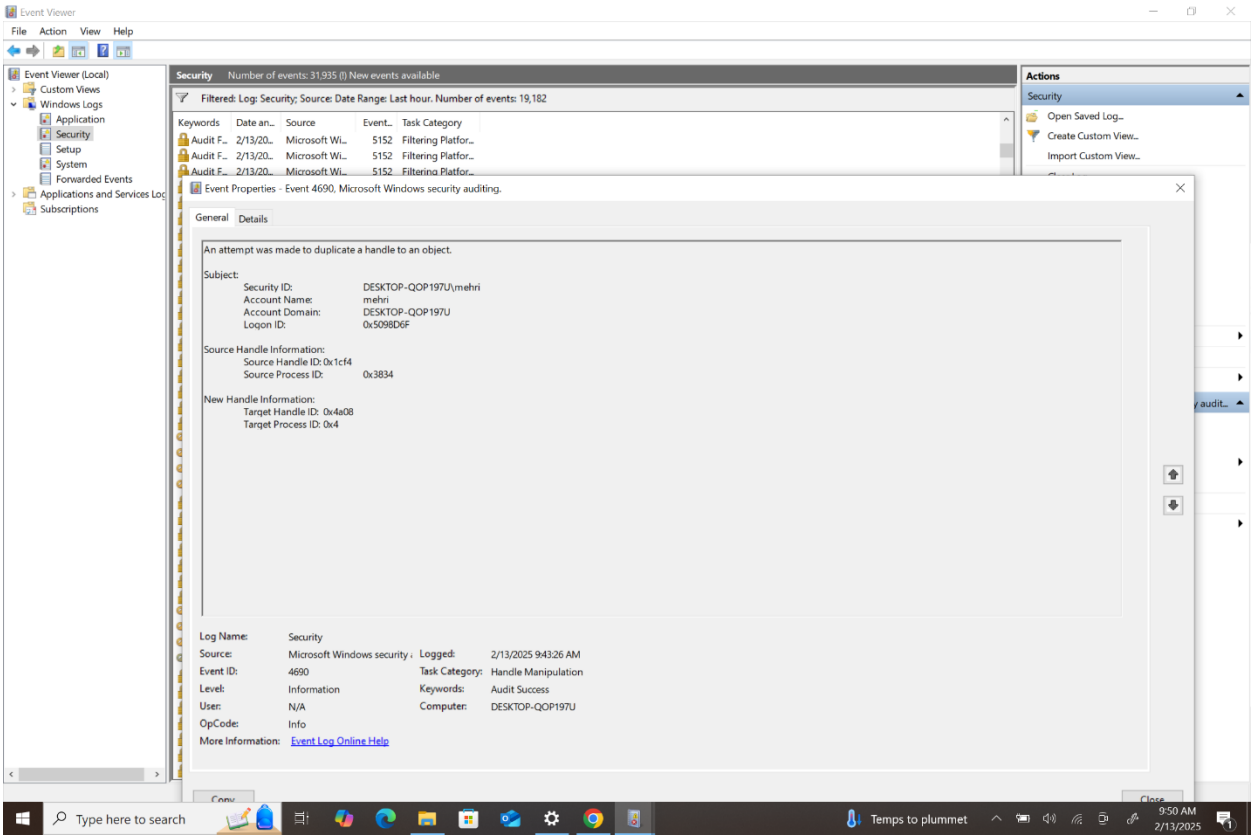
Threat Analysis Using MITRE ATT&CK Framework by Mehrier B. Touhid

The PowerShell was run at 2/13/2025 at 9 :43AM

The following occurred in the computer:

- A desktop foler " System LoG Test" was created
- The folder created 4 text files and deleted another one after creating
- One text file called "systeminfo" has a detailed list of all programs installed on the current computer .

Looking into the event viewer we find the following logs that map to the described MITRE Att&ck tactics.



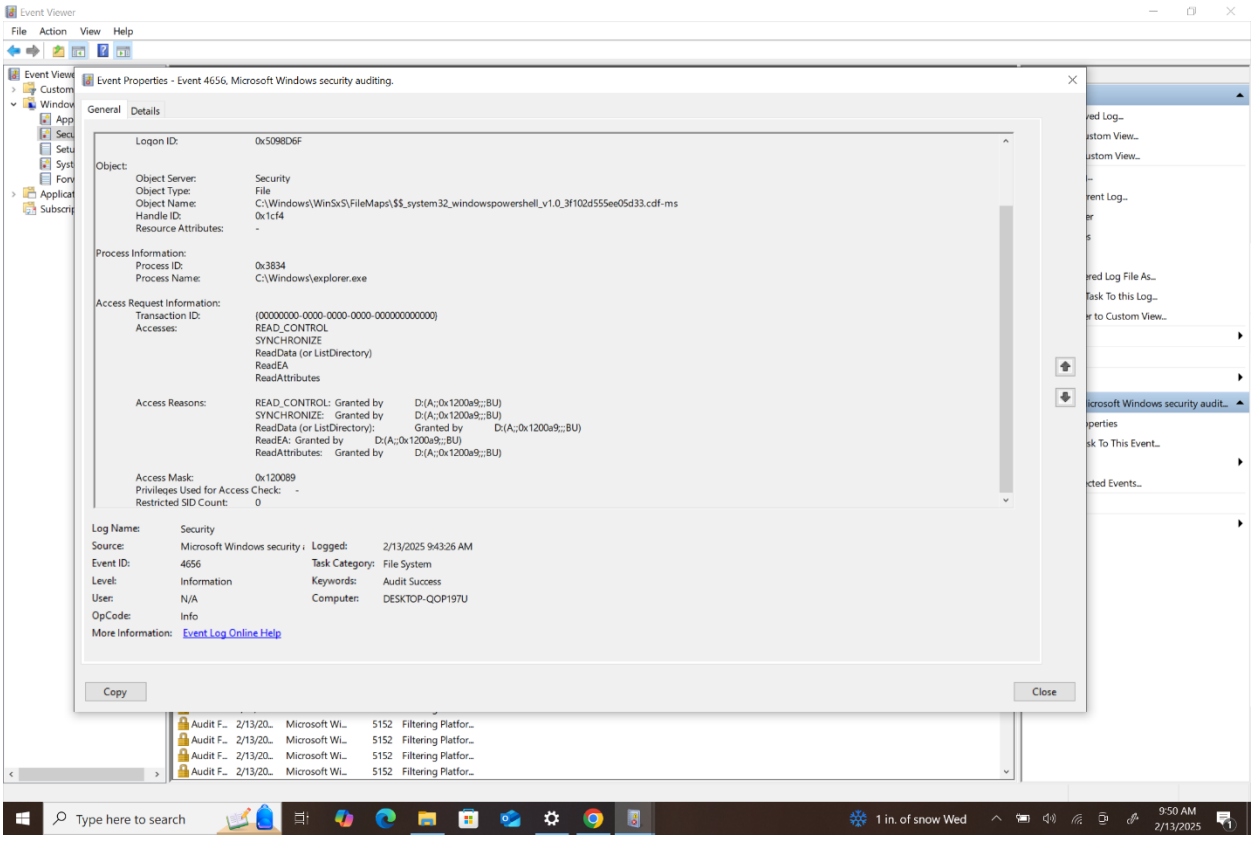
Tacticts: Privilege Escalation (TA0004) & Defense Evasion (TA0005)

Process Injection (T1055)

Handle duplication is often associated with process injection techniques, where an attacker attempts to manipulate process memory to execute malicious code within another process.

Technique: Access Token Manipulation (T1134)

If the duplicated handle is used to access another process's token, it could be an attempt to elevate privileges or impersonate another user



Tactic : Credential Access (TA0006) & Discovery (TA0007)

File and Directory Discovery (T1083)

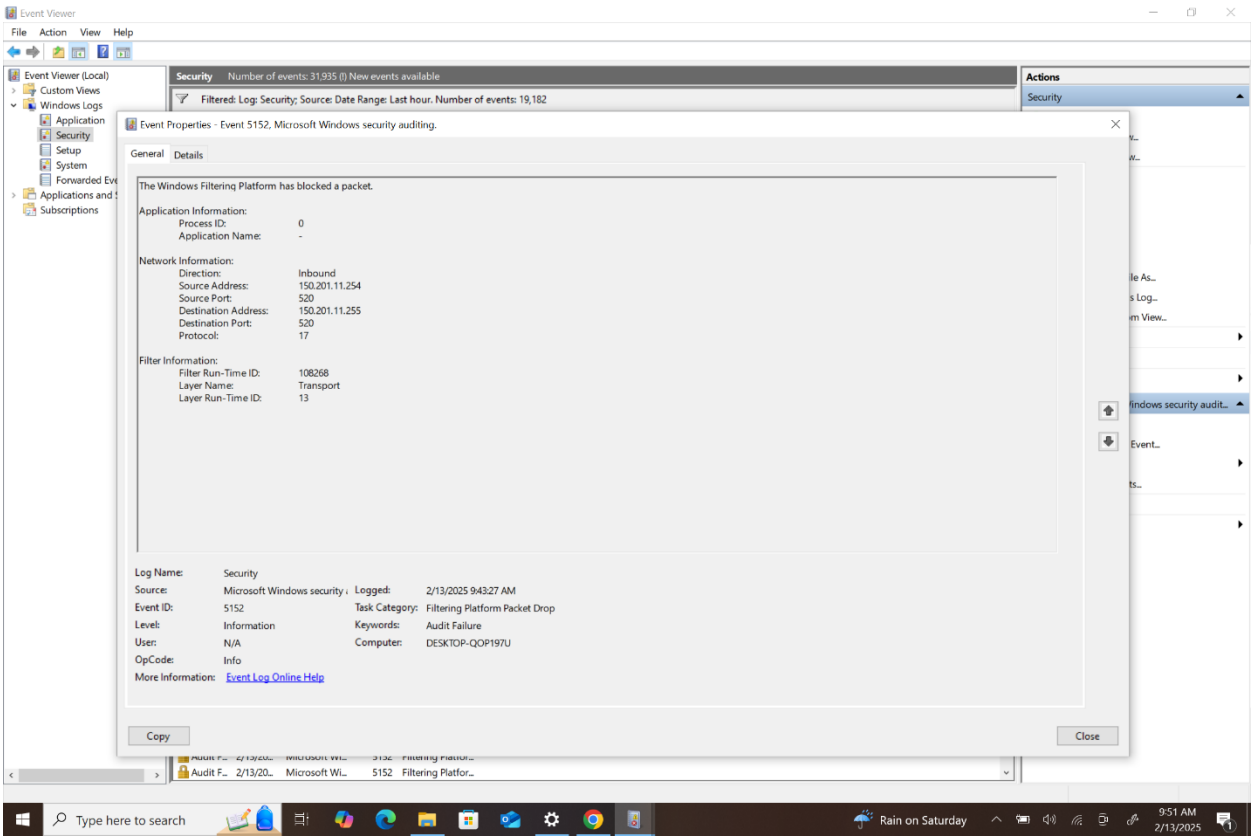
The log shows access to a file related to Windows PowerShell within the WinSxS (Windows Side-by-Side) directory, suggesting an attempt to read or manipulate system files.

Permission Groups Discovery (T1069)

If an attacker is enumerating access control lists (ACLs) or attempting to access restricted files, this event could indicate reconnaissance for privilege escalation.

Accessing Sensitive Files (T1005)

If the accessed file contains credentials, configurations, or sensitive system information, this event could indicate an attempt to gather such data.



Tactic : Defense Evasion (TA0005) & Command and Control (TA0011)

Network Denial of Service (T1498)

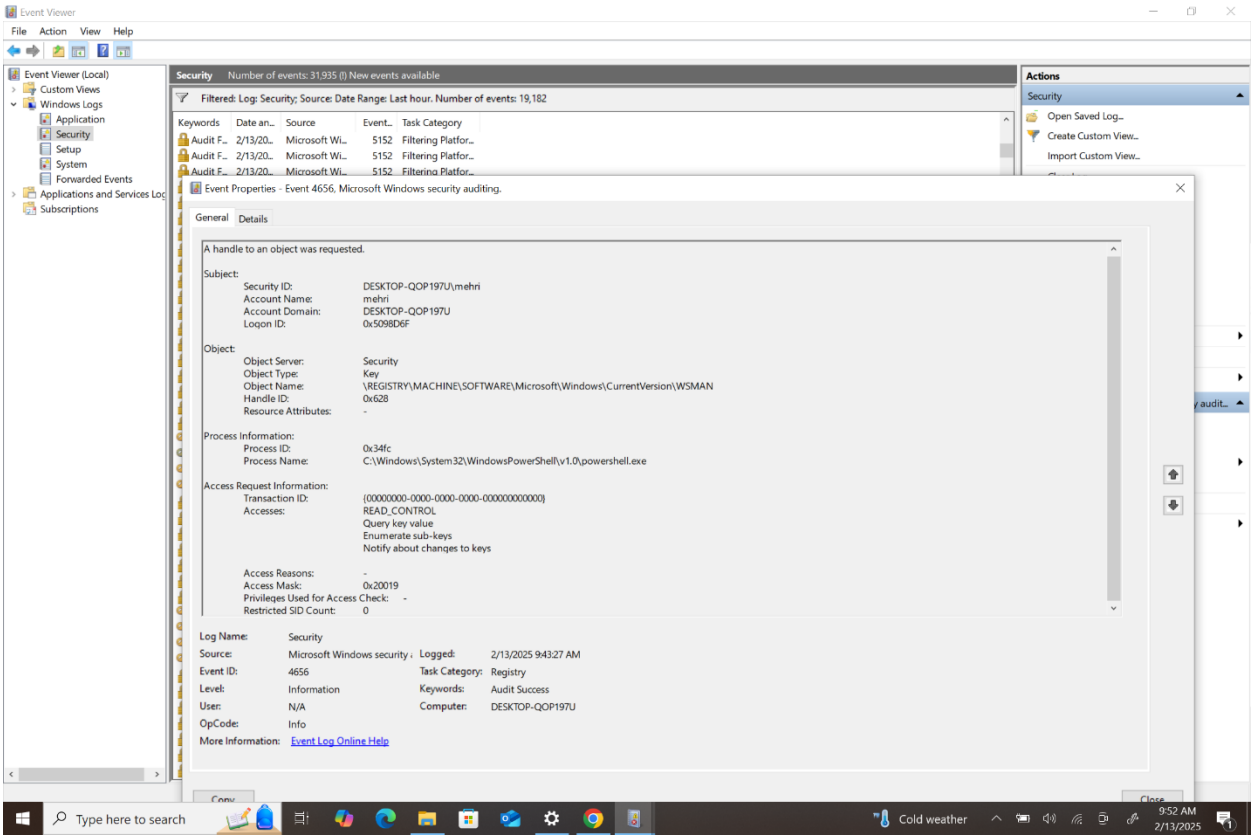
If this blocked packet was part of repeated or unusual network traffic, it could indicate an attempt to overload network resources.

Unsecured Network Communication (T1071)

The blocked packet is using UDP protocol on port 520, which is associated with RIP (Routing Information Protocol). Attackers sometimes abuse RIP for reconnaissance or network manipulation.

Ingress/Egress Filtering (T1048)

If this event occurs frequently, it may suggest an attempt to exfiltrate data or bypass firewall rules, but the system is blocking it.



Tactic **: T1003.002 - OS Credential Dumping: Security Account Manager (SAM)**

T1082 - System Information Discovery

The registry key accessed is related to Windows Remote Management (WSMAN), which could be part of reconnaissance or privilege escalation.

T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Attackers may access registry keys to establish persistence.

Suggested Defensive measures to prevent these attack tactics from being executed :

- ✓ Setup SIEM Tool such as Splunk to Monitor any suspicious activity .

- ✓ Configure Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) like Zeek ,Suricata & Snort .

- ✓ Configure Firewall settings to block any malicious IP

- ✓ Setup Antivirus that would block any harmful files that create ,modify files or system settings .