IMPLEMENTAZIONE DEL PROTOCOLLO DNSSEC TRAMITE SOFTWARE KATHARÀ

UNIVERSITÀ
DI PAVIA

Candidato: Didyk Iryna
Matricola: 466488
Relatore: prof. Massari Luisa
Correlatore: dott. Zanussi Luca

Facoltà di Ingegneria
Corso di laurea in Ingegneria Elettronica e Informatica
2022/2023

Indice

1. Katharà
2. DNS
3. Laboratorio
4. DNSSEC
5. Conclusioni

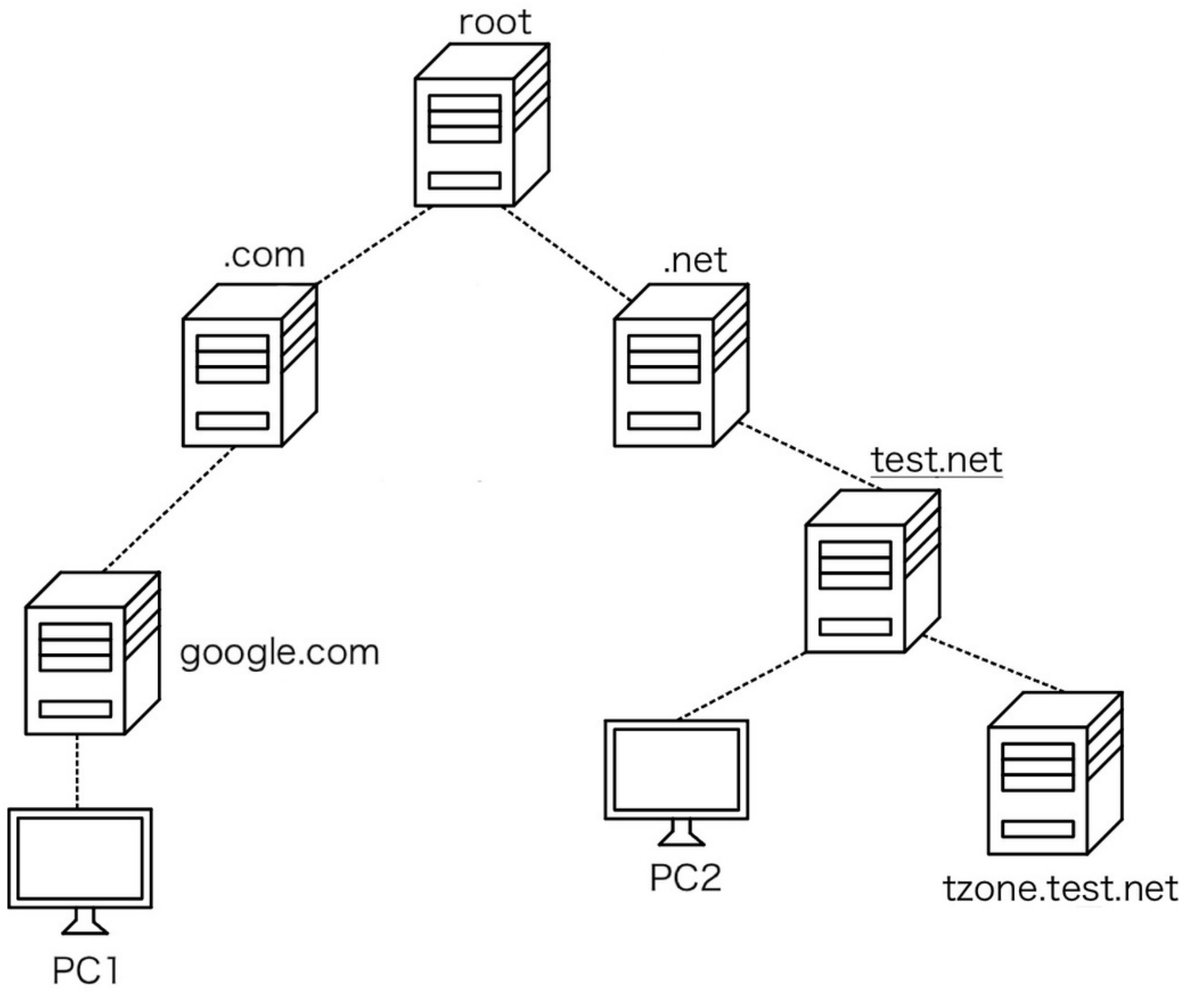
Katharà

Ambiente di sviluppo che utilizza container per emulare dispositivi e interfacce di rete

DNS - Domain Name System

Protocollo che permette di associare ai nomi di dominio i corrispondenti indirizzi IP numerici

Laboratorio



Ad ogni server vengono associati due file:

- named.conf

```
zone "." {
    type hint;
    file "/etc/bind/db.root";
};

zone "com" {
    type master;
    file "/etc/bind/db.com";
};
```

- file di zona:

```
$TTL    60000
@               IN      SOA     rcom.com.    root.rcom.com. (
                        2023090301 ; serial
                        28800 ; refresh
                        14400 ; retry
                        3600000 ; expire
                        0 ; negative cache ttl
                        )
@               IN      NS      rcom.com.
rcom            IN      A       192.168.0.2

google          IN      NS      rgoogle.google.com.
rgoogle.google  IN      A       192.168.0.20
```

DNSSEC

Estensione del protocollo DNS necessaria per verificare l’autenticità ed integrità dei dati

DNSSEC - Come funziona

DNSSEC utilizza delle chiavi per firmare digitalmente i record DNS.
Vengono utilizzate due coppie di chiavi:

- ZSK - Zone Signing Key
- KSK - Key-Signing key

Cosa fanno le chiavi?

- La parte privata della ZSK viene utilizzata per firmare i RRset della zona, mentre la parte pubblica serve per verificare la firma
- La KSK privata serve a convalidare sia i record ZSK sia i record DNSKEY, in modo da fornire un livello di sicurezza aggiuntivo

Generazione delle chiavi

Viene utilizzato l’hash RSA / SHA256

> dnssec-keygen -a RSASHA256 -b 1024 test.net

> dnssec-keygen -a RSASHA256 -b 2048 -f KSK test.net

```
root@rtest:/etc/bind/keys# dnssec-keygen -a RSASHA256 -b 1024 test.net
Generating key pair.....................................................
++++++++++++++++++++++++++++++ ..............................++++++++++++++++++++++++++
Ktest.net.+008+58206
root@rtest:/etc/bind/keys# dnssec-keygen -a RSASHA256 -b 2048 -f KSK test.net
Generating key pair............++++++++++++++++++++++++++++++++++++++++++++++++++++++
.+....+..+.+........+....+...+..+...+............+..++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++ .+.+..+....+........+.....+.+.....+........+......+...
+++++++++++++*.+.....+........+.............+.........+.....+...+...+...+......
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Ktest.net.+008+53860
root@rtest:/etc/bind/keys#
```

Salvataggio delle chiavi pubbliche

Una copia delle chiavi pubbliche dovrà essere riportata nel file di zona

```
> cat /etc/bind/keys/Ktest.net.+008*.key >> db.net.test
```

Firma della zona

```
root@rtest:/etc/bind# dnssec-signzone -t -g -o test.net db.net.test /etc/bind/keys/Ktest.net.+008+*.private
Verifying the zone using the following algorithms:
- RSASHA256
Zone fully signed:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 0 stand-by, 0 revoked
db.net.test.signed
Signatures generated:                       10
Signatures retained:                         0
Signatures dropped:                          0
Signatures successfully verified:            0
Signatures unsuccessfully verified:          0
Signing time in seconds:                 0.008
Signatures per second:                1250.000
Runtime in seconds:                      0.020
root@rtest:/etc/bind#
```

Otterremo due nuovi file, db.net.test.signed e dsset-test.net.

File di zona prima e dopo la firma

Record del nameserver test senza firma

```
@               IN      NS      rtest.test.net.
rtest           IN      A       192.168.0.30
```

Record del nameserver test firmato

```
rtest.test.net.         60000   IN A    192.168.0.30
                        60000   RRSIG    A 8 3 60000 (
                                         20231120163300 20231021163300 58206 test.net.
                                         Lz/+MQcLSfEhNKi5uZ1lYa8MhhFDbC0CWGf8
                                         /EVAIkZUZwj/uTfLFESAvGxZVVJb1VysObzS
                                         iJZDrbb89CaSTNe4RiPRRfsajuZqizcTZOTu
                                         f54o6cvqasXsZf0NVmpoeQ2ObB+s8nyGu48L
                                         04sWOMTiPj4NC5lhgw9CPmp5XHA= )
                        15      NSEC     tzone.test.net. A RRSIG NSEC
                        15      RRSIG    NSEC 8 3 15 (
                                         20231120163300 20231021163300 58206 test.net.
                                         o5LV6fUYk0Xbx6LlO5HPGNIGKHaFHfdtfEwl
                                         m/x/SlmaWD52lZ09II4G2nZkDeuOdlFDWYla
                                         IePLiFXvZ05YBo4V5ieHBi4KImcaDN6TDHjE
                                         PL2sR8FpF9PHfucMBn0yHKj6vdC7DF1JuAy4
                                         bi8GZJZApaCq+EqPaMS7+2kaWGU= )
```

Aggiornamento del file named.conf

Il nuovo file di zona andrà a sostituire il precedente

```
zone "test.net" {
    type master;
    file "/etc/bind/db.net.test.signed";
};
```

Verifica della corretta configurazione

```
root@rtest:/etc/bind# dig DNSKEY test.net. @192.168.0.30

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> DNSKEY test.net. @192.168.0.30
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6131
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 1772d13b90cc6ca201000000652bea9cb5f59ffdcd5638ad (good)
;; QUESTION SECTION:
;test.net.                      IN      DNSKEY

;; ANSWER SECTION:
test.net.               60000   IN      DNSKEY  257 3 8 AwEAAa4t7rutZMqwzUAEJX8OhZrjTsVNzVbWloAtq2CS6
8w+UqgPKI+p cR5oDZoHlj+IFZiSjivxapJNhMmhpIkSI+gupc5E3YqqUqp/T0awiFau sSskVivWqu+Iqn49ZW5xAReSWyqgvq+h
0CEUJWlZJymOYHy9qVs9cRSH f620sJb01UwzGhI7mlKCVymcLbNkHUgUFYp+IEqKbPhoKq2Iih8TtoKT tVOyuDYQQPx4y5QKY2Y
i+8TNzBnMw5IU3dg7eys+D94CEJYRVj6SA9PD G3FYll1Lp+jFNZpgcl0VgZiU4S+VqUGynfeILmR3b+Mzf28z2y3AbBM5 MfGE63
enURs=
test.net.               60000   IN      DNSKEY  256 3 8 AwEAAZ95tqOOECQhOLQQPbWHLQ18kkPd/XG7w2r73V9oK
LU+glhU9NEU qDGhKo29fYMg2siCZPiwui8VG/luCaSVHA2ITZR65Lc0UffP8WfUeOKj +DdDNrSS8UJYvtRlvSGIGTBPZZHMtsWT
1SkgtwhOF/JZB7eSBPJwJQYC 3j99gFSSysCndQ3yGrwSbV1lEebB8/7amjGB1lNgF8uGsQ3KycU=
```

Verifica del corretto funzionamento

Il comando dnssec-verify permette di verificare la correttezza delle firme digitali

```
root@rtest:/etc/bind# dnssec-verify -o test.net db.net.test.signed /etc/bind/keys/Ktest.net.+008+5*.key
Loading zone 'test.net' from file 'db.net.test.signed'

Verifying the zone using the following algorithms:
- RSASHA256
Zone fully signed:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 0 stand-by, 0 revoked
```

Verifica del corretto funzionamento

Cambiando un indirizzo IP da 192.168.0.225 a 192.168.0.223

```
pc2.test.net.           60000   IN A    192.168.0.223
                        60000   RRSIG   A 8 3 60000 (
                                        20231120163300 20231021163300 58206 test.net.
                                        lZdyZ1nQw0noJCqvBUSNFiEcXM9/R1s9CsYs
                                        6w+iItOMD6OAUsxQob5lyuPcizxZIyxc3nyN
                                        MqAsKtwpoboNzEDzoFDoJ7CLlcHLcaoq8OsS
                                        7SNmgIOlZdpRlYLViEe2gdKpPHaR1zGtmWAO
                                        Rfbkel/FtbekGmDiHrhktNGyGI8= )
```

Verrà riconosciuto l’errore nella firma e il test risulterà fallito

```
root@rtest:/etc/bind# dnssec-verify -o test.net db.signed /etc/bind/keys/Ktest.net.+008+5*.key
Loading zone 'test.net' from file 'db.signed'

Verifying the zone using the following algorithms:
- RSASHA256
No correct RSASHA256 signature for pc2.test.net A
The zone is not fully signed for the following algorithms:
 RSASHA256
.
DNSSEC completeness test failed.
```

Conclusioni

Nel corso di questo lavoro di tesi, ho effettuato un approfondito lavoro di ricerca per comprendere ed implementare il protocollo DNS e il DNSSEC

Grazie all'utilizzo di Katharà ho imparato cosa sono i container e come usarli

Infine ho acquisito una maggiore consapevolezza sull'importanza della sicurezza informatica e sulle sfide che risiedono dietro all'implementazione di protocolli di rete

Grazie per l’attenzione