

Securing Windows Internet Servers

Jon Miller

Senior Security Engineer

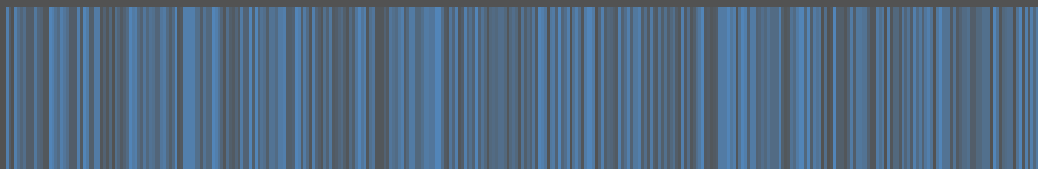
Covert Systems, Inc.



jon.miller@covertsistemas.net

23.org / Covert Systems

23
.org



- t w e n t y t h r e e d o t o r g -



Installation



Upgrading?

Always try to use a fresh install and migrate existing data over

Make sure to convert to NTFS

Default Security Settings are not applied **Y**ou must apply them manually using MMC

Installation



Service Packs

Always check windows update and TechNet to make sure you have the most current patches and SPs

HFNETCHK

File Systems



NTFS or FAT

Services

Always decide what services you require prior to installation

Never install superfluous services

Now is the time to decide what form of remote administration software, if any you will use...

- Terminal Server

- Vshell SSH & SFTP

- (www.vandyke.com)

Services

COMPAQ INSTALLATION =

DEVIL



Network Configuration

- TCP/IP should be the only protocol
- Use TCP/IP Filtering
(and IPSec when applicable)
- Nmap the server to make sure you don't have any surprise ports open
- If it is an IIS box it can NEVER be on a domain
- Use second Ethernet card for remote admin and have only the "Internet Service" on the primary interface

Using the MMC

- Customize your own security template and use it
- Establish standards within your template that apply to all servers
 - from "PDCs" to desktops

Security Configuration

- Password Complexity / Length
 - Always remember passwords so they cannot be reused

- Event Log Access

- Define Permissions for Services

- Rename Administrator Account

Common Sense

- Delete or rename files that may be used against you in the event of an attack
 - Do you really use MS TFTP?
 - Rename CMD.exe
- Create partitions or move directory structure to protect against directory transversal
- Do you really want an IIS server running on your companies Mail server?
- Remove OWA
- Microsoft Security Alerts
microsoft.com/technet/security/notify.asp

IIS 4 / 5

- Try to run only base services
- *The services below are the only services required to run a functional IIS server:*
 - Event Log
 - License Logging Service
 - Windows NTLM Security Support Provider
 - Remote Procedure Call (RPC) Service
 - Windows NT Server or Windows NT Workstation
 - IIS Admin Service
 - MSDTC
 - World Wide Web Publishing Service
 - Protected Storage

Stuff to Remove

- C:\inetpub - sample files

c:\inetpub\iissamples

c:\inetpub\iissamples\sdk

c:\inetpub\AdminScripts

c:\Program Files\Common Files\System\msadc\Samples *

- HTW Mapping

- IISADMPWD

- RDS (Remote Data Services)

Stuff to Remove

- Parent Paths?

- (Disallows “..” *be careful*)

Web server | Properties | Home Directory | Configuration | App Options

- Script Mappings

(.htr .idc .stm .shtml .shtm .printer .ida .idq .hta)

Web server | Properties | Master Properties |

WWW Service | Edit | Home Directory | Configuration

Misc.

■ Restrict Anonymous

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA  
Name: RestrictAnonymous  
Type: REG_DWORD Value: 1.
```

Permissions

- Set Your ACL's (next page)
- Make sure that the IIS log files
- are not publicly readable

`winnt\system32\LogFiles`

Permissions

CGI's - (.exe, .dll, .cmd, .pl)

- Everyone (X)
- Administrators (Full Control)
- System (Full Control)

Permissions

Script Files - (.asp)

- Everyone (X)
- Administrators (Full Control)
- System (Full Control)

Permissions

Include Files - (.inc, .shtm, .shtml)

- Everyone (X)
- Administrators (Full Control)
- System (Full Control)

Permissions

Static Content - (.txt, .gif, .jpg, .html)

- Everyone (R)
- Administrators (Full Control)
- System (Full Control)

Exchange

- Exchange is one of the few servers
- that does outgoing mail authentication
- well **Take** advantage of that and don't
- an open relay (5.5)
- Use Encrypted File System (EFS) to
- protect data
- Anti-Virus
- Internet Mail Connector
 - Limit your outgoing size
- Relaying from DMZ server to Exchange
 - Use sendmail to relay all mail to an internal exchange server
 - Or with another copy of Exchange: install Exchange, add the Internet Mail Connector, and add it to your existing site.
 - No mailboxes or folders are required

Exchange

- Setup Exchange Administrators (2000)
- Not All Admins are Full Admins
 - Exchange Administrator
 - Exchange Full Administrator
 - Exchange View Only Administrator
- Security Page
 - HKCU\Software\Microsoft\Exchange\ExAdmin
 - Value: ShowSecurityPage
 - Date: 1 (REG_DWORD)
- Tracking Logs
 - Remove Everyone Read
 - \Exchsrvr\%COMPUTERNAME%.log

Outlook Web Access

- Lock Down IIS
- Use SSL
- Front End / Back End Mode

<http://www.microsoft.com/Exchange/techinfo/deployment/2000/E2KFrontBack.asp>

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)

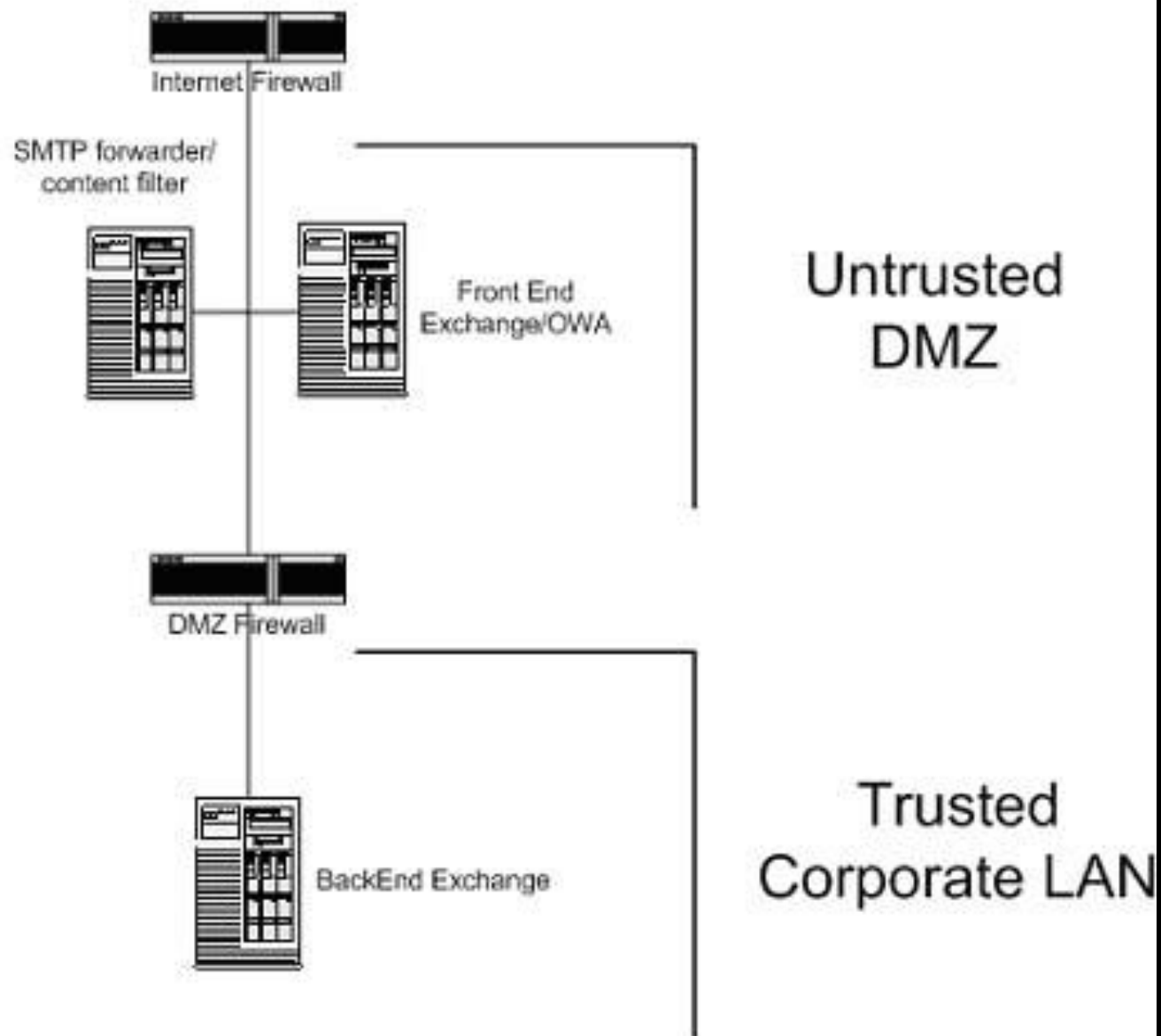
- TCP port 445 (SMB/CIFS)

- TCP port 1025 (optional RPC static port - hey, it's either this or 1024+)

- TCP port 3268 (GC)

Outgoing Allow:

- Only established connections



Tools

- URL Scan (Microsoft)
- Baseline Security Analyzer (Microsoft)
- IIS Lockdown (Microsoft)
- Secure IIS (Eeye)
- Tripwire for NT (Tripwire)
- Anti-Virus (Symantec, McAfee)
- Hire a Security Company

<http://www.23.org/~humperdink/>

Q & A

Y'all ask me stuff

jon.miller@covertsystems.net

<http://www.23.org/~humperdink/>

<http://www.covertsystems.net>