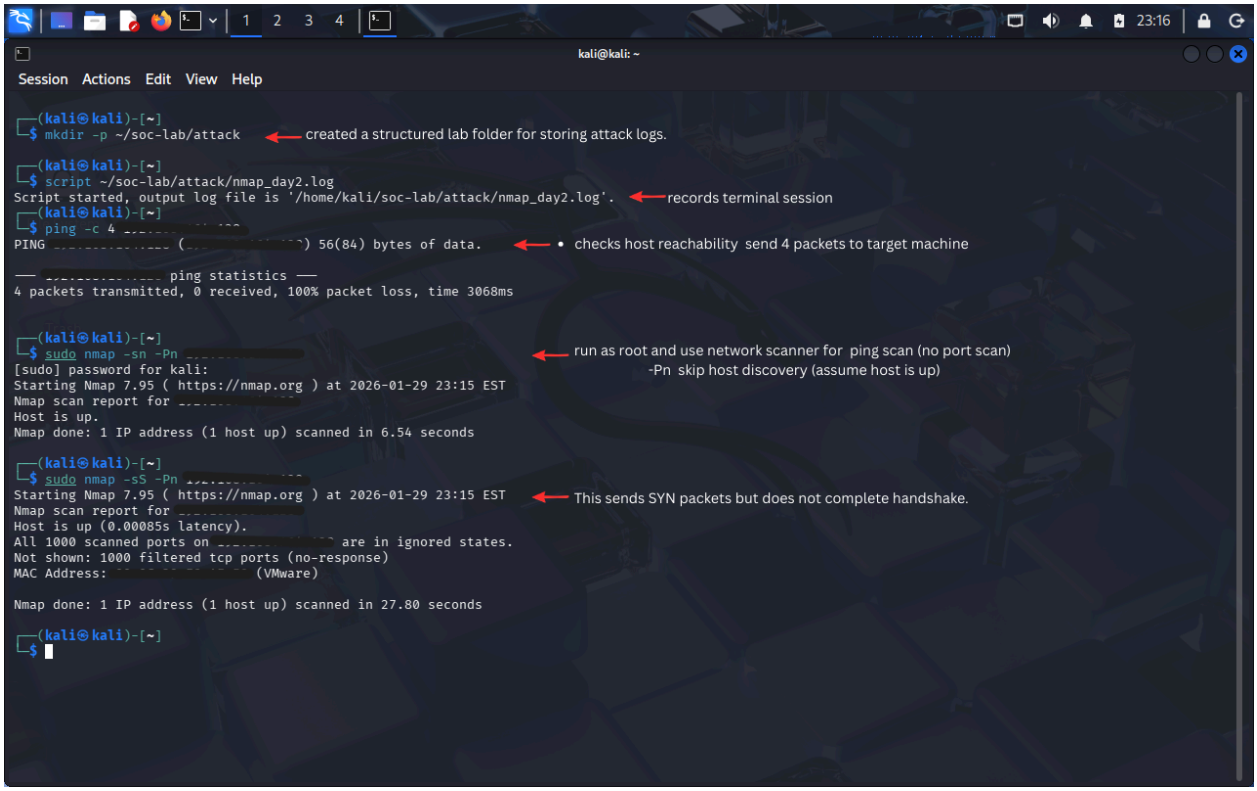
Technical Evidence: Network Reconnaissance Lab

Lab Objective: To detect and analyze network reconnaissance using native Windows security telemetry.

Key Findings: Confirmed that **Windows Filtering Platform (WFP)** successfully neutralized stealth scans, generating high-fidelity logs (Event ID 5157).

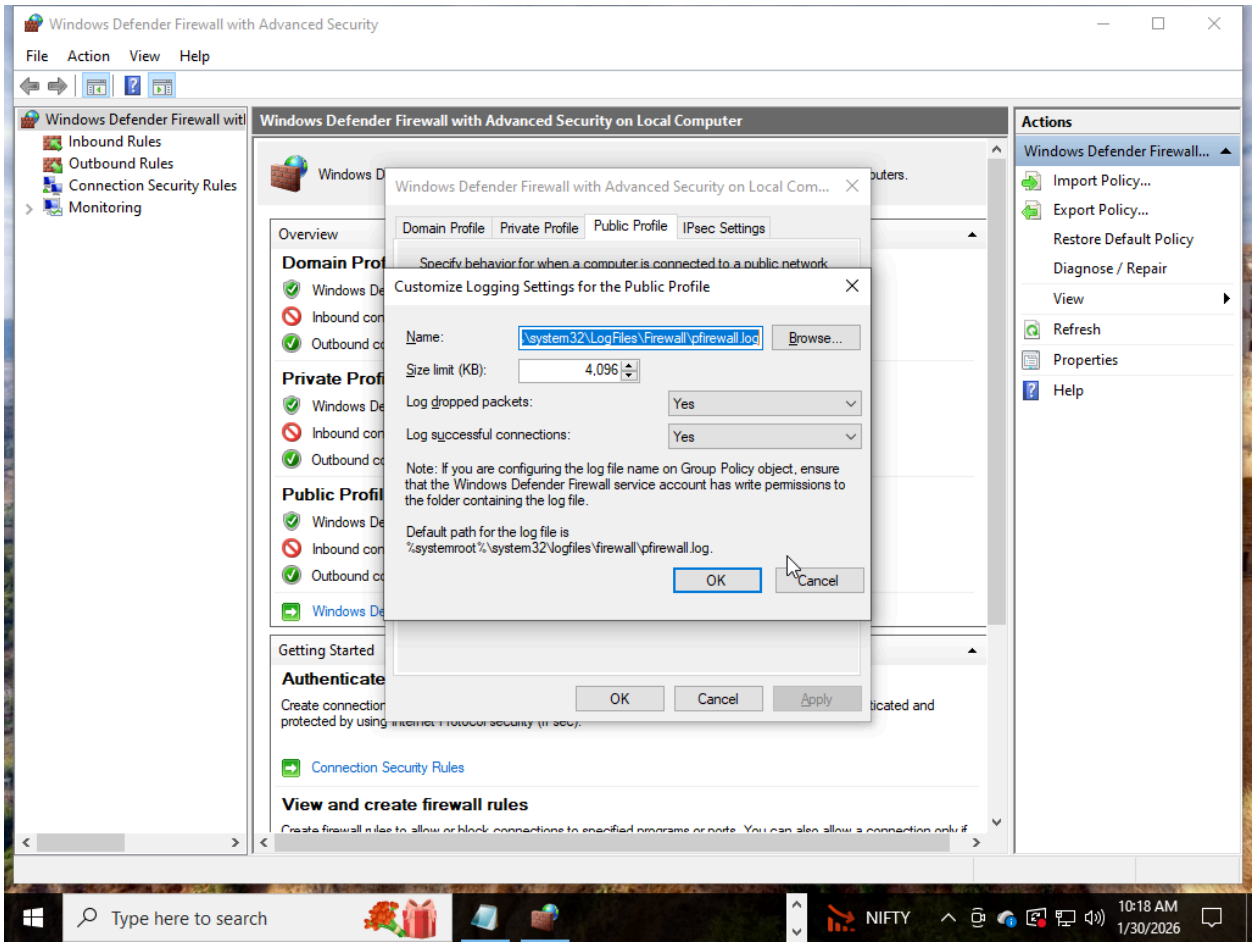
Kali: Attacker-side Nmap results showing filtered ports.



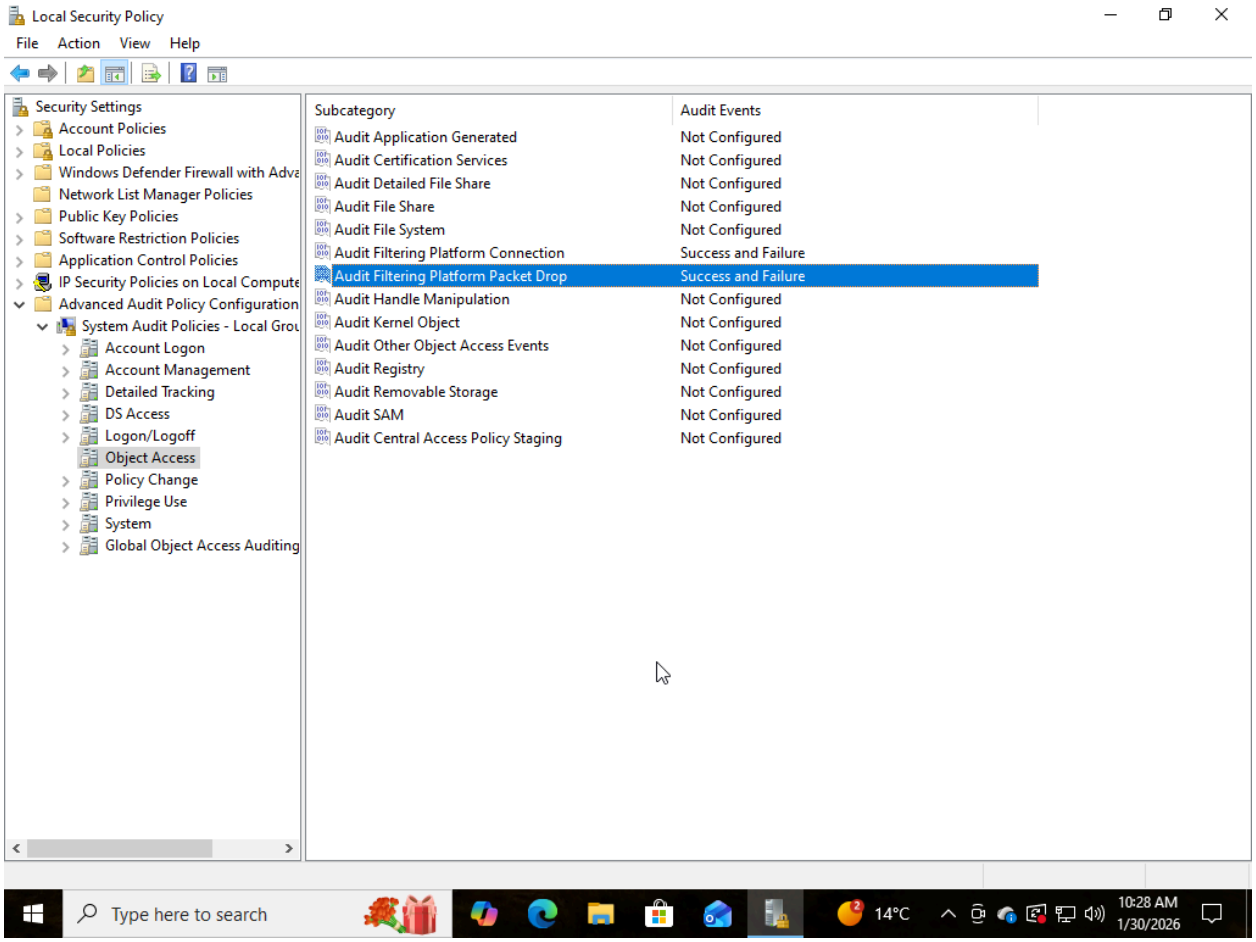
Reconnaissance Summary Report

- A controlled Nmap reconnaissance scan was conducted against the target host Target IP.
- Initial ICMP ping test resulted in 100% packet loss, indicating ICMP traffic is likely blocked.
- Host discovery using `nmap -sn -Pn` confirmed the target system is online.
- A TCP SYN scan (`-sS`) was performed to identify open ports.
- All top 1000 TCP ports were reported as filtered, suggesting active firewall filtering.
- Service version detection (`-sV`) did not identify any services due to absence of open ports.
- The target MAC address indicates the system is running in a VMware virtualized environment.
- Network distance was determined to be 1 hop, confirming the host is on the same local network segment.
- Overall assessment indicates a live host protected by firewall rules blocking inbound TCP connections.

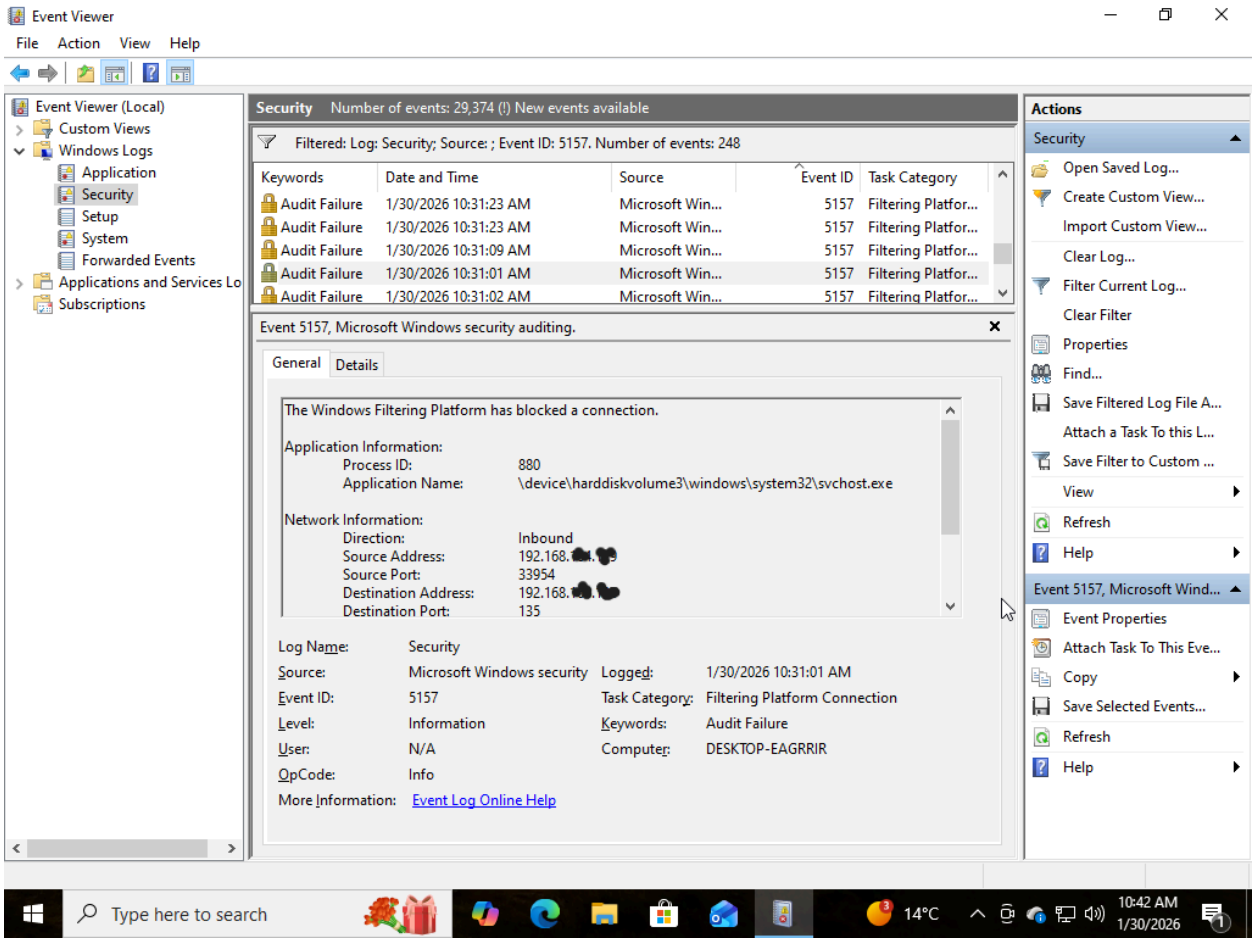
Windows: Defender-side WFP block events matching attack timestamps.



Windows Firewall logs configuration



Windows 10 Rules and Policy Change



Windows Event Viewer: event 5157 blocked

Firewall Monitoring and Logging Configuration Report

- Windows Defender Firewall logging was enabled for the Public Profile.
- Log file configured at the default path: %systemroot%\system32\logfiles\firewall\pfirewall.log.
- Log size limit set to 4096 KB.
- Logging of dropped packets enabled.
- Logging of successful connections enabled.
- Advanced Audit Policy Configuration was modified under Local Security Policy.
- “Audit Filtering Platform Connection” configured for Success and Failure.
- “Audit Filtering Platform Packet Drop” configured for Success and Failure.
- These settings ensure firewall connection attempts and packet drops are recorded in the Security log.
- Event Viewer (Security Log) shows multiple Event ID 5157 entries.
- Event ID 5157 indicates Windows Filtering Platform blocked a network connection.
- Blocked traffic was inbound.

- Destination port 135 (RPC) was targeted.
- The blocking process identified as svchost.exe.
- The system successfully logged firewall enforcement actions for monitoring and investigation.

Assessment:
The firewall is actively blocking inbound connections and audit logging is properly configured to record both successful and failed filtering events, enabling effective SOC monitoring and analysis.