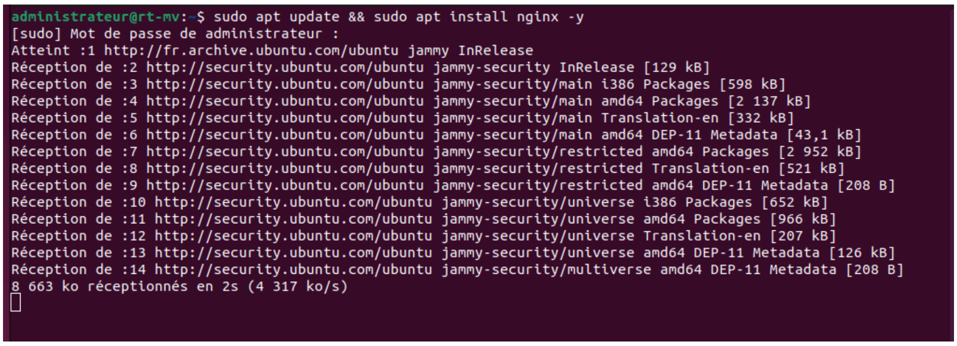
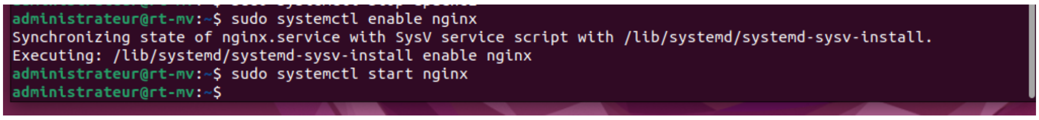
CTP : R4.Cyber.11 HTTP (nginx)

1. **Installation et configuration de base de Nginx** :
    - Installation de Nginx sur un système Linux.

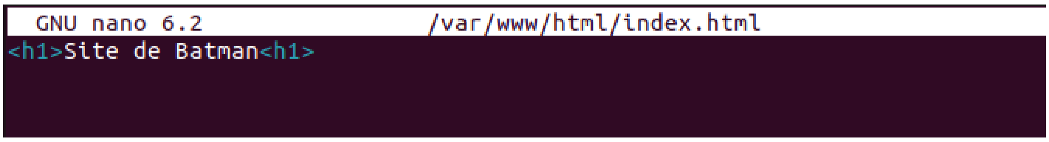


```
administrateur@rt-mv:~$ sudo apt update && sudo apt install nginx -y
[sudo] Mot de passe de administrateur :
Atteint :1 http://fr.archive.ubuntu.com/ubuntu jammy InRelease
Réception de :2 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Réception de :3 http://security.ubuntu.com/ubuntu jammy-security/main i386 Packages [598 kB]
Réception de :4 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [2 137 kB]
Réception de :5 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [332 kB]
Réception de :6 http://security.ubuntu.com/ubuntu jammy-security/main amd64 DEP-11 Metadata [43,1 kB]
Réception de :7 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [2 952 kB]
Réception de :8 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [521 kB]
Réception de :9 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 DEP-11 Metadata [208 B]
Réception de :10 http://security.ubuntu.com/ubuntu jammy-security/universe i386 Packages [652 kB]
Réception de :11 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [966 kB]
Réception de :12 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [207 kB]
Réception de :13 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 DEP-11 Metadata [126 kB]
Réception de :14 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 DEP-11 Metadata [208 B]
8 663 ko réceptionnés en 2s (4 317 ko/s)
```

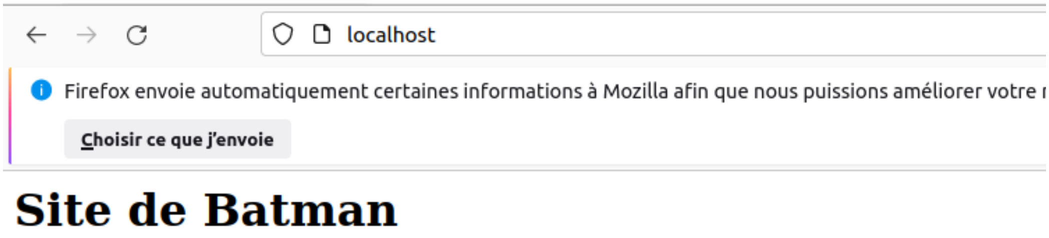
    - Configuration d'un site web simple avec Nginx, accessible via HTTP.



```
administrateur@rt-mv:~$ sudo systemctl enable nginx
Synchronizing state of nginx.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable nginx
administrateur@rt-mv:~$ sudo systemctl start nginx
administrateur@rt-mv:~$
```



```
  GNU nano 6.2                    /var/www/html/index.html
<h1>Site de Batman<h1>
```



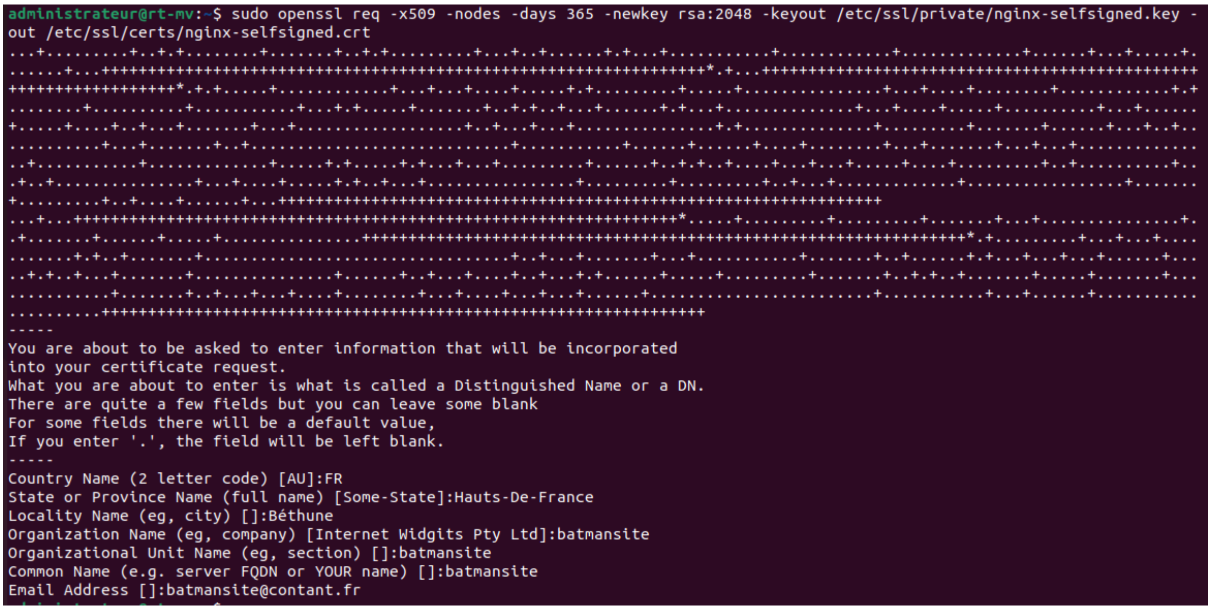
Firefox envoie automatiquement certaines informations à Mozilla afin que nous puissions améliorer votre r

Site de Batman

2. Sécurisation de Nginx avec SSL/TLS :

- Génération d'un certificat SSL auto-signé ou obtention d'un certificat

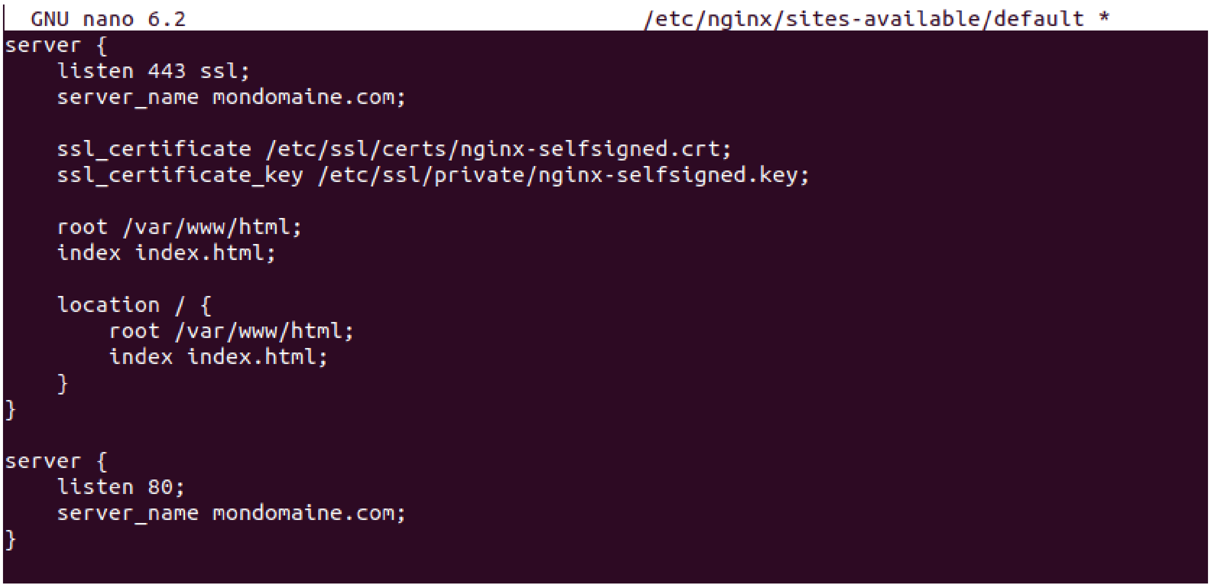
d'une autorité de certification (comme Let's Encrypt).



```
administrateur@rt-mv:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/nginx-selfsigned.key -
out /etc/ssl/certs/nginx-selfsigned.crt
...+.........+..+.+........+.......+..+.+.........+...+..+......+.+...+...........+...........+............+......+...+.....+.
......+...+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+...+++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++*.+.+.....+...........+...+...+....+.....+.+.........+......+...............+...+....+........+...........+.+
........+..........+...........+...+.+.....+.......+..+.+..+...+......+.+...+...............+...+....+.....+..........+...+.....
+.....+....+..+...+.......+...+..................+..+...+...+...............+.+.............+.........+.......+......+...+..+..
..........+...+.......+..+............................+...........+......+......+...+........+...+.......+...+...+............
..+...........+.............+.....+.+.....+.+...+...+..........+......+..+.+..+....+...+...+......+....+.........+..+..........+..
.+..+...............+...+....+.....+.+..+...+................+.........+.........+..+...+..............+................+.......
+.........+..+....+......+...++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
...+...+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.....+.........+.........+.......+...+...............+.
.+.......+.......+.....+...............+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+.........+...+...+....
.......+.+..+.......+...............................+..+...+........+...+............+.......+..+.......+.+...+...+...+......+...
..+.+..+...+.......+..............+......+..+...+....+..+...+.+.......+.....+.........+.......+..+.+..+.......+.......+.......+...
..........+.......+..+...+...+...+........+...+....+...+...+......+......................+...........+...+......+..........
..........++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Hauts-De-France
Locality Name (eg, city) []:Béthune
Organization Name (eg, company) [Internet Widgits Pty Ltd]:batmansite
Organizational Unit Name (eg, section) []:batmansite
Common Name (e.g. server FQDN or YOUR name) []:batmansite
Email Address []:batmansite@contant.fr
```

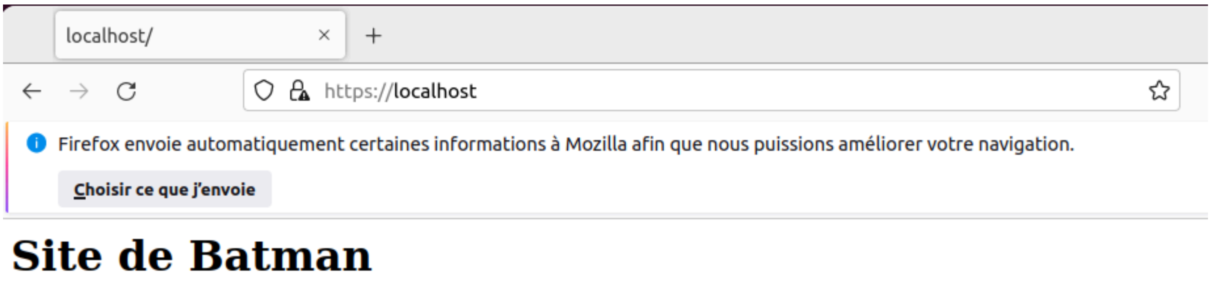
- Configuration de Nginx pour utiliser le certificat SSL et activer HTTPS.

sudo nano /etc/nginx/sites-available/default



```
  GNU nano 6.2                              /etc/nginx/sites-available/default *
server {
    listen 443 ssl;
    server_name mondomaine.com;

    ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;
    ssl_certificate_key /etc/ssl/private/nginx-selfsigned.key;

    root /var/www/html;
    index index.html;

    location / {
        root /var/www/html;
        index index.html;
    }
}

server {
    listen 80;
    server_name mondomaine.com;
}
```

- Test de la configuration SSL/TLS.

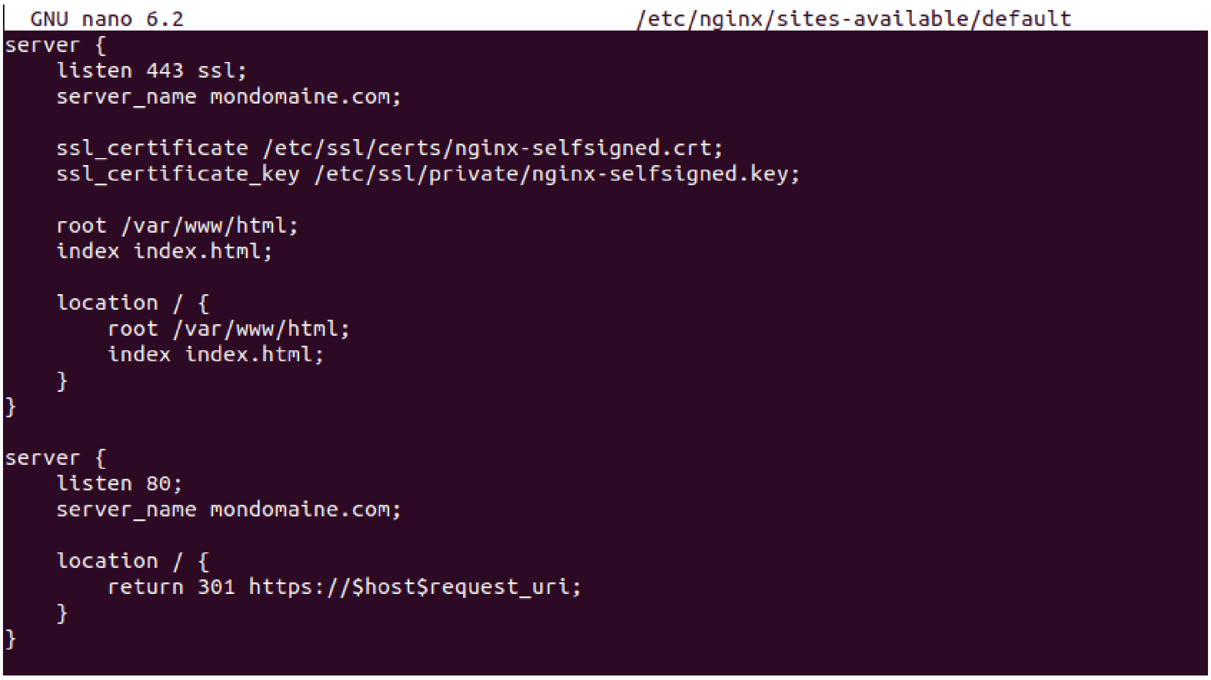


Firefox envoie automatiquement certaines informations à Mozilla afin que nous puissions améliorer votre navigation.

Site de Batman

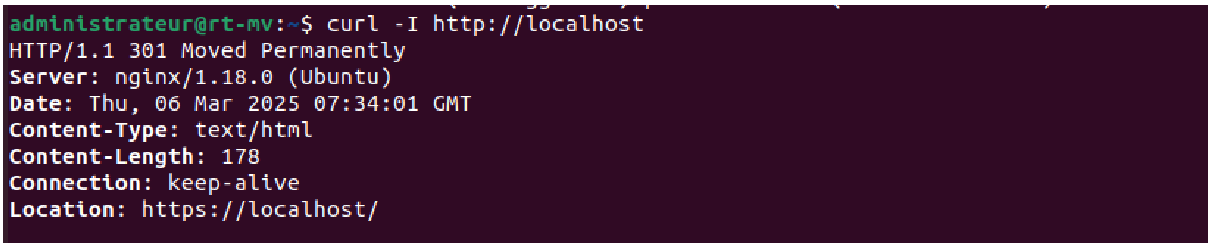
3. Redirection de HTTP vers HTTPS :

- Configuration de Nginx pour rediriger automatiquement toutes les requêtes HTTP vers HTTPS.



```
 GNU nano 6.2                                  /etc/nginx/sites-available/default
server {
    listen 443 ssl;
    server_name mondomaine.com;

    ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;
    ssl_certificate_key /etc/ssl/private/nginx-selfsigned.key;

    root /var/www/html;
    index index.html;

    location / {
        root /var/www/html;
        index index.html;
    }
}

server {
    listen 80;
    server_name mondomaine.com;

    location / {
        return 301 https://$host$request_uri;
    }
}
```

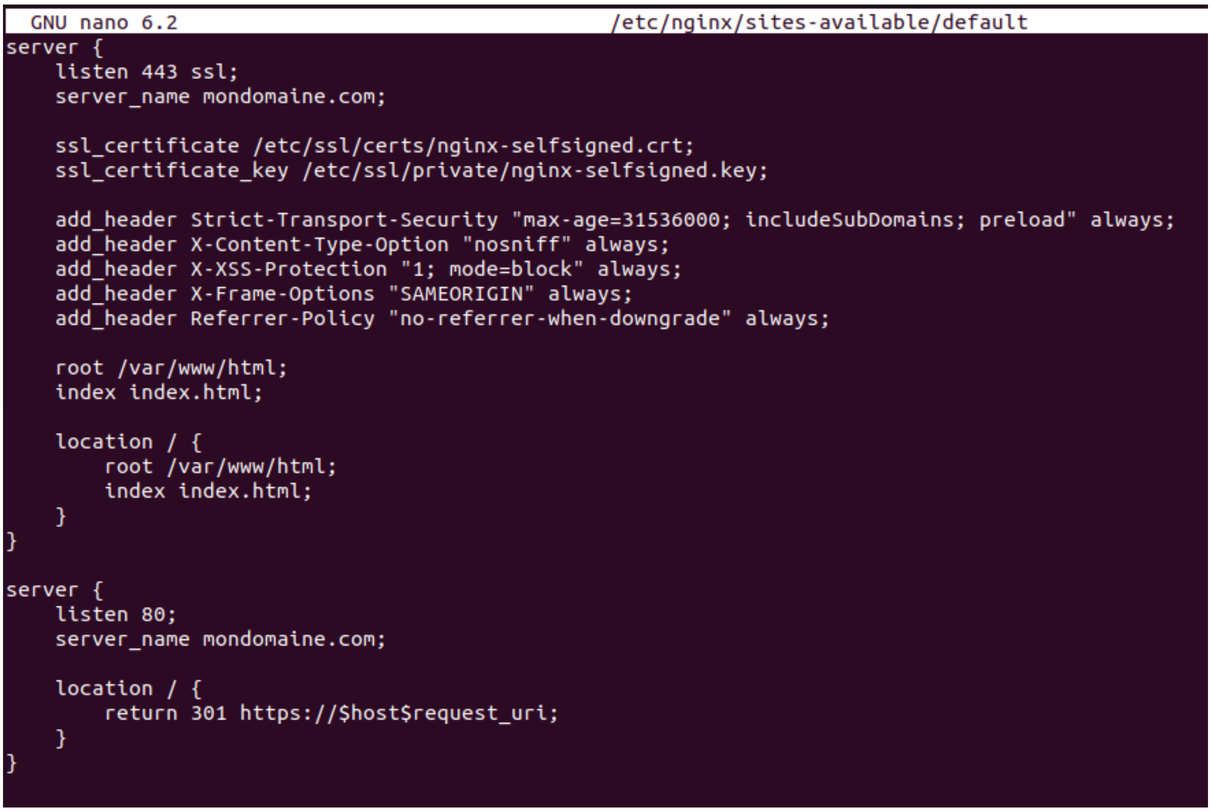
- Test et validation de la redirection



```
administrateur@rt-mv:~$ curl -I http://localhost
HTTP/1.1 301 Moved Permanently
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 06 Mar 2025 07:34:01 GMT
Content-Type: text/html
Content-Length: 178
Connection: keep-alive
Location: https://localhost/
```

4. Configuration des en-têtes de sécurité :

- Ajout et configuration des en-têtes de sécurité recommandés (HSTS,X-Content-Type-Options, X-XSS-Protection, X-Frame-Options, Referrer-Policy) dans la configuration de Nginx.



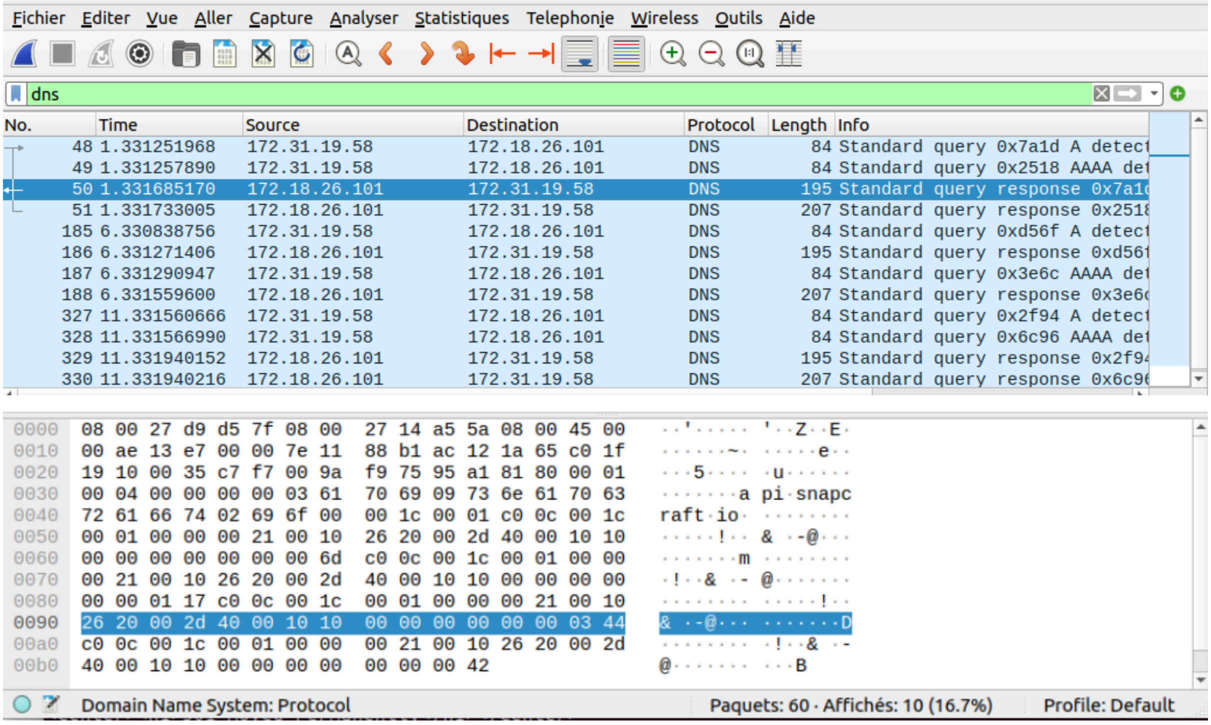
```
  GNU nano 6.2                                   /etc/nginx/sites-available/default
server {
    listen 443 ssl;
    server_name mondomaine.com;

    ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;
    ssl_certificate_key /etc/ssl/private/nginx-selfsigned.key;

    add_header Strict-Transport-Security "max-age=31536000; includeSubDomains; preload" always;
    add_header X-Content-Type-Option "nosniff" always;
    add_header X-XSS-Protection "1; mode=block" always;
    add_header X-Frame-Options "SAMEORIGIN" always;
    add_header Referrer-Policy "no-referrer-when-downgrade" always;

    root /var/www/html;
    index index.html;

    location / {
        root /var/www/html;
        index index.html;
    }
}

server {
    listen 80;
    server_name mondomaine.com;

    location / {
        return 301 https://$host$request_uri;
    }
}
```

- Explication de l'importance de chaque en-tête pour la sécurité du site web.

HSTS : Empêche les attaques de type downgrade et force l'utilisation de HTTPS.
X-Content-Type-Options : Empêche les attaques de type MIME sniffing.
X-XSS-Protection : Protège contre les attaques Cross-Site Scripting.
X-Frame-Options : Protège contre le clickjacking.
Referrer-Policy : Protège la confidentialité des utilisateurs en contrôlant l'envoi des informations de référence.

5. Analyse des communications sécurisées :

- Utilisation de Wireshark pour analyser les communications entre le client et le serveur, mettant en évidence les différences entre les communications HTTP et HTTPS.



dns

No.	Time	Source	Destination	Protocol	Length	Info
48	1.331251968	172.31.19.58	172.18.26.101	DNS	84	Standard query 0x7a1d A detect
49	1.331257890	172.31.19.58	172.18.26.101	DNS	84	Standard query 0x2518 AAAA det
50	1.331685170	172.18.26.101	172.31.19.58	DNS	195	Standard query response 0x7a1d
51	1.331733005	172.18.26.101	172.31.19.58	DNS	207	Standard query response 0x2518
185	6.330838756	172.31.19.58	172.18.26.101	DNS	84	Standard query 0xd56f A detect
186	6.331271406	172.18.26.101	172.31.19.58	DNS	195	Standard query response 0xd56f
187	6.331290947	172.31.19.58	172.18.26.101	DNS	84	Standard query 0x3e6c AAAA det
188	6.331559600	172.18.26.101	172.31.19.58	DNS	207	Standard query response 0x3e6c
327	11.331560666	172.31.19.58	172.18.26.101	DNS	84	Standard query 0x2f94 A detect
328	11.331566990	172.31.19.58	172.18.26.101	DNS	84	Standard query 0x6c96 AAAA det
329	11.331940152	172.18.26.101	172.31.19.58	DNS	195	Standard query response 0x2f94
330	11.331940216	172.18.26.101	172.31.19.58	DNS	207	Standard query response 0x6c96

```
0000  08 00 27 d9 d5 7f 08 00  27 14 a5 5a 08 00 45 00   ··'·····  '··Z··E·
0010  00 ae 13 e7 00 00 7e 11  88 b1 ac 12 1a 65 c0 1f   ······~·  ·····e··
0020  19 10 00 35 c7 f7 00 9a  f9 75 95 a1 81 80 00 01   ···5····  ·u······
0030  00 04 00 00 00 00 03 61  70 69 09 73 6e 61 70 63   ·······a  pi·snapc
0040  72 61 66 74 02 69 6f 00  00 1c 00 01 c0 0c 00 1c   raft·io·  ········
0050  00 01 00 00 00 21 00 10  26 20 00 2d 40 00 10 10   ·····!··  & ·-@···
0060  00 00 00 00 00 00 00 6d  c0 0c 00 1c 00 01 00 00   ·······m  ········
0070  00 21 00 10 26 20 00 2d  40 00 10 10 00 00 00 00   ·!··& ·-  @·······
0080  00 00 01 17 c0 0c 00 1c  00 01 00 00 00 21 00 10   ········  ·····!··
0090  26 20 00 2d 40 00 10 10  00 00 00 00 00 00 03 44   & ·-@···  ·······D
00a0  c0 0c 00 1c 00 01 00 00  00 21 00 10 26 20 00 2d   ········  ·!··& ·-
00b0  40 00 10 10 00 00 00 00  00 00 00 42               @·······  ···B
```

Domain Name System: Protocol — Paquets: 60 · Affichés: 10 (16.7%) — Profile: Default

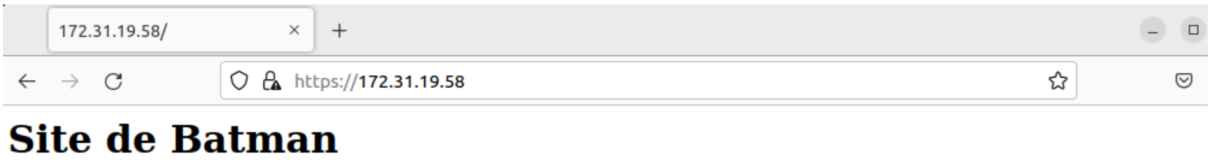
Communication HTTP (non sécurisé) :

- message non crypté, le texte est lisible.

Communication HTTPS (sécurisé) :

- handshake SSL/TLS avec des paquets contenant des informations cryptées

- Testez l'accès sécurisé à votre site en visitant https://<adresse IP de votre serveur> ou https://votre_domaine.com. Vous devriez voir la page d'accueil de votre site servie via HTTPS avec un cadenas dans la barre d'adresse du navigateur.

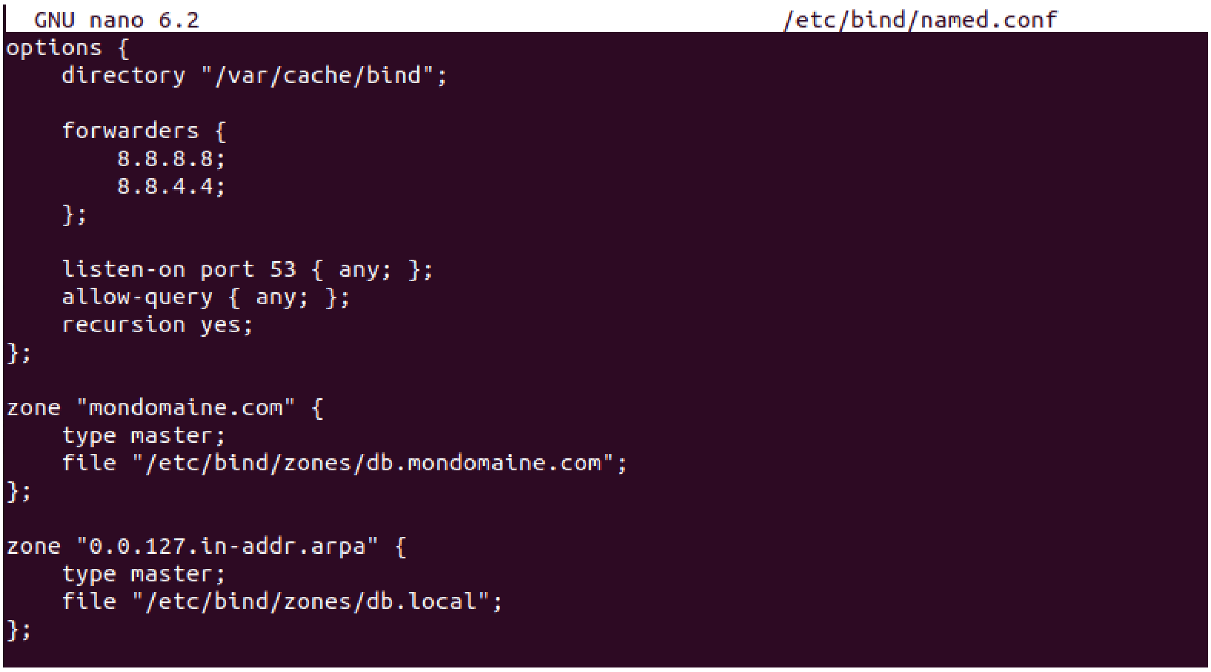


Site de Batman

6. DNS (Bonus) :

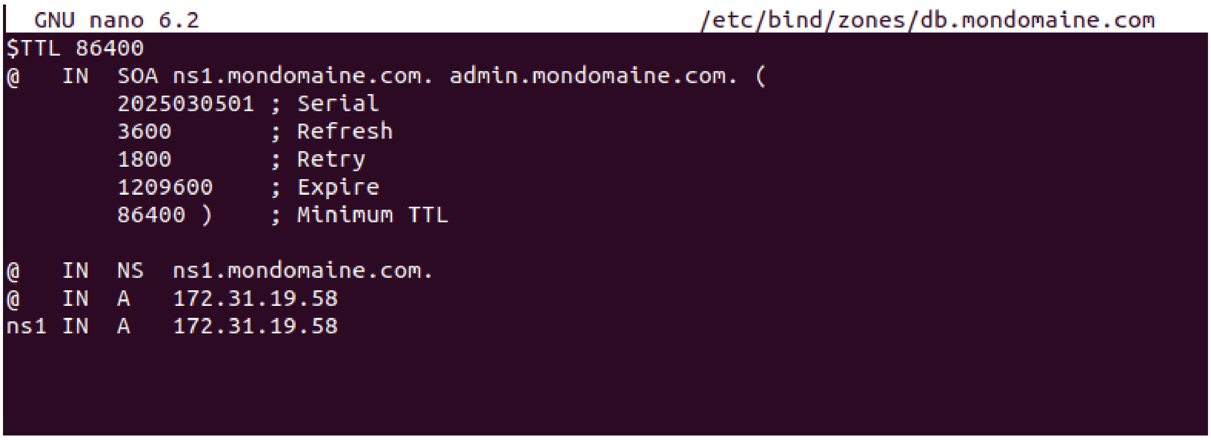
- Configurer votre serveur et client pour qu’ils utilisent des noms de domaine au lieu d’adresses IP.

- sudo /etc/bind/named.conf



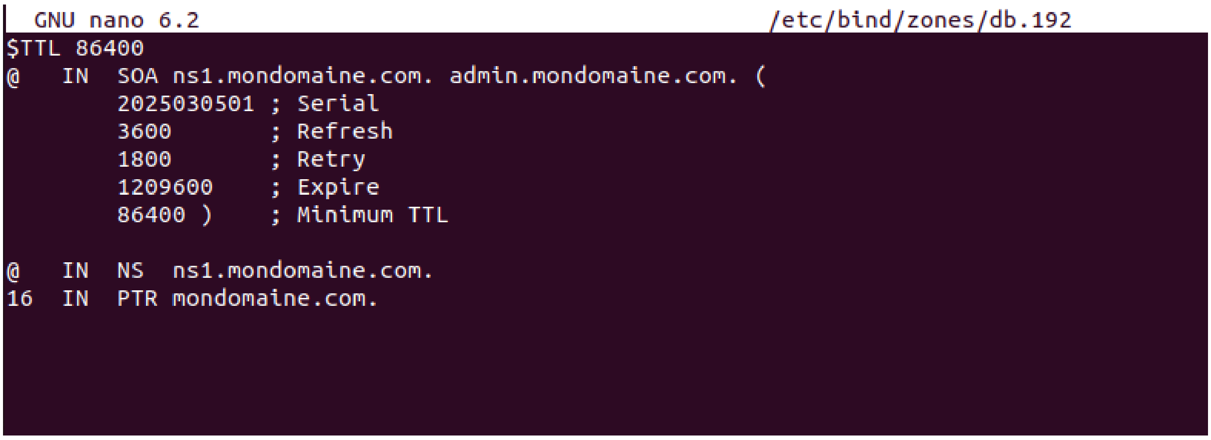
```
  GNU nano 6.2                                          /etc/bind/named.conf
options {
    directory "/var/cache/bind";

    forwarders {
        8.8.8.8;
        8.8.4.4;
    };

    listen-on port 53 { any; };
    allow-query { any; };
    recursion yes;
};

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

zone "0.0.127.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/db.local";
};
```

- sudo nano /etc/bind/zones/db.mondomaine.com



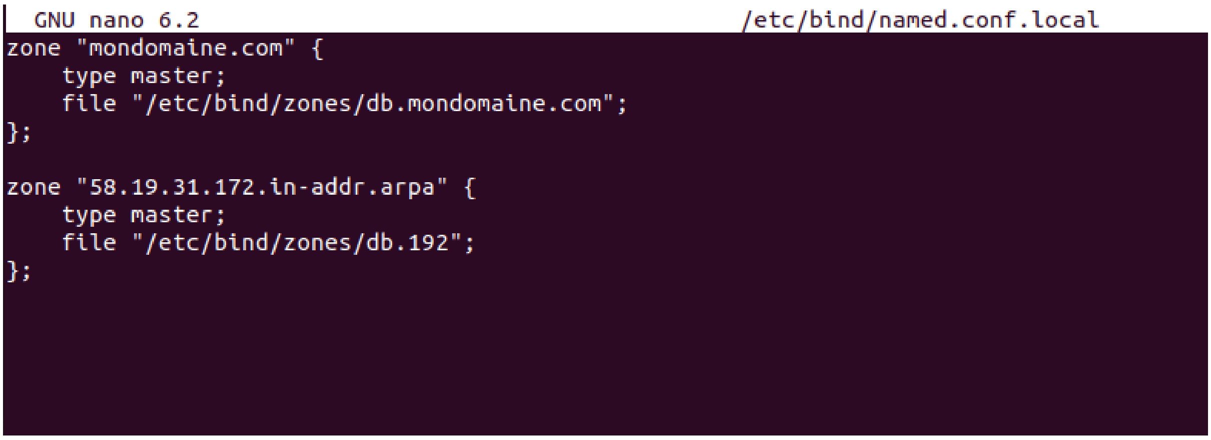
```
  GNU nano 6.2                                    /etc/bind/zones/db.mondomaine.com
$TTL 86400
@   IN  SOA ns1.mondomaine.com. admin.mondomaine.com. (
        2025030501 ; Serial
        3600       ; Refresh
        1800       ; Retry
        1209600    ; Expire
        86400 )    ; Minimum TTL

@   IN  NS  ns1.mondomaine.com.
@   IN  A   172.31.19.58
ns1 IN  A   172.31.19.58
```

- sudo nano /etc/bind/zones/db.192



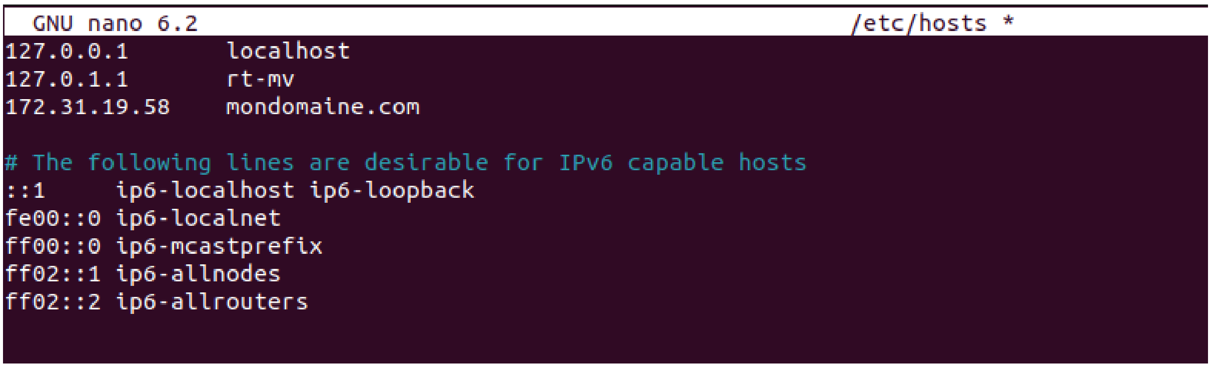
```
$TTL 86400
@   IN  SOA ns1.mondomaine.com. admin.mondomaine.com. (
        2025030501 ; Serial
        3600       ; Refresh
        1800       ; Retry
        1209600    ; Expire
        86400 )    ; Minimum TTL

@   IN  NS  ns1.mondomaine.com.
16  IN  PTR mondomaine.com.
```

- sudo nano /etc/bind/named.conf.local



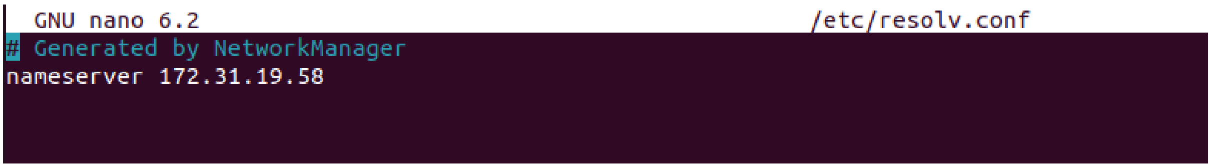
```
zone "mondomaine.com" {
    type master;
    file "/etc/bind/zones/db.mondomaine.com";
};

zone "58.19.31.172.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/db.192";
};
```

- sudo nano /etc/hosts

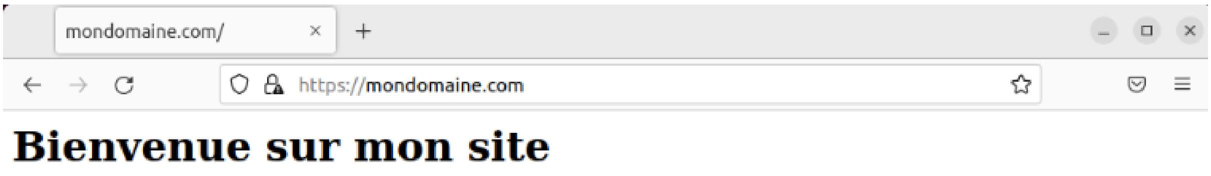


```
127.0.0.1       localhost
127.0.1.1       rt-mv
172.31.19.58    mondomaine.com

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

- sudo nano /etc/resolv.conf



```
# Generated by NetworkManager
nameserver 172.31.19.58
```



Bienvenue sur mon site