Active Directory Attack

Most Common Windows Event IDs to Hunt – Mind Map

By **BalaGanesh** - November 3, 2021 0

Windows Event Logs mindmap provides a simplified view of Windows Event logs and their capacities that enables defenders to enhance visibility for different purposes:

- Log collection (eg: into a SIEM)
- Threat hunting
- Forensic / DFIR
- Troubleshooting

Scheduled tasks:

- Event ID 4697 , This event generates when new service was installed in the system.
- Event ID 106, This event is logged when the user registered the Task Scheduler task.
- Event ID 4702, This event generates when scheduled task was updated.
- Event ID 140,This event is logged when the time service has stopped advertising as a time source because the local machine is not an Active Directory Domain Controller.

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

- Event ID 4699, A scheduled task was deleted.
- Event ID 141, The time service has stopped advertising as a time source because there are no providers running.

- Event ID 201, This event is logged when the task scheduler successfully completed the task.

Credits:https://github.com/christophetd/

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

Services:

- Event ID 4697,A service was installed in the system.
- Event ID 7045,Created when new services are created on the local Windows machine.
- Event ID 7034,The service terminated unexpectedly.
- Event ID 7036,The Windows Firewall/Internet Connection Sharing (ICS) service entered the stopped state or , The Print Spooler service entered the running state.
- Event ID 7040, The start type of the IPSEC services was chnaged from disabled to auto start.

Event Log Manipulation:

- Event ID 1102, Whenever Windows Security audit log is cleared, event ID 1102 is logged.
- Event ID 104 , This event is logged when the log file was cleared.

Authentication:

- Event ID 4776, The domain controller attempted to validate the credentials for an account.
- Event ID 4771,This event is logged on domain controllers only and only failure instances of this event are logged (Kerberos pre-authentication failed).
- Event ID 4768, This event is logged on domain controllers only and both success and failure instances of this event are logged (A Kerberos authentication ticket TGT) was requested.
- Event ID 4769,Windows uses this event ID for both successful and failed service ticket requests (A Kerberos service ticket was requested).

Also Read: **Directory Services Restore Mode Password Reset – Event IDs to Monitor**

Sessions:

- Event ID 4624 ,An account was successfully logged on.
- Event ID 4625, An account failed to log on.

- Event ID 4634 + 4647 , User initiated logoff/An account was logged off
- Event ID 4648, A logon was attempted using explicit credentials
- Event ID 4672,Special privileges assigned to new logon

Account Management:

- Event ID 4720, A user account was created
- Event ID 4722, A user account was enabled
- Event ID 4724, An attempt was made to reset an accounts password
- Event ID 4728/4732/4756, group membership changes.

Network Shares:

- Event ID 5140,A network share object was accessed
- Event ID 5145, Network share object was checked to see whether client can be granted desired access.

Also Read: **Threat Hunting with EventID 5145 – Object Access – Detailed File Share**

TAGS Event ID 104 Event ID 106 event id 1102 Event ID 140 Event ID 141 Event ID 201 event id 4624 event id 4625 Event ID 4634 Event ID 4647 event id 4648 event id 4672 event id 4697 event id 4699 event id 4702 event id 4720 Event ID 4722 event id 4724 event id 4728 event id 4732 event id 4756 Event ID 4768 Event ID 4769 event id 4771 Event ID 4776 Event ID 5140 event id 5145 Event ID 7034 Event ID 7036 Event ID 7040 event id 7045 windows event id threat hunting windows event ids to monitor

Previous article

Event ID 4663 -Occurrence , Log fields Explanation & Use cases

Next article

Finding the Evil in TLS 1.2 Traffic – Detecting Malware on Encrypted Traffic

BalaGanesh

https://www.socinvestigation.com

Balaganesh is a Incident Responder. Certified Ethical Hacker, Penetration Tester, Security blogger, Founder & Author of Soc Investigation.

LEAVE A REPLY

Comment:

Name:*

Email:*

Website:

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

Post Comment