Global Information Assurance Certification Paper

SANS/GIAC Practical Assignment
For GSEC Certification
Version 1.4c
Option 2

OUTLOOK WEB ACCESS 2000 SECURITY

BY
TIM M. ALLISON

SUBMITTED OCTOBER 20, 2004

Table of Contents

Abstract

Every corporation today has the need to utilize email to conduct business. The MC consulting firm is no exception. Microsoft Exchange was chosen as the email system for MC consulting because it is a full-featured email solution providing the benefit of email, group calendaring, contact management, and other useful communication and collaboration tools.

MC utilized many of the features of Microsoft Exchange including the Windows-based Outlook client as well as the web-based Outlook Web Access. Because of the mobile nature of the corporation's users, most access to email was via the Internet. As useful as Microsoft Exchange was to the MC consulting firm, it was not, in its initial configuration, a secure solution. Unapproved access, denial-of-service risks, and data security vulnerabilities were all real issues that needed to be addressed to secure the Microsoft Exchange installation.

Before

Description of the MC Consulting Firm

The MC consulting firm is a small group of computer consultants with the goal to provide excellent service to the firm's clients. MC exists to service the technology needs of enterprise clients, as well as small-medium businesses. Much of the work performed by the MC consultants was at the client site or from other remote locations; very little of the consultants time was spent in the main MC office.

MC Business Practices

In order for the MC consultants to maintain contact when they were at different sites, the consultants utilized email as the communication method of choice. In order to effectively provide MC's clients with the high-quality service that the clients have come to expect, email is more than just simple communication, it becomes a collaboration tool.

The MC consultants require email to support the following business processes:

- The exchange of ideas, new technologies, best practices, etc.
- Issuance of project status reports
- Requests for technical assistance from clients and coworkers
- Submission of proposals to clients
- Invoicing of current projects
- Record keeping of project information in the MC project website
- Group calendaring

- Resource reservations (conference rooms, projectors, etc.)

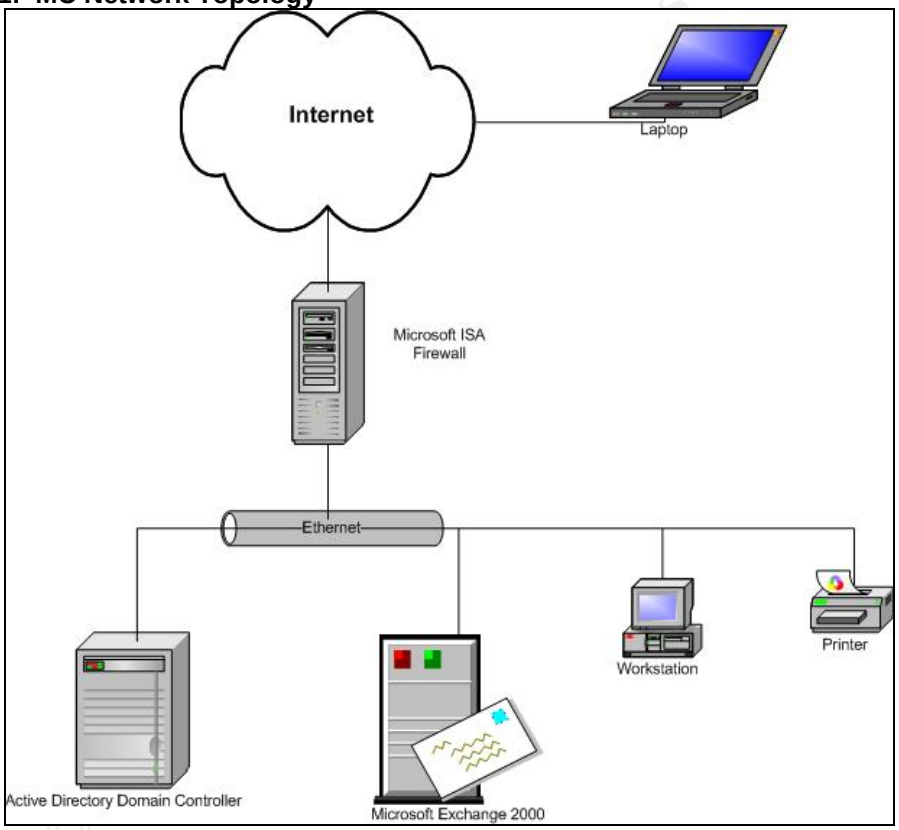
The MC Network

The MC network consisted of the following network components:

- Microsoft Active Directory based on Windows 2000
- Exchange 2000
- Microsoft Internet Security and Acceleration (ISA) Server 2000 firewall
- Various other servers providing services required for day-to-day operations and management

The MC network topology (simplified) is shown below in Figure 1:

Figure 1: MC Network Topology



Microsoft Active Directory Implementation

The Microsoft Active Directory was an upgraded Windows NT 4.0 domain. Active Directory was required for the installation of Exchange 2000 and its ongoing operation. In a Windows NT 4.0 domain environment, Exchange 5.5 can be utilized, but not integrated. Active Directory integrates the domain and Exchange 2000 user and group management.

User IDs, security groups, user mailboxes, and email distribution groups are all located in Active Directory. Therefore, any objects that are used by Exchange 2000 are also located in Active Directory. The centralized management is a change from the previous Windows NT 4.0 domain and Exchange 5.5 environment.

In the previous model, users were created in the Windows NT 4.0 domain to be used for authentication. Within Exchange 5.5 a second step was required to create a mailbox and possibly assign the mailbox to an email distribution group. Deleting a userID or mailbox did not mean the associated userID or mailbox would also be deleted. Keeping these two separate user/group systems synchronized was time consuming and error prone. Exchange 2000 integrates with Active Directory and uses the same user IDs and groups that are used for authentication for email purposes.

Because of this integration between Active Directory and Exchange, passwords and password requirements are enforced by Active Directory. These requirements include password minimum length, maximum length, maximum age, and complexity requirements (the requirement to utilize three of the four following characters in the password: a-z, A-Z, 0-9, special characters: !@#$%^&*) and are stored as a group policy object in the Default Domain Policy.

The password settings were migrated from the Windows NT 4.0 account policy and were set as:

Requirement	MC Consulting Setting
minimum length	5
maximum length	Not enforced
maximum age	90 days
complexity requirements	Not enforced

Exchange 2000 Implementation

The upgrade to Exchange 2000 required that the upgrade to Active Directory occur first. After upgrading to Active Directory, the Microsoft Active Directory Connector was installed to synchronize the Exchange 5.5 mailboxes and distribution groups with Active Directory. Exchange 5.5 could then be upgraded to Exchange 2000.

In preparation for the Exchange installation, a default installation of Windows 2000 as the host operating system was installed on new server hardware. Microsoft Exchange 2000 requires the installation of Internet Information Server, to host the Outlook Web Access service, the Microsoft Simple Mail Transport Protocol (SMTP) service, the Microsoft Network News Transport Protocol

(NNTP) services, and to send and receive email. Included was the installation of Windows 2000 Service Pack 2, which was the current service pack at the time of the installation. This server was then joined to Active Directory.

Microsoft Exchange 2000 was installed using the default settings. Very little customization was completed other than to provide for a functioning email system. The user accounts were then mail enabled by using the Active Directory Users & Computers console.

Outlook Web Access, the browser-based email client, was installed by default when Exchange 2000 was installed. The server hosting Outlook Web Access required access to and from the Internet. Using the corporate firewall, the Outlook Web Access web site was published to the Internet for users to access the web based email utility. The configuration required to allow this access is described below in the Microsoft ISA section.

The default authentication used by Outlook Web Access is to utilize Windows Integrated authentication. This default setting will request the end-user to enter credentials to access the Outlook Web Access web site. These credentials are in the form *NTDOMAIN\Userid.* Most versions of Internet Explorer running on Windows 2000 Professional or Windows XP Professional will utilize this form of authentication. Non-Microsoft browsers do not support the Windows Integrated authentication[1], therefore, the Outlook Web Access web site was changed to "Basic Authentication," or clear text, to allow access to the Outlook Web Access web site. This was thought to be a secure installation since the Microsoft ISA firewall was protecting the web site.

The Outlook Clients

The choice to utilize Microsoft Exchange as the collaboration tool also meant that several choices existed when connecting to the server. The most popular client-side email applications for connecting to Exchange were Outlook Express, Outlook Web Access and/or the full Microsoft Outlook client.

Outlook Express is a free product that is installed as part of Internet Explorer on most versions of Microsoft Windows. However, the limited feature set of Outlook Express kept it from being the choice for an email client for the MC consultants.

Outlook Web Access is the web based tool that is provided free-of-charge as part of the Microsoft Exchange 2000 server product. Exchange 2000 information can be accessed from any workstation that has either Internet Explorer or Netscape

---

[1] Microsoft Corporation. "STS: Must Enable Basic Authentication for Browsers Running on Macintosh OS." Version 2.0. 15 November 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;288354 (10 June 2004).

Navigator installed and has access to the Exchange sever either via the Internet or the Local Area Network. It is a fairly robust client, but does not provide all the functionality of the full Outlook client. It is a good alternative for those instances when the full Outlook client can not be used.

The Microsoft Outlook 2000 client is a full-featured, client-side application that provides the maximum features of all of the email clients. This client was chosen as the primary choice for the MC Consultants for the following reasons:

- Email, calendar, tasks, contacts and Public Folder information could be accessed and managed.
- Outlook data could be "cached" for off-line access when not connected to the Exchange server.
- A change made to email information was synchronized back to the Exchange server.
- Group scheduling was made easier with free-busy searching.
- An extensible spell checker was included.

Choosing the full Outlook client required the installation and configuration of Outlook on all end-user workstations to connect to the Exchange server. The use of the full-featured client also meant more work to keep it secure.

The Outlook client required the use of the RPC protocol, TCP/IP port 135, to establish a connection to the Exchange server and Active Directory. This is not an issue when the workstation having Outlook installed is directly connected to the same Local Area Network as the Exchange server. However, when connecting over the Internet, a more substantial and secure connection[2] is required. The RPC protocol, according to a 2001 vulnerability report published by Cisco Systems, is "The most vulnerable Internet service, ranked by the percentage of times that the service was visible and found to have a security problem."[3]

To accomplish the goal of allowing the Outlook client to connect to the Exchange server, the Microsoft ISA firewall was configured to pass secure RPC traffic.

---

[2]Sakellariadis, Spyros. "Protecting Windows RPC Traffic." 29 August 2002. URL: http://www.microsoft.com/technet/prodtechnol/isa/2000/maintain/rpcwisa.mspx (12 May 2004).

[3] Cisco Systems, Inc. "What are the Most Dangerous Internet Services?" 2001. URL: http://www.cisco.com/warp/public/146/news_cisco/ekits/vulnerability_report.pdf (6 October 2004)

Microsoft ISA Server Implementation

Microsoft ISA Server 2000 is the Microsoft firewall that provides security to networks by allowing customized access via users, groups, and protocols. ISA includes the capability to securely provide Exchange RPC communications to Internet connected Outlook clients.

When first installed, Microsoft ISA server will not allow any traffic to pass in or out of the network. Several areas must first be configured to allow Internet traffic to flow. The MC Consulting ISA server was configured to allow Internet access from the workstations, and servers were published to allow access from the Internet.

Figure 2 shows how the ISA Server was configured to allow Internet access from the LAN:

Figure 2: ISA Server Configuration – LAN to Internet

Site and Content Rule (Access Policy)

Site and content rules allow the restriction of valid destinations. The MC consultants were not being restricted to any Internet resources. This rule allows access to any and all Internet destinations, present and future.

Settings

Name	Allow Internet Access
Destinations	All Destinations
Schedule	Always
Action	Allowed
Applies to	Any Request
HTTP Content	All Content Groups

Protocol Rules (Access Policy)

Protocol rules allow the configuration of which protocols can and cannot be used, by whom, and when. The MC consultants were not being restricted from any Internet resources. This rule opened up the access to all protocols defined on the ISA server, not all IP protocols.

Settings

Name	Internet Browsing
Action	Allow
Protocol	All IP Traffic
Schedule	Always
Applies to	MC Workstations (a client address set)

Client Address Set (Policy Elements)
Client Address Sets allow the creation of a group of computers to be treated as a single unit. This set was created to only allow Internet browsing access for the workstations in the MC office.

Settings

Name	MC Workstations
Addresses	172.16.1.50-172.16.1.254

The following settings allowed the MC servers to be accessed from the Internet:

Web Publishing Rules (Publishing)
Web publishing allows a web server to be accessed from the Internet through the ISA server. This special type of server publishing includes the ability to restrict access to portions of the web site.

Figure 3: Web Publishing Rules

Name:	Outlook Web Access
Destinations:	Selected Destination Set: OWA (see below)
Action:	Redirect the request: email.mcconsulting.com
	Send the original host header
Bridging:	Redirect HTTP: HTTP
	Redirect HTTPS: HTTPS
	Do not Require SSL
	No certificate configured
Applies to:	Any request
Link Translation:	Not configured or required

Destination Set:
A destination set will define what paths of a web site are valid to be accessed from the Internet. In this case, the OWA destination set is being setup to provide access to the root and all items contained in the root. In other words, this allows access to the entire web site with no restrictions.

Figure 4: Destination Set
Name: OWA

Name/IP Range:	Path
email.mcconsulting.com/*	(allow access to all paths)

Server Publishing Rules (Publishing)
Server publishing rules differ slightly from web publishing in that they do not allow restrictions to portions of the server. In this case, the server is fully available on the specified port.

Figure 5: Server Publishing Rules

Name:	Outlook via RPC
Action:	IP of internal Server: 172.31.0.10 External IP address: x.x.x.x Mapped server protocol: Exchange RPC Server
Applies to:	Any Request

This ISA / Exchange combination worked until the release of the Blaster Virus. The Blaster Virus was a worm that exploited the RPC vulnerability (first described in Microsoft Security Bulletin MS03-026)[4]:

> "W32.Blaster.Worm is a worm that exploits the DCOM RPC vulnerability (first described in Microsoft Security Bulletin MS03-026)(users are recommended to patch this vulnerability by applying Microsoft Security Bulletin MS03-039) using TCP port 135. The worm targets only Windows 2000 and Windows XP machines. While Windows NT and Windows 2003 Server machines are vulnerable to the aforementioned exploit (if not properly patched), the worm is not coded to replicate to those systems. This worm attempts to download the msblast.exe file to the %WinDir%\system32 directory and then execute it. W32.Blaster.Worm does not have a mass-mailing functionality."

As a result of the Blaster worm, the RPC protocol was widely restricted at both the Internet service Provider (ISP) level and at the client locations where the MC consultants were working. The Outlook client functionality was limited to operate in an "offline mode" only, rendering it useless as a real-time collaboration tool.

One solution to this problem was to provide the MC consultants with a Virtual Private Network (VPN) to access the MC network and therefore the Exchange server. A VPN would allow the remote workstation to connect to the MC Local Area Network as if the workstation was directly connected. This solution failed for the very same reason as the full Outlook client: VPN access from the client sites was also restricted by the clients' firewall.

If the consultant required access to the Exchange information when they were not in the office, then Outlook Web Access was the only choice. Since most of the MC consultants were working at client sites, they could utilize the client's Internet connection to use Outlook Web Access. Outlook Web Access utilized the HTTP and HTTPS protocols to operate properly and most client firewalls allowed this traffic to pass.

During

Attacks on OWA and Exchange

[4]Knowles, Douglas; Perriot, Frederic and Szor, Peter, "Symantec Security Response." 26 February 2004. URL: http://www.sarc.com/avcenter/venc/data/w32.blaster.worm.html (30 July 2004).

The MC consultants made use of the Exchange email server via Outlook Web Access from the various client sites where they were located. Outlook Web Access was working as intended and allowed the MC consultants to successfully collaborate from the various remote sites.

While this configuration proved to be useful to the MC consultants, several issues arose from the default installation of Windows 2000 Server, Internet Information Server, Exchange 2000 and Outlook Web Access on the MC email server.

Outlook Web Access Web Site Was Defaced

The first of these issues became apparent when the Outlook Web Access web site was defaced. The Outlook Web Access web site operated properly for a period of time until one morning it was discovered that the site no longer showed the familiar logon prompt, but rather an offensive web site. Once this was detected, a call was placed to the Exchange administrator.

The Exchange administrator immediately unplugged the network cable connecting the compromised server to the MC network to isolate the server from the network. While this was an important step, the fact that the defacement had happened sometime during the night probably meant that this server, if it was intended to do so, had already infected the rest of the network servers.

The Exchange server's antivirus signature files were updated via a diskette and the server was scanned. The antivirus scan did not find any known viruses. The virus scan process was repeated on all the servers on the network to insure that they did not contain any viruses.

Research on the Internet into what the possible cause was, produced the obvious culprit: Outlook Web Access relies on the host operating system's Internet Information Server. In its default installation state, Internet Information Services (IIS) is not secure[5]. The IIS install on the Exchange server had not been secured when the server was implemented, leaving it dangerously vulnerable to attacks.

The next task was to return the server to a properly configured state. This meant the web site, and possibly the Microsoft Windows operating system files, needed to be restored. The backup and restore process was designed to provide coverage for this type of incident. The Exchange server was imaged using a 3rd party disk imaging tool. Because the Exchange databases could be very large, they were kept on a separate disk volume and not backed up as part of the disk image. This meant that the server could be restored quickly by simply recovering

[5] SANS Institute. "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." Version 4.0. 8 October 2003. URL: http://www.sans.org/top20/ (12 June 2004).

the server from the disk image. This would not only restore the web site files, but also the server's operating system files. However, it also meant that the server's vulnerabilities would be restored. The vulnerabilities would still need to be addressed or this incident would happen again. The greatest risk was the unsecured Internet Information Services 5.0 (IIS).

The Microsoft technical article "IIS lockdown and URLscan configurations in an Exchange environment" describes the use of free security tools from Microsoft called IISLOCKD and URLscan[6] that can be used to secure Microsoft Internet Information Services 5.0. The Internet Information Services Lockdown tool can be used to secure the IIS default installation from known vulnerabilities.

Special care was required when using these tools since they were being installed in a Microsoft Exchange environment. Installing IISLOCKD onto an IIS server that hosts Outlook Web Access (OWA) would disable some of the functionality. These include, but are not limited to:

- Items may be missing when accessing OWA
- A "Runtime Error" will be displayed if OWA is accessed from the Exchange server
- In Exchange System Manager, administrators may be unable to expand the public folder tree

The default install of IISLOCKD will also break some of the Outlook Web Access functionality if not configured properly. Examples of some of the lost functionality are:

- The Logoff button will not function
- Multimedia functionality will cease to operate

When the IISLOCKD application was run, the following steps were taken to secure the Windows 2000 Internet Information Services that hosted the Outlook Web Access site on the Microsoft Exchange server:

- MC Consultants ran the IISLOCKD utility on the Internet Information Services web server. When the **Remove Script Mappings** dialog box was displayed, the following selections were chosen:
    - Deselected the **Disable support for Active Server Pages (.asp)** checkbox to allow the Outlook Web Access "Multimedia" and "Logoff" buttons to continue to function. This option was set initially to stop the use of ASP pages on a web site. Since Outlook Web Access utilizes ASP pages for it's functionality, it is necessary to allow support for ASP pages.

[6] Microsoft Corporation. "IIS lockdown and URLscan configurations in an Exchange environment." Version 5.0. 11 June 2004. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;309508&sd=tech (14 May 2004).

- Under the **Additional Lockdown Actions** dialog box the following were cleared:
    - Disable Distributed Authoring and Versioning (WebDAV)
    - Set file permissions to prevent the Internet Information Services anonymous users from writing to content directories

The URLScan tool keeps IIS secure by allowing only certain URL formats into the server it is protecting, therefore reducing the possible attacks. This reduces the attack surface of the web site, reducing the possibility of an improperly formatted URL exploiting an unknown vulnerability. If a corporate firewall cannot restrict the access to the web site, then the URLSCAN tool is a solid tool to accomplish this task. URLSCAN was not installed because it was decided to use the Microsoft ISA firewall to restrict access to the Outlook Web Access installation.

The Microsoft ISA firewall was changed to restrict access to only allow valid URL combinations for the Outlook Web Access web site. This was accomplished by modifying the "Destination Set" configuration for the published Outlook Web Access web site. Figure 6 shows the new Destination Set configuration:

Figure 6: New Destination Set Configuration

Name: OWA

Name/IP Range:	Path
email.mcconsulting.com	/exchange/*
email.mcconsulting.com	/public/*
email.mcconsulting.com	/exchweb/*

Finally the Windows operating system was patched with the latest patches and hot fixes published on the Microsoft Windows Update web site. In addition, the Exchange installation was patched with the latest patches available from the Microsoft Exchange web site.

Once these steps had been completed the server was again scanned with the antivirus application to insure the server remained "clean" of viruses. The server was then reintegrated into the MC Consulting network and tested for full functionality.

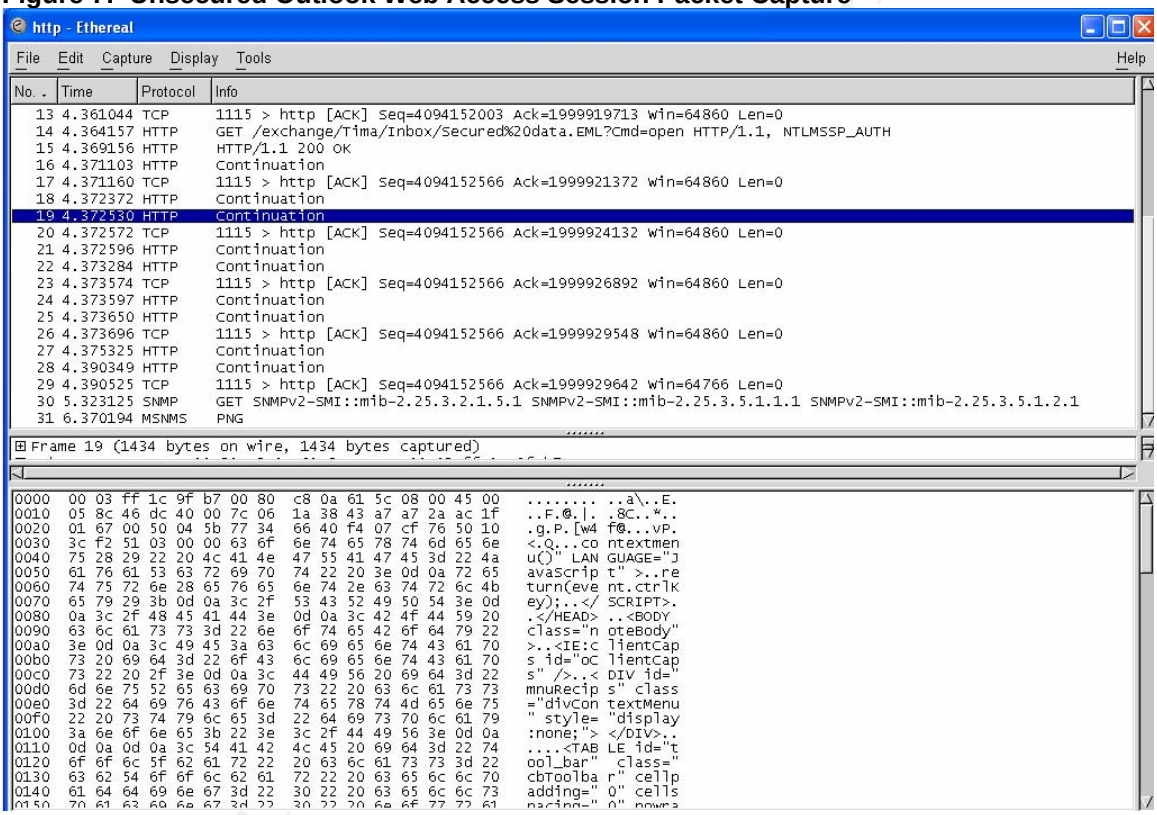
Unencrypted data was being sent across the Internet

A second vulnerability concerning an unreported issue surfaced. Several articles and reports were posted at the time providing evidence that there was a lack of data security in the default installation of Outlook Web Access. These reports were not focused on the idea that the default installation of the Windows operating system and IIS were vulnerable, rather that the lack of encryption on the web site used for Outlook Web Access should be cause for concern.

As data was being accessed via Outlook Web Access the information was being sent between the client and server in a non-encrypted form, or clear-text. Anyone that wanted to intercept the data transmission between the client and the server could very easily read the contents of the data being sent. This technique is called sniffing[7].

Using Ethereal, an inexpensive "sniffer," the theory was tested and determined to be true: The data traffic being sent between client and server when using Outlook Web Access was, in fact, in human readable form. Figure 7 shows a packet capture of an unsecured Outlook Web Access session:

Figure 7: Unsecured Outlook Web Access Session Packet Capture



Research into this issue revealed the Microsoft technical article "XCCC: Turning On SSL for Exchange 2000 Server Outlook Web Access" with the details necessary to secure the Outlook Web Access web site using a digital certificate[8]. The process seemed simple except for one key element: Obtaining a digital

[7] Juniper Networks. "ISP Glossary." 26 August 2004. URL: http://isp.webopedia.com/TERM/s/sniffer.html (31 August 2004)

[8] Microsoft Corporation. "XCCC: Turning On SSL for Exchange 2000 Server Outlook Web Access." Version 3.1. 14 July 2004. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;320291 13 May 2004.

certificate. The Microsoft article did not give information regarding obtaining a digital certificate for use on the Outlook Web Access web site.

The choice to "purchase a certificate from a number of third-party certification authorities" or "use Microsoft Certificate Server to install your own certification authorities" was not clear. There were several pros and cons to each choice as presented in Figure 8:

Figure 8: Third Party Certificate Authority vs. In House Certificate Authority Table

Certificate Provider	Pro	Con
Third-party certificate (VeriSign, Thwate, Equifax, etc,)	Trusted by default by most browsers including Internet Explorer. The third party certificate provider provides the necessary operations to insure that the public key infrastructure (PKI) is secured, backed up and recovered as needed.	Required a periodic purchase of a certificate from provider to maintain the certificate expiration.
Microsoft Certificate Server (home grown)	Did not require the periodic purchase of certificate since the certificate is generated on a corporate server.	Will not be automatically trusted by browsers and will require an installation technique on each workstation that will access the protected site. Requires an operations procedure to secure, backup and recover the "home grown" public key infrastructure (PKI).

The MC firm chose to use a third-party digital certificate from the VeriSign, Inc. provider since it was a well-known name in the industry. Since the VeriSign root server certificate was already trusted by the MC consultants' browsers, no workstation configuration was required to implement the solution.

While the process to secure the site was straight forward and well documented, the purchase of the certificate from VeriSign Inc. required more work to identify the correct certificate to purchase. Each provider most likely will have their own uniqueness when obtaining a certificate. In any case, the following order of events must be followed:

- Create a "Certificate Request" file
- Purchase the certificate using the "Certificate Request" file
- Install the certificate into the IIS web site

To order the digital certificate, several steps were required:

1. From the IIS Manager on the server hosting Outlook Web Access

    a. selected the web site hosting Outlook Web Access
    b. right-clicked the web site
    c. clicked Properties
2. Selected the Directory Security tab
3. Clicked Server Certificate to begin the new certificate request
4. The Certificate Wizard started
    a. Selected Create a New Certificate and clicked Next
    b. Selected Prepare a New Request but Send it Later and clicked Next
    c. Entered a Friendly Name for the web site.
    d. Entered the bit length of the key of 1024 and clicked Next
    e. Entered the appropriate Organization (O), Organizational Unit (OU) and clicked Next
    f. Entered the common name of the web site (email.mcconsulting.com), then clicked Next
    g. Entered the Country/Region, City, and State, then clicked Next
    h. Entered the contact information responsible person and clicked Next
    i. Entered a name for the certificate request file and clicked Next
    j. Clicked Next on the summary screen.
5. Via the VeriSign web site, the SSL certificate was purchased by following the Secure Site Services link and entering the appropriate information. At one point, the information contained in the certificate request file created above was required to be pasted into the registration web page.
6. Later, a verification email was sent and eventually the certificate itself was sent via email.

The following steps were required to complete the process of installing the digital certificate to the IIS web server:

1. From the IIS Manager on the server hosting Outlook Web Access
    a. Selected the web site hosting Outlook Web Access
    b. Right-clicked the web site
    c. Clicked Properties
2. Selected the Directory Security tab
3. Clicked Process the pending request and install the certificate
4. Clicked the file that was sent from VeriSign and then clicked Next

5. Checked the values to make sure they were correct, clicked Next, then clicked Finish

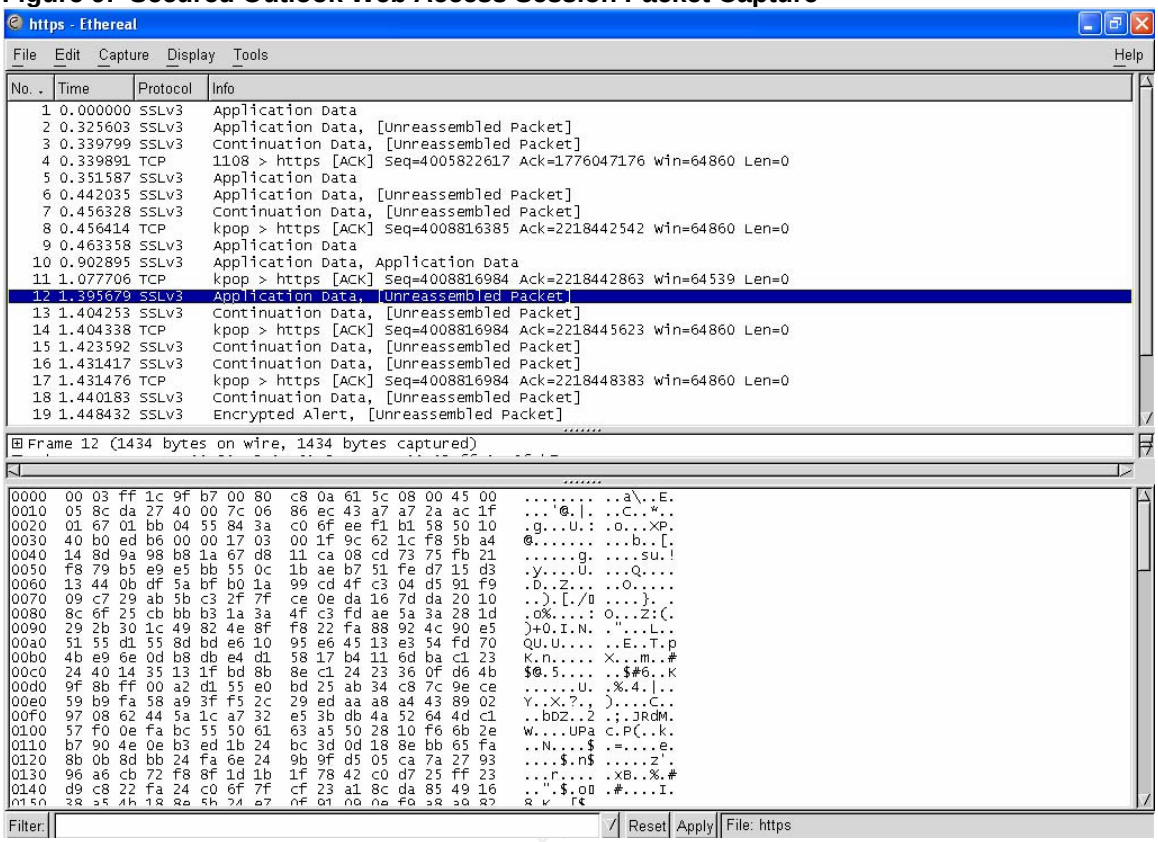
The final step was to require the use of SSL on the Outlook Web Access web site. The steps outlined in the Microsoft technical article "XCCC: Turning On SSL for Exchange 2000 Server Outlook Web Access" explained how:

> If you want to enforce the use of SSL, you can require secure channel communication on each Exchange 2000 virtual root:
>
> a. In the Internet Information Server MMC snap-in, click the Exchange 2000 virtual root that you want to secure (for example, click Exchange or Public)
> b. Right-click the virtual root and then click Properties
> c. Click the Directory Security tab
> d. Under Secure communications, click Edit
> e. Click to select the Require secure channel (SSL) check box

This configuration required the use of a different URL for the MC consultants to use when accessing the Outlook Web Access web site. Instead of using http://email.mcconsulting.com they would use https://email.mcconsulting.com. If the non-secure (HTTP) URL was used, IIS would respond with a page indicating the secure (HTTPS) version of the URL is required.

A repeat of the "sniffer" process verified that the Outlook Web Access web site, secured with a digital certificate, encrypted the data and made it unreadable in the packet capture. Figure 9 shows a packet capture of a secured Outlook Web Access session:

Figure 9: Secured Outlook Web Access Session Packet Capture



Unauthorized access to mailboxes.

Lastly, Outlook Web Access requires authentication to access a mailbox. One of the MC consultants began to see strange emails apparently being sent from her mailbox that she did not send. The consultant also found many messages in her "Sent Items" that were not valid. There were also replies to messages that had not apparently been sent. Somehow the access to this consultant's Outlook Web Access mailbox had been compromised.

It was obvious that the consultant's userID and password had been obtained, either through "sniffing" the previously unprotected Outlook Web Access web site or via the AutoComplete setting in Internet Explorer on a client's workstation.

A review of the suspect Exchange mailbox did show the use of the mailbox during non-working and non-waking hours: 2am-4am. Evidence was found that the web site had been accessed "normally" indicating a correct authentication sequence. This was seen by a review of the Exchange server "Event Log" which recorded each logon attempt by IIS.

The MC consultant's user account was set to "User must change password at next logon" via Active Directory Users & Computers console. The consultant was then instructed to logon and change her password. This change was successful

in stopping the "borrowed email" account abuse. However, this change was not permanent and the "borrowing" could happen again. A more secure method of protecting the authentication credentials was needed.

The default installation of Outlook Web Access configures the authentication for the web site to "Anonymous" and "Windows Integrated" authentication. This was changed at the time of the Exchange server implementation to only use "Basic" authentication. This allowed access from non-Microsoft clients that do not support Windows Integrated authentication[9]. Basic Authentication does not encrypt the userID and password during the transmission. For this reason Basic authentication is also called "clear-text." The userID and password information can then be "sniffed" and saved for later use.

The option to utilize the more secure "Windows Integrated" authentication was not available since the non-Microsoft clients still existed and needed to be supported. The other available option was to secure the Outlook Web Access web site with a digital certificate, which was also the proposed solution to correct the unencrypted data issue.

The use of a digital certificate not only secured the email messages being sent over the Internet, but it also encrypted the "clear-text" userID passwords used during the authentication to the Exchange server. The use of a digital certificate with Basic Authentication is a secure method for accessing Outlook Web Access[10].

The remaining issue was the possibility of the Internet Explorer AutoComplete functionality allowing unauthorized access into an email mailbox. The AutoComplete functionality in Internet Explorer will maintain a userID and password for web sites that have been visited[11]. This means that Internet Explorer has the ability to retain or "cache" information on the workstation in use, including userID and passwords, which are used when accessing web sites. This functionality is also available when accessing Outlook Web Access. This made it possible for an MC consultant to save his or her OWA username and password on an MC Consulting client's workstation (or any public kiosk type

---

[9] Microsoft Corporation. "STS: Must Enable Basic Authentication for Browsers Running on Macintosh OS." Version 2.0. 15 November 2003. URL:
http://support.microsoft.com/default.aspx?scid=kb;EN-US;288354 (10 June 2004).

[10] George, Christopher. "Outlook Web Access for Exchange 2000." InstantDoc #22969. December 2001. URL: http://www.winnetmag.com/Articles/Print.cfm?ArticleID=22969 (May 28 2004).

[11] Granneman, Scott. **"Securing Privacy Part Four: Internet Issues."** 29 May 2002. URL:http://www.securityfocus.com/infocus/1585 31 August 2004.

workstation) that was used when using the MC Consulting Outlook Web Access web site.

Since these types of workstations are not connected to the MC Consulting network, Active Directory group policies could not be utilized to control the Internet Explorer setting. It was left up to the MC consultant to exercise care when using non-MC workstations. The consultants were instructed not to select the "remember password" option when logging in.

In addition, a new log review policy was put in place. The event logs on the Exchange server are now reviewed daily to determine if after hours logons are being recorded. If new events are found, this may indicate another unauthorized access attempt.

It was also decided to modify the password policy implemented via the Default Domain Policy in Active Directory to following settings:

Requirement	MC Consulting Setting
minimum length	7
maximum length	Not enforced
maximum age	45 days
complexity requirements	Enforced

These changes would require the MC Consultants to have more complex passwords that are harder to guess and to change their password more frequently. Should a password become compromised, it would not be valid for more than 45 days.

Because the minimum length of the password was also changed, the chances that an attacker could brute force, or guess, the passwords using a password "cracking" program was further decreased.

Finally, the password complexity requirements were set to be enforced, causing the passwords to utilize more "unique" characters and therefore reduce the likelihood that they would be "cracked" or guessed. Enabling complexity requires that a password include three of the four following character types in the password: a-z, A-Z, 0-9, special characters: !@#$%^&*).

After

The changes that were implemented have made the MC Consulting network more secure.

- The Outlook Web Access web site has been protected from malicious attacks. While there may be future vulnerabilities and attacks to the web site, it was configured to resist the well-known attacks.

- The Microsoft Exchange Server has been patched at both the OS and application levels.
- The IIS LockDown utility has been run on the Exchange server to lock down the IIS 5.0 implementation.
- The Microsoft ISA Server has been configured to restrict access to the Outlook Web Access site.
- The userIDs and passwords that were used to access the web site have been enhanced to keep them secure and make them more difficult to obtain.
- The sensitive client data that was being transmitted as "clear text" is now more secure and encrypted.
- The MC consultants grew in their awareness of the risks of improperly using unsecured workstations.
- The MC consultants' knowledge of the vulnerabilities within a Microsoft Exchange implementation was much more detailed.

Figure 10 illustrates the vulnerabilities found in the Outlook Web Access configuration prior to the security incidents and the decision that was used to correct the vulnerability.

Figure 10: Outlook Web Access Vulnerabilities and Mitigations Table

Basic Vulnerability	Mitigation
IIS installation utilized the default install which contained many vulnerabilities.	Execution of the IIS lockdown (IISLOCKD) tool to remove unnecessary default settings from the host Internet Information Services and to configure proper directory and file access rights. Reduced the "Destination Set" directories as defined for the Outlook Web Access web site being published to the Internet.
Unencrypted data being sent over the Internet	Installation of a VeriSign, Inc. digital certificate to secure the transmission of the user authentication credentials and email data. Configuration of the OWA website to only accept SSL encrypted communications.
User credentials "stolen" or "borrowed"	Installation of a VeriSign, Inc. digital certificate to secure the transmission of the user authentication credentials and email data.
Internet Explorer AutoComplete may have remembered a userID/password.	MC consultants were instructed not to select the remember password option when using non MC workstations. Exchange server event logs reviewed daily for "after hours" logons.
Passwords may have been weak.	The password policy was changed in Active Directory to require more complex passwords.

While there were many improvements over the previous security configuration, the Outlook Web Access web site configuration still comes up short:

- Monitoring of the Exchange event logs is tedious. An automated solution should be implemented to review these logs and send alerts to the proper people when certain events occur.
- The IIS logs could be enabled, therefore tracking the authentication and access much more closely. This would require the installation of a management platform, as these logs are extremely detailed. This was not included as it was outside of the budget for the existing year.
- The use of a digital certificate to secure the Outlook Web Access web site will require future updates since the certificate has a one year expiration date. A new certificate will need to be purchased and installed on the web site.

Lessons Learned

A look back on the installation, problems and implementation of a solution is always a good idea. These insights can produce valuable information for future projects and help ensure they are not repeated.

The following list of "lessons" was gleaned from this implementation project:

- New installations will begin with a research process to determine any possible security vulnerabilities. This will include all systems that will be implemented or changed as a result of the project.

- The project will be evaluated to determine if there will be new policies required as a result of the implementation. This should include the updating of policies already in place.

- "Once secure" does not mean "always secure." Due diligence requires constant checking for updates. The corporate patch policy should be updated to reflect any new processes that will be required to be completed as a result of the new project.

- Not only should the applications, servers and workstations be secure, the data transmitted on the wire should also be protected. Data security is often overlooked. It is important to consider all of the locations from which data will be accessed, not just the internal local area network.

- Beware of mixed mode environments. Mixed environments frequently require the relaxing of security standards or the identification and implementation of a more advanced form of security to allow the components to work together. Factor this into the cost of the project and the total cost of ownership for these "mixed" devices.

- Educate end users about security. The MC consultants were well seasoned computer users, yet they still fell victim to the seemingly obvious security risk of caching their usernames and passwords on a foreign workstation. All end users need the occasional reminder about secure computing.

Conclusion

Installations of Microsoft Exchange 2000 are common. Many of these implementations utilize the default installation options and therefore are not secure by default. Care should be taken to secure the Exchange 2000 installations for all features that are used in the normal daily operations. Research and planning is crucial to installing and configuring a secure Exchange environment system. An improperly configured Exchange 2000 server and its associated Windows 2000 host server will require more administration to keep it running smoothly and securely.

References

1. Microsoft Corporation. “STS: Must Enable Basic Authentication for Browsers Running on Macintosh OS.” Version 2.0. 15 November 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;288354 (10 June 2004).

2. Sakellariadis, Spyros. “Protecting Windows RPC Traffic.” 29 August 2002. URL: http://www.microsoft.com/technet/prodtechnol/isa/maintain/rpcwisa.mspx (12 May 2004).

3. Cisco Systems, Inc. “What are the Most Dangerous Internet Services?” 2001. URL: http://www.cisco.com/warp/public/146/news_cisco/ekits/vulnerability_report.pdf (6 October 2004)

4. Knowles, Douglas; Perriot, Frederic and Szor, Peter, “Symantec Security Response.” 26 February 2004. URL: http://www.sarc.com/avcenter/venc/data/w32.blaster.worm.html (30 July 2004).

5. SANS Institute. “The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus.” Version 4.0. 8 October 2003. URL: http://www.sans.org/top20/ (12 June 2004).

6. Microsoft Corporation. “IIS lockdown and URLscan configurations in an Exchange environment.” Version 5.0. 11 June 2004. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;309508&sd=tech (14 May 2004).

7. Juniper Networks. “ISP Glossary.” 26 August 2004. URL: http://isp.webopedia.com/TERM/s/sniffer.html (31 August 2004)

8. Microsoft Corporation. “XCCC: Turning On SSL for Exchange 2000 Server Outlook Web Access.” Version 3.1. 14 July 2004. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;320291 13 May 2004.

9. Microsoft Corporation. “STS: Must Enable Basic Authentication for Browsers Running on Macintosh OS.” Version 2.0. 15 November 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;288354 (10 June 2004).

10. George, Christopher. “Outlook Web Access for Exchange 2000.” InstantDoc #22969. December 2001. URL: http://www.winnetmag.com/Articles/Print.cfm?ArticleID=22969 (May 28 2004).

11. Granneman, Scott. “Securing Privacy Part Four: Internet Issues.” 29 May 2002. URL:http://www.securityfocus.com/infocus/1585 31 August 2004.

Last Updated: September 25th, 2017

Upcoming Training

SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event