

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 client interface with a list of connected clients. The clients are listed in a table with columns: Client ID, Hostname, FQDN, OS Version, and Labels. All clients are connected and running Microsoft Windows 10 Pro22H2.

	Client ID	Hostname	FQDN	OS Version	Labels
0	C.15cafb9f37205860	DESKTOP-F57FH34	DESKTOP-F57FH34.localdomain	Microsoft Windows 10 Pro22H2	
1	C.575966f7e8113738	DESKTOP-F57FH34	DESKTOP-F57FH34.localdomain	Microsoft Windows 10 Pro22H2	
2	C.7894b0649d098b2e	vm-win02	vm-win02.localdomain	Microsoft Windows 10 Pro22H2	
3	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 interface with a list of hunts. There are two hunts listed: H.D58KIH212NQVE and H.D58KGF9VMR020. Both hunts are in progress (State: X) and were created by admin on 2025-12-28T15:14:12.924Z.

State	Tags	HuntId	Description	Created	Started	Expires	Scheduled	Creator
X		H.D58KIH212NQVE		2025-12-28T15:14:12.924Z	2025-12-28T15:18:28.682Z	2026-01-04T15:11:43.002Z	0	admin
X		H.D58KGF9VMR020		2025-12-28T15:20:10.100Z	2025-12-28T15:20:10.100Z	2026-01-04T15:20:00.320Z	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	StartTime	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	

Overview Requests Clients Notebook

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

ClientId	Hostname	FlowId	StartTime	State	Duration	TotalBytes	TotalRows	88
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.15cafb9f37205868	DESKTOP-F57FH34	F.D58KGF9VMR020.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:

```
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 ThisIsFakeMAware > C:\Temp\svchost_update.exe
```

The file was intentionally named to resemble a system process.

Artifact Used

- **Windows.Search.FileFinder**

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	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

Timestamp started vfs_path Type file_size uploaded_size

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

Artifact Collection Uploaded Files Requests Results Log Notebook

Windows.Search.FileFinder

OSPath Inode Mode Size MTime ATime CTime BTime Keywords IsDir Upload

OSPath	Inode	Mode	Size	MTime	ATime	CTime	BTime	Keywords	IsDir	Upload
C:\Temp\svchost_update.exe	-rw-rw-rw-	20	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

client_time level message

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:

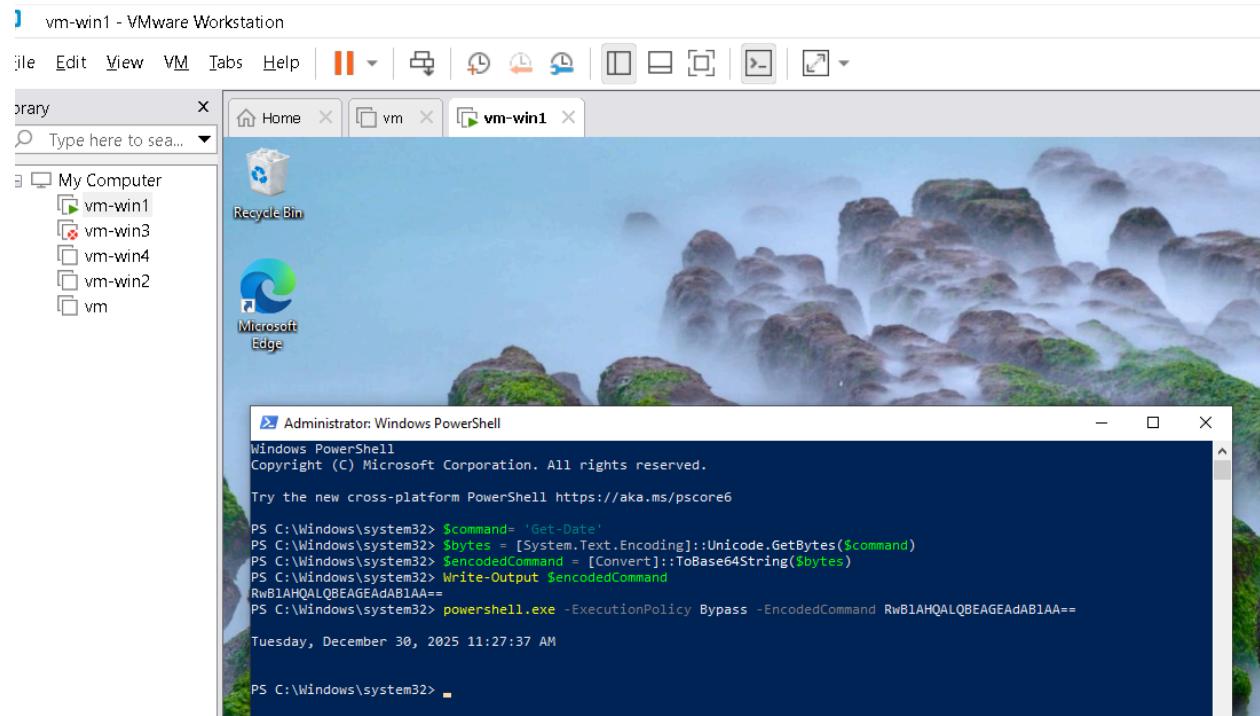
- Detected the file
- Uploaded it to the server
- Calculated MD5, SHA1, and SHA256 hashes
- Displayed file metadata and timestamps

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.D59N8G00MJ52G	Windows.System.PowerShell	2025-12-30T06:42:11.188Z	2025-12-30T06:42:13.488Z	admin	0 b	1
✓	F.D59MJQFJF6ELE	Windows.Search.FileFinder	2025-12-30T05:58:01.618Z	2025-12-30T05:58:01.618Z	admin	20 b	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 RwBIAHQALQBEGEAdABIAA==
---------	--

The screenshot shows a log viewer with the following tabs: Artifact Collection, Uploaded Files, Requests, Results (highlighted in green), Log, and Notebook. The results section displays a PowerShell command execution. The command was run at 2025-12-30T06:42:13.488Z. The output shows the command being decoded and executed, resulting in the preparation of modules for first use.

```

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">
</><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></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 Windows Registry Editor window. At the top, there is a command-line interface with the following text:
PS C:\Windows\system32> reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v TestPersistence /t REG_SZ /d "notepad.exe"
The operation completed successfully.
Below the command line is the Registry Editor interface. The title bar says 'File Edit View Favorites Help'. The left pane shows a tree structure with 'Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run'. Under this key, there are three entries: 'TestPersistence' (REG_SZ), 'REG_SZ', and 'notepad.exe'. The 'notepad.exe' entry has a small icon next to it.

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.