SearchSecurity.com   INFORMATION SECURITY

Web Security School
Lesson 2

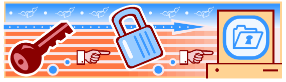
Web attacks and how to defeat them

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

searchsecurity.com / WebSecuritySchool

SearchSecurity.com
Security School

Web Security School overview



- Lesson 1: How to secure a Web server and understanding risks to your Web site
- **Lesson 2**

Webcast: Web attacks and how to defeat them
*** Includes: Windows tools for investigating an attack**
Essential fortification list

Article: Life at the edge: Securing the network perimeter

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

- **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.

searchsecurity.com / WebSecuritySchool

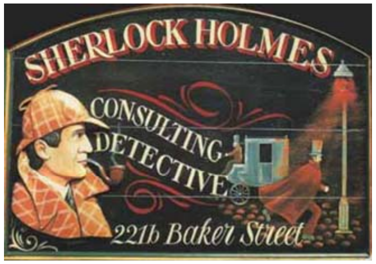
SearchSecurity.com
Security School

Today's agenda

- What to expect and look for when analyzing an attack
- A guide to logging and auditing
- Essential fortification
- Five best countermeasures
- Other recommended enhancements

A forensic analysis

- "Prevention is ideal, but detection is a must."
- What did the attacker…
  - …do to get in?
  - …use to get in?
  - …do to your server?
  - …do with your data?



Analyzing an attack

- ✓ Where did the attack start?
- ✓ Information gathering stage
- ✓ Find the vulnerability
- ✓ Determine why it existed
- ✓ Find out how to fix it
- ✓ Review security policy

Probable and improbable threats

- ✓ Cost-effective risk assessment

- ✓ Balance the value of the Web site against the cost of protecting it

The weakest link is on the inside

- 65% of computer related losses are due to errors and omissions
- 13% are due to dishonest employees
- 6% to disgruntled employees
- only 3% to hackers
- 79% of all network attacks originate from within the local network

SearchSecurity.com Security School

A guide to logging and auditing

✓Log system events

✓Log Web service activity

✓Audit your logs

SearchSecurity.com Security School

Log management

- ✓ Log Web traffic both locally and to a remote log server
- ✓ Log all systems to a remote log server
- ✓ Store your local log files on an NTFS volume or write once media

Auditing

- Tracks specific events
- Analyzes specific events
- Outcomes for an audited event = *success* or *failure*
- Determine what information to capture

Auditing goals and objectives

- Establish your audit goals and objectives
- Decide which events and resources need auditing

Potential threat	Audit Type	Events Outcomes
Random password hack	User Account	Failure audit for logon/logoff events. A large number indicates repeated attempts that are frequently the result of a systematic attack.
Stolen password break-in	User Account	Success audit for logon/logoff events to identify users of the system to identify where they came from.
Improper access to sensitive files	File System	Success and failure audit for file-access and object-access events on high security resources. Success and failure audit of read/write access by suspect users or groups for the sensitive files.
Misuse of privileges	File System & Registry	Success audit for user rights, user and group management, security change policies, restart, shutdown and system events to observe who made changes and what changes were made.

Events that can help identify a security problem

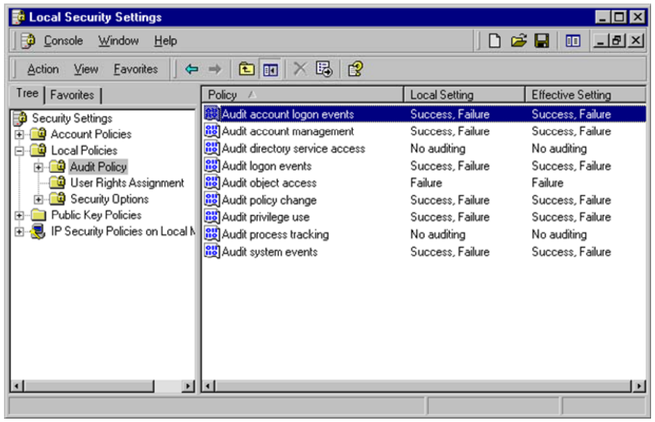
Audit categories

The nine audit categories and the recommended settings for an audit policy on an IIS Web server

Property	Success	Failure
Account Logon	On	On
Account Management	On	On
Directory Service Access	Off	Off
Logon	On	On
Object Access	Off	On
Policy Change	On	On
Privilege Use	On	On
Process Tracking	Off	Off
System	On	On

Recommended settings for IIS Audit Policy

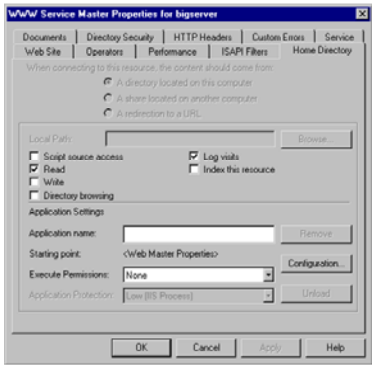
Local Security Policy Tool



Policy	Local Setting	Effective Setting
Audit account logon events	Success, Failure	Success, Failure
Audit account management	Success, Failure	Success, Failure
Audit directory service access	No auditing	No auditing
Audit logon events	Success, Failure	Success, Failure
Audit object access	Failure	Failure
Audit policy change	Success, Failure	Success, Failure
Audit privilege use	Success, Failure	Success, Failure
Audit process tracking	No auditing	No auditing
Audit system events	Success, Failure	Success, Failure

Auditing for IIS

- ✓ Log all IIS services
  - ✓ HTTP, FTP, NNTP, SMTP
- ✓ Use W3C Extended log file format for auditing
- ✓ Write unsuccessful client requests To event log



When connecting to this resource, the content should come from:

● A directory located on this computer
○ A share located on another computer
○ A redirection to a URL

Local Path:

☐ Script source access
☑ Read
☐ Write
☐ Directory browsing
☑ Log visits
☐ Index this resource

Application Settings

Application name:

Starting point: <Web Master Properties>

Execute Permissions: None

Application Protection: Low (IIS Process)

Auditing checklist

- Examine log files
- Check for odd user accounts and groups
- Look for incorrect group memberships
- Look for incorrect user rights
- Check for unauthorized applications from starting
- Check system binaries
- Check network configuration and activity
- Check for unauthorized shares
- Examine jobs run by the scheduler service.
- Check for unauthorized processes
- Search for unusual files
- Check for altered permissions on files or registry keys
- Check for changes in user or computer policies
- Check system has not been moved to a different Workgroup or Domain
- Examine all machines on the local network

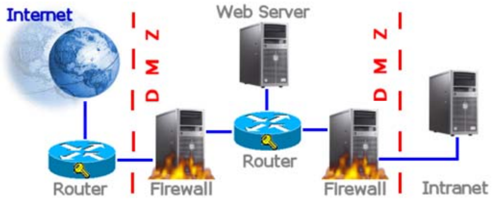
Essential fortification

- Five best countermeasures
  - ✓ Firewall
  - ✓ Intrusion-detection system (IDS)
  - ✓ Log analyzer
  - ✓ Antivirus scanner (AV scanner)
  - ✓ Security awareness training

Firewall

- All traffic must enter it
- Only authorized traffic can pass through it
- Must be resistant to penetration

- ICSA Firewall Buyer's Guide
  - www.icsalabs.com

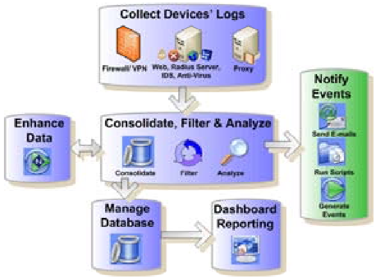


Intrusion-detection systems

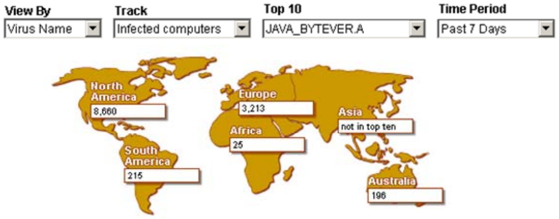
- Threshold barriers - Specific events, such as a failed login
- Profiling - Analysis of actual usage versus a baseline profile
- Known attack signatures - Network activity is screened for things like invalid TCP headers or sudden mass e-mailings
- Host-based or network-based

Log analyzers

- Automate auditing and analysis
- Notify of unusual events
- Provide a basis for:
  - focused security awareness training
  - reduced network misuse
  - stronger policy enforcement



Antivirus scanners



View By: Virus Name

Track: Infected computers

Top 10: JAVA_BYTEVER.A

Time Period: Past 7 Days

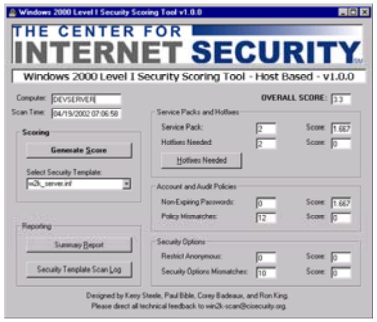
- Antivirus software is of no use without an antivirus policy
- Consider the Lock Down Alternative

Security awareness training

- ✓ Training
- ✓ Get users on your side
- ✓ Accountability
- ✓ Security is everyone’s job
- ✓ A Human Firewall
  - ✓ www.humanfirewall.org

Additional recommended enhancements

- ✓ Web security scanners
- ✓ Benchmarking tools
  - ✓ www.cisecurity.org


Windows 2000 Level I Security Scoring Tool v1.0.0
THE CENTER FOR INTERNET SECURITY
Windows 2000 Level I Security Scoring Tool - Host Based - v1.0.0
Scoring
Generate Score
Reporting
Summary Report
Security Template Scan Log
Hotfixes Needed

Computer: DEVSERVER
Scan Time: 04/19/2002 07:06:58
OVERALL SCORE: 3.3
Select Security Template: w2k_server.inf

Service Packs and Hotfixes
Service Pack: 2 Score: 1.667
Hotfixes Needed: 2 Score: 0

Account and Audit Policies
Non-Expiring Passwords: 0 Score: 1.667
Policy Mismatches: 12 Score: 0

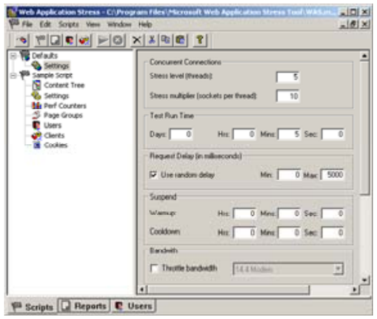
Security Options
Restrict Anonymous: 0 Score: 0
Security Options Mismatches: 10 Score: 0

Designed by Kerry Steele, Paul Bible, Corey Badeaux, and Ron King.
Please direct all technical feedback to win2k-scan@cisecurity.org

Additional recommended enhancements

Stress tests

- ✓ Web Application Stress Tool


Web Application Stress - C:\Program Files\Microsoft Web Application Stress Tool\WAS.m...
File Edit Scripts View Window Help
Defaults
Settings
Sample Script
Content Tree
Settings
Perf Counters
Page Groups
Users
Clients
Cookies
Scripts
Reports
Users

Concurrent Connections

Stress level (threads): 5

Stress multiplier (sockets per thread): 10

Test Run Time

Days: 0 Hrs: 0 Mins: 5 Sec: 0

Request Delay (in milliseconds)

☑ Use random delay Min: 0 Max: 5000

Suspend

Warmup: Hrs: 0 Mins: 0 Sec: 0

Cooldown: Hrs: 0 Mins: 0 Sec: 0

Bandwidth

☐ Throttle bandwidth 14.4 Modem

- ✓ Change control
- ✓ Web site monitoring services
- ✓ Red Teams

SearchSecurity.com Security School

A cost-effective solution

- ✓ Risk analysis & vulnerability assessment
- ✓ Protect critical assets first
- ✓ Free tools
- ✓ Top 75 security tools
  - ✓ www.insecure.org

SearchSecurity.com Security School

Homework

- Run the CIS Benchmark and Scoring Tool
- Review and implement recommendations
- Update security policies
- Run a Stress Test against your Web server

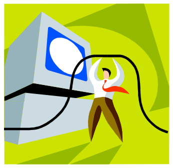
Web Security School, Lesson 2

Webcast: Web attacks and how to defeat them
* Includes: Windows tools for investigating an attack
Essential fortification list

Article: Life at the edge: Securing the network perimeter

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

searchsecurity.com / WebSecuritySchool



Next in Lesson 3

Webcast: Locking down your Web applications

Article: Top tools for testing your online security

Quiz: Test your knowledge of the materials covered in Lesson 3

searchsecurity.com / WebSecuritySchool

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

SearchSecurity.com Security School