Uygulamalı Beyaz Şapkalı Hacker Eğitimi #8

Parola Kırma Saldırıları

Konular

- Parola ve Şifre Kavramları
- Hash ve Salt Kavramları
- Parola Kırma Saldırılarında Püf Noktalar
- Saldırı Türleri
- Wordlist Oluşturma
- Kullanılan Araçlar

Parola ve Şifre Kavramları

- Parola: Açık metin, gizli tutulması gereken karakter dizisidir. Kullanıcı kendi belirler ve parolayı kullanarak belirli alanlara giriş sağlar.
- Şifre: Parolanın bir algoritma aracılığı ile yeni bir formata dönüştürülmüş halidir.

Hash ve Salt Kavramları

- Hash: Bir verinin sabit sayıda bir özete çevrilmiş halidir. Özetten geri açık metin hale döndürme algoritması yoktur ve doğrulama amacıyla kullanılır. Örn: MD5
- Salt: Veriler hash algoritmalarından geçirilirken Rainbow Table saldırıları aracılığıyla kolayca kırılamasın diye verinin sonuna, başına veya ortasında bir yere yerleştirilen karakter dizisidir.
  - Prisma -> hash -> 112312311231
  - Prisma -> salt(sona +++) -> Prisma+++ -> 1823891239812

Parola Kırma Saldırılarında Püf Noktalar

- Saldırıların temelinde her zaman istihbarat vardır.
- Yapacağını bir parola kırma saldırısı için öncesinde kurum veya şahısa karşı bir istihbarat çalışması yapıldıysa ve burada internete sızdırılmış bir parola yakalandıysa bu kesinlikle wordlistlere eklenmelidir.
- En doğru saldırı, istihbarat eşliğinde gerçekleşecek!
- Baştan sona tüm adımları doğru atmak bu yüzden önemli. Sızıntı kaynaklarını kontrol etmek gerek.
  - Paste siteleri
  - Haveibeenpwned vs.

Parola Kırma Saldırılarında Püf Noktalar

- Parola tahmini için brute force (kaba kuvvet) saldırıları gerçekleştirilebilir. Bu saldırıların dezavantajları şöyledir:
  - Yapılan saldırı sonucu kullanıcıların hesapları kilitlenebilir. Bknz: Lockout Policy
  - Bu yapılan saldırı sonrası ağ cihazlarında veya SIEM üzerinde çok fazla alarm üretilebilir. Bu durum işimize gelmeyecektir.
- Bir sisteme sızıldığında oradan parola özetleri (hash) elde edilebilir. Bu durumda Hash Crack saldırısı gerçekleştirmek gerekir.
  - Genelde localde ve sessiz, sakin bir süreç ile tamamlanır.
  - Elde edilen hash bilgileri kırıldığında siber saldırı evrimleşir.

Parola Kırma Saldırılarında Püf Noktalar

- Bir sisteme sızıldığında ve elde edilen hashler kırıldığında siber saldırı evrimleşir dedik. Neden?
  - Kurum içi parola politikaları genelde yeterince sıkılaştırılmış olmuyor.
  - Bu kırılan parola ile bir Password Spraying Attack gerçekleştirildiğinde birçok sistemin parolasının aynı olduğu görülebilir.
  - Böylece elde edilen bir parola aracılığı ile birden fazla sisteme sızılabilir.
  - Domain exploitation konusunu hatırlayın ☺ Belki de domain admine giden yolu elde etmenize olanak sağlayacaktır.

Saldırı Türleri

- Aktif Saldırılar:
  - Brute Force (Kava Kuvvet) Saldırıları
  - Password Spraying Saldırıları
- Pasif Saldırılar:
  - Hash Crack Saldırıları
  - Rainbow Table Saldırıları

Wordlist Oluşturma

- Bir parola kırma saldırısı içerisinde random oluşturulacak parola kombinasyonları yerine tespit edilen bir formata göre kendinize wordlist oluşturabilirsiniz.
- Bu formatı nasıl tespit edebilirsiniz?
  - Siber istihbarat ☺
  - Aynı kurum veya şirketten birden fazla kişinin parolası internete sızmış mı?
  - Sızdıysa aralarında bir benzerlik var mı?
    - Ankara8817!
    - Ankara7625!

Wordlist Oluşturma

- Wordlist oluşturulurken genelde crunch aracını kullanıyoruz.
- Oldukça kullanışlı ve esnek, dolayısıyla istediğiniz kombinasyonları üretmenize olanak sağlıyor.
- Basit kullanım:
  - crunch 6 7 abc123
    - 6 ve7 karakterden oluşan ve içeriğinde abc123 karakterlerini barındıran bir wordlist
  - crunch 6 8 1234567890 -o numericwordlist.lst
    - 6 ve 8 karakterden oluşan ve içeriğinde tüm rakamları barındıran bir wordlist

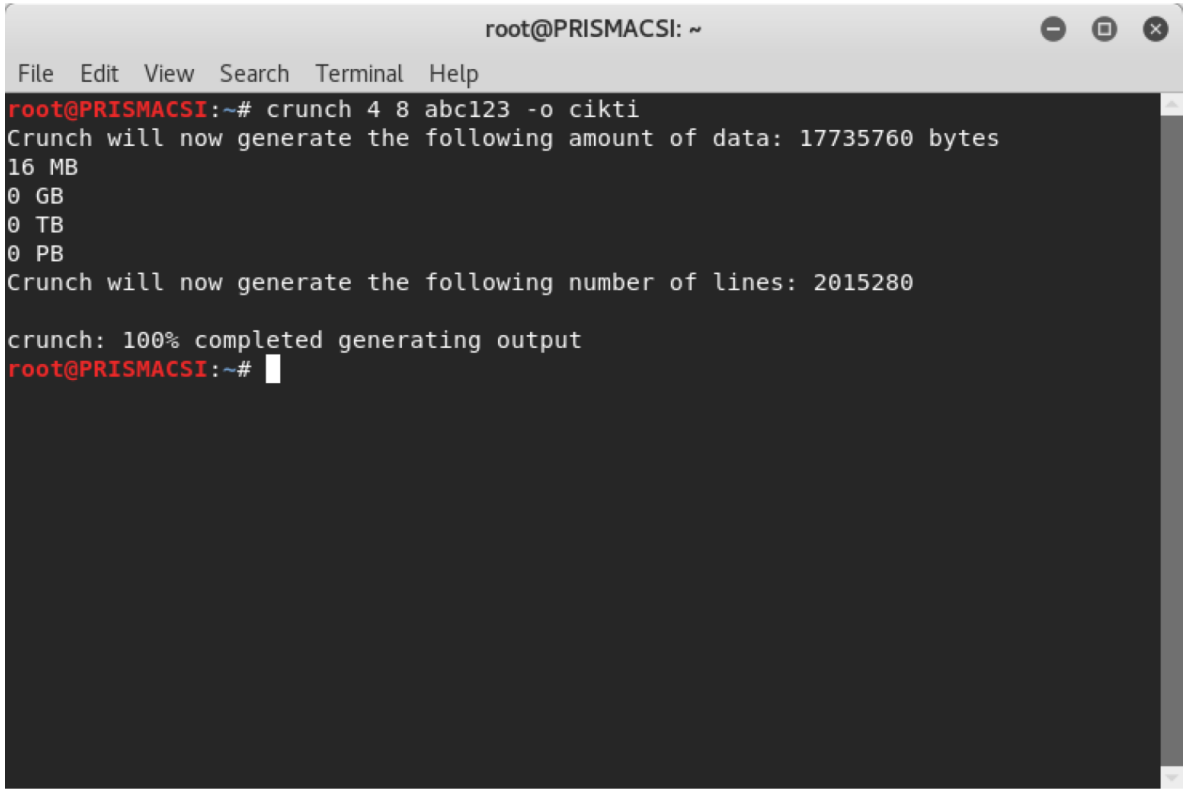
Wordlist Oluşturma

- Peki ya biraz önce keşfettiğimiz Ankara'lı formata göre bir parola listesi oluşturmak istesek?
  - Ankara0000!
  - Ankara0001!
  - Ankara0002!
- İşte bu noktada crunchın güzel parametrelerinden faydalanabilirsiniz.
  - crunch 11 11 1234567890 –t Ankara@@@@! –o wordlist –z
    - -z parametresi ziplemek amacıyla kullanılır

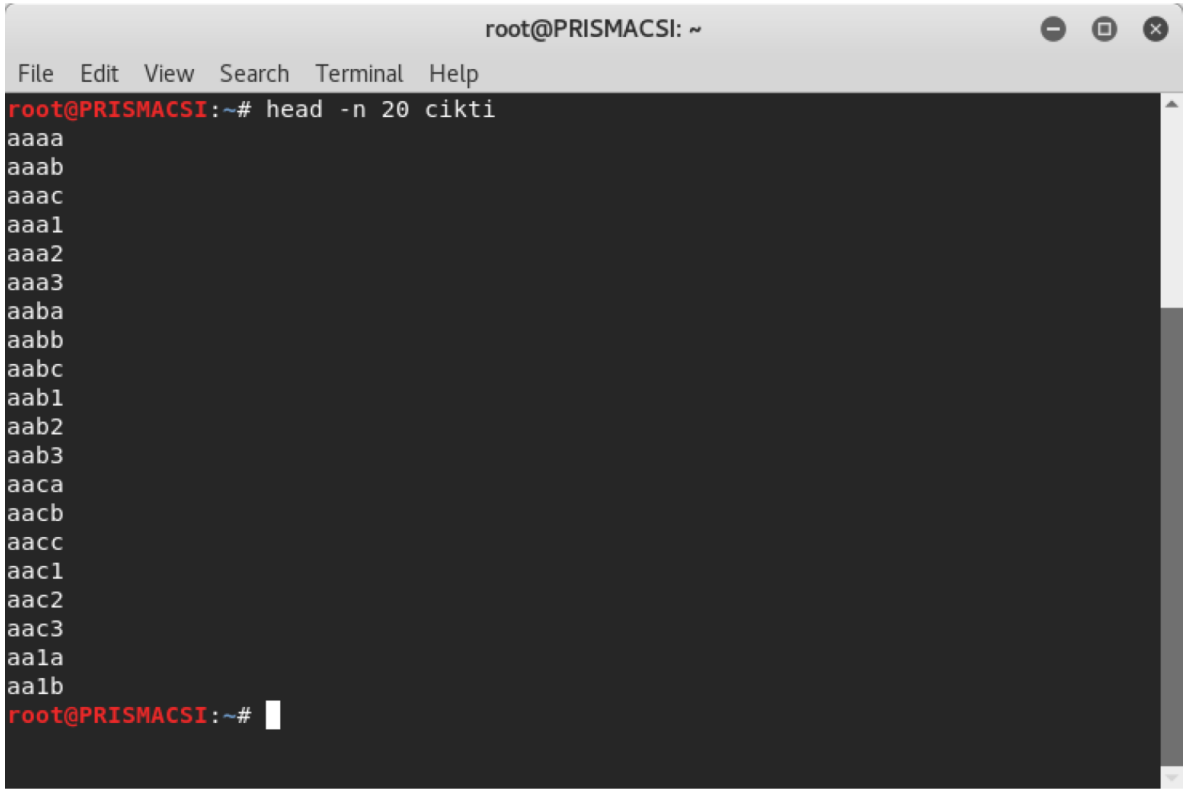
Wordlist Oluşturma

- Karakter setleri ile de bir wordlist oluşturabilirsiniz.
- Karakter listeleri şurada:
  - /usr/share/rainbowcrack/charset.txt
  - crunch 7 7 -f /usr/share/rainbowcrack/charset.txt mixalpha -o liste -z

Crunch - Uygulama



Crunch - Uygulama



CUPP - Uygulama

- CUPP isim, soy isim, nickname, doğum tarihi gibi parametreleri alarak wordlist oluşturmaktadır.

```
root@kali:~/Desktop/cupp# ./cupp3.py -i

  cupp.py!                  # Common
     \                      # User
      \   ,__,              # Passwords
       \  (oo)____          # Profiler
          (__)    )\
             ||--|| *   Muris Kurgas <j0rgan@remote-exploit.org>



[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

First Name: prisma
Surname: csi
Nickname:
Birthdate (DDMMYYYY):
```

Hydra

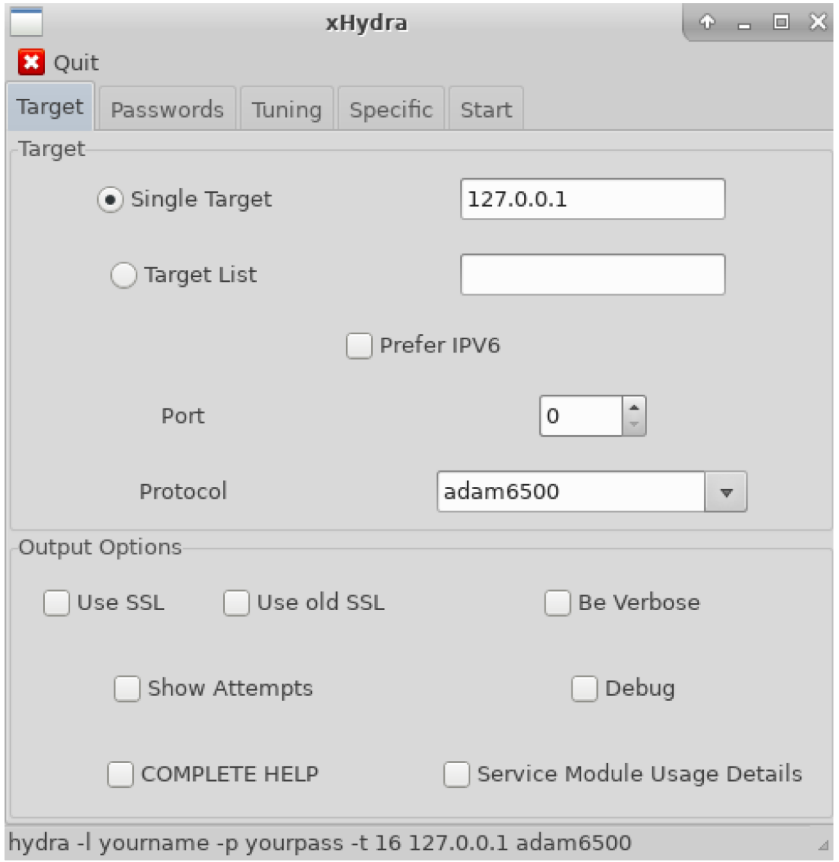
- Tespit edilen servislere bruteforce saldırıları ypaılmak istendiğinde hydra oldukça kullanışlıdır.
- Aracı komut satırı üstünden veya var olan GUI'si (xHydra) aracılığı ile kullanabilirsiniz.
- Bir veya birden fazla kullanıcıya veya hedefe parola kırma saldırısı gerçekleştirebilirsiniz.

Hydra - Uygulama

- Örnek kullanımlar:
  - hydra -l user -P passlist.txt ftp://192.168.0.1
  - hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
  - hydra -C defaults.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5
  - hydra -l admin -p password ftp://[192.168.0.0/24]/
  - hydra -L logins.txt -P pws.txt -M targets.txt ssh

xHydra - Uygulama

- xHydra, Hydra'nın grafik arayüzlü halidir.



Medusa

- Komut satırı üzerinden kullanılan ve bizim en sık kullandıklarımız arasında yer alan bir parola kırma saldırısı aracıdır.
- Yine hydra nın özelikleri içerisinde de bulunduğu gibi birden fazla hedefe saldırı yapılabilir ve wordlistler aracılığıyla birçok protokole parola kırma saldırısı gerçekleştirilebilir.

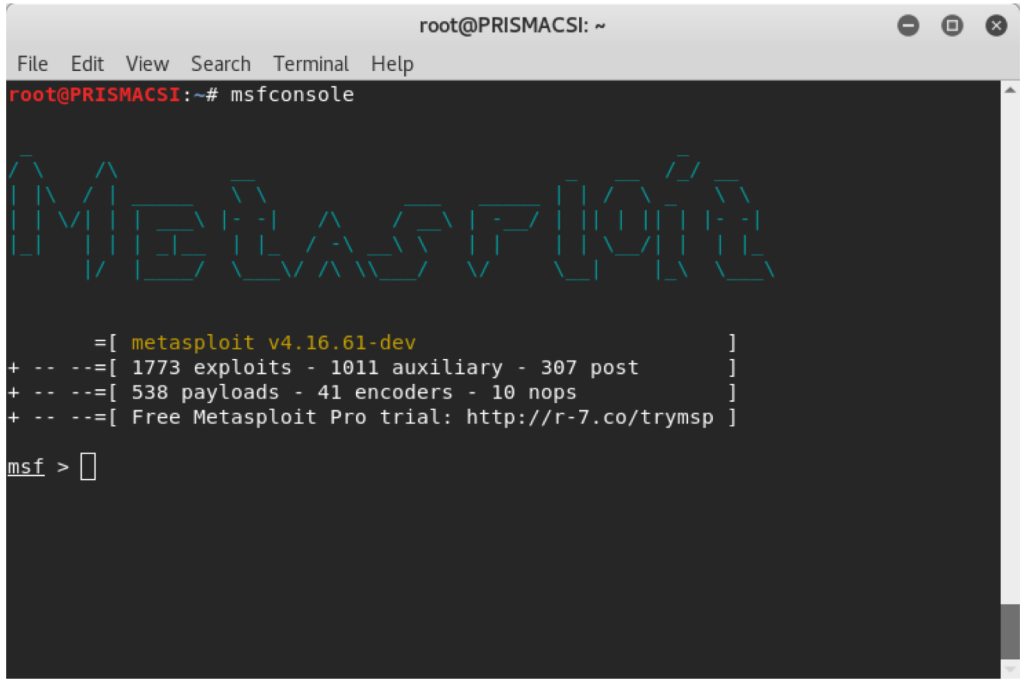
Medusa - Uygulama

- medusa -h 10.0.1.5 -u "root" -P parolalistesi.txt -M http
- medusa -h 10.0.1.5 –U userlistesi.txt –p "secretpass" -M smbnt
- medusa -h 10.0.1.5 -u "root" -P parolalistesi.txt -M ftp
- medusa -h 10.0.1.5 -u "root" -P parolalistesi.txt -M telnet

- Medusa aşağıdaki tüm servisleri desteklemektedir.
  - AFP, CVS, FTP, HTTP, IMAP, MS-SQL, MySQL, NetWare NCP, NNTP, PcAnywhere, POP3, PostgreSQL, REXEC, RLOGIN, RSH, SMBNT, SMTP-AUTH, SMTP-VRFY, SNMP, SSHv2, Subversion (SVN), Telnet, VNC

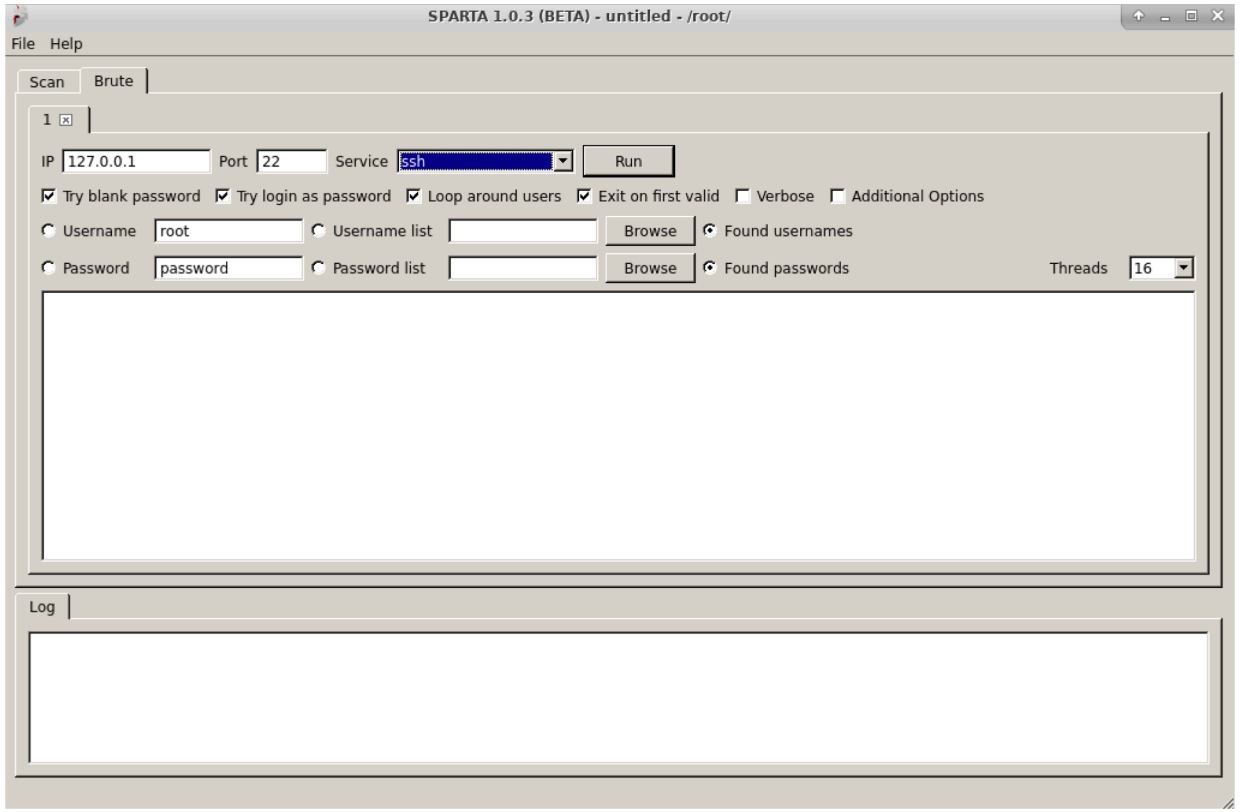
Metasploit

- Metasploit içerisinde parola kırma saldırılarına imkan sunan auxiliary modülleri barındırmaktadır.
- Örnek olarak smb ye bruteforce saldırısı yapılmak istendiğinde aşağıdaki modül kullanılabilir.
  - use auxiliary/scanner/smb/smb_login



Sparta

- Sparta basit seviyede zafiyet tarama aracı olmasıyla birlikte arayüz üzerinden bruteforce parola kırma saldırılarına izin veren kullanışlı bir toldur.



Patator

- Kali'de default olarak kurulu olarak gelmez.
  - https://github.com/lanjelot/patator
- Komut satırından çalışmaktadır ve oldukça basit bir kullanımı vardır.

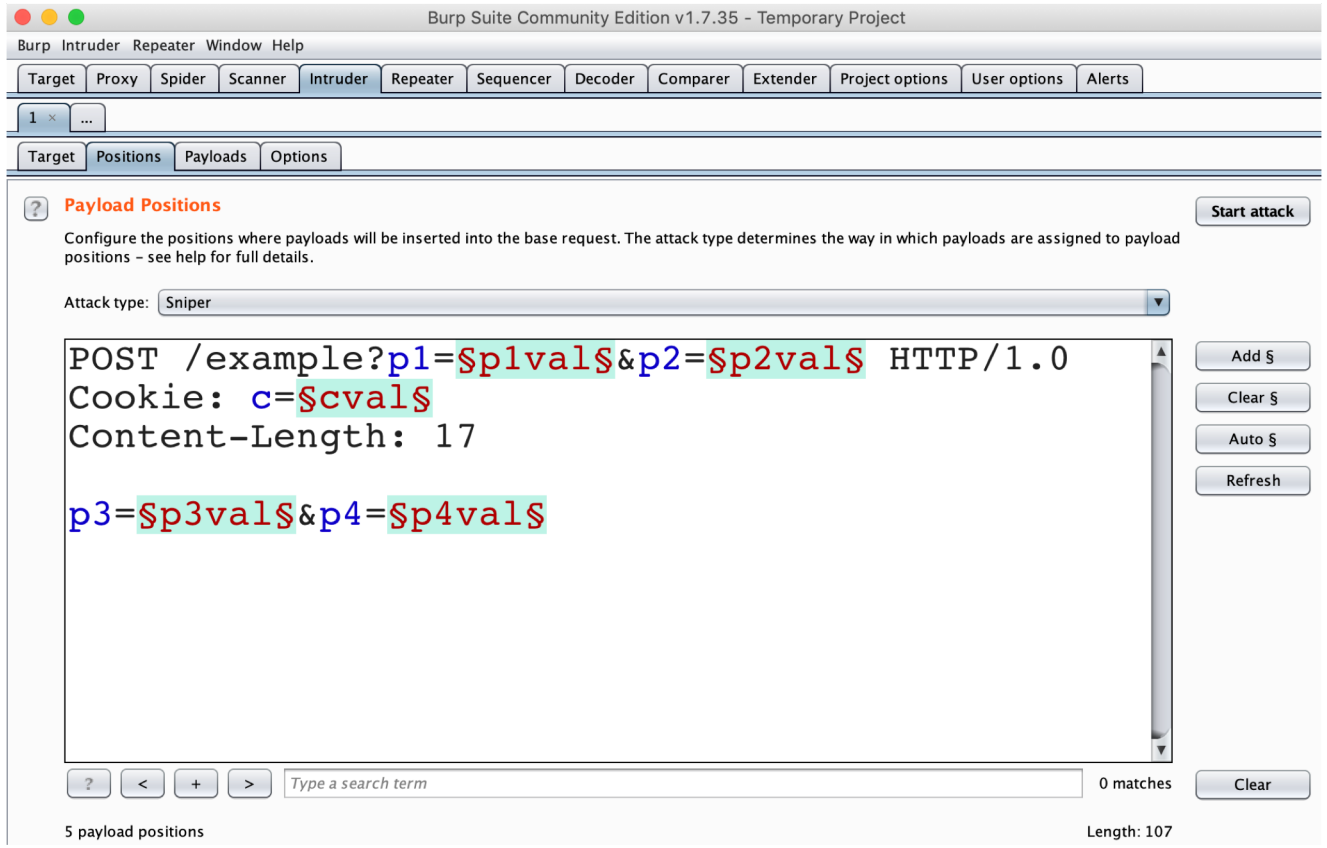
```
root@kali:~# patator ssh_login --help
Patator v0.7 (https://github.com/lanjelot/patator)
Usage: ssh_login <module-options ...> [global-options ...]

Examples:
  ssh_login host=10.0.0.1 user=root password=FILE0 0=passwords.txt -x ignore:mesg='Authentication failed.'

Module options:
  host          : target host
  port          : target port [22]
  user          : usernames to test
  password      : passwords to test
  auth_type     : type of password authentication to use [password|keyboard-interactive|auto]
  keyfile       : file with RSA, DSA or ECDSA private key to test
  persistent    : use persistent connections [1|0]
```

Burp Suite

- Web uygulamalarına Burp Suite Intruder kullanılarak bruteforce saldırısı gerçekleştirilebilir.
- Uygulama



Hash Kırma Saldırıları

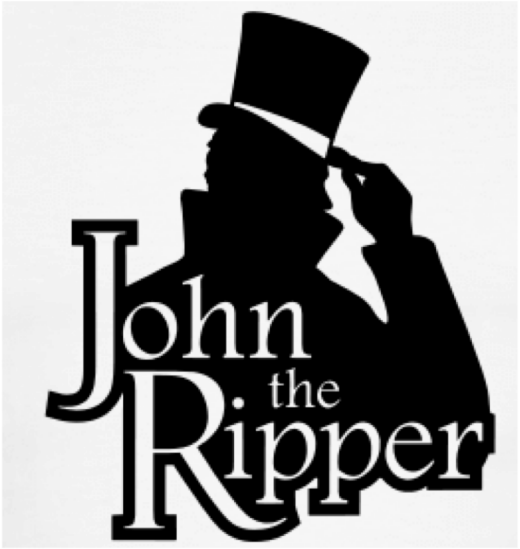
- Hash-Buster
  - https://github.com/s0md3v/Hash-Buster
  - Online birçok adresten otomatize hash kontrolü
  - buster –s <hash>
  - buster –f /root/hash.txt
  - buster –d /root/Desktop

Hash Kırma Saldırıları

- John-the-ripper
- Offline (Çevrimdışı) hash kırma aracı olarak tanımlanır.
- Oldukça kullanışlı ve pratiktir.
- Bir linux makineye sızdınız ve hashleri alacaksınız.
  - unshadow /etc/passwd /etc/shadow > hashlist
  - john --wordlist /usr/share/wordlists/rockyou.txt hashlist
  - cat /root/.john/john.pot

Hash Kırma Saldırıları

- John-the-ripper birçok formatı desteklemektedir.
  - john --list=formats : formatları görüntüleyebilirsiniz.
  - john --format=LM hashfile
  - john --format=oracle hashfile

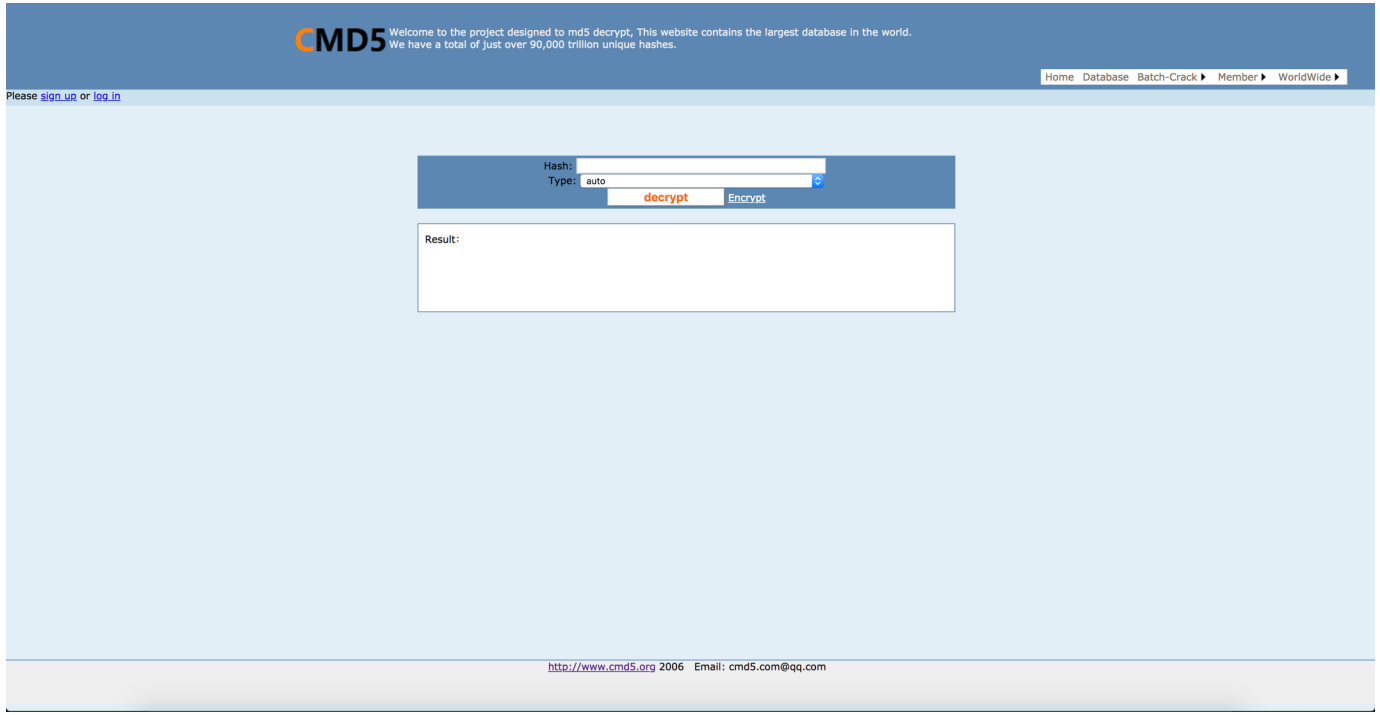


Hash Kırma Saldırıları

- Hashcat yine komut satırı üstünden yönetebileceğiniz ve size gpu cracking dahil birçok fonksiyon sunan gelişmiş bir parola kırma aracıdır.
- Birçok parametresi mevcut bu yüzden kullanırken manuali okumakta fayda var.
  - hashcat -h
- Örneğin bir md5 ile hashlenmiş parolayı kırmak istediğinizde:
  - hashcat -m 0 -a 0 -o passlist hashlist /usr/share/wordlists/rockyou.txt
    - -m 0 : md5 algoritmasını işaretlemekte
    - -a 0 : sözlük saldırısı yapmayı işaretlemekte

Rainbow Table Atakları

- Bruteforce ataklar zaman alıyor.
- Daha önceden elimizde hashlenmiş bir wordlist varsa?
  - parola - hash karşılığı
  - parola2 - hash karşılığı
  - parola3 - hash karşılığı
- Saniyeler içerisinde çözümlenebilir.
  - www.cmd5.org



Hafızadan Parola Elde Etme

- Mimikatz ile hafızadan açık metin parola yakalayabilirsiniz.
- Bunun için sistemde yetkili bir session elde etmek gerekiyor.
- Mimikatz binaryleri ile veya crackmapexec ile bu işi çözebilirsiniz.
  - https://github.com/gentilkiwi/mimikatz
    - mimikatz.exe
    - privilege::debug
    - sekurlsa::logonPasswords full
  - crackmapexec smb 10.0.1.5 -u Administrator -p 'Passwd123!' -M mimikatz

Pass the Hash Saldırıları

- Crackmapexec ile gösterimini yapmıştık.
- Windows makineden hashdump ile alınan hashleri bir başka suncuya giriş için kullanabilirsiniz.
- Hash kırmanıza gerek yok, direk hash i parola olarak kullanabiliyorsunuz.
- Metasploit üzerindeki smb_login ile giriş denemesi yapabilir, psexec exploiti ile makineye sızabilirsiniz.
- Crackmapexec :
  - crackmapexec smb 10.0.1.5 -u username -H NTHASH

Uygulamalar

Sorular?

İletişim

www.prismacsi.com

info@prismacsi.com

0 850 303 85 35

/prismacsi