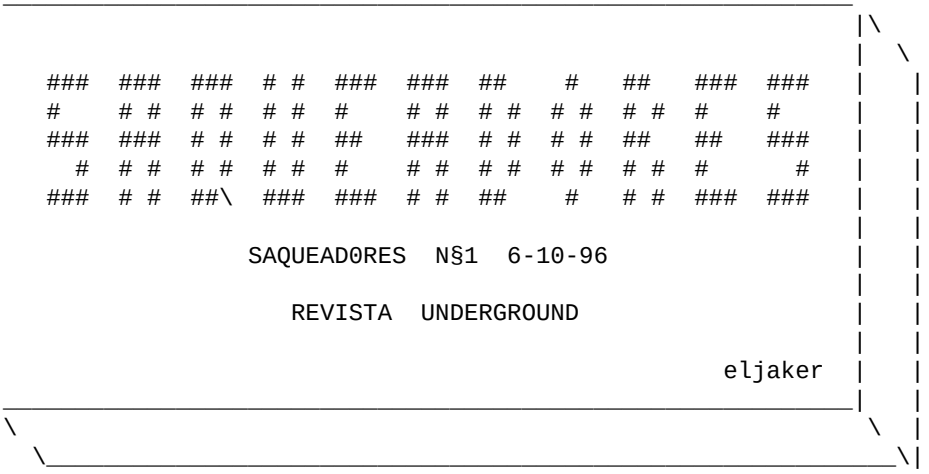

Saqueadores: Revista dedicada al hackin, crackin, virus y demas asuntos
para mentes abiertas y libres.

Editor: eljaker

Colaboradores: Por ahora no hay colaboradores, si tienes algo interesante que
contar sobre estos temas y te gustaria colaborar, contacta con nosotros en bbs
club...

0. CONTENIDOS:

EOF

1. PRESENTACION:

Hola lector, bienvenido a esta recien nacida revista underground, que tratara sobre temas como el hackin, crackin, virus y cualquier tema que no pueda ser tratado libremente en nuestra sociedad de "la libertad de expresion" debido a que la censura aun sigue trabajando.

No pretendemos extender el crimen ni incitar a la ilegalidad, simplemente queremos que todo el mundo pueda descubrir estas formas alternativas de conocimiento.

Espero que os guste...

eljaker

EOF

2. Como pescar claves en el irc I

Este capitulo va a ser el primero de una larga serie de articulos que van a tratar de como conseguir password en el irc.

Hacer que otras personas te "confiesen" su password, es una de las ramas mas importentes del hacking. Este estilo de conseguir claves, se llama ingenieria social, y se puede hacer en persona, por telefono, por escrito y como no, en el irc, que es el lugar de accion de estas lecciones.

La ingenieria social en el irc, es muy ventajosa con respecto a las otras:
-No te pueden pillar, ni conseguir pistas sobre ti. En persona te ven, por telefono conocen tu voz, por correo ven tu letra, pero por irc, no tienen nada contra ti.
-No te ven, ni te oyen, o sea, que te puedes hacer pasar por una persona totalemente opuesta de lo que eres sin que se enteren. Cosa que ni en persona ni por telefono se puede hacer.
-Puedes soltar la mentira mas gorda, sin que se enteren, ya que no perciben tu reaccion al mentir y no necesitas ser un buen actor para disimular tus sentimientos.
-No es necesario conocer al "sujeto", auqnue si es conveniente saber algo de el.

Yo no suelo practicar mucho la ingenieria social, para mi propositos, pero las pocas veces que lo he hecho han sido por irc.

Ademas de en el irc, estas tecnicas se pueden usar, para los chats de bbs, para el correo electronico, etc...

En otras entregas de esta serie, tratare sistemas mas concretos de robo de passwords en el irc, pero por ahora solo voy a dar unas tecnicas generales que sirven para cualquier situacion.

A.) Donde actuar - Si controlas en ingles, puedes intentarlo en un canal de habla en ingles, pero para la ingenieria social hay que hacer un uso extensivo del lenguaje, a si que, si no controlas el ingles dedicate a canales en espa¤ol.
- Procura empezar por canales donde se reunan los novatos y la gente que no controle mucho, de esto, como pueden ser #newbies, #help, #f.c.barcelona, etc... :-)
- Luego con el tiempo puedes ir intentandolo en canales, donde la gente sepa mas de informatica, aunque tienes que andar con cuidado, porque seran mas cuidadosos y desconfiados a la hora de dar la clave.
- Tambien es facil intentarlo en canales de "vacilones" ya que por su propia naturaleza, revelaran un password (aunque sea el suyo) para no quedar mal. Lo malo es que su informacion sera muy poco fiable.
- En los chats de algunas bbs, donde llama gente desesperada por algo. No quiero dar mas detalles sobre esto, porque un amigo mio es sysop de una bbs de ese estilo, y no quiero llenarle la bbs de ladrones de passwords.

B.) Actuar con sicologia - Para hacer revelar a alguien algo que no quiere decir hay que tener unos dotes grandes de conviccion o conocer la sicologia de la persona con la que se trata. A si que si quereis ser unos buenos timadores de irc, os conviene estudiar sicologia y practicar bastante.
- Ante una chica, o novato, se debe actuar con seguridad y procurando aparentar un cargo importante dentro del mundo de la informatica. Tienes que hacerle creer que sabes de lo que hablas, y que todo lo que digas es correcto y que debe obedecerte.
- Muy util para el caso anterior, es hacerse pasar por el operador del irc o de la bbs. En el irc, habria que ponerse nombres como, daemon, root, sysop, master, o cosas por el estilo. En la bbs, si el sysop se hace llamar

ropero por ejemplo, pues te pones de apodo roperro, a ver si cuela, o nombres como, sysop, jefe, etc...
- Al tratar con "chulillos" que se creen que lo saben todo, habria que cambiar de estrategia, y hacerle creer que eres un novato, que no tiene ni idea, y convencerle de que si te da un password no vas a saber que hacer con el. de esta manera se confiara y empezara a hablar y a hacerse el listo, hasta que suelte algo importante.

C.) Tecnicas generales - Ser convincente, no contradecirse, ni parecer dudoso. Hablar con seguridad, como si controlaseis el tema.
- Hacerle hablar de algo que le guste, para que se confie, y luego sacarle las cosas mas facilemente. Por ejemplo, si esta en el canal de linux, le haces preguntas para que se enrolle, y luego cuando este despistado le sueltas, la gorda.
- Prometerle cosas a cambio, como otros password (inventados, claro) quedar con el otro dia, pasarle algun fichero, etc...
- Que piense, que lo que os da no os va a servir de nada, o que lo vais a usar pocas veces.
- No intentarlo con personas que conozcan esta tecnicas. No te pases de listo y lo intentes con gente que sabe mas que tu, por que, puedes acabar siendo tu, el que confiese el password o termines baneado del canal.

Bueno, en el proximo numero de esta serie, empezaremos ya con casos concretos, y tecnicas especificas para distintas situaciones. Mientras llega la proxima entrega ir practicando, y si descubris alguna tecnica milagrosa hacermelo saber.

eljaker

EOF

3. Elegir un buen debugger I

Todo el que haya intenetado, empezar en el cracking, lo primero que se habra preguntado es con que debugger empezar. No es que haya muchos debuggers en el mercado, pero son programas tan complejos y cripticos, que es dificil decidirse entre uno de ellos.

En este caso, lo ideal seria elegir un debugger sencillo de usar y no se necesitarian muchas capacidades. Luego, cuando ya fueseis controlando interesaria pasar a un debugger mas potente.

Ahora voy a describir brevemente los debuggers mas comunes y luego, en siguientes entregas ya trataremos cosas mas generales:

La mayoria de los debuggers que voy a comentar estan disponibles en internet, aunque muchos de ellos sean software comercial. Yo recomendaria, si se dispusiese de dinero, el comprarlos legalemente, ya que es la unica manera de conseguir los manuales, muy utiles para programas como estos muy dificles de usar y con muchas posibilidades de uso. Si no tuvieseis dinero, no os preocupeis, os va a resultar muy facil encontrarlos en la red, pero tendreis el problema de aprender a usarlos sin manual.

#El debug de dos:
->Ventajas
+Esta en cualquier ordenador que funcione con ms-dos
+Aunque parezca peque¤o es muy potente, aunque no lo suficiente, como para ser un buen debugger.
+Ocupa muy poca memoria, y en casos extremos puede ser el unico debugger que funcione.
+hay mucha informacion sobre su uso.
->Inconvenientes
-Aunque sea bueno para aprender a usar un debugger por ser muy limitado y peque¤o, es muy poco intuitivo.
-Visualmente es horrible, ya que el debugger no posee pantalla propia y puede tener problemas con programas graficos y la informacion no esta a la vista.
-Es muy lento de usar.
-No evita los codigos anti-debugging.
->Conclusiones
Puedes echarle un vistazo antes de empezar con otros mas completos y probar a debuggear algo simple para ver como funciona esto del debugging, pero ni mucho menos es un debugger de uso diario. Tambien puede ser util en casos extremos, como en ordenadores ajenos, donde no haya ningun debugger o en ordenadores antiguos con poca memoria.

#Borland turbo debugger
->Ventajas
+Muy sencillo de usar, permite el uso de raton y dispone de menus despegables.
+Su uso a base de ventanas es muy comodo y permite tener mucha informacion a la vista.
+Comodo y rapido de usar.
->Inconvenientes
-Es poco potente, carece de muchas caracteristicas basicas en un debugger.
-Escasa proteccion ante codigos anti-debugging.
-Ocupa mucha memoria.
-Poca seguridad ante los cuelgues.
-Hay poca informacion sobre su uso.
->Conclusiones
Es el debugger ideal para empezar. Es muy comodo y facil de usar, a si que puede ser una herramienta de uso permanente. Aunque a la larga se acaba

quedando corto en prestaciones y no es apto para trabajos complicados.

#Soft-ice para dos
->Ventajas
+Probablemente el mas potenete del mercado, para dos.
+Infinitas posibilidades.
+Comodo de usar.
+Seguro ante cuelgues y ante codigos anti-debugging.
+Existen versiones de este debugger para las windows 3.1 y 95, a si que si te acostumbras a el te sera facil, aprender a usar su hermanos mayores.
+No ocupa memoria base.
+Muchos cursos de cracking lo usan como herramienta basica, y su manual esta disponible en internet (y en bbs club).
->Inconvenientes
-Debido a sus grandes posibilidades, al principio puede resultar dificil de usar.
-Se instala al arrancar y no permite el uso de programas controladores del modo extendido del 386, como el himem.sys, lo que hace que no pueda debuggear algunos programas.
-No permite debuggear programas en modo protegido, auqnue sus hermanos mayores si.
->Conclusiones
Sin duda el mejor debugger del mercado. Es la herramiente de cracker profesional. Si quieres trabajar en serio, este debugger es inprescindible. Ademas la mayoria de tutoriales de cracking, asumen que usas este debugger, a si que si dispones de el, es el mas apropiado para seguir estos cursos.

#Game tools
->Ventajas
+Tiene propiedades que otros debuggers no tienen.
+Es facil de usar.
+Algunas veces facilita mucho el trabajo, como en el caso de contadores o de datos variables.
+Ademas de crackear, te permite hacer cheats para los juegos.
+Es seguro y potente.
->Incnvenientes
-No es un debugger, propiamente dicho, y carece de muchas opciones de los verdaderos debuggers.
-Es incomodo de usar.
-Poca documentacion.
->Conclusiones
Puede ser una herramineta util para los aficionados a los juegos, pero no es muy bueno para crackear en serio. Aunque hay una escuela de crackers, (muy buenos algunos de ellos) que lo usan como herramienta principal, y lo prefieren al soft-ice (?). Como dato interesante, quiero decir que hay un curso de su uso en castellano!! a si que no os resultara dificil aprender a usarlo.

#Soft-ice para windows
->Ventajas
+Es uno de los pocos debuggers para este sistema
+Posee la mayoria de las posibilidades de la version para dos
+Permite el debugging (aunque con problemas) de progrmas dos, en modo protegido.
->Inconvenientes
+Poca documentacion.
+Las propias del debugging en un sistema operativo tan precario como windows.
->Conclusiones
El complemento ideal para el soft-ice del dos. Igual, o mas potente que su hermano menor, y con control casi total sobre windows (algo que ni los de

microsoft han conseguido :-)). Estoy comentando las posibilidades en general de las versiones de soft-ice para los 2 windows, pero queria decir que la version para w95 es mas potente y segura que la de su hermano de 16 bits para windows 3.1. Como a la larga, los programas bajo dos iran desapareciendo, el entorno windows, se situara como estandar, a si que crackear en windows va a ser imprescindible en poco tiempo.

#Otros debuggers
->Conclusiones
Hay otros debuggers mas raros y dificiles de encontrar, como son los que vienen con los entornos de programacion de borland o microsoft, que son mas limitados, pero tambien pueden ser utiles. Tambien hay otros como el avputil, muy bueno para debuggear virus, otros shareware, etc.. Todos ellos serviran, para nuestros propositos, algunos mejor, otros peor, decide el que mas te guste, aprende a usarlo bien y

.
 .
  .
   .
    .
     .
      .
       .

a crackear!!

En la proxima entrega de este capitulo, explicare las caracteristicas generales de un buen debugger, y un par de tecnicas muy utiles, para su uso.

eljaker

EOF

4. Despedida:

Bueno aqui acaba la primera entrega de este e-zine, espero que os haya gustado y que os animeis a colaborar.

hasta, la proxima entrega, os saluda.

eljaker

$$ Los otros numeros de esta revista pueden encontrarse en:

- BBS CLUB MURCIA 968-201819 y 968-201262

- y en internet en http://www.geocities.com/SiliconValley/park/7574/

$$ Para contactar con nosotros, pasate por el area de hackin-crackin de bbs club o por el canal #warezspain (undernet) del irc, y pregunta por eljaker.

talavista

el editor

EOF