Huiswerk Linux: DNS misbruik

DNS kan op verschillende manieren gehackt worden. De belangrijkste twee zijn die van Dan Kamisky uit 2008 en de amplification-attacks van de laatste jaren. De opdracht voor deze week is: zorg dat deze twee hacks niet mogelijk zijn op jouw DNS server.

Over DNS misbruik

Stel je voor je zit in een leuk cafeetje en je wilt betalen met internet-bankieren. Je hele internet-verkeer gaat dan via het wifi-modem van het café. De eigenaar van het café kan daarom 'meeluisteren'. Of erger nog, en veel waarschijnlijker, er zit een hacker in het café die Wifi vanuit haar laptop aanbiedt onder een vergelijkbare naam als die van het café. De telefoons van de klanten gebruiken dan het Wifi van de laptop, waardoor de hacker kan 'meeluisteren' en bijvoorbeeld DNS-records wijzigen, zodat klanten van het café doorgestuurd worden naar de website van de hacker. Dit noemen we een *man in the middle* hack.

Dan Kaminsky 'hack'

Dan Kaminski meldde in 2008 dat je met het *dig* programma de complete database van een domein kon neerladen. Normaal moet je een domeinnaam eerst kennen voordat je hem kan opzoeken. Dan Kaminsky ontdekte dat je met een feature van het DNS protocol in één keer alle records van de database kon neerladen. Deze feature heet *AXFR* (Asynchronous Transfer Full zone Request) en is eigenlijk bedoeld voor database back-ups tussen servers die elkaar vertrouwen.

DNS reflection attack

Vanaf ongeveer 2011 begonnen tot nu toe onbekende partijen DDOS aanvallen uit te voeren op DNS servers. Dit soort aanvallen worden ook wel *amplification attacks* (versterkte aanvallen) genoemd. Het opvragen van enorme hoeveelheden domeinnamen zorgt ervoor dat jouw DNS server domeinnamen die hij zelf niet kent gaat opzoeken bij collega-DNSsen. Het effect is dat de aanval op jouw server versterkt wordt. Als je bovendien *logging* hebt aanstaan in je DNS-server, zal uiteindelijk je server crashen, omdat de hard-disk de snelheid waarmee de DNS-verzoeken binnenkomen niet kan bijhouden.

Normaal zijn alleen webservers het doel van dit soort aanvallen, maar genoemde partijen zijn blijkbaar tegenwoordig ook geïnteresseerd in DNS. Mijn persoonlijke theorie is dat dit te maken heeft met *spam*. Het is in mijn netwerk al meerdere malen voorgekomen dat er eerst een DDOS aanval op mijn DNS server werd uitgevoerd. Deze duurde ongeveer een dag. Een week later kreeg ik ik dubbel zoveel spam binnen als dat ik normaaal gewend was.

Het *sudo* mechanisme

Het configureren van Linux doen we namens de *super-user*. We moeten daarom tijdelijk inloggen als Administrator (root).

Cygwin gebruikers

Sudo voor Cygwin gebruikers: rechts-klik op het icoon van de Cygwin terminal, en kies voor **Als administrator uitvoeren**. Zorg ervoor dat de BIND nameserver is gestart:

```
service bind start
```

Andere Linux gebruikers

Sudo voor gebruikers van andere Linux-versies (*Ubuntu*, *Lubuntu*, *Android*, *Debian, UberStudent*, etc): start een terminal met de toetsencombinatie **<Ctrl><Alt>-T**. We gebruiken het commando *sudo* om in te loggen met het *su* (become Super User) commando. Daardoor blijven we ingelogd:

```
sudo su
```

Uitproberen Kaminsky hack

Hacks zijn uiteraard niet gemakkelijk uit te proberen. Je zou dan je eigen systeem moeten beschadigen. De Kaminsky-hack kunnen we wél veilig uitproberen op onze eigen DNS server. Dit doen we met het *dig* (domain information groper) programma:

dig AXFR testdomein.dmz

Het resultaat ziet er ongeveer alsvolgt uit:

```
; <<>> DiG 9.10.2 <<>> IN AXFR testdomein.dmz
;; global options: +cmd
testdomein.dmz.         43200   IN      SOA     dimension.testdomein.dmz.
     hostmaster.testdomein.dmz. 2010011201 86400 1800 1209600 43200
testdomein.dmz.         43200   IN      NS      ns1.testdomein.dmz.
controller.testdomein.dmz. 43200 IN     A       192.168.137.50
dimension.testdomein.dmz. 43200 IN      A       192.168.137.1
ns1.testdomein.dmz.     43200   IN      A       192.168.137.1
testdomein.dmz.         43200   IN      SOA     dimension.testdomein.dmz.
     hostmaster.testdomein.dmz. 2010011201 86400 1800 1209600 43200
;; Query time: 10 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Sep 15 15:14:34 CEST 2015
;; XFR size: 6 records (messages 1, bytes 213)
```

Zoals je kunt zien, zijn *alle* domeinnamen met IP-adressen zichtbaar. Met name de interne IP-adressen zijn voor hackers interessant. Ze kunnen dan zien hoe je netwerk er van binnen uitziet.

DNS configureren

We gaan ervoor zorgen dat het AXFR commando voor buitenstaanders uitgeschakeld wordt. Dit doen we met een instelling in het BIND configuratie-bestand (*named.conf*).

Cygwin gebruikers

Open het configuratiebestand met de *vi* editor:

vi /etc/named.conf

Andere Linux gebruikers

Bij andere Linux-versies (*Ubuntu*, *Lubuntu*, *Debian, Mint*, etc) staat het bestand in de */etc/bind* directory:

vi /etc/bind/named.conf.local

```
options {
     version "";     // remove this to allow version queries
     directory "/var/named";
     listen-on    { 127.0.0.1; };
     dnssec-enable no;
     listen-on-v6 { none; };
     allow-recursion { clients; };
     dnssec-validation no;
     // Kaminsky
     allow-transfer {
         none;
     };
};

logging {
     // Amplification
     category security { null; };
     category lame-servers { null; };
};
```

Middels de optie **allow-transfer** geven we aan dat niemand (*none*) een zone transfer mag uitvoeren. Ook wijzelf niet. De **logging** opties zorgen ervoor dat er geen foutmeldingen betreffende onbevoegd gebruik (*category security*) of verkeerd ingestelde servers (*lame-servers*) naar het log-bestand

worden geschreven. Hierdoor wordt de harde schijf van onze server zo min mogelijk belast tijdens een DDOS-aanval.

Het hoera-moment

Eerst moeten we ervoor zorgen dat de BIND name daemon de gewijzigde instellingen opnieuw inleest. Dit doen we door BIND te herstarten met het *service* programma:

```
service bind --full-restart
```

Let op: in andere Linux versies (*Ubuntu*, *Lubuntu*, *Debian, Mint*, etc.) heet de service **bind9**.

Nu kunnen we opnieuw kijken of het mogelijk is om de complete zone neer te laden:

```
dig AXFR testdomein.dmz
```

Als het goed is, krijg je nu het volgende antwoord:

```
; <<>> DiG 9.10.2 <<>> AXFR testdomein.dmz
;; global options: +cmd
; Transfer failed.
```

Huiswerk opsturen

Je kunt de opdracht aftekenen door mij een e-mail met de output van het *nslookup* commando te sturen. Dit doe je met een pijpleiding tussen de commando's *dig* en *email*. Zorg dat het onderwerp van de e-mail tussen aanhalingstekens staat:

```
dig AXFR testdomein.dmz | email -s "DNS Misbruik" docent@localhost
```

Als je geen foutmelding ziet is de e-mail succesvol verstuurd.

Administrator uitloggen

We hebben maatregelen genomen om onze DNS te beschermen tegen misbruik, maar we zijn nog steeds ingelogd als Administrator (*root*).

Geef tot slot **<Ctrl>-D** om de Administrator uit te loggen.