SearchSecurity.com INFORMATION SECURITY

Web Security School
Lesson 1

An insider's guide to Web server security

Michael Cobb, Founder & Managing Director, Cobweb Applications, Ltd.

searchsecurity.com / WebSecuritySchool

SearchSecurity.com Security School

Web Security School overview

- **Lesson 1**

Webcast: An insider's guide to Web server security
*** Includes: Windows IIS Server hardening checklist**
Network configuration: IIS SMTP Mail Relay Service
Essential vs. nonessential services

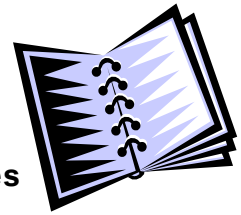
Article: Know your enemy: Why your Web site is at risk
*** Includes: Checklist of known IIS vulnerabilities**

Quiz: Test your knowledge of the materials covered in Lesson 1

- **Lesson 2:** How to secure the network perimeter and defeat Web attacks
- **Lesson 3:** How to lock down Web apps and tools for testing online security

Through an agreement with (ISC)2, all CISSPs and SSCPs earn one CPE credit for each Security School webcast attended.

Today's agenda



- Secure installation prerequisites
- Component installation
- Hardening procedures
- Access control and security policies
- Securing other network services
- Secure remote management
- Recovery plans

Laying the foundations for a secure server

- Plan ahead
- Identify and assemble required installation prerequisites
- Install and configure components
- Harden the system
- Enable audit and recovery capabilities

Secure installation requirements

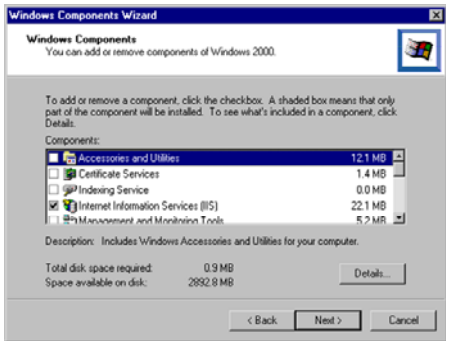
- Provide a physically secure location for your Web server
- Make the Web server a single function server
- Do not make a Web server a Windows network domain controller
- Use two network interface cards

Secure installation prerequisites

- If your Web server will be on the Internet, isolate it from your intranet
- Install multiple drives or drive partitions
- Use NTFS on all hard drives
- Do not install application software or development tools
- Do not install a printer
- Create a list of people granted system-level access

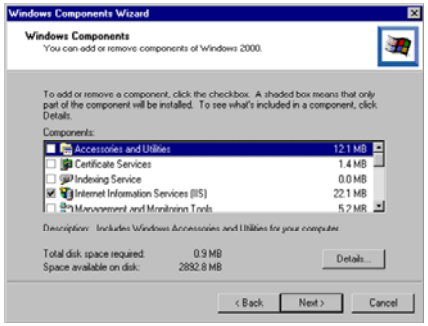
OS component installation

- X ***Accessories and Utilities***
- X ***Certificate Services***
- X ***Indexing Service***
- X ***Management and Monitoring Tools***
- X ***Message Queuing Services***
- X ***Networking Services***



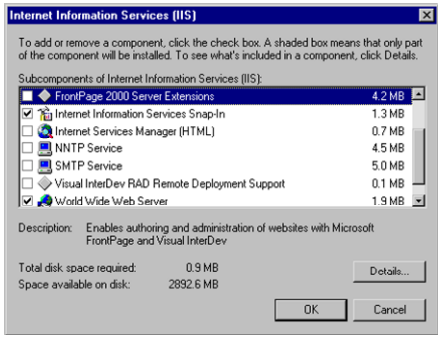
OS component installation

- X ***Other Network File and Print Services***
- X ***Remote Installation Services***
- X ***Remote Storage***
- X ***Script Debugger***
- ? **Terminal Services**
- X ***Windows Media Services***
- ✓ **Internet Information Services**



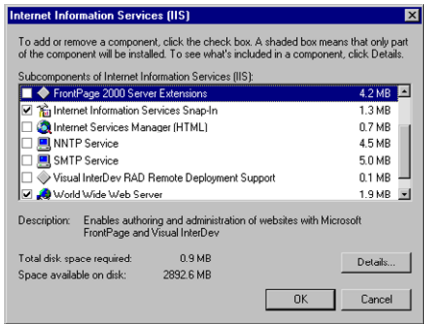
IIS component installation

- ✓ Common Files
- X IIS documentation and help topics
- X FrontPage 2000 Server Extensions
- ✓ Internet Information Services Snap-in
- ✓ World Wide Web Server



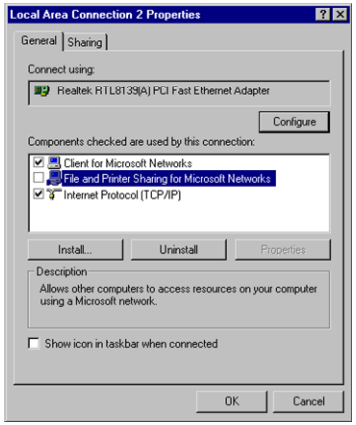
IIS component installation

- X Internet Services Manager HTML
- X File Transfer Protocol (FTP) Server
- X NNTP Service Internet News server
- X SMTP Service Simple Mail Transfer Protocol
- X Visual InterDev RAD Remote Deployment



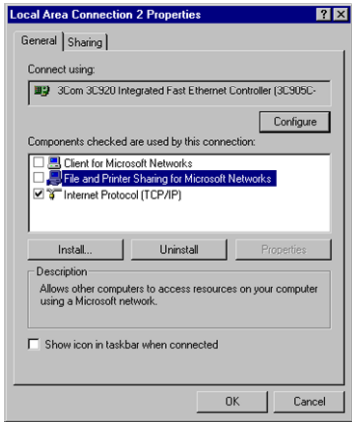
Network component installation

- ✓ **Internal-facing network card**
  - ✓ **Client for Microsoft Networks**
  - X **File and Printer Sharing**
  - ✓ **Internet Protocol (TCP/IP)**
- ✓ **Fixed IP address**



Network component installation

- ✓ **Internet-facing network card**
  - X **Client for Microsoft Networks**
  - X **File and Printer Sharing**
  - ✓ **Internet Protocol (TCP/IP)**
- ✓ **Fixed IP address**
- X **NetBIOS protocol**



Service packs and security patches

- Service packs
- Security patches
- Microsoft Security Notification Service
- Microsoft Baseline Security Analyzer
- Microsoft TechNet Web site

www.microsoft.com/technet/security/

Hardening your Web server

- Hardening tools and guidelines
  - NSA Guide to the Secure Configuration of IIS
    - http://nsa2.www.conxion.com/win2k/download.htm
  - IIS 5.0 Baseline Security Checklist
    - www.microsoft.com/technet/security/
  - IIS Lockdown Tool
    - http://www.microsoft.com/technet/security/tools/locktool.mspx
  - Hisecweb Security Template
    - http://www.securitymap.net/sdm/docs/windows/iis5chk.html

Hardening your Web server

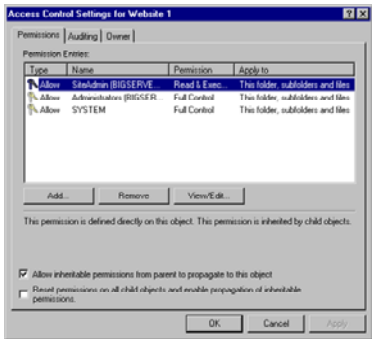
- **Hardening procedures**
  - Run the IIS Lockdown Tool
  - Manually harden the server
    - Disable Nonessential Services
    - Modify the default IIS Server environment
      - Create a new site and root directory for Web content
      - Disable parent paths
      - Remove unnecessary application mappings
      - Remove IIS Internet printing folder
      - Delete all sample directories, help files and scripts
      - Disable IP Address in content-location header
      - Reconfigure how system data is handled

Hardening your Web server

- **Miscellaneous procedures**
  - Remove the SAM File from the WINNT/REPAIR Directory
  - Disable the MS DOS Subsystems
  - Move the IIS Metabase and change the Registry Key
    - http://support.microsoft.com/default.aspx?scid=kb;en-us;Q321142
  - Secure Physical, Boot and Media settings

Access control lists - Administration

- Remove unused accounts from the server
- Remove storage administration rights for the Everyone group
- Create a delegated Administration group for Web content
- Rename Administrator account and set a strong password



SearchSecurity.com Security School

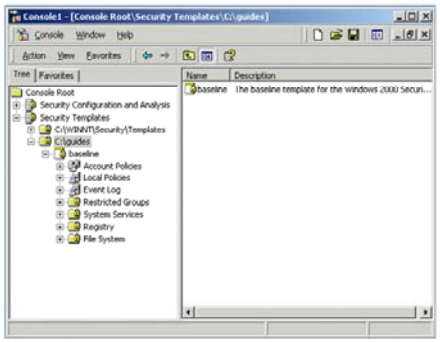
Access control lists – Anonymous access

- Rename default Internet Guest account
- Remove default Internet Guest account rights from Local Security Policy
- Create a custom least-privileged Internet Guest account for anonymous access
- Set renamed Internet Guest account to Read Only access permissions

SearchSecurity.com Security School

Security policies

- Enforce strong password policies
- Restrict remote logons
- Require Administrators to log on locally OR have a secure remote administration solution
- Ensure accounts are not shared among administrators



SearchSecurity.com Security School

The Hisecweb Security Policy template

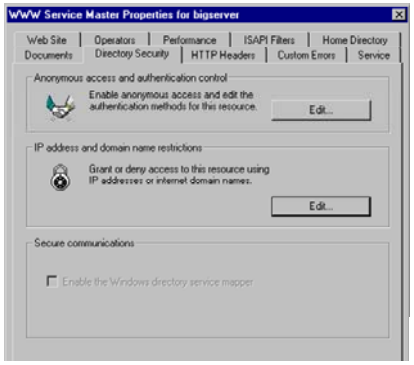
The Hisecweb Security Policy template includes settings for the following:

- Account Policies Security for passwords, account lockouts and Kerberos
- Authentication
- Local Policies Logging for security events and user/group rights assignment
- Restricted Groups Local group membership administration
- Registry Security for local Registry keys
- System Services Security and start-up mode for local services
- Security Options Rules for numerous and miscellaneous security settings

SearchSecurity.com Security School

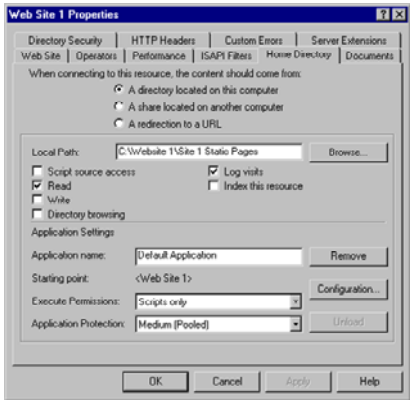
Configuring IIS site properties

- Configure site to allow only Anonymous access
- IP address and domain filters
- IIS Access Permissions



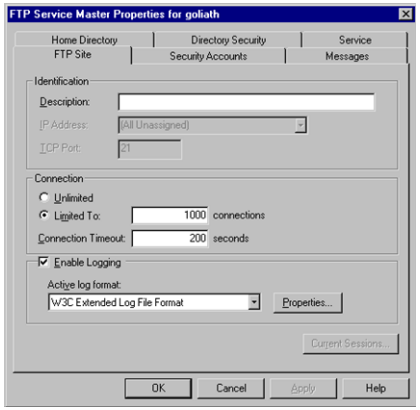
Configuring IIS site properties

- Set IIS Access Control to Read Only in content directories and Read and Execute for scripts
- Disable directory browsing



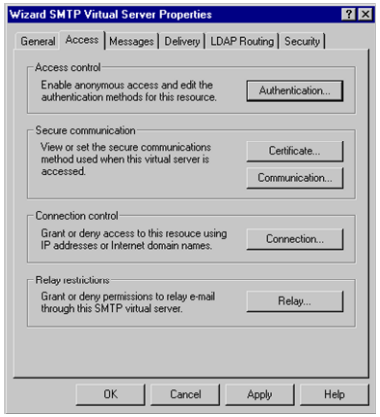
Securing other network services - FTP

- Limit connections
- Log FTP activity
- Configure account access
- Set logon message
- Configure directory location
- Configure folder and file permissions
- Configure access restrictions



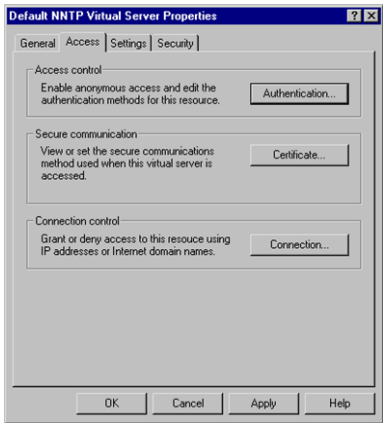
Securing other network services - SMTP

- Limit connections
- Configure access control
- Configure connection control
- Configure secure communications
- Configure relay restrictions
  - www.mail-abuse.com/
  - www.unicom.com/sw/rlytest/



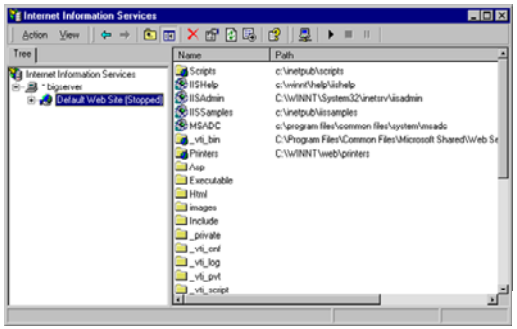
Securing other network services - NNTP

- Configure directory location
- Enable logging
- Limit connections
- Configure access control
- Configure access restrictions
- Disallow control messages



Secure remote management

- Internet Services Manager
  - ✓ VPN
  - ✓ Windows Terminal Services
- X HTML Administration



Recovery plans

- Server content and configuration backup
- Emergency repair disks
- Disaster recovery plan
- Backup security issues
  - Backup privileges
  - Separate logon accounts
  - Media check-in and check-out

Homework

- Visit Microsoft TechNet Security
- Run Microsoft Baseline Security Analyzer
- Update Security Policies
- Sign up for Microsoft Security Notification Service
- Review my checklists to see if you're complying with my recommendations at searchsecurity.com / WebSecuritySchool

Web Security School, Lesson 1

Webcast: An insider's guide to Web server security

*** Includes: Windows IIS Server hardening checklist**
Network configuration: IIS SMTP Mail Relay Service
Essential vs. nonessential services

Article: Know your enemy: Why your Web site is at risk
*** Includes: Checklist of known IIS vulnerabilities**

Quiz: Test your knowledge of the materials covered in Lesson 1

searchsecurity.com / WebSecuritySchool

Next in Lesson 2

Webcast: Web attacks and how to defeat them

Article: Life at the edge: Securing the network perimeter

Quiz: Test your knowledge of the materials covered in Lesson 2

searchsecurity.com / WebSecuritySchool

Through an agreement with (ISC)2, all CISSPs and SSCPs earn one CPE credit for each Security School webcast attended.