

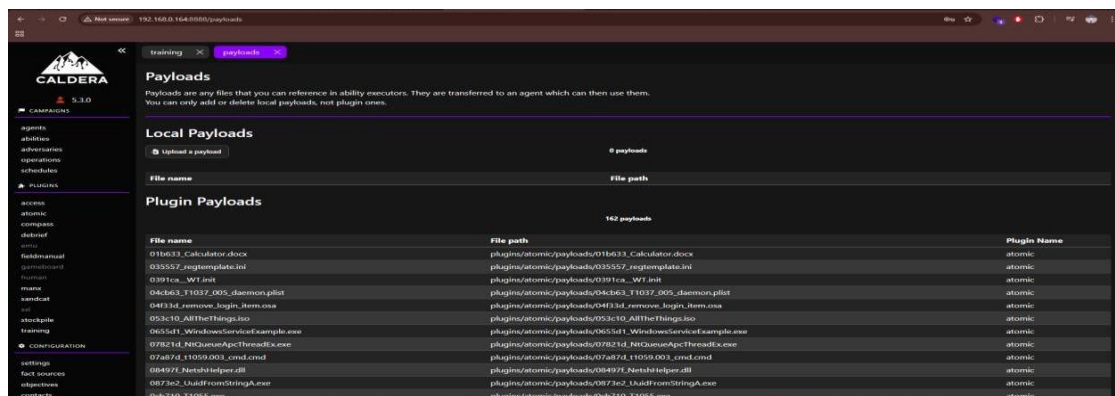


## 4. Incident Response Simulation Activities:

- **Tools:** Velociraptor, MITRE Caldera.
- **Task:** Simulate a phishing attack with Caldera and collect artifacts with Velociraptor.

## Enhanced Tasks:

- **Phishing Simulation:** Deploy a mock phishing payload with Caldera on a Windows VM. Document the attack path in a 100-word summary.





Using the Caldera framework with the "manipulate" plugin, a mock phishing payload was deployed to a Windows 10 VM. The operation simulated an initial phishing email containing a malicious HTA file crafted with the "hunter" adversary profile. Upon execution, the HTA payload used PowerShell to establish a connection back to the Caldera server. The agent was successfully installed and beacons back to the server, enabling post-exploitation steps such as privilege enumeration and credential dumping. This simulated attack path demonstrated a typical phishing-to-initial-access vector, leveraging native Windows tools for stealth and persistence within a controlled test environment.

- **Artifact Collection:** Use Velociraptor to collect process and network artifacts (SELECT \* FROM processes; SELECT \* FROM netstat;). Save to CSV and analyze for IOCs.

The screenshot shows the Velociraptor web interface. The top navigation bar includes links for 'Velociraptor Response', 'VQL Reference', and 'Velociraptor'. The main content area displays a notebook titled 'SELECT \* FROM processes()'. The notebook contains a table with columns: NotebookId, Name, Description, Creation Time, Modified Time, Creator, and Collaborators. The table has one row with the following data: N.D2K00NC55HEVI, New Notebook, 2025-08-22T05:30:05Z, 2025-08-22T05:30:05Z, admin, and Collaborators. Below the table, there is a section for 'Supertimeline' with instructions on how to add time-series data. The supertimeline view shows a timeline from Wednesday, December 31, 1969, to Thursday, January 1, 1970, with a table view and an annotation view.

The screenshot shows the Velociraptor web interface. The top navigation bar includes links for 'Velociraptor Response', 'VQL Reference', and 'Velociraptor'. The main content area displays a notebook titled 'SELECT \* FROM processes()'. The notebook contains a table with columns: Client ID, Hostname, FQDN, OS Version, and Labels. The table has one row with the following data: 8-8/8, 8-8/8, 8-8/8, 8-8/8, and 8-8/8. Below the table, there is a section for 'Supertimeline' with instructions on how to add time-series data. The supertimeline view shows a timeline from Wednesday, December 31, 1969, to Thursday, January 1, 1970, with a table view and an annotation view.



Velociraptor Response

SELECT \* FROM netstat()

Client ID Hostname FQDN OS Version Labels

2025-08-22T05:32:31.166Z

Velociraptor Response

SELECT \* FROM netstat()

Name OrgId ClientConfig

<root> root client.root.config.yaml

Disk Space

Filesystem	Size	Used	Avail	Use%	Mounted
overlay	79G	46G	30G	61%	/
tmpfs	64M	0	64M	0%	/dev
shm	64M	0	64M	0%	/dev/shm
/dev/sda1	79G	46G	30G	61%	/velociraptor
tmpfs	2.0G	0	2.0G	0%	/proc/asound
tmpfs	2.0G	0	2.0G	0%	/proc/acpi
tmpfs	2.0G	0	2.0G	0%	/sys/firmware

Users

2025-08-22T05:36:36.841Z