DNS/DNSSEC

15 AUGUST 2016

EGA
e-Government Agency

G-CERT by EGA

Who am I

- ธงไชย จารุสุรเกษม (เบิร์ด)
  - วิศวกรความมั่นคงปลอดภัยสารสนเทศ 2
  - Tongchai@ega.or.th
  - 02-612-6000 Ext. 4307

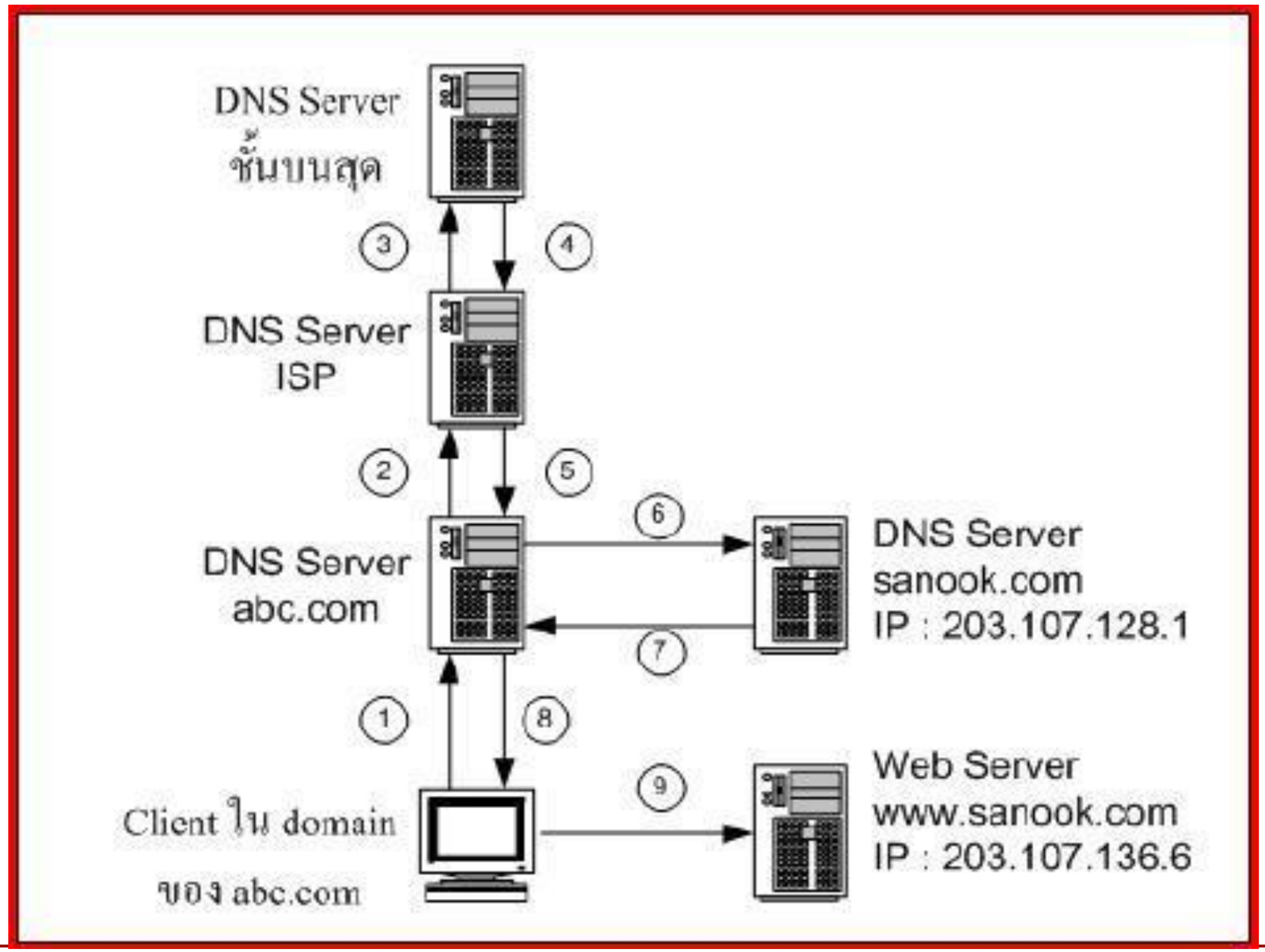
Agenda

- DNS Concepts
- BIND Installation & Configuration (Labs)
- Domains Configuration (Labs)
- Master(Primary) and Slave(Secondary) (Labs)
- DNS Attacks
- TSIG (Transaction Signature) (Labs)
- DNSSEC (Domain Name System Security Extensions) (Labs)

DNS Concepts

DNS Works

❖ DNS ย่อมาจาก Domain Name System หมายถึง ระบบจัดการแปลง Name ไปเป็น IP Address โดยมีหลักการทำงาน ดังนี้



DNS Types

- DNS แบ่งออกได้เป็น 2 ประเภท ได้แก่
  - Master Name Server(Primary) - เป็นฐานข้อมูลหลักของโดเมน การเพิ่ม/แก้ไข/ลบข้อมูลทำที่ Master อย่างเดียว
  - Slave Name Server(Secondary) - จะทำหน้าที่สำเนาข้อมูลมาจาก Master ตามเวลาที่กำหนดโดยอัตโนมัติ

Name Server ข้างต้นยังสามารถแยกการทำงานได้ 2 แบบ คือ

- Forward Lookup Zone – ทำหน้าที่แปลง Domain Name หรือ Host Name ให้เป็น IP Address
- Reverse Lookup Zone - ทำหน้าที่แปลงค่า IP Address ให้เป็น Host Name

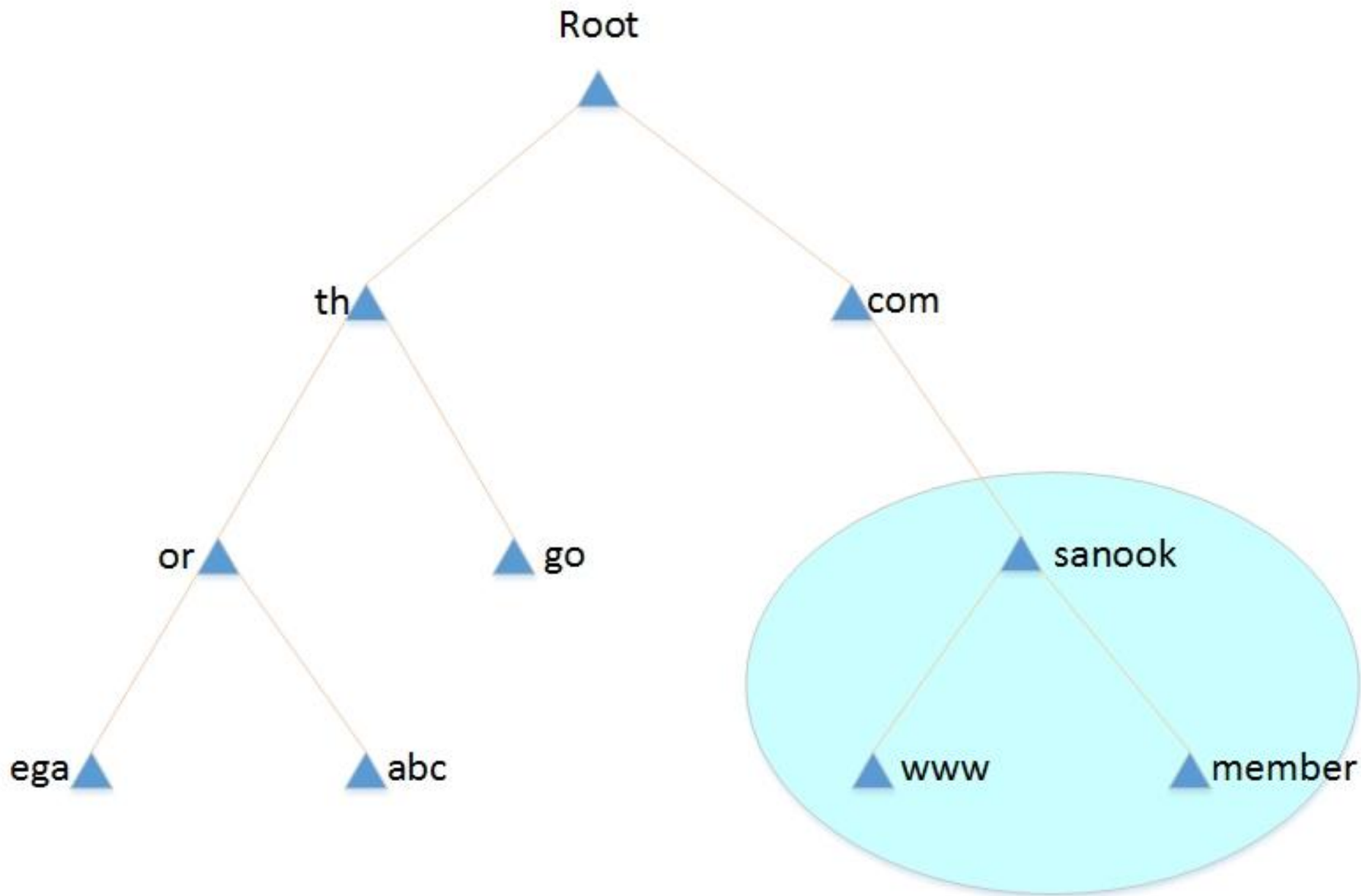
Name Space

- Name Space - บน Internet จะมีการควบคุมการตั้งชื่อต่างๆ และ IP Address ซึ่งจะต้องมีชื่อที่ไม่ซ้ำกัน แบ่งออกเป็น 2 แบบ คือ
  - Flat Name Space - การตั้งชื่อ Name Space ไม่มีโครงสร้าง เช่น 123.testx, asdf.12
  - Hierarchical Name space - การตั้งชื่อ Name Space แบบมีโครงสร้างเป็นลำดับชั้น เช่น .th , .or.th , ega.or.th

Domain Name Space

- Domain Name Space - มีโครงสร้างแบบลำดับชั้น เป็น Tree โดยมี Root อยู่ด้านบนสุด
  - Label - ในแต่ละ node จะมี Label กำกับอยู่ และ label ของ root จะเป็น null string หรือ ไม่มีชื่อ โดย node ลูกที่แตกออกมาจาก node แม่จะต้องมี label ไม่ซ้ำกับ node แม่
  - Domain Name – เป็นลำดับของ label โดยใช้จุด (.) เป็นตัวแยก domain name และจะอ่านจากข้างล่างขึ้นด้านบนไปยัง root

Domain Name Space



DNS Server and Zone

- DNS Server - เครื่องคอมพิวเตอร์ หรือ โปรแกรมที่เก็บฐานข้อมูลเกี่ยวกับ Domain Name และ IP Address และ ให้บริการแปลง Domain Name ไปเป็น IP Address เมื่อมีการร้องขอ เพื่อใช้อ้างอิงถึงที่อยู่ของเครื่องคอมพิวเตอร์ที่มี IP Address ตรงกับ Domain ที่ร้องขอ
  - Zone - หรือ Domain คือ สิ่งเดียวกัน โดย DNS Server จะสร้างฐานข้อมูลที่เรียกว่า Zone file เพื่อเก็บข้อมูลของทุกๆ node ภายใต้ Domain นั้นๆ โดยที่
    - Primary Server - ทำหน้าที่เก็บ Zone file ปรับปรุง/แก้ไข/ดูแล Zone file นั้นๆ
    - Secondary Server – ทำหน้าที่ถ่ายโอนข้อมูลเกี่ยวกับ Zone file มาจาก DNS Server อื่นๆ (ได้ทั้ง Primary และ Secondary)

- Zone file คือ file ที่ใช้เก็บข้อมูลเกี่ยวกับ Domain โดยจะมี Resource Record เป็นตัวบ่งบอกชนิดของ Record ที่บันทึกไว้ใน Zone file

Resource Record

- A - Address record คือ record ที่ใช้สำหรับ map Host name เป็น IP Address

  <host> IN A <IP-address>

- AAAA – Address record คือ record ที่ใช้สำหรับ map Host name เป็น IP Address IPv6

  <host> IN AAAA <IP-address-IPv6>

- CNAME - Canonical name record คือ record ที่ใช้ map ไปอีกชื่อหนึ่ง

  <alias-name> IN CNAME <real-name>

- MX - Mail Exchange record คือ record ที่ใช้เกี่ยวกับระบบ email

  IN MX <preference-value> <email-server-name>

Resource Record

- NS - Name Server record คือ record ที่แจ้ง name server ที่เป็น Authorize server ของ domain นั้นๆ

IN NS <nameserver-name>

- PTR - Pointer record คือ record ที่ใช้สำหรับ map IP Address ไปเป็น Host name

<IP-address> IN PTR <host-name>

Resource Record

❖ SOA - Start Of Authority resource record คือ record ที่เก็บรายละเอียดว่า DNS Server ตัวไหนทำหน้าที่เป็น Primary server ของโดเมนนั้นรวมทั้งกระบวนการเก็บความถี่ในการ update ข้อมูลของ Secondary server

@ IN SOA <primary-name-server> <hostmaster-email> (

<serial-number>

<time-to-refresh>

<time-to-retry>

<time-to-expire>

<minimum-TTL>)

Forward Zone File (Example)

```
$TTL 86400
@           IN    SOA    dns1.example.com.    hostmaster.example.com. (
                         2016081501      ; serial
                         21600           ; refresh after 6 hours
                         3600            ; retry after 1 hour
                         604800          ; expire after 1 week
                         86400           ; minimum TTL of 1 day )
            IN    NS          dns1.example.com.
            IN    NS          dns2.example.com.
            IN    MX      10  mail.example.com.
            IN    MX      20  mail2.example.com.
            IN    A           10.0.1.5
server1     IN    A           10.0.1.5
server2     IN    A           10.0.1.7
dns1        IN    A           10.0.1.2
dns2        IN    A           10.0.1.3
ftp         IN    CNAME       server1
mail        IN    CNAME       server1
mail2       IN    CNAME       server2
www         IN    CNAME       server2
```

Reverse Zone File (Example)

```
$TTL 86400
@       IN    SOA    dns1.example.com.    hostmaster.example.com. (
                     2016081501           ; serial
                     21600                ; refresh after 6 hours
                     3600                 ; retry after 1 hour
                     604800               ; expire after 1 week
                     86400                ; minimum TTL of 1 day )
              IN     NS     dns1.example.com.
              IN     NS     dns2.example.com.
20            IN     PTR    alice.example.com.
21            IN     PTR    betty.example.com.
22            IN     PTR    charlie.example.com.
23            IN     PTR    doug.example.com.
24            IN     PTR    ernest.example.com.
25            IN     PTR    fanny.example.com.
```

BIND Installation

& Configuration

BIND Installation

- ติดตั้ง BIND

  [root@master ~]# yum install bind bind-utils –y

- Config ให้ Service BIND run โดยอัตโนมัติ หากมีการ Restart Server

  [root@master ~]# systemctl enable named

  Created symlink from /etc/systemd/system/multi-user.target.wants/named.service to /usr/lib/systemd/system/named.service.

- สั่งให้ Service BIND Start

  [root@master ~]# systemctl start named

- คำสั่งในการตรวจสอบว่า Service ทำงานอยู่หรือไม่

  [root@master ~]# systemctl status named

  - named.service - Berkeley Internet Name Domain (DNS)

    Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; vendor preset: disabled)

    Active: active (running) since Fri 2016-07-29 02:00:12 ICT; 3s ago

Iptables Configuration

- เพิ่ม Policy firewall สำหรับ Service DNS

```
[root@master ~]# vi /etc/sysconfig/iptables
# sample configuration for iptables service
# you can edit this manually or use system-config-firewall
# please do not ask us to add additional ports/services to this default configuration
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 53 -j ACCEPT
-A INPUT -p udp -m state --state NEW -m udp --dport 53 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

BIND Configuration

- Config DNS Server ให้สามารถใช้งานได้จากเครื่อง Client

```
[root@master ~]# vi /etc/named.conf
options {
        listen-on port 53 { any; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { any; };
                ......
};
```

Domains Configuration

Domain Configuration

- Config ค่า Domain

```
[root@master ~]# vi /etc/named.conf
.....
zone "labs.test" IN {
        type master;
        file "labs.test.db";
        allow-update { none; };
};
zone “125.168.192.in-addr.arpa" IN {
        type master;
        file "125.168.192.in-addr.arpa.db";
        allow-update { none; };
};
```

Forward Zone File (Create)

- สร้าง Forward Zone file ใหม่โดยสร้างไว้ที่ folder /var/named/

[root@master ~]# vi /var/named/labs.test.db

```
$TTL 86400
@           IN    SOA   ns.labs.test.     root.labs.test. (
                                2016081501          ; serial
                                21600               ; refresh after 6 hours
                                3600                ; retry after 1 hour
                                604800              ; expire after 1 week
                                86400 )             ; minimum TTL of 1 day
            IN    NS          ns.labs.test.
            IN    MX          10     mail.labs.test.
            IN    MX           20     mail2.labs.test.
            IN    A           192.168.125.134
server1     IN    A           192.168.125.10
server2     IN    A           192.168.125.20
ns          IN    A           192.168.125.134
ftp         IN    CNAME       server1
mail        IN    CNAME       server1
mail2       IN    CNAME       server2
www         IN    CNAME       server2
```

Reverse Zone File (Create)

- สร้าง Reverse Zone file ใหม่โดยสร้างไว้ที่ folder /var/named/

```
[root@master ~]# vi /var/named/125.168.192.in-addr.arpa.db
$TTL 86400
@       IN      SOA     ns.labs.test.   root.labs.test. (
                        2016081501              ; serial
                        21600                   ; refresh after 6 hours
                        3600                    ; retry after 1 hour
                        604800                  ; expire after 1 week
                        86400   )               ; minimum TTL of 1 day
                IN      NS      ns.labs.test.
10      IN      PTR     server1.labs.test.
20      IN      PTR     server2.labs.test.
```

Master(Primary)

&

Slave(Secondary)

Master Server Configuration

❖ Config เพิ่มเติมในส่วนของ Zone ที่อนุญาตให้สามารถ transfer zone file ไปยัง Slave ได้ (Config ที่ Master Server)

```
[root@master ~]# vi /etc/named.conf
        .....
zone "labs.test" IN {
        type master;
        file "labs.test.db";
        allow-update { none; };
        allow-transfer { 192.168.125.135; };
};
        .....
```

Slave Server Configuration

- Config ให้ Slave transfer zone จาก Master (Config ที่ Slave Server)

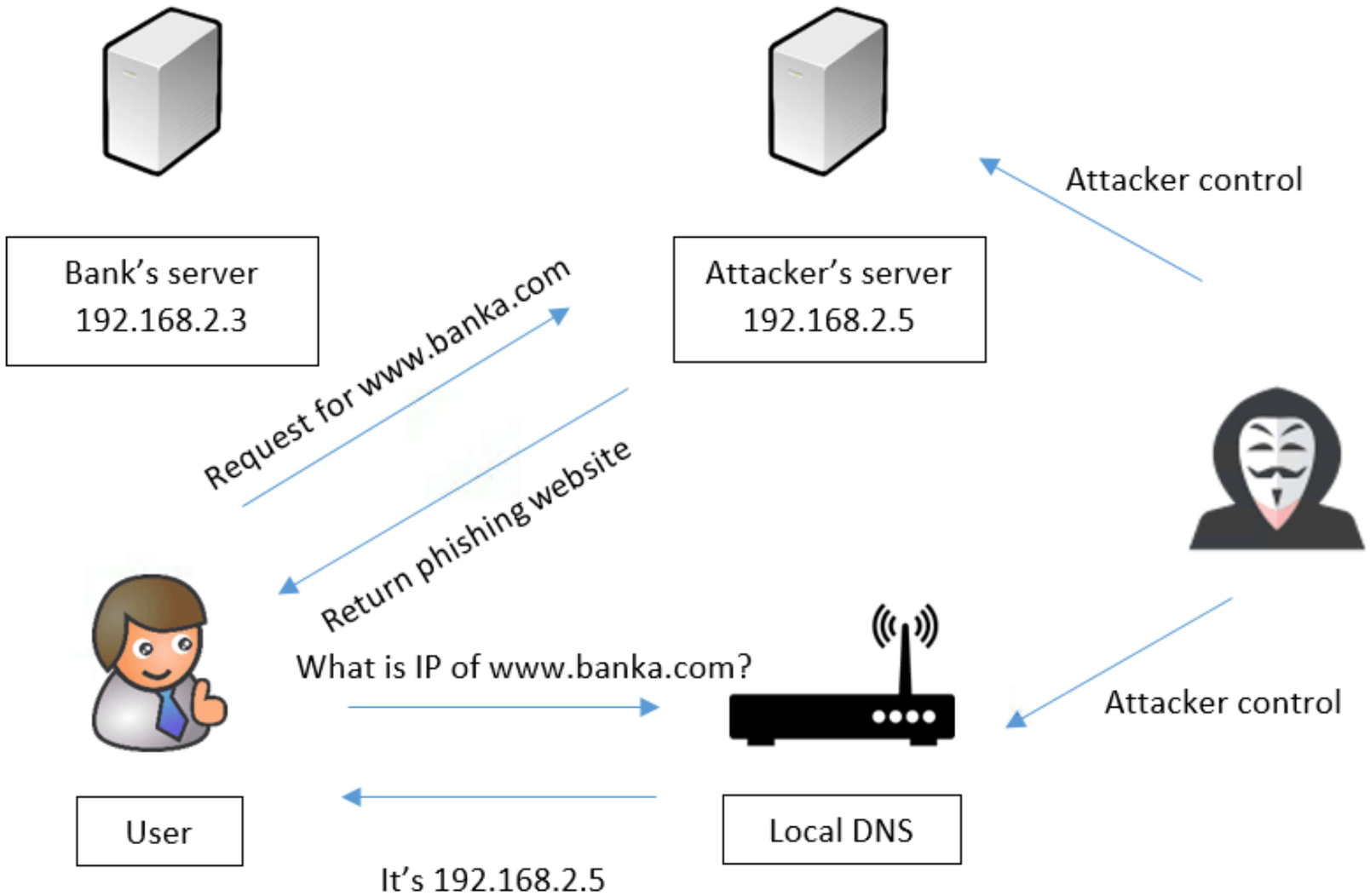
[root@slave ~]# vi /ect/named.conf

```
zone "labs.test" IN {
        type slave;
        masters { 192.168.125.134; };
        file “/var/named/slaves/labs.test.db";
        allow-update{ none; };
};
```

DNS Attacks

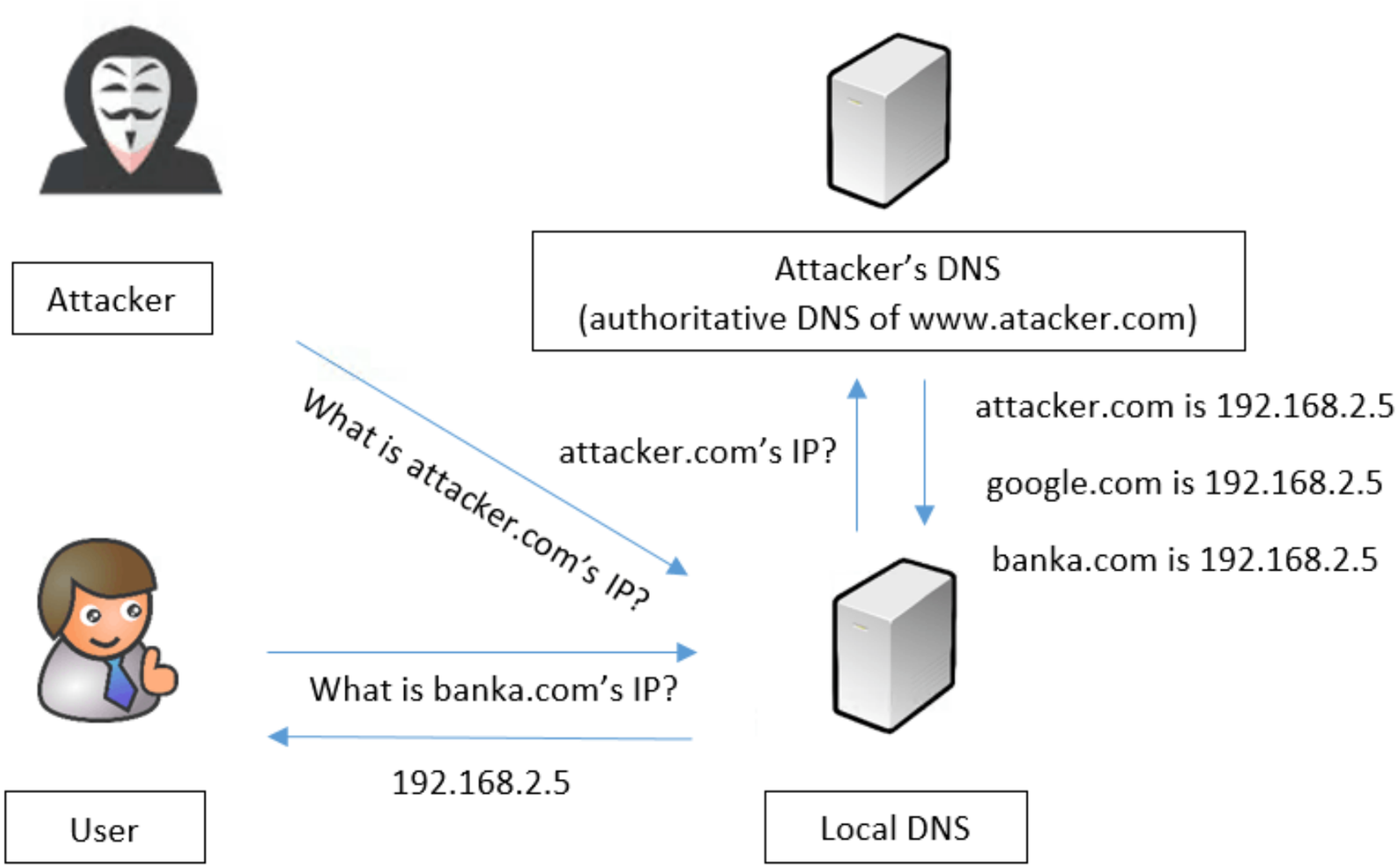
Malicious Local DNS

❖ Malicious Local DNS คือ การโจมตีโดยที่ Attacker สามารถเข้ามาควบคุม Local DNS ได้



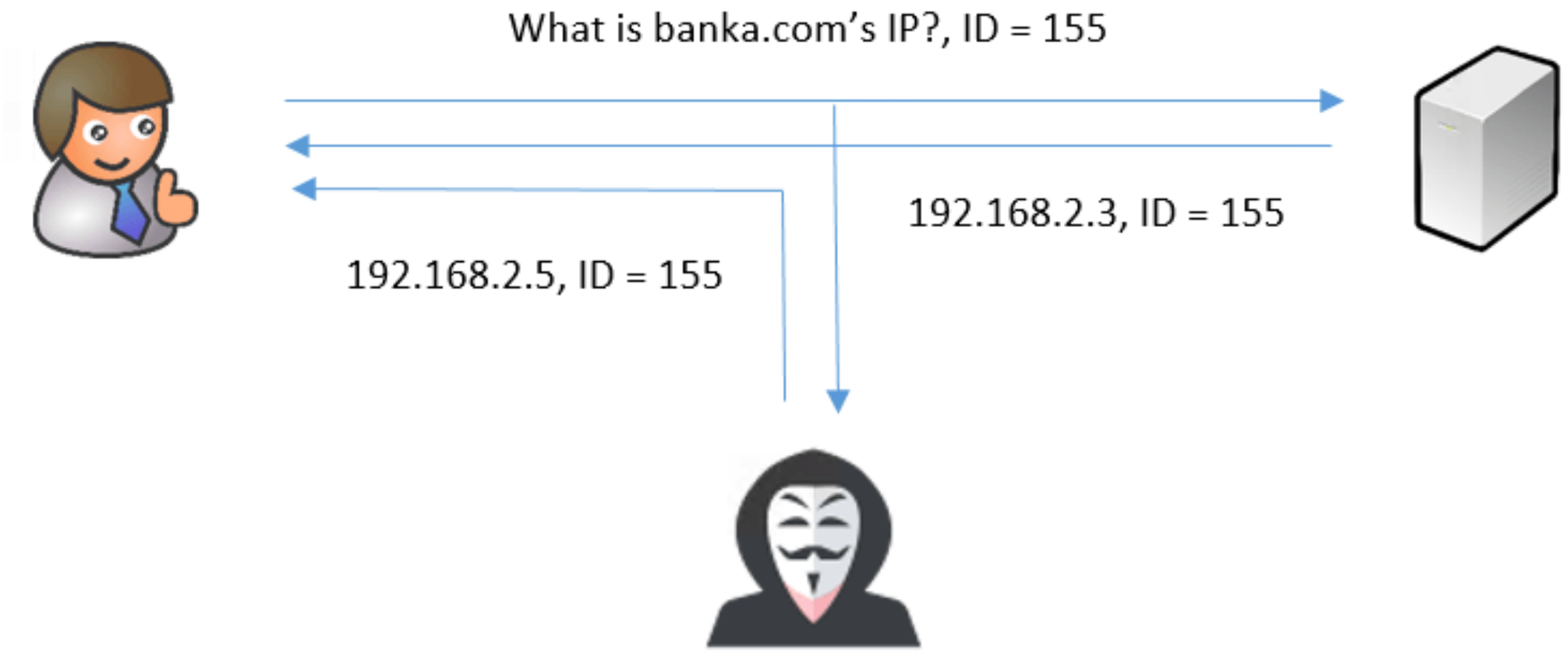
DNS Cache Poisoning

❖ DNS Cache Poisoning คือ การโจมตีโดยการส่ง update cache ที่ไม่ถูกต้องลงไปที่ Local DNS



DNS Spoofing

❖ DNS Spoofing คือ การที่ Attacker หลอกส่งข้อมูลที่ไม่ถูกต้องให้กับ User ก่อนที่ DNS Server จะตอบกลับ



TSIG

(Transaction Signature)

TSIG (Transaction Signature)

- Config TSIG เริ่มต้นจากการสร้าง Key โดยใช้คำสั่ง

[root@master ~]#dnssec-keygen -a HMAC-MD5 -b 128 -n HOST master.local

หมายเหตุ HMAC-MD5 คือ algorithm ในการสร้าง key

128 คือจำนวน bit ที่ใช้

master.local ชื่อของ key ที่จะสร้าง สามารถเปลี่ยนแปลงได้

เมื่อสร้างเสร็จแล้วจะได้ไฟล์ออกมา 2 ไฟล์ดังนี้

- Kmaster.local.+157+09515.key
- Kmaster.local.+157+09515.private

TSIG (Transaction Signature)

- ให้ Copy ค่า Key ออกมาจากไฟล์

[root@master ~]# cat Kmaster.local.+157+09515.private

Private-key-format: v1.3

Algorithm: 157 (HMAC_MD5)

Key: 2TcRvcR1rggkH5W3aGGf4g==

Bits: AAA=

Created: 20160808035403

Publish: 20160808035403

Activate: 20160808035403

TSIG (Transaction Signature)

- Config ค่าเพิ่มเติมที่ named.conf

```
[root@master ~]# vi /etc/named.conf
optyions {
        .....
};
        .....
key tsig.key {
        algorithm hmac-md5 ;
        secret “2TcRvcR1rggkH5W3aGGf4g==” ;
};

server 192.168.125.135 {
        keys { tsig.key; };
};
        .....
```

หมายเหตุ ค่า server 192.168.125.135 คือ IP Address ของ Slave Server

TSIG (Transaction Signature)

- Config ค่าเพิ่มเติมที่ named.conf (ต่อ)

```
.....
zone "labs.test" IN {
        type master;
        file "labs.test.db";
        allow-update { none; };
        //allow-transfer { 192.168.125.135; };
        allow-transfer { key tsig.key; };
};
```

TSIG (Transaction Signature)

- Config ค่าเพิ่มเติมที่ named.conf (Slave Server)

```
[root@master ~]# vi /etc/named.conf
options {
        .....
};
        .....
key tsig.key {
        algorithm hmac-md5 ;
        secret “2TcRvcR1rggkH5W3aGGf4g==” ;
};

server 192.168.125.134 {
        keys { tsig.key; };
};
```

หมายเหตุ ค่า server 192.168.125.134 คือ IP Address ของ Master Server

DNSSEC

(Domain Name System Security Extensions)

DNSSEC

- Config Enable ฟังก์ชั่น DNSSEC

```
[root@master ~]#vi /etc/named.conf
options {
        .....
        recursion yes;

        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;
        .....
};
```

DNSSEC

- สร้าง Zone Signing Key(ZSK) และ Key Signing Key(KSK) สำหรับ Signed Zone

```
[root@master ~]# cd /var/named/
[root@master named]# dnssec-keygen -a rsasha1 -b 1024 -n zone labs.test
[root@master named]# dnssec-keygen -a rsasha1 -b 2048 -f KSK -n zone
labs.test
```

จะได้ไฟล์ออกมา 4 ไฟล์ดังนี้

ZSK

- Klabs.test.+005+22665.key
- Klabs.test.+005+22665.private

KSK

- Klabs.test.+005+28729.key
- Klabs.test.+005+28729.private

DNSSEC

- Config Zone file ที่เราต้องการจะทำ DNSSEC

```
[root@master ~]# vi /var/named/labs.test.db
$TTL 86400
$INCLUDE /var/named/Klabs.test.+005+22665.key ; ZSK
$INCLUDE /var/named/Klabs.test.+005+28729.key ; KSK
@       IN      SOA     ns.labs.test.   root.labs.test. (
                .....
```

- Signing Zone File

```
[root@master named]# dnssec-signzone -o labs.test -t -k
Klabs.test.+005+28729 Klabs.test.+005+22665
```

DNSSEC

ผลจากการ Signing Zone file

Verifying the zone using the following algorithms: RSASHA1.

Zone fully signed:

Algorithm: RSASHA1: KSKs: 1 active, 0 stand-by, 0 revoked

ZSKs: 1 active, 0 stand-by, 0 revoked

labs.test.db.signed

Signatures generated:	21
Signatures retained:	0
Signatures dropped:	0
Signatures successfully verified:	0
Signatures unsuccessfully verified:	0
Signing time in seconds:	0.007
Signatures per second:	2636.203
Runtime in seconds:	0.019

DNSSEC

- Config ให้ใช้งาน Zone file ที่ถูก Signed แล้ว

```
zone "labs.test" IN {
        type master;
        //file "labs.test.db";
        file "labs.test.db.signed";
        allow-update { none; };
        //allow-transfer { 192.168.125.135; };
        allow-transfer { key tsig.key; };
};
```

DNSSEC

- Config ให้ Slave Server ให้ Transfer Zone เป็น .signed (Optional)

```
zone "labs.test" IN {
        type slave;
        masters { 192.168.125.134; };
        //file "/var/named/slaves/labs.test.db";
        file "/var/named/slaves/labs.test.db.signed";
        allow-update { none; };
};
```

DNSSEC

- ค่า DS ที่จะนำไปติดตั้งบน Registra

[root@master named]# cat dsset-labs.test.

labs.test. IN DS 9826 5 1 D8E1A4DB01C7CD35E410E1A9E2010E065F1DBCE2

labs.test. IN DS 9826 5 2 807E3B07BEFC441EF387520E8F96BB6AF2F2A382F9D68BBE891C385F502E0E6D

Q & A