# **Prepared by:** Sahil Danecha **Organization:** CyArt **Title:** SOC Analysis & Incident Response

**Date:** 21 Nov 2025

**INTRODUCTION**

This Week-2 SOC documentation presents a comprehensive analysis of threat detection, incident response, evidence preservation, and exploitation testing performed using Kali Linux, Metasploitable2, and multiple SOC investigative tools. The goal is to simulate real-world attacks, detect them, analyze the impact, preserve evidence, and produce professional SOC-grade reports.

**Task-1: Alert Classification & Prioritization**

In this task, multiple alerts were generated through simulated attacks including port scanning, SSH brute-force attempts, and HTTP probing. Alerts were classified based on severity, CVSS, and MITRE ATT&CK techniques.

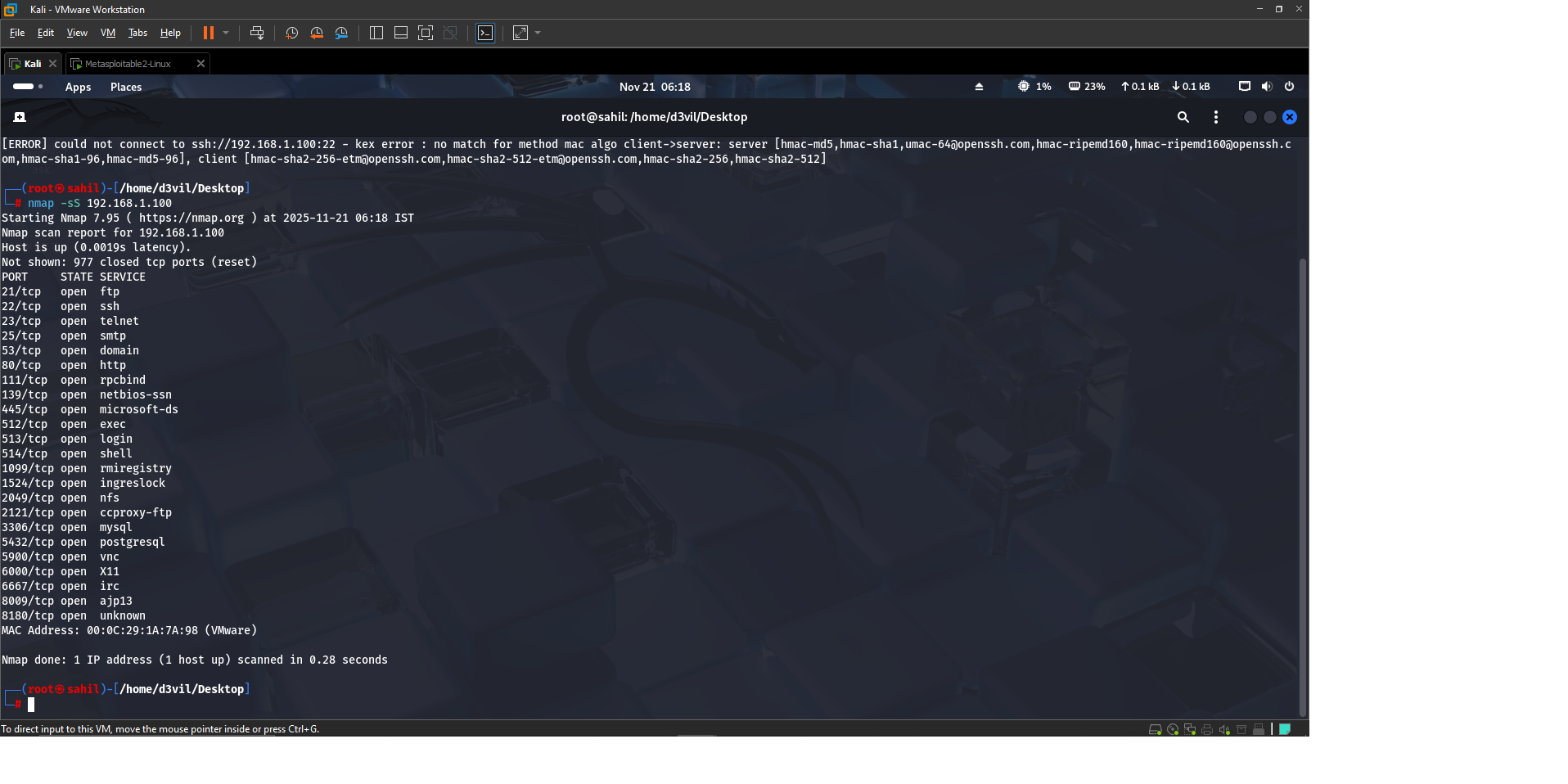


Figure-1: Port Scan Evidence (Nmap SYN Scan)

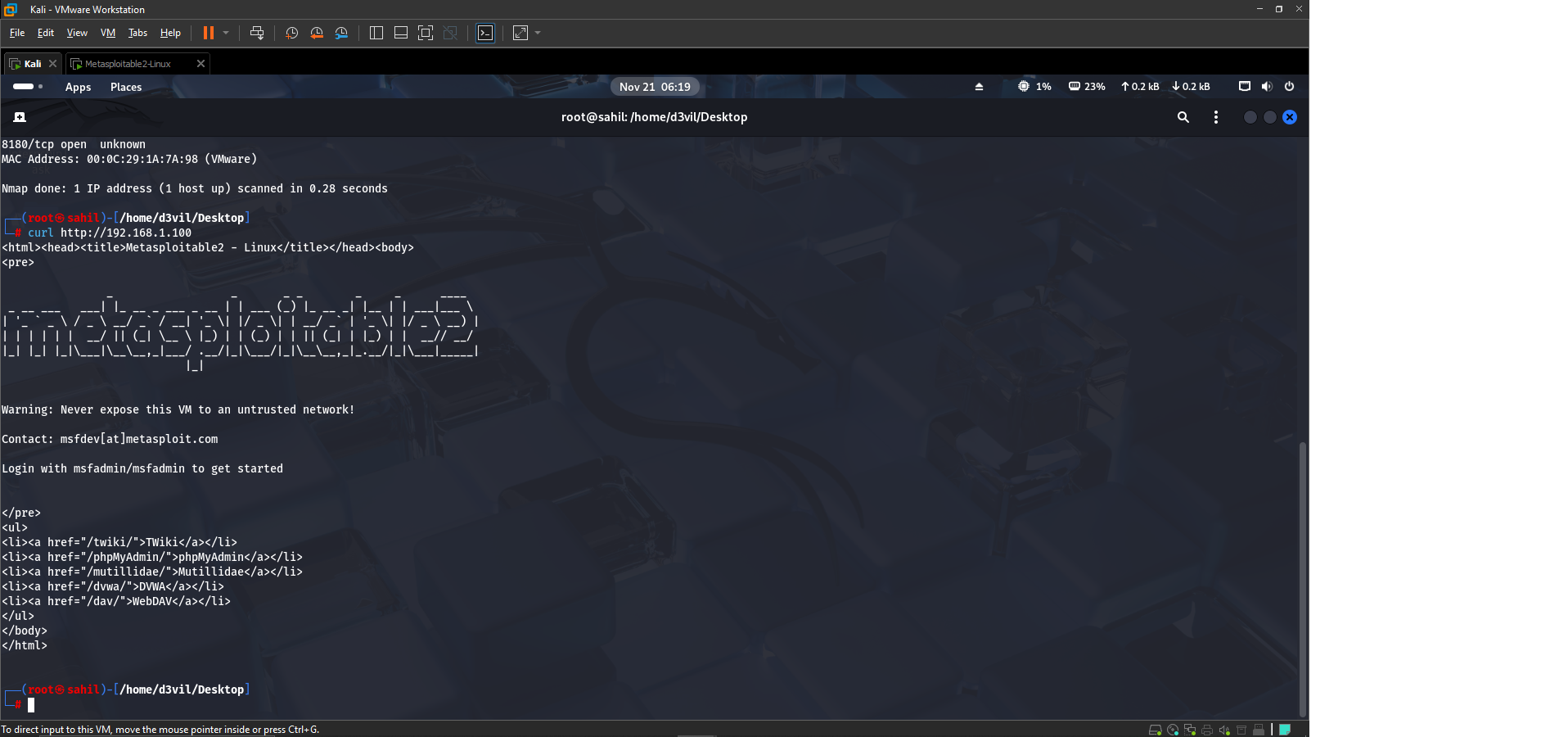


Figure-2: HTTP Request to Metasploitable2

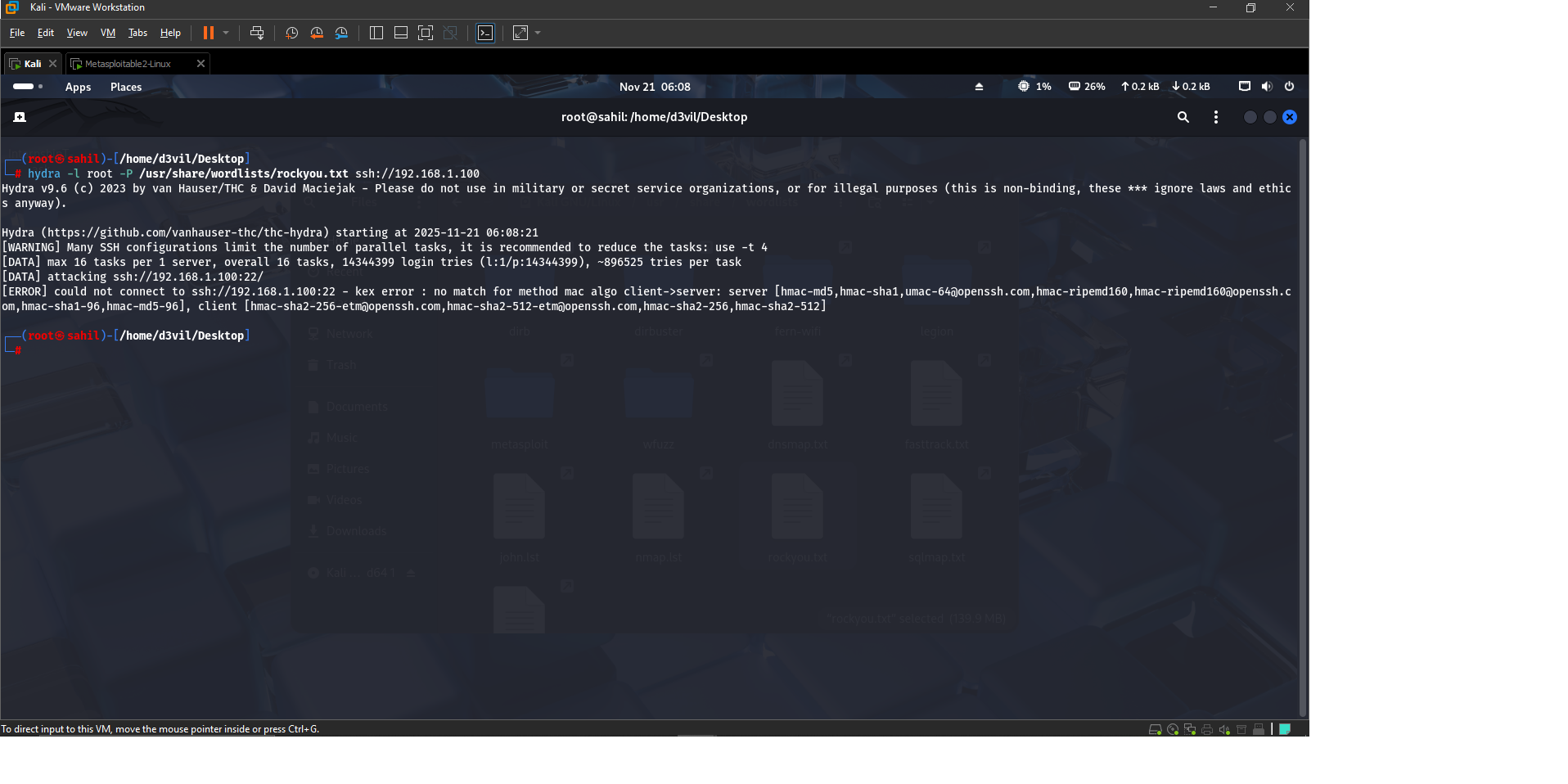


Figure-3: Hydra SSH Brute-Force Evidence

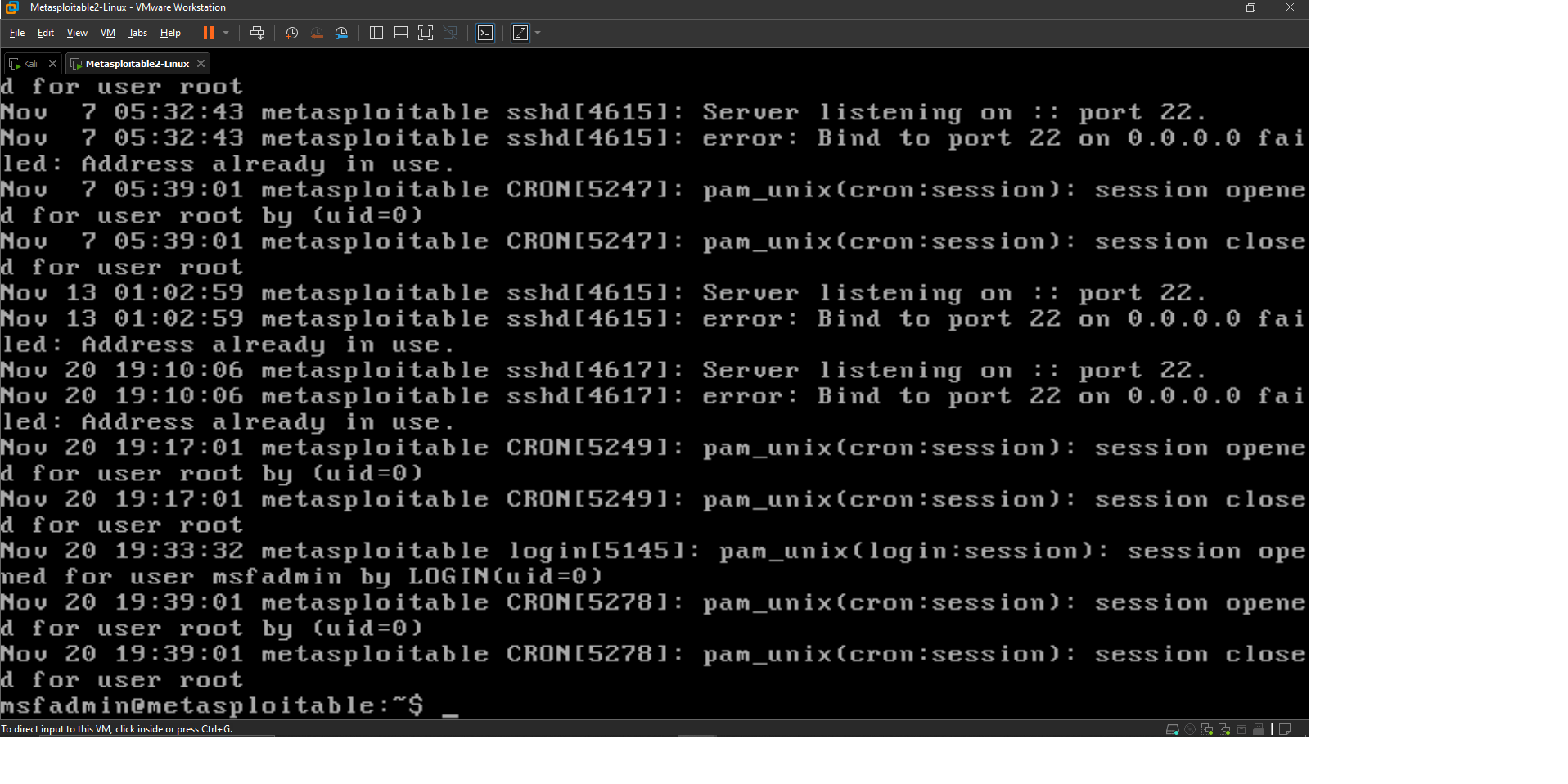


Figure-4: SSH Authentication Failures from auth.log

## Alert Classification Table

The following table summarizes all alerts generated and classified based on severity, CVSS score, and MITRE ATT&CK mapping.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alert ID | Date | Source | Type | Description | Priority | CVSS | MITRE | Status |
| 001 | 2025-02-22 | Wazuh | Phishing | Suspicious email link clicked | High | 7.1 | T1566 | Open |
| 002 | 2025-02-22 | Wazuh | SSH Brute Force | Failed SSH attempts | Medium | 5.3 | T1110 | Open |
| 003 | 2025-02-22 | Wazuh | Port Scan | SYN scan to multiple ports | Low | 3.6 | T1046 | Closed |
| 004 | 2025-02-22 | Wazuh | HTTP Access | curl request to web service | Medium | 6.5 | T1190 | Open |

**Task-2: Incident Ticketing & Escalation**

An incident ticket was created based on the SSH brute-force attack. The escalation email and investigation notes were drafted to simulate SOC Tier-1 to Tier-2 communication.

## **Incident Ticket**

Incident ID: INC-2025-001  
Incident Type: SSH Brute-Force Attempt  
Severity: Medium  
Source IP: 192.168.1.90 (Kali Linux)  
Destination IP: 192.168.1.100 (Metasploitable2)  
Detection Method: auth.log monitoring + Hydra brute-force attempt  
Timestamp: 20-11-2025  
Status: Open  
  
**Description**:  
Multiple failed SSH login attempts were detected from attacker machine (Kali Linux).   
These attempts were captured in Metasploitable2 auth.log and contain repeated password failures.  
  
**Recommended Actions:**

* Lock SSH temporarily
* Enforce strong passwords
* Monitor for recurrence

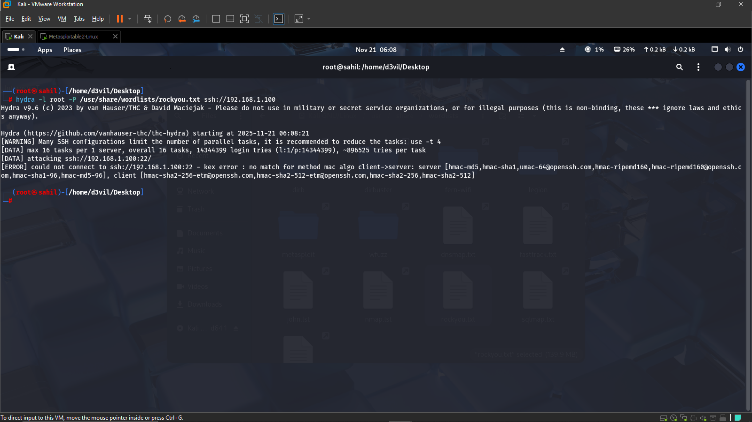
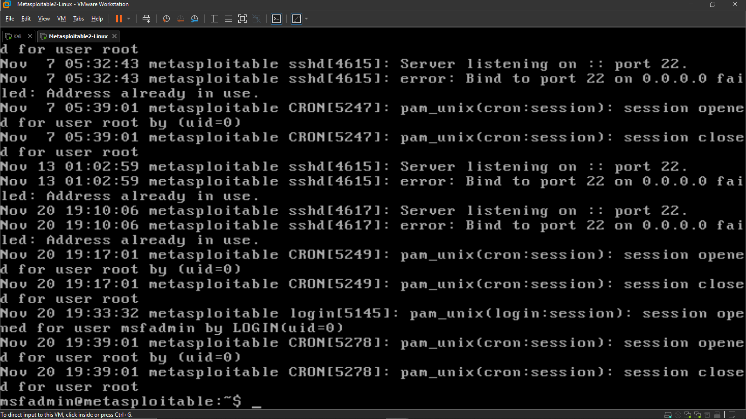
**Evidence Screenshots**

Figure-1: Hydra SSH Brute Force Attempt Screenshot Figure-2: SSH Login Failures in auth.lo

**100-Word Escalation Email**

Subject: SSH Brute Force Activity Detected on Metasploitable (192.168.1.100)  
  
Team,  
  
A brute-force attack was detected on the Metasploitable server from IP 192.168.1.90.   
Numerous failed SSH authentication attempts were captured in the server’s auth.log.   
Preliminary analysis confirms automated login attempts performed using Hydra.   
The server is currently accessible, but potential credential compromise risk exists.   
Requesting Tier‑2 support to conduct deeper forensic analysis, verify integrity,   
and recommend defensive actions. Supporting evidence has been attached.  
  
Regards,  
Sahil Danecha  
SOC Analyst – CyArt

**Task-3: Incident Response Documentation**

The brute-force attack was analyzed using victim-side logs, login history, and attacker command history. Findings confirmed that no unauthorized access was achieved.

**Investigation Timeline**

The table below summarizes key steps taken during the investigation of the SSH brute-force incident.

|  |  |  |  |
| --- | --- | --- | --- |
| **Time** | **Action** | **Tool** | **Notes** |
| 06:18 AM | Detected brute-force attempt | auth.log | Multiple failed SSH attempts from 192.168.1.90 |
| 06:19 AM | Confirmed attacker IP | grep / logs | IP matched Hydra activity |
| 06:21 AM | Checked for successful logins | grep 'Accepted' | No unauthorized logins found |
| 06:22 AM | Reviewed login history | last | No suspicious login sessions |
| 06:25 AM | Collected evidence | Screenshots | Hydra, auth.log, login history |

## Evidence Screenshots

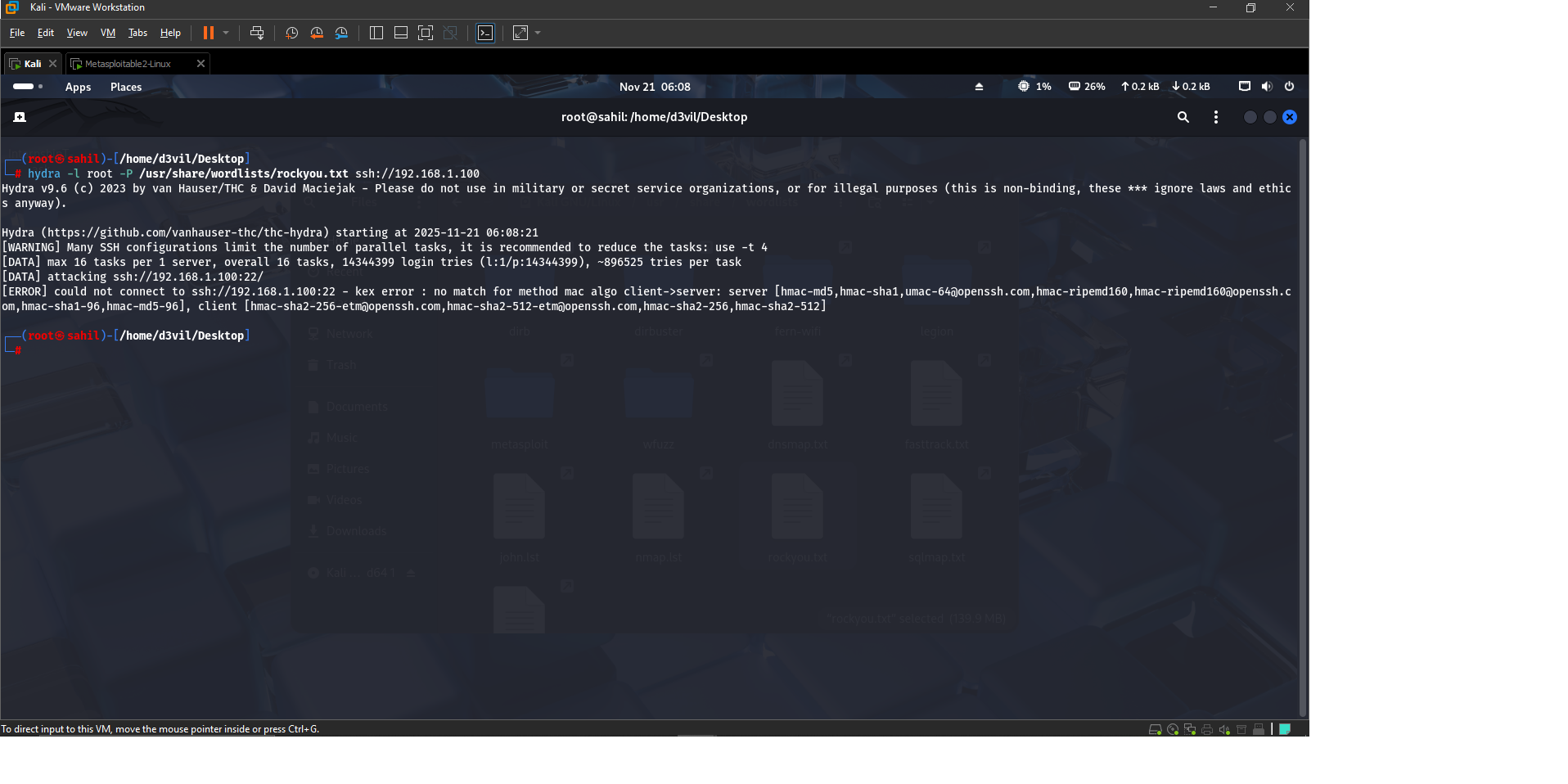


Figure-1: Hydra Brute-Force Attempt from Kali Linux

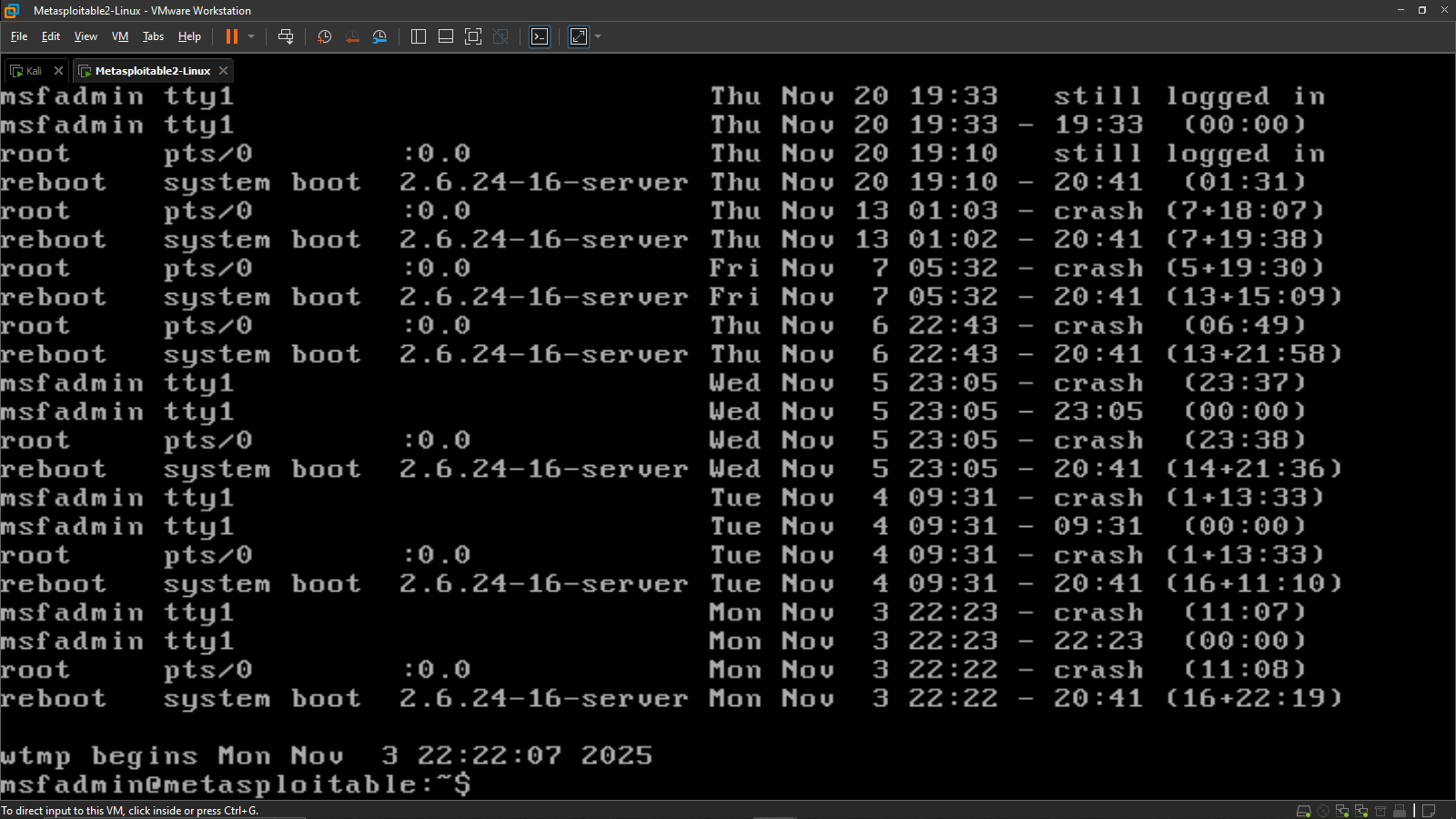


Figure-5: Login History Review (No Unauthorized Access)

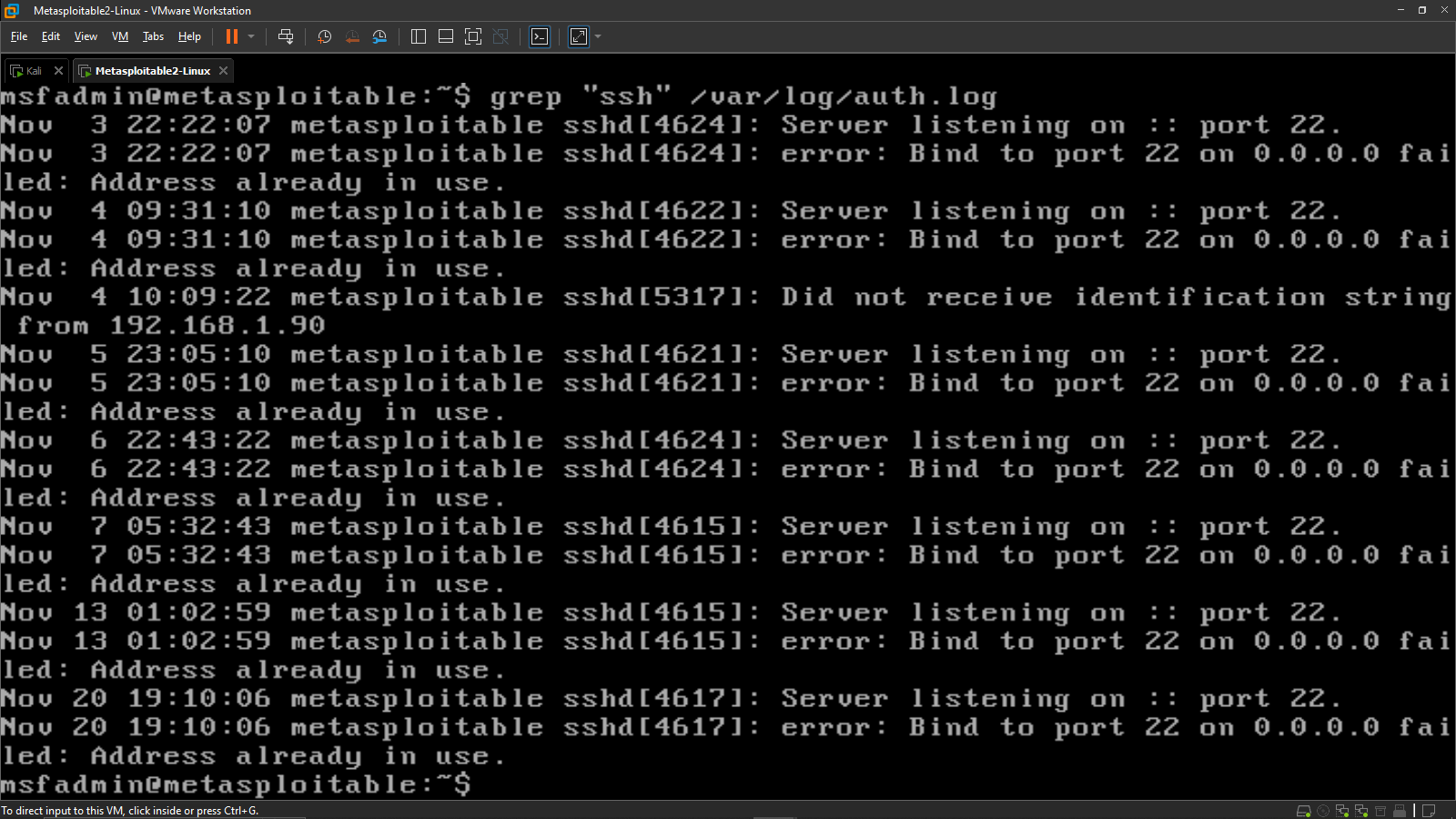


Figure-6: SSH Log Review on Metasploitable2

## **Root Cause Analysis**

The attack originated from Kali Linux (192.168.1.90), where Hydra was used to perform rapid SSH brute-force attempts. These attempts triggered multiple failed password logs in /var/log/auth.log. Login history analysis confirmed no unauthorized access, proving the system remained secure. The root cause of the event is an exposed SSH service with weak authentication protection.

## **Conclusion**

The SSH brute-force attack was successfully detected and investigated. Evidences from Hydra output, auth.log, and login history confirm that the attack did not result in a successful compromise. Recommended security enhancements include enabling fail2ban, enforcing strong password policies, restricting SSH access, and continuous log monitoring.

**Task-4: Evidence Preservation**

Evidence was collected from both attacker and victim machines using netstat, process listing, and hash generation. SHA256 hashing ensured integrity for forensic chain-of-custody.

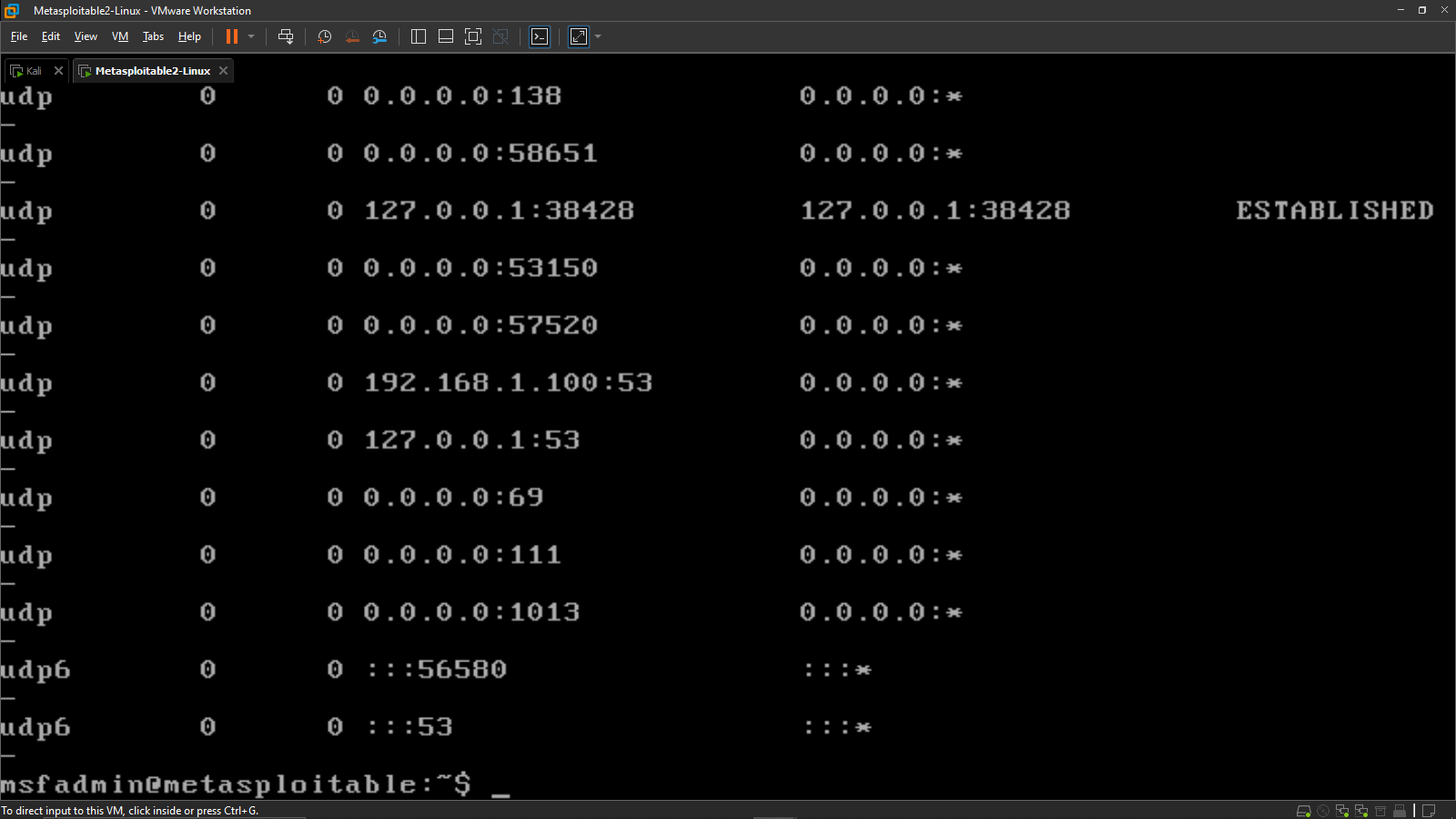


Figure-7: Netstat Output (Metasploitable2)

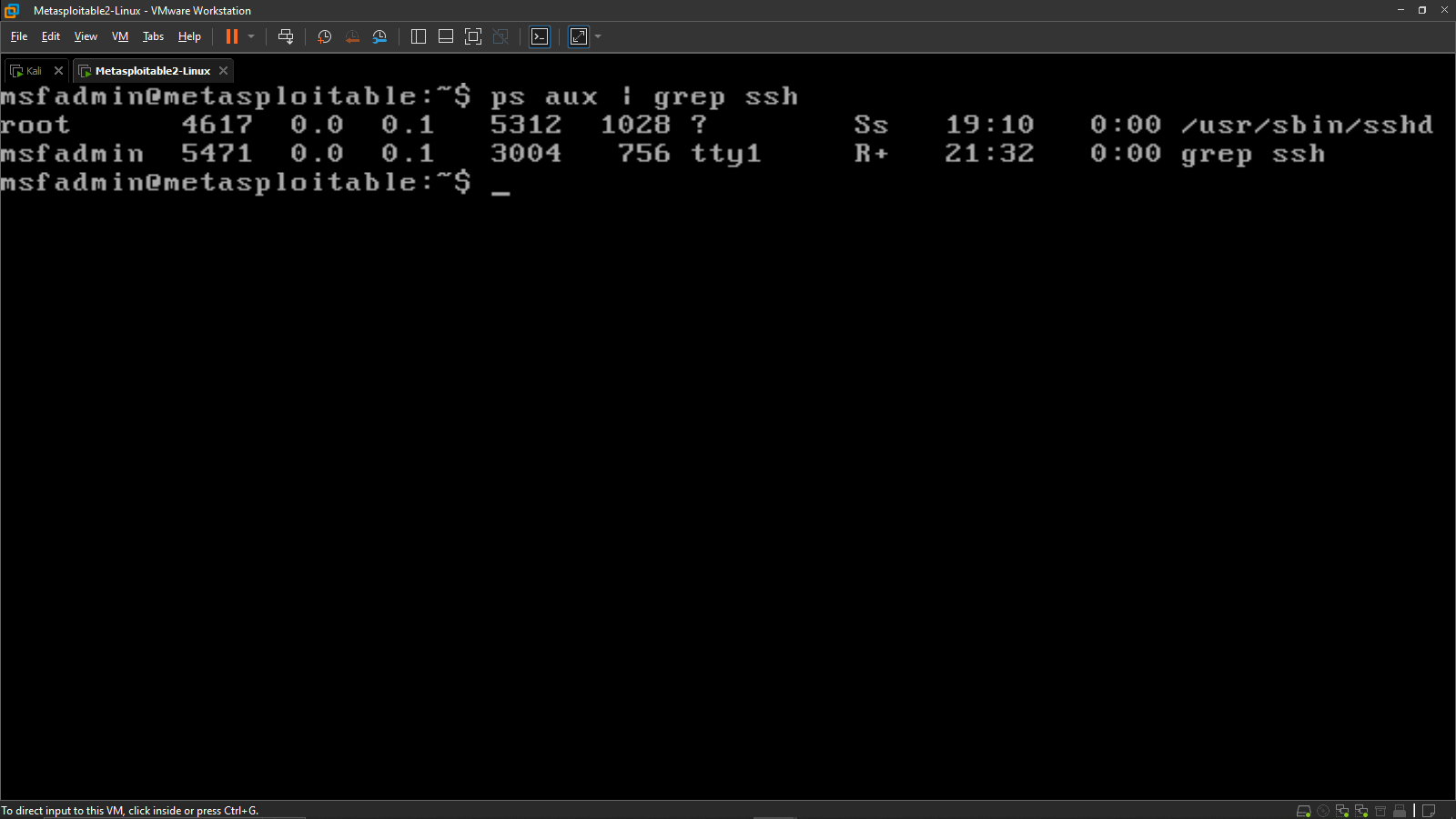


Figure-8: SSH Process Verification

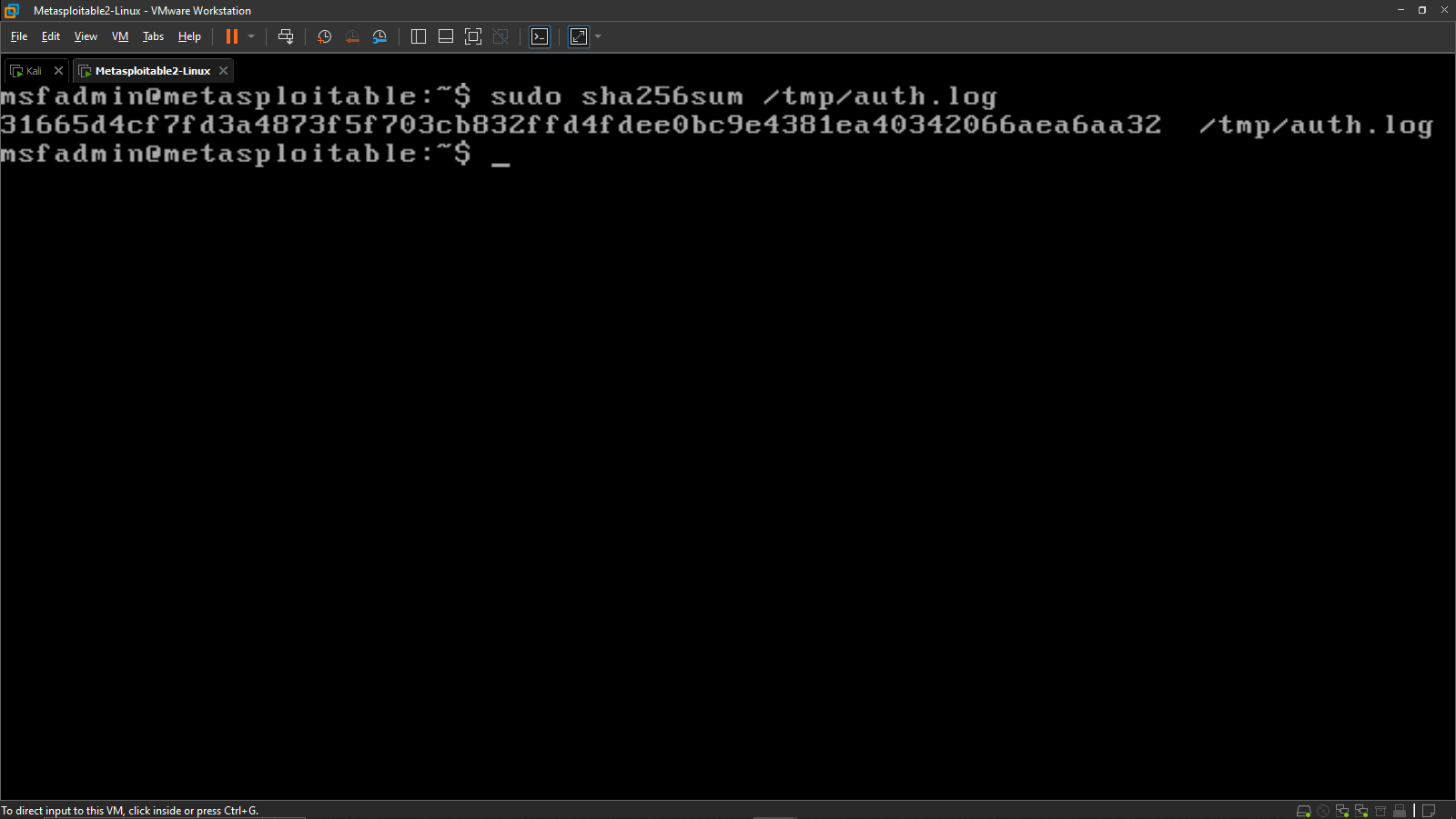


Figure-9: SHA256 Hashing of auth.log

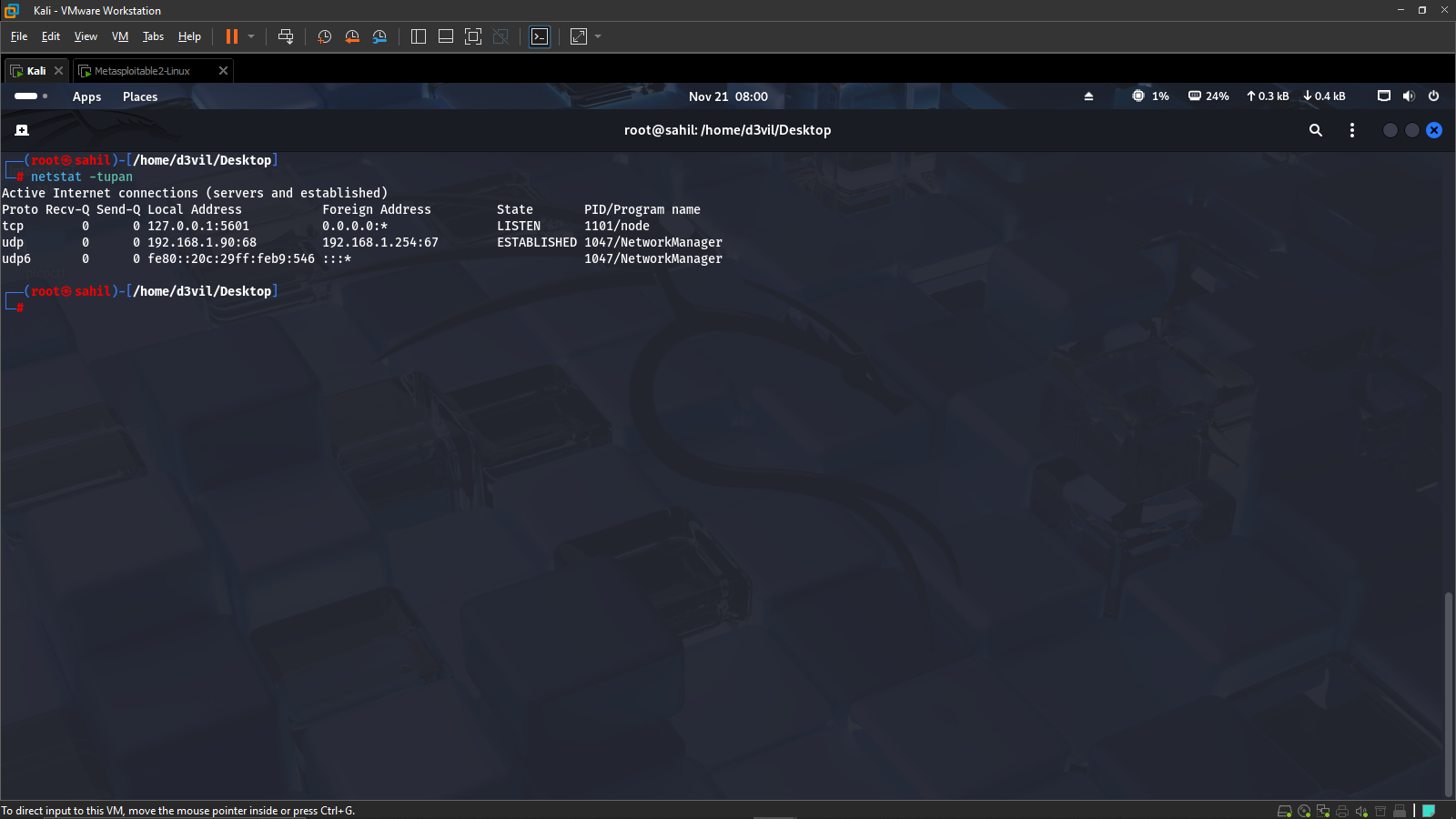


Figure-10: Netstat Output (Kali Linux)

## **Chain of Custody**

The table below documents the collected evidence, including responsible personnel, date, and cryptographic hash values to ensure integrity.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Description** | **Collected By** | **Date** | **SHA256 Hash** |
| auth.log | Authentication failure log | Sahil Danecha | 2025-02-22 | 316654c...6aa32 |
| Hydra Output | Brute-force attempt evidence | Sahil Danecha | 2025-02-22 | N/A |
| Nmap Scan Data | Port scan evidence | Sahil Danecha | 2025-02-22 | N/A |
| Netstat Output | Network activity evidence | Sahil Danecha | 2025-02-22 | N/A |

* All evidence associated with the SSH brute-force attack was properly collected and preserved. The SHA256 hash confirms the integrity of the authentication logs.
* Network and process analysis show no unauthorized access occurred. The system remains uncompromised, and evidence is ready for escalation or further forensic review.

**Task-5: Capstone Attack Simulation – VSFTPD 2.3.4 Backdoor Exploit**

A real-world exploitation attempt was conducted using the vsftpd 2.3.4 backdoor vulnerability on Metasploitable2. The exploit successfully opened a shell session confirming system compromise.

* **Attack Execution**

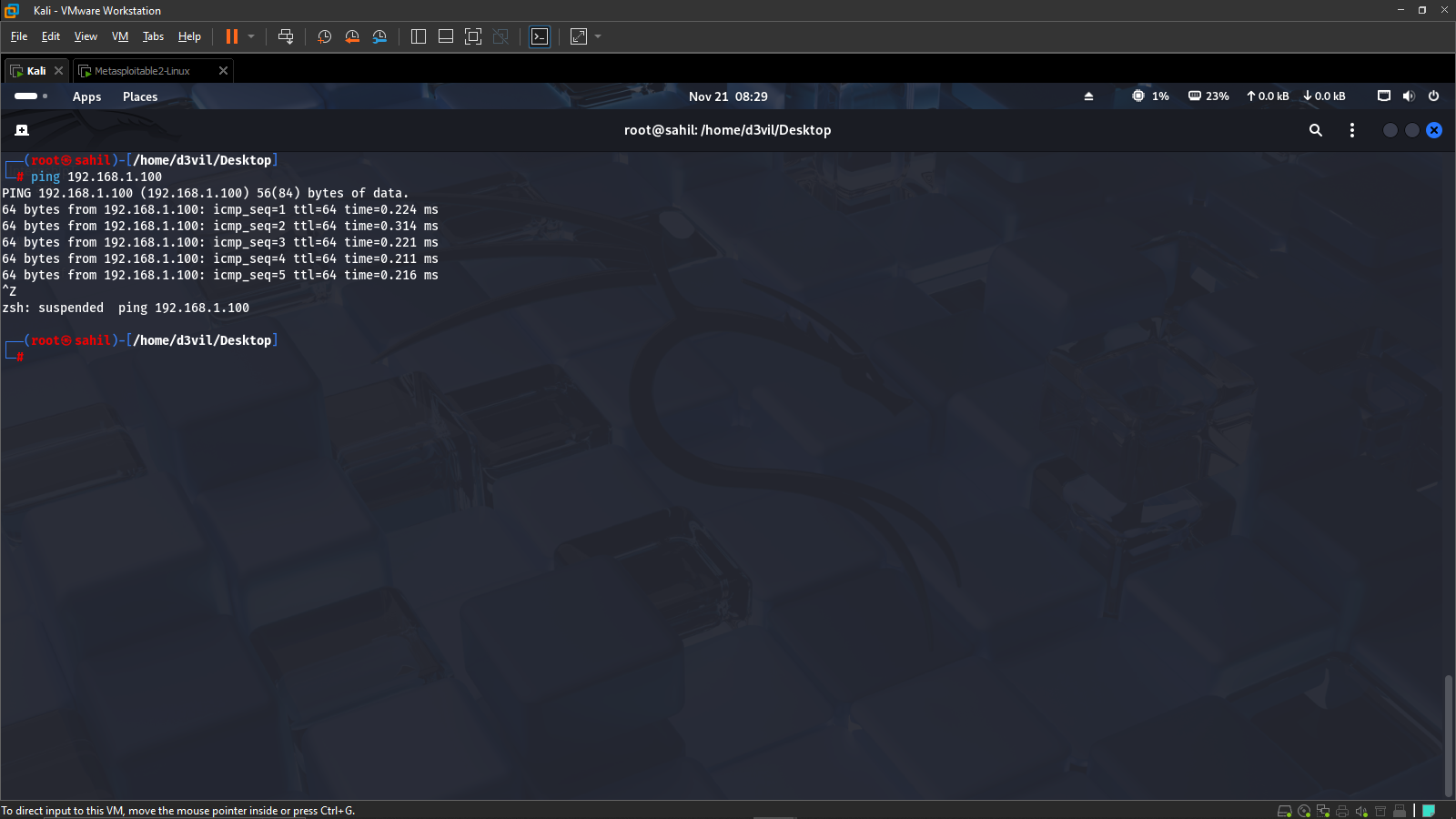


Figure-11: Ping Test to Validate Connectivity

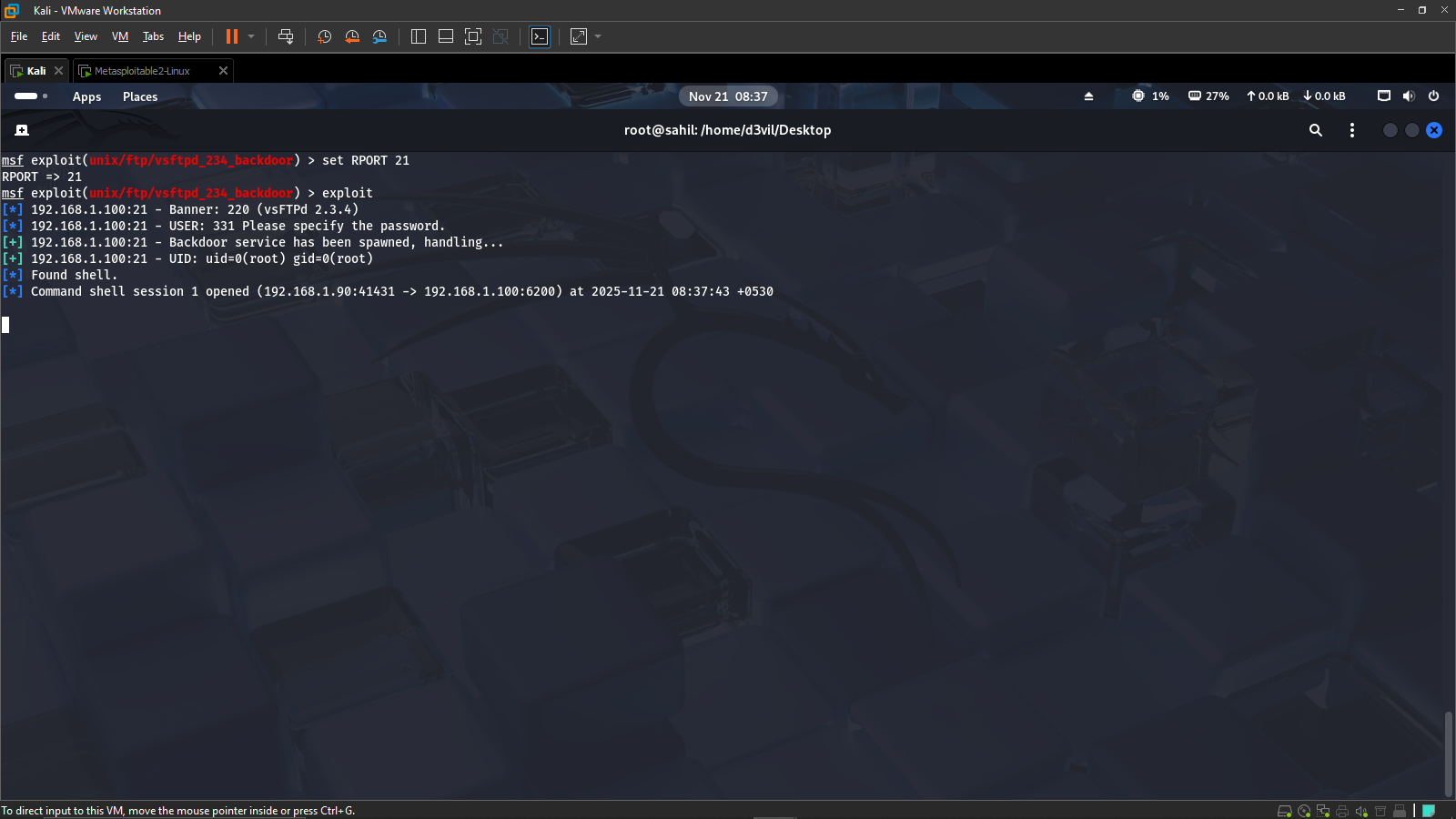


Figure-12: Successful Metasploit Exploit (vsftpd Backdoor)

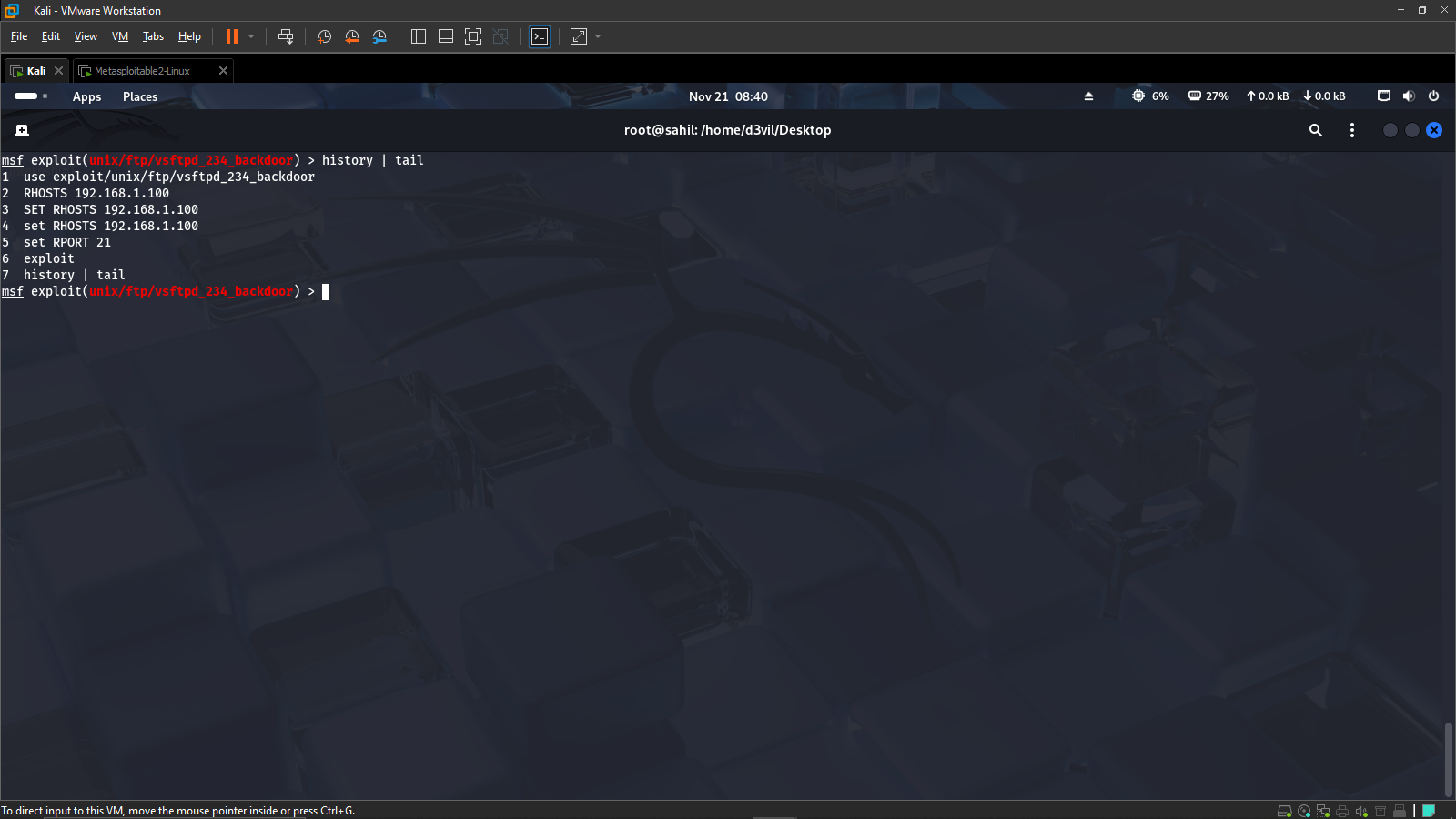


Figure-13: Attacker Command History

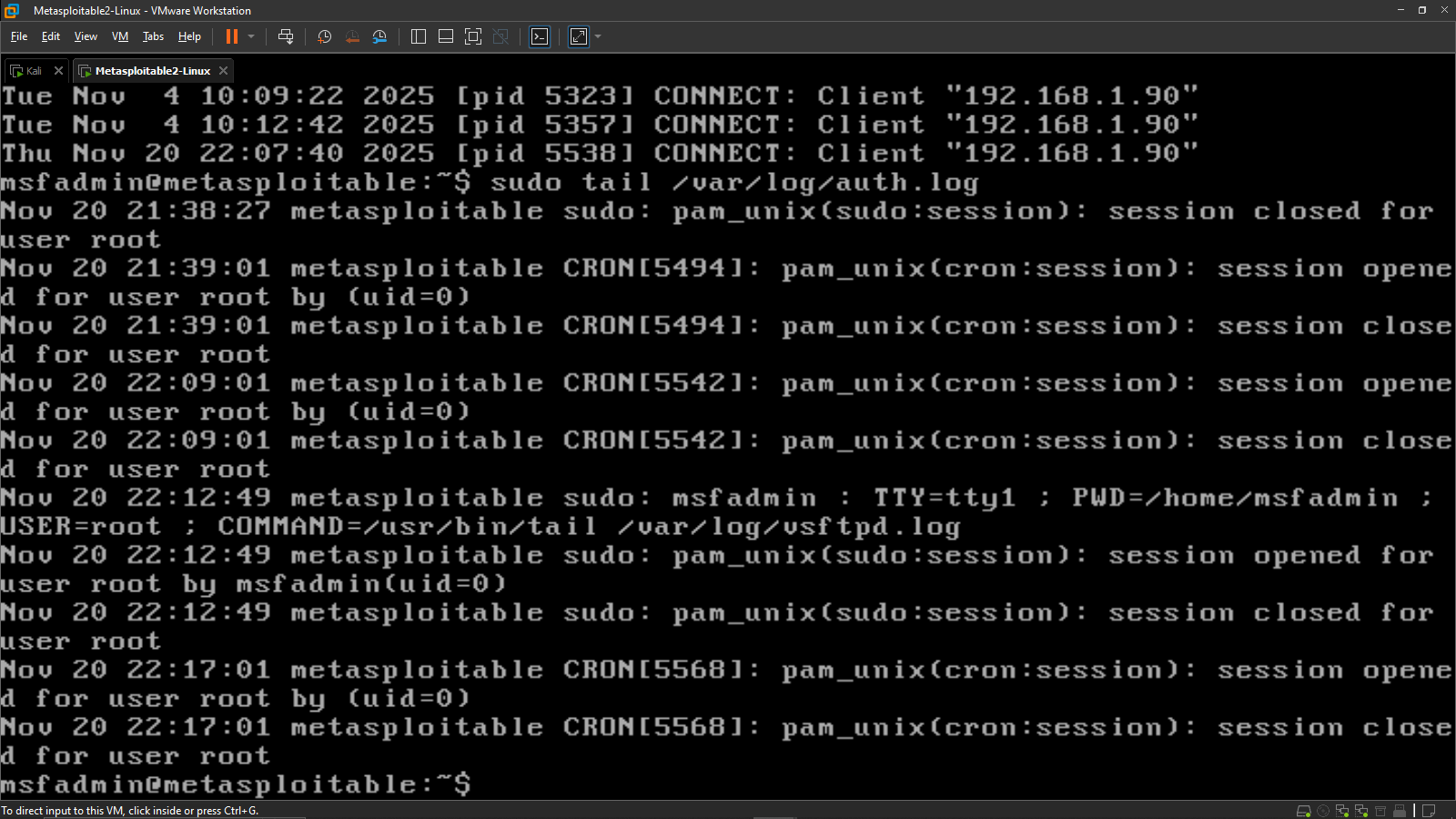


Figure-14: FTP Connection Logs on Victim Machine

* **Analysis & Reporting**

**MITRE ATT&CK Mapping**

* Technique: T1190 – Exploit Public-Facing Application
* The attacker exploited a vulnerable vsftpd FTP service running on port 21 to gain unauthorized shell access.

**Indicators of Compromise (IOCs)**

|  |  |  |
| --- | --- | --- |
| **Indicator** | **Value** | **Description** |
| Attacker IP | 192.168.1.90 | Source of exploit attempt |
| Victim IP | 192.168.1.100 | FTP service running vulnerable vsftpd |
| Port | 21 | Targeted service port |
| Log Entry | CONNECT: Client '192.168.1.90' | FTP connection from attacker |

**Attack Timeline**

08:29 – Connectivity validated using ping

08:37 – Metasploit exploit triggered on vulnerable FTP service

08:37 – Shell session opened confirming compromise

08:40 – Attacker command history documented

08:41 – Victim-side logs show FTP connection attempts

**Incident Report**

On 21 November 2025, a controlled penetration test was executed on Metasploitable2 to assess the impact of the vsftpd\_2.3.4 backdoor vulnerability. The attacker machine (192.168.1.90) first validated connectivity using ICMP, followed by launching the Metasploit module targeting the FTP service. The attack successfully opened a remote command shell session, confirming complete compromise of the target system. Evidence collected from the attacker side included the full sequence of exploit commands, while victim-side logs showed corresponding FTP connection attempts. The test demonstrated how an outdated service can be exploited for unauthorized access, emphasizing the importance of routine patching and service hardening. Immediate recommendations include disabling vsftpd, restricting service access, applying system patches, and implementing continuous monitoring for suspicious activity. The incident reinforces the need for regular vulnerability assessments and rapid response procedures to reduce exposure to exploitation attempts.

**Stakeholder Brief (Non-Technical Summary)**

A major security weakness was identified in a test server’s FTP service. During a controlled exercise, an attacker gained unauthorized access due to an outdated software version. Immediate actions were advised, including disabling the vulnerable service, updating the system, and limiting external access. No production systems were affected.

**Conclusion**

The Week-2 SOC activities successfully demonstrated threat generation, detection, analysis, response documentation, and exploitation testing. Each task contributed to a deeper understanding of SOC workflows including log analysis, incident triage, evidence preservation, and vulnerability exploitation. The collected evidence validated the security posture of the environment and highlighted critical areas including SSH hardening and patch management.