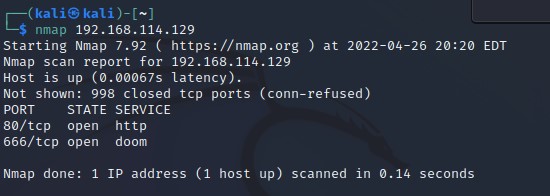
GATHERING INFORMATION SYSTEM WITH NMAP

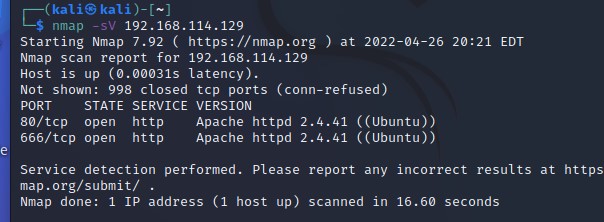
Nmap ile karşı taraftan bilgi toplamak mümkün eğer aynı ağ üzerindeyseniz veya makineler birbirlerine bağlıysa. Bunu şu şekilde yapabiliriz bilgi toplayacak olduğumuz sistem üzerinden ”ifconfig” diyerek karşı tarafın ip adresini öğreniyoruz. Öğrendiğimiz ip adresini saldırı yapacak olduğumuz tarafa geçip nmap komutuyla bilgi toplamaya başlıyoruz.



Burada görüldüğü üzere 80 ve 666 ‘ıncı port üzerinden internete çıkıyormuş bu makine.

Dipnot: 666 port u ben ekledim kısaca anlatmak gerekirse apache serverını kurduktan sonra

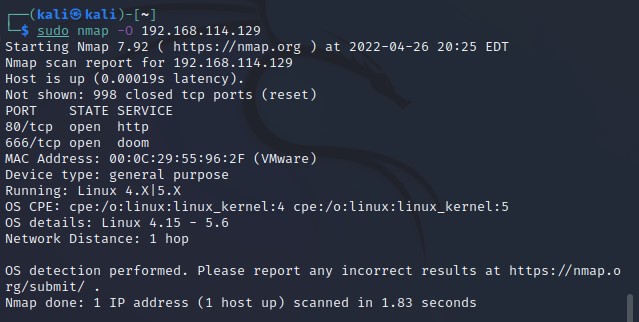
Bazı parametreler ve 666 olarak atadım sonrasında apache sunucusuna girerek admin yetkileriyle 80 port un yanına “Listen 666” diyerek tanımladım sonrasında tekrar başlattım apache sunucusunu ve 666 port internete çıkmaya hazır.



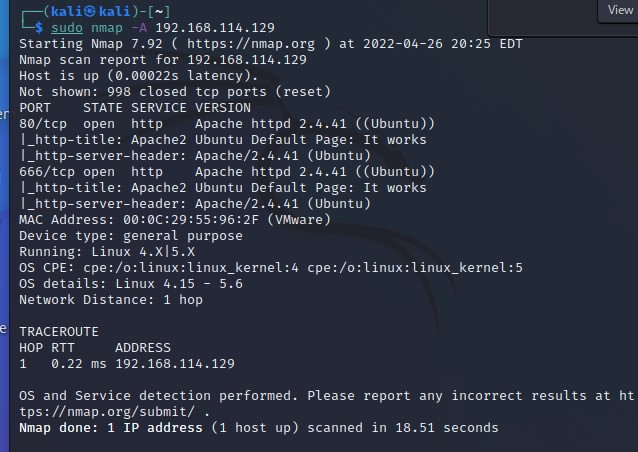
Burada nmap komutunun yanına “-sV” parametresini getirerek işletim sisteminin ne olduğunu öğrendim.



Burada ise “-p-“ komutu ile 65000 portu yani bütün portları taradım ve gene 2 tane açık olan buldum.



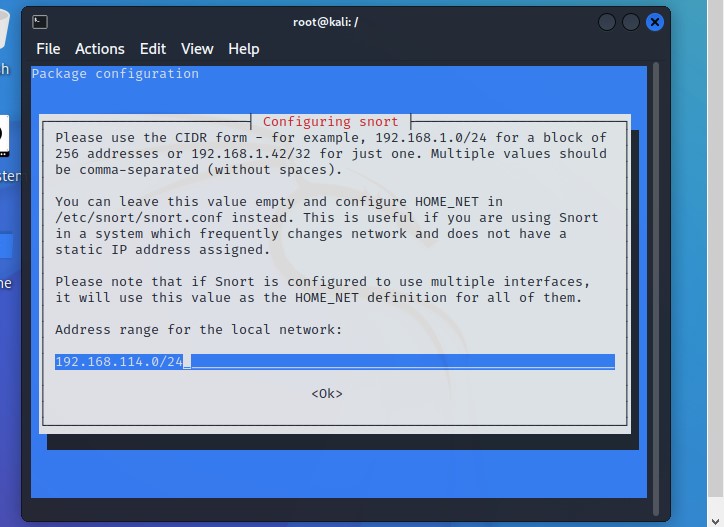
Burada ise “-O” parametresini kullanarak saldıracak olduğum sistemin işletim sisteminin hangi versiyonunu kullanıyor nereden bağlanıyor sanla makine mi değil mi onları öğrendim.



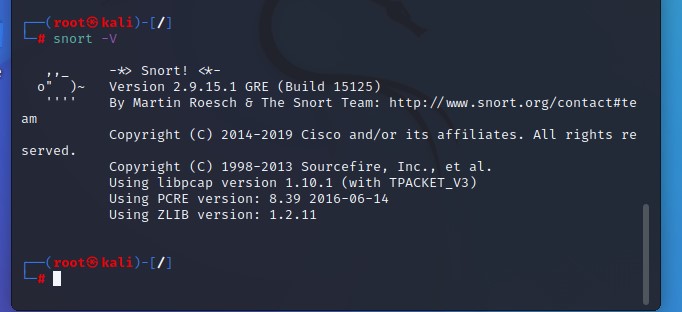
Burada ise “-A” parametresini kullanarak karşı tarafın genel olarak tüm bilgilerini toplamaya çalıştım karşıma ise böyle bir ekran çıktı.

Bu bilgileri aldıktan sonra karşı saldıracak olduğum makineye

Snort kuruyorum. Snort gelen ping veya benzeri saldırılarda çalışan uyarı sistemidir.

“apt-get ınstall snort diyerek kurulumu başlattım. Sonrasında bana configuration ayarlarını yapmamı isteyecek şöyle bir ekran çıktı.

Bu ekranda ip adres ağımı girdim. Sonrasında kurulum ekranı tamamlandı kurulup kurulmadığını öğrenmek için “snort -V” komutunu yazdım ve karşıma şöyle bir ekran çıktı başarılı şekilde kurulmuş. Aslında burada aldığım bilgi versiyon bilgisi.



Bundan sonra bazı ayarlar yapmam gerekti o ayarlar ise şöyle;

/etc/snort