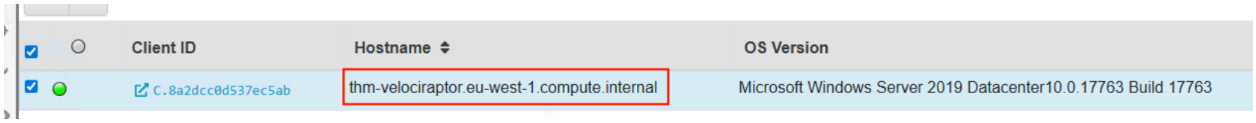
Velociraptor

Task 2 Deployment

Using the documentation, how would you launch an Instant Velociraptor on Windows?
velociraptor.exe gui

Task 3 Interacting with client machines

What is the hostname for the client?
Login into the dashboard
Then search with with nothing



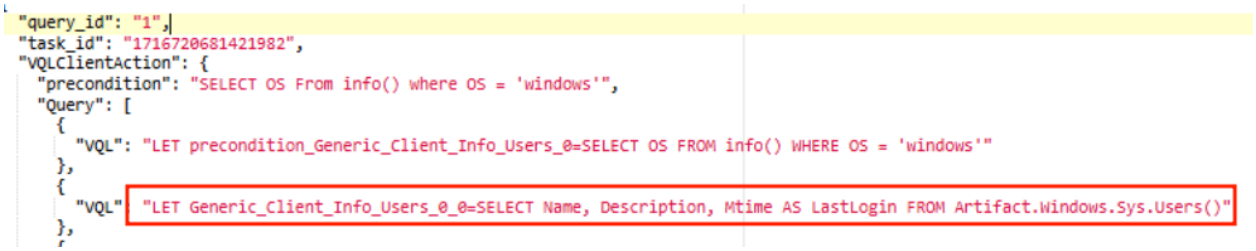
THM-VELOCIRAPTOR.eu-west-1.compute.internal

What is listed as the agent version?

Click on the agent id

2021-04-11T22:11:10Z

In the Collected tab, what was the VQL command to query the client user accounts?
Go to the collected artifacts tab -> requests



LET Generic_Client_Info_Users_0_0=SELECT Name, Description, Mtime AS LastLogin FROM Artifact.Windows.Sys.Users()

In the Collected tab, check the results for the PowerShell whoami command you executed previously. What is the column header that shows the output of the command?

Click one the results in the completed tab

stdout

In the Shell, run the following PowerShell command Get-Date. What was the PowerShell command executed with VQL to retrieve the result?

After executing the command click on the logs same as above

powershell -ExecutionPolicy Unrestricted -encodedCommand ZwBIAHQALQBkAGEAdABIAA==

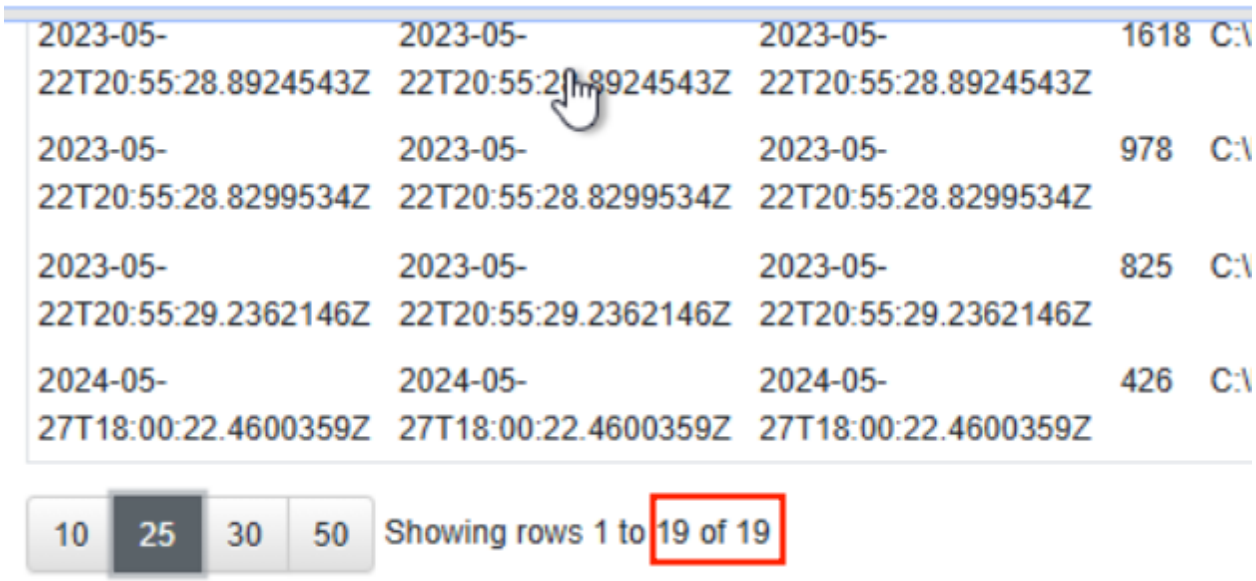
Task 4 Creating a new collection

Earlier you created a new artifact collection for Windows.KapeFiles.Targets. You configured the parameters to include Ubuntu artifacts. Review the parameter description for this setting. What is this parameter specifically looking for?

Just the see the description while putting tick mark for ubuntu / even in the walkthrough screenshot

Ubuntu on Windows Subsystem for Linux

Review the output. How many files were uploaded?
Click on the results



19

Task 5 VFS (Virtual File System)

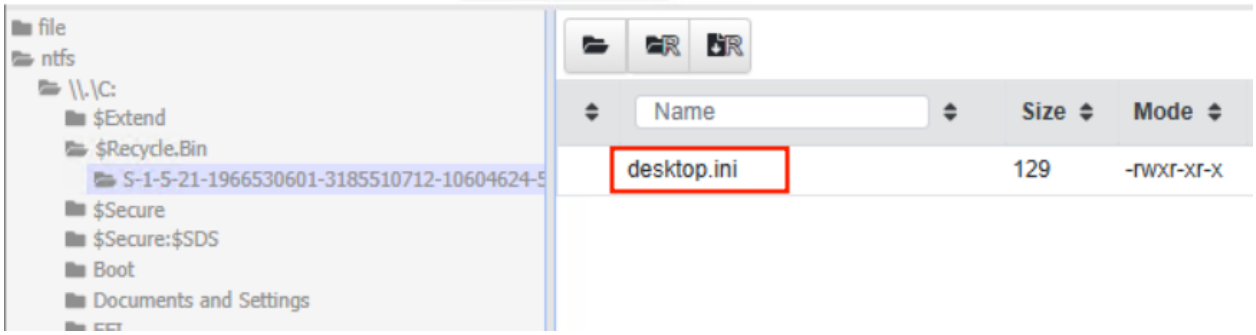
Which accessor can access hidden NTFS files and Alternate Data Streams? (format: xyz accessor)

ntfs accessor

Which accessor provides file-like access to the registry? (format: xyz accessor)

registry accessor

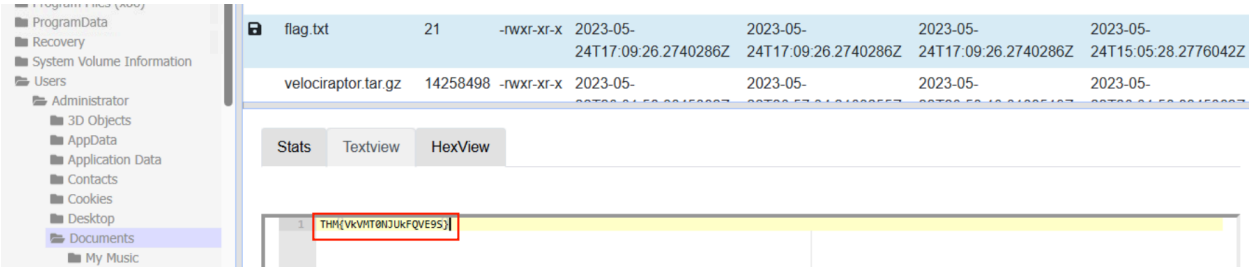
What is the name of the file in $Recycle.Bin?



Follow the path in the screenshot , after reaching each step in the path click on the first button (folder) to sync the refresh the files and directories

There is hidden text in a file located in the Admin's Documents folder. What is the flag?

Follow the path ntfs -> C -> users -> administrator -> documents
After that download the file or try to sync the file (The option re-collect from the client) , then click on text view

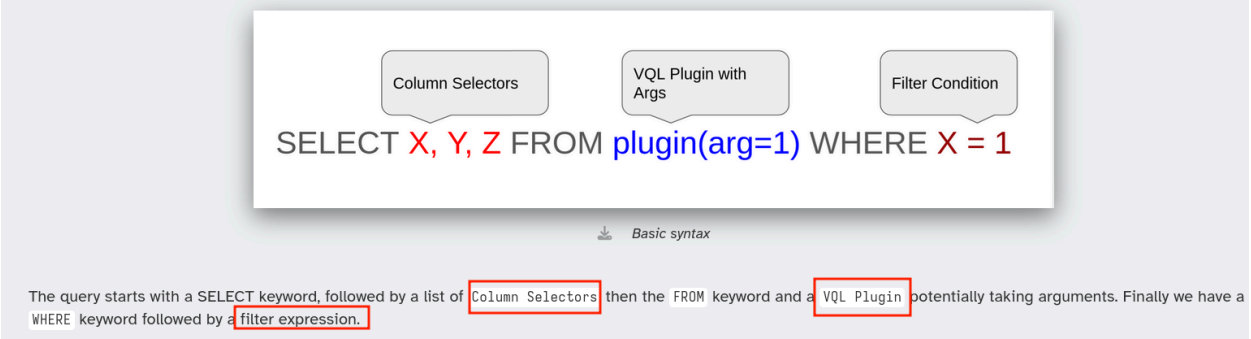


THM{VkVMT0NJUkFQVE9S}

Task 6 VQL (Velociraptor Query Language)

Refer to the documentation to answer these questions
https://docs.velociraptor.app/docs/vql/fundamentals/

What is followed after the SELECT keyword in a standard VQL query?



Column Selectors

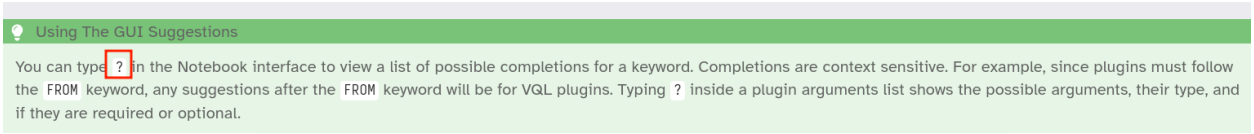
What goes after the FROM keyword?

VQL Plugin

What is followed by the WHERE keyword?

Filter expression

What can you type in the Notepad interface to view a list of possible completions for a keyword?



?

What plugin would you use to run PowerShell code from Velociraptor?

Read the documentation page https://docs.velociraptor.app/docs/vql/extending_vql/

Extending artifacts - PowerShell

Powershell is a powerful systems automation language mainly used on Windows systems where is comes built in and almost always available.

Many complex software products contain powershell modules around automation and system administration. It does not make sense for Velociraptor to directly support complex software packages such as Office365, Azure which already come with extensive powershell support.

But it is critical to be able to recover forensically relevant data from these package. Therefore it makes sense to wrap powershell scripts in VQL artifacts.

In the following we see how to wrap a simple powershell snippet in VQL. The process for wrapping other powershell snippets is very similar.

For this example we will use the following very simple snippet of PowerShell which simply lists the names, process id and binary path of all running processes.

```
Get-Process | Select Name, Id, Path
```

```
PS C:\Program Files\Velociraptor> Get-Process | Select Name, Id, Path

Name                                                  Id Path
----                                                  -- ----
ApplicationFrameHost                                4568 C:\WINDOWS\system32\ApplicationFrameHost.exe
browser_broker                                      6568 C:\WINDOWS\system32\browser_broker.exe
cmd                                                 1384 C:\WINDOWS\system32\cmd.exe
cmd                                                 5208 C:\WINDOWS\system32\cmd.exe
cmd                                                 5396 C:\WINDOWS\system32\cmd.exe
conhost                                             1660 C:\WINDOWS\system32\conhost.exe
conhost                                             2564 C:\WINDOWS\system32\conhost.exe
```

Powershell snippet for listing processes

In order to run powershell code from Velociraptor we will use the `execve()` plugin to shell out to powershell. The `execve()` plugin takes a list of args and builds a correctly escaped command line.

execve()

Task 7 Forensic Analysis VQL Plugins

Refer to the documentation to answer these questions

https://docs.velociraptor.app/docs/forensic/ntfs/#parsing-the-mft

What plugin would be used for parsing the Master File Table (MFT)?

Parsing the MFT

Since the `ntfs` accessor allows accessing the `$MFT` file as a regular file, you can download the entire $MFT file from the endpoint using the ntfs accessor, then process it offline. For example using the `Windows.Search.FileFinder` artifact with the `ntfs` accessor - or simply using the VQL:

```
SELECT upload(path="C:/$MFT", accessor="ntfs")
FROM scope()
```

However, in practice this is inefficient and does not scale. Typically we want to parse the MFT in order to answer some questions about the system, such as which files were modified within a timerange.

Velociraptor provides access to the $MFT parser using the `parse_mft()` plugin, so the MFT can be parsed directly on the endpoint using Velociraptor. The plugin emits a high level summary of each MFT entry, including its timestamps (for the $STANDARD_INFORMATION and $FILENAME streams) and MFT ID.

This plugin is most useful when you need to pass over all the files in the disk - it is more efficient than a recursive glob and might recover deleted files. For example to recover all the files with a .exe extension from the drive:

```
SELECT * FROM parse_mft(filename="C:/$MFT", accessor="ntfs")
WHERE FileName =~ ".exe$"
```

parse_mft

What filter expression will ensure that no directories are returned in the results?

Read this https://docs.velociraptor.app/docs/forensic/filesystem/

Some of the more important columns available are

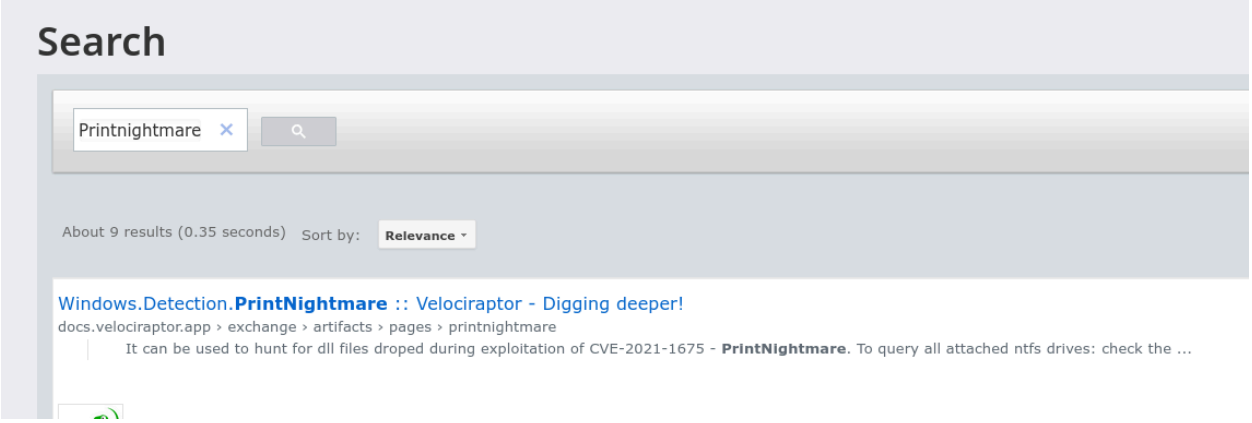
1. The `OSPath` is the complete path to the matching file, whereas the `Name` is just the filename.
2. The `Mtime`, `Atime`, `Ctime` and `Btime` are timestamps of the file.
3. The `Data` column is a free form dictionary containing key/value data about the file. This data depends on the accessor used.
4. `IsDir`, `IsLink` and `Mode` indicate what kind of file matched. (`Mode.String` can present the mode in a more human readable way).
5. Finally, in `Globs` the plugin reports which glob expression matched this particular file. This is handy when you provided a list of glob expressions to the plugin and need to know which ones produced the match.

IsDir

Task 8 Hunt for a nightmare

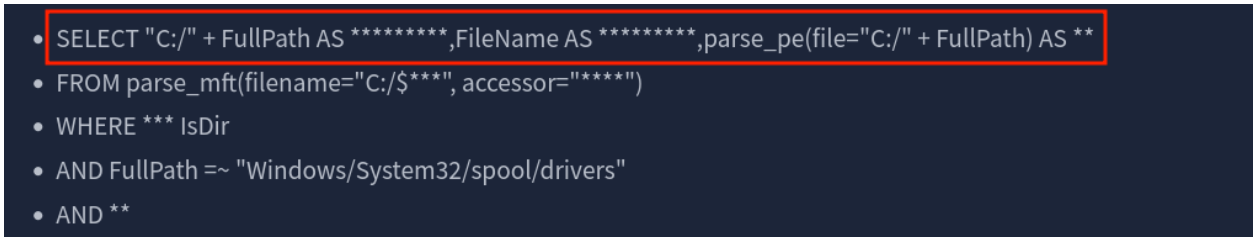
What is the name in the Artifact Exchange to detect Printnightmare?

Refer to the documentation



Windows.Detection.PrintNightmare

Per the above instructions, what is your Select clause? (no spaces after commas)
Just we need to provide the that was given by them by modifying according to the instructions

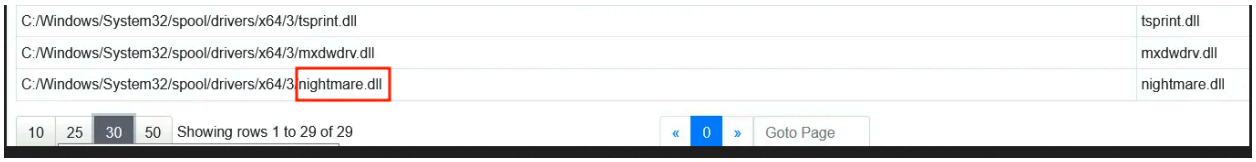


SELECT "C:/" + FullPath AS Full_Path,FileName AS File_Name,parse_pe(file="C:/" + FullPath) AS PE

What is the name of the DLL that was placed by the attacker?
For this we need to create a notebook as we learnt earlier , with query they mentioned

```
SELECT "C:/" + FullPath AS full_path,FileName AS file_name,parse_pe(file="C:/" + FullPath)
AS PE
FROM parse_mft(filename="C:/$mft", accessor="ntfs")
WHERE NOT IsDir
AND FullPath =~ "Windows/System32/spool/drivers"
AND PE
```

After creating the note book it will show calculation , after completion , get the answer



nightmare.dll

What is the PDB entry?

I used google to know about PDB , later I came to know that A .pdb is a Program Database file, which is containing the information about .dll or .exe.