Monday, September 27, 2021, 7:20 am

Live IOC Latest Cyber Security News New CVE's AbuseIPDB Phishing Domain Search Sucuri Web Malware Urlabuse Urlvoid WebPage Historic Checks

Soc Investigation
The Cyber Defenders Home

HOME ACTIVE DIRECTORY ATTACK NETWORK ATTACK SIEM TOOLS IOC MITRE ATT&CK E-MAIL ATTACK

Home › Active Directory Attack › Threat Hunting Using Windows Security Log

Active Directory Attack

Threat Hunting Using Windows Security Log

By **Anusthika Jeyashankar** - September 27, 2021 0

Every action in Windows has its own event id. Each event id has its own set of characteristics. We have no idea what attackers are thinking when their techniques work at a higher degree than usual. As a result, SOC analysts will save time by creating rules with the majority of the windows event ids for specialized hunting. Let's have a look at various event IDs and how to effectively hunt with them.

1. Event ID 4771 – Failed Kerberos Pre-Authentication

Description:

- When the Key Distribution Center fails to issue a Kerberos Ticket Granting Ticket, this event occurs (TGT).
- This issue can arise if a domain controller does not have a certificate installed for smart card authentication (for example, with a "Domain Controller" or "Domain Controller Authentication" template), the user's password has expired, or the user has provided the incorrect password.
- Only domain controllers generate this event.
- If the account's "Do not require Kerberos preauthentication" option is enabled, this event will not be generated.

Required monitoring & Recommendations:

- Need to keep track of High-value domain or local accounts. Database administrators, built-in local administrator accounts, domain administrators, service accounts, domain controller accounts, and so on are examples of high-value accounts. Keep an eye on this occurrence using the "Security ID" associated with the high-value account or accounts.

- Need to monitor the anonymous or potential malicious activities. You might need to keep an eye on an account that has been used outside of working hours by using the **"**Security ID**"** (with other information) to monitor how or when a particular account is being used.
- There will be inactive accounts, deactivated accounts, or guest accounts, as well as others that should never be utilized. Keep an eye on this event using the "Security ID" associated with the accounts that should never be used.
- Accounts that are only allowed to conduct actions in response to specified events are listed in a specific allow list. If this event corresponds to a "allow list-only" action, review the "Security ID" for accounts that are outside the allow list.
- Account names may follow certain naming conventions in our organization. Keep an eye on the "Subject\Account Name" field for names that don't follow naming rules.

Tips for detecting threats:

- Hunt for spikes of events from a single machine.
- Hunt for the client address if it's not from your internal IP range or not from private IP ranges.
- Check for the result codes if the authentication gets failed. This will be more useful if it's an real attack. For example, **0x18** (Pre-authentication information was invalid) that means wrong password is provided and 0x12 (Clients credentials have been revoked) that means account might be disabled, expired or locked out.
- Create a rule based on a client address that isn't in the list of allowed addresses. Client IP addresses from which highly valued accounts should be logged in must be included in the Allow list.

2. Event ID 4625 – Failed Logins

Description:

- If an account logon attempt fails while the account is already locked out, this event is triggered. It also generates for a failed logon attempt, which results in the account being locked out.
- It appears on the machine where the logon attempt was made; for example, if the logon attempt was made on the user's workstation, the event will appear on that workstation.
- On domain controllers, member servers, and workstations, this event will occur.

Required monitoring & Recommendations:

- Monitor the "**Process Name**" if it is not in the standard folder (for example, not in **System32** or **Program Files**) or is in a restricted folder (for example, **Temporary Internet Files).**
- Make a list of restricted substrings or words in process names (for example, "mimikatz" or "cain.exe"), then look for them in the "Process Name" field.
- Monitor the service/user accounts which got failed to investigate whether that account is allowed (or expected) to request logon towards the server/machine.
- Monitor the logon type 10 (remote login) 4(Batch operations) & 5 (service) to confirm whether the user/account who is trying to login has the permissions to do such logins and they are part of domain administrative group.
- If you have a high-value domain or local account for which you need to monitor every lockout, monitor all 4625 events with the "Subject\Security ID" that corresponds to the account.
- We suggest keeping an eye on all 4625 events for local and service accounts, as these accounts should never be locked out. Critical servers, administrative workstations, and other high-value assets should all be monitored.
- Alert should be generated if Logon Process is not from a trusted logon processes list.

Tips for detecting threats:

- Check whether it has large number of failed logins on a single source within a small amount of time. Because it will end in Brute Force attacks.

- Sort by hosts with highest number of failed logins within a period of time, sorted by username to identify whether it is an genuine user names or not.
- Need to think twice if the failed logins are initiated after business hours.
- Check for the failure reasons. Mostly for the status codes :
    - 0XC000005E – "There are currently no logon servers available to service the logon request."
    - 0xC0000064 – "User logon with misspelled or bad user account".
    - 0xC000006A – "User logon with misspelled or bad password" for critical accounts or service accounts.
    - 0XC000006D – "This is either due to a bad username or authentication information" for critical accounts or service accounts.
    - 0xC000006F – "User logon outside authorized hours".
    - 0xC0000070 – "User logon from unauthorized workstation".
    - 0XC000015B – "The user has not been granted the requested logon type (aka logon right) at this machine".
    - 0XC0000192 – "An attempt was made to logon, but the Netlogon service was not started".
    - 0xC0000193 – "User logon with expired account".
    - 0XC0000413 – "Logon Failure: The machine you are logging onto is protected by an authentication firewall. The specified account is not allowed to authenticate to the machine".

3. Event ID 4794 – An attempt was made to set the Directory Services Restore Mode administrator password

Description:

When the administrator password for Directory Services Restore Mode (DSRM) is updated, this event is triggered. Only domain controllers generate this event.

Directory Services Restore Mode (DSRM) is a safe mode boot option for Windows Server domain controllers. DSRM allows an administrator to repair or recover to repair or restore an Active Directory database. When Active Directory is installed, the install wizard prompts the administrator to choose a DSRM password.

Required monitoring & Recommendations:

This attempt will be made to change the administrator password for Directory Services Restore Mode. Hence, it's a good idea to keep an eye on 4794 occurrences and set up alerts when the change happens.

Tips for detecting threats:

If this isn't expected, could be malicious. Set DSRM==edit/access the AD database.

4. Event ID's – 4793/643, 4713/617, 4719/612 – Policy Changes

Event ID 4793 – The Password Policy Checking API was called:

Description:

This event generates on the computer where Password Policy Checking API was called. This event is generated, for example, during the password reset operation for a Directory Services Restore Mode (DSRM) account to verify the new DSRM password.

Required monitoring & Recommendations:

This is usually an informative event that tells you when and by whom Password Policy Checking APIs were called. The Provided Account Name does not always have a value—sometimes it’s not really possible to determine for which account the password policy check was performed.

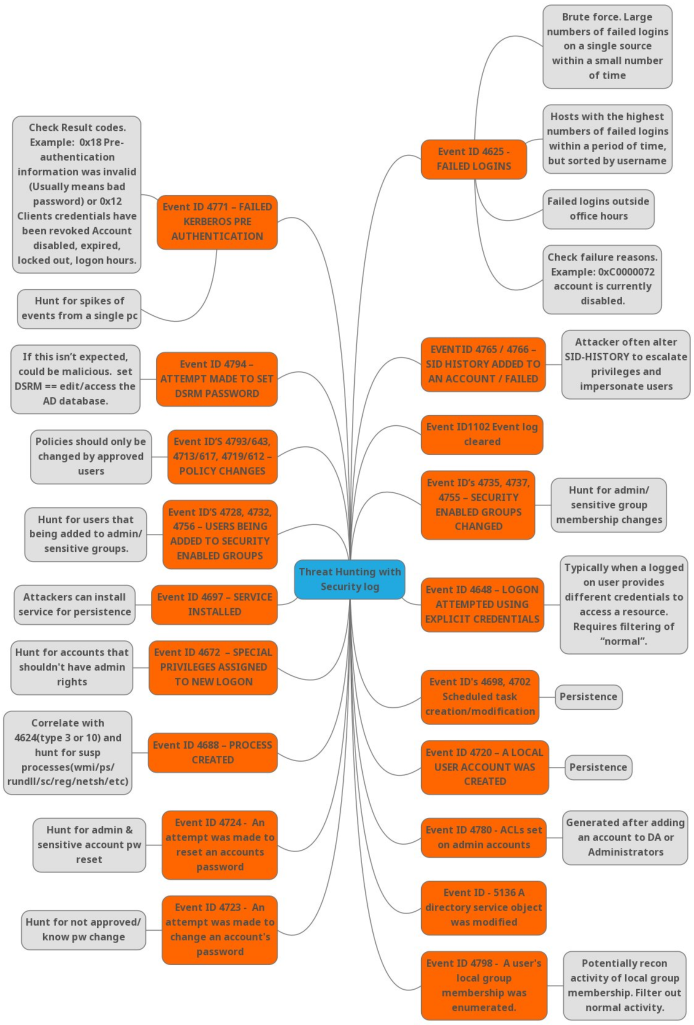
5. Event ID 4713 – Kerberos policy was changed

Description:

When the Kerberos policy is modified, this event is triggered. Only domain controllers generate this event.

Required monitoring & Recommendations:

Any changes in Kerberos policy reported by the current event should be monitored and an alert should be triggered. Investigate the reason for the change if it was not planned.


Threat Hunting with Security log
Event ID 4771 – FAILED KERBEROS PRE AUTHENTICATION
Check Result codes. Example: 0x18 Pre-authentication information was invalid (Usually means bad password) or 0x12 Clients credentials have been revoked Account disabled, expired, locked out, logon hours.
Hunt for spikes of events from a single pc
Event ID 4794 – ATTEMPT MADE TO SET DSRM PASSWORD
If this isn’t expected, could be malicious. set DSRM == edit/access the AD database.
Event ID’S 4793/643, 4713/617, 4719/612 – POLICY CHANGES
Policies should only be changed by approved users
Event ID’S 4728, 4732, 4756 – USERS BEING ADDED TO SECURITY ENABLED GROUPS
Hunt for users that being added to admin/ sensitive groups.
Event ID 4697 – SERVICE INSTALLED
Attackers can install service for persistence
Event ID 4672 – SPECIAL PRIVILEGES ASSIGNED TO NEW LOGON
Hunt for accounts that shouldn't have admin rights
Event ID 4688 – PROCESS CREATED
Correlate with 4624(type 3 or 10) and hunt for susp processes(wmi/ps/ rundll/sc/reg/netsh/etc)
Event ID 4724 - An attempt was made to reset an accounts password
Hunt for admin & sensitive account pw reset
Event ID 4723 - An attempt was made to change an account's password
Hunt for not approved/ know pw change
Event ID 4625 - FAILED LOGINS
Brute force. Large numbers of failed logins on a single source within a small number of time
Hosts with the highest numbers of failed logins within a period of time, but sorted by username
Failed logins outside office hours
Check failure reasons. Example: 0xC0000072 account is currently disabled.
EVENTID 4765 / 4766 – SID HISTORY ADDED TO AN ACCOUNT / FAILED
Attacker often alter SID-HISTORY to escalate privileges and impersonate users
Event ID1102 Event log cleared
Event ID’s 4735, 4737, 4755 – SECURITY ENABLED GROUPS CHANGED
Hunt for admin/ sensitive group membership changes
Event ID 4648 – LOGON ATTEMPTED USING EXPLICIT CREDENTIALS
Typically when a logged on user provides different credentials to access a resource. Requires filtering of “normal”.
Event ID's 4698, 4702 Scheduled task creation/modification
Persistence
Event ID 4720 – A LOCAL USER ACCOUNT WAS CREATED
Persistence
Event ID 4780 - ACLs set on admin accounts
Generated after adding an account to DA or Administrators
Event ID - 5136 A directory service object was modified
Event ID 4798 - A user's local group membership was enumerated.
Potentially recon activity of local group membership. Filter out normal activity.

Image_Source_Credits: https://twitter.com/SBousseaden

6. Event ID – 4719 – System audit policy was changed

Description:

This event generates when the computer’s audit policy changes. This event is always logged regardless of the “Audit Policy Change” sub-category setting.

Required monitoring & Recommendations:

Any change in local audit policy should be planned, so keep an eye out for any such events, especially on high-value assets or computers. Investigate the reason for the change if it was not planned.

Tips for detecting threats:

Policies should only be changed by approved users. So Only authorized users should be able to alter policies. As a consequence, individuals who do not have access are unable to update it. If it is altered by an unauthorized user, we can only assume that something bothersome is going on.

Also Read : Important Windows processes for Threat Hunting

7. Event ID's – 4728, 4732 & 4756 – Users being added to security-enabled groups

Event ID – 4728 – A member was added to a security-enabled global group

Description:

When Active Directory objects such as a user/group/computer are added to a security global group, event ID 4728 gets logged.

Event ID – 4732 – A member was added to a security-enabled local group.

Description:

This event generates every time a new member was added to a security-enabled (security) local group. You will typically see "4735: A security-enabled local group was changed." event without any changes in it prior to the 4732 events. This event generates on domain controllers, member servers, and workstations.

Event ID – 4756 – A member was added to a security-enabled universal group

Description:

When Active Directory objects such as a user/group/computer are added to a universal security group, event ID 4756 gets logged.

Required monitoring & Recommendations:

- In order to prevent privilege abuse activities and to detect potential malicious activity, and to get information on user activity like user attendance, peak logon times etc, the above mentioned 3 events ID's should be monitored.
- Need to monitor the addition of members to local or domain security groups. Especially need to monitor list of critical local or domain security groups in the organization.
- Organizations have non-active, disabled, or guest accounts, or other accounts that should never be used. We might have a specific allow list of accounts that are the only ones allowed to perform actions corresponding to particular events. These all are should be monitored by creating rules.
- Need to ensure that a computer account was not added to a group intended for users, or a user account was not added to a group intended for computers.

Tips for detecting threats:

Hunt for the users that are being added/removed to/from the admin/sensitive groups.

8. Event ID – 4697 – A service was installed in the system

Description:

This event generates when new service was installed in the system.

Required monitoring & Recommendations:

- We recommend monitoring for this event, especially on high-value assets or PCs, because a new service installation should be planned and expected. An alert should be triggered if a service is installed unexpectedly.
- Keep an eye on any events where the "Service File Name" isn't in the "%windir%" or "Program Files/Program Files (x86)" directories. These folders are usually where new services are stored.
- All "Service Type" values of "0x1", "0x2", or "0x8" should be reported. These service types start first and have almost unlimited access to the operating system from the beginning of operating system startup. These types are very rarely installed.
- All "Service Start Type" values of "0" or "1" should be reported. These service start types are used by drivers, which have unlimited access to the operating system. It is not common to install a new service in the Disabled state.
- Report all "Service Account" not equals "localSystem", "localService" or "networkService" to identify services which are running under a user account.

Tips for detecting threats:

Attackers can install services for persistence. So make sure to monitor the event id with the above-mentioned points.

Also Read: Soc Interview Questions and Answers – CYBER SECURITY ANALYST

9. Event ID – 4672 – Special privileges assigned to new logon

Description:

This event generates new account logins if any of the following sensitive privileges are assigned to the new login session:

- SeTcbPrivilege – Act as part of the operating system
- SeBackupPrivilege – Back up files and directories
- SeCreateTokenPrivilege – Create a token object
- SeDebugPrivilege – Debug programs
- SeEnableDelegationPrivilege – Enable computer and user accounts to be trusted for delegation
- SeAuditPrivilege – Generate security audits
- SeImpersonatePrivilege – Impersonate a client after authentication
- SeLoadDriverPrivilege – Load and unload device drivers
- SeSecurityPrivilege – Manage auditing and security log
- SeSystemEnvironmentPrivilege – Modify firmware environment values
- SeAssignPrimaryTokenPrivilege – Replace a process-level token
- SeRestorePrivilege – Restore files and directories,
- SeTakeOwnershipPrivilege – Take ownership of files or other objects

Required monitoring & Recommendations:

- Need to monitor the list of specific privileges which should never be granted, or granted only to a few accounts (for example, SeDebugPrivilege), use this event to monitor for those "**Privileges**."
- Monitor for this event where "Subject\Security ID" is not one of these well-known security principals: LOCAL SYSTEM, NETWORK SERVICE, LOCAL SERVICE, and where "Subject\Security ID" is not an administrative account that is expected to have the listed Privileges.

Tips for detecting threats:

Particularly hunt for accounts that shouldn’t have admin rights.

10. Event ID – 4688 – A new process has been created

Description:

This event generates every time a new process starts.

Tips for detecting threats:

Correlate with Event ID 4624 for logon type 3 & 10 and hunt for suspicious processes like wmi, ps, rundll, sc, reg, netsh, etc.

Event ID – 4724 – An attempt was made to reset an account’s password:

Description:

When an account tries to reset the password for another account, this event is triggered. This event is generated for user accounts on domain controllers, member servers, and workstations. If the new password does not comply with the password rules, a Failure event is triggered for domain accounts. If the user receives “Access Denied” while attempting to reset their password, no failure event is generated. If a computer account reset procedure was completed, this event is also triggered. If the new password does not comply with the local password rules, a Failure event is triggered for local accounts.

Required monitoring & Recommendations:

- Monitor each and every change and password reset attempt for high-value domain or local user account with event ID 4724.
- If you do have domain or local accounts for which the password should never be reset, you can monitor all 4724 events, because local accounts’ passwords are rarely changed. This is particularly important for high-value assets such as critical servers, administrative workstations, and other high-value assets.

Tips for detecting threats:

Hunt for admin & sensitive account password reset.

11. Event ID – 4723 – An attempt was made to change an account’s password

Description:

When a user tries to change his or her password, this event is triggered. This event is generated for user accounts on domain controllers, member servers, and workstations. If the new password does not comply with the password rules, a Failure event is triggered for domain accounts.

If the new password does not fit the password rules or the old password is incorrect, a Failure event is triggered for local accounts. If the old password for a domain account was incorrect, the domain controller would emit “4771: Kerberos pre-authentication failed” or “4776: The computer attempted to check the credentials for an account” if particular subcategories were enabled on it.

Kindly follow the Event ID 4723 required monitoring & Recommendations.

Tips for detecting threats:

Hunt for not approved or unknown password change.

12. Event ID – 4798 – A user’s local group membership was enumerated

Description:

This event generates when a process enumerates a user's security-enabled local groups on a computer or device.

Required monitoring & Recommendations:

- Need to monitor each enumeration of their group membership, or any access attempt for high value domain or local accounts.
- Monitor if the process name is not in a standard folder (for example, not in System32 or Program Files) or is in a restricted folder (for example, Temporary Internet Files).

Tips for detecting threats:

Potentially recon activity local group membership. Need to filter out the normal activity.

Also Read: Splunk Features – Quick Guide on Key Elements

13. Event ID – 4720 – A Local user account was created

Description:

When a new user object is created, this event is triggered. On domain controllers, member servers, and workstations, this event occurs.

Tips for detecting threats:

Mostly all organizations monitor every event of this event ID since it persistent attack.

14. Event ID – 4698 & 4702 – Scheduled task creation/modification

Event ID – 4698 – A scheduled task was created:

Description:

This event generates every time a new scheduled task is created.

Event ID – 4702 – A scheduled task was updated:

Description:

This event generates every time the scheduled task was updated/changed.

Required monitoring & Recommendations:

- All scheduled task creation/updated events should be monitored, especially on essential systems or devices. Malware frequently uses scheduled activities to stay on the system after a reboot or to do other malicious actions.
- Monitor for new tasks located in the "Task Scheduler Library" root node, that is, where "Task Name" looks like '\TASK_NAME'. Scheduled tasks that are created manually or by malware are often located in the "Task Scheduler Library" root node.

Tips for detecting threats:

Hunt for every scheduled task creation and modification event. Sometimes if any application is uninstalled, the scheduled task related to it will be modified. This will result in a false positive.

15. Event ID – 4648 – A logon was attempted using

explicit credentials

Description:

This event is generated when a process attempts an account logon by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the "RUNAS" command. It is also a routine event that periodically occurs during normal operating system activity.

Tips for detecting threats:

Typically need to monitor when a logged-on user provides different credentials to access a resource. This requires filtering of normal activities.

16. Event ID – 4735, 4737 & 4755 – Security enabled groups changed

Description:

4735 – A security-enabled local group was changed.

4737 – A security-enabled global group was changed.

4755 – A security-enabled universal group was changed

Required monitoring & Recommendations:

- Monitor events with the "Group\Group Name" values that match to the critical local or domain security groups if you have a list of critical local or domain security groups in the organisation and need to explicitly monitor these groups for any changes.
- If you want to keep track of who and when a member is added to a local or domain security group, you may use this event to accomplish so.
- If your company has naming rules for account names, keep an eye on "Attributes\SAM Account Name" for names that don't follow them.

Tips for detecting threats:

Hunt for admin/sensitive group membership changes.

Also Read: **Latest IOCs – Threat Actor URLs , IP's & Malware Hashes**

17. Event ID – 1102 – The audit log was cleared

Description:

This event generates every time the Windows Security audit log was cleared.

Required monitoring & Recommendations:

Normally, we should not be able to observe this event. In most circumstances, there is no need to manually clear the Security event log. We recommend keeping an eye on this occurrence and looking into why this action was taken.

Tips for detecting threats:

Hunt for the audit logs cleared events to track why it was done so and by whom.

Also Read: **Latest Cyber Security News – Hacker News !**

18. Event ID – 4765 & 4766 – SID history added to an account/failed

Description:

4765 – This event generates when SID History was added to an account.

4766 – This event generates when an attempt to add SID History to an account failed.

Tips for detecting threats:

The attacker often alters SID-HISTORY to escalate privileges and impersonate users.

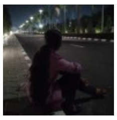
Happy Hunting!

TAGS event id 1102 event id 4625 event id 4648 event id 4672 event id 4688 event id 4697 event id 4698 event id 4702 event id 4713 event id 4719 event id 4720 event id 4723 event id 4728 event id 4732 event id 4735 event id 4737 event id 4755 event id 4756 event id 4765 event id 4766 event id 4771 event id 4793 event id 4794 event id 4798 event id 612 event id 617 event id 643 threat hunting security logs threat hunting windows event logs Windows eventids to monitor

Share and Support Us :

Previous article

Threat Hunting with Windows Event IDs 4625 & 4624



Anusthika Jeyashankar

https://www.socinvestigation.com

Ambitious Blue Teamer; Enthused Security Analyst

RELATED ARTICLES MORE FROM AUTHOR

Threat Hunting with Windows Event IDs 4625 & 4624

Important Windows processes for Threat Hunting

Malware Persistence on Boot – Monitor Modified Registry Keys & Possible Windows Event ID

‹ ›

LEAVE A REPLY

Comment:

Name:*

Email:*

Website:

□ Save my name, email, and website in this browser for the next time I comment.

Post Comment

EDITOR PICKS

Threat Hunting Using Windows Security Log
September 27, 2021

Threat Hunting with Windows Event IDs 4625 & 4624
September 24, 2021

Important Windows processes for Threat Hunting
September 23, 2021

POPULAR POSTS

Topmost Signs of Compromise Detected with Windows operating System
August 5, 2021

Top Windows Security Events Logs You Must Monitor
January 5, 2021

Malware Hiding Techniques in Windows Operating System
July 14, 2021

POPULAR CATEGORY

IOC	34
TOOLS	28
Active Directory Attack	20
Editors Pick	19
SIEM	12
Network Attack	11
E-Mail Attack	7
Mitre Att&ck	6

Soc Investigation
The Cyber Defenders Home

ABOUT US

Soc Investigation is a Cyber Security platform that covers daily Cyber Threats, Incident Response ,SIEM , SOC Tools and Mitre Att&CK. Our expedition is to keep the defense community updated with the latest offensive trends in cyberspace.

Contact us: admin@socinvestigation.com

FOLLOW US

About Us Privacy Policy Contact Us