**ReconFTW Nedir?**

**ReconFTW**, siber güvenlikte özellikle **bilgi toplama (reconnaissance)** aşaması için kullanılan **otomatik bir pasif ve aktif bilgi toplama aracıdır**. Red team ve bug bounty toplulukları tarafından yoğun şekilde kullanılır. Arka planda birçok popüler bilgi toplama aracını entegre çalıştırır.

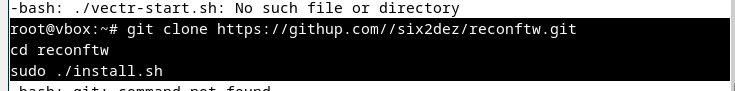
**ReconFTW Özellikleri**

* **Tam Otomatik:** Tek bir komutla hedef hakkında kapsamlı bilgi toplar.
* **Aktif ve Pasif Bilgi Toplama:** Subdomain, IP, port, servis, zafiyet vs. keşfeder.
* **Entagrasyon:** Amass, Subfinder, Nmap, Httpx, Waybackurls, Shodan, Github Search gibi birçok aracı bir arada kullanır.
* **Hedefe Özel Dizinleme:** Hedef domain veya IP’ye özel klasör oluşturur ve çıktıları oraya kayıt eder.
* **Zafiyet Tespiti:** Potansiyel açıklar hakkında uyarılar verir.
* **Kolay Kullanım:** Basit bir terminal komutu ile çalışır.
* **Açık Kaynak:** GitHub üzerinden erişilebilir.

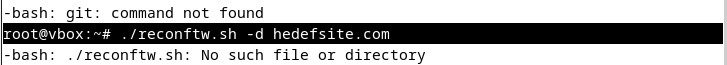
**ReconFTW Kurulum Aşamaları**

**Gereksinimler:**

* Linux (Debian/Ubuntu önerilir)
* Git
* sudo yetkisi
* İnternet bağlantısı
* Golang (bazı entegre araçlar için)

**1. GitHub Üzerinden Kurulum: **

**-**Bu komut, ReconFTW’yi kurar ve tüm bağlı araçları otomatik olarak indirir.

**2. Çalıştırma: **

**-**Yukarıdaki komut, “hedefsite.com” için bilgi toplamaya başlar.

# ReconFTW Kullanımı

### Temel Kullanım:

### Parametreli Kullanım

* -d: Domain belirtir.
* -r: Sadece pasif toplama (aktif test yapmaz).
* -p: Sadece port taraması.
* -s: Tüm adımları çalıştırır (varsayılan).
* -o: Çıktı dizini belirtir.

### Örnek:

**Dikkat Edilmesi Gereken Noktalar**

* İlk kurulum uzun sürebilir çünkü birçok araç yüklenir (~30 dakika).
* İnternete bağlı olman şart.
* Aktif bilgi toplama kısmı hedef sistem üzerinde trafik oluşturabilir (legal izin olmadan **asla kullanılmamalıdır!**).
* Golang yüklü değilse bazı araçlar çalışmaz.
* Sistem kaynağı fazla tüketebilir, güçlü bir makinede çalıştırılması önerilir.
* install.sh dosyası tüm bağımlılıkları root olarak kurar, dikkatli kullanılmalıdır.

**ReconFTW Kullanım Alanları**

* **CTF Yarışmaları:** Hızlı bilgi toplama için.
* **Bug Bounty (Açık Kaynak Güvenliği):** Web uygulamalarında zafiyet ararken kapsamlı veri toplar.
* **Kırmızı Takım Operasyonları:** Saldırı öncesi hedef hakkında detaylı analiz yapılmasını sağlar.
* **Pentest (Sızma Testi):** Hedef sistemler hakkında otomatik ön keşif.
* **Eğitim Amaçlı:** Yeni başlayanlar için bilgi toplama araçlarını tanıma ve kullanma pratiği sağlar.