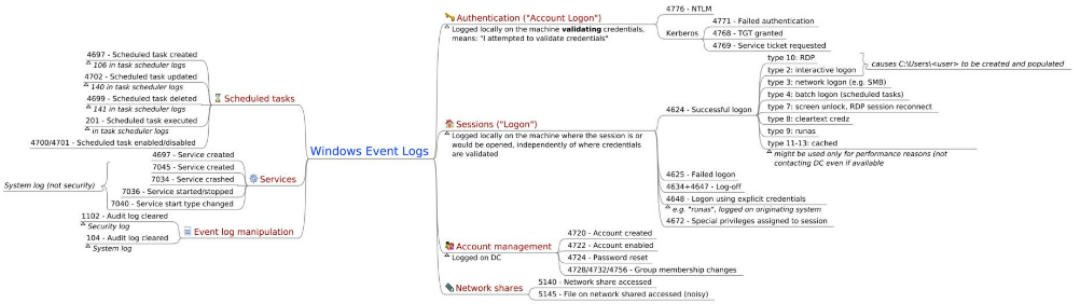
Most Common Windows Event IDs to Hunt

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.
- 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.



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).

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.

Here are some security-related Windows events. You can use the event IDs in this list to search for suspicious activities.

Event ID	What it means
4624	Successful account log on
4625	Failed account log on
4634	An account logged off
4648	A logon attempt was made with explicit credentials
4719	System audit policy was changed.
4964	A special group has been assigned to a new log on
1102	Audit log was cleared. This can relate to a potential attack
4720	A user account was created
4722	A user account was enabled
4723	An attempt was made to change the password of an account
4725	A user account was disabled
4728	A user was added to a privileged global group
4732	A user was added to a privileged local group
4756	A user was added to a privileged universal group
4738	A user account was changed
4740	A user account was locked out
4767	A user account was unlocked
4735	A privileged local group was modified
4737	A privileged global group was modified
4755	A privileged universal group was modified
4772	A Kerberos authentication ticket request failed
4777	The domain controller failed to validate the credentials of an account.
4782	Password hash an account was accessed
4616	System time was changed
4657	A registry value was changed
4697	An attempt was made to install a service

4698, 4699, 4700, 4701, 4702 Events related to Windows scheduled tasks being created, modified, deleted, enabled or disabled

4946 A rule was added to the Windows Firewall exception list

4947 A rule was modified in the Windows Firewall exception list

4950 A setting was changed in Windows Firewall

4954 Group Policy settings for Windows Firewall has changed

5025 The Windows Firewall service has been stopped

5031 Windows Firewall blocked an application from accepting incoming traffic

5152, 5153 A network packet was blocked by Windows Filtering Platform

5155 Windows Filtering Platform blocked an application or service from listening on a port

5157 Windows Filtering Platform blocked a connection

5447 A Windows Filtering Platform filter was changed