WINDOWS OPERATING SYSTEMS SECURITY TECHNICAL IMPLEMENTATION GUIDES (STIGs) OVERVIEW

Version 1, Release 4

22 April 2016

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. INTRODUCTION

1.1 Executive Summary

The Windows Operating Systems Security Technical Implementation Guides (STIGs) are published as tools to improve the security of Department of Defense (DoD) information systems. The requirements were developed from DoD consensus, as well as Windows security guidance by Microsoft Corporation.

The Windows OS STIGs are produced by major versions. Workstation versions such as Windows Vista, 7, 8, and 10 support standard desktops as well as mobile devices such as laptops and tablets. Server versions such as Windows Server 2008, 2008 R2, and 2012/2012 R2 are produced to support member server and domain controller configurations. Active Directory Domain and Forest STIGs address requirements at those levels in Active Directory environments.

These STIGs are meant for use in conjunction with other applicable STIGs including, but not limited to, such topics as, Browsers, Antivirus, Web Services, Database, and Domain Name Services (DNS), depending on products installed or configured on a system.

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provide an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will, **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.mil/.

1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.6 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configurations settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system’s particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100% secure.

1.7 Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect vendor's proprietary information.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

2. ASSESSMENT CONSIDERATIONS

2.1 Windows Interfaces

Prior to Windows 8 and Server 2012, the standard Windows interface was the Desktop, which included a menu for launching applications and tools. The standard interface has changed several times since then with each version of Windows. The menu available in earlier versions of Windows has been replaced with a Start Screen or revised versions of the menu. Server Manager in later versions of Windows Server editions includes a tools menu for quick access to management tools.

With the navigation of systems changed, a helpful keyboard shortcut from the Desktop is the Windows key + x, which brings up a quick menu of management tools.

2.2 Updating Systems to Display "MSS" Settings

2.2.1 Updating the Windows Security Options File

Some of the requirements in this STIG depend on the use of a Microsoft security options file (sceregvl.inf) that has been updated to include additional security settings identified with “MSS” that are not visible in policies by default. An updated copy of the security options file is included with the Windows STIGs. (The Windows 10 STIG does not use the updated security options file, see the next section.)

To load the updated Security Options file, complete the following (due to changes in Windows security, the administrator must first take ownership of the file before changes are made):

- Open a command prompt with elevated privileges
- Take ownership of the file with the command ‘takeown /f c:\windows\inf\sceregvl.inf’
- Add Full permissions with the command ‘icacls c:\windows\inf\sceregvl.inf /grant username:f’ where ‘username’ is the administrator account
- Rename the sceregvl.inf file in the %WinDir%\inf directory
- Copy the updated sceregvl.inf file from the media provided to the %WinDir%\inf directory
  - File can be found in the Templates directory included in the STIG zip file
- Re-register scecli.dll by executing ‘regsvr32 scecli.dll’ in the command prompt with elevated privileges

The additional options will now appear in Windows policy tools, such as the Group Policy Editor (a restart of the tool may be required).

2.2.2 MSS-Legacy Custom Administrative Templates

The Windows 10 STIG replaced the security options file update (sceregvl.inf) with custom administrative template files (.admx and .adml file types) as the method for configuring the

"MSS" settings. This is an easier update and has the benefit of not changing the permissions on a system file.

The custom administrative template files are provided in the Templates directory of the STIG package.

The MSS-legacy.admx file must be copied to the \Windows\PolicyDefinitions\ directory.
The MSS-legacy.adml file must be copied to the \Windows\PolicyDefinitions\en-US\ directory.

The MSS-Legacy administrative template files provided with the Windows 10 STIG can be used on previous versions of Windows. They will update the same registry items specified in the requirements. However the configuration settings in group policy will be located under "Computer Configuration >> Administrative Templates >> MSS (Legacy)" instead of "Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options". Also, verification must be done with the registry values as the settings will not show in the “Security Configuration and Analysis” tool if the security options file is not updated.

2.3 Performing Analysis with the Security Configuration and Analysis Snap-In

The Security Analysis and Configuration tool compares the effective systems settings to a security template which is configured with STIG requirements. The tool is identified in the Checks section for the individual STIG requirements that can be analyzed using it. The security templates are provided with the STIG zip file in a Templates directory. They are intended for analysis only and can have unknown impacts if used to configure a system without adequate testing. (This method of verification is no longer provided as the Windows Server 2012 STIG. Alternate methods such as registry checks are used instead of providing a security template.)

To load the Security Configuration and Analysis snap-in and analyze the system, perform the following steps:

- Select “Start”
- Enter “MMC” in the “Search programs and files” field and Enter
- Select “File” from the “MMC” menu bar
- Select “Add/Remove snap-in” from the drop-down menu
- Select the “Security Configuration and Analysis” snap-in and click the “Add” button
- Select “OK”
- Right-click on the “Security Configuration and Analysis” object in the left window
- Select “Open Database” (this will create the database file if one does not exist)
- Enter a name and path for the database file (e.g., “C:\temp\scan\srr.sdb”)
  - The path entered must exist prior to this step
- Select “Open”
- If this was a new database file, a new window will open looking for a template to import. If an existing database file was used, right click on “Security Configuration and Analysis” in the left pane and select “Import Policy”

- In the “Import Template” window select the appropriate file name for the type of system
  - The security templates can be found in the Templates directory included in the STIG zip file
  - U_WinVersion_Analyze_Only.inf
- Check the box to “Clear the database before importing”
- Select “Open”
- Right-click on the “Security Configuration and Analysis” object in the left window
- Select “Analyze Computer Now…” (Important: DO NOT select “Configure Computer Now…”, this will import the settings in the “Analyze_Only” template to the system’s local policy and cannot be undone automatically)
- Enter a name and path for the log file (e.g., “C:\temp\scan\srr.log”)
- Select “OK”
- “Analyzing System Security” windows will appear
- When the analysis is complete, the “Security Configuration and Analysis” node can be expanded to view current configurations
  - “Database Settings” are the required settings imported from the analysis template file
  - “Computer Settings” are the effective settings on the system
  - Settings with a green check indicate the Database and Computer settings match
  - Settings with a red x indicate the Database and Computer settings do not match

2.4 Configuration and Verification

The use of Local or Group policies is the preferred method of configuring Windows STIG requirements where applicable. The policy settings are provided in the Fix Text of the requirements. In an Active Directory environment, Group and Local policies must be applied appropriately to ensure the effective settings support STIG requirements.

The verification of many of these requirements is done in the registry with the specifics provided in the Check Content section. This aligns with verification methods used by automated tools for these requirements.

2.5 Group Policy Effective Settings

In an Active Directory environment, effective settings can come from a number of sources including Local Computer Policy, and Group Policies that may be linked at various levels such as Sites, Domains, or Organizational Units. Several utilities are available to help administrators determine the source of the effective security configuration settings that are in force on a system.

The Resultant Set of Policy (RSoP) MMC Snap-in and GPResult.exe will report the source policy for security settings that are enforced on the system. This will allow an Administrator to determine which policy must be changed to fix a specific setting that is the cause or a finding on the system. (These tools do not report if a setting is configured in the Local Policy.)

The Group Policy Management Console (GPMC) MMC Snap-in is another tool that combines the features of the RSOP and Group Policy Object Editor.

Refer to system or Microsoft documentation for details on the use of these tools.

2.6 DumpSec

The DumpSec application is an analysis tool that permits the user to systematically review ACL, audit, and user information from the local system. This tool is not included with Windows, but may be acquired or downloaded from SystemTools Software, Inc. (www.systemtools.com). It is also available on the IASE website under Windows Support Files at http://iase.disa.mil/stigs/os/windows/support_files.html.

The data from DumpSec can be copied to another program, such as a spreadsheet, for analysis by selecting “Copy all items” from the Edit menu and pasting in to the other program.

2.7 Requirements with Potential Compatibility Issues

Some settings in the STIGs have been noted by Microsoft as potential issues. If the environment is a mixed one, the following requirements should be reviewed. Variations between systems in configuration of these settings may cause compatibility issues.

These are located in group policy under Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options. (Identifiers have changed between STIGs, search for the policy name listed for additional information.)

Domain Member: Digitally encrypt or sign secure channel data (always)
Domain Member: Digitally encrypt secure channel data (when possible)
Domain Member: Require Strong (Windows 2000 or Later) Session Key
Microsoft Network Client: Digitally sign communications (always)
Microsoft Network Server: Digitally sign communications (always)
Network access: Do not allow anonymous enumeration of SAM accounts
Network access: Do not allow anonymous enumeration of SAM accounts and shares
Network access: Let everyone permissions apply to anonymous users
Network security: Do not store LAN Manager hash value on next password change
Network security: LAN Manager authentication level
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 Server Core and Minimal GUI Installations

Windows Servers, starting with 2008, have installation options which can reduce the footprint of the system, potentially reducing the attack profile. The STIG requirements are applicable to all installation versions unless otherwise noted.

The Windows "Server with a GUI" (graphical user interface) installation option provides the standard interfaces for interacting with the system.

The "Server Core Installation" option provides a minimal installation. The standard GUI interfaces are not available with a few exceptions. Interacting with the system when logged on locally is done through a command line environment. Server Core installations may also be managed remotely from another system with many of the standard GUI interfaces. Not all server roles are supported in Server Core installations.

Windows Server 2012 added another option called the "Minimal Server Interface", where the Server Graphical Shell is removed from a Server with a GUI installation. This is an intermediate state with some GUI interfaces are still available, such as, Microsoft Management Console (MMC) and a subset of Control Panel.

3.2 Active Directory Introduction

Active Directory Domain Services (AD DS) is the central location for configuration information, authentication requests, and information about all the objects that are stored within the forest. AD manages communication between users and domains, including user logon processes, authentication, and directory searches. Using AD, administrators can efficiently manage users, computers, groups, printers, applications, and other directory-enabled objects from one secure, centralized location. A domain controller is a server that is running AD DS.

AD also facilitates centralized role-based management, so administrators can assign policies, deploy software, and apply critical updates to an organization's endpoint systems and applications. Although AD stores information and settings in a central database, the product supports networks from small installations with a few users and resources (e.g., computers, printers, servers, and applications) to tens of thousands of users and resources. Larger implementations can be organized using multiple domains, server farms, and can span geographic locations.

3.2.1 Architectural Considerations

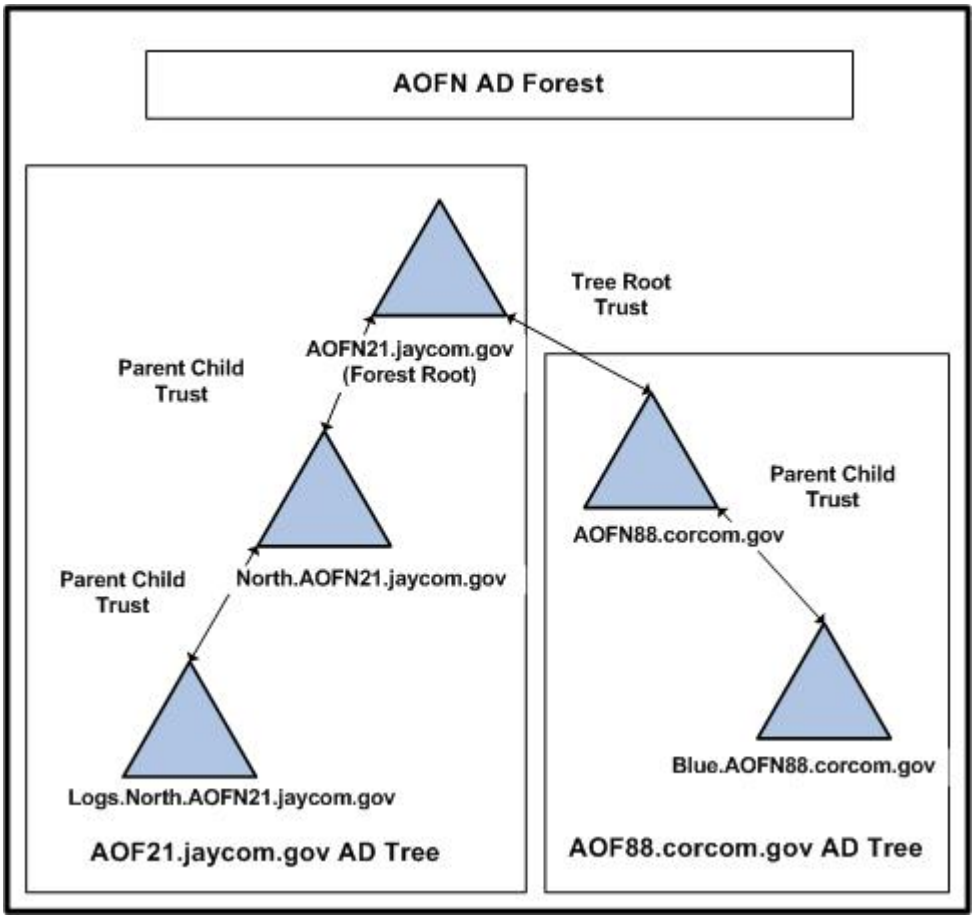
The decisions made during the design and implementation phase of the domain and forest have a major impact on the ability to isolate and secure the user, endpoint clients, and other domain resources. The type and characteristics of manually-defined trusts, as an implementation of cross-directory authentication, also has a significant impact. The resulting directory services

environment affects account and resource definition, user authentication, and resource access control.

Domains, trees, and forests are key terms used to describe hierarchical elements in AD architecture. The following illustrates a relatively simple forest implementation.

Note: Domain and forest names used throughout this document are fictitious.

Figure 3-1: Sample AD Forest



Keep in mind the following architectural considerations:

- Automatic trust exists between the parent/child domains and the root domain; they share a common naming context that maps to their names used in the DNS database
- Account is defined in only one domain in a forest, but can be used anywhere in the same forest (that resource access permissions permit) because of the automatic trust relationships between domains
- Security settings that can be managed through Group Policy are implemented at the domain level; if the same policy is desired for multiple domains, it must be copied between them

- Forest root domain is said to be an "empty" domain if it contains only the accounts used to administer that domain and forest
- Concept of resource and account domains can be used to partition user definitions from the resources they access; in this model, user accounts are defined in one domain, known as the account domain
  - Resources, such as email servers, web servers, database servers, and application servers, are defined in one or more domains known as resource domains

3.2.2 Security Considerations

The AD elements are impacted by the forest, tree, and domain architecture and have security considerations including the following:

- After a user is authenticated in his native domain, they do not have to be authenticated again to access resources in another domain in the forest
  - This is the effect of the automatic trusts between domains
  - This provides a kind of single sign-on capability
- In cases where cross-domain resource access is common, placement and security of a forest root domain controller can have a significant impact on the authorization process
- Implementation of an empty root domain allows stronger security policies to be defined for the sensitive accounts in that domain
  - Allows fewer accounts to be defined there, including privileged accounts that might otherwise be needed to support applications
  - Domain with fewer applications presents a smaller target that might be attacked
- Where network perimeter protections include Demilitarized Zone (DMZ) architecture, the strongest security is obtained by the use of a separate forest for the hosts in that DMZ
  - Allows fewer network ports to be open because replication traffic is eliminated
  - Eliminates the exposure of some information that would otherwise be replicated from the domain controllers on the protected side of the network

3.2.3 Replication

Replication is the mechanism by which AD data is synchronized among the domain controllers. Some AD data is duplicated on every domain controller in the forest and some AD data is exclusive to all the domain controllers within a single domain. In addition to the Windows directory data held in AD, the settings and information captured for and used by the Group Policy feature are also considered AD data. Other applications, most notably the Microsoft Exchange and Systems Management Server products, utilize AD for storage of their directory-enabled application data.

3.2.4 Site Definitions

When Windows hosts in an AD forest are distributed across a geographical area connected by network links not operating at (or close to) Local Area Network (LAN) speeds, it is common to define AD sites. AD site definitions typically mirror physical network boundaries.

Although site definitions are most directly related to network architecture, there are security considerations that must be addressed, such as:

- When sites are defined, it is also necessary to define site links
  - Site links have properties related to AD replication
  - Correctly configured properties ensure replication occurs on a timely basis so distributed AD security data is kept current
- AD site is one level at which Group Policy can be applied
- When an AD client is logging on to a domain, it attempts to locate a domain controller within the same AD site; a proper site configuration enhances availability and reduces network traffic

3.2.5 Deployment in the Perimeter Network (RODC in the DMZ)

Installation of a fully trusted active directory network into a DMZ or across enclave boundaries substantially increases the network's vulnerability.

Microsoft has provided guidance on use of read-only domain controllers (RODC) in the DMZ (http://technet.microsoft.com/en-us/library/dd728028(WS.10).aspx). Communications between the DMZ and the AD forest or domain on the trusted network are cross security boundaries. Directory Services traffic that cross security boundaries must be protected by an encrypted VPN and services and ports must be registered.

RODC is considered part of the site's forest or domain installation since it is not a standalone product, but rather a role. Configuration of the VPN and IPSec must comply with Network Infrastructure guidance. IPSec and block mode must be enabled to prevent transmission of unencrypted traffic during machine boot-up. IPSec and other communications and security configurations for the management and replication of the RODC will be managed by use of the minimum required Group Policy Objects (GPOs).

3.2.6 FSMO Roles

Because AD data is distributed among the domain controllers in a domain, the design of AD includes mechanisms to manage updates from multiple domain controllers. While the design does accommodate updates from multiple sources through the process of multi-master replication, there were some instances in which data integrity required a single-threaded approach. The resolution to this requirement is the implementation of Flexible Single Master Operations (FSMO) roles. Please note that FSMO roles are also referred to as operations master roles.

FSMO roles represent specific AD management responsibilities held by assigned domain controllers. Two of the roles apply at the forest level and three at the domain level. AD elements, such as AD database schema definitions and certain namespace controls, must be managed at the forest level. AD elements, such as security identifier (SID) assignment, are managed at the

domain level. Please note that the subject of FSMO roles is complex and should be thoroughly reviewed in the Microsoft documentation.

The following table summarizes the FSMO roles and lists some of the functions each performs.

Table 3-1: Flexible Single Master Operations Roles

Scope	Role Name	Functions
Forest	Domain Naming Master	Controls the addition or removal of domains.
	Schema Master	Controls updates to the AD database schema.
Domain	Primary Domain Controller (PDC) Emulator	Provides a source for time synchronization throughout the domain. At the forest root domain PDC Emulator, provides an authoritative time source for the entire forest. Receives preferential password and account lockout updates from other domain controllers and resolves authentication failures due to changed passwords. Propagates password changes from down-level clients to other domain controllers. Periodically checks and resets ACLs on accounts in certain privileged groups.
	Relative Identifier (RID) Master	Maintains the RID pool assignments used when a domain controller creates a SID for a new account.
	Infrastructure Master	Checks references to objects in other domains in the forest, using a Global Catalog (GC) server, and maintains the references as changes occur.

The AD security considerations for FSMO roles include:

- The availability of the FSMO role holders is directly related to the availability of resources within domains
  - In some cases, an outage of a FSMO role holder can cause an immediate loss of client access to resources
  - In other cases, the loss will eventually result in the inability to make changes to AD objects
- The integrity of the AD database is directly related to the integrity of the Schema Master role holder; while some products, such as Microsoft Exchange and Systems Management Server, require updates at installation time, there is no need for routine schema updates and any changes should be very carefully considered
- The Infrastructure Master role is only relevant in forests of more than one domain; also, placing this role on a domain controller that is also a GC server impedes its function

3.3 Windows Auditing

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect

attacks. The Windows STIGs define a minimum set of auditing to be configured. Audit settings beyond those required in the STIGs can be enabled to meet an organization's needs.

Some audit settings such as object access auditing, produce excessive events when enabled in an ongoing basis and are not included in the STIGs. Object access auditing can be enabled to monitor sensitive data or for specific debugging and investigative needs.

4. PASS-THE-HASH (PTH) ATTACKS AND CREDENTIAL THEFTS

A number of requirements are included in the Windows STIGs to help prevent the compromise of credentials that could be used in a PtH attack. Through lateral movements and privilege escalations an attacker can very quickly completely compromise a domain with PtH techniques. The requirements include separation of administrative privileges based on the systems they are supporting and restricting administrative access based on this separation.

Microsoft has released papers, Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques, Version 1 and 2, that details the issue and provides various mitigations. The papers can be downloaded from Microsoft at:

http://www.microsoft.com/en-us/download/details.aspx?id=36036.

NSA has also published Pass-the-Hash related papers, "Spotting the Adversary with Windows Event Log Monitoring" and "Reducing the effectiveness of Pass-the-Hash", available under the Microsoft Windows Applications section at:

https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml.

5. ENHANCED MITIGATION EXPERIENCE TOOLKIT (EMET)

The Enhanced Mitigation Experience Toolkit is an add-on available from Microsoft which allows the configuration of several security mechanisms at the system level and for applications, providing additional levels of protection. These include Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), and Structured Exception Handler Overwrite Protection (SEHOP), as well as other mitigations.

The requirements for EMET included configurations using Administrative Template settings. The EMET related Administrative Template files must be copied from the installation directory (EMET\Deployment\Group Policy Files) to the system's Policy Definitions directory to provide access to these settings.

Copy "EMET.admx" to the %WinDir%\PolicyDefinitions directory.

Copy "EMET.adml" to the %WinDir%\PolicyDefinitions\en-US directory (assumes US English language version).

See the "EMET User's Guide", included with the installation, for additional information regarding the tool.

6. APPLOCKER - APPLICATION WHITELISTING

AppLocker is a whitelisting application available in Enterprise client versions of Windows 7 and later, as well as server versions, Windows 2008 R2 and later.

A deny by default implementation is initiated by enabling any AppLocker rules within a category. AppLocker rules are established for Executables, Windows Installer, Scripts, Packaged apps (Windows Store/Universal apps), and DLLs. AppLocker includes the capability to automatically define several default rules to ensure executables and DLLs required by the system are allowed. It can also scan a system for installed applications to automatically create rules for those.

NSA has published a guide for implementing AppLocker, "Application Whitelisting using Microsoft AppLocker". Specific configuration guidance is provided for establishing rules for Executables, Windows Installer, Scripts, and DLLs based on executable paths. This allows applications from well-known locations as well as blocking some areas malware may use. This is generally sufficient for a baseline configuration, though more restrictive rules may also be used.

General guidance is included for Packaged app rules for systems that include Windows Store/Universal apps. Care must be taken when creating rules for Packaged apps as some system related items are also in this form.

The NSA guidance is available under the Microsoft Windows Applications section of the following link:

www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml.

7. LOCAL ADMINISTRATOR PASSWORD SOLUTION (LAPS)

Local administrator accounts on domain-joined systems are not frequently used and may go unmonitored and without regular password updates. They can also be difficult to manually manage to ensure passwords are unique between systems. These accounts are regularly targeted by attackers looking for accounts that once compromised, can be used to move laterally between systems until more highly privileged domain accounts are found and compromised.

Microsoft's Local Administrator Password Solution (LAPS) provides an automated solution for maintaining and regularly changing the local administrator password for domain-joined systems.

LAPS requires a schema update to the domain which adds attributes to the computer objects in Active Directory for storing the local administrator passwords and expiration dates. It is enabled and managed with group policy as well as Client Side Extensions (CSE) installed on each of the managed systems.

LAPS can only manage a single local administrator account on a system. Due to this, only a single active local administrator account must exist on domain joined systems. By default LAPS will manage the built-in Administrator account. This would be acceptable for servers where it remains active. This account is disabled by default (and per STIG requirements) on workstations. Another single local administrator account with a standardized name must be defined on workstations for LAPS to manage (this can be done per Organizational Unit).

The passwords are stored in attributes of the computer object in Active Directory. This information is accessible to Domain Admins as well as potentially other accounts or groups that have been delegated permission to the OU and attributes. This access must be restricted to accounts that absolutely require it. Due to the potential for access to the passwords, this must be actively monitored.

Microsoft Security Advisory 3062591 provides summary information and links for the LAPS tool and documentation at:

https://technet.microsoft.com/en-us/library/security/3062591.aspx

8. REFERENCES

Microsoft, "Mitigating Pass-the-Hash (PtH) Attacks and other Credential Theft Techniques", Version 1.1, 12 June 2013

Microsoft, "Mitigating Pass-the-Hash and Other Credential Theft, version 2", 7 July 2014

National Security Agency (NSA), "Reducing the Effectiveness of Pass-the-Hash", Revision 1, 19 November 2013

National Security Agency (NSA), "Spotting the Adversary with Windows Event Log Monitoring", Revision 2, 16 December 2013

Microsoft, "Enhanced Mitigation Experience Toolkit User Guide" versions and dates based on version of EMET.

National Security Agency (NSA), "Application Whitelisting using Microsoft AppLocker", August 2014