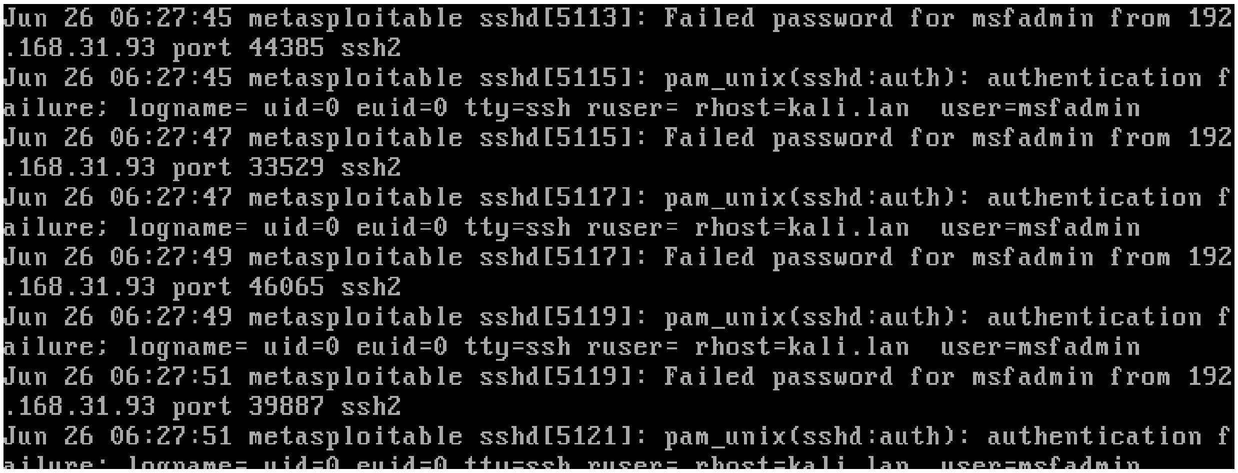
Alert Triage Practice

1. Triage Simulation

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

Alert Simulation:

For this triage simulation generating an alert for “Multiple failed login attempts” to the SSH service and sending logs to the Wazuh SIEM tool. Logs are analyzed.



```
Jun 26 06:27:45 metasploitable sshd[5113]: Failed password for msfadmin from 192
.168.31.93 port 44385 ssh2
Jun 26 06:27:45 metasploitable sshd[5115]: pam_unix(sshd:auth): authentication f
ailure; logname= uid=0 euid=0 tty=ssh ruser= rhost=kali.lan  user=msfadmin
Jun 26 06:27:47 metasploitable sshd[5115]: Failed password for msfadmin from 192
.168.31.93 port 33529 ssh2
Jun 26 06:27:47 metasploitable sshd[5117]: pam_unix(sshd:auth): authentication f
ailure; logname= uid=0 euid=0 tty=ssh ruser= rhost=kali.lan  user=msfadmin
Jun 26 06:27:49 metasploitable sshd[5117]: Failed password for msfadmin from 192
.168.31.93 port 46065 ssh2
Jun 26 06:27:49 metasploitable sshd[5119]: pam_unix(sshd:auth): authentication f
ailure; logname= uid=0 euid=0 tty=ssh ruser= rhost=kali.lan  user=msfadmin
Jun 26 06:27:51 metasploitable sshd[5119]: Failed password for msfadmin from 192
.168.31.93 port 39887 ssh2
Jun 26 06:27:51 metasploitable sshd[5121]: pam_unix(sshd:auth): authentication f
ailure; logname= uid=0 euid=0 tty=ssh ruser= rhost=kali.lan  user=msfadmin
```

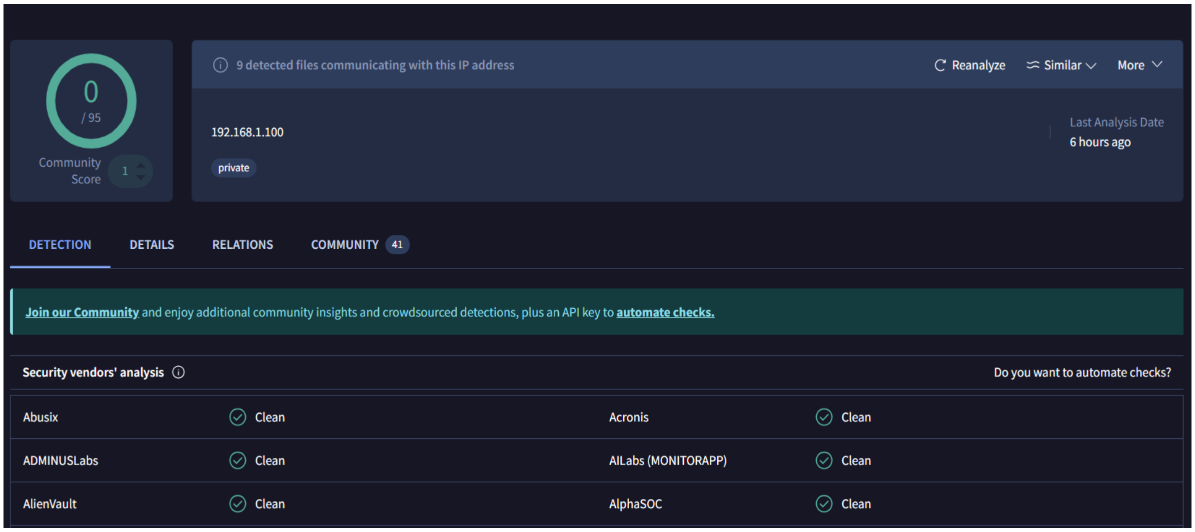
Alert Analysis:

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

Alert ID	**Description**	**Source IP**	**Priority**	**Status**
002	Brute-Force SSH Attempts	192.168.1.100	Medium	Open

2. Threat Intelligence Validation

Threat Intelligence validation means validation of threats that uses Indicators of Compromise (IOCs) in the tools like AlienVaultOTX (Open Threat Exchange) or VirusTotal to validate IOCs. This Threat Intelligence tool used to analyze the IOCs like file hashes, Domains, IP address, and URLs.



9 detected files communicating with this IP address

192.168.1.100

private

Last Analysis Date
6 hours 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?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	AlphaSOC	✓ Clean