Cyberprotection Systems

Laboratory Work 3. Response Automation

(Active Response Automation to Attacks)

NAME AND SURNAME:

Austėja Bauraitė

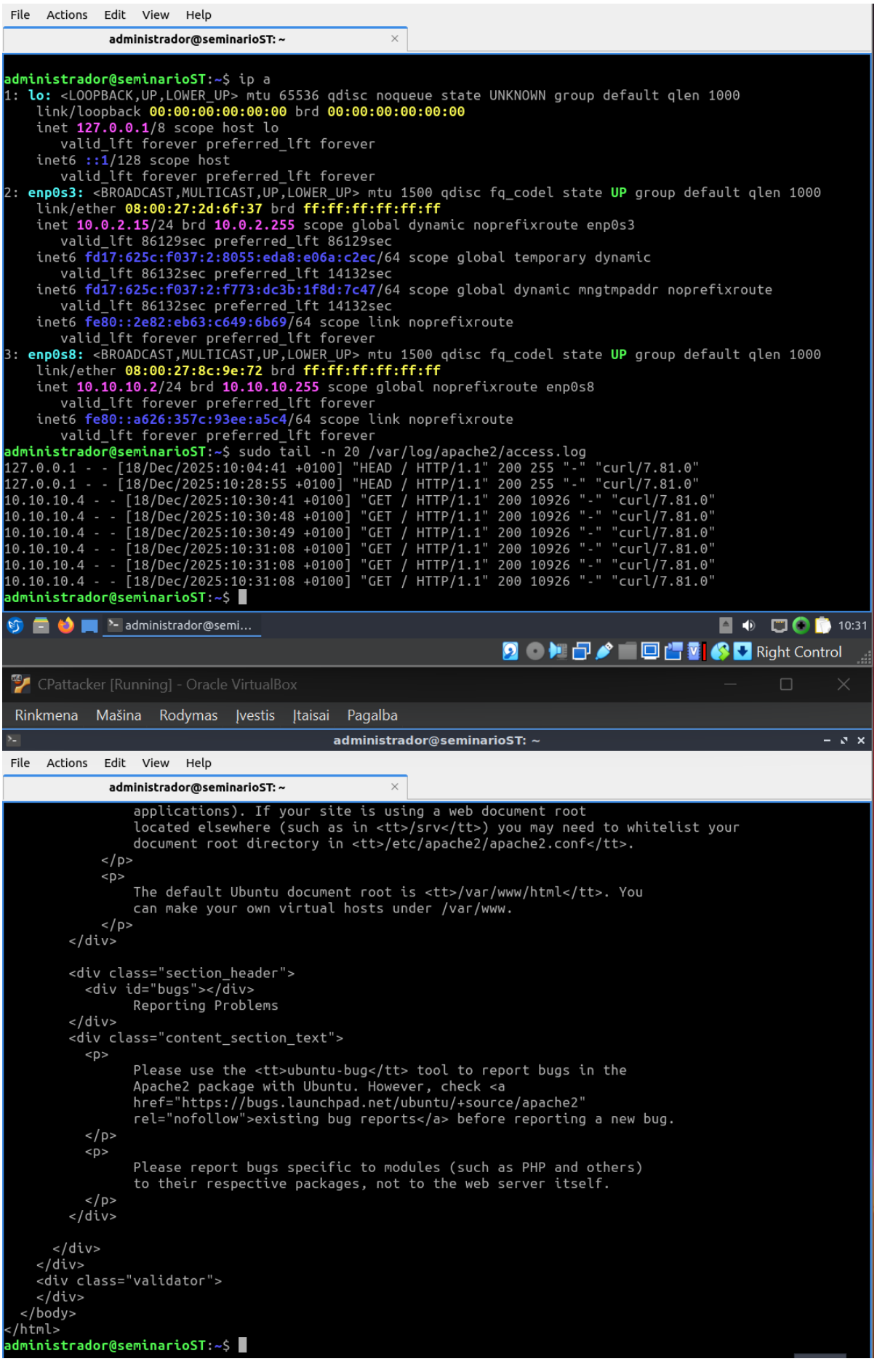
1. Apache installing

Put a screenshot from Linux machine showing Apache has been successfully installed.

```
Reading state information... Done
apache2 is already the newest version (2.4.52-1ubuntu4.16).
0 to upgrade, 0 to newly install, 0 to remove and 106 not to upgrade.
administrador@seminarioST:~$ apache2 -v
Server version: Apache/2.4.52 (Ubuntu)
Server built:   2025-08-11T12:10:10
administrador@seminarioST:~$ sudo systemctl status apache2 --no-pager
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2025-12-18 10:25:47 CET; 2min 59s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 581 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 682 (apache2)
      Tasks: 55 (limit: 2210)
     Memory: 7.7M
        CPU: 35ms
     CGroup: /system.slice/apache2.service
             ├─682 /usr/sbin/apache2 -k start
             ├─690 /usr/sbin/apache2 -k start
             └─691 /usr/sbin/apache2 -k start

Dec 18 10:25:46 seminarioST systemd[1]: Starting The Apache HTTP Server...
Dec 18 10:25:47 seminarioST apachectl[645]: AH00558: apache2: Could not reliably determine the se…essage
Dec 18 10:25:47 seminarioST systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
administrador@seminarioST:~$ curl -I http://127.0.0.1
HTTP/1.1 200 OK
Date: Thu, 18 Dec 2025 09:28:55 GMT
Server: Apache/2.4.52 (Ubuntu)
Last-Modified: Wed, 29 Oct 2025 17:55:18 GMT
ETag: "29af-6424fd5e23346"
Accept-Ranges: bytes
Content-Length: 10671
Vary: Accept-Encoding
```

2. Apache log

Show an example part of the log file produced by Apache after some webpages have been accessed.


File Actions Edit View Help
administrador@seminarioST: ~
administrador@seminarioST:~$ ip a
1: 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 86129sec preferred_lft 86129sec
inet6 fd17:625c:f037:2:8055:eda8:e06a:c2ec/64 scope global temporary dynamic
valid_lft 86132sec preferred_lft 14132sec
inet6 fd17:625c:f037:2:f773:dc3b:1f8d:7c47/64 scope global dynamic mngtmpaddr noprefixroute
valid_lft 86132sec preferred_lft 14132sec
inet6 fe80::2e82:eb63:c649:6b69/64 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::a626:357c:93ee:a5c4/64 scope link noprefixroute
valid_lft forever preferred_lft forever
administrador@seminarioST:~$ sudo tail -n 20 /var/log/apache2/access.log
127.0.0.1 - - [18/Dec/2025:10:04:41 +0100] "HEAD / HTTP/1.1" 200 255 "-" "curl/7.81.0"
127.0.0.1 - - [18/Dec/2025:10:28:55 +0100] "HEAD / HTTP/1.1" 200 255 "-" "curl/7.81.0"
10.10.10.4 - - [18/Dec/2025:10:30:41 +0100] "GET / HTTP/1.1" 200 10926 "-" "curl/7.81.0"
10.10.10.4 - - [18/Dec/2025:10:30:48 +0100] "GET / HTTP/1.1" 200 10926 "-" "curl/7.81.0"
10.10.10.4 - - [18/Dec/2025:10:30:49 +0100] "GET / HTTP/1.1" 200 10926 "-" "curl/7.81.0"
10.10.10.4 - - [18/Dec/2025:10:31:08 +0100] "GET / HTTP/1.1" 200 10926 "-" "curl/7.81.0"
10.10.10.4 - - [18/Dec/2025:10:31:08 +0100] "GET / HTTP/1.1" 200 10926 "-" "curl/7.81.0"
10.10.10.4 - - [18/Dec/2025:10:31:08 +0100] "GET / HTTP/1.1" 200 10926 "-" "curl/7.81.0"
administrador@seminarioST:~$
administrador@semi...
10:31
Right Control
CPattacker [Running] - Oracle VirtualBox
Rinkmena Mašina Rodymas Įvestis Įtaisai Pagalba
administrador@seminarioST: ~
File Actions Edit View Help
administrador@seminarioST: ~
applications). If your site is using a web document root
located elsewhere (such as in <tt>/srv</tt>) you may need to whitelist your
document root directory in <tt>/etc/apache2/apache2.conf</tt>.

The default Ubuntu document root is <tt>/var/www/html</tt>. You
can make your own virtual hosts under /var/www.

Reporting Problems

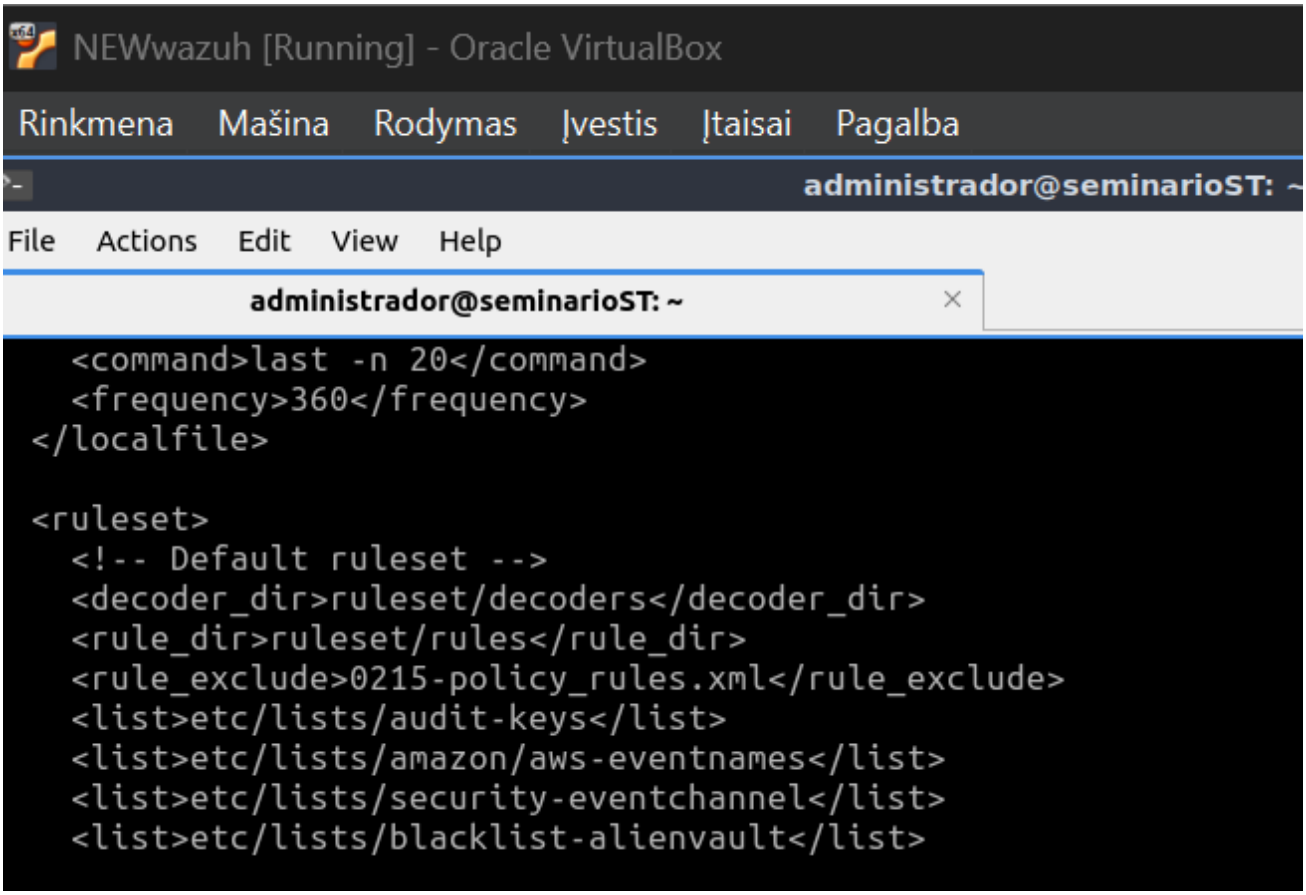
Please use the <tt>ubuntu-bug</tt> tool to report bugs in the
Apache2 package with Ubuntu. However, check <a
href="https://bugs.launchpad.net/ubuntu/+source/apache2"
rel="nofollow">existing bug reports before reporting a new bug.

Please report bugs specific to modules (such as PHP and others)
to their respective packages, not to the web server itself.

</body>
</html>
administrador@seminarioST:~$

3. Wazuh rules

Show the rule files defined in Wazuh.

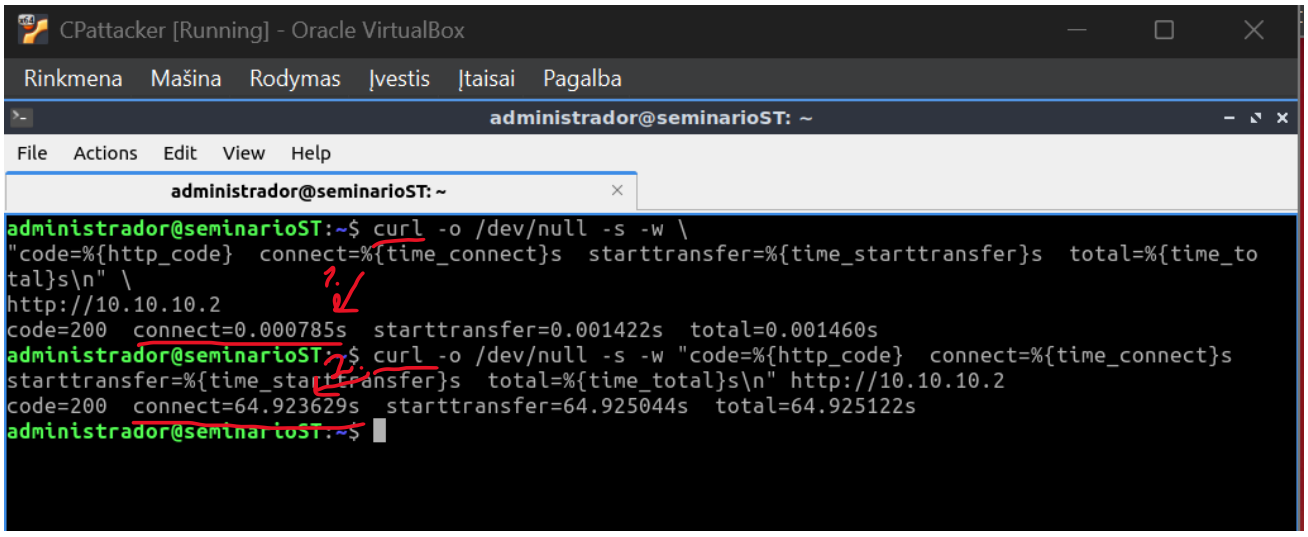


```
administrador@seminarioST:~$ sudo cat /var/ossec/etc/rules/local_rules.xml
<!-- Local rules -->

<!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->

<!-- Example -->
<group name="local,syslog,sshd,">

  <!--
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

</group>

<group name="attack,">
  <rule id="100100" level="10">
    <if_group>web|attack|attacks</if_group>
    <list field="srcip" lookup="address_match_key">etc/lists/blacklist-alienvault</list>
    <description>IP address found in AlienVault reputation database.</description>
  </rule>
</group>
administrador@seminarioST:~$
```

```
 GNU nano 6.2                                  /var/ossec/etc/ossec.conf
  </command>

  <active-response>
    <command>firewall-drop</command>
    <location>local</location>
    <rules_id>100100</rules_id>
    <timeout>60</timeout>
  </active-response>
```

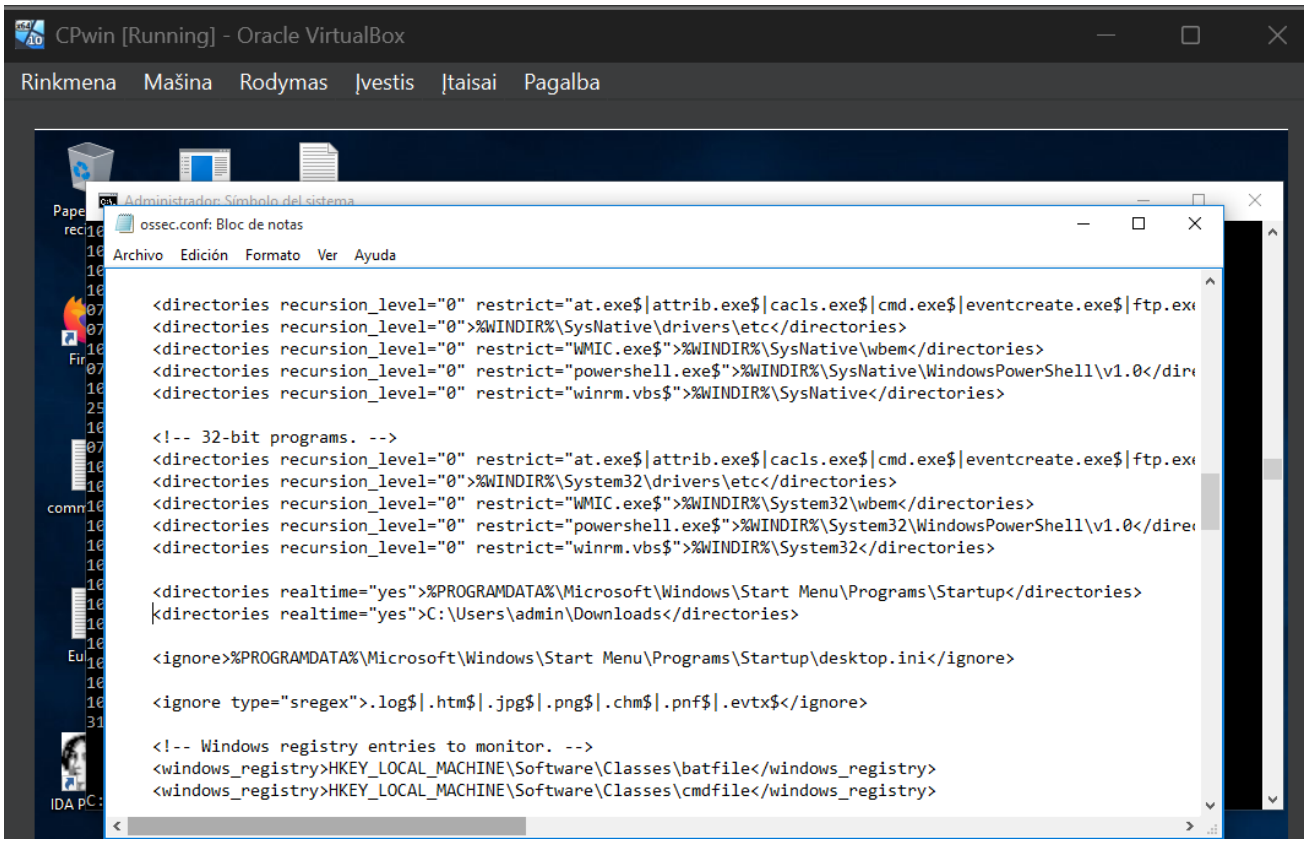
4. Web attack detection and response

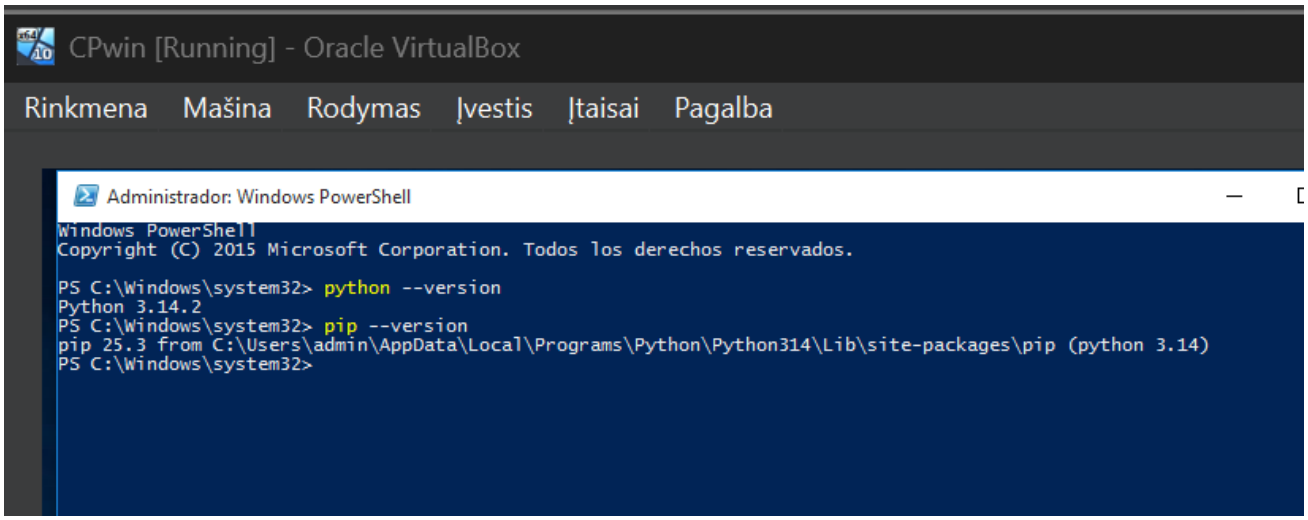
Show in a set of screenshots the “attack” from the attacker machine and the detection and related action in Wazuh.

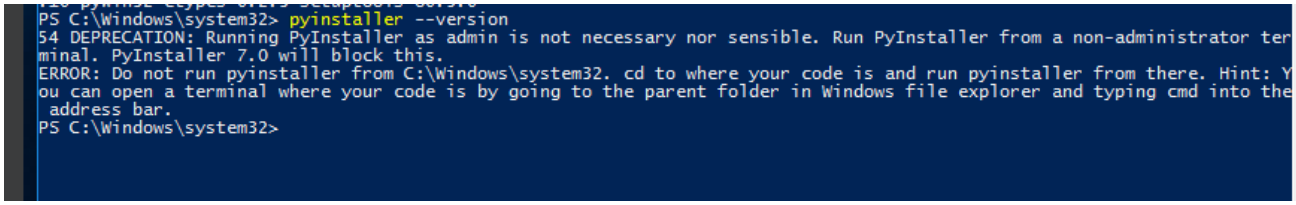


5. Configuration of Malware detection through Virustotal on the agent

a) Show a couple of screenshots with the configuration files and python installation on the machine to be monitored.


CPwin [Running] - Oracle VirtualBox
Rinkmena Mašina Rodymas Įvestis Įtaisai Pagalba
ossec.conf: Bloc de notas
Archivo Edición Formato Ver Ayuda
<directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe
<directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
<directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\SysNative\wbem</directories>
<directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\SysNative\WindowsPowerShell\v1.0</dire
<directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\SysNative</directories>
<!-- 32-bit programs. -->
<directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe
<directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
<directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\System32\wbem</directories>
<directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\System32\WindowsPowerShell\v1.0</dire
<directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\System32</directories>
<directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>
<directories realtime="yes">C:\Users\admin\Downloads</directories>
<ignore>%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini</ignore>
<ignore type="sregex">.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.evtx$</ignore>
<!-- Windows registry entries to monitor. -->
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\batfile</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\cmdfile</windows_registry>


CPwin [Running] - Oracle VirtualBox
Rinkmena Mašina Rodymas Įvestis Įtaisai Pagalba
Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Todos los derechos reservados.
PS C:\Windows\system32> python --version
Python 3.14.2
PS C:\Windows\system32> pip --version
pip 25.3 from C:\Users\admin\AppData\Local\Programs\Python\Python314\Lib\site-packages\pip (python 3.14)
PS C:\Windows\system32>


PS C:\Windows\system32> pyinstaller --version
54 DEPRECATION: Running PyInstaller as admin is not necessary nor sensible. Run PyInstaller from a non-administrator ter
minal. PyInstaller 7.0 will block this.
ERROR: Do not run pyinstaller from C:\Windows\system32. cd to where your code is and run pyinstaller from there. Hint: Y
ou can open a terminal where your code is by going to the parent folder in Windows file explorer and typing cmd into the
address bar.
PS C:\Windows\system32>

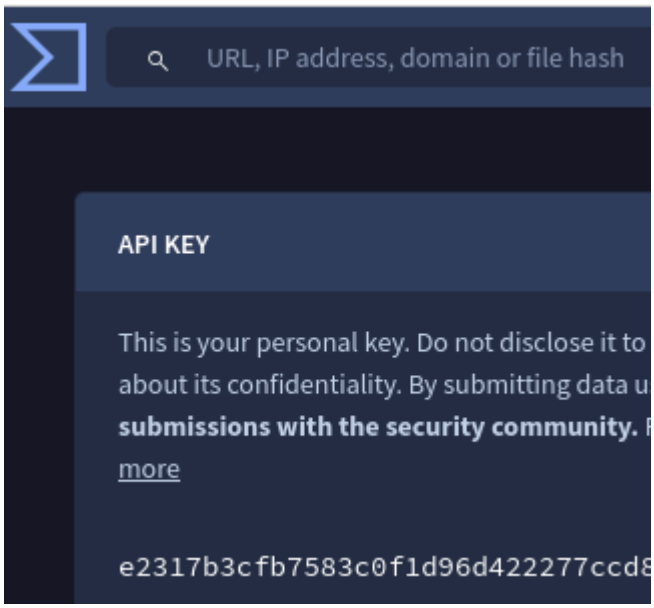
b) Show the placement of the executable file generated (`remove_threat.py`).

```
11967 INFO: Building EXE from EXE-00.toc completed successfully.
11970 INFO: Build complete! The results are available in: C:\Users\admin\Downloads\dist
PS C:\Users\admin\Downloads> ls


    Directorio: C:\Users\admin\Downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        19/12/2025     16:10                build
d-----        19/12/2025     16:10                dist
d-----        29/10/2025     15:39                sysmon-config-master
-a----        20/01/2018     18:40         311224 Firefox Installer.exe
-a----        20/01/2018     18:48       16374114 idafree50(1).exe
-a----        20/01/2018     18:43       16374114 idafree50.exe
-a----        18/12/2025     12:19              0 Nuevo documento de texto.txt
-a----        11/11/2025      8:49      113143808 PowerShell-7.5.4-win-x64.msi
-a----        18/12/2025     12:36       29882512 python-3.14.2-amd64.exe
-a----        19/12/2025     16:03           3800 remove-threat.py
-a----        19/12/2025     16:10            712 remove-threat.spec
-a----        29/10/2025     15:39          29422 sysmon-config-master.zip
-a----        16/10/2025     12:12        5423104 wazuh-agent-4.13.1-1.msi


PS C:\Users\admin\Downloads> cd .\dist\
PS C:\Users\admin\Downloads\dist> ls


    Directorio: C:\Users\admin\Downloads\dist


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        19/12/2025     16:10        8387081 remove-threat.exe
```

```
PS C:\Users\admin\Downloads\dist> Copy-Item remove-threat.exe "C:\Program Files (x86)\ossec-agent\active-response\bin\r
move-threat.exe"
PS C:\Users\admin\Downloads\dist> cd "C:\Program Files (x86)\ossec-agent\active-response\bin"
PS C:\Program Files (x86)\ossec-agent\active-response\bin> Restart-Service WazuhSvc
PS C:\Program Files (x86)\ossec-agent\active-response\bin> ls


    Directorio: C:\Program Files (x86)\ossec-agent\active-response\bin


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        28/10/2024     14:47         193136 netsh.exe
-a----        19/12/2025     16:10        8387081 remove-threat.exe
-a----        28/10/2024     14:47         186992 restart-wazuh.exe
-a----        28/10/2024     14:47         189552 route-null.exe
```

6. Configuration of Malware detection on the Wazuh server

a) Show the configuration file on the server with your API Key of VirusTotal.




```
<integration>
  <name>virustotal</name>
  <api_key>e2317b3cfb7583c0f1d96d4222
  <group>syscheck</group>
  <alert_format>json</alert_format>
</integration>
```

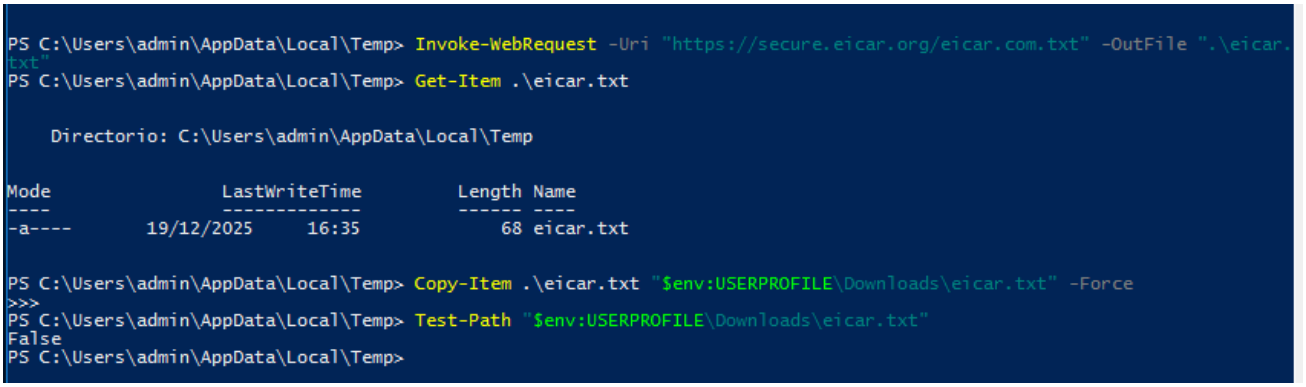
b) Show the active response configuration on Wazuh.

```
  <command>
    <name>remove-threat</name>
    <executable>remove-threat.exe</executable>
    <timeout_allowed>no</timeout_allowed>
  </command>

  <active-response>
    <disabled>no</disabled>
    <command>remove-threat</command>
    <location>local</location>
    <rules_id>87105</rules_id>
  </active-response>


  <alerts>
    <log_alert_level>3</log_alert_level>
                                  [ Wrote 353 lines ]
^G Help        ^O Write Out  ^W Where Is  ^K Cut         ^T Execute     ^C
```

```
  GNU nano 6.2                        /var/ossec/etc/rules/local_rules.xml *
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

</group>

<group name="attack,">
  <rule id="100100" level="10">
    <if_group>web|attack|attacks</if_group>
    <list field="srcip" lookup="address_match_key">etc/lists/blacklist-alienvault</list>
    <description>IP address found in AlienVault reputation database.</description>
  </rule>
</group>


<group name="virustotal,">
  <rule id="100092" level="12">
    <if_sid>657</if_sid>
    <match>Successfully removed threat</match>
    <description>$(parameters.program) removed threat located at $(parameters.alert.data.virustotal.sou
  </rule>

  <rule id="100093" level="12">
    <if_sid>657</if_sid>
    <match>Error removing threat</match>
    <description>Error removing threat located at $(parameters.alert.data.virustotal.source.file)</desc
  </rule>
</group>
```

7. Malware attack detection and response

Show in a set of screenshots the “attack” from the attacker machine (downloading the file) and the detection and related action in Wazuh.



manager.name: seminarioST × rule.level: 12 to 14 × + Add filter

4 hits

Dec 18, 2025 @ 16:42:25.251 - Dec 19, 2025 @ 16:42:25.251 per Auto

Time	_source
Dec 19, 2025 @ 16:37:11.060	input.type: log agent.ip: 10.10.10.3 agent.name: DESKTOP-O7BM7AU agent.id: 005 manager.name: seminarioST data.origin.module: wazuh-execd data.origin.name: node01 data.version: 1 data.parameters.alert.agent.ip: 10.10.10.3 data.parameters.alert.agent.name: DESKTOP-O7BM7AU data.parameters.alert.agent.id: 005 data.parameters.alert.manager.name: seminari
Dec 19, 2025 @ 16:37:09.207	input.type: log agent.ip: 10.10.10.3 agent.name: DESKTOP-O7BM7AU agent.id: 005 manager.name: seminarioST data.integration: virustotal data.virustotal.sha1: 3395856ce81f2b7382dee72602f798b642f14140 data.virustotal.malicious: 1 data.virustotal.total: 57 data.virustotal.found: 1 data.virustotal.positives: 52 data.virustotal.source.sha1: 3395856ce81f2b7382dee72602f798b642f14140
Dec 19, 2025 @ 16:37:08.076	input.type: log agent.ip: 10.10.10.3 agent.name: DESKTOP-O7BM7AU agent.id: 005 manager.name: seminarioST data.origin.module: wazuh-execd data.origin.name: node01 data.version: 1 data.parameters.alert.agent.ip: 10.10.10.3 data.parameters.alert.agent.name: DESKTOP-O7BM7AU data.parameters.alert.agent.id: 005 data.parameters.alert.manager.name: seminari
Dec 19, 2025 @ 16:37:07.239	input.type: log agent.ip: 10.10.10.3 agent.name: DESKTOP-O7BM7AU agent.id: 005 manager.name: seminarioST data.integration: virustotal data.virustotal.sha1: 3395856ce81f2b7382dee72602f798b642f14140 data.virustotal.malicious: 1 data.virustotal.total: 57 data.virustotal.found: 1 data.virustotal.positives: 52 data.virustotal.source.sha1: 3395856ce81f2b7382dee72602f798b642f14140

ID	Status	IP address	Version	Groups	Operating system	Cluster node
005	●	10.10.10.3	Wazuh v4.9.2	default	Microsoft Windows 1...	node01

Registration date: Oct 29, 2025 @ 16:50:14.000

Last keep alive: Dec 19, 2025 @ 16:59:38.000

Last 24 hours

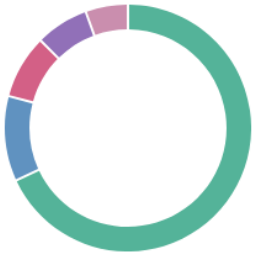
MITRE ATT&CK

Top Tactics

Defense Evasion	34
Impact	29
Initial Access	6
Persistence	6
Privilege Escalation	6

Compliance

PCI DSS



- 11.5 (49)
- 10.6.1 (8)
- 10.2.5 (6)
- 10.6 (5)
- 10.2.6 (4)

FIM: Recent events

Time ↓	Path	Action	Rule description	Rule Lev...	Rule Id
Dec 19, 2025 @ 16:37:07.570	c:\users\admin\downloads\eicar.txt	deleted	File deleted.	7	553
Dec 19, 2025 @ 16:37:05.062	c:\users\admin\downloads\eicar.txt	added	File added to the system.	5	554

t	_index	wazuh-alerts-4.x-2025.12.19
t	agent.id	005
t	agent.ip	10.10.10.3
t	agent.name	DESKTOP-O7BM7AU
t	data.integration	virustotal
t	data.virustotal.found	1
t	data.virustotal.malicious	1
t	data.virustotal.permalink	https://www.virustotal.com/gui/file/275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f/detection/f-275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f-1766158222
t	data.virustotal.positives	52
t	data.virustotal.scan_date	2025-12-19 15:30:22
t	data.virustotal.sha1	3395856ce81f2b7382dee72602f798b642f14140
t	data.virustotal.source.alert_id	1766158627.280798
t	data.virustotal.source.file	c:\users\admin\downloads\eicar.txt
t	data.virustotal.source.md5	44d88612fea8a8f36de82e1278abb02f
t	data.virustotal.source.sha1	3395856ce81f2b7382dee72602f798b642f14140
t	data.virustotal.total	57
t	decoder.name	json
t	id	1766158629.285700
t	input.type	log
t	location	virustotal
t	manager.name	seminarioST
t	rule.description	VirusTotal: Alert - c:\users\admin\downloads\eicar.txt - 52 nes detected this file
#	rule.firedtimes	2
t	rule.gdpr	IV_35.7.d
t	rule.groups	virustotal
t	rule.id	87105
#	rule.level	12
◕	rule.mail	true
t	rule.mitre.id	T1203
t	rule.mitre.tactic	Execution
t	rule.mitre.technique	Exploitation for Client Execution
t	rule.pci_dss	10.6.1, 11.4
🗓	timestamp	Dec 19, 2025 @ 16:37:09.207

> Dec 19, 2025 @ 16:37:07.570 syscheck.mode: realtime syscheck.path: c:\users\admin\downloads\eicar.txt syscheck.sha1_after: 3395856ce81f2b7382dee72602f798b642f14140 syscheck.uname_after: Administradores syscheck.mtime_after: Dec 19, 2025 @ 17:35:43.000 syscheck.attrs_after: ARCHIVE syscheck.size_after: 68 syscheck.uid_after: S-1-5-32-544 syscheck.win_perm_after.allowed: DELETE, READ_C