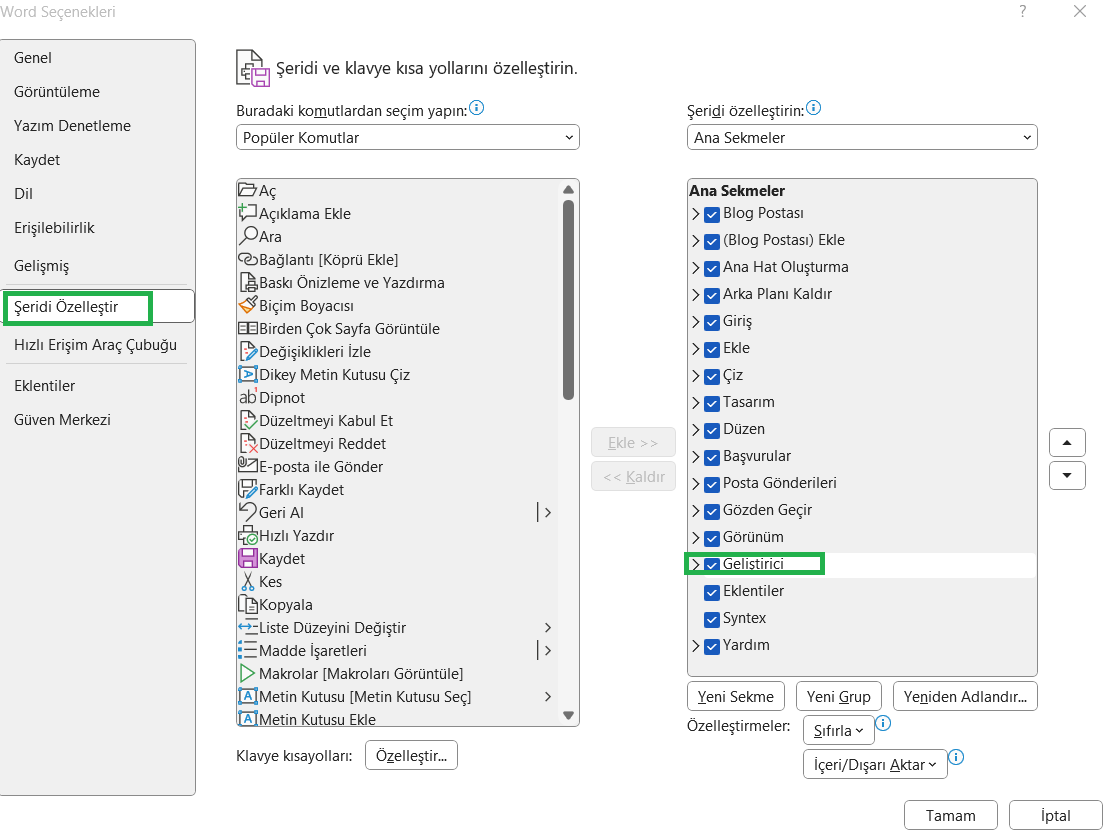
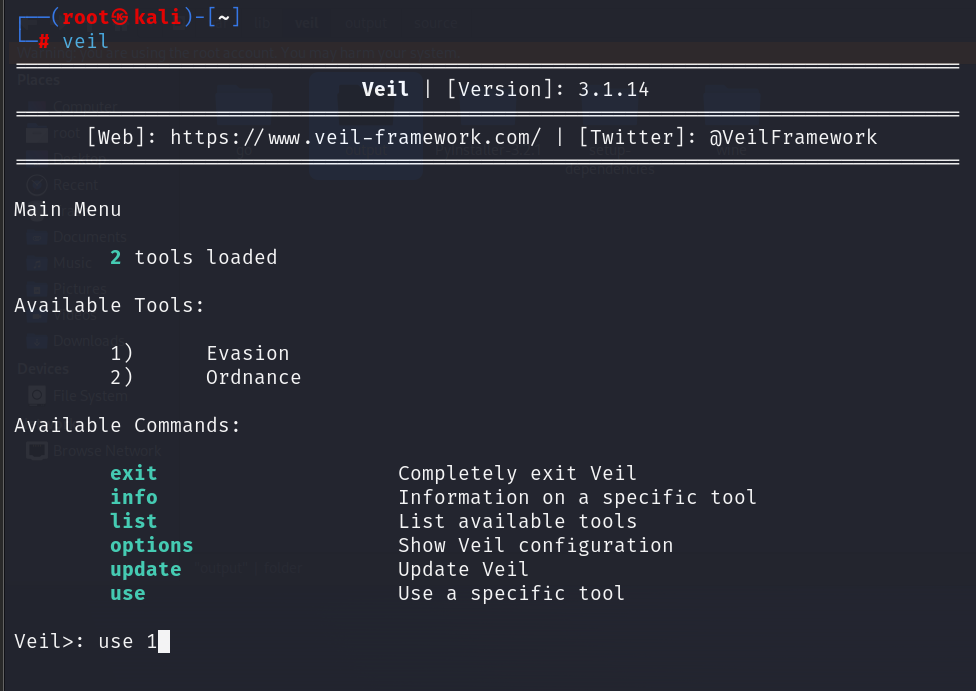
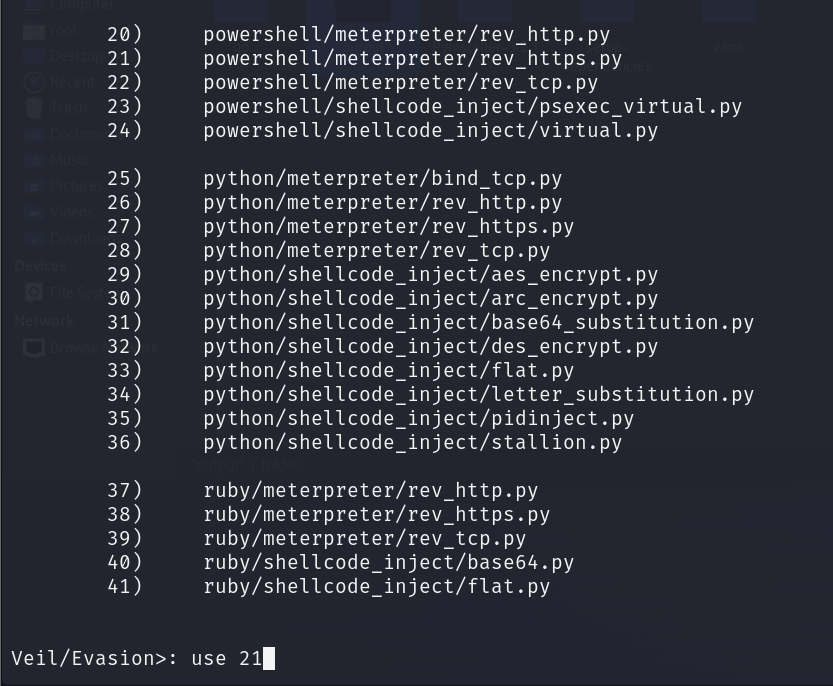
Word belgesinde makro yazabilmek için öncelikle ayarlar kısmına gelip "Şeridi özelleştir'e" tıkladıktan sonra sağ tarafta "Geliştir" seçeneğini aktif etmeniz gerekmektedir.



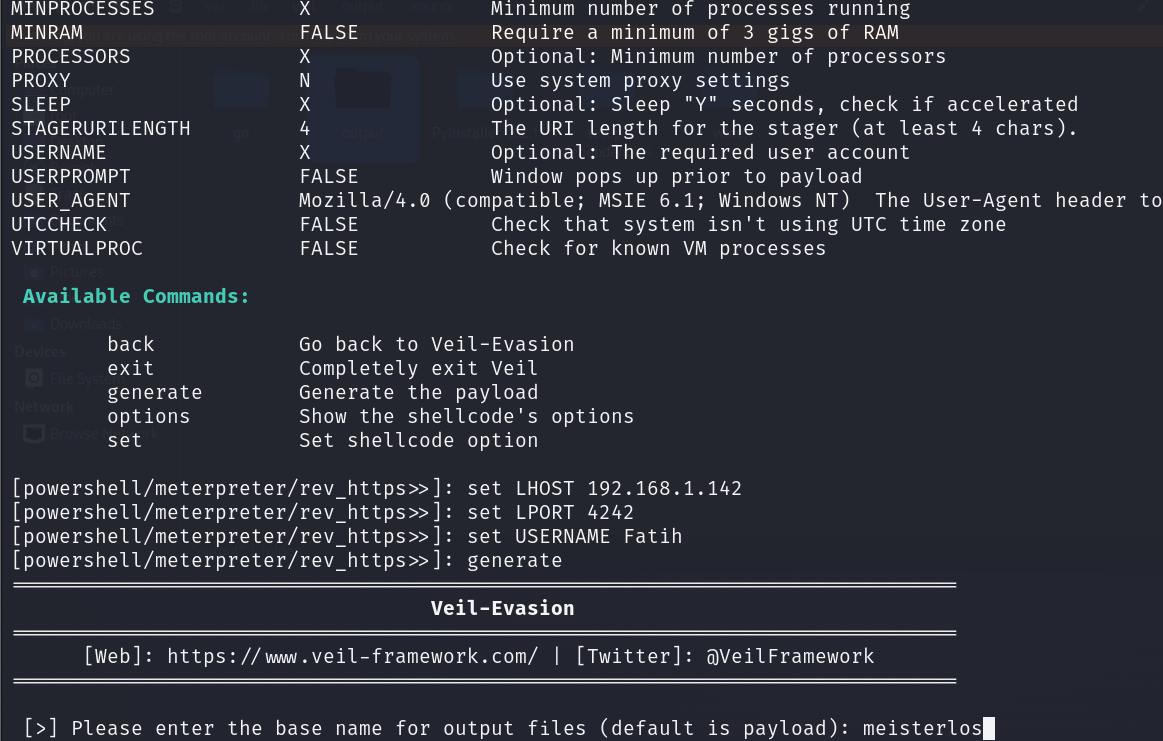
Daha sonrasında saldırı makinemize geliyoruz ve veil aracını kurduktan sonra veil aracımızı çalıştırıp "use 1" komutunu kullanalım.



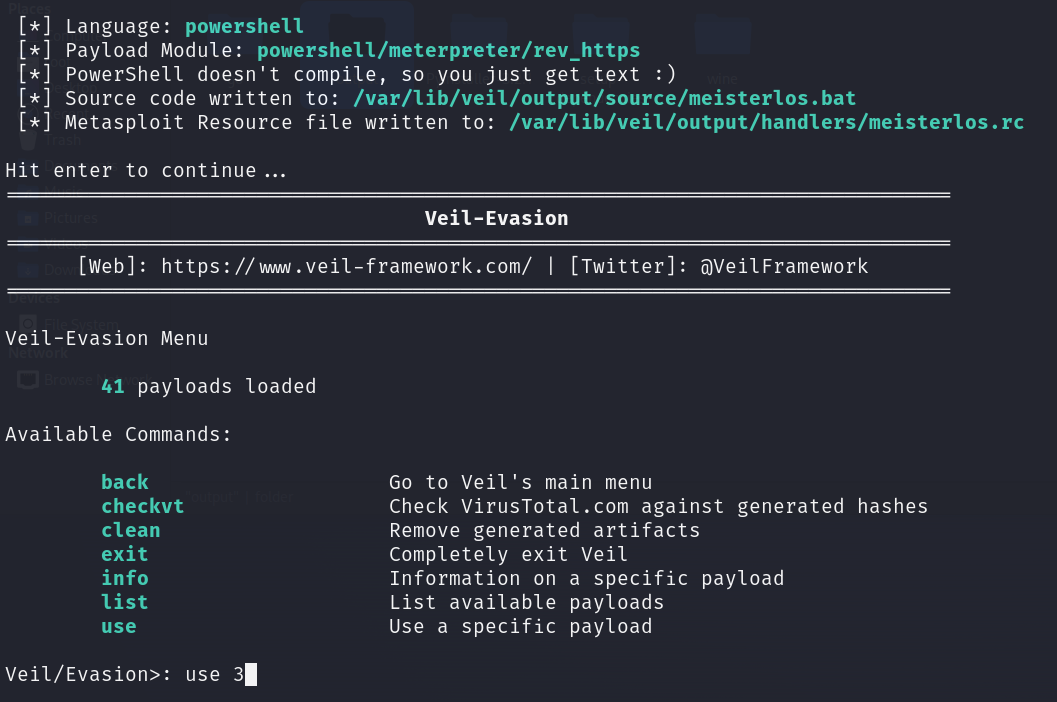
Daha sonrasında "list" komutunu kullanarak içerisindeki modülleri listeliyoruz ve ben bu örneğimde "use 21" komutunu kullanıp powershell/meterpreter/rev\_https.py modülünü seçiyorum. Burada rev\_tcp veya rev\_http de seçebilirsiniz tercih sizin.



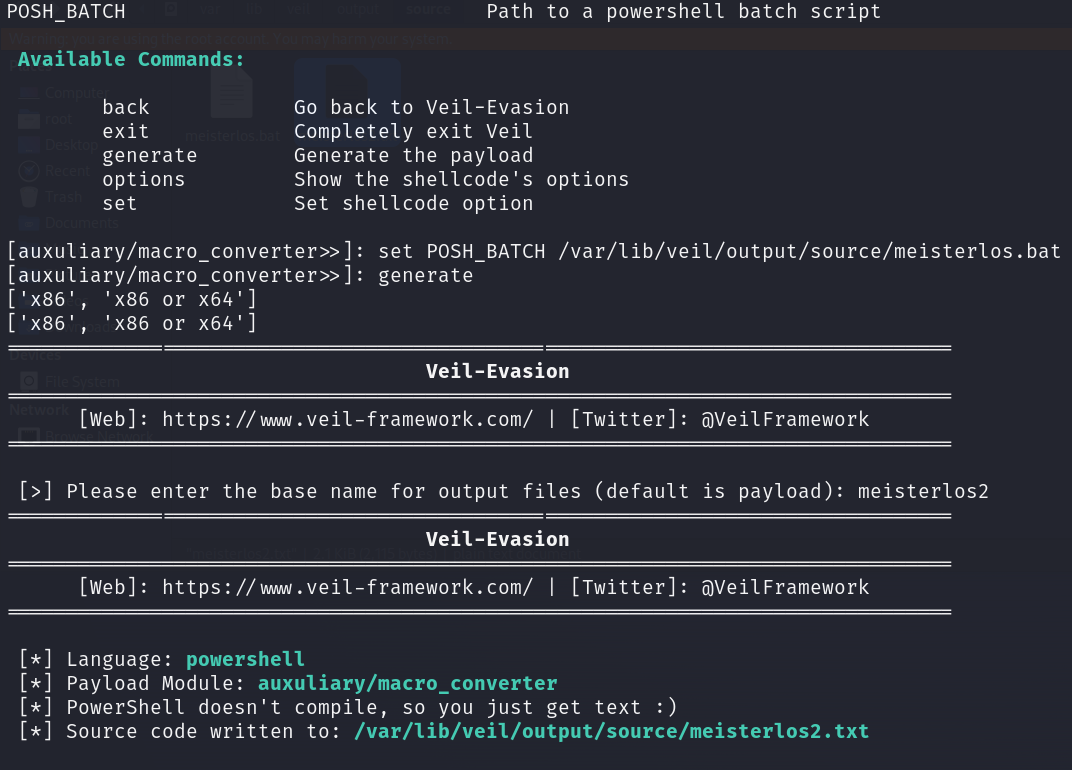
Daha sonrasında kendi ip adresimizi ve istediğimiz bir port numarasını giriyoruz. Burada girdiğiniz port numarası hem karşı cihazda kullanılmayıp hemde ortamdaki firewall tarafından izin verilmiş bir port olması lazım! Dosyayı istediğiniz isim ile kaydedin.



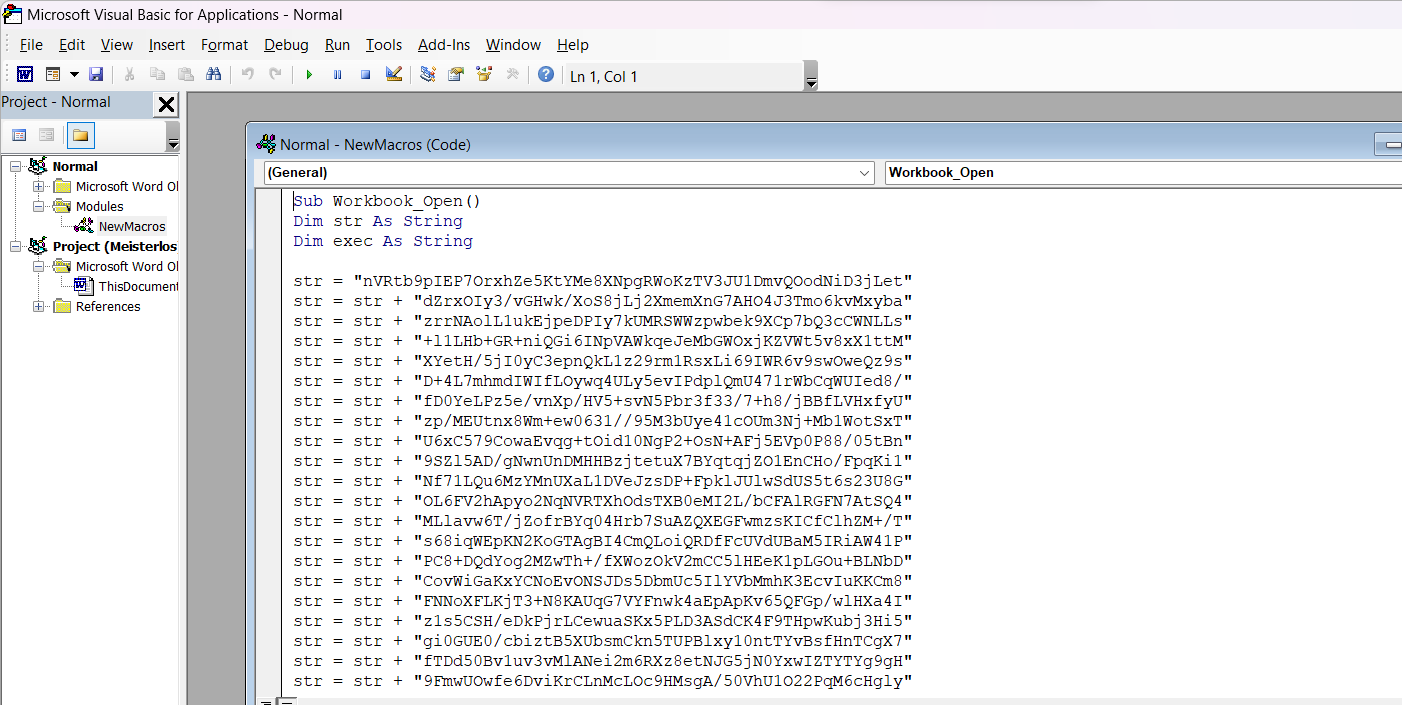
Program bize bir adet .bat uzantılı bir dosya oluşturdu şimdi bu bat dosyasını direkt karşı cihaza atar isek antivirüs tarafından engellenecektir. Bunun için veil programında bulunan bir başka modülü daha kullanacağız. Veil programında "use 3" komutunu kullanın ve auxuliary/macro\_converter modülünü seçelim.



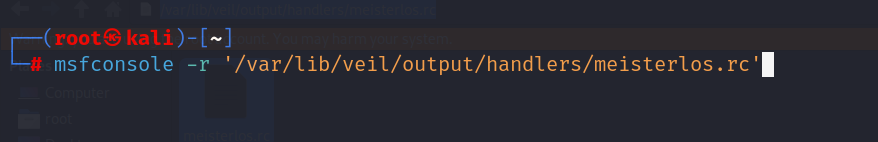
Bu kısımda oluşturduğumuz .bat uzantılı dosyayı kullanacağız ve set POSH\_BATCH dosya\_yolu.bat diye komutumuzu yazalım.



Program şimdi bize bir adet .txt uzantılı dosya verdi Bu vermiş olduğu dosyayı açıp içerisindeki kodu kopyalayın ve word dosyanıza gelin. Word'de bulunan geliştir sekmesine tıkladıktan sonra makro oluşturup içerisine bu komutu yapıştıralım. Ardından word dosyamızda makroları çalıştırabilmek için dosya uzantısını değiştirmek gerekiyor. Farklı kaydete tıklayın ve .docm .doc veya .dotm dosya uzantısında kaydedin.



Saldırı makinemizde veil programı bize .rc uzantılı bir dosya'da vermişti eğer isterseniz direkt olarak aşağıdaki komuttaki gibi kullanıp dinlemeye alabilirsiniz. Veil'in oluşturduğu .rc uzantısı metasploitteki exploit/multi/hundler'ı çalıştırır ve otomatik şekilde sizin vermiş olduğunuz ip adresini ve portu dinlemeye alır.



Eğer isterseniz netcat aracını'da kullanabilirsiniz, benim tavsiyem metasploit freamworkü kullanmak. Hedef kişi word dosyasını açtıktan sonra shell almış olacaksınız.

