Attaques par réflexion utilisant le DNS

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

JRES - 11 décembre 2013

Les attaques par déni de service

Les attaques par déni de service

- Une plaie classique de l'Internet

Les attaques par déni de service

- Une plaie classique de l'Internet
- Très anciennes, y compris la variante utilisant le DNS

Les attaques par déni de service

- Une plaie classique de l'Internet
- Très anciennes, y compris la variante utilisant le DNS
- Mais cette variante a brusquement refait surface en 2011

Le principe

Le principe

1. Générer un paquet IP dont l'adresse source est usurpée

Le principe

1. Générer un paquet IP dont l'adresse source est usurpée
2. L'envoyer à un **réflecteur**

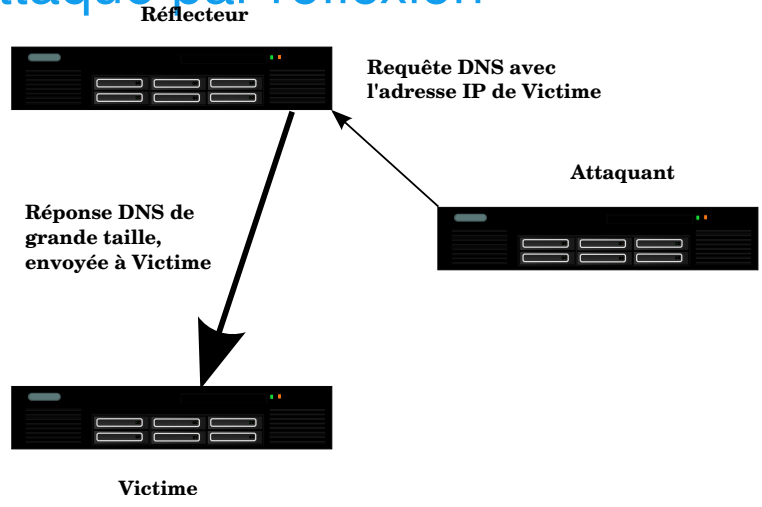
Le principe

1. Générer un paquet IP dont l'adresse source est usurpée
2. L'envoyer à un **réflecteur**
3. Le réflecteur répond à la **victime**

Le principe

1. Générer un paquet IP dont l'adresse source est usurpée
2. L'envoyer à un **réflecteur**
3. Le réflecteur répond à la **victime**
4. Avec le DNS, la réponse est plus grosse que la question : **amplification**

Attaque par réflexion



Bien choisir son réflecteur

1. Serveurs faisant autorité : rapides, bien connectés mais relativement peu nombreux et souvent administrés.

Bien choisir son réflecteur

1. Serveurs faisant autorité : rapides, bien connectés mais relativement peu nombreux et souvent administrés.
2. Résolveur ouvert : meilleure amplification, machines souvent lentes et mal connectées mais très nombreuses et rarement administrées.

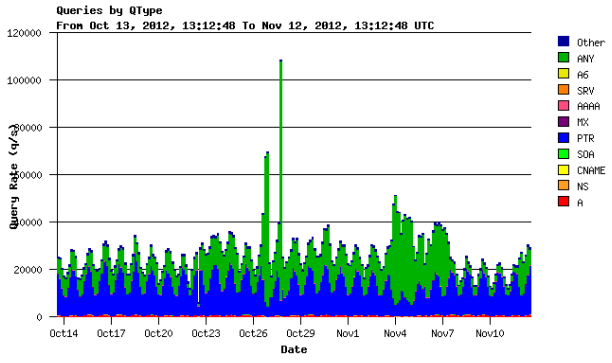
Bien choisir son réflecteur

1. Serveurs faisant autorité : rapides, bien connectés mais relativement peu nombreux et souvent administrés.
2. Résolveur ouvert : meilleure amplification, machines souvent lentes et mal connectées mais très nombreuses et rarement administrées.

En pratique, la plupart des attaques utilisent les résolveurs ouverts.

Attaque via le serveur faisant autorité

Attaque réelle vue sur un serveur de l'AFNIC utilisé comme réflecteur :



afnic

Tester les contre-mesures

Tester les contre-mesures

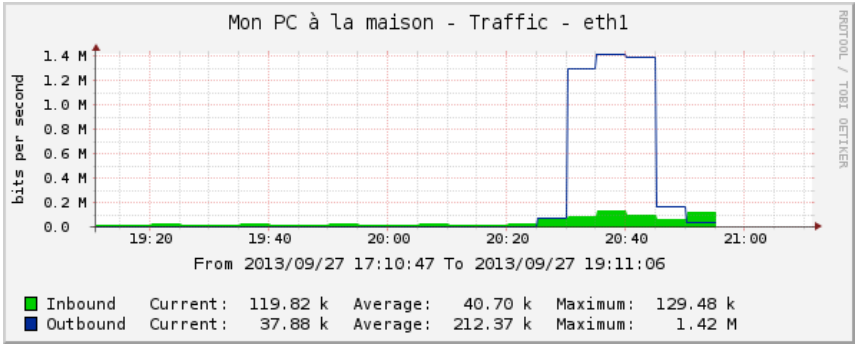
- On utilise le logiciel d'attaque SOP

Tester les contre-mesures

- On utilise le logiciel d'attaque SOP
- `sop --qnames example --source 192.168.2.4 192.0.2.1`

Tester les contre-mesures

- On utilise le logiciel d'attaque SOP
- `sop --qnames example --source 192.168.2.4 192.0.2.1`



Solutions possibles

Solutions possibles

- Empêcher l'usurpation d'adresse (norme « BCP 38 »). Les facteurs économiques limitent cette approche.

Solutions possibles

- Empêcher l'usurpation d'adresse (norme « BCP 38 »). Les facteurs économiques limitent cette approche.
- Fermer les résolveurs ouverts. En 2013, ils auraient dû tous disparaître depuis longtemps.

Solutions possibles

- Empêcher l'usurpation d'adresse (norme « BCP 38 »). Les facteurs économiques limitent cette approche.
- Fermer les résolveurs ouverts. En 2013, ils auraient dû tous disparaître depuis longtemps.
- Changements de protocoles : *cookies*, passer à TCP…

Limiter le trafic

Après tout, un vrai client DNS n'envoie jamais autant de requêtes à un serveur faisant autorité. . . Netfilter@Linux :

Limiter le trafic

Après tout, un vrai client DNS n'envoie jamais autant de requêtes à un serveur faisant autorité. . . Netfilter@Linux :

- Classifier : `iptables --u32 0>>22&0x3C@20&0xFFDFDFDF=0x07455841...`

Limiter le trafic

Après tout, un vrai client DNS n'envoie jamais autant de requêtes à un serveur faisant autorité. . . Netfilter@Linux :

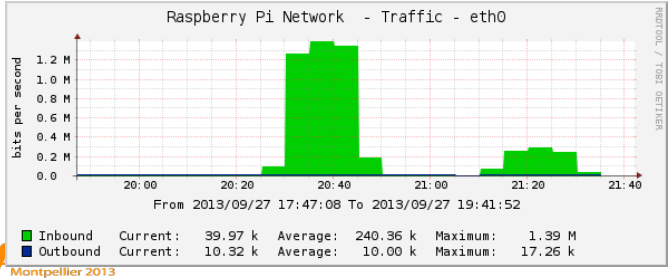
- Classifier : `iptables --u32 0>>22&0x3C@20&0xFFDFDFDF=0x07455841...`
- Limiter : `iptables --hashlimit-above 20/second --hashlimit-mode srcip`

Limiter le trafic

Après tout, un vrai client DNS n'envoie jamais autant de requêtes à un serveur faisant autorité. . . Netfilter@Linux :

- Classifier : `iptables --u32 0>>22&0x3C@20&0xFFDFDFDF=0x07455841...`
- Limiter : `iptables --hashlimit-above 20/second --hashlimit-mode srcip`

Avant et après la limitation de trafic :



RRL

```
# NSD
server :
    # 20 identical queries per second , maximum
   rrl-ratelimit : 20
```


afnic

RRL

- RRL = *Response Rate Limiting*. Mis en œuvre dans BIND, NSD, Knot.

```
# NSD
server :
   # 20 identical queries per second , maximum
  rrl-ratelimit : 20
```

RRL

- RRL = *Response Rate Limiting*. Mis en œuvre dans BIND, NSD, Knot.
- Principe : ne pas renvoyer la même réponse plus de N fois par seconde.

```
# NSD
server :
   # 20 identical queries per second , maximum
  rrl-ratelimit : 20
```

RRL

- RRL = *Response Rate Limiting*. Mis en œuvre dans BIND, NSD, Knot.
- Principe : ne pas renvoyer la même réponse plus de N fois par seconde.
- Deux gros avantages par rapport à la solution Netfilter :

```
# NSD
server :
   # 20 identical queries per second , maximum
  rrl-ratelimit : 20
```

RRL

- RRL = *Response Rate Limiting*. Mis en œuvre dans BIND, NSD, Knot.
- Principe : ne pas renvoyer la même réponse plus de N fois par seconde.
- Deux gros avantages par rapport à la solution Netfilter :
  1. Possibilité de renvoyer une réponse tronquée, disant aux vrais clients DNS de réessayer en TCP (SLIP)

```
# NSD
server :
   # 20 identical queries per second , maximum
  rrl-ratelimit : 20
```

RRL

- RRL = *Response Rate Limiting*. Mis en œuvre dans BIND, NSD, Knot.
- Principe : ne pas renvoyer la même réponse plus de N fois par seconde.
- Deux gros avantages par rapport à la solution Netfilter :
  1. Possibilité de renvoyer une réponse tronquée, disant aux vrais clients DNS de réessayer en TCP (SLIP)
  2. S'ajuste automatiquement aux attaques (pas de type codé en dur, comme ANY)

```
# NSD
server :
   # 20 identical queries per second , maximum
  rrl-ratelimit : 20
```

Au passage

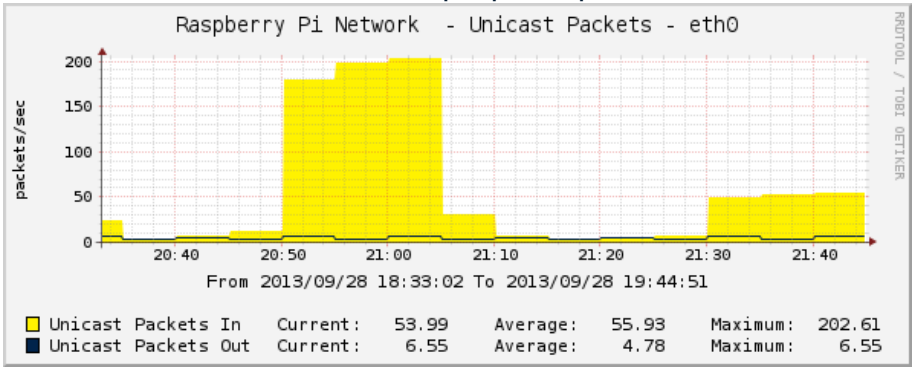
- Toutes les attaques vues à ce jour n'utilisaient qu'IPv4

Au passage

- Toutes les attaques vues à ce jour n'utilisaient qu'IPv4
- Mais Netfilter, RRL et SOP marchent parfaitement en IPv6 (testé en détail)

RRL contre l'attaque

Attention, c'est un nombre de paquets, pas d'octets.



Conclusion

Il **faut** déployer la limitation de trafic sur les serveurs faisant autorité

À plus long terme, il faut continuer à fermer les résolveurs ouverts, et à empêcher l'usurpation d'adresses

Merci !

www.afnic.fr
contact@afnic.fr