|  |
| --- |
| ***MSFVENOM*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| -Linux aracı üzerinde kurulu olarak gelen Msfvenom aracıyla Linux-Windows ve Android sistemlerde kullanılabilecek zararlı yazılım oluşturma işlemini birlikte yapacağız. |

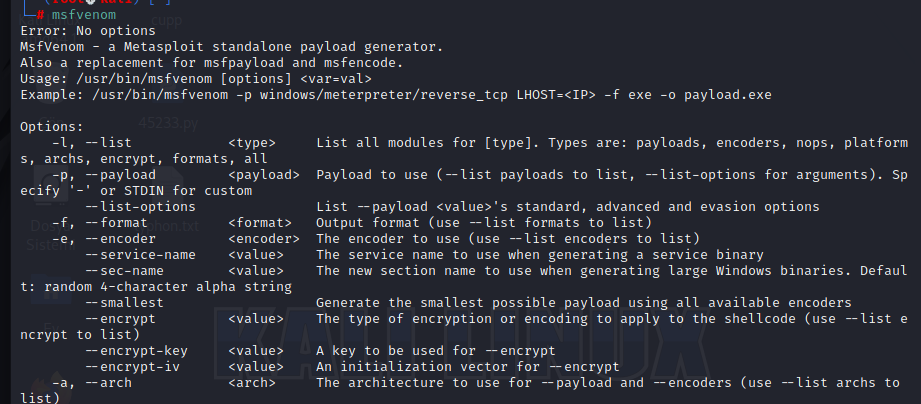
**09.08.2021**

***Msfvenom***

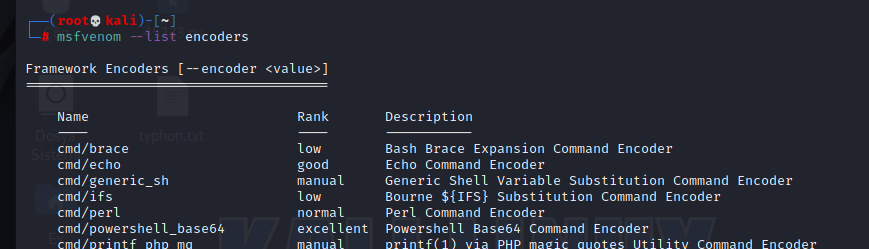
-Msfvenom linux makinelerinde kurulu olarak gelmektedir.

- Msfvenom üzerinden bir zararlı yazılım oluşturup test edeceğiz.

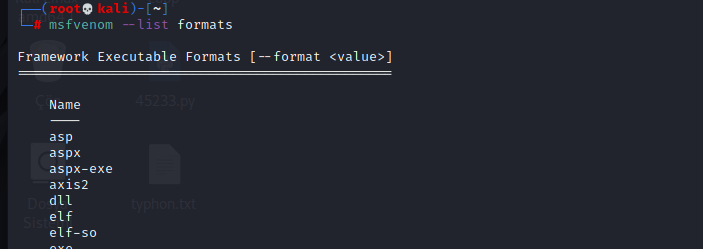
-Uçbirim üzerinde msfvenom ile aracı çalıştırıyorum.



-Bizim bu uygulama için kilit işletim sistemlerimiz Windows,Linux ve Android olacaktır.



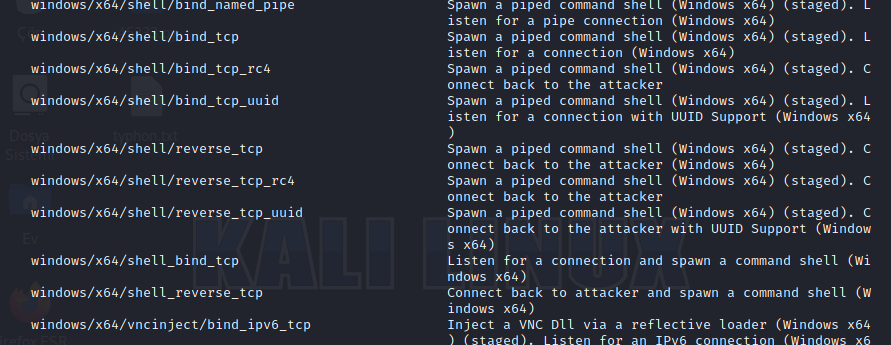
-“list –encoders” komutu ile Encode tekniklerini görüntüleyebiliyorum.



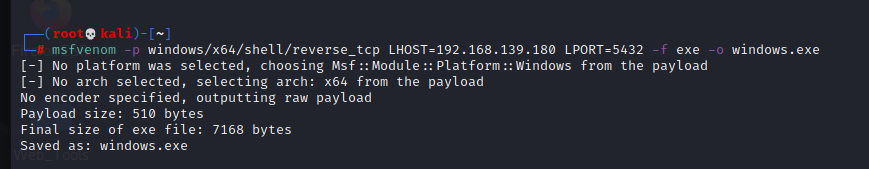
-“list –format” komutu ile Format teknikleri hakkında bilgi toplayabiliyoruz.

***Windows için Zararlı Yazılım***

-Windows işletim sistemlerinde uygulayabileceğim bir zararlı yazılım yazmak istiyorum.



-“msfvenom -l payloads” komutu ile Msfvenom üzerinde kullanabileceğim tüm payloadları görüntüleyebiliyorum.

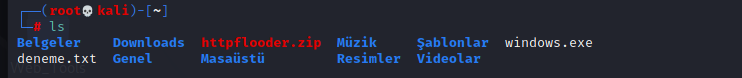


-Burada işlemler kendi Localim üzerinde gerçekleşeceği için LHOST= ayarını belirtmem gerekiyor.

-Eğer dış ağ üzerinde bir işlem gerçekleştireceksek Modemin IP adresi üzerinden port için işlem yapmamız gerekiyor

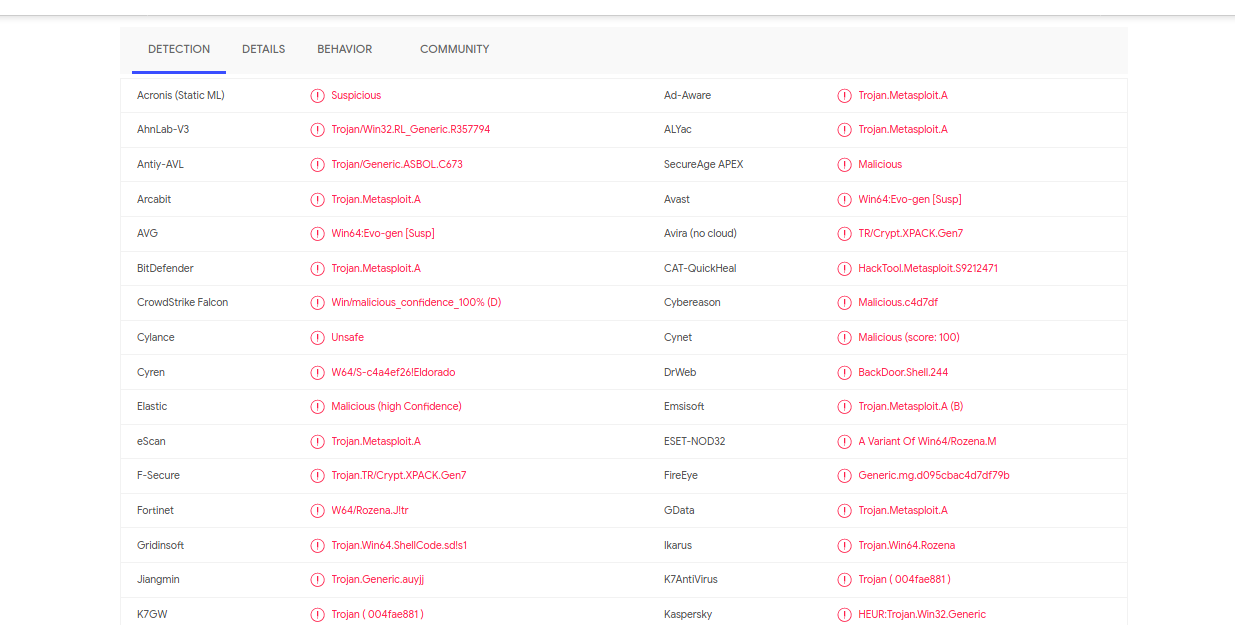
- “-f” parametresi ile oluşturacağım yazılımın uzantısını belirtiyorum.

-Başarılı bir şekilde zararlı yazılımı oluşturdum.



-“-Ls“ komutu ile baktığımda bulunduğum dizin içerisine oluşturduğunu görüntülüyorum.

-Şuan bu oluşturduğum virüsü öncelikle “Encode” etmeden “Virustotal” üzerinde denetleyeceğim.



-Ekran üzerinde görüntülediğim de virüs programlarının çoğunun bu virüsu tespit ettiğini görüntülüyorum.

-Genellikle “Trojan/Worm” olarak algılandığını görüntülüyorum.

-Bir sonraki uygulamamızda Encode işlemi gerçekleştirip tekrar test yapıp sonuçlarını görüntüleyeceğim.

***Windows için Zararlı Yazılım ve Encode***

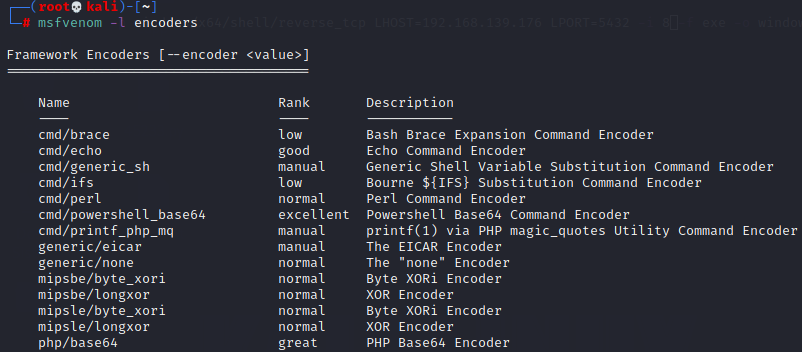
-Önceki uygulamamızda Encode işlemi gerçekleştirmeden zararlı yazılım oluşturduğumuz için bu işlemi atlıyorum.



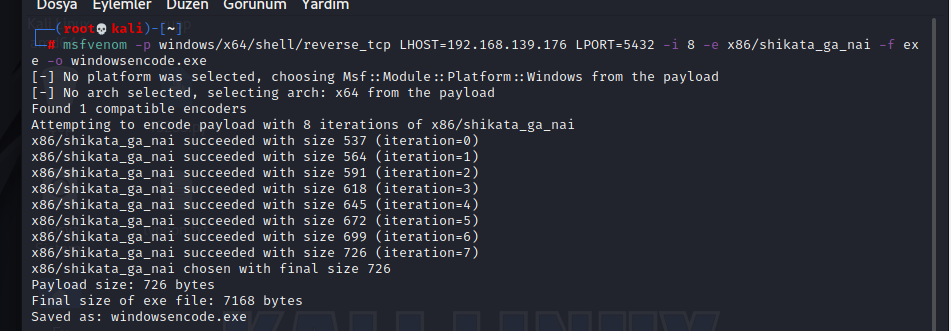
-Encode işlemsiz oluşturduğumuz zararlı yazılım haricinde sadece 2 adet parametre ekliyorum.

-“-i” parametresi ile kaç kere Encode edeceğimizi belirtiyoruz.Üst üste encode ederek çözülmesi o kadar zor olacaktır.

-“-e” parametresi ile Encode türünü belirtiyorum.Bunun hakkında giriş kısmında bilgi vermiştik.

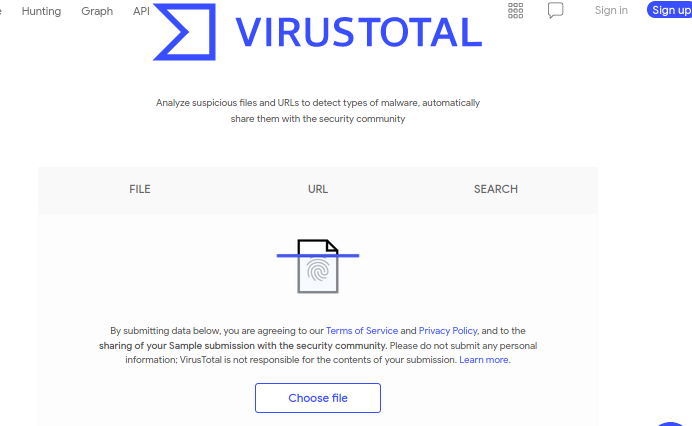


-Tekrardan göstermek istedim.

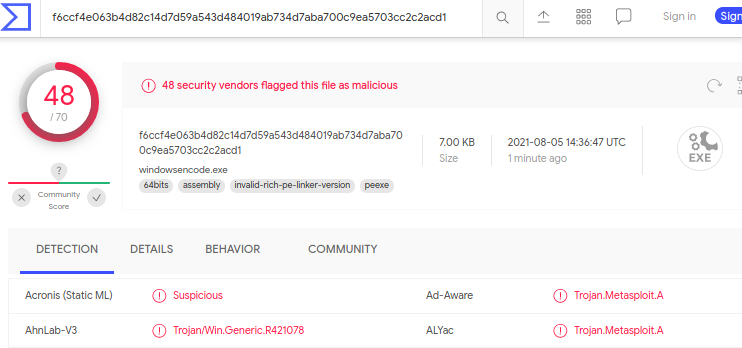


-Zararlı yazılımı başarılı bir şekilde oluşturdum.

-Şimdi sıra “Virüstotal” üzerinde bir deneme yapmakta;

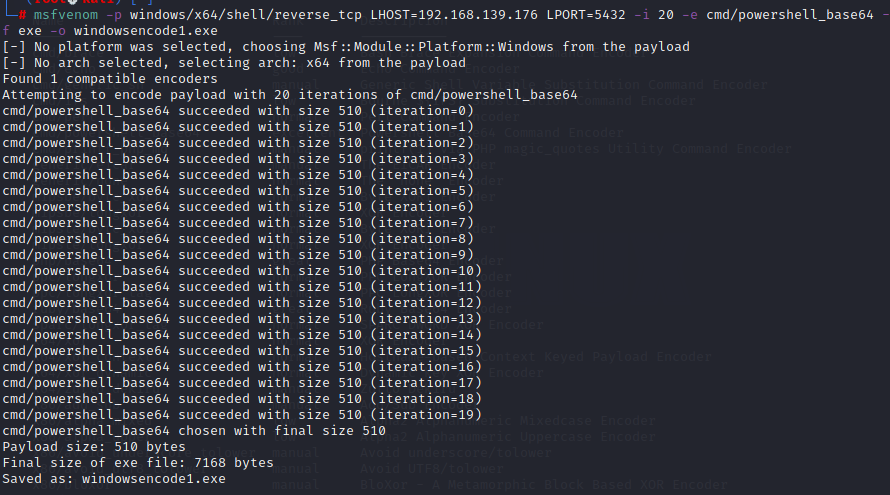


-Tarayıcı üzerinde Virüstotal’i açıyorum ve buraya oluşturduğum zararı yazılımı upload ediyorum.

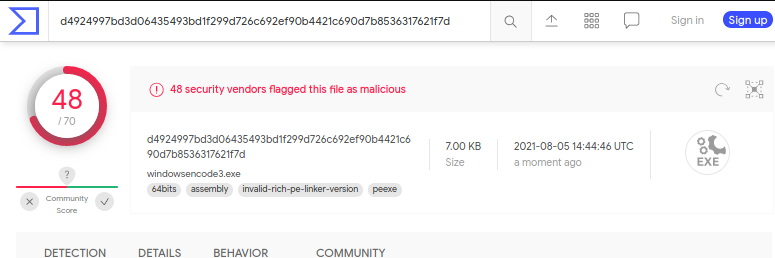


-Encode etmeme rağmen başarılı olmadığını görüntülüyorum.

-Bu sefer farklı bir Encode tekniği ile Encode etme sayısını arttırıp tekrar deneyeceğim.

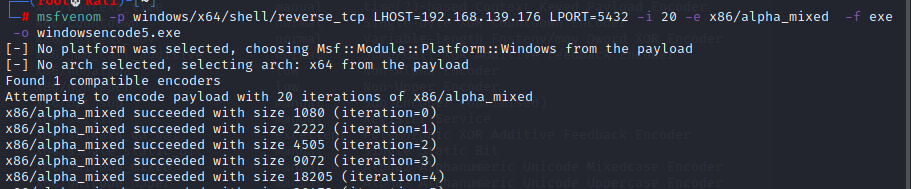


-Farklı bir Encode tekniği ve fazla Encode sayısı ile tekrar bir zararlı yazılım oluşturdum.

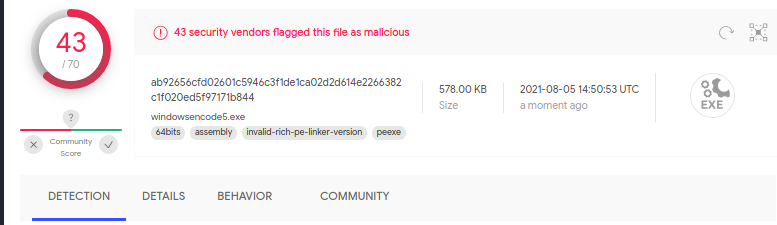


-Oluşturduğum zararlı yazılım tekrardan analiz ediyorum.

-Sonuçlarına baktığımda bir değişiklik göremedim.



-Bu sefer “low” derecesinde bir encode tekniği deneyerek işlemi gerçekleştireceğim.İşlemi başlatıyorum.



-Ardından tekrar “Virüstotal” üzerinden deneme gerçekleştireceğim.

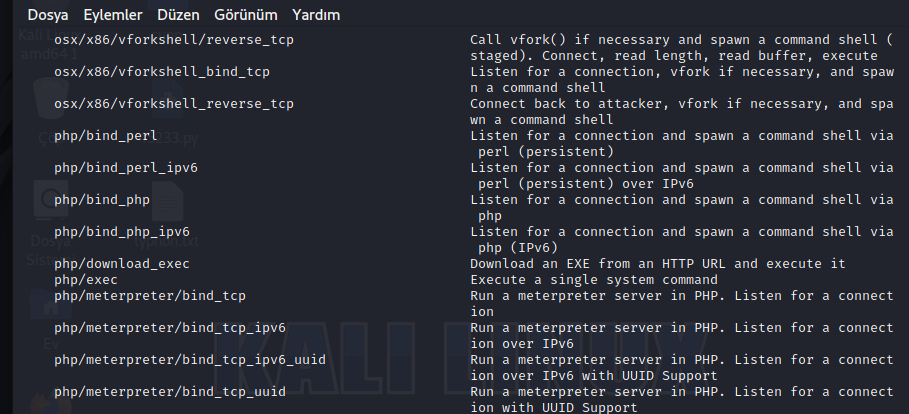
-Bunda da baktığımda sonucun çok değiştiğini gözlemleyemedim.

-MSFvenom aracı çok popüler bir araç olduğu için artık üzerinde ki tüm zararlı yazılımları Antivirüs şirketleri eklemiş.

-Bu sebeple zararlı yazılım oluşturmak için kullanılan “Veil Framework” aracından yararlanabiliriz.

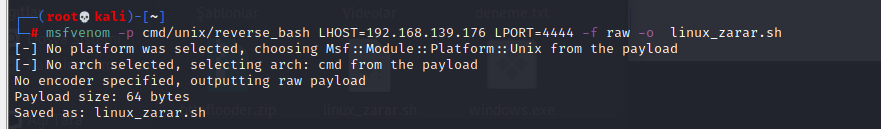
***Linux için Zararlı Yazılım ve Encode İşlemi***

-Windows için bir zararlı yazılım oluşturduğumuz gibi Linux içinde bir zararlı yazılım geliştireceğiz.



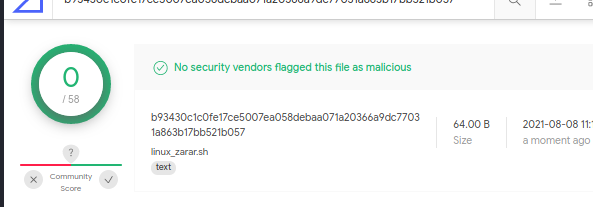
-"msfvenom -l payloads" komutu ile öncelikle msfvenom üzerinde ki payloadları görüntülüyorum.

-Bash formatında bir yazılımın daha etkili olacağını düşündüğüm için "cmd unix bash"'i seçiyorum.



-Çalıştırılabilir olması için "raw" dosya formatında oluşturuyorum

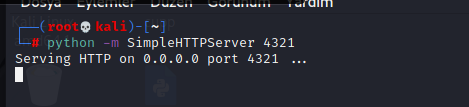
-Zararlı yazılımı oluşturdum şimdi ise virüs total üzerinden tarama gerçekleştireceğim.



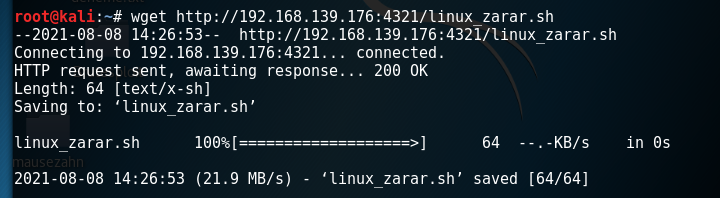
-Hiçbir Encode işlemi bile gerçekleştirmediğim halde Virüs'ü algılayamadı.Bu yüzden bu işlemler için Linux kanalının kullanılması çok mantıklı olacaktır.

-Şimdi Cihazım üzerinde başka bir Linux makineyi çalıştırıp oluşturduğum zararlı yazılımı burada çalıştıracağım.

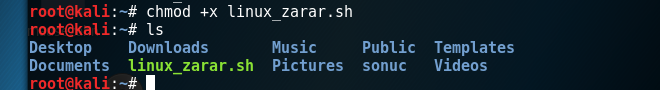
-Bunun için HTTP server kullanacağım önce HTTP Server'ı başlatıyorum.



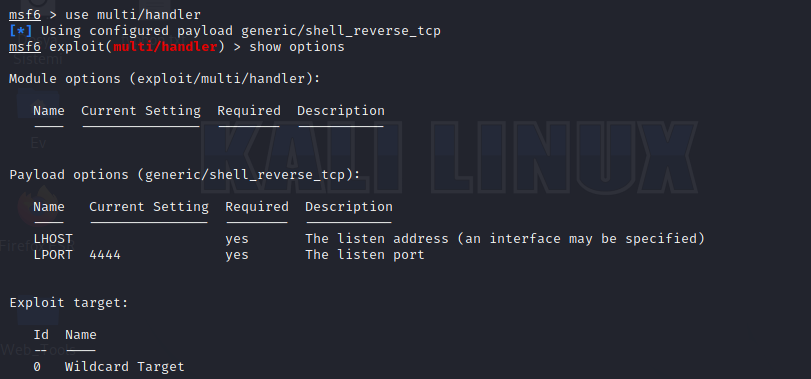
- Diğer sanal makineme geçiş yapıyorum ve uçbirim üzerinden “wget” komutu ile indirme işlemini gerçekleştiriyorum.



-İndirme işleminin gerçekleştiği makine üzerinde bu dosyayı çalıştırma ihtimalini düşünüyorum.



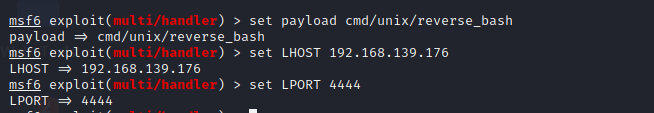
- Chmod ile çalıştırma yetkisi veriyorum ve başarılı bir şekilde görüntülüyorum.



- Zafiyet gerçekleştireceğim makineye geçiş yapıp burada Metasploit'i başlatıyorum.

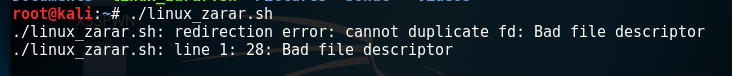
-Multi/handler scripti üzerinden işlem gerçekleştireceğim

-“Show options” ile de gerekli ayarları görüntülüyorum.



- Buraya kullandığım Payload'ı ,LHOST ve LPORT adreslerini set ediyorum.

-Bu işlem sonucunda kendi IP adresimi dinlemeye alıyorum.



- Dosyayı aktardığım diğer sanal makinem üzerinden çalıştırma işlemini gerçekleştiriyorum.

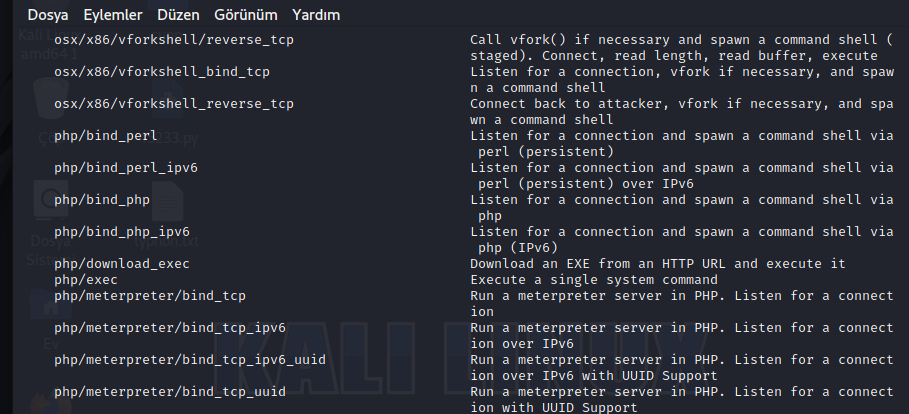


-Encode etme işlemi gerçekleştirmeden bile şuanda ” shell“ aldım ve bütün istediğim işlemleri gerçekleştirebiliyorum.

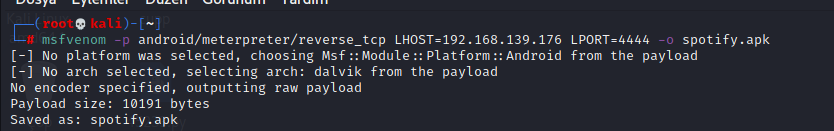
-Linux makineleri üzerinde zararlı yazılım ile zafiyet kullanma işlemi hiçbir güvenlik engeline takılmadan gerçekleştirilebilmektedir.

***Android için Zararlı Yazılım ve Encode İşlemi***

- Windows ve Linux üzerinde de oluşturduğumuz gibi burada da “msfvenom” aracı ile bir zararlı yazılım oluşturacağız.



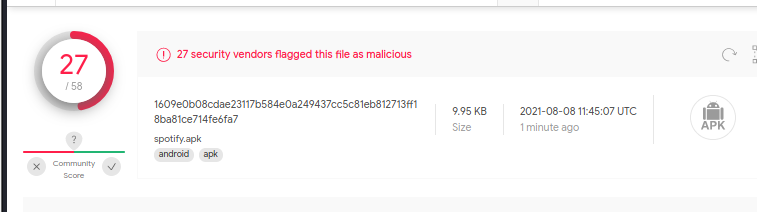
-“Msfvenom -l payload” komutu ile payload listesini görüntüleyebiliriz.



- Bu liste içerisinden "android/meterpreter/reverse\_tcp" scripti ile devam edeceğim.

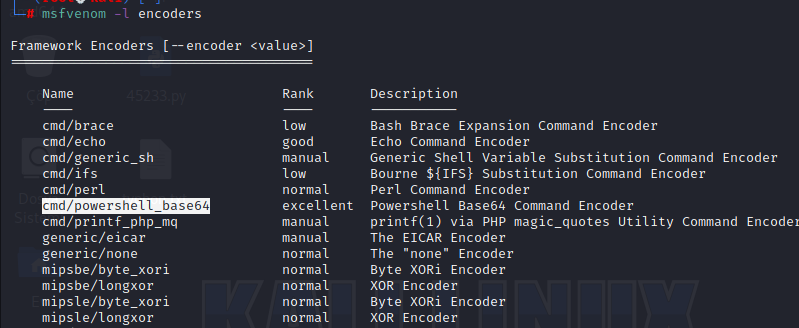
-Burada “-f” parametresi ile dosya türünü belirtmeme gerek yok.

-Ardından oluşturduğum zararlı yazılımı “virüs total” üzerinde tarıyorum.

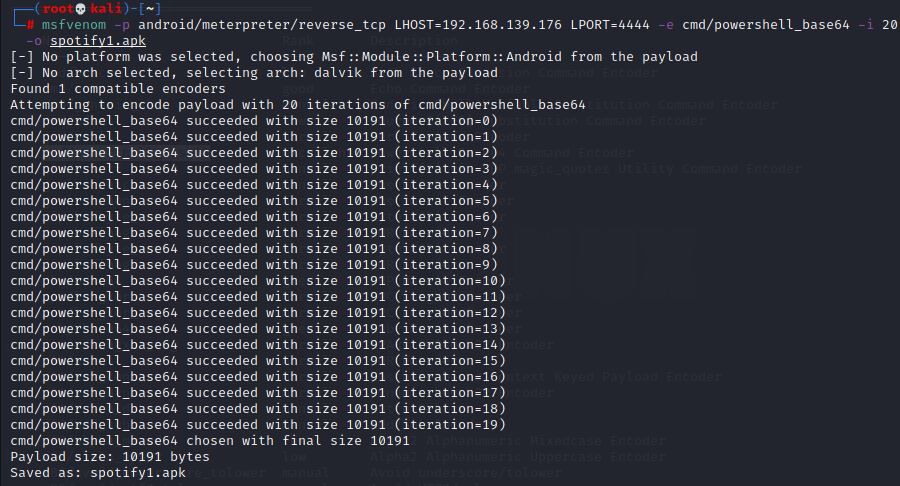


-Arama sonucunda 58 Virüs aracından 27 tanesi bu zararlı yazılımı tespit edebildi.

-Bu işlemi birde Encode etikten sonra denemek istiyorum.

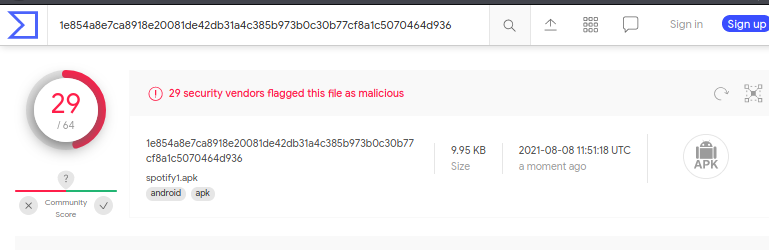


- Encode işlemi için buradan bir Encode türü seçiyorum.

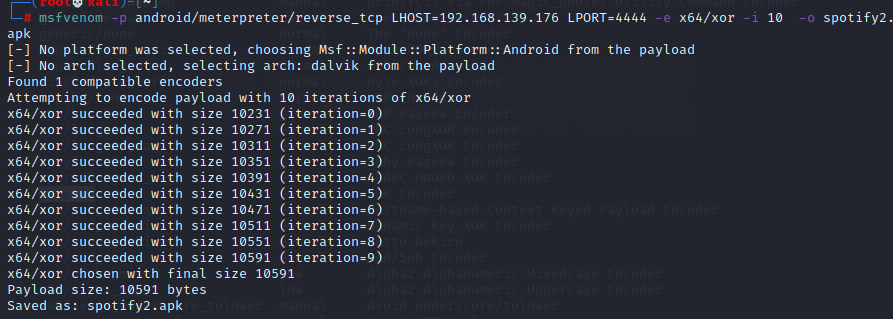


-20 Kere Encode etme işlemini gerçekleştirdim.

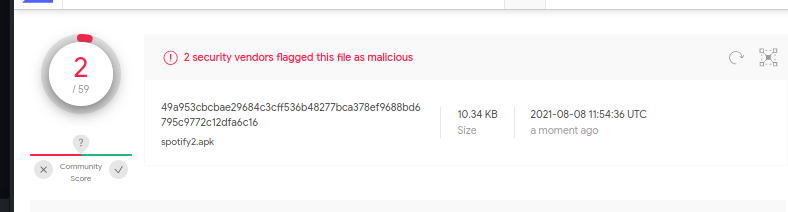
-Zararlı yazılımımı oluşturdum şimdi ise sırada bunu “Virüstotal” üzerinden taramak var.



- Yaptığım Encode sonrası aldığım sonuç çok tatmin etmediği için başka bir Encode türü daha denemek istiyorum.



-"Xor" encode türü ile bir zararlı yazılım daha oluşturdum.



- Bu zararlı yazılımı Virüstotal üzerinden tarattığımda sonuç bu şekildedir.Sonuç son derece tatmin edici oldu.

-Msfvenom üzerinde oluşturduğum.Normal derecede bir encode yöntemiyle bu sonucu almam çok şaşırtıcı.

-Windows üzerinde ne kadar başarılı olsa da Linux ve Android üzerinde çok başarısız olduklarını görüntüleyebiliyorum.