Windows Hacking - I

BGM 553 - Sızma Testleri ve Güvenlik Denetlemeleri-I

Bilgi Güvenliği Mühendisliği
Yüksek Lisans Programı

Dr. Ferhat Özgür Çatak
ozgur.catak@tubitak.gov.tr

İstanbul Şehir Üniversitesi
2017/2018 - Güz

İçindekiler

İçindekiler

Parola Saldırı Yöntemleri - Non-Electronic Attacks

Parola Saldırı Yöntemleri

- **Sosyal Saldırılar (Social Attacks)**:
  - *Omuz sörfü(shoulder surfing)*: En kolay yöntem, keskin bir göz ve güçlü bir hafıza gerekli.
  - *Çöp karıştırma (dumpster diving)*: yapışkan notlar üzerinde bulunan parolaları ele geçirme
  - *Sosyal Mühendislik (social engineering)*: En başarılı yöntemlerden biri, e-mail, telefon ile elde etme

Parola Saldırı Yöntemleri - Electronic Attacks

Parola Saldırıları

- **Aktif Online Saldırılar** : Saldırgan kurban bilgisayar ile direk iletişime geçerek parola saldırısı düzenlemektedir.
  - Sözlük ve Kaba Kuvvet Saldırıları
  - Hash injection
  - Trojan/Spyware/KeyLogger
  - Parola Tahmini
- **Pasif Online Saldırılar**: Kurban ile direk iletişime geçmeden parola saldırısı düzenlenmektedir.
  - Ağ dinleme
- **Offline Saldırılar** : Saldırgan, kurban bilgisayarın parola dosyasını kopyalar farklı bir sistemde parola saldırısı düzenler
  - Pre-Computed Hashes
  - Brute-Force

Aktif Online Saldırılar

Sözlük Saldırısı

Kullanıcı hesaplarının ele geçirilmesi amacıyla kullanılan saldırı aracına bir **sözlük dosyası** yüklenir

Kaba Kuvvet Saldırısı

Parola elde edilinceye kadar saldırı aracı bütün kombinasyonları dener

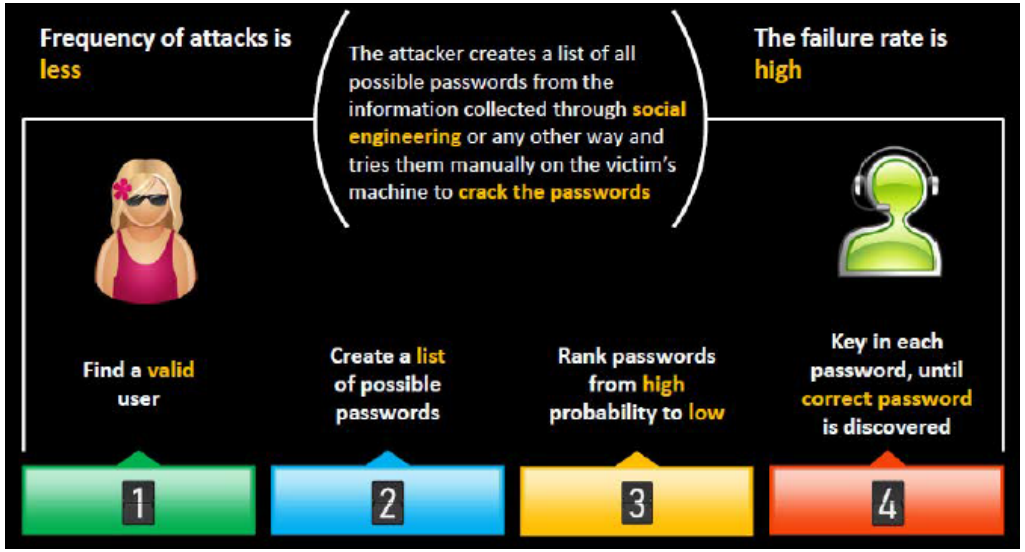
Kural Tabanlı Saldırısı

Saldırgan, parola hakkında bilgi sahibi olduğu durum

Password Guessing

Parola Tahmini

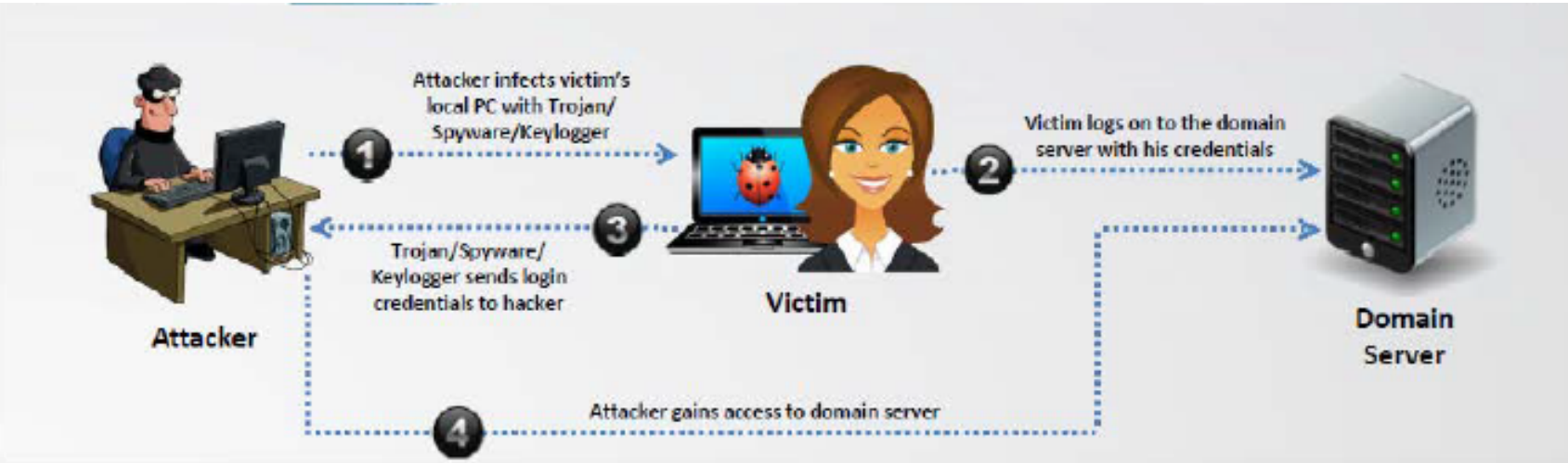
- Öneri: *password policy enforcement* sağlayan en kolay parolaların test edilmesi.
- Parola uzunluklarına bakılması
- Örnek parola: **!1qASw2q**. Klavye üzerinde birbirine yakın duran harfler
- Varsayılan parolalar
  - cirt.net



Aktif Online Saldırılar I

Trojan/Spyware/Keylogger

- Saldırgan, kurban bilgisayara zararlı yazılım yükleyerek kullanıcı adı/parola bilgisine elde eder.
- Kullanılan trojan/keylogger gibi bir zararlı yazılım arka planda çalışarak kullanıcı bilgilerini saldırgana gönderir.



Aktif Online Saldırılar II

Örnek yöntem: Gina

- Microsoft *Graphical Identification and Authentication (GINA)*, kullanıcı bilgilerinin elde edilmesi amacıyla kullanılan bir yöntemdir.
  - Windows oturum açma sürecinde uygulama geliştirmeye olanak sağlamaktadır. Tokens v.s.
  - Gina, msgina.dll dosyasında gerçekleştirilmiştir be WinLogon.exe tarafından oturum açma sırasında yüklenir.
  - WinLogon ve msgina.dll arasında geliştirilen diğer dll'ler yüklenir (man-in-the-middle saldırısı gibi)
  - Hangi DLL dosyalarının yükleneceği registry'de yer alır.

    HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL

- Genelde yapılan system32 veya drivers gibi özel kalsörlerinin içerisin sys veya dll uzantılı dosyalar oluşturarak içerisine kullanıcı adı/parola bilgisini girmektedir.

Winlogon Notify

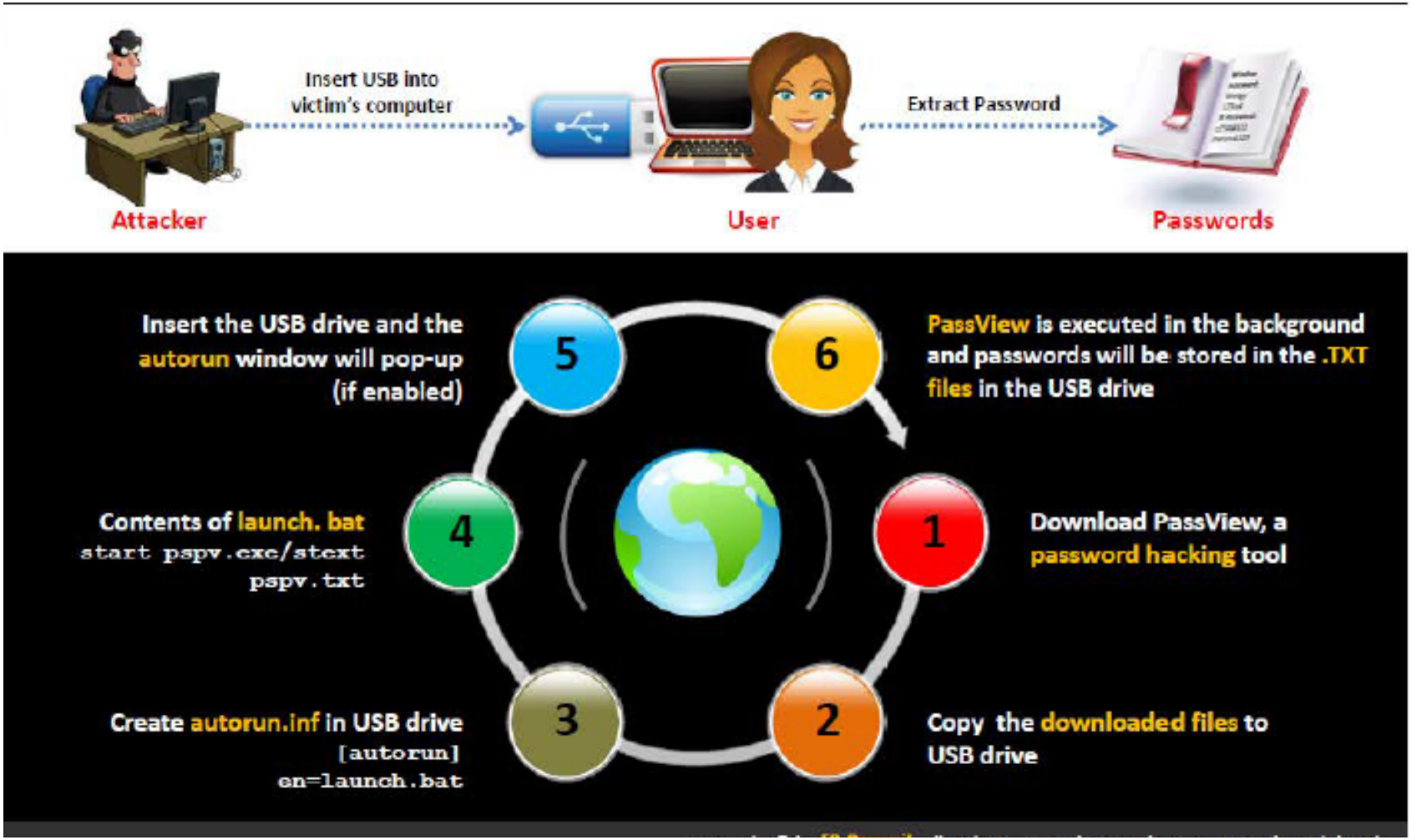
Winlogon Notify

- Zararlı yazılımlar **Winlogon** eventlerine kayıt olmaktadırlar: **logon**, **logoff**, **startup**, **shutdown**, **lock screen**
- İlgili registry kayıdı:

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\

- WinLogo.exe bir event oluşturulduğunda ilgili registry kayıdında yer alan DLL çalıştırılır.

USB Drive

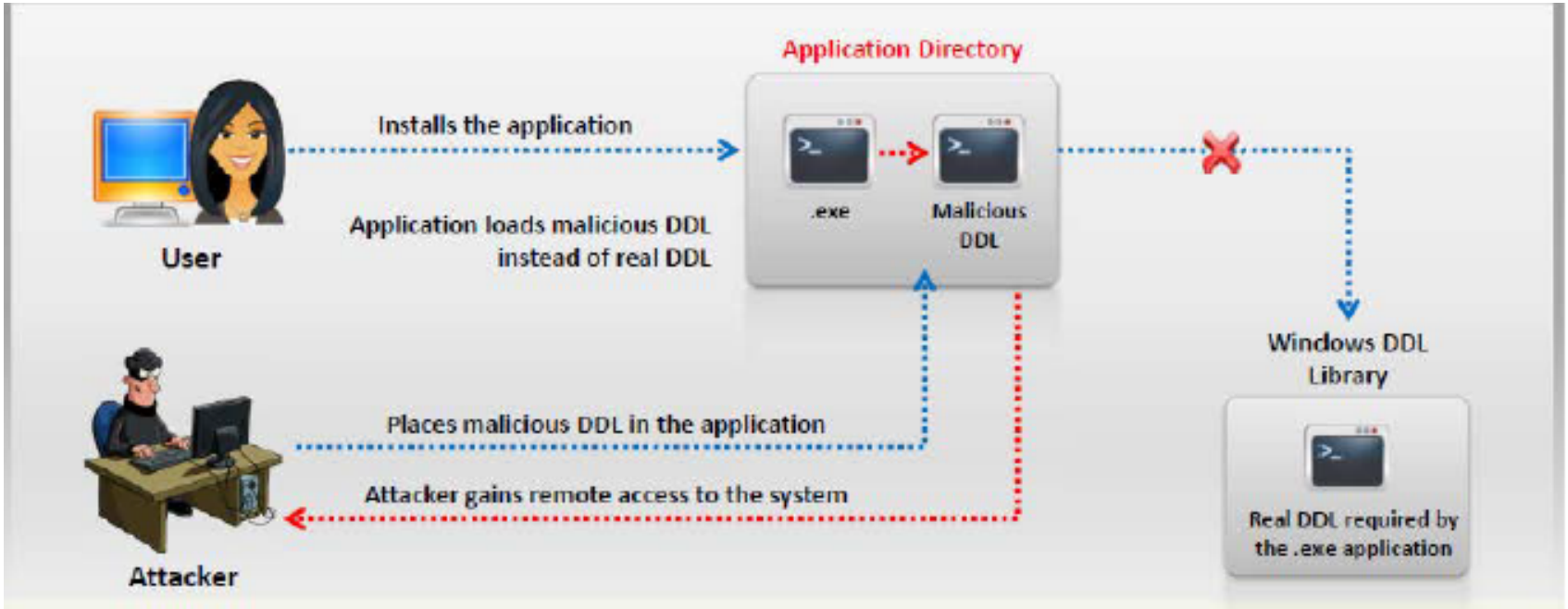

Insert USB into victim's computer
Extract Password
Attacker
User
Passwords
Insert the USB drive and the autorun window will pop-up (if enabled)
5
6
PassView is executed in the background and passwords will be stored in the .TXT files in the USB drive
Contents of launch. bat
start pspv.exe/stext pspv.txt
4
1
Download PassView, a password hacking tool
Create autorun.inf in USB drive
[autorun]
en=launch.bat
3
2
Copy the downloaded files to USB drive

DLL Hijacking I

DLL Load-Order Hijacking

- Windows işletim sisteminde DLL'ler için dosya arama sırası şu şekildedir:
  - The directory from which the application loaded
  - The current directory
  - The system directory
  - The Windows directory
  - The directories listed in the *PATH* environment variable
- KnownDLLs registry kayıdı ile Windows spesifik olarak System32 içerinde bakmasını istemektedir.
- Fakat System32 klasörü dışında yer alan dll için DLL load-order hijacking yapılabilir.
- Örnek olarak, Explorer.exe için *ntshrui.dll System32* klasöründe yer almaktadır. Fakat *ntshrui.dll* KnownDLLs içinde yer almaz. Varsayılan arama sırası izlenir. Eğer zararlı kod enjecte edilmiş bir *ntshrui.dll* yüklenirse Explorer.exe orjinal yerine bunu yükler.
- KnownDLLs içinde yer almayan her bir dll için bu şekilde bir tehdit mevcuttur. *Explorer.exe* yaklaşık 50 adet bu şekilde tehdit altında DLL dosyası mevcuttur.

DLL Hijacking II



Parola Özetleri ve Şifreleme I

Parola Özetleri

- Windows işletim sisteminde parolalar iki farklı yöntemle saklanmaktadır.
- **LM Hash (LAN manager)**:
  - Parolalar en fazla 14 karakter içerecek şekilde ve büyük harf olarak kayıt edilir.
  - 14 karakter parola 7 + 7 şeklinde 2 farklı parolaya ayrılır. Herbir parça ayrı şifrelenir ve tek bir özet olacak şekilde birleştirilir.
  - Windows Vista ve daha güncel işletim sistemlerinde kaldırılmıştır. Bazı sistemlerde geri-uyumluluk için aktif olarak kullanılabilmektedir.
  - LM Hash, Windows Vista ve üzeri işletim sistemlerinde kapatılmıştır. SAM Dosyasında LM alanı *blank* olarak geçmektedir.
- **NT Hash**:
  - 127 karakter. Büyük, küçük harf kabul eder.
  - Günümüzde 2. sürümü bulunmaktadır.

Parola Özetleri ve Şifreleme II

Parola Kayıtları

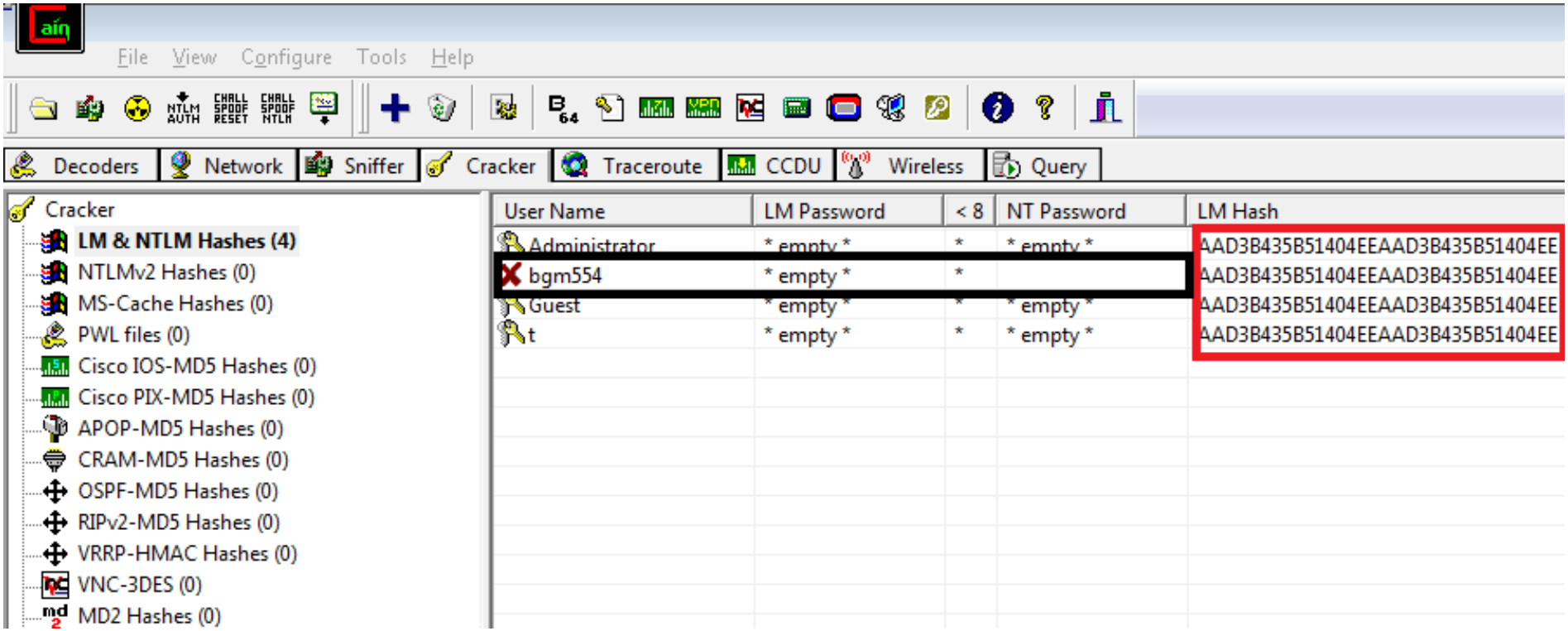
- Windows işletim sisteminde parolalar **SAM veritabanı** veya active directory server olması durumunda **AD veritabanında** saklanır.
- Veritabanı kopyalandığı veya çalındığı zaman çeşitli araçlar kullanılarak özet değerleri ele edilebilir.
  - bkhive/samdump2
  - John the Ripper
  - Cain and Abel

Cain and Abel NTLM I

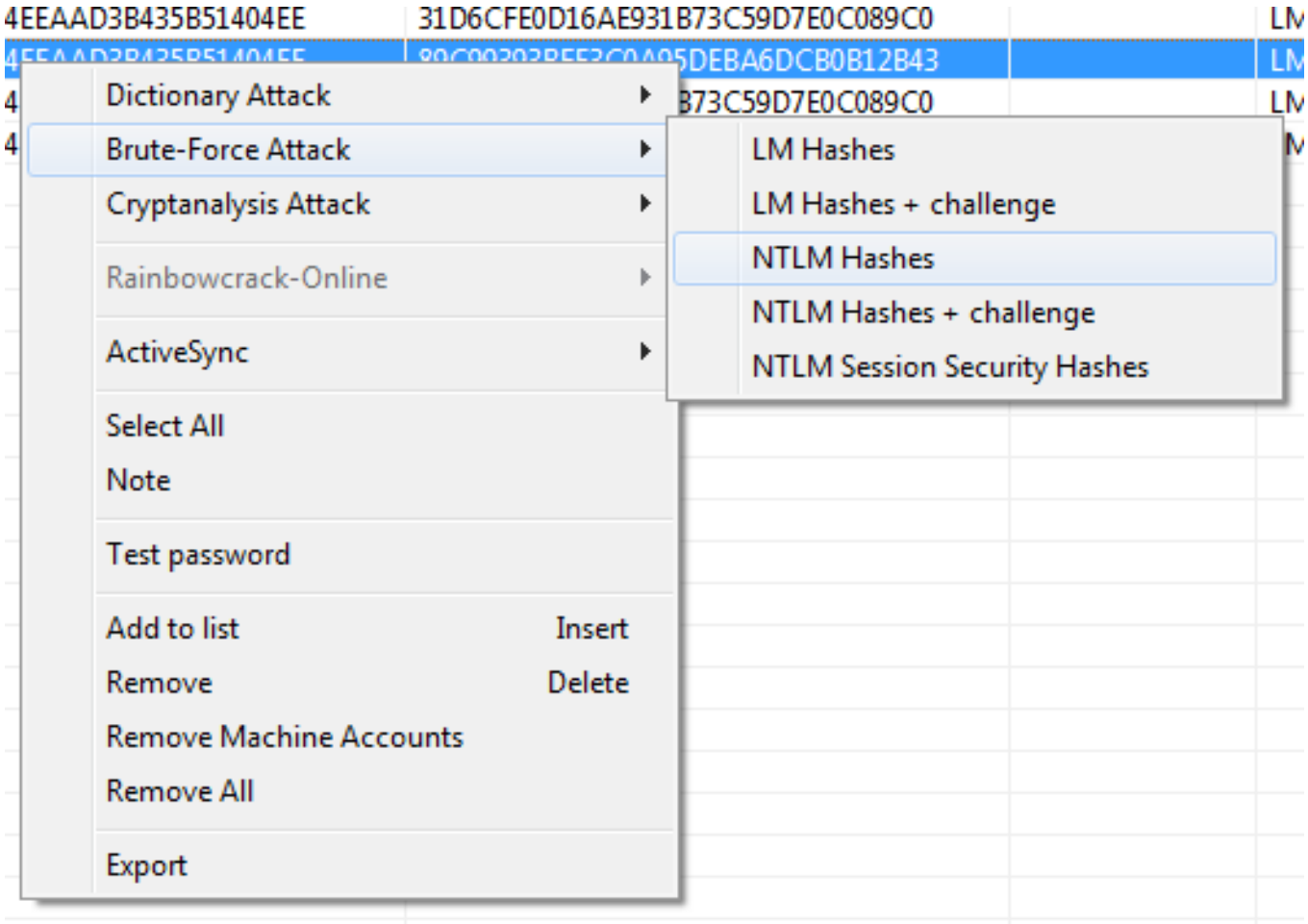
Cain and Abel

- En çok kullanılan araç
- Cracker sekmesi ile parola özetleri elde edilebilir.
  - Importing the hashes from the **local system**
  - hashes from a **text file**
  - importing hashes from the SAM **database**. Başka bir sistemden elde edilmiş SAM veritabanı Cain içerisine eklenerek parola elde edilebilir.

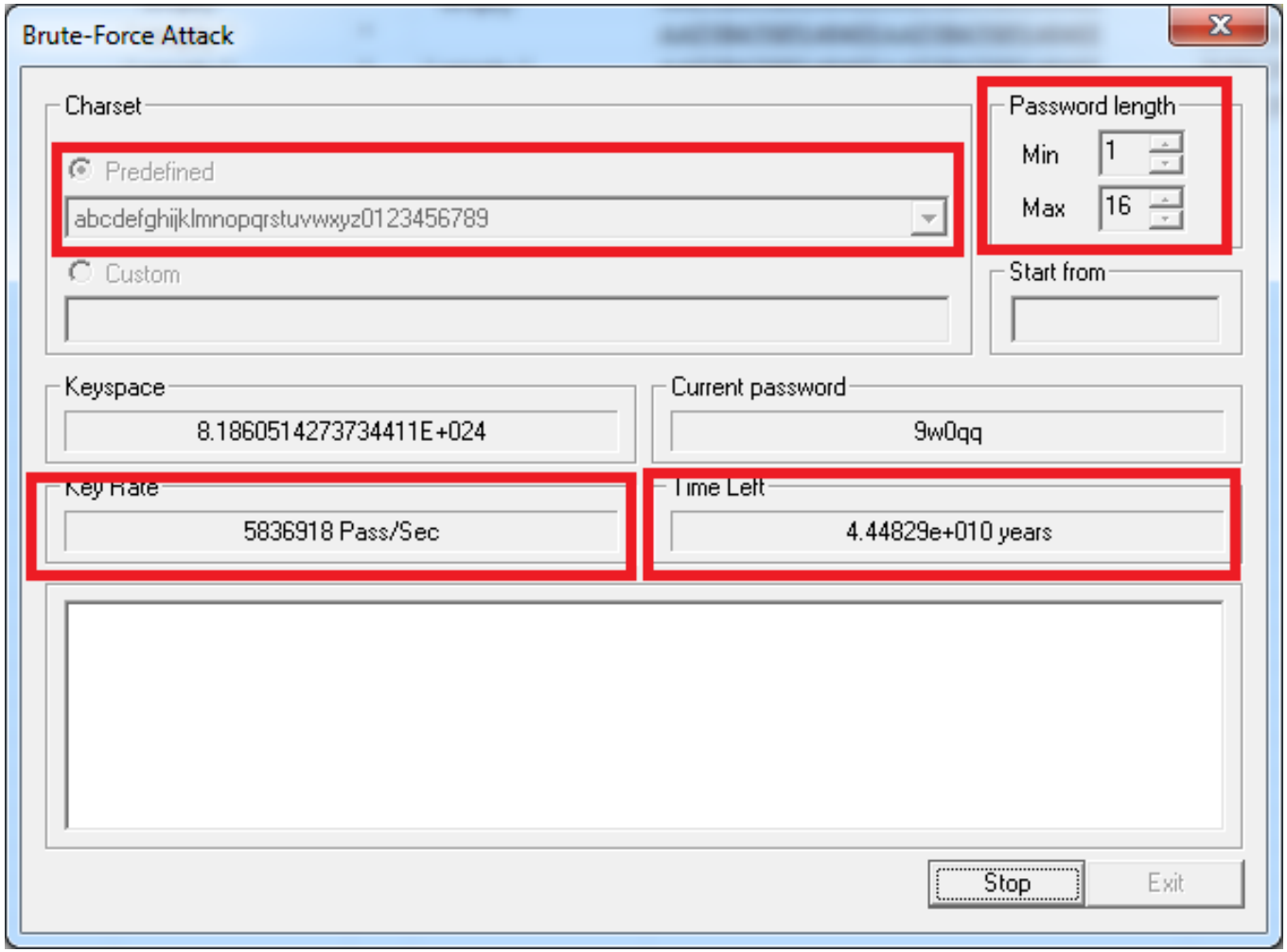
Cain and Abel NTLM II



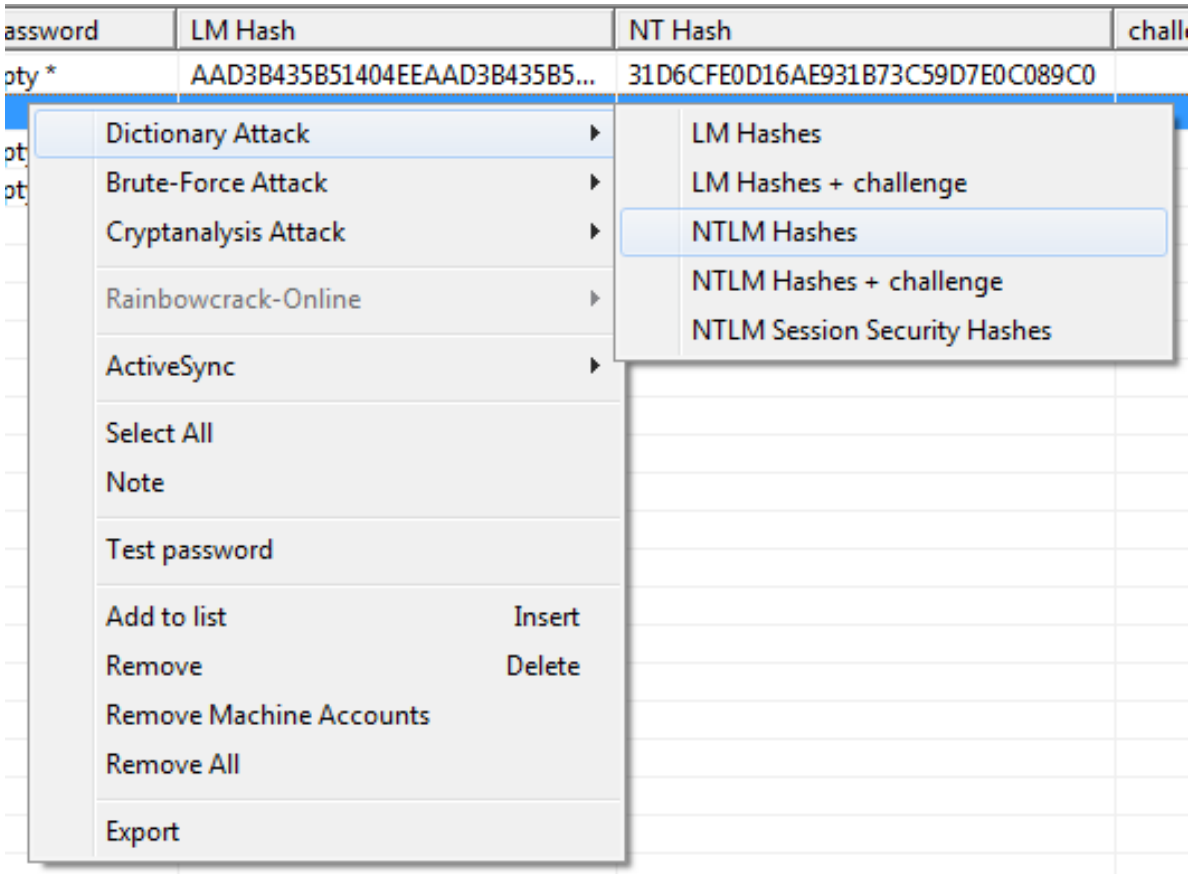
Cain and Abel NTLM III



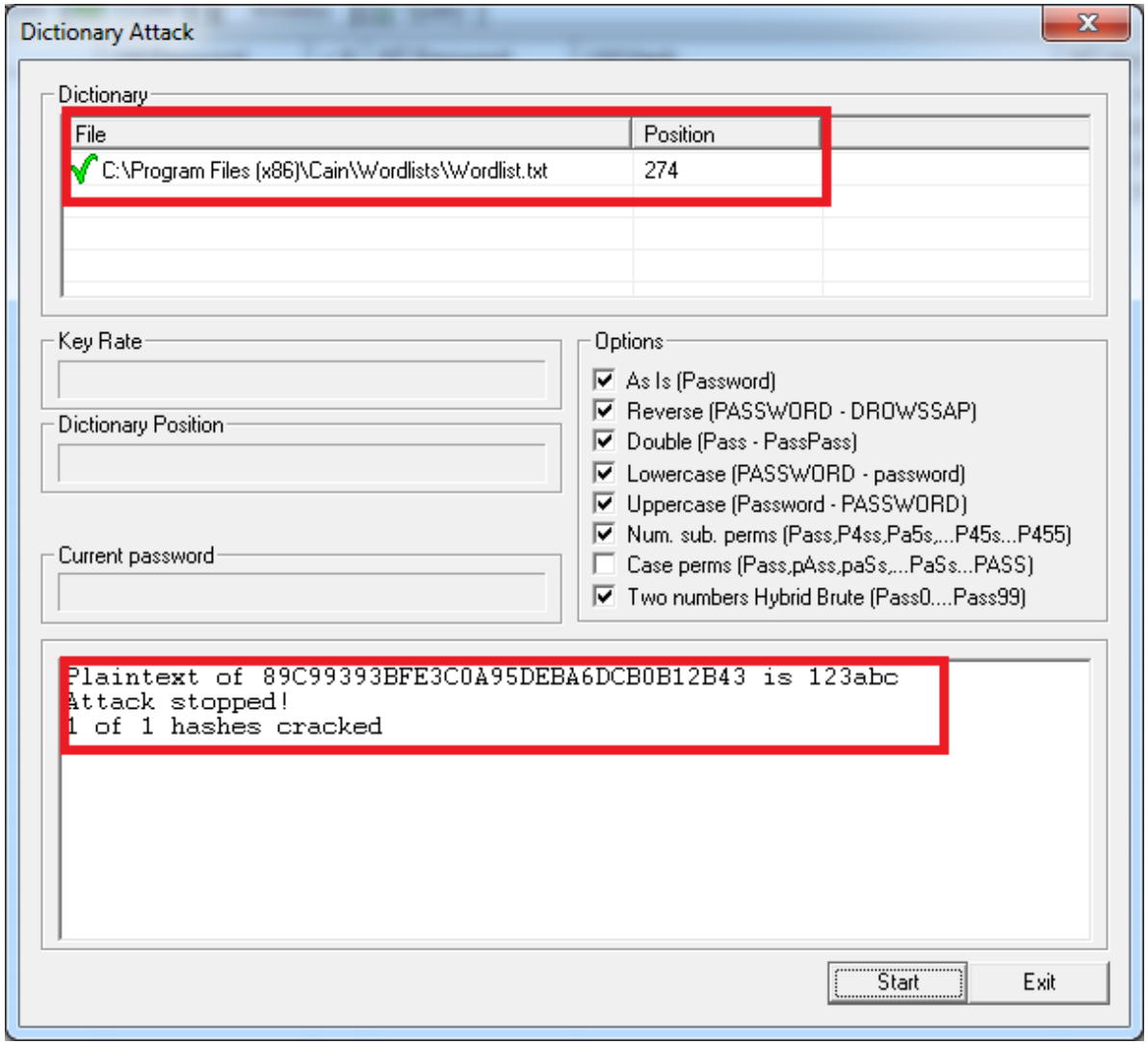
Cain and Abel NTLM IV



Cain and Abel NTLM V



Cain and Abel NTLM VI



SAM Veritabanı ve SYSKEY

SAM Veritabanı ve SYSKEY

- Windows NT 4 Service Pack 3 ile beraber SAM güvenliği artırıldı.
- SAM veritabanı 128-bit şifreleme, decryption key ise sistem dosyasında tutulmaya başlandı.
- SAM dosyası ele geçirilse bile Syskey olmadan SAM açılamaz.
- **BKHive**: SAM dosyasının açılabilmesi için system dosyasından bootkey elde edilir.
- **Cain and Abel** aynı şekilde bunu yapacaktır.

Salting İşlemi I

Salting

- Herhangi bir parolanın özet değerini tekil hale getirmek için kullanılan yöntem.
- Aynı parolaların farklı özet (hash) değeri oluşmasını sağlamak için ek bir değerin konulması
- **12-bit** salt değeri, md5 özeti uzayını **4096** kat artırmaktadır.
- *precomputed hash attack* veya *rainbow table attack* için koruma sağlamaktadır.

Salting İşlemi II

hash(”hello”) = 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824
hash(”hbllo”) = 58756879c05c68dfac9866712fad6a93f8146f337a69afe7dd238f3364946366

hash(”hello” + ”QxLUF1bgIAdeQX”) =
9e209040c863f84a31e719795b2577523954739fe5ed3b58a75cff2127075ed1 **hash**(”hello” +
”bv5PehSMfV11Cd”) =
d1d3ec2e6f20fd420d50e2642992841d8338a314b8ea157c9e18477aaef226ab **hash**(”hello” +
”YYLmfY6IehjZMQ”) =
a49670c3c18b9e079b9cfaf51634f563dc8ae3070db2c4a8544305df1b60f007

Salting İşlemi III

Salting

- **Windows işletim sisteminde ve Active Directory üzerinde salting işlemi yoktur.**
- Zayıf özet algoritmaları: MD5, SHA1
- *Önerilenler*: SHA256, SHA512, RipeMD, WHIRLPOOL, SHA3

Salt Gerçekleştirim Hataları

- **Public Salt veya Aynı Salt Kullanımı**: İki farklı kullanıcının aynı parolaya sahip olmaları durumunda, özet değerleri aynı olacaktır.
- **Kısa Salt**: Salt değerinin kısa olması durumunda saldırgan kolay bir şekilde Rainbow table oluşturabilir.

İçindekiler

Parola Kırma Tekniği I

Ön Bilgiler

- Özet (hash) işlemleri tek yönlüdür.
- Kullanılan matematik algoritmaları geri alınamaz şekilde tasarlanmıştır.
- Sözlük saldırısı (Dictionary attack) ile başarılı ve uzun sürmeyecek şekilde elde edilebilir.
- Sözlük dosyasında yer alan parolalar ilgili özet algoritması ile özeti alınarak ele geçirilmiş olan özet değeri ile karşılaştırılır.

Parola Kırma Tekniği II

Kaba Kuvvet Saldırısı (Brute Force Attack)

- Doğru parola elde edilene kadar olası kombinasyonlar
- Kesinlikle başarıya ulaşacaktır, fakat oldukça uzun süre alabilir.
- Hızlandırma yöntemleri
  - Parola politikasına uygun kaba kuvvet saldırısı yapılması.
  - GPU (graphic processor unit) kullanarak yapılan saldırılar.

Parola Kırma Tekniği III

Kaba Kuvvet Saldırısı Hızlandırma

- quad core i7 processor kullanarak yıllar sürecektir.
- https://arstechnica.com/security/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/
- 25 AMD Radeon HD9660 graphics cards
- Saniyede 350 milyar parola denemesi (NTLM).
- NTLM için 95^8 parola denemesi 5.5 saat
  - 95 printable chars: https://en.wikibooks.org/wiki/C%2B%2B_Programming/ASCII
- Linux-based GPU cluster üzerinde çalışan **Virtual OpenCL cluster platform**
- Tek bilgisayar üzerinde çalışma prensibi

Parola Kırma Tekniği IV

Hashcat: World's fastest password cracker

- Password-cracking suite optimized for GPU computing
- 44 farklı algoritma gerçekleştirimi
  - MD4, MD5, SHA1, SHA-224, SHA-256, SHA-384, SHA-512. SHA-3, Skip32, RipeMD160, Whirlpool, DES, 3DES ...
- Kaba kuvvet saldırısı yanında sözlük saldırısıda gerçekleştirebilmekte
- Saniyede 63 milyar SHA1 ve 180 milyar MD5 tahmini yapabilmektedir.
- **Sonuç**: saldırı teknikleri ve arkalarında bulunan güç artmaktadır.

Parola Kırma Tekniği V

```
hashcat -m 0 hashes wordlist.txt --force --potfile-disable
```

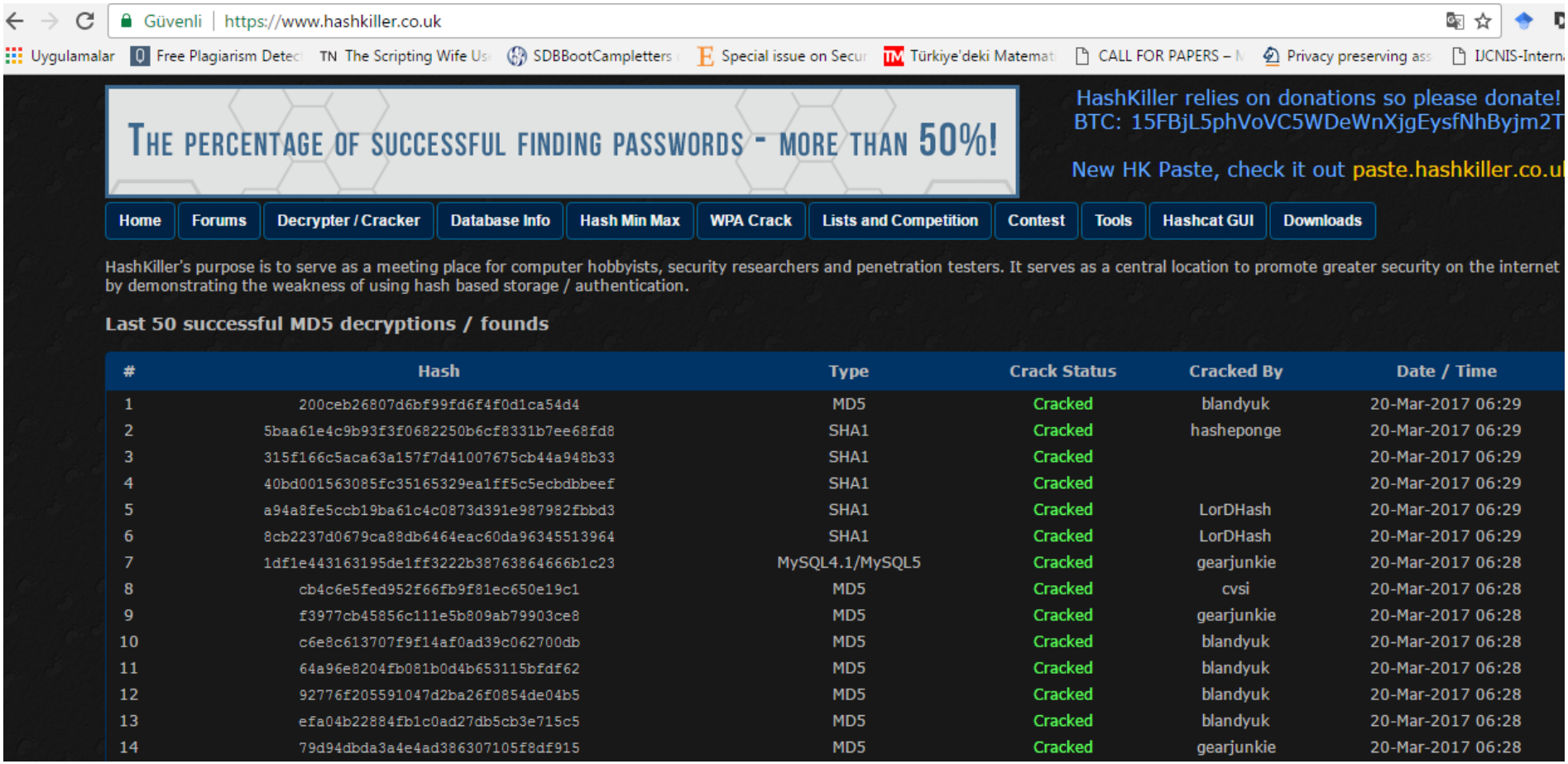
```
01b123de4f3da659c33ae098481b29d5:BGM554
eb61eead90e3b899c6bcbe27ac581660:HELLO
958152288f2d2303ae045cffc43a02cd:MYSECRET
2c9341ca4cf3d87b9e4eb905d6a3ec45:Test1234
75b71aa6842e450f12aca00fdf54c51d:P455w0rd
98bffa1e0b3872aa0813b0a62a2003ab:GuessMe3
b5af0b804ff7238bce48adef1e0c213f:S3CuReP455Word
5a53193b4cca4ccdabf3ccb1fa514162:HighlyUnlik3lyToB3Cr4ck3d…

Session..........: hashcat
Status...........: Cracked
Hash.Type........: MD5
Hash.Target......: hashes
Time.Started.....: Mon Mar 20 11:09:36 2017 (0 secs)
Time.Estimated...: Mon Mar 20 11:09:36 2017 (0 secs)
Input.Base.......: File (wordlist.txt)
Input.Queue......: 1/1 (100.00%)
Speed.Dev.#2.....:        0 H/s (0.04ms)
Recovered........: 8/8 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 8/8 (100.00%)
Rejected.........: 0/8 (0.00%)
Restore.Point....: 0/8 (0.00%)
Candidates.#2....: BGM554 -> HighlyUnlik3lyToB3Cr4ck3d…
```

Ön Hesaplama (Pre-Computing) - Rainbow Tables I

Rainbow Attack

- Rainbow Table: Parola özetlerinin kırılması için kullanılan özet fonksiyonlarının işlevlerini tersine çevirmek için **önceden hesaplanmış** bir tablodur.
- Ele geçirilen özet (hash) değeri bu tabloda yer alan liste ile karşılaştırılarak parola elde edilmeye çalışılır.

HashKiller



#	Hash	Type	Crack Status	Cracked By	Date / Time
1	200ceb26807d6bf99fd6f4f0d1ca54d4	MD5	Cracked	blandyuk	20-Mar-2017 06:29
2	5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8	SHA1	Cracked	hasheponge	20-Mar-2017 06:29
3	315f166c5aca63a157f7d41007675cb44a948b33	SHA1	Cracked		20-Mar-2017 06:29
4	40bd001563085fc35165329ea1ff5c5ecbdbbeef	SHA1	Cracked		20-Mar-2017 06:29
5	a94a8fe5ccb19ba61c4c0873d391e987982fbbd3	SHA1	Cracked	LorDHash	20-Mar-2017 06:29
6	8cb2237d0679ca88db6464eac60da96345513964	SHA1	Cracked	LorDHash	20-Mar-2017 06:29
7	1df1e443163195de1ff3222b38763864666b1c23	MySQL4.1/MySQL5	Cracked	gearjunkie	20-Mar-2017 06:28
8	cb4c6e5fed952f66fb9f81ec650e19c1	MD5	Cracked	cvsi	20-Mar-2017 06:28
9	f3977cb45856c111e5b809ab79903ce8	MD5	Cracked	gearjunkie	20-Mar-2017 06:28
10	c6e8c613707f9f14af0ad39c062700db	MD5	Cracked	blandyuk	20-Mar-2017 06:28
11	64a96e8204fb081b0d4b653115bfdf62	MD5	Cracked	blandyuk	20-Mar-2017 06:28
12	92776f205591047d2ba26f0854de04b5	MD5	Cracked	blandyuk	20-Mar-2017 06:28
13	efa04b22884fb1c0ad27db5cb3e715c5	MD5	Cracked	blandyuk	20-Mar-2017 06:28
14	79d94dbda3a4e4ad386307105f8df915	MD5	Cracked	gearjunkie	20-Mar-2017 06:28

- Özet değerleri
- algoritma/sistemler

rtgen demo I

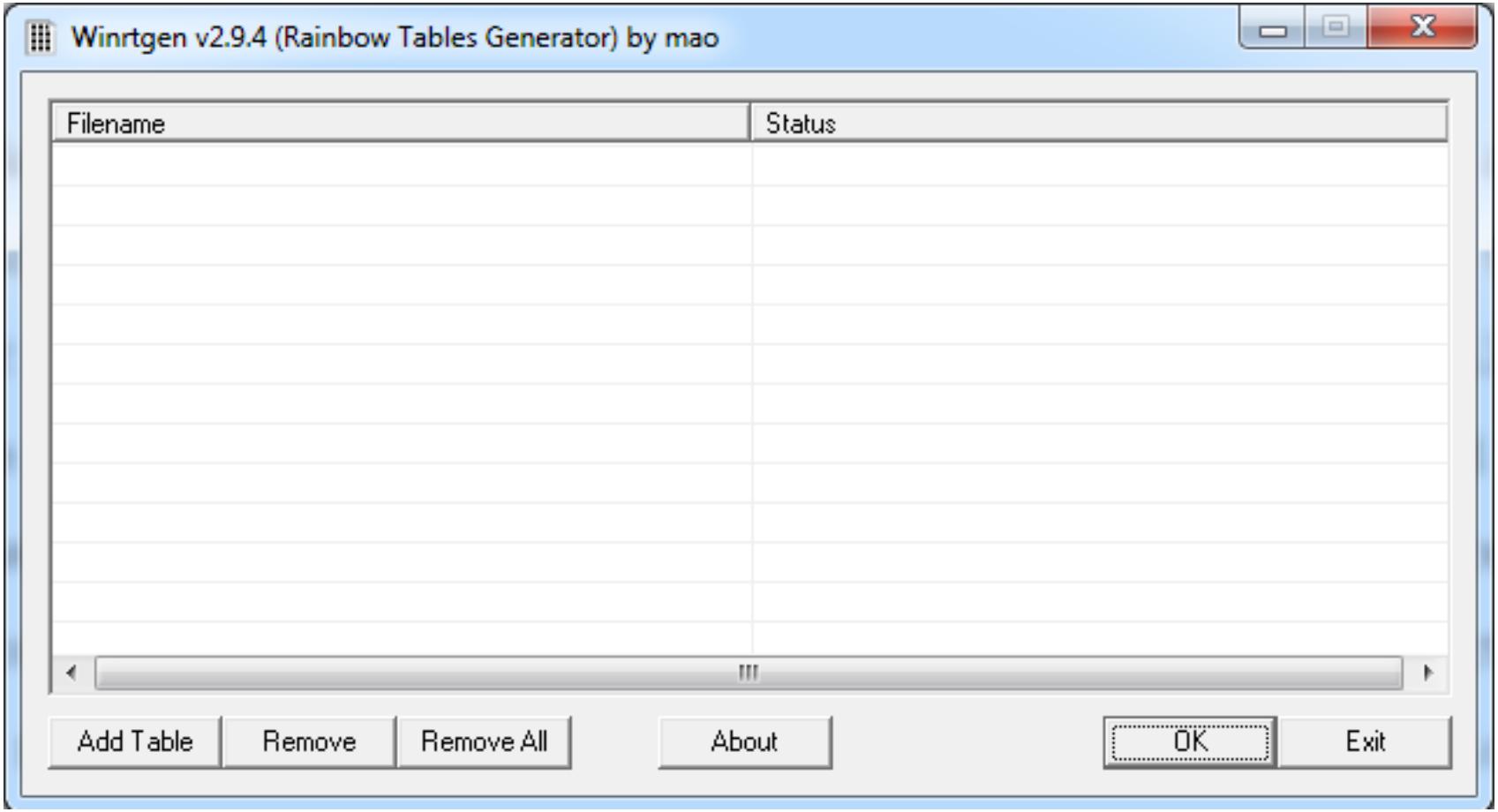
Rainbow Saldırısı

- Bir rainbow table ihtiyacı
- Satın alınabilir.
- İnternet indirilebilir.
- Oluşturulabilir.

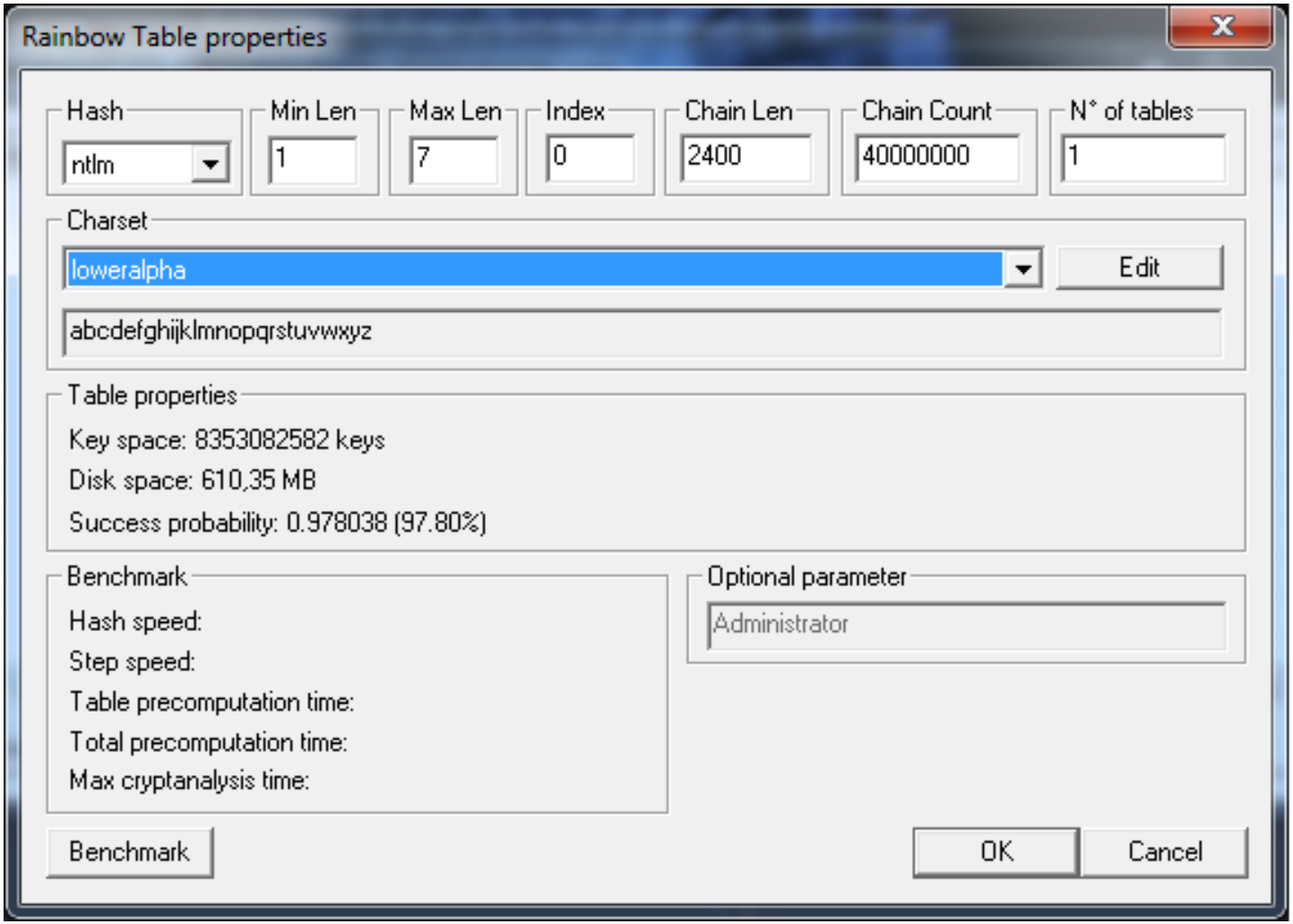
Winrtgen

- ”Cain and Abel” ile beraber gelen *Winrtgen*
- Windows ve Linux işletim sistemlerinde çalışabilmektedir.

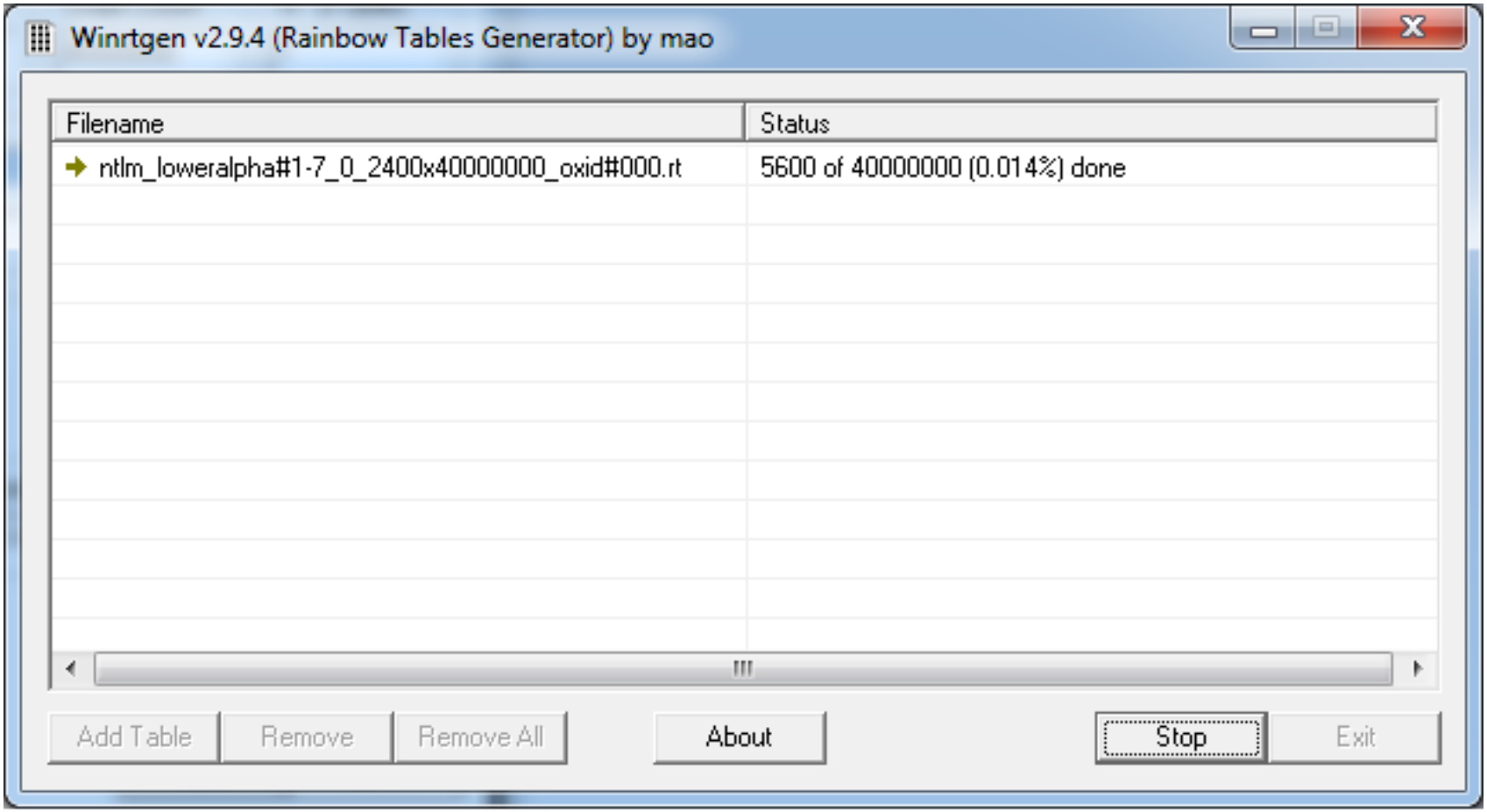
rtgen demo II



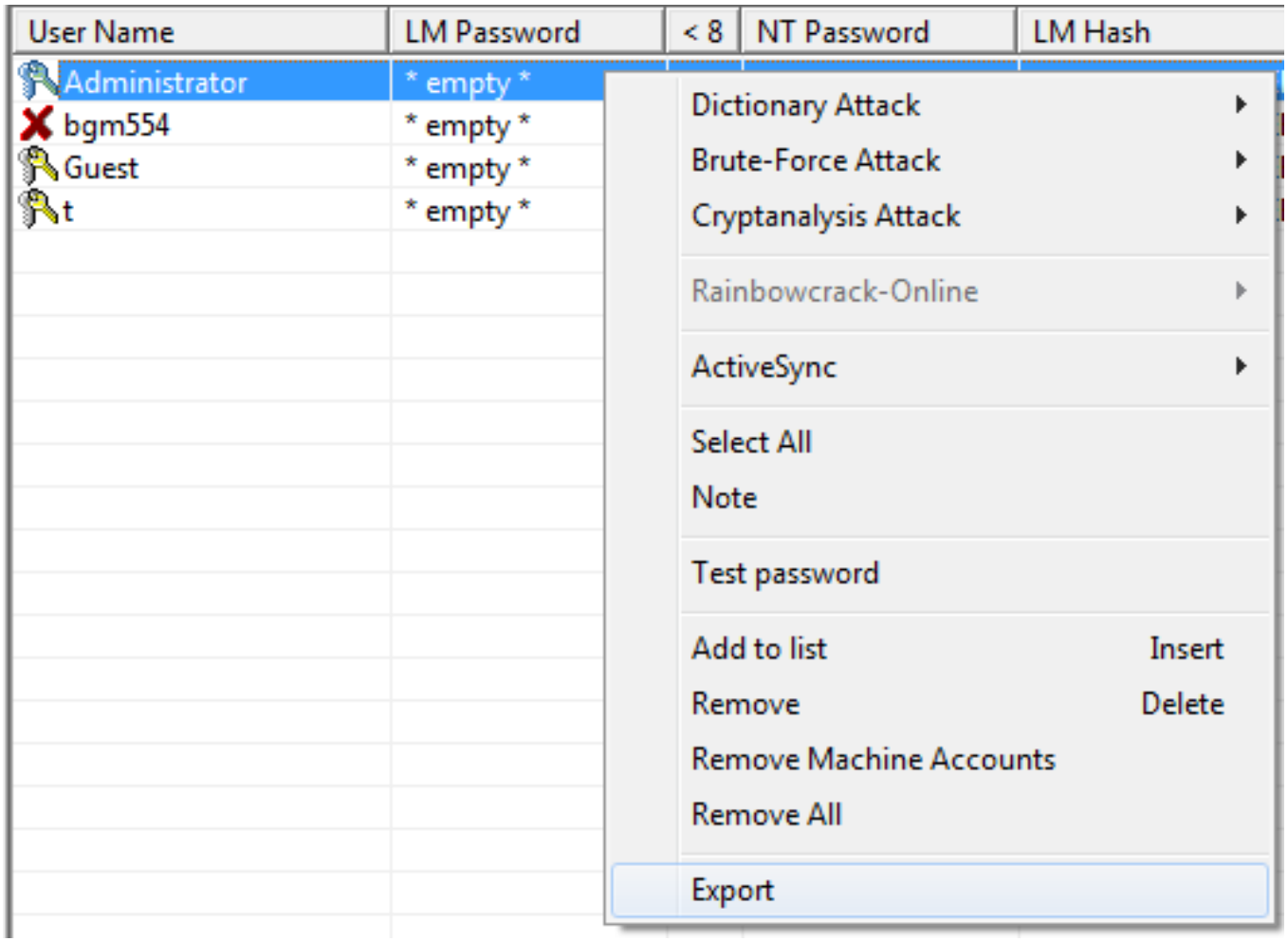
rtgen demo III



rtgen demo IV



HashKiller Demo I

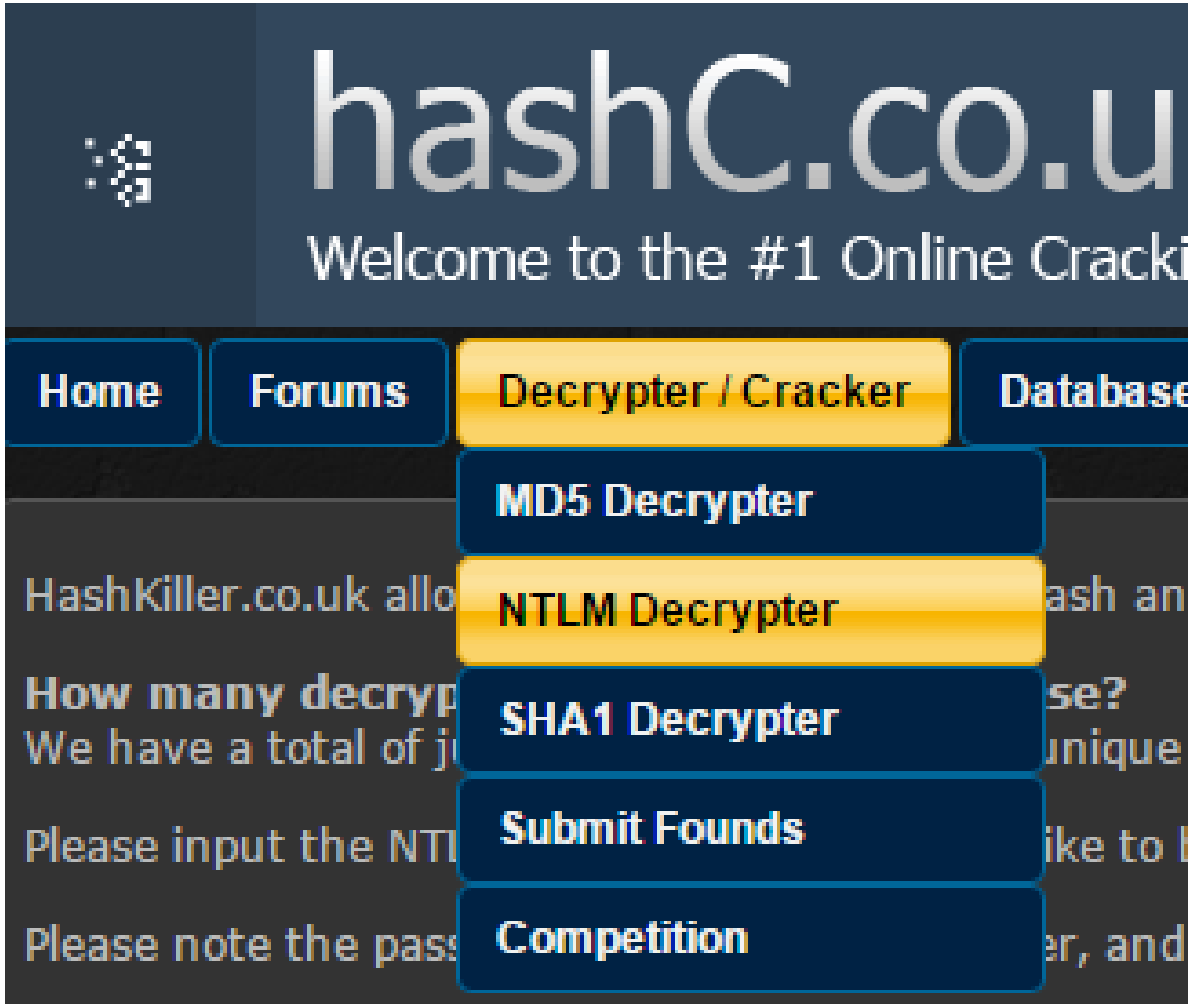


HashKiller Demo II

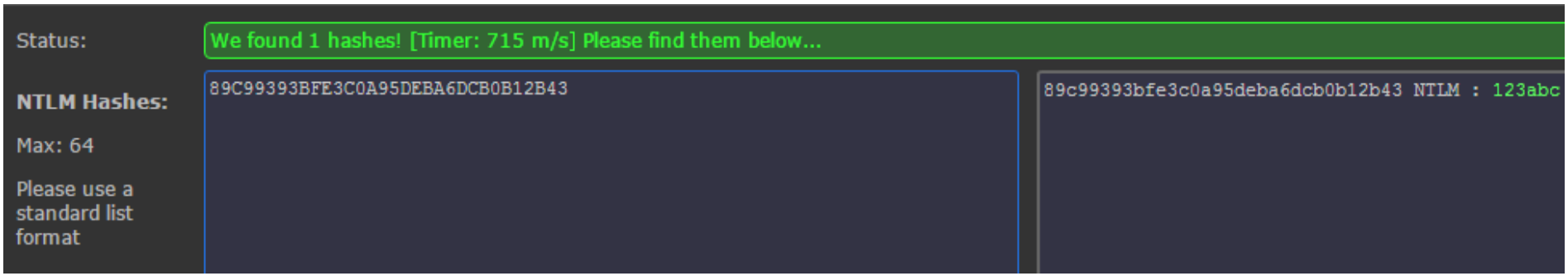
bgm554.lc

```
1  Administrator:"":"":AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
2  bgm554:"":"":AAD3B435B51404EEAAD3B435B51404EE:89C99393BFE3C0A95DEBA6DCB0B12B43
3  Guest:"":"":AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
4  t:"":"":AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
```

HashKiller Demo III



HashKiller Demo IV



Özet Ekleme Saldırısı - Hash Insertion Attack I

Hash Insertion Attack

- Saldırgan, bilgisayara fiziksel erişim olması durumunda birçok işlem yapabilmektedir.
- Özet değerlerinden plain-text parola elde etmek yerine yeni parola ekler (Windows SAM veritabanı)
- CD üzerinden Linux ile bilgisayar boot edilebilir.
- Bootable CD'ler yardımıyla sistem yöneticileri tarafından kullanılabilmektedir.

Windows Kimlik Doğrulama I

Kimlik Doğrulama (Authentication)

- **LM authentication protocol**:
  - Kullanıcı parolası büyük harfe çevrilir.
  - LM parolaları max 14 karakterdir. Az olması durumunda null-padding ile 14 karakter haline getirilir.

Windows Kimlik Doğrulama II

Örnek Senaryo (LM response)

- SecREt01 => SECRET01 (hex: 0x5345435245543031)
- 14 byte değer: 0x5345435245543031000000000000
- 2 tane 7-byte parça: ”0x53454352455430” ve ”0x31000000000000”
- DES anahtarları
  - **1. kısım** 0x53454352455430 binary değer:
    01010011 01000101 01000011 01010010 01000101 01010100 00110000
    Non-parity-adjusted
    0101001**0** 1010001**0** 0101000**0** 0110101**0** 0010010**0** 0010101**0** 0101000**0** 0110000**0**
    odd-parity-adjusted
    0101001**0** 1010001**0** 0101000**1** 0110101**1** 0010010**1** 0010101**0** 0101000**1** 0110000**1**
    hex : 0x52a2516b252a5161
  - **2. kısım** 0x31000000000000 binary değer
    00110001 00000000 00000000 00000000 00000000 00000000 00000000 *Non-parity-adjusted*
    0011000**0** 1000000**0** 0000000**0** 0000000**0** 0000000**0** 0000000**0** 0000000**0** 0000000**0**
    odd-parity-adjusted
    0011000**1** 1000000**0** 0000000**1** 0000000**1** 0000000**1** 0000000**1** 0000000**1** 0000000**1**
    hex : 0x3180010101010101
- Sabit string: `KGS!@#$%` (hex: ”0x4b47532140232425”), her iki anahtar kullanılarak şifrelenir.
  - 1. anahtar sonucu: 0xff3750bcc2b22412
  - 2. anahtar sonucu: 0xc2265b23734e0dac
  - 16-byte LM hash - 0xff3750bcc2b22412c2265b23734e0dac
  - Padding işlemi ile 21-byte: 0xff3750bcc2b22412c2265b23734e0dac0000000000
- 3 adet 7-byte parça: ”0xff3750bcc2b224”, ”0x12c2265b23734e” ve ”0x0dac0000000000”
- Aynı şekilde DES anahtarları elde edilir: ”0xfe9bd516cd15c849”, ”0x136189cbb31acd9d” ve ”0x0dd6010101010101”

Windows Kimlik Doğrulama III

- Örnek Type-2 mesajı (0x0123456789abcdef)
  - 1. anahtar: 0xc337cd5cbd44fc97
  - 2. anahtar: 0x82a667af6d427c6d
  - 3. anahtar: 0xe67c20c2d3e77c56
- 24-byte LM response: 0xc337cd5cbd44fc9782a667af6d427c6de67c20c2d3e77c56

Yöntemin Zayıflıkları

- Büyük harf olmasından dolayı parola arama uzayı azalmaktadır.
- Eğer parola 7 karakterden az ise bu durumda ikinci 7-byte blok sadece 0'lardan oluşur. DES anaharı ise 0x0101010101010101. `KGS!@#$%` ifadesi 0xaad3b435b51404ee

Windows Kimlik Doğrulama IV

NTLMv1 authentication protocol

- NTLMv1 kimlik doğrulama, temel olarak challenge-response mimarisi üzerine kurulmuştur.
- 3 farklı mesaj: Type 1 (negotiation), Type 2 (challenge) ve Type 3 (authentication)
- İstemci ”Type 1” mesajını sunucuya gönderir.
- Sunucu ”Type 2”, (Challenge) mesajını istemciye iletir.
- İstemci LM Response (Type 3) oluşturarak cevap verir.
- Sunucu tarafında aynı işlem gerçekleştirilerek kimlik doğrulama işlemi için parolayı kontrol eder.

Windows Kimlik Doğrulama V

Örnek Senaryo (NTLMv1)

- ”SecREt01” unicode mixed-case (0x5300650063005200450074003000 3100)
- MD4 değeri (0xcd06ca7c7e10c99b1d33b7485a2ed808)
- 21 byte null-padding (0xcd06ca7c7e10c99b1d33b7485a2ed808<u>0000000000</u>)
- 3 tane 7-byte parça: ”0xcd06ca7c7e10c9”, ”0x9b1d33b7485a2e” ve ”0xd8080000000000”
- DES anahtarları
  - 1. kısım binary değer:
    11001101 00000110 11001010 01111100 01111110 00010000 11001001
    Parity-adjusted
    11001101 10000011 10110011 01001111 11000111 11110001 01000011 10010010
  - 2. kısım binary değer:
    10011011 00011101 00110011 10110111 01001000 01011010 00101110
    parity-adjusted
    10011011 10001111 01001100 01110110 01110101 01000011 01101000 01011101
  - 3. kısım binary değer:
    11011000 00001000 00000000 00000000 00000000 00000000 00000000
    parity-adjusted
    11011001 00000100 00000001 00000001 00000001 00000001 00000001 00000001
- Hex değerleri: ”0xcd83b34fc7f14392”, ”0x9b8f4c767543685d” ve 0xd904010101010101
- Type 2 mesajı (0x0123456789abcdef) DES ile 0x25a98c1c31e81847 (1. anahtar kullanılarak), 0x466b29b2df4680f3 (2. anahtar kullanılarak) ve 0x9958fb8c213a9cc6 (3. anahtar kullanılarak)
- 24-byte NTLM response: **0x25a98c1c31e81847466b29b2df4680f39958fb8c213a9cc6**

Windows Kimlik Doğrulama VI

NTLMv2

- Benzer v1'e şekilde: challenge-response authentication protocol
- *8-byte server challenge* karşılık 2 adet cevap gönderir.
  - randomly generated client challenge
  - Büyük harf, unicode (kullanıcı adı + domain)

Kerberos Authentication [1]

- Windows 2000 işletim sisteminden itibaren kullanılmaktadır. (RFC 3244, RFC 4757)
- Günümüz *active directory domains* içinde yer almaktadır.
- Farklı bileşenler içermektedir
  - Kimlik doğrulama sunucusu (authentication server)
  - key distribution center
  - ticket-granting ticket

[1] https://web.mit.edu/kerberos/

İçindekiler

Bilgisayarın Farklı Bir Cihazla Açılması I

Yerel Parolaların Elde Edilmesi

- Keşif aşamasında yer alan ilk adım: Son kullanıcı bilgisayarının farklı bir işletim sistemi ile açılması
- Genellikle Linux işletim sistemine sahip *Live CD* ile açılıp *SYSTEM* ve *SAM* dosyaları alınır.

SAM ve SYSTEM dosyalarını alma

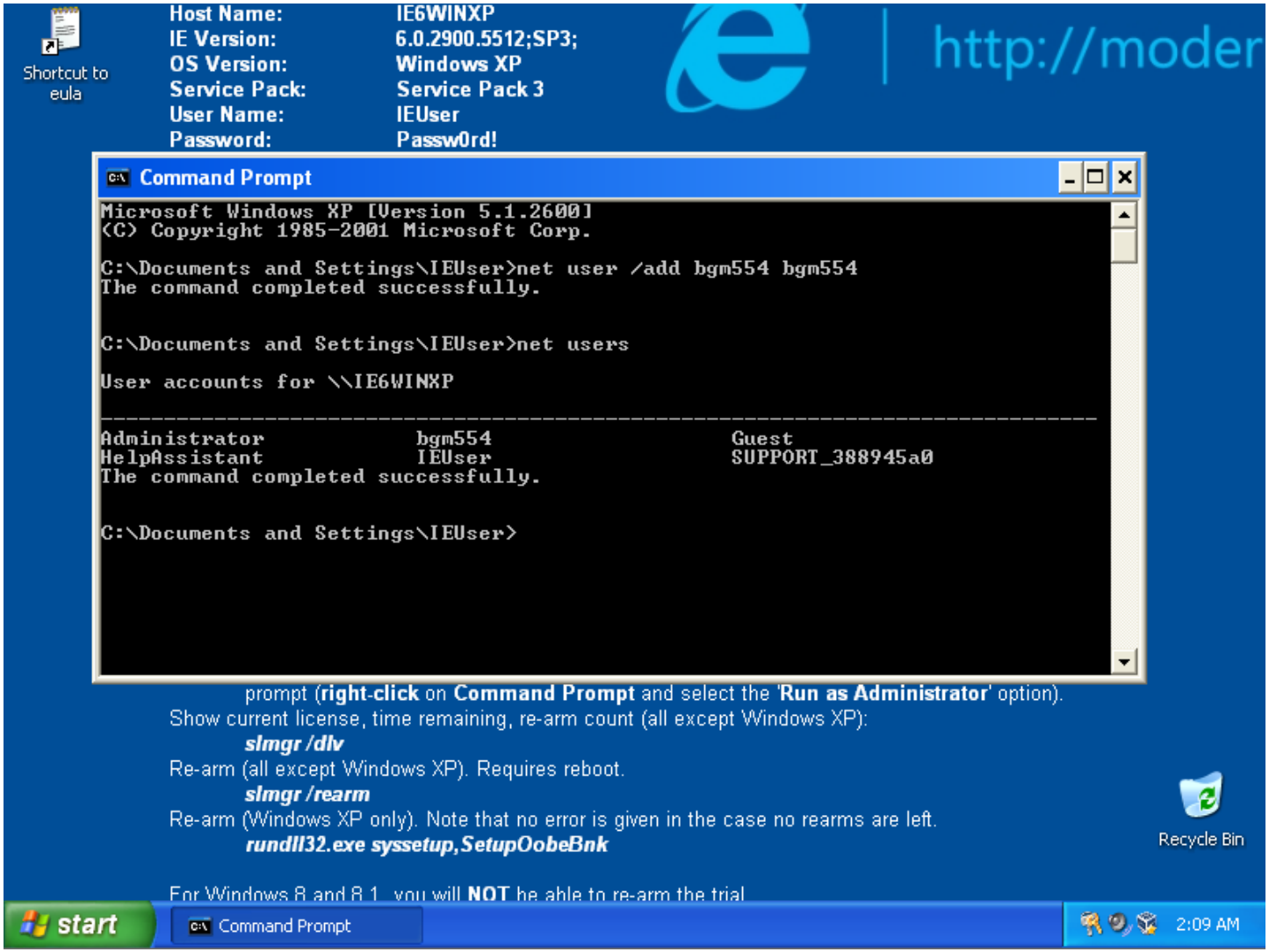
- **SAM veritabanı**: Security Accounts Manager.
  - Windows tarafından kullanıcılar için kullanılan dosya
  - İşletim sistemi çalışırken dosya kopyalanamaz.
  - `%WINDIR%\system32\config\SAM`
- **SYSTEM Dosyası**: dosyayı açabilmek için dosyanın özel anahtarına sahip olan dosya
  - `%WINDIR%\system32\config\SYSTEM`

Bilgisayarın Farklı Bir Cihazla Açılması II

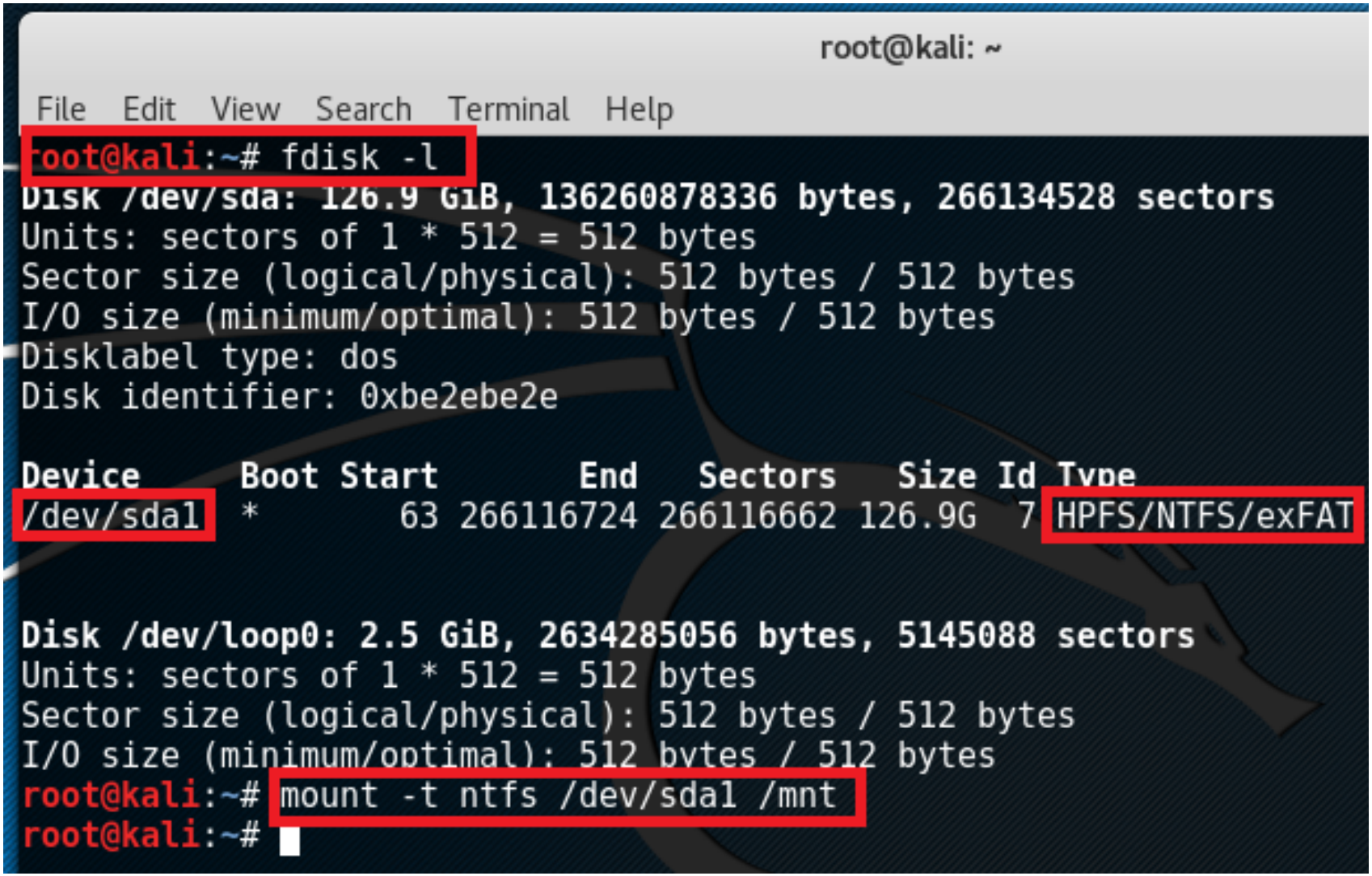
Yerel kullanıcılar ve Parola özetlerini ele geçirme

- SAM ve SYSTEM ele geçirildikten sonra çeşitli araçlar kullanılarak kullanıcıların parola özetleri elde edilir.
- bkhive
  - Bkhive SYSTEM keyfile
- Samdump2
  - Samdump2 SAM keyfile

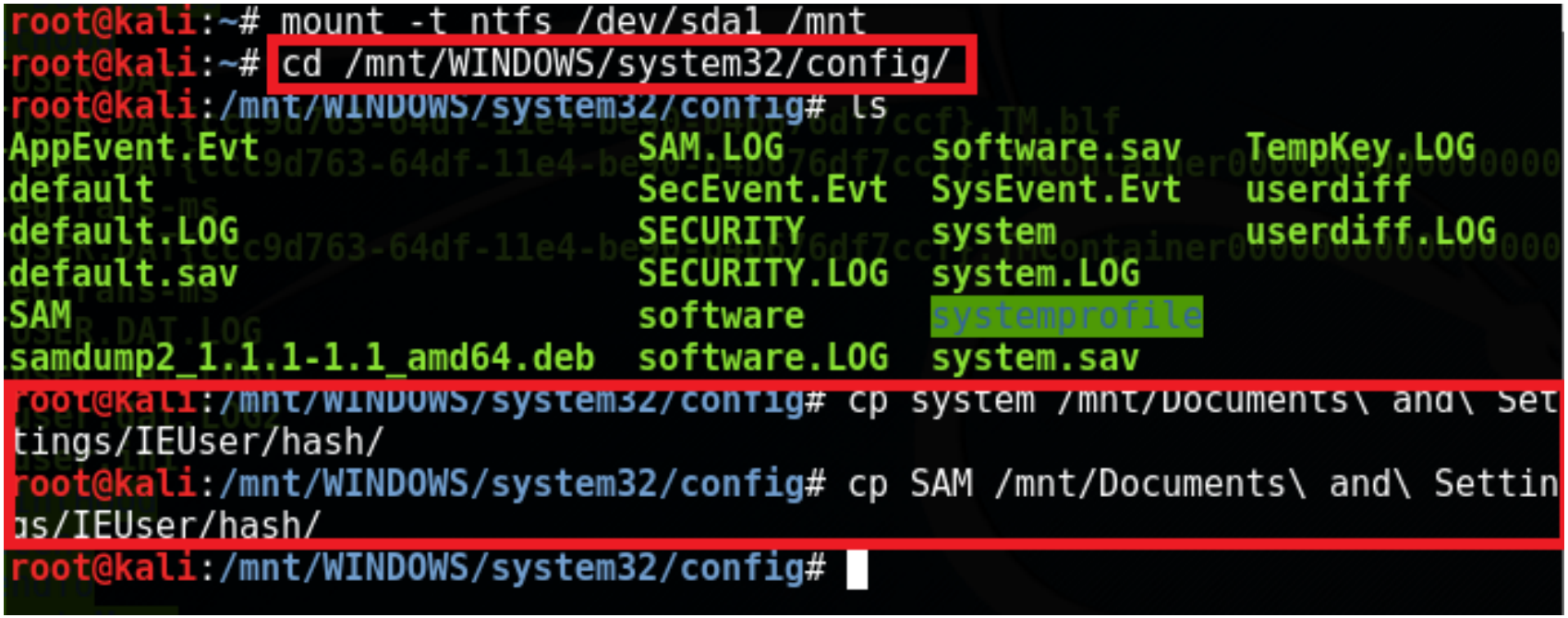
Bilgisayarın Farklı Bir Cihazla Açılması III



Bilgisayarın Farklı Bir Cihazla Açılması IV



Bilgisayarın Farklı Bir Cihazla Açılması V



Bilgisayarın Farklı Bir Cihazla Açılması VI

```
root@kali:/mnt/Documents and Settings/IEUser/hash# samdump2 system SAM > hash_values.txt
root@kali:/mnt/Documents and Settings/IEUser/hash# cat hash_values.txt
Administrator:500:b34ce522c3e4c87722c34254e51bff62:fc525c9683e8fe067095ba2ddc971889:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* HelpAssistant:1000:9b45eefa50cbd1f779518231c8ae0fb3:8da1ecee0f0c121facdfb869612a33c6:::
*disabled* SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:60a8616c6fd013a1aff2d7c3328b4af8:::
IEUser:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
bgm554:1004:83d4332c20265e91aad3b435b51404ee:d7874de73f8f874cee6c49d88d2f70af:::
root@kali:/mnt/Documents and Settings/IEUser/hash# john hash_values.txt  -user=bgm554
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "NT-old"
Use the "--format=NT-old" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 1 password hash (LM [DES 128/128 AVX-16])
Press 'q' or Ctrl-C to abort, almost any other key for status
BGM554           (bgm554)
1g 0:00:00:00 DONE 1/3 (2017-03-19 13:36) 100.0g/s 8900p/s 8900c/s 8900C/s BGM554..455MGB!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Kullanıcı Bilgileri Aynı Olan Bilgisayarlar I

Kullanıcı Adı/Parola Özetleri

- Keşif aşamasında elde edilen kullanıcı ad/parola özeti bilgilerinin farklı bilgisayarlar üzerinde denenmesi
- metasploit auxiliary modülü olan *smb_login*
- **Örnek senaryo**
  - Hazır imajdan kurulum yapılan yerlerde yerel yönetici kullanıcı adı/parola aynı olabilmektedir.
  - Bir kullanıcı ile bir çok bilgisayara atlayabilme.

Kullanıcı Bilgileri Aynı Olan Bilgisayarlar II

SMB_LOGIN

- Parametreler
  - BLANK_PASSWORDS: Verilen tüm kullanıcılar için boş parola dener.
  - RHOSTS: Hedef bilgisayarlara ait IP bilgisi
  - RPORT: Hedef bilgisayardaki SMB protokolünün port
  - SMBDomain: Hedef bilgisayar üzerinde denenecek kullanıcı hesaplarının üye olduğu etki alanı (Workgroup – Etki alanı)
  - SMBUser: Hedef bilgisayar üzerinde kullanıcı adı
  - SMBPass: Hedef bilgisayar üzerinde parola/parola özeti
  - USER_AS_PASS: Verilen tüm kullanıcılar için kullanıcı adını parola olarak dener.
  - *Parola politikası etkin olduğu durumlarda "BLANK_PASSWORDS" ve "USER_AS_PASS" parametrelerinin kaldırılması önerilir.*

Kullanıcı Bilgileri Aynı Olan Bilgisayarlar III