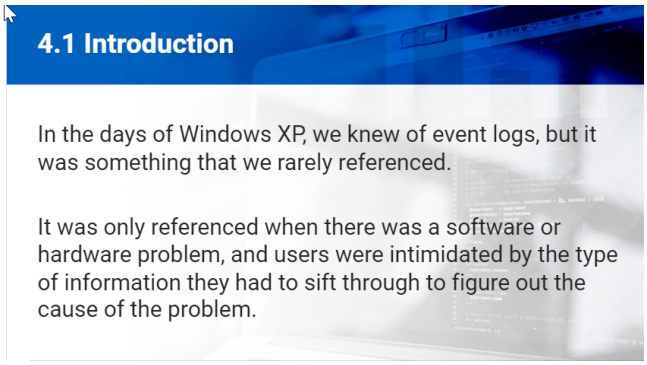
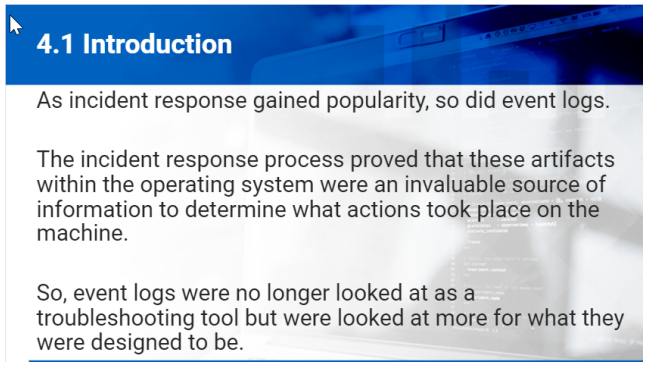
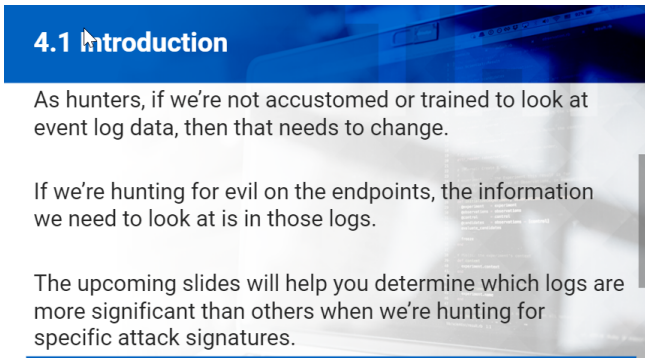
# Event IDs, Logging, & SIEMs

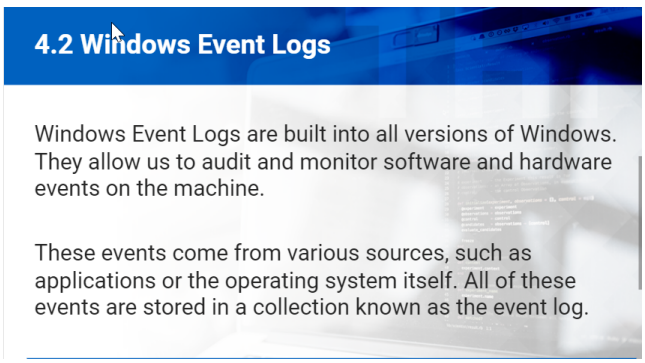
09 January 2023 12:00

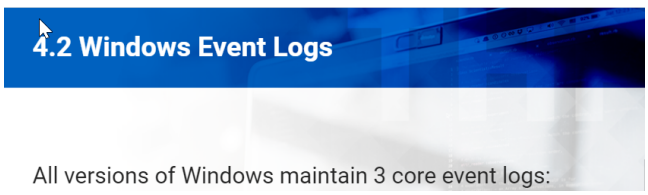


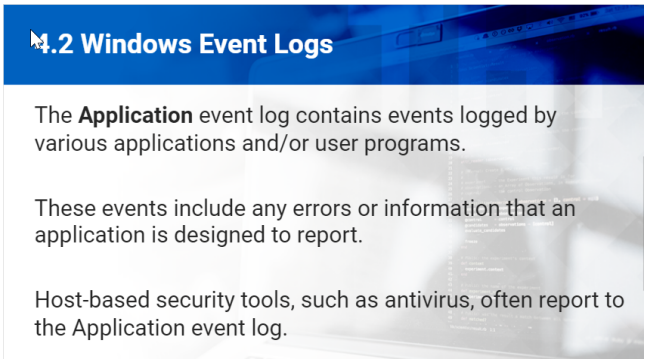

**Windows Event Logs**



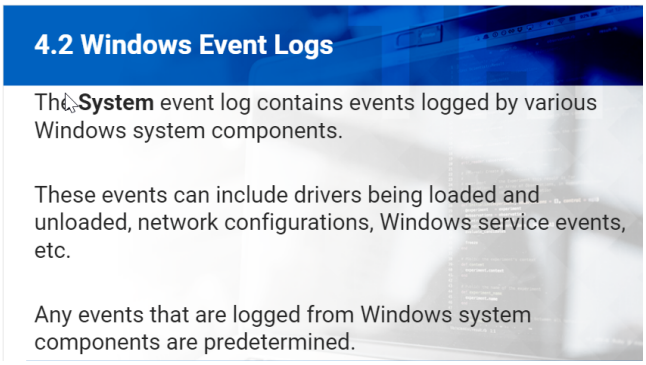



- Application
- System
- Security

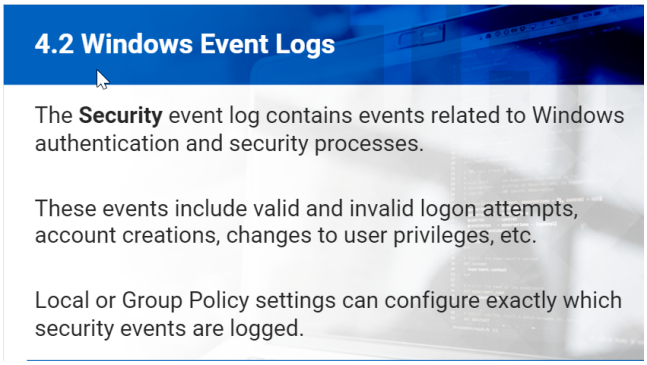
**Application logs**



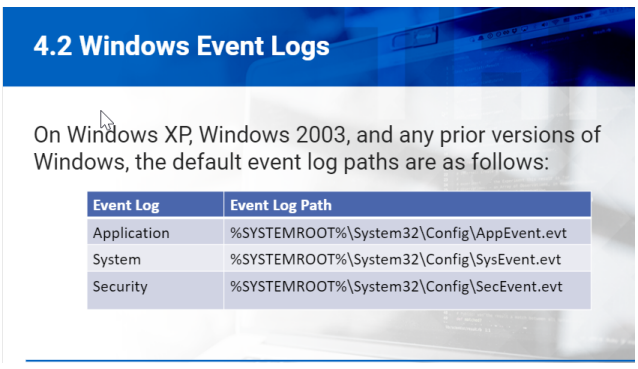

**System Logs**




**Security Event Logs**




**Old version of Windows event logs path.**



## 4.2 Windows Event Logs

With modern versions of Windows, beginning with Windows Vista and Windows Server 2008, Microsoft made significant changes to the event logging system.

The EVT format was eliminated for a XML-based format using the EVTX extension.

The location of the event logs was changed as well.

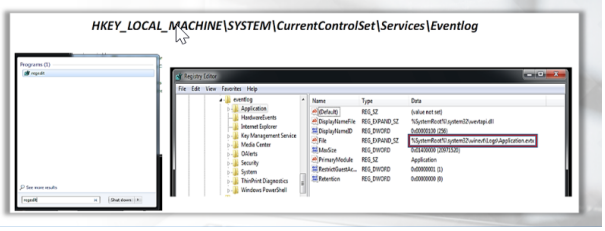
**New Update location of the windows event logs path**

## 4.2 Windows Event Logs

| Event Log | Event Log Path |
|---|---|
| Application | %SYSTEMROOT%\System32\Winevt\Logs\Application.evtx |
| System | %SYSTEMROOT%\System32\Winevt\Logs\System.evtx |
| Security | %SYSTEMROOT%\System32\Winevt\Logs\Security.evtx |

## 4.2 Windows Event Logs

Each event log location is also present within the registry.




## 4.2 Windows Event Logs

Under Windows Logs, you will see 2 additional sets of logs:

- ***Setup:*** logs contain events related to application setup.
- ***Forwarded Events:*** logs used to store events collected from remote computers.

## 4.2 Windows Event Logs

It's also worth mentioning that Microsoft added a new category of event logs, a second set of logs, called ***Applications and Services***.

These logs are used by individual applications or system components.

## 4.2 Windows Event Logs

These logs are saved in the same location as the 3 *core* logs previously mentioned.

A few examples of Windows components that maintain their own logs: *UAC, Windows Firewall with Advanced Security, AppLocker, Sysmon, Windows Defender, and PowerShell*.

## 4.2 Windows Event Logs

***Why are event logs important?***

- Monitor logons that failed or that were successful.
- Monitor system services that were created, started, or stopped.
- Monitor specific application usage.
- Monitor changes to the audit policy.
- Monitor changes to user permissions.
- Monitor events generated by installed applications, such as AV.

## 4.2 Windows Event Logs

So by now, you should know what event logs are, where they are located, and why they are important, but how do we access and view them?

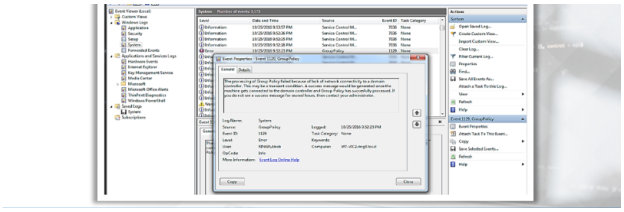
The answer to that is the ***Event Viewer***.

## 4.2 Windows Event Logs

You can access the Event Viewer by either double clicking the evtx file directly, by typing "*eventvwr*" in the Search box, or by navigating to *Control Panel > Administrative Tools > Event Viewer*.

## 4.2 Windows Event Logs

Below is a snapshot of the event viewer.



## 4.2 Windows Event Logs

In the previous slide, we saw an error recorded within the System event log related to Group Policy.

This particular event had an **ID** value of **1129**. In the properties for this particular event, we were fortunate enough to get some clear information as to why this error occurred. But what happens when the information is not clear?

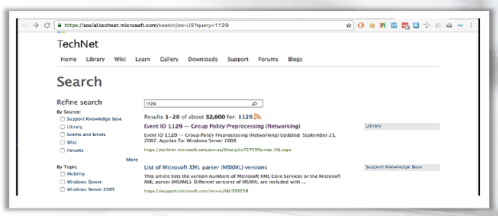
Luckily for us, Microsoft has documented the Event IDs here.

**Advanced security auditing FAQ**

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-auditing-faq

## 4.2 Windows Event Logs

If we use the search engine to research the recently discussed error, ID 1129, below are the results.




qa.social.technet.microsoft.com/wiki/contents/articles/1416.event-id-1129-microsoft-windows-grouppolicy.aspx

ARTICLE HISTORY

# Event ID 1129 — Microsoft-Windows-GroupPolicy

Table of Contents



Event ID 1129 — Group Policy Preprocessing (Networking)

## Applies To

Windows Server 2008

Group Policy processing requires network connectivity to one or more domain controllers. The Group Policy service reads information from Active Directory and the sysvol share located on a domain controller. The absence of network connectivity prevents Group Policy from applying to the user or computer.

## Event Details

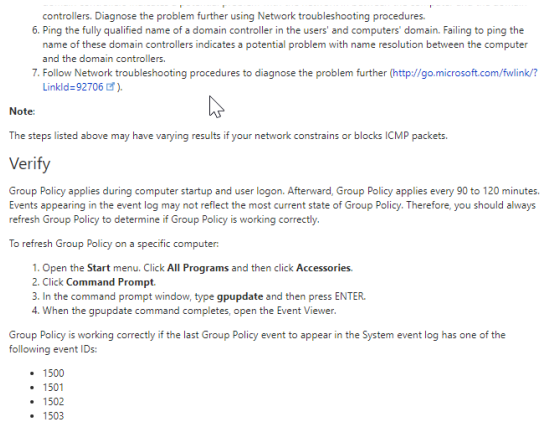
| | |
|---|---|
| **Product:** | Windows Operating System |
| **Event ID:** | 1129 |
| **Source:** | Microsoft-Windows-GroupPolicy |
| **Version:** | 6.0 |
| **Symbolic Name:** | gpEvent_NO_NETWORK |
| **Message:** | The processing of Group Policy failed because of lack of network connectivity to a domain controller. This may be a transient condition. A success message would be generated once the machine gets connected to the domain controller and Group Policy has succesfully processed. If you do not see a success message for several hours, then contact your administrator. |

## Resolve

### Correct network connectivity

To correct network connectivity:

1. Open a command prompt window on the computer, and then type **ipconfig /all**.
2. Make sure that the computer has an IP address in the correct IP address range and does not have an Automatic Private IP Addressing (APIPA) address (an IP address in the 169.254.x.x range).
3. Ping the loopback address of 127.0.0.1 to verify that TCP/IP is installed and correctly configured on the local computer. If the ping is unsuccessful, this may indicate a corrupt TCP/IP stack or a problem with the network adapter.
4. Test whether you can ping the local IP address. If you can ping the loopback address but not the local IP address, there may be an issue with the routing table or with the network adapter driver.
5. Ping the IP address of a domain controller in the users' and computers' domain. Failing to ping the these domain controllers indicates a potential problem with the network in between the computer and the domain



controllers. Diagnose the problem further using Network troubleshooting procedures.
6. Ping the fully qualified name of a domain controller in the users' and computers' domain. Failing to ping the name of these domain controllers indicates a potential problem with name resolution between the computer and the domain controllers.
7. Follow Network troubleshooting procedures to diagnose the problem further (http://go.microsoft.com/fwlink/?LinkId=92706 ).

**Note:**

The steps listed above may have varying results if your network constrains or blocks ICMP packets.

Verify

Group Policy applies during computer startup and user logon. Afterward, Group Policy applies every 90 to 120 minutes. Events appearing in the event log may not reflect the most current state of Group Policy. Therefore, you should always refresh Group Policy to determine if Group Policy is working correctly.

To refresh Group Policy on a specific computer:

1. Open the **Start** menu. Click **All Programs** and then click **Accessories**.
2. Click **Command Prompt**.
3. In the command prompt window, type **gpupdate** and then press ENTER.
4. When the gpupdate command completes, open the Event Viewer.

Group Policy is working correctly if the last Group Policy event to appear in the System event log has one of the following event IDs:

- 1500
- 1501
- 1502
- 1503

## Windows event IDs

### Hunting suspicious Accounts

### Event IDs:

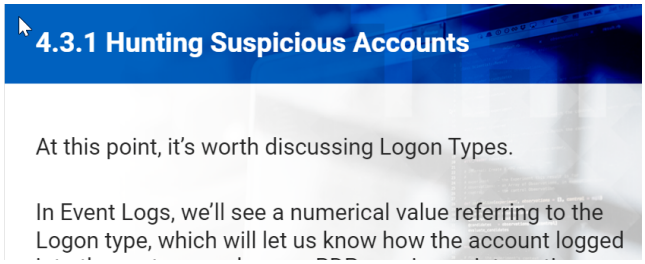
| | |
|---|---|
| **4624** | **Successful logo** |
| **4625** | **Failed logon** |
| **4634** | **Successful logoff** |
| **4647** | **User-initiated log off** |
| **4648** | **Logon using explicit credentials** |
| **4672** | **Special privileges assigned** |
| **4768** | **Kerberos ticket (TGT) requested** |
| **4769** | **Kerberos service ticket requested** |
| **4771** | **Kerberos pre-auth failed** |
| **4776** | **Attempt to validate credentials** |
| **4778** | **Session reconnected** |
| **4779** | **Session disconnected** |

### Event IDs specific to Account Management

| | |
|---|---|
| 4720 | Account created |
| 4722 | Account enabled |
| 4724 | Attempt to reset password |
| 4728 | User added to global group |
| 4732 | User added to local group |
| 4756 | User added to universal group |

### Finding the Elusive Active Directory Threat Hunting

https://adsecurity.org/wp-content/uploads/2017/04/2017-BSidesCharm-DetectingtheElusive-ActiveDirectoryThreatHunting-Final.pdf

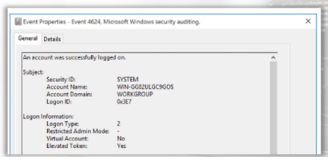


into the system, such as an RDP session or interactive logon.

## 4.3.1 Hunting Suspicious Accounts

**Logon Type 2** is an interactive login (a user physically logged into the computer).

- https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624



**Logon Type 2** is an interactive login (a user physically logged into the computer)
https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624

## 4.3.1 Hunting Suspicious Accounts

| Logon Type | Logon Title | Description |
|---|---|---|
| 2 | Interactive | A user physically logged onto this computer. |
| 3 | Network | A user or computer logged on from the network. |
| 4 | Batch | Used by batch servers where processes may be executing on behalf of a user, like scheduled tasks. |
| 5 | Service | A service started by the Service Control Manager. |
| 7 | Unlock | The workstation was unlocked. |
| 8 | NetworkClear text | Network credentials sent in cleartext. |
| 9 | NewCredentials | A caller cloned its current token and specified new credentials (runas command). |
| 10 | RemoteInteractive | A user logged onto computer using Terminal Services or RDP. |
| 11 | CachedInteractive | A user logged onto computer using network credentials which were stored locally on the computer. |

## 4.3.1 Hunting Suspicious Accounts

Another piece of information to note regarding Event IDs specific to accounts is the **Logon ID**.

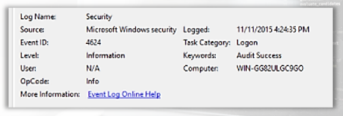
The Logon ID will let us know which Event ID is part of which logon session.

## 4.3.1 Hunting Suspicious Accounts

Start of session, **Event ID 4624,** and sessions ends, **Event ID 4634 or 4647**.

## 4.3.1 Hunting Suspicious Accounts

We will know the duration of the session by the timestamps at logon and at logoff by looking at the **Logged** field.




## 4.3.1 Hunting Suspicious Accounts

Another Event ID (also mentioned earlier) to hunt for would be **Event ID 4672** (Special privileges assigned to new logon).

We would like to see if there are any unusual accounts logged into machines with admin rights when they shouldn't have admin rights, or hunting for privileged local accounts being used to log into other machines remotely, instead of using legitimate network accounts.

**4672**
https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4672

## 4.3.1 Hunting Suspicious Accounts

Keep in mind that we will have to look at different sources to determine logon/session information via event logs.

Some event logs might be local to the workstation, but some might be on the server, such as the domain controller, or other machine that was accessed.

This outlines the importance of having a central logging server, which we discuss more in the upcoming slides.



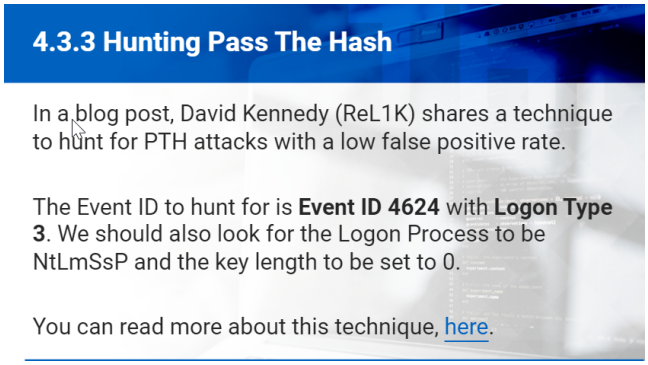
**Hunting for the Password Attacks**

## 4.3.2 Hunting Password Attacks

We will be looking for **Event ID 4625** (failed logon) and **Logon Type 3** (network logon).

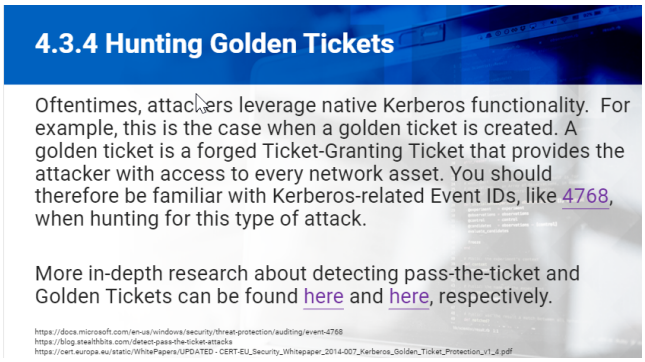
Overall, looking for a rapid succession of failed attempts to the same machine, or multiple machines, repeatedly in a small amount of time with each attempt, may indicate Password Spraying/Guessing attack. Of course, we know the attacker can change the timing between each attempt to make it look less suspicious.

**Hunting for the Pass the Hash**




**Hunting Golden Tickets**

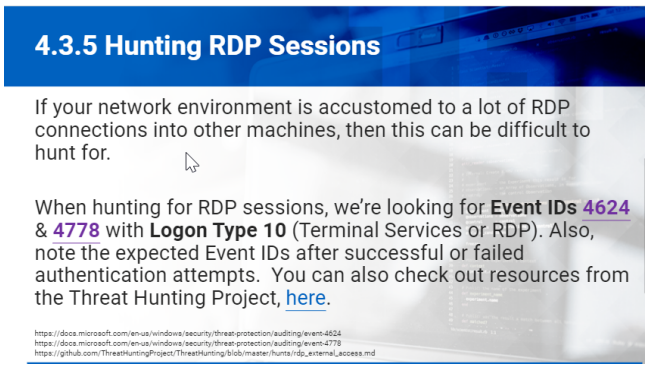
4768(S, F): A Kerberos authentication ticket (TGT) was requested.
https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4768




Researches about the detecting the ticket and golden tickets can be found

https://blog.netwrix.com/2022/09/28/how-to-detect-pass-the-ticket-attacks/

**Hunting RDP sessions**

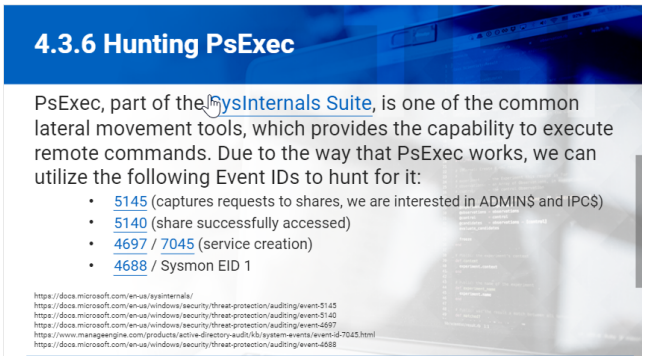



**4624(S):** An account was successfully logged on.
https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624

**4778(S):** A session was reconnected to a Window Station.
https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4778

Resources from threat hunting project
ThreatHuntingProject/ThreatHunting

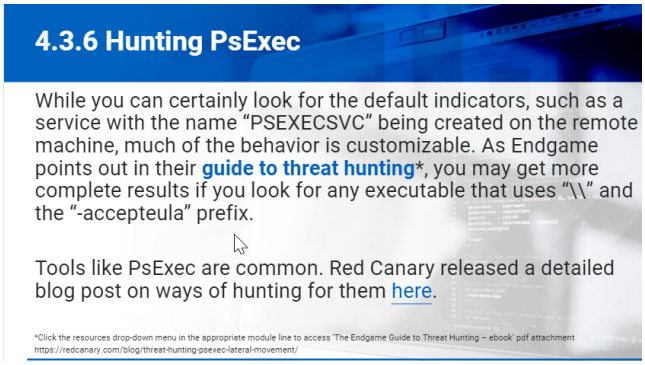
**Hunting PsEXec**




Sysinternals
https://learn.microsoft.com/en-us/sysinternals/

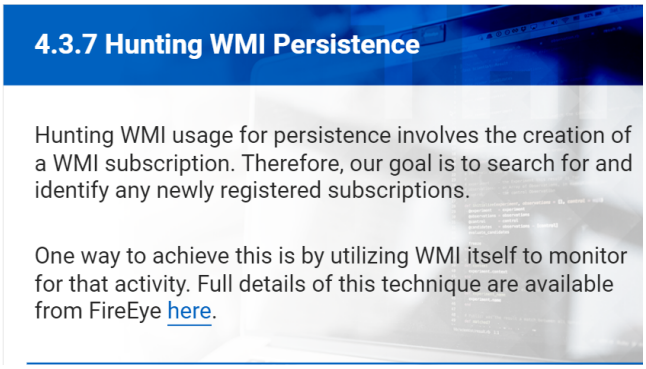
We can use this event IDs to hunt for PsEXec

| | |
|---|---|
| **5145** | Captures requests to shares, we are interested in ADMIN$ and IPC$ |
| **5140** | Share succesfully accessed |
| **4679/7045** | Service creation |
| **4688** | Sysmon EID 1 |




**Threat Hunting for PsExec, Open-Source Clones, and Other Lateral Movement Tools**
https://redcanary.com/blog/threat-hunting-psexec-lateral-movement/

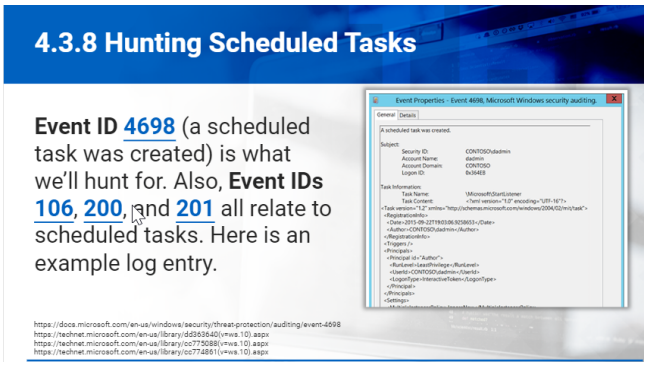
**Hunting WMI Persistence**




**WMI vs. WMI: Monitoring for Malicious Activity**

https://www.mandiant.com/resources/blog/wmi-vs-wmi-monitor

**Hunting for scheduled Tasks**




**4698(S): A scheduled task was created.**

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4698

**Event ID 106 — General Task Registration**
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd363640(v=ws.10)?redirectedfrom=MSDN

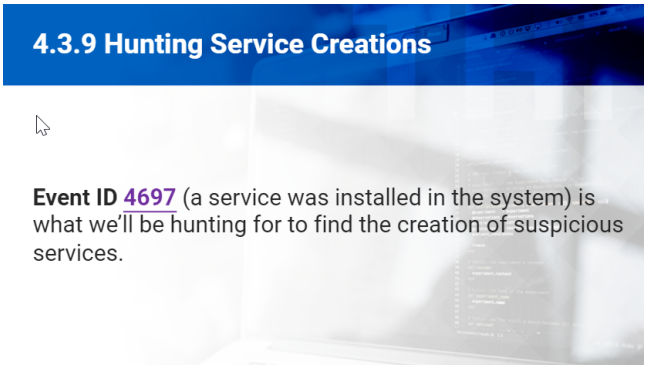
**Event ID 200 — Task Monitoring and Control**

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc775088(v=ws.10)?redirectedfrom=MSDN

**Event ID 201 — Task Monitoring and Control**

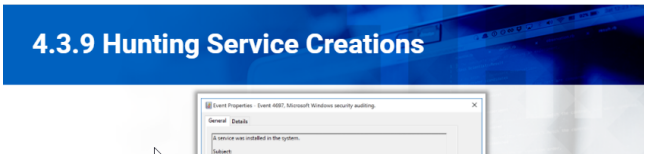
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc774861(v=ws.10)?redirectedfrom=MSDN

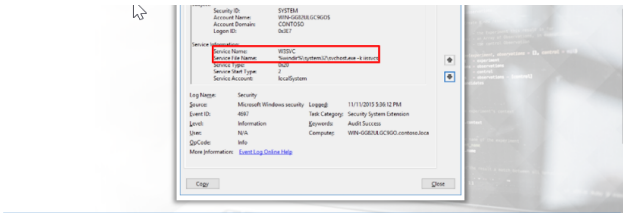
**Hunting For service creation**



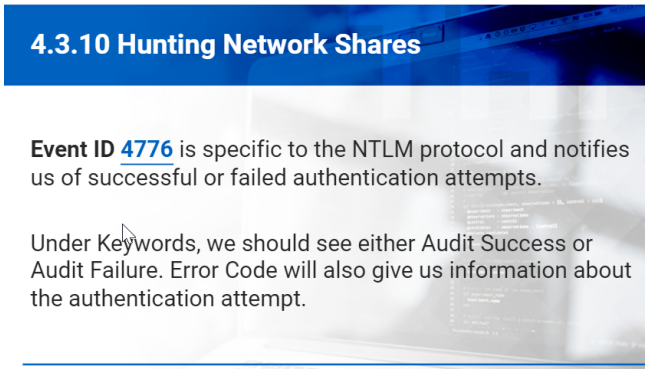

**EventID 4697**

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4698





**Hunting for Network shares**




**4777(F): The domain controller failed to validate the credentials for an account.**

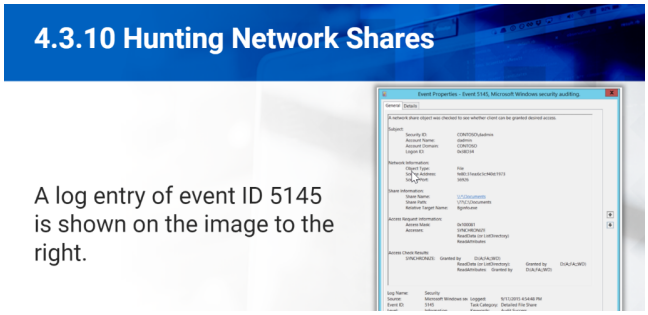
https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4777


**5140(S, F): A network share object was accessed**

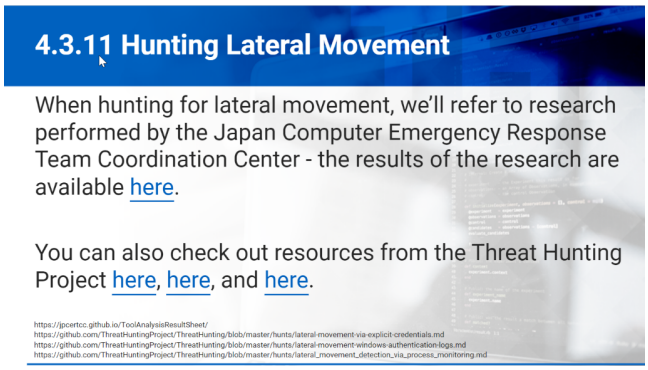
https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-5140

**5148(F): The Windows Filtering Platform has detected a DoS attack and entered a defensive mode; packets associated with this attack will be discarded.**

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-5148



**Hunting for lateral movement**




**Research paper from Japan Computer Emergency Response Team.**

https://jpcertcc.github.io/ToolAnalysisResultSheet/

**Windows Lateral Movement via Explicit Credentials**
ThreatHuntingProject/ThreatHunting

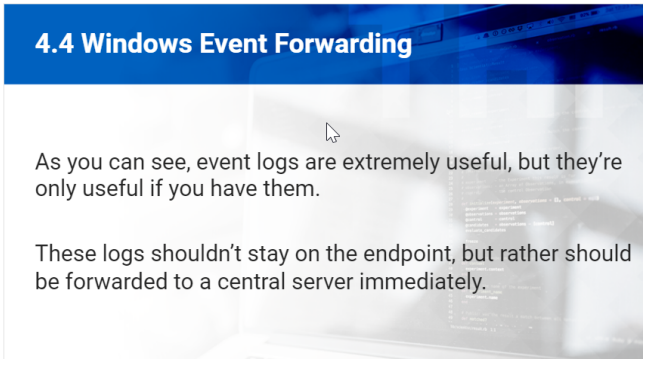
**Detecting Lateral Movement in Windows Event Logs**

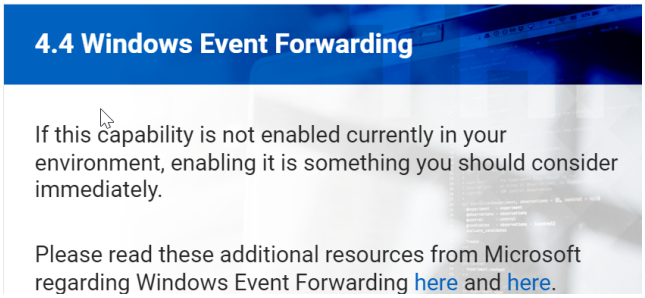
https://github.com/ThreatHuntingProject/ThreatHunting/blob/master/hunts/lateral-movement-windows-authentication-logs.md#detecting-lateral-movement-in-windows-event-logs

**#Lateral Movement Detection via Process Monitoring**

https://github.com/ThreatHuntingProject/ThreatHunting/blob/master/hunts/lateral_movement_detection_via_process_monitoring.md

**Windows Event Forwarding**



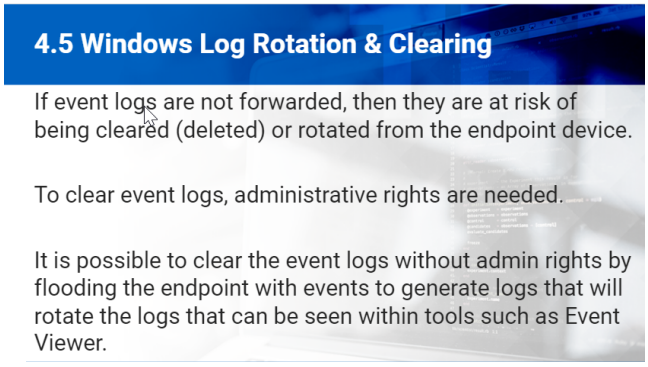

**Use Windows Event Forwarding to help with intrusion detection**

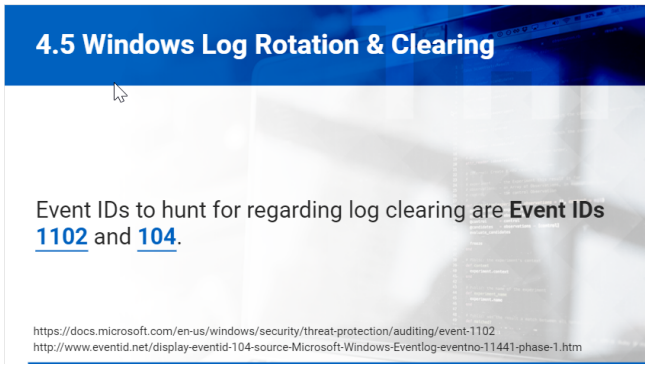
https://learn.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection

**Windows Event Collector**

https://learn.microsoft.com/en-in/windows/win32/wec/windows-event-collector?redirectedfrom=MSDN

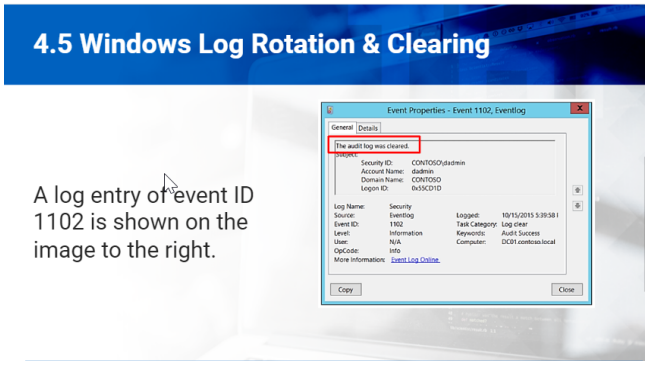
**Windows Log Rotation a& Clearing**

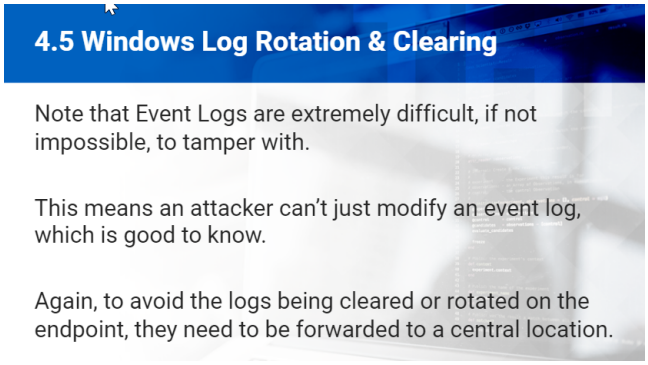


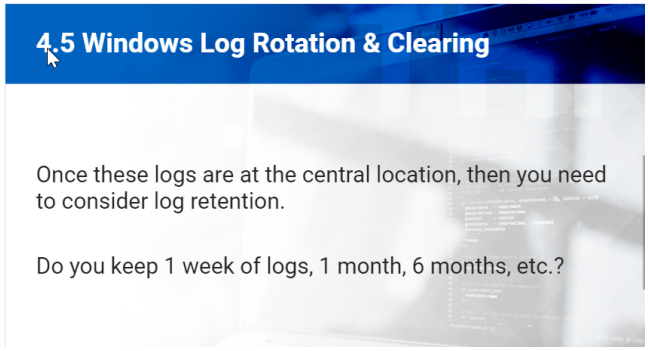




**1102(S): The audit log was cleared.**

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-1102

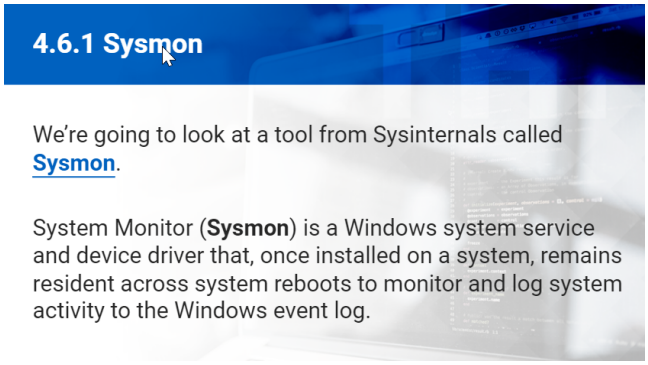




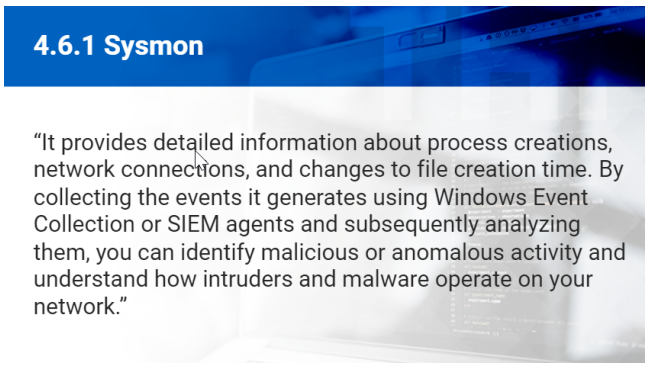



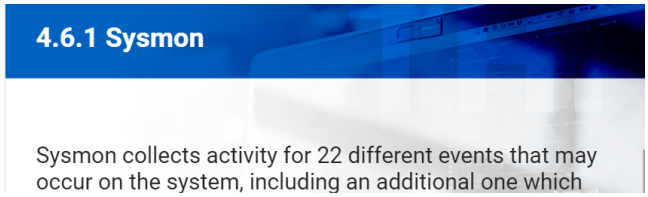

## Tools

### Sysmon




https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon



indicates an error within Sysmon itself.

A list of all Event IDs is shown on the next slide.

## 4.6.1 Sysmon

| Event description | Event ID |
|---|---|
| Process Create | 1 |
| File creation time changed | 2 |
| Network connection detected | 3 |
| Sysmon service state change | 4 |
| Process terminated | 5 |
| Driver loaded | 6 |
| Image loaded | 7 |
| CreateRemoteThread detected | 8 |
| RawAccessRead detected | 9 |
| Process accessed | 10 |

| Event description | Event ID |
|---|---|
| File created | 11 |
| Registry object added or deleted | 12 |
| Registry value set | 13 |
| Registry object renamed | 14 |
| File stream created | 15 |
| Sysmon configuration change | 16 |
| Named pipe created | 17 |
| Named pipe connected | 18 |
| WMI filter | 19 |
| WMI consumer | 20 |

| Event description | Event ID |
|---|---|
| WMI consumer filter | 21 |
| DNS query | 22 |
| Error | 255 |

## 4.6.1 Sysmon

Sysmon should be installed on all systems, which will ensure that data from them is available when you need it, either for Threat Hunting or for digital forensics and incident response (DFIR).

The events should be forwarded to a SIEM (discussed later in the module) to prevent deletion by adversaries, and for utilizing them centrally to detect anomalous activity on both single systems and also across multiple systems.

## 4.6.1 Sysmon

Sysmon requires configuration to be set, which tells it what events to capture, and whether to exclude certain events which are “known good”, for example.

The most widespread and recommended base configuration is the one from SwiftOnSecurity, available here. It can be used as a baseline, but additional configuration for your specific environment is also necessary and recommended.

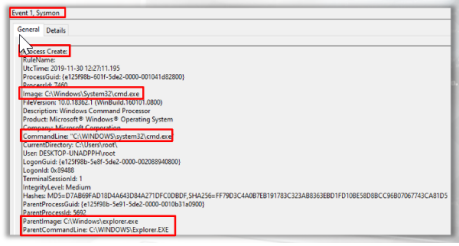
**sysmon-config | A Sysmon configuration file for everybody to fork**

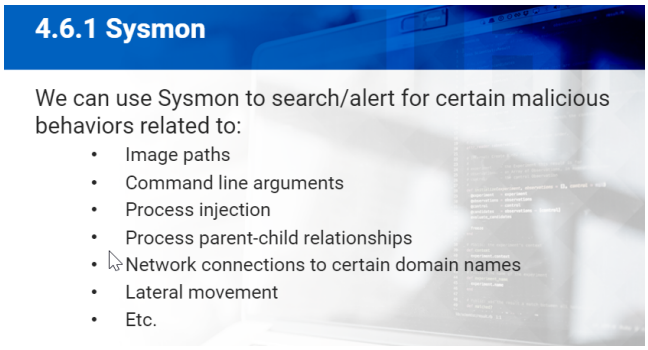
SwiftOnSecurity/sysmon-config

**Example**

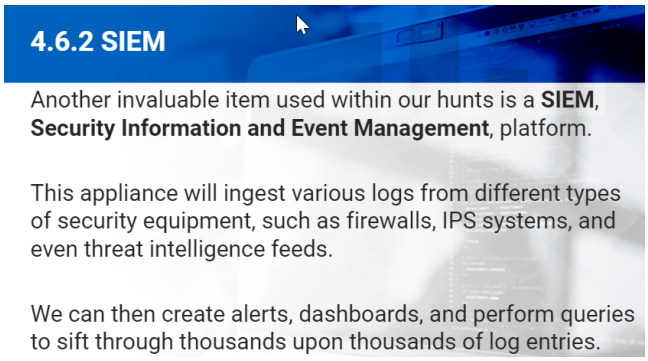
## 4.6.1 Sysmon

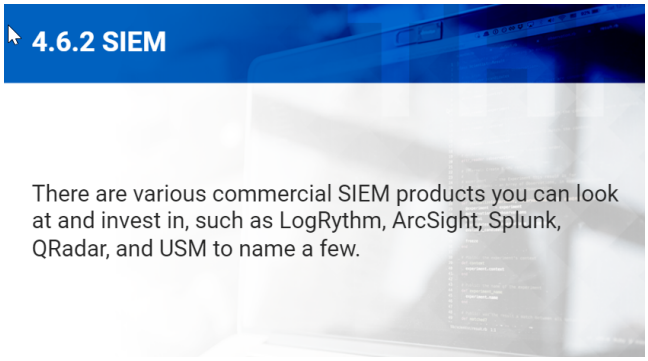
An example of Sysmon log event (ID 1) is shown below:



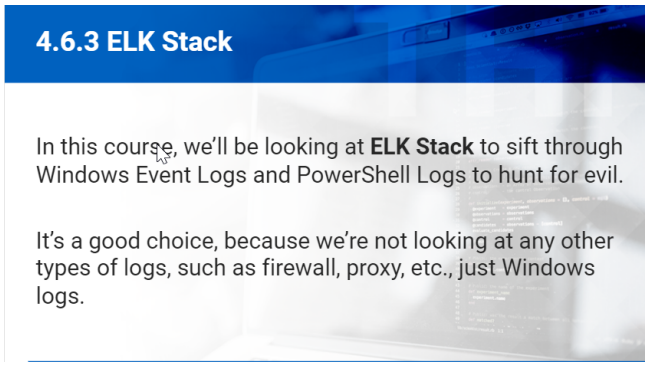


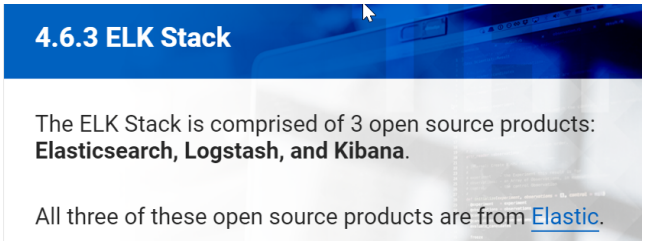

**SIEM**




**ELK Stack**



You can read more about the ELK Stack, including tutorials on how to implement and use these products here.

THE COMPLETE GUIDE TO THE ELK STACK

https://logz.io/learn/complete-guide-elk-stack/

CHOOSING THE RIGHT SIEM SOLUTION FOR YOUR NEEDS

https://www.netsurion.com/EventTracker/media/EventTracker/Files/whitepapers/WP-SIEM-Choosing.pdf

Splunk vs ELK: Which Works Best For You?

https://www.upguard.com/blog/splunk-vs-elk

a