Velociraptor Lab Assignment: Server and Client Deployment

Tools Used:
Linux Terminal
Windows Command Prompt
Python 3
Internet Browser
Velociraptor v0.74.2 (amd64)
Notepad

Lab Topology

Kali Linux VM
10.0.2.5

Windows Server VM
10.0.2.4

Velociraptor Lab Assignment: Server and Client Deployment

Table of Contents

Lab Environment Specifications

Client: Windows Server 2022 Standard, 21H2
Server: Kali Linux 6.12.13-amd64 (must have Python 3 installed)
Total RAM Required: 5 GB (2 GB for Windows Server 2022, 3 GB for Kali Linux)
Total CPU Processors Required: 3 (1 for Windows Server 2022, 2 for Kali Linux)
Total VirtualDisk Size Required: 30GB (14 GB for Windows Server 2022, 16 GB for Kali Linux)
Velociraptor Version: v0.74.2

Kali Linux Login: kali:kali
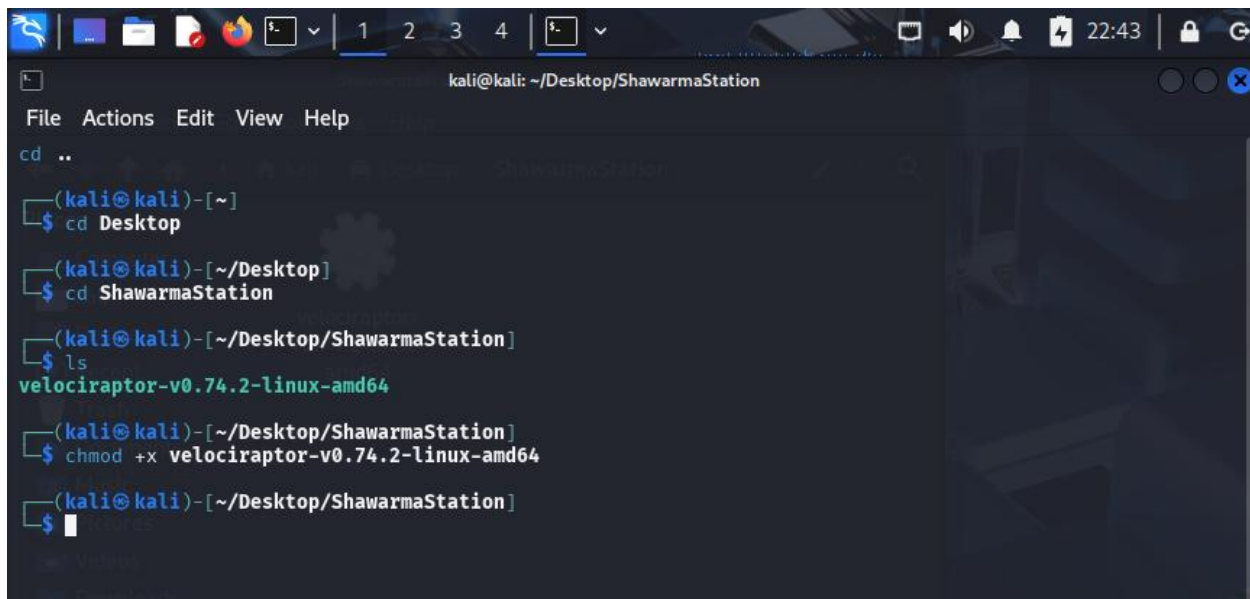Windows Server 2022 Login: Administrator:CYBR250!!!!

Pre-lab Notes

When going through this lab, the instructions may not be properly updated to reflect the Velociraptor versions available (this will only be the case for NetLab). Due to this, if you see any mention of "velociraptor-v0.74.2", and this velociraptor version is not available on either of the VMs, please update the name to reflect the version you see. NetLab cannot connect to the Internet, so installing prior versions of Velociraptor would be impossible for a student. If you are experiencing any difficulty with deploying a Velociraptor server or client, consult the Rapid7 documentation on Velociraptor.

Introduction

Being able to monitor endpoints in a network is crucial to the tasks that digital forensic analysts and incident responders will be performing. Velociraptor is a DFIR tool that can send out "Hunts" for retrieving artifacts on a chosen client device. This tool can be deployed locally on a system's storage, via a USB, or via a cloud deployment. As speed and flexibility are stressed in the realm of digital forensics and incident response, having an easily deployable monitoring program such as Velociraptor makes threat detection more efficient. This lab will cover the offline installation of Velociraptor, both from the server side and from the client side.

Part 1: Velociraptor Server Deployment in a Network

1. First, sign into the Kali Linux VM using the universal login "kali:kali".

2. Once you are logged in, open a new Terminal pane and change the directory to **ShawarmaStation** (located in the Desktop directory).

3. Inside ShawarmaStation, there should be a Velociraptor executable file for Linux. If there is no ShawarmaStation folder already made in the Desktop, or if the Velociraptor file is not in a ShawarmaStation folder, make sure that a ShawarmaStation folder is present and a Velociraptor file is present. Run the command "chmod +x velociraptor-v0.74.2-linux-amd64" to grant execution permissions for the Velociraptor executable file. If you do not see the specific velociraptor executable file name as listed, replace "velociraptor-v0.74.2-linux-amd64" with the name of the velociraptor executable found in ShawarmaStation.

4. Next, run the command "./velociraptor-v0.74.2-linux-amd64 config generate -i", which will start an interactive configuration file creation process for Velociraptor.

5. If prompted, select "Self Signed SSL" by pressing Enter on the highlighted selection. When selecting the OS, choose "Linux", as this is specifically a Linux installation file. For the path to the datastore and log directories, leave both paths as default. As this will be a temporary deployment for the lab, set the Internal PKI Certificate to expire in 1 Year, and select "No" when asked to restrict VQL functionality. Press enter when prompted about using a registry for client writeback. For the network parameters, set the DNS name to "localhost", the DNS type to "None", and deny using experimental websocket comms. Keep the default ports to "8000" for listening and "8889" for the GUI. Set the username to "admin" and the password as "CYBR250".

If there are any steps that were not specifically defined above, it is safe to keep the defaults for it.

6. To skip the user creation process again, just press enter twice to continue. The next panel should create a server configuration file, which will be needed in the next step of this configuration process.
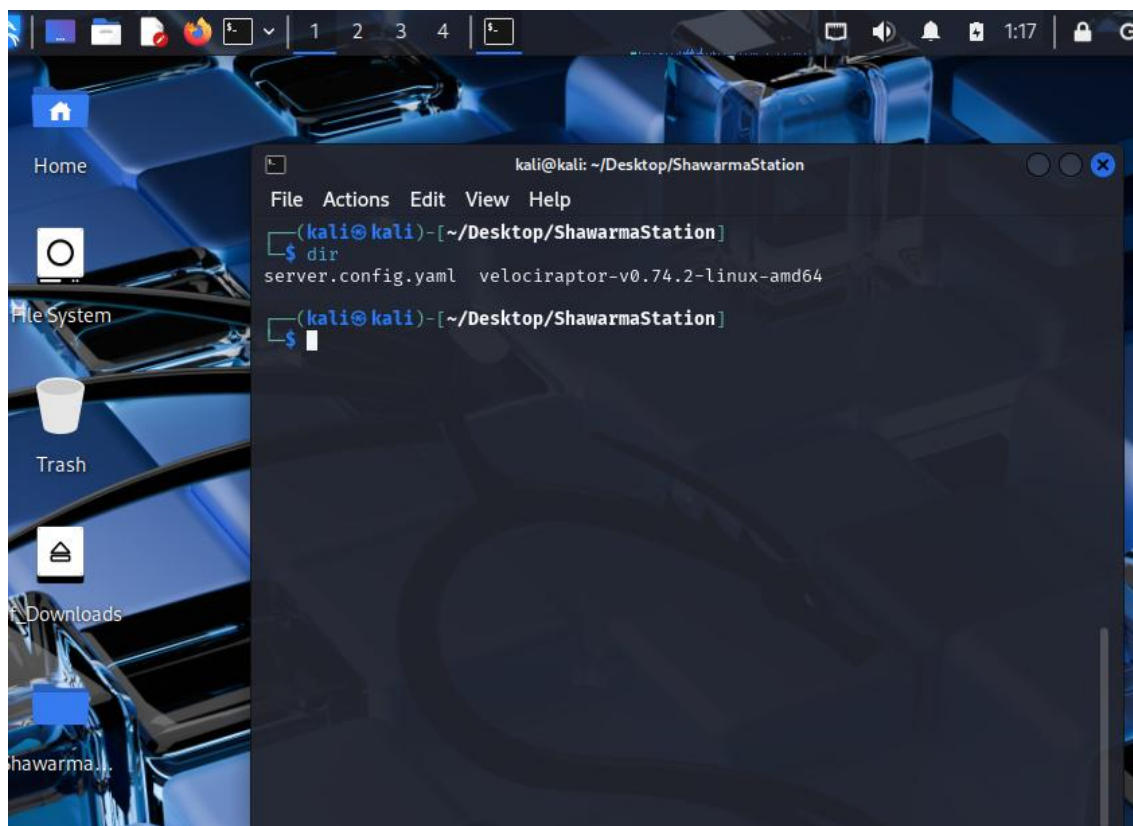
It should hopefully be known that Kali Linux is an instance of Debian, which means that it can run releases for Debian distributions. With this in mind, let's create a server binary that our Kali Linux machine can use.

7. To do this, execute the command "./velociraptor-v0.74.2-linux-amd64 debian server --config ./server.config.yaml", which should have created a new .deb file in the ShawarmaStation folder.

This is important, as we will now be using this file to install the actual server component of Velociraptor.

8. To do this, the command "sudo dpkg -i velociraptor_server_0.74.2_amd64.deb" should be executed, and if properly executed, it should start the Velociraptor service as soon as it de-packages the .deb file.

9. A quick way to check if Velociraptor is active is to go to the web browser and enter the address "127.0.0.1:8889" or "localhost:8889", whichever you may prefer. If it gives you a security warning, the server is active, and it may prompt you to provide credentials in the Kali Linux popup pane.

10. Simply enter the username and password made from the server setup stage, if they were different than admin:CYBR250. You should be able to see a welcome homepage as soon as your credentials are authenticated.
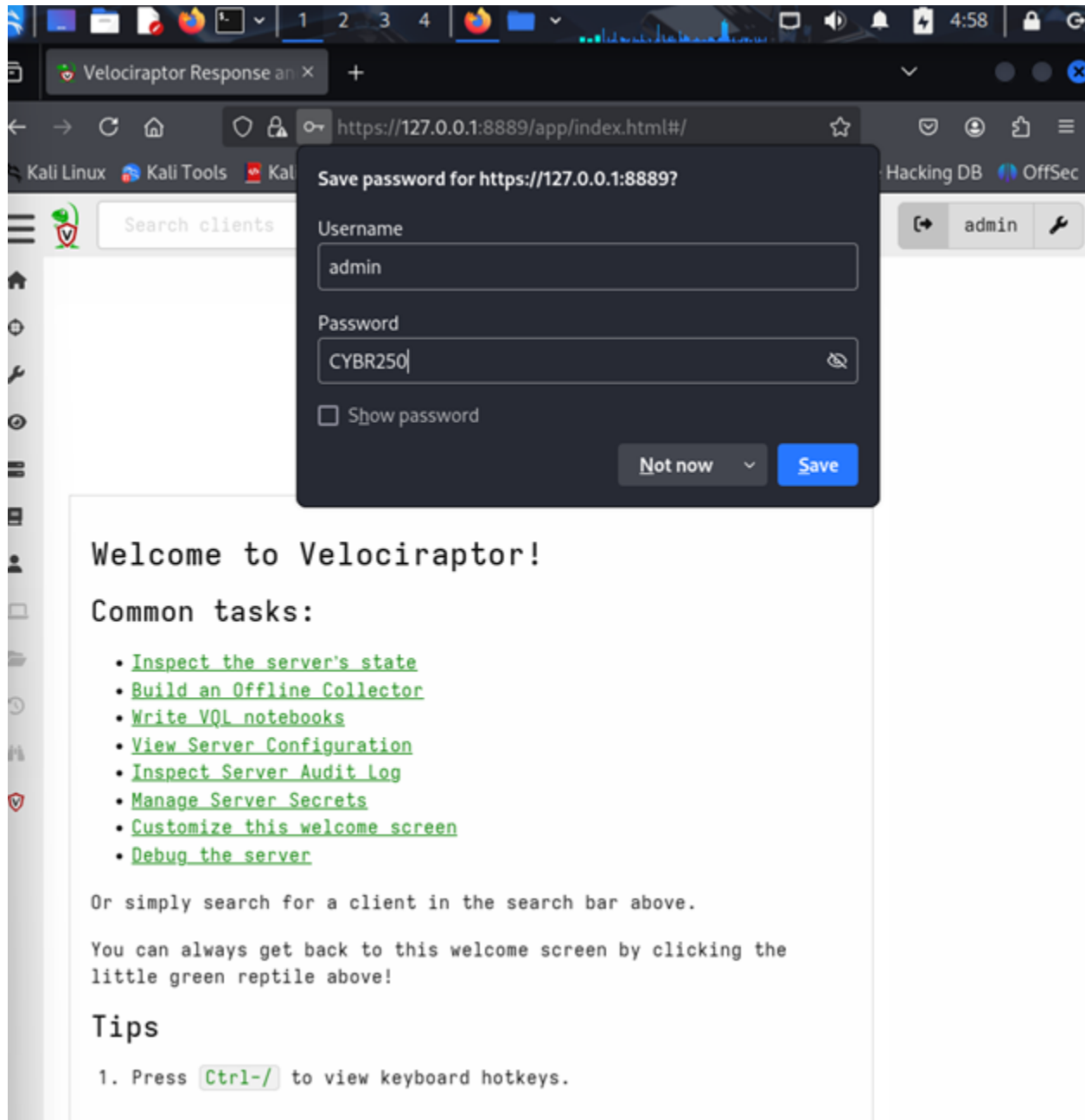
Part 2: Velociraptor Client Deployment in a Network

11. Once inside this welcome page, click on the Home icon and scroll down the web page until you see a section titled "Current Orgs". Here, we will be downloading a Client Config file so that we can connect the Windows Server 2022 VM to our Velociraptor instance. It may prompt you to re-enter your username and password, and after that the client file should be downloaded.
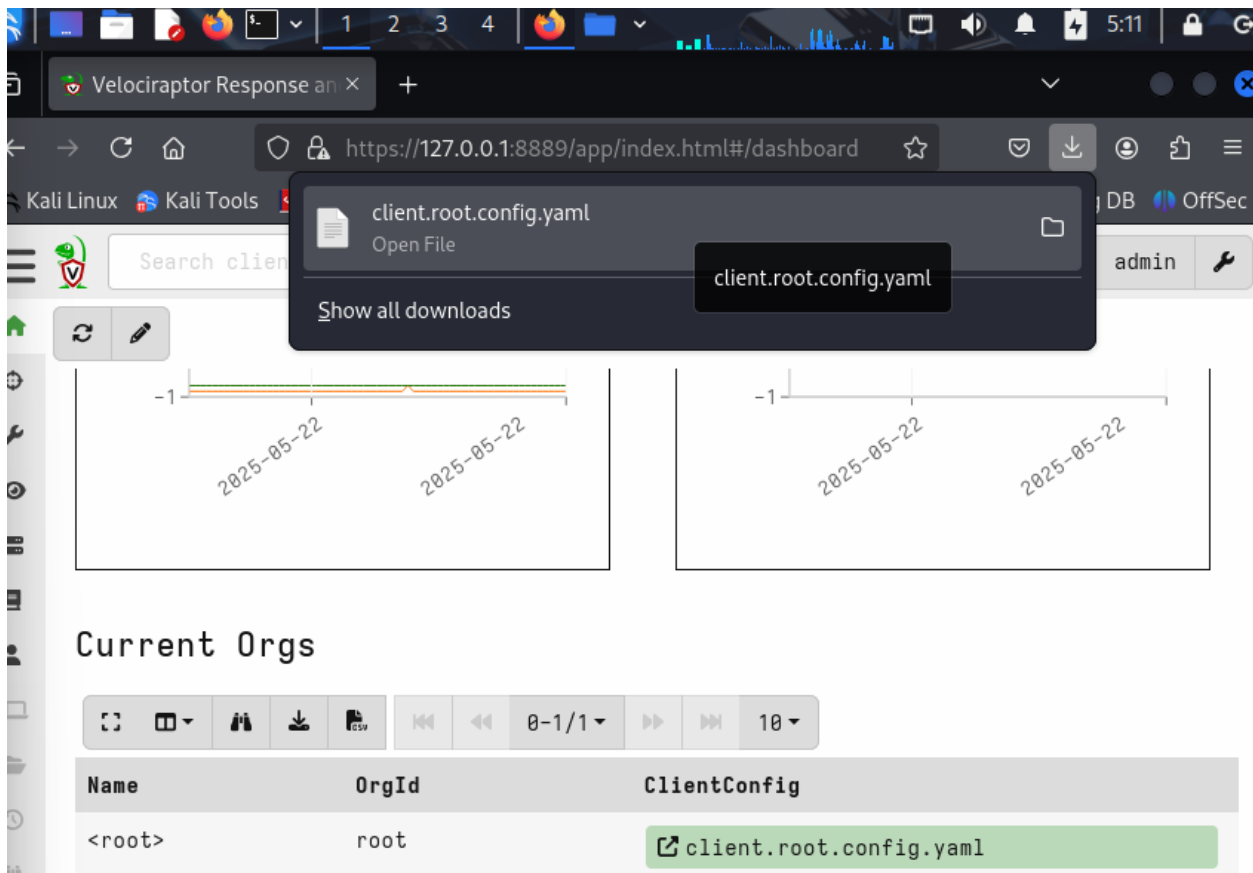

We will be utilizing Python for this next step, as Python's http.server module can be used to send the client file over.

12. As Kali Linux has Python pre-installed, we can use the command "python -m http.server 5150" to host an HTTP server on port 5150.

As this is well above the well-known port range, this port assignment will most likely not interfere with any preexisting protocols. Make sure that the downloaded Client Config file has been moved to the ShawarmaStation directory.

13. Move to the Windows Server 2022 VM, where you will enter the provided credentials to log in.

14. Once inside this machine, open Microsoft Edge (or another internet browser) and enter the address "10.0.2.5:5150", which will route to the Kali Linux VM.

15. Download the client config file that was downloaded from the Kali Linux HTTP server, and make sure to save it in the Downloads directory.
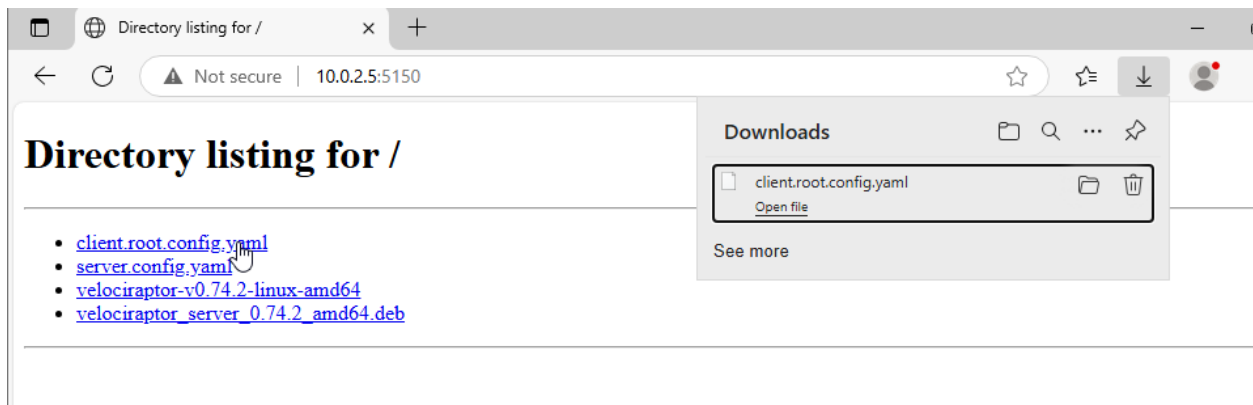
Inside the Downloads directory should also be an executable named "Velociraptor.exe", which is the v0.74.2 version but is renamed for simplicity. Now that we have the client configuration file in the Windows Server 2022 VM, we must make one crucial edit to it.

16. Open the client.root.config.yaml file in Notepad

17. Scroll until you see a section with "Client:" and a server_urls input of "https://localhost:8000/". The server_urls input should be changed to "https://10.0.2.5:/8000", as this is the routable address for the Kali Linux VM. Save your changes and close out of Notepad.

By doing this step, we are able to now provide this machine with the appropriate client files. This next installation command will be the easiest, as it will make every change itself.

18. Execute the command "velociraptor.exe --config client.root.config.yaml client -v", which will output verbose information whilst the process is ongoing.

19. Once you see that the output stops, switch over to the Kali Linux VM and refresh the Server Output page using the Redraw Dashboard button.

Very soon, you should be able to see a line forming, indicating that one client has been connected. This indicates that the Windows Server 2022 client has been successfully connected to the Kali Linux Velociraptor server and Hunts can now be performed.

Currently Connected Clients

2025-05-22T21:52:34.157Z
client_comms_current_connections 1
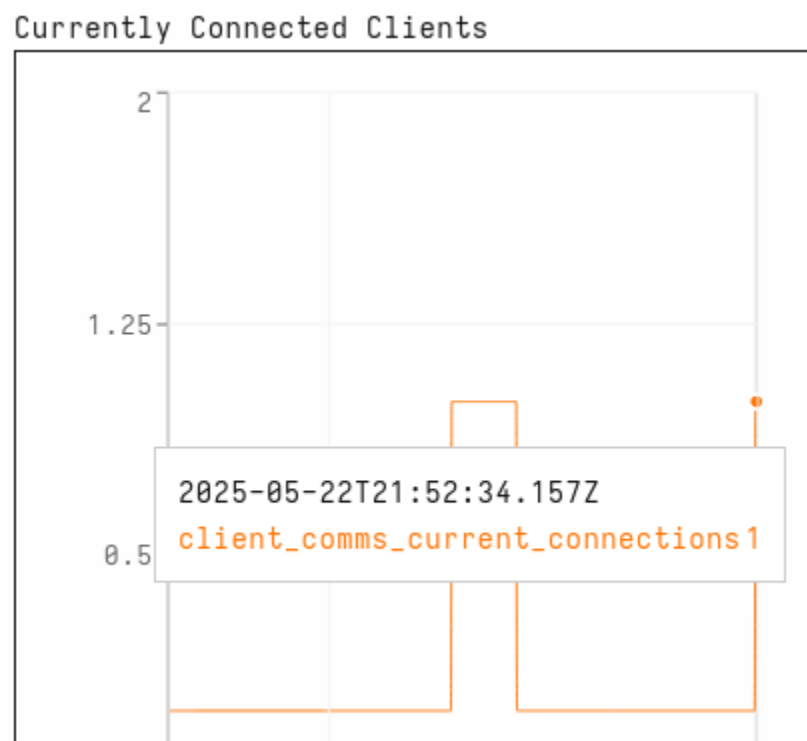
Conclusion

That is the end of this lab! The last command that you used created a binary along with a Velociraptor service in the Services part of Windows. This means that once you close the Command Prompt pane, you can just restart the Velociraptor service to stay connected. When running Hunts, it is crucial to select "All Orgs" and to make sure that the "Start Hunt Immediately" checkbox is marked if you wanted to quickly run a Hunt.