

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.



A screenshot of the Velociraptor EDR GUI interface. The top bar shows the title 'Velociraptor EDR' and the subtitle 'Advanced Detection Validation'. Below the title, there is a search bar with the placeholder 'all' and a dropdown menu set to 'Connected'. On the right side of the top bar, there are buttons for 'admin' and a user icon. The main area is a table with the following columns: Client ID, Hostname, FQDN, OS Version, and Labels. There are five rows of data, each representing a connected endpoint. The first four endpoints are physical Windows 10 Pro 22H2 machines with hostnames DESKTOP-F57FH34 and FQDNs DESKTOP-F57FH34.localdomain. The fifth endpoint is a virtual machine named vm-win02 with a hostname of vm-win02 and a FQDN of vm-win02.localdomain. All endpoints are listed as Microsoft Windows 10 Pro 22H2 and have a green status indicator.

Client ID	Hostname	FQDN	OS Version	Labels
C.15caf9f37205860	DESKTOP-F57FH34	DESKTOP-F57FH34.localdomain	Microsoft Windows 10 Pro 22H2	
C.575966f7e8113738	DESKTOP-F57FH34	DESKTOP-F57FH34.localdomain	Microsoft Windows 10 Pro 22H2	
C.7894b0649d098b2e	vm-win02	vm-win02.localdomain	Microsoft Windows 10 Pro 22H2	
C.9dfb18daaf7c821f	DESKTOP-F57FH34	DESKTOP-F57FH34.localdomain	Microsoft Windows 10 Pro 22H2	

Phase1:

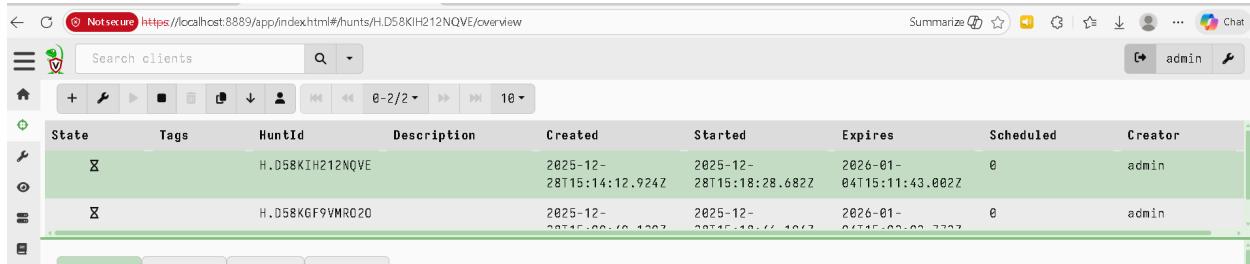
Artifact Execution Works

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 interface with the URL <https://localhost:8889/app/index.html#/hunts/H.D58KIH212NQVE/overview>. The page displays a table of artifact hunts. There are two entries in the table:

State	Tags	HuntId	Description	Created	Started	Expires	Scheduled	Creator
✗		H.D58KIH212NQVE		2025-12-28T15:14:12.924Z	2025-12-28T15:18:28.682Z	2026-01-04T15:11:43.802Z	0	admin
✗		H.D58KGF9VMR020		2025-12-28T15:14:12.924Z	2025-12-28T15:18:28.682Z	2026-01-04T15:11:43.802Z	0	admin

all

0-2/2 10

State	Tags	HuntId	Description	Created	Started	Expires	Schedule
X		H.D58KIH212NQVE		2025-12-28T15:14:12.924Z	2025-12-28T15:18:28.682Z	2026-01-04T15:11:43.002Z	4
X		H.D58KGF9VMR020		2025-12-28T15:14:12.923Z	2025-12-28T15:18:28.682Z	2026-01-04T15:11:43.002Z	4

Overview Requests Clients Notebook

Overview

Artifact Names [Windows.System.CmdShell](#)

Hunt ID H.D58KIH212NQVE

Creator admin

Creation Time 2025-12-28T15:14:12.924Z

Expiry Time 2026-01-04T15:11:43.002Z

State Scheduled

Ops/Sec Unlimited

CPU Limit Unlimited

IOPS Limit Unlimited

Parameters

Windows.System.CmdShell

Results

Total scheduled 4

Finished clients 4

Download Results

Available Downloads

[H.D58KIH212NQVE](#)

Uncompressed 1 Kb

Compressed 1 Kb

Container Files 3

Started 2025-12-28T15:16:15Z

Overview Requests Clients Notebook

Overview

Artifact Names [Windows.System.CmdShell](#)

Hunt ID H.D58KIH212NQVE

Creator admin

Creation Time 2025-12-28T15:14:12.924Z

Expiry Time 2026-01-04T15:11:43.002Z

State Scheduled

Ops/Sec Unlimited

CPU Limit Unlimited

IOPS Limit Unlimited

Parameters

Windows.System.CmdShell

Command whoami

ClientId	Hostname	FlowId	StartedTime	State	Duration	TotalBytes	TotalRows	88
C.9dfb18daaf7c821f	vm-win4	F.D58KIH212NQVE.H	2025-12-28T15:18:28.730Z	Completed	6	0	1	
C.575966f7e8113738	DESKTOP-F57FH34	F.D58KIH212NQVE.H	2025-12-28T15:18:29.788Z	Completed	3	0	1	
C.15cafb9f37205868	DESKTOP-F57FH34	F.D58KIH212NQVE.H	2025-12-28T15:18:28.509Z	Completed	0	0	1	
C.7894b0649d098b2e	vm-win02	F.D58KIH212NQVE.H	2025-12-28T15:18:29.582Z	Completed	1	0	1	

3.1 Baseline: Running Processes

`Windows.System.Pslist`

Baseline: Running Processes

The `Windows.System.Pslist` artifact was executed to establish a clean process baseline. The results showed only legitimate Windows system processes such as `smss.exe`, `csrss.exe`, `wininit.exe`, `winlogon.exe`, `services.exe`, `lsass.exe`, and `svchost.exe`.

All processes were digitally signed by Microsoft and marked as trusted. No unknown, suspicious, or user initiated processes were observed, confirming that the environment was clean at baseline.

State	Tags	HuntId	Description	Created	Started	Expires	Scheduled	Creator
X		H.D5F1DG2T2CM4C		2026-01-07T08:18:08.078Z	2026-01-07T08:18:35.838Z	2026-01-14T08:17:20.382Z	2	admin

Overview

Artifact Names Windows.System.Pslist

Hunt ID H.D5F1DG2T2CM4C

Creator admin

Creation Time 2026-01-07T08:18:08.078Z

Expiry Time 2026-01-14T08:17:20.382Z

State Scheduled

Ops/Sec Unlimited

CPU Limit Unlimited

IOPS Limit Unlimited

Parameters

Windows.System.Pslist

Results

Total scheduled: 2

Finished clients: 2

Download Results

Select a download method

Overview	Requests	Clients	Notebook					
Filter:								
List View								
ClientId	Hostname	FlowId	StartTime	State	Duration	TotalBytes	TotalRows	...
C.15cafb9f37205860	DESKTOP-F57FH34	F.D5F1DG2T2CM4C.H	2026-01-07T08:18:38.750Z	Completed	12	0	6	
C.9dfb18daef7c821f	vm-win4	F.D5F1DG2T2CM4C.H	2026-01-07T08:18:39.155Z	Completed	85	0	82	

Result:

3.2 Baseline: Scheduled Tasks

Scheduled tasks were reviewed to understand normal system behavior. Only standard Windows maintenance and system tasks were present, with no evidence of unauthorized or suspicious scheduled persistence.

all		Search	vm-win4.localdomain		Connected	admin		
			0-5/5		10			
State	Tags	HuntId	Description	Created	Started	Expires	Scheduled	Creator
✗		H.D5F1PDHIV0KP8		2026-01-07T08:43:34.600Z	2026-01-07T08:44:17.154Z	2026-01-14T08:42:18.719Z	2	admin

Overview Requests Clients Notebook

Overview

Artifact Names	Windows.System.TaskScheduler
Hunt ID	H.D5F1PDHIV0KP8
Creator	admin
Creation Time	2026-01-07T08:43:34.600Z
Expiry Time	2026-01-14T08:42:18.719Z
State	Scheduled
Ops/Sec	Unlimited
CPU Limit	Unlimited
IOPS Limit	Unlimited

Parameters

```
Windows.System.TaskScheduler
```

Overview Requests Clients Notebook

Client Id: C.15cafb9f37205866 Hostname: DESKTOP-F57FH34 FlowId: F.D5F1PDHIV0KP8. StartedTime: 2026-01-07T08:44:17.804Z State: Completed Duration: 4 TotalBytes: 0 TotalRows: 22

Client Id: C.9dfb18daaf7c821f Hostname: vm-win4 FlowId: F.D5F1PDHIV0KP8. StartedTime: 2026-01-07T08:44:16.788Z State: Completed Duration: 3 TotalBytes: 0 TotalRows: 209

Results:

TaskName	StartTime	Command	Arguments	UserId	RunLevel	LogonType	StateChange	Commander	RegistrationTime	StartBoundary	Authenticated
\MicrosoftEdgeUpdateTaskMachine	2025-12-26T11:33:06.876Z	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	/c	S-1-5-18	HighestAvailable	0				2025-12-26T04:08:06Z	> {...}
\MicrosoftEdgeUpdateTaskMachine	2025-12-26T11:33:06.886Z	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	/use /installsource	S-1-5-18	HighestAvailable	0				2025-12-26T03:38:06Z	> {...}
\OneDriveReportTask-S-1-5-21-4892012788-2994514832-2084181518-1001	2025-12-26T12:49:20.339Z	C:\Windows\system32\config\systemprofile\appData\local\Microsoft\OneDrive\OneDriveStandaloneUpdate.exe	/reporting	S-1-5-21-4892012788-2994514832-2084181518-1001	LeastPrivilege	InteractiveToken					88
\OneDriveStandaloneUpdateTask-S-1-5-21-4892012788-2994514832-2084181518-1001	2025-12-26T12:49:20.382Z	C:\Windows\system32\config\systemprofile\appData\local\Microsoft\OneDrive\OneDriveStandaloneUpdate.exe	/reporting	S-1-5-21-4892012788-2994514832-2084181518-1001	LeastPrivilege	InteractiveToken					88
\OneDriveStartupTask-S-1-5-21-4892012788-2994514832-2084181518-1001	2025-12-26T12:49:20.349Z	C:\Users\windws\AppData\Local\Microsoft\onedrive\25.224.1116.8003\OneDriveLauncher.exe	/startInstances	S-1-5-21-4892012788-2994514832-2084181518-1001	LeastPrivilege	InteractiveToken					88

74°F Sunny 2:17 PM 1/7/2026

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

Results

Total scheduled	2
Finished clients	2
Download Results	Select a download method

vm-win4.localdomain Connected

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

EventTime	Computer	EventID	SecurityID	Path	ScriptBlockId	ScriptBlockText	Message	EventRecordID	Level	Opcode
2026-01-07T08:35:38Z	vm-win4	4184	S-1-5-21-4992012788-	C:\Windows\TEMP\SDIAG_9833-fd17ee452dbc	6b9c6f29-7be2-48d5-c9318844-2994514832-2084181518-1001	# Copyright © 2008, Microsoft Corporation. All rights reserved. #Common utility function Import-LocalizedData -BindingVariable \$CL_UtilityLocalizationString -FileName CL_LocalizationData #Function to get user troubleshooting history function Get-UserTSHistoryPath { AdminTSHistoryPath { return "\$env:localappdata\Microsoft\Windows\PowerShell\Profile\\$CL_UtilityLocalizationString -FileName CL_LocalizationData #Function to get user troubleshooting history function Get-UserReportPath { AdminTSHistoryPath { return "\$env:localappdata\Microsoft\Windows\WER\reportQueue" } #Function to get system report folder path function Get-MachineReportPath { AdminTSHistoryPath { return "\$env>AllUsersProfile	Creating Scriptblock	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

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.D5F1V9A1Q0E68.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
<div style="display: flex; justify-content: space-between;"> <div style="flex: 1;"> <p>Overview</p> <p>Artifact Names: Windows.Network.Netstat</p> <p>Flow ID: F.D5F2H63IKHPVA.H</p> <p>Creator: admin</p> <p>Create Time: 2026-01-07T09:34:50.726Z</p> <p>Start Time: 2026-01-07T09:34:50.182Z</p> <p>Last Active: 2026-01-07T09:34:50.310Z</p> <p>Duration: 0.13 seconds</p> <p>State: Completed</p> <p>Ops/Sec: Unlimited</p> <p>CPU Limit: Unlimited</p> <p>IOPS Limit: Unlimited</p> <p>Timeout: 600 seconds</p> </div> <div style="flex: 1;"> <p>Results</p> <p>Artifacts with Results: Windows.Network.Netstat</p> <p>Total Rows: 47</p> <p>Uploaded Bytes: 0 / 0</p> <p>Files uploaded: 0</p> <p>Download Results: CSV JSON XML</p> <p>Select a download method</p> </div> </div>					

2026-01-07T09:41:18.039Z

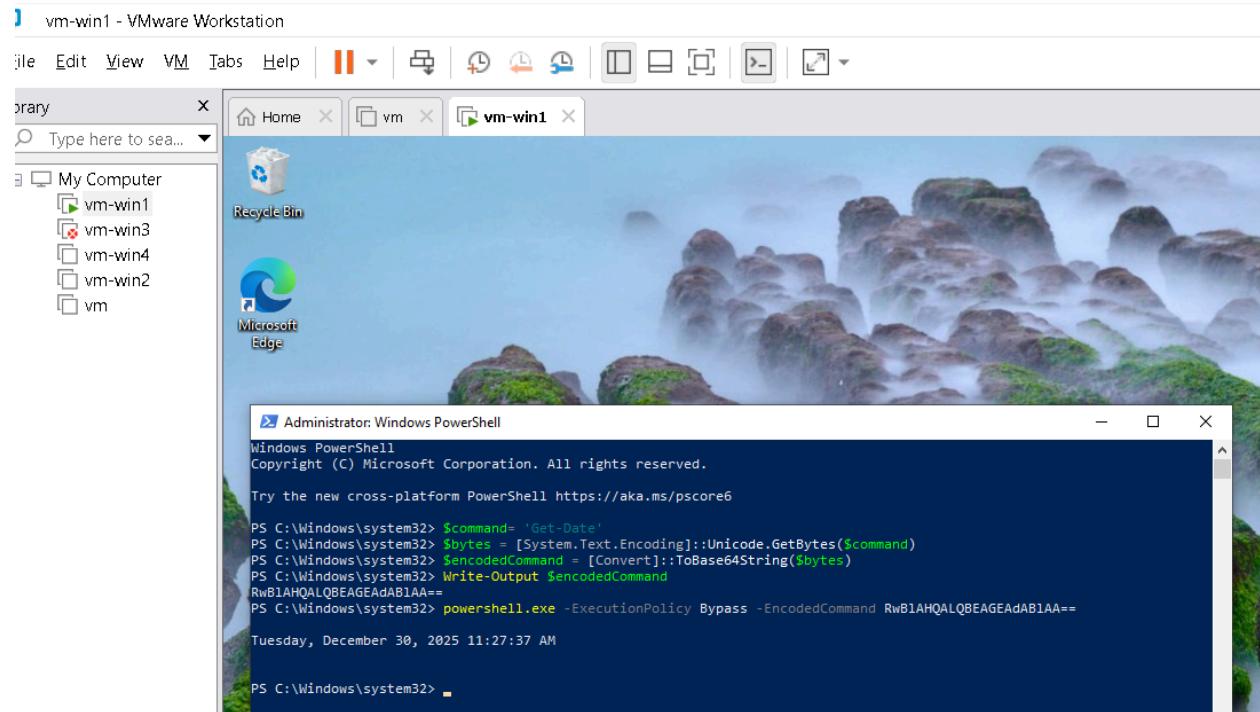
Pid	Name	Family	Type	Status	Laddr.IP	Laddr.Port	Raddr.IP	Raddr.Port	Timestamp
504	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	135	0.0.0.0	0	2026-01-07T08:07:22Z
4	System	IPv4	TCP	LISTEN	192.168.52.144	139	0.0.0.0	0	2026-01-07T09:06:44Z
1284	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	5040	0.0.0.0	0	2026-01-07T08:08:07Z
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.



The screenshot shows a VMware Workstation interface with a window titled "vm-win1 - VMware Workstation". Inside, a Windows 10 desktop environment is displayed. A Microsoft Edge browser window is open, showing a search results page for "My Computer". A PowerShell window titled "Administrator: Windows PowerShell" is active, showing the following command being run:

```
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
RwB1AHQALQBEGEAdAB1AA==
PS C:\Windows\system32> powershell.exe -ExecutionPolicy Bypass -EncodedCommand RwB1AHQALQBEGEAdAB1AA==
```

The PowerShell window also displays the current date and time: "Tuesday, December 30, 2025 11:27:37 AM".

Below the desktop, a table of captured artifacts is shown:

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.D59N8600MJ52G	Windows.System.PowerShell	2025-12-30T06:42:11.188Z	2025-12-30T06:42:13.488Z	admin	0 b	
✓	F.D59M9QFJF6ELE	Windows.Search.FileFinder	2025-12-30T05:58:01.618Z	2025-12-30T05:51:10.579Z	admin	20 b	

At the bottom, there are tabs for "Artifact Collection", "Uploaded Files", "Requests", "Results", "Log", and "Notebook". The "Results" tab is selected, showing a summary of the captured PowerShell artifact:

Artifacts with Results	Windows.System.PowerShell
Total Rows	1
Uploaded Bytes	0 / 0
Files uploaded	0
Download Results	Download

A message at the bottom right says "Select a download method".

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 RwBIAHQALQBEGEAdABIAA==
---------	--

The screenshot shows the Velociraptor interface with the 'Results' tab selected. It displays the command run and its output. The command was powershell.exe -ExecutionPolicy Bypass -EncodedCommand RwBIAHQALQBEGEAdABIAA==. The output shows the PowerShell session starting at 2025-12-30 11:42:13 AM, with the message "Preparing modules for first use.".

```

Windows.System.PowerShell
powershell.exe -ExecutionPolicy Bypass -EncodedCommand RwBIAHQALQBEGEAdABIAA==

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.

The screenshot shows the Velociraptor interface with the 'Log' tab selected. It displays a single log entry for a Windows System.CmdShell artifact. The entry shows the command was run by user 'admin' on 'DESKTOP-F57FH34.localdomain' at 2026-01-08T14:57:03.595Z, resulting in a success status with 0 bytes transferred.

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.D5FSBFODUIN08	Windows.System.CmdShell	2026-01-08T14:57:03.595Z	2026-01-08T14:57:05.113Z	admin	0 b	1

The screenshot shows the 'Artifact Collection' interface with two main sections: 'Overview' and 'Results'.
Overview:
 - **Artifact Names:** Windows.System.CmdShell
 - **Flow ID:** F.D5FSBFODUIN08
 - **Creator:** admin
 - **Create Time:** 2026-01-08T14:57:03.595Z
 - **Start Time:** 2026-01-08T14:57:04.980Z
 - **Last Active:** 2026-01-08T14:57:05.113Z
 - **Duration:** 0.13 seconds
 - **State:** Completed
 - **Ops/Sec:** Unlimited
 - **CPU Limit:** Unlimited
 - **IDPS Limit:** Unlimited
 - **Timeout:** 600 seconds
Results:
 - **Artifacts with Results:** Windows.System.CmdShell
 - **Total Rows:** 1
 - **Uploaded Bytes:** 0 / 0
 - **Files uploaded:** 0
 - **Download Results:** A button labeled 'Select a download method'.

The screenshot shows the 'Log' tab with a table of log entries.
Log Table Headers:
 - client_time
 - level
 - message
Log Entries:
 2026-01-08T14:57:04Z INFO Starting query execution for Windows.System.CmdShell.
 2026-01-08T14:57:04Z DEBUG execve: Running external command [cmd.exe /c whoami]
 2026-01-08T14:57:05Z DEBUG Windows.System.CmdShell: Time 0: Windows.System.CmdShell: Sending response part 0 58 B (1 rows).
 2026-01-08T14:57:05Z INFO Collection Windows.System.CmdShell is done after 131.6014ms
 2026-01-08T14:57:05Z DEBUG Query Stats: {"RowsScanned":4,"PluginsCalled":4,"FunctionsCalled":4,"ProtocolSearch":6,"ScopeCopy":15}

Suspicious EXE in User Path

A fake executable with a random name was created in a user writable directory to simulate malware placement. The **Windows.Search.FileFinder** artifact successfully detected the file, collected its hash, and confirmed its presence.

```
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
```

Search clients								Connected	admin	
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	28 b	1			

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

Timestamp started vfs_path Type file_size uploaded_size

1767074282 2025-12-30 05:58:02.1590235 +0000 UTC C:\Temp\svchost_update.exe 20 20 ThisIsFakeMalware

Windows.Search.FileFinder

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 2025-12-30T05:46:04 2025-12-30T05:46:04 2025-12-30T05:33:30 .395Z .395Z .395Z .378Z false

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.



The screenshot shows the Velociraptor interface with a terminal window. The command entered is:

```
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v TestPersist /t REG_SZ /d notepad.exe
```

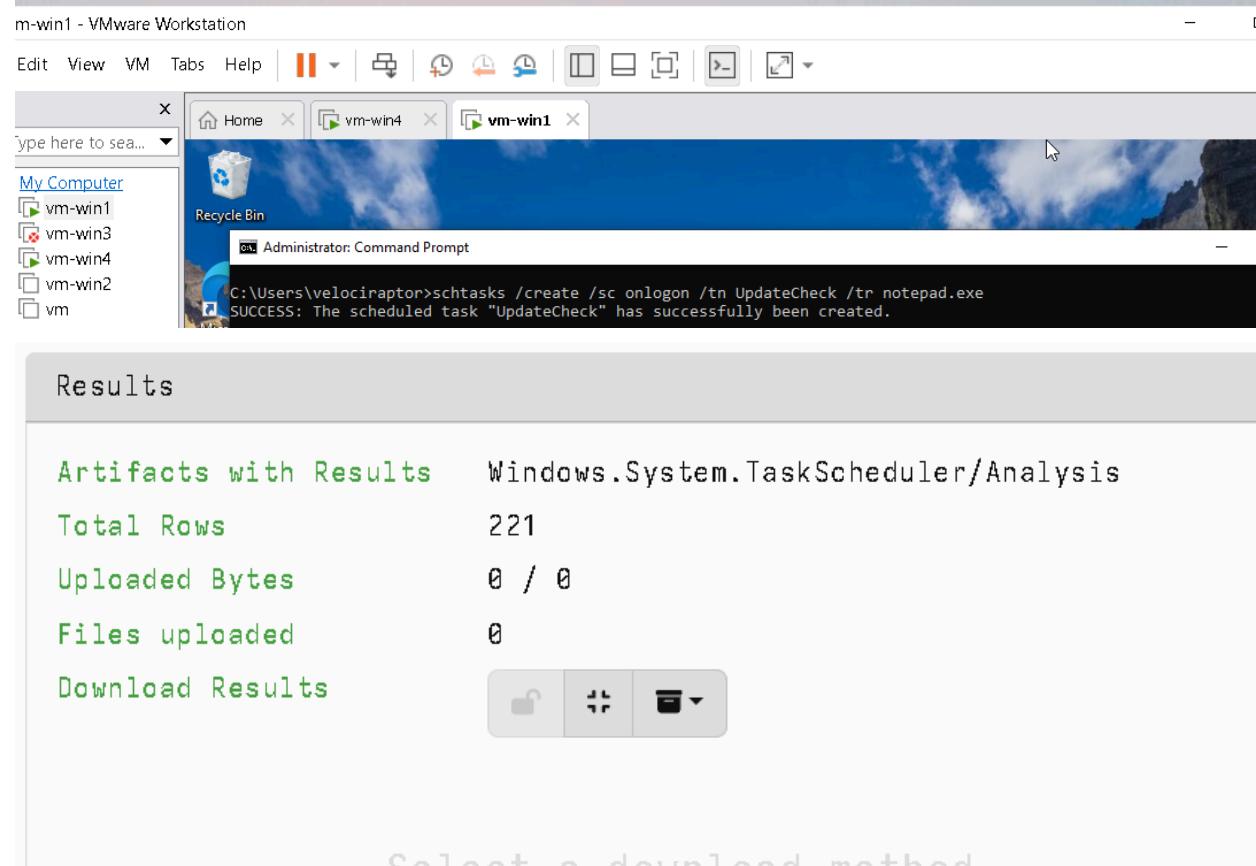
The output of the command is:

```
The operation completed successfully.
```

The interface includes tabs for Overview, VQL Drilldown, and Shell, with the Shell tab selected. A timestamp at the bottom right indicates the log entry was made on 2026-01-08T15:19:01.345Z by the user admin.

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.



The screenshot shows a VMware Workstation interface with a Windows 10 VM named 'vm-win1' running. An Administrator Command Prompt window is open, showing the command:

```
C:\Users\velociraptor>schtasks /create /sc onlogon /tn UpdateCheck /tr notepad.exe
```

The output of the command is:

```
SUCCESS: The scheduled task "UpdateCheck" has successfully been created.
```

Below the VM window, the Velociraptor interface displays the 'Results' section for the 'Windows.System.TaskScheduler/Analysis' artifact type. It shows the following data:

Artifacts with Results	Windows.System.TaskScheduler/Analysis
Total Rows	221
Uploaded Bytes	0 / 0
Files uploaded	0

At the bottom, there is a note: "Select a download method".

Results:

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>
```

The screenshot shows the Splunk search interface with the following details:

- Search Bar:** Contains "all" and a search icon.
- Host Information:** DESKTOP-F57FH34.localdomain Connected
- Toolbar:** Includes icons for search, refresh, and navigation.
- Table Headers:** State, FlowId, Artifacts, Created, Last Active, Creator, Mb, Rows.
- Table Data:** Two rows of results. The first row has FlowId F.056B775NDSSCS.H and Artifacts Windows.System.Services. The second row has FlowId F.056B48JU3ES5Q and Artifacts Windows.System.TaskScheduler.
- Artifact Details Panel:** Shows details for the selected artifact (Windows.System.Services). It includes fields like Flow ID, Creator, Create Time, Start Time, Last Active, Duration, State, Ops/Sec, CPU Limit, IOPS Limit, Timeout, Max Rows, and Max Mb.
- Results Summary Panel:** Shows summary statistics for the selected artifact: Total Rows (268), Uploaded Bytes (0 / 0), Files uploaded (0), and Download Results (with a download icon).
- Bottom Panel:** A message "Select a download method" with a dropdown menu.

Results

Windows Service Configuration														
State	Name	DisplayName	Status	Pid	ExitCode	StartMode	PathName	ServiceType	UserAccount	Created	ServiceDll	FailureCommand	FailureActions	
Stopped	AJRouter	AllSync Router Service	OK	8	1877	Manual	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestriction -p	Share Process	NT AUTHORITY\LocalService	2819-12-07T09:16:04.928Z	C:\Windows\System32\AJRouter.dll		✗ { "ResetPeriod": 86400 } ✗ { "FailureAction": [{ "type": "SC_ACT_ION_RESTART", "delay": 3 }] } ✗ { "type": "SC_ACT_ION_RESTART", "delay": 3 } ✗ { "type": "SC_ACT_ION_NODE", "delay": 0 } }] }	
Stopped	ALG	Application Layer Gateway Service	OK	8	1877	Manual	C:\Windows\System32\alg.exe	Own Process	NT AUTHORITY\LocalService	2819-12-07T09:15:07.846Z		✗ { "ResetPeriod": 960 } ✗ { "FailureAction": [{ "type": "SC_ACT_ION_RESTART", "delay": 120 }] } ✗ { "type": "SC_ACT_ION_RESTART", "delay": 300 } ✗ { "type": "SC_ACT_ION_NODE", "delay": 0 } }] }		

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.

```
C:\Users\velociraptor>wevtutil el
AMSI/Debug
Analytic
Application
DirectShowFilterGraph
DirectShowPluginControl
Els_Hyphenation/Analytic
EndpointMapper
FirstUXPerf-Analytic
ForwardedEvents
HardwareEvents
IHM_DebugChannel
Intel-iaLPSS-GPIO/Analytic
Intel-iaLPSS-I2C/Analytic
Intel-iaLPSS2-GPIO2/Debug
Intel-iaLPSS2-GPIO2/Performance
Intel-iaLPSS2-I2C/Debug
Intel-iaLPSS2-I2C/Performance
Internet Explorer
Key Management Service
MF_MediaFoundationDeviceMFT
MF_MediaFoundationDeviceProxy
MF_MediaFoundationFrameServer
```

all

DESKTOP-F57FH34.localdomain Connected

Interrogate VFS Collected Overview

Cmd wevtutil el Hide Output

wevtutil el

AMSI/Debug Analytic...

Logs

2026-01-09T08:11:55.791Z

2026-01-09T08:11:55.788Z

admin 50 Kb 1

2026-01-09T08:10:27.189Z

2026-01-09T08:10:27.146Z

admin 0 b 1

Artifact Collection Uploaded Files Requests Results Log Notebook

Windows.System.CmdShell

Stdout StdoutUpload

AMSI/Debug Analytic...

Artifact Collection Uploaded Files Requests Results Log Notebook

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.

The screenshot displays the Velociraptor interface with two main panes. The top pane shows a command prompt window with the following content:

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

Below the command prompt, a green box indicates "Handles NPM(K) ...". The bottom pane shows a log table with the following data:

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.D5GBIPMBPS20C	Windows.System.PowerShell	2026-01-09T08:16:38.158Z	2026-01-09T08:16:41.145Z	admin	9 Kb	1
✓	F.D5GBG1QUJJR26	Windows.System.CmdShell	2026-01-09T08:11:55.791Z	2026-01-09T08:11:55.788Z	admin	50 Kb	1

Below the table, a log viewer shows the following entries:

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 JABjAG0AZAA9ACIArwbIAHQALQBQAHIAbwBjAGUAcwBzACIA0wAgAHAAbwB3AGUAcgBzAGgAZQBsaGwAIATAEMAbwBtAG0AYQBuAGQAIAAKAGMAbQBKA AaA]
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.

The screenshot shows the Velociraptor interface with two main panes. The top pane displays a table of credential store entries:

State	Tags	HuntId	Description	Created	Started	Expires	Scheduled	Creator
X		H.D5GBSVPK4BBBBG		2026-01-09T08:38:23.749Z	2026-01-09T08:38:29.012Z	2026-01-16T08:38:06.380Z	2	admin
X		H.D5GBSFSU0RL2M		2026-01-09T08:38:23.749Z	2026-01-09T08:38:29.007Z	2026-01-16T08:38:06.380Z	2	admin

The bottom pane shows the "Overview" tab with details about the hunt:

Artifact Names	Windows.System.CmdShell
Hunt ID	H.D5GBSVPK4BBBBG
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 and Command:

```
Windows.System.CmdShell
Command      cmdkey /list
```

The bottom pane also shows a "Results" section with download statistics:

Total scheduled	2
Finished clients	2
Download Results	[Download Options]

Select a download method

The bottom pane also displays a table of artifacts:

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.D5GBSVPK4BBBBG.H	Windows.System.CmdShell	2026-01-09T08:38:29.023Z	2026-01-09T08:38:29.061Z	admin	0 b	1
✓	F.D5GBQF4H706V0	Windows.System.PowerShell	2026-01-09T08:33:00.942Z	2026-01-09T08:33:06.445Z	admin	0 b	1

Artifact Collection, Uploaded Files, Requests, Results (selected), Log, Notebook tabs are visible.

Stdout tab content:

```
Currently stored credentials: Target: Windowslive:target=virtualapp/didlogical Type: Generic User: 02yqgkizrquauks Local machine persistence
```

StdoutUpload button is present.

E. LATERAL MOVEMENT / C2 SIMULATION

WMI Remote Execution Simulation

Remote execution using WMI was simulated locally. Velociraptor captured the execution details, showing visibility into lateral movement techniques.

The screenshot shows the Velociraptor interface with the 'Results' tab selected. A table displays two WMI execution flows:

State	FlowId	Artifacts	Created	Last Active	Creator	Nb	Rows
✓	F.D56BUG1KGA05G	Windows.System.CmdShell	2026-01-09T08:41:41.763Z	2026-01-09T08:41:41:42.200Z	admin	7 Kb	1
✓	F.056BSVPK4BBB8G	Windows.System.CmdShell	2026-01-09T08:38:29.023Z	2026-01-09T08:38:29.061Z	admin	0 b	1

Details for the first flow (FlowId F.D56BUG1KGA05G):

- Creator: admin
- Create Time: 2026-01-09T08:41:41.763Z
- Start Time: 2026-01-09T08:41:41.683Z
- Last Active: 2026-01-09T08:41:42.200Z
- Duration: 0.52 seconds
- State: Completed
- Cps/Sec: Unlimited
- CPU Limit: Unlimited
- IOPS Limit: Unlimited
- Timeout: 600 seconds
- Max Rows: 1m rows
- Max Mb: 1000.00 Mb

Parameters:

```
Windows.System.CmdShell
Command      wmic process list brief
```

On the right, there's a panel titled "Select a download method" with options for "Files uploaded" (1) and "Download Results".

The screenshot shows the Velociraptor interface with the 'Results' tab selected. A table displays the results of the WMI command execution:

Stdout	StdoutUpload
	HandleCount Name ...

Below the table, a command-line interface shows the executed command:

```
Windows.System.CmdShell
wmic process list brief
```

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>
```

The screenshot shows the Velociraptor interface with two main panes. The top pane displays a terminal window with the output of a 'ping' command to 8.8.8.8. The bottom pane shows a log table and a detailed log view.

Log Table:

State	FlowId	Artifacts	Created	Last Active	Creator	Nb	Rows
✓	F.D56C2M3JCI2MO.H	Windows.System.CmdShell	2026-01-09T08:50:38.112Z	2026-01-09T08:50:38.187Z	admin	0	b
✓	F.D56B8U61KGA05G.H	Windows.System.CmdShell	2026-01-09T08:41:41.763Z	2026-01-09T08:41:42.200Z	admin	7	Kb

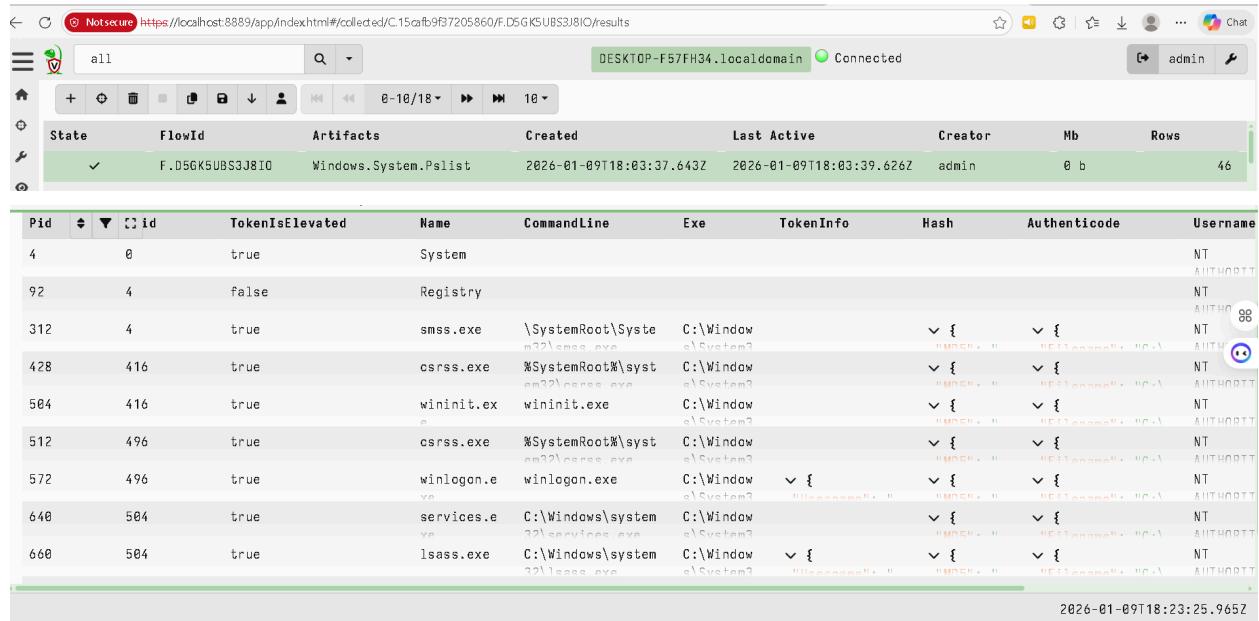
Log View:

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



The screenshot shows the Notsecure application interface with the URL <https://localhost:8889/app/index.html#/collected/C.15cafb937205860/F.D5GK5UBS3J8IO/results>. The main view displays a table of suspicious process activity. The table has columns: State, FlowId, Artifacts, Created, Last Active, Creator, Mb, and Rows. A single row is selected, showing the details for the artifact F.D5GK5UBS3J8IO, which is a Windows.System.Pslist file. The table below lists various system processes with their Pid, TokenIsElevated, Name, CommandLine, Exe, TokenInfo, Hash, Authenticode, and Username. All processes listed are System, smss.exe, csrss.exe, wininit.exe, winlogon.exe, and lsass.exe, all marked as NT AUTHORITY\SYSTEM.

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.D5GK5UBS3J8IO	Windows.System.Pslist	2026-01-09T18:03:37.643Z	2026-01-09T18:03:39.626Z	admin	0 b	46
Pid	TokenIsElevated	Name	CommandLine	Exe	TokenInfo	Hash	Authenticode
4	true	System		C:\Windows\system32\smss.exe	v {	v {	NT AUTHORITY\SYSTEM
92	false	Registry		C:\Windows\system32\csrss.exe	v {	v {	NT AUTHORITY\SYSTEM
312	true	smss.exe	\SystemRoot\System32\smss.exe	C:\Windows\system32\smss.exe	v {	v {	NT AUTHORITY\SYSTEM
428	true	csrss.exe	%SystemRoot%\system32\csrss.exe	C:\Windows\system32\csrss.exe	v {	v {	NT AUTHORITY\SYSTEM
504	true	wininit.exe	wininit.exe	C:\Windows\system32\wininit.exe	v {	v {	NT AUTHORITY\SYSTEM
512	true	csrss.exe	%SystemRoot%\system32\csrss.exe	C:\Windows\system32\csrss.exe	v {	v {	NT AUTHORITY\SYSTEM
572	true	winlogon.exe	winlogon.exe	C:\Windows\system32\winlogon.exe	v {	v {	NT AUTHORITY\SYSTEM
640	true	services.exe	C:\Windows\system32\services.exe	C:\Windows\system32\services.exe	v {	v {	NT AUTHORITY\SYSTEM
660	true	lsass.exe	C:\Windows\system32\lsass.exe	C:\Windows\system32\lsass.exe	v {	v {	NT AUTHORITY\SYSTEM

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.

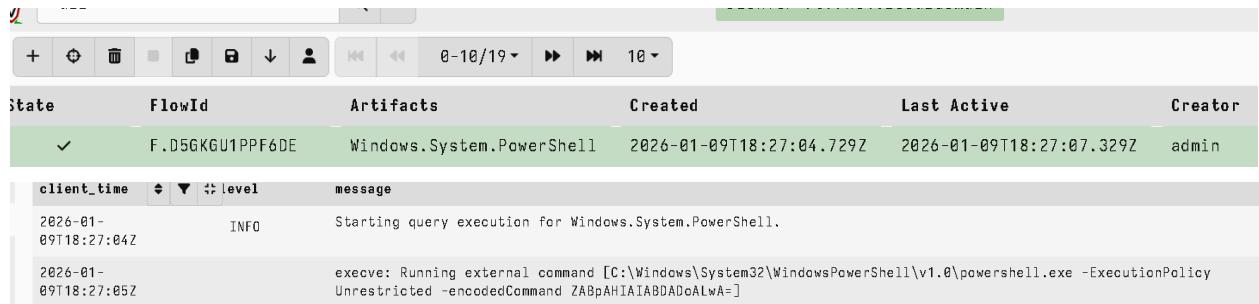
Encoded PowerShell Detection

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.



The screenshot shows the Notsecure application interface with the URL <https://localhost:8889/app/index.html#/collected/C.15cafb937205860/F.D5GK6GU1PPF6DE/results>. The main view displays a table of suspicious PowerShell activity. The table has columns: State, FlowId, Artifacts, Created, Last Active, and Creator. A single row is selected, showing the details for the artifact F.D5GK6GU1PPF6DE, which is a Windows.System.PowerShell file. The table below lists log entries with client_time, level, and message. The log shows the starting of the query execution and the execution of an external command.

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.D56KJR06CKBAQ	Windows.System.TaskSchedule	2026-01-09T18:33:19.607Z	2026-01-09T18:33:24.063Z	admin
\UpdateCheck	2026-01-09T07:44:11.711Z	notepad.exe	DESKTOP-F57FH34\windows	LeastPrivilege	InteractiveToken

New Executable Detection

Search clients Q ▾ DESKTOP-F57FH34.localdomain Connected admin 🔍

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.059MJQFJF6ELE	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

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

OPath	Inode	Mode	Size	MTime	ATime	CTime	BTime	Keywords	IsDir	Upload	
C:\Temp\svchost_update.exe	-rw-rw-rw-	20	2025-12-30T05:46:04	2025-12-30T05:46:04	2025-12-30T05:46:04	2025-12-30T05:33:30	.395Z	.395Z	.395Z	.378Z	false

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.

The screenshot shows the Logstash interface with the URL <https://localhost:8889/app/index.html#/collected/C.15cafb9f37205860/F.D5GL2M6GCGJG6.H/fogs>. The search bar contains "all". The results table shows two entries:

State	FlowId	Artifacts	Last Active	Creator	Mb	Rows
✓	F.D5GL2M6GCGJG6.H	Windows.System.PowerShell	2026-01-09T19:05:02.576Z	admin	0 b	1
✓	F.D5GL17G5B8QTC	Windows.Search.FileFinder	2026-01-09T18:36:14.559Z	admin	0 b	0

Below the table are tabs for Artifact Collection, Uploaded Files, Requests, Results, Log (which is selected), and Notebook. The Log tab displays log entries:

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

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.

The screenshot shows the Logstash interface with the URL <https://localhost:8889/app/index.html#/collected/C.15cafb9f37205860/F.D5GL40RU7PSFS.H/fogs>. The tabs at the top are Artifact Collection, Uploaded Files, Requests, Results, Log, and Notebook. The Artifact Collection tab is selected.

The left panel shows an "Overview" table with the following data:

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

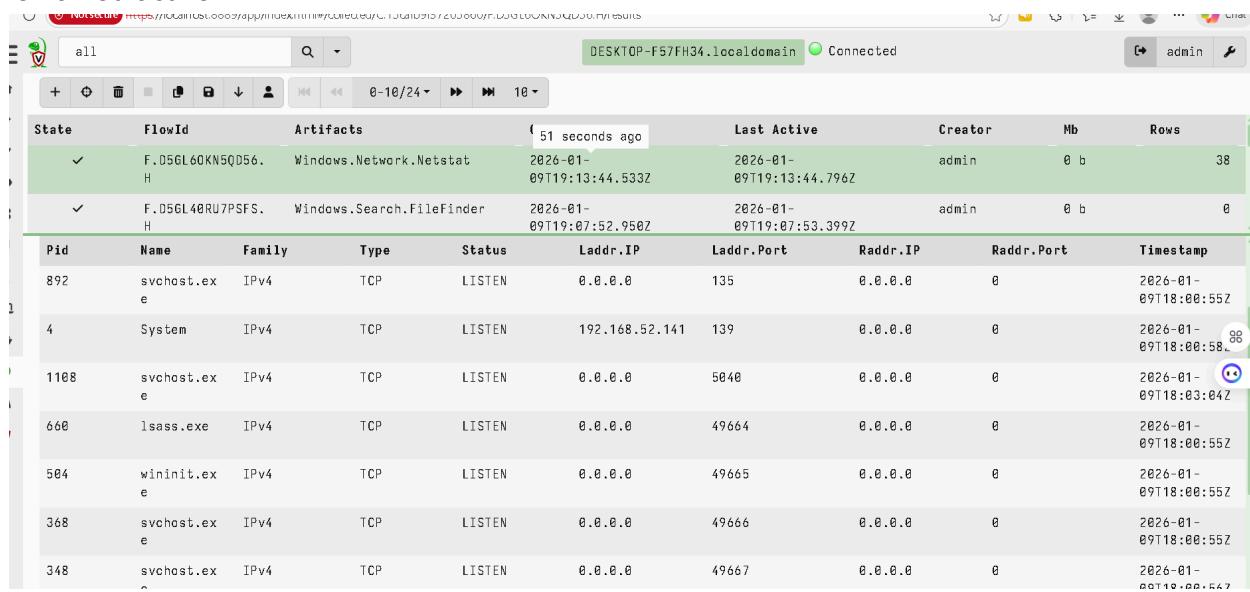
The right panel shows a "Results" section with the following data:

Artifacts with Results	Total Rows
	0
Uploaded Bytes	0 / 0
Files uploaded	0
Download Results	[Download Options]

A message at the bottom says "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.



A screenshot of the NetworkMiner tool interface. The title bar shows 'DESKTOP-F57FH34.localdomain Connected'. The main window displays two rows of network traffic artifacts. The first row is for 'Windows.Network.Netstat' (FlowID F.D56L60KN5QD56.H) and the second for 'Windows.Search.FileFinder' (FlowID F.D56L40RU7PSFS.H). Both entries show a timestamp of '51 seconds ago' and were last active on '2026-01-09T19:13:44.533Z'. The creator is 'admin' and the size is '0 b'. Below this, a detailed table lists system processes: svchost.exe, System, svchost.exe, lsass.exe, wininit.exe, svchost.exe, and svchost.exe. Each process is listed with its PID, name, family, type (TCP), status (LISTEN), local and remote IP addresses, ports, and timestamp. The table includes columns for Pid, Name, Family, Type, Status, Laddr.IP, Laddr.Port, Raddr.IP, Raddr.Port, and Timestamp.

State	FlowId	Artifacts	(51 seconds ago)	Last Active	Creator	Mb	Rows		
✓	F.D56L60KN5QD56.H	Windows.Network.Netstat	2026-01-09T19:13:44.533Z	2026-01-09T19:13:44.796Z	admin	0 b	38		
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
1188	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	5040	0.0.0.0	0	2026-01-09T18:03:04Z
668	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.

Create Hunt: Configure artifact parameters

Windows.EventLogs.PowershellModule

EventLog	C:\Windows\system32\winevt\logs\Microsoft-Windows-PowerShell%4Operational.evtx
DateAfter	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	<input checked="" type="checkbox"/> 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 shows the Notsecure web interface at <https://localhost:8889/app/index.html#/collected/C.9dfb18daaf7c821f/F.D5IU6M487TA8G.H>. The top navigation bar includes a logo, a search bar with 'all' selected, and a dropdown menu. The main header displays 'vm-win4.localdomain Connected' and user 'admin'. Below the header is a toolbar with various icons. The main content area features a table titled 'Collected Artifacts' with columns: State, FlowId, Artifacts, Created, Last Active, Creator, Mb, and Rows. A single row is visible, showing 'Windows.System.Plist' as the artifact type, created on 2026-01-13T06:17:15.571Z, last active on 2026-01-13T06:17:42.175Z, by user 'admin', with 0 Mb and 53 rows. To the left of the table is a sidebar with 'Artifact Names' and a table of hunt parameters. To the right is a panel for 'Artifacts with Results' showing 'Windows.System.Plist' with 53 total rows, 0 uploaded bytes, and 0 files uploaded. A download button is present. At the bottom, a message says 'Select a download method'.

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

Artifact Names	Windows.System.Plist
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.Plist
Total Rows	53
Uploaded Bytes	0 / 0
Files uploaded	0
Download Results	Download

Artifact Collection Uploaded Files Requests **Results** Log Notebook

Windows.System.Pplist

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	0%	0.8 MB	0.1 MB/s	0 Mbps	
> VMware Workstation (32 bit) (3)	0%	1.9 MB	0.1 MB/s	0 Mbps	
> Antimalware Service Executable	0%	65.8 MB	0.1 MB/s	0 Mbps	
Velociraptor: Digging Deeper!	0%	6.6 MB	0.1 MB/s	0 Mbps	

Create Hunt: Configure artifact parameters

Windows.Search.FileFinder

Filter artifact parameter name

SearchFilesGlobTable

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

Accessor: auto

YaraRule: ? for suggestions

Upload_File:

Calculate_Hash:

MoreRecentThan: Select Time

ModifiedBefore: Select Time

VSS_MAX_AGE_DAYS: If larger than 0 we restrict VSS age to this many days

Configure Hunt Select Artifacts **Configure Parameters** Specify Resources Review Launch

State FlowId Artifacts Created Last Active Creator Nb Rows

✓ F.D5IUIS0KK7GOEH Windows.Search.FileFinder 2026-01-13T06:43:04.094Z 2026-01-13T06:43:10.994Z admin 0 b 62

✓ F.D5IU6M487TA8G Windows.System.Pplist 2026-01-13T06:17:15.688Z 2026-01-13T06:17:18.272Z admin 0 b 4

Artifact Collection Uploaded Files Requests **Results** Log Notebook

Windows.Search.FileFinder

88

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	2026-01-13T06:10:53	.006Z	2019-12-07T09:09:34	2026-01-13T06:10:53	.006Z	.006Z	false



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.