking that you could spoof the IP address easily enough. And that would be true, except that the internal Exchange 2000 Server is also looking for a digital certificate (whose trusted certificate authority is an internal Windows 2000

Certificate Server) before it will accept the connection. So you'll not only need to spoof the IP address, but you'll need a valid certificate from the internal Certificate server as well to make such a connection. Obtaining such a certificate will be difficult, if the personnel are well-trained in network security. Social engineering is the route to take here if you want to get a certificate from the internal certificate authority. But even if the hacker could obtain a certificate and spoof the IP address, the hacker would need to traverse the outside firewall and then traverse the second firewall to get direct access to your internal Exchange 2000 Server. While not impossible, this may present enough headaches for the hacker they he'll go trotting off to another SMTP server that is easier to hack for his purposes.

Notice also that even if a hacker decides to bring down your perimeter Exchange servers, you've really lost nothing of value, other than your time to get the servers functioning again. Your company might lose some money due to the inability to communicate via e-mail, but they haven't lost any current data. This is important. While it is bad enough to lose internet e-mail capabilities, it is much worse to lose that *and* your data. The server that hosts your data is the one most protected. And the ones most exposed – as suggested in this paper – hosts no important data. If those servers are lost, at least all the business-critical data is saved on the internal Exchange 2000 Server. For many companies, this is an acceptable level of risk to assume.

You might also be thinking that you don't have three servers to dedicate to these functions. Don't despair. The content and virus scanning can be combined on one server through the user of port numbers. For instance, you can have the content scanning tool listening for incoming traffic on port 25. Then configure it to send e-mail to the server's local address, but on some port number above 1024, say 40,000. Have the anti-virus scanner listening on port 40,000 and then have it forward e-mail to the encryption server for passage to the internal Exchange 2000 Server. This approach allows for layered security while lower your hardware investments. For many companies, this is a preferred solution.

Finally, a word about the SMTP service in IIS that installs by default with every Windows 2000 Server. Best practice is to not install SMTP on any server unless it is required. Even though there may not be an MX (Mail Exchange) record in the public DNS tables for your Windows 2000 Server, port scanners will reveal that these servers are running SMTP and that they are accepting SMTP connections. Hackers can use these servers as additional entry-points for sending e-mail attacks into your organization. Ensure that the SMTP server on all your Windows 2000 Servers is either set to Manual for startup or is not installed at all.

Outlook Web Access

Outlook Web Access is a very popular feature of Exchange 2000 Server. Microsoft has a way of making a feature-rich platform that is attractive and compelling to those who decide which software to use. The problem with Outlook Web Access (OWA) is that our scenarios described above won't work because OWA uses HTTP traffic, not SMTP. But there are some things you can do to secure OWA. Fortunately, those who

use OWA are going to be your own users, so there is a much less chance of them introducing a virus into your e-mail system by sending their own e-mail through OWA.

Because OWA requires IIS, the problems that affect OWA which result from the vulnerabilities in IIS can be reduced by performing the following steps[10]:

- Install IIS on a different partition than the root c:\ partition. Some worms and/or viruses search for default installs on the c:\ partition
- Install OWA on it's own server between the two firewalls (refer back to figure 2)
- Remove any unnecessary web sites, including the IISHelp, IISAdmin and the IISSamples sites.
- Do not allow remote administration of the OWA server
- Do not install Index Server, Internet Services Manager and Front Page Extensions
- Disable unnecessary script mappings. OWA requires the .asp and .htr scripts to run. All the others, including .idc, .stm, .shtml, .printer, .htw, .ida and .idq can be disabled. And if you don't want users changing their passwords in OWA, then you can disable the .htr file extension too.
- Implement protocol logging and monitor the logs
- Use SSL between the client and the OWA server
- Ensure you have the most up-to-date virus definitions installed on each Exchange 2000 Server and Internet Information Server
- Use the new IIS Lockdown Tool to further lockdown IIS. Note that if you lock this down too far, you may remove some dynamic functionality in OWA, so test your configurations before deploying locked down IIS servers in your environment.

IIS has received some bad press recently. Gartner analyst John Pescatore's article *Nimda Worm Shows you Can't Always Patch Fast Enough*[11] offers the simplistic answer that enterprises should move away from Microsoft's IIS platform in favor of another platform. The problem with this approach is that it is difficult for many companies to simply throw out IIS and still expect their other investments in Microsoft products to perform at the level they need. IIS is really here to stay. The .NET world with have more and more applications that depend on IIS for their functionality because more and more, they will have internet capabilities written into the core of their code[12].

Even if removing IIS were possible, you would still need a replacement platform that offers the same services as IIS to allow Exchange 2000 Server to continue to operate as it does today. Without these services, Exchange 2000 is really a small messaging program that lacks the whistles and bells which form the compelling reason to purchase the product in the first place. So, instead of trying to bash or remove IIS, we need to focus on securing it as best we can, realizing all the while that new vulnerabilities will be discovered and new patches will need to be installed.

So, after you have secured your OWA server, you are ready to allow users access to their e-mail over the internet. Again, it is important to note that OWA, while external,

can be rightly thought of being on the *client* end of your e-mail system. When a user reads their e-mail using OWA, that mail will have passed through the three scanning servers before being deposited into the user's mailbox. If they send e-mail using OWA, then the mail did not originate from the "outside" as internet mail does. While communications over OWA are still through IIS and port 80 and thus not totally secure, these distinctions are important to keep in mind.

Scanning Outbound E-mail

When mail is sent out of your organization, you should have it routed back through the virus and content scanning servers. Even though the system outlined in this paper for incoming e-mails is tight, it is not fool-proof. At some point, HTML code or a virus might sneak through. Since most viruses propagate themselves using the local address book, it is highly possible that outbound mail will be generated sending a virus back out. To ensure that your organization isn't black listed and to help prevent the virus from spreading, you should scan your outbound e-mail as well.

By installing a comprehensive e-mail solution that includes content checking and anti-virus scanning, companies can protect themselves against the potential damage and lost work time that future viruses may cause.

More Information

If you want more information on how to stay current with updates to Microsoft products, be sure to visit their security web site at http://www.microsoft.com/security. At this web site, you can subscribe to receive e-mails about their latest security patches and updates. Also, be sure to visit regularly their public newsgroup, Microsoft.public.security at news.microsoft.com. There is no username or password to access this newsgroup, but you will need port 119 open for outbound traffic on your firewall.

---

[1] *Secrets and Lies: Digital Security in a Networked World*. Bruce Schneider, Wiley. Be sure to read the Preface to this book, as Bruce lays out this argument rather well.

[2] http://www.dshield.org/topports.html

[3] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-088.asp

[4] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-014.asp

[5] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-030.asp

[6] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-049.asp

[7] http://www.peapod.co.uk/seminars/journey/sectech.ppt

[8] http://www.gfi.com/me/wpcontentchecking.htm

[9] This is not intended to be an exhaustive list of exploits that could be run over port 25, but rather a representative sample of the types of exploits that are available.

[10] http://rr.sans.org/e-mail/corp_e-mail.php

[11] FT-14-5524, September 19, 2001

[12] http://www.exchangeadmin.com/articles/print.cfm?articleID=22955