# VELOCIRAPTOR

Velociraptor is an open source end point monitoring and digital forensic tool developed by Velocidex professionals which monitors activities across end points.

Some of the important activities that velociraptor performs:

1. Hunt for the evidence
2. Investigation of malware and other suspicious activities.
3. Continuous monitoring of suspicious activities.
4. Discover any disclosure of confidential information occurred outside the network.
5. Gather end point data, which is used in threat hunting and future investigations.

## Velociraptor as Threat Hunting

Velociraptor helps us to gather data from hosts that are deployed on the machine. There are options like artifacts and hunts in velociraptor to carry out checks on hosts. By collecting these data across multiple endpoints, velociraptor helps to identify potential threats.

## Velociraptor as Incident Response

Incident response teams can rapidly collect and examine artifacts from velociraptor, Velociraptor also helps in forensic details aiding in investigations. With all these features and fast processing velociraptor will act as valuable asset during critical incidents.

## VQL

Velociraptor has separate language called VQL. VQL also called as Velociraptor Query Language, helps us to identify IOC. It helps us to create our own queries and implement those queries that make our analysis faster as we are working with multiple host devices.

## Velociraptor Installation

To install velociraptor you can visit the official site and download or else there is official GitHub repository provided by Velocidex to download.

**Official Site:**

Velociraptor Download --- https://docs.velociraptor.app/downloads/

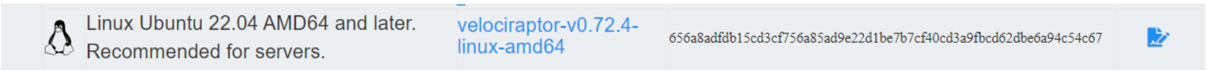
**GitHub:**

Velociraptor Download --- https://github.com/Velocidex/velociraptor/releases

So I am currently using Ubuntu version 22 as server and windows 10 as client machine. So from the document, we are going to download the compatible versions.

### Server Configuration

In my Ubuntu machine I downloaded the following version.



| | | | |
|---|---|---|---|
| Linux Ubuntu 22.04 AMD64 and later.<br>Recommended for servers. | velociraptor-v0.72.4-linux-amd64 | 656a8adfdb15cd3cf756a85ad9e22d1be7b7cf40cd3a9fbcd62dbe6a94c54c67 | |

Make sure to create a directory as mentioned below.

**sudo mkdir /opt/velociraptor**

The above is the default location that we are going to include in the upcoming velociraptor packages.

After successful download, navigate to the path of velociraptor.

Now type the following command.

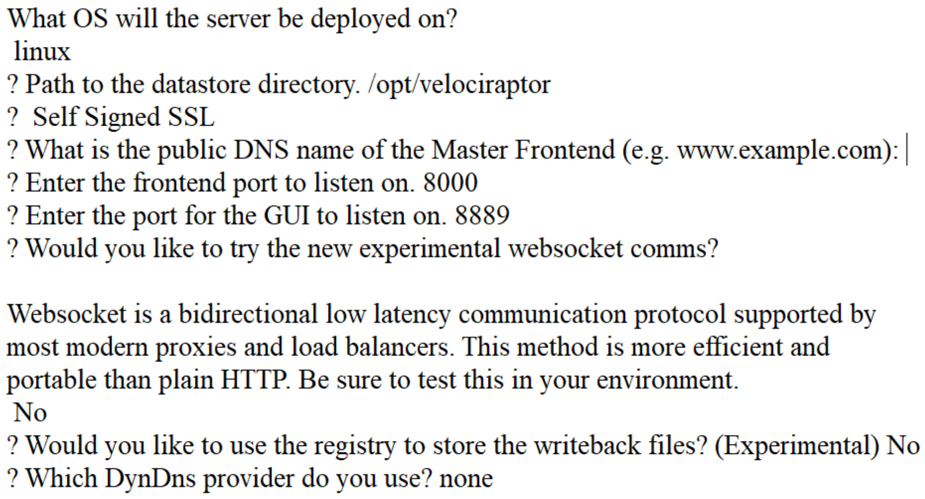
**sudo ./velociraptor-v0.72.4-linux-amd64 config generate –i**

The above command generates a velociraptor configuration file interactively.

- sudo – Admin privileges
- ./velociraptor-v0.72.4-linux-amd64 – execution of velociraptor binary file
- config generate – initiate configuration process
- -i – interactive mode

Now you will be asked the few questions. Answer the questions as per your OS that is being used. Velociraptor gives some default options. Leave it as default.

For example I have listed out the following options



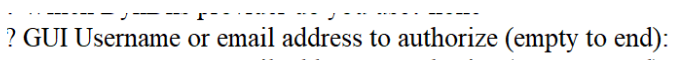
```
What OS will the server be deployed on?
 linux
? Path to the datastore directory. /opt/velociraptor
?  Self Signed SSL
? What is the public DNS name of the Master Frontend (e.g. www.example.com):
? Enter the frontend port to listen on. 8000
? Enter the port for the GUI to listen on. 8889
? Would you like to try the new experimental websocket comms?

Websocket is a bidirectional low latency communication protocol supported by
most modern proxies and load balancers. This method is more efficient and
portable than plain HTTP. Be sure to test this in your environment.
 No
? Would you like to use the registry to store the writeback files? (Experimental) No
? Which DynDns provider do you use? none
```

As my OS is Ubuntu so I choose **linux**. Now for directory, we had already created. Enter the directory path **/opt/velociraptor.** The next, choose the **Self Signed SSL** option. Now for the DNS enter your IP address. [Since I don't have any private domain]. Now for the rest you can leave it as default [follow the defaults].

There registry options and DynDns you can use **no.**

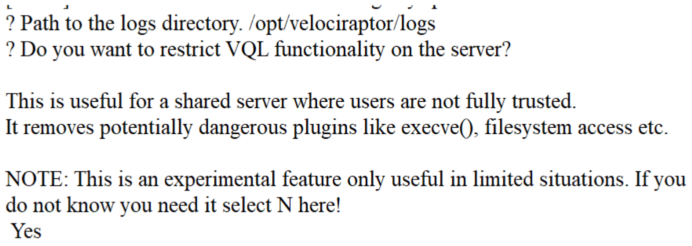
Now it will ask username and password.



```
? GUI Username or email address to authorize (empty to end):
```

Enter username and password and click enter. Remember your username and password, since it will be required when we are using velociraptor as GUI.

Again you will be asked some questions.



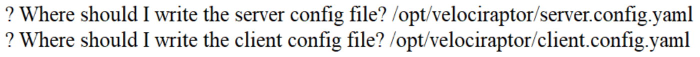
```
? Path to the logs directory. /opt/velociraptor/logs
? Do you want to restrict VQL functionality on the server?

This is useful for a shared server where users are not fully trusted.
It removes potentially dangerous plugins like execve(), filesystem access etc.

NOTE: This is an experimental feature only useful in limited situations. If you
do not know you need it select N here!
 Yes
```

Just follow the instructions that velociraptor provides. [Velociraptor provides that what you need to do at end of questions]

Now it will ask where to write client and server configuration file. You can follow as mentioned below.



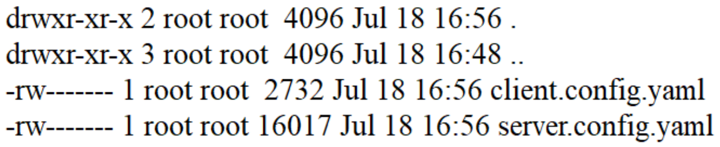
```
? Where should I write the server config file? /opt/velociraptor/server.config.yaml
? Where should I write the client config file? /opt/velociraptor/client.config.yaml
```

The path will be - **/opt/velociraptor/"type of file"**

The file extensions will be yaml format.

You can also see the permissions of the file by using the following command as mentioned below.

Command **-- ls –la /opt/velociraptor**

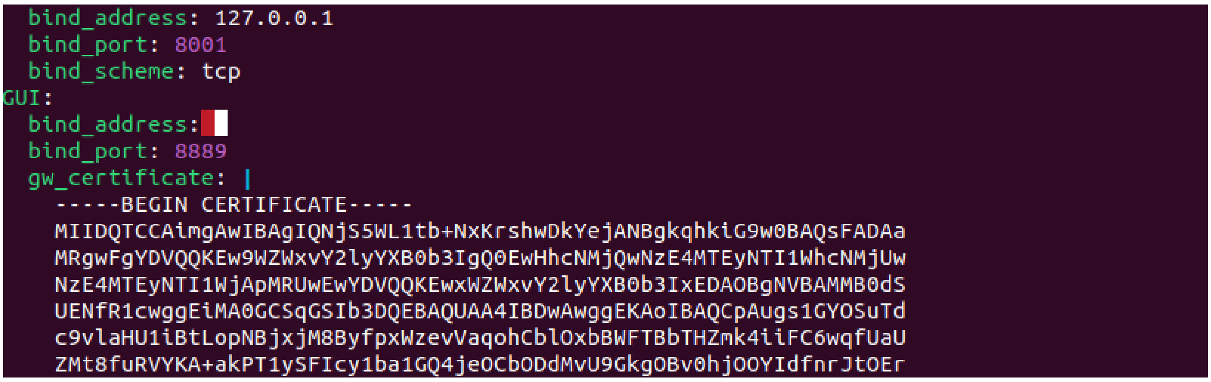


```
drwxr-xr-x 2 root root  4096 Jul 18 16:56 .
drwxr-xr-x 3 root root  4096 Jul 18 16:48 ..
-rw------- 1 root root  2732 Jul 18 16:56 client.config.yaml
-rw------- 1 root root 16017 Jul 18 16:56 server.config.yaml
```

Now we need to change the GUI part of server configuration file. To do so enter the following command.

**sudo nano /opt/velociraptor/server.config.yaml**

Search for GUI and enter your IP address. Save It and exit.



```
  bind_address: 127.0.0.1
  bind_port: 8001
  bind_scheme: tcp
GUI:
  bind_address:
  bind_port: 8889
  gw_certificate: |
    -----BEGIN CERTIFICATE-----
    MIIDQTCCAimgAwIBAgIQNjS5WL1tb+NxKrshwDkYejANBgkqhkiG9w0BAQsFADAa
    MRgwFgYDVQQKEw9WZWxvY2lyYXB0b3IgQ0EwHhcNMjQwNzE4MTEyNTI1WhcNMjUw
    NzE4MTEyNTI1WjApMRUwEwYDVQQKEwxWZWxvY2lyYXB0b3IxEDAOBgNVBAMMB0dS
    UENfR1cwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCpAugs1GYOSuTd
    c9vlaHU1iBtLopNBjxjM8ByfpxWzevVaqohCblOxbBWFTBbTHZmk4iiFC6wqfUaU
    ZMt8fuRVYKA+akPT1ySFIcy1ba1GQ4jeOCbODdMvU9GkgOBv0hjOOYIdfnrJtOEr
```

Now we need to create the server package.

**sudo ./velociraptor-v0.72.4-linux-amd64 --config /opt/velociraptor/server.config.yaml debian server --binary velociraptor-v0.72.4-linux-amd64**

This command runs Velociraptor as a server on a Debian system, using the specified configuration file. The sudo prefix ensures elevated privileges for this operation.

A server package named **velociraptor_server_0.72.4_amd64.deb** will be created.

Now we need to install the server package that was created.

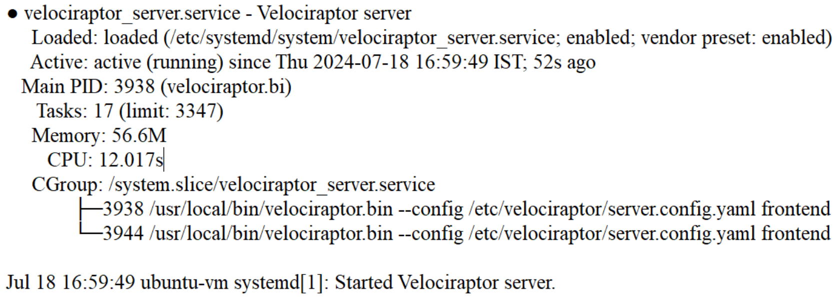
**sudo dpkg -i velociraptor_server_0.72.4_amd64.deb**

The dpkg tool is a package manager which handles package installation, removal, and management. It's for debian based systems. This command installs the Velociraptor server package from the specified .deb file.

After installation if you check list of files you will get the following by using ls –la.

```
drwxr-xr-x 9 velociraptor velociraptor  4096 Jul 18 16:59 .
drwxr-xr-x 3 root         root          4096 Jul 18 16:48 ..
drwx------ 2 velociraptor velociraptor  4096 Jul 18 16:59 acl
-rw------- 1 velociraptor velociraptor  2732 Jul 18 16:56 client.config.yaml
drwx------ 3 velociraptor velociraptor  4096 Jul 18 16:59 clients
drwxr-xr-x 3 velociraptor velociraptor  4096 Jul 18 16:59 config
drwx------ 2 velociraptor velociraptor  4096 Jul 18 16:59 logs
drwx------ 3 velociraptor velociraptor  4096 Jul 18 16:59 server_artifact_logs
drwx------ 5 velociraptor velociraptor  4096 Jul 18 17:00 server_artifacts
-rw------- 1 velociraptor velociraptor 16022 Jul 18 16:58 server.config.yaml
drwx------ 2 velociraptor velociraptor  4096 Jul 18 16:59 users
```

Now to start the velociraptor service **systemctl status velociraptor_server.service.**



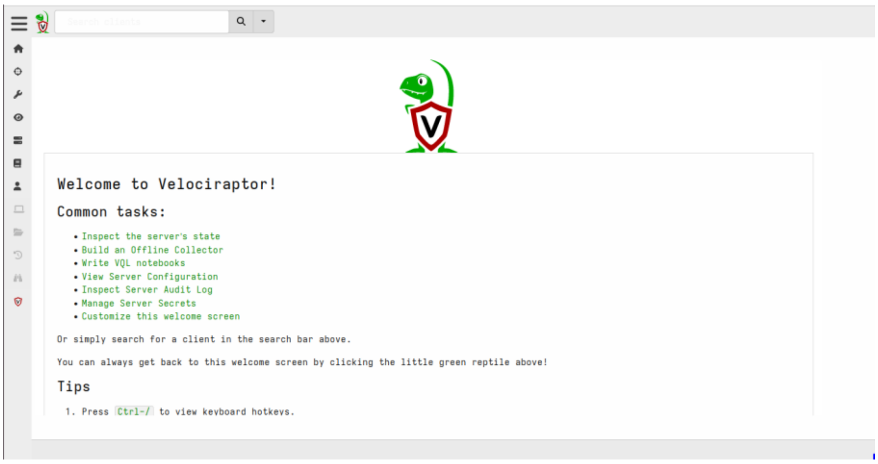
```
● velociraptor_server.service - Velociraptor server
   Loaded: loaded (/etc/systemd/system/velociraptor_server.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2024-07-18 16:59:49 IST; 52s ago
 Main PID: 3938 (velociraptor.bi)
    Tasks: 17 (limit: 3347)
   Memory: 56.6M
      CPU: 12.017s
   CGroup: /system.slice/velociraptor_server.service
           ├─3938 /usr/local/bin/velociraptor.bin --config /etc/velociraptor/server.config.yaml frontend
           └─3944 /usr/local/bin/velociraptor.bin --config /etc/velociraptor/server.config.yaml frontend

Jul 18 16:59:49 ubuntu-vm systemd[1]: Started Velociraptor server.
```

The server configuration is completed. To open the server open the browser and type IP with the port 8889.

We are using 8889 as port because we mentioned it as GUI port in the previous steps.

Search **-- https://ip:8889**



Welcome to Velociraptor!

Common tasks:

- Inspect the server's state
- Build an Offline Collector
- Write VQL notebooks
- View Server Configuration
- Inspect Server Audit Log
- Manage Server Secrets
- Customize this welcome screen

Or simply search for a client in the search bar above.

You can always get back to this welcome screen by clicking the little green reptile above!

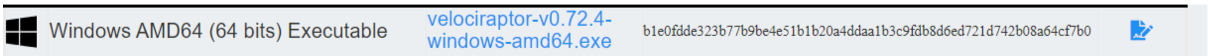
Tips

1. Press Ctrl-/ to view keyboard hotkeys.

Now we had complete installation of server. Click on the search icon. You will find empty.

Now we need to client machine to the server.

Since I am using my windows 10 as operating system, I am going to install the following executable in my server machine.



| | | | |
|---|---|---|---|
| Windows AMD64 (64 bits) Executable | velociraptor-v0.72.4-windows-amd64.exe | b1e0fdde323b77b9be4e51b1b20a4ddaa1b3c9fdb8d6ed721d742b08a64cf7b0 | |

After successful installation of windows, follow the given steps.

**sudo ./velociraptor-v0.72.4-linux-amd64 config repack --exe velociraptor**

This command repacks the velociraptor binary, potentially embedding additional configuration information.

repack function -- modifies and repackages a binary or MSI (Microsoft Installer) file.

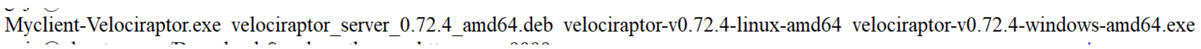
Repackaging involves creating a new binary that includes the modifications. This repacked binary can then be distributed or deployed. It allows you to tailor Velociraptor to your specific needs without altering the original source code.

**sudo ./velociraptor-v0.72.4-linux-amd64 config repack --exe velociraptor-v0.72.4-windows-amd64.exe /opt/velociraptor/client.config.yaml Myclient-Velociraptor.exe**

**Myclient-Velociraptor.exe – you can name as per your wish but need to be exe format.**

This command repacks the velociraptor-v0.72.4-windows-amd64.exe binary with the specified client configuration (client.config.yaml) and creates a new binary named Myclient-Velociraptor.exe

Now you will find the following files



```
Myclient-Velociraptor.exe  velociraptor_server_0.72.4_amd64.deb  velociraptor-v0.72.4-linux-amd64  velociraptor-v0.72.4-windows-amd64.exe
```

Myclient-Velocirapotor.exe is the executable file and we need to transfer this file to the windows machine.

Now open the http server, in Ubuntu machine and transfer the file

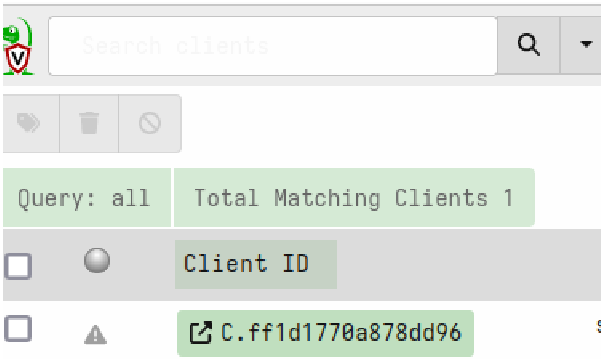
**sudo python -m http.server 8080**

The above command will open the http port and now in windows enter the Ubuntu IP along the port.

Download the Myclient-Velocirapotor.exe. Open power shell as administrator, navigate to the downloaded path. Now enter the following command.

**Myclient-Velocirapotor.exe service install**

That's it. Now refresh the server screen and click on the search icon, there you will the client.

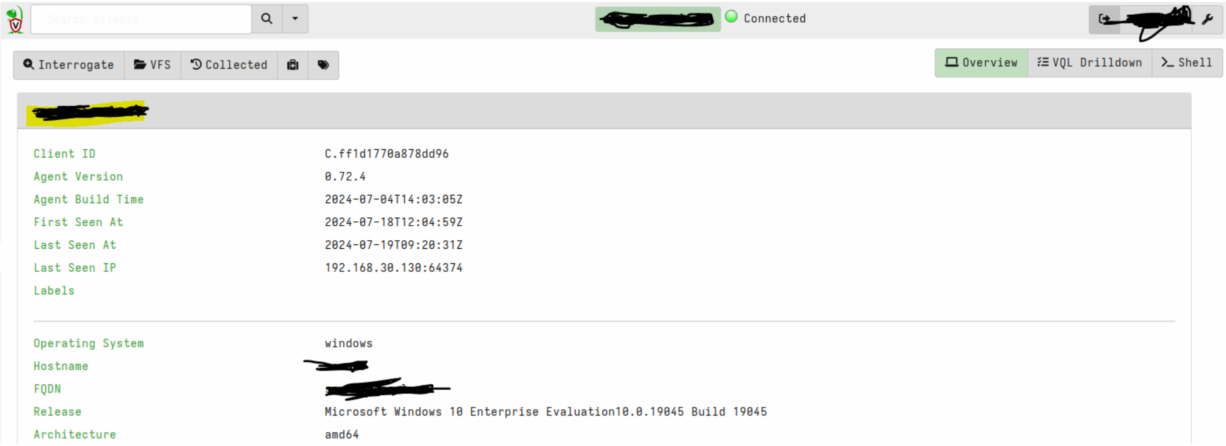


Query: all

Total Matching Clients 1

| | | Client ID |
|---|---|---|
| □ | ● | C.ff1d1770a878dd96 |

Now click on the client, you will find the host information

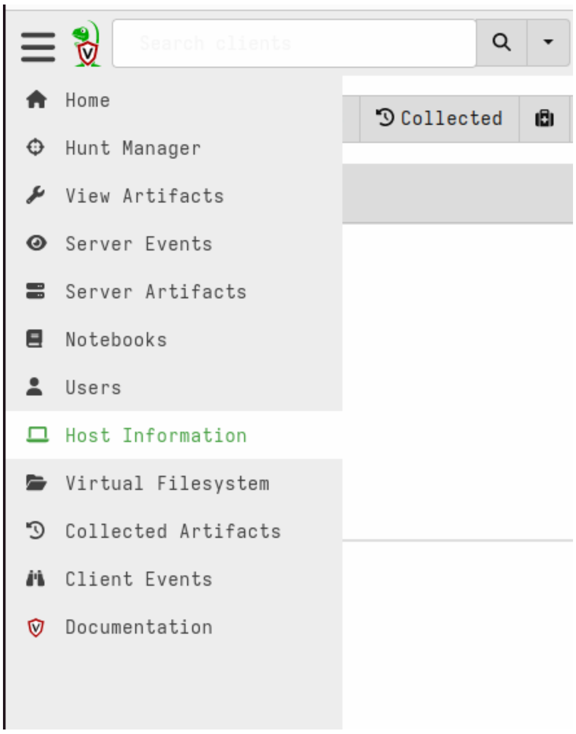


[redacted]

Client ID C.ff1d1770a878dd96
Agent Version 0.72.4
Agent Build Time 2024-07-04T14:03:05Z
First Seen At 2024-07-18T12:04:59Z
Last Seen At 2024-07-19T09:20:31Z
Last Seen IP 192.168.30.130:64374
Labels

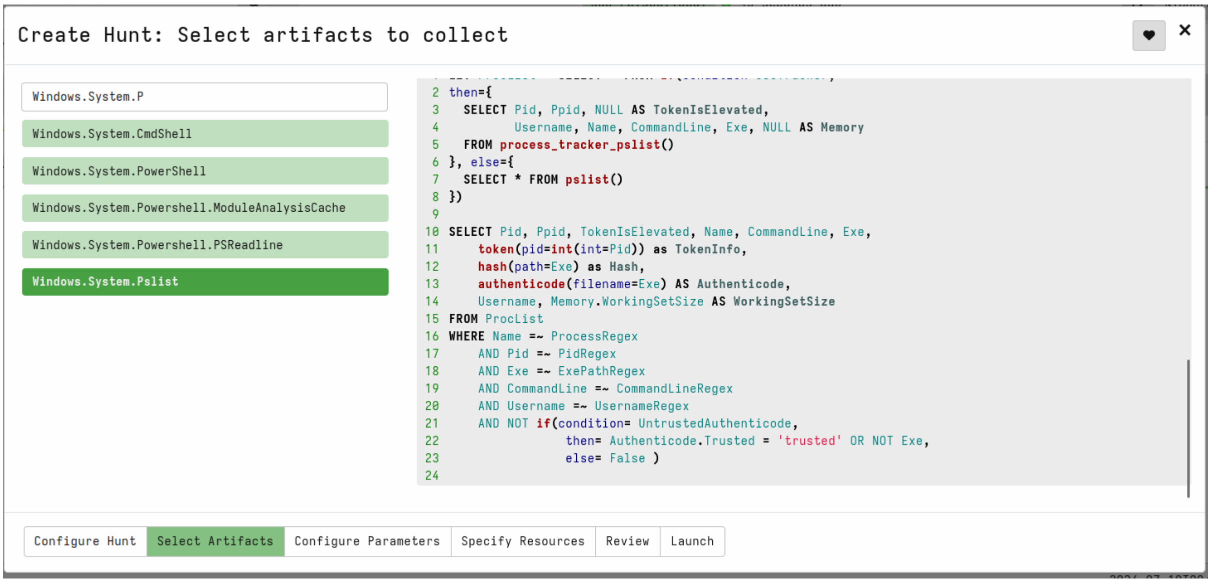
Operating System windows
Hostname [redacted]
FQDN [redacted]
Release Microsoft Windows 10 Enterprise Evaluation10.0.19045 Build 19045
Architecture amd64

The functionalities provided by the velociraptor



We had hunt manager which was used to create new hunts from client, Artifacts which was used to perform the operation as per our requirements etc.

Artifacts in Velociraptor are predefined queries or scripts designed to collect, parse, and analyse specific types of data from endpoints.



Create Hunt: Select artifacts to collect

Windows.System.P

- Windows.System.CmdShell
- Windows.System.PowerShell
- Windows.System.Powershell.ModuleAnalysisCache
- Windows.System.Powershell.PSReadline
- Windows.System.Pslist

```
then={
  SELECT Pid, Ppid, NULL AS TokenIsElevated,
         Username, Name, CommandLine, Exe, NULL AS Memory
  FROM process_tracker_pslist()
}, else={
  SELECT * FROM pslist()
})

SELECT Pid, Ppid, TokenIsElevated, Name, CommandLine, Exe,
    token(pid=int(int=Pid)) as TokenInfo,
    hash(path=Exe) as Hash,
    authenticode(filename=Exe) AS Authenticode,
    Username, Memory.WorkingSetSize AS WorkingSetSize
FROM ProcList
WHERE Name =~ ProcessRegex
    AND Pid =~ PidRegex
    AND Exe =~ ExePathRegex
    AND CommandLine =~ CommandLineRegex
    AND Username =~ UsernameRegex
    AND NOT if(condition= UntrustedAuthenticode,
                then= Authenticode.Trusted = 'trusted' OR NOT Exe,
                else= False )
```

The left side represents Artifact list and the right side represent VQL.

NOTE: VQL is case sensitive. You can create your own VQL queries for analysis of data.

Artifacts are a core component of Velociraptor, enabling security teams to efficiently collect and analyse endpoint data, enhancing their ability to respond to and investigate security incidents.

In short Velociraptor, An open source end point tool used for threat hunting, Digital Forensics and Incident Response, uses VQL to collect and analyse data from endpoints. It uses artifacts to gather system information, detect threats, and investigate incidents efficiently.