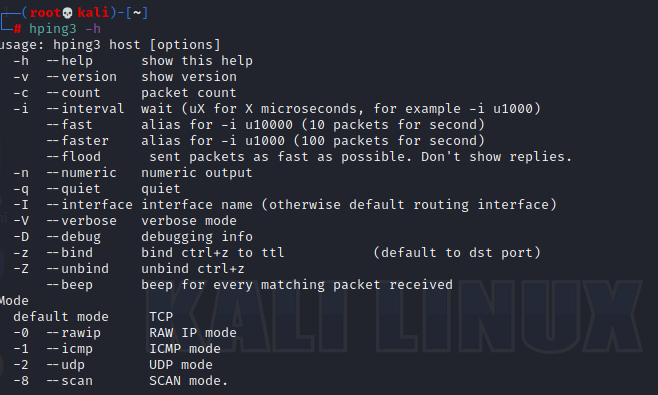
|  |
| --- |
| ***Hping3*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| -Ddos saldırılarında sıkça kullanılan bu araç ile Portlar üzerine saldırılar gerçekleştirip güvenlik testi gerçekleştireceğiz. |

**04.11.2021**

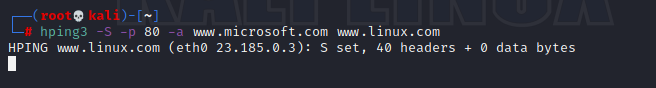
Hping3 ile IP Spofing

-Donanım ve yazılımları test etmemize olanak sağlar.

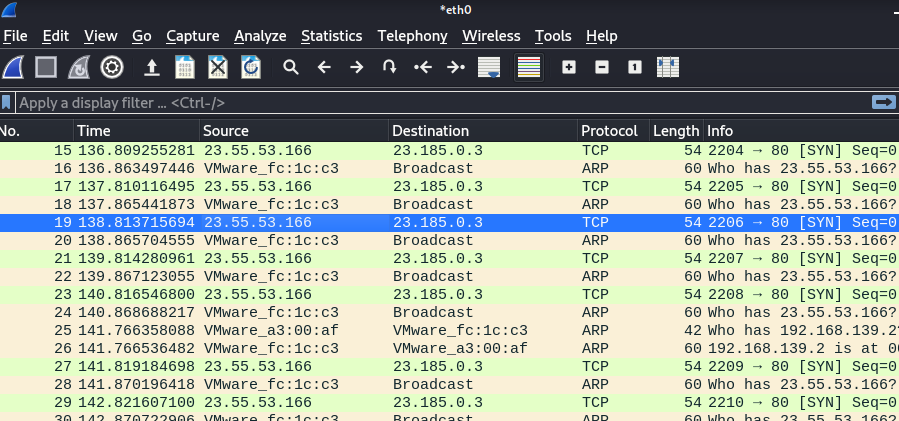
-Bu araç linux sürümlerinde kurulu olarak gelmektedir.



-Aracın kullanımı hakkında bilgi sahibi olmak için "hping3 -h" komutunu kullanıyorum.



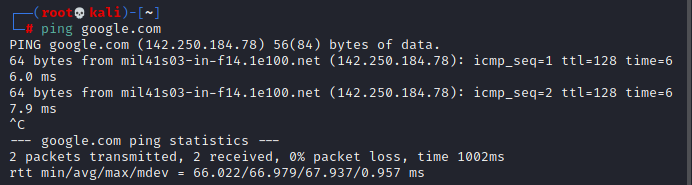
- Araç üzerinden Microsoft'a bir ping gönderme işlemi gerçekleştiriyorum.



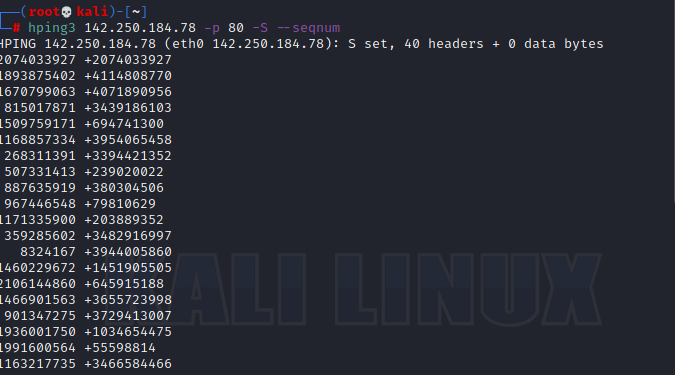
-Bu işlemi Wireshark üzerinden kontrol ettiğimde başarılı bir şekilde paket gönderdiğimi görebiliyorum.

Initial Sequence Number Attack

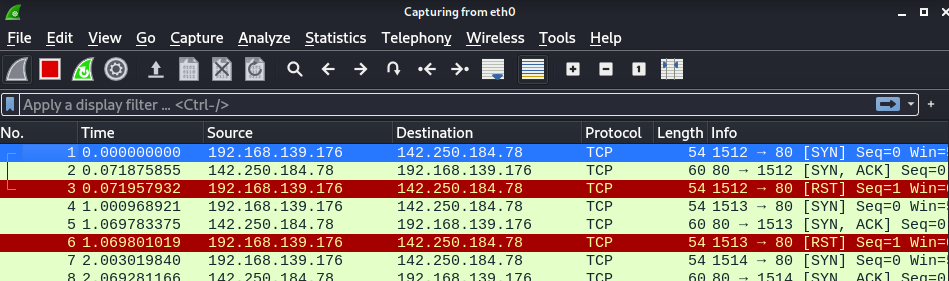
-TCP iletişiminde IP spoofing yapılıp yapılamayacağını öğrenmek için yapılan işlemdir.



-Öncelikle işlem gerçekleştireceğim Servisin IP adresini görüntülemek için ping gönderiyorum.



-Burada -S parametresi ile SYN paketleri gönderiyorum.Bu yazılım biçiminde bu işlemi başlatıyorum.

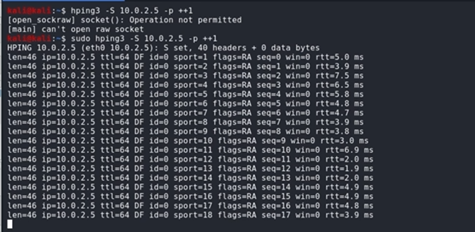


- Wireshark üzerinde de görüntülediğimde başarılı bir şekilde saldırı yapabildiğimi görebiliyorum.

-Bu şekilde değer yakalamak ve iletişim kurmak çok zor fakat imkansız değildir.

Port tarama

-Genellikle nmap aracı ile gerçekleştirdiğimiz bu işlemi hping3aracı ile de gerçekleştirebiliriz.



-Hping aracıyla yazmış olduğum komut ile 1.Porttan başlayıp sırasıyla arttırarak port'a istek atıp geri dönüş aldığı portlarda servis olduğunu döndürüyor.