
CMSC 426

Principles of Computer Security

Lecture 18

Windows Security Features

Today's Topics

- Hardening
- Windows hardening methods
 - Defender
 - Automatic updates
 - Security and group policy
 - etc.

Hardening

What is Hardening?

- Securing a system against attack, often using things that are built-in or already available on the system
- Examples of hardening:
 - Reducing avenues of attack
 - Patching known vulnerabilities
 - Using encryption
 - Installing security measures
 - Firewall, anti-virus software
 - User-end (strong passwords, etc.)

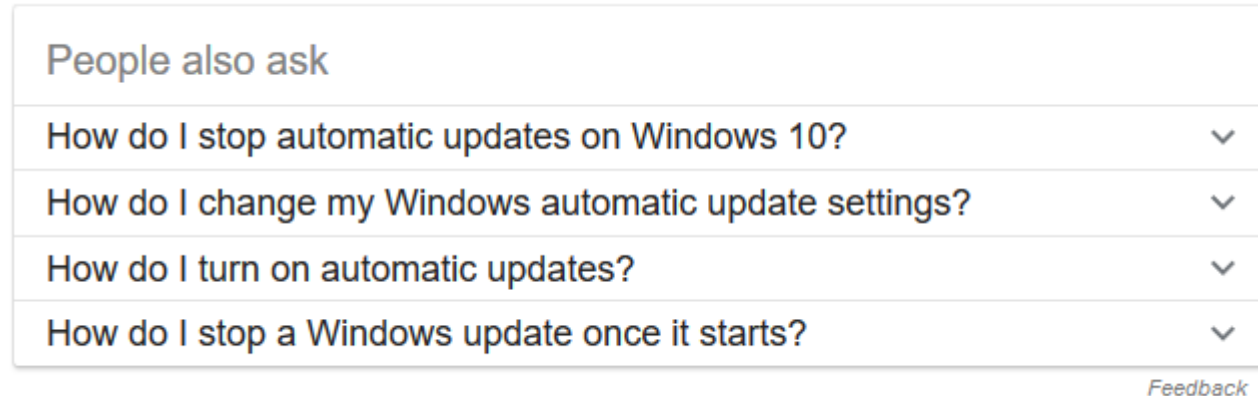
Windows Features

Windows “Defender” Firewall

- Sets the policy for inbound and outbound network traffic
- By default, every network connection has the firewall enabled
 - Only default exception is machines on local network
- Both outgoing and ingoing have it enabled
- Thanks to the default state, the network connection is protected immediately, with no window of vulnerability

Windows Automated Updates

- Automatically downloads and installs patches for the OS



- Patches include fixes related to:
 - ❑ Bugs and issues (performance, etc.)
 - ❑ New features (updates to IE, etc.)
 - ❑ Security fixes and vulnerabilities

Microsoft Security Essentials (MSE)

- Anti-virus software that provides protection against malware
- Provides real-time protection
 - Monitors activity on the system
 - Scans new files as they are downloaded or created
 - If threat is detected, attempts to disable
- **Ethics:** since it comes pre-installed with Windows, is this a violation of competition law?

Windows Defender

- Replaces Microsoft Security Essentials in Windows 8 and up
 - Before that, Defender only protected against spyware
- Switches itself off when third-party anti-virus is installed
 - Can still optionally perform periodic checks in this situation
- Checks files from IE/Edge as they are downloaded
- “Block at First Sight” uses machine learning to predict whether a file is malicious

Security Policy

- Allows configuration of nearly all Windows security settings
- Examples:
 - Password policy (min length, char types, etc.)
 - Guest accounts, lock out timer, etc.
 - LM, NTLM, and SAM settings
 - Access to machine via local connections
 - Shared desktop
 - Backup scheduling and restoring files

Group Policy

- Allows network administrators to configure the security settings for an entire network of machines from one central location
 - Can also allow control of user accounts on a single machine
- Settings are stored in “Group Policy Objects”
- Policy examples:
 - Users may only run specific programs
 - Users may not have access to specific drives
 - Users may be prohibited from running a program as administrator

Auditing

- Administrators can configure Windows to record different types of operating system activity
- Activity examples:
 - Logon and logoff events
 - Changes made to user accounts
 - Changes made to security policies
 - Launching of applications
 - Users being granted or denied access to something
 - Windows starting up or shutting down

Security Log

- These audited events are written to a security log
- After a breach of security or a malware attack, the security log can be examined for information/evidence
 - Is actually admissible in court as evidence
 - Also possible to write false events to the log, but few accounts have the privilege to do that
- Very important for accountability

User Account Control (UAC)

- Helps prevent unauthorized changes to the operating system
- The age-old question: “Do you want to allow the following program to make changes to this computer?”
- Mitigates the effects of dumb users, as well as malware
 - If the account attempting to make changes is not an administrator, the changes are either not allowed, or a PIN or an admin’s password must be entered

Windows File Protection (WFP)

- Present on Windows 2000 and XP
- Ensures critical system files are not deleted or replaced
 - Windows keeps backups of these files in the location
`C:\WINDOWS\System32\D11Cache`
 - If a file is deleted or replaced, the OS restores it from that location
- Uses authenticode digital signatures (*i.e.*, file signing) to identify publisher and check for modifications to files

Windows Resource Protection (WRP)

- Improved version of WFP in Windows Vista and beyond
- Like WFP, protects essential system files
- Also protects critical registry keys and folders
 - Admins no longer have full permissions to interact with system files
 - Full access is only granted to TrustedInstaller

BitLocker

- Full disk encryption
 - Available in most professional and enterprise versions of Windows, starting with Vista
- Older versions only encrypt the OS disk volume
 - Newer versions can encrypt the entire disk
- Uses AES 128 or 256, and Cipher Block Chaining mode (CBC)
- Unique CBC “chain” on each sector of the disk
 - Why do this?
 - Don't have to re-encrypt the entire disk to save something

General Hardening Tips

- Patch! Patch! Patch!
- Remove or disable unnecessary services
- Good account and password practices
- Good firewall practices
 - Your current Windows defaults are NOT good enough