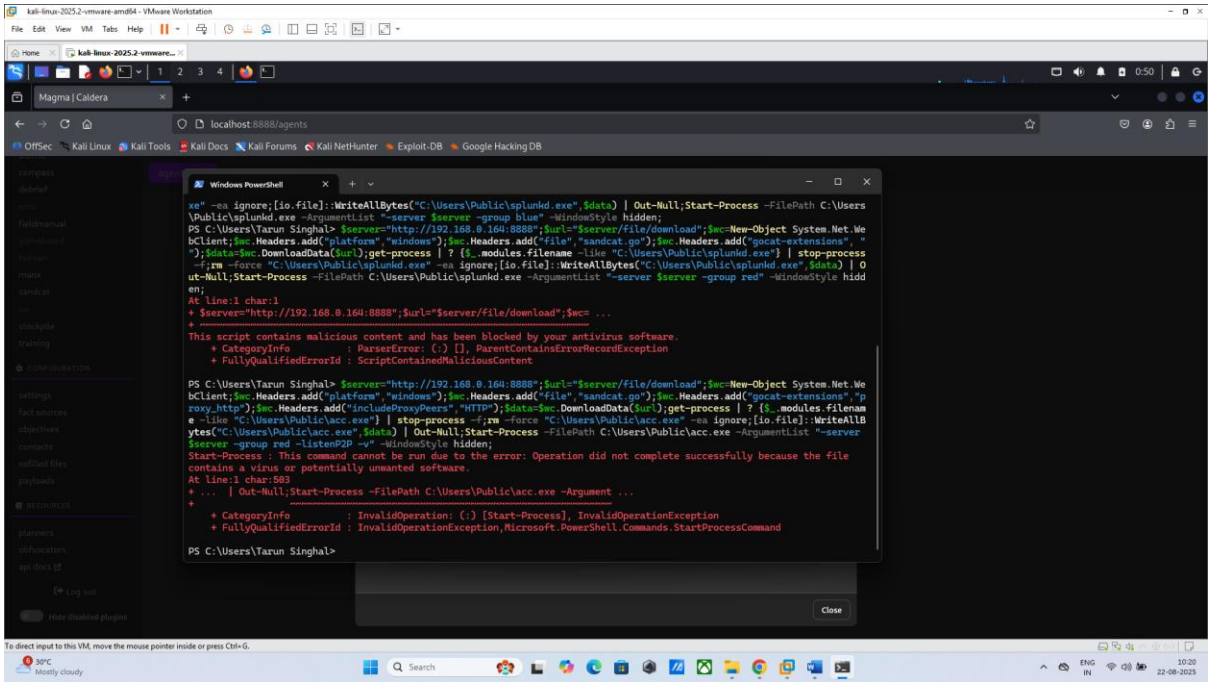
4. Incident Response Simulation

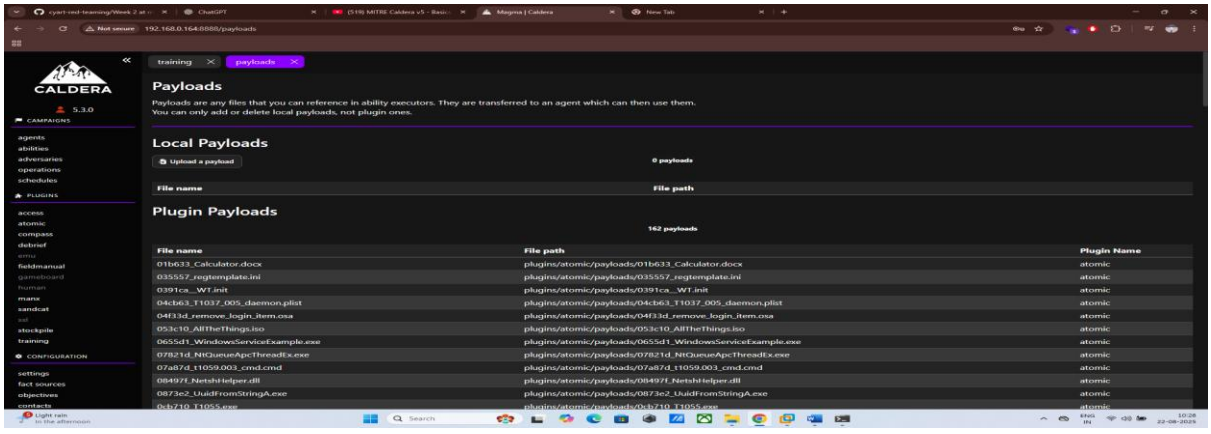
Activities:

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



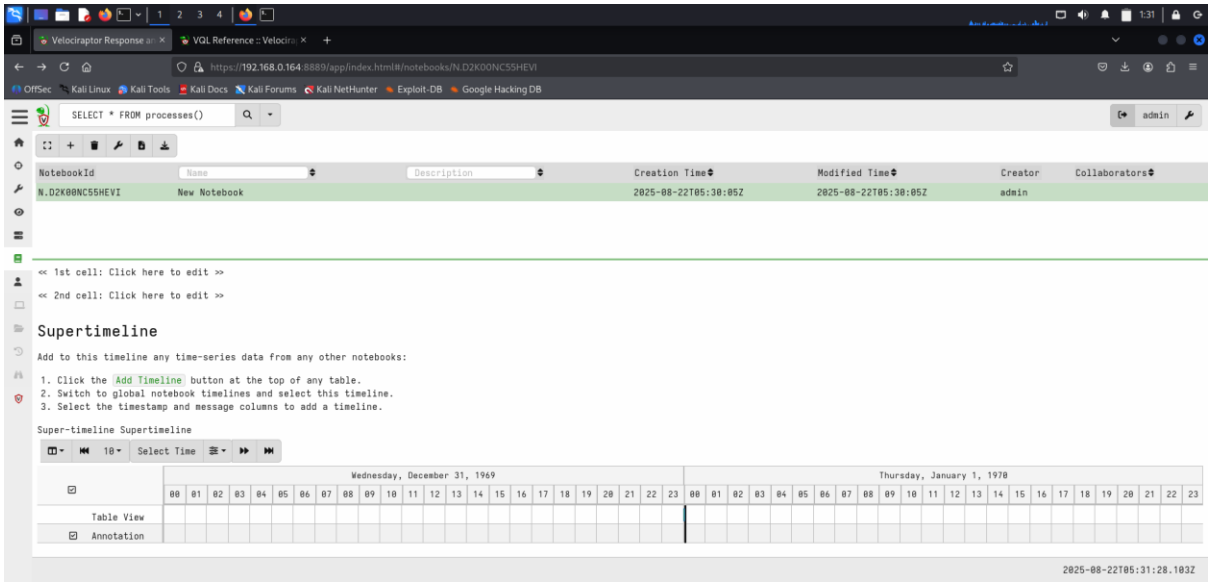
Enhanced Tasks:

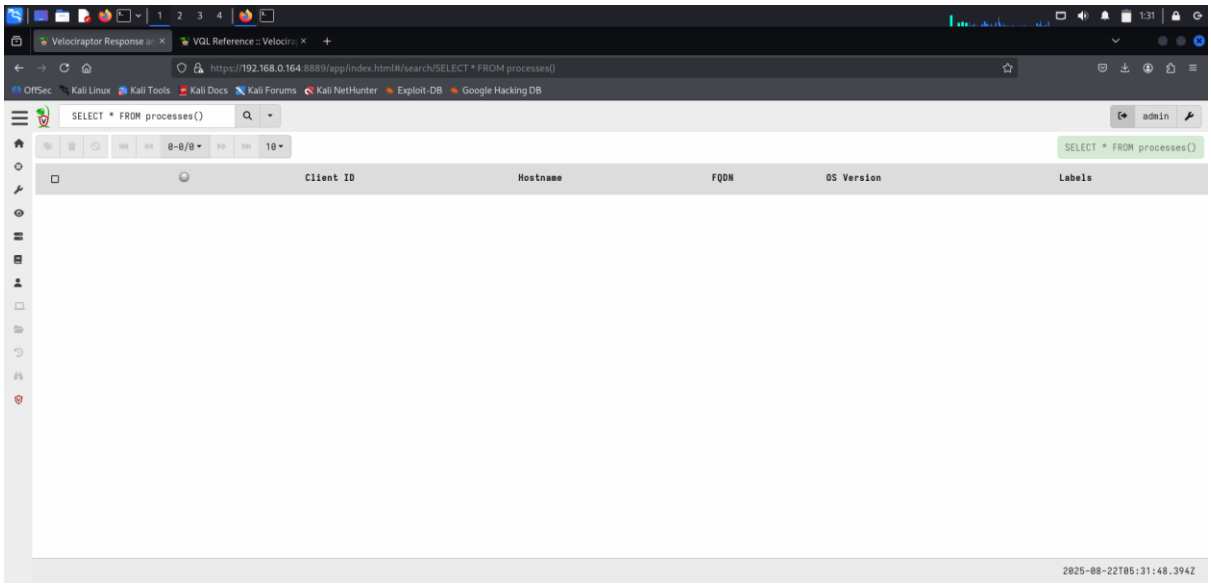
- **Phishing Simulation:** Deploy a mock phishing payload with Caldera on a Windows VM. Document the attack path in a 100-word summary.

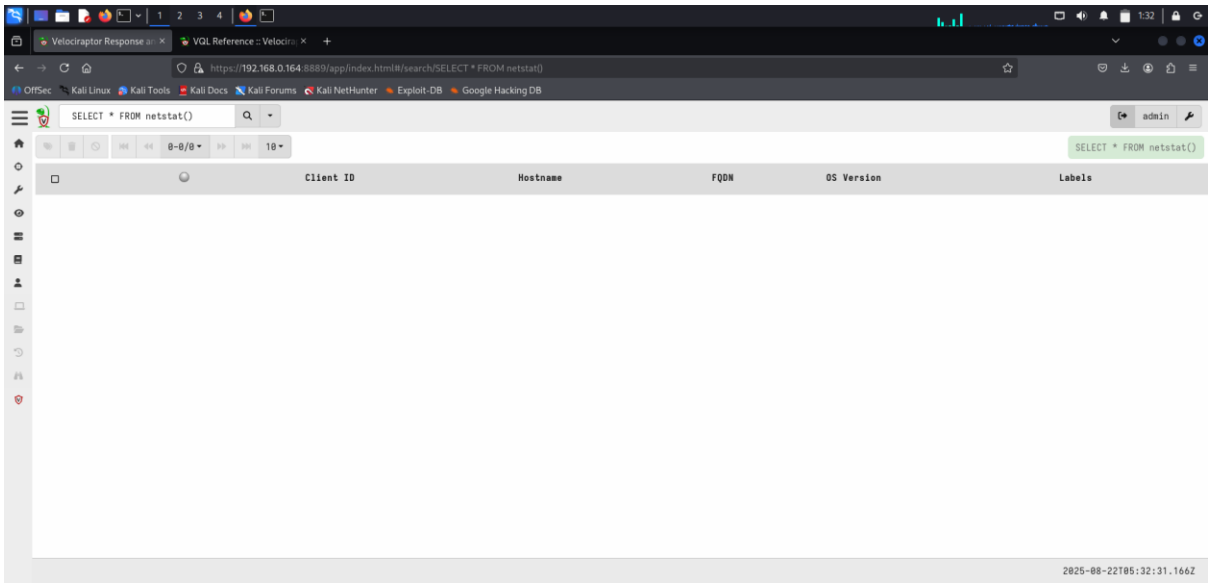


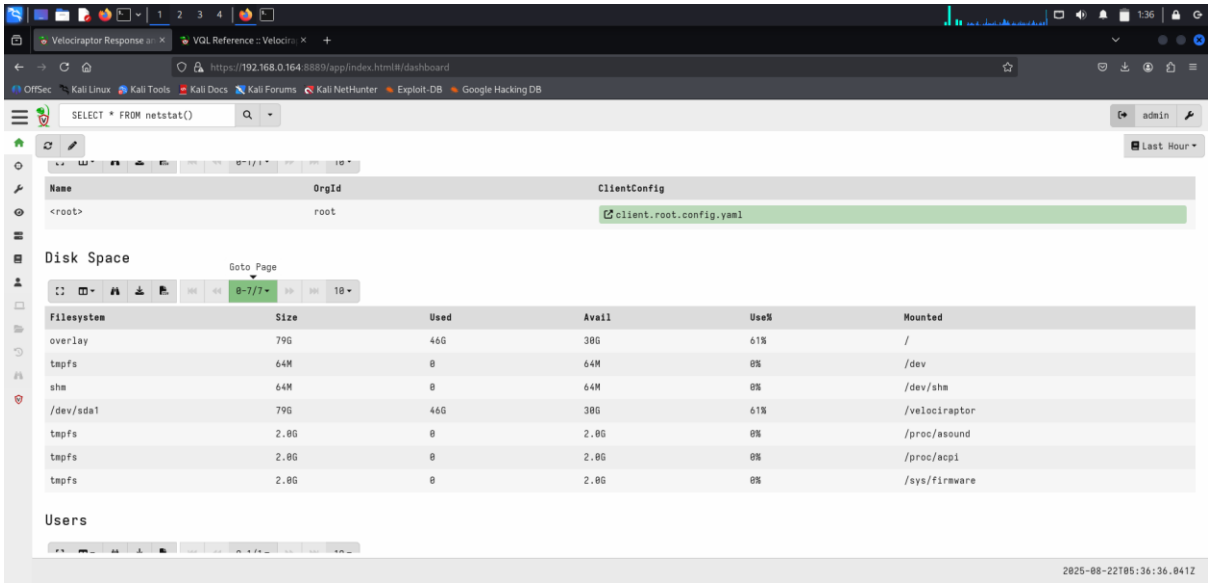
Using the Caldera framework with the "manipulate" plugin, a mock phishing payload was deployed to a Windows 10 VM. The operation simulated an initial phishing email containing a malicious HTA file crafted with the "hunter" adversary profile. Upon execution, the HTA payload used PowerShell to establish a connection back to the Caldera server. The agent was successfully installed and beaconed 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.






SELECT * FROM netstat()
admin
Client ID
Hostname
FQDN
OS Version
Labels
2025-08-22T05:32:31.166Z


SELECT * FROM netstat()
admin
Last Hour
Name
OrgId
ClientConfig
<root>
root
client.root.config.yaml
Disk Space
Goto Page
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
2025-08-22T05:36:36.041Z