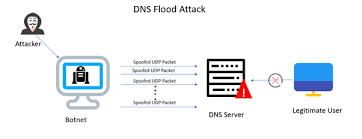
|  |
| --- |
| ***DDOS*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ*  -DNS Flood  -HTTP Get&Post Flood  -ICMP Flood  -IP Spoofing  -Syn Flood  -UDP Flood |
|  |

**06.08.2021**

***DNS Flood***

-Hedefe yoğun bir şekilde DNS paketleri göndererek devre dışı bırakma.

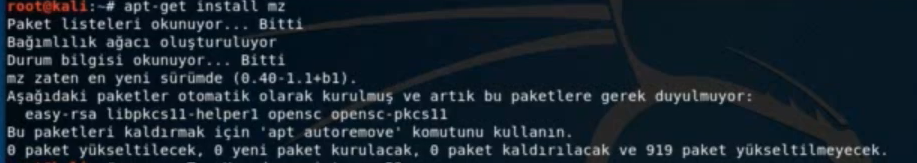


-Bu ugulama için “mz” ve tcpdump aracı kullanılacaktır.

-Bu uygulama için yüksek hızlı botnetler işlem gerçekleştirmektedir.

-DNS Server çökme durumunda içerisinde bulunan bütün web siteleri çöker ve erişim engellenir.

***Uygulama***



-Kullanacağımız araç mz aracıdır."apt-get install mz" komutu ile indirip kuruyorum.

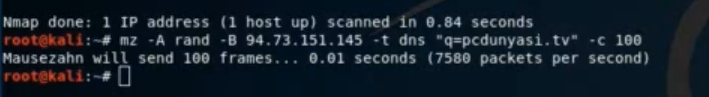


-Ardından hangi port üzerinden işlem yapacağımı bilmediğim için nmap ile bir tarama gerçekleştiriyorum ve açık olan portları görüntülüyorum.

-53.Portun aktif bir şekilde çalışmakta olduğunu görüyorum.

C:\Users\ogutk\AppData\Local\Microsoft\Windows\INetCache\Content.Word\4.png

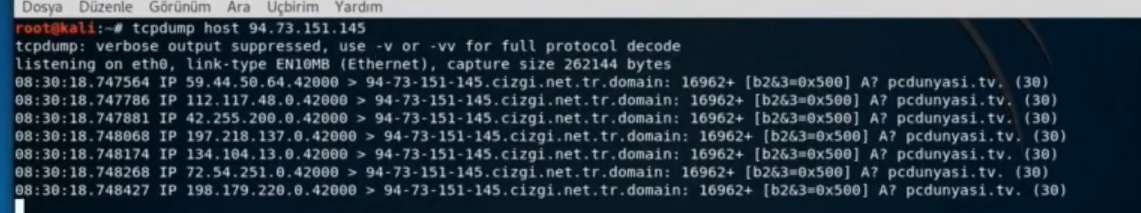
-Tcpdump aracı ile IP adresi üzerinden dinleme işlemini başlatıyorum.



-c komutu ile kaç adet paket göndereceğimi belirtiyorum.

-“-q=”Standart olarak gelmektedir burada sitenin ismini yazıyorum.

- “-A” random olarak farklı adreslerden gönderim yapacağımı belirtiyorum.

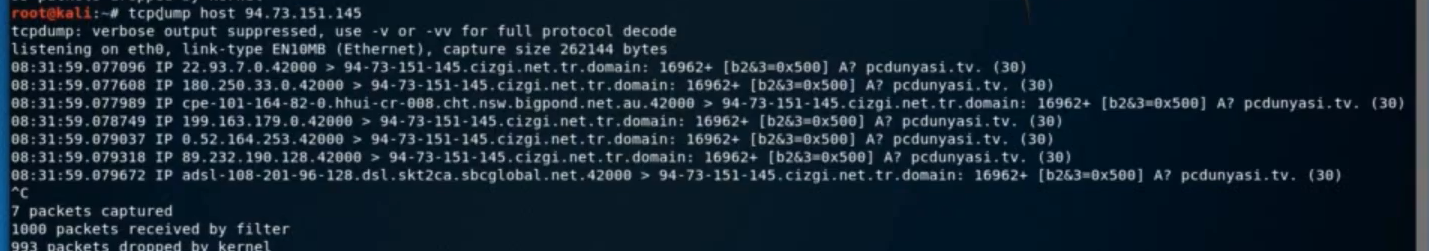


-Saldırı işlemi başladı fakat 7 adet paket gönderildiğini görüyorum.



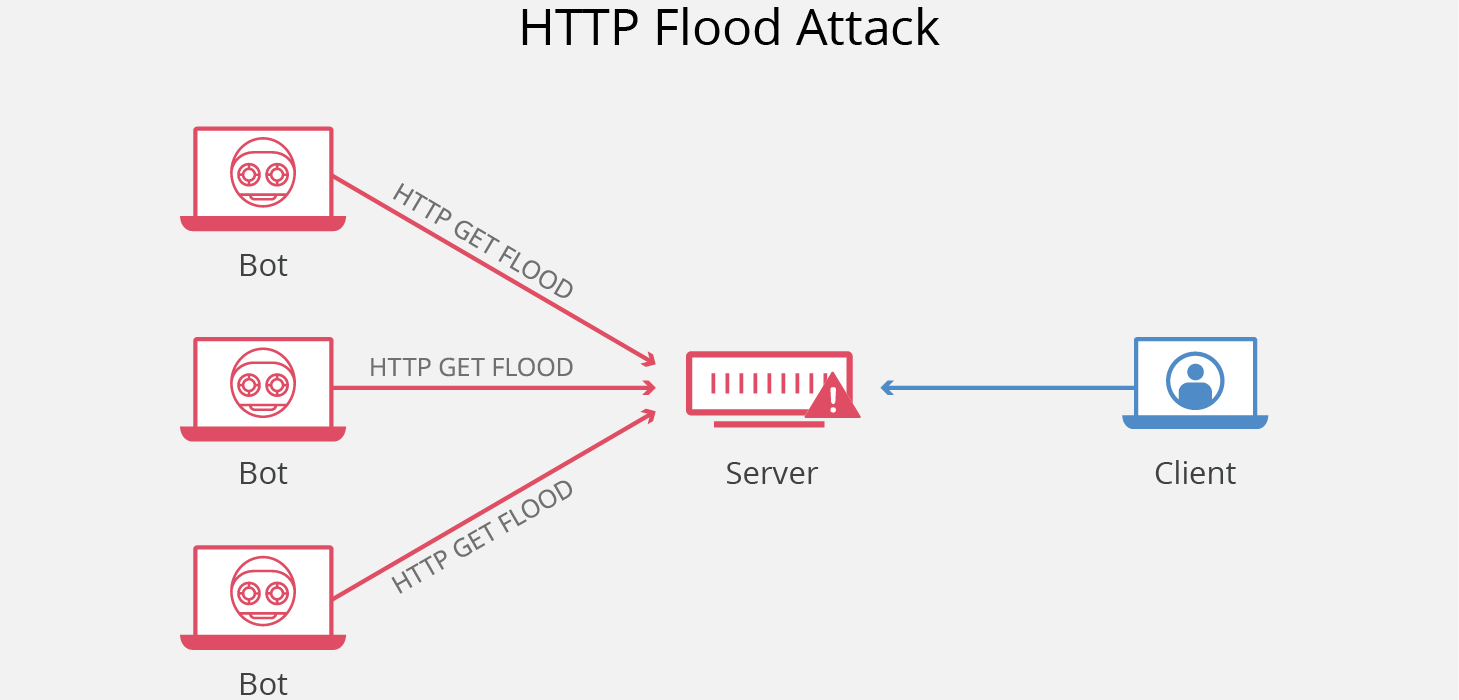
-İşlemi sonlandırdığımda bana vermiş olduğu yanıttan baktığımda 100 adet paket gönderdiğimi fakat 7 tanesinin geçtiğini ve diğerlerinin filtreye takıldığını görüntülüyorum.

-Paket sayısını arttırdığımda fazla paket geçip geçmeyeceğini deniyorum.



-Paket sayısını arttırsam da yine 7 adet paket geçme işlemi olduğunu görüntülüyor.

***HTTP GET&POST Flood***

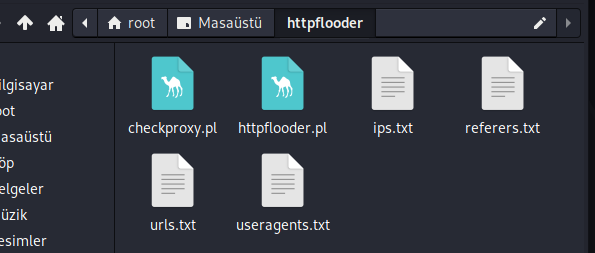


-Bu uygulamada amaç web sitesinin servis dışı bırakılmasıdır.

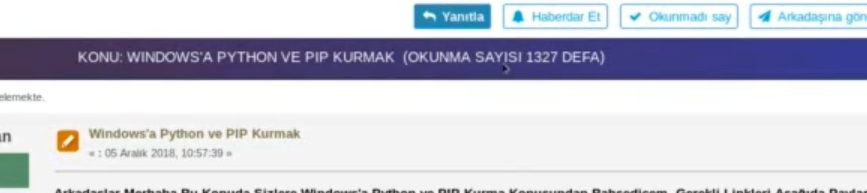
**HTTP Get :** -Sürekli yenileme işlemi gibi düşünebiliriz.Bir araç üzerinden sürekli sayfa yenilenmesi ile web sitesini çökertmeye yönelik bir saldırıdır.

**HTTP Post :** Yüzlerce bilgisayar ile bir sayfanın form kısmını doldurarak siteyi çökertmeye yönelik yapılan bir ataktır.

***Uygulama***

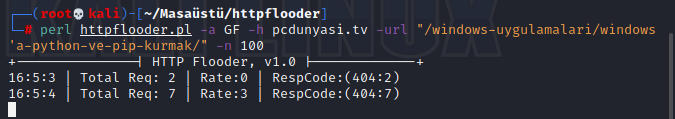


-Bu saldırı için HTTP flooder aracından yararlanacağız.Bu aracı "https://yadi.sk/d/O1PeDkSrVh9Evw" bağlantısı üzerinden indirebiliriz.



-İndirim sonrasında saldırı gerçekleştireceğim siteye geçiş yapıyorum.Burada sadece site üzerinde şu kadar okundu iletisinin olması yeterlidir.

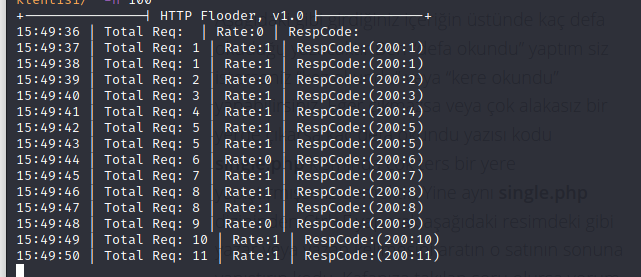
-Uçbirim üzerinden aracı çalıştıracağım.



-Perl komutu ile aracı başlatıyorum.

-GF=GetForce & “-h” parametresi ile host adresini belirtiyorum.

-“-URL” ile uzantı bilgilerini aktarıyorum. “–n” ile kaç kere yapılacağını belirtiyorum.

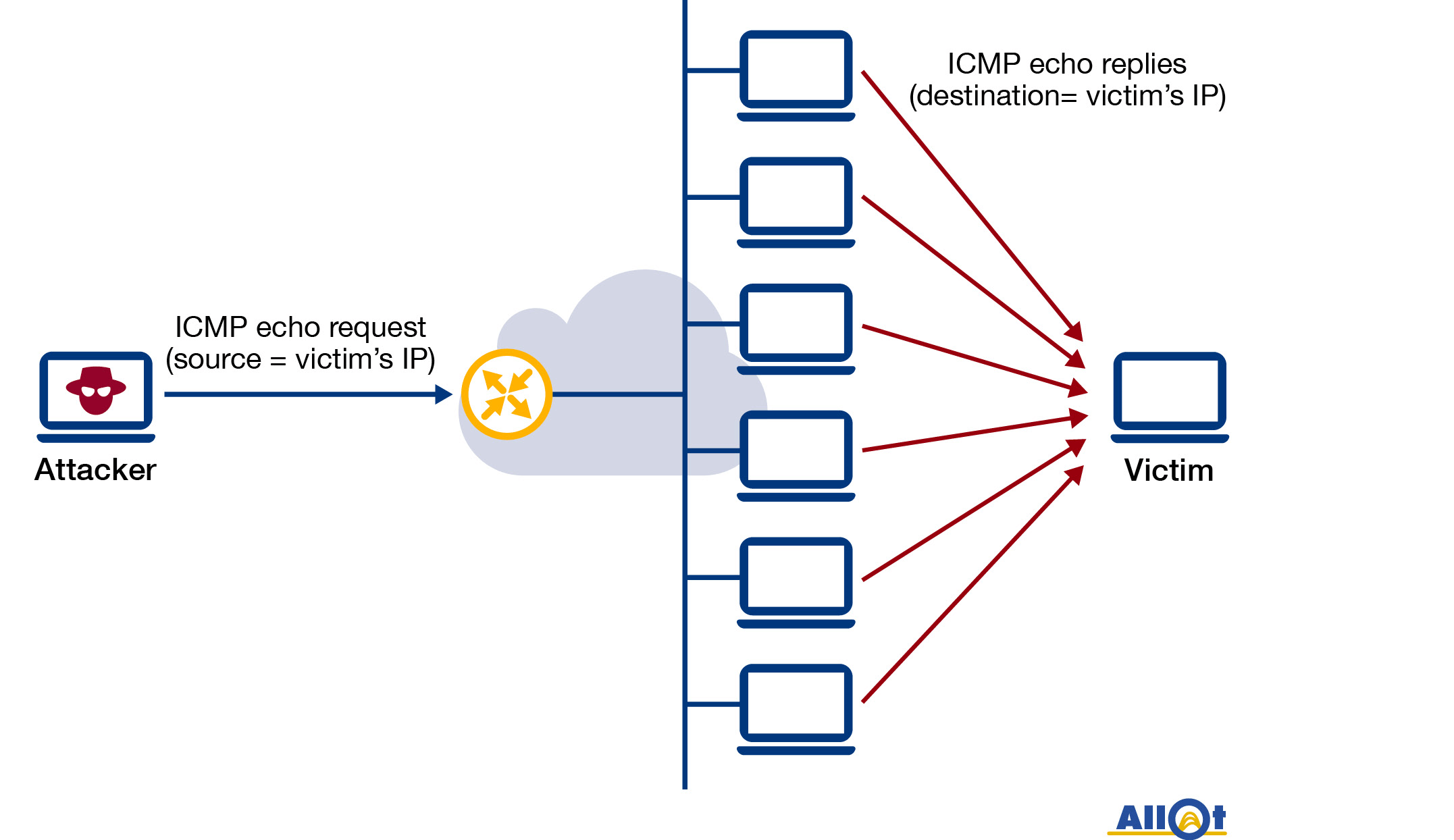


-İşlemin devam ettiğini buradan görüntülüyorum.”Req” sayısı n sayısına eşit olduğunda işlem başarılı bir şekilde tamamlanacaktır.



-İşlem bittiğinde siteyi kontrol ettiğimde işlemin başarılı bir şekilde gerçekleştiğini görüntülüyorum.

***ICMP Flood***

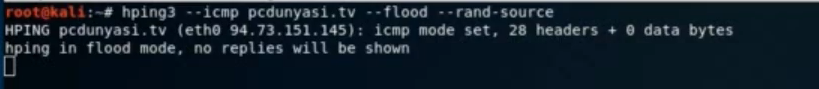


-Botnet üzerinden bir sorgu ve cevap alma şeklinde çalışan yapı üzerinden yapılan işlemdir.Sistem cevap verememeye başlayıp sistem çökecektir.

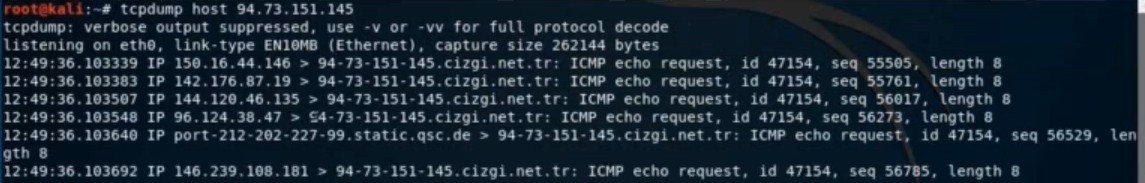
-Önce Hping3 ve Tcpdump araçları üzerinden işlem gerçekleştireceğim.Ardından alternatif araç olarak ICMPFlooder aracı ile işleme devam edeceğim.

***Uygulama***

-Bu saldırıya başlamadan önce Linux makinemi çalıştırıyorum ve uçbirimi açıyorum.



-İlk işlemi Hping ile başlatıyorum.Burada saldırı gerçekleştireceğim IP'yi kopyalıyorum.

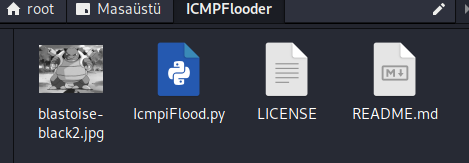


-Kopyaladığım Ip üzerinden dinleme işlemini başlatıp işlemin çalıştığını görüntülüyorum.

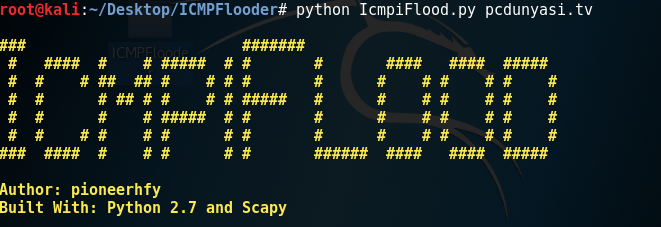
-Bu işlem Hping3 aracı ile basit bir şekilde yapılmaktadır.

-Eğer IP adresimizin gözükmesi problem olmaz ise “—rand-source” parametresini kaldırıp daha hızlı bir saldırı gerçekleştirebiliriz.

***ICMP Flooder***



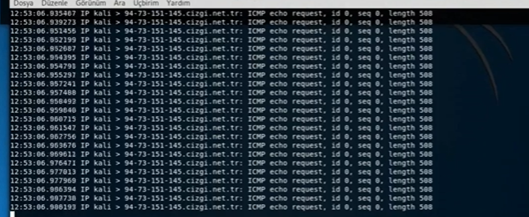
-"https://yadi.sk/d/rsKrTrL3bASWvg" bağlantısı üzerinden ICMPFlooder aracını indiriyorum.Dizinin içeriği bu şekildedir.



-Şimdi ise uçbirim üzerinden “python” komutu yardımıyla çalıştırıyorum.

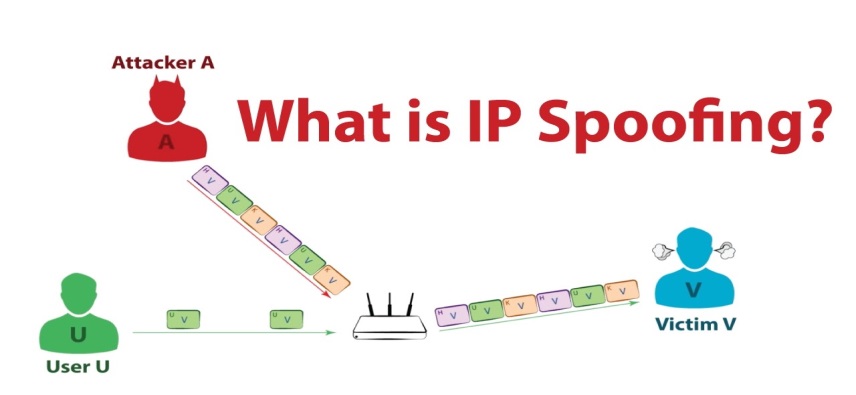


-Ardından pcdunyasi.tv adresini “tcpdump” üzerinden dinlemeye alıyorum.



-Ardından işlemin başarılı bir şekilde çalıştığını görüntülüyorum.

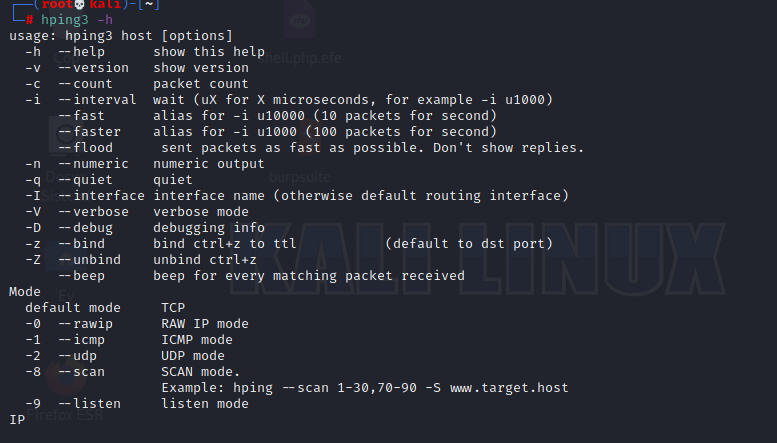
***IP Spoofing***



-Kullanacağımız araçlar hping3,tcpdump:Dinleme yapıp işlemin gerçekleşip gerçekleşmediğini görüntülüyoruz.

-Hping3 ve tcpdump aracı linux üzerinde kurulu olarak gelmektedir.

***Uygulama***

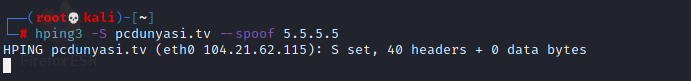


-Linux makineme geçiş yapıyorum ve uçbirimi açıyorum.

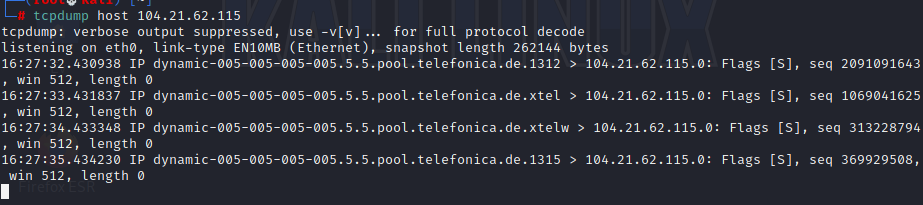
-Hping -h komutunu kullanıoyurm aracının kullanımını -h ile öğrenebilirim.



-Eğer bu şekilde işlemi başlatırsam kendi IP adresim üzerinden işlem gerçekleştirir.Benim istediğim IP adresimin gizlenmesi olduğu için sonuna “--spoof” parametresi ekliyorum.

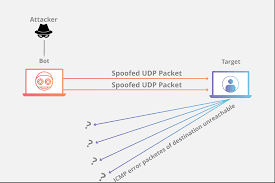


-Sonuna --spoof parametresi ile farklı bir IP adresi ekliyorum ve bu IP üzerinden işleme başlanacak.İşlem başladıktan sonra Eth0 Ip adresini kopyalıyorum.



-Ardından Tcpdump aracı ile dinleme işlemini başlatıyorum ve Başarılı bir şekilde saldırı gerçekleşiyor.

***UDP Flood***



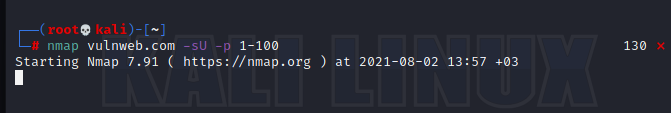
-Hedefe sürekli olarak UDP Paketleri göndererek Hedefin/Uygulamanın servis dışı bırakılması.

-İşlem bir botnet ağı tarafından yapılır.

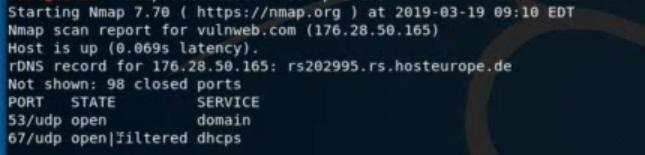
-Sistemde var olmayan bir adresi sorup sürekli sistemi oyalayarak yapılır.

-Bu işlem için hping3 ve tcpdump araçlarından yararlanacağız.Ayrıca alternatif olarak “mz” aracından da faydalanacağız.

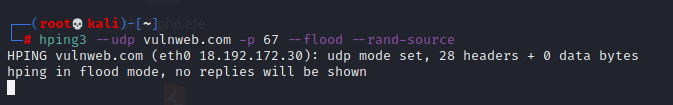
***Uygulama***



-Uçbirimi açıyorum ve saldırı yapacağım adresin UDP portlarını tarıyorum.Nmap vulnweb.com -sU komutu ile bakacağım ve.1-100 arasında ki hostları tarayacağım.



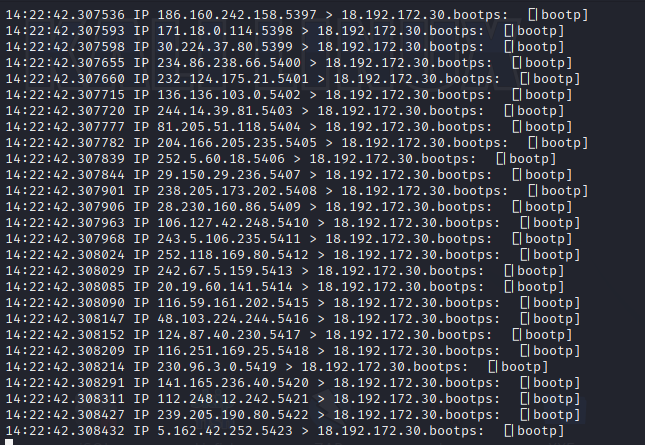
-Sonuçları döndürdüğünde 67. portun UDP olduğunu görüntülüyorum.



-Ardından hping3 aracı ile UDP üzerinden bir ddos atağı başlatıyorum.Saldırının başladığı IP'yi kopyalıyorum.

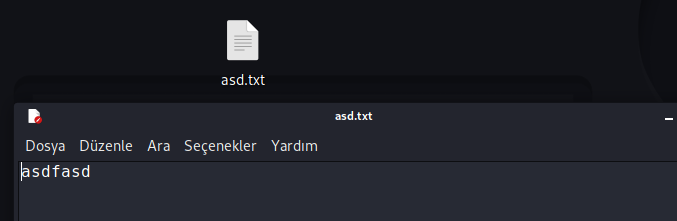


-Başlattığım atağı kontrol edebilmek için tcpdump aracı ile saldırı yaptığım IP'yi dinlemeye alıyorum.

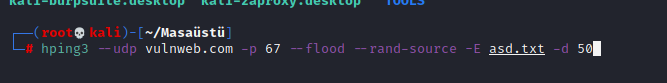


-Farklı IP'ler üzerinden saldırılar gerçekleştirdiğini görüntülüyoruz.

-Boş paketler gönderdiğimiz için Güvenlik duvarında bir engelleme olabilir.Bu sebeple paketleri gönderirken içerik ekleyebiliriz.



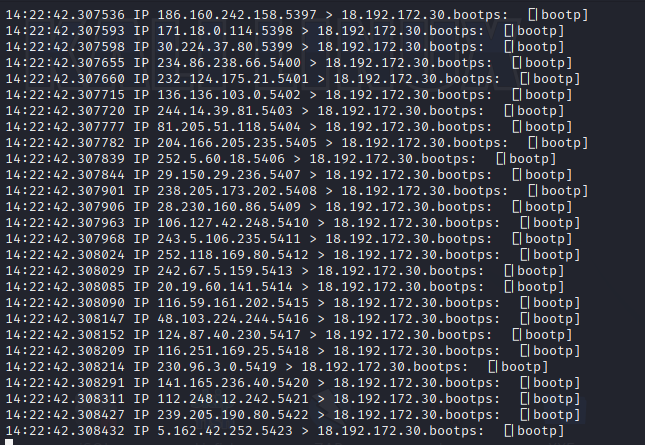
-Gedit komutu ile bir adet txt oluşturuyorum.İçerisine rastgele bir değer giriyorum.



-“--d “komutu ile boyutunun 50 bayt olacağını belirtiyorum.

-E komutu ile de .txt dosyamı ekliyorum.

-Aynı dizin üzerinde olmam gerekli ve işlemi başlattım.



-Bu şekilde boş paket göndermeyipte bu işlem gerçekleştirilebiliriz.