MIS 5170

# Operating System Security

## Week 4

## Windows Configuration Management

Fox School of Business
TEMPLE UNIVERSITY®

# Tonight's Plan

- ❑ Questions from Last Week
- ❑ Review on-line posts
- ❑ In The News
- ❑ Configuration Management Practices
- ❑ Windows Group Policies
- ❑ Baselines
- ❑ Intrusion Detection/Prevention
- ❑ Assignment 2 Overview
- ❑ Next Week
- ❑ Quiz

# Questions From Last Week

- Any Questions from last week?
- Quiz; review via Blackboard.
- AH with IPSec; remember it only signs the packet between two computers, not the content
- Primary and Secondary storage
- Firewalls are a network device that controls which two computers and on which network ports they can communication. These are different from ports on a switch
- Switch; Protections for an OS

# Questions From Last Week (cont)

- Questions?

# Review On-Line Posts

- Top Posts
  - SMB Traffic 0-Day
    - http://www.securityweek.com/windows-smb-0-day-exposes-systems-attacks
  - SockPuppet

# Review On-Line Posts (cont)

- ❑ Questions?

# In the News

- IRS: Scam Blends CEO Fraud, W-2 Phising
  - Maybe the most un-patchable code base of our operating systems.
    - https://krebsonsecurity.com/2017/02/irs-scam-blends-ceo-fraud-w-2-phishing/
- SANS Reading Room
  - Dissect the Phish to Hunt Infections
    - https://www.sans.org/reading-room/whitepapers/awareness/dissect-phish-hunt-infections-37587
- Internet Storm Center
  - Patch Tuesday…? (Always changing)
    - https://isc.sans.edu/
    - https://isc.sans.edu/podcast.html
    - http://www.networkworld.com/article/3031653/security/microsoft-released-13-security-bulletins-for-feb-patch-tuesday-6-rated-critical.html

# In the News (cont)

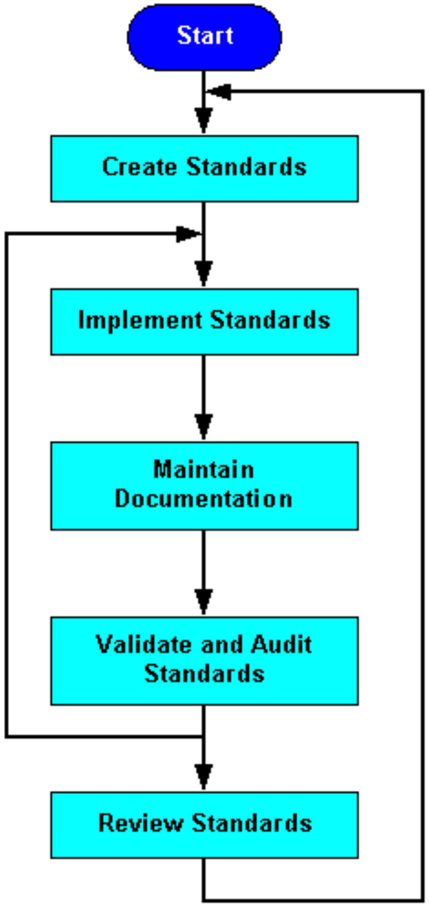
- Questions?

# Configuration Management Practices

- ❑ What is configuration Management?
- ❑ How can it help us?
- ❑ How can it secure an operating system?
- ❑ What are the steps?

# Configuration Management Practices (cont)

- What is configuration Management?
  - Configuration Management is a set of steps that creates and maintains consistency in our case of an operating system.
  - This can be a Baseline, which we will look at later tonight.
  - Can be as simple as a run-book, which is a set of documents that is followed when installing an operating system or application on top of said operating system.

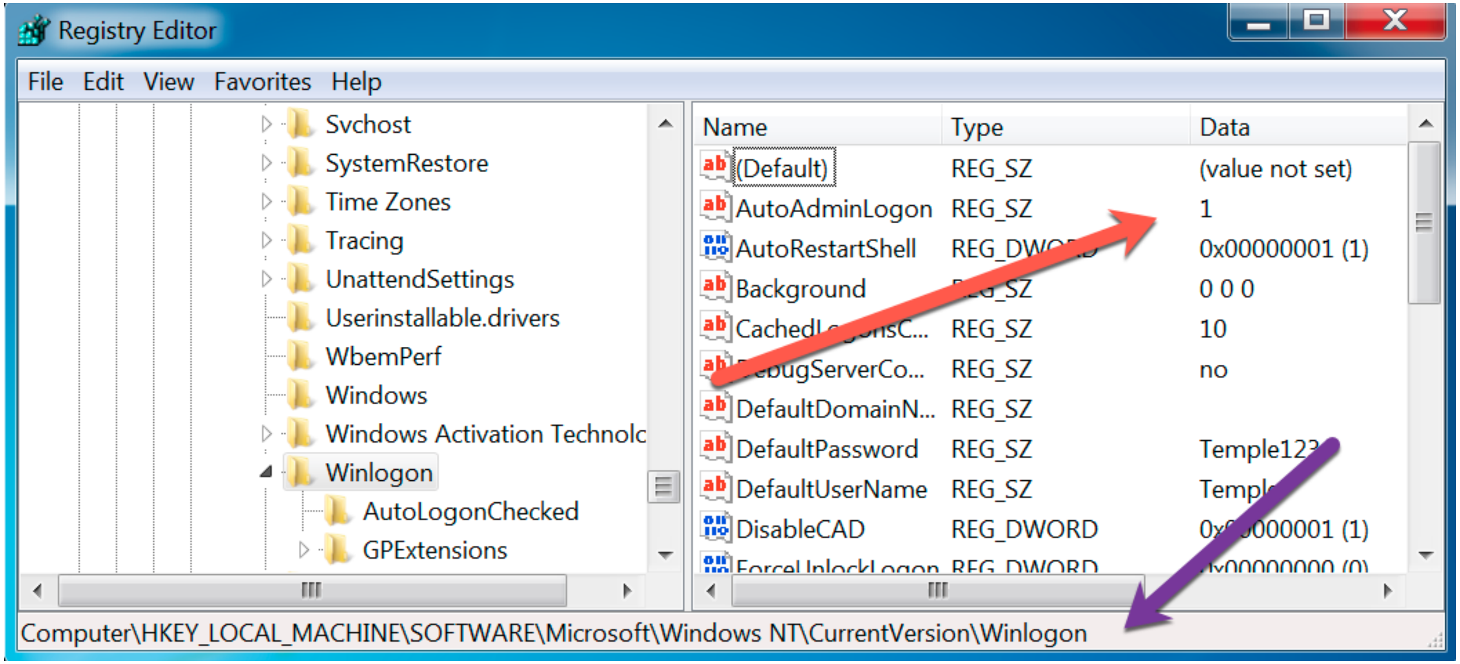


# Configuration Management Practices (cont)

- How can it help us?
  - This can help us to find deviation when we run a baseline difference scan.
    - Baseline Difference Scan = what has changed or is no longer equal to a setting we want to maintain
  - Tools like PowerShell Desired State Configuration
    - https://msdn.microsoft.com/en-us/PowerShell/dsc/overview
    - Download of PowerShell 5: https://www.microsoft.com/en-us/download/confirmation.aspx?id=50395
    - How to : https://msdn.microsoft.com/en-us/powershell/dsc/configurations#compiling-the-configuration

# Configuration Management Practices (cont)

- How can it secure an operating system?
  - Track things we don't want to ever see; and flag them as invalid values in areas we have seen last week.

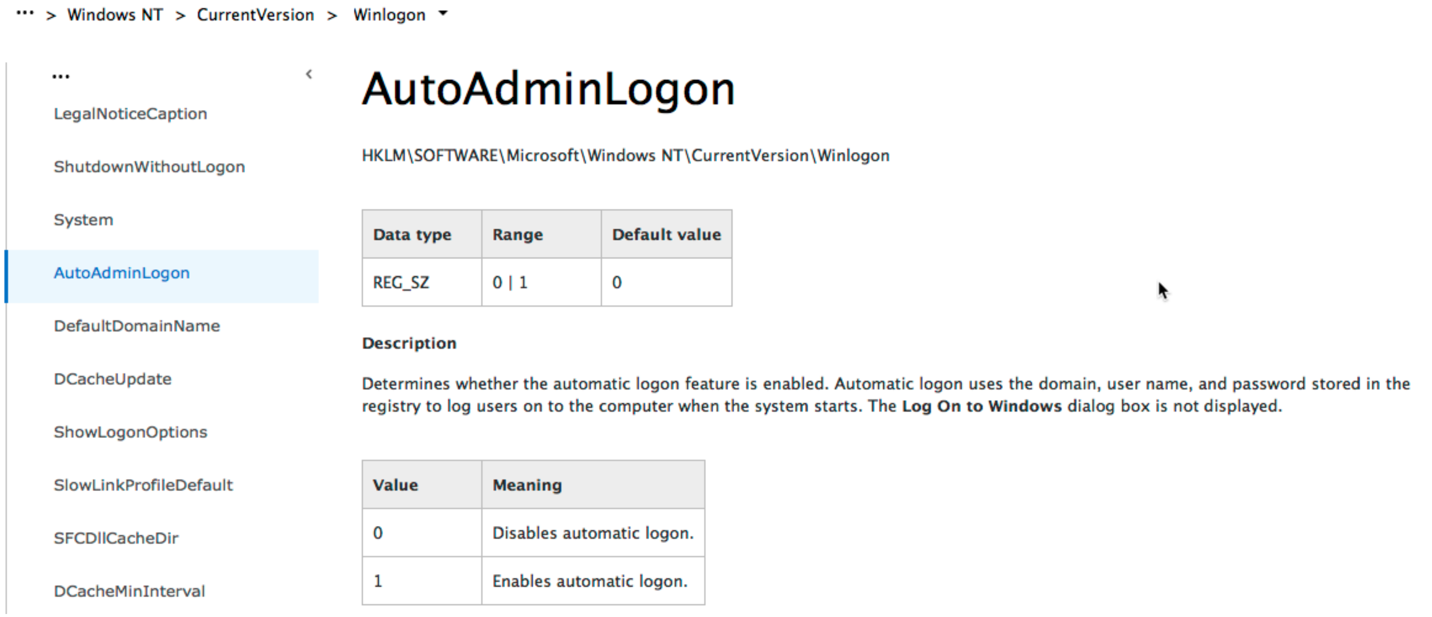


| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| AutoAdminLogon | REG_SZ | 1 |
| AutoRestartShell | REG_DWORD | 0x00000001 (1) |
| Background | REG_SZ | 0 0 0 |
| CachedLogonsC... | REG_SZ | 10 |
| DebugServerCo... | REG_SZ | no |
| DefaultDomainN... | REG_SZ | |
| DefaultPassword | REG_SZ | Temple123 |
| DefaultUserName | REG_SZ | Templ |
| DisableCAD | REG_DWORD | 0x00000001 (1) |
| ForceUnlockLogon | REG_DWORD | 0x00000000 (0) |

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

# Configuration Management Practices (cont)

- How can it secure an operating system? (cont)
  - By tracking and alerting for those settings that just should not be in the environment.
    - https://technet.microsoft.com/en-us/library/cc939702.aspx



## AutoAdminLogon

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

| Data type | Range | Default value |
|---|---|---|
| REG_SZ | 0 \| 1 | 0 |

**Description**

Determines whether the automatic logon feature is enabled. Automatic logon uses the domain, user name, and password stored in the registry to log users on to the computer when the system starts. The **Log On to Windows** dialog box is not displayed.

| Value | Meaning |
|---|---|
| 0 | Disables automatic logon. |
| 1 | Enables automatic logon. |

# Configuration Management Practices (cont)

- What are the steps?
  - Review company policies or best practices like:
    - CIS Windows 7 Security Baseline: On-Line
    - Windows 7 Baseline: On-Line
  - Create a run-book or use tools like PowerShell DSC (Desired State Configuration)
  - Create a script or an Image, similar to what we have done with our snap-shots
  - Use an Imaging utility or SCCM Deployment, VM VDIs, etc
  - Run a difference baseline to see if there is drift
    - If so chose set them back or alert on drift

# Configuration Management Practices (cont)

- Questions?

# Windows Group Policies

- What is it?
- How can it help us?
- How can it secure our operating system?
- How can it help improve efficiency?
- How can it hurt us?
- Demo

# Windows Group Policies (cont)

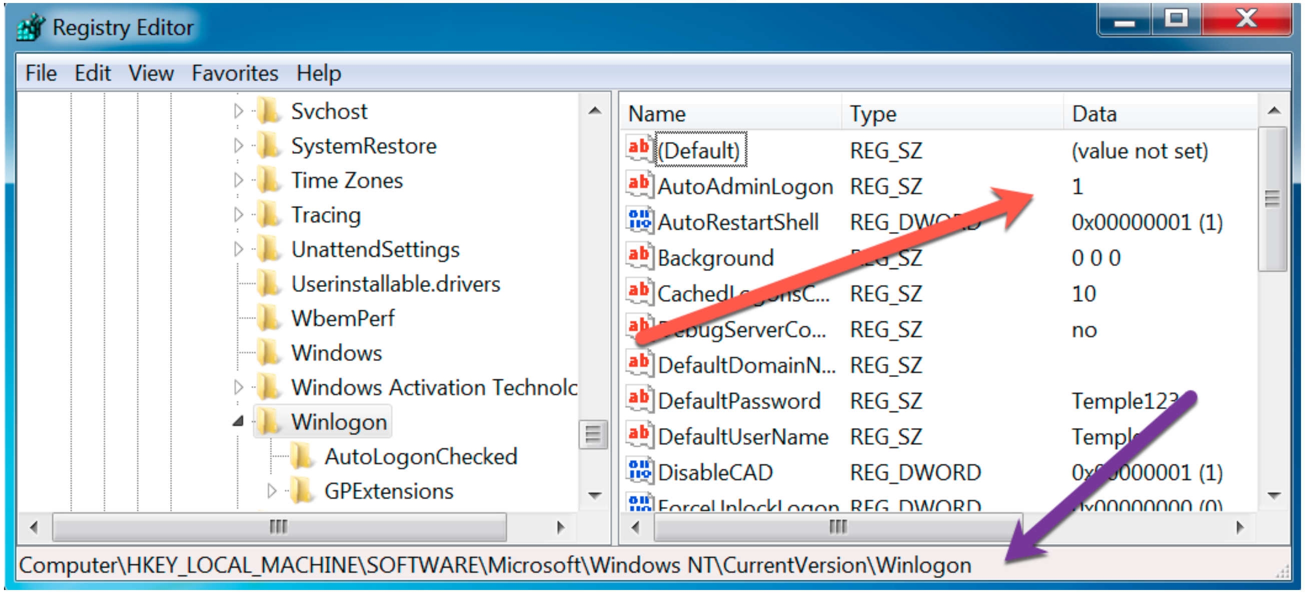
- What is it?
  - Windows Group Policy is a Microsoft answer to
    - Group Policy is the central component of the Change and Configuration Management features of the Microsoft® Windows® 2000 operating system.
      - https://msdn.microsoft.com/en-us/library/bb742376.aspx
  - A tool that allows you to better control and manage your Windows operating system.  We extensions even non-Windows computers can be managed and configured.

# Windows Group Policies (cont)

- How can it help us?
  - Create a set of settings or find a set of settings from a Baseline standard (I promise we will get to a baseline)
  - Use Group Policies to apply them to computers via Groups, OUs, etc.
  - Set the interval of refresh (Fancy term every 8 hours)
  - Enforce settings or start where they need to be
    - Preferences = where I should set them if they have never been set before.

# Windows Group Policies (cont)

- How can it secure our operating system?
  - This tool can help us keep settings like our example below from ever being an issue in our computing environment.
    - Apply to all our admins to always have this value = 0



| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| AutoAdminLogon | REG_SZ | 1 |
| AutoRestartShell | REG_DWORD | 0x00000001 (1) |
| Background | REG_SZ | 0 0 0 |
| CachedLogonsC... | REG_SZ | 10 |
| DebugServerCo... | REG_SZ | no |
| DefaultDomainN... | REG_SZ | |
| DefaultPassword | REG_SZ | Temple123 |
| DefaultUserName | REG_SZ | Templ |
| DisableCAD | REG_DWORD | 0x00000001 (1) |
| ForceUnlockLogon | REG_DWORD | 0x00000000 (0) |

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

# Windows Group Policies (cont)

- How can it help improve efficiency?
  - Once you have created these setting, you can apply them to all computer(s).  100s if not 1000s of computers.
  - Once you have them, you can change those settings in one place to update all you computer(s)
    - Create test policies for one of testing
    - Update main policy once individual testing has taken place
    - Move single computer to new testing OU to test changes.

# Windows Group Policies (cont)

- How can it hurt us?
  - You will be making the change to possibly all computers in your company at once if you are not careful.
  - Tattooing – No not the thing you hide on your arm or some place worse when you flew to Vegas and had to much to drink
    - A setting that is applied to a computer and can not be rolled-back by clearing that setting.
  - Delegation required might need you to limit who should and can do this operations

# Windows Group Policies (cont)

- Demo
  - https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/plan/delegating-administration-of-account-ous-and-resource-ous
  - http://www.howtogeek.com/howto/7553/remove-shutdown-and-restart-buttons-in-windows-7/

# Windows Group Policies (cont)

- Questions?

# Baselines

- What is a Baseline?
- How can this help us?
- What are some Baselines?
- Specific Details about Baselines.
- Demo

# Baselines (cont)

- What is a Baseline?
  - A Baseline is (aka Merriam-Webster) – information that is used as a starting point by which to compare other information.
    - Not very helpful?
    - For a computer the starting point is when you install it from an ISO.
  - Let us think of it as What we want a computer to allow it's users or process to be able to do or not do.  A minimum security model, 'Least Privileges' or where is that line in the sand?

# Baselines (cont)

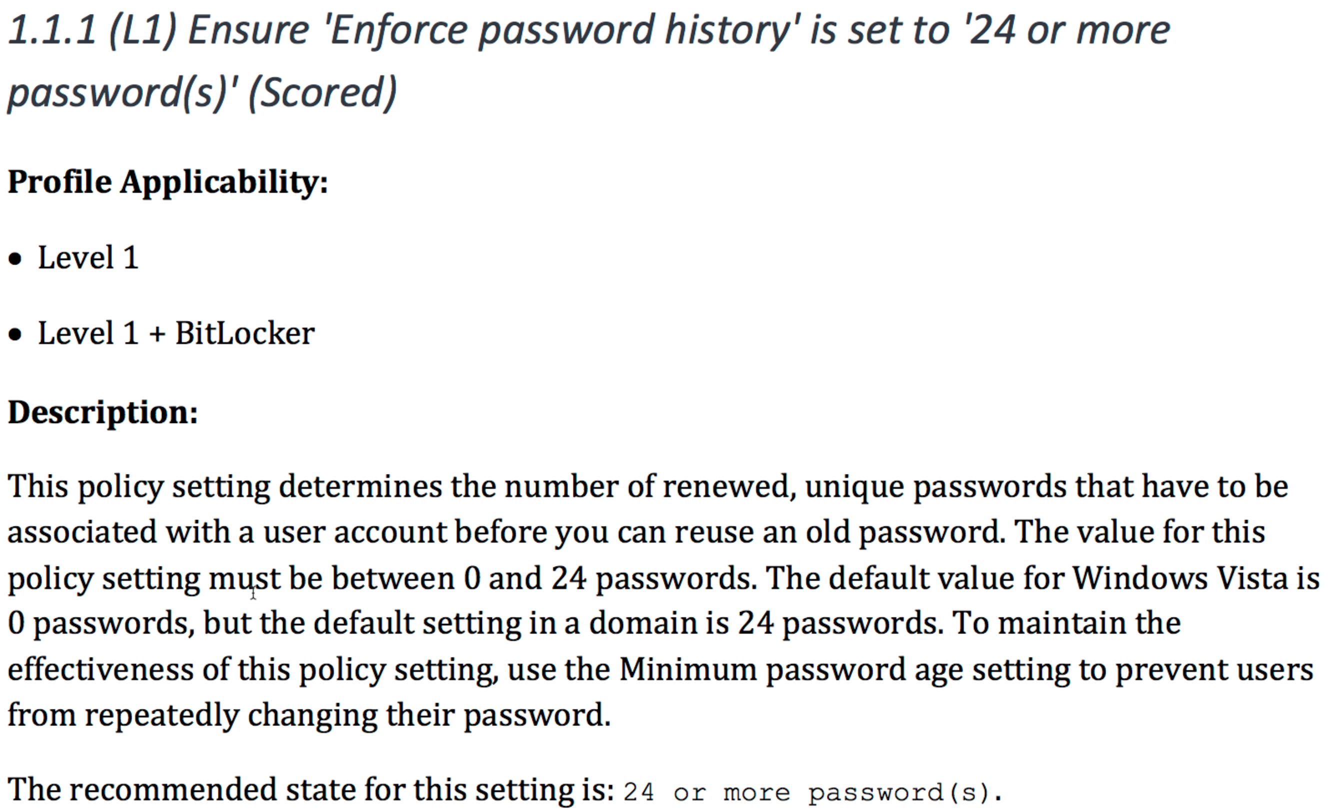
- How can this help us?
  - This can help us trigger that something is wrong or someone is trying to make something go wrong.
  - Should we write a vulnerability (Possibly known as a ‘Risk’) against the delta or is it an exception we should track
  - Should we tighten up from detective to preventative?
- These are some questions that could help frame the specifics of what we find.

# Baselines (cont)

- What are some Baselines?
  - NIST – National Institute of Standards and Technology
    - https://usgcb.nist.gov/usgcb/microsoft/download_win7.html
  - CIS Benchmark – Center for Internet Security.
    - http://community.mis.temple.edu/mis5170sec001sp2017/files/2017/02/CIS_Microsoft_Windows_7_Benchmark_v3.0.0.pdf
  - ISO 27002 – Information security standard published by the International Organization for Standardization.
  - ISF – Information Security Forum.
    - https://www.securityforum.org/consultancy/information-security-readiness-benchmark/

# Baselines (cont)

- Specific Details about Baselines.



*1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (Scored)*

**Profile Applicability:**

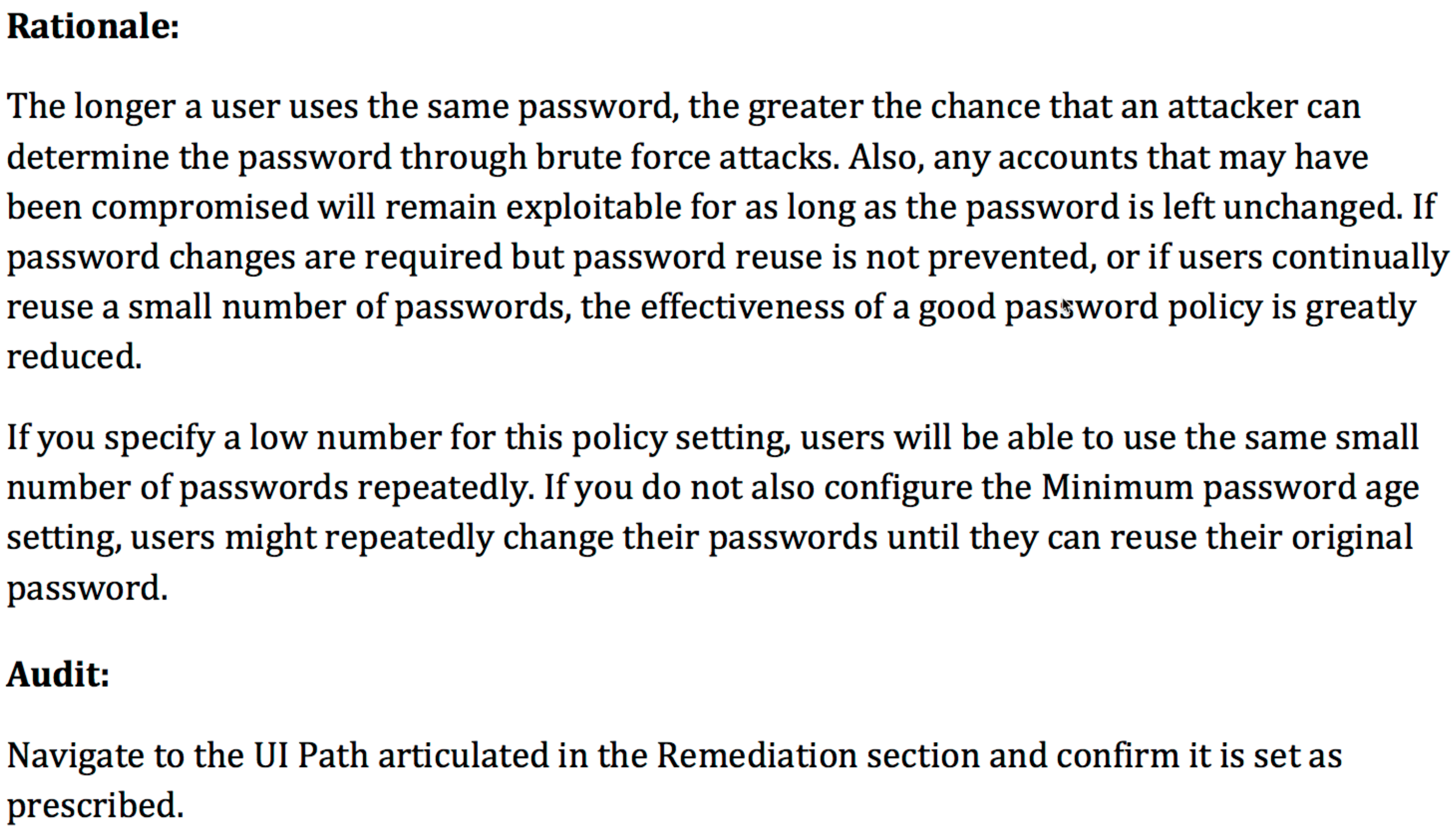
- Level 1
- Level 1 + BitLocker

**Description:**

This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for Windows Vista is 0 passwords, but the default setting in a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password.

The recommended state for this setting is: `24 or more password(s)`.

# Baselines (cont)



**Rationale:**

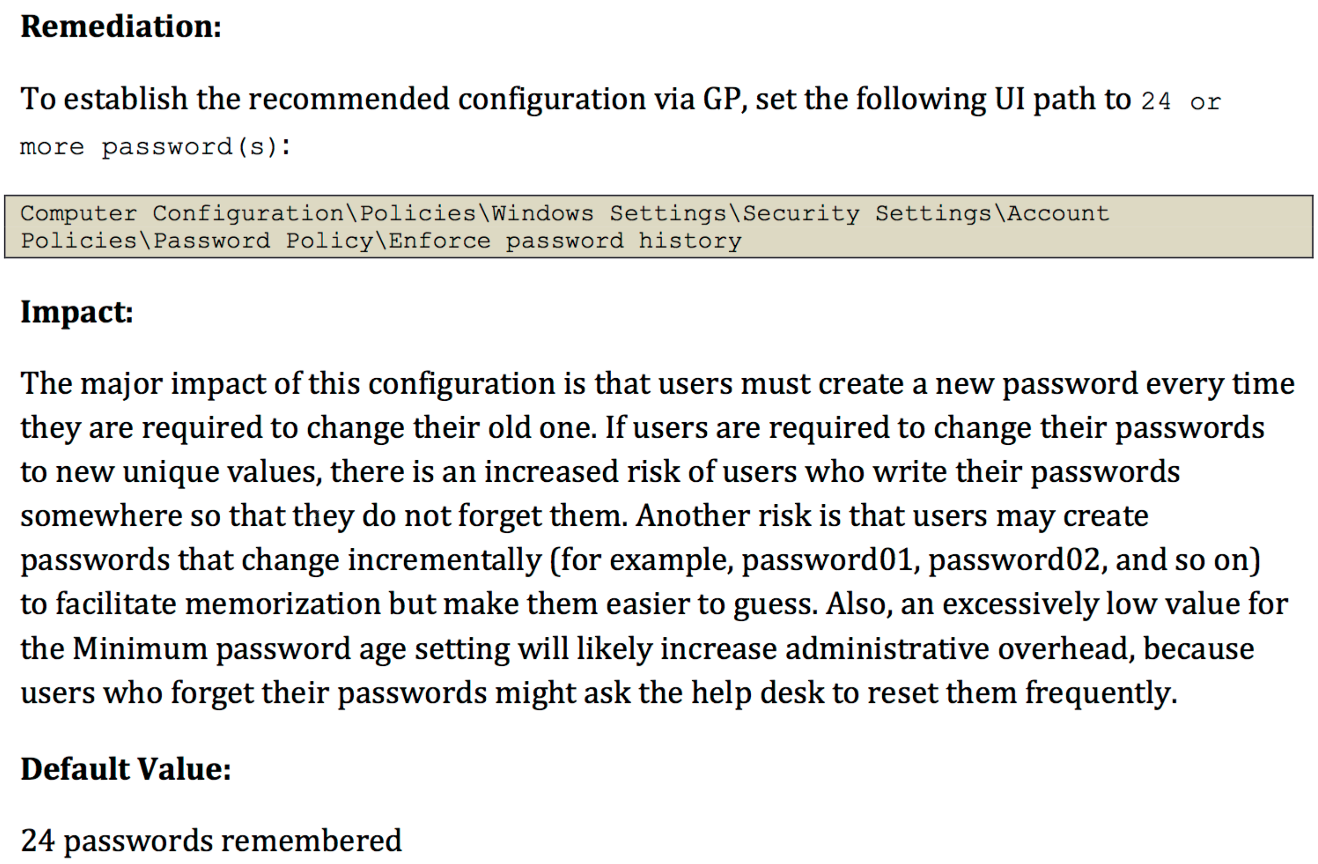
The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced.

If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, users might repeatedly change their passwords until they can reuse their original password.

**Audit:**

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

# Baselines (cont)



**Remediation:**

To establish the recommended configuration via GP, set the following UI path to `24 or more password(s)`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account
Policies\Password Policy\Enforce password history
```

**Impact:**

The major impact of this configuration is that users must create a new password every time they are required to change their old one. If users are required to change their passwords to new unique values, there is an increased risk of users who write their passwords somewhere so that they do not forget them. Another risk is that users may create passwords that change incrementally (for example, password01, password02, and so on) to facilitate memorization but make them easier to guess. Also, an excessively low value for the Minimum password age setting will likely increase administrative overhead, because users who forget their passwords might ask the help desk to reset them frequently.

**Default Value:**

24 passwords remembered

# Baselines (cont)

- Demo

# Baselines (cont)

- Questions?

# Intrusion Detection

- A

# Intrusion Detection (cont)

- Questions?

# Intrusion Prevention

- A

# Intrusion Prevention (cont)

- Questions?

# Assignment 2 Overview

- Requirements – a presentation style document and video to C-Level team on your choices and justification
  - Build a video of what you did with justification.
  - 8 – 10 page power point on the teams recommendation for the baselines items being implemented
  - Create a Windows 2008 Domain Controller a type 2 hypervisor.
  - Create a Windows 7 box connected to the Domain.
  - Apply the settings from your baseline via  a Group Policy to the Windows 7 box.
- Due Date: Feb 22nd

# Next Week

- Questions from previous week
- Patching
  - Native Patching Tools
  - Third-Party
- Vulnerability Scanning and Remediation
- Free Group Working Sessions
- Questions about Assignment 2 (Due Feb 22nd)

# Quiz

- We can start the Quiz