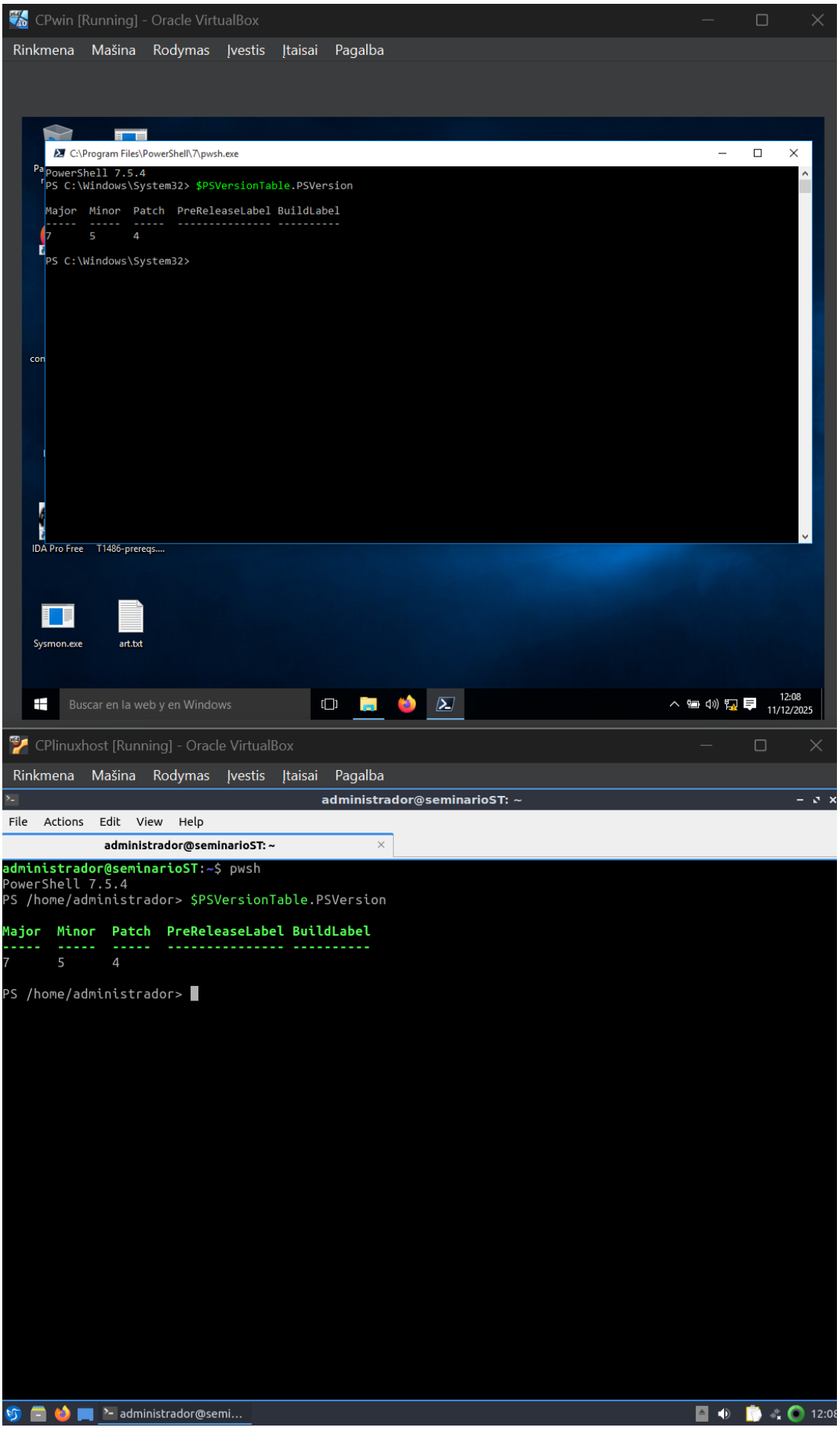
Cyberprotection Systems

Laboratory Work 2. Analysis and Containment of Security Incidents (MEMORY)

NAME AND SURNAME: Austėja Bauraitė

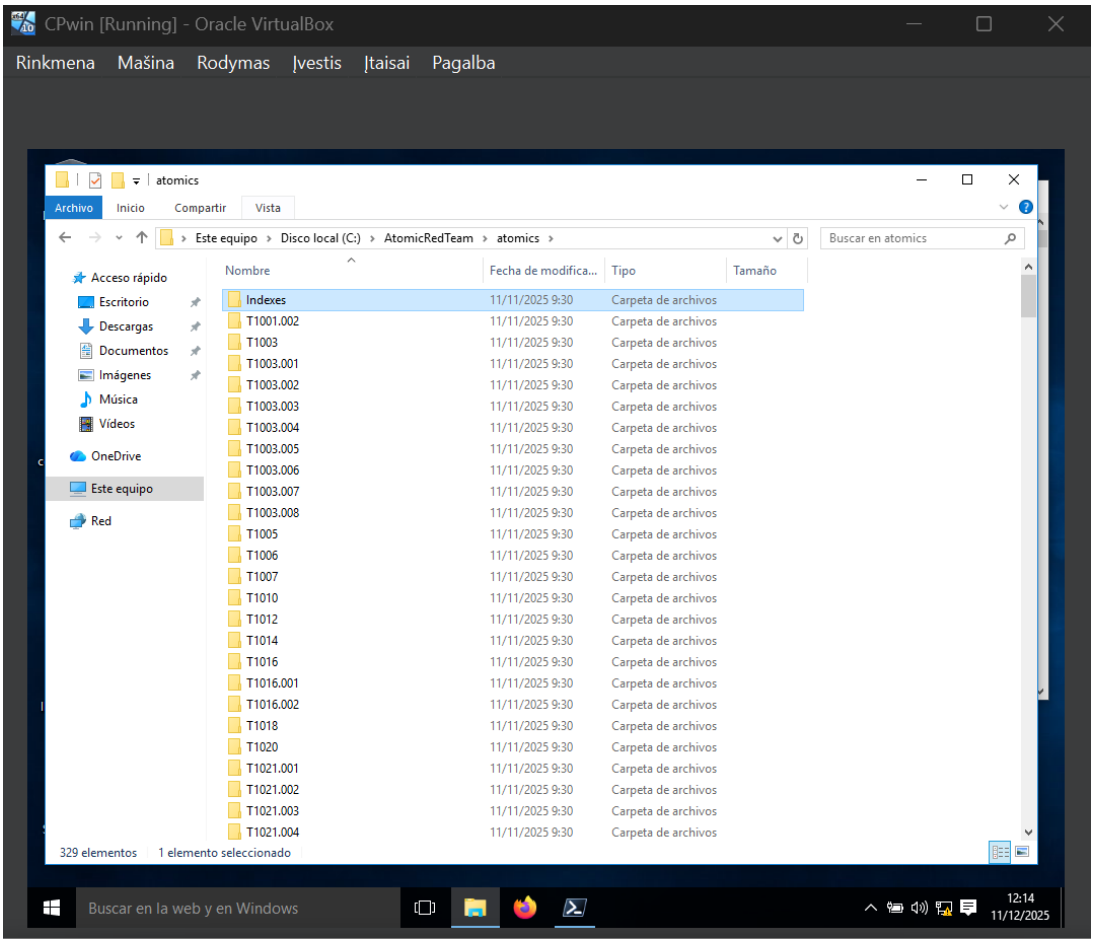
1. Powershell installing

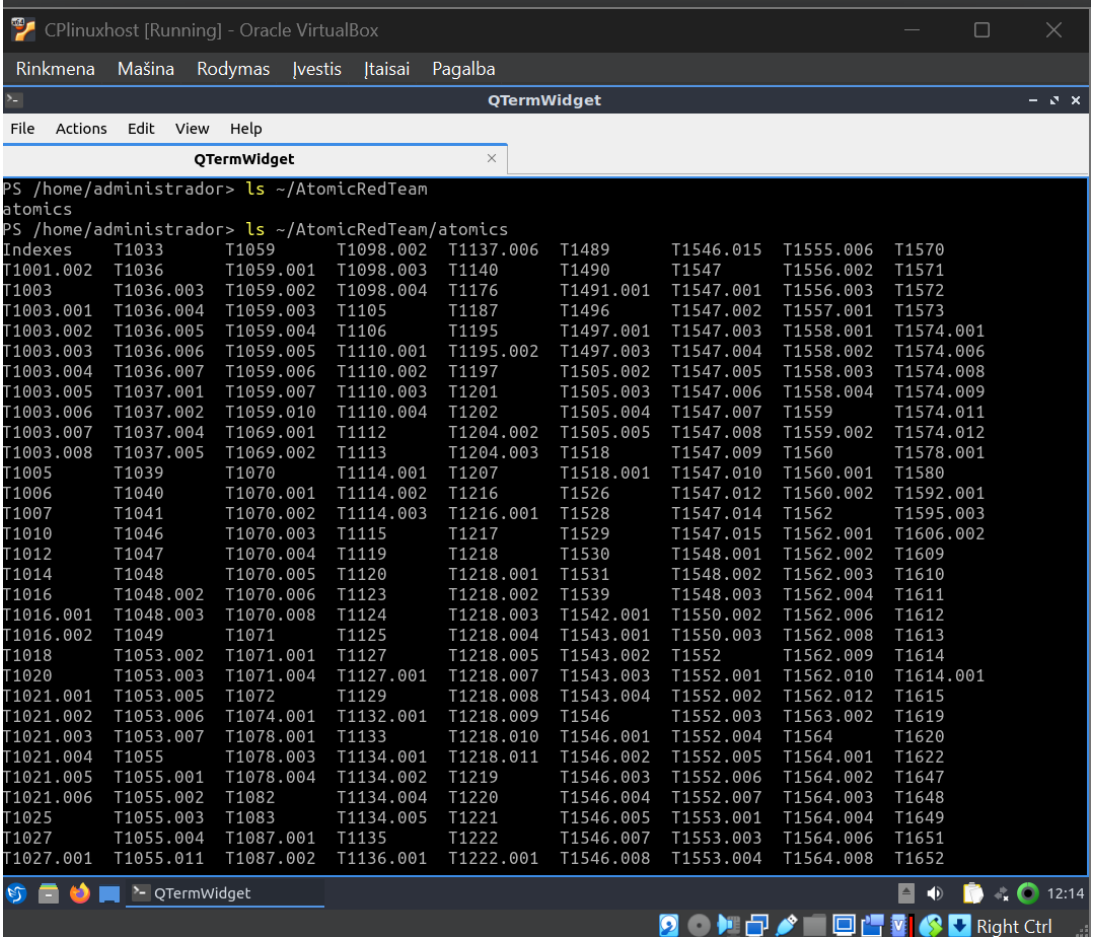
Put a screenshot on Windows and Linux machines showing Powershell tool.


CPwin [Running] - Oracle VirtualBox
Rinkmena Mašina Rodymas Įvestis Įtaisai Pagalba
C:\Program Files\PowerShell\7\pwsh.exe
PowerShell 7.5.4
PS C:\Windows\System32> $PSVersionTable.PSVersion
Major Minor Patch PreReleaseLabel BuildLabel
7 5 4
PS C:\Windows\System32>
IDA Pro Free
T1486-prereqs....
Sysmon.exe
art.txt
Buscar en la web y en Windows
12:08
11/12/2025
CPlinuxhost [Running] - Oracle VirtualBox
Rinkmena Mašina Rodymas Įvestis Įtaisai Pagalba
administrador@seminarioST: ~
File Actions Edit View Help
administrador@seminarioST: ~
administrador@seminarioST:~$ pwsh
PowerShell 7.5.4
PS /home/administrador> $PSVersionTable.PSVersion
Major Minor Patch PreReleaseLabel BuildLabel
7 5 4
PS /home/administrador>
administrador@semi...
12:08

2. Atomic Red Team Tool installing

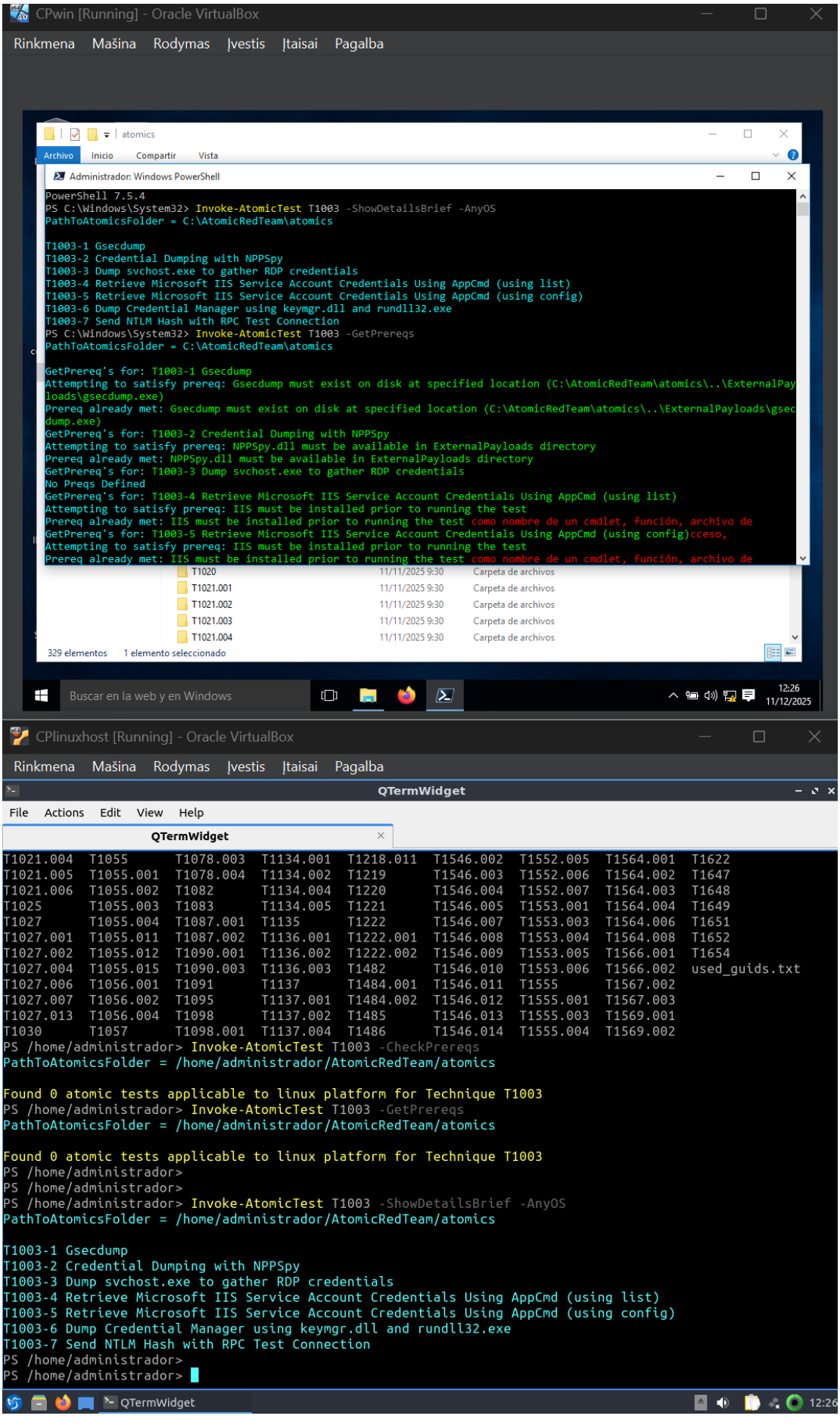
Show a screenshot (or some) where it can be seen the created default folders in Linux and Windows machines related to ART.


CPwin [Running] - Oracle VirtualBox
Rinkmena Mašina Rodymas Įvestis Įtaisai Pagalba
atomics
Archivo Inicio Compartir Vista
Este equipo › Disco local (C:) › AtomicRedTeam › atomics ›
Buscar en atomics
Acceso rápido
Escritorio
Descargas
Documentos
Imágenes
Música
Vídeos
OneDrive
Este equipo
Red
Nombre Fecha de modifica... Tipo Tamaño
Indexes 11/11/2025 9:30 Carpeta de archivos
T1001.002 11/11/2025 9:30 Carpeta de archivos
T1003 11/11/2025 9:30 Carpeta de archivos
T1003.001 11/11/2025 9:30 Carpeta de archivos
T1003.002 11/11/2025 9:30 Carpeta de archivos
T1003.003 11/11/2025 9:30 Carpeta de archivos
T1003.004 11/11/2025 9:30 Carpeta de archivos
T1003.005 11/11/2025 9:30 Carpeta de archivos
T1003.006 11/11/2025 9:30 Carpeta de archivos
T1003.007 11/11/2025 9:30 Carpeta de archivos
T1003.008 11/11/2025 9:30 Carpeta de archivos
T1005 11/11/2025 9:30 Carpeta de archivos
T1006 11/11/2025 9:30 Carpeta de archivos
T1007 11/11/2025 9:30 Carpeta de archivos
T1010 11/11/2025 9:30 Carpeta de archivos
T1012 11/11/2025 9:30 Carpeta de archivos
T1014 11/11/2025 9:30 Carpeta de archivos
T1016 11/11/2025 9:30 Carpeta de archivos
T1016.001 11/11/2025 9:30 Carpeta de archivos
T1016.002 11/11/2025 9:30 Carpeta de archivos
T1018 11/11/2025 9:30 Carpeta de archivos
T1020 11/11/2025 9:30 Carpeta de archivos
T1021.001 11/11/2025 9:30 Carpeta de archivos
T1021.002 11/11/2025 9:30 Carpeta de archivos
T1021.003 11/11/2025 9:30 Carpeta de archivos
T1021.004 11/11/2025 9:30 Carpeta de archivos
329 elementos 1 elemento seleccionado
Buscar en la web y en Windows
12:14
11/12/2025


CPlinuxhost [Running] - Oracle VirtualBox
Rinkmena Mašina Rodymas Įvestis Įtaisai Pagalba
QTermWidget
File Actions Edit View Help
QTermWidget
PS /home/administrador> ls ~/AtomicRedTeam
atomics
PS /home/administrador> ls ~/AtomicRedTeam/atomics
Indexes T1033 T1059 T1098.002 T1137.006 T1489 T1546.015 T1555.006 T1570
T1001.002 T1036 T1059.001 T1098.003 T1140 T1490 T1547 T1556.002 T1571
T1003 T1036.003 T1059.002 T1098.004 T1176 T1491.001 T1547.001 T1556.003 T1572
T1003.001 T1036.004 T1059.003 T1105 T1187 T1496 T1547.002 T1557.001 T1573
T1003.002 T1036.005 T1059.004 T1106 T1195 T1497.001 T1547.003 T1558.001 T1574.001
T1003.003 T1036.006 T1059.005 T1110.001 T1195.002 T1497.003 T1547.004 T1558.002 T1574.006
T1003.004 T1036.007 T1059.006 T1110.002 T1197 T1505.002 T1547.005 T1558.003 T1574.008
T1003.005 T1037.001 T1059.007 T1110.003 T1201 T1505.003 T1547.006 T1558.004 T1574.009
T1003.006 T1037.002 T1059.010 T1110.004 T1202 T1505.004 T1547.007 T1559 T1574.011
T1003.007 T1037.004 T1069.001 T1112 T1204.002 T1505.005 T1547.008 T1559.002 T1574.012
T1003.008 T1037.005 T1069.002 T1113 T1204.003 T1518 T1547.009 T1560 T1578.001
T1005 T1039 T1070 T1114.001 T1207 T1518.001 T1547.010 T1560.001 T1580
T1006 T1040 T1070.001 T1114.002 T1216 T1526 T1547.012 T1560.002 T1592.001
T1007 T1041 T1070.002 T1114.003 T1216.001 T1528 T1547.014 T1562 T1595.003
T1010 T1046 T1070.003 T1115 T1217 T1529 T1547.015 T1562.001 T1606.002
T1012 T1047 T1070.004 T1119 T1218 T1530 T1548.001 T1562.002 T1609
T1014 T1048 T1070.005 T1120 T1218.001 T1531 T1548.002 T1562.003 T1610
T1016 T1048.002 T1070.006 T1123 T1218.002 T1539 T1548.003 T1562.004 T1611
T1016.001 T1048.003 T1070.008 T1124 T1218.003 T1542.001 T1550.002 T1562.006 T1612
T1016.002 T1049 T1071 T1125 T1218.004 T1543.001 T1550.003 T1562.008 T1613
T1018 T1053.002 T1071.001 T1127 T1218.005 T1543.002 T1552 T1562.009 T1614
T1020 T1053.003 T1071.004 T1127.001 T1218.007 T1543.003 T1552.001 T1562.010 T1614.001
T1021.001 T1053.005 T1072 T1129 T1218.008 T1543.004 T1552.002 T1562.012 T1615
T1021.002 T1053.006 T1074.001 T1132.001 T1218.009 T1546 T1552.003 T1563.002 T1619
T1021.003 T1053.007 T1078.001 T1133 T1218.010 T1546.001 T1552.004 T1564 T1620
T1021.004 T1055 T1078.003 T1134.001 T1218.011 T1546.002 T1552.005 T1564.001 T1622
T1021.005 T1055.001 T1078.004 T1134.002 T1219 T1546.003 T1552.006 T1564.002 T1647
T1021.006 T1055.002 T1082 T1134.004 T1220 T1546.004 T1552.007 T1564.003 T1648
T1025 T1055.003 T1083 T1134.005 T1221 T1546.005 T1553.001 T1564.004 T1649
T1027 T1055.004 T1087.001 T1135 T1222 T1546.007 T1553.003 T1564.006 T1651
T1027.001 T1055.011 T1087.002 T1136.001 T1222.001 T1546.008 T1553.004 T1564.008 T1652
QTermWidget
12:14
Right Ctrl

3. Check technique T1003

Consult the details and available tests to run on Technique T1003 (in Linux and Windows), as well as its prerequisites. Present one or some screenshots related with this.


CPwin [Running] - Oracle VirtualBox
Rinkmena Mašina Rodymas Įvestis Įtaisai Pagalba
atomics
Archivo Inicio Compartir Vista
Administrador: Windows PowerShell
PowerShell 7.5.4
PS C:\Windows\System32> Invoke-AtomicTest T1003 -ShowDetailsBrief -AnyOS
PathToAtomicsFolder = C:\AtomicRedTeam\atomics
T1003-1 Gsecdump
T1003-2 Credential Dumping with NPPSpy
T1003-3 Dump svchost.exe to gather RDP credentials
T1003-4 Retrieve Microsoft IIS Service Account Credentials Using AppCmd (using list)
T1003-5 Retrieve Microsoft IIS Service Account Credentials Using AppCmd (using config)
T1003-6 Dump Credential Manager using keymgr.dll and rundll32.exe
T1003-7 Send NTLM Hash with RPC Test Connection
PS C:\Windows\System32> Invoke-AtomicTest T1003 -GetPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics
GetPrereq's for: T1003-1 Gsecdump
Attempting to satisfy prereq: Gsecdump must exist on disk at specified location (C:\AtomicRedTeam\atomics\..\ExternalPayloads\gsecdump.exe)
Prereq already met: Gsecdump must exist on disk at specified location (C:\AtomicRedTeam\atomics\..\ExternalPayloads\gsecdump.exe)
GetPrereq's for: T1003-2 Credential Dumping with NPPSpy
Attempting to satisfy prereq: NPPSpy.dll must be available in ExternalPayloads directory
Prereq already met: NPPSpy.dll must be available in ExternalPayloads directory
GetPrereq's for: T1003-3 Dump svchost.exe to gather RDP credentials
No Preqs Defined
GetPrereq's for: T1003-4 Retrieve Microsoft IIS Service Account Credentials Using AppCmd (using list)
Attempting to satisfy prereq: IIS must be installed prior to running the test
Prereq already met: IIS must be installed prior to running the test como nombre de un cmdlet, función, archivo de
GetPrereq's for: T1003-5 Retrieve Microsoft IIS Service Account Credentials Using AppCmd (using config)cceso,
Attempting to satisfy prereq: IIS must be installed prior to running the test
Prereq already met: IIS must be installed prior to running the test como nombre de un cmdlet, función, archivo de
T1020 11/11/2025 9:30 Carpeta de archivos
T1021.001 11/11/2025 9:30 Carpeta de archivos
T1021.002 11/11/2025 9:30 Carpeta de archivos
T1021.003 11/11/2025 9:30 Carpeta de archivos
T1021.004 11/11/2025 9:30 Carpeta de archivos
329 elementos 1 elemento seleccionado
Buscar en la web y en Windows
12:26 11/12/2025
CPlinuxhost [Running] - Oracle VirtualBox
Rinkmena Mašina Rodymas Įvestis Įtaisai Pagalba
QTermWidget
File Actions Edit View Help
QTermWidget
T1021.004 T1055 T1078.003 T1134.001 T1218.011 T1546.002 T1552.005 T1564.001 T1622
T1021.005 T1055.001 T1078.004 T1134.002 T1219 T1546.003 T1552.006 T1564.002 T1647
T1021.006 T1055.002 T1082 T1134.004 T1220 T1546.004 T1552.007 T1564.003 T1648
T1025 T1055.003 T1083 T1134.005 T1221 T1546.005 T1553.001 T1564.004 T1649
T1027 T1055.004 T1087.001 T1135 T1222 T1546.007 T1553.003 T1564.006 T1651
T1027.001 T1055.011 T1087.002 T1136.001 T1222.001 T1546.008 T1553.004 T1564.008 T1652
T1027.002 T1055.012 T1090.001 T1136.002 T1222.002 T1546.009 T1553.005 T1566.001 T1654
T1027.004 T1055.015 T1090.003 T1136.003 T1482 T1546.010 T1553.006 T1566.002 used_guids.txt
T1027.006 T1056.001 T1091 T1137 T1484.001 T1546.011 T1555 T1567.002
T1027.007 T1056.002 T1095 T1137.001 T1484.002 T1546.012 T1555.001 T1567.003
T1027.013 T1056.004 T1098 T1137.002 T1485 T1546.013 T1555.003 T1569.001
T1030 T1057 T1098.001 T1137.004 T1486 T1546.014 T1555.004 T1569.002
PS /home/administrador> Invoke-AtomicTest T1003 -CheckPrereqs
PathToAtomicsFolder = /home/administrador/AtomicRedTeam/atomics
Found 0 atomic tests applicable to linux platform for Technique T1003
PS /home/administrador> Invoke-AtomicTest T1003 -GetPrereqs
PathToAtomicsFolder = /home/administrador/AtomicRedTeam/atomics
Found 0 atomic tests applicable to linux platform for Technique T1003
PS /home/administrador>
PS /home/administrador>
PS /home/administrador> Invoke-AtomicTest T1003 -ShowDetailsBrief -AnyOS
PathToAtomicsFolder = /home/administrador/AtomicRedTeam/atomics
T1003-1 Gsecdump
T1003-2 Credential Dumping with NPPSpy
T1003-3 Dump svchost.exe to gather RDP credentials
T1003-4 Retrieve Microsoft IIS Service Account Credentials Using AppCmd (using list)
T1003-5 Retrieve Microsoft IIS Service Account Credentials Using AppCmd (using config)
T1003-6 Dump Credential Manager using keymgr.dll and rundll32.exe
T1003-7 Send NTLM Hash with RPC Test Connection
PS /home/administrador>
PS /home/administrador>
QTermWidget
12:26

On the Linux machine:

Invoke-AtomicTest T1003 -CheckPrereqs and Invoke-AtomicTest T1003 -GetPrereqs. The output was: “Found 0 atomic tests applicable to linux platform for Technique T1003”. This indicates that, in our Atomic Red Team version, T1003 tests are only defined for Windows, not Linux. Then used Invoke-AtomicTest T1003 -ShowDetailsBrief -AnyOS to see all existing tests for this technique even though they are not applicable on Linux.

4. Data Exfiltration (T1048) in Linux

a) Describe technique T1048, according to Mitre ATT&ACK.

https://attack.mitre.org/techniques/T1048/

The idea is that an attacker does not send stolen data using the same protocol as the command-and-control (C2) channel, but instead uses some other protocol that may look more “legit”.

Examples of alternative protocols are FTP, SMTP, HTTP/HTTPS, DNS or SMB, or even cloud services like collaboration platforms. Instead of uploading data directly to the C2 server, the attacker can push files to an external FTP server, send them as email attachments, or hide the data inside DNS queries. They can also encrypt or obfuscate the traffic to make detection harder.

On Linux/macOS, this can be done with normal system tools such as curl, wget, scp …, so the exfiltration may look like a totally normal admin operation from the point of view of the system

b) Check the associated tests and their requirements

```
ModuleType Version    PreRelease Name                                PSEdition ExportedCommands
---------- -------    ---------- ----                                --------- ----------------
Script     2.3.0                 Invoke-AtomicRedTeam                Desk      {Invoke-AtomicTest, Get…

PS /home/administrador> Set-PSRepository -Name PSGallery -InstallationPolicy Trusted
PS /home/administrador> Install-Module -Name Invoke-AtomicRedTeam -Scope CurrentUser
WARNING: Unable to resolve package source 'https://www.powershellgallery.com/api/v2'.
Install-Package: No match was found for the specified search criteria and module name 'Invoke-AtomicRedT
eam'. Try
Get-PSRepository to see all available registered module repositories.
PS /home/administrador> Import-Module Invoke-AtomicRedTeam -Force
PS /home/administrador> Get-Module Invoke-AtomicRedTeam

ModuleType Version    PreRelease Name                                ExportedCommands
---------- -------    ---------- ----                                ----------------
Script     2.3.0                 Invoke-AtomicRedTeam                {Get-AtomicTechnique, Get-Preferr…

PS /home/administrador> Get-Command Invoke-AtomicTest

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        Invoke-AtomicTest                                  2.3.0      Invoke-AtomicRedTeam

PS /home/administrador> Invoke-AtomicTest T1048 -ShowDetailsBrief
PathToAtomicsFolder = /home/administrador/AtomicRedTeam/atomics

T1048-1 Exfiltration Over Alternative Protocol - SSH
T1048-2 Exfiltration Over Alternative Protocol - SSH
T1048-4 Exfiltrate Data using DNS Queries via dig
PS /home/administrador>
```

```
PS /home/administrador> Invoke-AtomicTest T1048 -CheckPrereqs
PathToAtomicsFolder = /home/administrador/AtomicRedTeam/atomics

CheckPrereq's for: T1048-1 Exfiltration Over Alternative Protocol - SSH
Prerequisites met: T1048-1 Exfiltration Over Alternative Protocol - SSH
CheckPrereq's for: T1048-2 Exfiltration Over Alternative Protocol - SSH
Prerequisites met: T1048-2 Exfiltration Over Alternative Protocol - SSH
CheckPrereq's for: T1048-4 Exfiltrate Data using DNS Queries via dig
/usr/bin/dig
Prerequisites met: T1048-4 Exfiltrate Data using DNS Queries via dig
PS /home/administrador>
```

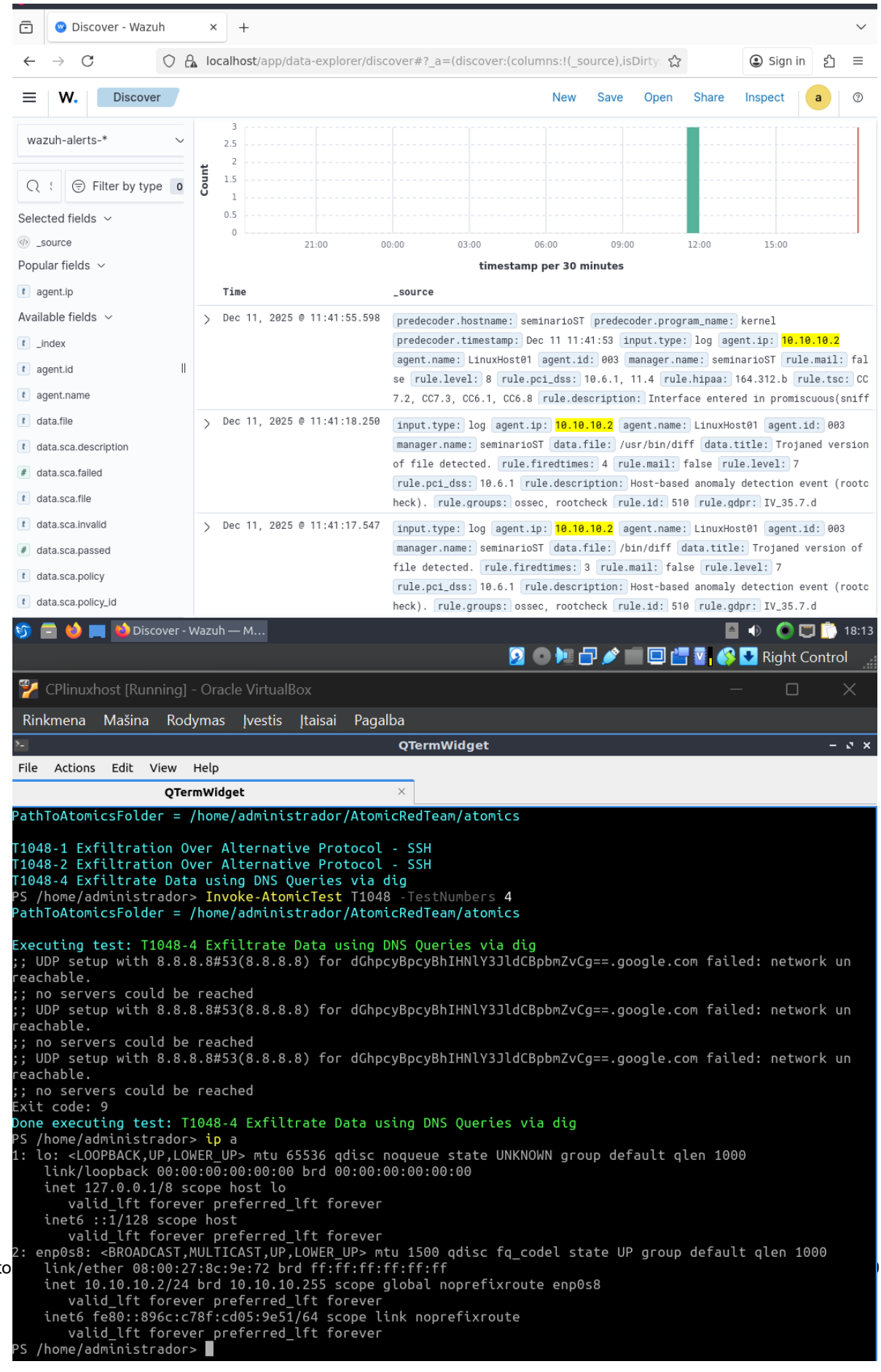
c) Show screenshots with evidences on the run of test 4.

```
PS /home/administrador> Invoke-AtomicTest T1048 -ShowDetailsBrief
PathToAtomicsFolder = /home/administrador/AtomicRedTeam/atomics

T1048-1 Exfiltration Over Alternative Protocol - SSH
T1048-2 Exfiltration Over Alternative Protocol - SSH
T1048-4 Exfiltrate Data using DNS Queries via dig
PS /home/administrador> Invoke-AtomicTest T1048 -TestNumbers 4
PathToAtomicsFolder = /home/administrador/AtomicRedTeam/atomics

Executing test: T1048-4 Exfiltrate Data using DNS Queries via dig
;; UDP setup with 8.8.8.8#53(8.8.8.8) for dGhpcyBpcyBhIHNlY3JldCBpbmZvCg==.google.com failed: network un
reachable.
;; no servers could be reached
;; UDP setup with 8.8.8.8#53(8.8.8.8) for dGhpcyBpcyBhIHNlY3JldCBpbmZvCg==.google.com failed: network un
reachable.
;; no servers could be reached
;; UDP setup with 8.8.8.8#53(8.8.8.8) for dGhpcyBpcyBhIHNlY3JldCBpbmZvCg==.google.com failed: network un
reachable.
;; no servers could be reached
Exit code: 9
Done executing test: T1048-4 Exfiltrate Data using DNS Queries via dig
PS /home/administrador>
```

d) Show the related detection of this Technique in Wazuh (with the standard rules or with your own created new rules). Which which main rule group should alert to this behaviour in Wazuh?

After running the T1048 atomic test on the Linux host (10.10.10.2), I checked the Wazuh alert console and filtered by that agent and time. Wazuh generated several alerts, for example with rule.id 510 and the description “Host-based anomaly detection event (rootcheck)”, where the data.title field said “Trojaned version of file detected” for /usr/bin/diff and /bin/ddiff.

These alerts belong to the ossec, rootcheck rule group, so the main rule group that detects this behaviour in Wazuh is rootcheck (host-based anomaly detection).


Discover - Wazuh
localhost/app/data-explorer/discover#?_a=(discover:(columns:!(_source),isDirty
Sign in
Discover
New
Save
Open
Share
Inspect
wazuh-alerts-*
Filter by type 0
Selected fields
_source
Popular fields
agent.ip
Available fields
_index
agent.id
agent.name
data.file
data.sca.description
data.sca.failed
data.sca.file
data.sca.invalid
data.sca.passed
data.sca.policy
data.sca.policy_id
Count
timestamp per 30 minutes
Time
_source
Dec 11, 2025 @ 11:41:55.598
Dec 11, 2025 @ 11:41:18.250
Dec 11, 2025 @ 11:41:17.547
Discover - Wazuh — M...
18:13
Right Control
CPlinuxhost [Running] - Oracle VirtualBox
Rinkmena Mašina Rodymas Įvestis Įtaisai Pagalba
QTermWidget
File Actions Edit View Help
QTermWidget
PathToAtomicsFolder = /home/administrador/AtomicRedTeam/atomics
T1048-1 Exfiltration Over Alternative Protocol - SSH
T1048-2 Exfiltration Over Alternative Protocol - SSH
T1048-4 Exfiltrate Data using DNS Queries via dig
PS /home/administrador> Invoke-AtomicTest T1048 -TestNumbers 4
PathToAtomicsFolder = /home/administrador/AtomicRedTeam/atomics
Executing test: T1048-4 Exfiltrate Data using DNS Queries via dig
;; UDP setup with 8.8.8.8#53(8.8.8.8) for dGhpcyBpcyBhIHNlY3JldCBpbmZvCg==.google.com failed: network unreachable.
;; no servers could be reached
;; UDP setup with 8.8.8.8#53(8.8.8.8) for dGhpcyBpcyBhIHNlY3JldCBpbmZvCg==.google.com failed: network unreachable.
;; no servers could be reached
;; UDP setup with 8.8.8.8#53(8.8.8.8) for dGhpcyBpcyBhIHNlY3JldCBpbmZvCg==.google.com failed: network unreachable.
;; no servers could be reached
Exit code: 9
Done executing test: T1048-4 Exfiltrate Data using DNS Queries via dig
PS /home/administrador> 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: 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:c78f:cd05:9e51/64 scope link noprefixroute
valid_lft forever preferred_lft forever
PS /home/administrador>

e) Proceed with the analysis of the expected alert at its source. What do you observe? What final conclusions do you reach? Describe the actions you have taken to reach your final conclusion

To analyse the alert at its source, I first opened the full Wazuh alert for the Linux host 10.10.10.2 (LinuxHost01) around the time I ran the T1048 test. There I saw several events: one from the kernel saying “Interface entered in promiscuous (sniffing) mode” and others with rule.id 510, data.title “Trojaned version of file detected” for /usr/bin/diff and /bin/ddiff, all in the ossec/rootcheck rule group.

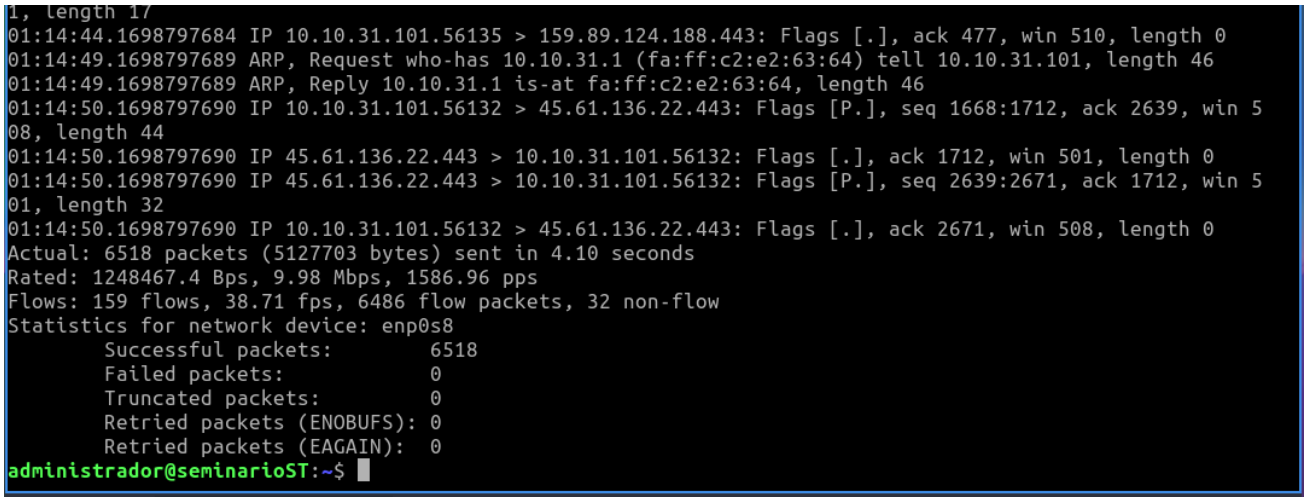
Then I went to the Linux machine and checked the local logs (journalctl / /var/log/syslog, dmseg) around that timestamp and confirmed the same kernel message about the interface going into promiscuous mode, plus entries related to the modified binaries. I also inspected the files reported by Wazuh to verify that they had been altered as part of the Atomic test and were not the original system binaries.

```
            10:41:09.359681 main     Package type: LINUX_64BITS_GENERIC
  24.757824] 10:41:09.361470 main     6.1.38 r153438 started. Verbose level = 0
  24.763711] 10:41:09.367335 main     vbglR3GuestCtrlDetectPeekGetCancelSupport: Supported (#1)
  69.345659] device enp0s8 entered promiscuous mode
2980.650416] 11:30:26.448164 control  Session 0 is about to close ...
```

From this I conclude that the T1048 atomic test not only generates exfiltration-style network traffic, but also leaves traces such as trojaned binaries and a network interface in sniffing mode. Wazuh, via the rootcheck (host-based anomaly detection) rules, correctly detects these suspicious changes and raises an alert that points to a possible compromise and data-exfiltration behaviour.

5. Trace analysis of the network behaviour of real *malware*

a) Show in one or more screenshots how the `tcpreplay` tool work with the *pcap* file and is seen in Wireshark.


1, length 17
01:14:44.1698797684 IP 10.10.31.101.56135 > 159.89.124.188.443: Flags [.], ack 477, win 510, length 0
01:14:49.1698797689 ARP, Request who-has 10.10.31.1 (fa:ff:c2:e2:63:64) tell 10.10.31.101, length 46
01:14:49.1698797689 ARP, Reply 10.10.31.1 is-at fa:ff:c2:e2:63:64, length 46
01:14:50.1698797690 IP 10.10.31.101.56132 > 45.61.136.22.443: Flags [P.], seq 1668:1712, ack 2639, win 5
08, length 44
01:14:50.1698797690 IP 45.61.136.22.443 > 10.10.31.101.56132: Flags [.], ack 1712, win 501, length 0
01:14:50.1698797690 IP 45.61.136.22.443 > 10.10.31.101.56132: Flags [P.], seq 2639:2671, ack 1712, win 5
01, length 32
01:14:50.1698797690 IP 10.10.31.101.56132 > 45.61.136.22.443: Flags [.], ack 2671, win 508, length 0
Actual: 6518 packets (5127703 bytes) sent in 4.10 seconds
Rated: 1248467.4 Bps, 9.98 Mbps, 1586.96 pps
Flows: 159 flows, 38.71 fps, 6486 flow packets, 32 non-flow
Statistics for network device: enp0s8
Successful packets: 6518
Failed packets: 0
Truncated packets: 0
Retried packets (ENOBUFS): 0
Retried packets (EAGAIN): 0
administrador@seminarioST:~$

19	2.904323021	10.10.31.101	104.21.32.6	HTTP	361	GET / HTTP/1.1
20	2.904419447	104.21.32.6	10.10.31.101	TCP	60	80 → 56108 [ACK] Seq=1 Ack=308 W
21	2.904515721	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=1 Ack=308 W
22	2.904609605	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=1377 Ack=30
23	2.904952317	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=2753 Ack=30
24	2.905043994	10.10.31.101	104.21.32.6	TCP	60	56108 → 80 [ACK] Seq=308 Ack=275
25	2.905473654	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=4129 Ack=30
26	2.906688073	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=5505 Ack=30
27	2.906838149	10.10.31.101	104.21.32.6	TCP	60	56108 → 80 [ACK] Seq=308 Ack=550
28	2.907835902	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=6881 Ack=30
29	2.908965860	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=8257 Ack=30
30	2.910109825	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=9633 Ack=30
31	2.910209378	10.10.31.101	104.21.32.6	TCP	60	56108 → 80 [ACK] Seq=308 Ack=825
32	2.911266731	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=11009 Ack=3
33	2.911361825	10.10.31.101	104.21.32.6	TCP	60	56108 → 80 [ACK] Seq=308 Ack=110
34	2.912456304	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=12385 Ack=3
35	2.913392486	104.21.32.6	10.10.31.101	TCP	1186	80 → 56108 [PSH, ACK] Seq=13761
36	2.913489746	10.10.31.101	104.21.32.6	TCP	60	56108 → 80 [ACK] Seq=308 Ack=137
37	2.913581173	10.10.31.101	104.21.32.6	TCP	60	56108 → 80 [ACK] Seq=308 Ack=148
38	2.914651457	104.21.32.6	10.10.31.101	TCP	1430	[TCP Previous segment not captur
39	2.916187116	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=17645 Ack=3
40	2.916971425	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=19021 Ack=3
41	2.917075388	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#1] 56108 → 80 [A
42	2.918136543	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=20397 Ack=3
43	2.918234474	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#2] 56108 → 80 [A
44	2.918328855	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#3] 56108 → 80 [A
45	2.919525509	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=21773 Ack=3
46	2.919735611	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#4] 56108 → 80 [A
47	2.920827187	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=23149 Ack=3
48	2.921033737	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#5] 56108 → 80 [A
49	2.921983587	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=24525 Ack=3
50	2.922177388	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#6] 56108 → 80 [A
51	2.923171746	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=25901 Ack=3
52	2.923319908	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#7] 56108 → 80 [A
53	2.924227873	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=27277 Ack=3
54	2.924341111	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#8] 56108 → 80 [A
55	2.925383247	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=28653 Ack=3
56	2.925505033	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#9] 56108 → 80 [A
57	2.926587721	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=30029 Ack=3
58	2.926689333	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#10] 56108 → 80 [
59	2.927768852	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=31405 Ack=3
60	2.927872684	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#11] 56108 → 80 [
61	2.928957852	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=32781 Ack=3
62	2.929096040	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#12] 56108 → 80 [
63	2.930137801	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=34157 Ack=3
64	2.930264047	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#13] 56108 → 80 [
65	2.931377334	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=35533 Ack=3
66	2.931473617	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#14] 56108 → 80 [
67	2.932570701	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=36909 Ack=3
68	2.932685346	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#15] 56108 → 80 [
69	2.938014929	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=38285 Ack=3
70	2.938600963	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#16] 56108 → 80 [
71	2.938904586	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=39661 Ack=3
72	2.939092858	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#17] 56108 → 80 [
73	2.939237323	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=41037 Ack=3
74	2.939487608	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#18] 56108 → 80 [
75	2.939711203	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=42413 Ack=3
76	2.939848142	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#19] 56108 → 80 [
77	2.939967522	104.21.32.6	10.10.31.101	TCP	118	80 → 56108 [PSH, ACK] Seq=43789
78	2.940079065	104.21.32.6	10.10.31.101	TCP	1430	[TCP Fast Retransmission] 80 → 5
79	2.940190058	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#20] 56108 → 80 [
80	2.940285775	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 37#21] 56108 → 80 [
81	2.940449139	10.10.31.101	104.21.32.6	TCP	60	56108 → 80 [ACK] Seq=308 Ack=438
82	2.940598753	104.21.32.6	10.10.31.101	TCP	1430	[TCP Spurious Retransmission] 80
83	2.940712630	10.10.31.101	104.21.32.6	TCP	66	[TCP Dup ACK 81#1] 56108 → 80 [A
84	2.941294073	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=43853 Ack=3
85	2.942248646	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=45229 Ack=3
86	2.943382597	104.21.32.6	10.10.31.101	TCP	1430	80 → 56108 [ACK] Seq=46605 Ack=3

2023	4.346979674	45.61.137.225	10.10.31.101	TLSv1.2	86 Application Data
2024	4.347070359	10.10.31.101	45.61.137.225	TCP	60 56110 → 443 [ACK] Seq=532 Ack=18
2025	4.347169881	10.10.31.101	10.10.31.1	DNS	88 Standard query 0x41e4 A msedge.a
2026	4.347270021	10.10.31.1	10.10.31.101	DNS	172 Standard query response 0x41e4 A
2027	4.347373358	10.10.31.101	23.102.129.60	TCP	66 56111 → 443 [SYN] Seq=0 Win=6424
2028	4.347471460	23.102.129.60	10.10.31.101	TCP	66 443 → 56111 [SYN, ACK] Seq=0 Ack
2029	4.348175663	10.10.31.101	23.102.129.60	TCP	60 56111 → 443 [ACK] Seq=1 Ack=1 Wi
2030	4.348272278	10.10.31.101	23.102.129.60	TLSv1.2	267 Client Hello
2031	4.348649467	23.102.129.60	10.10.31.101	TCP	1430 443 → 56111 [ACK] Seq=1 Ack=214
2032	4.349786612	23.102.129.60	10.10.31.101	TCP	1430 443 → 56111 [ACK] Seq=1377 Ack=2
2033	4.350714392	23.102.129.60	10.10.31.101	TLSv1.2	1164 Server Hello, Certificate, Serve
2034	4.350808981	10.10.31.101	23.102.129.60	TCP	60 56111 → 443 [ACK] Seq=214 Ack=27
2035	4.350949600	10.10.31.101	23.102.129.60	TLSv1.2	212 Client Key Exchange, Change Ciph
2036	4.351045022	23.102.129.60	10.10.31.101	TLSv1.2	105 Change Cipher Spec, Encrypted Ha
2037	4.351515769	10.10.31.101	23.102.129.60	TLSv1.2	607 Application Data
2038	4.352707487	10.10.31.101	23.102.129.60	TCP	1450 56111 → 443 [ACK] Seq=925 Ack=39
2039	4.353839283	10.10.31.101	23.102.129.60	TLSv1.2	1356 Application Data
2040	4.353943731	23.102.129.60	10.10.31.101	TCP	60 443 → 56111 [ACK] Seq=3914 Ack=2
2041	4.354374081	23.102.129.60	10.10.31.101	TLSv1.2	700 Application Data
2042	4.354917035	10.10.31.101	23.102.129.60	TLSv1.2	706 Application Data
2043	4.355027820	10.10.31.101	23.102.129.60	TLSv1.2	85 Application Data
2044	4.355134207	23.102.129.60	10.10.31.101	TCP	60 443 → 56111 [ACK] Seq=4560 Ack=4
2045	4.356225162	23.102.129.60	10.10.31.101	TCP	1430 443 → 56111 [ACK] Seq=4560 Ack=4
2046	4.357343909	23.102.129.60	10.10.31.101	TCP	1430 443 → 56111 [ACK] Seq=5936 Ack=4
2047	4.358472020	23.102.129.60	10.10.31.101	TLSv1.2	1427 Application Data
2048	4.358543247	10.10.31.101	23.102.129.60	TCP	60 56111 → 443 [ACK] Seq=4306 Ack=7
2049	4.359662756	23.102.129.60	10.10.31.101	TCP	1430 443 → 56111 [ACK] Seq=8685 Ack=4
2050	4.359885352	23.102.129.60	10.10.31.101	TLSv1.2	274 Application Data
2051	4.359984226	10.10.31.101	23.102.129.60	TCP	60 56111 → 443 [ACK] Seq=4306 Ack=1
2052	4.360084378	10.10.31.101	23.102.129.60	TCP	60 56111 → 443 [ACK] Seq=4306 Ack=1
2053	4.360225149	10.10.31.101	10.10.31.1	DNS	81 Standard query 0xb766 A config.e
2054	4.360355088	10.10.31.1	10.10.31.101	DNS	241 Standard query response 0xb766 A
2055	4.360475698	10.10.31.101	13.107.42.16	TCP	66 56117 → 443 [SYN] Seq=0 Win=6424
2056	4.360592409	13.107.42.16	10.10.31.101	TCP	66 443 → 56117 [SYN, ACK] Seq=0 Ack
2057	4.360689149	10.10.31.101	13.107.42.16	TCP	60 56117 → 443 [ACK] Seq=1 Ack=1 Wi
2058	4.360782576	10.10.31.101	13.107.42.16	TLSv1.2	260 Client Hello
2059	4.360851221	13.107.42.16	10.10.31.101	TCP	60 443 → 56117 [ACK] Seq=1 Ack=207
2060	4.361875404	13.107.42.16	10.10.31.101	TCP	1430 443 → 56117 [ACK] Seq=1 Ack=207
2061	4.362921616	13.107.42.16	10.10.31.101	TCP	1430 443 → 56117 [ACK] Seq=1377 Ack=2
2062	4.364217182	13.107.42.16	10.10.31.101	TCP	1430 443 → 56117 [ACK] Seq=2753 Ack=2
2063	4.365281294	13.107.42.16	10.10.31.101	TCP	1430 443 → 56117 [ACK] Seq=4129 Ack=2
2064	4.365345585	10.10.31.101	13.107.42.16	TCP	60 56117 → 443 [ACK] Seq=207 Ack=27
2065	4.365654550	13.107.42.16	10.10.31.101	TLSv1.2	520 Server Hello, Certificate, Certi
2066	4.365715617	10.10.31.101	13.107.42.16	TCP	60 56117 → 443 [ACK] Seq=207 Ack=55
2067	4.365867957	10.10.31.101	13.107.42.16	TLSv1.2	212 Client Key Exchange, Change Ciph
2068	4.365954176	13.107.42.16	10.10.31.101	TCP	60 443 → 56117 [ACK] Seq=5971 Ack=3
2069	4.366278606	13.107.42.16	10.10.31.101	TLSv1.2	396 New Session Ticket, Change Ciphe
2070	4.366405738	13.107.42.16	10.10.31.101	TLSv1.2	123 Application Data
2071	4.366510207	10.10.31.101	13.107.42.16	TCP	60 56117 → 443 [ACK] Seq=365 Ack=63
2072	4.366614825	10.10.31.101	13.107.42.16	TLSv1.2	141 Application Data
2073	4.367702400	10.10.31.101	13.107.42.16	TCP	1450 56117 → 443 [ACK] Seq=452 Ack=63
2074	4.368225555	10.10.31.101	13.107.42.16	TLSv1.2	687 Application Data
2075	4.368329992	10.10.31.101	13.107.42.16	TLSv1.2	92 Application Data
2076	4.368437131	13.107.42.16	10.10.31.101	TCP	60 443 → 56117 [ACK] Seq=6382 Ack=4
2077	4.368547302	13.107.42.16	10.10.31.101	TLSv1.2	92 Application Data
2078	4.368660737	13.107.42.16	10.10.31.101	TCP	60 443 → 56117 [ACK] Seq=6420 Ack=1
2079	4.368762787	10.10.31.101	13.107.42.16	TCP	60 56117 → 443 [ACK] Seq=2519 Ack=6
2080	4.368870951	13.107.42.16	10.10.31.101	TCP	60 443 → 56117 [ACK] Seq=6420 Ack=2
2081	4.368967546	13.107.42.16	10.10.31.101	TCP	60 443 → 56117 [ACK] Seq=6420 Ack=2
2082	4.369165397	13.107.42.16	10.10.31.101	TLSv1.2	659 Application Data
2083	4.369261542	10.10.31.101	13.107.42.16	TCP	60 56117 → 443 [FIN, ACK] Seq=2519
2084	4.369358154	10.10.31.101	23.102.129.60	TCP	60 56111 → 443 [RST, ACK] Seq=4306
2085	4.369463859	13.107.42.16	10.10.31.101	TCP	60 443 → 56117 [ACK] Seq=7025 Ack=2
2086	4.369580344	13.107.42.16	10.10.31.101	TLSv1.2	96 Application Data
2087	4.369688200	13.107.42.16	10.10.31.101	TCP	60 443 → 56117 [FIN, ACK] Seq=7067
2088	4.369829400	10.10.31.101	13.107.42.16	TCP	60 56117 → 443 [RST, ACK] Seq=2520
2089	4.369897948	10.10.31.101	13.107.42.16	TCP	60 56117 → 443 [RST] Seq=2520 Win=0
2090	4.369984293	10.10.31.101	10.10.31.1	DNS	73 Standard query 0xccc1 A gousahaf

b) What do you see in Wazuh console? Check the rising alerts and identify the possible attack/campaign associated with them, as well as the tactics and techniques associated with the alerts (according to Mitre ATT&CK).

In the Wazuh console, after replaying the PCAP I observed several Suricata alerts from the Linux sensor (agent 10.10.10.2). The signatures are “SURICATA STREAM ESTABLISHED SYNACK resent / SYN resend” and “tcp.retransmission.alerted”, with source and destination IPs matching the flows seen in Wireshark (10.10.31.101 <-> 159.89.124.188:443, 23.102.129.60:443, and so on..).

These alerts indicate anomalous TCP behaviour inside HTTPS sessions and point to suspicious encrypted communication between an internal host and external servers, which is consistent with malware command-and-control traffic rather than normal browsing.

Even though the rules do not name a specific malware family, the pattern fits an unknown malware / C2 campaign using HTTPS as its channel. In terms of Mitre ATT&CK, this behaviour could be mapped to something like:

TA0011 – Command and Control, mainly

T1071.001 – Application Layer Protocol: Web protocols (HTTP/HTTPS)

T1573 – Encrypted Channel (the traffic is over TLS)

So, yes, Wazuh is detecting the replayed malware traffic, but in this case the detections appear as Suricata stream/anomaly alerts rather than a specific named malware signature.

timestamp per 30 minutes

Time	_source
Dec 11, 2025 @ 21:30	predecoder.hostname: seminarioST predecoder.program_name: sudo predecoder.timestamp: Dec 11 21:29:59 input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.dstuser: root rule.firedtimes: 8 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: Logi
Dec 11, 2025 @ 21:29:57.233	predecoder.hostname: seminarioST predecoder.program_name: sudo predecoder.timestamp: Dec 11 21:29:55 input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.srcuser: administrador data.dstuser: root data.tty: pts/1 data.pwd: /home/administrador data.command: /usr/bin/tcpreplay -v -i enp0s8 -M10 malware.pcap rule.mail: false
Dec 11, 2025 @ 21:29:57.233	predecoder.hostname: seminarioST predecoder.program_name: sudo predecoder.timestamp: Dec 11 21:29:55 input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.uid: 1000 data.dstuser: root(uid=0) 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: Logi
Dec 11, 2025 @ 21:29:53.440	input.type: log agent.ip: 10.10.10.3 agent.name: DESKTOP-O7BM7AU agent.id: 005 manager.name: seminarioST data.win.eventdata.data: 2025-12-12T20:28:53Z, RulesEngine data.win.system.eventID: 16384 data.win.system.eventSourceName: Software Protection Platform Service data.win.system.keywords: 0x80000000000000 data.win.system.providerGuid: {E23B33B0-C8C9-472C-A5F9-F2BDFEA0F156}
Dec 11, 2025 @ 21:29:32.229	input.type: log agent.ip: 10.10.10.3 agent.name: DESKTOP-O7BM7AU agent.id: 005 manager.name: seminarioST data.win.eventdata.data: hr=0x8007007B, RuleId=502ff3ba-669a-4674-bbb1-601f34a3b968;Action=AutoActivateSilent;AppId=55c92734-d682-4d71-983e-d6ec3f16059f;SkuId=73111121-5638-40f6-bc11-f1d7b0d64300;NotificationInterval=1440;Trigger=NetworkAvailable data.win.system.eventID: 8198
Dec 11, 2025 @ 21:29:32.135	input.type: log agent.ip: 10.10.10.3 agent.name: DESKTOP-O7BM7AU agent.id: 005 manager.name: seminarioST data.win.eventdata.data: hr=0x8007007B, RuleId=502ff3ba-669a-4674-bbb1-601f34a3b968;Action=AutoActivateSilent;AppId=55c92734-d682-4d71-983e-d6ec3f16059f;SkuId=73111121-5638-40f6-bc11-f1d7b0d64300;NotificationInterval=1440;Trigger=NetworkAvailable data.win.system.eventID: 8198
Dec 11, 2025 @ 21:29:30.434	input.type: log agent.ip: 10.10.10.3 agent.name: DESKTOP-O7BM7AU agent.id: 005 manager.name: seminarioST data.win.eventdata.subjectLogonId: 0x3e7 data.win.eventdata.previousTime: 2025-12-11T19:41:57.818443700Z data.win.eventdata.subjectUserSid: S-1-5-18 data.win.eventdata.processId: 0x354 data.win.eventdata.processName: C:\\Windows\\System32\\VBoxService.exe
Dec 11, 2025 @ 21:28:19.128	input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.metadata.flowints.tcp.retransmission.count: 11 data.metadata.flowbits: tcp.retransmission.alerted data.app_proto: failed data.ip_v: 4 data.in_iface: enp0s8 data.src_ip: 10.10.31.101 data.src_port: 56135 data.event_type: alert data.alert.severity: 3 data.alert.signature_id: 2210
Dec 11, 2025 @ 21:28:19.128	predecoder.hostname: seminarioST predecoder.program_name: sudo predecoder.timestamp: Dec 11 21:28:18 input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.dstuser: root rule.firedtimes: 7 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: Logi
Dec 11, 2025 @ 21:28:17.182	input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.app_proto: failed data.ip_v: 4 data.in_iface: enp0s8 data.src_ip: 159.89.124.188 data.src_port: 443 data.event_type: alert data.alert.severity: 3 data.alert.signature_id: 2210023 data.alert.rev: 3 data.alert.gid: 1 data.alert.signature: SURICATA STREAM ESTABLISHED SYNACK resen
Dec 11, 2025 @ 21:28:17.180	input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.app_proto: failed data.ip_v: 4 data.in_iface: enp0s8 data.src_ip: 10.10.31.101 data.src_port: 56135 data.event_type: alert data.alert.severity: 3 data.alert.signature_id: 2210027 data.alert.rev: 3 data.alert.gid: 1 data.alert.signature: SURICATA STREAM ESTABLISHED SYN resend w
Dec 11, 2025 @ 21:28:17.172	input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.metadata.flowints.tcp.retransmission.count: 11

t	data.alert.signature	SURICATA STREAM excessive retransmissions
t	data.alert.signature_id	2210054
t	data.app_proto	failed
t	data.dest_ip	159.89.124.188
t	data.dest_port	443
t	data.direction	to_server
t	data.event_type	alert
t	data.flow.bytes_toclient	2831
t	data.flow.bytes_toserver	4990
t	data.flow.dest_ip	159.89.124.188
t	data.flow.dest_port	443
t	data.flow.pkts_toclient	41
t	data.flow.pkts_toserver	69
t	data.flow.src_ip	10.10.31.101
t	data.flow.src_port	56135
t	data.flow.start	2025-12-11T21:26:47.106503+0100
t	data.flow_id	2146277063530390.000000
t	data.in_iface	enp0s8
t	data.ip_v	4
?	data.metadata.flowbits	⚠ tcp.retransmission.alerted
?	data.metadata.flowints.tcp.retransmission.count	⚠ 11
t	data.pkt_src	wire/pcap
t	data.proto	TCP
t	data.src_ip	10.10.31.101
t	data.src_port	56135
📅	data.timestamp	Dec 11, 2025 @ 21:28:17.680
t	decoder.name	json
t	id	1765484899.339072
t	input.type	log
t	location	/var/log/suricata/eve.json
t	manager.name	seminarioST
t	rule.description	Suricata: Alert - SURICATA STREAM excessive retransmissions

6. Ransomware Attack (T1486) in Windows

a) Describe technique T1486, according to Mitre ATT&ACK.

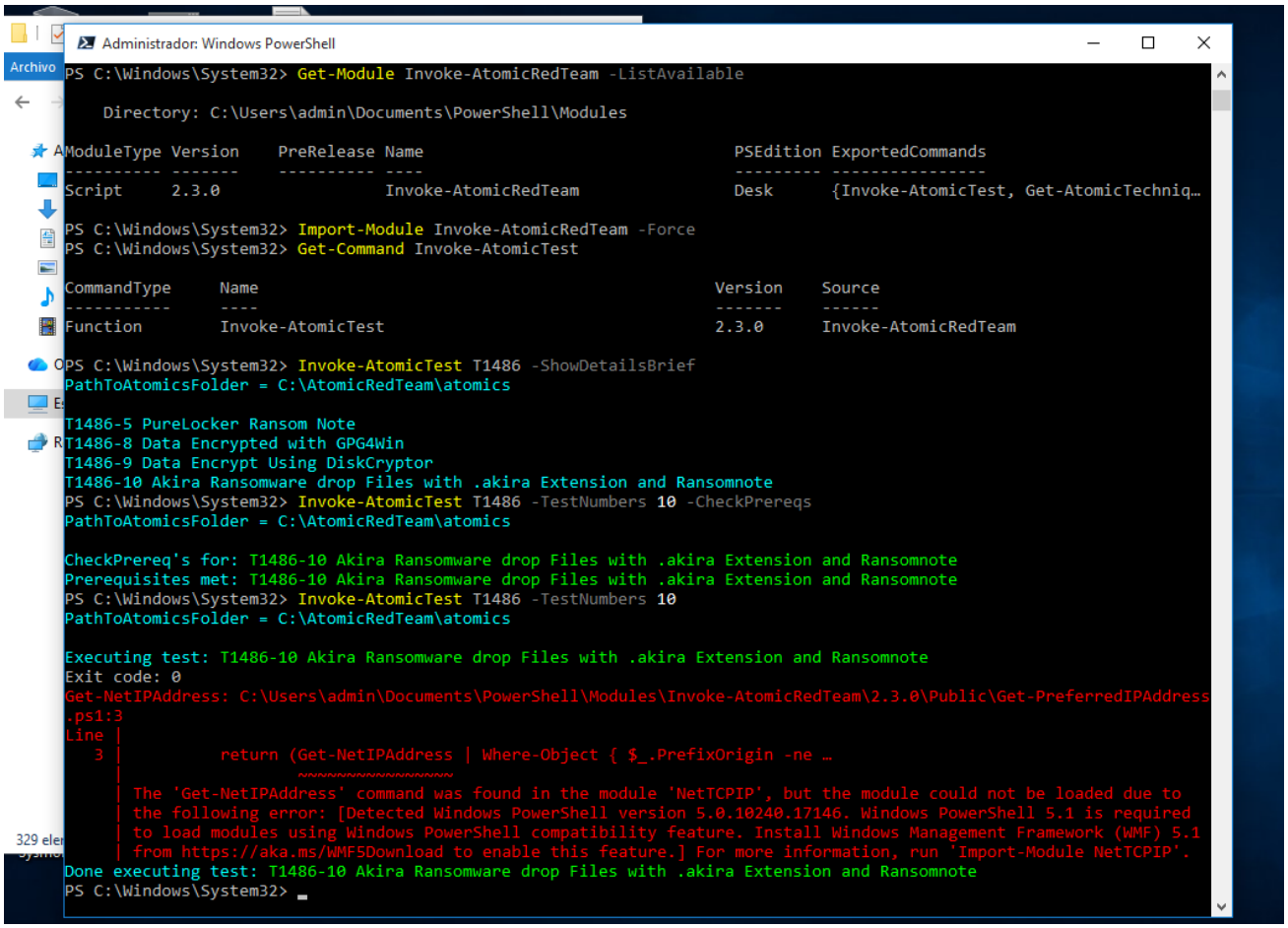
Technique T1486 is Data Encrypted for Impact belongs to the Impact tactic in MITRE ATT&CK. It describes situations where an attacker encrypts data on one or many systems in order to break availability of data and services.

So instead of just stealing files, the adversary makes the data unusable by encrypting files on local disks, network shares or even whole partitions, and then usually withholds the decryption key. This is the classic behaviour of ransomware: the victim's documents, images, databases, etc. are encrypted and the attacker demands money in exchange for the key. In more destructive campaigns, the key might never be stored, so the data is basically wiped.

Typical real-world examples include families like WannaCry, NotPetya, which encrypt user and business data and sometimes also try to propagate to other systems.

b) Run test 10 of T1486.

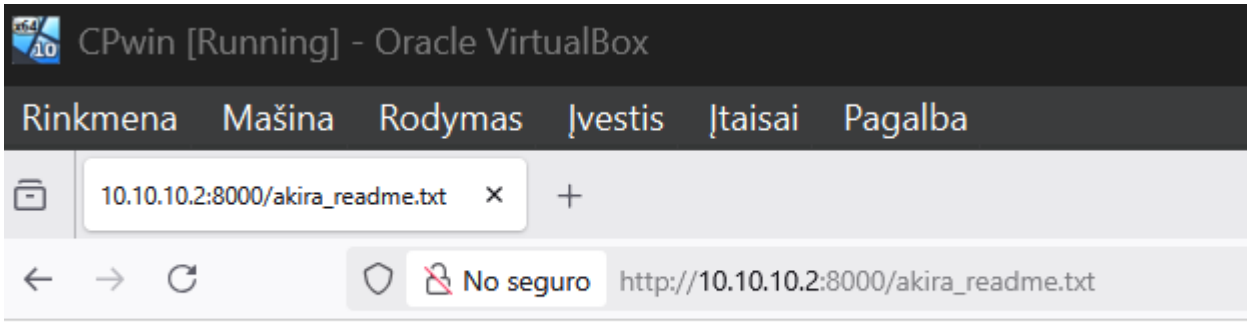
The prerequisites for T1486-10 Akira Ransomware drop Files with .akira Extension and Ransomnote were met and the test executed with exit code 0. During execution I got a warning related to the Get-NetIPAddress cmdlet (NetTCPIP module), because my VM runs an older Windows PowerShell version and the compatibility feature for Get-NetIPAddress is not available. However, this did not affect the test itself: the Akira simulation still created multiple .akira files and a ransom note as expected.



c) Based on the test's definition, operation, and objective, which main rule group should alert you to this behaviour in Wazuh? Check the alert console in Wazuh for this purpose (show a screenshot).

```
administrador@seminarioST:~$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 8.0.1 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 1
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: suricata: Preparing unexpected signal handling
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 2 rule files processed. 46153 rules successfully loaded, 0 rules failed, 0 rules skipped
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 46156 signatures processed. 941 are IP-only rules, 4420 are inspecting packet payload, 4056
3 inspect application layer, 110 are decoder event only
Notice: mpm-hs: Rule group caching - loaded: 34 newly cached: 78 total cacheable: 112
Notice: suricata: Configuration provided was successfully loaded. Exiting.
administrador@seminarioST:~$ 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.method;  cont
ent:"GET"; nocase; content:"/pass.html"; nocase; sid:1000002; rev:1;)
alert http any any -> $HOME_NET any (msg:"LOCAL Akira ransomware- ransom note akira readme over HTTP"; fl
ow:established;  content:"akira_readme.txt"; nocase; http_uri; classtype:trojan-activity; reference:url,a
ttack.mitre.org/techniques/T1486/; sid:9000010; rev:1;)
alert http any any -> $HOME_NET any (msg:"LOCAL Akira ransomeware - .akira encrypted file over HTTP"; flo
w:established; file_data; content:".akira"; nocase; classtype:trojan-activity; reference:url,attack.mitre
.org/techniques/T1486/; sid:9000011; rev:1;)
administrador@seminarioST:~$
```

```
administrador@seminarioST:~$ echo "This is a ransome note" > akira_readme.txt
administrador@seminarioST:~$ sudo python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```



> Dec 11, 2025 @ 22:37:53.294 input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.tx_id: 0 data.app_proto: http data.ip_v: 4 data.in_iface: enp0s8 data.src_ip: 10.10.10.2 data.src_port: 8000 data.event_type: alert data.alert.severity: 3 data.alert.signature_id: 2034636 data.alert.rev: 2 data.alert.metadata.affected_product: Windows_XP_Vista_7_8_10_

> Dec 11, 2025 @ 22:37:53.287 input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.tx_id: 0 data.app_proto: http data.ip_v: 4 data.in_iface: enp0s8 data.src_ip: 10.10.10.2 data.src_port: 8000 data.event_type: alert data.alert.severity: 3 data.alert.signature_id: 2034636 data.alert.rev: 2 data.alert.metadata.affected_product: Windows_XP_Vista_7_8_10_

> Dec 11, 2025 @ 22:37:53.285 input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.tx_id: 0 data.app_proto: http data.ip_v: 4 data.in_iface: enp0s8 data.src_ip: 10.10.10.3 data.src_port: 49441 data.event_type: alert data.alert.severity: 1 data.alert.signature_id: 9000010 data.alert.rev: 1 data.alert.gid: 1 data.alert.signature: LOCAL Akira ransomwar

> Dec 11, 2025 @ 22:36:27.245 predecoder.hostname: seminarioST predecoder.program_name: sudo predecoder.timestamp: Dec 11 22:36:26 input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.uid: 1000 data.dstuser: root(uid=0) 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: Logi

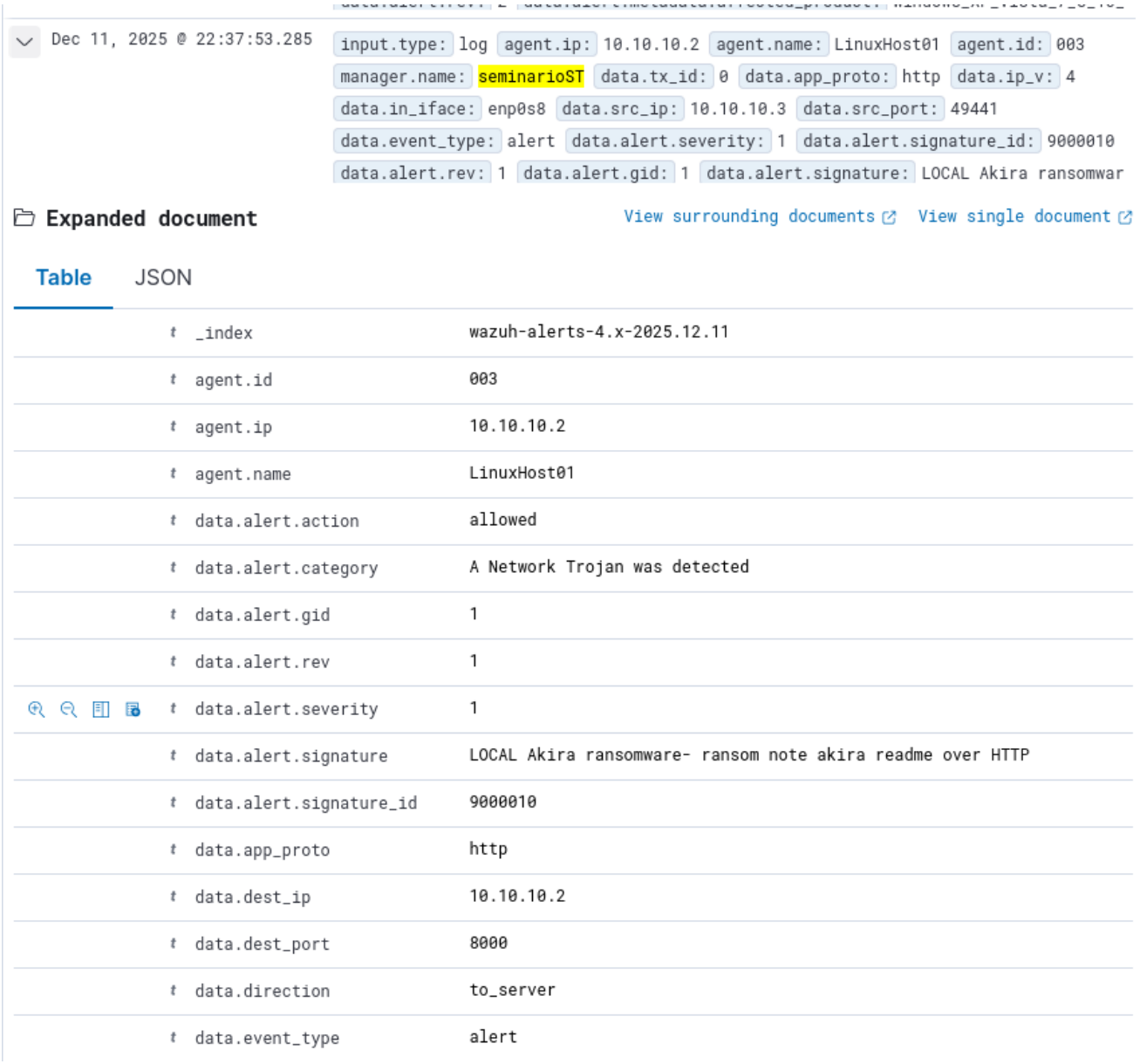
> Dec 11, 2025 @ 22:36:27.202 predecoder.hostname: seminarioST predecoder.program_name: sudo predecoder.timestamp: Dec 11 22:36:26 input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.srcuser: administrador data.dstuser: root data.tty: pts/1 data.pwd: /home/administrador data.command: /usr/bin/python3 -m http.server 8000 rule.mail: false

> Dec 11, 2025 @ 22:35:09.176 predecoder.hostname: seminarioST predecoder.program_name: sudo predecoder.timestamp: Dec 11 22:35:07 input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.uid: 1000 data.dstuser: root(uid=0) 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: Logi

> Dec 11, 2025 @ 22:35:09.176 predecoder.hostname: seminarioST predecoder.program_name: sudo predecoder.timestamp: Dec 11 22:35:07 input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.dstuser: root rule.firedtimes: 15 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: Logi

> Dec 11, 2025 @ 22:35:09.128 predecoder.hostname: seminarioST predecoder.program_name: sudo predecoder.timestamp: Dec 11 22:35:07 input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.srcuser: administrador data.dstuser: root data.tty: pts/1 data.pwd: /home/administrador data.command: /usr/bin/python3 -m http.server 80 rule.mail: false rule.level: 3

> Dec 11, 2025 @ 22:32:06.940 predecoder.hostname: seminarioST predecoder.program_name: sudo predecoder.timestamp: Dec 11 22:32:06 input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003 manager.name: seminarioST data.dstuser:



Dec 11, 2025 @ 22:37:53.285

input.type: log agent.ip: 10.10.10.2 agent.name: LinuxHost01 agent.id: 003
manager.name: seminarioST data.tx_id: 0 data.app_proto: http data.ip_v: 4
data.in_iface: enp0s8 data.src_ip: 10.10.10.3 data.src_port: 49441
data.event_type: alert data.alert.severity: 1 data.alert.signature_id: 9000010
data.alert.rev: 1 data.alert.gid: 1 data.alert.signature: LOCAL Akira ransomwar

Expanded document View surrounding documents View single document

Table JSON

t _index	wazuh-alerts-4.x-2025.12.11
t agent.id	003
t agent.ip	10.10.10.2
t agent.name	LinuxHost01
t data.alert.action	allowed
t data.alert.category	A Network Trojan was detected
t data.alert.gid	1
t data.alert.rev	1
t data.alert.severity	1
t data.alert.signature	LOCAL Akira ransomware- ransom note akira readme over HTTP
t data.alert.signature_id	9000010
t data.app_proto	http
t data.dest_ip	10.10.10.2
t data.dest_port	8000
t data.direction	to_server
t data.event_type	alert

After running the T1486-10 Akira atomic on the Windows VM and not seeing any built-in Wazuh alerts, I created my own Suricata rule to detect Akira simulation indicators over HTTP. The rule looks for requests containing the ransom-note name akira_readme.txt and is tagged as trojan/ransomware and mapped to ATT&CK T1486.

On the Linux sensor (10.10.10.2) I created the file akira_readme.txt and started a small HTTP server on port 8000

From the Windows machine I then browsed to http://10.10.10.2:8000/akira_readme.txt. This generated HTTP traffic between the Windows host and the Linux sensor.

In the Wazuh console, after filtering by the Linux agent (10.10.10.2) and the time of the request, I saw several new alerts coming from Suricata. One of them had: (screenshot)

In the alert details, the rule group for this event is the IDS/Suricata group (e.g. suricata, ids, network), which is the part of Wazuh in charge of network-intrusion detections. Therefore, the main rule group that alerts on this behaviour in Wazuh is the Suricata/IDS rule group, using my custom Akira ransomware signature.

d) Analyse the expected alert at its source. What do you observe? What final conclusions do you reach? Describe the actions you have taken to reach your final conclusion.

To analyse the alert at its source, I followed the path backwards from Wazuh to the Linux sensor that generated the event. In the Wazuh UI I opened the full details of the alert with signature “LOCAL Akira ransomware - ransom note akira_readme.txt over HTTP”. The fields show that the log came from the Suricata IDS running on LinuxHost01 (10.10.10.2), on interface enp0s8, with application protocol http and the source/destination IPs and ports that match my test (10.10.10.3 to 10.10.10.2:8000).

On the Linux sensor I then checked the Suricata log (eve.json) using grep for the same signature text. This confirms that the original detection was produced by my custom Suricata rule when the Windows host requested akira_readme.txt from the Python HTTP server.

The T1486-10 Akira atomic simulates ransomware by dropping .akira files and a ransom note on the Windows host. I extended the detection surface by adding a network IDS rule that looks for the Akira ransom note being transferred over HTTP. Suricata on the Linux sensor generated an event with signature ID 9000010 when the Windows machine downloaded akira_readme.txt. Wazuh ingested this Suricata event and raised an alert in the Suricata/IDS rule group.

My final conclusion is that, even though the original atomic test did not trigger any built-in Wazuh alerts on Windows, it is possible to detect Akira-related behaviour or any other by writing a custom Suricata rule. Wazuh correctly collects this IDS event, enriches it, and displays it as a ransomware-related alert for further analysis.