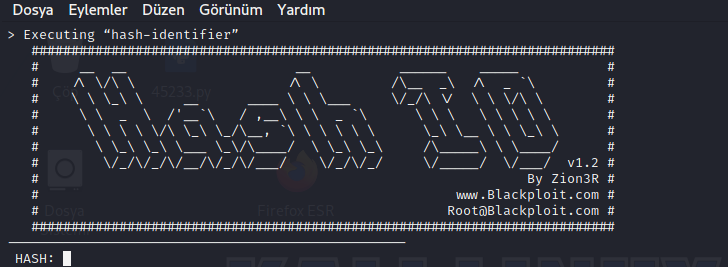
|  |
| --- |
| ***Hash & Şifre Kırma*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| -Hash İdentifier  -John The Ripper  -Hydra  -Medusa |

**11.08.2021**

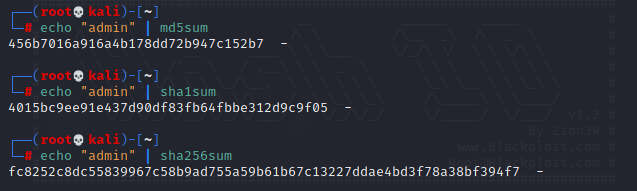
***Hash İdentifier***

-Linux üzerinde kurulu olarak gelmektedir.

-Bu araç bizim baktığımızda anlamsız gelen bir karakter dizinini hangi formatta şifrelendiğini öğrenmemize yaramaktadır.

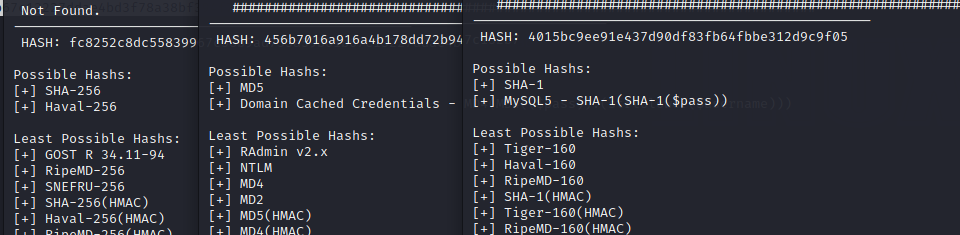


- Kullanımı çok basittir.Açılan sayfa üzerine hash değeri kopyalanır ve çalıştırılır.



-MD5,SHA1,SHA256 formatında bir hash oluşturma işlemi gerçekleştiriyorum.

-Oluşturduğum hash değerlerini sırasıyla bu araç üzerinde deneyeceğim.

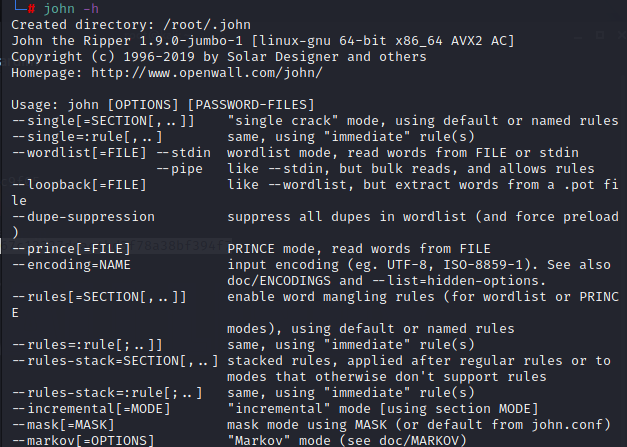


- İşlemi çok uzatmadan tek tek göstermek yerine toplu şekilde gösteriyorum.Hepsini başarılı bir şekilde bulduğunu görüntülüyorum.

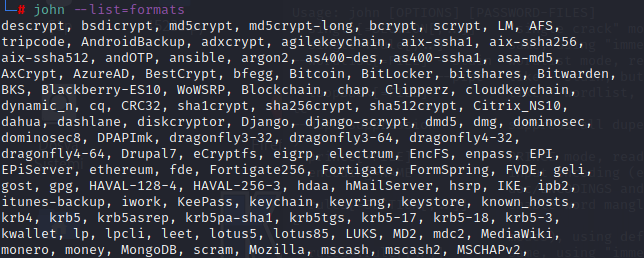
***John The Ripper***

-Linux üzerinde kurulu olarak gelmektedir.

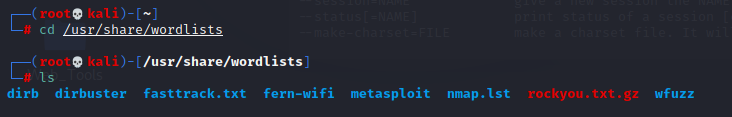
-Linux üzerinde sadece "john" komutunu girerek çalıştırmaya başlayabiliriz.



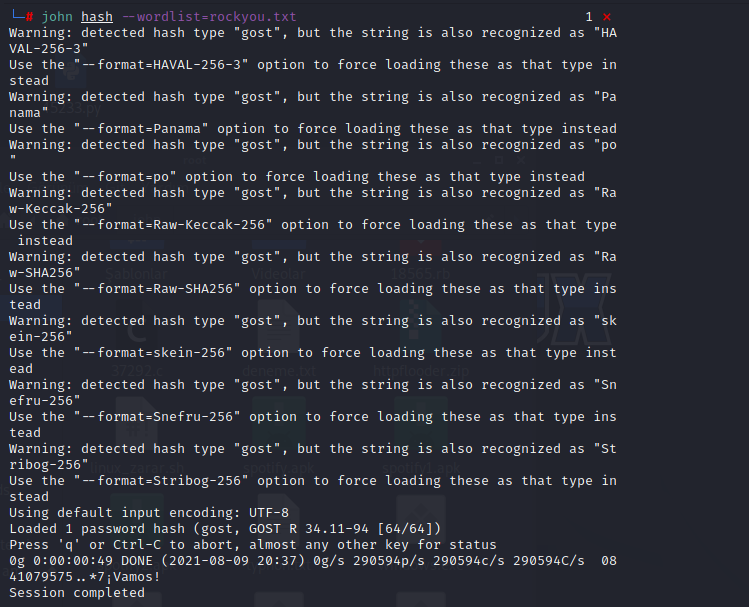
-"john -h" komutunu çalıştırıyorum burada bu araç ile kullanabileceğim parametrelere erişiyorum.



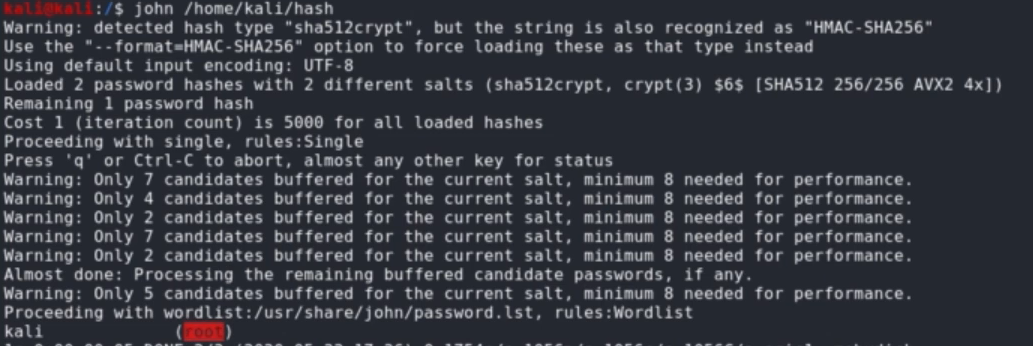
- "john --list=formats" komutu ile kullanılabilen formatları görüntüleyebiliyoruz.



- Linux üzerinde çok kullanılan Rockyou.txt “Wordlistini masaüstüne kopyalıyorum.



-“john hash –wordlist=rockyou.txt” formatında bir tarama gerçekleştirip içerisinde ki hash formatını çözümleyebiliriz.



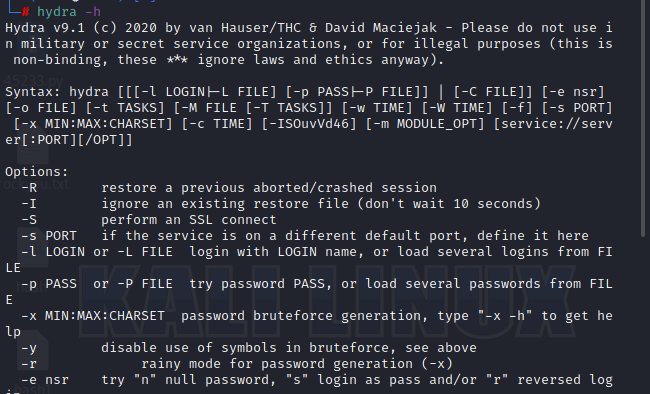
-Wordlist kullanmadan “john hashiçeren.txt” formatında işlemi başlatabiliriz



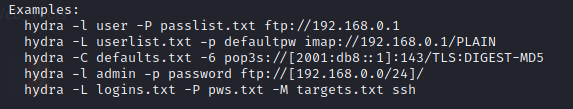
-Ayrıca sonuna eklediğimiz –show komutu ile bulmuş olduğu şifreyi görüntüleyebiliriz.

***Hydra ile Parola Saldırısı***

- Hydra aracı ile şifreli araca Bruteforce işlemi gerçekleştirerek şifreyi kırmaya çalışacağız.

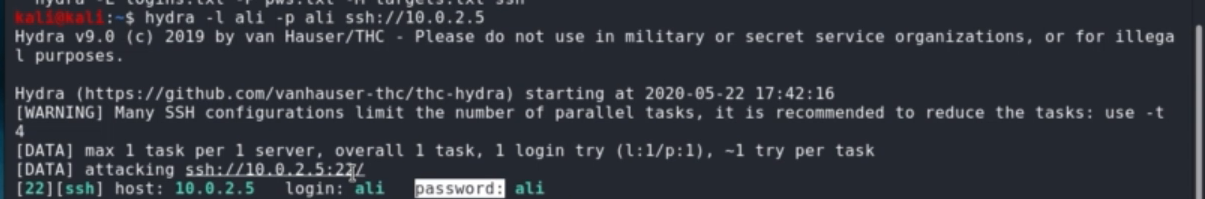


- "hydra -h" ile bu aracın kullanımı hakkında bilgi alabiliriz.

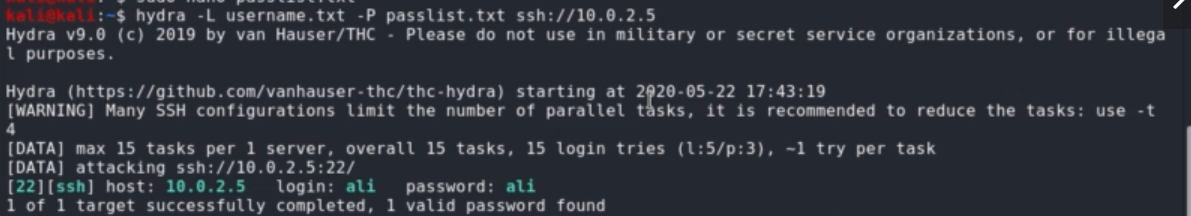


- Example kısmında da tam olarak kullanımını görüntülüyoruz.

**-Firewall kaynaklı bir sorun yaşadığım için bundan sonra ki SS’ler temsilidir.**

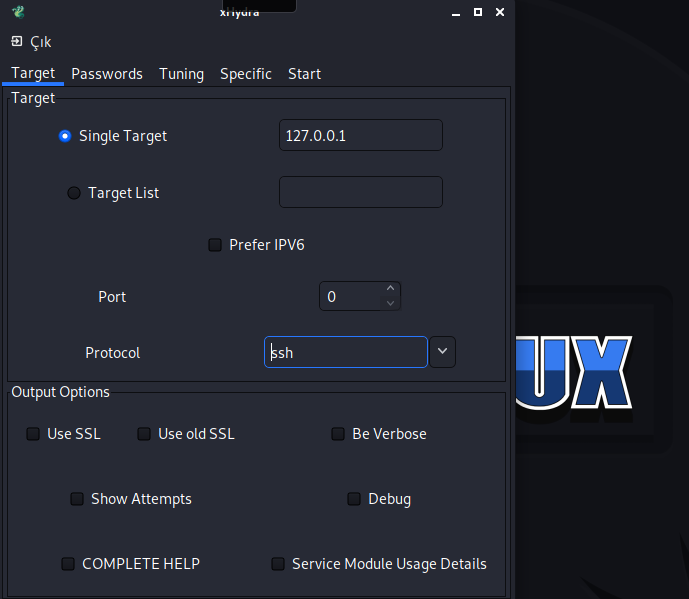


- Ayrıca şifresini bilmediğimiz bir sunucu üzerinde bir Bruteforce denemesi ile şifreyi kırabiliriz.



-Payload kullanımı yaparak bu işlemi çok daha hızlı bir şekilde tamamlayabiliriz.

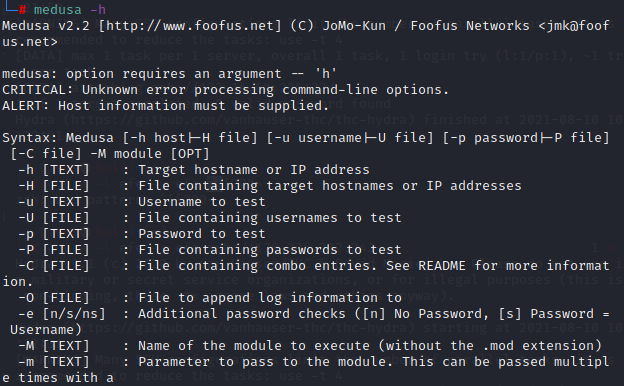
- Hydra'nın bir değişik versiyonu olan xHydra ile de görsel olarak işlemimizi tamamlayabiliriz.



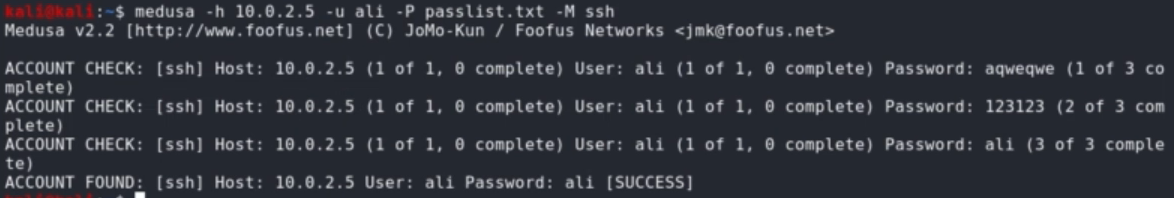
***Medusa ile Parola Saldırısı***

-"Medusa" Hydra gibi linux üzerinde kurulu olarak gelmektedir.

-Hydra aracıyla karşılaştırdığımızda bu araç biraz daha yavaş kalmaktadır.



- "Medusa -h" komutu ile medusanın kullanımı hakkında bilgi sahibi olabiliriz.



-Kullanımı bu şekilde fazlasıyla basittir.

-"-h" ile bir Host adresi veriyoruz.

-"-u" ile bir kullanıcı adı veriyoruz.

-"-P" ile bir passlist tanımlıyoruz.

-"-M" ile bağlantı türünü belirtiyoruz.