|  |
| --- |
| ***Wordlist Oluşturma*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| Pentesting esnasında çok kullandığımız Wordlistleri,kişisel bilgiler doğrultusunda nasıl oluşturabiliriz bunun hakkında bilgi vereceğim. |

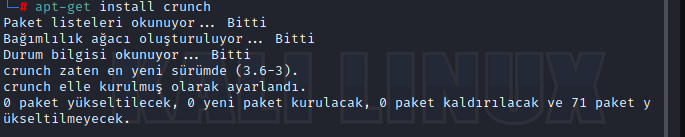
2

**08.08.2021**

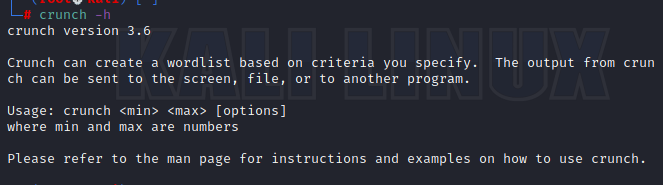
***Crunch***

-Kullanımı basit bir araçtır.

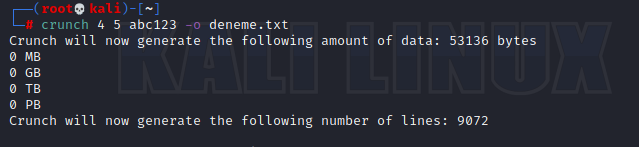
- Linux üzerinde çoğu sürümde kurulu olarak gelmektedir.



- Eğer yüklü değil ise "apt-get install crunch" komutu ile yükleme işlemi yapılabilir.

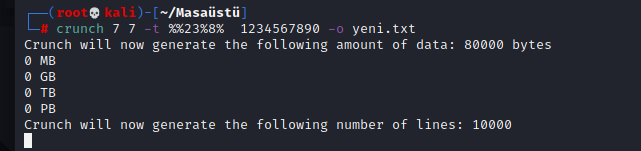


-“crunch –h” komutu ile kullanımı hakkında bilgi sahibi olabiliriz.



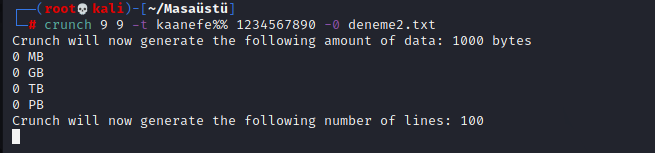
-Min. 4,Max. 5 karakterli olmak üzere “abc123” harf ve rakamlarını kullanarak “deneme.txt” isimli bir wordlist oluşturuyorum.

-Çözmek istediğimiz metnin belirli bir kısmını biliyorsak,bilmediğimiz kısmı üzerinden işlem gerçekleştirebiliriz.



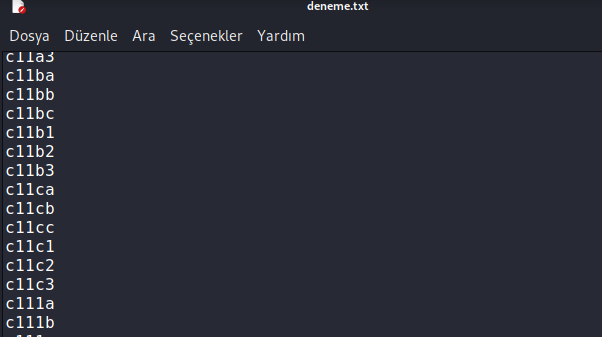
-“ ? ? 2 3 ? 8 ? "?" kısmında “?” olan yerler bilinmiyor.

-7 karakterli içerisinde 3 adet sabit rakamdan oluşan Wordlist oluşturduk.



- "1234567890" yerine alfabe koyulup işlem gerçekleştirilebilir.

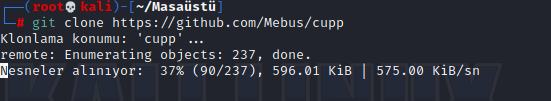
-Şifrenin başını bilip sonunda ki sayıyı bilmediğimizde böyle bir çalışma gerçekleştirebiliriz.



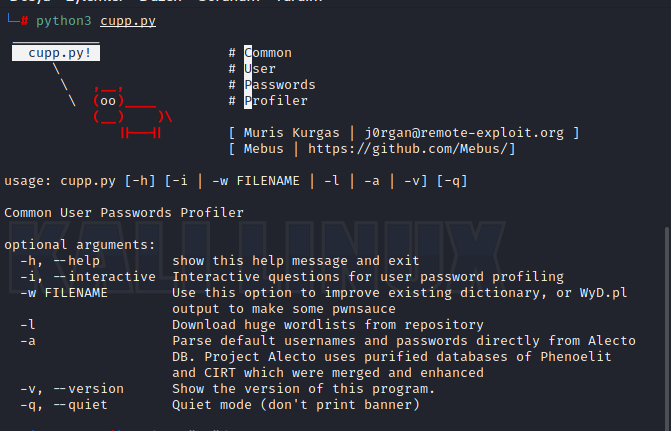
-Oluşturduğumuz Wordlist’in oluşturma düzeni alfabetik olarak devam etmektedir.

***Cuppy.py***

-Cuppy.py ile Crunch’tan farklı olarak kişisel bilgiler üzerinden bir şifre oluşturma işlemi gerçekleştirir.

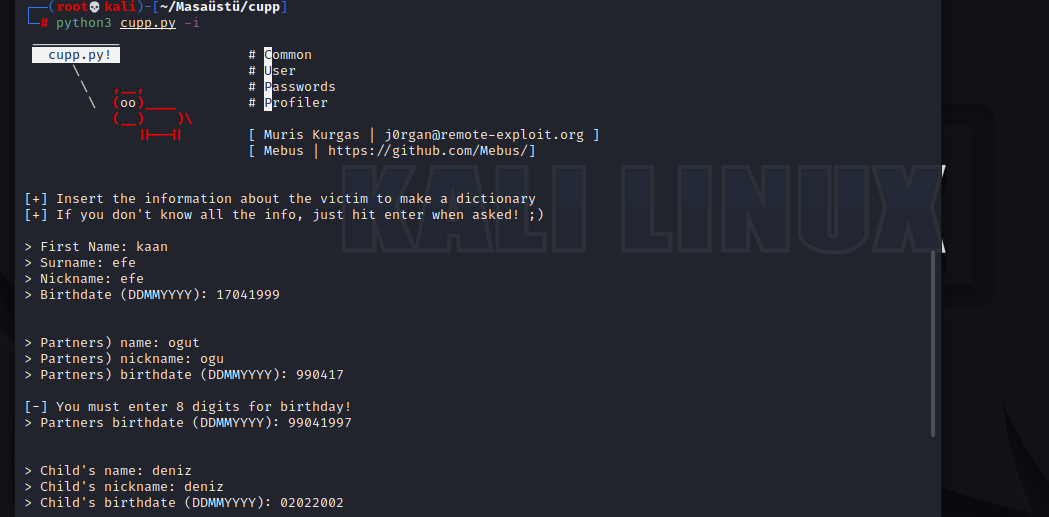


- Github üzerinden indirme işlemini başlatıyorum.



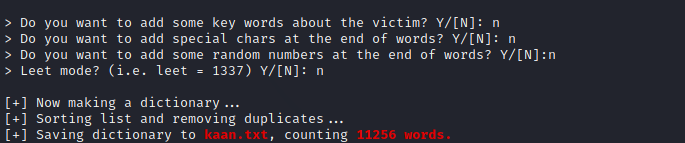
- İndirme işleminin ardından dosyanın bulunduğu dizine geçiş yapıyorum ve burada "python3 cupp.py" ile bu dosyayı çalıştırıyorum.

-Burada kullanabileceğim komutların kullanımı hakkında bilgi sahibi olabiliyoruz.



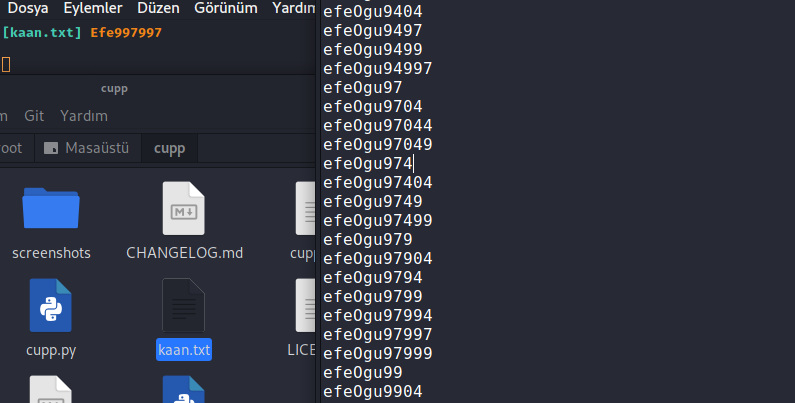
-"python3 cupp.py -i" komutu ile aracı çalıştırıyorum.

-Ardından bana oluşturacağı Wordlist için gerekli kişisel bilgileri soruyor.Bu sorulara cevap vermeyip boş geçebiliriz.



- Özel karakter-Random Sayı-Başka eklemek istediğim özel karakter var mı sorularını soruyor.

-Bunları yanıtlıyorum ardından "11256" adet payload oluşturuyor.



- Şuanda arka planda işlem devam ederken “cupp” dosyasının içerisine bir kaan.txt dosyası oluşturdu.Dosyanın içerisinde ise oluşturduğu payloadları bu şekilde görüntüleyebiliyoruz.