Audit, Mitigation M1047 - Enterprise

Archived: 2026-04-05 16:06:34 UTC

Enterprise T1548 Abuse Elevation Control Mechanism

Check for common UAC bypass weaknesses on Windows systems to be aware of the risk posture and address issues where appropriate.[1]

.002 Bypass User Account Control

Check for common UAC bypass weaknesses on Windows systems to be aware of the risk posture and address issues where appropriate.[1]

.006 TCC Manipulation

Routinely check applications using Automation under Security & Privacy System Preferences. To reset permissions, user's can utilize the `tccutil reset` command. When using Mobile Device Management (MDM), review the list of enabled or disabled applications in the `MDMOverrides.plist` which overrides the TCC database. [2]

Enterprise T1087 .004 Account Discovery: Cloud Account

Routinely check user permissions to ensure only the expected users have the ability to list IAM identities or otherwise discover cloud accounts.

Enterprise T1560 Archive Collected Data

System scans can be performed to identify unauthorized archival utilities.

.001 Archive via Utility

System scans can be performed to identify unauthorized archival utilities.

Enterprise T1612 Build Image on Host

Audit images deployed within the environment to ensure they do not contain any malicious components.

Enterprise T1671 Cloud Application Integration

Periodically review SaaS integrations for unapproved or potentially malicious applications.

Enterprise T1059 Command and Scripting Interpreter

Inventory systems for unauthorized command and scripting interpreter installations.

.006 Python

Inventory systems for unauthorized Python installations.

.011 Lua

Inventory systems for unauthorized Lua installations.

Enterprise T1543 Create or Modify System Process

Use auditing tools capable of detecting privilege and service abuse opportunities on systems within an enterprise and correct them.

.003 Windows Service

Use auditing tools capable of detecting privilege and service abuse opportunities on systems within an enterprise and correct them.

.004 Launch Daemon

Use auditing tools capable of detecting folder permissions abuse opportunities on systems, especially reviewing changes made to folders by third-party software.

Enterprise T1530 Data from Cloud Storage

Frequently check permissions on cloud storage to ensure proper permissions are set to deny open or unprivileged access to resources.[3]

Enterprise T1213 Data from Information Repositories

Consider periodic review of accounts and privileges for critical and sensitive repositories. Ensure that repositories such as cloud-hosted databases are not unintentionally exposed to the public, and that security groups assigned to them permit only necessary and authorized hosts.[4]

.001 Confluence

Consider periodic review of accounts and privileges for critical and sensitive Confluence repositories.

.002 Sharepoint

Consider periodic review of accounts and privileges for critical and sensitive SharePoint repositories.

.003 Code Repositories

Consider periodic reviews of accounts and privileges for critical and sensitive code repositories. Scan code repositories for exposed credentials or other sensitive information.

.004 Customer Relationship Management Software

Consider periodic review of accounts and privileges for critical and sensitive CRM data.

.005 Messaging Applications

Preemptively search through communication services to find inappropriately shared data, and take actions to reduce exposure when found.

.006 Databases

Consider periodic review of accounts and privileges for critical and sensitive databases.

Enterprise T1610 Deploy Container

Scan images before deployment, and block those that are not in compliance with security policies. In Kubernetes environments, the admission controller can be used to validate images after a container deployment request is authenticated but before the container is deployed.[5]

Enterprise T1484 Domain or Tenant Policy Modification

Identify and correct GPO permissions abuse opportunities (ex: GPO modification privileges) using auditing tools such as BloodHound (version 1.5.1 and later)[6].

.001 Group Policy Modification

Identify and correct GPO permissions abuse opportunities (ex: GPO modification privileges) using auditing tools such as BloodHound (version 1.5.1 and later).[6]

Enterprise T1482 Domain Trust Discovery

Map the trusts within existing domains/forests and keep trust relationships to a minimum.

Enterprise T1114 Email Collection

Enterprise email solutions have monitoring mechanisms that may include the ability to audit auto-forwarding rules on a regular basis.

In an Exchange environment, Administrators can use Get-InboxRule to discover and remove potentially malicious auto-forwarding rules.[7]

.003 Email Forwarding Rule

Enterprise email solutions have monitoring mechanisms that may include the ability to audit auto-forwarding rules on a regular basis.

In an Exchange environment, Administrators can use `Get-InboxRule` / `Remove-InboxRule` and `Get-TransportRule` / `Remove-TransportRule` to discover and remove potentially malicious auto-fowarding and transport rules.[7][8][9] In addition to this, a MAPI Editor can be utilized to examine the underlying database structure and discover any modifications/tampering of the properties of auto-forwarding rules.[10]

Enterprise T1546 .006 Event Triggered Execution: LC_LOAD_DYLIB Addition

Binaries can also be baselined for what dynamic libraries they require, and if an app requires a new dynamic library that wasn't included as part of an update, it should be investigated.

Enterprise T1606 Forge Web Credentials

Administrators should perform an audit of all access lists and the permissions they have been granted to access web applications and services. This should be done extensively on all resources in order to establish a baseline, followed up on with periodic audits of new or updated resources. Suspicious accounts/credentials should be investigated and removed.

Enable advanced auditing on ADFS. Check the success and failure audit options in the ADFS Management snap-in. Enable Audit Application Generated events on the AD FS farm via Group Policy Object.[11]

.001 Web Cookies

Administrators should perform an audit of all access lists and the permissions they have been granted to access web applications and services. This should be done extensively on all resources in order to establish a baseline, followed up on with periodic audits of new or updated resources. Suspicious accounts/credentials should be investigated and removed.

.002 SAML Tokens

Enable advanced auditing on AD FS. Check the success and failure audit options in the AD FS Management snap-in. Enable Audit Application Generated events on the AD FS farm via Group Policy Object.[11]

Enterprise T1564 Hide Artifacts

Periodically audit virtual machines for abnormalities.

.006 Run Virtual Instance

Periodically audit virtual machines for abnormalities. On ESXi servers, periodically compare the output of `vim-cmd vmsvc/getallvms`, which lists all VMs in vCenter, and `escxli vm process list | grep Display`, which lists all VMs hosted on ESXi.[12]

.008 Email Hiding Rules

Enterprise email solutions may have monitoring mechanisms that may include the ability to audit inbox rules on a regular basis.

In an Exchange environment, Administrators can use `Get-InboxRule` / `Remove-InboxRule` and `Get-TransportRule` / `Remove-TransportRule` to discover and remove potentially malicious inbox and transport rules.[9][8]

Enterprise T1574 Hijack Execution Flow

Use auditing tools capable of detecting hijacking opportunities on systems within an enterprise and correct them. Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for

hijacking weaknesses.[13]

Use the program sxstrace.exe that is included with Windows along with manual inspection to check manifest files for side-loading vulnerabilities in software.

Find and eliminate path interception weaknesses in program configuration files, scripts, the PATH environment variable, services, and in shortcuts by surrounding PATH variables with quotation marks when functions allow for them. Be aware of the search order Windows uses for executing or loading binaries and use fully qualified paths wherever appropriate.

Clean up old Windows Registry keys when software is uninstalled to avoid keys with no associated legitimate binaries. Periodically search for and correct or report path interception weaknesses on systems that may have been introduced using custom or available tools that report software using insecure path configurations.[14][15][16]

.001 DLL

Use auditing tools capable of detecting DLL search order hijacking opportunities on systems within an enterprise and correct them. Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for DLL hijacking weaknesses.[13]

Use the program `sxstrace.exe` that is included with Windows, along with manual inspection, to check manifest files for side-by-side problems in software.[17]

.005 Executable Installer File Permissions Weakness

Use auditing tools capable of detecting file system permissions abuse opportunities on systems within an enterprise and correct them. Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for service file system permissions weaknesses.[13]

.007 Path Interception by PATH Environment Variable

Find and eliminate path interception weaknesses in program configuration files, scripts, the PATH environment variable, services, and in shortcuts by surrounding PATH variables with quotation marks when functions allow for them. Be aware of the search order Windows uses for executing or loading binaries and use fully qualified paths wherever appropriate.

Clean up old Windows Registry keys when software is uninstalled to avoid keys with no associated legitimate binaries. Periodically search for and correct or report path interception weaknesses on systems that may have been introduced using custom or available tools that report software using insecure path configurations.[14][15][16]

.008 Path Interception by Search Order Hijacking

Find and eliminate path interception weaknesses in program configuration files, scripts, the PATH environment variable, services, and in shortcuts by surrounding PATH variables with quotation marks when functions allow for them. Be aware of the search order Windows uses for executing or loading binaries and use fully qualified paths wherever appropriate.

Clean up old Windows Registry keys when software is uninstalled to avoid keys with no associated legitimate binaries. Periodically search for and correct or report path interception weaknesses on systems that may have been introduced using custom or available tools that report software using insecure path configurations.[14][15][16]

.009 Path Interception by Unquoted Path

Find and eliminate path interception weaknesses in program configuration files, scripts, the PATH environment variable, services, and in shortcuts by surrounding PATH variables with quotation marks when functions allow for them. Be aware of the search order Windows uses for executing or loading binaries and use fully qualified paths wherever appropriate.

Clean up old Windows Registry keys when software is uninstalled to avoid keys with no associated legitimate binaries. Periodically search for and correct or report path interception weaknesses on systems that may have been introduced using custom or available tools that report software using insecure path configurations.[14][15][16]

.010 Services File Permissions Weakness

Use auditing tools capable of detecting file system permissions abuse opportunities on systems within an enterprise and correct them. Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for service file system permissions weaknesses.[13]

Enterprise T1562 Impair Defenses

Routinely check account role permissions to ensure only expected users and roles have permission to modify defensive tools and settings. Periodically verify that tools such as EDRs are functioning as expected.

.001 Disable or Modify Tools

Periodically verify that tools are functioning appropriately – for example, that all expected hosts with EDRs or monitoring agents are checking in to the central console. Check EDRs to ensure that no unexpected exclusion paths have been added. In Microsoft Defender for Endpoint, exclusions can be reviewed with the `Get-MpPreference` cmdlet.[18]

.002 Disable Windows Event Logging

Consider periodic review of `auditpol` settings for Administrator accounts and perform dynamic baselining on SIEM(s) to investigate potential malicious activity. Also ensure that the EventLog service and its threads are properly running.

.004 Disable or Modify System Firewall

Routinely check account role permissions to ensure only expected users and roles have permission to modify system firewalls.

.007 Disable or Modify Cloud Firewall

Routinely check account role permissions to ensure only expected users and roles have permission to modify cloud firewalls.

.012 Disable or Modify Linux Audit System

Routinely check account role permissions to ensure only expected users and roles have permission to modify logging settings.

To ensure Audit rules can not be modified at runtime, add the `auditctl -e 2` as the last command in the audit.rules files. Once started, any attempt to change the configuration in this mode will be audited and denied. The configuration can only be changed by rebooting the machine.

.013 Disable or Modify Network Device Firewall

Routinely check account role permissions to ensure only expected users and roles have permission to modify system firewalls.

Enterprise T1525 Implant Internal Image

Periodically check the integrity of images and containers used in cloud deployments to ensure they have not been modified to include malicious software.

Enterprise T1070 .008 Indicator Removal: Clear Mailbox Data

In an Exchange environment, Administrators can use `Get-TransportRule` / `Remove-TransportRule` to discover and remove potentially malicious transport rules.[8]

Enterprise T1036 Masquerading

Audit user accounts to ensure that each one has a defined purpose.

.010 Masquerade Account Name

Audit user accounts to ensure that each one has a defined purpose.

.012 Browser Fingerprint

Review and limit the fingerprinting surface to only necessary information on each browser to make the browser less unique. For example, the available fonts may be limited to a standard font list. [19]

Enterprise T1556 Modify Authentication Process

Review authentication logs to ensure that mechanisms such as enforcement of MFA are functioning as intended.

Periodically review the hybrid identity solution in use for any discrepancies. For example, review all Pass Through Authentication (PTA) agents in the Azure Management Portal to identify any unwanted or unapproved ones.[20] If ADFS is in use, review DLLs and executable files in the AD FS and Global Assembly Cache directories to ensure that they are signed by Microsoft. Note that in some cases binaries may be catalog-signed, which may cause the file to appear unsigned when viewing file properties.[21]

Periodically review for new and unknown network provider DLLs within the Registry (`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<NetworkProviderName>\NetworkProvider\ProviderPath`). Ensure only valid network provider DLLs are registered. The name of these can be found in the Registry key at `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order` , and have corresponding service subkey pointing to a DLL at `HKEY_LOCAL_MACHINE\SYSTEM\CurrentC ontrolSet\Services\<NetworkProviderName>\NetworkProvider` .

.006 Multi-Factor Authentication

Review MFA actions alongside authentication logs to ensure that MFA-based logins are functioning as intended. Review user accounts to ensure that all accounts have MFA enabled.[22]

.007 Hybrid Identity

Periodically review the hybrid identity solution in use for any discrepancies. For example, review all PTA agents in the Entra ID Management Portal to identify any unwanted or unapproved ones.[20] If ADFS is in use, review DLLs and executable files in the AD FS and Global Assembly Cache directories to ensure that they are signed by Microsoft. Note that in some cases binaries may be catalog-signed, which may cause the file to appear unsigned when viewing file properties.[21]

.008 Network Provider DLL

Periodically review for new and unknown network provider DLLs within the Registry (`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<NetworkProviderName>\NetworkProvider\ProviderPath`).

Ensure only valid network provider DLLs are registered. The name of these can be found in the Registry key at `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order` , and have corresponding service subkey pointing to a DLL at `HKEY_LOCAL_MACHINE\SYSTEM\CurrentC ontrolSet\Services\<NetworkProviderName>\NetworkProvider` .

Enterprise T1578 Modify Cloud Compute Infrastructure

Routinely monitor user permissions to ensure only the expected users have the capability to modify cloud compute infrastructure components.

.001 Create Snapshot

Routinely check user permissions to ensure only the expected users have the capability to create snapshots and backups.

.002 Create Cloud Instance

Routinely check user permissions to ensure only the expected users have the capability to create new instances.

.003 Delete Cloud Instance

Routinely check user permissions to ensure only the expected users have the capability to delete new instances.

.005 Modify Cloud Compute Configurations

Routinely monitor user permissions to ensure only the expected users have the capability to request quota adjustments or modify tenant-level compute settings.

Enterprise T1666 Modify Cloud Resource Hierarchy

Periodically audit resource groups in the cloud management console to ensure that only expected items exist, especially close to the top of the hierarchy (e.g., AWS accounts and Azure subscriptions). Typically, top-level accounts (such as the AWS management account) should not contain any workloads or resources.[23]

Enterprise T1095 Non-Application Layer Protocol

Periodically investigate ESXi hosts for open VMCI ports. Running the `lsof -A` command and inspecting results with a type of `SOCKET_VMCI` will reveal processes that have open VMCI ports.[24]

Enterprise T1027 Obfuscated Files or Information

Consider periodic review of common fileless storage locations (such as the Registry or WMI repository) to potentially identify abnormal and malicious data.

.011 Fileless Storage

Consider periodic review of common fileless storage locations (such as the Registry or WMI repository) to potentially identify abnormal and malicious data.

Enterprise T1566 Phishing

Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.

.001 Spearphishing Attachment

Enable auditing and monitoring for email attachments and file transfers to detect and investigate suspicious activity. Regularly review logs for anomalies related to attachments containing potentially malicious content, as well as any attempts to execute or interact with these files. This practice helps identify spearphishing attempts before they can lead to further compromise.

.002 Spearphishing Link

Audit applications and their permissions to ensure access to data and resources are limited based upon necessity and principle of least privilege.

.003 Spearphishing via Service

Implement auditing and logging for interactions with third-party messaging services or collaboration platforms. Monitor user activity and review logs for signs of suspicious links, downloads, or file exchanges that could

indicate spearphishing attempts. Effective auditing allows for the quick identification of malicious activity originating from compromised service accounts.

Enterprise T1653 Power Settings

Periodically inspect systems for abnormal and unexpected power settings that may indicate malicious activty.

Enterprise T1542 Pre-OS Boot

Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.

.004 ROMMONkit

Periodically check the integrity of system image to ensure it has not been modified. [25] [26] [27]

.005 TFTP Boot

Periodically check the integrity of the running configuration and system image to ensure they have not been modified. [26] [25] [27]

Enterprise T1563 .002 Remote Service Session Hijacking: RDP Hijacking

Audit the Remote Desktop Users group membership regularly. Remove unnecessary accounts and groups from Remote Desktop Users groups.

Enterprise T1021 Remote Services

Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.

.001 Remote Desktop Protocol

Audit the Remote Desktop Users group membership regularly. Remove unnecessary accounts and groups from Remote Desktop Users groups.

.005 VNC

Inventory workstations for unauthorized VNC server software.

Enterprise T1053 Scheduled Task/Job

Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for permission weaknesses in scheduled tasks that could be used to escalate privileges. [13]

.002 At

Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for permission weaknesses in scheduled tasks that could be used to escalate privileges. [13] Windows operating

system also creates a registry key specifically associated with the creation of a scheduled task on the destination host at: Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\At1. [28] In Linux and macOS environments, scheduled tasks using `at` can be audited locally, or through centrally collected logging, using syslog, or auditd events from the host. [29]

.003 Cron

Review changes to the `cron` schedule. `cron` execution can be reviewed within the `/var/log` directory. To validate the location of the `cron` log file, check the syslog config at `/etc/rsyslog.conf` or `/etc/syslog.conf`.

.005 Scheduled Task

Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for permission weaknesses in scheduled tasks that could be used to escalate privileges. [13]

Enterprise T1593 Search Open Websites/Domains

Scan public code repositories for exposed credentials or other sensitive information before making commits. Ensure that any leaked credentials are removed from the commit history, not just the current latest version of the code.

.003 Code Repositories

Scan public code repositories for exposed credentials or other sensitive information before making commits. Ensure that any leaked credentials are removed from the commit history, not just the current latest version of the code.

Enterprise T1505 Server Software Component

Regularly check component software on critical services that adversaries may target for persistence to verify the integrity of the systems and identify if unexpected changes have been made.

.001 SQL Stored Procedures

Regularly check component software on critical services that adversaries may target for persistence to verify the integrity of the systems and identify if unexpected changes have been made.

.002 Transport Agent

Regularly check component software on critical services that adversaries may target for persistence to verify the integrity of the systems and identify if unexpected changes have been made.

.004 IIS Components

Regularly check installed IIS components to verify the integrity of the web server and identify if unexpected changes have been made.

.005 Terminal Services DLL

Regularly check component software on critical services that adversaries may target for persistence to verify the integrity of the systems and identify if unexpected changes have been made.

.006 vSphere Installation Bundles

Periodically audit ESXi hosts to ensure that only approved VIBs are installed. The command `esxcli software vib list` lists installed VIBs, while the command `esxcli software vib signature verify` verifies the signatures of installed VIBs.[30]

Enterprise T1176 Software Extensions

Ensure extensions that are installed are the intended ones, as many malicious extensions may masquerade as legitimate ones.

.001 Browser Extensions

Ensure extensions that are installed are the intended ones, as many malicious extensions will masquerade as legitimate ones.

.002 IDE Extensions

Ensure extensions that are installed are the intended ones, as many malicious extensions may masquerade as legitimate ones.

Enterprise T1528 Steal Application Access Token

Administrators should audit all cloud and container accounts to ensure that they are necessary and that the permissions granted to them are appropriate. Additionally, administrators should perform an audit of all OAuth applications and the permissions they have been granted to access organizational data. This should be done extensively on all applications in order to establish a baseline, followed up on with periodic audits of new or updated applications. Suspicious applications should be investigated and removed.

Enterprise T1649 Steal or Forge Authentication Certificates

Check and remediate unneeded existing authentication certificates as well as common abusable misconfigurations of CA settings and permissions, such as AD CS certificate enrollment permissions and published overly permissive certificate templates (which define available settings for created certificates). For example, available AD CS certificate templates can be checked via the Certificate Authority MMC snap-in (`certsrv.msc`). `certutil.exe` can also be used to examine various information within an AD CS CA database.[31][32][33]

Enterprise T1558 Steal or Forge Kerberos Tickets

Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.

.004 AS-REP Roasting

Kerberos preauthentication is enabled by default. Older protocols might not support preauthentication therefore it is possible to have this setting disabled. Make sure that all accounts have preauthentication whenever possible and audit changes to setting. Windows tools such as PowerShell may be used to easily find which accounts have preauthentication disabled. [34][35]

.005 Ccache Files

Enable and perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.[36] For example, use `auditd` to audit access to hashes, machine tickets, or `/tmp` files. If using sssd and Vintela, ensure kerberos is disabled if not being used.[37]

Enterprise T1539 Steal Web Session Cookie

Implement auditing for authentication activities and user logins to detect the use of stolen session cookies. Monitor for impossible travel scenarios and anomalous behavior that could indicate the use of compromised session tokens or cookies.

Enterprise T1552 Unsecured Credentials

Preemptively search for files containing passwords or other credentials and take actions to reduce the exposure risk when found.

.001 Credentials In Files

Preemptively search for files containing passwords and take actions to reduce the exposure risk when found.

.002 Credentials in Registry

Proactively search for credentials within the Registry and attempt to remediate the risk.

.004 Private Keys

Ensure only authorized keys are allowed access to critical resources and audit access lists regularly.

.006 Group Policy Preferences

Search SYSVOL for any existing GGPs that may contain credentials and remove them.[38]

.008 Chat Messages

Preemptively search through communication services to find shared unsecured credentials. Searching for common patterns like "`password is `", "`password=`" and take actions to reduce exposure when found.

Enterprise T1550 Use Alternate Authentication Material

Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.

.001 Application Access Token

Administrators should audit all cloud and container accounts to ensure that they are necessary and that the permissions granted to them are appropriate. Where possible, the ability to request temporary account tokens on behalf of another accounts should be disabled. Additionally, administrators can leverage audit tools to monitor actions that can be conducted as a result of OAuth 2.0 access. For instance, audit reports enable admins to identify privilege escalation actions such as role creations or policy modifications, which could be actions performed after initial access.

Enterprise T1204 .003 User Execution: Malicious Image

Audit images deployed within the environment to ensure they do not contain any malicious components.

Source: https://attack.mitre.org/mitigations/M1047