

# 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

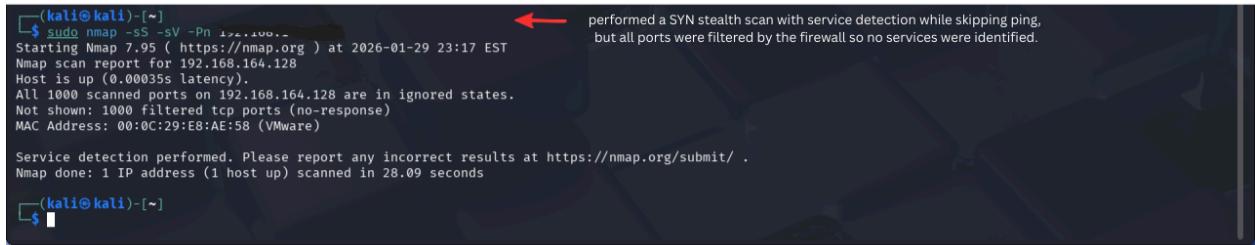
(kali㉿kali)-[~]
$ ping -c 4 ...
PING ... (...) 56(84) bytes of data.   ← • checks host reachability send 4 packets to target machine
...
ping statistics ...
4 packets transmitted, 0 received, 100% packet loss, time 3068ms

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

(kali㉿kali)-[~]
$ sudo nmap -sS ...
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-29 23:15 EST
Nmap scan report for ...
Host is up (0.00085s latency).
All 1000 scanned ports on ... are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: ... (VMware)

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

(kali㉿kali)-[~]
```



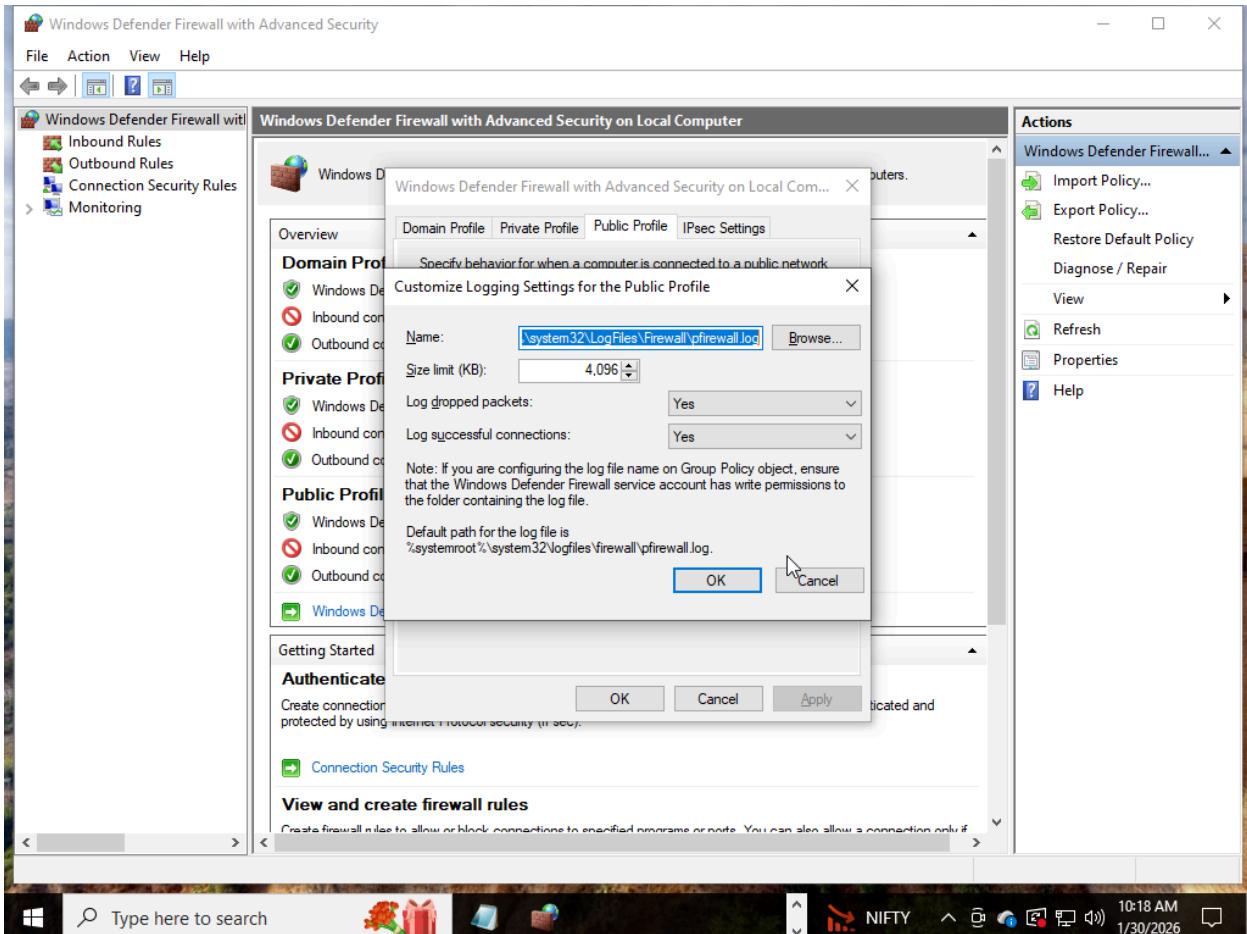
```
(kali㉿kali)-[~] $ sudo nmap -sS -sV -Pn 192.168.128.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-29 23:17 EST
Nmap scan report for 192.168.164.128
Host is up (0.00035s latency).
All 1000 scanned ports on 192.168.164.128 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
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
```

## 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

Local Security Policy

File Action View Help

Security Settings

Account Policies

Local Policies

Windows Defender Firewall with Advanced Firewall Policies

Network List Manager Policies

Public Key Policies

Software Restriction Policies

Application Control Policies

IP Security Policies on Local Computer

Advanced Audit Policy Configuration

System Audit Policies - Local Group

Account Logon

Account Management

Detailed Tracking

DS Access

Logon/Logoff

Object Access

Policy Change

Privilege Use

System

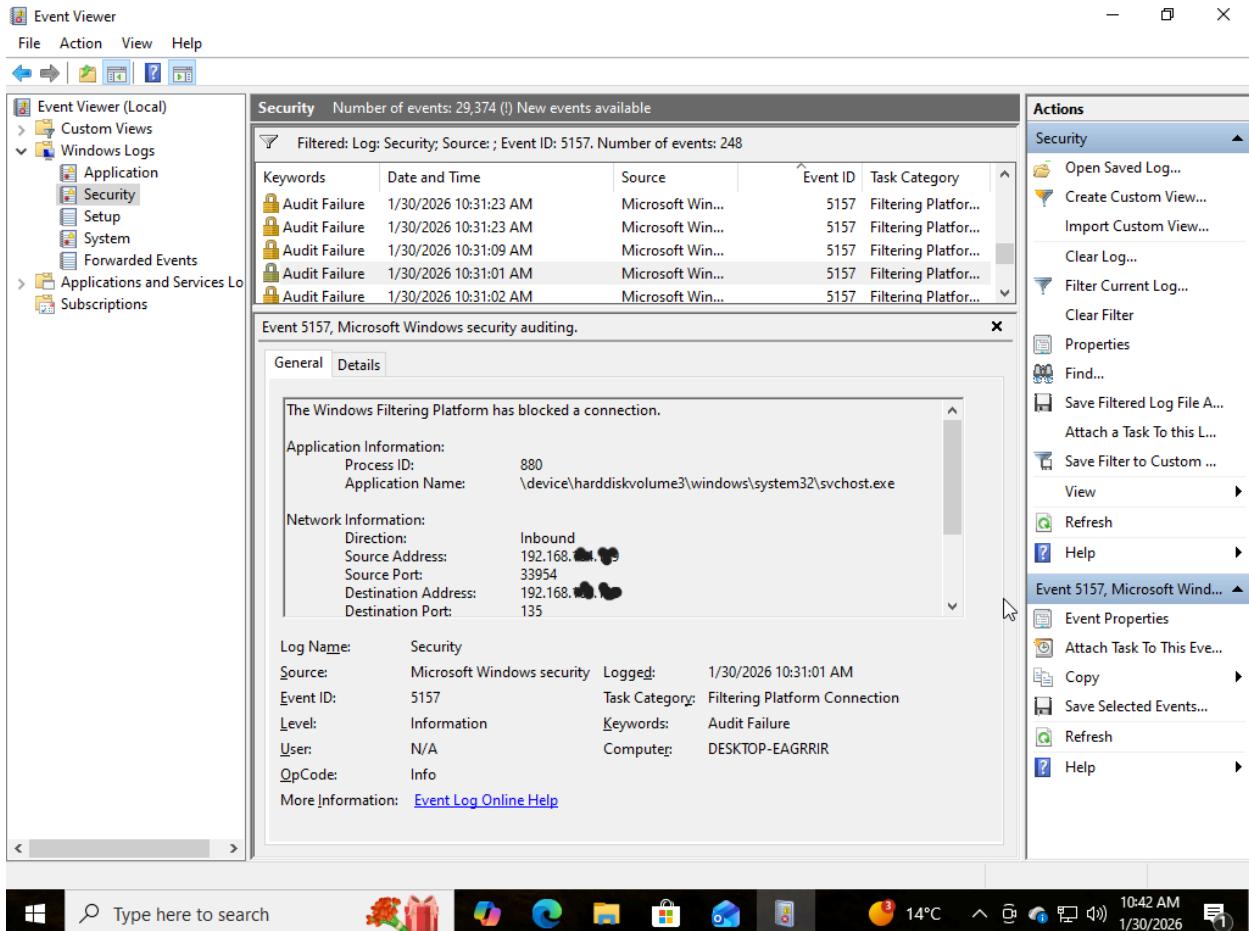
Global Object Access Auditing

Subcategory	Audit Events
[001] Audit Application Generated	Not Configured
[002] Audit Certification Services	Not Configured
[003] Audit Detailed File Share	Not Configured
[004] Audit File Share	Not Configured
[005] Audit File System	Not Configured
[006] Audit Filtering Platform Connection	Success and Failure
[007] Audit Filtering Platform Packet Drop	Success and Failure
[008] Audit Handle Manipulation	Not Configured
[009] Audit Kernel Object	Not Configured
[010] Audit Other Object Access Events	Not Configured
[011] Audit Registry	Not Configured
[012] Audit Removable Storage	Not Configured
[013] Audit SAM	Not Configured
[014] Audit Central Access Policy Staging	Not Configured

Type here to search

10:28 AM 1/30/2026

## 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.