**Cobalt Strike**, yetkili sızma testleri ve Red Team tatbikatlarında kullanılan, tam özellikli bir **C2 (Command & Control) ve post‑exploitation** çerçevesidir. Saldırı simülasyonlarını gerçekçi kılan **Malleable C2 profilleri**, **Beacon** implantı, yanal hareket (lateral movement) ve kalıcılık (persistence) teknikleri için zengin modüller sunar.

**Bu aracın öne çıkan özellikleri**

* **Beacon**: HTTP/HTTPS/DNS gibi kanallar üzerinden gizlenebilir komuta‑kontrol iletişimi
* **Malleable C2**: Trafiğin görünümünü (HTTP header, URI şablonu, zamanlama vb.) özelleştirebilme
* **Post‑exploitation modülleri**: Kimlik bilgisi elde etme, süreç enjekte etme, yanal hareket vb.
* **Sosyoteknik destekleri**: Payload/droper üreteçleri, sahte belgeler, macro vb.
* **Takım çalışması**: “Team Server” üzerinde oturum ve hedef yönetimi, operatör işbirliği

**Bu Aracın Kali’ye Kurulumu**

**Adım 1-) Java 11 kur**

**“sudo apt update**

**sudo apt install -y openjdk-11-jdk**

**java -version”**

**Adım 2 -) Cobalt Strike paket(ler)ini indir ve çıkar**

Fortra portalından gelen **Linux** dağıtım paket(ler)ini indirin. Ardından:

**“sudo mkdir -p /opt/cobaltstrike && cd /opt/cobaltstrike**

**# Team server veya client .tgz için tar komutu:**

**“sudo tar zxvf ~/Downloads/cobaltstrike-dist-linux.tgz -C /opt/cobaltstrike --strip-components=1”**

**Adım 3-) Güncelleme (update) aracıyla kurulumu tamamla**

**“cd /opt/cobaltstrike**

**sudo chmod +x update**

**./update”**

**metin, yazı tipi, ekran görüntüsü, siyah içeren bir resim

Açıklama otomatik olarak oluşturuldu**

Bu adımda **lisans anahtarınızı** girersiniz; updater gerekli dosyaları indirir. (Team server ve client için ayrı paket aldıysanız her biri kendi dizininde güncellenir.)

**Adım 4-) Team Server’ı başlat (opsiyonel profil ile)**

Team Server Linux üzerinde çalışır. Örnek:

“cd /opt/cobaltstrike/server

sudo chmod +x teamserver

./teamserver 192.168.1.100 MyStrongPassword

[/opt/cobaltstrike/profiles/my.profile]”

metin, yazı tipi, ekran görüntüsü içeren bir resim

Açıklama otomatik olarak oluşturuldu

Komut söz dizimi ve isteğe bağlı **Malleable C2 profile**/kill‑date parametreleri resmî kılavuzdadır. Varsayılan yönetim portu **50050**’dir (istemci bağlanırken kullanır).

**Ağ notu**: Güvenlik grubunuz/firewall’da 50050 (CS client bağlantısı) ve kullanacağınız listener portlarını (örn. 80/443) uygun şekilde açın. (Port 50050 bilgisi resmî kılavuzda geçer.)

**Adım 5-) İstemciyi (Client) başlat ve bağlan**

**“cd /opt/cobaltstrike/client**

**chmod +x cobaltstrike**

**./cobaltstrike”**

Açılan **Connect** penceresinde:

* **Host**: Team Server IP/DNS
* **Port**: 50050 (değiştirmediyseniz)
* **User**: Takma adınız
* **Password**: Team Server başlatırken verdiğiniz şifre

İlk bağlanışta istemci, Team Server’ın **SHA256 sertifika hash**’ini onaylatır.