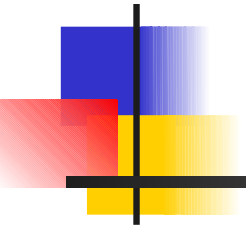


SEC520

Hardening Windows 2003 Server

Today's Objectives

Hardening Windows 2003 Server:

- Elements of Server Hardening
  - Review / Community
- Security Configuration Wizard (SCW)
  - Security Polcies
  - Network / Registry / Audit & Policies
- New Technology File System (NTFS)
  - ACLs
- Automatic Updates

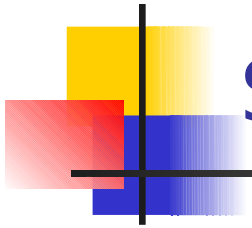
Server Hardening

Elements of Server Hardening

We have already looked at hardening a Linux server in labs 4 and 5. The basic concepts of hardening a Windows server is similar (although the approach or tools may vary or be grouped in different areas).

Below are several <u>common</u> elements of server hardening:

- Lock down BIOS / Access upon Bootup
- Turn off unnecessary services (ports)
- Limit users to processes (ports)
- Using Digital Encryption (for remote access)
- Using Access Control Lists (Advanced Permissions)
- Logging user and system activity (Manage by Exception)
- Setting automatic updates (patches)



Server Hardening

Hardening Guidelines / Societies

There are various organizations / institutions that provide guidance (i.e. “Best Practices”) for Internet Security:

- **SANS Institute**
  - Private US company that concentrates on Internet security (i.e. “best practices”)
- **NSA** (National Security Agency)
  - US Government organization specializing in security (including password encryption methods used by Unix/Linux and Internet security)
- **NIST** (National Institute of Standards and Technology)
  - Best practices to safeguard economic security.

Hardening of Windows 2003 Server

Security Configuration Wizard

It can be confusing and time-consuming to follow check-lists and guides from Internet security institutes such as SANS, NSA, and NIST.

In an effort to help simply the process, Microsoft provides the SCW (Security Configuration Wizard) to incorporate most of these elements in terms of policies and assigned roles including:

- Disable unnecessary services
- Block unused ports
- Enable additional security restrictions
- Enable LDAP services

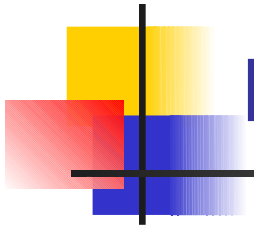
Hardening of Windows 2003 Server

Security Configuration Wizard

In order to use SCW, you need to download and install Service Pack 1.

The Following sections are set during the process:

- **Defining Roles** (client / admin / additional services)
- **Network Security** (firewall, Web-server - IIS)
- **Registry Settings** (allowed communication protocols)
- **Audit Policy** (eg. Reporting / accounting)



Hardening of Windows 2003 Server

New Technology File System (NTFS)

NTFS is a newer file system developed for Windows operating systems that provide improved disk space utilization, file system journalling, as well as security.

This newer file system technology incorporates Access Control Lists (**ACLs**) which you have learned and configured in *Lab #5: Linux Hardening - Part 2*.

Reference:

http://www.windowsecurity.com/articles/understanding-windows-ntfs-permissions.html

Hardening of Windows 2003 Server

Monitoring Activity / IDS Applications

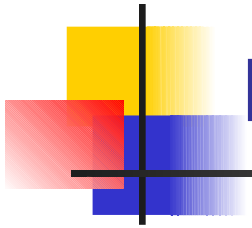
Although SCW makes it easier to harden the Windows 2003 server, it is recommended to also monitor suspicious activity.

In Lab 8, you will be learning commands (via SANS institute publications) on how to monitor suspicious activity including:

- Large files
- Strange processes / installed programs
- Network activity
- User accounts

In order to simply the process (like SWC), is to use Intrusion Detection Systems (IDSs).

There are many ones available (both proprietary and open-source)...

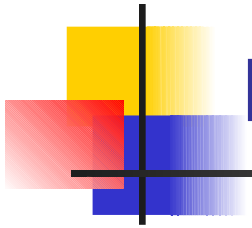


Hardening of Windows 2003 Server

Automatic Updates (Patches)

Similar to hardening your Linux system, it is necessary to apply patches on a consistent (timely) basis.

In Lab8, you will be setting up automatic updates to further harden your Windows 2003 server.



Lab Time

Perform:

Lab 8: Hardening Windows 2003 Server