

Assessing Server Security

- General principles
- Windows 2000/2003 Servers
- Web Servers
 - IIS
 - Apache
- Linux servers
- IBM iSeries (AS/400) – optional
- IBM mainframe (os/390, RACF) - optional

Class 7

1

What's a server?

- Provides a service, typically to many clients
- Service involves network communication between client and server
- Many clients may use the services of a server
- Services range from simple name lookup (DNS) to complex organizational business transactions (SAP/R3)

Class 7

2

Common elements to server security

- Proper management
- Fix software flaws
- Control who has access
- Control type of access by users
- Log events
- *Enforces organizational security policy*

Class 7

3

Server Operating Systems

- Microsoft Windows Server 2000/2003
- UNIX (specifically Red Hat Enterprise)
- IBM iSeries (AS/400)
- IBM zOS (MVS/RACF)

Class 7

4

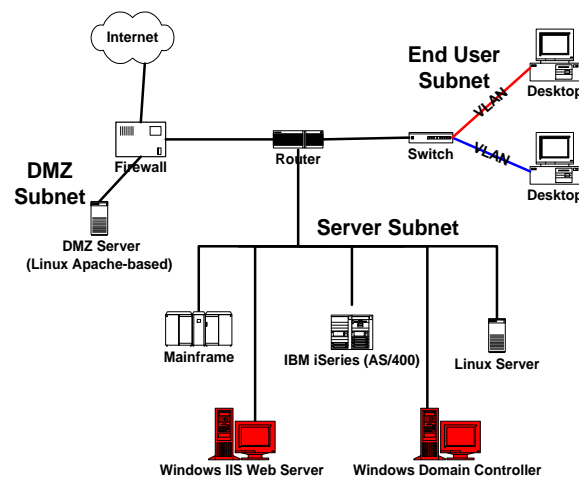
Server Applications Systems

- Web server
 - Microsoft IIS Web server
 - Apache Web Server
- And of course many others, but this class will only cover Web servers

Class 7

5

Windows 2000/2003 Servers



Class 7

6

Microsoft Windows Server 2000/2003

- Background:
 - Servers may be stand-alone, members of a workgroup, or members of a domain
 - A domain requires one or more domain controllers
 - Within a domain or workgroup, certain services are required to manage the collection of servers
 - Servers have both local accounts and resources as well as domain accounts and resources
 - Securing a single machine is much easier than securing a domain

Class 7

7

Microsoft Windows Server 2000/2003

- Assessing local system security:
 - File system NTFS (supports file security)
 - Patches and service packs current
 - Only required services running
 - Good account and password practices
 - Null sessions not allowed?
 - Event logging in use?
 - Users granted only required authority?

Class 7

8

Microsoft Windows Server 2000/2003

- Assessing domain security:
 - The domain is the basic unit of security
 - A domain is a collection of servers (and clients) to which common policies apply
 - Control may be delegated to subunits called organizational units (OUs)
 - In some cases, there are defined best practices for domain security
 - For the most part, security is policy-based and specific to the organization

Class 7

9

Microsoft Windows Server 2000/2003

- Assessing domain security:
 - Domains are governed by servers configured as Domain Controllers
 - Services used to manage a domain include DNS, LDAP, and Kerberos
 - A domain is really a kerberos realm
 - Domains may be joined together in trees and forests. Trees and forests are of secondary importance for security.

Class 7

10

Microsoft Windows Server 2000/2003

- Domain security best practices:
 - Domain administrator accounts
 - Strong authentication
 - Restrict use
 - Audit use
 - Kerberos configuration
 - Domain-wide password policies
 - Secured Domain Controllers

Class 7

11

Microsoft Windows Server 2000/2003

- Policy-based security practices:
 - Define OUs to contain users and objects
 - Delegate authority to OU administrators
 - Local system configuration governed properly by Group Policies associated with OUs.
- Are these consistent with:
 - Management directives?
 - Regulatory requirements?

Class 7

12

Microsoft Windows Server 2000/2003

- Change control is important
 - Changes authorized
 - Changes documented
 - Changes only occur per documented processes
- Physical security is important
 - Servers in physically secure area (especially domain controllers)
 - Ability to reboot or boot from foreign media may be restricted

Class 7

13

Technical Assessment Tools – Microsoft Baseline Security Analyzer

- <http://www.microsoft.com/technet/security/tools/mbsahome.aspx>
- Can review:
 - IIS
 - SQL Server
 - Exchange
 - Office (local scan only)
- Can scan a local machine or a group of remote machines
- Can run in graphical or command line mode

Class 7

14

Microsoft Baseline Security Analyzer

- What the MBSA tests:
 - All current security patches in place?
 - Is the file system NTFS?
 - Are there obvious poorly chosen passwords?
 - Are critical security events logged?
 - Etc.
- Tests are provided by Microsoft and are downloaded at start of assessment

Class 7

15

Microsoft Baseline Security Analyzer

The screenshot displays the Microsoft Baseline Security Analyzer (MBSA) interface. The main window is titled "View security report" and shows the following information:

- Computer name:** WORKGROUP\FANTASY
- IP address:** 192.168.1.150
- Security report name:** WORKGROUP - FANTASY (3-17-2007 5:15 PM)
- Scan date:** 3/17/2007 5:15 PM
- Scanned with MBSA version:** 2.0.5029.2
- Catalog synchronization date:** 2/9/2007 2:00:00 AM
- Security update catalog:** Microsoft Update
- Security assessment:** Potential Risk (One or more non-critical checks failed.)

The "Security Update Scan Results" section shows the following:

Score	Issue	Result
✗	Windows Security Updates	1 service packs or update rolls are missing. What was scanned Result details How to correct this
✓	Office Security Updates	No security updates are missing. What was scanned Result details

The "Windows Scan Results" section shows the following:

Score	Issue	Result
✗	Incomplete Updates	No incomplete software update installations were found. What was scanned How to correct this
✗	Windows Firewall	Windows Firewall is disabled and has exceptions configured. What was scanned Result details How to correct this
✓	Local Account Password Test	No user accounts have simple passwords. What was scanned Result details
✓	Automatic Updates	Updates are automatically downloaded and installed on this computer. What was scanned Result details
✓	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details

Class 7

16

Microsoft Windows Server 2000/2003

- Using Security Templates to assess Windows Servers:
 - Good for assessing compliance with organizational policies and standards (vs. best practices)
 - Available from Microsoft, NSA, SANS, CIS, and others
 - Can apply security settings as well as assess

Class 7

17

Microsoft Windows Server 2000/2003

- Using Security Templates to assess Windows Servers:
 - Text files with recommended settings (*.inf)
 - Use MMC Security Configuration and Analysis snap-in to perform assessment
 - Use MMC Security Templates snap-in to edit template
 - Create database from *.inf file
 - Use database to analyze security

Class 7

18

Microsoft Windows Server 2000/2003

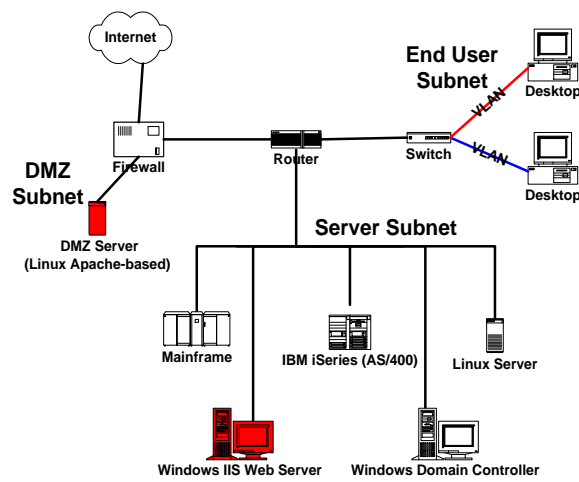
Using Security Templates to assess Windows Servers

Class 7

19

Web Servers

Microsoft IIS and Apache



Class 7

20

General Web server security assessment

- Many Web-based security vulnerabilities are independent of the actual server used
 - Web configuration
 - Handling of input
 - Flaws shared by servers and scripting languages
- NIST Special Publication 800-44, "Guidelines on Securing Public Web Servers"

Class 7

21

General Web server security assessment

- Vulnerabilities:
 - SQL injection
 - Cross-site scripting
 - Directory traversal

Class 7

22

General Web server security assessment methods

- Manual:
 - Review site coding and server configuration
 - Use a browser (or a proxy) to test various types of “interesting” input
- Automated
 - Web site scanning tools (Nikto)
 - Special purpose testing tools (absinthe for SQL injection, etc.)

Class 7

23

Microsoft IIS Web server

- Server operating system configuration (Is this a secure Windows server?)
- Web server application configuration (Is IIS running securely?)
- Web site design (does the HTML, .asp, javascript, etc. provide protection?)
- Web site back end services (is the SQLServer database protected?)

Class 7

24

Microsoft IIS Servers

- MBSA provides options for analysis of IIS:
 - Was IIS Lockdown Tool used?
 - Have sample applications been removed
 - Is the IISAdmin virtual directory removed?
 - Are parent paths not enabled
 - Are MSADC and scripts virtual directories not present?

Class 7

25

Microsoft IIS Servers

- Templates are specifically designed for Web servers specifically HISECWEB.INF, provided by Microsoft

Class 7

26

Apache Web Servers

- CIS provides a hardening document, but unfortunately no automated tool.
- This document is designed for pro-active server hardening, but can be adapted for use as assessment checklist
- Specifies a Level I (basic) and Level II (enhanced) security configurations
- **Apache Benchmark for Unix**

Class 7

27

Apache Web Servers

- Underlying Operating System hardening
- Web user groups
- Web user account
- Apache patches
- Apache configuration file(s)
- Remove Default/Unneeded Apache Files
- Updating Ownership and Permissions for Enhanced Security
- Implementing Secure Socket Layer (SSL) with Mod_SSL 30

Class 7

28

Apache Web Servers

- Apache configuration file(s):
 - Apache process owner, user, and server admin
 - Disable Unnecessary Apache Modules
 - Denial of Service (DoS) Protective General Directives (timeout, keepalive)
 - Web Server Software Obfuscation General Directives
 - Mod_Security (use general purpose intrusion prevention)
 - Access Control Directives
 - Authentication Mechanisms
 - Directory Functionality/Features Directives
 - Limiting HTTP Request Methods
 - Logging General Directives

Class 7

29

Apache Web Servers

- CIS gives us instructions for hardening a server
- But we want to assess how well someone else hardened a server
- So we need to find evidence hardening steps were performed
- E.g., where CIS says to set configuration file parameters, we need to obtain a copy of the config file and examine it for those settings

Class 7

30

Apache Web Servers

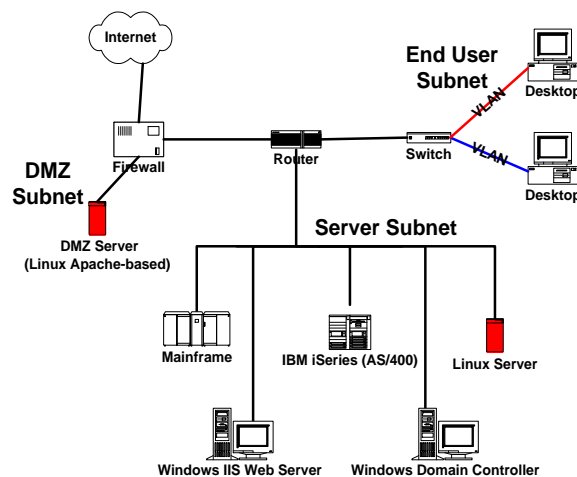
- Note that the Apache configuration instructions only describe how to configure the server:
 - They don't deal with Web site design
 - They don't address the most common Web site vulnerabilities, such as SQL injection and Cross Site Scripting (XSS)
- These fall under the category of secure coding

Class 7

31

Linux Servers

Red Hat Enterprise as an example



Class 7

32

Red Hat Enterprise

- CISecurity uses the Bastille software to assess Linux security
 - Bastille may be found at <http://www.bastille-linux.org/>
 - Use in Assessment and Reporting Mode only!

Class 7

33

Red Hat Enterprise

- Bastille checks the following:
 - File permissions for administrative utilities
 - Account policy settings
 - System boot password protection
 - Service/daemon configuration
 - Compilers disabled
 - Logging settings
 - Specific settings for Sendmail, DNS, Apache, FTP and printing

Class 7

34

Red Hat Enterprise

- Bastille does NOT seem to check for the following:
 - Operating system patch level
 - Service/daemon/utility patch level
 - Permissions and settings for most user software (e.g., OpenOffice)
 - Password strength

Class 7

35

Red Hat Enterprise

Installing and Using Bastille

- Download Bastille rpm file
- Build using `rpm -i`
- You may need to install supporting software (perl Tk, etc.)!
- Execute in assessment mode:

```
bastille --assess
```
- Only works on Red Hat Linux (Fedora, Legacy and Enterprise) and SUSE Linux (Professional, Personal and Enterprise)

Class 7

36

Red Hat Enterprise Bastille sample

Bastille Hardening Assessment Report

Score	Weights File
5.95 / 10.00	Bastille Default Weights

[Contract all Modules](#) | [Expand all Modules](#)

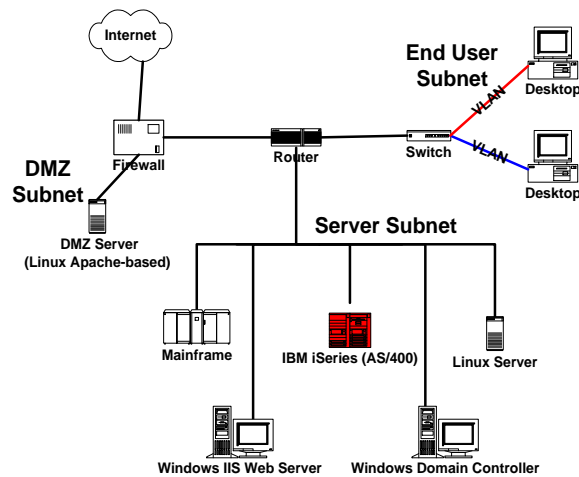
(contract) FilePermissions

Item	Question	State	Weight	Score Contrib
generalperms_1_1	Are more restrictive permissions on the administration utilities set?	No	0	0.00
suidmount	Is SUID status for mount/umount disabled?	No	1	0.00
suidping	Is SUID status for ping disabled?	No	1	0.00
suiddump	Is SUID status for dump and restore disabled?	Yes	1	1.00
suidcard	Is SUID status for cardctl disabled?	Yes	1	1.00
suidat	Is SUID status for at disabled?	No	1	0.00
suiddos	Is SUID status for DOSBMU disabled?	Yes	1	1.00
suidnews	Is SUID status for news server tools disabled?	Yes	1	1.00
suidprint	Is SUID status for printing utilities disabled?	Yes	1	1.00

Class 7

37

IBM iSeries (AS/400)



Class 7

38

IBM iSeries (AS/400)

- IBM midrange system with roots in early 1980s System/38
- Once popular for mid sized businesses running turnkey applications

Class 7

39

IBM iSeries (AS/400)

- Basic, manual iSeries security assessment:
 - Review system values
 - Overall system security policy (QSECURITY)
 - Authentication and password values
 - Event logging
 - Review user profiles
 - Profiles can override global system values
 - Review other object properties (files, directories, etc.)
 - Who can access?
 - What is logged?

Class 7

40

IBM iSeries (AS/400)

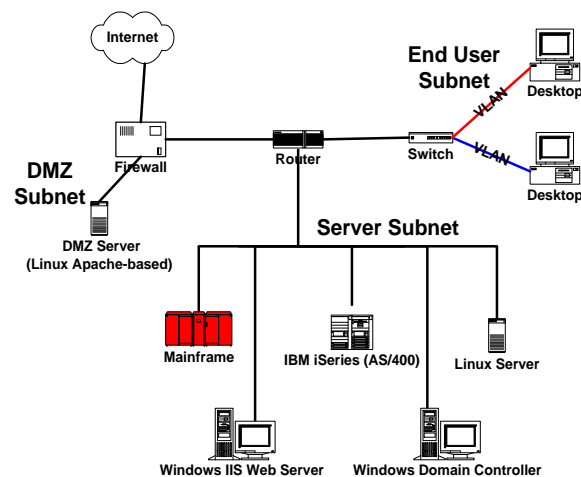
- Security review products:
 - NetIQ Security Solutions for iSeries (formerly PentaSafe)
 - IBM security toolkit (on older versions)
- See “AS/400 for Pentesters” by Shalom Carmel at:

<http://blackhatnetworks.com/presentations/bh-europe-06/bh-eu-06-Carmel/bh-eu-06-Carmel.pdf>

Class 7

41

Mainframe Computers



Class 7

42

IBM zOS (MVS/RACF)

- “Big Iron”, descendant of 1960s big systems
- Still used in high volume transaction environments
- Proprietary operating system, increasingly uses open system features
- Can host Linux
- System may have multiple partitions
- Security software is add-on to base operating system

Class 7

43

IBM zOS (MVS/RACF)

- Security software is add-on to base operating system
- Base OS only provides memory protection
- Additional software is required to support user authentication and access controls:
 - IBM RACF
 - Computer Associates ACF2 and Top Secret
- It is possible to install security software so that critical components are not protected by access controls!

Class 7

44

IBM zOS (MVS/RACF)

- Review of RACF configuration vs. assessment of operating system integrity
- A basic RACF review can be done with the following:
 - SETROPTS listing
 - DSMON report

Class 7

45

IBM zOS (MVS/RACF)

- SETROPTS listing
 - Lists RACF options (how RACF is set up)
 - Sets operating philosophy of RACF (off/warning/protect)
 - Which security events are logged?
 - What are the password and user authentication rules?

Class 7

46

IBM zOS (MVS/RACF)

- DSMON reports
 - A set of self-audit reports that can be created from RACF
 - Provides additional information on what is or is not protected by RACF
 - Summarizes how users are defined to RACF and how resources are protected

Class 7

47

IBM zOS (MVS/RACF)

- DSMON reports
 - System Report
 - Program Properties Table Report
 - RACF Authorized Caller Table Report
 - RACF Exits Report
 - Selected User Attribute Report
 - RACF Started Procedures Table Report
 - RACF Class Descriptor Table Report
 - RACF Global Access Table Report
 - RACF Group Tree Report
 - Selected Data Sets Report

Class 7

48

IBM zOS (MVS/RACF)

- What these tell you (sample):
 - System Report – Is RACF running and what version?
 - RACF Exits Report – Programmatic hooks into OS. Should be documented if any exist.
 - Selected User Attribute Report – A very informative and detailed report. Who has what authority. Look for Special, Operations, Auditor.

Class 7

49

IBM zOS (MVS/RACF)

- What these tell you (sample):
 - RACF Started Procedures Table Report – Associates a user ID to a started procedure
 - RACF Global Access Table Report – Automatic “authorize” for performance purposes
 - Selected Data Sets Report – Is an important file protected by RACF?

Class 7

50

IBM zOS (MVS/RACF)

- What these tell you (summarized):
 - Is RACF running?
 - Can RACF be bypassed?
 - Are all important files (data sets) protected by RACF?
 - Which users have privileged authority?