Web/Proxy Auth

Oleh:
Idris Winarno

Authentication Scheme in Web Server/Squid

- The user credentials can be passed from the web browser to the proxy in several ways. These methods are called authentication schemes. Squid supports the following schemes:
  - **basic**. This is the oldest and most insecure scheme. User name and password are transferred in clear text and can be read by anyone who can access the transferred data. You need to be aware of this and decide if this is acceptable in your environment.
  - **digest**. This a better, more secure authentication scheme. Instead of passing the password in clear text, this scheme uses a hash based on the password and several other parameters.
  - **NTLM**. NTLM is a protocol that is used in several Microsoft network implementations to enable single sign-on across different services. Squid supports NTLM for proxy authentication, although it is not an official HTTP extension.

Installation

- # apt-get install squid3 apache2 php5 wireshark

Basic Scheme
(Web server)

Web Server Configuration: apache2.conf

- # vim /etc/apache2/apache.conf

```
<Directory />
        Options FollowSymLinks
        # AllowOverride None
        AllowOverride All
        Require all denied
</Directory>

<Directory /usr/share>
        AllowOverride None
        Require all granted
</Directory>

<Directory /var/www/>
        Options Indexes FollowSymLinks
        # AllowOverride None
        AllowOverride All
        Require all granted
</Directory>
```

Web Server Configuration: .htaccess

- # service apache2 restart
- # mkdir /var/www/html/coba
- # cd /var/www/html/coba
- # vim .htaccess

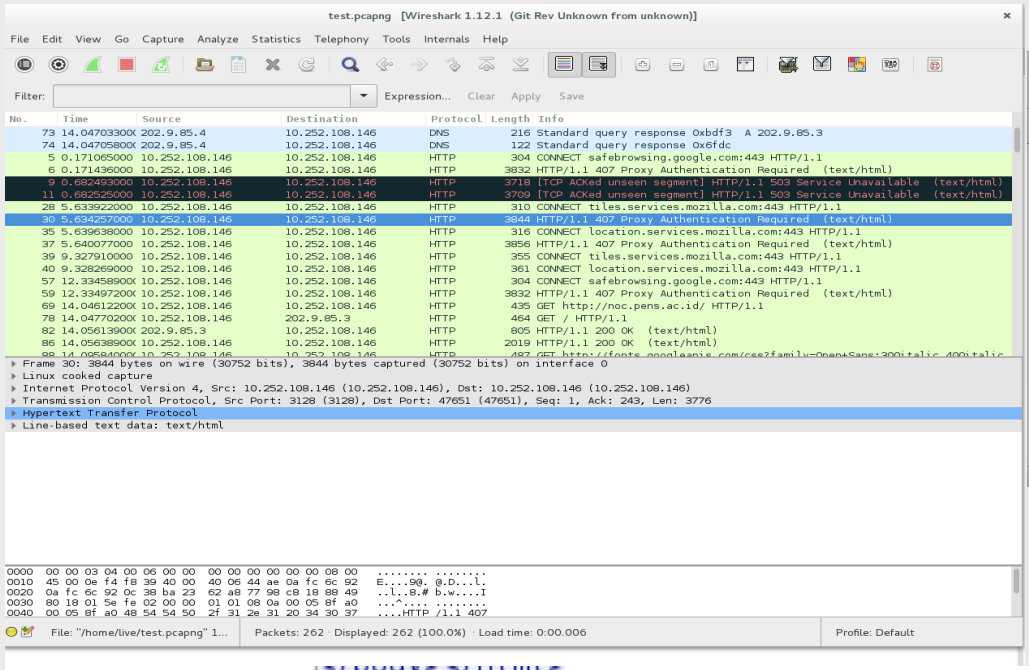
```
Authtype Basic
AuthName "Masukkan password anda"
AuthUserFile /etc/squid3/passwd
Require valid-user
```

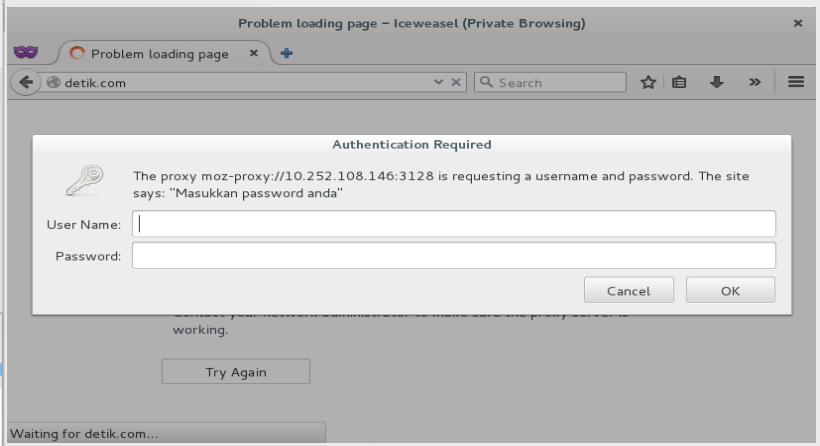
Create Password File

- Untuk membuat file password pertama kali
- # htpasswd -c /etc/squid3/passwd idris
- Untuk akun tambahan
- # htpasswd /etc/squid3/passwd test

```
root@debian:/home/live# htpasswd -c /etc/squid3/passwd  idris
New password:
Re-type new password:
Adding password for user idris
root@debian:/home/live# htpasswd /etc/squid3/passwd  test
New password:
Re-type new password:
Adding password for user test
root@debian:/home/live# cat /etc/squid3/passwd
idris:$apr1$kB/8wIPJ$Wx7T7i51lyFrP3APcFrjC.
test:$apr1$DgOg/xtt$JeSsU3nfQZbPodm/wQXhi.
root@debian:/home/live#
```

Wireshark and Browser






```
CONNECT tiles.services.mozilla.com:443 HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0
Iceweasel/38.5.0
Proxy-Connection: keep-alive
Connection: keep-alive
Host: tiles.services.mozilla.com:443
Proxy-Authorization: Basic aWRyaXM6aWRyaXM=
```

```
root@debian:/home/live# echo -n aWRyaXM6aWRyaXM=|base64 -d; echo
idris:idris
```

Basic Scheme (SQUID)

Squid Configuration

- # vim /etc/squid3/squid.conf

find a string “INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS”

Code in after the “INSERT….

```
auth_param basic program /usr/lib/squid3/basic_ncsa_auth /etc/squid3/passwd
auth_param basic children 5
auth_param basic realm Proxy
auth_param basic credentialsttl 15 minutes

acl password proxy_auth REQUIRED
acl jarkom src 10.252.108.0/24
http_access allow jarkom password
```

Restart and Testing

- # service squid3 restart
- Open your browser and set your proxy server as localhost on port 3128
- Access a website
- Analyze using wireshark

DIGEST Scheme (WEB SERVER)

Enable Digest Module for Apache

- # a2enmod auth_digest
- # service apache2 restart

```
root@debian:/etc/apache2/mods-enabled# a2enmod auth_digest
Considering dependency authn_core for auth_digest:
Module authn_core already enabled
Enabling module auth_digest.
To activate the new configuration, you need to run:
  service apache2 restart
root@debian:/etc/apache2/mods-enabled# service apache2 restart
```

Web Server Configuration: .htaccess

- # mkdir /var/www/html/coba2
- # vim /var/www/html/coba2/.htaccess

```
AuthType Digest
Require valid-user
AuthName "pens"
AuthUserFile /etc/squid3/passwdDigest
```

Create Digest Password File

- # htdigest -c /etc/squid3/passwdDigest pens idris

```
root@debian:/home/live# htdigest -c /etc/squid3/passwdDigest pens idris
Adding password for idris in realm pens.
New password:
Re-type new password:
root@debian:/home/live# cat /etc/squid3/passwdDigest
idris:pens:92424467a32f2283a33d079eaca1ce46
root@debian:/home/live#
```

DIGEST Scheme (SQUID)

Squid Configuration

- # vim /etc/squid3/squid.conf

Code in after the “INSERT….

```
auth_param digest program /usr/lib/squid/digest_pw_auth -c /etc/squid3/
passwdDigest
auth_param digest children 2000
auth_param digest realm pens
auth_param digest nonce_garbage_interval 5 minutes
auth_param digest nonce_max_duration 30 minutes
auth_param digest nonce_max_count 50
auth_param digest post_workaround off

acl password proxy_auth REQUIRED
acl jarkom src 10.252.108.0/255.255.255.0
http_access allow jarkom password
```

Restart and Testing

- # service squid3 restart
- Open your browser and set your proxy server as localhost on port 3128
- Access a website

Wireshark

- Use wireshark to analyze and make a comparation of both authentication scheme!

THANK YOU