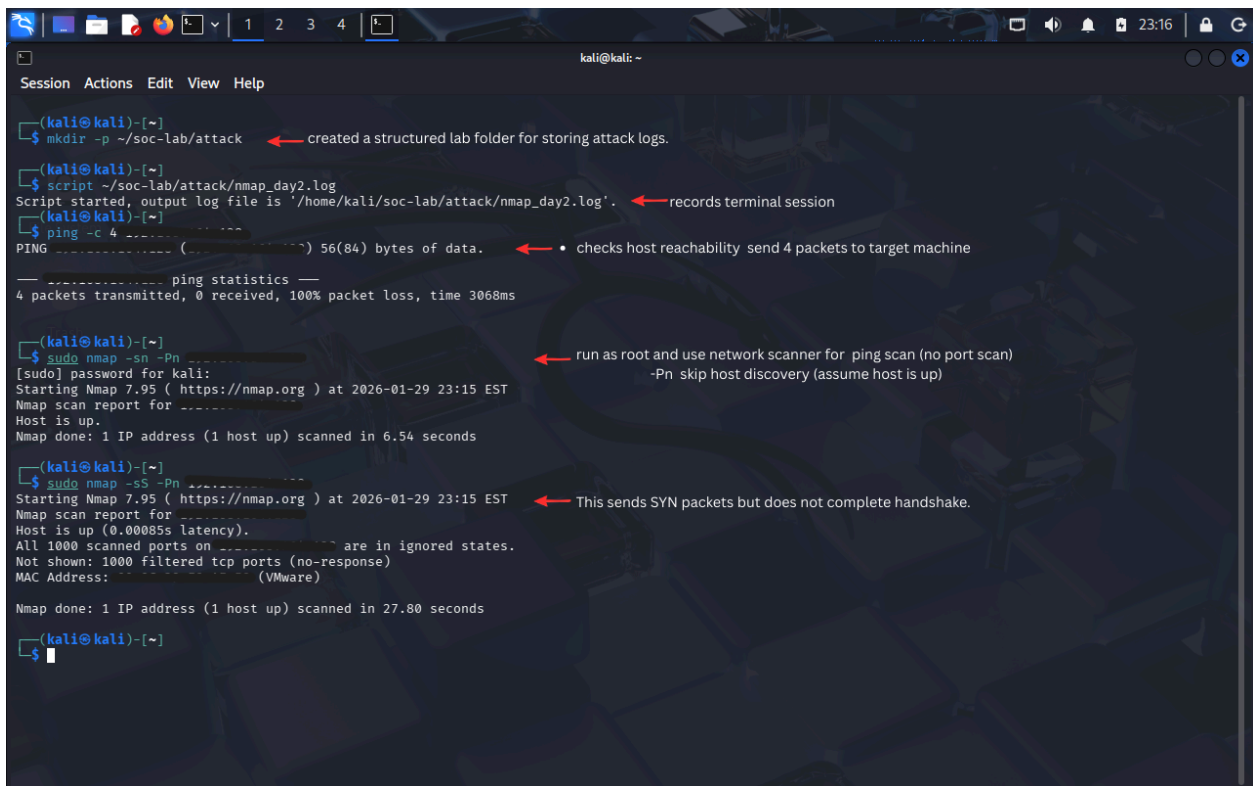


Technical Evidence: Network Reconnaissance Lab

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.



```
(kali@kali)-[~]
└─$ mkdir -p ~/soc-lab/attack ← created a structured lab folder for storing attack logs.

(kali@kali)-[~]
└─$ script ~/soc-lab/attack/nmap_day2.log
Script started, output log file is '/home/kali/soc-lab/attack/nmap_day2.log'. ← records terminal session

(kali@kali)-[~]
└─$ ping -c 4 10.10.10.10
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data. ← • checks host reachability send 4 packets to target machine
---
0.000000 0.000000 0.000000 0.000000 0.000000 0.000000
---
ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3068ms

(kali@kali)-[~]
└─$ sudo nmap -sn -Pn 10.10.10.10 ← run as root and use network scanner for ping scan (no port scan)
                                     -Pn skip host discovery (assume host is up)
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-29 23:15 EST
Nmap scan report for 10.10.10.10
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 6.54 seconds

(kali@kali)-[~]
└─$ sudo nmap -sS -Pn 10.10.10.10 ← This sends SYN packets but does not complete handshake.
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-29 23:15 EST
Nmap scan report for 10.10.10.10
Host is up (0.00085s latency).
All 1000 scanned ports on 10.10.10.10 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:00:00:00 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 27.80 seconds

(kali@kali)-[~]
└─$
```

```
(kali@kali)-[~]
└─$ sudo nmap -sS -sV -Pn 192.168.100.1
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-29 23:17 EST
Nmap scan report for 192.168.164.128
Host is up (0.00035s latency).
All 1000 scanned ports on 192.168.164.128 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:0C:29:E8:AE:58 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.09 seconds

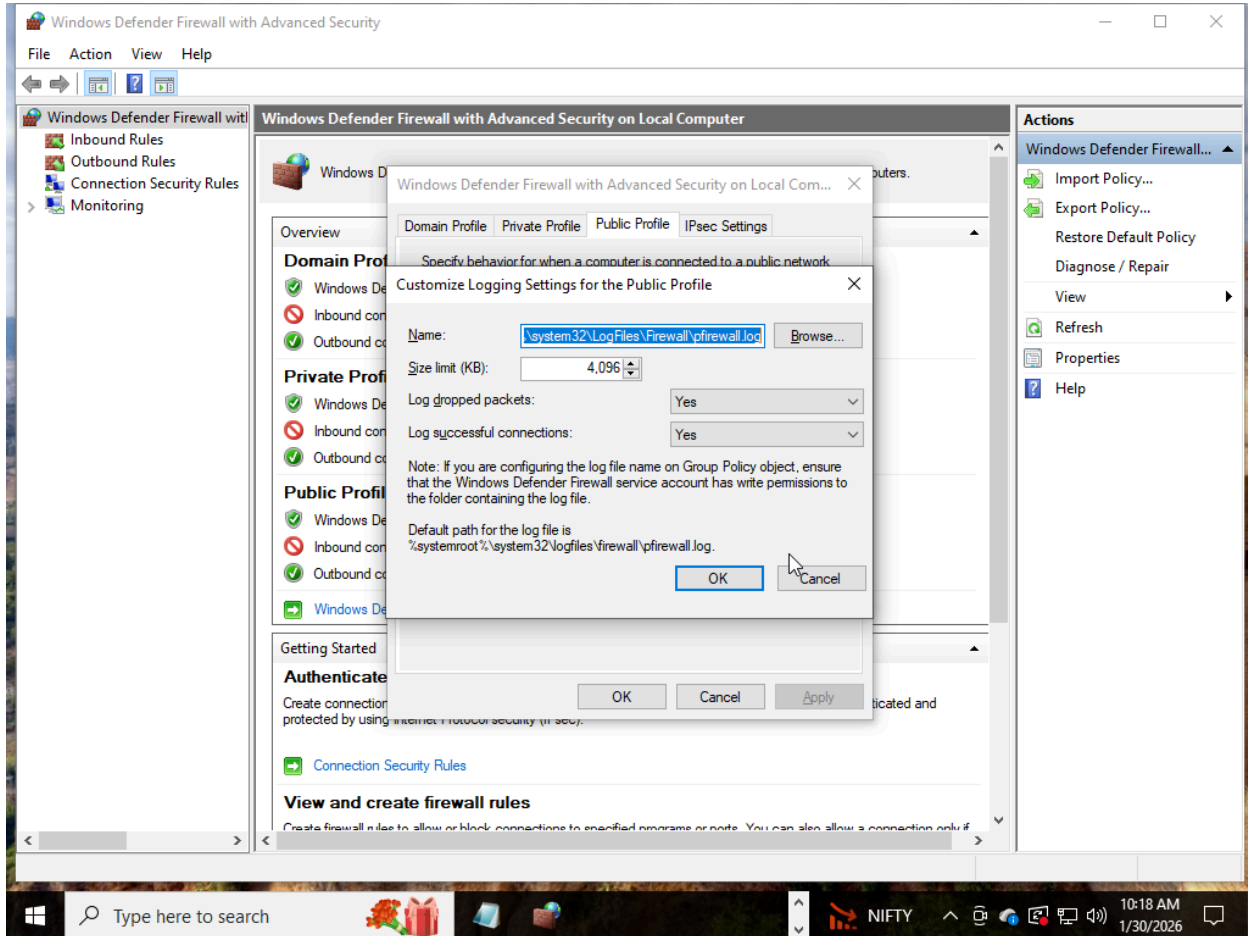
(kali@kali)-[~]
└─$
```

performed a SYN stealth scan with service detection while skipping ping, but all ports were filtered by the firewall so no services were identified.

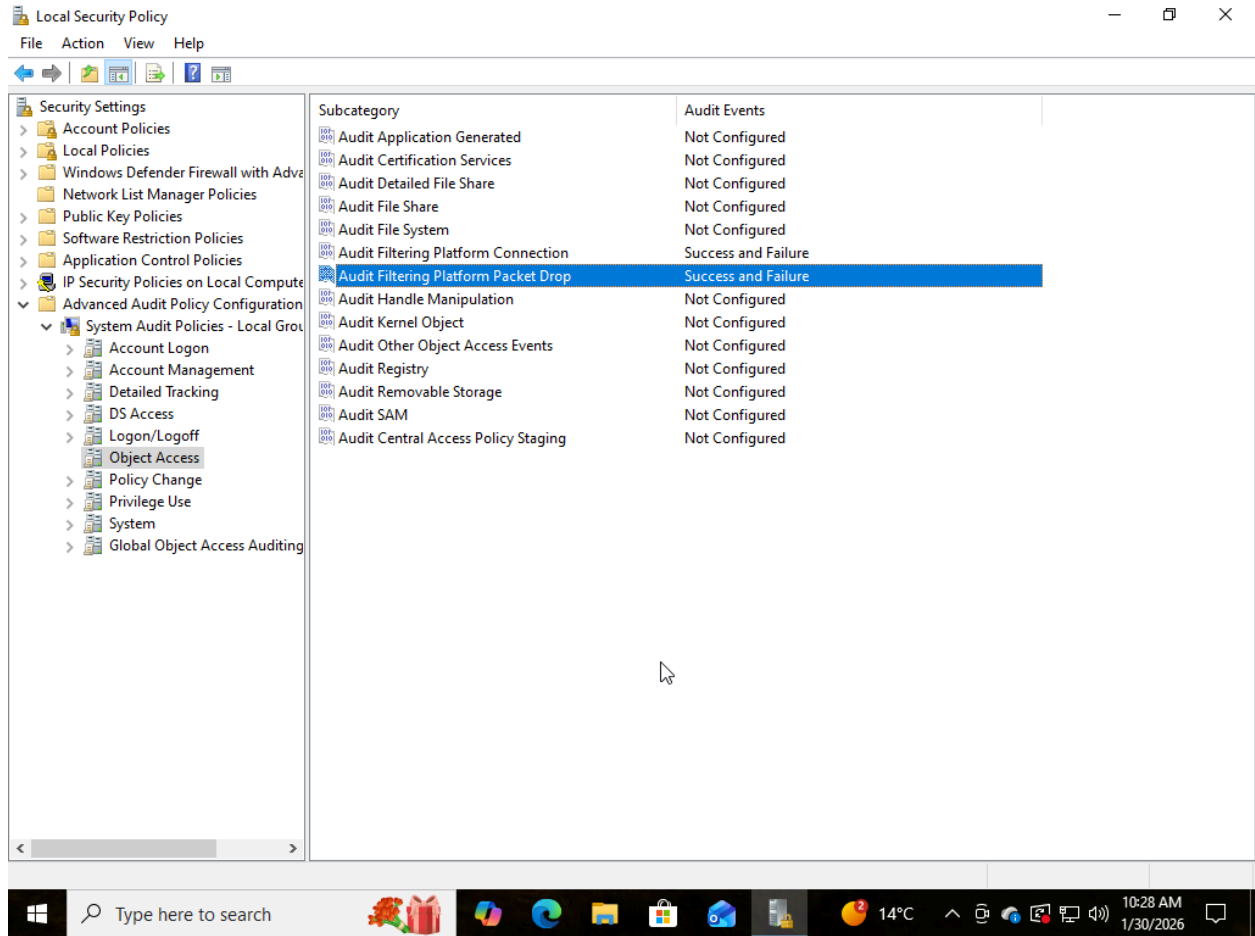
Reconnaissance Summary Report

- 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.

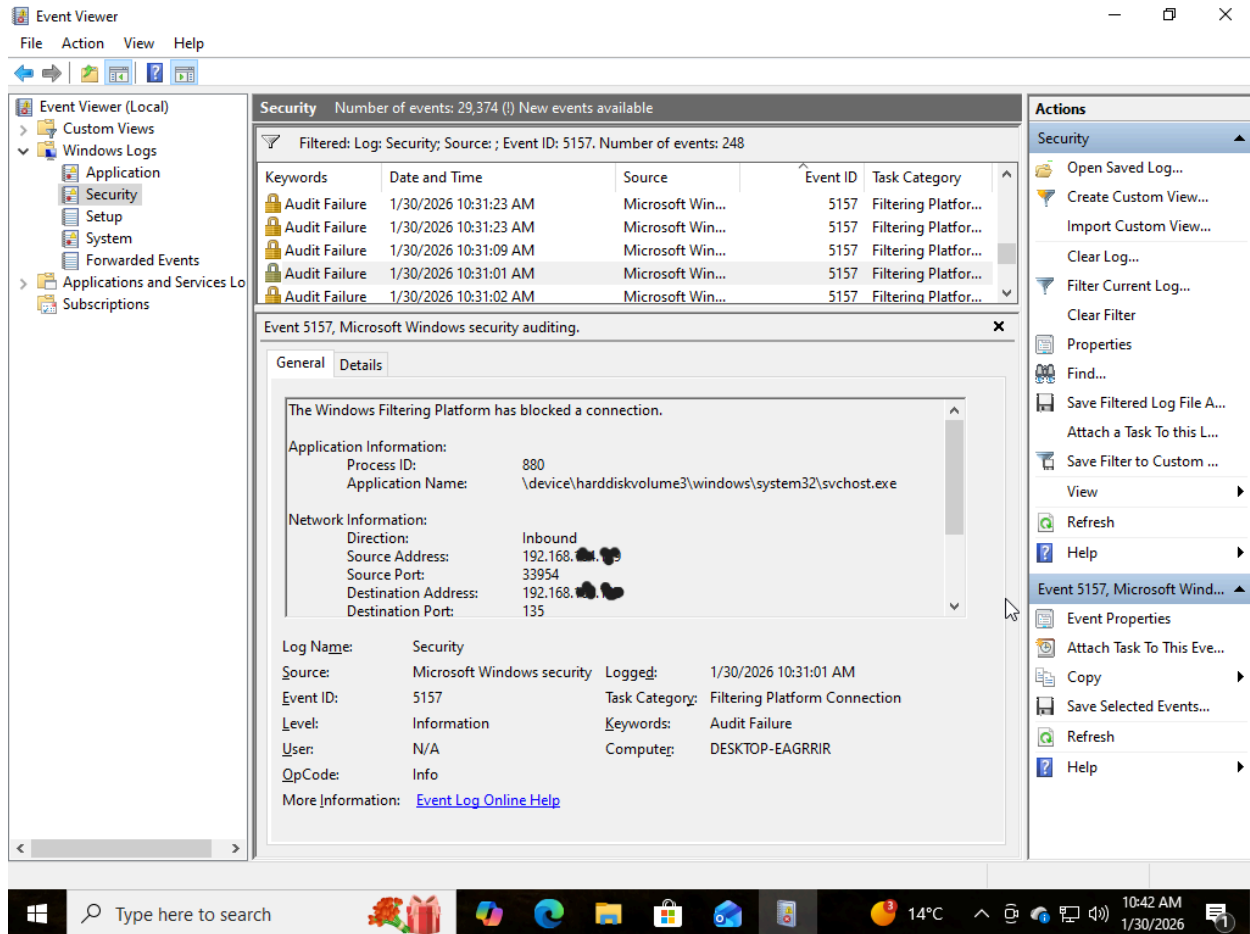
Windows: Defender-side WFP block events matching attack timestamps.



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.