

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

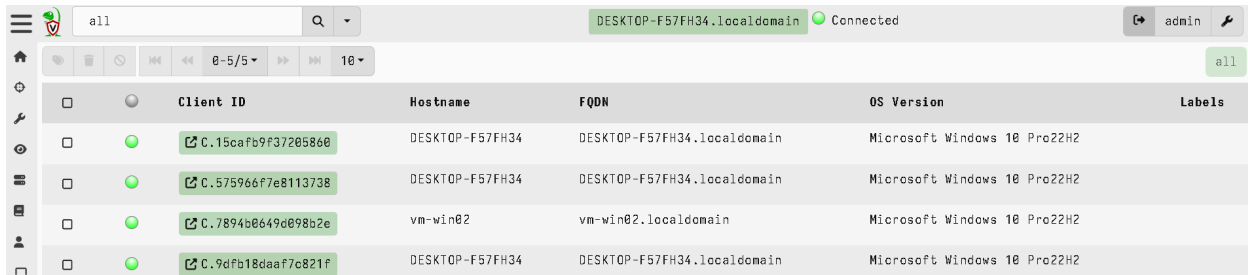
2. Client Deployment on Windows Machines

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



The screenshot shows the Velociraptor web interface with a search bar at the top containing 'all'. Below the search bar, there's a table of connected clients. The table has columns for Client ID, Hostname, FQDN, OS Version, and Labels. There are four clients listed, all with a green status icon indicating they are connected.

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	

3. Remote Command Execution Test (Hunt Execution)

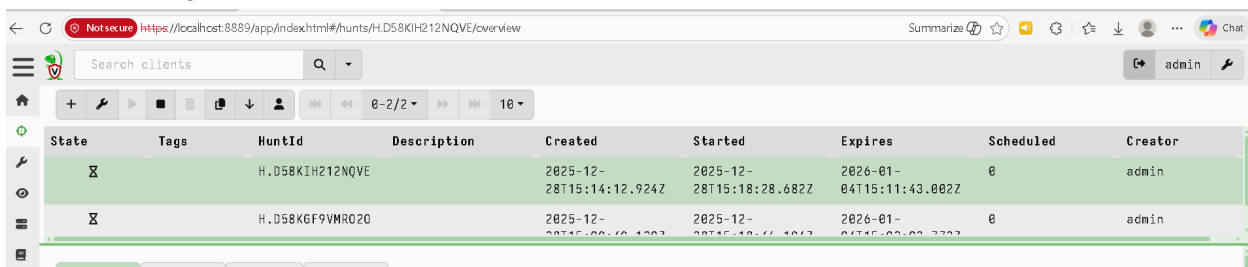
To verify that Velociraptor can remotely execute commands, Server Artifacts were used.

Artifacts Used

- Windows.System.Cmdshell

Commands Executed

- Whoami
- ipconfig



The screenshot shows the Velociraptor web interface with a search bar at the top containing 'Search clients'. Below the search bar, there's a table of hunt artifacts. The table has columns for State, Tags, HuntId, Description, Created, Started, Expires, Scheduled, and Creator. There are two artifacts listed, both with a green status icon indicating they are successful.

State	Tags	HuntId	Description	Created	Started	Expires	Scheduled	Creator
Success		H.D58KI212NQVE		2025-12-28T15:14:12.924Z	2025-12-28T15:18:28.682Z	2026-01-04T15:11:43.002Z	0	admin
Success		H.D58KGF9VMRQ20		2025-12-28T15:18:28.682Z	2025-12-28T15:18:28.682Z	2026-01-04T15:11:43.002Z	0	admin

all

Q

0-2/2

10

State	Tags	HuntId	Description	Created	Started	Expires	Score
⌵		H.D58KIH212NQVE		2025-12-28T15:14:12.924Z	2025-12-28T15:18:28.682Z	2026-01-04T15:11:43.002Z	4
⌵		H.D58KGF9VMR020		2025-12-28T15:00:10.400Z	2025-12-28T15:18:16.101Z	2026-01-04T15:02:02.777Z	4

Overview

Requests

Clients

Notebook

Overview

Results

Artifact Names

Hunt ID

Creator

Creation Time

Expiry Time

State

Ops/Sec

CPU Limit

IOPS Limit

Parameters

Windows.System.CmdShell

Windows.System.CmdShell

Total scheduled

Finished clients

Download Results

Available Downloads

H.D58KIH212NQVE

Uncompressed

Compressed

Container Files

Started

4

4

H.D58KIH212NQVE

1 Kb

1 Kb

3

2025-12-28T15:16:15Z

Overview

Requests

Clients

Notebook

Overview

Artifact Names

Hunt ID

Creator

Creation Time

Expiry Time

State

Ops/Sec

CPU Limit

IOPS Limit

Parameters

Windows.System.CmdShell

Command

Windows.System.CmdShell

H.D58KIH212NQVE

admin

2025-12-28T15:14:12.924Z

2026-01-04T15:11:43.002Z

Scheduled

Unlimited

Unlimited

Unlimited

whoami

Overview

Requests


Clients

Notebook

0-4/4

ClientId	Hostname	FlowId	StartedTime	State	Duration	TotalBytes	TotalRows	
<div>C.9dfb18daaf7c821f</div>	vm-win4	F.D58KIH212NQVE.H	2025-12-28T15:18:28.730Z	Completed	6	0		<div></div>
<div>C.575966f7e8113738</div>	DESKTOP-F57FH34	F.D58KIH212NQVE.H	2025-12-28T15:18:29.788Z	Completed	3	0	1	<div></div>
<div>C.15caf9f37205860</div>	DESKTOP-F57FH34	F.D58KIH212NQVE.H	2025-12-28T15:18:28.509Z	Completed	0	0	1	
<div>C.7894b0649d098b2e</div>	vm-win02	F.D58KIH212NQVE.H	2025-12-28T15:18:29.582Z	Completed	1	0	1	

10

OverviewRequestsClientsNotebook	
Overview	
Artifact Names	 Windows.System.CmdShell
Hunt ID	H.D58KGF9VMR020
Creator	admin
Creation Time	2025-12-28T15:09:49.130Z
Expiry Time	2026-01-04T15:03:03.773Z
State	Scheduled
Ops/Sec	Unlimited
CPU Limit	Unlimited
IOPS Limit	Unlimited
Parameters	
Windows.System.CmdShell	
Command	ipconfig

Overview

Requests

Clients

Notebook

0-4/4

ClientId	Hostname	FlowId	StartedTime	State	Duration	TotalBytes	TotalRows	
C.7894b0649d098b2e	vm-win02	F.D58KGF9VMR020. H	2025-12-28T15:18:46.923Z	Completed	0	0	1	
C.575966f7e8113738	DESKTOP-F57FH34	F.D58KGF9VMR020. H	2025-12-28T15:18:47.139Z	Completed	0	0	1	
C.9dfb18daaf7c821f	vm-win4	F.D58KGF9VMR020. H	2025-12-28T15:18:46.145Z	Completed	0	0	1	
C.15caf9f37205860	DESKTOP-F57FH34	F.D58KGF9VMR020. H	2025-12-28T15:18:45.984Z	Completed	0	0	1	

10

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:

```
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 bytes free

C:\Users>echo ThisIsFakeMALware > C:\Temp\svchost_update.exe
```

The file was intentionally named to resemble a system process.

Artifact Used

- Windows.Search.FileFinder

Search clients		DESKTOP-F57FH34.localdomain		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	20 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

0-1/1

10

Timestamp

started

vfs_path

Type

file_size

uploaded_

Artifact Collection		Uploaded Files		Requests	Results	Log	Notebook
<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></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><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><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><div></div><div></div><div></div><div></div><div></div><div></div></div></div> <div>0-1/1</div> <div>10</div>							
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					
<div>0-5/510</div>					
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

Results

Velociraptor successfully:

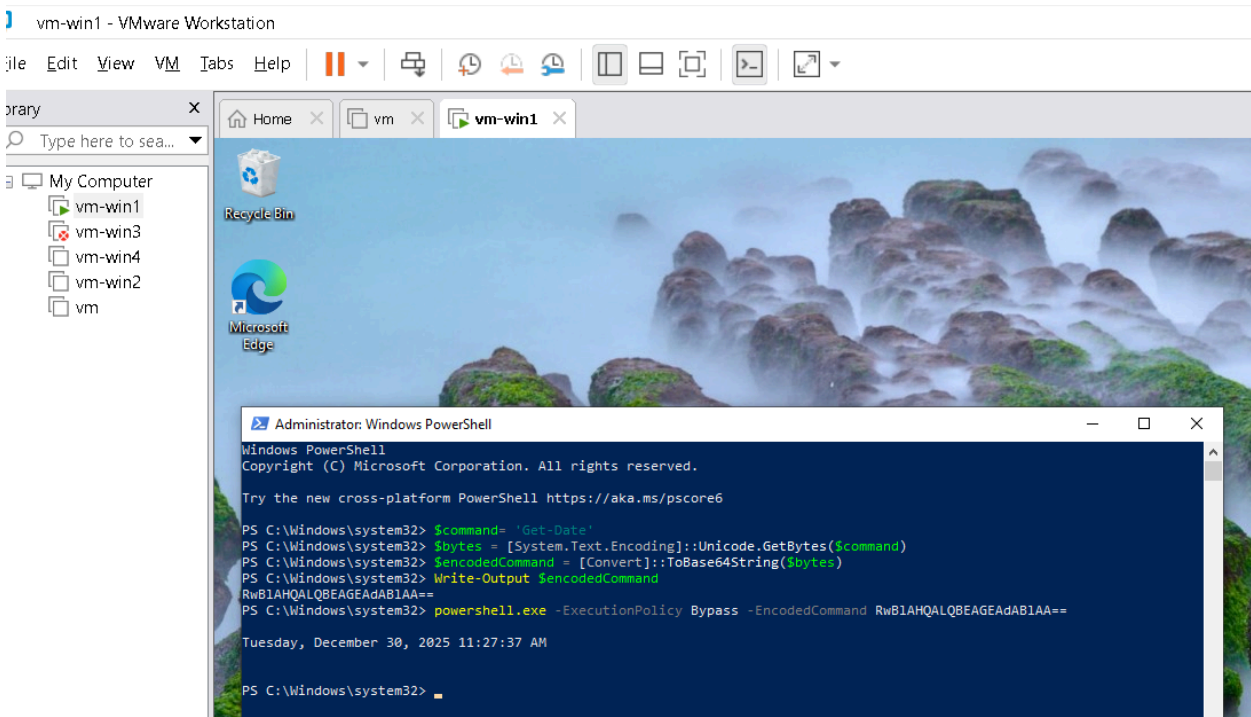
- Detected the file
- Uploaded it to the server
- Calculated MD5, SHA1, and SHA256 hashes
- Displayed file metadata and timestamps

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:



State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F.D59N8G0MJ52G	Windows.System.PowerShell	2025-12-30T06:42:11.188Z	2025-12-30T06:42:13.488Z	admin	0 b	
✓	F.D59MJQFJF6ELE	Windows.Search.FileFinde	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.D59N8G0MJ52G				
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	<div>Download</div>				
Select a download method					

2025-12-30T06:51:14.11Z

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 Rwb1AHQALQBEAGEAdAB1AA==

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>	

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

- Obfuscate malicious scripts
- Evade detection

Velociraptor Detection

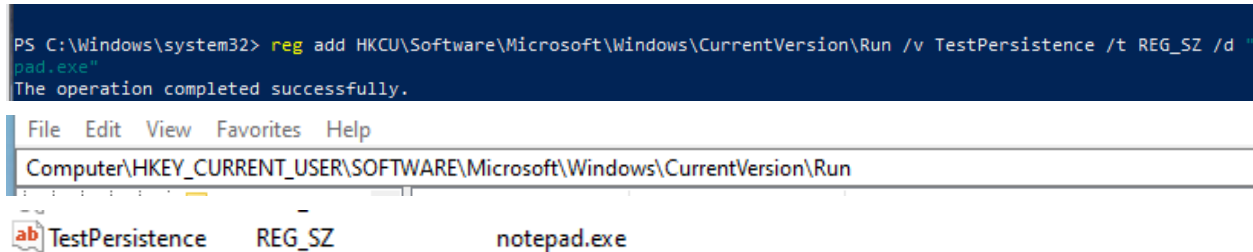
- Detected under Windows.System.Powershell
- Logged execution details
- Generated a Flow ID
- Recorded execution timestamps and parameters

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:



The screenshot shows a PowerShell terminal window with the command `reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v TestPersistence /t REG_SZ /d "notepad.exe"` and the output `The operation completed successfully.` Below the terminal is a screenshot of the Windows Registry Editor. The left pane shows the path `Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`. The right pane shows a single registry value named `TestPersistence` of type `REG_SZ` with the data `notepad.exe`.

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.