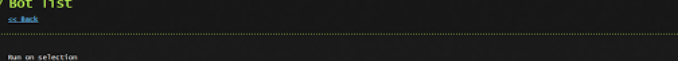


Lydecker Black on 6:28 PM



The screenshot shows a terminal window with a green prompt `./ Bot list` and a red cursor. Below the prompt, the text `cc Back` is visible. A dialog box titled "Run on selection" is open, featuring a search bar and a "Run" button. The dialog displays a table of bots with the following data:

Name	Last Online	IP	OS	Sel.
online			Windows 8	<input checked="" type="checkbox"/>
...	Fri Dec 4 10:57:45 2013	...	Windows 10	<input checked="" type="checkbox"/>
...	Fri Dec 4 18:51:47 2013	...	Windows 7	<input checked="" type="checkbox"/>
...	Sun Nov 29 22:20:50 2013	...	Windows 7	<input checked="" type="checkbox"/>

[illegible]

- A Command and Control server, which is a Web interface to administer the agents
- An agent program, which is run on the compromised host, and ensures communication with the CNC

The client is a Python program meant to be compiled as a win32 executable using `pyinstaller`. It depends on the **requests**, **pythoncom**, **pyhook** python modules and on **PIL** (Python Imaging Library).

Easy, Automated and Scalable  
Web Application Security



**Register For a Free Trial**

- remote cmd.exe shell
- persistence
- file upload/download
- screenshot
- key logging

**Python for Offensive**  
**Penetration Testing**

Learn how to hack using Python

One Time Offer

**15\$**

The image shows the front cover of a book titled "Build Automation eBook". At the top, there are four square icons arranged horizontally: Facebook (blue with white 'f'), Twitter (light blue with white 't'), Google+ (red with white 'g+'), and an RSS feed icon (orange with white symbol). Below these is a yellow rounded rectangle button with the text "Submit a Tool" in black and a small wrench and screwdriver icon. The title "Build Automation eBook" is prominently displayed in a large, blue, serif font. Below the title, the subtitle "Building and Testing with Gradle" is in a smaller, black, sans-serif font, followed by "Free download by" and the publisher "O'Reilly" in a larger, black, serif font. At the bottom, there are two small circles (one filled, one empty) and a large, dark gray button with a white right-pointing chevron ">".

## Installation

### Server

To install the server, first create the sqlite database:

```
cd server/
python db_init.py
```

If no installed, install the **cherrypy** python package.

Then launch the server by issuing: **python server.py**

By default, the server listens on `http://localhost:8080`

### Agent

The agent can be launched as a python script, but it is ultimately meant to be compiled as a win32 executable using `pyinstaller`.

First, install all the dependencies:

- requests
- pythoncom
- pyhook
- PIL

Then, configure `agent/settings.py` according to your needs:

`SERVER_URL` = URL of the CNC http server

`BOT_ID` = the (unique) name of the bot, leave empty to use hostname

`DEBUG` = should debug messages be printed to stdout ?

`IDLE_TIME` = time of inactivity before going in idle mode (the agent checks the CNC for commands far less often when idle).

`REQUEST_INTERVAL` = interval between each query to the CNC when active

Finally, use `pyinstaller` to compile the agent into a single exe file:

```
Shell - Konsole
cd client/
pyinstaller --onefile --noconsole agent.py
```

## Download Ares

Is your website vulnerable to SQL INJECTION and XSS Vulnerabilities?

Scan it with the only False-Positive-Free Web Security Scanner

**netsparker®**  
Web Application Security Scanner

**DOWNLOAD NOW**

Subscribe via e-mail for updates!

Subscribe

Tweet

G+ 6

in Share

1



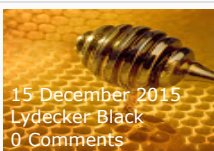
### Next

This is the most recent post.

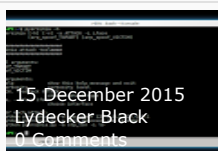
### Previous

[credmap - The Credential Mapper](#)

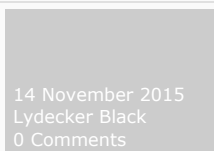
### Related Posts



15 December 2015  
Lydecker Black  
0 Comments



15 December 2015  
Lydecker Black  
0 Comments



14 November 2015  
Lydecker Black  
0 Comments



15 October 2015  
Lydecker Black  
0 Comments

## Booking.com



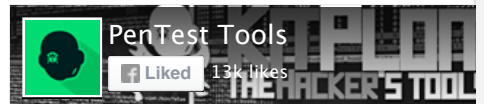
★★★★★  
**Las Vegas**  
Tuscany Hotel & Casino  
From  
**\$1,990**  
Book now



★★★★★  
**Las Vegas**  
Fortune Hotel & Suites  
From  
**\$1,069**  
Book now



★★★★★  
**Las Vegas**  
The LINQ Hotel & Casino  
From  
**\$2,506**  
Book now



Follow @KitPloit

51.4K followers



KitPloit

G+ Follow

+1

+ 4,416

1149 listeners  
BY FEEDBURNER

**DedicatedSolutions.com**  
www.dedicatedsolutions.com

**Best Dedicated Servers**

- 1 & 10Gbps Servers!
- Unlimited Bandwidth!
- Private Cloud Ready!
- SAN/NAS & DR Backup!

from **\$59/month!**

**Order Now**

SAVE 20% W/ COUPON K16ZC

### Populars

### Comments

### Archive



#### Collection Of Awesome Honeypots

A curated list of awesome honeypots, tools, components and much more. The list is divided into categories such as web, services, and ot...



#### Pyersinia - Network Attack Tool

Pyersinia is a similar tool to Yersinia, but Pyersinia is implemented in Python using Scapy. The main objective is the realization of ne...



#### Flashlight - Automated Information Gathering Tool for Penetration Testers

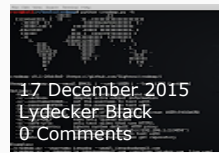
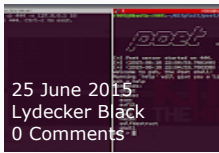
Pentesters spend too much time during information gathering phase. Flashlight (Fener) provides services to scan network/ports and gathe...



#### Mosca - Static Analysis Tool To Find Bugs

Just another Simple static analysis tool to find bugs like a grep unix command, at mosca have a modules, that was call egg, each eg...

**Joomla - A Black Box, Joomla Vulnerability**



#### SPONSORED



- 1. [Pirates : The Strategy Game Phenomenon of 2015](#) 2 weeks ago [Plarium.com](#) [Plarium](#) [Plarium.com](#) (sponsored)



0 Comments

KitPloit - Tools for your PenTest Arsenal!

1 Login

Recommend

Share

Sort by Best



Start the discussion...

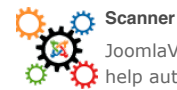
Be the first to comment.

Subscribe

Add Disqus to your site Add Disqus Add

Privacy

DISQUS



#### Scanner

JoomlaVS is a Ruby application that can help automate assessing how vulnerable a Joomla installation is to exploitation. It supports bas...



#### ATSCAN - Server, Site and Dork Scanner

Description: ATSCAN Version 2 Dork scanner. XSS scanner. Sqlmap. LFI scanner. Filter wordpress and Joomla sites in the serve...



#### USBTracker - Script to track USB devices events and artifacts in a Windows OS

USBTracker is a quick & dirty coded incident response and forensics Python script to dump USB related information and artifacts from...

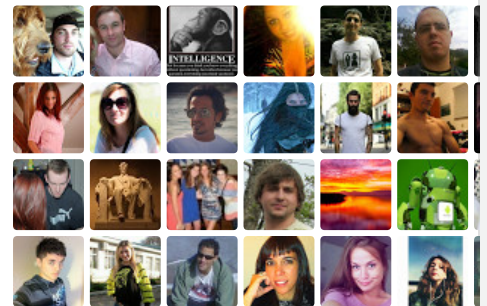
#### Labels



#### Google+ Followers

##### KitPloit

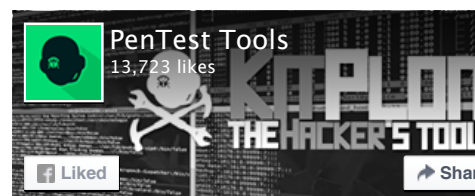
+ Follow



3,594 have us in circles

Fund this site and millions more with Contributor.





You like this



## Tweets

Follow

**Hacker Tools** @KitPloit

1h

Ares - Python Botnet and Backdoor [goo.gl/124np3](http://goo.gl/124np3) #Ares #Backdoor #Botnet [pic.twitter.com/kAxkBlrz6J](https://pic.twitter.com/kAxkBlrz6J)



Expand

**Hacker Tools** @KitPloit

1h

Ares - Python Botnet and Backdoor: Ares is made of two main programs: A Command and Control server, w... [bit.ly/1YqQuBg](http://bit.ly/1YqQuBg) #PenTest

Tweet to @KitPloit

## Contact Form

Name

Email \*

Message \*

Send

## Recommended:

Blackploit [Pentest]

DedicatedSolutions (Private Cloud)

DedicatedSolutions (Server Products)

DigitalOcean

ExoClick

Funeek!

Th3 R4v3n

TraffBoost

7PRO

Underc0de

Sunploit

**Site Info**  
kitploit.com  
Dec 18, 2015

Traffic Rank:  
**311,806**

Links in:  
**49**

Powered by  
Alexa

13online

## Follow us!




PenTest ...

Liked

Follow @KitPloit


51.4K followers



**KitPloit**

google.com/+KitPloitWeb

Hacking and PenTest Tools for your Security Arsenal!

 Follow

+1

+ 4,416

1149 listeners

BY FEEDBURNER

Copyright © 2012 [KitPloit](#) - PenTest Tools for your Security Arsenal! All Right Reserved  
Designed by [IVYthemes](#) | [MKR Site](#)