Security Monitoring Operations

Introduction and/or Background

OSSEC/Wazuh is a free, open-source host-based intrusion detection system. It performs log analysis, integrity checking, Windows registry monitoring, rootkit detection, time-based alerting, and active response.

Objectives

In this project/lab the student will:

- Gain familiarity with OSSEC

Equipment/Supplies Needed

- Computer with internet access
- VMware Workstation Virtualization Software
- Linux Installation File: Wazuh OVA, VMSVR1
- Accounts:
  - Wazuh server
    - user: wazuhuser
    - password: wazuh
  - Wazuh Admin Console
    - user: wazuh
    - password: ax4ecOZ77bekP8JDY21yadNcs8XdPA4x

Procedure

Perform the steps in this lab in the order they are presented to you. Answer all questions and record the requested information. Use the Linux Virtual Machine to perform lab activities as directed. Unless otherwise stated, all tasks done as a non-root user. If root access is needed use the sudo command.

Assignment

Installation

Download and import Wazuh into WMWare. The server should start automatically.

Shut Wazuh server down.

Tune Up

On VMWare, select wazuh. Select settings. Set the number of CPUs to 2. Set the network settings to bridged. Save the settings.

On VMWare, select VMSVR1. Select settings. Set the number of CPUs to 1. Set the network settings to bridged. Save the settings.

On wazuh and VMSVR1 record the ip addresses of each,

1. `ip ad`

Tip: If the wazuh server does not have a Ipv4 address execute,

2. `su -`
3. `dhclient -v -r eth0`

On VMSVR1, perform the following,

4. `su -`
5. `apt-get install curl`

Confirm that both devices can view each other on the network,

6. `ping <wazuh ip address>` from VMSVR1.
7. `ping  <VMSVR1 ip address>` from wazuh.

Do NOT proceed till the pings are successful; diagnose your network problem.

Restart server. Login into console using the credentials provided above.

8. `systemctl start elasticsearch.service`
9. `systemctl status elasticsearch.service`

Note: If at any time you shutdown the wazuh server it will be necessary to repeat these two steps. If needed pause the server in VMWare to save your effort.

Web Console

Start VMSVR1 if not already running and login.

Start your web browser and direct it to,

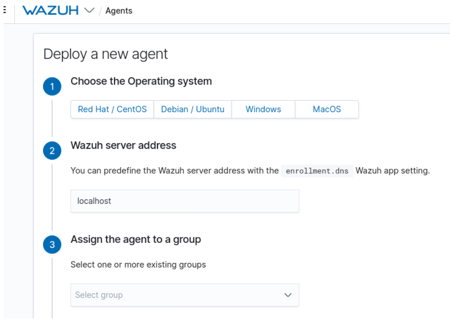
10. https://<ip address wazuh>

If prompted enter the wazuh admin console id and long password provided.

Patience, this will take time to load. Success, you will see the default wazuh display. Congrats. Record a screenshot for submission. If you see 'Kibana is not ready' you need to repeat the elasticsearch routine again, it failed or is not running.

Agent Install

Still on VMSVR1 at the wazuh display, select 'add agent'. You should see a screen thus --



Deploy a new agent

1 Choose the Operating system

2 Wazuh server address

You can predefine the Wazuh server address with the `enrollment.dns` Wazuh app setting.

localhost

3 Assign the agent to a group

Select one or more existing groups

We are going to add a wazuh agent to VMSVR1. So we will select,

11. OS Debian/Ubuntu.
12. Architecture x86_64.
13. Server address localhost.
14. Agent to group default.

Copy the curl command in step 5. Open a terminal window in VMSVR1 and execute,

i. curl -so wazuh-agent.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-

```
agent_4.1.5-1_amd64.deb && sudo WAZUH_MANAGER='localhost'
dpkg -i ./wazuh-agent.deb
```

Still at the terminal window, execute the following,

i. cd /var/ossec/etc/
ii. Open ossec.conf
iii. Find and modify <address>wazuh server IP</address> with nano, save file.
iv. At terminal execute, /var/ossec/bin/agent-auth -m MANAGER_IP

15. Still at the terminal window, execute,

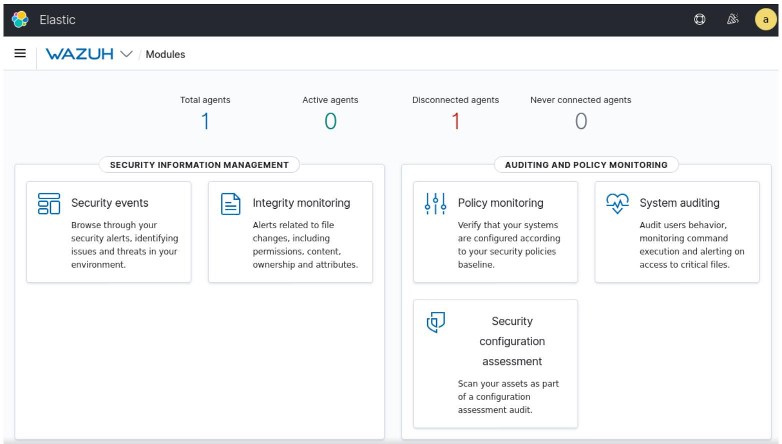
i. sudo systemctl daemon-reload
ii. sudo systemctl enable wazuh-agent
iii. sudo systemctl start wazuh-agent

16. Close the terminal, return to the wazuh screen and wait. In a moment your agent count should go from 0 to 1. Success, you have registered your first server to the wazuh system! Record a screenshot for submission.

Discovery

Lets recap, your whole point was to be notifed of security alerts for monitored systems. You had to install wazuh (aka ossec) server, configure modifications, add an agent and configure said agent on a machine. Lot of work and kudos for getting this far. So lets see what is dessert for all the work --

On the wazuh server you should be at this screen,



Elastic
a
WAZUH
Modules
SECURITY INFORMATION MANAGEMENT
AUDITING AND POLICY MONITORING

Total agents 1
Active agents 0
Disconnected agents 1
Never connected agents 0

Security events
Browse through your security alerts, identifying issues and threats in your environment.

Integrity monitoring
Alerts related to file changes, including permissions, content, ownership and attributes.

Policy monitoring
Verify that your systems are configured according to your security policies baseline.

System auditing
Audit users behavior, monitoring command execution and alerting on access to critical files.

Security configuration assessment
Scan your assets as part of a configuration assessment audit.

Click on Security events. Record a screenshot for submission. Notice that this screen provides an overall view of events and, if you scroll down, individual events that can be reviewed.

Click on WAZUH/Modules. Click System auditing. Record a screenshot for submission. This screen provides an overview of the current audit rules in force for the system

Click Explore agent in the top right corner. This subpanel provides a list of current active agents on systems that make up the auditing report.

Reflection

1. What might be an issue with using a tool like wazuh/ossec?

Lab Submissions Proof: Provide screenshots as indicated in the lab; upload your proofs for grading.

Rubric

Checklist/Single Point Mastery

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency
	Criteria #1: Screenshot showing default wazuh screen (25 points)	
	Criteria #2: Screenshot showing default wazuh screen with agent count at 1 (25 points)	
	Criteria #3: Screenshot of Security events screen (25 points)	
	Criteria #4: Screenshot of System auditing screen (15 points)	
	Criteria #5: Response to Reflection question 1. (10 points)	