TechCareerCTF Write Up

# İlk olarak nmap <ip> -Scv -T4 -vv -Pn taraması yaparak işe başlıyoruz

# Bu tarama sonucu 22,8080,11,445,139,901 portlarının açık olduğunu görüyoruz

# 

# <ip>:8080 portuna gidiyoruz ve burada bizi bir sayfa karşılıyor kariyer.net üzgünüz sistemimiz şu an bakımda diye, hemen kaynak kodunu inceledik ve orda fazladan yazılmış garip bir şifreli metin bulduk. Daha sonrasında ise internetten bu şifreyi çözdüğümüzde şifreli metinin kariyer.php olduğunu gördük

# Hemen <ip>:8080/kariyer.php sayfasına gittik ve bizi böyle bir sayfa karşıladı

# Burada hemen SQL injection,XSS veya command injection zafiyetlerinden biri var mıdır diye denemeler yaptım ve command injection olduğunu fark ettim. Normal olarak arama kısmına terminal komutları girdiğimizde çalışmıyordu fakat hemen önüne bir ; koyarak bunu aşabiliyorduk ;ls ve ;cat flag1 komutları ile ilk bayrağı aldık.

# Daha sonrasında internette Reverse Shell Generator’ten bir tane bash komutu çalıştırarak ve aynı zamanda terminalden de pwncat yardımı ile 4444 portunu dinlemeye alarak sisteme giriş yaptım

# 

# Sistemdeki kullanıcıları görmek için hemen bir cat /etc/passwd komutu yapıp kariyer1 adında bir tane kullanıcı olduğunu fark ettim ve cd komutu ile kariyer1 kullanıcısın masaüstüne gittiğimde flag2’nin orda olduğunu gördüm ama okumaya iznimiz yoktu ve aynı zamanda yanında bir tane de resim dosyası olduğunu gördüm

# Resimi indirmek için hemen kısa bir süreliğine Python kullanarak bir web server açtım Python -m SimpleHTTPServer komutunu kullanarak sonrasında ise 8000 portunda açtığımız bu server’a bağlanmak için <ip>:8000 adresine gittim

# Buradan resmi indirdim ve içinde şifrelenmiş bir şeyler olabilir diye online siteler yardımıyla decrypt ettim. Base 64’e çevirince resmin en başında gizli bir şifre yazıyordu onu da md5 ile çözdüm ve bana kariyer1 kullanıcısının şifresini verdi. Hemen terminale gidip su kariyer1 komutu ile kariyer 1 kullanıcısına geçip flag2’yi de elde ettim

# Artık sadece root olmak kalmıştı onun için de kullanabileceğim dosyalara bakmak için find / -perm -u=s -type f 2>/dev/null komutunu çalıştırdım. Pek kullanılabilcek bir dosya yok gibiydi daha sonrasında ise sudo -l komutu ile ne kullanabileceğime baktım ve (root) NOPASSWD: /bin/nano böyle bir şey gördüm yani nano kullanarak root seviyesine çıkabilirdim.

# GTFOBins sayfasına giderek nano’yu nasıl kullanabilceğime baktım. Root olabilmek için

nano

^R^X

reset; sh 1>&0 2>&0

# komutunu kullandım ve işe yaradı artık root kullanıcısı oldum ve root dizininde ki son flag’i de almayı başardım, CTF’in sonuna ulaştım

# 