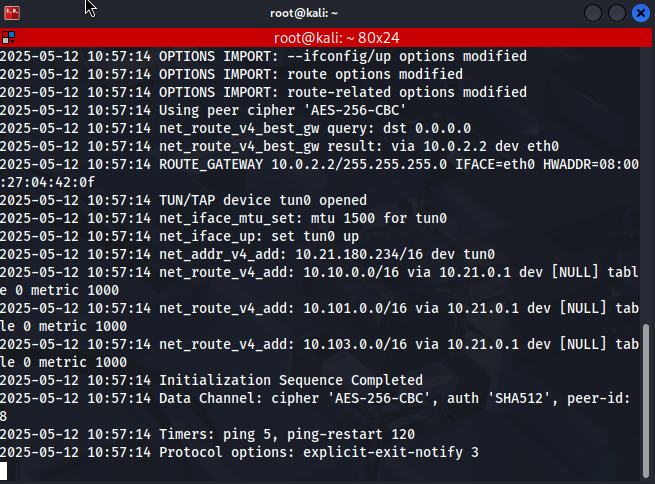
Mr.Robot CTF

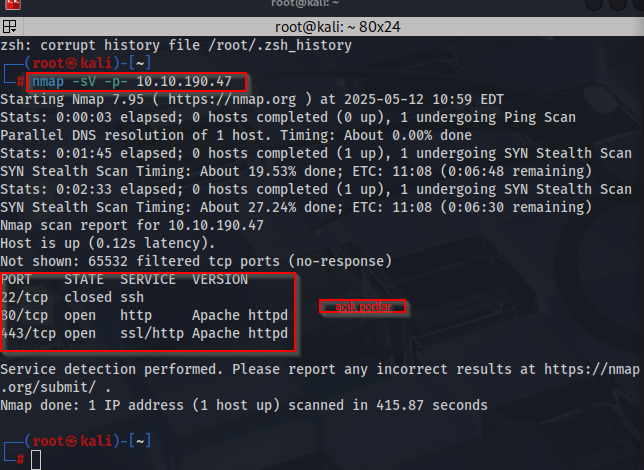
12 Mayıs 2025 Pazartesi

18:26

1. İlk başta TryHackme de Openvpn açtım ve hedef makinası açtık
2. Terminale "openvpn ~/Downloads/yourname.ovpn" yazdık ki çalışsın



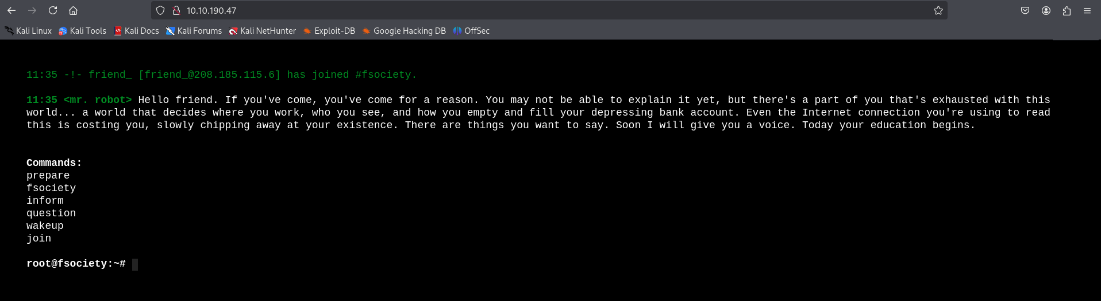
1. Hedef ip mizi öğrendik (TryHackme sitesinde veya hedef makinada).
2. Nmap tool u ile açık portları tarayıp hizmet versiyonlarını öğrenmeye çalıştık.
3. \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Komut Açıklaması\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*
4. nmap -sV -p- <target-ip> kodu ne işe yarar tek tek aşağıda açıklayayım.
5. -sV: Servis ve versiyon bilgilerini öğrenir. -p-: 1-65535 arasındaki tüm TCP tarar.
6. 80 (HTTP) - Web sunucusu , 443 (HTTPS) -Güvenli Web, 22 (SSH) güvenlü Bağlantı.



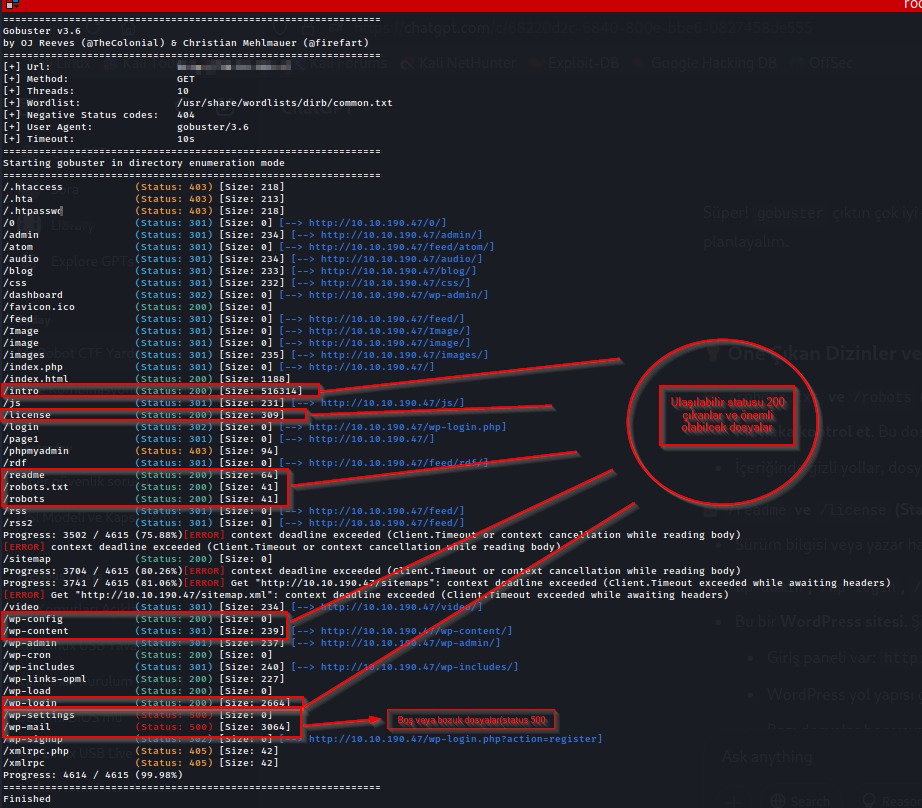
* 1. Şimdi ne yapmalısın ? Açıklayalım.
  2. Eğer 80 veya 443 açıksa tarayıcıda <target-ip>'yi aç ve sitenin içeriğine göz at.
  3. Kaynak koduna (Ctrl + U Tarayıcı içinde) veya curl (terminal içinde) gibi komutlarla ana sayfa içeriğine bak.
  4. Şimdi gobuster toolu ile wordlisteki her kelimeyi denicez uygun dizin bulucaz(Web dizin Taraması)

* 1. \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Komut Açıklaması\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*
  2. Komut: "gobuster dir -u http://<hedef-ip> -w /usr/share/wordlists/dirb/common.txt" Tek tek açıklayalım.
  3. Gobuster: web sitesine istekler göndererek, gizli dizinleri ve dosyaları bulmaya çalışır.
  4. Dir: toolun mod seçimidir dizin keşfi yapar. Başka mod örnekleri(dns,vhost,s3,fuzz) gibi.
  5. -u: tarama yapılacak hedefin URL'si belirtilir. (-u http://<hedef\_ip>).
  6. -w: wordlist demektir, tarama sırasında denenecek dizin adı içerir.
  7. Common.txt: En çok kullanılan dizin isimlerini içerir(admin,login,wp-content,images,vb).
  8. /usr/share/wordlists/dirb/common.txt: dosyasındaki her satırı tek tek alır.
  9. Bu url lere tek tek GET requestler 200,301,403 yanıtana göre gerçekten varmı bakar.

Tarayıcada Target İp açınca



Gobuseter çıktısı



* 1. Peki şimdi ne yapıcaz?
  2. "curl <http://10.10.190.47/robots.txt> " gibi komutlarla terminale robots.txt sini açabiliz veya wget ile kendi makinenize indirebilirsiniz ("wget <http://10.10.190.47/intro>"). Ya da Tarayıcıda aç.