Velociraptor Incident Response and Monitoring | Setup and Configuration

Contents

Abstract:

In the ever-evolving world of cybersecurity, incident response and monitoring tools have become indispensable for organizations of all sizes to effectively identify, investigate, and remediate security incidents. Velociraptor, an open-source incident response platform, stands out as a powerful and versatile tool that can be tailored to meet the specific needs of any organization.

Target Audiences:

This blog post is specifically geared towards two primary audiences:

1. Small and startup organizations or DFIR teams who do not have enough budget to buy commercial tools with the same use cases. Velociraptor offers a cost-effective and feature-rich alternative to expensive commercial solutions, making it an ideal choice for resource-constrained teams.

2. DFIR practitioners who are looking for a robust and customizable incident response platform to enhance their investigative capabilities and streamline their workflow.

Key Takeaways:

- Velociraptor is a versatile and powerful incident response platform that can be used to manage investigations, gather evidence, and remediate security incidents across multiple platforms.

- Velociraptor's open-source nature allows for extensive customization and integration with other tools, making it a flexible solution for a wide range of organizations.

- Velociraptor's scalability makes it suitable for both small and large organizations, with the ability to manage hundreds or even thousands of endpoints.

Overview of the Velociraptor Incident Response and Monitoring Tool:

Velociraptor is a comprehensive incident response and monitoring platform that provides a centralized repository for collecting, storing, and analysing event data. It utilizes a distributed architecture that allows it to gather data from endpoints and cloud environments, enabling organizations to gain a holistic view of their security posture.

Velociraptor's key features include:

- Artifact Collection: Velociraptor can collect a wide range of artifacts from endpoints, including files, registry entries, and network traffic.

- Evidence Analysis: Velociraptor provides powerful tools for analysing collected artifacts, enabling investigators to identify and interpret potential security threats.

- Incident Response Automation: Velociraptor can automate incident response workflows, streamlining the process of identifying, investigating, and remediating security incidents.

- Integrations: Velociraptor seamlessly integrates with a variety of other tools, including SIEMs, EDRs, and threat intelligence platforms.

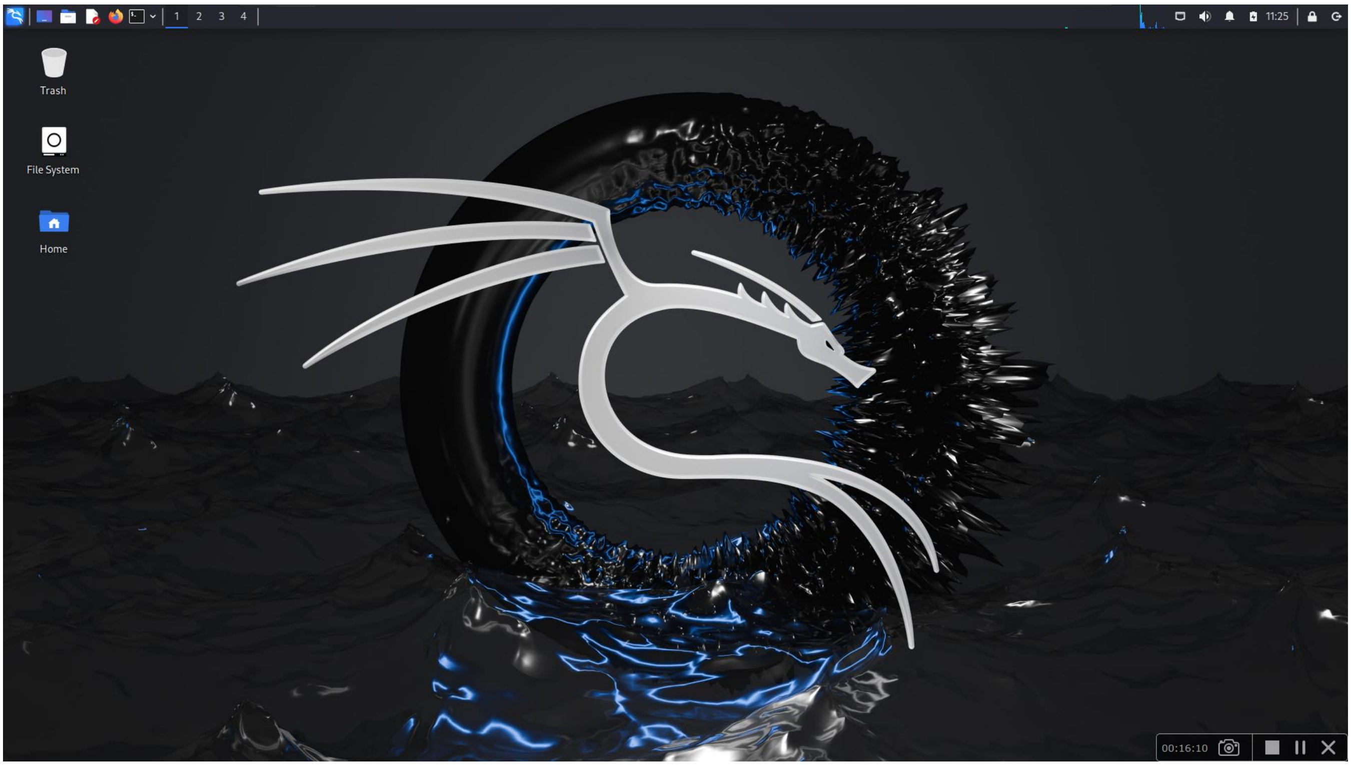
BLUF (Bottom Line Upfront):

Velociraptor stands as a compelling incident response and monitoring solution for organizations of all sizes. Its open-source nature, scalability, and versatility make it an attractive choice for those seeking a cost-effective, powerful, and customizable tool to enhance their security posture.

Technical Guide | Unleash the Power of Velociraptor

Velociraptor can be deployed on both Linux and Windows systems. This guide will walk you through the process of installing and configuring Velociraptor on both platforms.

Part 1: Server Installation and Configuration of Velociraptor (Kali)



1. Create a folder for Velociraptor in the /opt Linux directory named vraptor using the command mkdir vraptor.
2. Change the directory into vraptor with cd vraptor.
3. Download the Velociraptor executable Version 0.6.9 from GitHub using the command:
    - wget https://github.com/Velocidex/velociraptor/releases/download/v0.6.9/velociraptor-v0.6.9-linux-amd64.
4. Rename the downloaded file to vraptor for convenience.
5. Make the file executable using the command chmod +x vraptor.
6. Generate a configuration file using the command vraptor config generate and store it in /etc/velociraptor.config.yml.
    - ./vraptor config generate > /etc/velociraptor.config.
7. Update the configuration file with your IP addresses using nano /etc/velociraptor.config.yml. You need to change the IP address in four places: the server URL, the API, the GUI, and the monitoring host.

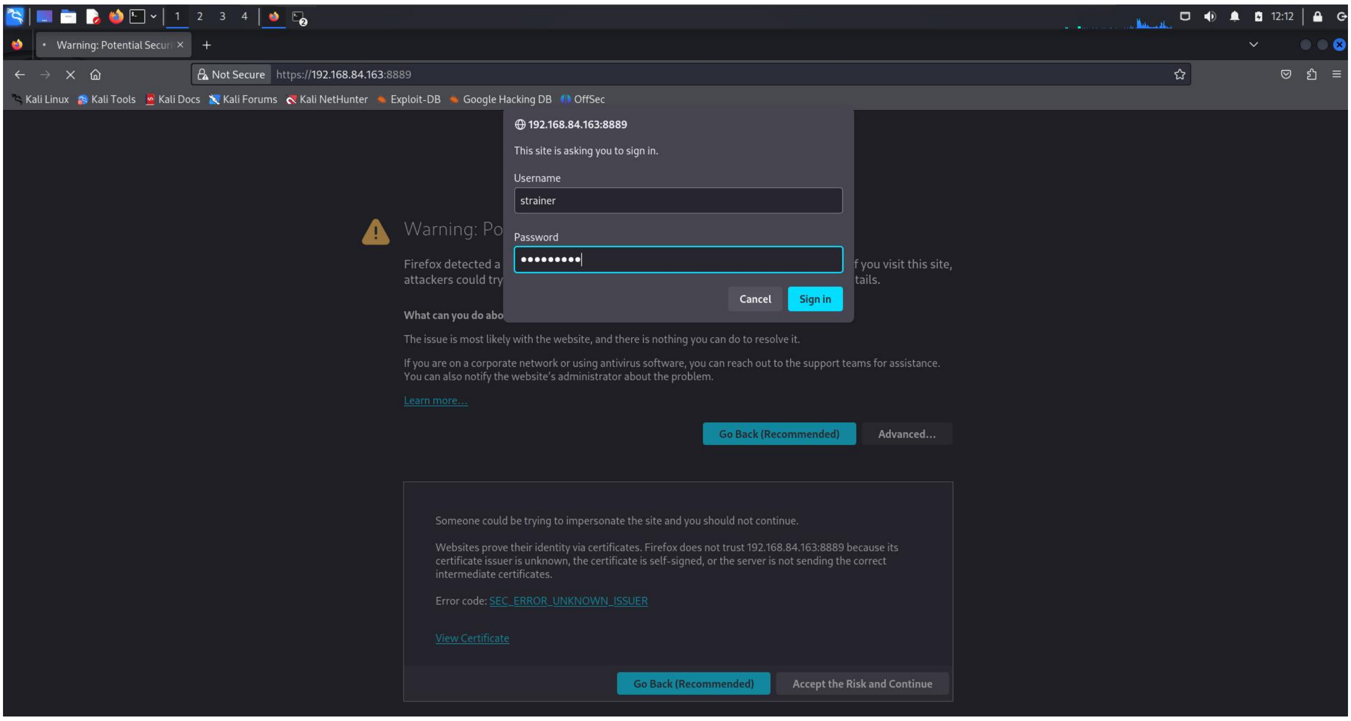
8. Allow self-signed certificates when using HTTPS by adding the line use_self_signed_ssl: true below the server URL () in the configuration file.
9. Create a strainer admin user with the command. /vraptor --config /etc/velociraptor.config.yaml user add strainer --role administrator. Set the password as a “strainer”.
   - ./vraptor --config /etc/velociraptor.config.yml user add strainer --role administrator
10. Start Velociraptor using the command:
    - ./vraptor --config /etc/velociraptor.config.yml frontend -v
11. Access the frontend through Port 8889 (https://192.168.84.163:8889/) and log in with your credentials.
12. *Change the IP to your own address.*
13. Create a service definition file /etc/systemd/system/vraptor.service and set the Unit, Service, and Install sections accordingly.

```
[Unit]
Description=Velociraptor IR
After=network.target

[Service]
Type=simple
User=root
ExecStart=/opt/vraptor/vraptor --config /etc/velociraptor.config.yml frontend -v

[Install]
WantedBy=multi-user.target
```

14. Enable the service with sudo systemctl enable vraptor.
    - systemctl enable vraptor
    - Created symlink /etc/systemd/system/multi-user.target.wants/vraptor.service → /etc/systemd/system/vraptor.service.

Please replace **192.168.84.163** with your actual IP address and the username also. Ensure that you have the necessary permissions to execute these commands.

Ping me on [LinkedIn]() if you need further assistance! 😊



192.168.84.163:8889

This site is asking you to sign in.

Username: strainer

Password: •••••••••

Firefox detected a ... if you visit this site, attackers could try ... tails.

What can you do abo

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Learn more...

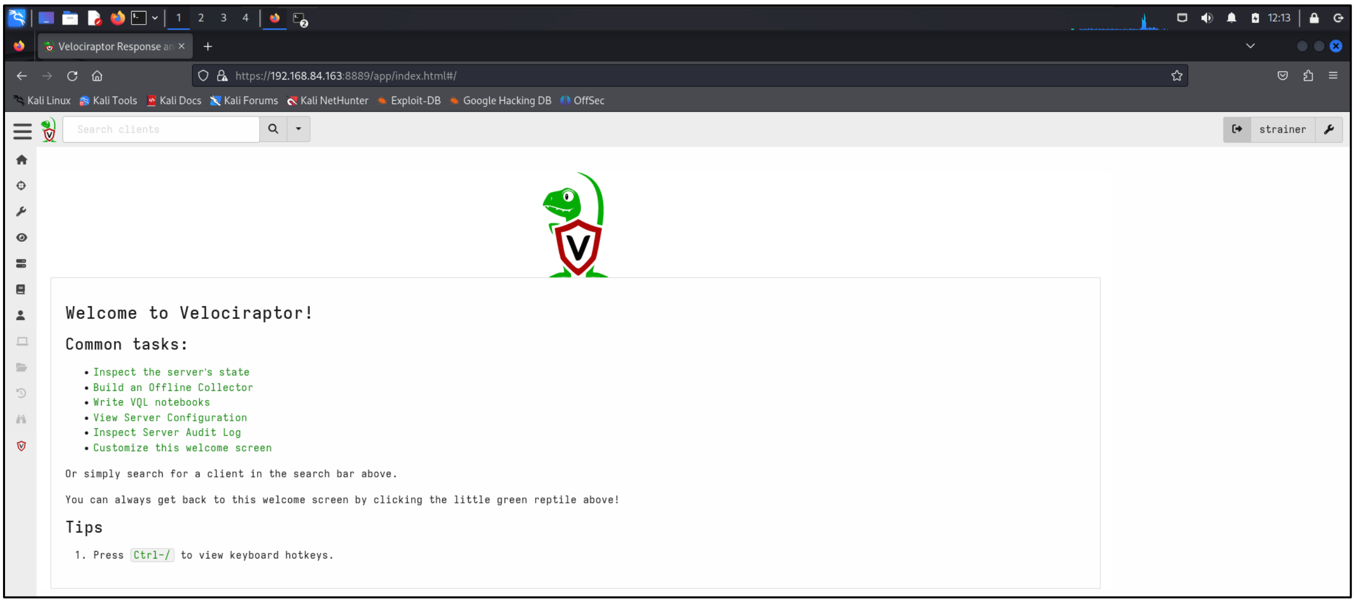
Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust 192.168.84.163:8889 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

View Certificate

Go Back (Recommended)
Accept the Risk and Continue



Velociraptor Response an
https://192.168.84.163:8889/app/index.html#/
Search clients
strainer

Welcome to Velociraptor!

Common tasks:

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

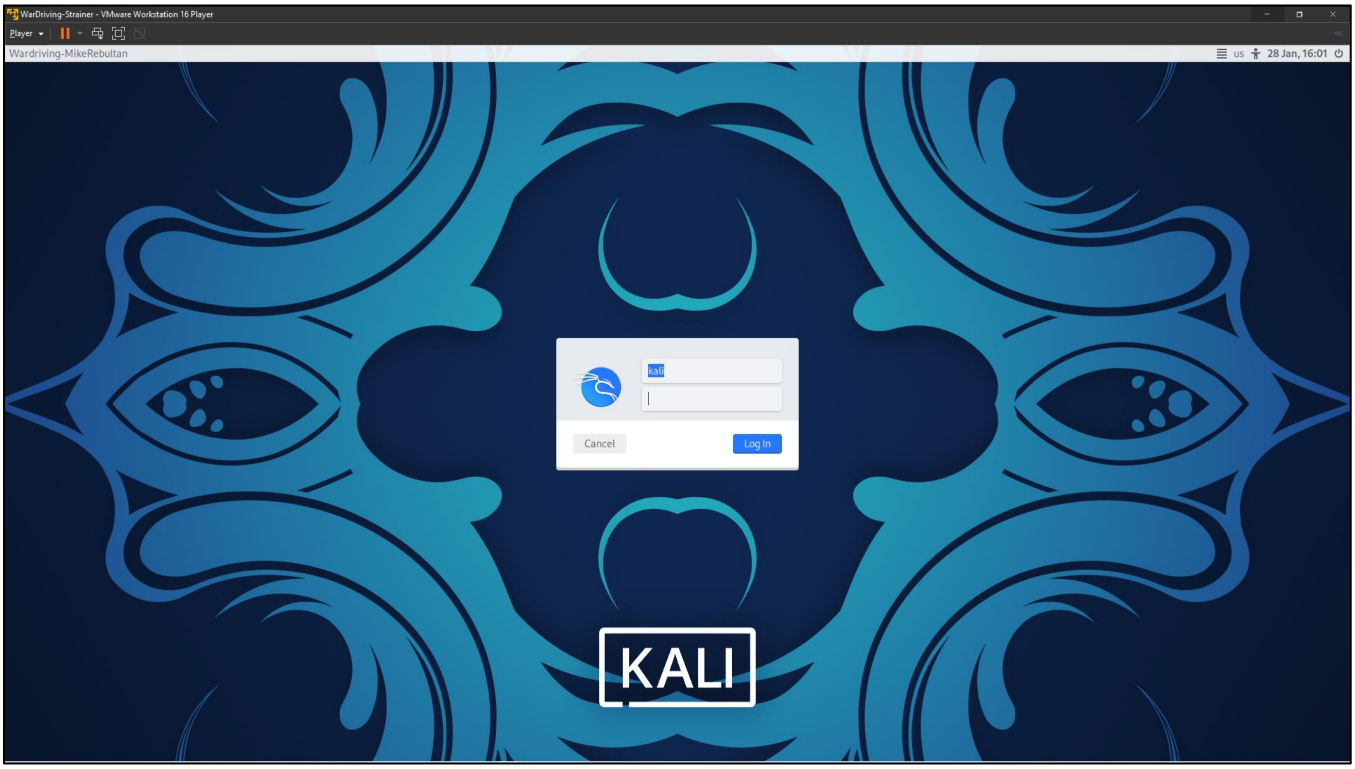
Or simply search for a client in the search bar above.

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

Tips

1. Press `Ctrl-/` to view keyboard hotkeys.

Part 2: Connecting Linux hosts to Velociraptor (Debian OS Client)



1. Generate a client configuration file on your Velociraptor server using the command vraptor --config /etc/velociraptor.config.yaml config client > client.config.yaml.

- └─# ./vraptor --config /etc/velociraptor.config.yml config client > client.config.yaml

2. Open a web server to download the executable and configuration files to your clients. If Velociraptor is running, stop it with systemctl stop vraptor and then restart the server using start.

- systemctl stop vraptor
- systemctl start vraptor

3. On your client machine (e.g., web01), create a `vraptor` folder with mkdir vraptor and change directory into it with cd vraptor.
   - mkdir /opt/vraptor
   - cd /opt/vraptor/
4. Download the binary and configuration files from the server using
   - Option 1: Download directly from the server with “wget” command
     - wget http://192.168.84.163:8000/vraptor
     - wget http://192.168.84.163:8000/client.config.yaml.

   - Option 2: Manually download the 2 files from the server then upload them in the client.

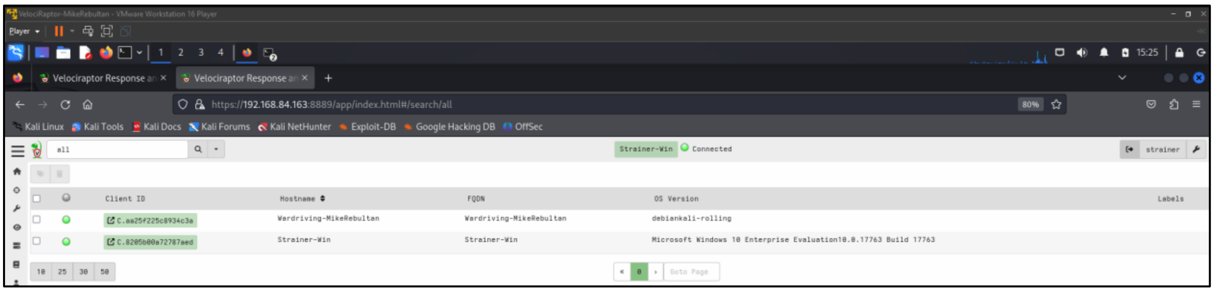
5. Set up the client to automatically start on reboot. Create a service definition file /etc/systemd/system/vraptor.service and set the Unit, Service, and Install sections accordingly.

6. vi /etc/systemd/system/vraptor.service

```
[Unit]
Description=Velociraptor Agent
After=network.target

[Service]
Type=simple
User=root
ExecStart=/opt/vraptor/vraptor --config /opt/vraptor/client.config.yaml client -v

[Install]
WantedBy=multi-user.target
```

7. Start the Velociraptor agent. First, make it executable with sudo chmod +x vraptor, then enable and start the service with sudo systemctl enable vraptor --now and sudo systemctl start vraptor.
   - systemctl daemon-reload
   - systemctl enable vraptor
   - systemctl start vraptor

8. Verify the connection. Go back to your Velociraptor server, start it up, and check the home screen to see if your client is now connected.



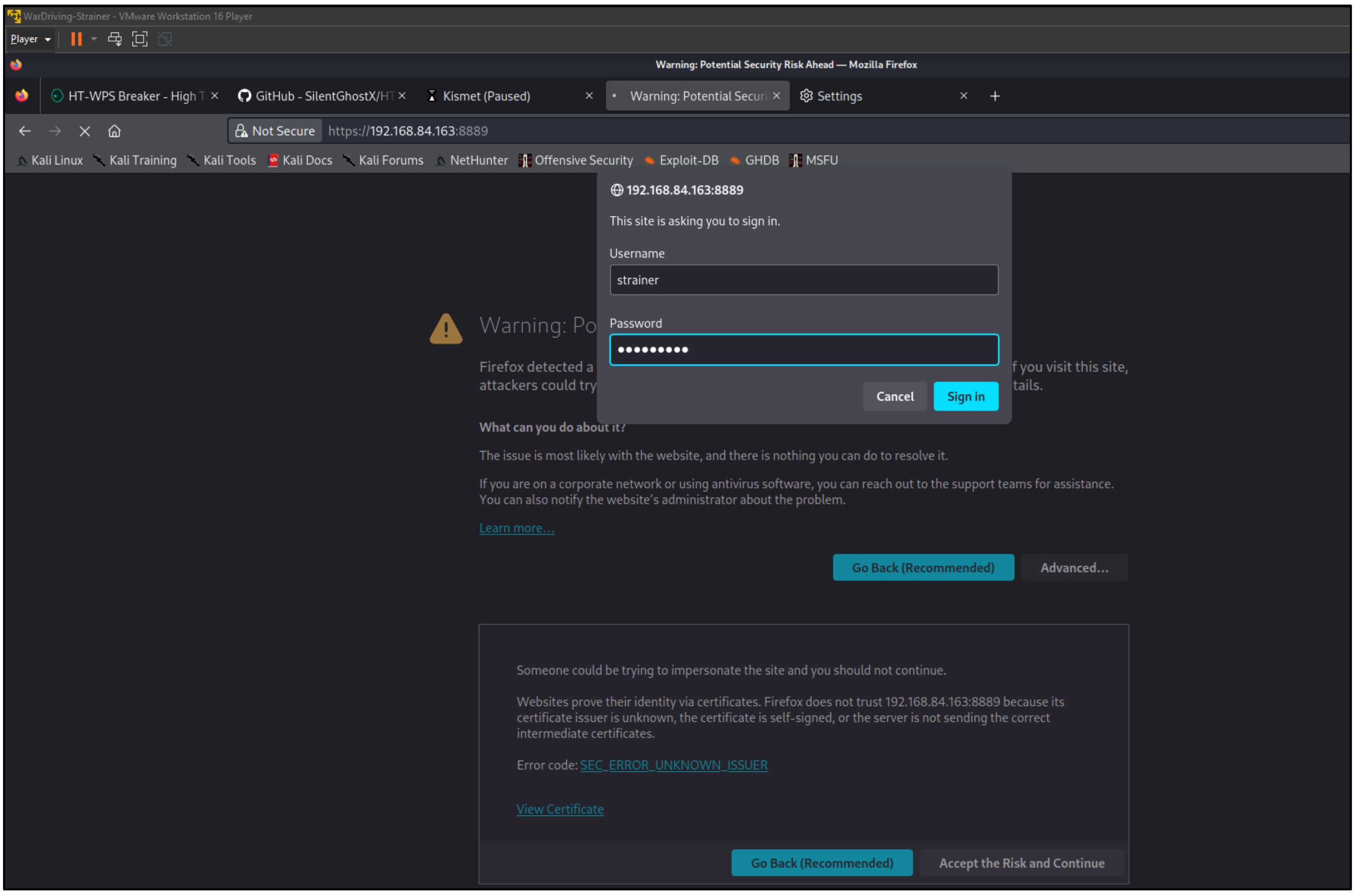
		Client ID	Hostname	FQDN	OS Version	Labels
□	●	C.aa25f225c8934c3a	Wardriving-MikeRebultan	Wardriving-MikeRebultan	debiankali-rolling	
□	●	C.8205b00a72787aed	Strainer-Win	Strainer-Win	Microsoft Windows 10 Enterprise Evaluation10.0.17763 Build 17763	

10 25 30 50

9. Repeat the process for other hosts.

Please replace **192.168.84.163** with your actual server IP address and /opt/vraptor with your actual home folder. Also, ensure that you have the necessary permissions to execute these commands.

Ping me on LinkedIn if you need further assistance! 😊



192.168.84.163:8889

This site is asking you to sign in.

Username: strainer

Password: •••••••••

Warning: Po

Firefox detected a ... f you visit this site, attackers could try ... tails.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

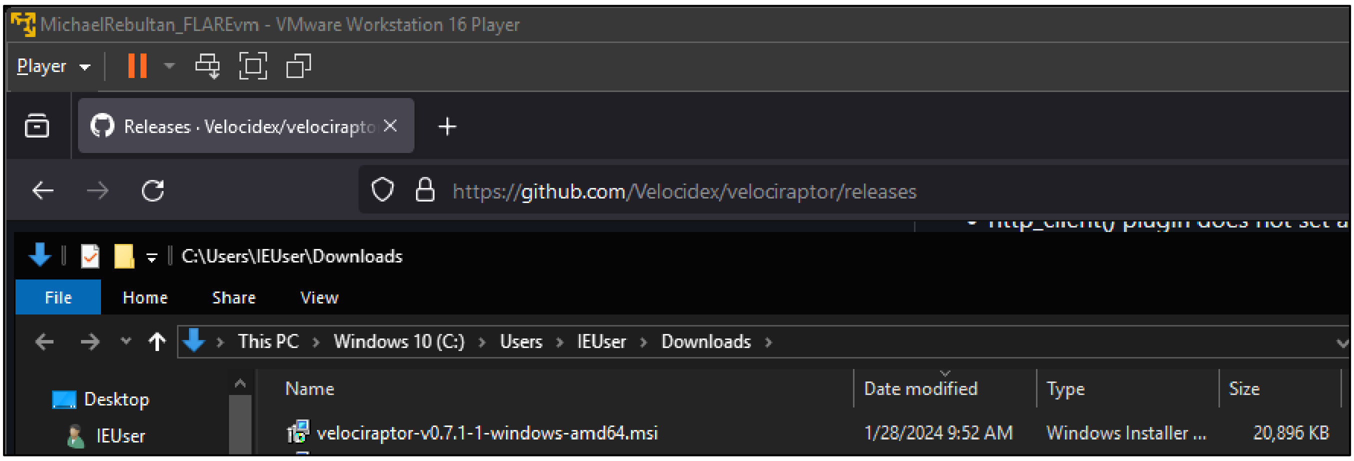
Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust 192.168.84.163:8889 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

Part 3: Connecting Windows hosts to Velociraptor (Client)

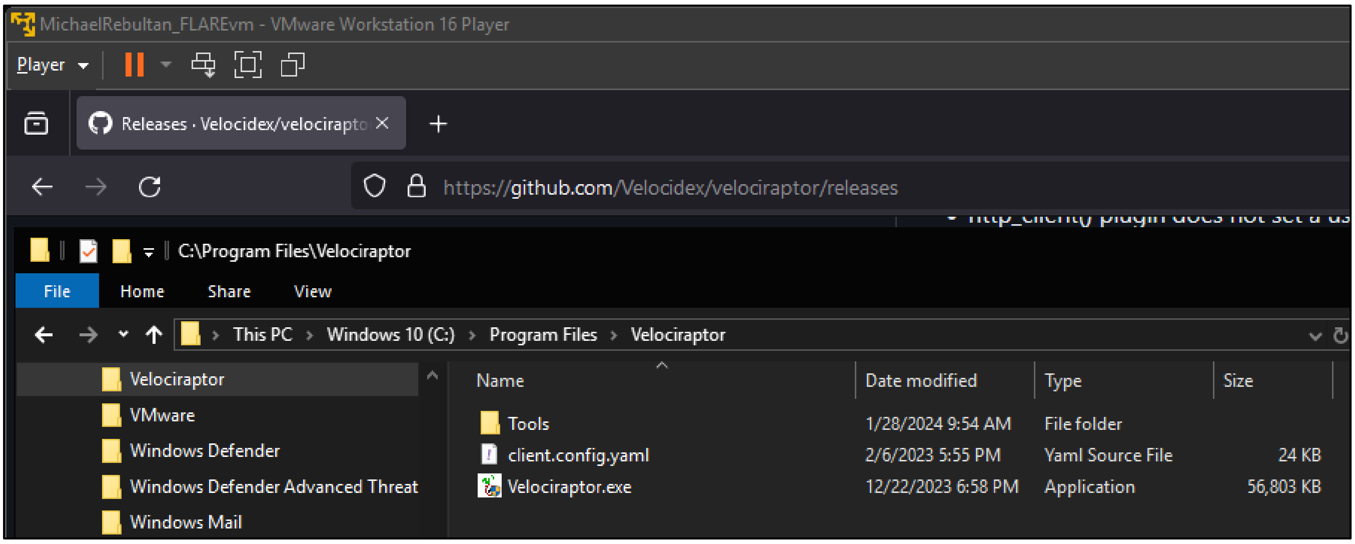
1. **Download the Velociraptor MSI file** from the Releases · Velocidex/velociraptor (github.com).


MichaelRebultan_FLAREvm - VMware Workstation 16 Player
Player
Releases · Velocidex/velocirapto
https://github.com/Velocidex/velociraptor/releases
C:\Users\IEUser\Downloads
File
Home
Share
View
This PC › Windows 10 (C:) › Users › IEUser › Downloads ›
Desktop
IEUser

Name	Date modified	Type	Size
velociraptor-v0.7.1-1-windows-amd64.msi	1/28/2024 9:52 AM	Windows Installer ...	20,896 KB

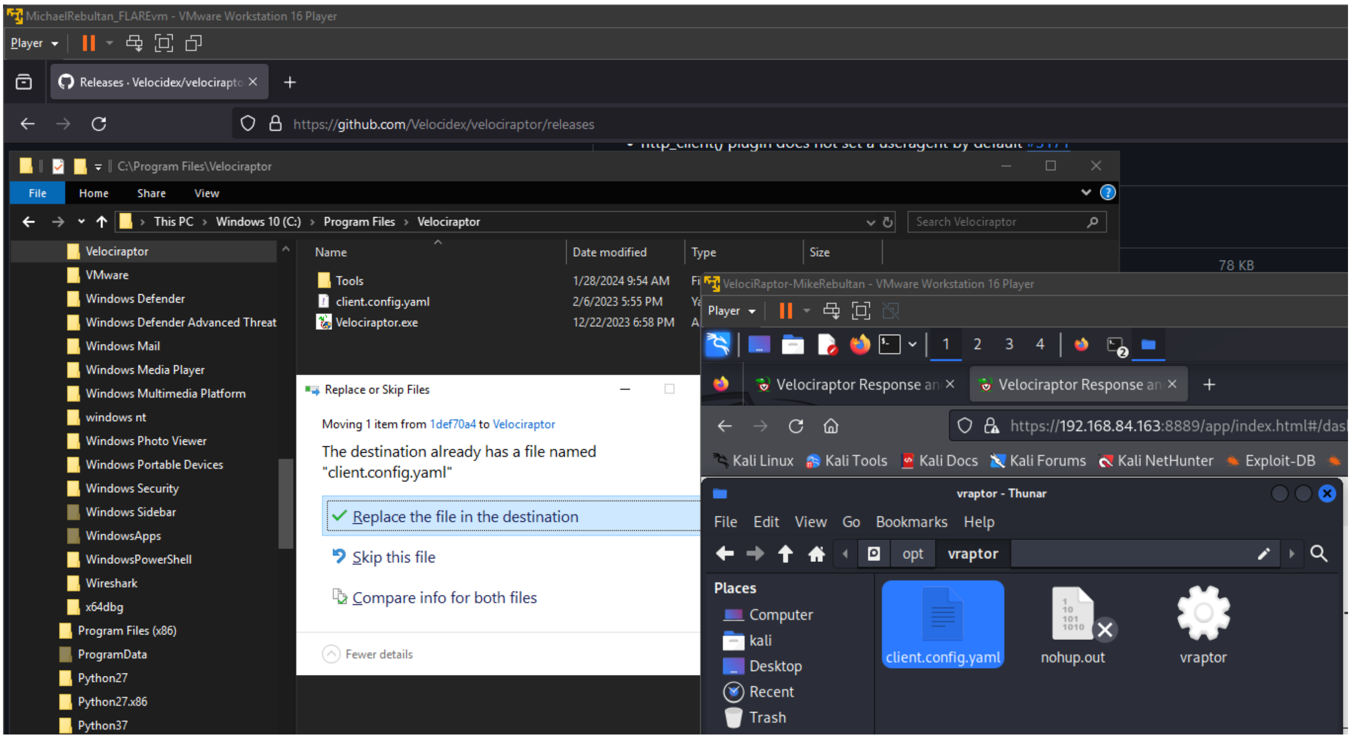
- ➢ **velociraptor-v0.7.1-1-windows-amd64.msi**

2. **Install Velociraptor** by double-clicking the downloaded MSI file. The installation is quick, and you'll find Velociraptor under Program Files\Velociraptor.


MichaelRebultan_FLAREvm - VMware Workstation 16 Player
Player
Releases · Velocidex/velocirapto
https://github.com/Velocidex/velociraptor/releases
C:\Program Files\Velociraptor
File
Home
Share
View
This PC › Windows 10 (C:) › Program Files › Velociraptor
Velociraptor
VMware
Windows Defender
Windows Defender Advanced Threat
Windows Mail

Name	Date modified	Type	Size
Tools	1/28/2024 9:54 AM	File folder	
client.config.yaml	2/6/2023 5:55 PM	Yaml Source File	24 KB
Velociraptor.exe	12/22/2023 6:58 PM	Application	56,803 KB

3. **Replace the placeholder configuration file** with your own. Copy your client.config.yaml file from your server (or wherever it's stored) and replace the client.config.yaml in Program Files\Velociraptor.



Name	Date modified	Type	Size
Tools	1/28/2024 9:54 AM		
client.config.yaml	2/6/2023 5:55 PM		
Velociraptor.exe	12/22/2023 6:58 PM		

Replace or Skip Files

Moving 1 item from 1def70a4 to Velociraptor

The destination already has a file named "client.config.yaml"

✓ Replace the file in the destination

Skip this file

Compare info for both files

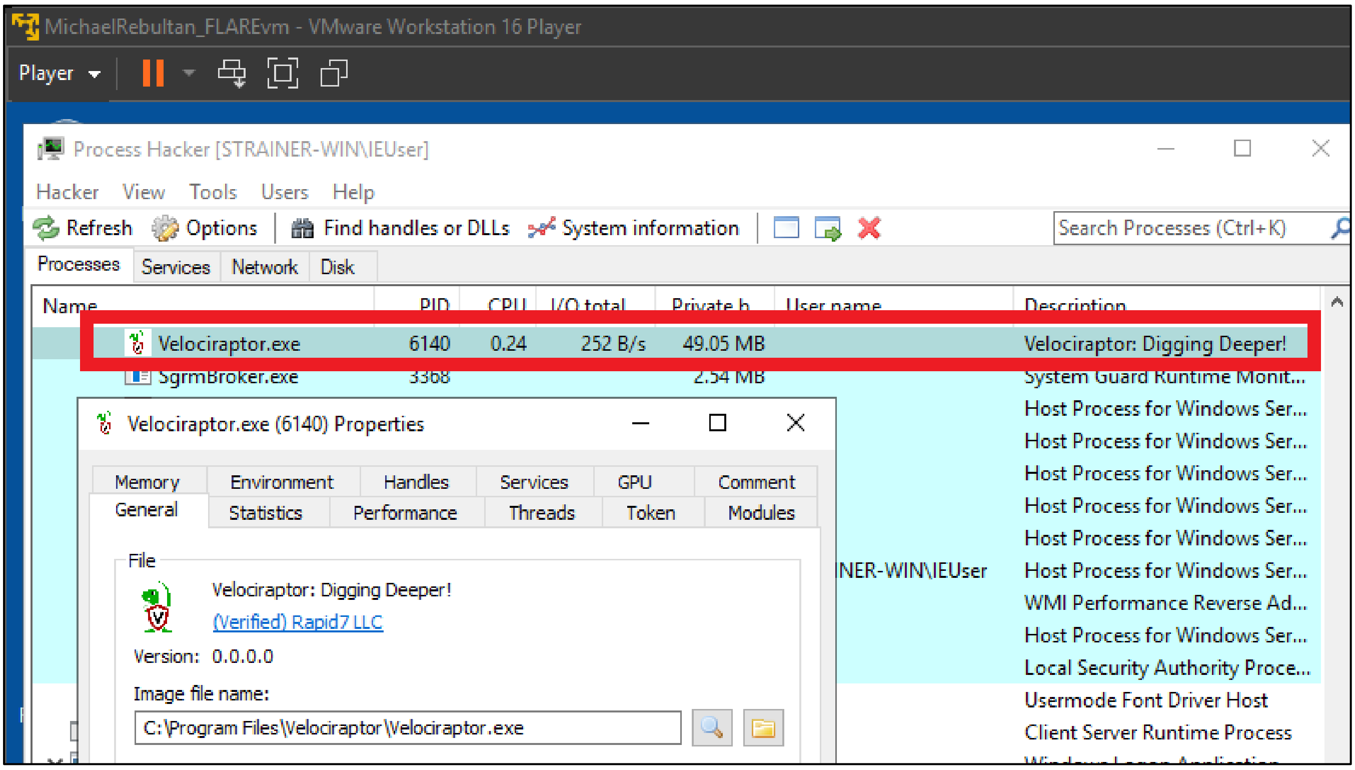
Fewer details

4. **Open a command shell** and navigate to the Velociraptor directory with cd \Program Files\Velociraptor.

5. **Set up Velociraptor as a service** using the command Velociraptor --config client.config.yaml service install.

    - ➤ **C:\Program Files\Velociraptor>Velociraptor.exe config client.config.yaml service install**

6. **Check your services files** to confirm that Velociraptor is installed and running.


MichaelRebultan_FLAREvm - VMware Workstation 16 Player
Player
Process Hacker [STRAINER-WIN\IEUser]
Hacker View Tools Users Help
Refresh
Options
Find handles or DLLs
System information
Search Processes (Ctrl+K)
Processes Services Network Disk
Memory Environment Handles Services GPU Comment
General Statistics Performance Threads Token Modules

Name	PID	CPU	I/O total	Private b...	User name	Description
Velociraptor.exe	6140	0.24	252 B/s	49.05 MB		Velociraptor: Digging Deeper!
SgrmBroker.exe	3368			2.54 MB		System Guard Runtime Monit...
						Host Process for Windows Ser...
						Host Process for Windows Ser...
						Host Process for Windows Ser...
						Host Process for Windows Ser...
						Host Process for Windows Ser...
					NER-WIN\IEUser	Host Process for Windows Ser...
						WMI Performance Reverse Ad...
						Host Process for Windows Ser...
						Local Security Authority Proce...
						Usermode Font Driver Host
						Client Server Runtime Process

Velociraptor.exe (6140) Properties

File

Velociraptor: Digging Deeper!

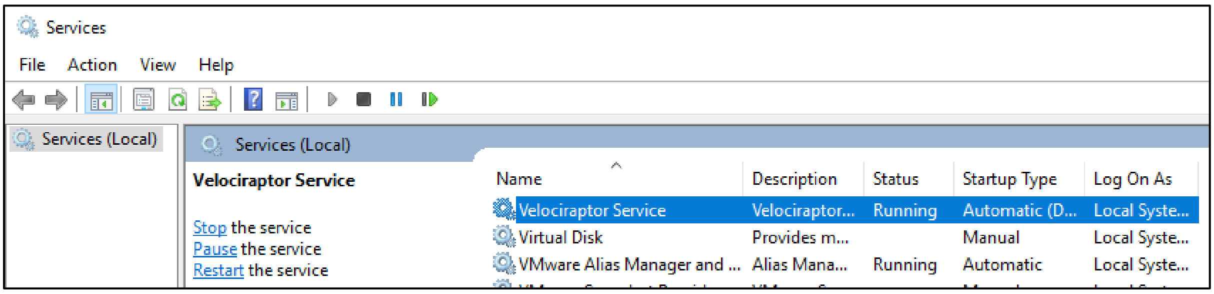
(Verified) Rapid7 LLC

Version: 0.0.0.0

Image file name:

C:\Program Files\Velociraptor\Velociraptor.exe

7. **Restart the service** to activate your new configuration.



Velociraptor Service

Stop the service
Pause the service
Restart the service

Name	Description	Status	Startup Type	Log On As
Velociraptor Service	Velociraptor...	Running	Automatic (D...	Local Syste...
Virtual Disk	Provides m...		Manual	Local Syste...
VMware Alias Manager and ...	Alias Mana...	Running	Automatic	Local Syste...

8. **Verify the connection**. It may take a while for the dashboard to update, but eventually, you should see your connected clients when you check the 'search clients' dropdown and select 'show all'.

Please ensure that you have the necessary permissions to execute these commands.

Ping me on LinkedIn if you need further assistance! 😊

About the Author

Mike Art Rebultan is a seasoned IT and OT security professional with over 20 years of experience in the industry. He has been a digital forensics and incident response specialist in different ICS/OT organizations for 12 years, leveraging his expertise in IT and OT security, offensive security, and cyber threat intelligence to protect critical infrastructure. He works with a few cyber security organizations, government sector, data center, bpo, retail, OT/IIoT, swiss bank, semi-conductor, academe, and more —he is currently an adjunct cybersecurity professor in a few colleges/university in Toronto, Canada.

He holds a master's degree in IT with a concentration in E-Commerce Security. He has further supplemented his education with a Professional Graduate Diploma in Digital Forensics and Cyber Security. This demonstrates his commitment to staying at the forefront of his field and his dedication to providing his clients with the highest level of expertise and knowledge.

With a focus on computer forensics, network intrusion, data breach, cybercrime investigation, malware analysis, and reverse engineering, Mike Art Rebultan has established himself as a seasoned expert in the field. In addition to his professional work, Mike enjoys technical writing with the ISACA Blog portal and public speaking in RSA, HITB, FOSS Asia, and more. He has discovered eight zero-day malware during IoC extractions as part of threat-hunting activities and managed at least 12 cyber breaches which demonstrates his deep understanding of the industry.