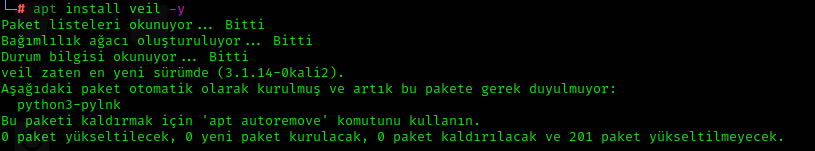
|  |
| --- |
| ***Trojan-Embed File*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| Veil Framework aracı ile Trojan oluşturup bunu embed file yöntemi ile gizleyerek antivirüs atlatmaya çalışacağım. |

**07.01.2022**

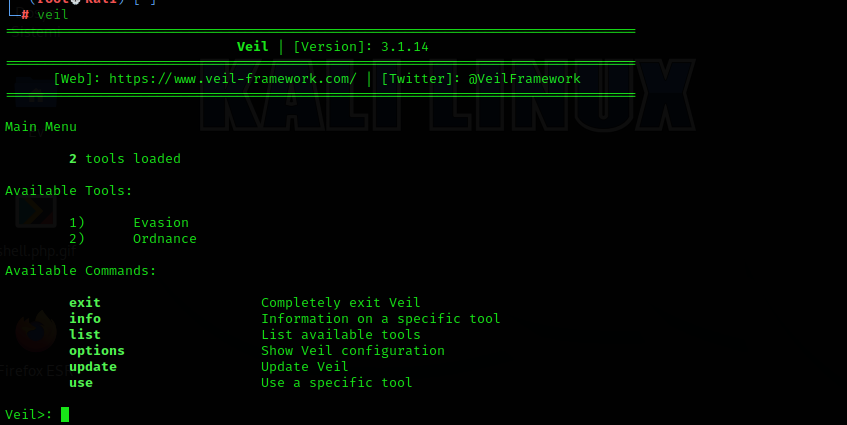
***Veil Framework Kurulumu***

-Linux üzerinde bulunan msfvenom aracıyla daha önce zararlı yazılım oluşturmuştuk.

-Bu sefer bu işlemi "Veil Framework" aracı ile gerçekleştireceğiz.Bu araç ile virüs atlatmalarını çok daha kolay gerçekleştireceğiz.



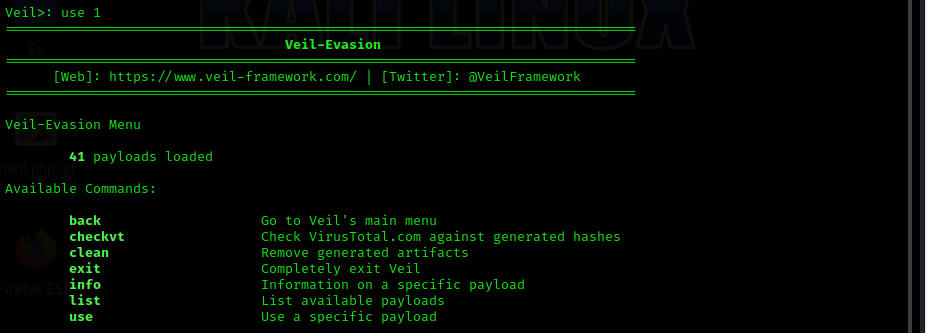
- Aracı "apt install veil -y" komutu ile kurabiliriz.Linux kütüphanelerinde mevcuttur.



- Ardından uçbirim üzerinde çalıştırdığımız "veil" komutu ile aracın kullanımı hakkında bilgi sahibi oluyorum.

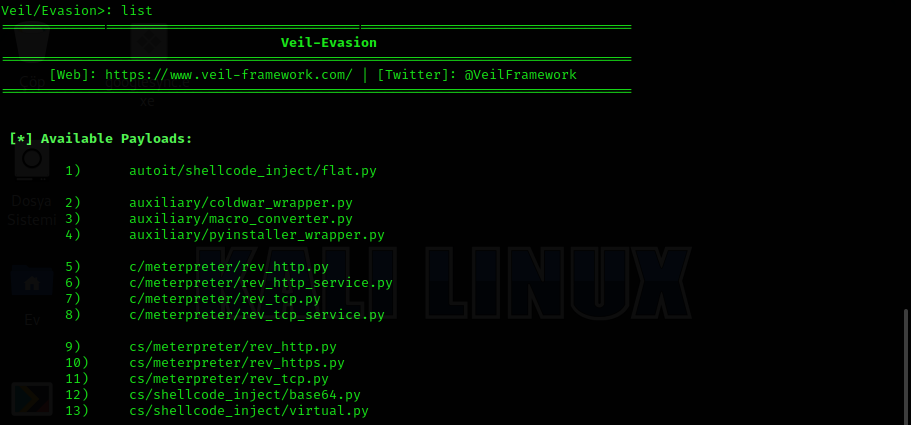
***Trojan Oluşturma***

-Veil aracını çalıştırdığım da kullanılabilir "Evasion ve Ordnance" araçları olduğunu görüntülüyorum.

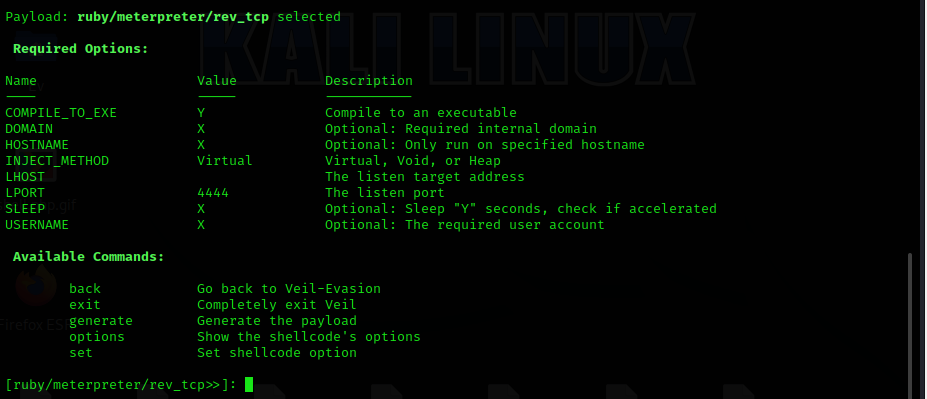


- Evasion seçeneği ile devam etmek için "use 1" komutunu çalıştırıyorum.

-Ardından bana kullanabileceğim seçenekleri gösteriyor.



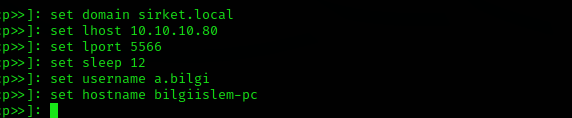
- List komutu ile kullanabileceğimiz payloadları bize listeliyor.



- Ruby dili ile yazılmış reverse\_tcp ile işlemlerime devam ediyorum.

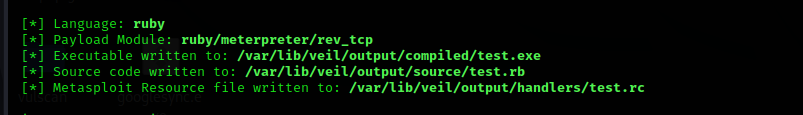
-Burada metasploit aracının arayüzüne benzer bir şekilde yapmamı istediği değişiklikleri görüntülüyorum.

-Burada değiştirebileceğimiz tüm ayarları değiştirirsek antivirüsü atlatmak daha kolay olacaktır.

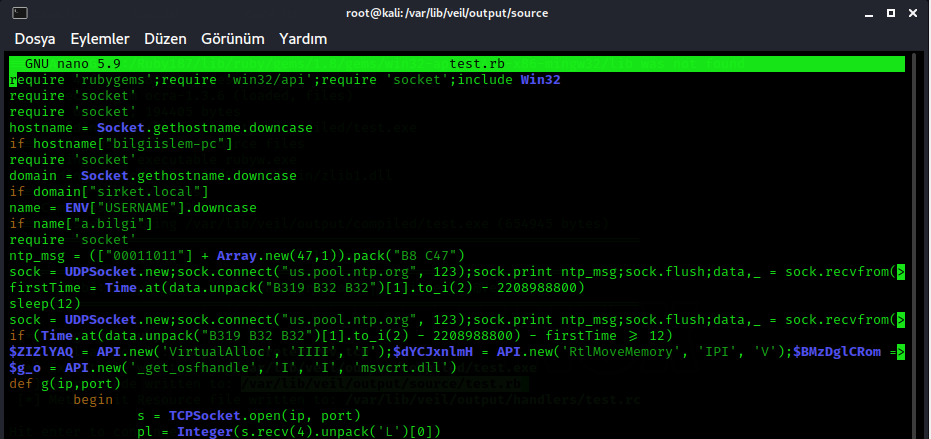


- Metasploit üzerinde yapmaya alışık olduğumuz gibi bilgileri buraya set ediyorum.

-Burada ne kadar değer verirsem ve farklı olursa antivirüs'e takılma oranım o kadar düşecektir.



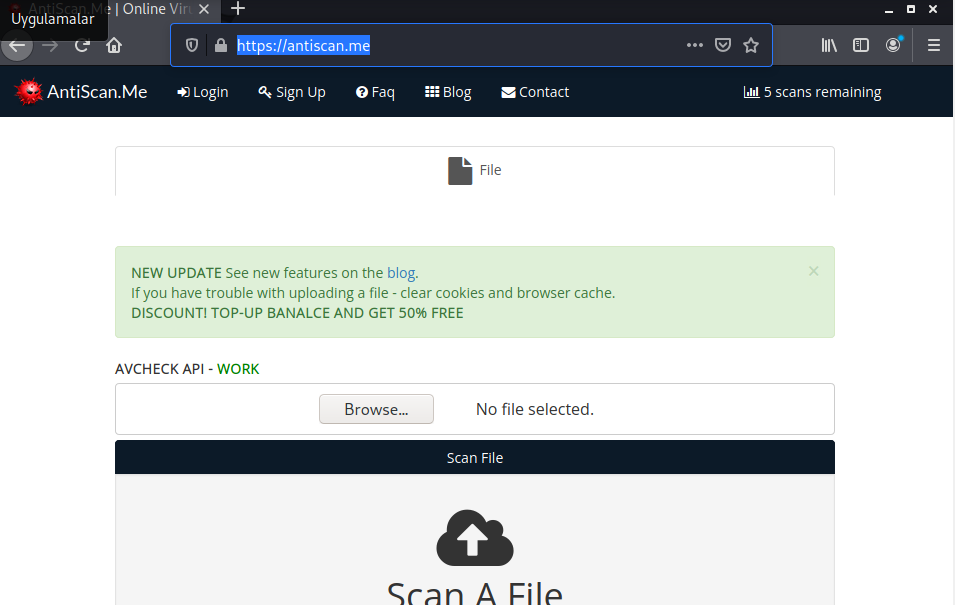
- Generate komutu ile zararlı yazılımı oluşturuyorum.



- Oluşturduğum zararlı yazılımın kod halini burada görüntülüyorum.

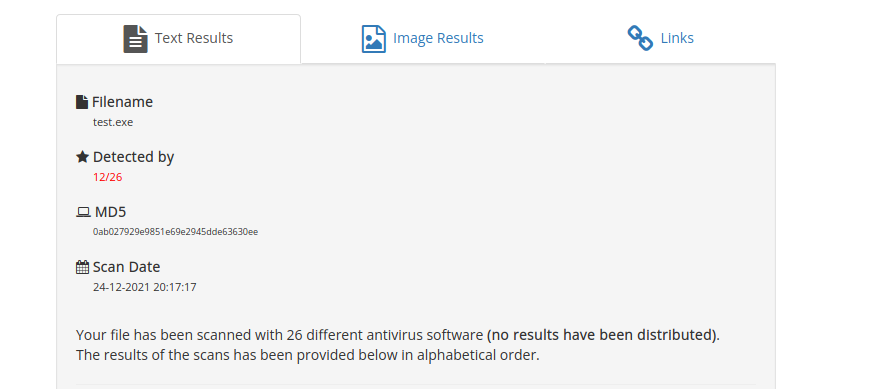
***Trojan Test Etme***

-Tarayıcı üzerinden hazırladığımız zararlı yazılımları test edebilirim fakat çoğu site oluşturulan zararlı yazılımları antivirüs firması ile paylaşır.



-"https://antiscan.me/" online olarak tarama gerçekleştirip antivirüs şirketleri ile paylaşmayan siteler üzerinde bilinenlerdendir.

-Sitenin arayüzü bu şekildedir.

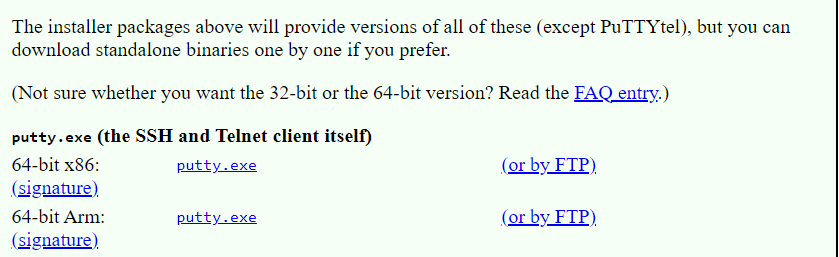


-Oluşturduğum zararlı yazılımı bu tarayıcı üzerinde test ediyorum fakat 26 antivirüsten 12 tanesine yakalandığını görüntülüyorum.

-Burada başarıyı arttırmak için kaynak kodları üzerinde oynama yapmak gerekmektedir.

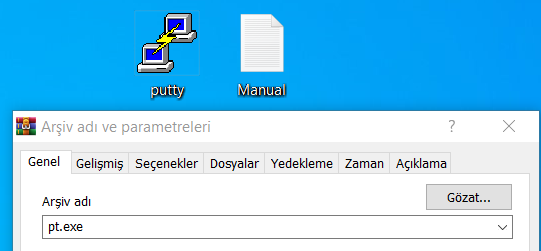
***Embed File Oluşturma***

-Gömülü şekilde trojan hazırlamak için bir exe dosya yanına da bir .txt dosyası açıldığını düşünelim.



-Bu işlem için daha önce SSH bağlantısı kullandığım "PuTTY.exe" aracından yararlanacağım.

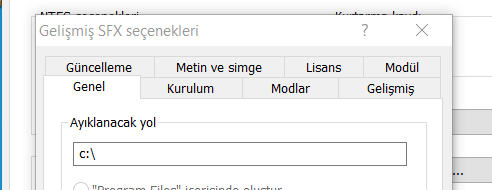
-Öncelikle PuTTy aracını indiriyorum.



-Bu aracın yanına bir .txt dosyası ekliyorum.

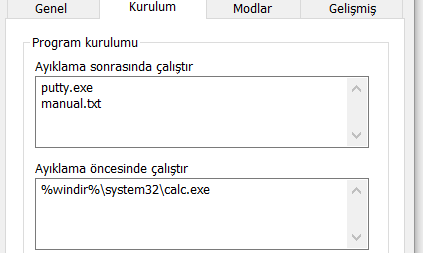
-Ardından "WinRAR" yardımı ile bu dosyayı rar haline getiriyorum.

-Burada "SFX Arşivi oluştur" seçeneğini belirtiyorum.Bu seçenek ile .exe haline geldi.



-Winrar üzerinde gelişmiş seçeneğine geçiş yapıyorum.

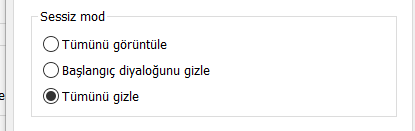
-Gelişmiş SFX seçenekleri üzerinde "c:\" yolu içerisine ayıklayacağını belirtiyorum.



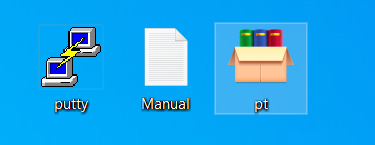
-SFX Seçenekleri üzeride kurulum kısmına geçiş yapıyorum.

-Burada ayıklama sonrasında çalışacak "putty.exe ve manual.txt" dosyalarını belirtiyorum.

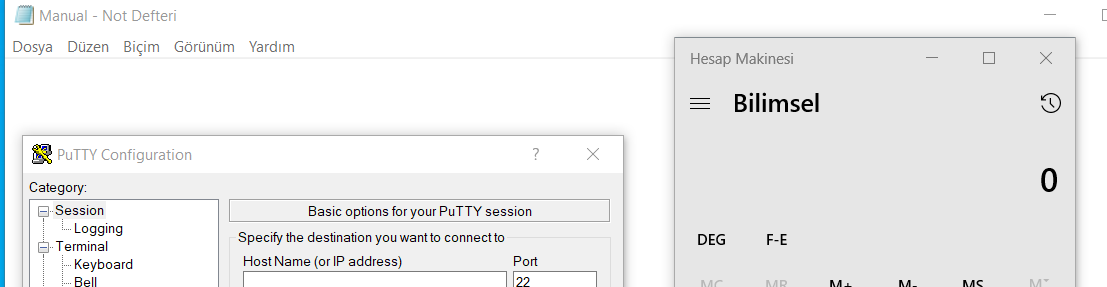
-Ayıklama öncesinde ise calculator çalıştırmasını istiyorum.



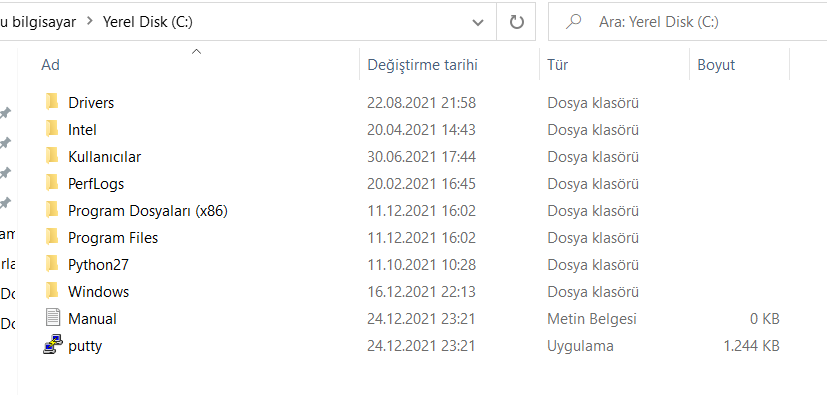
-"Sessiz Mod" üzerinde çalışma esnasında nereye çıkaracağını kullanıcıya sormaması gerektiğini belirtiyorum.



"WinRAR" aracı ile "pt.exe" uzantısını oluşturdum sıra geldi test etmeye;



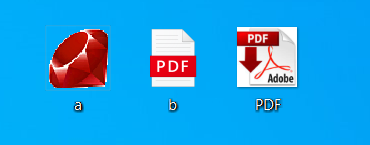
-Oluşturduğum aracı çalıştırıyorum ve çalışma esnasında belirttiğim 3 uygulamada çalıştı.



-C dizini altına gittiğim de ise belirttiğim gibi dizin oluşturduğunu görüntülüyorum.

***Embed Trojan Hazırlama***

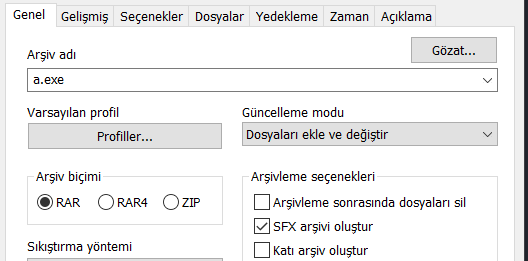
-Oluşturduğum zararlı yazılımları windows üzerine aktarıyorum ve burada sosyal mühendislik ile de birleştirip embed file haline getireceğim.



-Veil ile oluşturduğum zararlı yazılımı windows üzerine çekiyorum.

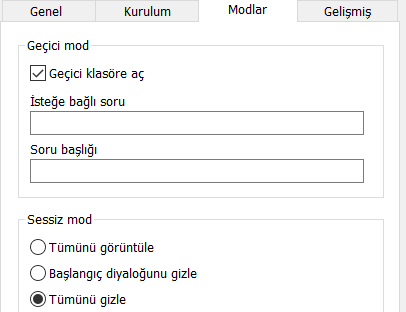
-Bu dosyaların yanına dikkat çekmemesi için bir pdf dosyası alıyorum.

-İcon lazım olursa diye de bir PDF İconu alıyorum.



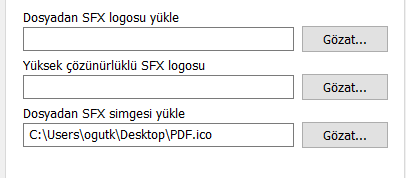
-Şimdi ise bir önceki uygulamada yaptığım gibi bu dosyaları embed file haline getireceğim.

-Winrar ile arşive ekliyorum ve SFX olarak kayıt ediyorum.

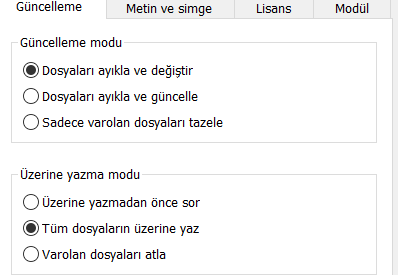


-SFX Seçeneklerine geçiş yapıyorum ve burada "Tmp" dosyasına aktarım yapacağını,kullanıcıya hiçbir şey sormayacağını belirtiyorum.

-TMP dosyasında yetkim olmasa da işlem gerçekleştirebiliyorum.

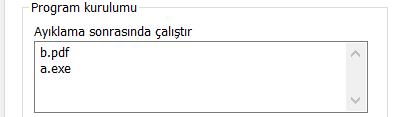


-Dikkat çekmemesi için İcon olarak PDF iconu ekliyorum.



-Güncelleme kısmında kullanıcıya hiçbir şey sormaması için burada ayarları değiştiriyorum.

-Kullanıcının fark etmemesi burada önemli.



-Başlatıldığında çalışacak uygulamaları da belirtiyorum.



-Gerekli ayarlardan sonra "Desktop5" ismi ile kaydediyorum.

***Trojan Uzantısını Ters Çevirme***

-"File extansion spoof" işlemlerinden biri olan RTLO ile işlem gerçekleştireceğim.



-Bu işlem için Windows üzerinde bulunan "Karakter Eşlem" aracından yararlanıyorum.

-Burada aşağı indiğimde "U+202E" karakterini buluyorum.Bu karakter ile soldan sağa kaydırma işlemi yapacağım.

----🡪

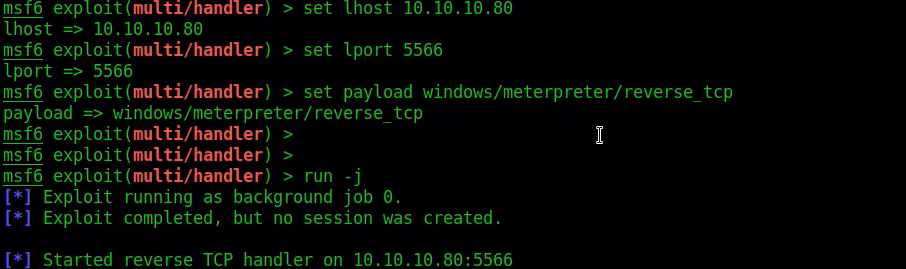


-Oluşturduğum zararlı yazılımın adını tersten gideceği için "alfpd.exe" yapıyorum ve kopyaladığım karakter ile "CTRL+V" yapıştırma işlemi yapıyorum.

-Görüldüğü gibi ismini tersten doğru yazdırarak bir pdf dosyası gibi gözükmesini sağladı.

***Windows 10 Üzerinde Test***

-Trojanımızı Embed File haline getirdikten sonra şimdi sıra Windows ortamında test etmede;



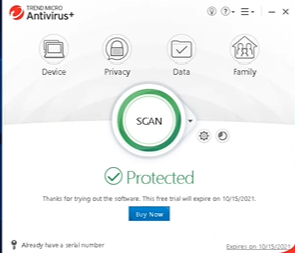
-Bu işlem için öncelikle Metasploit aracımı çalıştırıyorum ve içinde bulunan Multi/handler aracını başlatıyorum.

-Buraya gerekli bilgileri set edip portu dinlemeye alıyorum.

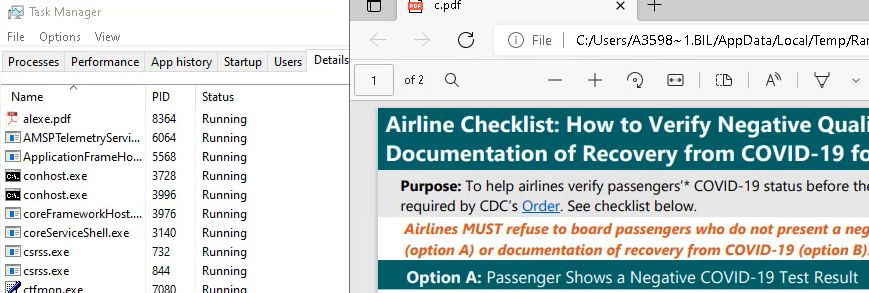
-Burada payload bilgisini düzgün vermemiz aracın çalışması için önemlidir.



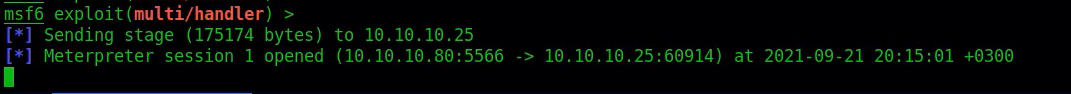
-Bilgi işlem içerisine oluşturduğum zararlı yazılımı ekliyorum.



-Antivirüs aracı hiçbir zararlı yazılım olup olmadığını anlayamadı.



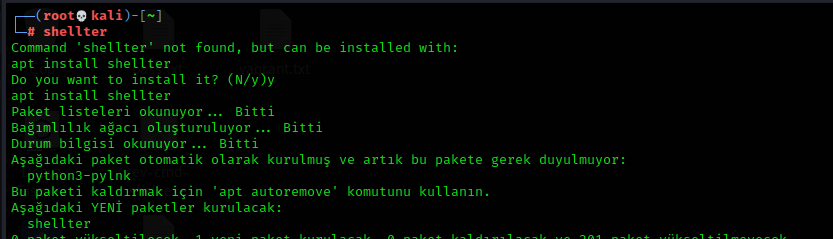
-Oluşturduğum zararlı yazılımı çalıştırıyorum ve ayarladığım gibi pdf dosyam da yanında başlamaktadır.



-Başarılı bir şekilde session bağlantısı kurabildim.

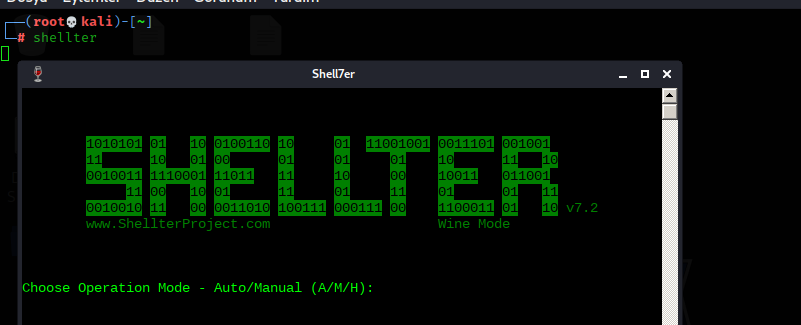
***Otomatik Embed Trojan Hazırlama***

-Manuel olarak yaptığımız Embed File işlemini Linux üzerinde "shellter" aracı ile gerçekleştireceğim.



-Öncelikle "shellter" komutu ile aracı çalıştırıyorum.

-Burada kurulu değil ise kurulum yapar.

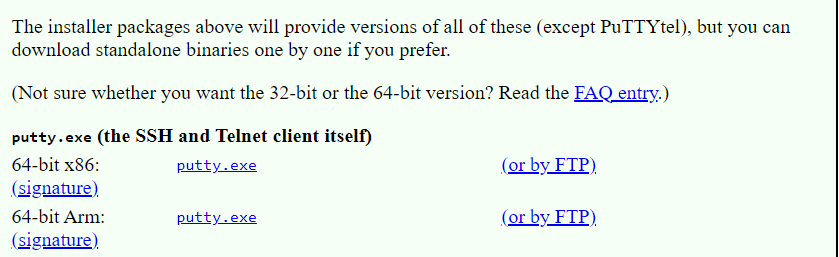


-Kurulum sonrasında aracı başlattığım da karşıma böyle bir sekme geliyor.



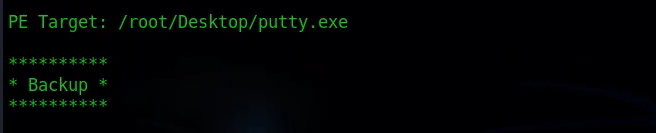
-Otomatik seçeneği ile devam ediyorum.

-Ardından benden bir hedef istiyor yine aynı şekilde PuTTy aracı ile işlemlerime devam edeceğim.



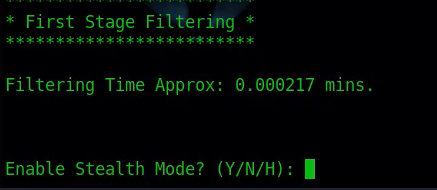
-PuTTy aracını tarayıcı üzerinden indiriyorum.

-Burada 32 bit olmasına dikkat edelim.



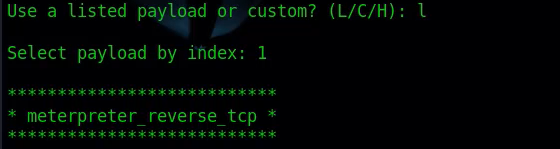
-Hedef olarak PuTTy aracını belirtiyorum ve işlemi başlatıyorum.

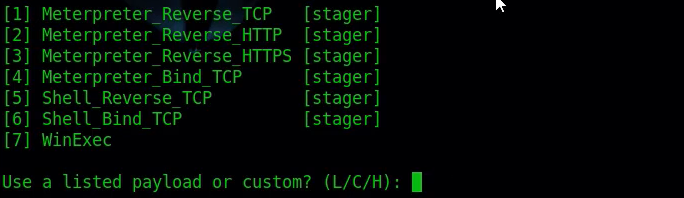
-Bu işlem biraz sürebilir.



-Bir sonraki adımda gizli Modu kullanmak isteyip istemediğimi soruyor.

-Burada kullanmak istediğimi belirtiyorum.

---



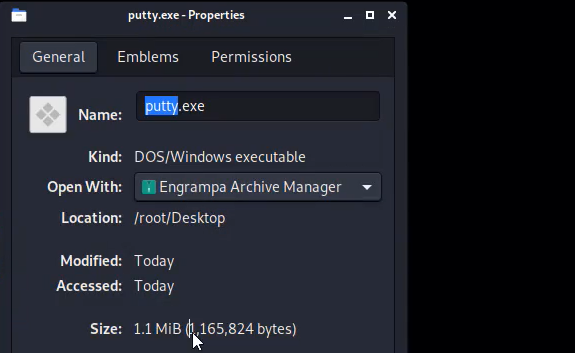
-Sonraki adımda Payload belirtmemi istiyor.

-"-l" komutu ile listeden gideceğimi belirtiyorum.

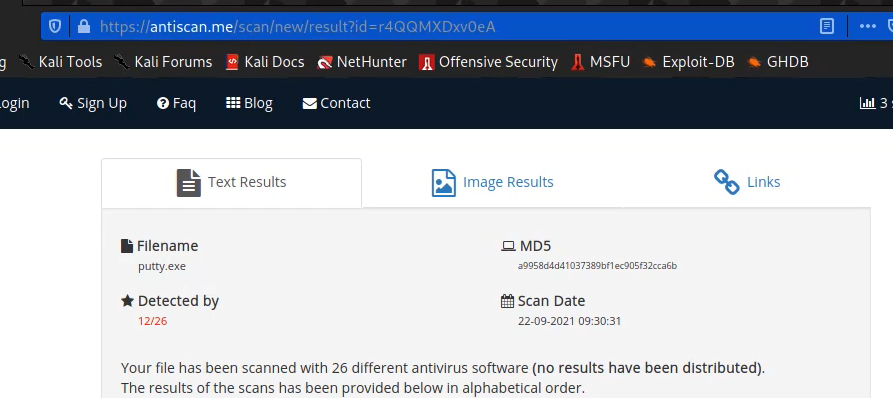
-Listeden meterpreter reverse tcp ile devam ediyorum.



-Port ve Host bilgisini de set ettikten sonra Embed Trojanım oluşmaya başlıyor.



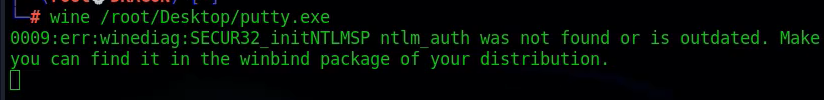
-PuTTY.exe uygulamasının boyutuna baktığım da boyutunda da değişiklik olduğunu görüntülüyorum.



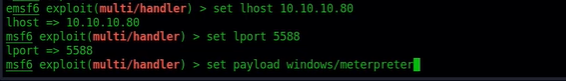
-"Antiscan" üzerinde test ettiğim de 26 virüs programından 12 sine yakalandığını görüntülüyorum.

***Shelter Aracı ile Oluşturulan Trojanı Test Etme***

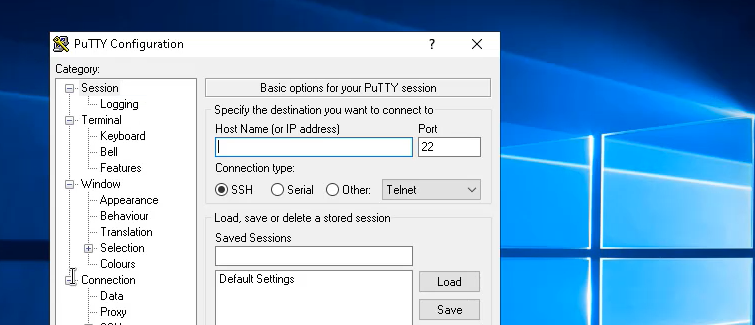
--"Shellter" aracı üzerinde oluşturmuş olduğum embed trojanımı windows üzerinde test edeceğim.



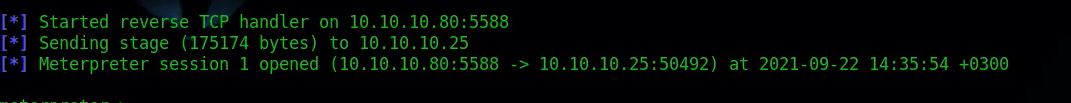
-Oluşturmuş olduğum "putty.exe" aracını wine ile çalıştırıp test edebilirim.



-Test işleminin ardından Metasploit aracımı başlatıyorum ve burada Multihandler aracı ile belirttiğim portu dinlemeye alıyorum.



-Bİlgiişlem üzerine oluşturduğum zararlı yazılımı aktarıyorum ve çalıştırıyorum.



-Metasploit üzerine shell bağlantımın geldiğini görüntülüyorum.