Seunghyuk Baek

Sbaek44@vt.edu

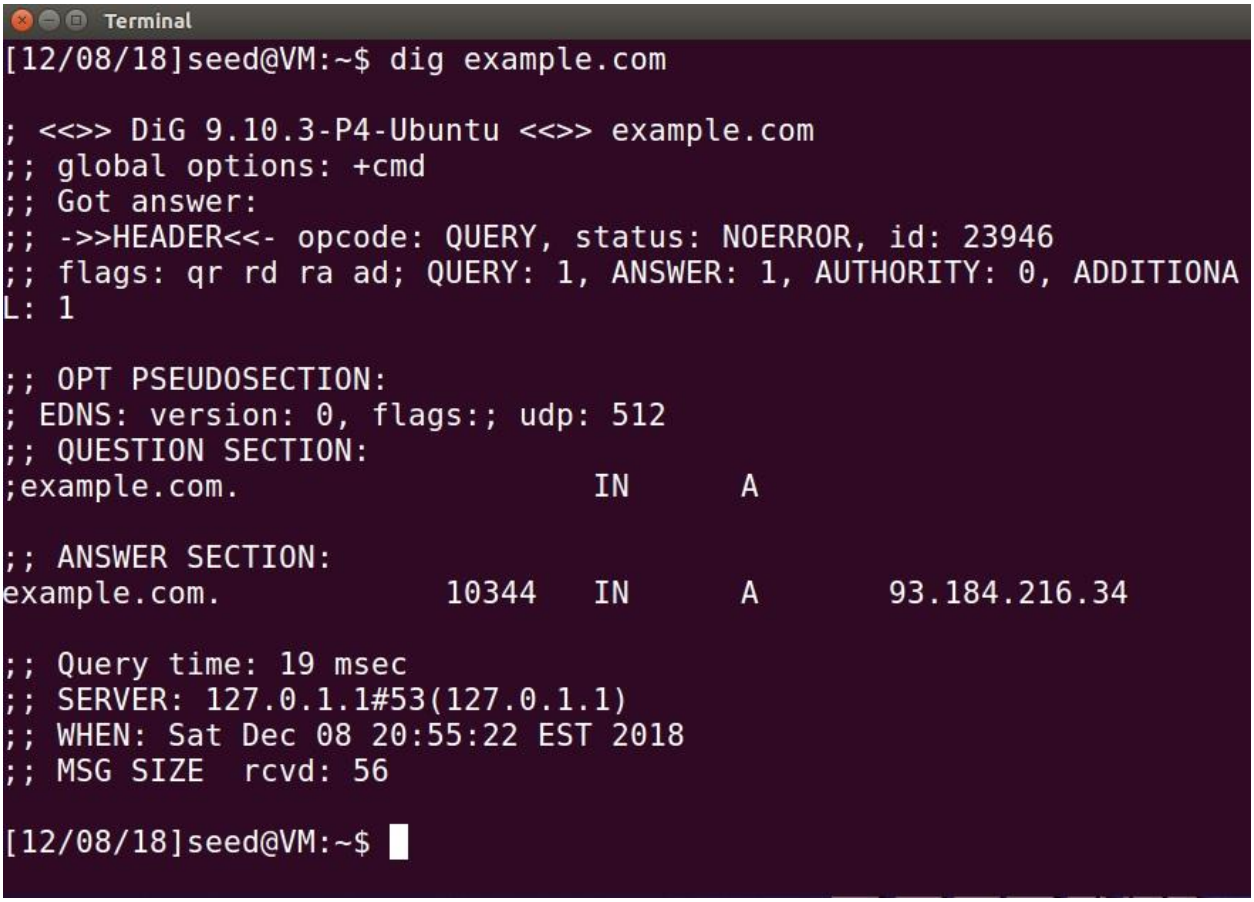
ECE5480 Project 7.

Objective

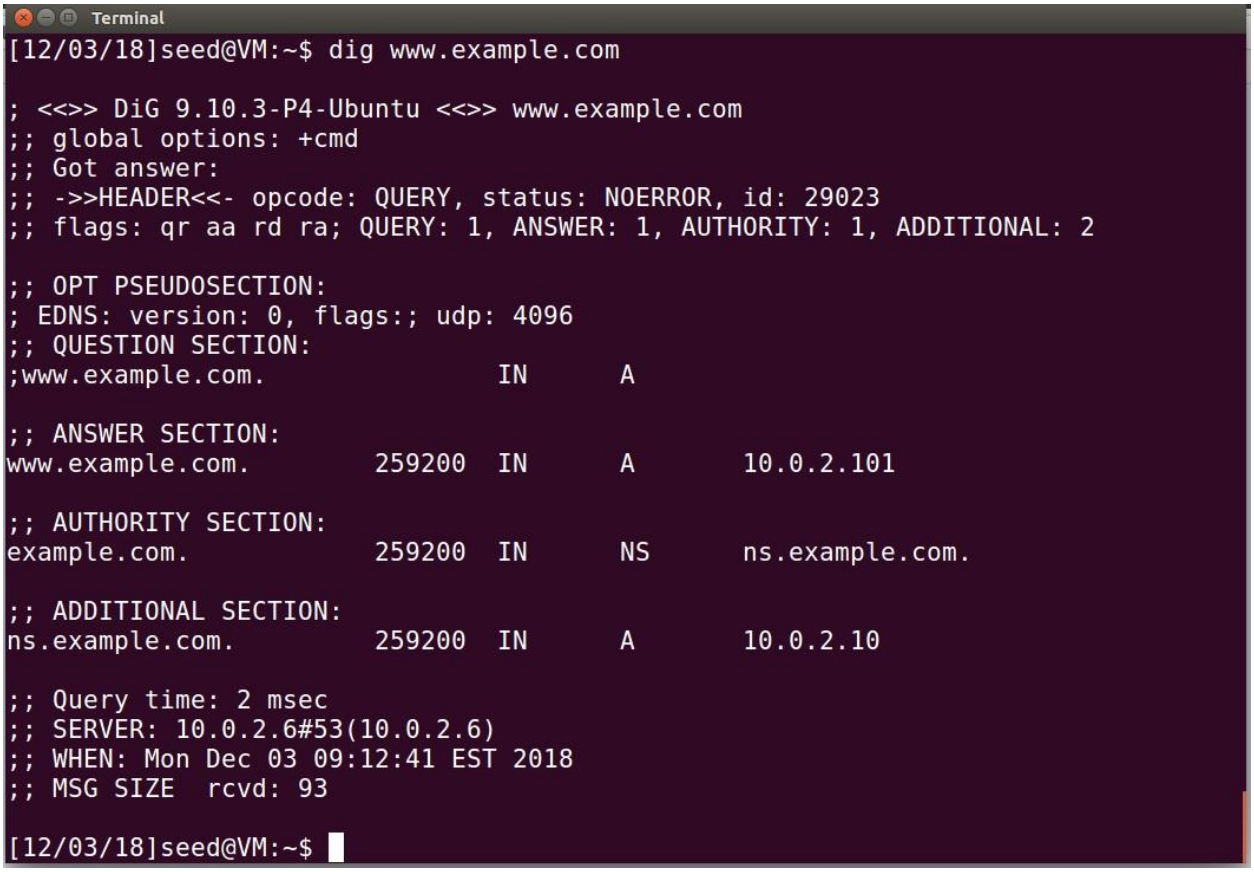
This lab is to demonstrate DNS attack in 3 different ways. First DNS attack is placed with assumption that the victim's system is already compromised by a hacker, so the hacker has all privileges to modify victim's system. Second DNS attack simulates when a hacker is using same private network with victim and can steal traffic between the victim and DNS server. Last scenario is to simulate when the traffic between DNS server and other authoritative DNS servers is captured and modified by a hacker.

Lab Environment Setup

To simulate such scenarios, three linux virtual machines were set up in a private NAT network. Each of these VM takes role of hacker, user and DNS server. If all VMs are set up correctly, each VM machine can connect to internet.



Next, we need to set up one VM as dns server (here ip address 10.0.2.6 is DNS). Which will result in



Task 1.

If victim's computer is compromised by a hacker, the hacker can modify HOST file which serves as local lookup. This HOST file is preferred over remote DNS lookups.

www.bank32.com ip address is changed from 184.168.221.58 (above figure) to 198.82.215.14 (below).

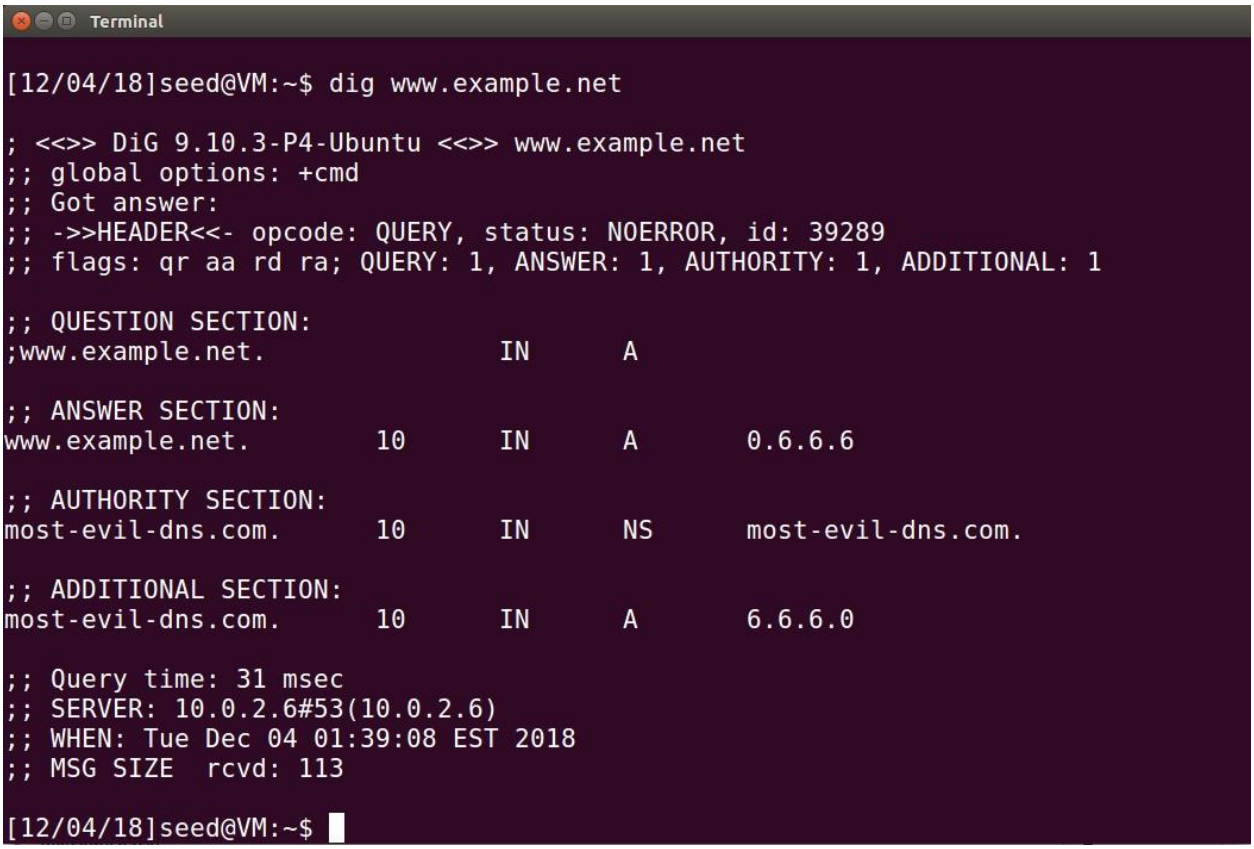
```
[12/03/18]seed@VM:~$ ping www.bank32.com
PING www.bank32.com (198.82.215.14) 56(84) bytes of data.
64 bytes from www.bank32.com (198.82.215.14): icmp_seq=1 ttl=243 time=32.5 ms
64 bytes from www.bank32.com (198.82.215.14): icmp_seq=2 ttl=243 time=28.8 ms
64 bytes from www.bank32.com (198.82.215.14): icmp_seq=3 ttl=243 time=29.3 ms
^C
--- www.bank32.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 28.865/30.244/32.506/1.612 ms
[12/03/18]seed@VM:~$
```

Task 2.

In this task, a hacker sniffs the packet between the user and the local DNS server. When the user asks for service to local DNS server, the hacker intercepts user's query and sends malicious response to the user.

```
Terminal
[12/03/18]seed@VM:~$ dig www.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29023
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       10.0.2.101

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

;; ADDITIONAL SECTION:
ns.example.com.         259200  IN      A       10.0.2.10

;; Query time: 2 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Mon Dec 03 09:12:41 EST 2018
;; MSG SIZE  rcvd: 93

[12/03/18]seed@VM:~$
```

Above is the result of dig www.example.com before hacker attack



Above is dig www.example.com command after successful DNS attack by sniffing transaction between user and DNS server. Note that ip address of example.com and the name of DNS server had been changed.

Takas3.

In this task, the hacker poisons local DNS server so any user who connects to this DNS can be affected by hacker. To do this, hacker intercept the traffic between local DNS and remote DNS. Once, local DNS receives spoofed query from the hacker, the DNS saves spoofed ip address in cache and uses it for other queries.

```
[12/04/18]seed@VM:~$ dig google.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26495
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             600     IN      A       125.6.6.6

;; AUTHORITY SECTION:
.                       600     IN      NS      most-evil-dns.com.

;; ADDITIONAL SECTION:
most-evil-dns.com.      600     IN      A       123.0.6.6

;; Query time: 21 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Tue Dec 04 02:45:57 EST 2018
;; MSG SIZE  rcvd: 98

[12/04/18]seed@VM:~$
```

Above picture is screenshot of user after DNS poisoning attack is successful.

```
Open                                                                    Save
                                        KybsEebqGIKdnmXlWKqqWLuaoJgj1/aLLaB/
                                        QejN95q53keNwUJjT8nH8d554Cit6Ef7pK9I
                                        shkT0zVoTvqniOBPkoskZ2CGJmYk7FOOia+q
                                        s0pRu5KL15GtY/qsxQ== )
; authanswer
google.com.             347     A       125.6.6.6
; answer
most-evil-dns.com.      733     \-ANY   ;-$NXDOMAIN
; com. SOA a.gtld-servers.net. nstld.verisign-grs.com. 1543909619 1800 900 604800 86400
; com. RRSIG SOA ...
; 3RL2Q58205687C8I9KC9MV46DGHCNS45.com. RRSIG NSEC3 ...
; 3RL2Q58205687C8I9KC9MV46DGHCNS45.com. NSEC3 1 1 0 - 3RL3ODP8D910939I655B97GAQU6VE1Q7 NS DS RRSIG
; CK0POJMG874LJREF7EFN8430QVIT8BSM.com. RRSIG NSEC3 ...
; CK0POJMG874LJREF7EFN8430QVIT8BSM.com. NSEC3 1 1 0 - CK0Q1GIN43N1ARRC9OSM6QPQR81H5M9A NS SOA
RRSIG DNSKEY NSEC3PARAM
; I5KVKGRJE9ENOA87RQTDT95ULKSBIB5L.com. RRSIG NSEC3 ...
; I5KVKGRJE9ENOA87RQTDT95ULKSBIB5L.com. NSEC3 1 1 0 - I5L1O3PK9G43O6LLE30JBTLUQ11KVK4A NS DS RRSIG
; glue
a.gtld-servers.net.     172633  A       192.5.6.30
; glue
                        172633  AAAA    2001:503:a83e::2:30
; glue
b.gtld-servers.net.     172633  A       192.33.14.30
; glue
                        172633  AAAA    2001:503:231d::2:30
; glue
c.gtld-servers.net.     172633  A       192.26.92.30
; glue
                        172633  AAAA    2001:503:83eb::30
; glue
d.gtld-servers.net.     172633  A       192.31.80.30
; glue
                        172633  AAAA    2001:500:856e::30
; glue
e.gtld-servers.net.     172633  A       192.12.94.30
; glue
                        172633  AAAA    2001:502:1ca1::30
; glue
                                Plain Text   Tab Width: 8   Ln 12, Col 34   INS
```

Above is dumped cache from DNS server.

Conclusion.

By attacking DNS, hacker can lead victims to malicious web site without notice. DNS attack is especially effective when a user's system is already compromised to a hacker. Therefore, it is needed to check whether DNS is valid. For NAT network, network administrator's care is necessary to avoid DNS attack by hacker. Also, it is much easier for a hacker to attack from the inside network. Therefore, effective user control is needed. For this assignment, setting up VMs and each systems according to their role was hardest part. It took around 8 hours to finish this lab.