



## **MALWARE DOWNLOAD AND INCIDENT RESPONSE EVALUATION USING PFSENSE AND WAZUH**

**SOC ANALYST TASK WEEK 03  
SUBMITTED BY: SIMRA FATIMA  
TEAM LEAD: ABDULLAH UMAR  
SOC TEAM DELTA**



## ABSTRACT

This report documents a malware simulation exercise conducted on August 15th, 2024, to evaluate the performance of a pfSense firewall and Wazuh SIEM system. The exercise involved a Kali Linux VM downloading a freely available malware sample from eicar.org. The pfSense firewall, configured with specific rules to block known malware, successfully intercepted the download attempt. Wazuh SIEM monitored and logged the event, capturing detailed information for analysis. The report includes a thorough examination of Indicators of Compromise (IOCs) and Indicators of Attack (IOAs) identified during the exercise. It also presents a detailed incident response plan following industry standards, covering detection, analysis, containment, eradication, and recovery steps. The results validate the effectiveness of the security measures in place and provide a structured approach for future incident management.

### Pre-requisites:

- Ensure that pfSense is properly installed and configured.
- Ensure a virtual machine is prepared (I used Kali Linux).
- Verify that Wazuh is installed and configured.
- Ensure that pfSense has been integrated as an agent in Wazuh. For detailed instructions, refer to the documentation here:  
<https://benheater.com/integrating-pfsense-with-wazuh/>

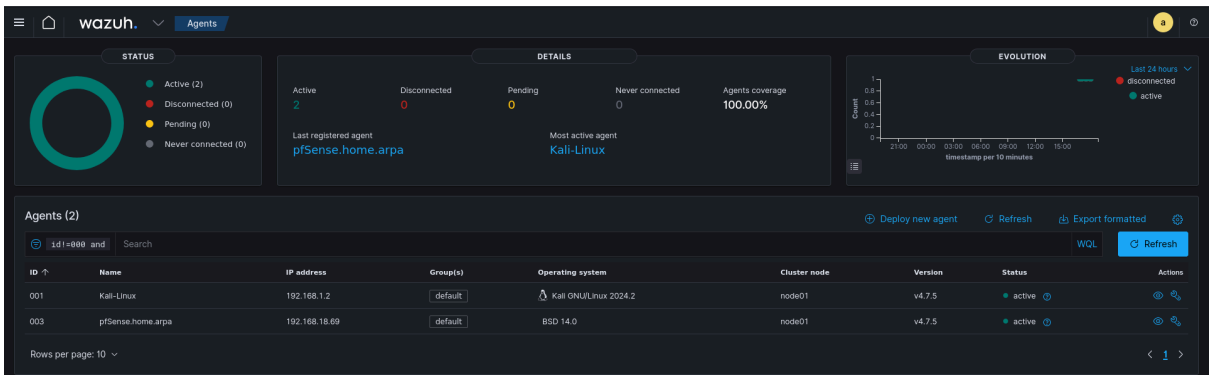
Here are the details and IPs of components used in the task.

- Kali Linux: 192.168.1.2
- Wazuh Manager: 192.168.18.68
- pfSense LAN IP: 192.168.1.1
- pfSense LAN IP: 192.168.18.69

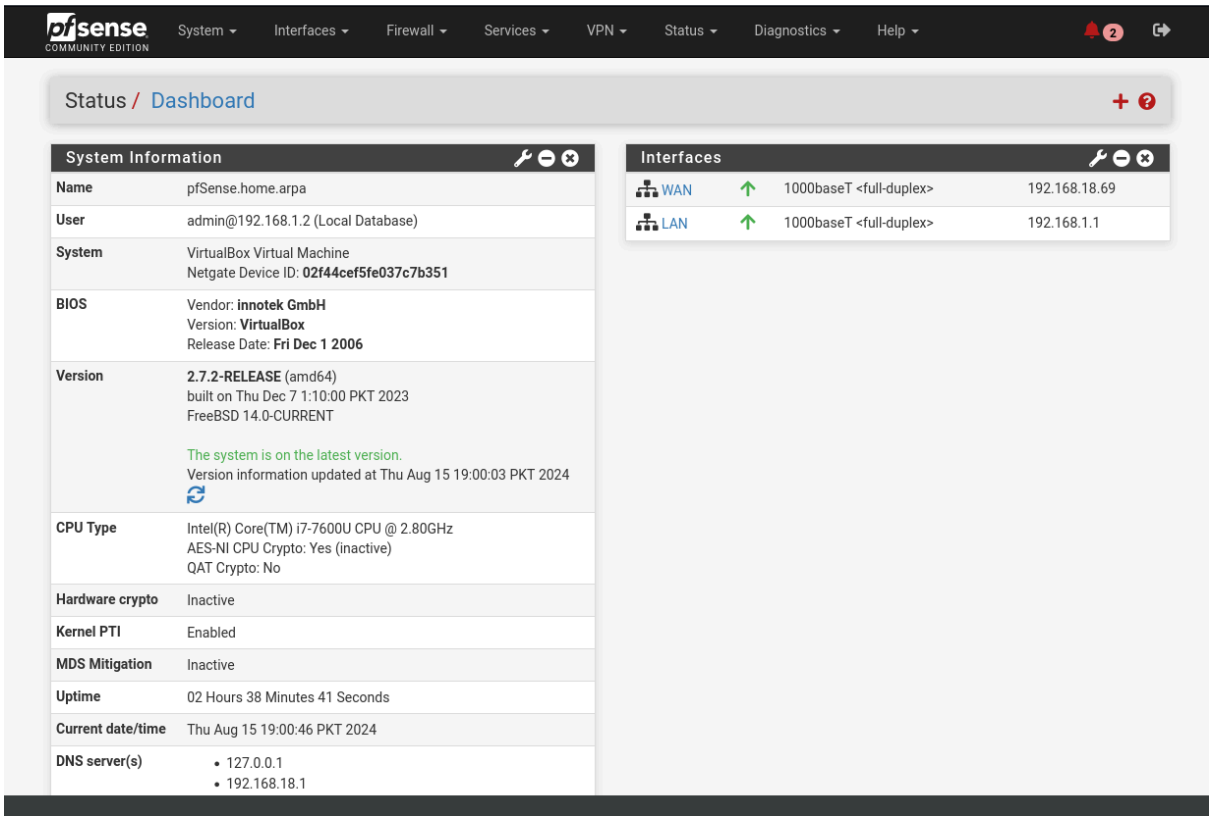
### STEPS:

#### 1. Connecting to the Wazuh Dashboard via Kali Linux

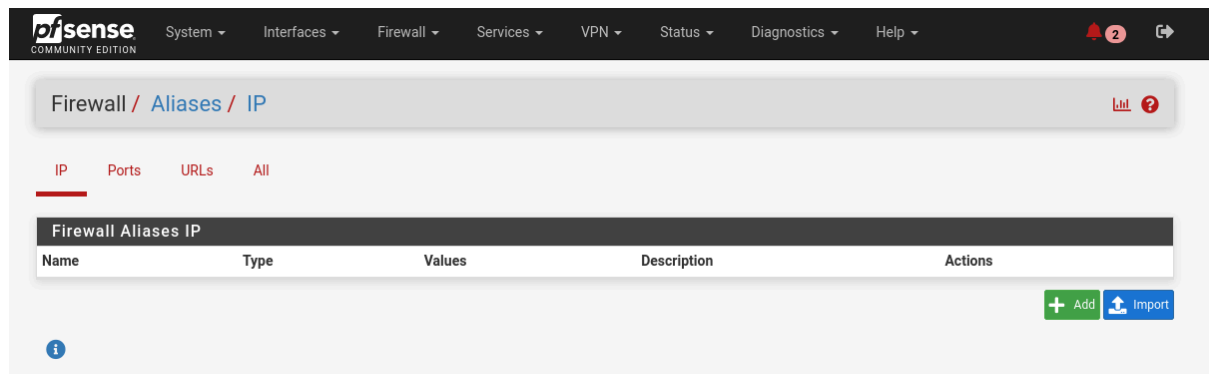
The agents for Kali Linux and pfSense are both configured and operational.



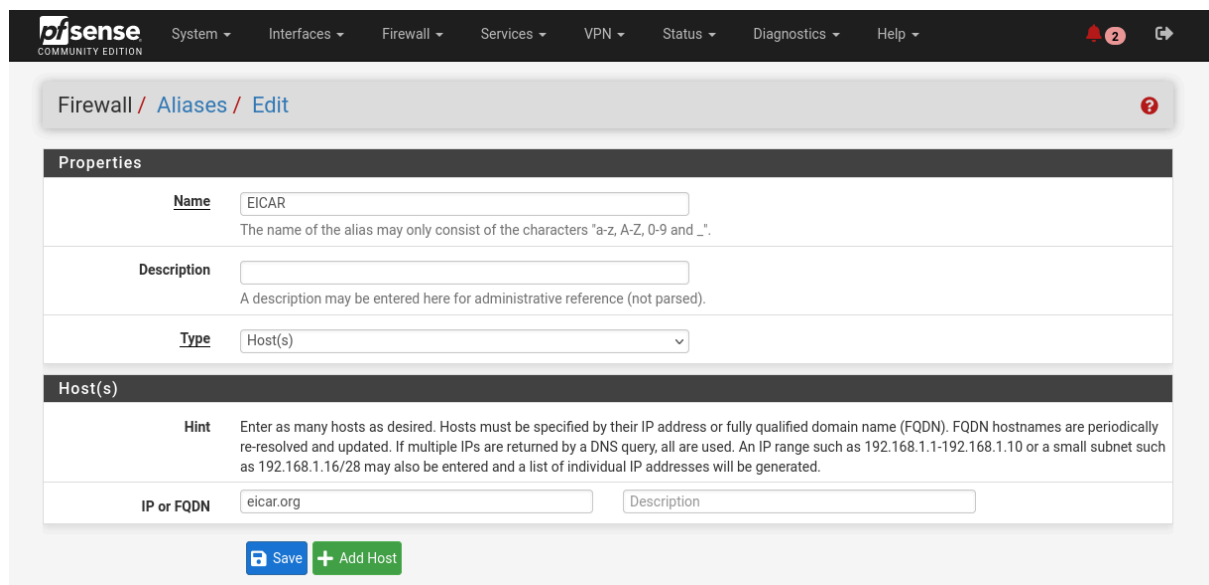
2. Setting up an alias for the designated malware file in pfsense



Go to Firewall → Aliases

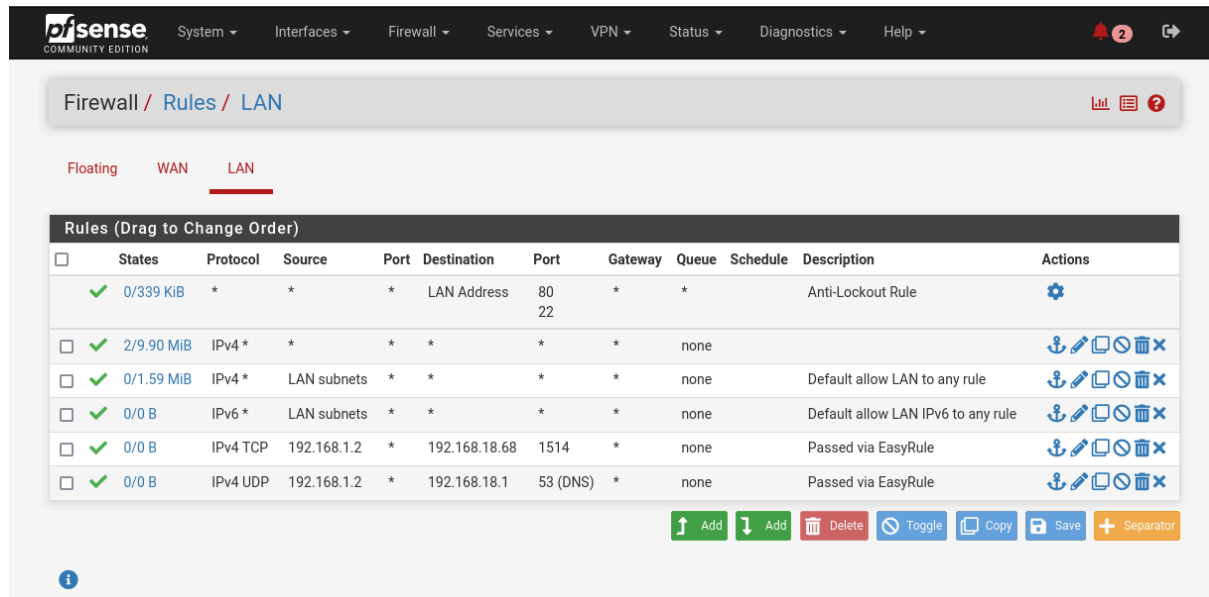


Select “Add” to create an alias. Assign a name to the alias, such as “EICAR.” Choose the “Host(s)” type to detect any domain related to the specified IP/FQDN, which in this case is “eicar.org.” Click “Save” to finalize the configuration.



### 3. Creating firewall rule to block the malware download

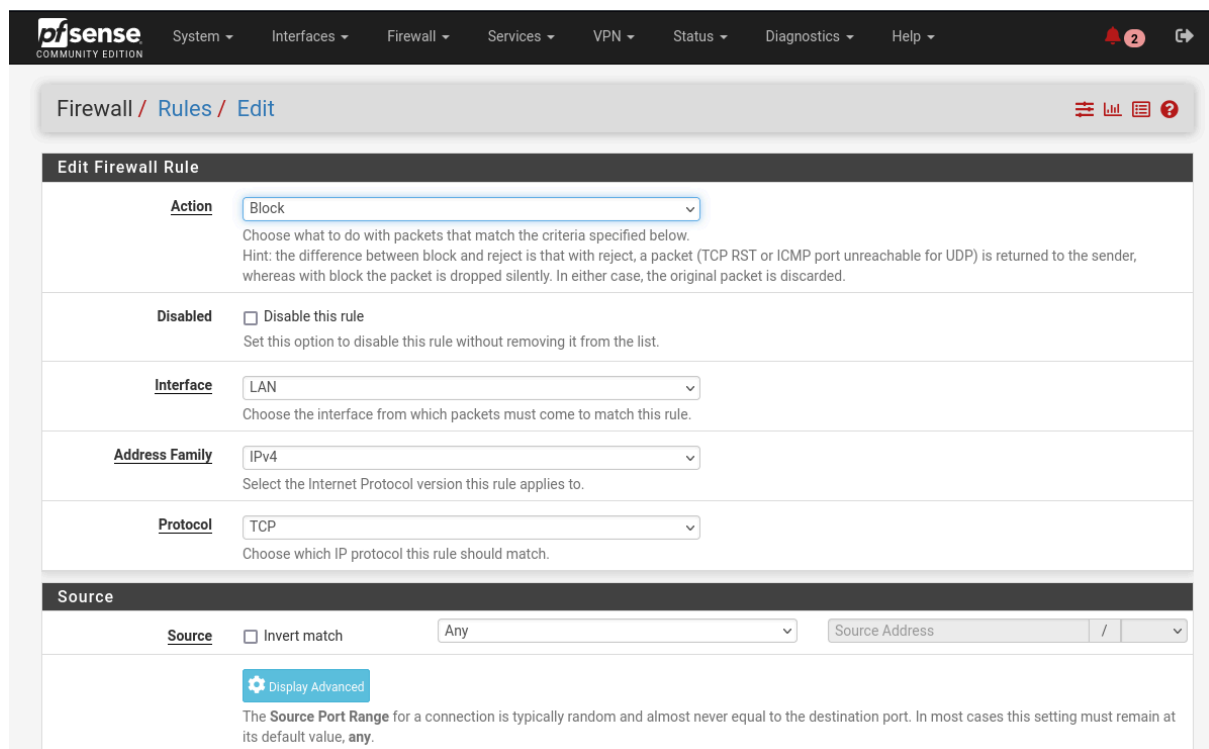
Go to Firewall → Rules → LAN and click on “Add” to add a new rule.



The screenshot shows the pfSense Firewall Rules configuration page. The breadcrumb trail is Firewall / Rules / LAN. The 'LAN' tab is selected. Below the tabs, there is a table of rules. The first rule is 'Anti-Lockout Rule' with a status of '0/339 KiB'. Below the table, there are buttons for 'Add', 'Delete', 'Toggle', 'Copy', 'Save', and 'Separator'.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/339 KiB	*	*	*	LAN Address	80 22	*	*		Anti-Lockout Rule	⚙️
✓ 2/9.90 MiB	IPv4 *	*	*	*	*	*	none			🔗 📄 🗑️ ✖️
✓ 0/1.59 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	🔗 📄 🗑️ ✖️
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	🔗 📄 🗑️ ✖️
✓ 0/0 B	IPv4 TCP	192.168.1.2	*	192.168.18.68	1514	*	none		Passed via EasyRule	🔗 📄 🗑️ ✖️
✓ 0/0 B	IPv4 UDP	192.168.1.2	*	192.168.18.1	53 (DNS)	*	none		Passed via EasyRule	🔗 📄 🗑️ ✖️

Set the action to “Block,” configure the interface to “LAN,” and leave the source as “Any.”



The screenshot shows the 'Edit Firewall Rule' page in pfSense. The 'Action' is set to 'Block'. The 'Interface' is set to 'LAN'. The 'Address Family' is set to 'IPv4'. The 'Protocol' is set to 'TCP'. The 'Source' is set to 'Any'. The 'Source Address' is set to 'Source Address'. The 'Source Port Range' is set to 'any'.

**Edit Firewall Rule**

**Action** Block  
Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface** LAN  
Choose the interface from which packets must come to match this rule.

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** TCP  
Choose which IP protocol this rule should match.

**Source**

**Source** ☐ Invert match Any Source Address /

**Display Advanced**  
The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Choose “Address or Alias” for the destination and select the “EICAR” alias from the prior setup. Enable logging to ensure pfSense captures the activity. Provide a description and click “Save” to finalize.

Destination

Destination

☐ Invert match

Address or Alias

EICAR

Destination Port Range

any

From

Custom

To

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log

☒ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

Block Access to EICAR

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Save

The rule is created successfully

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	*	*	*	LAN Address	80 22	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	EICAR	*	*	none		Block Access to EICAR	

#### 4. Downloading the malware and monitoring logs in pfsense

Visit <https://www.eicar.org/download-anti-malware-testfile/#top> in your browser to download the malware; EICAR Test File. The URL doesn't load, hence blocking the malware download based on the alias and firewall rule created. This will cause pfSense to generate logs.

Go to Status → System Logs → Firewall to view the logs.

**PiSense** COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Status / System Logs / Firewall / Normal View

System Firewall DHCP Authentication IPsec PPP PPPoE/L2TP Server OpenVPN NTP Packages Settings

Normal View Dynamic View Summary View

**Last 312 Firewall Log Entries. (Maximum 500)**

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Aug 12 13:13:47	WAN	Default deny rule IPv6 (1000000105)	[fe80::c8d:2bf2:5494:e999]:53727	[ff02::1:3]:5355	UDP
✗	Aug 12 13:15:39	WAN	Default deny rule IPv6 (1000000105)	[fe80::c8d:2bf2:5494:e999]:50447	[ff02::1:3]:5355	UDP
✗	Aug 12 13:32:35	WAN	block bogon IPv4 networks from WAN (11001)	0.0.0.0:68	255.255.255.255:67	UDP
✗	Aug 12 13:33:42	WAN	block bogon IPv4 networks from WAN (11001)	0.0.0.0:68	255.255.255.255:67	UDP
✗	Aug 12 13:45:39	WAN	Default deny rule IPv6 (1000000105)	[fe80::c8d:2bf2:5494:e999]:65091	[ff02::1:3]:5355	UDP
✗	Aug 12 15:02:40	WAN	(11003)	0.0.0.0:68	255.255.255.255:67	UDP
✗	Aug 12 15:02:42	WAN	(11003)	0.0.0.0:68	255.255.255.255:67	UDP
✗	Aug 12 15:03:25	WAN	(11003)	0.0.0.0:68	255.255.255.255:67	UDP
✗	Aug 12 15:03:25	WAN	Default deny rule IPv6 (1000000105)	[fe80::c8d:2bf2:5494:e999]:53516	[ff02::1:3]:5355	UDP
✗	Aug 12 15:03:26	WAN	Default deny rule IPv6 (1000000105)	[fe80::c8d:2bf2:5494:e999]:63339	[ff02::1:3]:5355	UDP
✗	Aug 12 15:03:27	WAN	Default deny rule IPv6 (1000000105)	[fe80::c8d:2bf2:5494:e999]:52879	[ff02::1:3]:5355	UDP
✗	Aug 12 15:03:27	WAN	Default deny rule IPv6 (1000000105)	[fe80::c8d:2bf2:5494:e999]:55455	[ff02::1:3]:5355	UDP
✗	Aug 12 15:03:28	WAN	Default deny rule IPv6 (1000000105)	[fe80::c8d:2bf2:5494:e999]:60807	[ff02::1:3]:5355	UDP

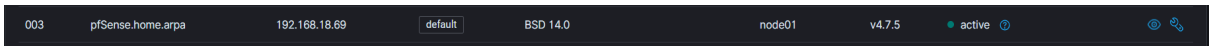
Scroll to the bottom to view the logs generated by this activity.

✗	Aug 15 21:49:48	LAN	Block Access to EICAR (1723740237)	192.168.1.2:57528	89.238.73.97:443	TCP:S
✗	Aug 15 21:49:50	LAN	Block Access to EICAR (1723740237)	192.168.1.2:49594	89.238.73.97:443	TCP:S
✗	Aug 15 21:49:50	LAN	Block Access to EICAR (1723740237)	192.168.1.2:49600	89.238.73.97:443	TCP:S
✗	Aug 15 21:49:51	LAN	Block Access to EICAR (1723740237)	192.168.1.2:49594	89.238.73.97:443	TCP:S
✗	Aug 15 21:49:51	LAN	Block Access to EICAR (1723740237)	192.168.1.2:49600	89.238.73.97:443	TCP:S
✗	Aug 15 21:49:52	LAN	Block Access to EICAR (1723740237)	192.168.1.2:49594	89.238.73.97:443	TCP:S
✗	Aug 15 21:49:52	LAN	Block Access to EICAR (1723740237)	192.168.1.2:49600	89.238.73.97:443	TCP:S
✗	Aug 15 21:49:53	LAN	Block Access to EICAR (1723740237)	192.168.1.2:49594	89.238.73.97:443	TCP:S
✗	Aug 15 21:49:53	LAN	Block Access to EICAR (1723740237)	192.168.1.2:49600	89.238.73.97:443	TCP:S
✗	Aug 15 21:49:54	LAN	Block Access to EICAR (1723740237)	192.168.1.2:49594	89.238.73.97:443	TCP:S
✗	Aug 15 21:49:54	LAN	Block Access to EICAR (1723740237)	192.168.1.2:49600	89.238.73.97:443	TCP:S
✗	Aug 15 21:49:55	LAN	Block Access to EICAR (1723740237)	192.168.1.2:49594	89.238.73.97:443	TCP:S
✗	Aug 15 21:49:55	LAN	Block Access to EICAR (1723740237)	192.168.1.2:49600	89.238.73.97:443	TCP:S
✗	Aug 15 21:49:57	LAN	Block Access to EICAR (1723740237)	192.168.1.2:49594	89.238.73.97:443	TCP:S
✗	Aug 15 21:49:57	LAN	Block Access to EICAR (1723740237)	192.168.1.2:49600	89.238.73.97:443	TCP:S
✗	Aug 15 21:50:01	LAN	Block Access to EICAR (1723740237)	192.168.1.2:49594	89.238.73.97:443	TCP:S
✗	Aug 15 21:50:01	LAN	Block Access to EICAR (1723740237)	192.168.1.2:49600	89.238.73.97:443	TCP:S
✗	Aug 15 21:50:09	LAN	Block Access to EICAR (1723740237)	192.168.1.2:49594	89.238.73.97:443	TCP:S
✗	Aug 15 21:50:10	LAN	Block Access to EICAR (1723740237)	192.168.1.2:49600	89.238.73.97:443	TCP:S

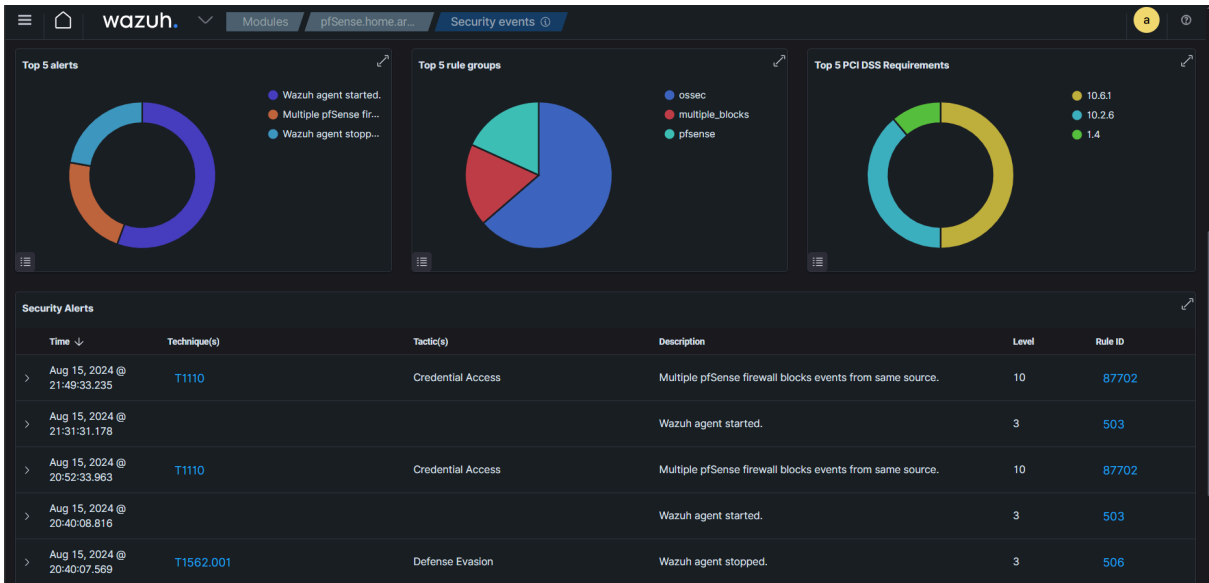
The malware download attempt is successfully blocked by the firewall from the source IP 192.168.1.2 to the destination IP 89.238.73.97 (EICAR's IP).

## 5. Monitoring logs in Wazuh

Head to the pfsense agent on your Wazuh dashboard to view the pfsense logs on Wazuh



Here you can see the logs in security events as “Multiple pfSense firewall blocks events from same source”



Examining the details reveals that access was blocked from the source IP 192.168.1.2 to the destination IP 89.238.73.97 (EICAR’s IP), effectively stopping the malware download.

The JSON view shows the following details for the alert:

@timestamp	Aug 15, 2024 @ 21:49:33.235
_index	wazuh-alerts-4.x-2024.08.15
agent.id	003
agent.ip	192.168.18.69
agent.name	pfSense.home.arpa
data.action	block
data.dstip	89.238.73.97
data.dstport	443
data.id	1723748237
data.length	0
data.protocol	tcp
data.srcip	192.168.1.2
data.srcport	57528
decoder.name	pf
full_log	Aug 15 21:49:31 pfSense filterlog[97289]: 84...1723748237,en1,match,block,in,4,0x0,,64,9333,0,DF,6,tcp,60,192.168.1.2,89.238.73.97,57528,443,0,S,255815727,,32128,,msg;sack OK;TS;nop;wscale
id	1723748573.4962670
input.type	log
location	/var/log/filter.log
manager.name	wazuh-server



Discoverwazuht-alerts-4.x-2024.08.15#3BfxVpEBmelrj_aS147Q	
predecoder.hostname	pfSense
predecoder.program_name	filterlog
predecoder.timestamp	Aug 15 21:49:31
previous_output	<div><div></div><div>Aug 15 21:49:31 pfSense filterlog[97289]: 84,,,1723748237,em1,match,block,in,4,0x0,,64,39634,0,DF,6,tcp,60,192.168.1.2,89.238.73.97,57514,443,0,S,2867329585,,32120,,mss;sa ckOK;TS:nop;wscale Aug 15 21:49:23 pfSense filterlog[97289]: 84,,,1723748237,em1,match,block,in,4,0x0,,64,9332,0,DF,6,tcp,60,192.168.1.2,89.238.73.97,57528,443,0,S,255815727,,32120,,mss;sack OK;TS:nop;wscale Aug 15 21:49:23 pfSense filterlog[97289]: 84,,,1723748237,em1,match,block,in,4,0x0,,64,39633,0,DF,6,tcp,60,192.168.1.2,89.238.73.97,57514,443,0,S,2867329585,,32120,,mss;sa ckOK;TS:nop;wscale Aug 15 21:49:10 pfSense filterlog[97289]: 84,,,1723748237,em1,match,block,in,4,0x0,,64,9331,0,DF,6,tcp,60,192.168.1.2,89.238.73.97,57528,443,0,S,255815727,,32120,,mss;sack OK;TS:nop;wscale</div></div>
rule.description	Multiple pfSense firewall blocks events from same source.
rule.firedtimes	1
rule.frequency	18
rule.gpg13	4.12
rule.groups	pfsense, multiple_blocks
rule.hipaa	164.312.a.1, 164.312.b
rule.id	87782
rule.level	10
rule.mail	false
rule.mitre.id	T1110
rule.mitre.tactic	Credential Access
rule.mitre.technique	Brute Force
rule.nist_800_53	SC.7, AU.6
rule.pci_dss	1.4, 10.6.1
rule.tsc	CC6.7, CC6.8, CC7.2, CC7.3

# IOCs and IOAs

## Incident Overview

- **Incident Date and Time:** August 15th, 2024, 15:35 UTC
- **Source IP Address:** 192.168.1.2 (Kali Linux VM)
- **Destination IP Address:** 89.238.73.97 (EICAR server)
- **Malware URL:** <https://www.eicar.org/download-anti-malware-testfile/#top>
- **Reported by:** Simra Fatima
- **Reported to:** ITSOLERA SOC Department

## Incident Summary

On August 15th, 2024, at 15:35 UTC, the Kali Linux VM (IP: 192.168.1.2) attempted to download the EICAR test file from eicar.org (IP: 89.238.73.97). The pfSense firewall, configured with rules to block known malware test files, successfully intercepted this attempt. The event was logged and alerted by the Wazuh SIEM system, demonstrating the effectiveness of both the firewall and SIEM in detecting and responding to potential threats.

## Indicators of Compromise (IOCs)

### IP Addresses:

- **Source IP:** 192.168.1.2
- **Description:** IP address of the Kali Linux VM initiating the download attempt.
- **Destination IP:** 89.238.73.97
- **Description:** IP address of the server hosting the EICAR test file.

### Domain Names:

- **Domain:** eicar.org
- **Description:** Domain associated with the EICAR test file, used for evaluating malware detection systems.

### Malicious files or URLs Accessed:

- **Malware-URL:** <https://www.eicar.org/download-anti-malware-testfile/#top>
- **Description:** URL used to attempt the download of the EICAR test file, a known test file used to assess the effectiveness of security defenses.

## Indicators of Attack (IOAs)

- **Malware Test File Download Attempt:**
  - **Behavior:** Attempt to download the EICAR test file.
  - **Intent:** Test or bypass network defenses.
  - **Technique:** Direct download from a known test domain.

- **Credential Access Attempts:**
  - **Behavior:** Detected unauthorized access attempts.
  - **Intent:** Gain unauthorized access to systems or data.
  - **Technique:** Brute force or credential dumping methods.
- **Defense Evasion Techniques:**
  - **Behavior:** Actions to avoid detection by security systems.
  - **Intent:** Reduce likelihood of triggering security alerts.
  - **Technique:** Obfuscation or disabling security tools.
- **Connection to Suspicious Domain:**
  - **Behavior:** Connection attempt to eicar.org.
  - **Intent:** Validate network defenses or test response mechanisms.
  - **Technique:** Utilizing domains known for test files.
- **Firewall Rule Triggered:**
  - **Behavior:** Firewall rules activated to block the connection.
  - **Intent:** Intercept and neutralize the potential threat.
  - **Technique:** Rule-based blocking based on test file signatures.

# Incident Response Plan

## 1. Detection

- **Standards:** Follow NIST SP 800-61 for incident detection procedures.
- **Action:** Use Wazuh SIEM to monitor for and alert on suspicious activities and traffic patterns.
- **Tools:** Wazuh SIEM and pfSense firewall logs.

## 2. Analysis

- **Standards:** Align with NIST SP 800-86 for forensic analysis.
- **Action:** Investigate and validate the nature of the alert. Correlate with known IOCs and attack patterns.
- **Tools:** Log analysis from Wazuh and pfSense.

## 3. Containment

- **Standards:** Refer to NIST SP 800-61 for containment strategies.
- **Action:** Implement immediate measures to prevent further interactions with the threat source. Block relevant IP addresses and domains.
- **Tools:** pfSense firewall rules and network access controls.

## 4. Eradication

- **Standards:** Follow NIST SP 800-61 for eradication procedures.
- **Action:** Remove any residual threats from affected systems and apply patches as needed.
- **Tools:** System cleanup and updates.

## 5. Recovery

- **Standards:** Adhere to NIST SP 800-61 for recovery processes.
- **Action:** Restore systems to normal operation. Ensure that all security measures are effective and monitor for signs of residual threats.
- **Tools:** System monitoring and validation.

## 6. Post-Incident Review

- **Standards:** Align with ISO/IEC 27035 for post-incident analysis.
- **Action:** Conduct a review of the incident, assess response effectiveness, and update incident response plans as needed.
- **Tools:** Incident review documentation and lessons learned.

## Report Sharing

- **Document Compilation:** This report, including detailed IOCs and IOAs, and compliance by regulatory standards will be compiled into a comprehensive incident response plan.
- **Review and Implementation:** The document will be shared with relevant stakeholders for review and implementation of the incident response procedures.

## Behavioral Analysis

The incident involved a simulated malware download attempt detected and blocked by network defenses. Credential Access and Defense Evasion tactics were identified, suggesting advanced persistent threat (APT) behavior aimed at unauthorized access and evasion.

## Impact Assessment

The incident was contained effectively with no malware entering the network. The pfSense firewall and Wazuh SIEM systems successfully detected and responded to the threat, demonstrating their capability in real-time threat management.

---

---

LinkedIn

[www.linkedin.com/in/simra-fatima-39b068252](https://www.linkedin.com/in/simra-fatima-39b068252)