



Cyberprotection Systems

Laboratory Work 1. Event Gathering and Correlation (MEMORY)

NAME AND SURNAME: Austėja Bauraitė

1. Topology configuration

Describe the configured topology (machines, O.S), as well as the technologies used (VirtualBox, Dockers, etc).

The lab runs a simple, flat network with four virtual machines, a Wazuh manager , a Linux endpoint where Suricata is installed alongside the Wazuh agent, plus two additional VMs to play the roles of user/attacker and generate traffic (e.g., nmap) toward LinuxHost. Suricata inspects the network interface on LinuxHost and logs alerts to /var/log/suricata/eve.json, which the Wazuh agent forwards to the manager for correlation and visualization, configuration points include setting HOME_NET, default-rule-path, and enabling rule-files in suricata.yaml. The whole setup is virtualized (in VirtualBox) and uses Suricata with the ET Open ruleset and Wazuh for SIEM/alerting, same as the lab guide.

Put a screenshot (or some) to show them running.

The screenshot shows two side-by-side terminal windows from Oracle VirtualBox. The left window is titled 'NEWwazuh [Running] - Oracle VirtualBox' and shows a terminal session for 'administrador@seminarioST: ~'. The right window is titled 'Clinuxhost [Running] - Oracle VirtualBox' and shows a terminal session for 'administrador@seminarioST: /var/www/testsite'. Both terminals are displaying command-line output related to network interfaces and routing tables, with identical content across both hosts, indicating a synchronized environment.

```
administrator@seminarioST:~$ hostname -I; ip a
10.0.2.15 10.10.10.1 brd 00:00:00:00:00:00
  lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
      valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
      valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
  link/ether 08:00:27:1b:a3:64 brd ff:ff:ff:ff:ff:ff
  inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
    valid_lft 83784sec preferred_lft 83784sec
  inet6 fd17:625c:f037:2:295b:c407:dcba:df5/64 scope global temporary dynamic
    valid_lft 14054sec preferred_lft 14054sec
  inet6 fd17:625c:f037:2:6138:1443:9a4e:d13a/64 scope global dynamic mngtmpaddr noprefixroute
  utl
    valid_lft 86054sec preferred_lft 14054sec
  inet fe80::8c05:1644:b93:8fc/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
  link/ether 08:00:27:32:3f:95 brd ff:ff:ff:ff:ff:ff
  inet 10.10.10.1/24 brd 10.10.10.255 scope global noprefixroute enp0s8
    valid_lft forever preferred_lft forever
  inet6 fe80::a626:357c:93ee:5c4/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
administrator@seminarioST:~$
```

```
administrator@seminarioST:/var/www/testsite$ hostname -I; ip a
10.0.2.15 10.10.10.2 brd 00:00:00:00:00:00
  lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
      valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
      valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
  link/ether 08:00:27:2d:6f:37 brd ff:ff:ff:ff:ff:ff
  inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
    valid_lft 64339sec preferred_lft 64339sec
  inet6 fd17:625c:f037:2:295b:c435:4904:c716/64 scope global temporary dynamic
    valid_lft 14077sec preferred_lft 14077sec
  inet6 fd17:625c:f037:2:f773:dc3b:1f8d:7c47/64 scope global dynamic mngtmpaddr noprefixroute
  utl
    valid_lft 86077sec preferred_lft 14077sec
  inet fe80::2e82:eb03:ce49:eb69/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
  link/ether 08:00:27:8c:9e:72 brd ff:ff:ff:ff:ff:ff
  inet 10.10.10.2/24 brd 10.10.10.255 scope global noprefixroute enp0s8
    valid_lft forever preferred_lft forever
  inet6 fe80::896c:c70f:cd05:9e51/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
administrator@seminarioST:/var/www/testsite$
```



```
Administrator@seminarioST:~
```

```
1: lo <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00 state UNKNOWN
    inet 127.0.0.1/8 brd 00:00:00:00:00:00 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 brd ff00::1 scope host lo
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:78:b7:d5 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 74585sec preferred_lft 74585sec
    inet6 fe80::fe00:27ff:fe78:b7d5/64 scope global temporary dynamic
        valid_lft 86051sec preferred_lft 14095sec
    inet6 fd17:625c:f037:2:640b:eb3f:42b8:bbdb/64 scope global dynamic mngtmpaddr noprefixro
ute
        valid_lft 86051sec preferred_lft 14095sec
    inet6 fe80::7102:42ff:fe00:27ce/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c1:7d:a4 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.4/24 brd 10.10.10.255 scope global dynamic noprefixroute enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::be25:a5::6411:9239/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
Administrator@seminarioST:~
```

```
Administrador Símbolo del sistema
```

```
Microsoft Windows [Versión 10.0.10240]
(c) 2015 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>pconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:
```

```
Sufijo DNS específico para la conexión. . . : 
Dirección IPv6 . . . . . : fd17:625c:f037:2:7436:460:5d85:42f5
Dirección IPv6 temporal . . . . . : fd17:625c:f037:2:a104:ef43:3ba6:a1e6
Vinculo: dirección IPv6 local. . . . . : fe80::7436:460:5d85:42f5%4
Número de interfaz . . . . . : 4
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 10.0.2.2
```

```
Adaptador de ethernet Ethernet 2:
```

```
Sufijo DNS específico para la conexión. . . :
Número de dirección IPv6 local. . . . . : fe80::7436:460:5d85:42f5%7
Dirección IPv4 . . . . . : 10.10.10.3
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . :
```

```
Adaptador de túnel isatap.{428EDD2E-495E-4A08-B8E8-BB6FB4740044}:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :
```

```
Adaptador de túnel isatap.{C46FB87C-4B20-457F-B981-7135170D6F1E}:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :
```

```
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>clear
"clear" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.
C:\Windows\system32>
```

2. Wazuh setting

Show a screenshot (or some) where it can be seen the deployed agents in Wazuh. Explain it.

This Wazuh “Agents” view shows the two endpoints that are actively enrolled with the manager. Agent **003 (LinuxHost01)** at **10.10.10.2** is an **Ubuntu 22.04.5 LTS** host in the **default** group, and agent **005 (DESKTOP-O7BM7AU)** at **10.10.10.3** is a **Windows 10 Enterprise** host, also in **default**. Both are reporting to cluster node **node01** with the same agent major version, registered, and communicating so their logs and security events can be collected and shown in dashboards.

| Agents (2) | | | | | | | <input type="button" value="Deploy new agent"/> | <input type="button" value="Import"/> |
|------------|-----------------|------------|----------|--|--------------|------|---|---------------------------------------|
| Search | | | | | | | | |
| ID | Name | IP address | Group(s) | Operating system | Cluster node | Vers | | |
| 003 | LinuxHost01 | 10.10.10.2 | default | Ubuntu 22.04.5 LTS | node01 | v4.5 | | |
| 005 | DESKTOP-O7BM7AU | 10.10.10.3 | default | Microsoft Windows 10 Enterprise 10.0.10240.17443 | node01 | v4.5 | | |

Rows per page: 10 ▾

3. Wazuh agents

Show a screenshot (or some) with the configuration files of the agents.



```
administrador@seminarioST:~$ sudo cat /var/ossec/etc/ossec.conf
<!--
Wazuh - Agent - Configuration for Ubuntu 22.04
This version collects classic syslog files (auth.log + syslog) and avoids
duplicate ingestion from journald. It also keeps FIM, SCA, and Syscollector enabled.
Replace only the content of /var/ossec/etc/ossec.conf with this block.
-->

<ossec_config>

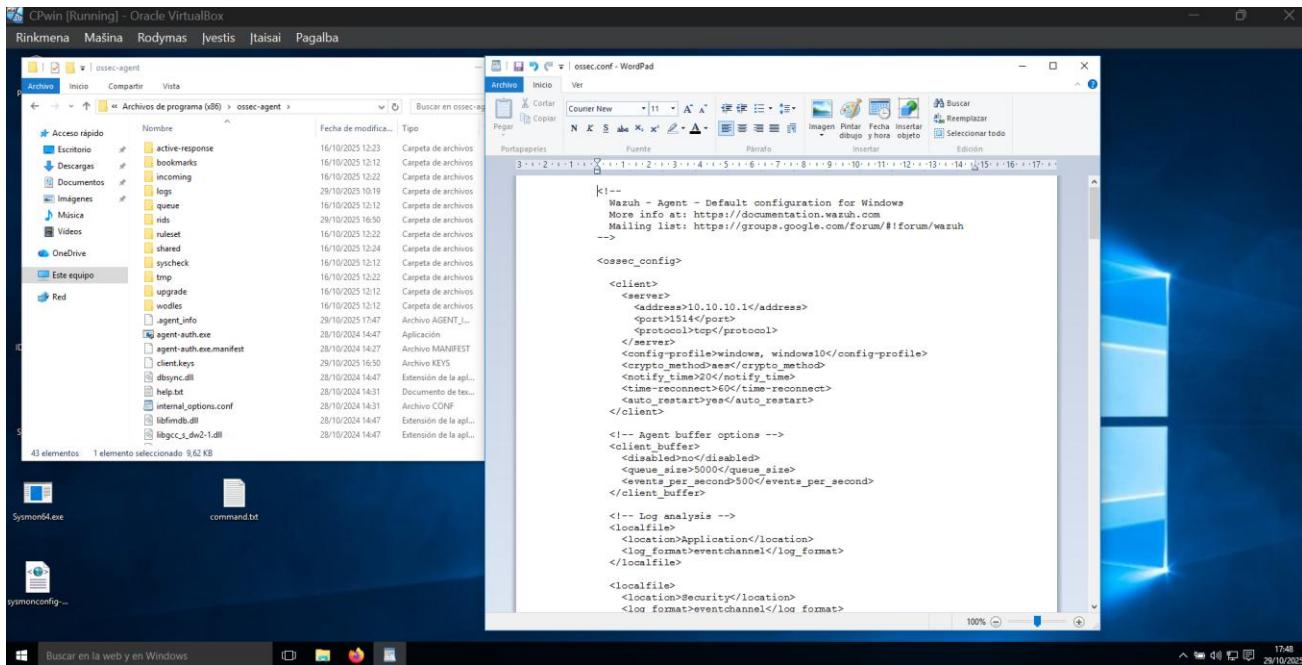
<!-- =====
    Agent -> Manager settings
    ===== -->
<client>
    <server>
        <address>10.10.10.1</address>
        <port>1514</port>
        <protocol>tcp</protocol>
    </server>

    <!-- Profile tags are fine to keep -->
    <config-profile>ubuntu, ubuntu22, ubuntu22.04</config-profile>

    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>

    <!-- Enrollment (leave enabled until the agent is enrolled) -->
    <enrollment>
        <enabled>yes</enabled>
        <agent_name>LinuxHost01</agent_name>
        <!-- Absolute path is clearer -->
        <authorization_pass_path>/var/ossec/etc/authd.pass</authorization_pass_path>
    </enrollment>
</client>

<client_buffer>
```



4. Event generation

- a) Show a screenshot (or some) in which the SSH connection task (from Practical part 1.1) is shown; i.e. present the SSH connection, the actions performed, the log events produced, and the generated events in Wazuh. Explain what it is shown.

An attacker from 10.10.10.2 logged into **LinuxHost01** over SSH as administrador, then ran a few sudo commands (things like whoami). Those actions show up in the host's /var/log/auth.log as SSH accept messages and sudo entries, and the Wazuh agent picked them up and turned them into alerts, you can see the SSH login, the PAM session open/close, and the successful sudo to ROOT executed events in the Wazuh console, complete with the exact commands, the user, the source IP and rule IDs for quick reference.



The image shows two terminal windows side-by-side. Both are running on Oracle VirtualBox. The left window is titled 'CPAttacker [Running] - Oracle VirtualBox' and the right window is titled 'CPlinuxhost [Running] - Oracle VirtualBox'. Both windows show a terminal session for the user 'administrador@seminarioST: ~'. In the left window, the user runs several commands including 'hostname -I', 'ssh', and 'apt update'. In the right window, the user runs 'tail -n 15 /var/log/auth.log' and other log-related commands. The terminal output is in black text on a white background.

With the KQL filter:

```
agent.name:"LinuxHost01" and (
    rule.groups : ("sshd" or "sudo")
    or predecoder.program_name : (sshd or sudo)
)
```

and not agent.id:"000"

The image shows the 'Discover' interface of the Wazuh Data Explorer. The search bar at the top contains the query 'agent.name:"LinuxHost01" and (rule.groups : ("sshd" or "sudo") or predecoder.program_name : (sshd or sudo)) and not agent.id:"000"'. The results table on the right lists several log entries from October 29, 2025, matching the search criteria. The columns include '_source', '_index', 'agent.id', 'agent.ip', 'agent.name', 'data.command', 'data.dsuser', 'data.pwd', 'data.scp', 'data.srport', 'data.sruser', 'data.tty', 'data.uid', 'decoder.fsc comment', 'decoder.name', 'decoder.parent', and 'full_log'. The log entries detail various sudo and sshd activities on the host.



- b) Relate at least three events from the dashboard to the corresponding lines in the auth.log file.

In the auth.log file, we can clearly see the SSH session and the actions that followed, which match the alerts captured in Wazuh. At **17:26:08**, the log records the SSH authentication success “sshd: authentication success” for user *administrador* coming from 10.10.10.2. This corresponds directly to the Wazuh event with **rule ID 5715**, where the agent LinuxHost01 reports a successful SSH login. Just after that, the log shows the PAM session opening message (“pam_unix(sshd:session): session opened for user *administrador*”), which matches the Wazuh alert with **rule ID 5501**, describing the start of an SSH session. Later, at **17:31:38**, the log shows the session closing (“pam_unix(sshd:session): session closed for user *administrador*”) this is reflected in Wazuh by the **rule ID 5502** event that marks the termination of that session. Together, these correlated entries show the full SSH activity chain: a successful login, session initiation, and proper logout, all detected by Wazuh and tied back to the same timestamps and user actions recorded in /var/log/auth.log.



```
Oct 29 17:31:38 seminarioST sshd[58145]: Received disconnect from 10.10.10.4 port 39562:11:  
disconnected by user  
Oct 29 17:31:38 seminarioST sshd[58145]: Disconnected from user administrador 10.10.10.4 por  
t 39562  
Oct 29 17:31:38 seminarioST sshd[58107]: pam_unix(sshd:session): session closed for user adm  
inistrador  
Oct 29 17:31:38 seminarioST systemd-logind[525]: Session 14 logged out. Waiting for processe  
s to exit.  
Oct 29 17:31:38 seminarioST systemd-logind[525]: Removed session 14.  
Oct 29 17:32:37 seminarioST sudo: administrador : TTY=pts/0 ; PWD=/home/administrador ; USER  
=root ; COMMAND=/usr/bin/tail -n 30 /var/log/auth.log  
Oct 29 17:32:37 seminarioST sudo: pam_unix(sudo:session): session opened for user root(uid=0  
) by (uid=1000)  
Oct 29 17:32:37 seminarioST sudo: pam_unix(sudo:session): session closed for user root  
Oct 29 17:33:00 seminarioST sudo: administrador : TTY=pts/0 ; PWD=/home/administrador ; USER  
=root ; COMMAND=/usr/bin/tail -n 20 /var/log/auth.log  
Oct 29 17:33:00 seminarioST sudo: pam_unix(sudo:session): session opened for user root(uid=0  
) by (uid=1000)  
Oct 29 17:33:00 seminarioST sudo: pam_unix(sudo:session): session closed for user root  
Oct 29 17:33:13 seminarioST sudo: administrador : TTY=pts/0 ; PWD=/home/administrador ; USER  
=root ; COMMAND=/usr/bin/tail -n 15 /var/log/auth.log  
Oct 29 17:33:13 seminarioST sudo: pam_unix(sudo:session): session opened for user root(uid=0  
) by (uid=1000)  
Oct 29 17:33:13 seminarioST sudo: pam_unix(sudo:session): session closed for user root  
Oct 29 17:39:01 seminarioST CRON[58205]: pam_unix(cron:session): session opened for user roo  
t(uid=0) by (uid=0)  
Oct 29 17:39:01 seminarioST CRON[58205]: pam_unix(cron:session): session closed for user roo  
t  
Oct 29 17:41:56 seminarioST sudo: administrador : TTY=pts/0 ; PWD=/home/administrador ; USER  
=root ; COMMAND=/usr/bin/cat /var/ossec/etc/ossec.conf  
Oct 29 17:41:56 seminarioST sudo: pam_unix(sudo:session): session opened for user root(uid=0  
) by (uid=1000)  
Oct 29 17:41:56 seminarioST sudo: pam_unix(sudo:session): session closed for user root  
Oct 29 17:52:10 seminarioST sudo: administrador : TTY=pts/0 ; PWD=/home/administrador ; USER  
=root ; COMMAND=/usr/bin/cat /var/log/auth.log  
Oct 29 17:52:10 seminarioST sudo: pam_unix(sudo:session): session opened for user root(uid=0  
) by (uid=1000)  
administrador@seminarioST:~$ █
```



| Time | _source |
|-------------------------------|--|
| > Oct 29, 2025 @ 17:31:39.835 | predecoder.hostname: seminarioST predecoder.program_name: sshd predecoder.timestamp: Oct 29 17:31:38 input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.dstuser: administrador rule.firetimes: 26 rule.mail: false rule.level: 3 rule.pci_dss: 10.2.5 rule.hipaa: 164.312.b rule.tsc: CC6.8, CC7.2, CC7.3 rule.description: PAM: Login session closed. rule.groups: pam, syslog rule.id: 5502 rule.nist_800_53: AU.14, AC.7 rule.gpp13: 7.8, 7.9 rule.gdpr: IV_32.2 location: /var/log/auth.log decoder.parent: pam decoder.name: pam id: 1761755499.2369261 full_log: Oct 29 17:31:38 seminarioST sshd[58107]: pam_unix(sshd:session) session closed for user administrador timestamp: Oct 29, 2025 @ 17:31:39.835 _index: wazuh-alerts-4.x-2025.10.29 |
| > Oct 29, 2025 @ 17:26:09.561 | predecoder.hostname: seminarioST predecoder.program_name: sshd predecoder.timestamp: Oct 29 17:26:08 input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.uid: 0 data.dstuser: administrador(uid=1000) rule.mail: false rule.level: 3 rule.pci_dss: 10.2.5 rule.hipaa: 164.312.b rule.tsc: CC6.8, CC7.2, CC7.3 rule.description: PAM: Login session opened. rule.groups: pam, syslog, authentication_success rule.nist_800_53: AU.14, AC.7 rule.gdpr: IV_3 2.2 rule.firetimes: 23 rule.mitre.technique: Valid Accounts rule.mitre.id: T1078 rule.mitre.tactic: Defense Evasion, Persistence, Privilege Escalation, Initial Access rule.id: 5501 rule.gpp13: 7.8, 7.9 location: /var/log/auth.log decoder.parent: pam decoder.name: pam id: 1761755169.2364333 full_log: Oct 29 17:26:08 seminarioST sshd[58107]: pam_unix(sshd:session) session opened for user administrador timestamp: Oct 29, 2025 @ 17:26:09.561 _index: wazuh-alerts-4.x-2025.10.29 |
| > Oct 29, 2025 @ 17:26:09.509 | predecoder.hostname: seminarioST predecoder.program_name: sshd predecoder.timestamp: Oct 29 17:26:08 input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.scpip: 10.10.10.4 data.dstuser: administrador data.scpport: 39562 rule.mail: false rule.level: 3 rule.hipaa: 164.312.b rule.pci_dss: 10.2.5 rule.tsc: CC6.8, CC7.2, CC7.3 rule.description: sshd: authentication success. rule.groups: syslog, sshd, authentication.success rule.nist_800_53: AU.1 4, AC.7 rule.gdpr: IV_32.2 rule.firetimes: 2 rule.mitre.technique: Valid Accounts, Remote Services rule.mitre.id: T1078 rule.mitre.tactic: Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement rule.id: 5715 rule.gpp13: 7.1, 7.2 location: /var/log/auth.log decoder.parent: pam decoder.name: pam id: 1761755169.2364333 full_log: Oct 29 17:26:08 seminarioST sshd[58107]: pam_unix(sshd:session) session opened for user administrador timestamp: Oct 29, 2025 @ 17:26:09.509 _index: wazuh-alerts-4.x-2025.10.29 |
| > Oct 29, 2025 @ 17:14:38.931 | predecoder.hostname: seminarioST predecoder.program_name: sshd predecoder.timestamp: Oct 29 17:14:37 input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.dstuser: administrador rule.firetimes: 19 rule.mail: false rule.level: 3 rule.pci_dss: 10.2.5 rule.hipaa: 164.312.b rule.tsc: CC6.8, CC7.2, CC7.3 rule.description: PAM: Login session closed. rule.groups: pam, syslog rule.id: 5502 rule.nist_800_53: AU.14, AC.7 rule.gpp13: 7.8, 7.9 rule.gdpr: IV_32.2 location: /var/log/auth.log decoder.parent: pam decoder.name: pam id: 1761754478.2357196 full_log: Oct 29 17:14:38 seminarioST sshd[57953]: pam_unix(sshd:session) session closed for user administrador timestamp: Oct 29, 2025 @ 17:14:38.931 _index: wazuh-alerts-4.x-2025.10.29 |
| > Oct 29, 2025 @ 17:13:44.876 | predecoder.hostname: seminarioST predecoder.program_name: sshd predecoder.timestamp: Oct 29 17:13:43 input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.uid: 0 data.dstuser: administrador(uid=1000) rule.mail: false rule.level: 3 rule.pci_dss: 10.2.5 rule.hipaa: 164.312.b rule.tsc: CC6.8, CC7.2, CC7.3 rule.description: PAM: Login session opened. rule.groups: pam, syslog, authentication_success rule.nist_800_53: AU.14, AC.7 rule.gdpr: IV_3 2.2 rule.firetimes: 19 rule.mitre.technique: Valid Accounts rule.mitre.id: T1078 rule.mitre.tactic: Defense Evasion, Persistence, Privilege Escalation, Initial Access rule.id: 5501 rule.gpp13: 7.8, 7.9 location: /var/log/auth.log decoder.parent: pam decoder.name: pam id: 1761754424.2356728 full_log: Oct 29 17:13:43 seminarioST sshd[57953]: pam_unix(sshd:session) session opened for user administrador timestamp: Oct 29, 2025 @ 17:13:44.876 _index: wazuh-alerts-4.x-2025.10.29 |
| > Oct 29, 2025 @ 17:13:44.831 | predecoder.hostname: seminarioST predecoder.program_name: sshd predecoder.timestamp: Oct 29 17:13:43 input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 |

- c) Analyze whether the dashboard displays additional information that was not present in the original logs. Investigate how Wazuh is able to provide enriched data and document your findings.

When I compare the raw Linux logs to what Wazuh shows in its alerts, Wazuh is clearly adding extra context that the original logs don't have. For example, /var/log/auth.log just says things like "Accepted password for administrador from 10.10.10.4" or "sudo: administrador : USER=root ; COMMAND=/usr/bin/hostname," but in alerts.json that same activity is turned into security event that includes a rule ID, a severity level, tags like "Privilege Escalation," the exact MITRE ATT&CK technique (for example T1548.003 for sudo abuse, T1078 for valid accounts over SSH), compliance mappings (PCI, HIPAA, etc.), and clean parsed fields like srcip, dstuser, and the exact command the user ran. So the dashboard/alerts aren't just reprinting logs, they're basically telling who did what, from where, with which command, and why that might matter from a security/compliance point of view.

- d) Identify three different decoders used and the rule sets involved:
- Decoders used: Identify the decoders applied to the logs to normalize the information.
 - Rule sets involved: Indicate the rules that were triggered and their severity level.

From the alerts pulled, we can clearly see multiple decoders, and which rules they triggered along with their severities. The sshd decoder handled SSH login lines like "Accepted password for administrador...", and that triggered rule 5715 ("sshd: authentication success.") with severity level 3, which Wazuh tags to MITRE techniques like Valid Accounts and Remote Services. The sudo decoder parsed sudo activity such as USER=root ; COMMAND=/usr/bin/hostname, and that fired rule 5402 ("Successful sudo to ROOT executed."), also level 3, which Wazuh classifies as privilege escalation (MITRE T1548.003). The pam decoder processed session events like pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000) and triggered rules 5501 ("PAM: Login session opened.") and 5502 ("PAM: Login session closed."), again level 3, used to track session start/stop for both SSH and sudo. We also saw the dpkg-decoder, which parsed /var/log/dpkg.log entries about packages being installed or half-configured and raised rules 2902 ("New dpkg installed") and 2904



("Dpkg half configured") with severity level 7, marking those as configuration changes. So in short: sshd -> rule 5715 (level 3), sudo -> rule 5402 (level 3), pam -> rules 5501/5502 (level 3), and dpkg-decoder -> rules 2902/2904 (level 7).

5. Suricata installation

Show a screenshot (or some) where it can be seen the Suricata folders and configuration file (/etc/suricata/suricata.yaml) contents.

```
administrador@seminarioST:~$ sudo suricata --build-info
sudo: password for administrador:
This is Suricata version 8.0.1 RELEASE
Features: NFQ PCAP SET_BUFF AF_PACKET HAVE_PACKET_FANOUT LIBCAP_NG LIBNET1.1 HAVE_HTP_URI_NO
RMALIZE_HOOK PCRE_JIT HAVE_NSS HTTP2_DECOMPRESSION HAVE_LUA HAVE_JA3 HAVE_JA4 HAVE_LIBJANSSO
TLS TLS_C11 MAGIC RUST POPCNT64
SIMD support: SSE_2
Atomic intrinsics: 1 2 4 8 byte(s)
64-bits, little-endian architecture
GCC version 11.4.0, C version 201112
compiled with _FORTIFY_SOURCE=2
1 cache line size (CLS)=64
thread local storage method: _Thread_local
compiled with LibHTTP v8.0.1

Suricata Configuration:
  AF_PACKET support: yes
  AF_XDP support: no
  DPDK support: no
  ebPF support: no
  XDP support: no
  PF_RING support: no
  NFQueue support: yes
  NFLOG support: no
  IPFW support: no
  Netmap support: no
  DAG enabled: no
  Npatchet enabled: no
  WinDivert enabled: no
  Npcap support: no

  Unix socket enabled: yes
  Detection enabled: yes

  Libmagic support: yes
  libjansson support: yes
  hiredis support: yes
  hiredis async with libevent: yes
```

```
ls: cannot open directory '/var/log/suricata': Permission denied
administrador@seminarioST:~$ sudo ls -R /var/log/suricata
/var/log/suricata:
certs core eve.json fast.log files stats.log suricata.log

/var/log/suricata/certs:
/var/log/suricata/core:
/var/log/suricata/files:
administrador@seminarioST:~$ sudo ls -R /etc/suricata
/etc/suricata:
classification.config local.rules reference.config rules sid-msg.map suricata.yaml suricata.yaml.broken.1761034437 suricata.yaml.broken.1761034535 threshold.config

/etc/suricata/rules:
botcc.portgrouped.rules      emerging-chat.rules      emerging-games.rules      emerging-misc.rules      emerging-scada.rules      emerging-voip.rules
botcc.rules                  emerging-coincminer.rules      emerging-hunting.rules      emerging-mobile_malware.rules      emerging-scan.rules      emerging-web_client.rules
clarmy.rules                 emerging-current_events.rules      emerging-icmp_info.rules      emerging-netbios.rules      emerging-shellcode.rules      emerging-web_server.rules
compromised.rules            emerging-deleted.rules      emerging-icmp.rules      emerging-p2p.rules      emerging-sntp.rules      emerging-web_specific_apps.rules
drop.rules                   emerging-dns.rules      emerging-imap.rules      emerging-phishing.rules      emerging-snmp.rules      emerging-worm.rules
dshield.rules                emerging-dos.rules      emerging-exploit_kit.rules      emerging-inappropriate.rules      emerging-policy.rules      suricata.rules
emerging-activex.rules       emerging-exploit.rules      emerging-info.rules      emerging-pop3.rules      emerging-telnet.rules      threatview_CS_C2.rules
emerging-adware_pup.rules    emerging-exploit.rules      emerging-ja3.rules      emerging-retired.rules      emerging-tftp.rules      tor.rules
emerging-attack_response.rules      emerging-ftp.rules      emerging-malware.rules      emerging-rpc.rules      emerging-user_agents.rules
```



```
%YAML 1.1
---
# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml.html

# This configuration file was generated by Suricata 8.0.1.
suricata-version: "8.0"

## Step 1: Inform Suricata about your network
##

vars:
    # more specific is better for alert accuracy and performance
    address-groups:
        HOME_NET: "10.10.10.2"
        #HOME_NET: "[192.168.0.0/16]"
        #HOME_NET: "[10.0.0.0/8]"
        #HOME_NET: "[172.16.0.0/12]"
        #HOME_NET: "any"

        EXTERNAL_NET: "!$HOME_NET"
        #EXTERNAL_NET: "any"

    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"
    SQL_SERVERS: "$HOME_NET"
    DNS_SERVERS: "$HOME_NET"
    TELNET_SERVERS: "$HOME_NET"
    AIM_SERVERS: "$EXTERNAL_NET"
    DC_SERVERS: "$HOME_NET"
    DNP3_SERVER: "$HOME_NET"
    DNP3_CLIENT: "$HOME_NET"
    MODBUS_CLIENT: "$HOME_NET"
    MODBUS_SERVER: "$HOME_NET"
    ENIP_CLIENT: "$HOME_NET"
```

6. Suricata events

Generate some events and show a screenshot (or some) where it can be seen the contents of Suricata events json file.

The screenshot shows two Oracle VirtualBox windows. The left window is titled 'CPTattacker [Running] - Oracle VirtualBox' and contains a terminal session for 'administrador@seminarioST:~'. It runs an nmap scan on port 22 of the host (10.10.10.2) and prints the results. The right window is titled 'CPlinuhost [Running] - Oracle VirtualBox' and also has a terminal session for 'administrador@seminarioST:~'. It shows a detailed analysis of network traffic, specifically focusing on a connection between port 22 and port 10.10.10.2, with various flags and states visible.

```
File Actions Edit View Help
administrador@seminarioST:~ x
File Actions Edit View Help
administrador@seminarioST:~ x

administrador@seminarioST:~$ sudo nmap -sS -Pn -p 22,80,443 10.10.10.2
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-29 18:29 CET
Nmap scan report for 10.10.10.2 (10.10.10.2)
Host is up (0.00086s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    closed http
443/tcp   closed https
MAC Address: 08:00:27:8C:9E:72 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
administrador@seminarioST:~ |
```

```
File Actions Edit View Help
administrador@seminarioST:~ x
File Actions Edit View Help
administrador@seminarioST:~ x

;internal=0,"slp_udp":{ "alloc":0,"parser":0,"internal":0}, "ldap_udp":{ "alloc":0,"parser":0,"internal":0}, "tx":{ "http":0,"ftp":0,"smtp":0,"tel":0,"ssh":0,"imap":0,"smb":0,"dcerpc":0,"dns_tcp":0,"dns_tcp_0":0,"ntp":0,"pop3":0,"telnet":0,"krb5_tcp":0,"quit":0,"dhcp":0,"sip_tcp":0,"http":0,"http_0":0,"microsoft_websocket":0,"ldap_top":0,"doh2":0,"rdp":0,"http2":0,"bittorrent_dht":0,"pop3":0,"mdns":34,"snmp":0,"dcerpc_w":0,"dns_udp":0,"nfss_udp":0,"krb5_udp":0,"slp_udp":0,"ldap_udp":0}, "expectations":0}, "memcap":{ "pressure":5,"pressure_max":5}, "http":{ "Memuse":0,"mencap":1677216}, "host":{ "Memuse":382144,"mencap":33554432}, "file_store":{ "open_files":0}}
{ "timestamp": "2025-10-29T18:29:36.774850000", "flow_id": "852458600562283", "in_iface": "enp0s2", "event_type": "flow", "src_ip": "10.10.10.2", "dest_ip": "10.10.10.2", "start_port": 22, "tp_v": 4, "proto": "TCP", "flow": { "pkts": { "toserver": 2, "pkts_toclient": 0, "bytes_toserver": 12, "bytes_toclient": 58, "start": "2025-10-29T18:28:35.264016000", "end": "2025-10-29T18:28:35.564556000", "age": 0, "state": "closed", "reason": "timeout"}, "alerted": 0, "tcp_flags": "16", "tcp_flags_tc": "12", "syn": true, "rst": true, "ack": true, "state": "closed", "ts_max_regions": 1, "tc_max_regions": 1}}, "flow": { "pkts": { "toserver": 2, "pkts_toclient": 0, "bytes_toserver": 12, "bytes_toclient": 58, "start": "2025-10-29T18:29:41.671210000", "end": "2025-10-29T18:29:41.671210000", "age": 0, "state": "closed", "reason": "timeout"}, "alerted": 0, "tcp_flags": "16", "tcp_flags_tc": "12", "syn": true, "rst": true, "ack": true, "state": "closed", "ts_max_regions": 1, "tc_max_regions": 1}}
```

7. Suricata rule for “HTTP Attack Detected”

Show with screenshots the created rule. Access the protected file and show the event detection in Suricata (json file), and in Wazuh (generated event).



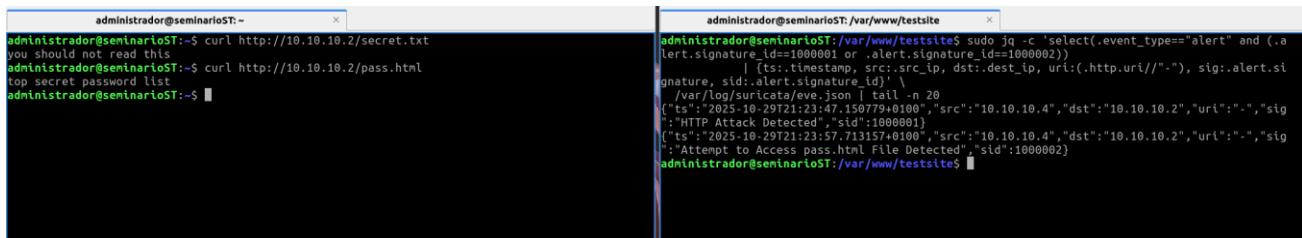
```
default-rule-path: /var/lib/suricata/rules

rule-files:
  - suricata.rules
  - /etc/suricata/rules/local.rules
##
## Auxiliary configuration files.
##
```

```
[root@2025-10-29T21:23:47.150779+0100] suricata[1]: Starting Suricata 1.0.3, NSM, FW detection.
administrador@seminarioST:/var/www/testsite$ sudo cat /etc/suricata/rules/local.rules
alert http any any -> $HOME_NET any (msg:"HTTP Attack Detected"; http.method; content:"GET";
  nocase; http.uri; content:"/secret.txt"; nocase; sid:1000001; rev:1;)
alert http any any -> $HOME_NET any (msg:"Attempt to Access pass.html File Detected"; http.m
ethod; content:"GET"; nocase; http.uri; content:"/pass.html"; nocase; sid:1000002; rev:1;)
administrador@seminarioST:/var/www/testsite$
```

8. Suricata rule for “Attempt to Access pass.html File Detected”

Show with screenshots the created rule. Access the protected file and show the event detection in Suricata (json file), and in Wazuh (generated event).

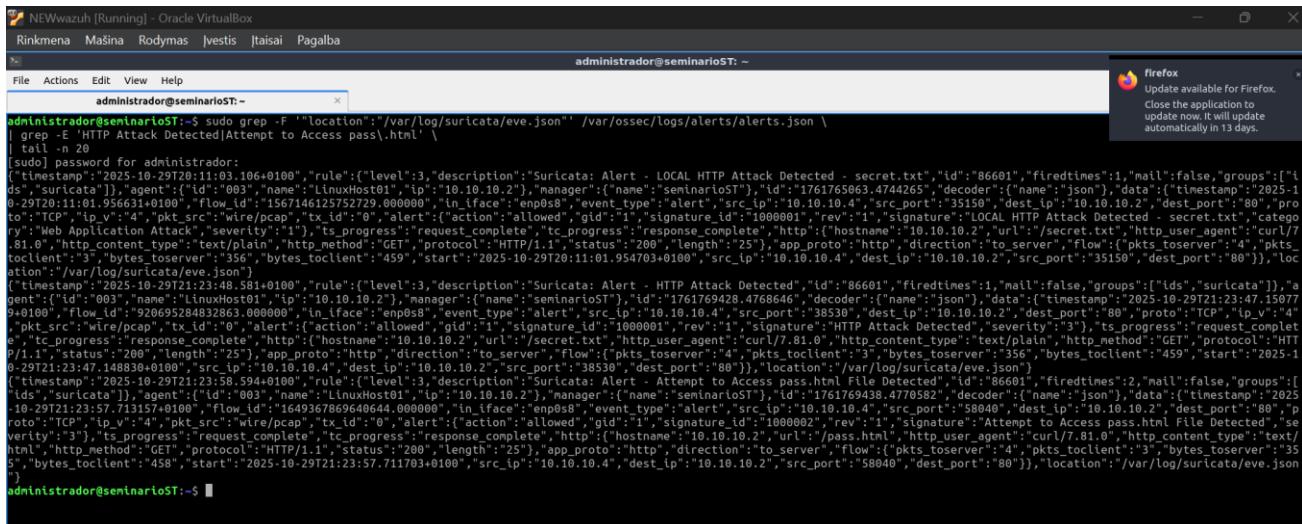


```
administrador@seminarioST:~
```

```
administrador@seminarioST:~$ curl http://10.10.10.2/secret.txt
you should not read this
administrador@seminarioST:~$ curl http://10.10.10.2/pass.html
top secret password list
administrador@seminarioST:~$
```

```
administrador@seminarioST:/var/www/testsite
```

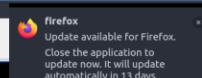
```
administrador@seminarioST:/var/www/testsite$ sudo jq -c 'select(.event_type=="alert" and (.a
lert.signature_id==1000001 or .alert.signature_id==1000002))'
| [ts:timestamp, src:.src_ip, dst:.dest_ip, uri:(http.uri//"/"), sig:.alert.si
gnature, sid:.alert.signature_id]' \
| /var/log/suricata/eve.json | tail -n 20
["ts":"2025-10-29T21:23:47.150779+0100","src":"10.10.10.4","dst":"10.10.10.2","uri":","sig
":"HTTP Attack Detected","sid":1000001}
["ts":"2025-10-29T21:23:57.713157+0100","src":"10.10.10.4","dst":"10.10.10.2","uri":","sig
":"Attempt to Access pass.html File Detected","sid":1000002}
administrador@seminarioST:/var/www/testsite$
```



```
NEWwazuh [Running] - Oracle VirtualBox
Rinkmena Mašina Rodymas Jvestis Jtaisai Pagalba
administrador@seminarioST:~
```

```
administrador@seminarioST:~$ sudo grep -F "location: '/var/log/suricata/eve.json'" /var/ossec/logs/alerts/alerts.json \
| grep -E 'HTTP Attack Detected|Attempt to Access pass.html' \
| tail -n 20
[sudo] password for administrador:
[{"timestamp": "2025-10-29T20:11:03.106+0100", "rule": {"level": 3, "description": "Suricata: Alert - LOCAL HTTP Attack Detected - secret.txt", "id": "86601", "firetimes": 1, "mail": false, "groups": [{"ids": "suricata"}], "agent": {"id": "003", "name": "LinuxHost01", "ip": "10.10.10.2"}, "manager": {"name": "seminarioST", "id": "1761765063.4744265", "decoder": {"name": "json"}, "data": {"timestamp": "2025-10-29T20:11:03.106+0100", "flow_id": "15671461257229.000000", "in_iface": "enp0s8", "event_type": "alert", "src_ip": "10.10.10.4", "src_port": "35150", "dest_ip": "10.10.10.2", "dest_port": "80", "proto": "TCP", "ip_v": "4", "pkt_src": "wire/pcap", "tx_id": "0", "alert": {"action": "allowed", "gid": "1", "signature_id": "1000001", "rev": "1", "signature": "LOCAL HTTP Attack Detected - secret.txt", "category": "Web Application Attack", "severity": "1"}, "ts_progress": "request_complete", "tc_progress": "response_complete", "http": {"hostname": "10.10.10.2", "url": "/secret.txt", "http_user_agent": "curl/7.81.0", "http_content_type": "text/plain", "http_method": "GET", "protocol": "HTTP/1.1", "status": "200", "length": "25"}, "app_proto": "http", "direction": "to_server", "flow": {"pkts_toserver": "4", "pkts_toclient": "3", "bytes_toserver": "356", "bytes_toclient": "459", "start": "2025-10-29T20:11:03.106+0100", "src_ip": "10.10.10.4", "dest_ip": "10.10.10.2", "src_port": "35150", "dest_port": "80"}}, "location": "/var/log/suricata/eve.json"}], "firetimes": 1, "mail": false, "groups": [{"ids": "suricata"}], "agent": {"id": "003", "name": "LinuxHost01", "ip": "10.10.10.2"}, "manager": {"name": "seminarioST", "id": "1761769428.4768646", "decoder": {"name": "json"}, "data": {"timestamp": "2025-10-29T21:23:47.150779+0100", "flow_id": "92695284832863.000000", "in_iface": "enp0s8", "event_type": "alert", "src_ip": "10.10.10.4", "src_port": "38530", "dest_ip": "10.10.10.2", "dest_port": "80", "proto": "TCP", "ip_v": "4", "pkt_src": "wire/pcap", "tx_id": "0", "alert": {"action": "allowed", "gid": "1", "signature_id": "1000001", "rev": "1", "signature": "HTTP Attack Detected", "severity": "3"}, "ts_progress": "request_complet
e", "tc_progress": "response_complete", "http": {"hostname": "10.10.10.2", "url": "/secret.txt", "http_user_agent": "curl/7.81.0", "http_content_type": "text/plain", "http_method": "GET", "protocol": "HTTP/1.1", "status": "200", "length": "25"}, "app_proto": "http", "direction": "to_server", "flow": {"pkts_toserver": "4", "pkts_toclient": "3", "bytes_toserver": "356", "bytes_toclient": "459", "start": "2025-10-29T21:23:47.148830+0100", "src_ip": "10.10.10.4", "dest_ip": "10.10.10.2", "src_port": "35150", "dest_port": "80"}}, "location": "/var/log/suricata/eve.json"}], "firetimes": 2, "mail": false, "groups": [{"ids": "suricata"}], "agent": {"id": "003", "name": "LinuxHost01", "ip": "10.10.10.2"}, "manager": {"name": "seminarioST", "id": "1761769438.4770582", "decoder": {"name": "json"}, "data": {"timestamp": "2025-10-29T21:23:58.594+0100", "flow_id": "1649367869640644.000000", "in_iface": "enp0s8", "event_type": "alert", "src_ip": "10.10.10.4", "src_port": "58040", "dest_ip": "10.10.10.2", "dest_port": "80", "proto": "TCP", "ip_v": "4", "pkt_src": "wire/pcap", "tx_id": "0", "alert": {"action": "allowed", "gid": "1", "signature_id": "1000002", "rev": "1", "signature": "Attempt to Access pass.html File Detected", "severity": "3"}, "ts_progress": "request_complet
e", "tc_progress": "response_complete", "http": {"hostname": "10.10.10.2", "url": "/pass.html", "http_user_agent": "curl/7.81.0", "http_content_type": "text/html", "http_method": "GET", "protocol": "HTTP/1.1", "status": "200", "length": "25"}, "app_proto": "http", "direction": "to_server", "flow": {"pkts_toserver": "4", "pkts_toclient": "3", "bytes_toserver": "458", "bytes_toclient": "458", "start": "2025-10-29T21:23:57.713157+0100", "src_ip": "10.10.10.4", "dest_ip": "10.10.10.2", "src_port": "58040", "dest_port": "80"}}, "location": "/var/log/suricata/eve.json"}]
```

```
administrador@seminarioST:~$
```





With KQL:

`location:"/var/log/suricata/eve.json"` AND `(data.alert.signature_id:1000001` OR `data.alert.signature_id:1000002)`

