Velociraptor stands out as an innovative, open-source platform for endpoint monitoring, digital forensics, and cyber response. Created by professionals in Digital Forensic and Incident Response (DFIR), it offers an effective solution for artifact hunting and activity monitoring across numerous endpoints.

This platform is composed of two elements: a server, which can be hosted either locally or in the cloud, and multiple client modules deployed across network endpoints. Interestingly, both server and client functionalities are encompassed within the same binary file, simplifying deployment and allowing for swift setup.

A remarkable feature of Velociraptor is its scalability: a single server can efficiently manage up to 15,000 clients. For larger networks, its scalable architecture enables the deployment of multiple front-ends to monitor clients in various regions.

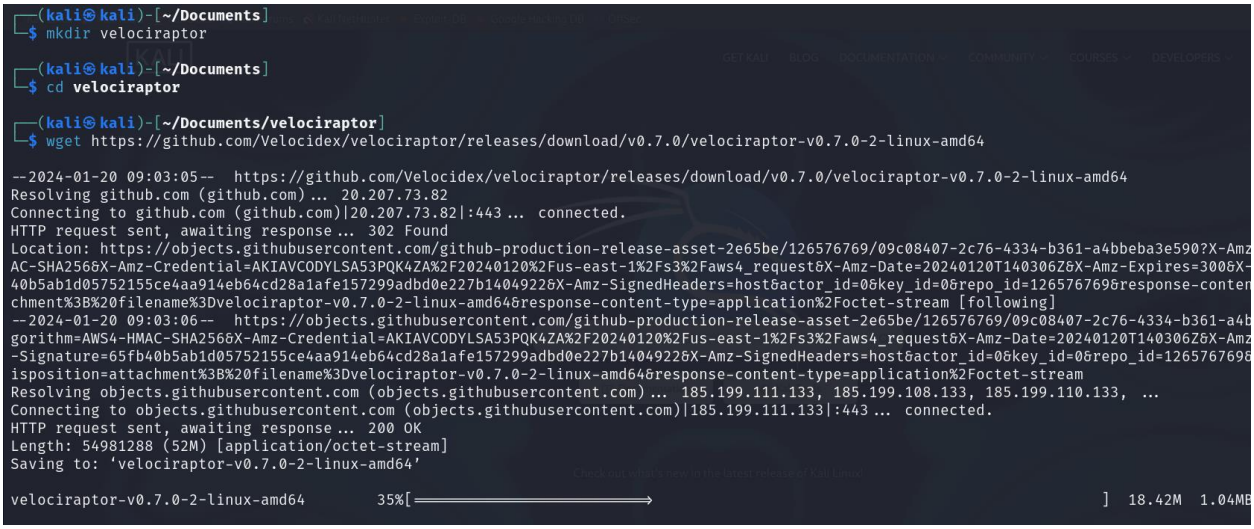
The server's role is primarily to collect and store query results, while the clients perform the bulk of data aggregation from multiple sources. This distributed workload approach might even result in a lower system footprint compared to some major commercial Endpoint Detection and Response (EDR) suites.

Velociraptor employs a versatile query language called VQL, enabling the collection, querying, and monitoring of virtually any endpoint aspect, whether individually, in groups, or across an entire network.

Now, let's delve into setting up a Velociraptor server on a local Kali Linux machine and a client on a Windows system. I will demonstrate this using virtual machines running Kali Linux and Windows 10.

First, download Velociraptor from its official GitHub repository:

```
wget
https://github.com/Velocidex/velociraptor/releases/download/v0.7.0/velociraptor-v0.7.0-2-linux-amd64
```



Next, assign the necessary execution permissions:

```
sudo chmod +x velociraptor-v0.7.0-2-linux-amd64
```

We then generate a configuration file:

```
. /velociraptor-v0.7.0-2-linux-amd64 config generate >
velociraptor.config.yaml
```

Edit the file with a text editor (I prefer nano):

```
nano velociraptor.config.yaml
```

Search and replace 'localhost' and '127.0.0.1' with your server's IP address (they appear twice and thrice, respectively). Save your changes.

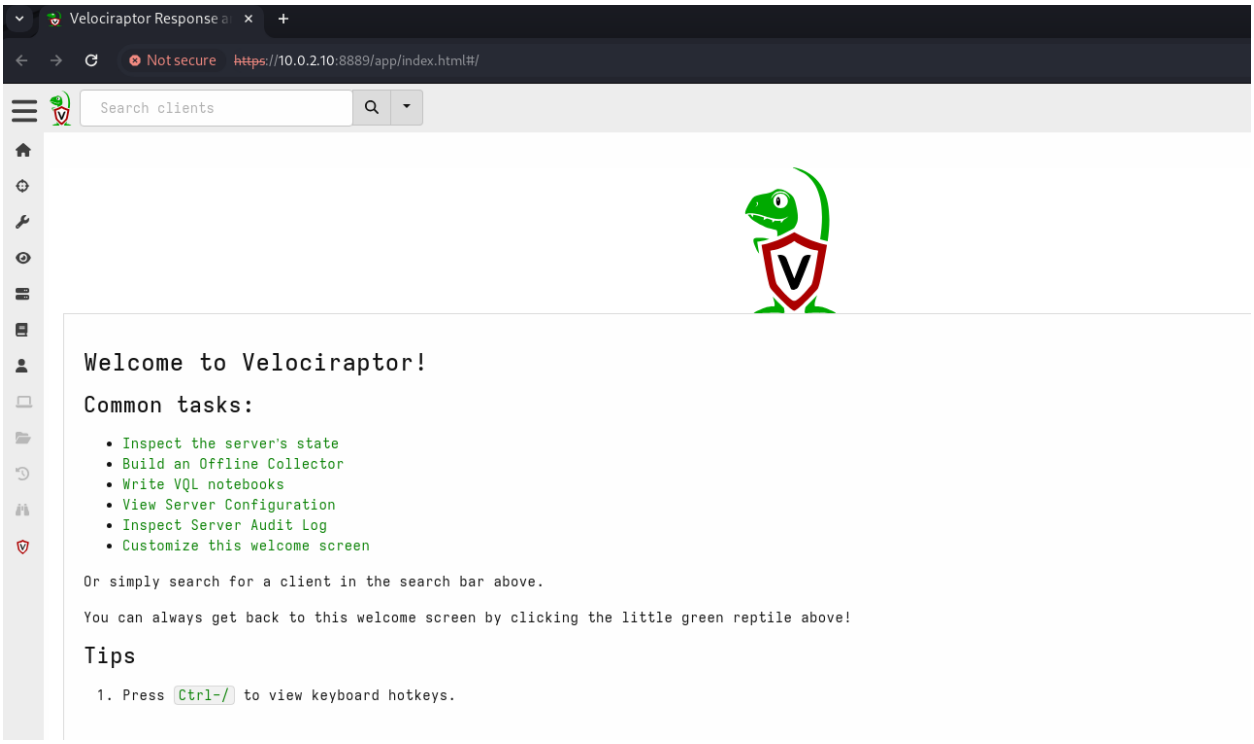
To utilize Velociraptor as a superuser, create an admin account with administrator privileges:

```
./velociraptor-v0.7.0-2-linux-amd64 --config /etc/velociraptor.config.yaml
user add admin --role administrator
```

Launch the server with the following command:

```
./velociraptor-v0.7.0-2-linux-amd64 --config /etc/velociraptor.config.yaml
frontend -v
```

Access the server using http://yourlocalhostaddress:8889/ and log in with your admin credentials.



The dashboard displays various metrics, like the number of connected clients, current server load, and memory usage. Notably, you can customize the dashboard to fit your needs.

Adding a Windows Client:

Modify the 'velociraptor.config.yaml' file (now in the etc directory):
`sudo nano /etc/velociraptor.config.yaml`

After the "END CERTIFICATE" line and the "nonce: line", add:
`use_self_signed_ssl: true`

```
    ttjJBA1/kRM8+sPMiGCMqARuKM3+nj2BTbMJD8AoP3dUQK/bJnOEo6/lFegd8mlz
    QzCHrxmERjUbLVJIp1ZmMkTUpHtnvqOszfAEMd87b82Z2SOfKF6vKxi69uLO1LWM
    BDh/lKhKKDGynMnhoODTPVGKhAinGd+AhbP6CI8iANfnA9n67HPzJSet1Hi5EkqB
    ZUhmEwJPQ4J1byqITzXHfvsrENL/2tlr114LI+n1Il69DVTGAB9zAgMBAAGjgYww
    gYkwDgYDVR0PAQH/BAQDAgKkMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcD
    AjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBS5DuNADAIaNS6uJ237aiLISoG9
    wDAoBgNVHREEITAfgh1WZWxvY2lyYXB0b3JfY2EudmVsb2NpZGV4LmNvbTANBgkq
    hkiG9w0BAQsFAAOCAQEAqbRNT6mqidE/4UzpxgCy+GGdfBJDA4wSgmXDAHadFRa6
    PVxcuer/rQBSsYifO1fcukLzuE+ypOZ+GIZ9jiSeDfyhwzJHtbBBML5uZF9svLmK
    TdFkyjAsnb21xRGae2bq3mhO3M3MUFSKZdlc4jU6vqVshwfWCZbLJ5CWahMcHX+a
    0Wj4eds8WWX0LnlhT1yzAfJsG2F3G7xoj1JJna5DFDjZl0ehnVdrpD7UIVTuDPSK
    DuNUh83Ac0hjP+1zQCG4lvvGRiQlUyEvjB0KcdB0uDyEJC42Ul2On/ZIHvQQQ5c6
    Ny98iwGGJvsSeKX9d5UhnJugk9Dxitmk1eLwasWF+A==
    -----END CERTIFICATE-----
nonce: 1cG09Q8xTOY=
use_self_signed_ssl: true
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:
```

Execute these commands to prepare a Windows installer:

```
./velociraptor-v0.7.0-2-linux-amd64 --config /etc/velociraptor.config.yaml
config client > client.config.yaml
```

```
wget
https://github.com/Velocidex/velociraptor/releases/download/v0.7.0/velociraptor-v0.7.0-2-windows-amd64.exe
```

```
./velociraptor-v0.7.0-2-linux-amd64 config repack --exe velociraptor-v0.7.0-2-windows-amd64.exe client.config.yaml repackaged_velociraptor.exe
```

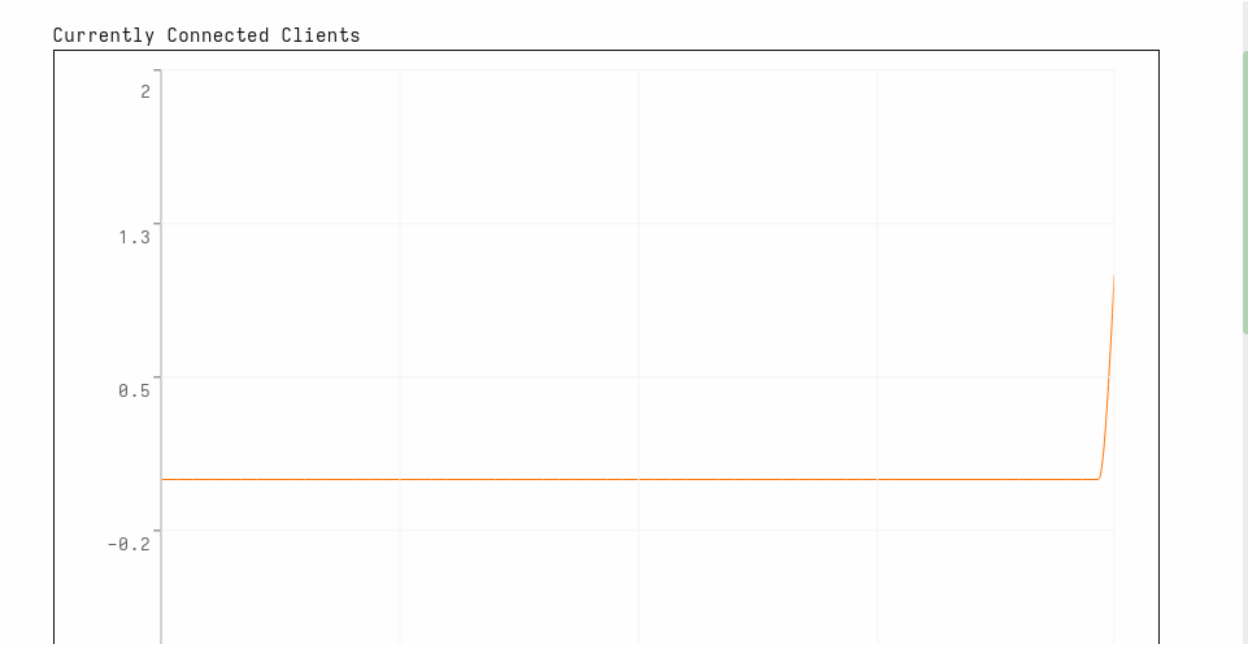
Transfer the repackaged file to the Windows machine. I used netcat:

Receiver: nc -nvlp 10.0.2.15 2555 > repackaged_velociraptor.exe
Sender: nc –v 10.0.2.15 2555 < repackaged_velociraptor.exe

On the Windows machine, run:
`repackaged_velociraptor.exe service install`

Note: Ensure all Windows Defender and antivirus services are disabled for this setup.

On server you will see and client has been added successfully.



References

For further information, refer to the Velociraptor Documentation.

Using Velociraptor for large-scale endpoint visibility and rapid threat

https://www.pentestpartners.com/security-blog/using-velociraptor-for-large-scale-endpoint-visibility-and-rapid-threat-hunting/.