# Raven1:

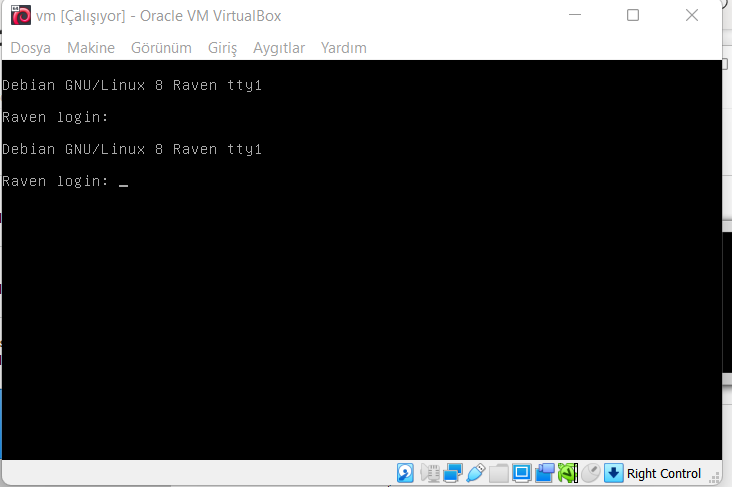
# Walkthrough | Vulnhub

**Giriş:**

Raven 1 makinesi giriş ve orta seviye bir makine olarak Vulnhubda listelenmiş.

Bence kolay makine olarak sınıflandırmak biraz daha doğru olabilir. Ama sonuçta bu kullanılan skillsetle alakalı olduğu için kabul edilebilir bir seçim.

Ben sanal makineyi kurarken Vİrtualbox’ı kullandım.Ama network ayarlarıyla biraz oynamam gerekti makineye ulaşabilmek için .



Makineyi kurduk ve network ayarlarından bridge moda çektik böylece ağımızdaki herhangi bir bilgisayar bu makineye erişebilecek. Sonuçta bu makine zafiyetli bir makine bu işlemi yaparken ne yaptığınızı bildiğinize emin olun.

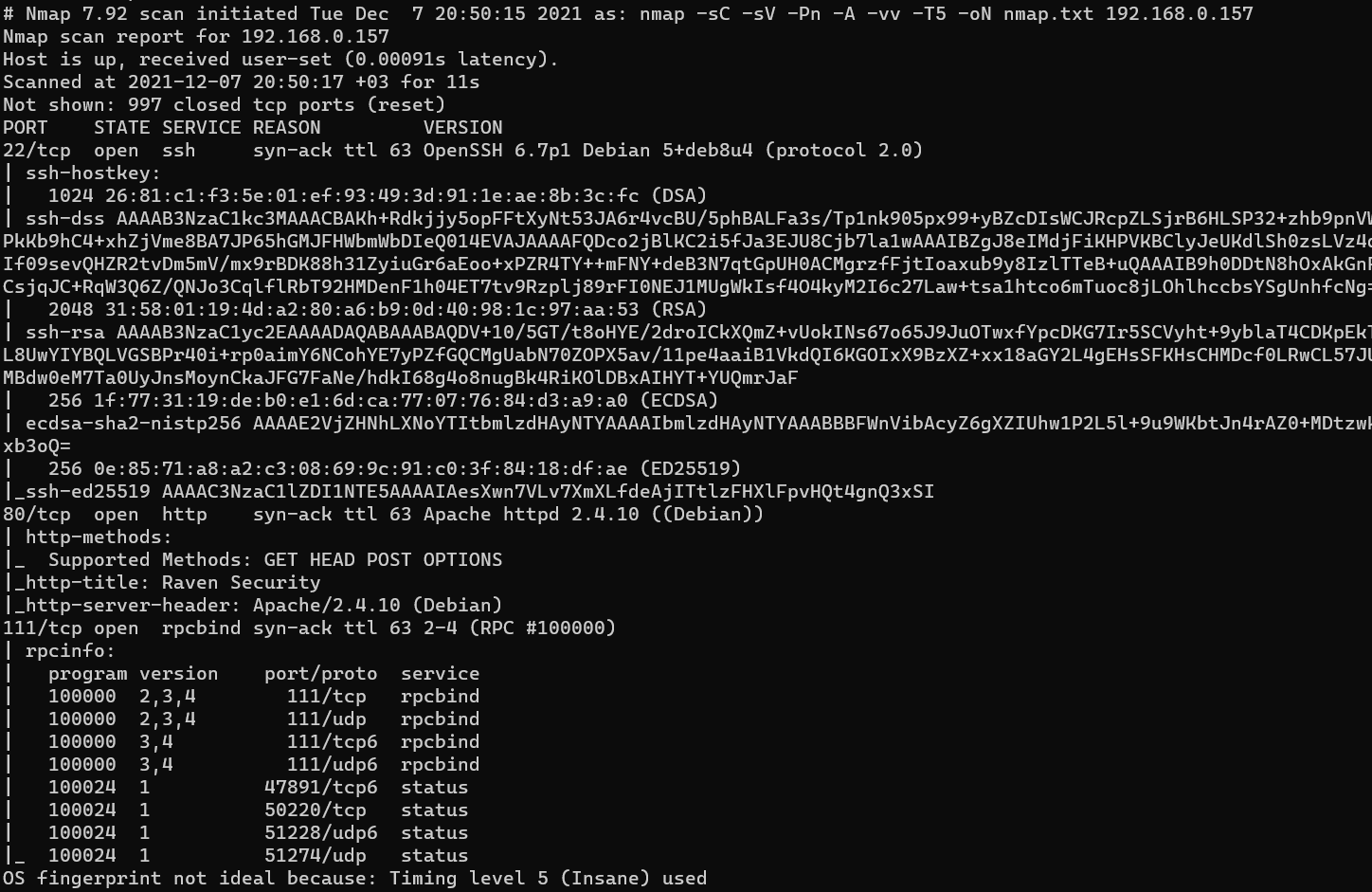
Öncelikle bu makinenin ip adresi bize lazım. Netdiscover gibi tooları kullanarak ya da nmap ile tarama yaparak ağımızı keşfedebiliriz.

Sudo nmap –sN 192.168.0.0/24 -T5

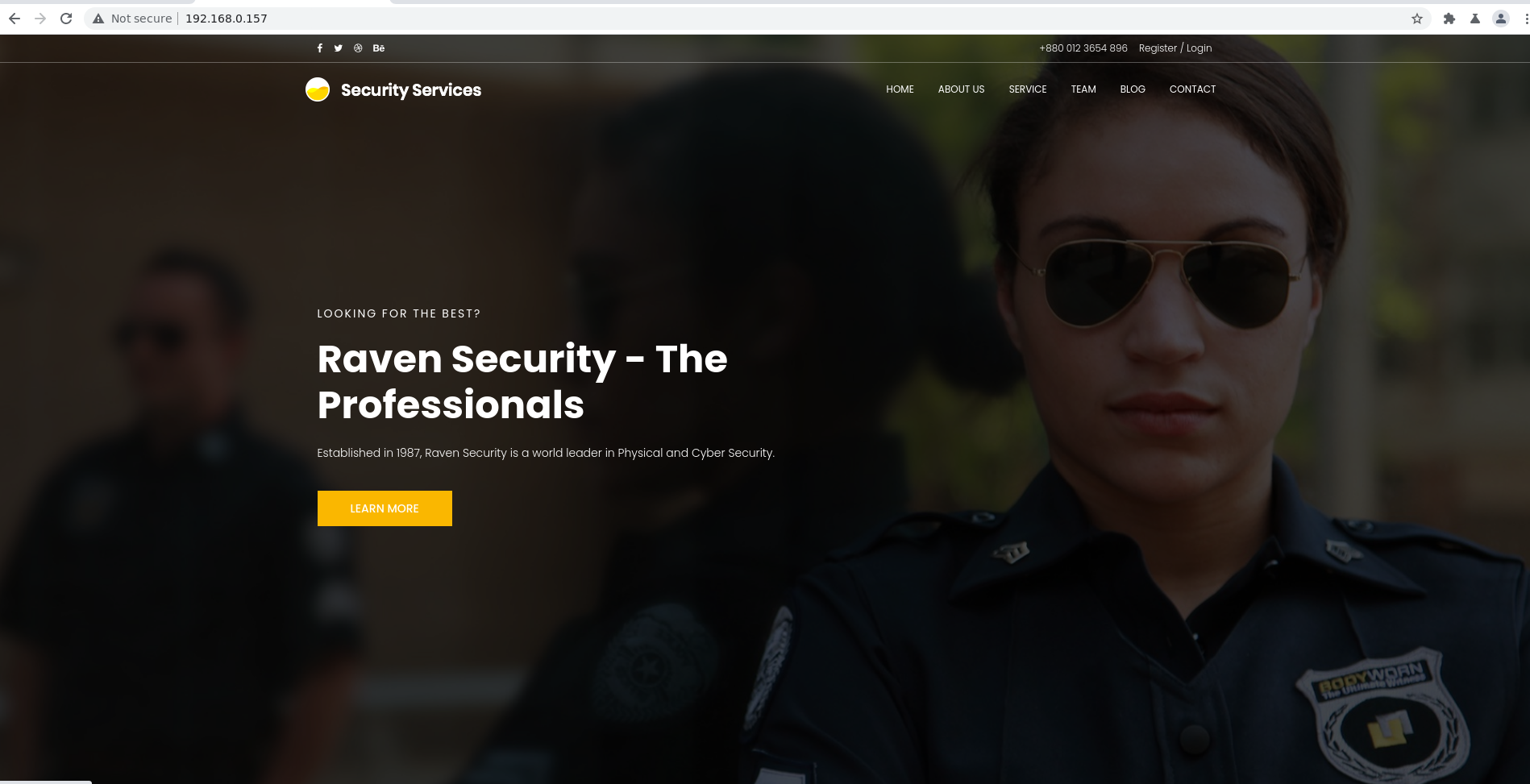
Komutunu kullanarak makinenin ip adresini 192.168.0.157 olarak buldum.

Hemen bir nmap taraması gerçekleştiriyoruz.

nmap -sC -sV -Pn -A -vv -T5 -oN nmap.txt 192.168.0.157



Burada bir http servisinin ayakta olduğunu görüyoruz.

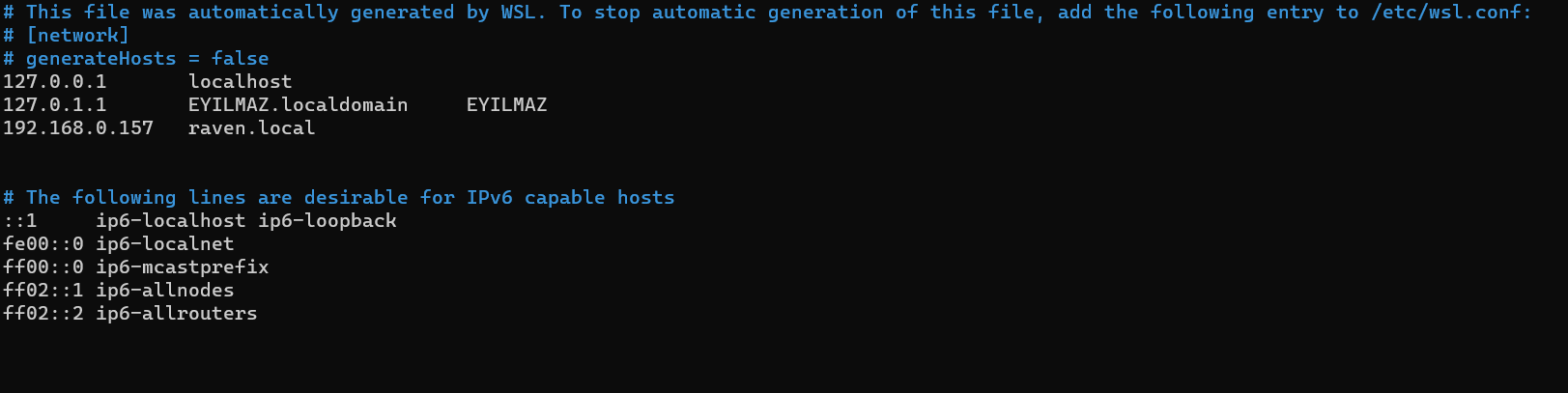


Wordpress sitesi gibi gözüküyor.

Kontrol etmek için service.html sayfasının soruce koduna bakarken ilk flagi buluyoruz.



Wordpresse bakarken sğrekli raven.local diye bir yere yönlendirmek istiyor bizim sitemiz yerine bunu farkedince raven.locali bizim ip adresimiz olarak çözsün diye /etc/hosts dosyasına ekleme yapıyoruz.

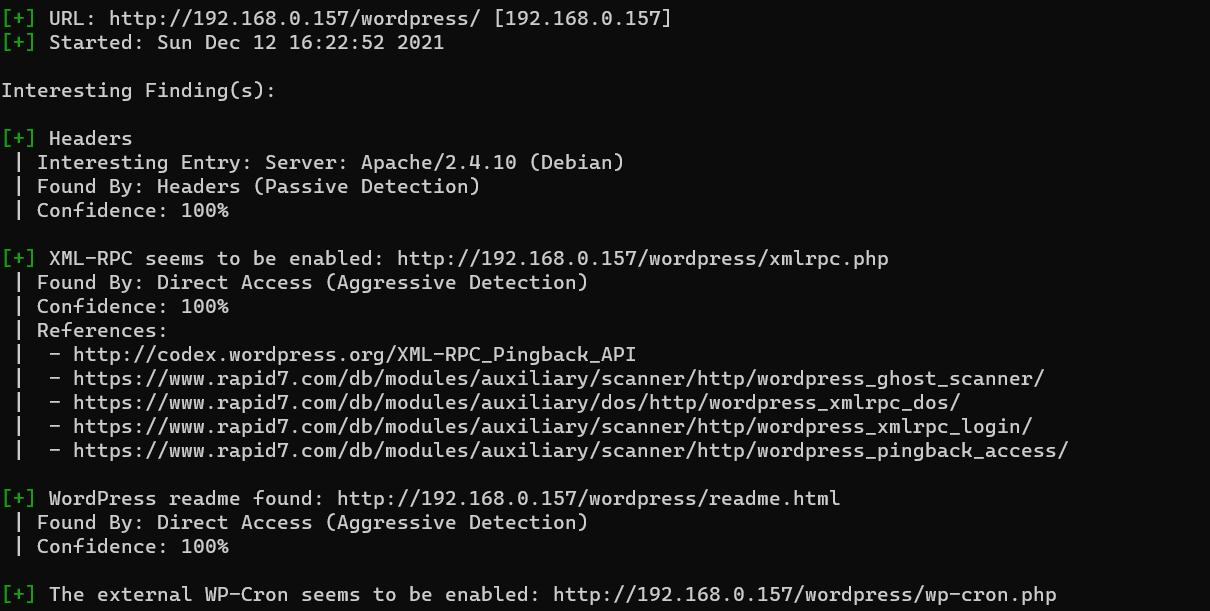


Bu eklemeden sonra wordpress sitesine rahatça gidebildiğimizi görüyoruz.

Öncelikle bir wpscan ile genel bilgi edinmeye çalışacağız.

wpscan --url 192.168.0.157/wordpress/

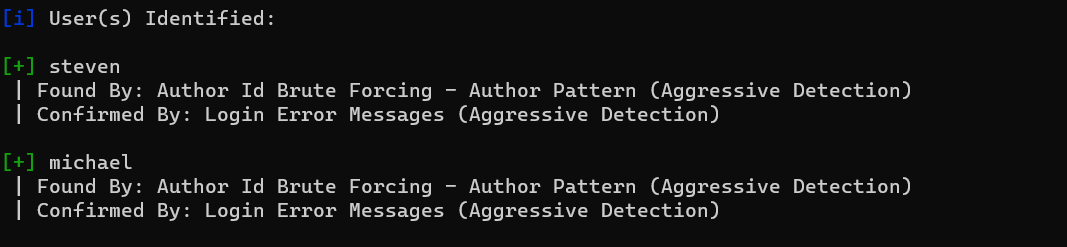
Komutunu çalıştırıyoruz.



Burada wordpress sürümü vb konular hakkında bilgi edindik. Aklimıza brute force saldırısı yapabileceğimiz geldi.

wpscan --url 192.168.0.157/wordpress -e u

Komutunu çalıştırarak kullanıcıları bulmaya çalıştık.



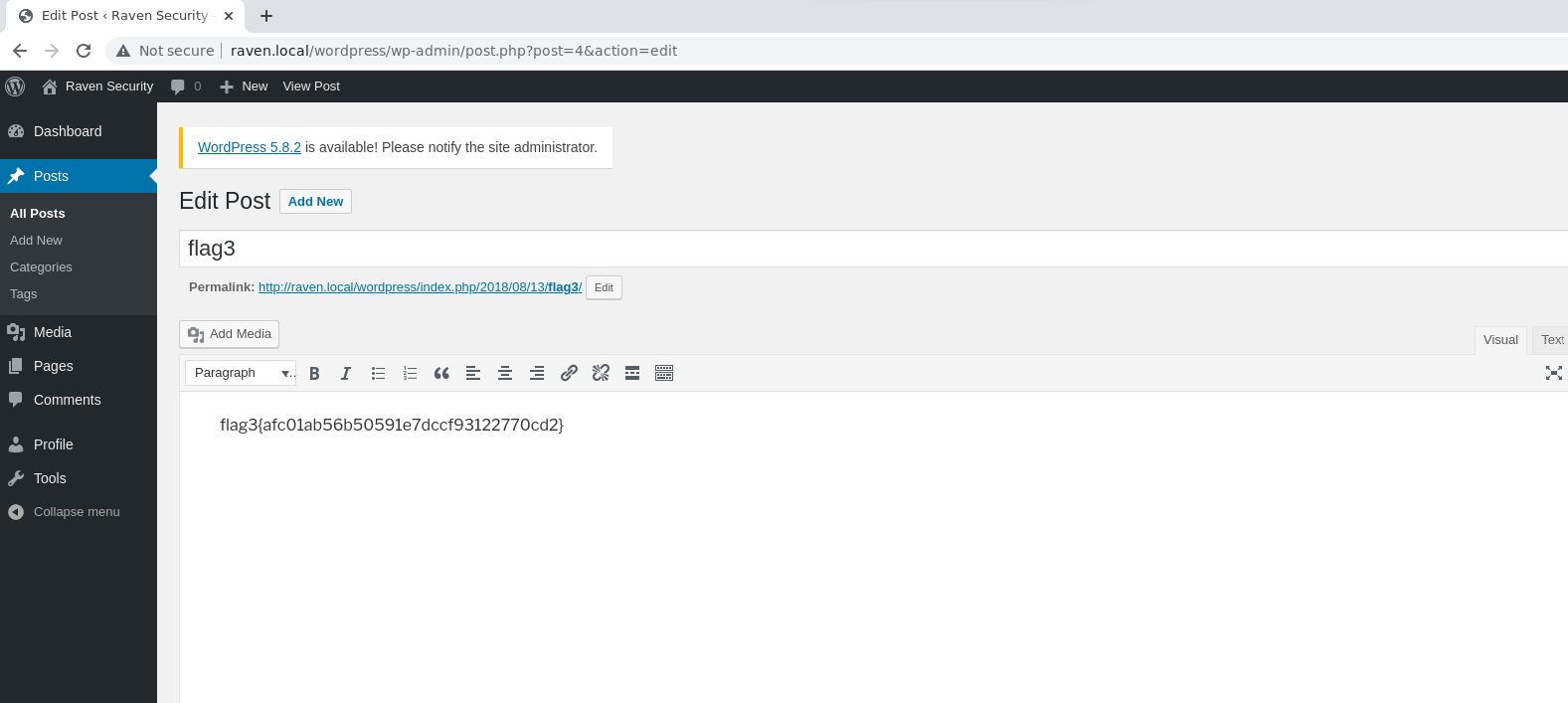
Evet iki tane kullanıcı bulduk .Şimdi steven için brute force uygulayacağız .ben bu iş için rockyou.txtyi kullanacağım.

wpscan --url 192.168.0.157/wordpress -e u -U steven,michael -P /usr/share/wordlists/rockyou.txt — threads 50

Komutunu çalıştırıyor ve bekliyoruz.

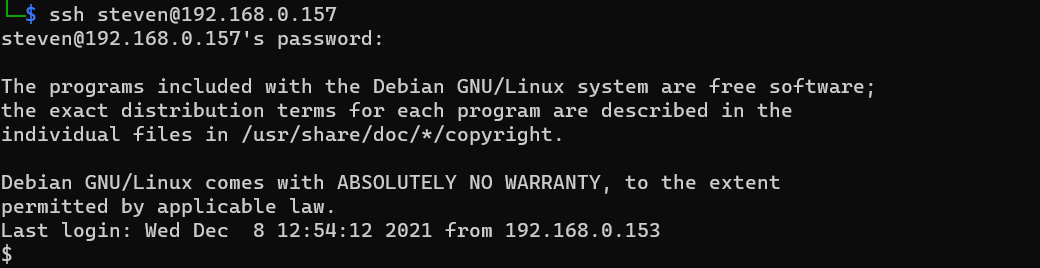


Evet steven adlı arkadaşın şifresini pink84 olarak bulduk.



Evet burada da bir flag bulduk.

Aklımıza ssh servisinin açık olduğu geldi. Ssh servisine steven ve kullanıcısı ve pink84 şifresiyle bağlanmayı deniyoruz.



Evet bağlantı başarılı.

**POST EXPLOİT AŞAMASI**

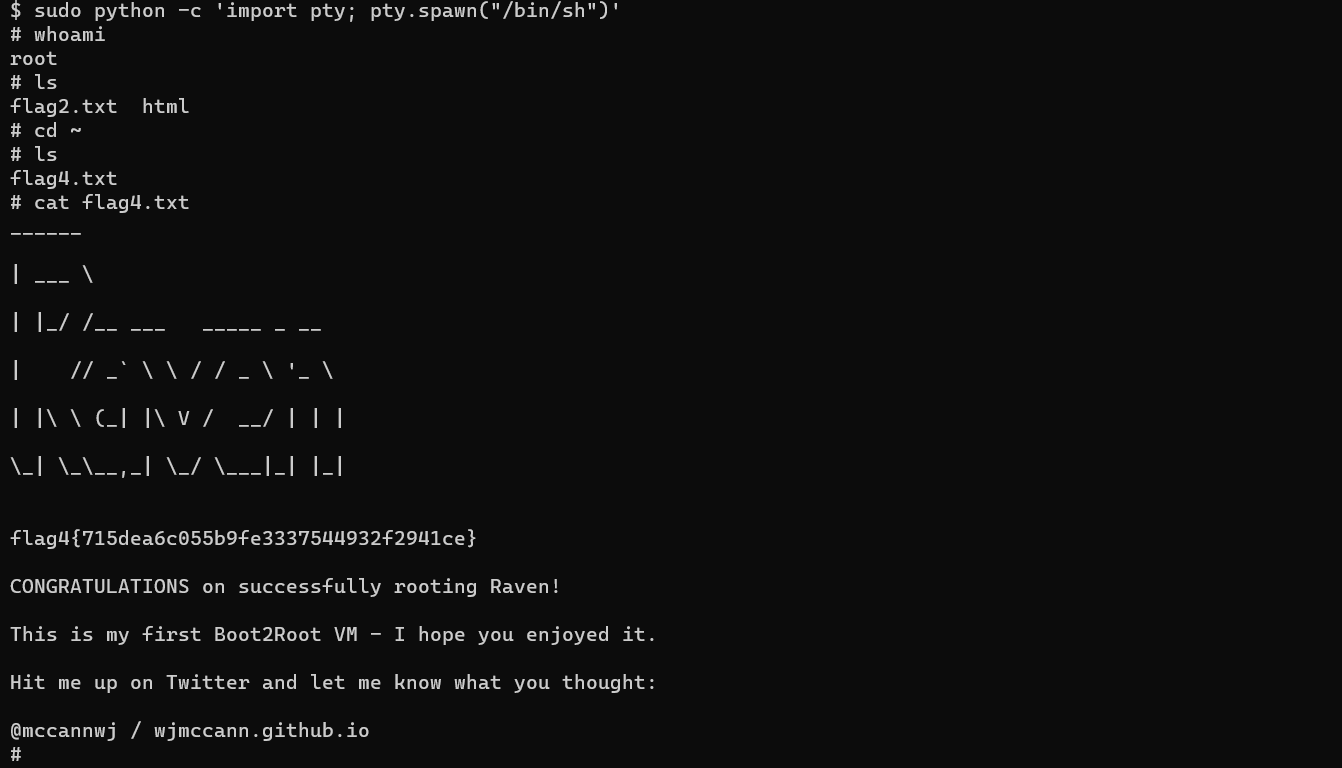
Sudo –l yaparak steven kullanıcısının hangi komutları root yetkisiyle kullanabileceğini görüyorum.



Evet steven kullanıcısı pythonı root yetkisiyle kullanabiliyormuş.

Sudo python -c 'import pty; pty.spawn("/bin/sh")'

Komutunu kullanarak shell spawn ediyoruz.



Evet root olduk.

Home directorysinde flag4.txt dosyasını bulduk ve içini okuduk.

Okuduğunuz için teşekkürler.