Account/Password Management (Fail2ban & TFA)

Oleh:

Idris Winarno

Fail2ban dan TFA

- fail2ban adalah aplikasi/program yang digunakan untuk melakukan pembatasan uji coba login ke sebuah layanan (mis. ssh, ftp, dll) dengan menggunakan mekanisme autentikasi brute-force.
- TFA (Two-Factor Authentication) adalah mekanisme keamanan tambahan yang dirancang untuk memastikan bahwa hanya pengguna/anda adalah orang yang benar-benar mengakses akun.

Instalasi dan ujicoba fail2ban

Instalasi:

- # apt-get install fail2ban
- # /etc/init.d/fail2ban restart

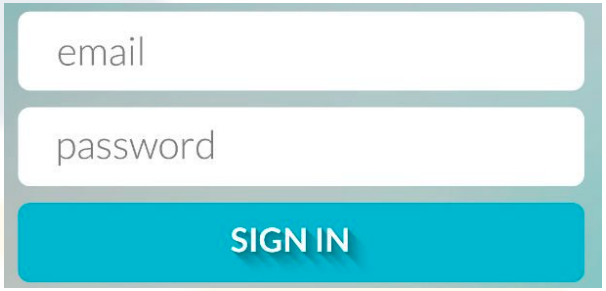
Ujicoba: ssh komputer yang telah terpasang fail2ban dan login beberapa kali

- # ssh <target>

```
root@slimline:/home/idris# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
f2b-sshd   tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 22

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain f2b-sshd (1 references)
target     prot opt source               destination
REJECT     all  --  10.252.13.90         0.0.0.0/0           reject-with icmp-port-unreachable
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
```

TFA

- Install apache2 dan PHP5/7
  - # apt-get install apache2 php
- Buatlah sebuah halaman login




```
<html>
<body>
      <form method="post" action="validate.php">
      Username: <input type="text"
name="username"><br>
      Password: <input type="password"
name="password"></br>
      OTP: <input type="text" name="c"><br>
      <input type="submit" name="submit">
      </form>
</body>
</html>
```

PHPOTP

Jika login username dan password sukses maka selanjutnya user harus terautentikasi menggunakan PHPOTP

Instalasi git

apt-get install git

Gunakan git untuk mendownload PHPOTP

cd /var/www/html

git clone https://github.com/Voronenko/PHPOTP.git

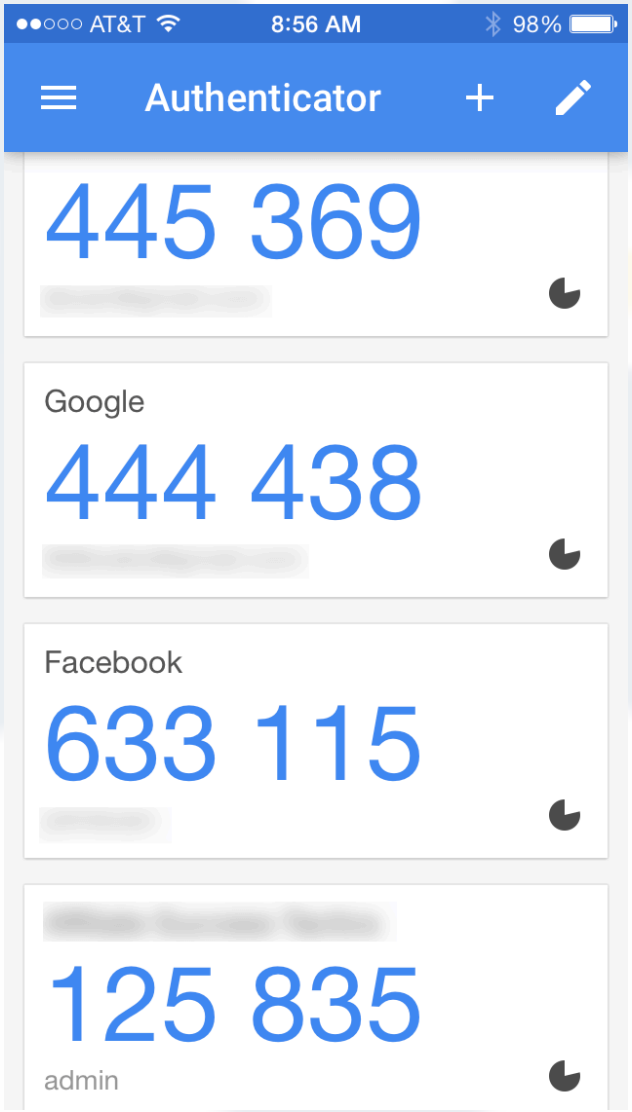
Validasi Password dan OTP code

```
<?php
        $code=$_POST['c'];
        $username=$_POST['username'];
        $password=$_POST['password'];
        require_once('rfc6238.php');
        $secretkey = 'GEZDGNBVGY3TQOJQGEZDGNBVGY3TQOJQ';
        $currentcode = $code;
        if (TokenAuth6238::verify($secretkey,$currentcode)) {
                if($username=="idris"&&$password=="winarno"){
                        echo "Code is valid\n";
                }else
                        echo "username and password is invalid";
        } else {
                if($username=="idris"&&$password=="winarno")
                        echo "Invalid code\n";
                else
                        echo "username and password is invalid";
        }
 print sprintf('<img src="%s"/>',TokenAuth6238::getBarCodeUrl('idris','idris.my.id',$secretkey,'Idris%20TFA'));
  // print TokenAuth6238::getTokenCodeDebug($secretkey,0);
?>
```

Google Authenticator

Download:

- Playstore
- Appstore



Testing

Username: idris
Password: ••••••••
OTP: 784406
Submit

Invalid code

Code is valid

Tugas

- Gabungkan fail2ban + OTP

  Ketika user 3x salah memasukkan kredensial (username,password dan OTP), maka akan diblokir oleh fail2ban

TERIMA KASIH