Wazuh File Integrity Monitoring (FIM) & Windows Firewall Lab

Wazuh File Integrity Monitoring (FIM) & Windows Firewall Lab

Project Overview

This project demonstrates how to configure Wazuh Agent on a Windows 11 host to perform:

- Advanced File Integrity Monitoring (FIM) with user attribution and detailed file change reports.
- Windows Firewall log collection and analysis to detect network connection events, including allowed and blocked traffic.

The lab is designed for beginner-level SOC analysts to gain practical experience in host-based security monitoring using Wazuh without external attacker VMs or Sysmon.

Lab Setup & Components

Component	Description
Host OS	Windows 11 (Wazuh Agent installed)
Security Tool	Wazuh Agent
Monitoring Focus	File integrity, Windows Firewall logs
Tools Used	Wazuh agent, Windows Firewall, PowerShell

Prerequisites

- Windows 11 machine with Administrator access
- Installed and registered Wazuh Agent connected to Wazuh Manager
- Basic familiarity with editing XML config files and PowerShell

Wazuh File Integrity Monitoring (FIM) & Windows Firewall Lab

Step 1: Configure Advanced File Integrity Monitoring (FIM)

1. Open ossec.conf located in C:\Program Files (x86)\ossec-agent\.
2. Add or update the following directory monitoring block within <ossec_config>:

```
<directories realtime="yes" check_all="yes" whodata="yes" report_changes="yes">
  C:\Sensitive
</directories>
```

3. Save the file.
4. Create the folder C:\Sensitive if it does not exist.
5. Restart the Wazuh Agent service via PowerShell (run as Administrator):

```
net stop wazuhsvc
net start wazuhsvc
```

Step 2: Test File Integrity Monitoring

- Place or modify files (e.g., .bat, .exe, .txt) inside C:\Sensitive.
- Wait 1-2 minutes to allow Wazuh to process the changes.
- Check the Wazuh dashboard or Kibana for alerts showing:
  - Which user made the changes
  - What files were modified or created
  - Detailed diffs for text files (if applicable)

Step 3: Enable Windows Firewall Logging

Wazuh File Integrity Monitoring (FIM) & Windows Firewall Lab

Open PowerShell as Administrator and run:

```
Set-NetFirewallProfile -Profile Domain,Private,Public -LogAllowed True
Set-NetFirewallProfile -Profile Domain,Private,Public -LogBlocked True
```

This enables logging of allowed and blocked firewall connections for all network profiles.

Step 4: Configure Wazuh to Collect Firewall Logs

1. Edit ossec.conf again.
2. Add this <localfile> entry inside <ossec_config> to monitor the firewall log:

```
<localfile>
  <location>C:\Windows\System32\LogFiles\Firewall\pfirewall.log</location>
  <log_format>full_command</log_format>
</localfile>
```

3. Save the file.
4. Restart the Wazuh Agent service:

```
net stop wazuhsvc
net start wazuhsvc
```

Step 5: Test Firewall Logging

- Generate network activity by browsing websites, pinging hosts, or running network scans.
- Wait a few minutes.

Wazuh File Integrity Monitoring (FIM) & Windows Firewall Lab

- Review firewall events in Wazuh dashboard, looking for ALLOW and BLOCK connection logs.

Expected Results

Use Case	Expected Alert Details
File Integrity Monitoring	User/process who changed files, file diffs, timestamps
Firewall Log Monitoring	Allowed/blocked connection details, ports, IPs

---

Troubleshooting Tips

- Ensure the Wazuh Agent service is running (Get-Service wazuhsvc).
- Validate ossec.conf for correct XML syntax.
- Verify firewall logging is enabled on all profiles.
- Tail Wazuh agent log for errors:

```
Get-Content "C:\Program Files (x86)\ossec-agent\logs\ossec.log" -Wait
```

Resume Highlights

- Implemented real-time file integrity monitoring with user attribution and content change diffs using Wazuh.
- Enabled and monitored Windows Firewall logs to detect suspicious network activity.
- Demonstrated hands-on experience in Windows host-based security monitoring and alert validation.

References

Wazuh File Integrity Monitoring (FIM) & Windows Firewall Lab

- Wazuh Documentation - File Integrity Monitoring
- Windows Firewall Logging

License