Advanced Windows Security

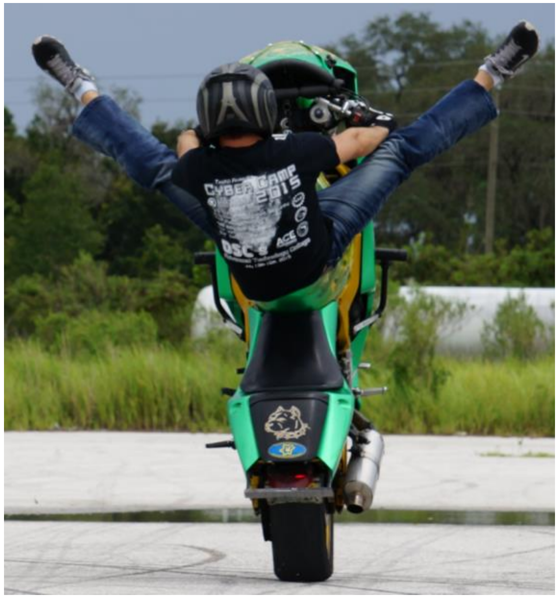
Ricky Payne CISSP, RHCE, RHCSA, Security+ , BS-IST, AS-CET

About Me

- Over 12 years of progressive DevSecOps experience from Intern to CSO
- Built “Gold Standard” federal security programs that produced 10+ federally certified systems.
- Expert generalist: from pre-sales proposal work, policy and reference architecture development, requirements decomposition into agile sprints, proof of concepts, implementation, operations, and technical training to incident response.

- Mentored/taught Windows and Linux security at CyberPatriot/CyberCamps since 2013. Accomplishments include 1st and 2nd in State and 1st in Regionals.

- As a CSO for a federal SaaS, leads end-to-end Security, Privacy, and Operations for a FedRAMP Moderate (325 NIST 800-53r4 security controls) authorized SaaS hosted in AWS GovCloud.



Ricky Payne
CISSP, RHCE, RHCSA
Security+, BS-IST, AS-CET
grep.rickp@gmail.com
@RickPayne929

Agenda

Windows Security:

- Access Control - Account Management
- Access Control - Account Lockout Policy
- Auditing
- Firewall
- Identification and Authentication - Password Policy
- Least Functionality – Features, Services, Sharing
- Patching – Application, System
- Prohibited file identification

Ricky Payne CISSP, RHCE, RHCSA, Security+ , BS-IST, AS-CET

Security Frameworks

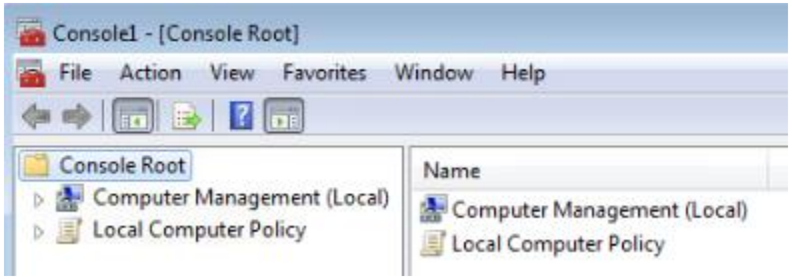
The core of this lesson is centered around critical security concepts required in nearly every control framework. Examples include: NIST CSF, ISO 27002, ASD Top 35, NSA Top 10, PCI DSS, HIPAA[1]…

- Access Control - Account Management
  - NIST 800-53r5 Access Control family: AC-6 Least Privilege - Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions[2].
- Patching – Application, System
  - PCI DSS Requirement 6 Develop and maintain secure systems and applications: 6.2 - Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release[3].

Management Console

Use MMC as a centralized means to manage Windows security.

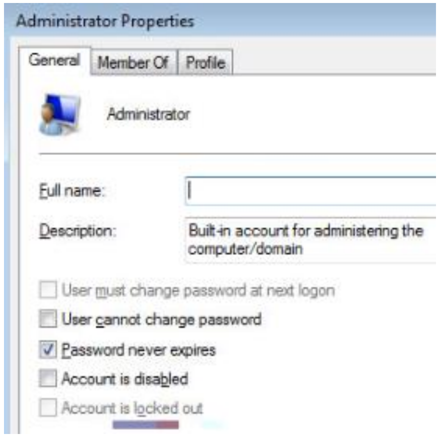
- Click: Start -> Type: mmc -> Open as administrator (Ctrl+Shift)
- File -> Add/Remove Snap-in… (Ctrl+M)
  - Computer Management
  - Group Policy Object Editor



Access Control - Account Management

Per the Principle of Least Privilege (PoLP), consider what users are on the system and what access they have.

- Expand Computer Management -> System Tools -> Local Users and Groups
  - Select: Users -> Review several users - > observe the General tab account attributes such as password expiration, disabled status, and group membership via the Member Of tab.
  - Select: Groups -> Review several Groups - > observe the members and the ability to add / remove.



Administrator

Full name: |

Description: Built-in account for administering the computer/domain

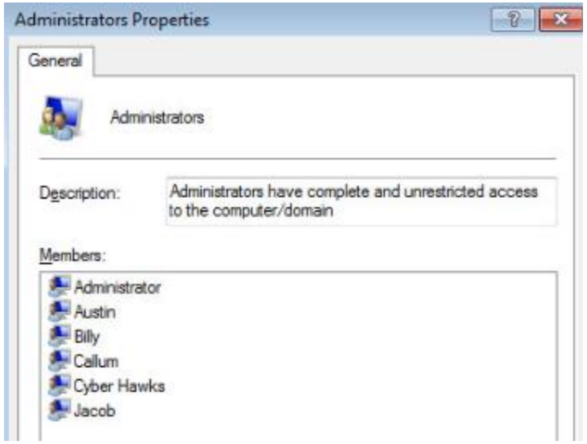
□ User must change password at next logon

□ User cannot change password

☑ Password never expires

□ Account is disabled

□ Account is locked out



Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

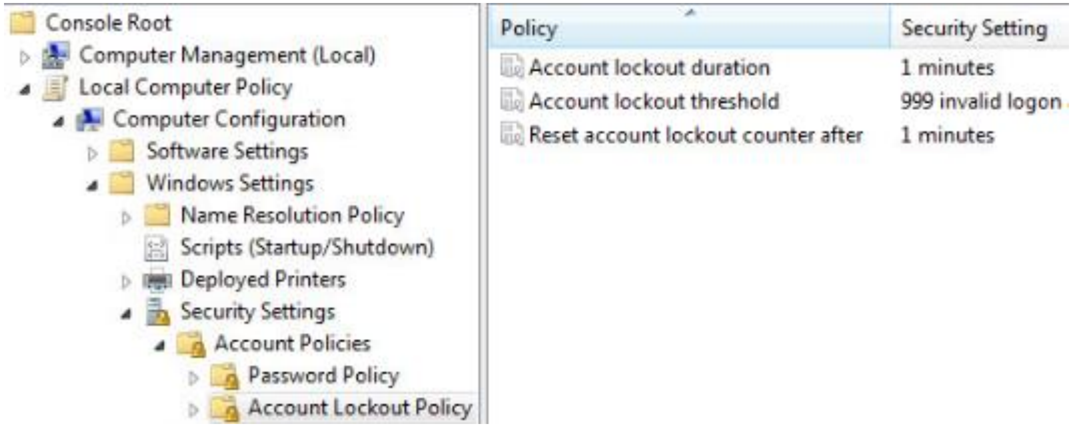
Members:

Administrator
Austin
Billy
Callum
Cyber Hawks
Jacob

Access Control -
Account Lockout Policy

The ALP can be configured to prevent brute-force attacks[4].

- Expand Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy
  - Explore all 3 settings and the Explanation tab to understand each configuration.

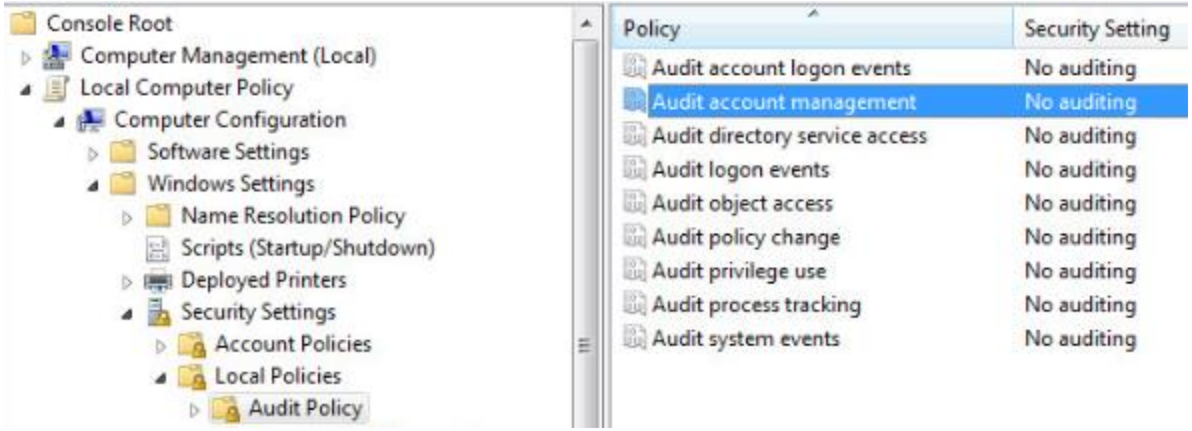


Policy	Security Setting
Account lockout duration	1 minutes
Account lockout threshold	999 invalid logon
Reset account lockout counter after	1 minutes

Auditing

Audit logs are necessary to provide a trail of evidence to help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred as well as detecting attacks[4].

- Expand Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Audit Policy
  - Explore the auditing settings and the Explanation tab to understand each configuration.



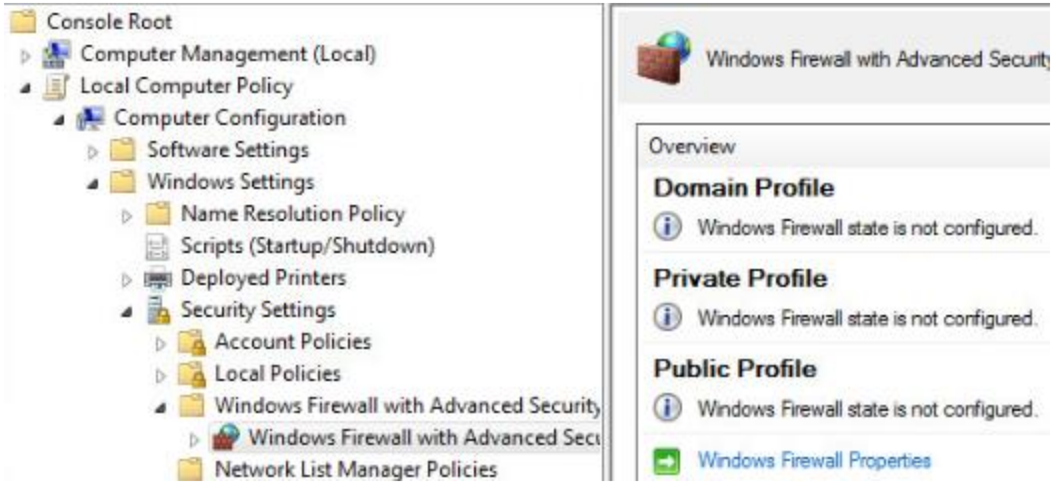
- Console Root
  - Computer Management (Local)
  - Local Computer Policy
    - Computer Configuration
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Deployed Printers
        - Security Settings
          - Account Policies
          - Local Policies
            - Audit Policy

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

Firewall

A firewall provides a line of defense against attack, allowing or blocking inbound and outbound connections based on a set of rules[4].

- Expand Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security
  - Explore the firewall properties to view various settings, such as on/off ang logging, for each Profile.



Console Root
Computer Management (Local)
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Windows Firewall with Advanced Security
Windows Firewall with Advanced Secu
Network List Manager Policies

Windows Firewall with Advanced Securit

Overview

Domain Profile

Windows Firewall state is not configured.

Private Profile

Windows Firewall state is not configured.

Public Profile

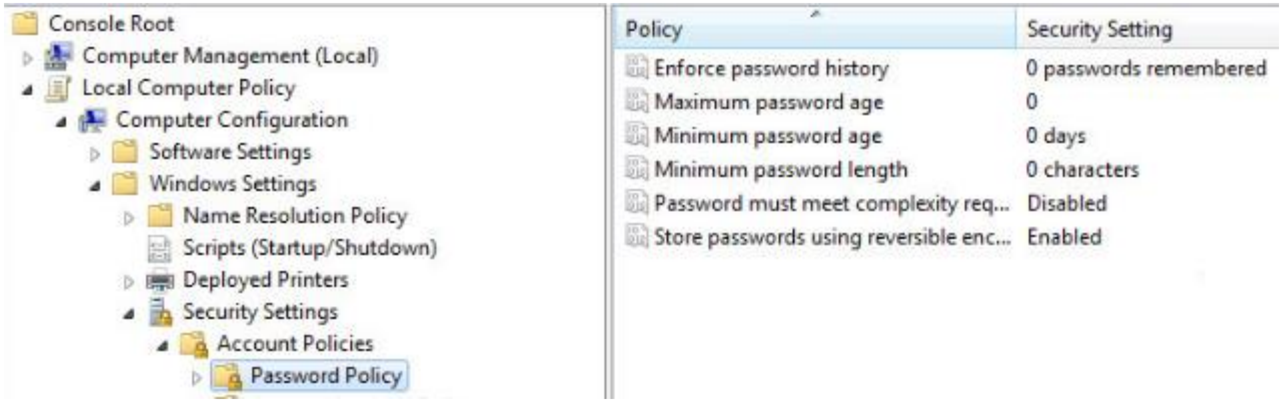
Windows Firewall state is not configured.

Windows Firewall Properties

Identification and Authentication - Password Policy

Default credentials and weak passwords often lead to breaches and botnets. Creating a strong password policy can greatly reduce these risks.

- Expand Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Password Policy
  - Explore all 6 settings and the Explanation tab to understand each configuration.

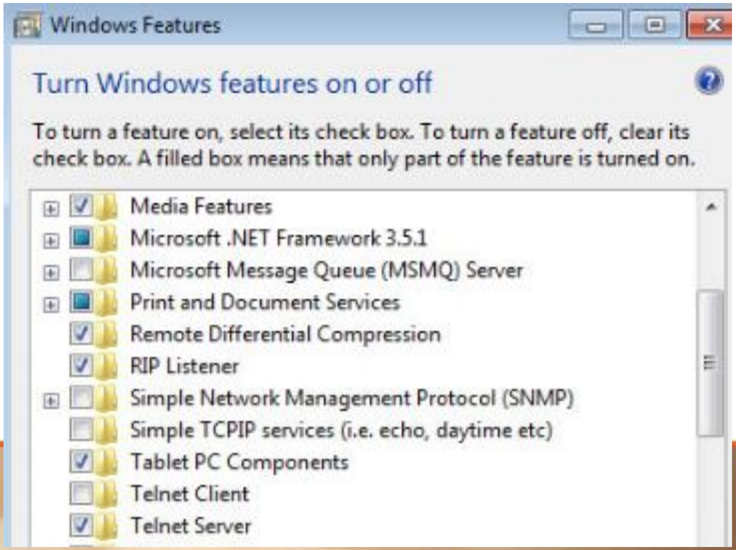


Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	0
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity req...	Disabled
Store passwords using reversible enc...	Enabled

Least Functionality – Features

Systems provide a wide variety of functions and services. Some of the functions and services routinely provided by default, may not be necessary to support essential organizational missions, functions, or operations. Organizations consider disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of devices, transfer of information, and tunneling[2].

- Click: Start -> Type: Features -> Open Turn Windows features on or off
  - Review the enabled features for prohibited or unnecessary items such as Media Features and Telnet.



Turn Windows features on or off

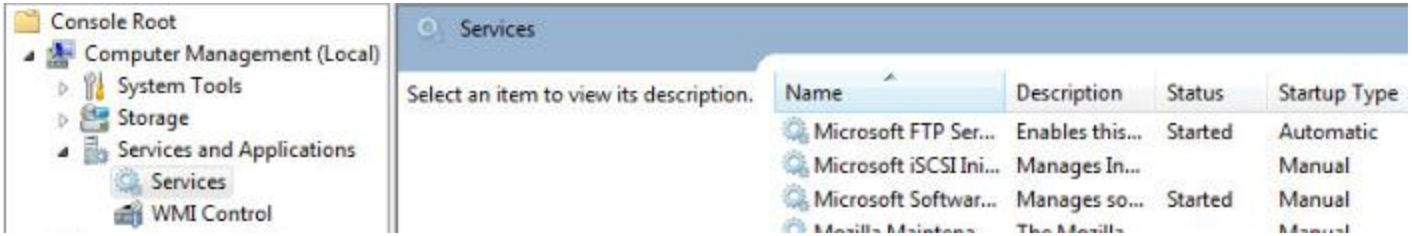
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☑ Media Features
- ■ Microsoft .NET Framework 3.5.1
- □ Microsoft Message Queue (MSMQ) Server
- ■ Print and Document Services
- ☑ Remote Differential Compression
- ☑ RIP Listener
- □ Simple Network Management Protocol (SNMP)
- □ Simple TCPIP services (i.e. echo, daytime etc)
- ☑ Tablet PC Components
- □ Telnet Client
- ☑ Telnet Server

Least Functionality – Services

Systems provide a wide variety of functions and services. Some of the functions and services routinely provided by default, may not be necessary to support essential organizational missions, functions, or operations. Organizations consider disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of devices, transfer of information, and tunneling[2].

- Expand Computer Management -> Services and Applications -> Services
  - Review the services for prohibited or unnecessary items such as FTP and Telnet.



- Console Root
  - Computer Management (Local)
    - System Tools
    - Storage
    - Services and Applications
      - Services
      - WMI Control

Services

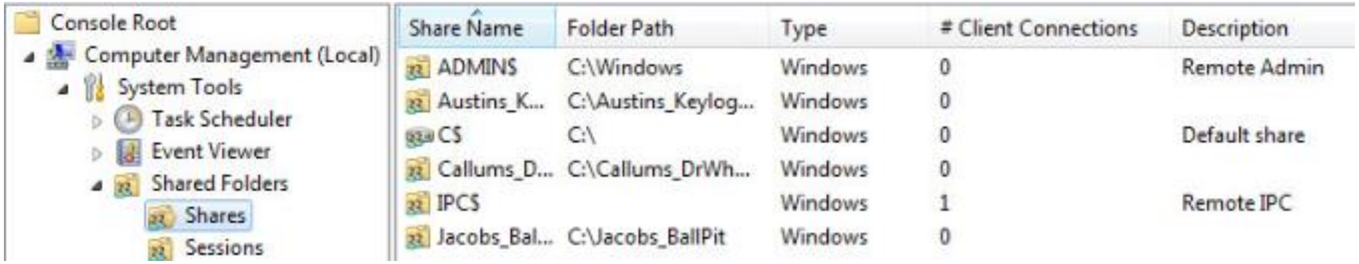
Select an item to view its description.

Name	Description	Status	Startup Type
Microsoft FTP Ser...	Enables this...	Started	Automatic
Microsoft iSCSI Ini...	Manages In...		Manual
Microsoft Softwar...	Manages so...	Started	Manual
Mozilla Maintena...	The Mozilla...		Manual

Least Functionality – Sharing

Uncontrolled resource sharing, such as Anonymous and Everyone, can lead to unauthorized system access, resource exposure, and/or corruption of sensitive data[4].

- Expand Computer Management -> System Tools -> Shared Folders -> Shares
  - Review each share for unnecessary or overly permissive shares.



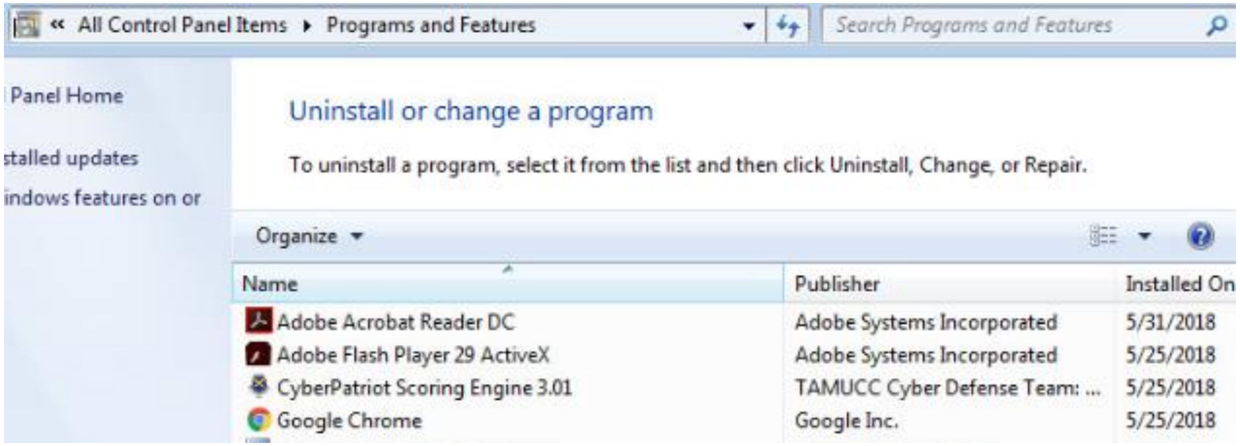
Console Root
- Computer Management (Local)
  - System Tools
    - Task Scheduler
    - Event Viewer
    - Shared Folders
      - Shares
      - Sessions

Share Name	Folder Path	Type	# Client Connections	Description
ADMIN$	C:\Windows	Windows	0	Remote Admin
Austins_K...	C:\Austins_Keylog...	Windows	0	
C$	C:\	Windows	0	Default share
Callums_D...	C:\Callums_DrWh...	Windows	0	
IPC$		Windows	1	Remote IPC
Jacobs_Bal...	C:\Jacobs_BallPit	Windows	0	

Patching – Application

Major software vendors release security patches and hot fixes to their products when security vulnerabilities are discovered. It is essential that these updates be applied in a timely manner to prevent unauthorized persons from exploiting identified vulnerabilities.[4]

- Click: Start -> Type: Features -> Open Programs and Features
  - Review the installed applications for prohibited or unnecessary items such as additional browsers or supporting applications.
  - Ideally, these programs are removed; otherwise, follow vendor guidance on application patching.


« All Control Panel Items ▸ Programs and Features
Search Programs and Features
Panel Home
stalled updates
indows features on or
Organize ▾

Uninstall or change a program

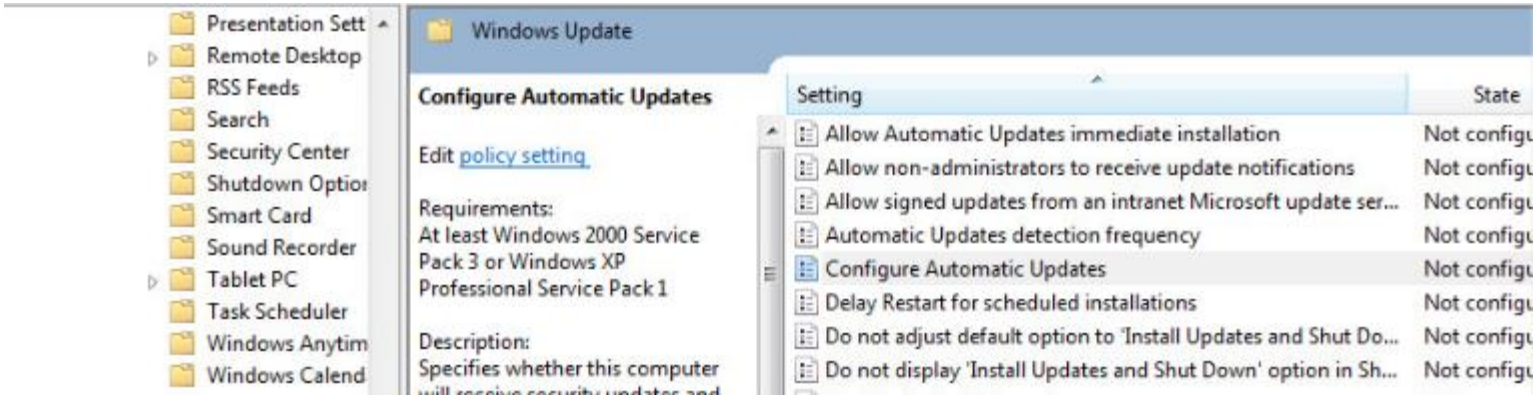
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On
Adobe Acrobat Reader DC	Adobe Systems Incorporated	5/31/2018
Adobe Flash Player 29 ActiveX	Adobe Systems Incorporated	5/25/2018
CyberPatriot Scoring Engine 3.01	TAMUCC Cyber Defense Team: ...	5/25/2018
Google Chrome	Google Inc.	5/25/2018

Patching – System

Major software vendors release security patches and hot fixes to their products when security vulnerabilities are discovered. It is essential that these updates be applied in a timely manner to prevent unauthorized persons from exploiting identified vulnerabilities.[4]

- Expand Local Computer Policy -> Computer Configuration -> Administrative Templates -> Windows Components -> Windows Update
  - Review the settings and Explanation tabs to configure an automated patch installation policy.



Configure Automatic Updates

Edit policy setting

Requirements:
At least Windows 2000 Service Pack 3 or Windows XP Professional Service Pack 1

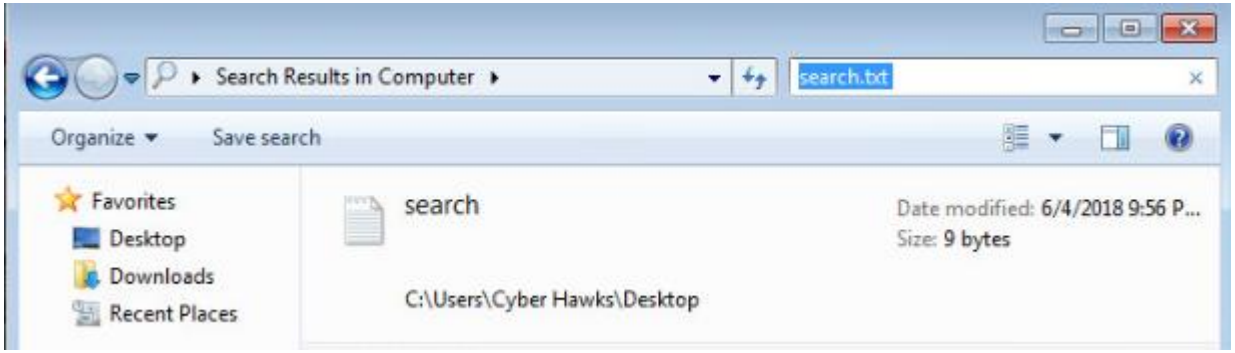
Description:
Specifies whether this computer

Setting	State
Allow Automatic Updates immediate installation	Not configu
Allow non-administrators to receive update notifications	Not configu
Allow signed updates from an intranet Microsoft update ser...	Not configu
Automatic Updates detection frequency	Not configu
Configure Automatic Updates	Not configu
Delay Restart for scheduled installations	Not configu
Do not adjust default option to 'Install Updates and Shut Do...	Not configu
Do not display 'Install Updates and Shut Down' option in Sh...	Not configu

Prohibited file identification

Quick file location methods can aide in incident response, support malicious file identification, and help locate prohibited files.

- Right Click: Desktop -> New (w) -> Text Document (t) -> Name: search.txt
- Open search.txt -> Type: CyberCamp -> Save (Ctrl+s) and Close the file (Alt+F4)
- On the Desktop -> Double click: Computer -> Type: “search.txt” in the Search Box

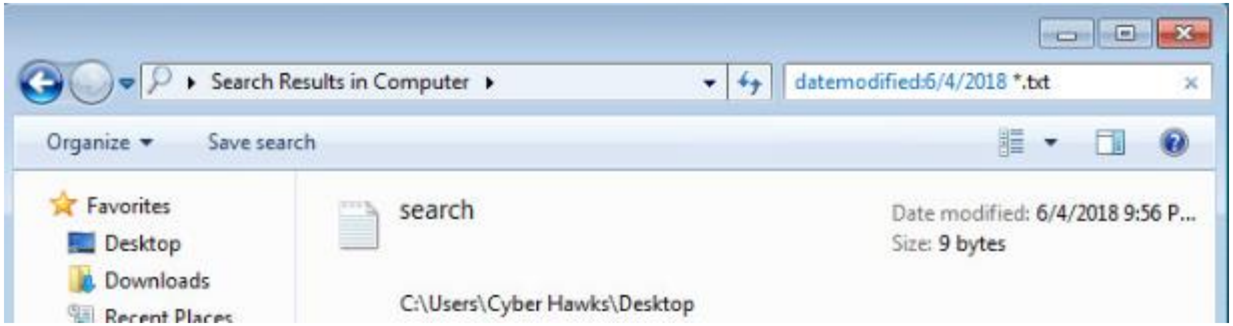


search
Date modified: 6/4/2018 9:56 P...
Size: 9 bytes
C:\Users\Cyber Hawks\Desktop

Prohibited file identification

Quick file location methods can aide in incident response, support malicious file identification, and help locate prohibited files.

- On the Desktop -> Double click: Computer -> Type: “datemodified: <today’s date> *.txt” in the Search Box



datemodified:6/4/2018 *.txt

search

Date modified: 6/4/2018 9:56 P...

Size: 9 bytes

C:\Users\Cyber Hawks\Desktop

References

1. CIS Critical Security Controls. SANS. Retrieved on June 4, 2018, from https://www.sans.org/security-resources/posters/20-critical-security-controls/55/download
2. NIST Special Publication 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations. Retrieved on June 4, 2018, from https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf
3. PCI DSS Prioritized Approach for PCI DSS 3.2. PCI Security Standards Council. Retrieved on June 4, 2018, from https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf
4. Windows 7 Security Technical Implementation Guide V1R30. DISA. Retrieved on June 4, 2018, from https://iase.disa.mil/stigs/sunset/Pages/index.aspx