TP DNS

Partie 1 : études de trame

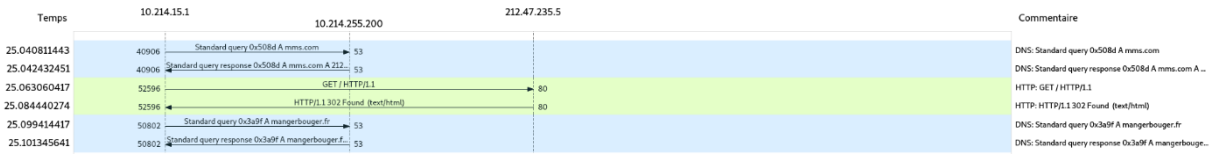
En utilisant Wire Shark lors d'une requête sur un navigateur, on peut voir plusieurs trames :

Les requêtes DNS :

On utilise une 'standard query' vers l'ip du DNS (10.214.255.200) pour lui demander une résolution en lui donnant le nom symbolique à résoudre.

Le DNS envoi une 'Standard query response' qui comporte l'ip à utiliser pour accéder au site demandé avec le nom symbolique.

L'ip renvoyé est donc utilisé dans la requête http pour aller sur un serveur web



Partie 2 : On prend l'adresse eot-consulting.world à la place de example.com

1 :

```
test@232-22:~$ dig -t a example.com

; <<>> DiG 9.16.22-Debian <<>> -t a example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46494
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 6f48f9b7475fe1b4b9fcbbc1623d8f6a1d0ec60715cc1b4d (good)
;; QUESTION SECTION:
;example.com.                   IN      A

;; ANSWER SECTION:
example.com.            85024   IN      A       93.184.216.34

;; AUTHORITY SECTION:
example.com.            171099  IN      NS      a.iana-servers.net.
example.com.            171099  IN      NS      b.iana-servers.net.

;; ADDITIONAL SECTION:
a.iana-servers.net.     221     IN      A       199.43.135.53
b.iana-servers.net.     221     IN      A       199.43.133.53
a.iana-servers.net.     100508  IN      AAAA    2001:500:8f::53
b.iana-servers.net.     100508  IN      AAAA    2001:500:8d::53

;; Query time: 0 msec
;; SERVER: 10.214.255.200#53(10.214.255.200)
;; WHEN: Fri Mar 25 10:46:18 CET 2022
;; MSG SIZE  rcvd: 220
```

2 :

```
test@232-22:~$ dig -t AAAA web.eot-consulting.world

; <<>> DiG 9.16.22-Debian <<>> -t AAAA web.eot-consulting.world
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59158
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 99d8bcc34eba98951abd7741623d9d132237985c1efdc00d (good)
;; QUESTION SECTION:
;web.eot-consulting.world.      IN      AAAA

;; ANSWER SECTION:
web.eot-consulting.world. 9794  IN      CNAME   www.eot-consulting.world.
www.eot-consulting.world. 9337  IN      AAAA    bad::b10
```

3 :

```
test@232-22:~$ dig -t TXT eot-consulting.world

; <<>> DiG 9.16.22-Debian <<>> -t TXT eot-consulting.world
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47695
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 6

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 95af3755227756542917150962 3d9e3d73525e09f25048ef (good)
;; QUESTION SECTION:
;eot-consulting.world.          IN      TXT

;; ANSWER SECTION:
eot-consulting.world.   9015    IN      TXT     "v=spf1 include:_mailcust.gandi.net ?all"
eot-consulting.world.   9015    IN      TXT     "L'adresse IPv6 sera la cle qui ouvrira la boite"
```

4 :

```
test@232-22:~$ dig -t TXT eot-consulting.world

; <<>> DiG 9.16.22-Debian <<>> -t TXT eot-consulting.world
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47695
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 6

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 95af3755227756542917150962 3d9e3d73525e09f25048ef (good)
;; QUESTION SECTION:
;eot-consulting.world.          IN      TXT

;; ANSWER SECTION:
eot-consulting.world.   9015    IN      TXT     "v=spf1 include:_mailcust.gandi.net ?all"
eot-consulting.world.   9015    IN      TXT     "L'adresse IPv6 sera la cle qui ouvrira la boite"
```

5 :

```
test@232-22:~$ dig -t MX eot-consulting.world

; <<>> DiG 9.16.22-Debian <<>> -t MX eot-consulting.world
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37674
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 6

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 03f0086251fb5f85cbcf7b28623d9e8a70a39cce0ebe0a51 (good)
;; QUESTION SECTION:
;eot-consulting.world.          IN      MX

;; ANSWER SECTION:
eot-consulting.world.   9341    IN      MX      50 fb.mail.gandi.net.
eot-consulting.world.   9341    IN      MX      10 spool.mail.gandi.net.
```

6 :

```
test@232-22:~$ dig -t SO eot-consulting.world
;; Warning, ignoring invalid type SO

; <<>> DiG 9.16.22-Debian <<>> -t SO eot-consulting.world
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59961
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 6

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 99c4a5a1eb959737f1fd3cd0623d9f1199fb89af68536eb1 (good)
;; QUESTION SECTION:
;eot-consulting.world.          IN      A

;; ANSWER SECTION:
eot-consulting.world.   9754    IN      A       212.47.235.5
```

7 :

```
test@232-22:~$ dig -t SOA eot-consulting.world

; <<>> DiG 9.16.22-Debian <<>> -t SOA eot-consulting.world
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31424
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 6

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: b68e23eaca34803f5655d6c1623d9f3037fc24820b885bba (good)
;; QUESTION SECTION:
;eot-consulting.world.          IN      SOA

;; ANSWER SECTION:
eot-consulting.world.   85154   IN      SOA     ns1.gandi.net. hostmaster.gandi.net. 1648204127 10800 3600 604800 10800
```

8 :

```
test@232-22:~$ dig -t TXT info.eot-consulting.world @ns-50-a.gandi.net

; <<>> DiG 9.16.22-Debian <<>> -t TXT info.eot-consulting.world @ns-50-a.gandi.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16136
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;info.eot-consulting.world.     IN      TXT

;; ANSWER SECTION:
info.eot-consulting.world. 24042 IN     TXT     "Pour la question ipv6 utiliser l'hote cryptexZ avec Z le TTL maximum de cet enregistrement TXT"

;; Query time: 40 msec
;; SERVER: 173.246.100.51#53(173.246.100.51)
;; WHEN: Fri Mar 25 12:10:07 CET 2022
;; MSG SIZE  rcvd: 161
```

9 :

```
test@232-22:~$ dig -t AAAA cryptex24042.eot-consulting.world

; <<>> DiG 9.16.22-Debian <<>> -t AAAA cryptex24042.eot-consulting.world
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57861
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d1f149c764622ac47058d5aa623da37ffc5dcdeb8d840240 (good)
;; QUESTION SECTION:
;cryptex24042.eot-consulting.world. IN  AAAA

;; ANSWER SECTION:
cryptex24042.eot-consulting.world. 9578 IN AAAA fab::d0c
```

10 :

```
mjennings@Fake-Web-2022:/home$ su admin
Password:
admin@SugarHost:/home$ ls
admin  debian  mjennings
admin@SugarHost:/home$ cd admin/
admin@SugarHost:~$ ls
runMeToStopTheConspiracy
admin@SugarHost:~$ ./runMeToStopTheConspiracy


-----------
Bien joué !
-----------


Tu as réussi à faire échouer le complot...

Les systèmes vont maintenant se réinitialiser.



--------------------------------------
Pour valider cette dernière partie merci de saisir votre nom et votre prénom.
Vous pourrez ensuite vous délogguer.


Prénom et nom : Arnaud Pruvost
```

On peut conclure que a cause du DNS on a réussi à déjouer le complot car lorsque l'on aller sur les sites de mms ou mars nous étions redirigé vers le site de manger bouger .fr