BÀI 5.
AN TOÀN AN NINH CHO ỨNG DỤNG MẠNG

Nguyễn Đức Toàn,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

1

1. AN TOÀN AN NINH TRÊN TẦNG GIAO VẬN

Nguyễn Đức Toàn,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

2

Nhắc lại về TCP

- Transmission Control Protocol
- Hướng liên kết (connection-oriented), tin cậy:
  - Thiết lập liên kết: bắt tay 3 bước
  - Truyền dữ liệu
  - Kết thúc liên kết
- Báo nhận, phát lại
- Điều khiển luồng
- Điều khiển tắc nghẽn

3

3

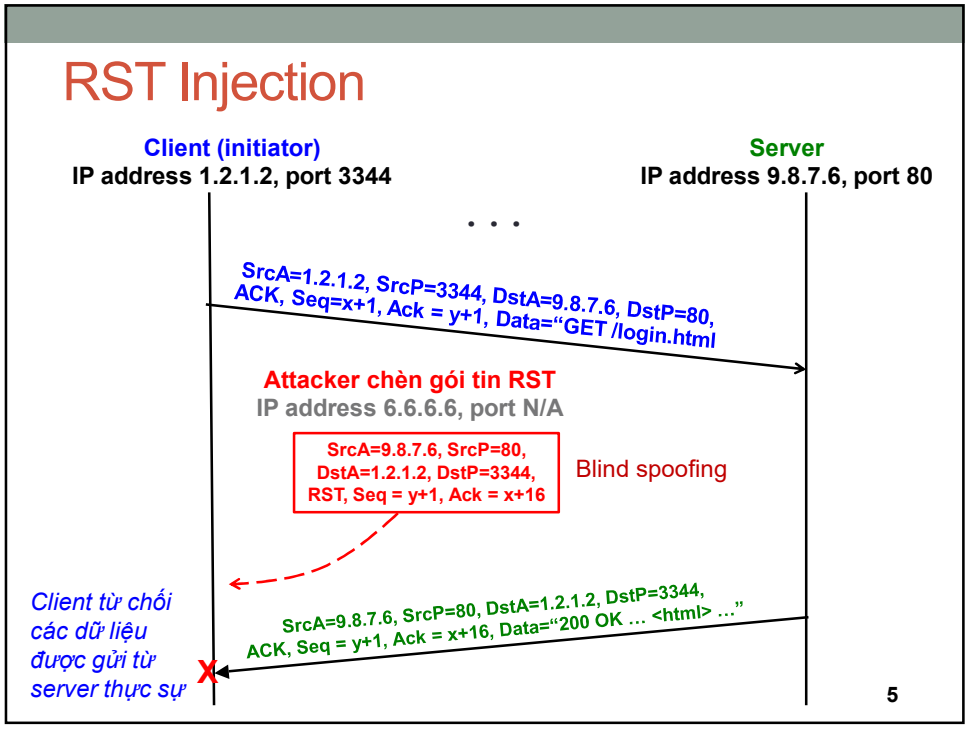
Tấn công can thiệp vào kết nối TCP

- Quá trình trao đổi dữ liệu kết thúc bình thường: giao thức TCP cho phép 2 bên đóng liên kết một cách độc lập (gửi gói tin FIN)
  - Tin cậy: chờ nhận ACK
  - Liên kết chỉ thực sự hủy khi 2 bên đã đóng
- Ngược lại, nếu quá trình trao đổi dữ liệu không thể kết thúc bình thường (tiến trình ứng dụng kết thúc đột ngột, các gói tin lỗi), gói tin RST (reset) được gửi đi:
  - Việc đóng liên kết xuất phát từ một bên
  - Không cần chờ ACK
  - Liên kết được hủy nếu Sequence Number là phù hợp

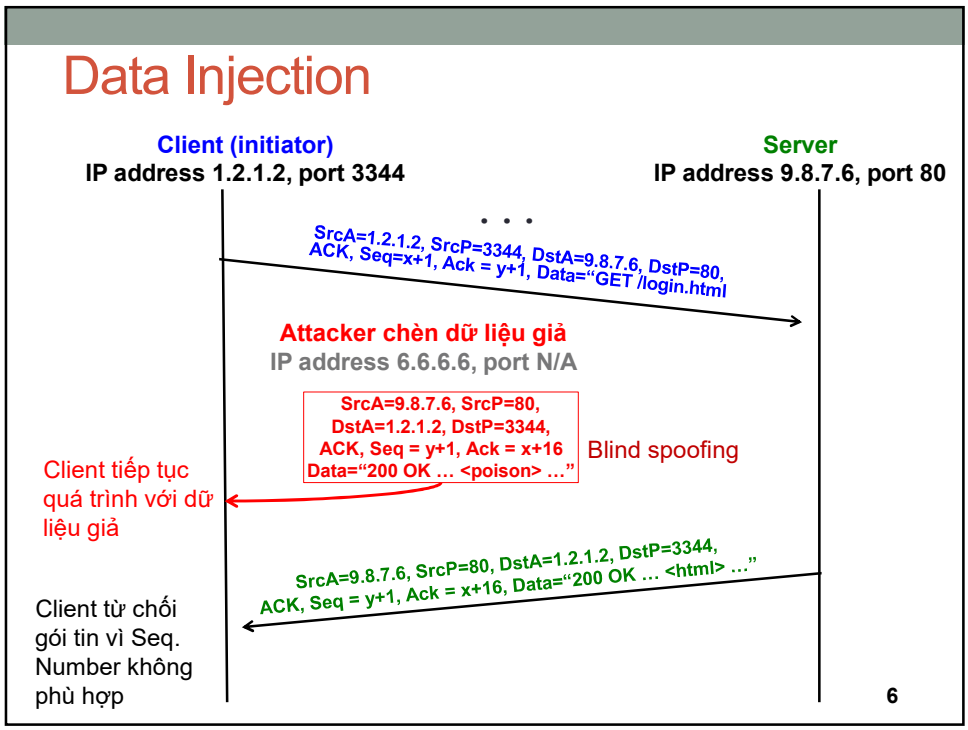
  → kẻ tấn công có thể ngắt kết nối đột ngột của người dùng nếu biết được thông tin về số hiệu cổng, Sequence Number

4

4


RST Injection
Client (initiator)
IP address 1.2.1.2, port 3344
Server
IP address 9.8.7.6, port 80
SrcA=1.2.1.2, SrcP=3344, DstA=9.8.7.6, DstP=80,
ACK, Seq=x+1, Ack = y+1, Data="GET /login.html
Attacker chèn gói tin RST
IP address 6.6.6.6, port N/A
SrcA=9.8.7.6, SrcP=80,
DstA=1.2.1.2, DstP=3344,
RST, Seq = y+1, Ack = x+16
Blind spoofing
Client từ chối
các dữ liệu
được gửi từ
server thực sự
SrcA=9.8.7.6, SrcP=80, DstA=1.2.1.2, DstP=3344,
ACK, Seq = y+1, Ack = x+16, Data="200 OK ... <html> ..."
X
5

5


Data Injection
Client (initiator)
IP address 1.2.1.2, port 3344
Server
IP address 9.8.7.6, port 80
SrcA=1.2.1.2, SrcP=3344, DstA=9.8.7.6, DstP=80,
ACK, Seq=x+1, Ack = y+1, Data="GET /login.html
Attacker chèn dữ liệu giả
IP address 6.6.6.6, port N/A
SrcA=9.8.7.6, SrcP=80,
DstA=1.2.1.2, DstP=3344,
ACK, Seq = y+1, Ack = x+16
Data="200 OK ... <poison> ..."
Blind spoofing
Client tiếp tục
quá trình với dữ
liệu giả
SrcA=9.8.7.6, SrcP=80, DstA=1.2.1.2, DstP=3344,
ACK, Seq = y+1, Ack = x+16, Data="200 OK ... <html> ..."
Client từ chối
gói tin vì Seq.
Number không
phù hợp
6

6

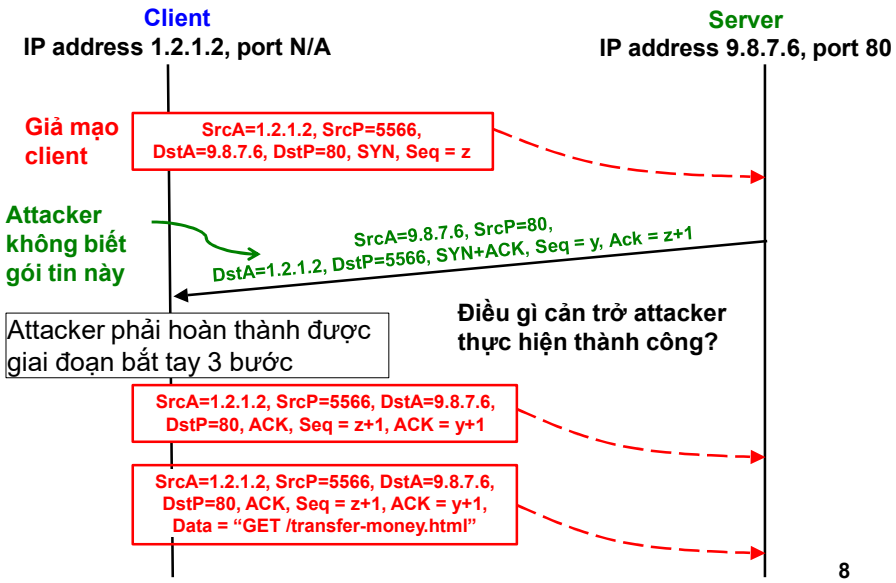
Tấn công kết nối TCP trong trường hợp không biết thông tin về kết nối

- Nhận xét: trong các kịch bản tấn công trên, kẻ tấn công cần phải theo dõi các thông số trên kết nối (cổng, Sequence Number...)
- Trong trường hợp không có các thông tin này, kẻ tấn công vẫn có thể thực hiện bằng cách đoán nhận → blind spoofing
- Hoặc đơn giản hơn: giả mạo kết nối TCP
- Phòng chống?

7

7

Tấn công giả mạo kết nối TCP



8

8

Kịch bản tấn công của Mitnick

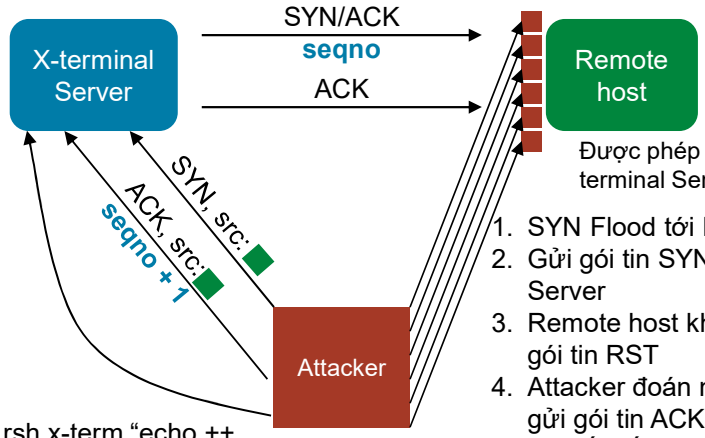
- Kevin Mitnick (1969) thực hiện cuộc tấn công vào hệ thống máy chủ của Tsutomu Shimomura(1964)
- Phát hiện lỗ hổng trên máy chủ X-terminal không sinh giá trị Seq ngẫu nhiên(= Seq_{i-1} + 128.000)
- Tấn công vào website của Shimomura và phát hiện danh sách các nút mạng được phép truy cập từ xa tới máy chủ X-terminal

→ tấn công giả mạo kết nối TCP(1992)

9

9

Kịch bản tấn công của Mitnick



Được phép truy cập tới X-terminal Server

1. SYN Flood tới Remote host
2. Gửi gói tin SYN tới X-terminal Server
3. Remote host không thể gửi gói tin RST
4. Attacker đoán nhận **seqno**, gửi gói tin ACK xác nhận thiết lập kết nối
5. Giành quyền truy cập vào X-terminal server
6. RST Flood tới Remote host

rsh x-term “echo ++ >>./rhosts”

10

10

5. AN TOÀN AN NINH TRÊN TẦNG ỨNG DỤNG

Nguyễn Đức Toàn,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

5.1. AN TOÀN BẢO MẬT DỊCH VỤ DNS

Nguyễn Đức Toàn,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

Tổng quan về DNS

- Tên miền: định danh trên tầng ứng dụng cho các nút mạng
  - Trên Internet được quản lý tập trung
  - Quốc tế: ICANN
  - Việt Nam: VNNIC
- DNS(Domain Name System): hệ thống tên miền
  - Không gian thông tin tên miền
  - Gồm các máy chủ quản lý thông tin tên miền và cung cấp dịch vụ DNS
- Vấn đề phân giải tên miền sang địa chỉ IP
  - Người sử dụng dùng tên miền để truy cập dịch vụ
  - Máy tính và các thiết bị mạng không sử dụng tên miền mà dùng địa chỉ IP khi trao đổi dữ liệu

→Dịch vụ DNS: phân giải tên miền thành địa chỉ IP và ngược lại

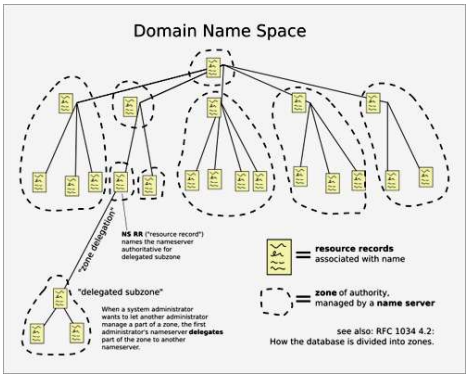
  - UDP, cổng 53

13

13

Hệ thống tên miền

- Không gian tên miền
- Kiến trúc : hình cây
  - Root
  - Zone
- Mỗi nút là một tập hợp các bản ghi mô tả tên miền tương ứng với nút lá đó.
  - SOA
  - NS
  - A
  - PTR
  - CNAME



14

14

Hệ thống máy chủ DNS

- Máy chủ tên miền gốc (Root server)
  - Trả lời truy vấn cho các máy chủ cục bộ
  - Quản lý các zone và phân quyền quản lý cho máy chủ cấp dưới
  - Có 13 máy chủ gốc trên mạng Internet

15

15

Hệ thống máy chủ (tiếp)

- Máy chủ tên miền cấp 1 (Top Level Domain)
  - Quản lý tên miền cấp 1
- Máy chủ được ủy quyền (Authoritative DNS servers)
  - Quản lý tên miền cấp dưới
- Máy chủ của các tổ chức: của ISP
  - Không nằm trong phân cấp của DNS
- Máy chủ cục bộ: dành cho mạng nội bộ của cơ quan tổ chức
  - Không nằm trong phân cấp của DNS

16

16

Thông điệp DNS

- DNS Query và DNS Reply
  - Chung khuôn dạng
- QUESTION: tên miền cần truy vấn
  - Số lượng: #Question
- ANSWER: thông tin tên miền tìm kiếm được
  - Số lượng: #Answer RRs
- AUTHORITY: địa chỉ server trả lời truy vấn
- ADDITIONAL: thông tin phân giải tên miền cho các địa chỉ khác

SRC = 53	DST = 53
checksum	length
Identification	Flags
#Question	#Answer RRs
#Authority RRs	#Additional RRs
QUESTION	
ANSWER	
AUTHORITY	
ADDITIONAL	

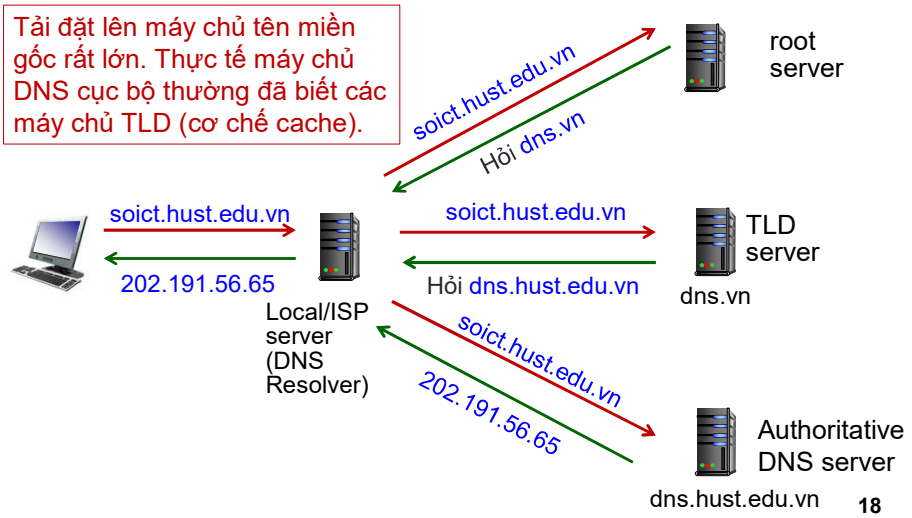
17

17

Phân giải tên miền

- Phân giải tương tác: Cơ chế mặc định trên các máy chủ DNS

Tải đặt lên máy chủ tên miền gốc rất lớn. Thực tế máy chủ DNS cục bộ thường đã biết các máy chủ TLD (cơ chế cache).

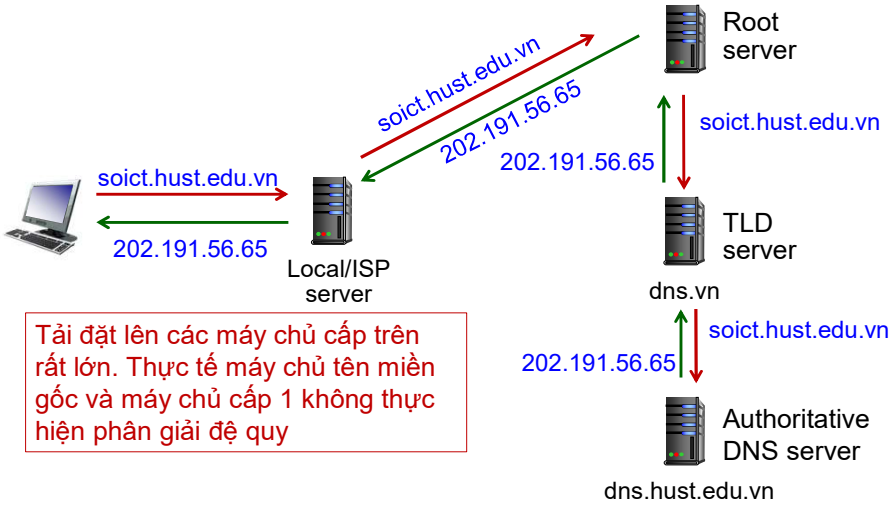


18

18

Phân giải tên miền

- Phân giải đệ quy



Tải đặt lên các máy chủ cấp trên rất lớn. Thực tế máy chủ tên miền gốc và máy chủ cấp 1 không thực hiện phân giải đệ quy

19

19

dig linux.com

```
; <> DiG 9.9.2-P1 <> linux.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21655
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2,
ADDITIONAL: 2
;; QUESTION SECTION:
;linux.com.  IN A
;; ANSWER SECTION:
linux.com.  1786 IN A 140.211.167.51
linux.com.  1786 IN A 140.211.167.50
;; AUTHORITY SECTION:
linux.com.  86386 IN NS ns1.linux-foundation.org.
linux.com.  86386 IN NS ns2.linux-foundation.org.
;; ADDITIONAL SECTION:
ns1.linux-foundation.org.  261 IN A 140.211.169.10
ns2.linux-foundation.org.  262 IN A 140.211.169.11
```

TTL: thời gian(s) lưu giữ trả lời trong cache

20

20

dig linux.com

```
; <> DiG 9.9.2-P1 <> linux.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21655
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2,
ADDITIONAL: 3
;; QUESTION SECTION:
;linux.com. IN A
;; ANSWER SECTION:
linux.com. 1786 IN A 140.211.167.51
linux.com. 1786 IN A 140.211.167.50
;; AUTHORITY SECTION:
linux.com. 86386 IN NS ns1.linux-foundation.org.
linux.com. 86386 IN NS ns2.linux-foundation.org.
;; ADDITIONAL SECTION:
ns1.linux-foundation.org. 261 IN A 140.211.169.10
ns2.linux-foundation.org. 262 IN A 140.211.169.11
```

Tên các máy chủ DNS server trả lời truy vấn. Nếu phần ANSWER rỗng, DNS Resolver gửi truy vấn tới các máy chủ này

21

21

dig linux.com

```
; <> DiG 9.9.2-P1 <> linux.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21655
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2,
ADDITIONAL: 3
;; QUESTION SECTION:
;linux.com. IN A
;; ANSWER SECTION:
linux.com. 1786 IN A 140.211.167.51
linux.com. 1786 IN A 140.211.167.50
;; AUTHORITY SECTION:
linux.com. 86386 IN NS ns1.linux-foundation.org.
linux.com. 86386 IN NS ns2.linux-foundation.org.
;; ADDITIONAL SECTION:
ns1.linux-foundation.org. 261 IN A 140.211.169.10
ns2.linux-foundation.org. 262 IN A 140.211.169.11
```

Địa chỉ IP của các máy chủ trả lời truy vấn. Thông tin này được lưu vào cache

22

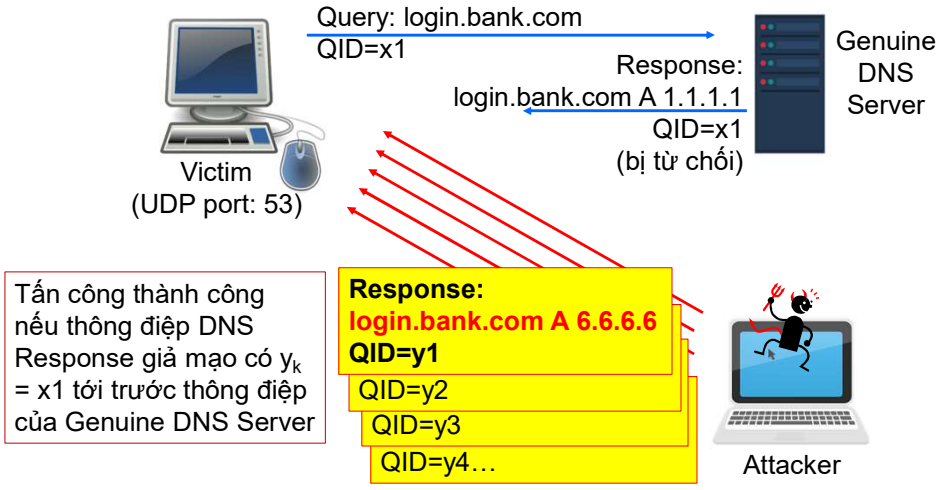
22

Một số dạng tấn công DNS

- Các vấn đề của DNS
  - Không có cơ chế xác thực thông tin phân giải
  - Không cần thiết lập kết nối
- Tấn công vào máy chủ cung cấp dịch vụ: DoS/DDoS, tấn công khai thác các lỗi phần mềm
- Tấn công vào giao thức DNS:
  - DNS cache poisioning
  - DNS spoofing
  - DNS rebinding
- Tấn công DDoS lợi dụng Open DNS Resolver
- DNS Amplification attack

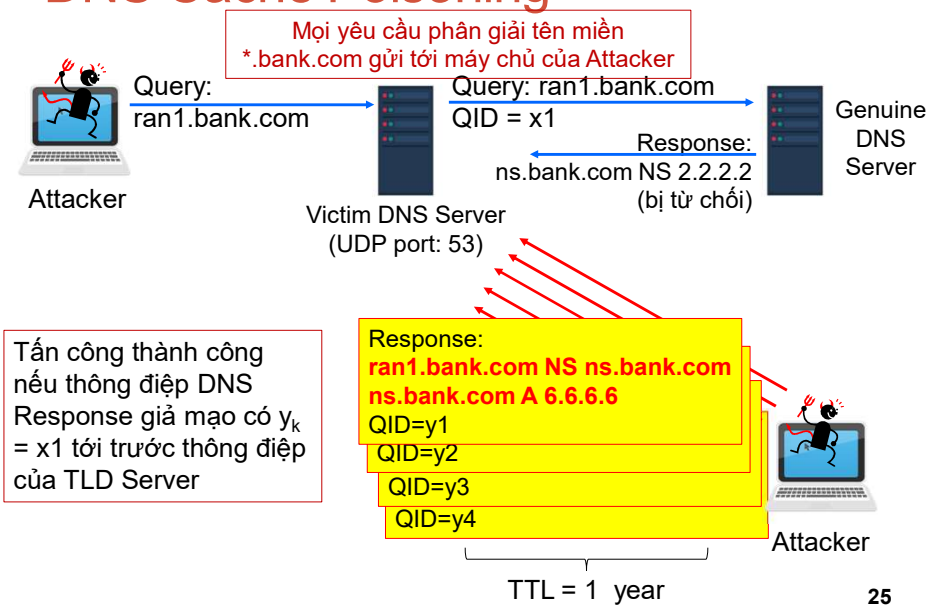
23

DNS Spoofing



24

DNS Cache Poisoning



25

25

DNS cache poisioning

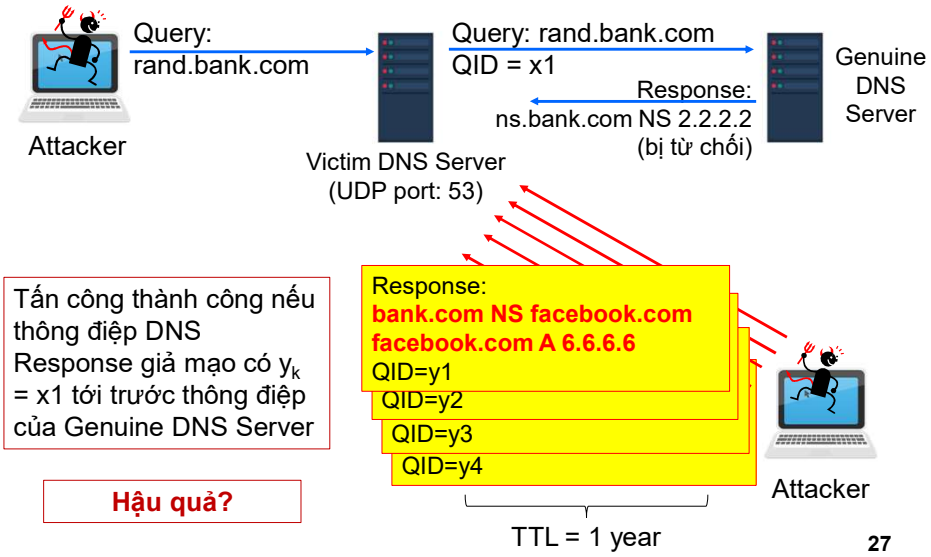
```
; <> DiG 9.9.2-P1 <> a.bank.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21655
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1,
ADDITIONAL: 1
;; QUESTION SECTION:
a.bank.com. IN A
;; ANSWER SECTION:
;; AUTHORITY SECTION:
bank.com. 86386 IN NS ns.bank.com.
;; ADDITIONAL SECTION:
ns.bank.com. 261 IN A 6.6.6.6
```

Địa chỉ của máy chủ DNS do kẻ tấn công điều khiển

26

26

DNS Cache Poisoning: cross-domain



Tấn công thành công nếu thông điệp DNS Response giả mạo có y_k = x1 tới trước thông điệp của Genuine DNS Server

Hậu quả?

27

27

dig rand.bank.com

```
; <> DiG 9.9.2-P1 <> rand.bank.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21655
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 2,
ADDITIONAL: 2
;; QUESTION SECTION:
rand.bank.com. IN A
;; ANSWER SECTION:
;; AUTHORITY SECTION:
bank.com. 86386 IN NS ns.bank.com.
bank.com. 86386 IN NS facebook.com.
;; ADDITIONAL SECTION:
ns.bank.com. 261 IN A 140.211.169.10
facebook.com. 262 IN A 6.6.6.6
```

Tên miền bị tấn công

28

28

DNS cache poisioning (tiếp)

- Nếu giá trị QueryID được sử dụng là ngẫu nhiên, xác suất thành công của kẻ tấn công không cao:
  - $P = k/2^{16}$
  - Thông điệp giả mạo có giá trị QueryID phù hợp phải đến trước thông điệp của DNS server tin cậy
- Cải tiến:
  - Tấn công DoS vào máy chủ Genuine DNS Server
  - Sử dụng kỹ thuật tấn công ngày sinh

29

29

DNS cache poisioning (D.Kaminsky '08)

- Kẻ tấn công gửi một loạt các yêu cầu truy vấn tên miền không tồn tại có cùng tên miền cấp trên với tên miền giả mạo
  - Ví dụ: random1.google.com, random2.google.com,…
  - Số lượt thử: 256
- Gửi các thông điệp trả lời giả mạo(QID ngẫu nhiên) với thông tin thêm vào phần Authority và Additional
  - Số bản tin cần giả mạo mỗi lượt thử: 256
- Phòng chống: DNS server sử dụng số hiệu cổng ngẫu nhiên khi gửi thông điệp truy vấn

30

30

DNS cache poisioning (D.Kaminsky '08)

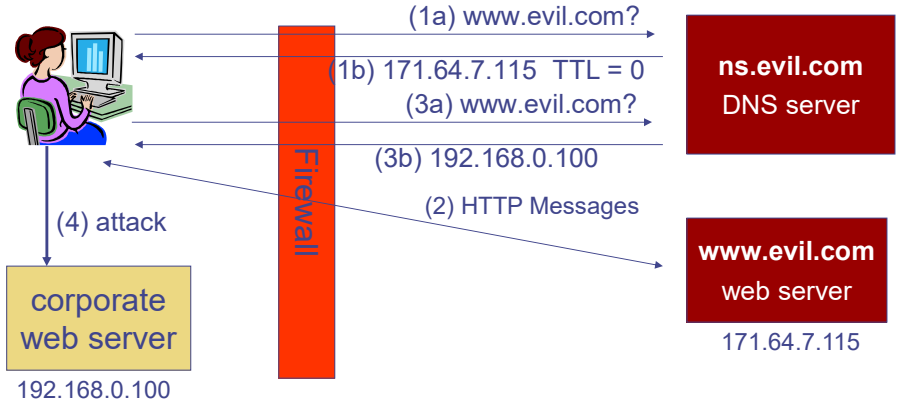
```
;; QUESTION SECTION:
;randomX.google.com.  IN A

;; ANSWER SECTION:

;; AUTHORITY SECTION:
google.com.  86386 IN NS mail.google.com.

;; ADDITIONAL SECTION:
mail.google.com.  86386 IN A 6.7.8.9
```

31

31

DNS Rebinding

<iframe src="**http://www.evil.com**">



32

32

Phòng chống tấn công DNS Rebinding

- Trình duyệt: DNS Pinning
  - Từ chối thay đổi ánh xạ tên miền sang địa chỉ IP khác trong một khoảng thời gian
  - Hạn chế tương tác với proxy, VPN, Dynamic DNS
- Máy trạm người dùng: sử dụng dịch vụ DNS tin cậy
- Máy chủ:
  - Từ chối các thông điệp HTTP request có trường Host là một tên miền không nhận diện được
  - Xác thực người dùng
- Firewall: chặn các thông điệp DNS Reponse phân giải tên miền thành 1 địa chỉ cục bộ

33

33

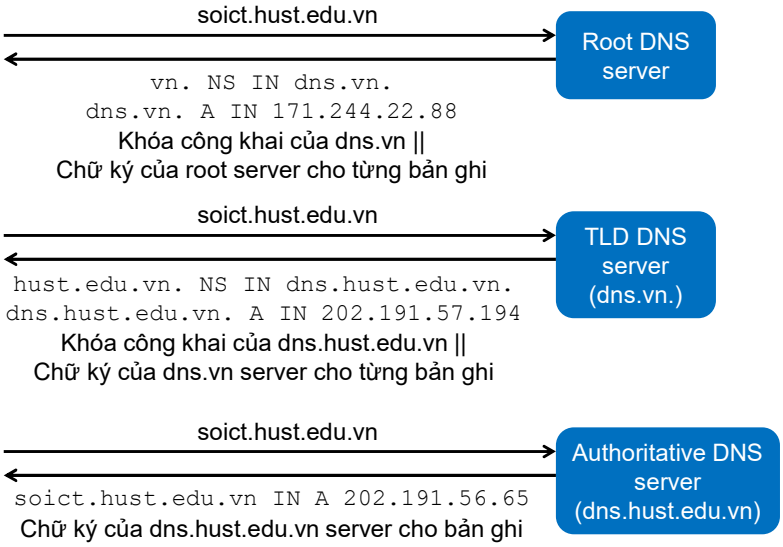
Làm thế nào để dịch vụ DNS an toàn hơn

- Ý tưởng cơ bản: sử dụng mật mã học
- Giải pháp 1: sử dụng kết nối SSL/TLS
  - Phân tích giải pháp?
- Giải pháp 2: chứng thực bản ghi DNS
  - DNSSEC
  - Phân tích giải pháp?

34

34

DNSSEC



35

35

5.2. AN TOÀN AN NINH DỊCH VỤ EMAIL(TỰ HỌC)

Pretty Good Privacy
S/MIME
DKIM
…

36

36

Bài giảng sử dụng một số hình vẽ và ví dụ từ các khóa học:

- Computer and Network Security, Stanford University
- Computer Security, Berkeley University
- Network Security, Illinois University
- Computer and Network Security, University of Maryland

37

37