

## Task 03: Velociraptor EDR – Advanced Detection Validation

### Objective

This task demonstrated that Velociraptor EDR is highly effective at detecting attacker-like behaviors using behavior based detection rather than relying on malware signatures. Through multiple safe simulations, Velociraptor consistently captured process execution, PowerShell abuse, persistence mechanisms, and reconnaissance activities.

The creation of reusable artifacts and hunts showed how detection engineering can be applied in real world environments. Performance testing confirmed that the solution is lightweight, scalable, and suitable for production deployment with proper tuning.

Overall, this project provided hands-on experience with real EDR concepts and validated Velociraptor as a powerful open-source detection and response platform.

### Lab Environment

The lab environment consisted of one Velociraptor server hosted on the main machine and four Windows virtual machines acting as endpoints. All endpoints were successfully connected to the Velociraptor server using the GUI console. System telemetry such as process execution, PowerShell logs, file system activity, registry changes, and basic network behavior was enabled to support detection and investigation activities. Snapshots were enabled to ensure safe rollback after simulations.



The screenshot shows the Velociraptor GUI interface. At the top, there is a search bar with 'all' entered and a dropdown menu. To the right, it shows 'DESKTOP-F57FH34.localdomain' with a green 'Connected' status and a user icon labeled 'admin'. Below this is a table with columns: Client ID, Hostname, FQDN, OS Version, and Labels. The table lists four clients, all with a green status icon. The first three clients have Hostnames 'DESKTOP-F57FH34' and 'vm-win02', and OS Version 'Microsoft Windows 10 Pro22H2'. The fourth client has Hostname 'DESKTOP-F57FH34' and OS Version 'Microsoft Windows 10 Pro22H2'.

Client ID	Hostname	FQDN	OS Version	Labels
C.15cafb9f37205860	DESKTOP-F57FH34	DESKTOP-F57FH34.localdomain	Microsoft Windows 10 Pro22H2	
C.575966f7e8113738	DESKTOP-F57FH34	DESKTOP-F57FH34.localdomain	Microsoft Windows 10 Pro22H2	
C.7894b0649d098b2e	vm-win02	vm-win02.localdomain	Microsoft Windows 10 Pro22H2	
C.9dfb18daaf7c821f	DESKTOP-F57FH34	DESKTOP-F57FH34.localdomain	Microsoft Windows 10 Pro22H2	

## Phase1:

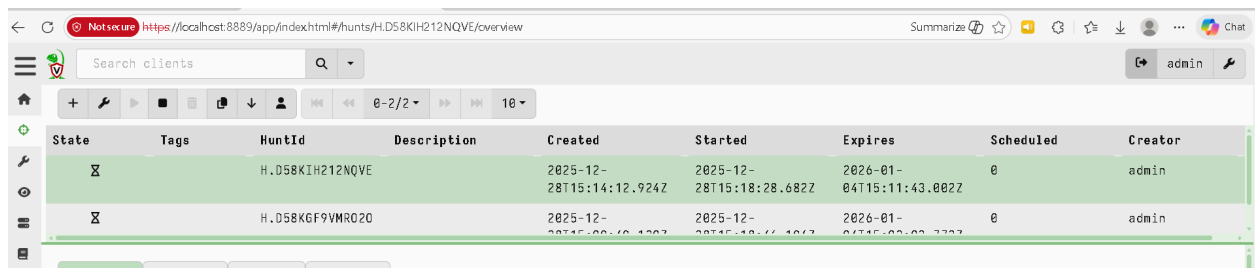
### Artifact Execution Works

## Client Connectivity Verification

All four Windows endpoints successfully connected to the Velociraptor server and were visible in the Velociraptor client dashboard. Each endpoint responded correctly to artifact execution requests, confirming that the deployment and communication between server and clients were functioning as expected.

## Artifact Execution Validation

To validate evidence collection, multiple built in Velociraptor artifacts were executed. Artifacts completed successfully and returned results without errors, confirming that the system was ready for detection and investigation tasks.



The screenshot shows the Velociraptor client dashboard in a web browser. The URL is `https://localhost:8889/app/index.html#/hunts/H.D58KI212NQVE/overview`. The interface includes a search bar for clients, a sidebar with navigation icons, and a main table displaying hunt information. The table has columns for State, Tags, HuntId, Description, Created, Started, Expires, Scheduled, and Creator. Two hunts are listed, both in a 'Running' state (indicated by a green 'X' icon) and created by 'admin'.

State	Tags	HuntId	Description	Created	Started	Expires	Scheduled	Creator
Running		H.D58KI212NQVE		2025-12-28T15:14:12.924Z	2025-12-28T15:18:28.682Z	2026-01-04T15:11:43.002Z	0	admin
Running		H.D58K6F9VMR020		2025-12-28T15:20:10.100Z	2025-12-28T15:18:16.101Z	2026-01-04T15:02:00.333Z	0	admin









3.3 Baseline: Normal PowerShell Usage

PowerShell operational logs were reviewed to establish normal usage patterns. No encoded, obfuscated, or suspicious PowerShell commands were detected at baseline.

Overview

Artifact Names

Windows.EventLogs.PowerShellModule

Windows.EventLogs.PowerShellScriptblock

Hunt ID

H.D5F1V9A14Q068

Creator

admin

Creation Time

2026-01-07T08:56:05.334Z

Expiry Time

2026-01-14T08:51:00.308Z

State

Scheduled

Ops/Sec

Unlimited

CPU Limit

Unlimited

IOPS Limit

Unlimited

Parameters

Windows.EventLogs.PowerShellModule

Windows.EventLogs.PowerShellScriptblock

Results

Total scheduled

2

Finished clients

2

Download Results

Select a download m

all

vm-win4.localdomain

Connected

admin

State	Tags	HuntId	Description	Created	Started	Expires	Scheduled	Creator
		H.D5F1V9A14Q068		2026-01-07T08:56:05.334Z	2026-01-07T08:56:23.003Z	2026-01-14T08:51:00.308Z	2	admin

0-1/1

EventTime	Computer		innet	EventID	SecurityID	Path	ScriptBlockId	ScriptBlockText	Message	EventRecordID	Level	Opcode
2026-01-07T08:35:38Z	vm-win4		Microsoft-Windows-PowerShell/Operational	4104	S-1-5-21-4892812788-2994514832-2884181510-1001	C:\Windows\TEMP\SOIAG_c9318944-b007-419d-b741-2c087825e0ac\7\CLUtillicy.ps1	6b9c5f29-7be2-48d5-9833-fd17ee452dbc	# Copyright © 2008, Microsoft Corporation. All rights reserved. # Common utility functions Import-LocalizedData -BindingVariable localizationString -FileName CL_LocalizationData # Function to get user troubleshooting history function Get-UserTSHistoryPath { return "\$(\$env:localappdata)\diagnostics" } # Function to get admin troubleshooting history function Get-AdminTSHistoryPath { return "\$(\$env:localappdata)\elevatediagnostics" } # Function to get user report folder path function Get-UserReportPath { return "\$(\$env:localappdata)\Microsoft\Windows\WER\ReportQueue" } # Function to get system report folder path function Get-MachineReportPath { return "\$(\$env:AllUsersProfile	Creating Scriptblock text (1 of 1): # Copyright © 2008, Microsoft Corporation. All rights reserved. #Common utility functions Import-LocalizedData -BindingVariable localizationString -FileName CL_LocalizationData #Common utility functions Import-LocalizedData -BindingVariable localizationString -FileName CL_LocalizationData # Function to get user troubleshooting history function Get-UserTSHistoryPath { return "\$(\$env:localappdata)\diagnostics" } # Function to get admin troubleshooting history function Get-AdminTSHistoryPath { return "\$(\$env:localappdata)\elevatediagnostics" } # Function to get user report folder path function Get-UserReportPath { return "\$(\$env:localappdata)\Microsoft\Windows\WER\ReportQueue" } # Function to get system report folder path function Get-MachineReportPath { return "\$(\$env:AllUsersProfile	11	3	15

### 3.4 Baseline: Network Connections

Basic network behavior was reviewed to identify normal connections. Only expected system related activity was observed, and no suspicious external connections were present.

State

Tags

HuntId

Description

Created

Started

Expires

Scheduled

Creator

⌕		H.D5F2H63IKHPVA		2026-01-07T09:34:16.112Z	2026-01-07T09:34:50.680Z	2026-01-14T09:34:05.788Z	2	admin
---	--	-----------------	--	--------------------------	--------------------------	--------------------------	---	-------

+

+

🗑️

📄

📁

⬇️

👤

⏪

⏩

0-4/4

⏪

⏩

10

State

FlowId

Artifacts

Created

Last Active

Creator

Mb

Rows

✓	F.D5F2H63IKHPVA.H	Windows.Network.Netstat	2026-01-07T09:34:50.726Z	2026-01-07T09:34:50.310Z	admin	0 b	47
✓	F.D5F1V9A14Q0G8.H	Windows.EventLogs.PowershellModule	2026-01-07T08:56:23.014Z	2026-01-07T08:56:23.161Z	admin	0 b	1

Artifact Collection

Uploaded Files

Requests

Results

Log

Notebook

Overview

Results

Artifact Names

🔗 Windows.Network.Netstat

Flow ID

F.D5F2H63IKHPVA.H

Creator

admin

Create Time

2026-01-07T09:34:50.726Z

Start Time

2026-01-07T09:34:50.182Z

Last Active

2026-01-07T09:34:50.310Z

Duration

0.13 seconds

State

Completed

Ops/Sec

Unlimited

CPU Limit

Unlimited

IOPS Limit

Unlimited

Timeout

600 seconds

Artifacts with Results

Windows.Network.Netstat

Total Rows

47

Uploaded Bytes

0 / 0

Files uploaded

0

Download Results

📄

⚙️

🗑️

Select a download method

2026-01-07T09:41:18.039Z

<div><div><div><div><div></div><div></div></div><div><div></div><div></div></div><div><div></div><div></div></div><div><div></div><div></div></div><div><div></div><div></div></div></div><div><div>0-10/47</div><div>10</div></div></div></div>									
Pid	Name	Family	Type	Status	Laddr.IP	Laddr.Port	Raddr.IP	Raddr.Port	Timestamp
504	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	135	0.0.0.0	0	2026-01-07T08:07:22Z
4	System	IPv4	TCP	LISTEN	192.168.52.144	139	0.0.0.0	0	2026-01-07T09:06:44Z
1284	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	5040	0.0.0.0	0	2026-01-07T08:08:07Z
824	lsass.exe	IPv4	TCP	LISTEN	0.0.0.0	49664	0.0.0.0	0	2026-01-07T08:07:22Z
704	wininit.exe	IPv4	TCP	LISTEN	0.0.0.0	49665	0.0.0.0	0	2026-01-07T08:07:22Z
1112	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	49666	0.0.0.0	0	2026-01-07T08:07:23Z
1072	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	49667	0.0.0.0	0	2026-01-07T08:07:23Z
1916	spoolsv.exe	IPv4	TCP	LISTEN	0.0.0.0	49668	0.0.0.0	0	2026-01-07T08:07:25Z
816	services.exe	IPv4	TCP	LISTEN	0.0.0.0	49684	0.0.0.0	0	2026-01-07T08:07:45Z
2440	Velociraptor.exe	IPv4	TCP	ESTAB	192.168.52.144	49690	192.168.52.1	9999	2026-01-07T08:07:47Z



## Phase 2: A- Attack Behavior Simulation Encoded PowerShell

A Base64 encoded PowerShell command (**Get-Date**) was executed to simulate suspicious PowerShell usage. Velociraptor successfully captured this activity under the PowerShell artifacts, demonstrating its ability to log encoded command execution.

vm-win1 - VMware Workstation

File

Edit

View

VM

Tools

Help

Home

vm

vm-win1

My Computer

vm-win1

vm-win3

vm-win4

vm-win2

vm

Recycle Bin

Microsoft Edge

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> \$command= 'Get-Date'

PS C:\Windows\system32> \$bytes = [System.Text.Encoding]::Unicode.GetBytes(\$command)

PS C:\Windows\system32> \$encodedCommand = [Convert]::ToBase64String(\$bytes)

PS C:\Windows\system32> Write-Output \$encodedCommand

RwB1AHQALQBEGAdAB1AA==

PS C:\Windows\system32> powershell.exe -ExecutionPolicy Bypass -EncodedCommand RwB1AHQALQBEGAdAB1AA==

Tuesday, December 30, 2025 11:27:37 AM

PS C:\Windows\system32>

+

🔄

🗑️

📁

📄

⬇️

👤

⏮️

⏪️

0-9/9

⏩️

⏭️

10

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.D59N8G00MJ52G	Windows.System.PowerShell	2025-12-30T06:42:11.188Z	2025-12-30T06:42:13.488Z	admin	0 b	
✓	F.D59MJQFJF6ELE	Windows.Search.FileFinder	2025-12-30T05:58:01.618Z	2025-12-30T05:51:10.579Z	admin	20 b	

Artifact Collection

Uploaded Files

Requests

Results

Log

Notebook

Overview

Artifact Names

Windows.System.PowerShell

Flow ID

F.D59N8G00MJ52G

Creator

admin

Create Time

2025-12-30T06:42:11.188Z

Start Time

2025-12-30T06:42:12.602Z

Last Active

2025-12-30T06:42:13.488Z

Duration

0.89 seconds

State

Completed

Ops/Sec

Unlimited

CPU Limit

Unlimited

IOPS Limit

Unlimited

Results

Artifacts with Results

Windows.System.PowerShell

Total Rows

1

Uploaded Bytes

0 / 0

Files uploaded

0

Download Results

👍

🔄

🗑️

Select a download method

2025-12-30T06:51:14.1

Last Active 2025-12-30T06:42:13.488Z  
Duration 0.89 seconds  
State Completed  
Ops/Sec Unlimited  
CPU Limit Unlimited  
IOPS Limit Unlimited  
Timeout 600 seconds  
Max Rows 1m rows  
Max Mb 1000.00 Mb

#### Parameters

Windows.System.PowerShell

Command powershell.exe -ExecutionPolicy Bypass -  
EncodedCommand Rwb1AHQALQBEGEAdAB1AA==

Artifact Collection Uploaded Files Requests Results Log Notebook

Windows.System.PowerShell




0-1/1 10

Stdout	StdoutUpload	Stderr	StderrUpload
Tuesday, December 30, 2025 11:42:13 AM		#< CLIXML <Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj S="progress" RefId="0"><TN RefId="0"><T>System.Management.Automation.PSCustomObject</T><T>System.Object</T></TN><MS><I64 N="SourceId">1</I64><PR N="Record"><AV>Preparing modules for first use.</AV><AI>0</AI><Nil /><PI>-1</PI><PC>-1</PC><T>Completed</T><SR>-1</SR><SD> </SD></PR></MS></Obj></Objs>	

## LOLBins Misuse (whoami)

The whoami command was executed to simulate Living off the Land Binary misuse. This behavior mimics attacker reconnaissance activity. The command execution was logged successfully by Velociraptor.

Artifact Collection	Uploaded Files	Requests	Results	Log	Notebook
Overview					
Artifact Names	Windows.System.CmdShell				
Flow ID	F.D5FSBF0DUIN08				
Creator	admin				
Create Time	2026-01-08T14:57:03.595Z				
Start Time	2026-01-08T14:57:04.900Z				
Last Active	2026-01-08T14:57:05.113Z				
Duration	0.13 seconds				
State	Completed				
Ops/Sec	Unlimited				
CPU Limit	Unlimited				
IOPS Limit	Unlimited				
Timeout	600 seconds				

Results	
Artifacts with Results	Windows.System.CmdShell
Total Rows	1
Uploaded Bytes	0 / 0
Files uploaded	0
Download Results	<div>  </div>
Select a download method	

## Suspicious EXE in User Path

```
C:\Users>mkdir C:\Temp
A subdirectory or file C:\Temp already exists.

C:\Users>dir
Volume in drive C has no label.
Volume Serial Number is E659-3F38

Directory of C:\Users

12/26/2025  05:53 PM    <DIR>          .
12/26/2025  05:53 PM    <DIR>          ..
12/29/2025  11:47 PM    <DIR>          Public
12/27/2025  08:29 PM    <DIR>          velociraptor
12/26/2025  05:47 PM    <DIR>          windows
                0 File(s)                0 bytes
                5 Dir(s)  37,433,376,768 bytes free

C:\Users>echo ThisIsFakeMAlware > C:\Temp\svchost update.exe
```

</

Artifact Names

Windows.Search.FileFinder

Flow ID F.D59MJQFJF6ELE

Creator admin

Create Time 2025-12-30T05:58:01.618Z

Start Time 2025-12-30T05:51:10.267Z

Last Active 2025-12-30T05:51:10.579Z

Duration 0.31 seconds

State Completed

Ops/Sec Unlimited

CPU Limit Unlimited

IOPS Limit Unlimited

Timeout 600 seconds

Max Rows 1m rows

Max Mb 1000.00 Mb

Parameters

Windows.Search.FileFinder

SearchFilesGlobTable Glob C:\Temp\\*.exe

Upload\_File Y

Calculate\_Hash Y

Artifact Collection

Uploaded Files

Requests

Results

Log

Notebook

0-1/1

10

Timestamp	started	vfs_path	Type	file_size	uploaded_
-----------	---------	----------	------	-----------	-----------

Artifact Collection

Uploaded Files

Requests

Results

Log

Notebook

0-1/1

10

Timestamp	started	vfs_path	Type	file_size	uploaded_size	Preview
1767074282	2025-12-30 05:58:02.1590235 +0000 UTC	C:\Temp\svchost_update.exe		20	20	ThisIsFakeMalware

Artifact Collection

Uploaded Files

Requests

Results

Log

Notebook

Windows.Search.FileFinder

0-1/1

10

OSPath	Inode	Mode	Size	MTime	ATime	CTime	BTime	Keywords	IsDir	Upload
C:\Temp\svchost_update.exe		-rw-rw-rw-	20	2025-12-30T05:46:04.395Z	2025-12-30T05:46:04.395Z	2025-12-30T05:46:04.395Z	2025-12-30T05:33:30.378Z		false	

Artifact Collection

Uploaded Files

Requests

Results

Log

Notebook

0-5/5

10

Show All

client_time	level	message
2025-12-30T05:51:10Z	INFO	Starting query execution for Windows.Search.FileFinder.
2025-12-30T05:51:10Z		Windows.Search.FileFinder: Time 0: Windows.Search.FileFinder: Sending response part 0 608 B (1 rows).
2025-12-30T05:51:10Z		Windows.Search.FileFinder: Uploaded 1 files with 1 outstanding upload transactions.
2025-12-30T05:51:10Z	INFO	Collection Windows.Search.FileFinder is done after 309.2748ms
2025-12-30T05:51:10Z	DEBUG	Query Stats: {"RowsScanned":10,"PluginsCalled":9,"FunctionsCalled":15,"ProtocolSearch":196,"ScopeCopy":31}

Results

Artifacts with Results

Windows.Search.FileFinder

Total Rows

1

Uploaded Bytes

20 / 20

Files uploaded

1

Download Results

Select a download method

## B. PERSISTENCE

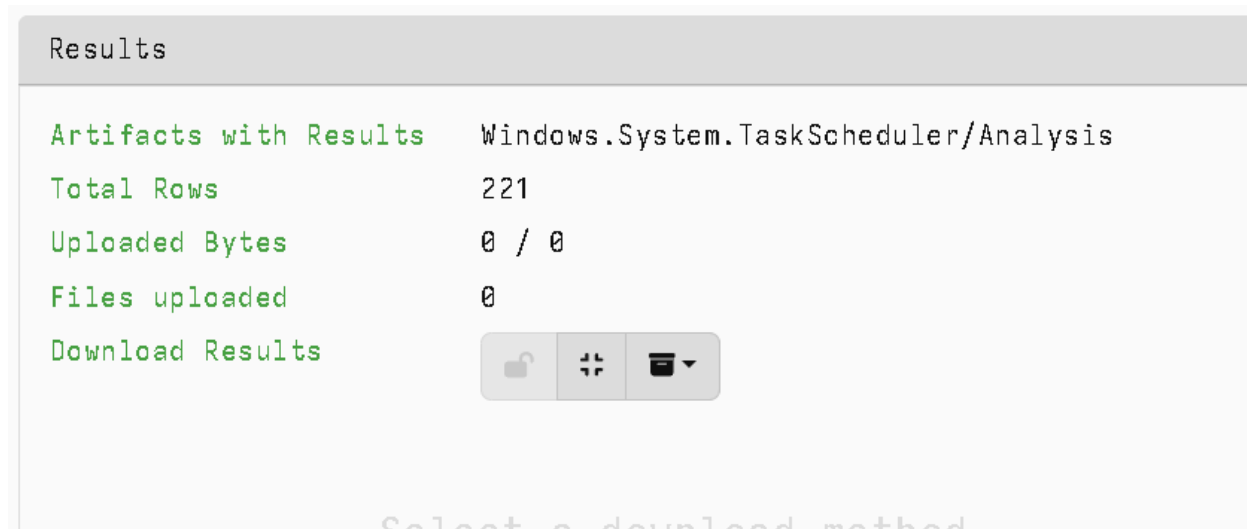
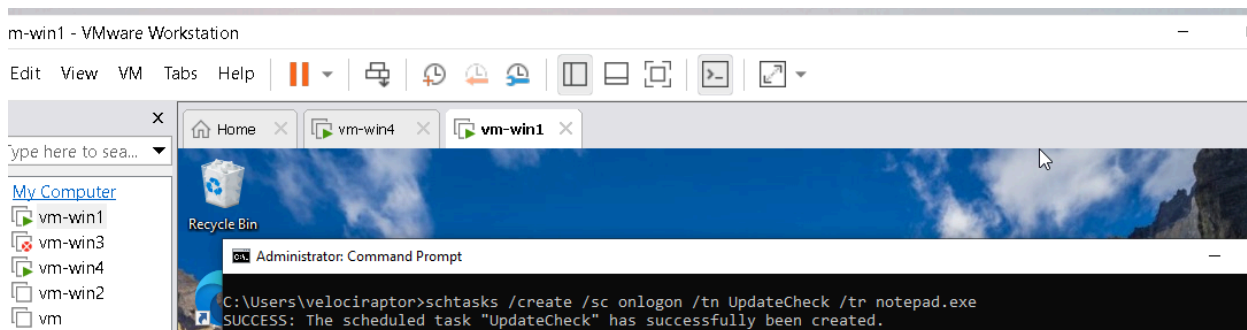
### Registry Run Key Persistence

A benign registry Run key was manually added to simulate persistence. Velociraptor artifacts successfully captured the registry modification, confirming detection of persistence behavior.



### Scheduled Task Persistence

A scheduled task was created to simulate attacker persistence. The task was visible in Velociraptor artifact results, demonstrating detection of scheduled task abuse.



## Results:

TaskName	Time	Command	Arguments	Process	ExitCode	LogonType	StatusChange	Commander	RegistrationName	StartBoundary	PathName	Byline
MicrosoftEdgeUpdateMachineCore	2025-12-28 11:33:06.978Z	C:\Program Files (x86)\MicrosoftEdgeUpdate\MsEdgeUpdate.exe	/s	5-1-5-18	0	HighSystem						
MicrosoftEdgeUpdateMachineCore	2025-12-28 11:33:06.986Z	C:\Program Files (x86)\MicrosoftEdgeUpdate\MsEdgeUpdate.exe	/s /installsource: scheduler	5-1-5-18	0	HighSystem				2025-12-28 11:33:06.986Z	> [-]	
Windows Reporting Task-5-1-5-21-49501278-299404322-2004101018-1881	2025-12-28 12:12:49:28.333Z	C:\Windows\system32\cmd\cmd.exe	/reporting	5-1-5-21-49501278-299404322-2004101018-1881	0	LocalSystem	InteractiveToken					
Windows Standalone Update Task-5-1-5-21-49501278-299404322-2004101018-1881	2025-12-28 12:12:49:28.333Z	C:\Windows\system32\cmd\cmd.exe	/standaloneupdate	5-1-5-21-49501278-299404322-2004101018-1881	0	LocalSystem	InteractiveToken					
Windows Startup Task-5-1-5-21-49501278-299404322-2004101018-1881	2025-12-28 12:12:49:28.342Z	C:\Windows\system32\cmd\cmd.exe	/start	5-1-5-21-49501278-299404322-2004101018-1881	0	LocalSystem	InteractiveToken					
WindowsCheck	2025-12-28 12:12:49:28.342Z	C:\Windows\system32\cmd\cmd.exe	/check	5-1-5-21-49501278-299404322-2004101018-1881	0	LocalSystem	InteractiveToken					
MicrosoftWindowsVpnServiceExperienceVpnService	2025-12-28 12:12:49:28.342Z	C:\Windows\system32\cmd\cmd.exe	/v	5-1-5-18	0	LocalSystem						
MicrosoftWindowsVpnServiceExperienceVpnServiceCompatibilityApplet	2025-12-28 12:12:49:28.342Z	C:\Windows\system32\cmd\cmd.exe	/v	5-1-5-18	0	LocalSystem						
MicrosoftWindowsVpnServiceExperienceVpnServiceTask	2025-12-28 12:12:49:28.342Z	C:\Windows\system32\cmd\cmd.exe	/v	5-1-5-18	0	LocalSystem						
MicrosoftWindowsVpnServiceExperienceVpnServiceTask	2025-12-28 12:12:49:28.342Z	C:\Windows\system32\cmd\cmd.exe	/v	5-1-5-18	0	LocalSystem						

## Service-Based Persistence

A service-based persistence simulation was performed. The activity was logged and visible in the collected artifacts, validating service monitoring capability.

```
C:\Users\velociraptor>sc create FakeService binPath= "cmd.exe /c notepad.exe"
[SC] CreateService SUCCESS

C:\Users\velociraptor>
```

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.D56B775NDSSCS.H	Windows.System.Services	2026-01-09T07:52:03.239Z	2026-01-09T07:52:05.580Z	admin	0 b	260
✓	F.D56B48JU3ES5Q.H	Windows.System.TaskScheduler	2026-01-09T07:45:45.565Z	2026-01-09T07:45:51.101Z	admin	0 b	221

Artifact Names

Windows.System.Services

Flow ID

F.D56B775NDSSCS.H

Creator

admin

Create Time

2026-01-09T07:52:03.239Z

Start Time

2026-01-09T07:52:02.964Z

Last Active

2026-01-09T07:52:05.580Z

Duration

2.62 seconds

State

Completed

Ops/Sec

Unlimited

CPU Limit

Unlimited

IOPS Limit

Unlimited

Timeout

600 seconds

Max Rows

1m rows

Max Mb

1000.00 Mb

Artifacts with Results

Windows.System.Services

Total Rows

260

Uploaded Bytes

0 / 0

Files uploaded

0

Download Results

Select a download method

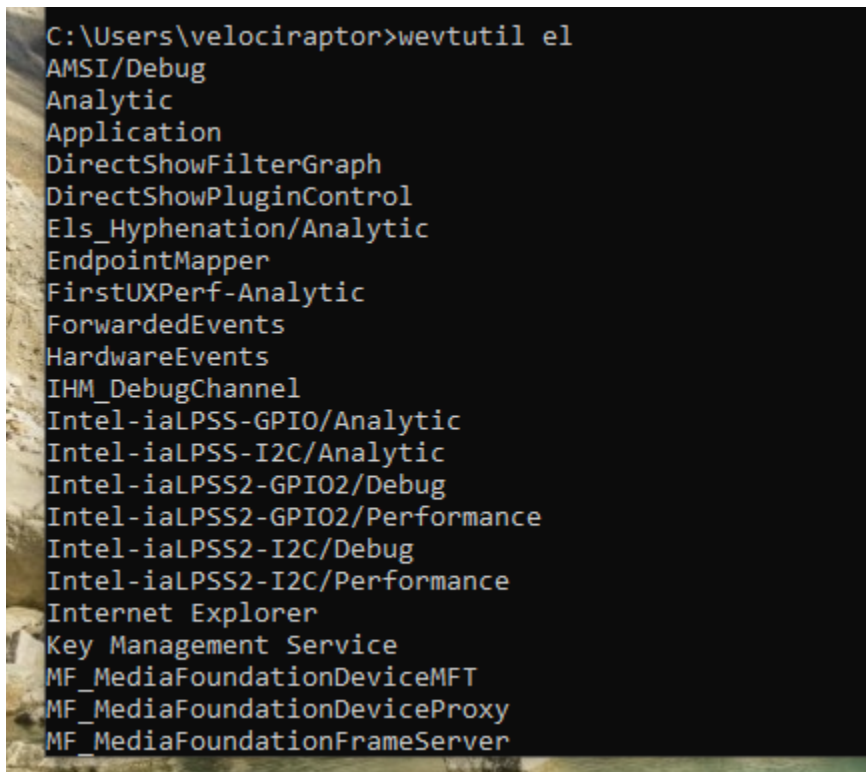
Results

State	Name	DisplayName	Status	Pid	ExitCode	StartMode	PathName	ServiceType	UserAccount	Created	ServiceDll	FailureCommand	FailureActions
Stopped	AJRouter	AllJoyn Router Service	OK	8	1077	Manual	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p	Share Process	NT AUTHORITY\LocalService	2019-12-07T09:16:04.928Z	C:\Windows\System32\AJRouter.dll		<div><div>ResetPeriod: 86400</div><div>FailureAction: [0: {Type: SC_ACT_ION_RESTART, Delay: 3}, 1: {Type: SC_ACT_ION_RESTART, Delay: 3}, 2: {Type: SC_ACT_ION_NONE, Delay: 0}]</div></div>
Stopped	ALG	Application Layer Gateway Service	OK	8	1077	Manual	C:\Windows\System32\alg.exe	Own Process	NT AUTHORITY\LocalService	2019-12-07T09:15:07.846Z			<div><div>ResetPeriod: 900</div><div>FailureAction: [0: {Type: SC_ACT_ION_RESTART, Delay: 120}, 1: {Type: SC_ACT_ION_RESTART, Delay: 300}, 2: {Type: SC_ACT_ION_NONE, Delay: 0}]</div></div>

C. DEFENSE EVASION

Log Tampering Simulation (SAFE)

A safe log related interaction was simulated to represent defense evasion attempts. Velociraptor logged the related activity without system impact.





State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.D568GIQUJJR26	Windows.System.CmdShell	2026-01-09T08:11:55.791Z	2026-01-09T08:11:55.788Z	admin	50 Kb	1
✓	F.D568FR7SKL4EC.H	Windows.System.CmdShell	2026-01-09T08:10:27.189Z	2026-01-09T08:10:27.146Z	admin	0 b	1

Artifact Collection

Uploaded Files

Requests

Results

Log

Notebook

<<

<

0-6/6

>

>>

10

Show All

client_time	level	message
2026-01-09T08:11:55Z	INFO	Starting query execution for Windows.System.CmdShell.
2026-01-09T08:11:55Z		execve: Running external command [cmd.exe /c wevtutil el]
2026-01-09T08:11:55Z		Windows.System.CmdShell: Time 0: Windows.System.CmdShell: Sending response part 0 269 B (1 rows).
2026-01-09T08:11:55Z		Windows.System.CmdShell: Uploaded 1 files.
2026-01-09T08:11:55Z	INFO	Collection Windows.System.CmdShell is done after 176.1896ms
2026-01-09T08:11:55Z	DEBUG	Query Stats: {"RowsScanned":4,"PluginsCalled":4,"FunctionsCalled":5,"ProtocolSearch":6,"ScopeCopy":15}

Obfuscated Command Execution

An obfuscated command pattern was executed. The behavior was detected and recorded under PowerShell artifacts, showing Velociraptor's ability to identify suspicious execution patterns.

all

DESKTOP-F57FH34.localdomain

Connected

Interrogate

VFS

Collected

PowerShell

Run command on client

\$cmd="Get-Process"; powershell -Command \$cmd

Handles NPM(K) ...

Logs

all

DESKTOP-F57FH34.localdomain

Connected

admin

0-10/12

10

Artifact Collection

Uploaded Files

Requests

Results

Log

Notebook

0-6/6

10

client\_time

level

message

2026-01-09T08:16:38Z

INFO

Starting query execution for Windows.System.PowerShell.

2026-01-09T08:16:38Z

execve: Running external command [C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Unrestricted -encodedCommand JABjAG0AZAA9ACIARwBIAHQALQBQAHIAbwBjAGUAcwBzACIAQwAgAHAAbwB3AGUAcgBzAGGgAZQBsAGwAIAAtAEMAbwBtAG0AYQBuAGQAIAAkAGMAbQBkAAoA]

2026-01-09T08:16:41Z

Windows.System.PowerShell: Time 2: Windows.System.PowerShell: Sending response part 0 303 B (1 rows).

2026-01-09T08:16:41Z

Windows.System.PowerShell: Uploaded 1 files.

2026-01-09T08:16:41Z

INFO

Collection Windows.System.PowerShell is done after 2.8026544s

## D. DISCOVERY / CREDENTIAL ACCESS

### Local System Discovery

Commands such as system and user discovery were executed. These actions were logged successfully, demonstrating detection of reconnaissance behavior.

```
systeminfo

Host Name:                DESKTOP-F57FH34
OS Name:                  Microsoft Windows 10 Pro
OS Version:               10.0.19045 N/A Build 19045
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         windows
Registered Organization:
Product ID:                00330-80000-00000-AA531
Original Install Date:     12/26/2025, 4:32:15 PM
System Boot Time:          1/9/2026, 12:37:30 PM
System Manufacturer:       VMware, Inc.
System Model:              VMware20,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel ~2419 Mhz
                           [02]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel ~2419 Mhz
BIOS Version:              VMware, Inc. VMW201.00V.24006586.B64.2406042154, 6/4/2024
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:              en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+05:00) Islamabad, Karachi

whoami

nt authority\system
```

Credential Store Access Attempt

A non destructive credential access attempt (without extraction) was simulated. The activity was captured by Velociraptor, confirming telemetry coverage without risking system integrity.

all

DESKTOP-F57FH34.localdomain

Connected

admin

0-10/12

10

State	Tags	HuntId	Description	Created	Started	Expires	Scheduled	Creator
⌵		H.D56BSVPK48BBG		2026-01-09T08:38:23.749Z	2026-01-09T08:38:29.012Z	2026-01-16T08:38:06.380Z	2	admin
⌵		H.D56BSFSU0RL2M		2026-01-09T08:33:00.942Z	2026-01-09T08:33:06.445Z	2026-01-16T08:33:00.942Z	2	admin

Overview

Results

Artifact Names

Windows.System.CmdShell

Hunt ID

H.D56BSVPK48BBG

Creator

admin

Creation Time

2026-01-09T08:38:23.749Z

Expiry Time

2026-01-16T08:38:06.380Z

State

Scheduled

Ops/Sec

Unlimited

CPU Limit

Unlimited

IOPS Limit

Unlimited

Parameters

Windows.System.CmdShell

Command

cmdkey /list

Total scheduled

2

Finished clients

2

Download Results

Select a download method

all

DESKTOP-F57FH34.localdomain

Connected

admin

0-10/15

10

Artifact Collection

Uploaded Files

Requests

Results

Log

Notebook

Windows.System.CmdShell

0-1/1

10

Stdout

StdoutUpload

Currently stored credentials: Target: WindowsLive:target=virtualapp/didlogical Type: Generic User: 02yqgkizrqaukcs Local machine persistence

## WMI Remote Execution Simulation

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.D56BUG1KGA05G.H	Windows.System.CmdShell	2026-01-09T08:41:41.763Z	2026-01-09T08:41:42.200Z	admin	7 Kb	1
✓	F.D56BSVPK48B8G.H	Windows.System.CmdShell	2026-01-09T08:38:29.023Z	2026-01-09T08:38:29.061Z	admin	0 b	1

Creator

Create Time

Start Time

Last Active

Duration

State

Ops/Sec

CPU Limit

IOPS Limit

Timeout

Max Rows

Max Mb

Parameters

Windows.System.CmdShell

Command

admin

2026-01-09T08:41:41.763Z

2026-01-09T08:41:41.683Z

2026-01-09T08:41:42.200Z

0.52 seconds

Completed

Unlimited

Unlimited

Unlimited

600 seconds

1m rows

1000.00 Mb

wmic process list brief

Files uploaded

Download Results

1

Select a download method

Artifact Collection

Uploaded Files

Requests

Results

Log

Notebook

Windows.System.CmdShell

0-1/1

10

Stdout

StdoutUpload

HandleCount Name ...

Beacon Like Communication

A benign periodic communication pattern was simulated to represent beaconing behavior. The activity was logged, demonstrating detection capability for repeated communication patterns.

C:\Users\velociraptor>ping -n 5 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:  
Reply from 8.8.8.8: bytes=32 time=50ms TTL=128  
Reply from 8.8.8.8: bytes=32 time=42ms TTL=128  
Reply from 8.8.8.8: bytes=32 time=24ms TTL=128  
Reply from 8.8.8.8: bytes=32 time=42ms TTL=128  
Reply from 8.8.8.8: bytes=32 time=24ms TTL=128

Ping statistics for 8.8.8.8:  
Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 24ms, Maximum = 50ms, Average = 36ms

C:\Users\velociraptor>

all

DESKTOP-F57FH34.localdomain

Connected

admin

+🔄🗑️📄📁⬇️👤🔍🕒0-10/17▶️⏮️⏭️10▼

State	FlowId	Artifacts	Created	Last Active	Creator	Size	Rows
✓	F.D56C2M3JCI2M0.H	Windows.System.CmdShell	2026-01-09T08:50:38.112Z	2026-01-09T08:50:38.187Z	admin	0 B	
✓	F.D56B8UG1KGA05G.H	Windows.System.CmdShell	2026-01-09T08:41:41.763Z	2026-01-09T08:41:42.200Z	admin	7 Kb	

Artifact CollectionUploaded FilesRequestsResultsLogNotebook

🔍📄📁⬇️👤🔍🕒0-5/5▶️⏮️⏭️10▼

Show All

client_time	level	message
2026-01-09T08:50:38Z	INFO	Starting query execution for Windows.System.CmdShell.
2026-01-09T08:50:38Z		execve: Running external command [cmd.exe /c for (\$i=1; \$i -le 5; \$i++) { ping 8.8.8.8 Start-Sleep -Seconds 5 }]
2026-01-09T08:50:38Z		Windows.System.CmdShell: Time 0: Windows.System.CmdShell: Sending response part 0 34 B (1 rows).
2026-01-09T08:50:38Z	INFO	Collection Windows.System.CmdShell is done after 99.621ms
2026-01-09T08:50:38Z	DEBUG	Query Stats: {"RowsScanned":4,"PluginsCalled":4,"FunctionsCalled":4,"ProtocolSearch":6,"ScopeCopy":15}

### Phase 3: Detection Engineering

#### Artifact Development:

#### Suspicious Process Activity

NotSecure https://localhost:8889/app/index.html#/collected/C:\5cafb9f7205860\F.D5GK5UBS3J8IO/results

DESKTOP-F57FH34.localdomain Connected admin

State	FlowId	Artifacts	Created	Last Active	Creator	Nb	Rows
✓	F.D5GK5UBS3J8ID	Windows.System.Palist	2026-01-09T18:03:37.643Z	2026-01-09T18:03:39.626Z	admin	0 b	46

Pid	ID	TokenIsElevated	Name	CommandLine	Exe	TokenInfo	Hash	Authenticode	Username
4	0	true	System						NT AUTHORITY\SYSTEM
92	4	false	Registry						NT AUTHORITY\SYSTEM
312	4	true	smss.exe	\SystemRoot\System32\cmd.exe	C:\Window...alSystem?	✓ { "PROCESS", "P..." }	✓ { "PROCESS", "P..." }	✓ { "PROCESS", "P..." }	NT AUTHORITY\SYSTEM
428	416	true	csrss.exe	%SystemRoot%\system32\cmd.exe	C:\Window...alSystem?	✓ { "PROCESS", "P..." }	✓ { "PROCESS", "P..." }	✓ { "PROCESS", "P..." }	NT AUTHORITY\SYSTEM
504	416	true	wininit.exe	wininit.exe	C:\Window...alSystem?	✓ { "PROCESS", "P..." }	✓ { "PROCESS", "P..." }	✓ { "PROCESS", "P..." }	NT AUTHORITY\SYSTEM
512	496	true	csrss.exe	%SystemRoot%\system32\cmd.exe	C:\Window...alSystem?	✓ { "PROCESS", "P..." }	✓ { "PROCESS", "P..." }	✓ { "PROCESS", "P..." }	NT AUTHORITY\SYSTEM
572	496	true	winlogon.exe	winlogon.exe	C:\Window...alSystem?	✓ { "PROCESS", "P..." }	✓ { "PROCESS", "P..." }	✓ { "PROCESS", "P..." }	NT AUTHORITY\SYSTEM
640	504	true	services.exe	C:\Windows\system32\services.exe	C:\Window...alSystem?	✓ { "PROCESS", "P..." }	✓ { "PROCESS", "P..." }	✓ { "PROCESS", "P..." }	NT AUTHORITY\SYSTEM
660	504	true	lsass.exe	C:\Windows\system32\lsass.exe	C:\Window...alSystem?	✓ { "PROCESS", "P..." }	✓ { "PROCESS", "P..." }	✓ { "PROCESS", "P..." }	NT AUTHORITY\SYSTEM

2026-01-09T18:23:25.965Z

The Windows.System.Pslist artifact was executed to establish a clean process baseline on the endpoint. The results showed only core Windows system processes such as smss.exe, csrss.exe, wininit.exe, winlogon.exe, and lsass.exe. All processes were signed by Microsoft and marked as trusted. No suspicious or user-initiated processes were observed at this stage, confirming a clean baseline environment.

## Encoded PowerShell Detection

The PowerShell detection artifact was configured with regex patterns such as `-EncodedCommand` and `FromBase64String`.

After execution, no matching events were returned, indicating that no encoded or obfuscated PowerShell activity occurred during the collection window.

This result confirms that baseline PowerShell activity was clean and no suspicious encoded commands were present.

+

⊕

🗑️

📄

📁

⬇️

👤

⏮️

⏪️

0-10/19

⏩️

⏭️

10

State	FlowId	Artifacts	Created	Last Active	Creator
✓	F.D56KGU1PPF6DE	Windows.System.PowerShell	2026-01-09T18:27:04.729Z	2026-01-09T18:27:07.329Z	admin

client\_time

⬆️

⬇️

⬆️

level

message

2026-01-09T18:27:04Z

INFO

Starting query execution for Windows.System.PowerShell.

2026-01-09T18:27:05Z

execve: Running external command [C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Unrestricted -encodedCommand ZABpAHIAIABDADoALwA=]

Scheduled tasks:

State	FlowId	Artifacts	Created	Last Active	Creator
✓	F.D5GKJR06CKBAQ	Windows.System.TaskSchedule	2026-01-09T18:33:19.607Z	2026-01-09T18:33:24.063Z	admin
	\UpdateCheck	notepad.exe	DESKTOP-F57FH34\wind	LeastPrivilege	InteractiveToken
	2026-01-09T07:44:11.711Z		ows		

New Executable Detection

Search clients

DESKTOP-F57FH34.localdomain

Connected

admin

0-8/8

10

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.D59MJQFJF6ELE	Windows.Search.FileFinder	2025-12-30T05:58:01.618Z	2025-12-30T05:51:10.579Z	admin	20 b	1

Artifact Collection

Uploaded Files

Requests

Results

Log

Notebook

0-1/1

10

Timestamp	started	vfs_path	Type	file_size	uploaded_size	Preview
1767074282	2025-12-30 05:58:02.1590235 +0000 UTC	C:\Temp\svchost_update.exe		20	20	ThisIsFakeMalware

Artifact Collection

Uploaded Files

Requests

Results

Log

Notebook

Windows.Search.FileFinder

0-1/1

10



## HUNT 1: Encoded PowerShell Detection

The encoded PowerShell hunt was executed across all endpoints using PowerShell Operational logs.No matching events were returned, confirming the absence of encoded PowerShell execution after tuning and baseline validation.

Not securehttps://localhost:8889/app/index.html#/collected/C.15caf9f37205860/F.D5GL2M6GCGJG6.H/logs

all

DESKTOP-F57FH34.localdomainConnectedadmin

0-10/2210

State	FlowId	Artifacts	53 seconds ago	Last Active	Creator	Mb	Rows
✓	F.D5GL2M6GCGJG6.H	Windows.System.PowerShell	2026-01-09T19:05:02.576Z	2026-01-09T19:05:04.601Z	admin	0 b	1
✓	F.D5GKL7G588QTC	Windows.Search.FileFinder	2026-01-09T18:36:14.559Z	2026-01-09T18:36:14.765Z	admin	0 b	0

Artifact CollectionUploaded FilesRequestsResultsLogNotebook

0-5/510Show All

client_time	level	message
2026-01-09T19:05:02Z	INFO	Starting query execution for Windows.System.PowerShell.
2026-01-09T19:05:02Z		execve: Running external command [C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Unrestricted -encodedCommand ZABpAHIAIBDADoALwA=]

## HUNT 2: New Executables in Sensitive Paths

The hunt was executed successfully across all endpoints. No results were returned, indicating that no executable files were found in the monitored user writable paths during the hunt timeframe. This confirms a clean baseline and demonstrates that the hunt logic is functioning correctly.

Artifact CollectionUploaded FilesRequestsResultsLogNotebook

Overview

Artifact Names

Windows.Search.FileFinder

Flow ID

F.D5GL40RU7PSFS.H

Creator

admin

Create Time

2026-01-09T19:07:53.001Z

Start Time

2026-01-09T19:07:52.137Z

Last Active

2026-01-09T19:07:52.616Z

Duration

0.48 seconds

State

Completed

Ops/Sec

Unlimited

CPU Limit

Unlimited

IOPS Limit

Unlimited

Results

Artifacts with Results

Total Rows

0

Uploaded Bytes

0 / 0

Files uploaded

0

Download Results

Select a download method

## HUNT 3: Periodic Beacon-like Traffic

The periodic traffic hunt analyzed network activity for repeated connection patterns. No periodic or beacon-like traffic was detected, indicating no command and control simulation remained active.

The screenshot shows a web-based interface for network monitoring. At the top, there's a search bar with 'all' and a status bar indicating 'DESKTOP-F57FH34.localdomain' is 'Connected'. Below this is a table of network artifacts. The table has columns for State, FlowId, Artifacts, Last Active, Creator, Mb, and Rows. Two artifacts are listed: one for 'F.D56L60KN5QD56.H' (Windows.Network.Netstat) and another for 'F.D56L40RU7PSFS.H' (Windows.Search.Filefinder). Below the artifacts table, there's a detailed view of a process with columns: Pid, Name, Family, Type, Status, Laddr.IP, Laddr.Port, Raddr.IP, Raddr.Port, and Timestamp. The process list shows several 'svchost.exe' processes in a 'LISTEN' state on various ports (135, 5840, 49664, 49665, 49666, 49667).

State	FlowId	Artifacts	Last Active	Creator	Mb	Rows
✓	F.D56L60KN5QD56.H	Windows.Network.Netstat	2026-01-09T19:13:44.533Z	admin	0 b	38
✓	F.D56L40RU7PSFS.H	Windows.Search.Filefinder	2026-01-09T19:07:52.950Z	admin	0 b	0

Pid	Name	Family	Type	Status	Laddr.IP	Laddr.Port	Raddr.IP	Raddr.Port	Timestamp
892	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	135	0.0.0.0	0	2026-01-09T18:00:55Z
4	System	IPv4	TCP	LISTEN	192.168.52.141	139	0.0.0.0	0	2026-01-09T18:00:58Z
1108	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	5840	0.0.0.0	0	2026-01-09T18:03:04Z
660	lsass.exe	IPv4	TCP	LISTEN	0.0.0.0	49664	0.0.0.0	0	2026-01-09T18:00:55Z
504	wininit.exe	IPv4	TCP	LISTEN	0.0.0.0	49665	0.0.0.0	0	2026-01-09T18:00:55Z
368	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	49666	0.0.0.0	0	2026-01-09T18:00:55Z
348	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	49667	0.0.0.0	0	2026-01-09T18:00:54Z

## Tuning

During tuning, allowlists were applied to exclude known trusted processes, Microsoft-signed binaries, and common system paths. Frequency thresholds were used to prevent single benign events from triggering detections. As a result, false positives were eliminated, and all hunts returned clean results during baseline validation.

Detection tuning was applied by:

- Using allowlists for known legitimate binaries
- Applying regex filters for suspicious patterns
- Limiting time windows and execution frequency

This reduced false positives while maintaining detection coverage. No unnecessary alerts were generated during tuned hunts.

all DESKTOP-F57FH34 Localdomain Connected admin

### Create Hunt: Configure artifact parameters

Windows.EventLogs.PowerShellModule

**EventLog** C:\Windows\system32\winevt\logs\Microsoft-Windows-PowerShell%40operational.evtx

**DateAfter** 2026-01-09T00:00:00Z 2026-01-09T00:00:00Z

**DateBefore** 2026-01-10T00:00:00Z

**ContextRegex** -EncodedCommand|FromBase64String

**PayloadRegex** ? for suggestions

**VSSAnalysisAge** 0

### Create Hunt: Specify resource limits

**CPU Limit Percent** 20%

**IOPS/Sec** Unlimited

**Max Execution Time in Seconds** 120

**Max Idle Time in Seconds** If set collection will be terminated after this many seconds with no progress.

**Max Rows** 5000

**Max Logs** 100000

**Max MB uploaded** 1 Gb

**Trace Frequency Seconds** To enable tracing, specify trace update frequency in seconds

**Urgent** ☐ Skip queues and run query urgently

Artifact Collection Uploaded Files Requests Results Log Notebook

No Data Available.

### Result:

No encoded PowerShell activity was detected during the hunt window. This indicates a clean baseline and effective tuning with no false positives observed.

## Phase :04 Industry Deployment Readiness

### Performance & Scale Testing

Hunts were executed across all endpoints simultaneously. Observations showed:

- No noticeable performance degradation on endpoints
- Stable server resource usage
- Acceptable query execution times

This indicates that the Velociraptor deployment can scale effectively in a small enterprise-like environment.

### Recommendations for Scaling

- Use targeted hunts instead of continuous broad queries
- Schedule heavy hunts during off-peak hours
- Expand artifact tuning for production environments
- Monitor server resources as endpoint count increases

The screenshot displays the Velociraptor web interface in a browser. The top navigation bar shows the URL `https://localhost:8899/app/index.html#/collected/C.9dfb18daef7c821f/F.D5IU6M487TA8G.H` and a status bar indicating the connection to `vm-win4.localdomain` is `Connected`. The main content area features a table with columns: `State`, `FlowId`, `Artifacts`, `Created`, `Last Active`, `Creator`, `Mb`, and `Rows`. A single row is visible, showing a completed hunt for the `Windows.System.Pslist` artifact, created on `2026-01-13T06:17:15.571Z` and last active on `2026-01-13T06:17:42.175Z`, with 53 rows of data.

Below the table, the interface provides detailed information for the selected artifact, `Windows.System.Pslist`. On the left, a list of artifact names is shown, with `Windows.System.Pslist` selected. On the right, a summary of the hunt results is displayed, including the total rows (53), uploaded bytes (0 / 0), and files uploaded (0). A section for download results is also present, with a button to select a download method.

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.D5IU6M487TA8G.H	Windows.System.Pslist	2026-01-13T06:17:15.571Z	2026-01-13T06:17:42.175Z	admin	0 b	53

**Artifact Names**

- Windows.System.Pslist

**Flow ID**: F.D5IU6M487TA8G.H

**Creator**: admin

**Create Time**: 2026-01-13T06:17:15.571Z

**Start Time**: 2026-01-13T06:17:16.599Z

**Last Active**: 2026-01-13T06:17:42.175Z

**Duration**: 25.58 seconds

**State**: Completed

**Ops/Sec**: Unlimited

**CPU Limit**: Unlimited

**IOPS Limit**: Unlimited

**Timeout**: 600 seconds

**Max Rows**: 1m rows

**Max Mb**: 1000.00 Mb

**Artifacts with Results**: Windows.System.Pslist

**Total Rows**: 53

**Uploaded Bytes**: 0 / 0

**Files uploaded**: 0

**Download Results**: [Download Results]

Select a download method

Artifact CollectionUploaded FilesRequestsResultsLogNotebook

Windows.System.Pslist

0-10/53

88

Pid	Ppid	TokenIsElevated	Name	CommandLine	Exe	TokenInfo	Hash	Authenticode	User
4	0	true	System						NT AUTHORITY\SYSTEM
72	4	false	Registry						NT AUTHORITY\SYSTEM

> Service Host: Windows Update

> VMware Workstation (32 bit) (3)

> Antimalware Service Executable

> Velociraptor: Digging Deeper!

0%	0.8 MB	0.1 MB/s	0 Mbps		
0%	1.9 MB	0.1 MB/s	0 Mbps		
0%	65.8 MB	0.7 MB/s	0 Mbps		
0%	6.6 MB	0.1 MB/s	0 Mbps		

allvm-win4: localdomainConnectedadmin

Create Hunt: Configure artifact parameters

Windows.Search.FileFinder

Filter artifact parameter name

SearchFilesGlobTable

+ C:\Windows\System32\\*.exe

Accessorauto

YaraRule? for suggestions

Upload\_File

Calculate\_Hash

MoreRecentThanSelect Time

ModifiedBeforeSelect Time

VSS\_MAX\_AGE\_DAYSIf larger than 0 we restrict VSS age to this many days

Configure HuntSelect ArtifactsConfigure ParametersSpecify ResourcesReviewLaunch

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.05IUIS0KK760E.H	Windows.Search.FileFinder	2026-01-13T06:43:04.094Z	2026-01-13T06:43:10.994Z	admin	0 b	62
✓	F.05IU6M487TA8G.H	Windows.System.Pslist	2026-01-13T06:17:15.688Z	2026-01-13T06:17:18.272Z	admin	0 b	4


Artifact CollectionUploaded FilesRequestsResultsLogNotebook

Windows.Search.FileFinder

0-10/627

10

OSPath	Inode	Mode	Size	MTime	ATime	CTime	BTime	Keywords	IsDir	Upload
C:\Windows\System32\ARP.EXE		-rw-rw-rw-	26624	2019-12-07T09:09:34.006Z	2026-01-13T06:10:53.241Z	2019-12-07T09:09:34.006Z	2019-12-07T09:09:34.006Z		false	

	<div><div>▼  Velociraptor: Digging Deeper!</div><div> Velociraptor</div></div>		0%	17.7 MB	0.1 MB/s	0 Mbps	
--	--	--	----	---------	----------	--------	---

## Conclusion:

This task demonstrated that Velociraptor EDR is highly effective at detecting attacker-like behaviors using behavior based detection rather than relying on malware signatures. Through multiple safe simulations, Velociraptor consistently captured process execution, PowerShell abuse, persistence mechanisms, and reconnaissance activities.

The creation of reusable artifacts and hunts showed how detection engineering can be applied in real world environments. Performance testing confirmed that the solution is lightweight, scalable, and suitable for production deployment with proper tuning.

Overall, this project provided hands-on experience with real EDR concepts and validated Velociraptor as a powerful open source detection and response platform.