Task 02 Report: Deploying Velociraptor & Performing Test Runs

Objective

The objective of this task was to deploy Velociraptor on multiple Windows machines, verify successful client server communication, execute commands remotely, and test Velociraptor's ability to detect safe, simulated malicious activity in a controlled and non destructive manner.

1. Velociraptor Server Setup

Velociraptor was first configured as a **server** on the host machine. The server was initialized and launched successfully, and the web based Velociraptor console was accessed through the browser.

Once the server was running, the Velociraptor GUI was used to:

- Manage clients
- Run hunts
- Execute server and client artifacts
- View collected results and logs

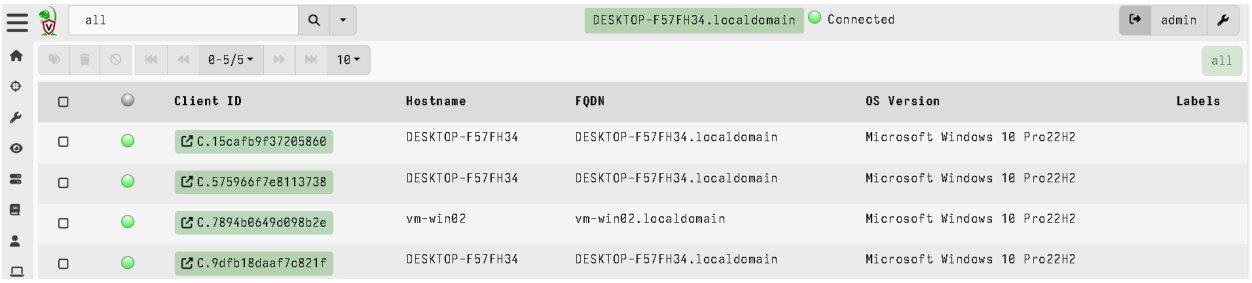
2. Client Deployment on Windows Machines

Velociraptor clients were installed on Windows virtual machines.

Each client:

- Was configured with the correct server address

- Started as a service
- Successfully established communication with the Velociraptor server



3. Remote Command Execution Test (Hunt Execution)

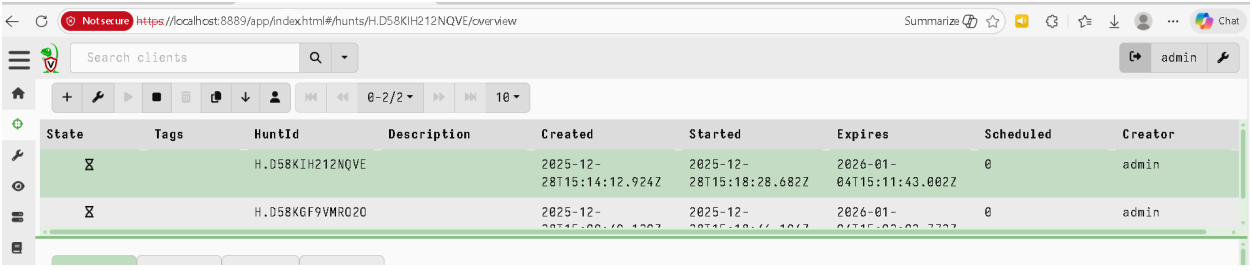
To verify that Velociraptor can remotely execute commands, Server Artifacts were used.

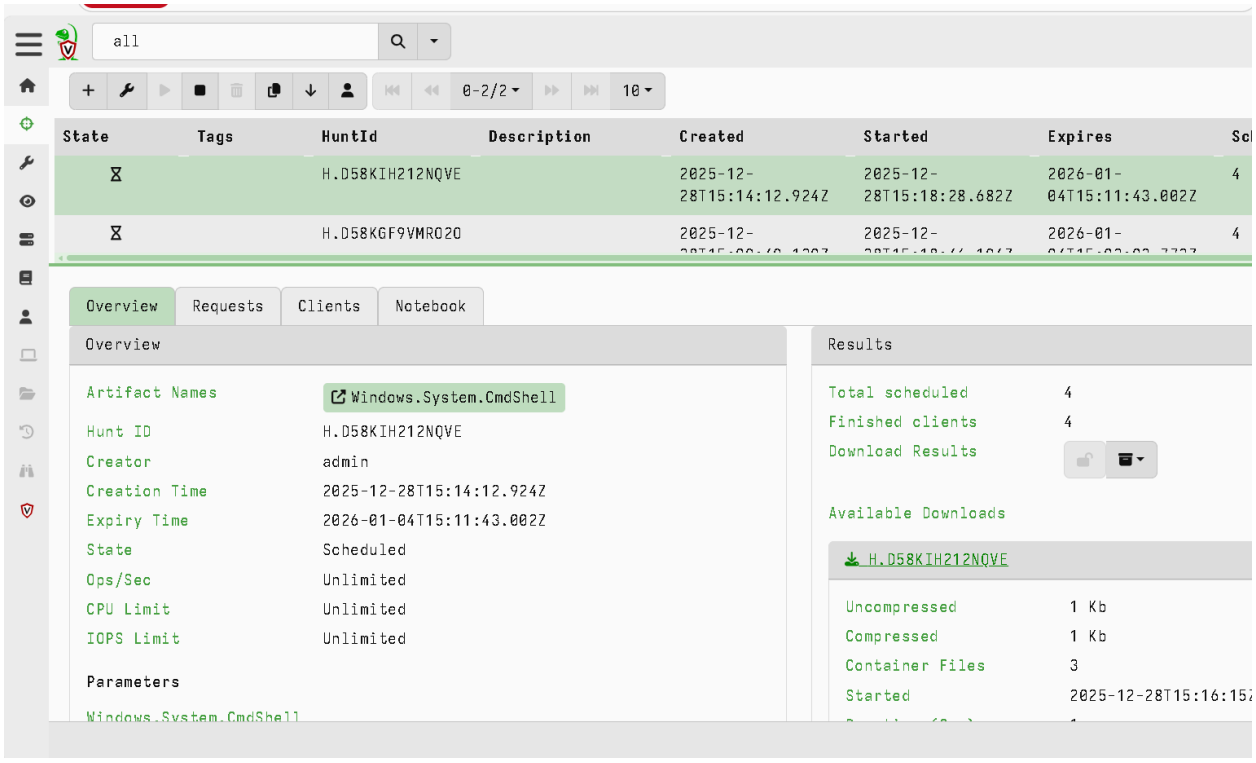
Artifacts Used

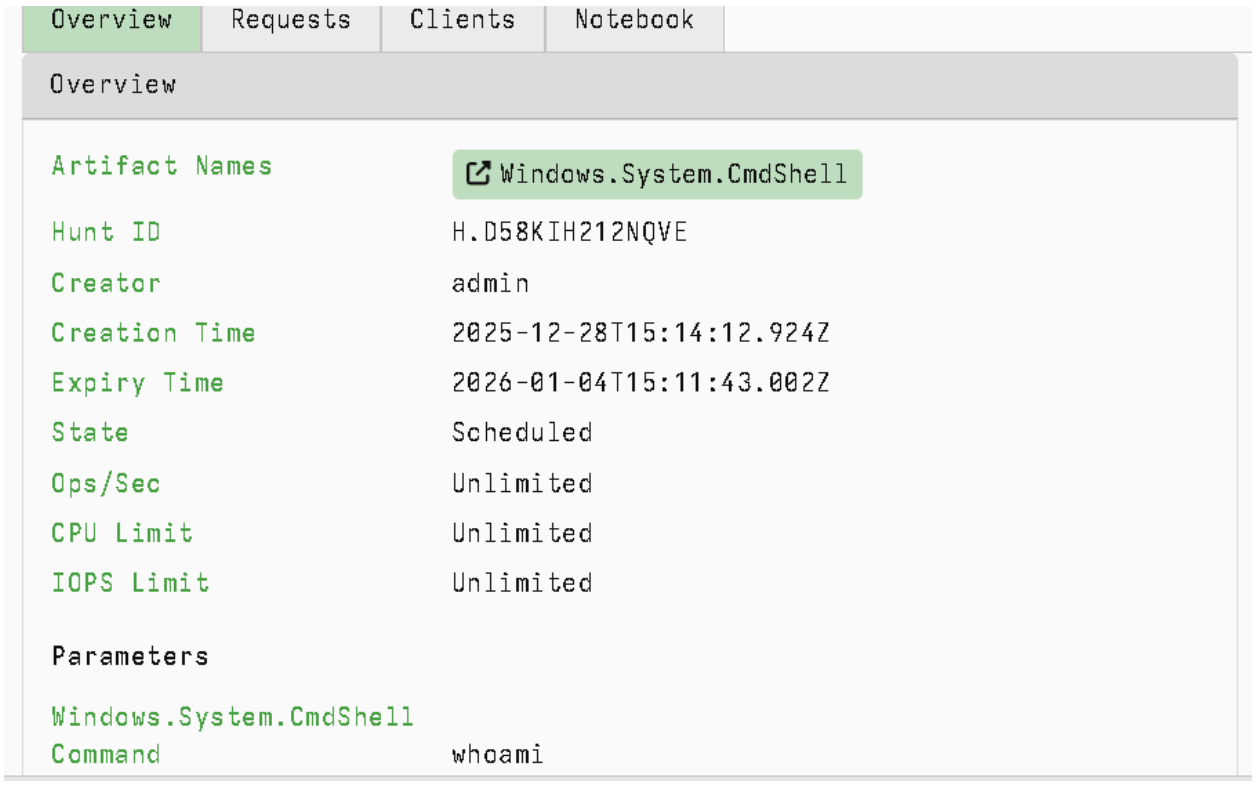
- **Windows.System.Cmdshell**

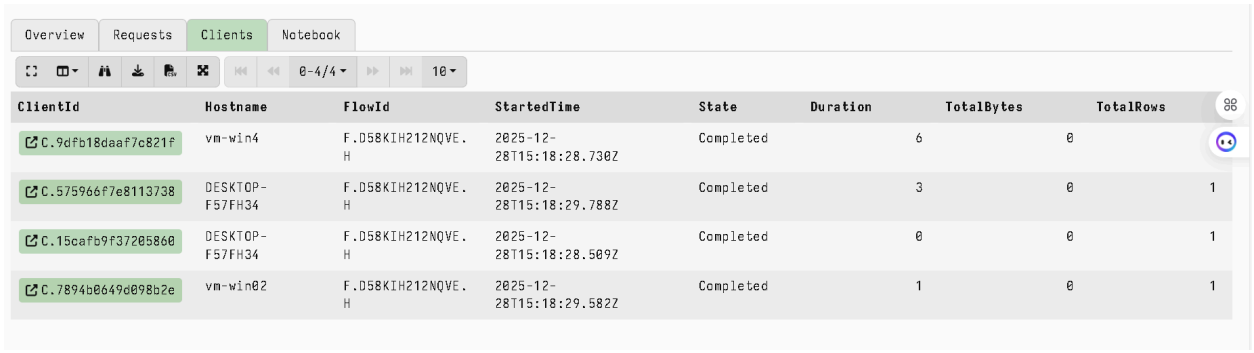
Commands Executed

- Whoami
- ipconfig

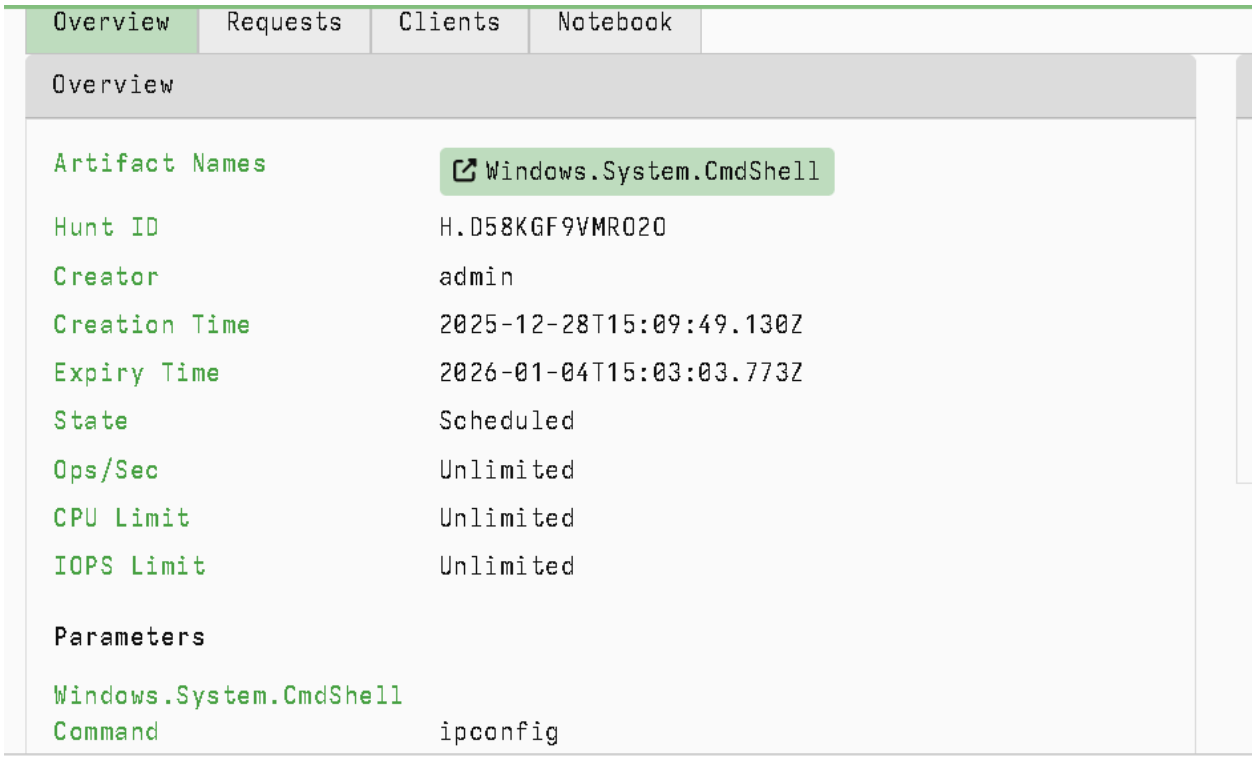


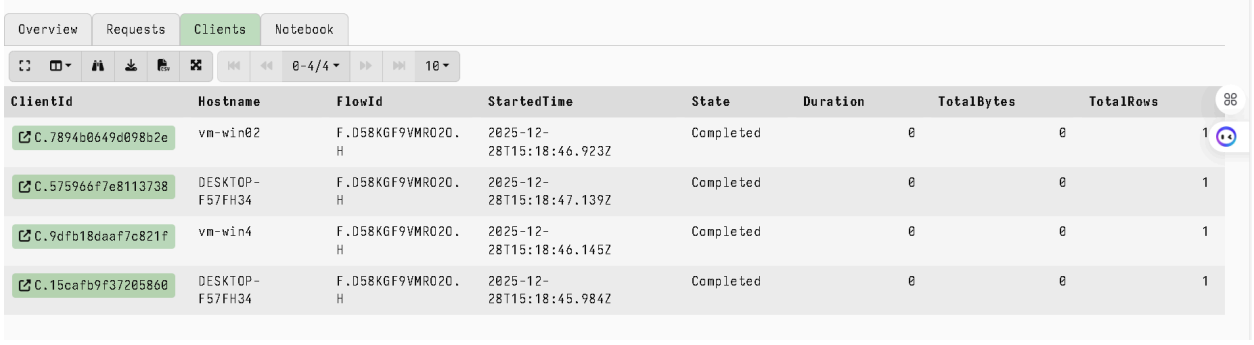

all
0-2/2
10
State
Tags
HuntId
Description
Created
Started
Expires
H.D58KIH212NQVE
2025-12-28T15:14:12.924Z
2025-12-28T15:18:28.682Z
2026-01-04T15:11:43.002Z
H.D58KGF9VMRO2O
Overview
Requests
Clients
Notebook
Artifact Names
Windows.System.CmdShell
Hunt ID
Creator
admin
Creation Time
Expiry Time
State
Scheduled
Ops/Sec
Unlimited
CPU Limit
IOPS Limit
Parameters
Results
Total scheduled
4
Finished clients
Download Results
Available Downloads
H.D58KIH212NQVE
Uncompressed
1 Kb
Compressed
Container Files
3
Started


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
C.9dfb18daaf7c821f	vm-win4	F.D58KIH212NQVE.H	2025-12-28T15:18:28.730Z	Completed	6	0	
C.575966f7e8113738	DESKTOP-F57FH34	F.D58KIH212NQVE.H	2025-12-28T15:18:29.788Z	Completed	3	0	1
C.15cafb9f37205860	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





ClientId	Hostname	FlowId	StartedTime	State	Duration	TotalBytes	TotalRows
C.7894b0649d098b2e	vm-win02	F.D58KGF9VMRO2O.H	2025-12-28T15:18:46.923Z	Completed	0	0	1
C.575966f7e8113738	DESKTOP-F57FH34	F.D58KGF9VMRO2O.H	2025-12-28T15:18:47.139Z	Completed	0	0	1
C.9dfb18daaf7c821f	vm-win4	F.D58KGF9VMRO2O.H	2025-12-28T15:18:46.145Z	Completed	0	0	1
C.15cafb9f37205860	DESKTOP-F57FH34	F.D58KGF9VMRO2O.H	2025-12-28T15:18:45.984Z	Completed	0	0	1

Results

- Each command executed successfully
- Output was returned to the Velociraptor console
- Flow IDs were generated for each execution
- Execution time, command details, and results were logged

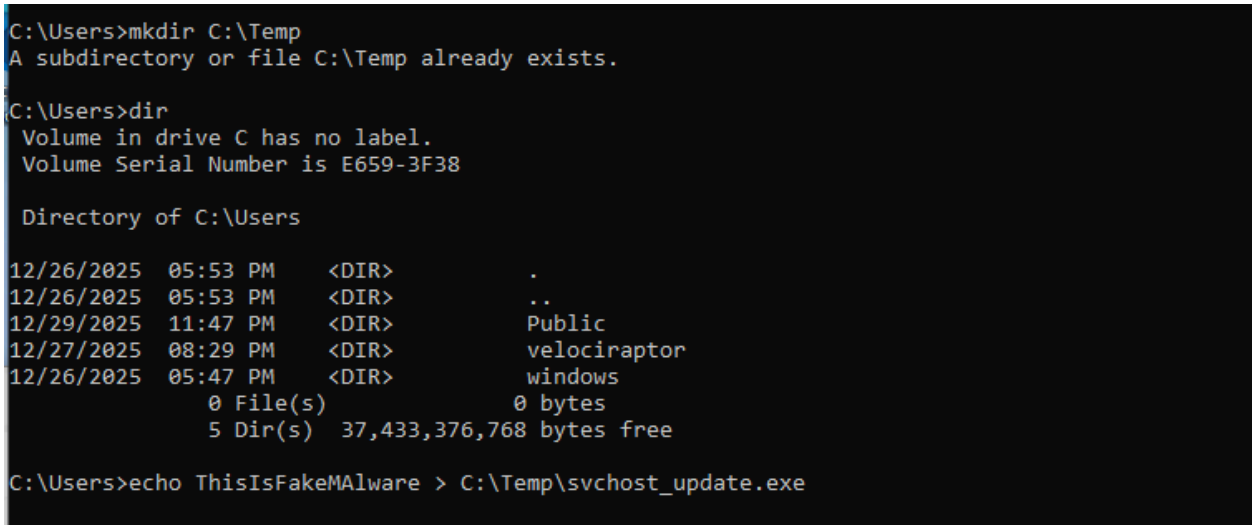
This confirmed that:

- The server can remotely run commands
- Clients correctly respond
- Output collection works as expected

4. Simulated Malicious Behavior Detection

4.1 Fake Malware File Creation (File Detection Test)

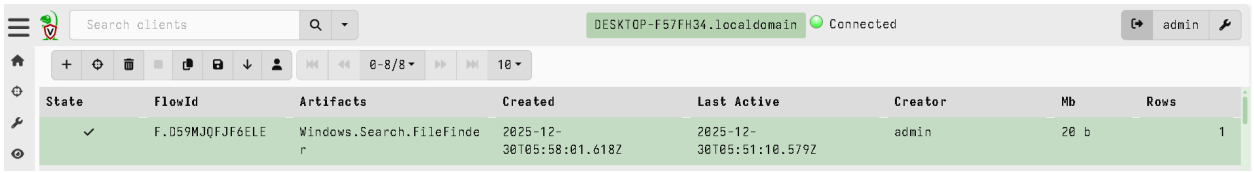
A fake malware-like executable was created safely:

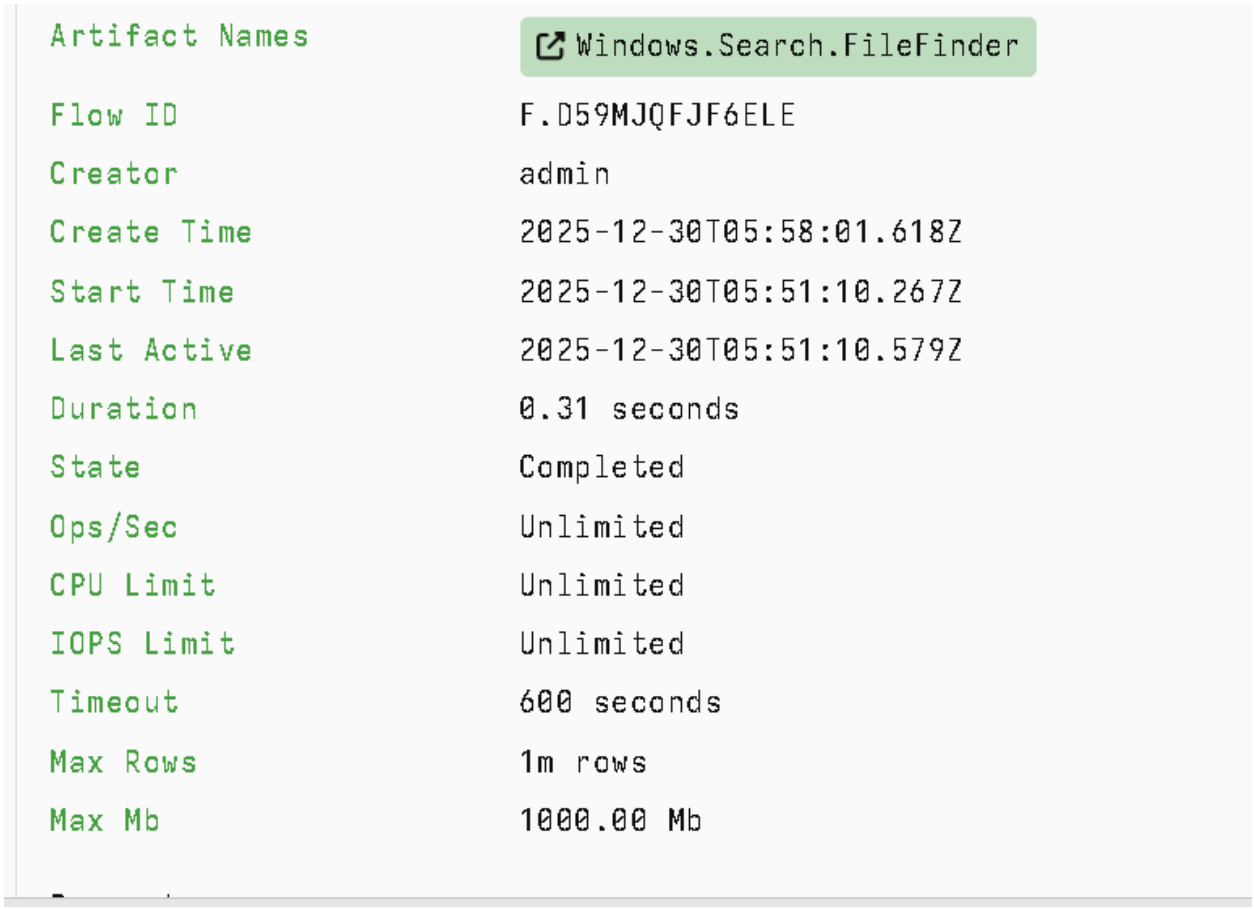


The file was intentionally named to resemble a system process.

Artifact Used

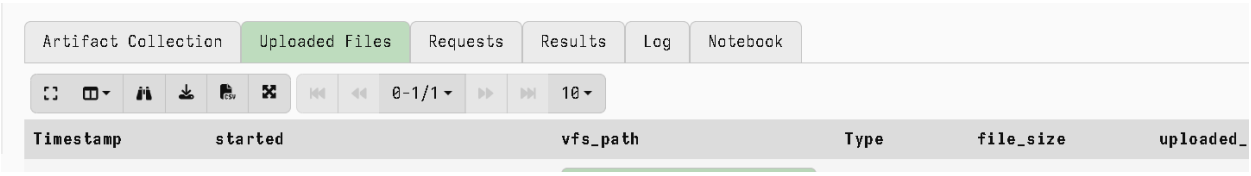
- **Windows.Search.FileFinder**

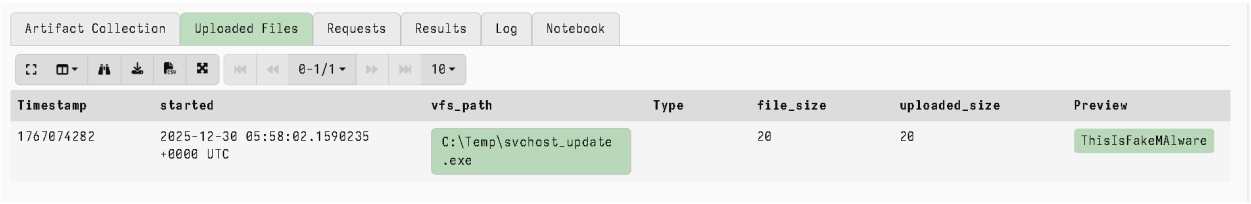


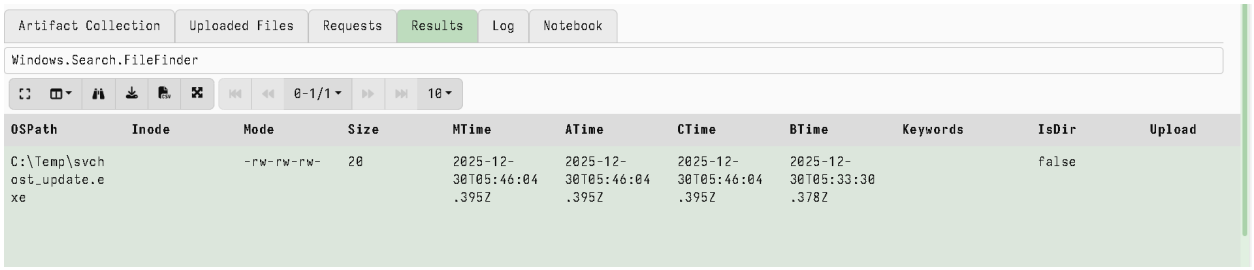


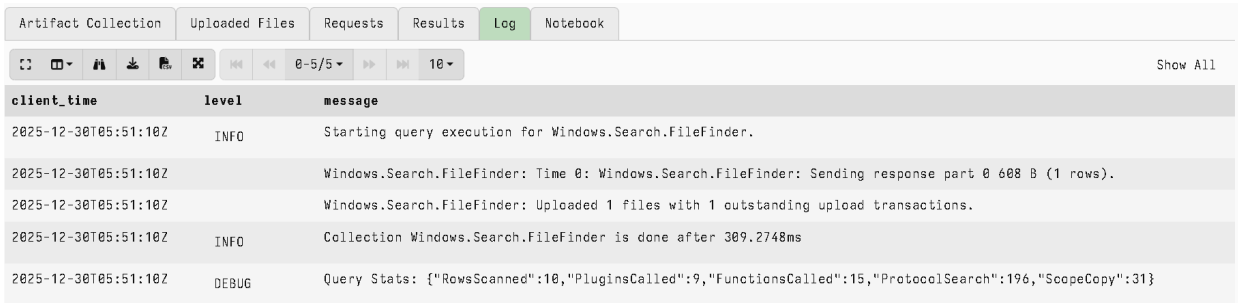
Parameters

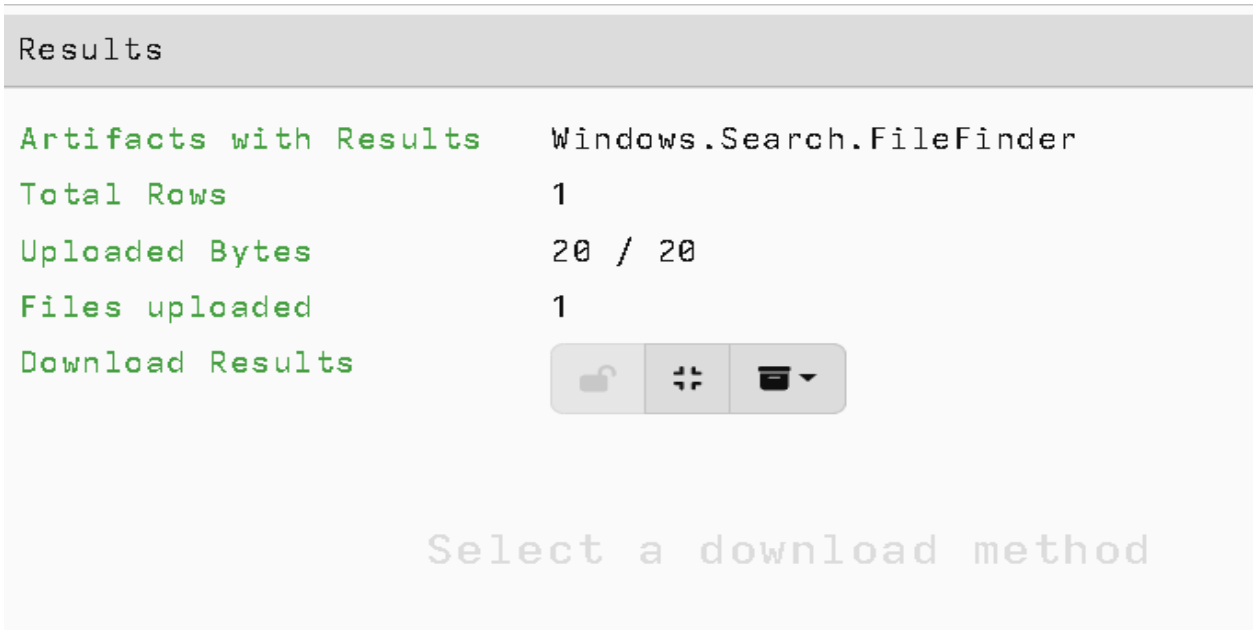
Windows.Search.FileFinder	
SearchFilesGlobTable	Glob C:\Temp*.exe
Upload_File	Y
Calculate_Hash	Y











Results

Velociraptor successfully:

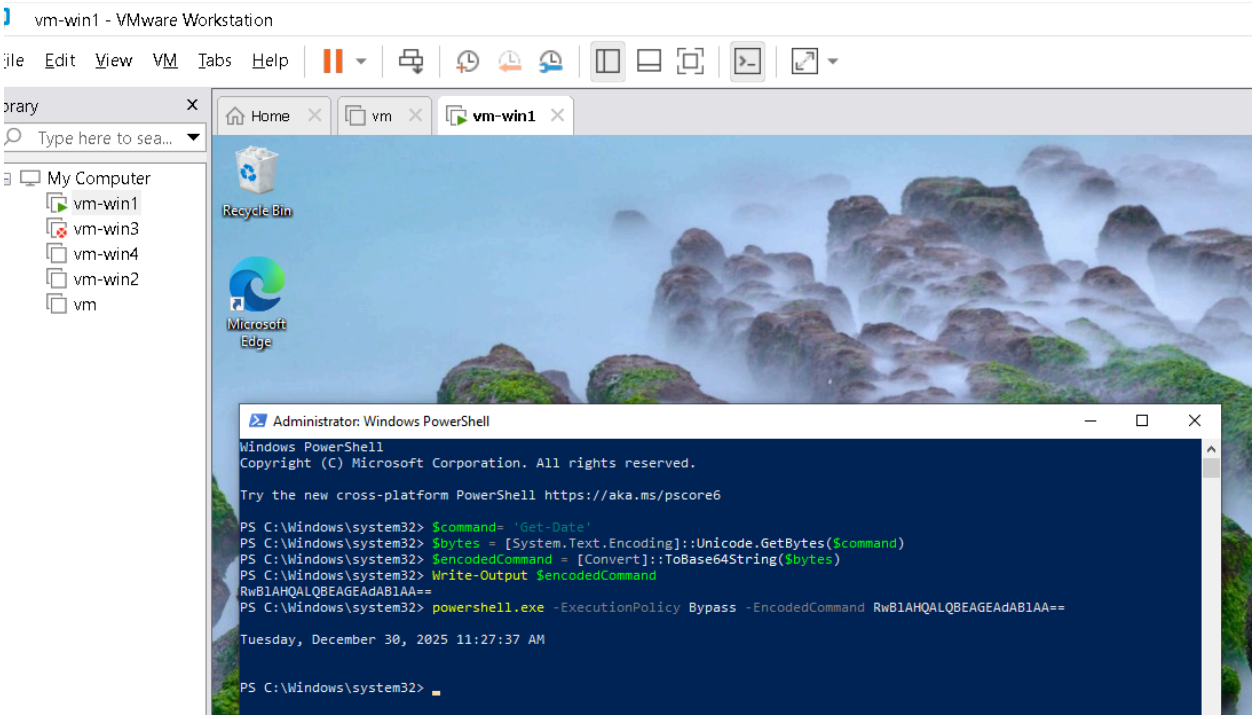
- Detected the file
- Uploaded it to the server
- Calculated MD5, SHA1, and SHA256 hashes
- Displayed file metadata and timestamps

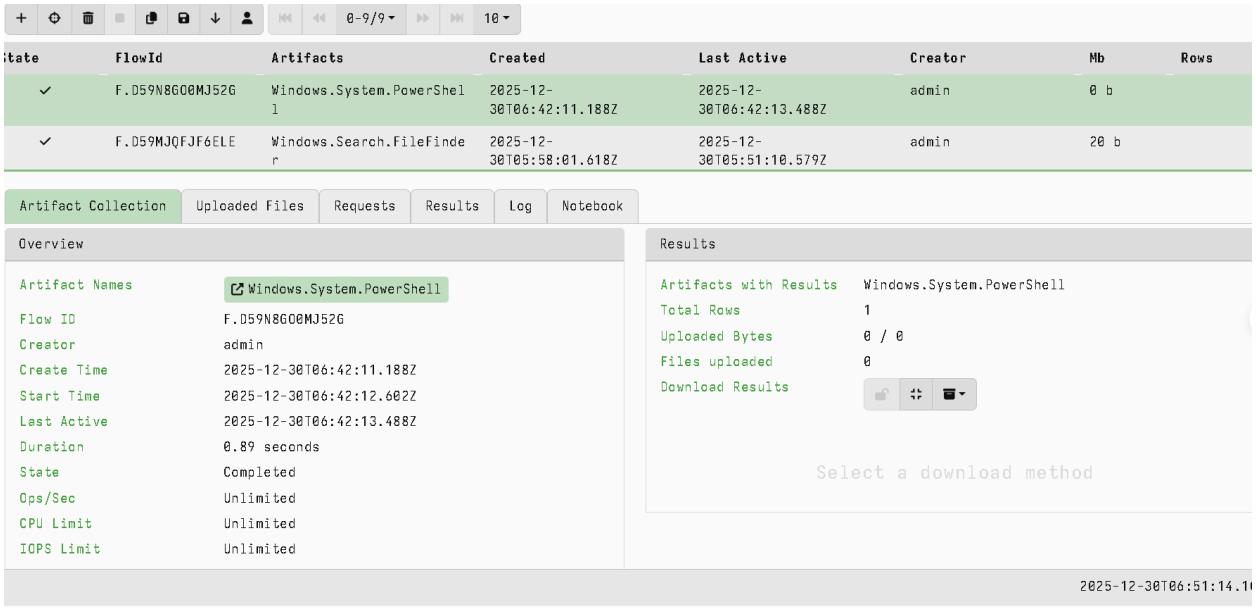
Conclusion:

- Velociraptor successfully located the file and collected artifact data, demonstrating file monitoring capabilities.

4.2 Suspicious PowerShell Execution (Base64 Encoded Command)

A benign PowerShell command (Get-Date) was encoded in Base64 and executed using:





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 RwBlAHQALQBEAGEAdABlAA==

Base64-encoded PowerShell commands are commonly used by attackers to:

- Obfuscate malicious scripts
- Evade detection

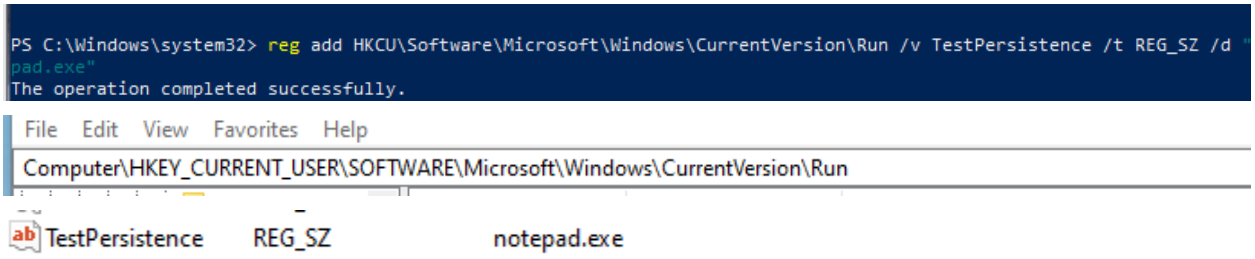
Velociraptor Detection

- Detected under Windows.System.Powershell
- Logged execution details
- Generated a Flow ID
- Recorded execution timestamps and parameters

Conclusion:
Although the command itself was harmless, Velociraptor correctly logged and captured behavior commonly associated with malicious activity.

4.3. Registry Run Key Persistence Simulation (Manual)

1. Opened PowerShell and added a benign registry Run key for persistence:



1. Verified in regedit that the key was created successfully.

Conclusion:

- Velociraptor detected changes to the registry, confirming its ability to monitor persistence mechanisms.

Final Conclusion

This task successfully demonstrated the practical use of Velociraptor as an endpoint monitoring and incident response tool. All four Windows machines were connected properly to the Velociraptor server, and remote command execution was verified through simple commands like **ipconfig** and **whoami**, confirming correct client server communication.

Safe, non-destructive simulations of malicious behavior were performed, including a Base64-encoded PowerShell command, creation of a fake malware like executable, and manual registry Run key persistence. Velociraptor accurately logged these activities, collected relevant artifacts, and displayed the results in hunts and collections.

Overall, the results show that velociraptor is effective in detecting suspicious commands, file based threats, and persistence mechanisms. This setup proves that the environment is correctly configured and capable of supporting real world security monitoring and forensic investigations.