
HACKHISPANO
ELECTRONIC FANZINE

Desde el Staff de HackHispano queremos, antes de nada y para empezar, dar las gracias de corazón a todos los que formáis la comunidad de HackHispano. ¿Por qué? Porque sin vosotros no habría comunidad, vosotros formáis parte de este proyecto; vosotros sois realmente HackHispano.

Hemos decidido ampliar horizontes y hacer más grande lo que ya de por si es enorme. Para ello tenemos muchas cosillas pensadas y muchas cosas para vosotros, todas buenas y todas gratis.
Para comenzar ésta es la primera muestra de ello, el eZine.

Sin ánimo de ser una publicación que englobe todo el conocimiento o todo a lo que se puede acceder desde nuestra espina dorsal (el foro de HackHispano), pretende ser una recopilación de información y una forma de ver las cosas bien presentadas, accesibles a todo el mundo y, por qué no, coleccionable.

Esperando que todos disfrutéis de este recién-nacido primer número, nos despedimos sin más para que podáis comenzar.

Antes de nada deciros que, por favor, si tenéis alguna sugerencia para el próximo número, alguna pega de este mismo, o cualquier cosa que queráis aportar a esta publicación, no dudéis en acudir al foro; todas serán bien recibidas.

#Sumario#

HACKHISPANO ELECTRONIC FANZINE

HACKHISPANO v2.0

HackHispano es una comunidad libre donde todo el mundo es bienvenido, donde nadie es extranjero, donde todos buscamos algo y donde todos lo ofrecemos.

Nuestra comunidad no es más que un punto de encuentro para todos los que estáis perdidos en este cada vez más confuso mundo de la sobreinformación, donde encontrareis gente como vosotros que intentará ayudaros y donde seguro encontraréis alguien que precisa de vuestra ayuda.

Sed bienvenidos a HackHispano.com

HACKERS, Autodidactas del Siglo X

By Sn@ke

Dueños de una brillante habilidad para deslizarse por el denominado, underground electrónico, sin dejar huella, los hackers continuan haciendo de las suyas utilizando su vasto conocimiento tecnológico y su experiencia en Internet, como una llave maestra capaz de abrir todas y cada una de las puertas que dotan (o intentan dotar) de seguridad a la Red. Su único objetivo: hacer de la información un bien libre, gratuito y accesible.
Perseguidos por la justicia por falta de conocimientos de esta última, son el futuro de los científicos que dentro de unos años nos harán la vida más fácil y más segura dentro de la gran telaraña que es la Red.

De un tiempo a esta parte, la figura del hacker ha despertado gran expectación en la sociedad. Su astucia y brillante capacidad para desenvolverse en el denominado "underground de la Red ", han sido en ocasiones objeto de estudio, así como motivo suficiente como para convertir su actividad en el argumento de una película de acción. De hecho, filmes como "Juegos de guerra" o "Hackers", intentaron retratar a este tipo de intrusos, mostrando a jóvenes prodigio capaces de acceder a complejos sistemas de información, con un único objetivo: poner en evidencia la seguridad de los mismos. Pero no es en realidad un prototipo, y todos sabemos que la ficción no supera la realidad.

Los primeros hackers comenzaron a actuar en la década de los ochenta. Desde entonces, el continuo crecimiento del número de ordenadores conectados a Internet, -se ha llegado a registrar una cifra de 407,1 millones de internautas en el último año- ha facilitado no sólo la aparición de nuevos "fichajes", sino también su futura preparación. El término fue popularizado por el escritor Steven Lery en su obra titulada "Hackers", donde se retrata a una serie de individuos cuya única pretensión era la de convertir la tecnología en un bien accesible para todo el mundo. Sin embargo, desde entonces, el término "hacker" ha ido adoptando un sentido mucho más peyorativo, utilizando para calificar a aquellos programadores capaces de causar la caída de un sistema en vez de solucionar el problema a través de la tecnología. De hecho, en la obra "A prueba de Hackers", su autor Lars Klander llega a definir a este colectivo como a un conjunto de "personas que se divierten rompiendo sistemas, robando contraseñas y el código de programas, y generalmente, intentando resultar tan problemáticos como sea posible". (Pobre ignorante, su concepto de hackers seguro que está influido por algún ataque sufrido o algún resentimiento personal).

No obstante, no todos los intrusos que se introducen ilegalmente en los sistemas no tienen el mismo afán de destrucción, por lo que no merecen el mismo tratamiento. Según el conocimiento que presenten del medio en el que operan, estos individuos pueden definirse de un modo u otro. En este sentido, Eric S. Raymond en su obra "The New Hacker's Dictionary", (Diccionario del Hácker), define a este tipo de intrusos como personas que disfrutan del reto intelectual de superar las limitaciones de forma creativa. El autor también señala que los hackers se consideran a sí mismos como parte de una élite, en la que la habilidad es una de sus virtudes, y el deseo de encontrar modos de quebrantar nuevas medidas, uno de sus móviles.. Su orgullo y elevada autoestima indujo a estos personajes a acuñar en 1985 otros términos como cracker, para aludir a un tipo de intrusos que, con menor experiencia técnica que el resto, son incluso más peligrosos que ellos mismos. Considerados como verdaderos vándalos, los crackers suelen agruparse en grupos pequeños y privados. Es el denominado lado oscuro del hacking, donde prima el objetivo de introducirse ilegalmente en sistemas, desproteger productos y, en definitiva, destruir.

Por todo ello, y a pesar de la ilegalidad de cualquiera de estas acciones, el hacker es posiblemente la figura mejor considerada dentro del denominado submundo electrónico. Es más, su conocimiento y experiencia se han convertido en ocasiones en un recurso muy codiciado por algunas entidades y compañías, deslumbradas por la habilidad de estos individuos. Fue el caso de "El bruxo", un pirata que consiguió acceder a la Web oficial del presidente de Irán, y dejar un escrito, sin dañar ningún tipo de información. La brillantez del hacker sorprendió tanto al presidente que, sin dudarlo, le ofreció un puesto de trabajo, cosa que el rechazó pues su país de origen era España, es el día de hoy que nadie todavía sabe quién es ni dónde está ubicado, tan solo un grupo de sus amigos lo conocen.

Antes de realizar cualquier ataque, el hacker comienza a husmear por la red, con el fín de recopilar toda la información posible sobre el sistema al que desea acceder. Es el denominado ataque de sniffer, basado principalmente en conseguir la clave de un usuario y su contraseña, y utilizarla después para introducirse en una red distribuida. Para ello se utilizan unos programas (sniffers), capaz de capturar paquetes de datos que pasan por un servidor, para conseguir los login. Otra técnica muy utilizada por la comunidad de hackers durante la fase de recopilación de información es la denominada Ingeniería Social. Se trata de una estrategia que el intruso pone en marcha, fingiendo ser otra persona para obtener información relevante. Uno de los escenarios en los que se utiliza esta técnica con mas frecuencia es el IRC. A menudo, y tras establecer amistad con un usuario fingiendo ser otra persona, algunos hackers llegan incluso a convencer a su víctima de que la cuenta que está utilizando no es propia y que debe desconectarse. Es entonces cuando le comenta que, a pesar de ello, le gustaría seguir manteniendo su amistad y que por tanto, la única solución es que el segundo le deje utilizar su password.

Un método mas sofisticado es el basado en la predicción de secuencias de números adjudicados a cada uno de los paquetes transportados sobre protocolos TCP/IP. En la obra "A prueba de Hackers" de Lars Klander, el autor explica como se lleva a cabo este ataque. En primer lugar el intruso averigua las

direcciones IP del servidor, espiando los paquetes de datos que van dirigidos a él o bien conectando con el sitio que desea atacar a través de un explorador Web y viendo la dirección que aparece en la barra de estado. Una vez conocida la dirección IP del sistema y sabiendo el número de ordenadores que pueden estar conectados a la Red, el intruso puede lograr su objetivo. Solo tendrá que probar distintas secuencias numéricas hasta dar con la deseada. Una vez logrado el primer paso, el intruso podrá acceder fácilmente a los datos que contenga el servidor.

Otra de las amenazas preferidas de los hackers es el ataque basado en contraseñas, mediante el uso de programas específicos capaces de comprobar las password automáticamente. Uno de los mas populares es el basado en diccionarios. En el caso de herramientas como DCM 2.0, Dictionary File Creater 1.1, DictMake, Zip Password Recovery o John the ripper para LINUX/UNIX, capaces de recorrer todas las palabras de un diccionario hasta encontrar la contraseña. Son aplicaciones muy útiles para todos aquellos que desconocen la password por completo. Sin embargo, no hay que olvidar que, en función de las capacidades técnicas que posea el hacker, deberá invertir mas o menos tiempo en la búsqueda.

No obstante, es posible que el intruso conozca algunos de los caracteres alfanuméricos que configuran una contraseña. En este caso, puede utilizar aplicaciones como Refiner, que tras un proceso de búsqueda y partiendo de algunos caracteres predefinidos por el usuario, muestran diferentes combinaciones de contraseñas en un documento de texto. La mayoría de estos programas se encuentra disponibles de forma gratuita en Internet, en cualquiera de las miles de páginas Web dedicadas al mundo del hacking y del cracking. Sin embargo, el hacker ha de tener siempre en cuenta, que su intromisión puede a veces volverse contra él ya que, normalmente, éste ha de revelar su situación para llevar a cabo la amenaza. Si es detectado por su víctima, el servidor también será localizado.

A pesar de las “buenas intenciones” que pueden inducir a este tipo de individuos a cometer su ataque, lo cierto es que esta actividad es ilegal y, por tanto, esta contemplada como delito.

En cualquier caso, un hacker que se precie nunca cometerá tal error, sino que utilizará un ordenador que no le pertenezca. En este caso, la dificultad de cazar al intruso con las manos en la masa se incrementa, teniendo en cuenta que sus ataques duran escasamente unos minutos. Por tanto, en la mayoría de los casos, las víctimas se han de conformar con lograr reiniciar el servicio una vez producida la amenaza. No obstante, estos últimos pueden plantear medidas de seguridad que les permitan evitar futuras amenazas. No hay que olvidar que la utilización de firewalls o cortafuegos, a la hora de conectar una red local a Internet puede evitar males mayores. Otra posibilidad consiste en utilizar firmas digitales para asegurar la confidencialidad de un documento, o codificar las transmisiones que se realicen, sobre todo a través de la red. Para ello, el receptor deberá contar con una clave para poder traducir el mensaje.

A pesar de las “buenas intenciones” que pueden inducir a este tipo de individuos a cometer su ataque, lo cierto es que esta actividad es ilegal y, por tanto, esta contemplada como delito penal. De hecho, recientemente el mundo entero ha podido asistir a un importante juicio celebrado contra un hacker en Estados Unidos. En esta ocasión, el acusado era un joven de 16 años llamado Mafiaboy. El motivo de su detención no fue otro que hackear las páginas Web de Yahoo!, CNN, Amazon y eBay. La acción del joven, que finalmente se declaró culpable de 55 de los 65 cargos que se le imputaron, provocó unos daños que ascendieron a 1.700 millones de dólares. Unas cifras escalofriantes que llevaran a Mafiaboy a permanecer en libertad condicional hasta el dictamen de la sentencia.

En cualquier caso, el interés por poner punto y final al brillante currículum de estos intrusos no es una pretensión actual. Ya en 1.990 se inició en Estados Unidos una caza de hackers, traducida en multitud de denuncias, arrestos, juicios e incluso confiscaciones de equipos. El escritor Bruce Sterling lo refleja en su libro electrónico “The Hackers Crackdown”, y explica cómo el Servicio Secreto de EE.UU., civiles expertos en seguridad telefónica y departamentos y brigadas de policía estatales y locales “unieron sus fuerzas en un decidido esfuerzo por aplastar la cabeza del underground electrónico americano”. Desde entonces, han surgido multitud de grupos de presión generados con el único objetivo de poner fin a las acciones de este colectivo y regular la situación. De hecho, una de las últimas iniciativas ha sido la constitución de la organización IT Information Sharing and Analisis Center (IT-ISAC. Formada por un total de 19 compañías, entre las que se encuentran Computer Associates, Cisco Systems, Microsoft, Oracle, Veridian, CSC, IBM y Hewlett-Packard, la entidad se ha creado con la finalidad de informar al sector de las tecnologías de la información e intercambiar información sobre incidentes, amenazas, ataques, vulnerabilidades, soluciones, contramedidas, mejores prácticas de seguridad y otras medidas de protección. Al IT-ISAC, que trabajará junto con el Gobierno de EE.UU. para evitar futuros ataques a sus miembros, pueden adherirse todas aquellas compañías que lo deseen abonando por ello una cuota de cinco mil dólares anuales. En España, la legislación contempla igualmente como delito la intromisión y la interceptación de las comunicaciones.

En concreto, el artículo 197 del Código Penal establece que “el que para descubrir los secretos o vulnerar la intimidad de otros sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro millones”. El mismo artículo argumenta a su vez que “las mismas penas se impondrán al que, sin estar autorizado se apodere en perjuicio de terceros, de datos reservados de carácter personal de otro que se hallen registrados en ficheros o soportes informáticos”. Asimismo, en el artículo 256 del Código Penal se especifica que “el que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a este un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses”.

En definitiva, medidas que se plantearan como nuevos retos para todos aquellos que deseen iniciarse en el apasionante e ilegal mundo del Hacking.

NOTA:

Sres. Si después de leer esto se dan cuenta Uds de quienes son los hackers pagados por los gobiernos y grandes empresas y con todos los medios a su alcance, estarán uds en el buen camino pues es cierto que los mayores Hackers del Mundo son las propias Multinacionacionales y los que invitan a realizar este tipo de ataques. Si en la Red no existe una justicia con una jurisprudencia ya definida, nadie puede meter en la cárcel a nadie y menos si no se hace daño, sino que encima se aprovechan de la información obtenida por estos grupos.

En un ordenador puede crearse arte y belleza

De nada les valdrá su hipocresía, su prepotencia. Siempre habrá "mentes inquietas" dispuestas a despertarles de su sueño de control total. Algunos lo harán sólo por autoestima, otros por demostrar la imposibilidad de controlar los bits...y algunos lo harán por el simple hecho de sentirse libres...sentirse bien. Indudablemente alguno lo hará por demostrar que tiene cualidades más que sobradas para ser un gran administrador de sistemas. ¡Hay que comer, qué coño!. Pero ahí estan, es un hecho. Para algunos, un atisbo de esperanza para la humanidad por sus grandes ideales altruistas. Para muchos, auténtica basura que hay que eliminar como sea, pues son lo único que se interpone ante su poder. Que cada cual saque sus propias conclusiones.

Steven Levy establece en su obra “Hackers, Héroes de la Revolución Informática”, algunos principios básicos del hacking:

1º. - El acceso a los ordenadores y a cualquier cosa que pueda enseñar algo acerca del modo en que funciona el mundo debe ser ilimitado.

2º. - Apelar siempre a la expresión: ¡Manos a la obra!

3º. - Toda información ha de ser libre y gratuita.

4º. - Hay que desconfiar de la autoridad.

5º. - Los hackers deberán de ser juzgados por sus actos, y no por falsos criterios como títulos, edad, raza o posición.

6º. - En un ordenador puede crearse arte y belleza.

7º. - El ordenador puede mejorar la vida.

Muchas gracias por leer todo esto e intentar comprenderlo.
Sin la libertad no se puede vivir ¿quién nos la quiere quitar?, ¿por qué debemos borrar nuestras huellas y caminar sin pisar el suelo?

Tomás Soto (Sn@ke)
León (España)

Introducción a la API de Windows

By HySTD

El objetivo básico de la API es ofrecer a una aplicación correr en el sistema operativo, ofreciendo la posibilidad de manejar y depurar errores, controlar procesos, hilos y dispositivos de entrada-salida, manejar la interfaz gráfica y la memoria, etc... Es por ello por lo que no está demás conocer algunas funciones interesantes para poder usar en nuestros programas y aplicaciones.

En este artículo veremos:

_ Creación de un repelente de mosquitos
_ Trasteando con el sistema

Este artículo no se trata de un tutorial, pero si de una pequeña guía introductoria a este amplio tema, para que ustedes los lectores, tengan una opinión personal a lo que ofrece Windows, con sus pro y sus contras. Antes de comenzar a explicar nada, debemos saber ¿qué es la API?. La API (Application Programming Interface "Interfaz de programación de aplicaciones") no es mas que un conjunto de funciones y procedimientos almacenados en librerías que posee el sistema operativo. En Windows, estas se encuentran almacenadas en ficheros .DLL, de entre los que, personalmente, destaco "Kernel32.dll", "user32.dll", "gdi32.dll", "shell32.dll", "advapi32.dll", "WinInet.dll y wsock.dll".

El objetivo básico de la API es ofrecer a una aplicación correr en el sistema operativo, ofreciendo la posibilidad de manejar y depurar errores, controlar procesos, hilos y dispositivos de entrada-salida, manejar la interfaz gráfica y la memoria, etc... Es por ello por lo que no está demás conocer algunas funciones interesantes para poder usar en nuestros programas y aplicaciones. Tan sólo necesitamos declarar la función a utilizar en nuestro código fuente, para esto tenemos que conocer la cabecera de la función y/o procedimiento y a qué librería pertenece para poder cargarla, usando el estándar Stdcall. En este artículo voy a explicar algunas de estas funciones, y en posteriores publicaciones iré explicando más.

Kernel32.dll (949 funciones exportadas) contiene funciones a bajo nivel del sistema operativo, dirigidas al manejo de procesos, gestión de hilos en el sistema operativo, control de dispositivos de entrada-salida, manejo de la memoria, etc..., cuando inicias Windows, esta librería se carga en un espacio reservado de memoria.

User32.dll (732 funciones exportadas) contiene las funciones de Interfaz de usuario de Windows, encargadas para la administración de Windows en general, con ellas podemos realizar todo tipo de operaciones: como puede ser administrar tareas, manejar las ventanas, Desktops, iconos, menús, comunicaciones y objetos en general. Para ello hablaremos del uso de un "manejador" o Handle y por qué se utiliza.

Gdi32.dll (609 funciones exportadas) GDI = Graphics Device Interface (Interfaz de dispositivo de gráficos) contiene aquellas que se usan para la gestión de la interfaz gráfica de Windows en general, dibujos, fuentes, presentaciones, etc...

Shell32.dll (309 funciones exportadas) se utilizará para ejecutar aplicaciones, correr procesos, manejar propiedades del sistema, etc...

Advapi32.dll (675 funciones exportadas), (advanced api "Api avanzada"), contiene funciones diversas, relacionadas con la seguridad y criptografía, acceso al registro, y numerosas funciones de sistema.

WinInet.dll y Wsock32.dll (225 + 75 funciones exportadas respectivamente), contiene las funciones relacionadas con Internet, permiten establecer conexiones y comunicaciones entre sistemas controlando los sockets de comunicación, así como gestionar protocolos y seguridad.

Existen muchísimas mas librerías, en Windows, en el directorio del sistema podrás encontrarlas.

Con esta suite de herramientas, imaginad las virguerías que se pueden hacer, desde un simple "hola mundo" hasta una poderosa "herramienta de administración de sistema" (a lo que se denominará RootKit) echadle imaginación, seguro que lo que penséis se puede hacer...

La ventaja principal de usar la API, es que no necesitamos implementar las funciones para usarlas, porque ya lo hicieron por nosotros, y además cuando compilemos nuestra aplicación, el tamaño del fichero binario (.EXE), no se ve afectado, ya que lo único que hacemos es una llamada a una función nativa del sistema operativo, sin incluir ningún código de dicha función.

Dicho esto comenzaré a enumerar y explicar algunas funciones sencillas e interesantes, y haremos un programa de ejemplo.

Para aquellos que no estéis puesto en el tema, vamos a hacer una muy simple. Haremos sonar el altavoz interno del PC. Así que si tenéis papel y lápiz, anotad vuestra primera función del API:

```
Funcion  Beep (dwFrecuencia, dwDuracion: DWord)
devuelve un LongBool
```

Esta función está contenida en Kernel32.dll

Donde dwFrecuencia es la frecuencia del sonido a emitir, y la dwDuracion es el tiempo que va esta sonando en milisegundos. Estos parámetros son en realidad de tipo Dword (de ahí el 'dw', en plataformas x86 si un "Word" o palabra es de 16 bits, un Dword es el doble de un Word, esto es 32 bits = LongWord), pero que se interpretará como enteros largos positivos.

Para poder usar esta función, como hemos dicho antes, necesitamos declararla previamente en nuestro código fuente y decir que la vamos a importar desde "kernel32.dll", usando el estándar Stdcall. Este paso se realizará de una manera o de otra, dependiendo del lenguaje que estemos usando. Por ejemplo:

En Visual Basic se declararía:

```
Private Declare Function Beep Lib "Kernel32"
Alias "Beep" (ByVal dwFrecuencia As Long, ByVal
dwDuracion As Long) As Boolean
```

Y en Delphi:

```
function Beep(dwFrecuencia, dwDuracion:
DWord): LongBool; stdcall
external 'Kernel32.dll' name 'Beep';
```

Como veis varía un poco dependiendo del lenguaje, pero conceptualmente es lo mismo, y sólo basta conocer la cabecera de la función.

Así, podemos hacer como ejemplo, un programa que sirva para ahuyentar mosquitos. Estos escapan a frecuencias de alrededor de 22KHz, frecuencia inaudible por la mayoría de las personas, aunque algunos dicen que si pueden oírla, yo no.

El código queda como sigue: Beep (22000, 28800000), esto emitirá 22KHz durante 8 horas (28800 segundos). Si vas a dormir más tiempo, aumenta la duración, pero recuerda que este parámetro debe pasarse en milisegundos, o bien usa algún bucle.

Ya tienes tu repelente de mosquitos, usando la API de Windows. Como comentario adicional en el Reino Unido venden aparatos que se instalan en las calles y generan estas frecuencias para que la juventud no haga botellonas, ya que dicen que los jóvenes también escapan de este sonido, y para los ancianos es totalmente imperceptible.

Visto este sencillo y llamativo ejemplo, podemos pasar a cosas más útiles para el ámbito de nuestros programas. No explicaré cada una de las funciones de la API ya que como comprenderéis esto es una tarea digna de biblioteca y no de artículo, y en Internet hay buena documentación sobre cada una de ellas, por ello me centraré en aquellas que son interesantes para nuestro propósito. Así, vamos a trastear un poco, describiendo funciones para la obtención de datos del sistema, con el único objetivo de conocer algunas funciones más e iniciar conceptos de estructuras de datos, distintos de los básicos (enteros, carácter, booleanos, cadenas, etc...) necesarios para pasar como parámetros a algunas de éstas.

```
Procedimiento GetSystemTime
(lpSystemTime: TFecha).

Contenida en Kernel32.dll. Alias
"GetSystemTime"
```

Este procedimiento obtiene la fecha y hora del sistema. lpSystemTime es un parámetro de entrada/salida de tipo TFecha, que podemos estructurar en 128 bits, con 8 campos de tipo Word (16 bits), cada campo contendrá el año, el mes, el día del mes, el día de la semana, la hora, el minuto, segundo, y milisegundo. Quedando la estructura de datos así:

```
tipo TFecha = paquete
wAnyo: word;
wMes: word;
wDiaMes: word;
wDiaSemana: word;
wHora: word;
wMinuto: word;
wSegundo: word;
wMilisegundos: word;
fin
```

Esta declaración es similar al typedef struct del C.

Procedimiento GetLocalTime (lpSystemTime: TFecha).

De Kernel32.dll. Alias "GetLocalTime"

Con una simple declaración de variable local de tipo TFecha, en nuestra función principal, haremos una llamada a GetSystemTime (variable); recordando que dicho parámetro debe pasarse como entrada salida, es decir es un parámetro pasado como referencia (puntero a dicho dato), almacenando en cada uno de los campos anteriores el valor correspondiente.

Análogamente existe:

Funcion GetUserName (lpUsuario: array of char, nLongitud: Long).

Contenida en advapi32.dll. Alias "GetUserNameA".

Exactamente igual que el anterior, pero obteniéndose los datos correspondientes a la fecha y hora local. (La que vemos en el reloj de Windows por ejemplo).

Otras funciones interesantes son:

lpUsuario es un array (vector) de caracteres, y nLongitud es un entero largo (32 bits). Ambos son parámetros de entrada-salida. nLongitud debemos inicializarlo a la longitud que se va a copiar, antes de pasarlo en la función, esta longitud debe ser igual a la dimensión del vector, el resultado se copiará en el array lpUsuario.

Ya hemos visto algunas funciones y procedimientos más, y hemos observado el paso de parámetros por valor (caso del Beep), o por referencia, así como la creación de un tipo de datos necesario para pasar a estas funciones, sólo es cuestión de conocer el tamaño (en bits) del parámetro y si no existe como tipo básico, pues lo definimos nosotros como ha sido el caso de TFecha. Este tamaño se puede obtener simplemente usando operadores del tipo similar al SizeOf() del C.

En el próximo artículo publicaré como, usando el API, se puede manipular desde nuestra aplicación otros procesos, ya sea cerrarlos, simular eventos o pulsaciones de teclas, útil por ejemplo para eliminar aquellas ventanas molestas (pop-ups) que aparecen repetidamente, o para hacer trampas en juegos que requieren de habilidad con las teclas o el ratón.

Samir Sabbagh Sequera (HySTD)

Seguridad Inalámbrica: WEP

By j8k6f4v9j

En este caso vamos a ver una pequeña y breve guía de cómo la seguridad WEP no es la mejor forma de proteger nuestras redes, siempre y cuando halla alguien con un mínimo de conocimientos y ganas de perder 10 minutos en romper la protección.

Hay ya varios manuales, pero ahí va una mini guía:

- Descargar Troppix1.2. Esta livecd ya tiene los controladores para esta tarjeta (y la mayoría de ellas, sólo que para algunas sería recomendable tener las últimas versiones.. (Por ejemplo para las atheros). Quemar el cd y obviamente arrancar el equipo con él.

- Luego sería más o menos así:

```
iwlist ra0 scan
```

Con esto escaneamos las redes al alcance. Nos daría un resultado similar a éste (es un ejemplo, en realidad al momento de escribir esto tengo 22 entradas en la lista ;D):

```
Cell 01 - Address: 00:03:C9:BB:CC::DD
                   Mode:Managed
                   ESSID:"Essid1"
                   Encryption KEY:on
                   Channel:11
                   Quality:0/100   Signal
level:-62 dBm   Noise level:-202 dBm

Cell 02 - Address: 00:03:C9:EE:FF:11
                   Mode:Managed
                   ESSID:"Essid2"
                   Encryption KEY:on
                   Channel:6
                   Quality:0/100   Signal
level:-71 dBm   Noise level:-193 dBm
```

Suponiendo que queremos probar la seguridad de la primera entrada de la lista, y teniendo en cuenta que ya disponemos de las herramientas necesarias en nuestro sistema, comenzamos a hacer el trabajo. : P

```
airodump ra0 captura1 11
```

Con este comando hacemos que la tarjeta entre en modo monitor y se ponga a "escuchar" en el canal 11.

```
iwconfig ra0 rate 1
```

Este comando es muy recomendable ejecutarlo, ya que al bajar la velocidad de transmisión a 1 megabyte hacemos que la comunicación sea más estable a mayor distancia.

```
aireplay -1 0 -e Essid1 -a
00:03:C9:BB:CC::DD -h 55:44:33:22:11:00
ra0
```

Sólo clientes debidamente autenticados y asociados al AP podrán "entablar comunicación" con éste. El ataque -1 lo que hace es asocias la dirección MAC que definimos en -h con el AP con ESSID 'Essid1' y BSSID (esto es la MAC del AP) 00:03:C9:BB:CC:DD

Ahora, y si no recibimos paquetes de deautenticación, estamos asociados al AP. O mejor dicho está la MAC 00:03:C9:BB:CC:DD asociada al AP

Necesitaremos aproximadamente un mínimo de un millón de paquetes encriptados para poder averiguar la clave WEP que se está utilizando para cifrar la comunicación. Si pretendemos capturar este volumen de datos de forma pasiva (sólo "oyendo") pues hay que esperar sentados. Y mucho tiempo por cierto. Es por ello por lo que se usa la reinyección.

La reinyección consiste en básicamente capturar un paquete ARP para modificarlo ligeramente y enviárselo al AP. Éste, aunque fuera para mandarnos a hacer gárgaras, nos responde con un paquete también cifrado, pero con un nuevo vector de inicialización. Estos vectores de inicialización diferentes son justo lo que necesitamos.

Si en el comando que escribimos anteriormente para ejecutar airodump escribiésemos un '1' al final, entonces le estaríamos diciendo que sólo capturase los vectores de inicialización (de aquí en adelante IVs), en lugar de los paquetes cifrados completos. El comando quedaría así:

```
airodump ra0 captura1 11 1
```

Pasamos a reinyectar, como si fuésemos el cliente asociado:

```
aireplay -3 -b 00:03:C9:BB:CC::DD -h
55:44:33:22:11:00 ra0
```

Debemos esperar. Vamos, mode_paciencia=on, ya que hasta que no capturemos ese ARP no comenzará la reinyección.

Cuando ésta se produzcan veremos como el valor de #data comienza a subir rápidamente. Todos esos paquetes quedarán almacenados en el archivo de captura que airodump ha creado al iniciarse. Pero ojo, se perderán si reiniciamos, ya que estamos trabajando con una livecd. Hay dos soluciones alternativas: Usar un linux instalada al disco duro (recomiendo ésta por supuesto) o guardar la captura en algún tipo de medio.

Una vez tenemos ese ansiado millón de paquetes podemos probar a lanzar aircrack sobre él para ver si nos da la clave.

Desde el mismo directorio donde lanzamos la captura:

```
aircrack *.cap
```

hará que aircrack se ponga manos a la obra. Si todo ha ido bien, dará sus frutos, y habremos demostrado una vez más que nuestro AP es vulnerable.

Troppix 1.2 http://tinyurl.com/rp9fu (Pobierz para descargar)

Cómo instalar el módulo para nuestra tarjeta inalámbrica en linux (debian)

En esta guía explicaré cómo instalar el módulo encargado de controlar una tarjeta inalámbrica con chipset rt2500.

Para poder añadir módulos a nuestro sistema debemos tener instaladas en éste bien las fuente o bien los headers del kernel que estemos usando.

En debian es bastante sencillo, ya que el mismo comando averiguará la versión del kernel que estamos usando y nos instalará los headers adecuados:

```
apt-get install kernel-headers-$(uname -r)
```

Una vez tengamos las cabeceras (headers) del kernel necesitaremos algunos programas más. Para estar seguros instalaremos el paquete buil-essential:

```
apt-get install build-essential
```

Luego de esto descargamos las fuentes de la última versión de los drivers para la tarjeta.

Para esta guía usaré:

```
rt2500 PCI/PCMCIA nightly CVS tarball:
                rt2500-CVS.
```

Las diferentes versiones de este driver las podéis encontrar en http://rt2x00.serialmonkey.com/wiki/index.php/Downloads

Bien, vamos al lío.

Antes de nada, por cuestiones personales de organización l o que yo hago es cambiar a un directorio donde poder operar sin líos innecesarios:

```
Cd /user
```

En este directorio no tenemos permisos de escritura como usuarios ordinarios, por lo que para mayor facilidad podemos hacernos root desde ya.

```
su
```

Tras introducir el password de root ya tenemos los privilegios de superuser. Pasamos a descargar el paquete con el módulo.

```
wget http://rt2x00.serialmonkey.com/
rt2500-cvs-daily.tar.gz
```

Una vez lo tenemos descargado lo podemos ver con:

```
ls
```

Ahora lo descomprimimos

```
tar -xvzf rt2500-cvs-daily.tar.gz
```

Esto nos creará una carpeta cuyo nombre comienza por 'rt'. Entramos en ese directorio:

```
Cd rt*
```

Si tenemos todo lo necesario bastará con compilar el controlador e instalarlo:

```
Cd Module;make
Make install
```

Ahora ya debemos poder iniciar el módulo. Para ello bastará con:

```
Modprobe rt2500
```

Y deberá aparecer una nueva interfaz en nuestro sistema llamada 'ra0'. La podemos ver con:

```
ifconfig -a
```

Si queremos configurar la conexión inalámbrica necesitaremos las wireless-tools. Pero eso ya es otro manual : P (próximamente)

Salu2

j8k6f4v9j

Realizar y estructurar un ataque.

By hail

Buenas como veo a mucha gente perdida en esto a ver si así os aclaro un poco. Todo esto lo voy a ver desde el lado bueno de la fuerza, intentando resolver los problemas, que un hacker puede crear en nuestras redes, es decir desde el lado del técnico en seguridad que intenta resolver todos los ataques, y para ello tiene que explicar como se ejecutan y como se contrarrestan.

Vayamos por pasos, empecemos enumerando.

1) Identificar el problema.

En esta parte voy a explicar como un hacker antes de entrar en nuestros sistemas, tiene que recompilar mucha información y como se puede hacer de forma fácil para que le sea difícil recompilarla.

2) Hack del sistema

Aquí explicare como después de recompilar la información necesaria se empieza a atacar el sistema. Esto abarca a todos los sistemas operativos y todos sus agujeros. Incluiremos también como borran todas sus huellas los que saben y como dejan brechas casi invisibles en nuestro sistema para entrar cuando quieran.

3) Hack a la red

Aquí detallare como se puede hacer uso de dispositivos tales como servidores de acceso telefónico, routers, cortafuegos, vulnerabilidades en protocolos de bajo nivel como el x25. Explicare como echar un candado hermético a tu red para solucionar estas posibles brechas.

4) Hack del soft.

Examinaremos aquí las aplicaciones que nos llevan de cabeza a los técnicos en seguridad informática, tales como por ejemplo programas de control remoto, puertas traseras, software de servidor de red y demás brechas potenciales de los mismos.

Como esto no va a ser cosa de diez minutos iré poniendo cada apartado, cada semana, así también me da tiempo a repasar mis apuntes a mí que no soy dios y siempre aunque se sepa hacer se debe consultar en los apuntes.

Un hacker antes de nada, cuando quiere atacar un sistema en concreto o una red, tiene que recompilar gran cantidad de información de la estructura intranet/extranet y de los sistemas de seguridad implementados en ellos.

Internet desde el principio fue diseñado para ser funcional, dando más información de la necesaria a quien sepa encontrarla.

En este apartado os vamos a enseñar como y donde se recompila esa información tan valiosa para poder llevar a cabo un buen ataque y como hacer para que sea mas difícil para el mismo recompilarla.

Un atacante puede recompilar una cantidad desconocida y reducirla a una extensión especifica de nombres de dominio, bloques de redes y direcciones IP individuales de sistemas conectados directamente a Internet, mediante una combinación de herramientas y técnicas.

Veamos la información critica que un atacante puede recompilar día a día de nuestros sistemas de seguridad y redes implementados.

: DE INTERNET :

Nombre de dominio, bloques de red, direcciones IP especificas de sistemas vía Internet, servicios TCP y UDP funcionando en cada sistema, arquitectura del siste ma, mecanismos de control de acceso y listas de control de accesos relacionadas (ACL),sistemas de detección de intrusión (IDS), enumeración del sistema (nombres de usuarios y grupos, encabezados del sistema, tablas de direccionamiento, información SNMP.)

: DE INTRANET :

Protocolos de red en uso (IP, IPX, DECNET), nombres de dominio internos, bloques de red, direcciones IP especificas de sistemas disponibles vía intranet, servicios TCP y UDP funcionando en cada uno de los sistemas, arquitectura del sistema, mecanismos de control de acceso y ACL, sistemas de detección de intrusión, enumeración del sistema (nombres de usuarios y grupos, encabezados del sistema, tablas de direccionamiento, información SNMP.)

: DE ACCESOS REMOTOS :

Números de teléfono analógico/digital, tipos de sistemas remotos, mecanismos de autentificación.

: DE EXTRANET :

Origen y destino de la conexión, tipos de conexión, mecanismos de control de acceso.

Veamos como seguir el rastro por Internet.

Todo esto lo voy a empezar guiando para seguir el rastro a una empresa conectada a Internet.

En primer lugar tendremos que decidir si solo vamos a seguir el rastro de esa empresa o si vamos a seguirlo también de todas las que tenga conectadas como podrían ser las filiales.

Lo primero será ir a la página Web de la empresa si la tiene para sacar la máxima información de la misma.

Buscaremos ubicaciones, compañías relacionadas, noticias de fusión o adquisición, nombres de contacto y direcciones de correo, políticas de seguridad y privacidad que indiquen los tipos de mecanismos de seguridad instalados, enlaces a otros servidores Web relacionados con la empresa, ver el código fuente de la página para leer los comentarios puesto que a veces se da información critica en los comentarios.

También buscaremos en Internet información sobre si esa empresa ha tenido ya ataques de seguridad puestos que podría revelar información muy útil para el atacante.

Una vez tengamos cuentas de correo apuntadas buscaremos en Usenet correos con el @dominio empresa. Para ver que tipo de comentarios hacen, si están en foros, preguntando dudas sobre sus aplicaciones y sistemas etc. Finalmente siempre podrás utilizar las búsquedas avanzadas de altavista o hotbot. Aquí puedes encontrar los sitios que enlacen con la empresa objetivo para seguir recompilando información.

Un fallo muy común en empresas que están fusionándose es dar conectividad entre ellas sin mirar la seguridad, en las Pág. de la empresa y las que linkean podemos encontrar este tipo de información además de muchas mas información relevante de la empresa.

La manera de solventar esto es eliminando de las Pág. Web de la empresa cualquier información sobre la misma en el ámbito de la seguridad de la red y de la estructura de la misma, otra cosa a evitar es que los usuarios de la red que gestionamos hagan consultas en foros sobre programas o implementaciones que existan en la red.

ENUMERACION DE LA RED.

El primer paso a dar es identificar nombres de dominio y redes asociadas relacionadas con la empresa en particular. Así constataremos la presencia de la empresa en Internet.

Para enumerar los dominios y empezar a averiguar cosas hacemos una búsqueda whois en los servidores whois de la zona geográfica en la que esta ubicada la empresa.

Dirección IP europea http://ripe.net
Dirección IP asiática http://whois.apnic.net
Dirección IP EEUU militar http://whois.nic.mil
(No disponible)
Dirección Gob EEUU http://whois.nic.goveste
(No disponible)

Sigue estando esta, del gobierno americano mirad:

```
alfredo@linux:~>  whois  nic.gov
%  DOTGOV  WHOIS  Server  ready
Domain  Name:  nic.gov
Status: Active
   Please be advised that this whois
server  only  contains  information
pertaining to the .GOV domain. For infor-
mation for other domains please use the
whois server at RS.INTERNIC.NET.

alfredo@linux:~>
```

Una vez que hemos identificado una red entidad u organización, nos vamos a Internic o a cualquier base de datos de este tipo, y hacemos 1 consulta whois, de este modo vemos los dominios asociados a la empresa y filiales, pero como bien sabemos no tienen porque estar activos todos, a veces se compran todos los nombres para proteger 1 marca con lo cual, habrá q seleccionar los activos, como bien sabemos Internic limita los documentos encontrados asociados a 1 dominio a los 50 primeros, pero en http://www.websitez.com suele aso- ciarse todos los documentos asociados al dominio. Parece haber cambiado la Pág. , pero aquí os dejo un nuevo link ,como no.

http://www.searchengines.net/websitez_se.htm

Realizamos una consulta whois en una consola de sistema poniendo el nombre de dominio de la victima, y nos dará los DNS de la misma.

Aquí tenéis un ejemplo:

```
Whois juanitoperez.com
Whois Server Version 2.0
Domain names in the .com and .net domains
can now be registered with many different
competing registrars. Go to http://
www.internic.net for detailed
information.
```

Continua...

```
Domain Name: juanitoperez.COM
Registrar: LAGORDA.INCWhois
Server: whois.opensrs.net
Referral URL: http://domainhelp.lagorda.com
Name Server: NS2.juanitoperez.COM
Name Server: NS1.juanitoperez.COM
Status: ACTIVE
Status: ok
Updated Date: 02-Jun-2005
Creation Date: 02-Jun-2005
Expiration Date: 02-Jun-2006

>>> Last update of whois database: Fri,
12 May 2006 07:01:41 EDT <<<

NOTICE: The expiration date displayed in
this record is the date the
registrar's sponsorship of the domain
name registration in the registry is
currently set to expire. This date does
not necessarily reflect the expiration
date of the domain name registrant's
agreement with the sponsoring
registrar. Users may consult the
sponsoring registrar's Whois database to
view the registrar's reported date of
expiration for this registration.


TERMS OF USE: You are not authorized to
access or query our Whois
database through the use of electronic
processes that are high-volume and
automated except as reasonably necessary
to register domain names or
modify existing registrations; the Data
in VeriSign Global Registry
Services' ("VeriSign") Whois database is
provided by VeriSign for
information purposes only, and to assist
persons in obtaining information
about or related to a domain name
registration record. VeriSign does not
guarantee its accuracy. By submitting a
Whois query, you agree to abide
by the following terms of use: You agree
that you may use this Data only
for lawful purposes and that under no
circumstances will you use this Data
to: (1) allow, enable, or otherwise
support the transmission of mass
unsolicited, commercial advertising or
solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume,
automated, electronic processes
that apply to VeriSign (or its computer
systems). The compilation,
repackaging, dissemination or other use
of this Data is expressly
```

```
use electronic processes that are
automated and high-volume to access or
query the Whois database except as
reasonably necessary to register
domain names or modify existing
registrations. VeriSign reserves the
right
to restrict your access to the Whois
database in its sole discretion to
ensure
operational stability. VeriSign may
restrict or terminate your access to the
Whois database for failure to abide by
these terms of use. VeriSign
reserves the right to modify these terms
at any time.

The Registry database contains
ONLY .COM, .NET, .EDU domains and
Registrars.
Registrant:
juanito perez SL
juanito perez SL
Murcia, Murcia 30009
ES

Domain name: juanito.COM
```

Basándonos en la consulta, el punto de partida más lógico, es nombre de la empresa.com, al hacer una consulta sobre el dominio, lo mas lógico es que, entre la información que nos da estén las IPS de los DNS del dominio.

Este tipo de consulta nos proporciona mucha información sobre el dominio, quien registro el dominio, el nombre del dominio, el administrador ,cuando fue creado y actualizado el registro, los servidores de nombres (DNS)...

Llegados a este punto, tendremos que empezar a analizar la información conseguida, en busca de datos necesarios para seguir acercándonos a nuestro o bjetivo . Los contactos administrativos son importantes, al igual que los números de teléfono, fax y direcciones de email, Con los primeros es posible identificar al responsable de la conexión del cortafuegos o al administrador, los teléfonos. y fax son útiles para la revisión de penetración telefónica, los mails nos proporcionan una vía de contacto, para intentar colar código, rastrear los mails y post de usuarios de ese dominio en busca de preguntas sobre soft y medidas implementadas para saltarlas, y para intentar engañar a un usuario de la red mediante ingeniería social.

Apunta todo esto y empezaras con buen pie. El buscar todos los dominios relacionados también te puede llevar hasta páginas Web ilegales dentro del dominio subida

por usuarios de la red sin permiso ni control del administrador.

Llegados a este punto y con un mail anónimo puedes suplantar la identidad del administrador y engañar a un usuario de la red en cuestión que no se entere mucho y hacerle cambiar su contraseña diciéndole que son políticas implementadas por el proyecto de seguridad que sigue la empresa. Las fechas en las q se crea y actualiza el registro del dominio nos indican si la información recopilada es válida o puede haber cambiado.

Si el documento fue creado hace 2 años y no se ha actualizado nunca es posible que ya no sea el mismo administrador o que la red debido a su crecimiento haya cambiado.

Utilizando la instrucción Server con el registro HST conseguido con una consulta whois podrás descubrir los otros dominios para los que esta autorizado un servidor DNS.

Ejecuta 1 consulta whois en tu dominio con un whois destino.com:
Localiza el primer dns .

```
Ejemplo:: whois Juanitoperez.com
```

Haz una consulta a tu DNS y ejecuta una consulta whois dirección IP del DNS
Localiza el registro HST para el servidor dns.

```
Ejemplo:: whois IP DESTINO
```

Ejecuta en consola whois con la instrucción server utilizando:
whois server NS9999-HST

CONSULTA DE RED

Ahora que ya tenemos un rango de redes suministrado por los anteriores servidores DNS , comenzamos una consulta para ver las redes reales asociadas al dominio de la empresa . Para esta consulta volvemos a las bases de datos de arin, ya q Internic solo contiene dominios.

En http://www.arin.net/whois

Aquí veremos cual es el proveedor ISP que ha concedido las IPS al DNS de nuestra víctima.

CONSULTA POC

Como el contacto administrativo puede serlo de varias empresas, realiza una consulta poc para intentar descubrir dominios que no hubiéramos encontrado anteriormente. Podemos realizar también una consulta del tipo @dominio.net para sacar todas las cuentas de correo pertenecientes al dominio.

Consulta el RFC 954-NIC-VALUE/WHOIS ¿Y si pones whois? Te sacara toda la ayuda del mismo. Para obtener una lista completa de los miembros de un grupo u organización, o una lista de todos los usuarios autorizados de un host ponga delante del nombre. Del host u organización un asterisco ejemplo *SRI-NIC

He de aclarar que toda esta documentación y todo lo que voy aclarando no lo se por ciencia infusa, estoy siguiendo mis apuntes y mis libros de los master y cursos que he realizado en seguridad informática.

CONTRAMEDIDAS SEGURIDAD EN BASES DE DATOS PÚBLICAS.

Cuando una empresa registra un dominio en Internet, necesita contactos administrativos, bloques de red registrados e información del servidor de nombres autorizado. Muchas veces el contacto administrativo cambia y es capaz de cambiar la información relativa a la empresa que aparece en estas bases de datos públicas.

Lo primero sería tener esa información bien actualizada y asegurarnos de que sea fiable.

Con los números de teléfono y fax lo que podemos hacer es utilizar números gratuitos o en su defecto sacarlos de la centralita de la red.

Cree una cuenta de administrativo ficticia y así conseguirá que si alguien intenta hacer ingeniería social con alguno de sus usuarios nos ponga en alerta de posibles ataques. Es importante que el método de autentificación para poder cambiar los datos de estas bases sea mediante contraseña y autentificación PGP. Así evitaremos que nos pase lo de a AOL.
La siguiente parte va desde la consulta de servidores DNS, de cómo determinar los registros mx contramedidas.

Reconocimiento de la red y sus contramedidas y ya paso a la exploración

Después de identificar todos los dominios asociados, empezaremos las consultas al dns.

El DNS es una base de datos distribuida, que transforma direcciones IP en nombres (nombres de host) y viceversa. Si el DNS no ha sido muy bien configurado, uno de las posibles fallas que nos encontraremos, es que se permite la transferencia de zonas, a usuarios no autorizados desde Internet. Las transferencias de zona, permiten al servidor secundario

actualizar su base de datos de zona, esto es lo normal puesto que siempre se pone un DNS secundario para tener redundancia a fallos, por posibles caídas puntuales del servidor DNS principal.

Lo que pasa aquí, es que si el no esta bien configurado transferirá las zonas a cualquier usuario que sepa pedírselas, poniendo así al descubierto el mapa interno de la red. Para realizar las transferencias de zona utilizaremos un cliente nslookup,

Una vez aquí ya estamos haciendo las consultas desde su DNS.

Después de que se complete la transferencia de zona, podemos mirar el archivo generado, para ver si podemos encontrar información especifica de algún sistema.

Podremos ver que en cada entrada tiene un registro A, que es una dirección IP, además veremos también que cada host, cuenta con un archivo HINFO, que nos identifica el sistema operativo que se esta utilizando. (RFC-952)

Esta es la forma manual, existen en muchas herramientas que lo harán automáticamente, por ejemplo el mandato host.

SamSpade, axfr, dig y en general muchas más.

DETERMINAR LOS REGISTROS MAIL EXCHANGE.

Normalmente en las redes en las que existen servidores de correo, en el mismo servidor, es donde se suele instalar un firewall, o por lo menos pertenecen a la misma red, si la empresa tiene subredes internas implementadas. Con la información que nos de el mandato host, y contrastándolo con las búsquedas anteriores, vamos a asegurarnos de que todos los datos encontrados son muy probablemente fiables.

CONTRAMEDIDA: SEGURIDAD EN EL DNS

Desde la perspectiva de configuración de un host, deberá restringir las transferencias de zona a usuarios autorizados.

```
Ejemplo:: nslookup >> Server (aquí pon el
servidor dns de la victima)
 - - - dale al intro y aparece - - -
     Default Server: (aquí te saldrá la
IP del dns de la victima)
     Address: (aquí te saldrá la IP del
dns de la victima)
     >> Set type=any (aquí le decimos
que nos muestre cualquier tipo de regis-
tro asociado con la consulta)
     >> ls -d (nombre de dominio victi-
ma).
     >>/tmp/zone_out (aquí le decimos
que lo liste y redirigimos la salida al
archivo /tmp/zone_out para poder manipu-
larlo cómodamente luego)
```

En BIND, en el archivo named.boot, podrá utilizar la directiva xfernets para imponer este tipo de restricciones. En Windows para restringir las transferencias de zona de un DNS de Microsoft, activando notify aplicara las restricciones. En la red puede activar un cortafuegos, o un router que filtre el puerto 53 TCP.

Como las transferencias de zona son TCP, desbarataremos sus planes.

Así conseguiremos que el que intente transferírselas, se quede con las ganas puesto que las consultas son UDP, y las transferencias TCP .

Además como ya sabemos, deberemos de configurar el DNS, para que solo ofrezca nombres de maquinas, que estén conectadas a Internet directamente.

```
@linux:~> host --help
host: illegal option -- -
host: illegal option -- h
host: illegal option -- e
host: illegal option -- p
Usage: host [-aCdlriTwv] [-c class] [-N
ndots] [-t type] [-W time]
[-R number] hostname [server]
-a is equivalent to -v -t *
-c specifies query class for non-IN data
-C compares SOA records on authoritative
nameservers
-d is equivalent to -v
-l lists all hosts in a domain, using
AXFR
-i IP6.INT reverse lookups
-N changes the number of dots allowed
before root lookup is done
-r disables recursive processing
-R specifies number of retries for UDP
packets
-t specifies the query type
-T enables TCP/IP mode
-v enables verbose output
-w specifies to wait forever for a reply
-W specifies how long to wait for a reply
-4 use IPv4 query transport only
-6 use IPv6 query transport only
```

Los archivos HINFO mejor no los uséis son peligrositos, puesto que facilitan la detección mediante el empleo de programas, de sistemas potencialmente vulnerables.

RECONOCIMIENTO DE LA RED.

Ahora que ya tenemos identificadas redes de la empresa, empezamos a utilizar el traceroute o tracert en Windows, para identificar las rutas de acceso potenciales. La herramienta de diagnostico traceroute, le indica la ruta que sigue un paquete IP desde un host al siguiente hasta llegar a su destino.

```
Ejemplo: traceroute -S -p53 (IP victima)
```

Utiliza un ttl para obtener un mensaje ICMP time_exceeded de cada router, de esta forma el campo ttl se vuelve un contador de saltos.

Esto nos permitirá, descubrir la topología de la red empleada por la red de la empresa, la red formada por el gateway, cortafuegos y sistemas conectados a Internet o que hagan uso de las listas de acceso de un router, con los dispositivos de enrutamiento de su ISP, además de identificar cortafuegos basados en aplicación, o routers con filtración de paquetes.

Con el mandato host anteriormente hemos visto los registros mx comparándolos con los registros del traceroute veremos que seguramente como mínimo concuerda uno, el cual va a ser un host activo de la empresa y el salto anterior a el, el router frontera de la empresa.

También podría ser un firewall o algún sistema de filtrado.

Aunque aun no lo sabemos con seguridad generalmente esto suele ser así.

En un entorno mas complejo, puede haber múltiples rutas, dispositivos de enrutamiento con múltiples interfaces tipo teldat, cisco 7500 y cosas así, y cada interface puede tener distintas listas de acceso, cosa que dificultara el trabajo del traceo puesto que no dejara pasar las peticiones, aunque en muchos casos si lo hará.

Así pues es importante asignar la red completa utilizando traceroute.

Después de indagar mucho los sistemas de la red empezaremos a poder tener una visión más amplia del diagrama de red, del gateway de Internet y los sistemas que están utilizando las listas de control de accesos. Esto es comúnmente llamado diagrama de ruta de acceso.

Conviene explicar que lo mas normal es que las medidas de filtrado paren nuestros paquetes. Lo que hay que hacer es ver qué tipo de paquetes bloquea, si ICMP o UDP, de todas también esta la posibilidad de que permitan el paso de paquetes encaminados a su DNS como consultas, puerto UDP 53, puesto que muchas empresas permiten en sus DNS consultas entrantes.

En este caso los paquetes habrán pasado felizmente por entre los dispositivos de control de acceso.

Al hacer este tipo de sondeo no se reciben paquetes normales de ICMP no alcanzado, sino que no se recibirá ningún paquete cuando alcance su destino final, con lo cual no veremos aparecer un host cuando llegue al final.

Si preferís el modo grafico visualroute va muy bien, aunque hay muchos programas que hacen esto. Existen técnicas adicionales que te permitirán determinar las ACL específicas para dispositivos de control de acceso dados.

La técnica Firewall protocol scanning es una de ellas y la trataremos mas adelante.

CONTRAMEDIDAS
FRUSTRAR EL RECONOCIMIENTO DE LA RED.

Muchos programas IDS detecten estos tipos de sondas de reconocimiento de la red, como tdetect que registra mediante logs cualquier paquete UDP ICMP con ttl 1.

También podemos generar respuesta falsa con Roto-Router que además registra las peticiones.

En nuestros sitios Web habría que emplear una seguridad que nos permitiera configurar los routers para limitar el trafico UDP e ICMP a ciertos sistemas.

Estas herramientas y técnicas eran las mas comunes hace unos cinco años pensad que como si dijéramos esta es la manera mas pura de rastrear, y que todos los días aparecen nuevas técnicas y programas.

Todas estas tareas se deberían automatizar con shells y scripts expect o programas perl.

Habrá por tanto que vigilar los accesos si se quiere

```
Ejemplo: traceroute -S -p53 (IP victima)
```

llevar un control de seguridad.

EXPLORACIÓN

Ya hemos merodeado en busca de información y ahora nos disponemos a empezar a buscar posibles vías de entrada. Hemos conseguido una lista de direcciones IP y de red utili-

zando las transferencias de zona y las consultas whois. Estas técnicas nos han proporcionado nombres de empleados, teléfonos, rangos IP, servidor DNS y servidor de correo. Ahora veremos los sistemas que se encuentran activos y cuales son accesibles desde Internet, mediante el uso de barridos ping, exploración de puertos y programas de búsqueda automatizadas.

Muchas veces nos encontraremos como decíamos, servidores de nombres que transfieren sus zonas e incluso una lista con direcciones IPS. Dado que ciertos rangos de direcciones IP no son direccionables en Internet, tendríamos muchos problemas para conseguir acceder a las mismas. Tendremos pues que seguir recompilando información en la fase de exploración.

Un paso básico en la exploración son los barridos ping, le asignamos un rango de direcciones IP y bloques de red a una utilidad que nos lo hará mas sencillo que es fping.

Fping fue diseñada para ser usada en una scripts de shell con gping.

Con gping generamos una lista de direcciones IP que se introduce en fping para determinar que sistemas están activos. También podremos realizar esta tarea con nmap. Cuando encontremos el trafico ICMP bloqueado en el router frontera de la empresa, lo mejor es que exploremos los puertos que las maquinas que están conectadas que hemos visto anteriormente tienen a la espera. Para determinar si el sistema esta activo lo mejor es utilizar nmap y su opción para hacer un ping TCP al puerto 80, puerto que los routers tendrán abierto al igual que los sistemas activos, y también veremos si bloquea ICMP. En general haremos lo mismo con los puertos mas comúnmente usados como 25, 110, 143, 23 .... también y mediante hping conseguiremos pasar muchas reglas de filtrado y dispositivos de control de acceso dado que podremos fragmentar los paquetes, cosa a la cual la mayoría de controles de acceso dejaran pasar. Esto es debido a que no manejan correctamente estos paquetes fragmentados y entonces los dejan pasar.

CONTRAMEDIDAS PARA BARRIDOS PING

Como se ha visto los barridos ping en redes son una muy buena herramienta, para saber cuales de los equipos encontramos activos después de indagar que servicios ofrecen y que puertas vamos a usar mediante la exploración que hemos hecho.

Los programas IDS basados en red, nos ofrecerán una manera de detección de los mismos, como bien sabéis también se puede generar código para detectar este tipo de barridos.

y etc. que no voy a desarrollar del todo buscar y aprender a programar estas cosillas que es sencillo. Si detectamos ICMP ECHO desde un sistema o red determinados es posible que nos estén haciendo un reconocimiento de red desde nuestro sitio Web. Por tanto convendría controlar estas cositas. Tendremos pues que evaluar el tipo de trafico ICMP que permiten nuestras redes, que yo sepa en la actualidad existen 18 tipos de ICMP, con lo cual a mirarlo todo muy bien.

Tendremos que presentar especial atención a las necesidades de la empresa, según que tipo de trafico ICMP necesite deberemos controlarlo pero no cortarlo, y cortar eso si el resto de trafico de este tipo a ser posible con un firewall de hardware. Una solución puede ser permitir únicamente el paso de la red DMZ de paquetes ICM ECHO_REPLY, HOST UNRECHABLE Y TIME EXCEEDED. Además deberíamos de limitar como siempre las ACL para asegurar bien y si es posible el trafico ICMP para direcciones IP especificas de nuestro ISP. Esto dificultara los barridos a sistemas conectados directamente a Internet.

Aunque ICMP nos permite diagnosticar problemas de red, también si esta habilitado en nuestro gateway o router frontera, permitirá que los atacantes pueda hacer una negación de servicios a nuestra red, incluso si quieren podrán ocultar paquetes en ICMP ECHO usando programas como loki, este programa se puede encontrar en la página de phrack.com.

Otro concepto importante es pingd, fue desarrollado por Tom Ptacek y pasado a Linux por Mike Schiffman, es un demonio de usuario que gestiona a nivel de host todo el trafico ICMP_ECHO e ICMP_ECHOREPLY, esto se consigue eliminando la compatibilidad del procesado ICMP_ECHO, desde el núcleo e implementa un demonio de usuario con un socket ICMP en bruto para manejar los paquetes. Esto proporcionara al administrador un sistema de control de acceso a nivel de sistema para ping.

```
#ICMP/Ping flood detection

ping_schema = library_schema:new( 1,
[ "time", "ip", "ip", "ethmac",
"ethmac" ],
scope ( ) ) ;
count = 0;
maxtime = 10;
maxcount =5;
dest = 0;
```

CONSULTAS ICMP

Los barridos ping es una mínima parte en lo que se refiere a la información que ICMP da.

Con icmpquery o icmpush, puedes solicitar desde la hora del sistema y ver en que franja horaria se encuentra, hasta la mascara de red de un dispositivo en concreto, con lo cual podríamos saber cuantas subredes o redes engloba la misma y evitar así las direcciones de difusión.

CONTRAMEDIDAS PARA ICMP

La contramedida a utilizar es evitar que los router frontera tales como los cisco de la empresa, acepten en su red paquetes TIMESTAMP y ADDRESS MASK utilizando las ACL para ello.

Esto en los routers cisco por ejemplo impediría estas peticiones , pero se debe de aplicar a la interfaz correspondiente. También sería factible utillizar la opción established para hacer esto.

EXPLORACION DE PUERTOS

Teniendo la información necesaria ya podemos empezar a explorar los puertos UDP y TCP del sistema escogido para ver que servicios hay y cuales de los puertos están LISTENING.

De esta manera podremos identificar programas utilizados por esos puertos y al juntar toda la información conseguiremos identificar el sistema operativo.

De esta manera también podremos intentar encontrar fallos en los programas a la escucha y en uso, e incluso malas configuraciones de los mismos que permitan a usuarios no autorizados entrar en el sistema.

Así conseguiremos ver cuales son las vías de entrada potenciales del sistema ;-)

Los pasos a seguir en una exploración de puertos son:

Un pionero en la exploración de puertos fue FYODOR con nmap.

EXPLORACION DE CONEXIONES

Este tipo de exploración conecta con el puerto y ejecuta el acuerdo de tres vías (SYN, SYN/ACK Y ACK).

EXPLORACION TCP

```
Ejemplo:

access-list 101 deny icmp any any 13 !
petición de estampación de hora
access_list 101 deny icmp any any 17 !
petición de mascara de direcciones
```

En esta no se realiza una conexión TCP completa, por ello recibe el nombre de semiabierta.

Se envía paquete SYN y si se recibe paquete SYN/ ACK podemos decir que esta "listening".

Si se recibe un RST/ACK el puerto no esta a la escucha.

Enviaremos entonces un paquete RST/ACK para no realizar nunca una conexión completa.

EXPLORACION TCP FIN

Enviaremos un paquete FIN al puerto objetivo y según el RFC 793, el sistema objetivo devolverá un RST para todos los puertos que estén cerrados.

Esta técnica nos funcionara en sistemas como Unix.

EXPLORACION ARBOL DE NAVIDAD TCP

Esta técnica se utiliza para enviar paquetes FIN, URG Y PUSH al puerto objetivo.

```
     Identificar los servicios UDP y TCP
que se ejecutan.
     Identificar el sistema operativo.
     Identificar versiones y aplicacio-
nes específicas de cada servicio.
```

El sistema objetivo devolverá un RST para todos los puertos cerrados.

EXPLORACION NULA

Esta apaga las flags y nos devuelve un RST para todos los puertos cerrados.

EXPLORACIÓN UDP

Enviaremos un paquete UDP al puerto objetivo y si el mismo nos contesta con un ICMP no alcanzable significara

que el puerto esta cerrado, si no hubiera respuesta tendríamos ahí un puerto UDP abierto.

Como este tipo de puertos tiene un protocolo sin conexión, dependerá la fiabilidad de la misma del tipo de uso que se este dando a los recursos del sistema y de la red. Por otra parte se ralentizará muchísimo si existe algún tipo de filtrado de paquetes.

Algunas instalaciones IP devuelven a todos los puertos escaneados un RST, con lo cual los resultados obtenidos podrán variar considerablemente.

Utilizar herramientas como Strobe, Udp_scan, Netcat en unix y linux,, en Windows tenemos PortPro, Portscan y netcat que no hace bien la exploración UDP en sistemas NT.

CONTRAMEDIDAS PARA LA EXPLORACION DE PUERTOS.

Detectar una actividad de escaneo de puertos es importante para la seguridad puesto que nos proporcionara información del atacante y de sobre que puertos esta dirigiendo el mismo, podremos utilizar programas IDS basados en red para detectarlos, NFR o mecanismos basados en host nos podrán ayudar en nuestra labor.

Deberemos buscar cortafuegos que no solo tengan opciones específicas para detectar exploraciones SYN sino también las FIN puesto que muchos ignoran estas últimas siendo un grave fallo de seguridad.

En Windows BlackIce nos ayudara a controlar los escaneos de puertos y los intentos de intrusión por los mismos, reportándonos información critica del atacante como pueda ser su IP y su nombre DNS.

En la medida de lo posible (puesto que el puerto 139 en Windows da muchos servicios) intentaremos dejar única y exclusivamente activos los servicios necesarios para nuestro trabajo diario, en resto de servicios deberíamos desactivarlos para evitar así riesgos innecesarios.

DETECCION DEL SISTEMA OPERATIVO.

Hemos identificado los puertos y ahora el sistema operativo con su versión.

Rastreo de pilas.-

El rastreo de pilas es una técnica que nos ayudara a identificar cual es el sistema operativo instalado en la máquina.

A la hora de escribir las pilas TCP/IP los fabricantes interpretan a su manera la normativa RFC, con lo cual si identificamos las diferencias podremos saber casi a ciencia cierta cual es el sistema operativo.

Con programas como nmap podremos siempre que haya un puerto a la escucha acertar cual es el sistema, aun así explicare cuales son los diferentes sondeos que podemos hacer:

Sondeo FIN.-

Se envía un paquete FIN a un puerto, el comportamiento correcto del sistema seria no responder pero sistemas como NT responderán con un FIN/ACK.

Sondeo Bogus Flag.-

Se introduce un flag TCP (bandera TCP) indefinida en la cabecera TCP del paquete SYN. Sistemas operativos como Linux responden con esta misma bandera en su paquete.

Valor ACK.-

Las pilas IP no son iguales en el valor de la secuencia del campo ACK, por lo que algunos responderán con el mismo desarrollo que han recibido y otros con el número de secuencia más 1.

Apagado del mensaje de error ICMP.-

Los sistemas se ajustan al RFC 1812 quedando así limitada la velocidad con la que se envían los mensajes de error, al enviar paquetes UDP a un puerto con un numero. Aleatorio alto, podremos contar los mensajes recibidos no contestados en un tiempo X.

Muestreo de número de secuencia inicial (ISN).-

Cuando se responde a una solicitud de conexión intentaremos encontrar un patrón en la secuencia inicial elegida por la implementación TCP.

Gestión de fragmentación.-

Cada pila trata de manera diferente la superposición de fragmentos, algunas pilas escriben datos nuevos encima de los viejos y al revés, cuando recomponen los fragmentos, si miramos como se recomponen los paquetes de sondeo sacaremos mas infamación sobre el sistema operativo en concreto.

Tipo de servicio.-

El TOS se puede analizar en los mensajes de respuesta tipo ICMP UNREACHABLE

Citado de mensajes ICMP.-

No todos los sistemas coinciden en la cantidad de información que dan cuando lanzan un mensaje de error ICMP, con los datos que da podremos sacar conclusiones de cual puede ser el sistema operativo.

Supervisión de BIT no fragmentado.-

Algunos sistemas para optimizar rendimientos activan el BIT no fragmentado, con lo cual estando atentos a ese BIT podemos saber si es de los que lo activan.

Tamaño de ventana inicial TCP.-

En los paquetes de respuesta el tamaño de la ventana inicial, que en algunas pilas es único también nos ayudara en nuestra labor.

Integridad de eco de mensaje de error ICMP.-

Algún desarrollo de pila puede alterar la cabecera IP al devolver mensaje de error ICMP. Examinando la cabecera podremos intuir cual es el sistema operativo.

Nmap utiliza estas técnicas mediante la opción -o

CONTRAMEDIDAS DETECCION SISTEMA OPERATIVO

Al igual que nmap y queso pueden averiguar estos datos también puede detectar si se esta intentando en nuestro sistema y avisarnos, por ejemplo si se esta utilizando banderas SYN.

En cuanto a intentar ocultar la información y que no dijera que sistema operativo es dando pistas de una manera u otra es casi imposible y afectaría si lo intentáramos al funcionamiento del sistema negativamente, puesto que cambiaríamos las características únicas del seguimiento de pila.

Hasta ahora hemos visto todas las técnicas necesarias para barridos ping (TCP, ICMP) exploración de puertos e identificación de sistemas operativos.

Mediante los barridos ping identificamos los sistemas que están activos y los objetivos potenciales. Mediante la exploración TCP/UDP identificamos los servicios que hay a la escucha.

Y por ultimo hemos visto como identificar el sistema operativo del sistema objetivo.

Con toda esta información crítica ya podremos empezar a ver como se desencadena un ataque bien dirigido.

ENUMERACIÓN

Existen varias formas de extraer nombres de recursos exportados y cuentas de usuario validas.

La diferencia entre la recopilación que hacíamos con las técnicas hasta ahora descritas y las técnicas de enumeración es que en las primeras no existe una conexión real al sistema y no quedan registrado nada, si lo haces medianamente bien, ahora bien, con la enumeración nuestros pasos deberían de quedar registrados.

En el momento en que un tío consiga averiguar un nombre de usuario de una cuenta valida del sistema o el nombre de un recurso compartido, solo será cuestión de tiempo que consiga la clave de acceso, también solo será cuestión de tiempo que identifique algún fallo en el protocolo de comparticion de recursos. Si cerramos las vías de acceso le quitaremos una pata a la mesa del tío en cuestión. En la enumeración el tipo de información que un hacker buscara serán, recursos de red y recursos compartidos, usuarios y grupos, aplicaciones y mensajes.

Llegados a este punto y con la información que habíamos conseguido anteriormente, aplicaremos técnicas específicas para cada sistema operativo utilizando esta información que tenemos.

WINDOWS EN GENERAL

Desgraciadamente Windows NT, 2000 y 2003server, no se diseñaron para la privacidad, sino todo lo contrario, para dar a quien sepa buscarla toda la información necesaria. Con el comando net view podemos identificar los dominios disponibles en la red, enumerar las maquinas de un dominio etc.

Casi todas las técnicas usadas en la enumeración van a sacar partido de un fallo de Windows, permitir a usuarios anónimos conectar y enumerar determinados recursos sin tener permisos.

Una conocida vulnerabilidad de Windows es redbutton, conexión de sesión nula o inicio de sesión anónima.

La línea anterior conecta con la comparticion de las comunicaciones ocultas entre procesos (IPC$) en la IP de destino mediante un usuario anónimo con una contraseña nula. Si esto funciona en ese momento tendrá un canal abierto por el que extraer mucha información critica de nuestros sistemas.

Esto se puede corregir no del todo pero si un poco para que no de tanta información:

Salimos del editor y reiniciamos para que lo cargue y listo.

Incluso en sistemas como Windows 2003 Server este valor esta a 0, existe la clave pero el valor no es correcto, tendremos que ponerlo en valor 1.

Aun así programas como sid2user se saltan estos filtrados.

Una vez que tenemos abierta una sesión nula, volvemos a utilizar net view para ver los recursos compartidos en la maquina.

Con herramientas como DumpACL enumeraremos cuentas compartidas y muchas más cositas claro. Esta herramienta audita desde los permisos en el sistema de archivos hasta los servicios disponibles en sistemas remotos. También utilizaremos scanner de NETBIOS como legión para escanear recursos compartidos en redes enteras. A partir de aquí podríamos usar programas de fuerza bruta para intentar conectar con un recurso compartido.

CONTRAMEDIDAS

La manera más sencilla de evitar que se filtre toda esta información es filtrando todos los puertos TCP y UDP desde el 135 al 139 en dispositivos de acceso de red perimetrales. También vendría bien desactivar los enlaces NetBios de la interfaz en la ficha enlaces pertenecientes a la aplicación de red del panel de control de red.

Por ultimo y como decíamos antes resolveremos el

```
NET USE \\(IP de destino)\IPC$ " "/USER:
" "
```

problema de las vulnerabilidades de sesiones nulas.

GRUPOS Y USUARIOS.

Al igual que para enumerar los recursos compartidos, para enumerar usuarios y grupos iniciaremos una conexión nula, para ejecutar las herramientas necesarias. Mediante nbtstat -A (dirección IP del sistema) (ver help nbtstat) enumeraremos los usuarios y grupos a los que pertenece la maquina y los que tiene conectados. La mejor herramienta para enumerar grupos, usuarios, políticas y permisos de usuarios es DumpACL

```
    ejecutamos regedt32
    buscamos
    HKEY_L0CAL_MACHINE\SYSTEM\CurrentCo
ntrolSet\Contro l\LSA
    Seleccionamos edición | agregar va-
lor e introducimos los siguientes datos.
    Nombre de valor: RestrictAnonymous
    Tipo de dato: REG_DW0RD
    Valor: 1
```

Con esta línea de comando desde la consola de sistema hacemos que DumpACL nos muestre información relativa a los usuarios de un sistema remoto, exportándolo a un txt.

Los sistemas NT en su instalación emiten un número de longitud variable SID de seguridad. Una vez identificado un SID de un dominio, para ello utilizaremos programas como user2sid, se podrán utilizar para enumerar los nombres de usuario.

Aquí vemos en la respuesta el SID de la maquina, cuya cadena de caracteres comienza con el identificador S-1, la cadena numérica que sigue al ultimo guión es la cadena de identificador relativo RID y es la predefinida para los grupos de usuarios predefinidos de Windows tales como los grupos de invitados, administradores, etc. Así el RID del administrador es 500, el de un usuario invitado 501 etc. Así pues podremos añadir a una cadena SID conocida un RID 500 para encontrar el nombre de la cuenta de administrador, por si este ha cambiado de nombre.

Así pues y sabiendo que a cualquier cuenta creada en un dominio NT se le asigna un RID 1000 y el siguiente objeto creado posteriormente recibe el siguiente RID libre, podremos enumerar todos los grupos y usuarios alojados en el sistema.

Además estos programas se saltaran RestrictAnonymous, pudiendo enumerar puesto que estos RID no se repiten, todos los grupos no solo que hay sino que había antes también, claro esta siempre y cuando pueda acceder al puerto 139.

En el agente SNMP se podría acceder utilizando cadenas como public, con snmputil podremos enumerar los usuarios.

El "25" que es el ultimo parámetro de la sintaxis anterior es el identificador de objeto (OID) el cual especifica una rama determinada de la base de datos de información de administración o (MIB) de Microsoft, esto es un espacio jerárquico en el que cuanto mas se asciende en el árbol, se obtienen mayores cantidades de información.

Lo normal es usar cadenas de texto equivalentes puesto que recordar estas ristras de números es un lío.

server.svSvcTable.svSvcEntry.svSvcName …

```
c:\>>dumpacl /computer=\\ (IP de desti-
no) /rpt=useronly /saveas=tsv /outfile=c:
\temp \users.txt
```

(servicios en ejecución)

server.svShareTable.svShareEntry.svSharePath …
(ruta de acceso compartidas)

y unas cuantas bastantes mas que no voy a enumerar, si queréis ampliar esto buscarlo en Internet que lo encontráis rápido.

```
    c:\>>user2sid  \\(IP  destino)
"domain users"
    S-1-7-23-8915389-1645823063-
1918254000-513
    Number of sbauthorities is 7
    Domain is WIND0WSNT
    Length of SID in memory is 28 bytes
    Type of SID is SidTypeGroup
```

De todas siempre podrás utilizar herramientas tales como el IP Network Browser que es en definitiva un explorador SNMP.

CONTRAMEDIDAS SNMP

Lo suyo seria si podemos detener el agente SNMP, si no podemos siempre podemos hacer lo siguiente:

evitar que "public" este habilitado ya que no es un

```
   C:\>>sid2user \\(IP destino) 7 23
   8915389 1645823063 1918254000 500
   Name is Ares
   Domain is WIND0WSNT
   Type of SID is SidTypeUser
```

nombre de comunidad privado,

utilizar nombres de comunidad privados he impedir que otros nombres puedan mostrar información relevante, tales como public.

Cambiar ciertas claves del registro podría ser muy beneficioso si es el caso que no podamos detener el agente SNMP.

Para ello ejecutaremos regedt3 en la clave :
HKLM\System\CurrentControlSet\Services\SNMPParameters\ValidCommunities
elegir Security|Permissions y luego definalos para per-

```
c:\\snmputil walk (IP de destino) pu-
blic .1.3.6.1.4.1.73.2.1.2
```

mitir solo el acceso a usuarios autorizados.

Después abrimos :
HKLM\System\CurrentControlSet\Services\SNMP\Parame ters\ExtensionAgents

borraremos el valor que contiene la cadena LANManagerMIB2Agent y renombraremos numéricamente el resto de cadenas de manera que si esta era la numero uno la siguiente a el pasaría a ser ahora la uno y sucesivamente.

Si estamos usando SNMP para gestionar la red tendremos que asegurarnos de bloquear los puertos UDP y TCP numero 161 y 162 a todos los dispositivos de acceso a red perimetrales.

Deberíamos también prestar atención especial a los puertos 135 y 139.

TELNET

Es un mecanismo mediante el cual podemos obtener información sobre aplicaciones y enumerar mensaje
Esto funciona en las aplicaciones normales que responden al puerto, tales como HTTP puerto 80, SMTP puerto 25, FTP puerto 21, etc.....

Así conseguiremos gran cantidad de información de los servidores Windows.

Utilizando netcat podremos conectar con un puerto TCP/IP remoto.

La respuesta a la instrucción anterior seria:

Conseguiríamos con esto como se ve claramente saber cual es el fabricante y la versión del servidor Web, ahora aplicando las técnicas necesarias para la plataforma implementada, se aprovecharan las rutinas hasta tener la respuesta que esperarnos. Con DumpACL podremos como todos bien sabemos, puesto que todos los programas dejan su huella en el registro, extraer el contenido del registro de Windows de la maquina atacada, para buscar las aplicaciones que hay instaladas.

Con DumpACL conseguiremos enumerar todos los servicios de Win32 y el controlador del núcleo del sistema.

Además en la medida de lo posible, intentaremos introducir punteros a puertas traseras.

CONTRAMEDIDAS

Las aplicaciones críticas deberíamos de restringir la forma en la que dan información, buscando pues la manera de conseguir que no la den.

Ya que disponemos de netcat y tenemos también scan de puertos no estaría mal hacerles una auditoria a los sistemas, así veremos la misma información que vea el atacante y nos será mas fácil ir restringiéndola.

Nos aseguraremos también de que el registro no es accesible en forma remota, analizaremos pues la clave del registro

```
telnet www.(dominio.com)80
HTTP/1.0 400 Bad Request
Server: Netscape-comrce/1.12

Your browser sent a non-HTTP compliant
message
```

HKLM\SYSTEM\CurrentControlSet\SecurePiperServers\w inreg

y todas las subclaves asociadas a la misma.

Esta clave denota que el registro de Windows esta restringido en forma remota para los administradores.

COMPARTICIÓN DE ARCHIVOS

```
     c:\>>nec   -v   www.(dominio.com)   80
www.(dominio.com) [IP del dominio] 80 (?)
open
```

Hay muchas herramientas para hacer exploraciones de comparticion de archivos, una muy utilizada es legion del grupo Rhino9 la cual, trae tambien un programa de fuerza bruta, la idea es que el programa buscara los recursos compartidos, intentando conectarse a los mismos, sacando nombre de usuario y contraseña por fuerza bruta, la unica manera de evitar esto es utilizar una contraseña lo mas larga posible alfanumerica y con metacaracteres %&() o caracteres ASCII. Tambien es recomendable incluir al final del nombre del recurso compartido el carácter $ para evitar que sea enumerado en una exploracion.

```
     HTTP/1.1   400   Bad   Request
Server: Microsoft-IIS/4.0
     Date: Mond, 06 Apr 2006 10:45:00 GMT
Content-Type:    text/html
Content-Length: 87


<html>
     <head><title>Error</tilte></head>
     <body>El parámetro es incorrecto. </
body>
     </html>
```

Por suerte o por desgracia, muchos sistemas Windows, utilizan una combinación del nombre de usuario y de este desafío para liar (hash o mezclar criptográficamente) la contraseña de usuario remoto, el nombre de usuario se envía en forma de texto, se podría enviar una petición de autenticación hash idéntica, dentro del intervalo de 15 minutos y montar con éxito el sistema de comparición de archivos, tal y como lo describe en sus artículos el grupo L0phtcrack.

Hail

Destripando Decodificadores CFT21XX.

By _SxR_

Bueno, comenzamos un manual detallado sobre cómo destripar el deco para aquellos que tengan curiosidad y para aquellos otros que se han cargado el puente de datos, quieren evitar soldar y desoldar muchas veces… simplemente dar unas ideas, trucos y opiniones.

Espero que lo disfruteis!!!

Comenzamos…

Lo primero es tener un deco, este manual está basado en un CFT2142 pero es aplicable a todos los decos de esta familia.

El primer paso comienza quitando los tornillos de seguridad de la parte inferior del deco con un destornillador especial o, en su defecto, unos alicates de punta fina y paciencia. El destornillador especial lo encontrareis en www.amidata.es , no me acuerdo de la referencia pero ahí está ;-).

Una vez quitados los 4 que hay, quitaremos la tapa de derivación de la parte posterior, lleva dos tornillos de estrella, quitadlos y luego tirad hacia fuera sin miedo, entra a presión y no rompe.

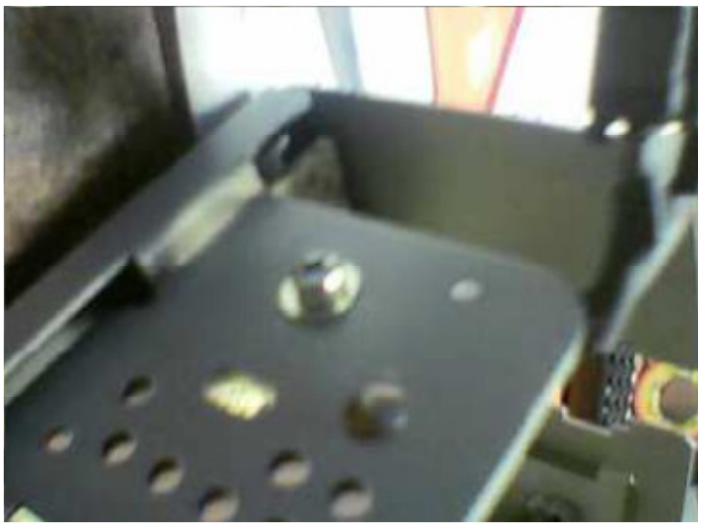
Veremos entonces las 3 tomas reales que tiene el deco, entrada de cable, salida de antena y comunicación PPV (Pay Per View, aunque no se si se escribe así :-P) de la operadora, además veremos el 'clip de seguridad' (más adelante explicaré cómo quitarlo sin romperlo (a que muchos tenéis miedo de eso eh!!!), por ahora lo romperemos, que resulta más sencillo y rápido.

Ahora vamos a quitar la PCB, para eso comenzaremos por quitar las tuercas que fijan las tomas de
cable al deco, simplemente con un alicate o con una llave del mismo calibre que los mismos.

Una vez quitado el clip, simplemente tiraremos hacia arriba de la tapa y voilá, tenemos el deco sin tapa!!! Jejeje

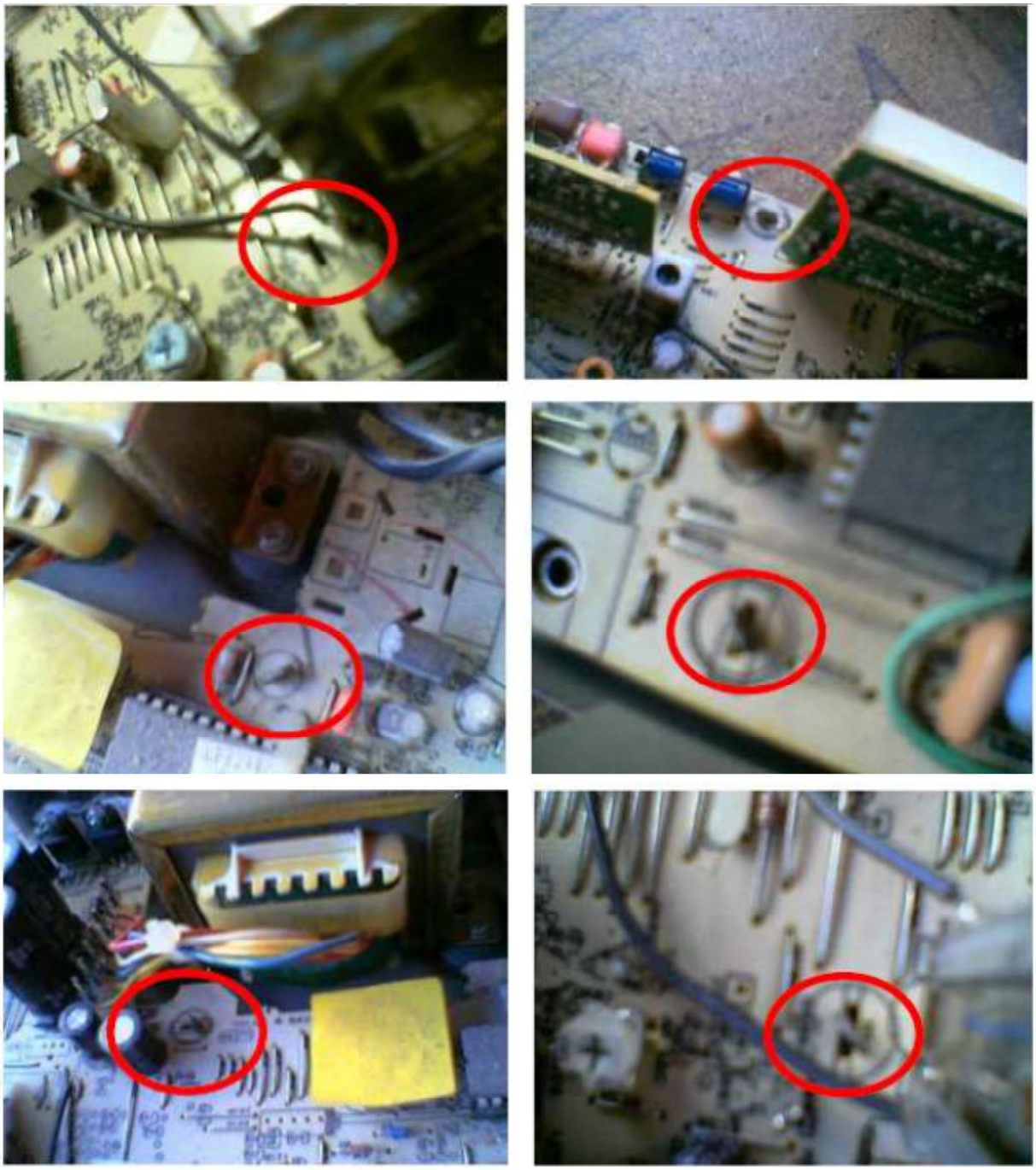
Ahora vamos a quitar la PCB, para eso comenzaremos por quitar las tuercas que fijan las tomas de cable al deco, simplemente con un alicate o con una llave del mismo calibre que los mismos.

Una vez quitadas las tuercas y las arandelas quitaremos los tornillos que fijan la PCB al deco, en principio sólo son dos, y además los que fijan el transformador a la carcasa del deco, 4 tornillos dentados.



Ahora debemos quitar los tornillos que fijan los reguladores y demás integrados a la carcasa para disipar el calor (cuidado que mancha de blanco, pasta térmica, luego no digáis que no avisé), son sólo 3 tornillos de rosca con tuerca.

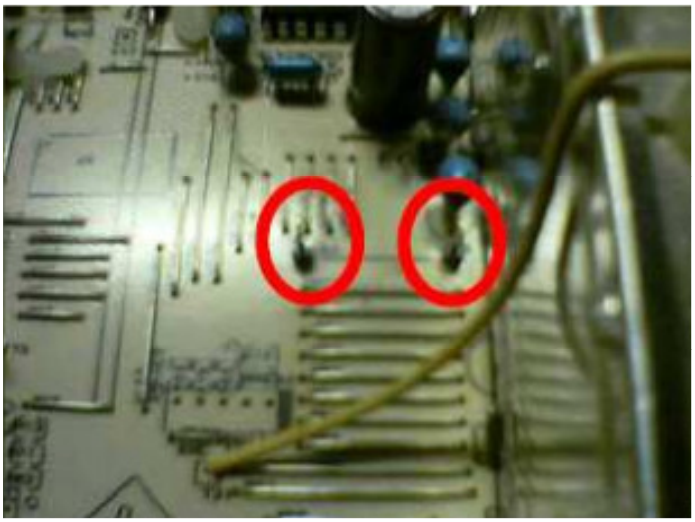
Ahora lo que nos queda por hacer es enderezar todas las muescas de no retorno que hay en la placa y que no dejan que la saquemos de la carcasa, son bastantes (no recuerdo exactamente el número) pero son todas iguales y no son difíciles de encontrar, adjunto algunas imágenes de algunas, para que veáis que aspecto tienen.



Mirad todas las que tenéis, y si la placa sigue sin salir, revisad que no os quede ninguna todavía doblada.

Los círculos rojos os indican dónde están en la foto, sólo hay que enderezarlas para que salgan por el agujerito al tirar y listo. Faltan algunas de las que no tengo foto, de todas formas, si vais quitando la PCB poco a poco y veis que no sale revisad que no se os quede ninguna presilla sin enderezar.

Ahora resta el último paso para poder extraer la PCB, s. En la parte de atrás veremos que tiene, debajo de las tomas de antena, 2 tomas RCA para Video y audio. Éstas están soldadas al PCB y a la carcasa por lo que nos resulta imposible extraer la PCB de un tirón (a no ser que nos la queramos cargar). Para ello usaremos un estañador, con un poco de presión hacia arriba del PCB (podemos tirar ligeramente por las tomas de cable hacia arriba) y aplicando calor a las soldaduras que se ven abajo, las tomas RCA se soltarán del PCB y podemos extraer el mismo.



Ahora simplemente resta tirar con cuidado por la placa hacia arriba y podremos extraer sin problemas el PCB de su carcasa para poder reparar puentes mal soldados, o hacer alguna chapucilla, todo lo que queramos

RECOMENDACIONES

Bueno, voy a comentaros algunos 'trucos' que uso yo para abrir el deco, evitar soldar-desoldar muy a menudo…

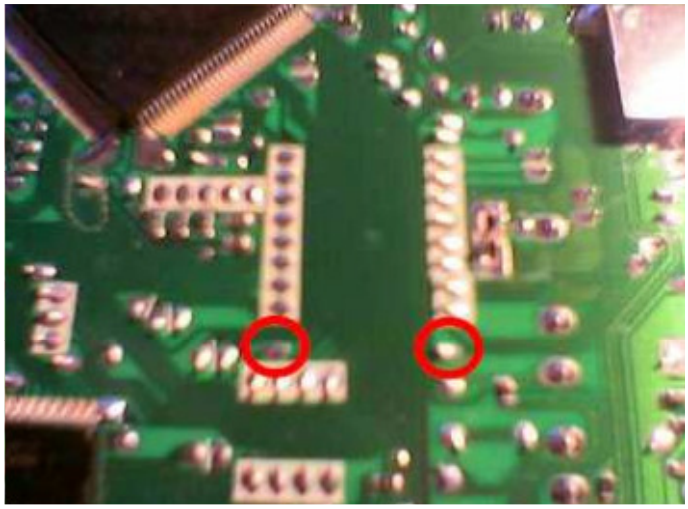
Evitar Soldar-Desoldar:

Para ello usaremos unos pines que se venden en cualquier tienda de electrónica.

Los soldamos una vez en dónde debemos soldar cada patilla del chip y así, simplemente conectando, enrollando… un cable a este pin tendremos colocado el chip y, si por cualquier motivo necesitamos quitarlo del todo, deshacernos de él, etc. podremos quitarlo sin tener que soldar-desoldar nada.

Localización del Puente de datos y reparación:

A más de uno le tiene loco el puente de datos y cómo poder repararlo, para ello Simplemente una vez extraída la placa, y con un pedazo de cable, una patilla de un diodo larga



o cualquier conductor de un hilo similar al que trae de fábrica lo sustituimos extrayendo el que trae con un soldador calentando desde abajo y listo. La localización es sencilla, abajo veis las fotos.

Colocación del Interruptor y desoldado de conexión PPV:

Una vez tenemos la PCB sacada nos resulta muy sencillo quitar, en lugar que envolver con cinta aislante, la conexión PPV de la operadora, con lo que evitaremos tener cacharros innecesarios dentro del deco, para ello lo desoldamos por la parte de abajo del PCB con un estañador y lo extraemos.

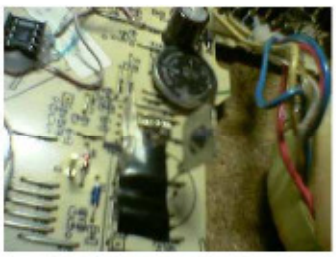
NOTA: ¡OJO! Si usáis esta sugerencia no podréis volver a poner la tapa de derivación por lo que sólo se podrá ver la televisión si tenéis el deco encendido, es decir, a través del deco.

Además de esta manera nos queda un hueco dónde iba esa toma que resulta ideal para colocar el interruptor, segura, y parece hecha a medida

Sustitución de la pila de un deco:

(¡OJO! No se debe quitar la pila, normalmente se destruye el deco, pero si por cualquier cosa os pasa, aquí tenéis la solución)

Bueno, lo he hecho pq, aunque no se debe hacer, a mi me ha pasado. Simplemente sustituiremos la pila por otras de iguales características (tb podeis usar la misma quitándole los enganches que tiene o aprovechándolos, ojo si haceis eso pq no podéis calentar la pila hasta aburriros eh!) y habilitando un ingenio para que haga buen contacto y que no se 'caiga' ni



toque donde no debe.

Unas fotos y luego cada uno que le eche imaginación.


Quitar precintos:

Esta aportación la he sacado de la web del cable, desde aqui un agradecimiento a 75Kw por este excelente trabajo. Simplemente consta de hacer un aparatejo como el que se muestra a continuación, del tamaño justo para que entre por la parte de encima de la entrada del cable que queda al lado del propio precinto y listo. Eso si, hace falta maña, paciencia y un poco de fe.


Ejemplo de cómo es el proceso con un precinto ya quitado.

Pues esto ha sido todo!!! Espero que os halla servido de ayuda este pequeño manual y que os animéis a hacer cosillas y luego compartir los resultados, el
conocimiento es y debe ser libre.

Un saludo a todos!!!

SxR


Este sería el proceso con un precinto en el deco, como es de imaginar, la tapa estaría puesta.

Xgl y Beryl

By M.Reedy

El sistema de ventanas X fue desarrollado a mediados de los años 1980 en el MIT para dotar de una interfaz gráfica a los sistemas Unix. Este protocolo permite la interacción gráfica en red entre un usuario y una o más computadoras haciendo transparente la red para éste.

Veremos cómo el futuro de este tipo de aplicaciones pasa, desde luego, por Linux.

X es el encargado de mostrar la información gráfica y es totalmente independiente del sistema operativo. El sistema de ventanas X funcia en modo cliente-servidor. El servidor provee servicios para acceder a la pantalla, teclado y ratón, mientras que los clientes son la aplicaciones que utilizan estos recursos para interacción con el usuario. De este modo mientras el servidor se ejecuta de manera local, las aplicaciones pueden ejecutarse remotamente desde otras máquinas, proporcionando así el concepto de transparencia de red.

Xgl es una arquitectura basada en el sistema de ventanas X, funcionando de modo de servidor iniciada por David Reveman, en realidad una capa que se encuentra sobre OpenGL vía glitz. Aprovecha las ventajas de las modernas tarjetas gráficas mediante sus controladores OpenGL, que soportan aceleración por hardware de todas las aplicaciones X, OpenGL y XVideo y los efectos gráficos, componiendo un gestor de ventanas, como Compiz o Beryl.

Xgl como otros grandes desarrollos del mundo del software libre, fue desarrollado a través de una lista de correo publica, aunque por mucho tiempo permaneció como un proyecto cerrado.

No fue hasta Enero de este mismo año, cuando el proyecto fue liberado e incluido en freedesktop.org.

A partir de entonces, su popularidad ha ido en aumento, gracias en gran parte a la presentacion de esta arquitectura y sus efectos que realizo la multinacional NOVELL, en la que se mostraban los efectos de escritorios giratorios, efectos translucidos y de traslacion de ventanas...

Las primeras fases de este proyecto fueron algo complejas y oscuras.Los gestores de ventanas desarrollados debian enfrentarse a incompatibilidades de hardware y software. Como solución David Reveman desarrolló Compiz, el primer gestor verdadero de composición de ventanas de un sistema de X Windows. Actualmente se usa una versión mejorada de este denominada Beryl, sobre la que vamos a trabajar en este articulo.

Beryl es el nuevo sustituto a Compiz. Este nuevo manejador de ventanas gana mucho en estabilidad con respecto al anterior pero aun así es un software sujeto a un fuerte proceso de desarrollo.

CARACTERISTICAS DE BERYL :

- Uso del decorador de ventanas ahora se llama Esmeralda
- Usa un archivo plano backend en vez de gconf.
- Plugins amentados y mejorados. .
- Actualizaciones diarias de la base de datos

Antes de nada indicar que para tener XGL+Beryl en nuestra Ubuntu hay que seguir 3 pasos básicos, que son:

1) Activar la aceleración 3D
2) Instalar XGL
3) Instalar Beryl.

En este enlace podemos encontrar la lista de gráficas que soportan o no este sistema;

http://gentoo-wiki.com/HARDWARE_Video_Card_Support_Under_XGL

ELIMINANDO LOS PAQUETES DE COMPIZ

Como ya habéis leído antes, vamos ha trabajar con el segundo de estos populares gestores de ventanas, por lo que deberemos desinstalar si la hubiese habido antes, los paquetes de Compiz.

```
$ sudo apt-get remove --purge compiz com-
piz-gnome cgwd cgwd-themes xserver-xgl
csm
```

Para ello lo podemos hacer de dos formas:

O bien, en una terminal de root (en ocasiones es pesado el

```
# apt-get remove --purge compiz compiz-
gnome cgwd cgwd-themes xserver-xgl csm
```

sudo todo el tiempo):

Habria mas opciones, como ejecutar un sudo -s, para que se quede la password del root, pero es otra historia.

INSTALANDO XGL

Repositorios:

Por defecto, estos paquetes no vienen en los repositorios oficiales de Ubuntu, por lo que debemos actualizar nuestros re-

positorios. Para ello deberemos hacer lo siguiente:

Primero haremos una copia de seguridad de los reposi-

```
$ sudo cp /etc/apt/sources.list /etc/apt/
sources.list_old
```

torios actuales, siempre importante, por si algo fuera mal.

```
$ sudo gedit /etc/apt/sources.list
```

Despues editaremos la lista de repositorios:
Y añadiremos esto al fichero para activar los reposito-

```
## Uncomment the following two lines to
fetch updated software from the network
deb http://archive.ubuntu.com/ubuntu dap-
per main restricted
deb-src http://archive.ubuntu.com/ubuntu
dapper main restricted

## Uncomment the following two lines to
fetch major bug fix updates produced
## after the final release of the distri-
bution.
deb http://archive.ubuntu.com/ubuntu dap-
per-updates main restricted
deb-src http://archive.ubuntu.com/ubuntu
dapper-updates main restricted

## Uncomment the following two lines to
add software from the 'universe'
## repository.
## N.B. software from this repository is
ENTIRELY UNSUPPORTED by the Ubuntu
## team, and may not be under a free li-
cence. Please satisfy yourself as to
## your rights to use the software. Also,
please note that software in
## universe WILL NOT receive any review
or updates from the Ubuntu security
## team.
deb http://archive.ubuntu.com/ubuntu dap-
per universe
deb-src http://archive.ubuntu.com/ubuntu
dapper universe

deb http://security.ubuntu.com/ubuntu
dapper-security main restricted
deb-src http://security.ubuntu.com/ubuntu
dapper-security main restricted
deb http://security.ubuntu.com/ubuntu
dapper-security universe
deb-src http://security.ubuntu.com/ubuntu
dapper-security universe
deb http://archive.ubuntu.com/ubuntu dap-
per multiverse
deb-src http://archive.ubuntu.com/ubuntu
dapper multiverse
```

rios universe y multiverse:

Después, en el final del documento introducimos las siguientes líneas:

```
deb http://www.beerorkid.com/compiz/ dap-
per main
deb http://xgl.compiz.info/ dapper main
deb-src http://xgl.compiz.info/ dapper
main
```

Si ustas usando una plataforma AMD 64bit, necesitarás añadir los repositorios AMD64:

```
deb http://xgl.compiz.info/ dapper main
main-amd64
```

Guardamos y cerramos el archivo.

Ahora, con wget, requerimos las claves publicas para adquirir nuestros programas:

```
$ wget http://www.beerorkid.com/compiz/
quinn.key.asc -O - | sudo apt-key add -
```

Actualizamos lista de paquetes y actualizamos:

```
$ sudo aptitude update && sudo aptitude
upgrade && sudo aptitude dist-upgrade
```

Instalamos el paquete

```
$ sudo apt-get install xserver-xgl
libgl1-mesa xserver-xorg libglitz-glx1
beryl beryl-core beryl-manager beryl-
plugins beryl-plugins-data beryl-settings
emerald emerald-themes
```

Tras realizar estos paso, deberemos configurar nuestro Ubuntu para que este gestor de ventanas este disponible al inicio, igual que podiran estar un KDE, un WindowMaker o cualquier otros gestor de ventanas.

Para que Beryl consiga hacer eso, vamos a hacer un par de pasos:

Primeromos vamos a “Sistema > Preferencias > Sesiones” y en la pestaña Programas al inicio pulsamos Añadir y escribimos

```
beryl-manager
```

Creamos una sesión para XGL

El siguiente paso es este:

Abrimos un terminal y creamos un archivo llamado startxgl.sh

```
$ sudo gedit /usr/bin/startgnomexgl.sh
```

Escribimos en el archivo lo siguiente:

```
Xgl -fullscreen :1 -ac -accel glx:pbuffer
-accel xv:pbuffer & sleep 2 && DISPLAY=:1
# Iniciar Gnome
exec gnome-session
```

Nvidia y ATI (consultar compatibilidades anteriormente descritas)

He leído bastante sobre esto y parece ser que algunas tarjetas Nvidia no funciona correctamente, pero se soluciona cambiando las dos primeras líneas por estas:

```
Xgl -fullscreen :0 -ac -br -accel
glx:pbuffer -accel xv:fbo & sleep 2 &&
DISPLAY=:0 gnome-session
```

Salvamos y cerramos el editor.

Opción en el menú sesiones

Esto deberemos hacerlo independientemente de la tarjeta que posea nuestro equipo.

Añadiremos la opción en el menú de sesiones creado el siguiente archivo:

```
sudo gedit /usr/share/xsessions/gnome-
xgl.desktop
```

Introducimos lo siguiente:

```
[Desktop Entry]
Encoding=UTF-8
Name=gnome-xgl
Exec=/usr/bin/startgnomexgl.sh
Icon=
Type=Application
Salvamos y cerramos el editor.
```

Ahora le tenemos que poner permisos de ejecucion a los dos archivos anteriores:

```
$ sudo chmod 755 /usr/share/xsessions/
gnome-xgl.desktop
$ sudo chmod 755 /usr/bin/
```

O bien, en mi terminal de root:

```
# chmod 755 /usr/share/xsessions/gnome-
xgl.desktop
# chmod 755 /usr/bin/startgnomexgl.sh
```

Ahora debemos reiniciar el entorno gráfico (ctrl + alt + tecla de borrar) .

Despues de esto volvemos a la pantalla del login de Ubuntu. Ahi, deberemos seleccionar como sesion la xgl-gnome, y preferiblemente decirle la primera vez que NO la convierta en predeterminada del sistema. El motivo es obvio. ¿Y si no nos marcha bien ?

Por ultimo, me gustaria exponer varias funciones basicas que vienen por defecto configuradas en Beryl (auqnue veremos una vez nos adentremos en el manejo que es del todo configurable)

- Cambiar ventanas: Alt + Tab
- Ordenar todas las ventanas en el escritorio (tipo Exposé de MacOSX) : F12 activa o desactiva; al pulsar (clic izquierdo) sobre la miniatura de una ventana, la trae al frente (wow que bonito).
- Cambiar entre escritorios: Ctrl + Alt + Flecha izquierda/derecha
- Cambiar entre escritorios de manera feliz: Ctrl + Alt + click izquierdo (arrastrando)
- Cambiar entre escritorios, llevandóte la ventana activa al nuevo escritorio: Ctrl + Shift + Alt + Flecha izquierda/derecha
- Ventana translucida/opaca: Alt + ruedecita del ratón
- Aumentar Zoom una vez: Tecla Super + clic derecho (Super=Windows).
- Aumentar Zoom manualmente: Tecla Super + rueda del ratón hacia arriba
- Disminuir Zoom manualmente: Tecla Super + rueda del ratón hacia abajo
- Mover ventana: Alt+arrastrar clic izquierdo
- Cambiar tamaño ventana (ideal cuando los bordes no lo permiten) : Alt + clic derecho

Problemas con el Teclado

La tecla de Windows suele ser bastante problemática de pillar por Beryl, pero tiene fácil arreglo:

```
xmodmap /usr/share/xmodmap/xmodmap.es
```

Vamos a sistema/preferencias/teclado y en la sección de Opciones de distribución marca en “comportamiento de Alt/Windows” selecciona “Super” está mapeado a las teclas Windows”

Despues, hacemos un mapeo del teclado, para curarnos en salud.

Uso de Beryl

Para el uso de Beryl, lo mas rapido es ejecutar en una terminal y ya lo tenemos activado:

```
$ beryl
```

Bibliografia

http://www.tuxpan.com/fcatrin/es/comments.php?guid=20060311

http://beryl-project.org/

http://www.x.org/

http://xserver.freedesktop.org/

Mr. Reedy

Lecciones Basicas de Virii

By Kirtash

Recientemente han surgido nuevos virus e intrusos que consiguen infectar miles de ordenadores en pocas horas, antes de que los antivirus tengan tiempo de actualizarse contra ellos. Sasser, Netsky, Mydoom o Sobig son buenos ejemplos de estos virus de nueva generación, que utilizan nuevos medios de propagación y se aprovechan de las vulnerabilidades en los sistemas operativos y programas más utilizados. Veremos qué son y qué hacen.

Comenzaremos por nombrar y definir los términos más utilizados del virii para saber un poquillo más y comprender de qué nos hablan muchas veces nuestros propios antivirus y, además poder diferenciarlos de otras amenazas que NO SON VIRUS.

·Bombas lógicas: Son programas o rutinas que permanecen dormidos en nuestro ordenador o sistema hasta un determinado evento del sistema (pulsar una combinación determinada de teclas) o una fecha dada, en ese momento se ponen en funcionamiento, destruyendo, modificando la información o provocando una caída del sistema informático.

·Gusanos/Worms: Son programas que se reproducen dentro del ordenador o máquina de los usuarios hasta producir una saturación total de los recursos de memoria, disco duro… Con lo cuál nuestro sistema se ralentiza hasta colapsarse. Algunos tienen como finalidad recompilar información y enviarla a una máquina donde tiene acceso el difusor del gusano. En el último año muchos de los famosos gusanos de la red establecen puertas traseras que permiten el acceso a terceros no autorizados a la máquina infectada.

·Troyanos: son impostores, realmente no son virus, ya que no se replican a si mismos. Se introducen al sistema y se alojan en la memoria bajo una apariencia totalmente diferente a la de su objetivo final; se presentan como información perdida o inofensivos archivos ejecutables(.EXE)

Al cabo de algún tiempo despiertan y se ejecutan pudiendo tomar el control de la máquina, o abrir una puerta trasera, habilitando la entrada a un intruso. Queda a la espera de las ordenes del intruso, teniendo la capacidad de enviar o recibir archivos, ejecutar programas, enviar información del usuario actual, etc.

Exploit: Código escrito (script) con el fin de aprovechar un error de programación para obtener diversos privilegios. La creación de un exploit es una tarea compleja, no apta para cualquier usuario, ya que para ello -casi siempre- debe utilizarse lenguaje ensamblador. El problema es que, en muchas ocasiones, el autor del exploit lo pone a disposición de otros usuarios maliciosos que, a su vez, lo incorporan a programas escritos con lenguajes de alto nivel. Esos programas pueden ser, obviamente, virus informáticos que gracias a la incorporación del exploit, pueden infectar ordenadores aprovechando la vulnerabilidad objeto del exploit. Este tipos de ataques son muy usados por usuarios denominados Script-kiddies, que no poseen altos conocimientos de programación ni de hacking, para ello los programadores de exploit suelen introducir errores en su código fuente, evitando así que este al alcance de cualquier desaprensivo.

·Virus: estos programas que conocen los usuarios de ordenadores, sus acciones son muy diversas , desde inofensivos mensajes, que aparecen en la pantalla del usuario, a la destrucción total de la información residente en la máquina infectada. Lo que hace a los virus informáticos tan peligrosos es su propia capacidad de auto reproducción y propagación entre ordenadores y red.

Clasificación de virus:

Virus que atacan a programas: el objetivo de dichos virus son los archivos ejecutables y provocan alteraciones en su funcionamiento.

Virus boot: infectan el arranque de la máquina: atacan solamente el sector de arranque de la máquina infectada o a la tabla de particiones.

Combinaciones de los dos métodos anteriores:Las consecuencias son la suma de los dos problemas anteriores.

Virus que atacan a la BIOS: generalmente se usan estos virus para una vez infectada la BIOS escribir desde ella en disco. Con este sistema no sería demasiado complicado formatear el disco duro.

-Ingeniería social: Es una técnica muy utilizada y consiste

en la manipulación de los usuarios para que estos den una información, que normalmente no darían a nadie, normalmente nombres de usuario y contraseña. Así a simple vista parece muy surrealista pero hay mucha gente que cae en esta trampa, cabe decir que una persona que domina el tema de ingeniería social, puede llegar a sacar casi cualquier información y más a gente inexperta.

La ingeniería social inversa es utilizada por el intruso cuando la propia ingeniería social no ha dado los resultados esperados, consiste en informar de algún servicio o tipo de ayuda, inicialmente sin coste, que se brinda a los usuarios para cuando experimenten algún problema, cuado esto sucede, el usuario es el que suele dirigirse al intruso, siendo éste el momento en que se obtiene la información necesaria.

Jokes, hoaxes: No son programas maliciosos pero últimamente su crecimiento en la red ha causado a muchos usuarios pérdidas de información o incluso inutilización de sus sistemas por puro desconocimiento. Son pequeños mensajes o presentaciones en tipo popup que nos alertan de ser, posiblemente, infectados por un nuevo y poderoso virus, recomendando renombrar o borrar determinados ficheros de nuestros sistemas; el usuario inexperto cae en la trampa y, siguiendo el consejo, borra información o inutiliza el ordenar. Hay que vigilar mucho con esto.

> "...las mayores pérdidas financieras son atribuidas a virus, a accesos desautorizados, y al robo de información propietaria" – FBI/CSI Cybercrime Report 2005

SPAM:Los correos electrónicos no deseados son también una amenaza para la seguridad. Entre ellos se pueden incluir los hoax o falsas amenazas de virus y los mensajes en cadena. Últimamente está en auge el fraude conocido como phising,y su evolución, el pharming, con el que se trata de robar datos personales a través de emails que simulan ser enviados por una entidad bancaria.

El correo no deseado incluye numerosos tipos de mensajes, desde la 'basura' más perniciosa (fraudes, phising, etc.) y los mensajes en cadena (leyendas urbanas, pirámides, hoax...) hasta los envíos publicitarios masivos (pornografía, medicamentos, 'gane dinero rápido', etc.) o los de los pequeños comercios que tratan de hacer un buzoneo barato. Tampoco sería un disparate incluir entre el spam muchos mensajes de amigos o colegas, que reenvían a su lista de contactos todas las tonterías que reciben -que incluyen falsas alarmas de virus o archivos adjuntos enormes-.

Clasificación:

Dentro del malware podemos distinguir tres tipos:

·Adware (Advertised Software): software que muestra publicidad. Incluye código que muestra publicidad en ventanas emergentes. A veces funciona junto al 'spyware', pero en este caso no se trata de espiar al usuario: estos parásitos modifican la página de inicio ('secuestradores'), instalan barras en el navegador y lanzan publicidad ('pop-ups') frecuentemente.

·Spyware (Spy Software): describen al software o a cierto tipo de cookies que monitorizan el uso del ordenador (páginas web visitadas, programas utilizados, etc.) y envían esa información a alguna empresa sin consentimiento ni conocimiento del usuario. A los programas que informan sobre los hábitos de navegación de los conoce como 'dataminer'.

·Rootkit: software que un intruso puede utilizar para esconder su infiltración en un sistema y poder acceder a él.

PROBLEMAS ACTUALES MAS COMUNES DE MALWARE

Primero, podemos hablar de los virus. Para detectar y eliminar a cada nuevo virus, los antivirus aplican normalmente un enfoque reactivo: tienen que esperar a que aparezca, infectando los primeros ordenadores, y a continuación actualizarse lo antes posible contra él.

Hasta ahora, el tiempo de respuesta de los antivirus era suficiente para atajar a todos los nuevos virus antes de que alcanzasen niveles significativos de propagación. Por ejemplo, los antivirus de Panda se actualizan de forma diaria y automática a través de Internet.

Sin embargo, recientemente han surgido nuevos virus e intrusos que consiguen infectar miles de ordenadores en pocas horas, antes de que los antivirus tengan tiempo de actualizarse contra ellos. Sasser, Netsky, Mydoom o Sobig son buenos ejemplos de estos virus de nueva generación, que utilizan nuevos medios de propagación y se aprovechan de las vulnerabilidades en los sistemas operativos y programas más utilizados.

Sin embargo, los efectos secundarios de los gusanos son los que han provocado los mayores estragos. Sus mecanismos de propagación aumentan las cargas de tráfico y causan procesamiento adicional en los dispositivos de red (escaneos aleatorios buscando destinos vulnerables, variaciones en los encabezados, o tráfico unicast enviado a direcciones multicast, por ejemplo). Al nivel del núcleo de la red, los efectos agregados de un gusano pueden ser sustanciales.

Un problema muy importante que nos podemos encontrar navegando por la Internet es el phishing (Password Har-

vesting).

El phising: es la capacidad de duplicar una página web para hacer creer al visitante que se encuentra en la página original en lugar de la copiada. Normalmente se utiliza con fines delictivos duplicando páginas web de bancos conocidos y enviando indiscriminadamente correos para que se acceda a esta página a actualizar los datos de acceso al banco.

Aún que parezca una bobada, una página bien duplicada a simple vista es muy difícil de distinguir de la real:

Este es un posible mensaje que te puede llegar de tu banco, ¿Cómo saber si es real?

Solución: NUNCA te fíes de esto, un banco nunca te pedirá una cosa tan privada por e-mail, **NUNCA**.

El spam es la tercera amenaza actual que vamos a trabajar en este articulo.

Hay muchas formas de que una dirección de correo caiga en manos de un spammer. Básicamente, el internauta que pretenda mantener su buzón electrónico libre de basura deberá poner cuidado en qué hace con su dirección de email. La forma más habitual de capturar direcciones de email es emplear un robot que, de la misma forma en que los buscadores analizan los textos para indexar páginas web, localizan las direcciones de correo (basta buscar una @ seguida de un dominio, como hotmail.com). Las direcciones también se consiguen rastreando los foros, grupos de noticias, mensajes en cadena o, de forma abiertamente ilegal, mediante la compraventa de CDs con bases de datos de usuarios y empresas (la oferta de CDs con miles de direcciones de email es correo spam habitual).

Combatir el spam

Por eso es conveniente tomar una serie de precauciones para conservar la dirección lo menos contaminada posible. Para empezar, hay que manejarla con el mismo celo que un número de teléfono, que no daríamos a cualquiera. Y además:

Al registrarse en sitios web o a boletines electrónicos hay que saber qué van a hacer exactamente con los datos personales. En algunos casos, el registro suscribe por defecto a una serie de boletines comerciales o se acepta que el email se ceda a los negocios asociados.

Colocar la dirección de correo electrónico habitual en chats, foros o grupos de discusión casi garantiza que termine en manos extrañas.

Ofrecer el email en una página web tiene sus riesgos (será capturada por los robots de los spammers), por lo que si es necesario darlo se puede tratar de engañar a los buscadores escribiendo la dirección de forma ininteligible para las máquinas (como 'minombre at yahoo.com' en lugar de minombre@yahoo.com). O emplear formularios como medio de contacto.

No reenviar los mensajes en cadena -ni en general reenviar cualquier mensaje de forma indiscriminada-, muchos de los cuales son trampas para capturar direcciones. Algunos son incluso directamente perjudiciales, como las falsas alarmas de virus que apremian a eliminar un archivo presente en la computadora que luego resulta ser vital para el sistema. En especial, jamás abrir o reenviar mensajes con documentos adjuntos provenientes de desconocidos.

A la hora de enviar mensajes a un grupo usuarios conviene colocar las direcciones en la 'copia oculta', pues de lo contrario cedemos el email de terceros sin su consentimiento, y nunca se sabe en las manos en que puede caer.

En caso de recibir spam...

Identificar el spam suele ser sencillo: hay que desconfiar de los remitentes desconocidos y en particular de los asuntos llamativos, los mensajes apremiantes y las ofertas irresistibles.

No se debe abrir ni mucho menos responder porque indica que la cuenta está activa, con lo que sólo se consigue que el spam se multiplique.

Si además de abrirlo pinchamos en alguna imagen o

enlace corremos el riesgo de caer un fraude de phishing , una página web falsa creada para robar datos personales.

> Se puede ayudar a combatir el spam informando al proveedor de correo de la naturaleza del mensaje. Prácticamente todos los correos-web disponen de un botón para indicar que el mensaje "es spam".

La dirección buena y la otra

Para participar en foros, suscribirse a determinados boletines o publicar la dirección en cualquier sitio público es interesante contar con una cuenta de email alternativa; a fin de cuentas los correos-web (los que se consultan a través de una página web) son gratuitos y se pueden crear decenas de direcciones. Así, al menos, podremos mantener la dirección 'buena' libre de spam, pues sólo será del conocimiento de personas de confianza.

Con un poco de ayuda... de los programas

Por mucho empeño que ponga el usuario en mimar su dirección de correo, no está garantizado que el buzón no termine inundado de basura, pues no depende sólo de él: cualquier destinatario 'amigo' puede reenviar el mensaje y éste acabar rebotando hasta un spammer. Por eso, tras la precaución, podemos echar mano de los filtros de los gestores de correo o de programas especializados.

Filtros. La forma más básica de filtrar el spam consiste en bloquear los remitentes de mensajes no deseados, algo que se puede completar con bases de datos públicas de 'sospechosos habituales'. Pero tanto los programas de correo como los correos-web suelen contar con opciones avanzadas que cada usuario puede personalizar, estableciendo reglas para filtrar el spam por el 'asunto', el contenido, etc.

Programas específicos. Existen en el mercado programas que se integran en los gestores de correo para detectar y eliminar el spam. Éstos contienen filtros por defecto (listas negras de remitentes, asuntos sospechosos, palabras clave...) que el usuario puede adaptar a sus necesidades. Los más radicales y efectivos crean una lista de remitentes autorizados por el usuario; el que no esté en la lista recibirá como respuesta un enlace para verificar su identidad y asegurar que no se trata de una máquina 'espameadora' (la inmensa mayoría del spam es enviado a través de programas de bombardeo masivo).

A MODO DE CONCLUSION

Después de ver unos ejemplos y definiciones de las amenazas a que estamos sometidos estaréis pensando en todos los antivirus que os pasen por la cabeza para intentar prevenir esto. Básicamente, la primera cosa que tenemos que hacer para una navegación segura es pensar:

- ·No abrir ningún correo que nos llegue de una dirección sospechosa i/o desconocida.
- ·Navegar siempre que podamos detrás de un firewall, preferiblemente uno que sea totalmente configurable.
- ·Mantenerse al día de las actualizaciones de windows.
- ·Instalar un programa contra software malicioso, como el spybot.
- ·Tener instalado y actualizado un antivirus, a mi parecer el nod32 és muy bueno ya que no consume tantos recursos como otros como el panda.

Si seguimos estos consejos y no nos metemos en paginas potencialmente inseguras, nuestro ordenador estará mucho mas seguro.

Kirtash

CarWishpering

By twilight

Bueno pues por fin he conseguido poner a punto el programa en mi ordenador aunque por desgracia aun no lo he podido probar como dios manda por falta de "victimas" y es que este mismo sábado por la noche me fui a un aparcamiento público, donde aproximadamente cada hora pasan entre 70-100 coches… pero por desgracia había caído una nevada terrible y la gente decidió dejar el coche en casa, así que la confirmación oficial de que funciona aun no puedo darla

En alguna ocasión anterior ya he hablado sobre el proyecto carwishperer, podéis seguirlo en:

http://twilight.blogsome.com/2005/08/

Bueno pues por fin he conseguido poner a punto el programa en mi ordenador aunque por desgracia aun no lo he podido probar como dios manda por falta de "victimas" y es que este mismo sábado por la noche me fui a un aparcamiento publico, donde aproximadamente cada hora pasan entre 70-100 coches… pero por desgracia había caído una nevada terrible y la gente decidió dejar el coche en casa, asi que la confirmación oficial de que funciona aun no puedo darla.

Por otro lado con algunos de los cambios realizados he liberado el parche _ES0.1 en el que aparte del manual traducido se incluyen algunas mejoras y archivos de sonido listos para inyectar (El mejor es el de KITT ;))).

Por si aun no sabéis que es el carwhispering (a partir de ahora cw) os lo cuento a grandes rasgos.

Objetivos.

El objetivo final del proyecto es concienciar a los fabricantes de bluetooth (a partir de ahora bt) sobre los riesgos de usar passwords por defecto para sus dispositivos sin teclado (manos libres).

¿Qué hace el programa cw?

Inyecta un archivo de audio haciéndose pasar por una llamada en el manos libres de un coche y graba lo que se dice en el vehiculo desde ese momento.

¿Cómo lo hace?

El programa cw consta de varios scripts y un binario (cuyo código fuente se incluye en el paquete).

El script para lanzar el programa es el cw_scanner. Este script, que usa el driver bluez para linux, escanea en busca de un dispositivo BT,una vez que lo encuentra comprueba su clase (para saber si es un teléfono, un manos libres, un modem, un ordenador…) y si detecta que se trata de un manos libres mediante bluez se asocia con él, usando un archivo de gestión de PIN propio: cw_pin.pl

cw_pin.pl genera una clave en función del fabricante del dispositivo. Todos los manos libres nokia tienen una clave, los siemens otra, etc… este script averigua el fabricante basándose en el SSID del manos libres, genera la clave correspondiente para ese fabricante y se la devuelve al driver para la asociación.

cw_scanner se asocia con el manos libres y lanza el binario carwhisperer:
carwhisperer envía al manos libres del coche comandos AT haciéndose pasar por una llamada, sube el volumen y la ganancia del altavoz al máximo, inyecta un archivo de audio .raw y recoge todo lo que proviene del altavoz del coche y lo guarda en un archivo .raw que podemos convertir en .wav o escuchar directamente con los drivers adecuados.

Consejos

1)Fabrica una antena de alta direccionalidad: En un post ya comente como hacerlo. Teniendo en cuenta el alcance del BT es muy recomendable.

2)Muy pocos coches tienen un manos libres (aunque cada vez hay mas) así que búscate un sitio donde pasen muchos coches y a poder ser que vayan despacio (para poder no perder la señal durante el proceso de escaneo e inyección), los mejores sitios son: Semáforo concurrido que tarda en ponerse en verde o aparcamiento con alto trafico.

3)Si usas debian puedes instalarte directamente el driver bluez con apt-get pero para compilar carwishperer necesitas las librerias bluez-libs (que yo en mi caso tuve que compilar a mano).

4)Si vas a usar el de la gente de trifinite comprueba el Makefile y el path usado en el script cw_scanner.

5)Ten cuidado con esto porque si bien es una broma muy divertida puedes estar violando la intimidad de las personas que viajan dentro del coche y mucho mas si no les adviertes de tu presencia (enviando un archivo de audio vacio, por ejemplo).

Aspectos a mejorar

1)Mas passwords por defecto para mas marcas.

2)Conseguir oir lo que se dice dentro del coche "in vivo" (esto no debe ser muy difícil, tengo que echarle un ojo)

Crédito.

Toda la información y archivos proceden de:

Project Carwhisperer:

http://trifinite.org/trifinite_stuff_carwhisperer.html

yo sólo me he limitado a publicar las mejoras que hice para mi uso personal, a investigar el funcionamiento, a traducir el manual y a escribir este post porque me parece algo muy divertido para una tarde de sábado ;))))

Twilight

Software Casero en la PS2 & Trucos

By Jouk & smaug

En este número traemos una sesión doble, comenzando por un tutorial sobre cómo hacer correr nuestro software casero (Pelis, programas…) en la PS2 hasta terminar con unos truquillos sobre el Héroes V para que se nos haga más llevadera la partida.

Supongo que la mayoría de personas usaran sus playstation2 para pasarse las horas muertas jugando. Pero nuestra pequeña consola dispone de mas posibilidades que ofrecernos horas de juego. Puede servirnos como reproductor de videos Divx, sacándonos de un apuro en mas de una ocasión, o reproductor de mp3, o incluso se puede usar emuladores para rememorar los viejos tiempos jugando un Mario Kart, al Sonic 3 & Knuckles o un Eternal Champions con un mando, ya que al menos yo, no tengo mando para el pc.

Este tutorial esta dirigido a personas con la consola chipeada. Bien comencemos, lo primero que necesitaremos será un lanzador de elf, los ficheros .elf son como los ejecutables de la play2, hay varios pero el que yo he probado y funciona a la perfección es ULaunchElf , lo podréis encontrar en la siguiente dirección:

http://ps2-scene.org/forums/showthread.php?t=37242
(hace falta registrarse grautitamente).

Y también necesitaremos:

Simple Media System for Playstation 2 (SMS), reproductor multimedia, para ver las pelis de divx y reproducir mp3. (http://home.casema.nl/eugene_plotnikov/)

CDGensPs2 3.0 , generador de imágenes de playstation 2. (http://download.elotrolado.net:81/ps2/cdgenPS23.0.zip)

Snes Station y PGen, emuladores de super nintendo y Megadrive respectivamente (http://people.freenet.de/ps2dev/emulators.html)

De estos solo es fundamental el UlaunchElf y CDGensPS2, ya os daréis cuenta porque. Pero ya que vamos a quemar un cd, lo llenamos con la mayoría de programas que podamos, conforme vaya encontrando mas utilidades las pondré aquí. Vosotros podéis poner las que queráis.

Seguimos, descomprimimos el UlaunchElf y borramos todo excepto BOOT.elf o en su defecto BOOTc.elf. Si es el segundo caso, lo renombramos a BOOT.elf. Luego creamos un fichero llamado System.cnf y ponemos en su interior:

```
B00T2 = cdrom0:\B00T.ELF;1
VER = 1.00
VMODE = NTSC
```

Cambiando NTSC por PAL si lo vamos a reproducir en televisores PAL, yo recomiendo esta opción, ya que en nuestro país se usa este sistema, aunque la mayoría de los televisores ya vienen con la compatibilidad NTSC. Y nota importante, darle a enter justo después de poner el modo, que quede una línea debajo.

El siguiente paso es abrir el CDGensPs2 y meter los archivos en el siguiente orden:

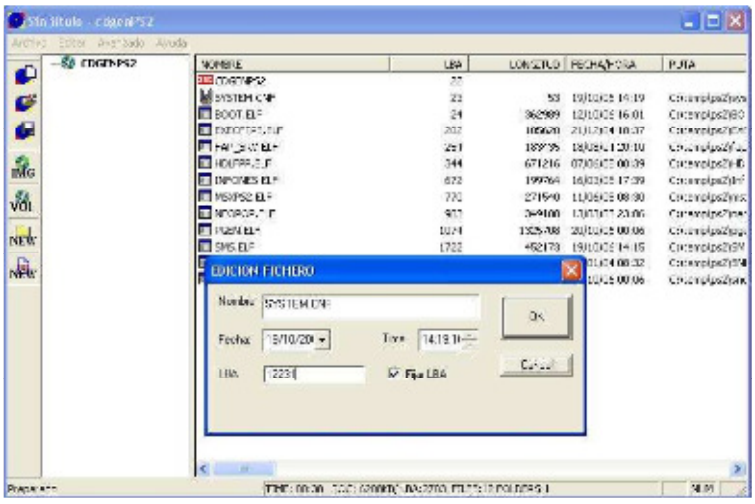
```
1º System.cnf

2º B00T.elf

3º Resto de .elf que vayamos a meter.
```

Para el resto de los elf, hay que tener cuidado con los nombres, han de seguir la normativa DOS , de 8+3 caracteres. Por ejemplo "SMS version 1.8.elf" no seria valido, pero si "SMS.elf".

Una vez añadido todos los ficheros, pulsamos con el botón derecho en System.cnf y le damos a editar. Marcamos la opción de "Fix LBA" y ponemos 12231.



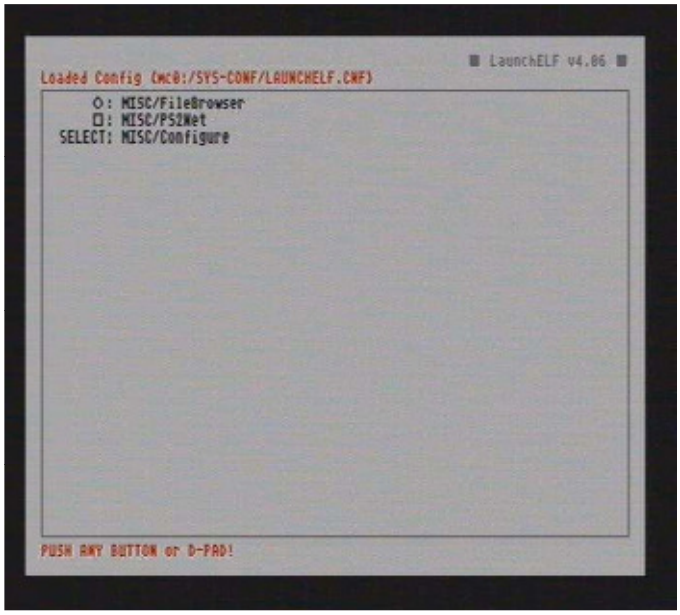
Con esto ya tenemos nuestro disco listo. Ahora solo File>Create Cd y guardamos la imagen.

Por ultimo solo falta quemar la imagen, para ello recomiendo usar el Alcohol 120, y poner el modo Playstation 2. Y con esto tenemos listo nuestro disco para lanzar programas de todo tipo en nuestra amada consola

Conociendo el UlaunchElf

Ahora solo hay que meter el disco recién quemado en la consola y arrancarla.

Si todo se ha hecho correctamente, arrancara automáticamente el UlaunchElf, asi lo primero que veremos será la siguiente pantalla:



Si pulsamos circulo, accederemos al navegador de archivos, donde podremos ver los diferentes dispositivos y elegir de donde cargar los ficheros.

Los dispositivos son los siguientes:

Mc0 y mc1, son las Memory Cards en los puertos del mando 1 y 2 respectivamente.
Hdd0 es el disco duro, si tenemos alguno conectado.
Cdfs corresponde al lector de cd/dvd de la consola.
Mass seria una memoria USB.
Host seria el ordenador si la playstation estuviera puesta en red.
Misc esta es un directorio del propio lanzador, que trae diversas aplicaciones.

Las aplicaciones que podremos encontrar dentro de Misc son las siguientes:

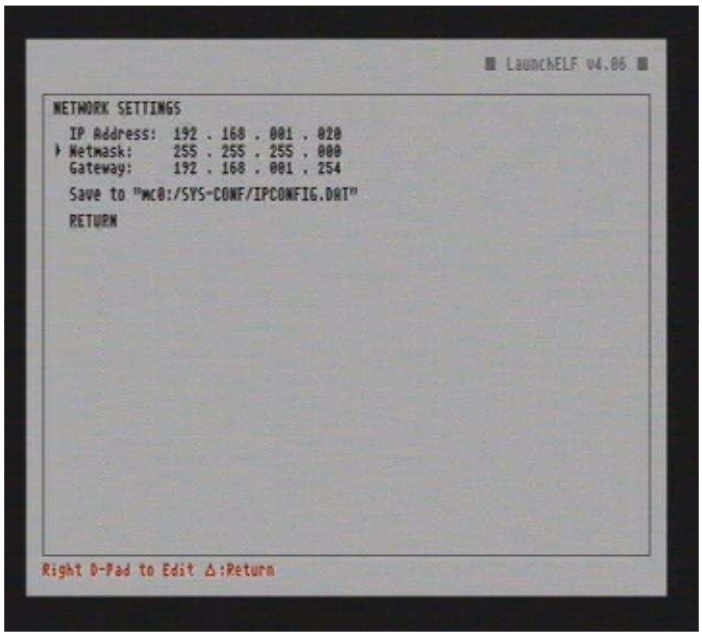
PS2Browser que es el navegador de ficheros, al que accedimos antes mediante el acceso directo.
PS2Disc, carga lo que tenga el disco de la playstation 2, si no has cambiado de disco, volveria a cargar el UlaunchElf
PS2Net, carga el servidor FTP para poder pasar ficheros a través de ftp a los dispositivos e la consola.
PS2PowerOff, realmente necesita una explicación?
HddManager, para gestionar el disco duro si tenemos alguno conectado.
TextEditor, un editor de textos, solo util si tenemos conectado un teclado USB.
JpgViewer, un visor de JPG, no necesita mucha mas explicación.
Configure, la configuración del UlauchElf.
LoadCNF recarga la configuración de UlaunchElf de la ruta que le indicamos.
SetCNF_Path, indicamos la ruta del fichero UlaunchElf.CNF.
ShowFont , nos muestra el mapa de caracteres que usa el programa.

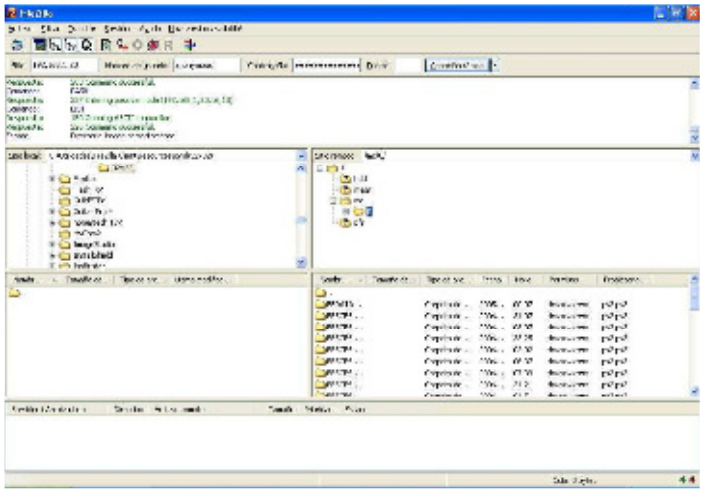
Como podeis ver, no tiene mayor complicación y los programas son totalmente intuitivos así que no merecen mayor explicación.

Conectando y pasando datos a través de la red.

Vamos a configurar la red para poder conectar el servidor ftp, vamos a MISC/Configure y desde aquí, podréis configurar accesos directos para las diferentes aplicaciones, configurar la pantalla y los colores y algunas opciones para el próximo inicio del lanzador, y por ultimo, quizás lo mas importante, la configuración de red. Entramos y configuramos los parámetros de nuestra red, ip de la maquina, mascara de red y puerta de enlace. Una vez hecho esto, guardamos la configuración en la memory card y salimos.

Ahora solo hay que ejecutar Misc/PS2Net, cargara los módulos y ya podremos acceder desde el PC. Ahora nos descargamos FileZilla, ya que con otros clientes FTP no funciona demasiado bien, y abrimos la dirección que le hemos puesto a la playstation:





Ahora ya podemos pasar lo que queramos a la memory card, otros elf y hacer backups de las partidas de nuestro juegos. Si tenemos un disco duro, también podremos pasar películas para verlas con el SMS.

Ahora investiga todo lo que puedes hacer con este programa y aprovecha al máximo tu playstation. En próximas entregas diremos algunos truquillos más para sacar el mayor partido a tu consola.

Smaug

TRUCOS PARA:

Héroes of Might & Magic V

En esta sección y en este número os vamos a presentar los secretos del Héroes of Might & Magic V, si alguno de vosotros se ha quedado atascado en alguna misión o simplemente quiere aniquilar a sus enemigos mas rápidamente en las escaramuzas aquí tiene los siguientes trucos:

Para introducir los siguientes trucos debes de editar un archivo del juego por lo que lo recomendable es crear una copia de dicho archivo antes de editarlo.

Abre el archivo autoexec.cfg en el directorio /gamedir/profiles/ con el editor de textos y añade la siguiente línea al final del documento:

setvar dev_console_password = schwinge-des-todes

Ahora, mientras juegas pulsa ~ para sacar la ventana de consola e introduce cualquiera de los siguientes códigos y pulsa Enter para activarlo:

add_exp [#] :Añade experiencia al héroe seleccionado (donde # es la cantidad establecida)

add_skill [“nombre de la habilidad”] :Añade puntos a dicha habilidad

show_player_money [“numero de jugador”] :Mostrar los recursos de dicho jugador

show_hero_mp :Eliminar los puntos de movimiento del héroe seleccionado

add_army town [“número de la ciudad”] [0 o 1] :Añadir criaturas de la ciudad escogida al héroe seleccionado

add_money [#] :Añadir recursos (donde # indica la cantidad)

add_all_spells :Conseguir todos los hechizos para el héroe seleccionado

clear_money :Hacer que todos los recursos sean 0

add_gold [#] :Conseguir oro (donde # indica dicha cantidad)

set_hero_luck_morale [“# suerte”] [“# moral”] :Modificar la moral y suerte del héroe seleccionado (donde # la cantidad de dichos atributos)

Bueno esto es todo en cuanto a la sección de trucos de este número os esperamos con más sorpresas en el siguiente número de la revista, esperamos que les ayuden estos trucos.

Jouk

Coordinadores del proyecto:

Clarinetista
SxR_
CrAcKzMe

Artículos de este número :

Sn@ke
HYStd
j8k6f4v9j
Hail
SxR
M.Reedy
Kirtash
Twilight
Jouk
Smaug