**Investigasi bruteforce password pada mail server ZIMBRA ZCS**

1. Baca do’a
2. Masuk ke console server zimbra /opt/zimbra/log
3. Dengan perintah ls perhatikan file audit.log
4. Jalankan perintah **grep invalid password audit.log**

**Contoh hasil dari perintah:**

[root@mail log]# grep invalid password audit.log

grep: password: No such file or directory

audit.log:2015-06-13 01:17:42,596 WARN  [Pop3Server-170] [ip=211.94.189.55;] security - cmd=Auth; account=akun\_saya@binadarma.ac.id; protocol=pop3; error=authentication failed for [akun\_saya], invalid password;

audit.log:2015-06-13 07:18:04,713 WARN  [Pop3Server-7] [ip=211.94.189.55;] security - cmd=Auth; account=akun\_saya@binadarma.ac.id; protocol=pop3; error=authentication failed for [akun\_saya], invalid password;

audit.log:2015-06-13 07:56:19,828 WARN  [btpool0-5://localhost/service/soap/AuthRequest] [name=akun\_saya@binadarma.ac.id;oip=211.94.189.55;ua=zclient/7.2.5\_GA\_2906;] security - cmd=Auth; account=akun\_saya@binadarma.ac.id; protocol=soap; error=authentication failed for [akun\_saya], invalid password;

audit.log:2015-06-13 07:56:36,180 WARN  [btpool0-16://localhost/service/soap/AuthRequest] [name=akun\_saya@binadarma.ac.id;oip=211.94.189.55;ua=zclient/7.2.5\_GA\_2906;] security - cmd=Auth; account=akun\_saya@binadarma.ac.id; protocol=soap; error=authentication failed for [akun\_saya], invalid password;

audit.log:2015-06-13 07:18:04,713 WARN  [Pop3Server-7] [ip=211.94.189.55;] security - cmd=Auth; account=akun\_saya@binadarma.ac.id; protocol=pop3; error=authentication failed for [akun\_saya], invalid password;

audit.log:2015-06-13 07:56:19,828 WARN  [btpool0-5://localhost/service/soap/AuthRequest] [name=akun\_saya@binadarma.ac.id;oip=211.94.189.55;ua=zclient/7.2.5\_GA\_2906;] security - cmd=Auth; account=akun\_saya@binadarma.ac.id; protocol=soap; error=authentication failed for [akun\_saya], invalid password;

audit.log:2015-06-13 07:56:36,180 WARN  [btpool0-16://localhost/service/soap/AuthRequest] [name=akun\_saya@binadarma.ac.id;oip=211.94.189.55;ua=zclient/7.2.5\_GA\_2906;] security - cmd=Auth; account=akun\_saya@binadarma.ac.id; protocol=soap; error=authentication failed for [akun\_saya], invalid password;

======dan seterusnya, baris record log ada sekitar 100 lebih…

1. Perhatikan pada bagian **oip da ip,** disitu terlihat ip penyerang. Mengapa IP tersebut menjadi tersangka ?

Jawab: karena pada komentar “error=authentication failed for [akun\_saya], invalid password;” audit.log menunjukkan berulang kali bahkan sampai ratusan baris record yang mengindikasi kegagalan login akibat bruteforce

1. Jika hal ini dibiarkan, maka akun yang di bruteforce akan terkunci bahkan server akan mengalami down dan membesarnya log, karena tidak ada system yang mengatur blokir IP bruteforce pada zimbra
2. Langkah sederhana untuk menghindari serangan pada bruteforce akun email, dengan melakukan investigasi IP penyerang yaitu mempelajari audit.log
3. Kemudian memblokir IP penyerang dengan iptables:  
   iptables -I INPUT -s 211.94.189.55 -j DROP

iptables -I INPUT -s 211.94.189.55 -p tcp --dport 7071 -j DROP

iptables -I INPUT -s 211.94.189.55 -p tcp --dport 80 -j DROP

1. Seorang sysadmin harus selalu memantau
2. Selesai.

