Blocking a Known Malicious Actor

This project focuses on enhancing security monitoring by using Wazuh's command monitoring and active response capabilities to detect and block a known malicious actor in real time. It secures Ubuntu endpoints within the 10ALYTICS-DC environment by configuring Wazuh agents and servers to monitor suspicious commands, unauthorized access attempts, and malicious behaviors. The investigation emphasizes detection, analysis, and automated mitigation ensuring timely response to threats and preventing the malicious actor from compromising production systems or escalating access.

BY RUTH KWAKOR QUARTEY

Scope of Investigation

Blocking Known Malicious Actors (IP Reputation Management)

- Leverage Wazuh's capabilities to detect and respond to common threats in the 10ALYTICS-DC environment by setting up Apache web server and configuring Wazuh to block a known malicious IP.

Methodology

Agent Deployment

Install and configure Wazuh agents on Ubuntu endpoints to monitor system activities and log files.

Custom Rule Creation

Develop specialized detection rules for unauthorized processes and a known malicious IP.

Active Response Setup

Configure automated responses to block malicious IPs and terminate unauthorized processes.

Testing & Validation

Simulate attacks to verify detection capabilities and response effectiveness.

- The implementation process involved deploying Wazuh agents on Ubuntu endpoints, creating custom detection rules, and configuring active response mechanisms. Each component was carefully tested to ensure proper functionality before proceeding to attack simulations.

Task 2: Blocking Known Malicious Actors (IP Reputation Management)

The project extended to blocking known malicious actors by leveraging Wazuh's IP reputation management. Using Kali Linux as an attacker, attempts to access an Apache web server on Ubuntu were detected and blocked by adding the attacker's IP to a reputation blacklist. Wazuh's active response automatically dropped incoming connections from the malicious IP for 60 seconds, effectively preventing unauthorized access. This approach mitigated risks from Malicious Actors IP by integrating threat intelligence with automated firewall rules.

Key Systems

Ubuntu web server, Wazuh SIEM, Kali attacker machine.

Threats

Attempts from a known blacklisted IP.

Response

Automatic IP blocking using firewall-drop active response.

Blocking Malicious Actors: IP Reputation

Apache2 Installation

Installed the Apache web server

IP Reputation Database

Configured Alienvault reputation database with known malicious IPs

Active Response

Implemented firewall-drop to block malicious IPs for 60 seconds

The implementation leveraged Wazuh's IP reputation management capabilities to automatically detect and respond to Known malicious actor IP. By integrating the Alienvault reputation database and adding custom rules, the system could identify attempts targeting 10ALYTICS-DC’s web server and immediately block the attacker's IP address using firewall-drop active response.

Detecting A Known Malicious Actor: IP Reputation

Attack Emulation

Attacker run this command curl http://192.168.0.10 to access the web server in Ubuntu endpoint

Login Attempts

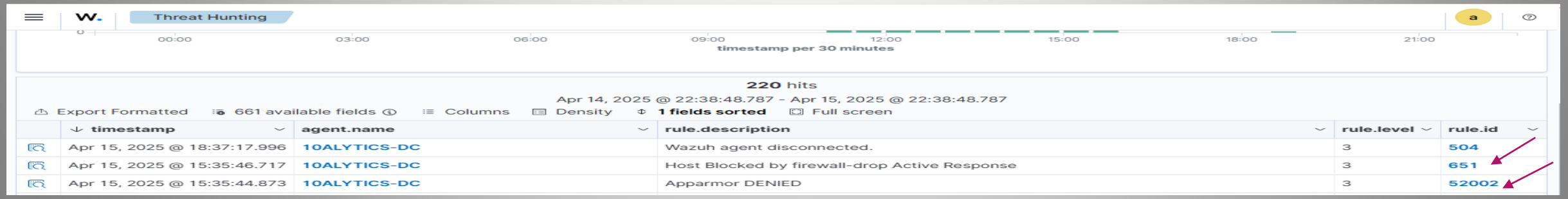
APPARMOR access attempts

Response

Active response blocks attacker IP with firewall-drop (Rule ID: 651)

Detection

The alert was visually presented in the Dashboard with rule triggered ID 52002, categorized at severity level 3



Blocking Known Malicious Actors (IP Reputation Management)

Findings

- The Wazuh monitoring system detected AppArmor Access Denial on the 10ALYTICS-DC server (Agent ID: 002, IP: 192.168.0.7). This was logged under rule ID 52002, categorized at severity level 3.
- Active Response functionality triggered(Rule ID 651) and operated as intended.

Recommendations

- Web Application Security: Implement WAF protections and input validation.
- Firewall Hardening: Automate IP blocking.
- Incident Response Compliance: Follow NIST 800-53, PCI DSS.
- Staff Training: Ongoing security awareness programs.
- Periodic Penetration Testing: Simulate attacks to validate defenses.

Conclusion

This simulation effectively demonstrated 10ALYTICS-DC's growing capability to detect and respond to unauthorized system access attempts using AppArmor. By integrating Wazuh's real-time alerting with Active Response mechanisms, the organization successfully blocked a potentially malicious activity triggered by AppArmor policy violations. This reinforces 10ALYTICS-DC's security posture, ensuring system integrity against internal misconfigurations or external exploitation attempts targeting system-level resources.

Conclusion

The project demonstrated Wazuh’s capability to block malicious actors through IP reputation management and active response. Automated detection and firewall integration provide robust protection against remote access threats.
By implementing the recommendations provided above, 10ALYTICS-DC can further strengthen their security posture and maintain their reputation for providing secure, reliable services to their clients.

Reference

Wazuh Documentation;

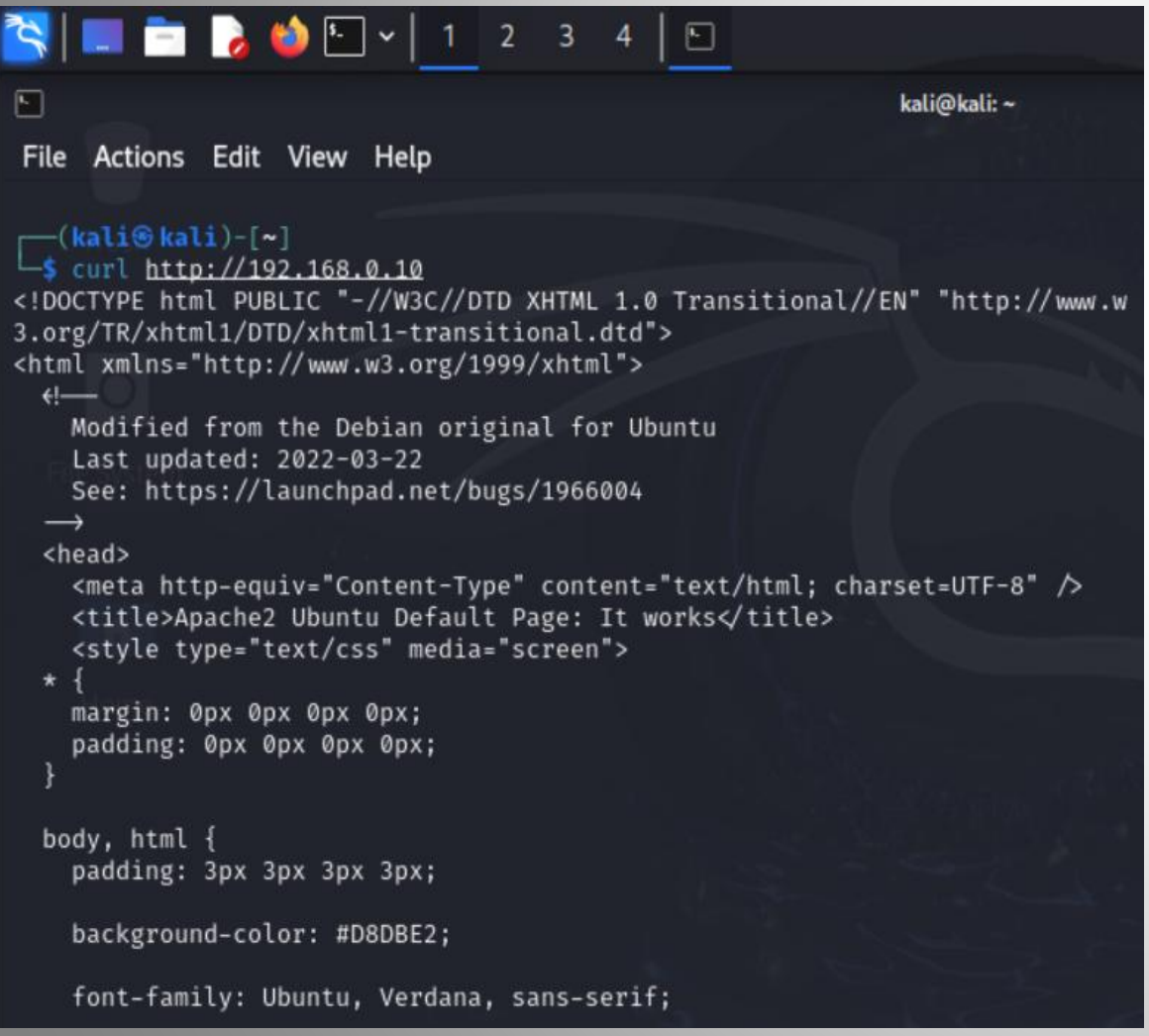
Proof of Concept guide/Blocking a known malicious actor

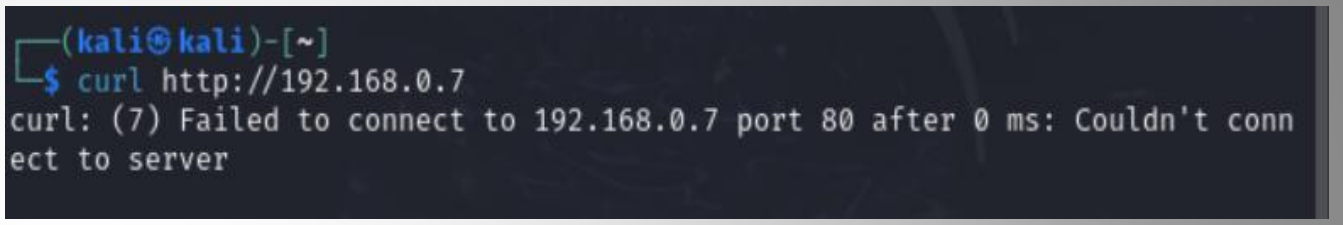
Google search engine

Appendices: Screenshots, Logs, and Commands

This section includes key screenshots of the Wazuh dashboard showing alerts for APPARMOR access attempts. It also contains attack emulation commands, and active response.

Attack Emulation on Kali curl http://<WEBSERVER_IP>





Dashboard visualizations showing blocked IP incidents