Research Paper By:

Syed Muhammad Shah

TEAM ~ OMEGA

OS Selection for Malware Analysis

Use a **single-purpose, isolated VM** (e.g. VirtualBox) dedicated to the malware test. Common choices are Windows 10 (easy setup, many tools) or a Linux distro like Ubuntu/REMnux. For example, a Windows 10 VM (free from Microsoft for testing) or Ubuntu with security tools is suitable[1]. Ensure the VM is on an **internal-only network** (no Internet except via the pfSense gateway)[2]. Take a snapshot immediately for recovery. Disable shared folders and USB passthrough for safety.

Malware Sample Source and Analysis Type

Obtain samples from **reputable, academic sources** – e.g. theZoo, MalwareBazaar, or Contagio (password-protected dumps)[3]. For simplicity and safety, you can use the **EICAR test file** (a harmless antivirus test string) from eicar.org[4]. Always handle any real malware with caution (offline and on the isolated VM).

For a basic internship project, use **static analysis** (no execution). Static analysis "helps experts quickly identify and understand malware without the risk of running it on a system"[5]. It is fast and safe for known patterns (like EICAR) and avoids accidentally activating malicious behavior. (Dynamic/sandbox analysis is more involved and riskier for novices.)

Integrating the New VM with pfSense & Wazuh

1. **Network setup:** Attach the new VM's virtual NIC to the same "LAN" network behind pfSense (e.g. VirtualBox *Internal Network*). Set the VM's IP (via DHCP or static) so that pfSense is the gateway/DNS. Confirm pfSense sees this VM on its LAN.
2. **Wazuh agent installation:** Install the Wazuh agent on the VM so it reports to the manager VM. For Linux: add Wazuh's apt repository, import the GPG key, then install with the manager's IP. For example:
3. `sudo apt-get update && sudo apt-get install gnupg apt-transport-https`
4. `curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo apt-key add -`
5. `echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee /etc/apt/sources.list.d/wazuh.list`
6. `sudo apt-get update`
7. `sudo WAZUH_MANAGER="<Wazuh-Manager-IP>" apt-get install wazuh-agent`

8. `sudo systemctl enable --now wazuh-agent`[6][7].
   For Windows: download the Wazuh MSI installer from Wazuh's site, run it (GUI or `msiexec`), specifying the manager's address (e.g. `wazuh-agent-4.12.0-1.msi /q WAZUH_MANAGER="<Wazuh-Manager-IP>"`)[8]. After install, ensure the agent registers in the Wazuh dashboard.
9. **pfSense log forwarding:** Make sure pfSense syslog is sent to Wazuh. On pfSense, enable remote logging (e.g. under **Status > System Logs > Settings**). If needed, install the pfSense **syslog-ng** package and configure it to forward logs (RFC3164) to the Wazuh manager (port 514/UDP)[9]. Verify in Wazuh that pfSense appears as a source (either via an agent or syslog input).
10. **Firewall rule (optional):** To ensure pfSense *blocks* the test download (and logs it), create a firewall rule on the LAN that blocks traffic to the test URL's IP or domain. For example, add an alias "EICAR" pointing to the EICAR download domain, then create a **Block** rule using that alias. Enable logging on the rule. (This step is optional but demonstrates pfSense detection.)

Malware Download, Detection, and Logging

1. **Acquire the sample:** On the isolated VM, download the malware test sample. For EICAR, use a browser or command
2. (e.g. `curl -O https://www.eicar.org/download/eicar.com.txt`). Since it's a harmless text containing "EICAR-STANDARD-ANTIVIRUS-TEST-FILE!", it will not harm the VM but will trigger AV scanners or signature-based detections.[4]
3. **Static analysis (VM side):** Do not execute the file. Instead, inspect it (e.g. open in a text editor or `strings`) to confirm it's the EICAR pattern. (You may also scan it with ClamAV/Windows Defender to see that it flags the signature.)
4. **Observe pfSense:** On pfSense, check **Status > System Logs > Firewall** for entries. You should see a log for the connection (and if the block rule is active, a "Blocked" log for the EICAR site). Wazuh will ingest this log via syslog; check the Wazuh agent entry for pfSense in the dashboard to confirm it recorded a firewall event (e.g. "LAN Blocked TCP from <VM IP> to <EICAR IP>"). In Studocu's example, the firewall "intercepted" the EICAR download attempt[10].
5. **Wazuh logs:** In the Wazuh Dashboard (Security Events or Vulnerability Detection), filter by the VM's hostname or source IP. Look for events around the download time. The agent will report system logs (e.g. on Windows, Application/Security events; on Linux, auth or syslog entries). Wazuh's built-in rules might flag the EICAR signature if malware detection is enabled. At minimum, find entries for the new file creation (if FIM was enabled) or outbound connection. Also check the *Logs* app (or Kibana Discovery) for the exact URL or filename. For example, search for "EICAR" or the file hash to see where it appears.
6. **Alert confirmation:** If everything is configured, Wazuh should generate an alert/event correlating to the malicious download or firewall block. You may see a rule like "Multiple firewall blocks from same source" on the pfSense agent (as in the example[11]). Verify that an alert was raised in Wazuh for the relevant agent.

Log Analysis and IOCs/IOAs

Collect relevant logs and identify **Indicators of Compromise (IOCs)** and **Indicators of Attack (IOAs)**:
- **Network IOCs:** Source IP of the VM and destination IP/domain of the malware host. In our example, the VM IP (e.g. 192.168.1.x) is an IOC, and the EICAR server domain/IP is a known IOC[10].
- **File IOCs:** The name and hash of the downloaded file (e.g. `eicar.com` or `eicar.com.txt`) act as IOCs. The EICAR signature itself is a static IOC.
- **Log IOCs:** PFsense log entries (source/dest IP, port, protocol) and any alerts in Wazuh referencing the URL or alias. The attempted URL ("https://www.eicar.org/download/eicar.com.txt") is an IOC[12].
- **IOAs (behaviors):** Look for telltale actions: the **download attempt behavior** itself is an IOA ("attempt to retrieve malicious file")[13]. Another IOA is the **firewall rule trigger** – the fact that our block rule fired (pfSense blocked the connection) indicates an attempted attack. Any repeated connection attempts or new process starts could be IOAs.
- **Analysis:** In Wazuh, correlate these logs. For example, Wazuh's "Threat Hunting" can track the VM agent for suspicious events. Note if any IDS (Snort/Suricata on pfSense) flagged the traffic. Document all suspicious signs. (In the student report example, the IOAs listed included the download attempt behavior and the firewall defense action[14].)

Incident Response Plan (NIST-Based)

Following NIST SP 800-61 guidelines, the IR plan covers **Detection/Analysis, Containment, Eradication, and Recovery**[15][16]. Key steps are:

- **Detection & Analysis:** Monitor alerts and logs to confirm an incident[17]. Here, detection comes from the pfSense firewall alert and Wazuh security events. The analyst verifies the incident (signs of the EICAR download attempt), documents all findings, and assesses severity[18][17]. Prioritize the incident based on impact (lab only) and notify stakeholders.

- **Containment:** Immediately isolate the affected VM to prevent further "infection." This could mean shutting down or disconnecting the VM from the network (leaving it offline). In our lab scenario, the download was blocked, but best practice is still to disconnect the host VM from the virtual LAN. Containment strategies "halt the effects of an incident before it can cause further damage"[19]. Also, apply temporary firewall rules (e.g. block the malicious domain for all hosts) if not already done. Document all containment actions.

- **Eradication:** Remove the threat from the system. Delete the malware file (EICAR sample) and any related scripts or payloads. Scan the VM with updated antivirus to ensure no hidden components remain. If credentials were exposed (unlikely with EICAR), reset them. Since this was a test, no actual malware installed persistence; but the general step is to **"remove threats from the environment, like deleting malicious files and closing unauthorized access points"**[16]. Verify Wazuh/FIM logs show no residual compromise.

- **Recovery:** Restore normal operations. Revert the VM to a clean snapshot (we took one before the test) to ensure a known-good state. Re-enable network connectivity and monitoring. Verify the VM is patched and re-hardened before reuse. According to NIST, recovery "focuses on restoring systems and operations to normal by repairing or replacing affected resources," ensuring no threats remain[16].
- **Post-Incident (Lessons Learned):** Finally, conduct a debrief. Gather the response team to review what happened. Document the timeline, what was detected (IOCs/IOAs), and how each phase was handled. Identify any gaps in detection or response. Update the incident response plan and firewall rules accordingly (e.g. add signatures, refine rules). As industry advice stresses, a **"lessons learned meeting"** should follow every incident[20]. Note improvements (e.g. ensure Wazuh rules catch the EICAR pattern in future) and share these with the CSIRT.

Each phase should be thoroughly documented. Following NIST's model ensures a structured approach[17][16]. The above steps align with best practices (NIST/SANS/CERT) for malware incidents and provide a clear path from detection through recovery.

Sources: Established guidelines and lab best practices (e.g. NIST IR life cycle[17][16], SentinelOne lab setup[1][2], Wazuh integration docs[9][8], and malware sample references[4][3]) were used to build this workflow. The process was demonstrated in a test exercise where a Kali VM's EICAR download was blocked by pfSense and logged by Wazuh[10], confirming end-to-end detection.

---

[1] [2] Building a Custom Malware Analysis Lab Environment - SentinelLabs

https://www.sentinelone.com/labs/building-a-custom-malware-analysis-lab-environment/

[3] Free Malware Sample Sources for Researchers

https://zeltser.com/malware-sample-sources/

[4] EICAR test file - Wikipedia

https://en.wikipedia.org/wiki/EICAR_test_file

[5] Static Malware Analysis vs Dynamic Malware Analysis - Comparison Chart

https://www.malwation.com/blog/static-malware-analysis-vs-dynamic-malware-analysis-comparison-chart

[6] Deploying Wazuh agents on Linux endpoints - Wazuh agent

https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-linux.html

[7] [8] Installing Wazuh agents on Windows endpoints - Wazuh agent

https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-windows.html

[9] Send Pfsense logs to Wazuh - devopstales

https://devopstales.github.io/linux/wazuh-pfsense-syslog/

[10] [11] [12] [13] [14] 1724139573808 - SOC Analyst Week 03: Malware Response with pfSense & Wazuh - Studocu

https://www.studocu.com/row/document/time-universite/network-security/1724139573808-soc-analysis-with-pfsense-and-wuzhu/102556725

[15] [17] NIST Incident Response: 4-Step Life Cycle, Templates and Tips

https://www.cynet.com/incident-response/nist-incident-response/

[16] NIST Incident Response: 4-Step Process and Critical Best Practices | Exabeam

https://www.exabeam.com/explainers/incident-response/nist-incident-response-4-step-process-and-critical-best-practices/

[18] [19] [20] Incident Response Plan: Frameworks and Steps | CrowdStrike

https://www.crowdstrike.com/en-us/cybersecurity-101/incident-response/incident-response-steps/