

KEAMANAN JARINGAN KOMPUTER

**HACK USERNAME DAN PASSWORD MENGGUNAKAN TOOLS *WIRESHARK* DAN
*CHAIN AND ABLE***



OLEH :

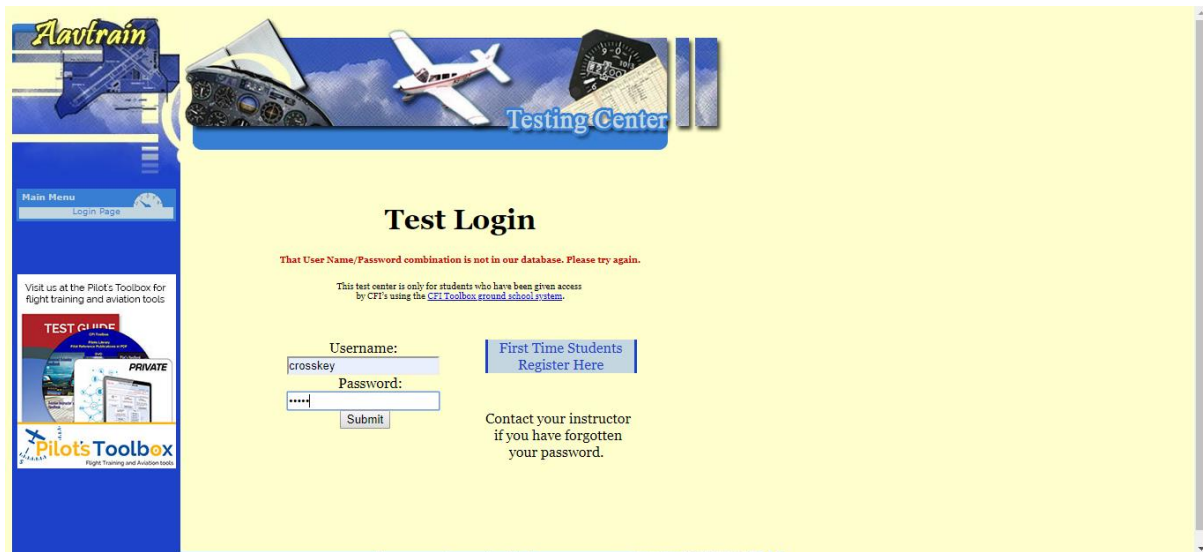
NAMA : SYUKRAN RIZKI
NIM : 09011181520019
KELAS : SK 8 A

FAKULTAS ILMU KOMPUTER
SISTEM KOMPUTER
UNIVERSITAS SRIWIJAYA

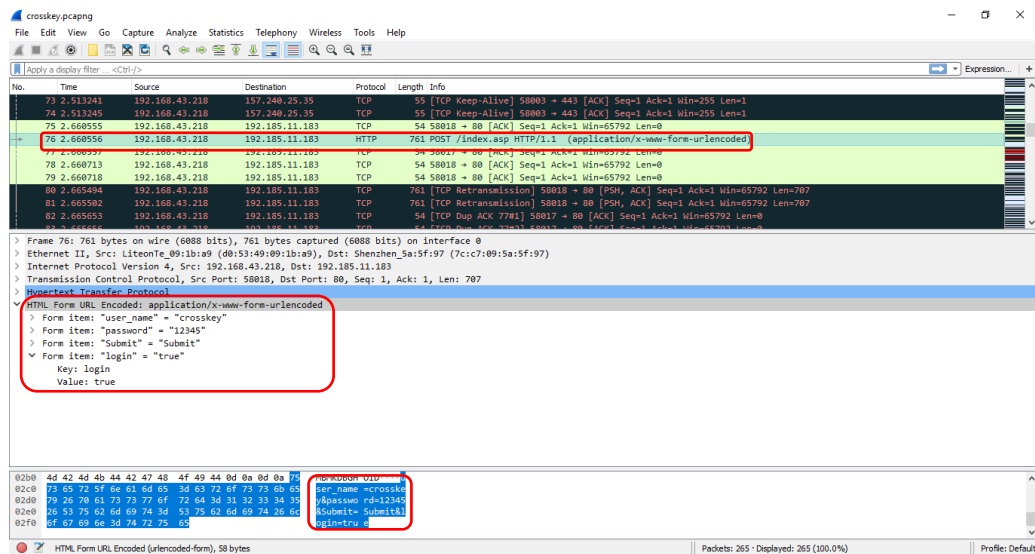
2019

HTTP

Website yang digunakan untuk protocol *Http* adalah <http://aavtrain.com/index.asp>.



Tools yang digunakan *Wireshark* sebagai pemantau jaringan dan *chain and able* sebagai poison (menyerang).



Penjelasan :

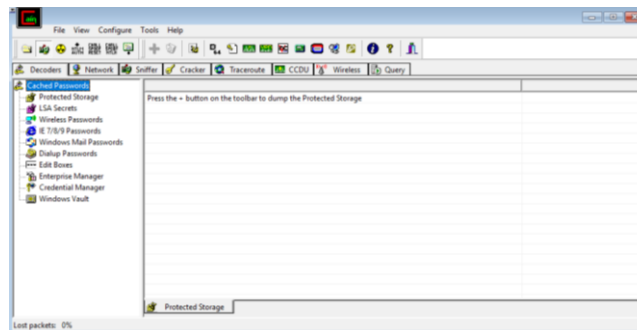
Didalam melakukan percobaan ini dibagi 2 dua kategori *penyerang* dan *Target*, *Penyerang* sebagai penangkap paket data di dalam jaringan menggunakan *wireshark* dan *chain and able* sebagai (menyerang), dan *Target* sebagai pengisi username dan password di website <http://aavtrain.com/index.asp>, ini dilakukan di satu jaringan.

HTTPS

Website yang ditargetkan untuk hack password adalah Website <https://akademik.unsri.ac.id>.



Tools yang digunakan *Chain and able*.



Berikut adalah hasil dari crack password tersebut.

```
HTTP/1.1 200 OK (text/html)
Date: Mon, 11 Mar 2019 09:54:33 GMT
Last-Modified: Fri, 22 Aug 2008 04:03:36 GMT
Connection: keep-alive
ETag: "48ae3a98-1e1dd"
Expires: Mon, 11 Mar 2019 10:54:33 GMT
Cache-Control: max-age=3600

[client-side-data (826 bytes)]POST /portal02/login/proses_login.php HTTP/1.1
Host: akademik.unsri.ac.id
Connection: keep-alive
Content-Length: 54
Cache-Control: max-age=0
Origin: https://akademik.unsri.ac.id
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://akademik.unsri.ac.id/portal02/login/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7,ms;q=0.6,fa;q=0.5
Cookie: _ga=GAl.3.1375185782.1552241309; _gid=GAl.3.41169025.1552241309; PHPSESSID=h17bvtd38f02p268ui6r7uiq36
username=crosskey&userpassword=cobaccoba&id_prodi=10001[Server-side-data (357 bytes)]HTTP/1.1 302 Moved Temporarily
Server: nginx/1.10.3 (Ubuntu)
Date: Mon, 11 Mar 2019 09:54:54 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
location: gagal.php

0

[client-side-data (657 bytes)]GET /portal02/login/gagal.php HTTP/1.1
Host: akademik.unsri.ac.id
```

Penjelasan :

Didalam melakukan percobaan ini dibagi 2 dua kategori *penyerang* dan *Target*, *Penyerang* sebagai penangkap paket data dan menyerang di dalam jaringan menggunakan *chain and able*, dan *Target* sebagai pengisi username dan password di website <https://akademik.unsri.ac.id>, ini dilakukan di satu jaringan.