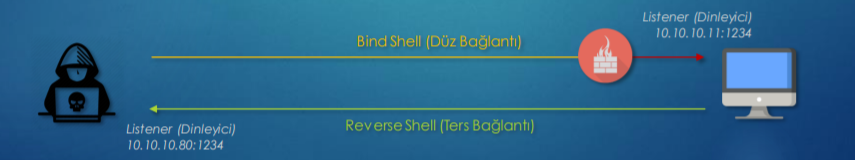
|  |
| --- |
| ***Metasploit*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| -Linux üzerinde kurulu olarak gelen ve Pentest işlemlerinde sıkça kullanılan Metasploit aracının kullanımı hakkında detaylı bilgi vereceğim. |

**13.12.2021**

Remote Shell Kavramı ve Türleri

-Remote Shell, hedef sistemin işletim sistemi kabuğunda uzaktan bağlantı erişimi ve kullanım yetkisi elde durumuna verilen addır. Gerçekleşirse “shell almak” olarak ifade edilir.

İki tür remote shell bağlantısı vardır;



1) Bind (Düz) Shell: Saldırgandan hedefe doğru yapılan bağlantıyla sağlanır. Hedef, bir IP ve port aracılığıyla, listener (dinleyici) konumundadır.

-Firewall tarafından engellenebilir olduğu için pek tercih edilmez.

2) Reverse (Ters) Shell: Hedeften saldırgana doğru yaptırılan bağlantıyla sağlanır. Bu kez de, saldırgan, bir IP ve port araclığıyla listener (dinleyici) konumundadır.

-En sık tercih edilen shell bağlantı türüdür.

Metasploit Araçları

Metasploit, hedef sistem için uzaktan çalıştırılabilir remote exploit’ler ve hedef sistem içinde çalıştırılabilir olan local exploit’ler yanı sıra diğer modülleri de barındıran bir istismar yönetim aracıdır.

Auxiliary: Hedef sistem hakkında bilgi çıkarmak (enumeration) için kullanılan yardımcı modüllerdir.

Payload: İstismar edilen sistemde, exploit’lerden sonra çalışan (gönderilen) modüllerdir. Hedef sistemin ve exploitlerin türüne bağlı olarak seçilirler. Örneğin, exploit edildikten sonra bağlantı sağlanması ve meterpreter çalıştırılması gibi.

Encoder: Antivirus ve firewall gibi güvenlik önlemlerini atlatmak için kullanılan modüllerdir. Exploit ve payload’lar tarafından otomatik olarak da seçilirler.

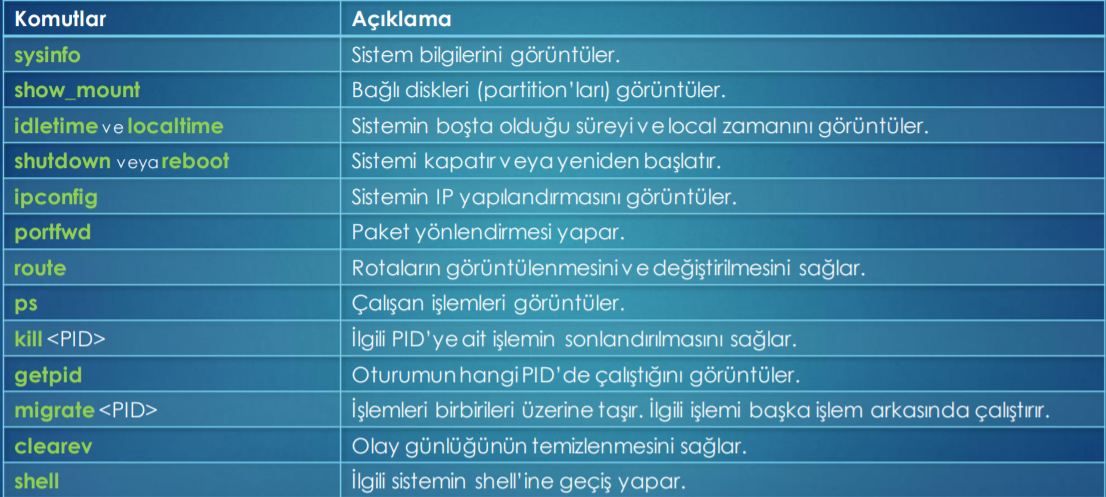
NOP: Payload kodunun yürütülebilmesi için hedef sistemdeki işlemcinin döngüye sokulmasını; payload için güvenilir bir alan yaratılmasını sağlar. No Operation’ın kısaltmasıdır.

Post: Exploit işlemi sonrası, post-exploitation fazında kullanılabilecek modüllerdir.

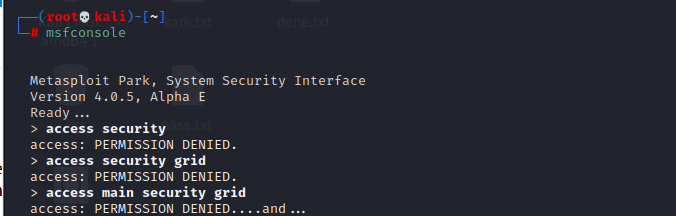
Metasploit Komutları



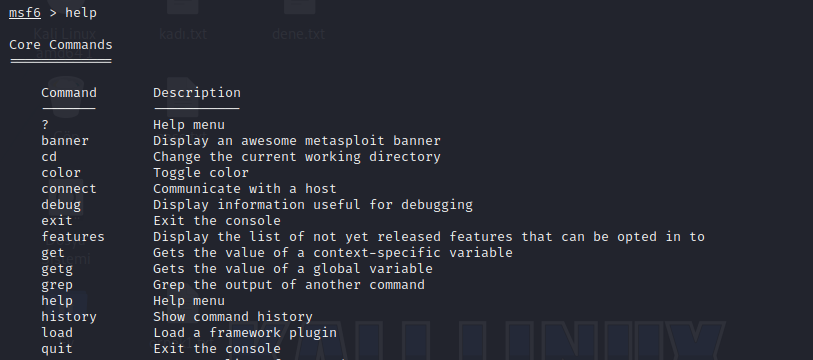
-Metasploit komutları



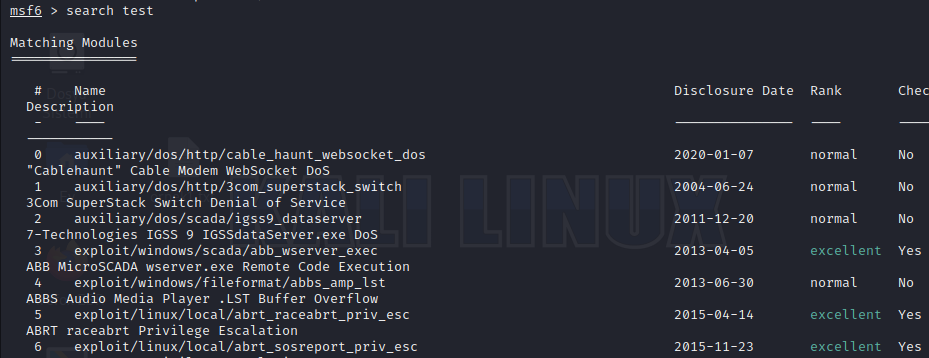
-Meterpreter komutları



-Linux üzerinde kurulu olarak gelen ve "postgresql" veritabanını kullanan ruby diliyle yazılan bu aracı "msfconsole" komutu ile başlatabilirim.



-Araç üzerinde "help" komutunu çalıştırdığımız da aracın kullanımı hakkında bilgi sahibi olabiliriz.

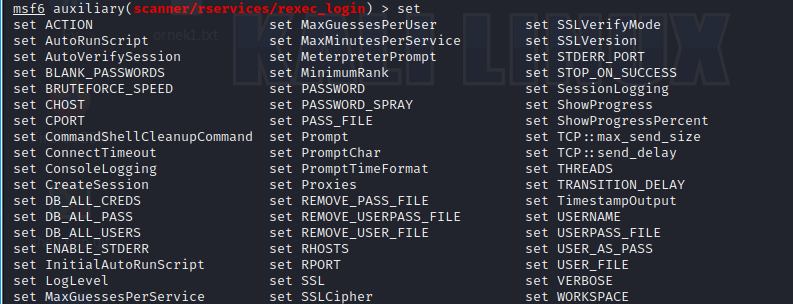


-Search komutu ile aramak istediğim bir exploiti aratabiliyorum.

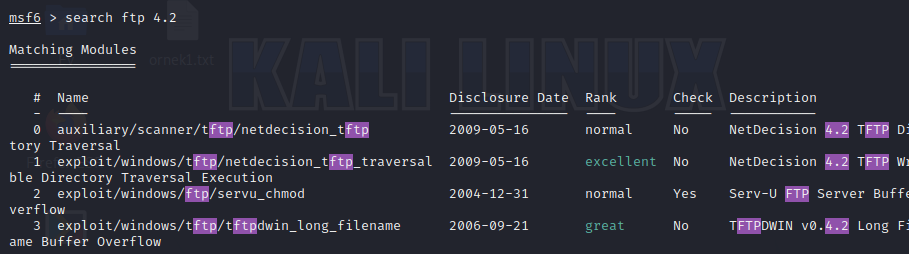


-Arattığım sonuç ile ilgili çıkan sonuçlardan bilgi almak için info komutundan yararlanabilirim.

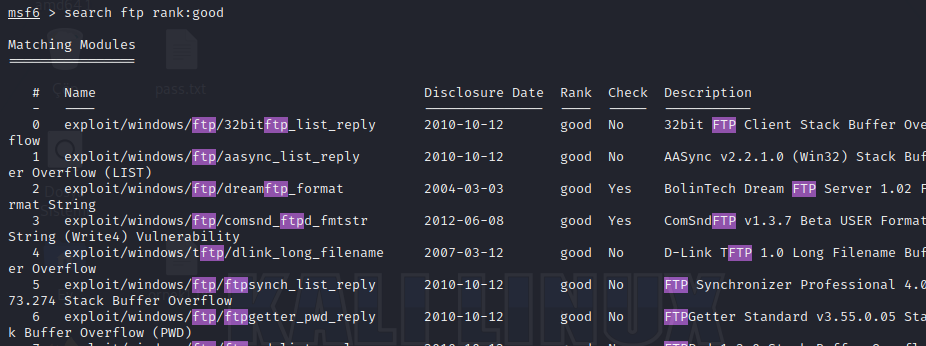
-Bu işlem ilgili modül üzerinden de gerçekleştirilebilir.



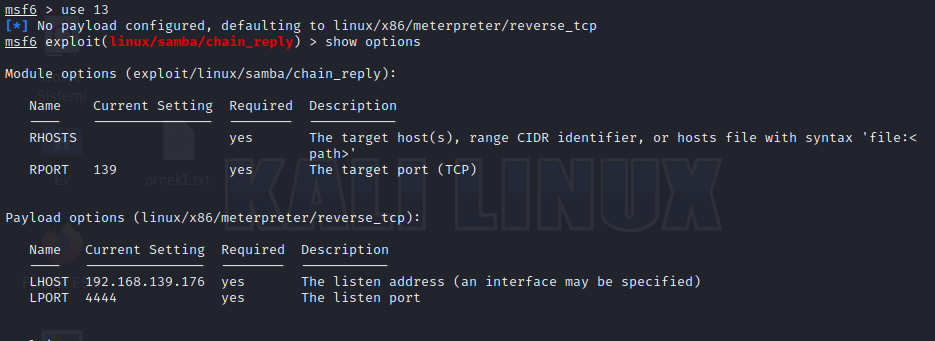
-Ayrıca modül üzerinde "set" komutunu yazdıktan sonra iki kere "TAB" tuşuna basılır ise ayarları görüntüleyebiliyoruz.



-"Search ftp" komutu ile Pentest sırasında karşılaştığım bir servis ile ilgili exploit taraması gerçekleştirebilirim.



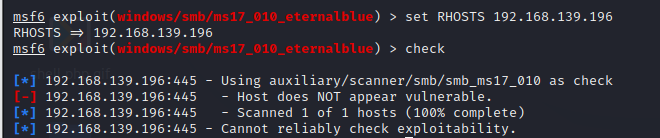
-Ayrıca arama sırasında sonuna eklediğim "rank:good" araması ile başarılı olma durumlarına göre bir tarama gerçekleştirebilirim.



Seçmiş olduğum rastgele exploit üzerinde "show options" komutu ile gerekli olan ayarları görüntüleyebiliyorum.

-Required kısmında bilginin gerekli olup olmadığını görüntüleyebiliyorum.

-Ayrıca "Desription" bölümünde ayar ile ilgili gerekli açıklamalar bulunmaktadır.



-Burada set komutu ile istenen ayarları set edebiliyorum.

-"Show payloads" komutu ile kullanım sağlayabileceğim payloadsları görüntüleyebilirim.

-"set payload\_ismi" komutu düzeniyle de set edebilirim.