Ingeniería Social

Webinar Gratuito

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Jueves 8 de Enero del 2015

Presentación

Alonso Eduardo Caballero Quezada es Brainbench Certified Network Security (Master), Computer Forensics (U.S.) & Linux Administration (General), IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling y Miembro de Open Web Application Security Project (OWASP).

Ha sido Instructor en el OWASP LATAM Tour Lima, Perú del año 2014, y Conferencista en PERUHACK 2014. Cuenta con más de once años de experiencia en el área y desde hace siete años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético & Informática Forense. Perteneció por muchos años al grupo internacional de Seguridad RareGaZz e integra actualmente el Grupo Peruano de Seguridad PeruSEC. Ha dictado cursos en Perú y Ecuador, presentándose también constantemente en exposiciones enfocadas a, Hacking Ético, Informática Forense, GNU/Linux y Software Libre.

@Alonso_ReYDeS

pe.linkedin.com/in/alonsocaballeroquezada/

Ingeniería Social

La Ingeniería Social es una de las más sencillas técnicas utilizadas para ganar acceso hacia una organización o computadora personal. Esto puede ser más difícil sino se hace una buena labor sobre el objetivo y las víctimas.

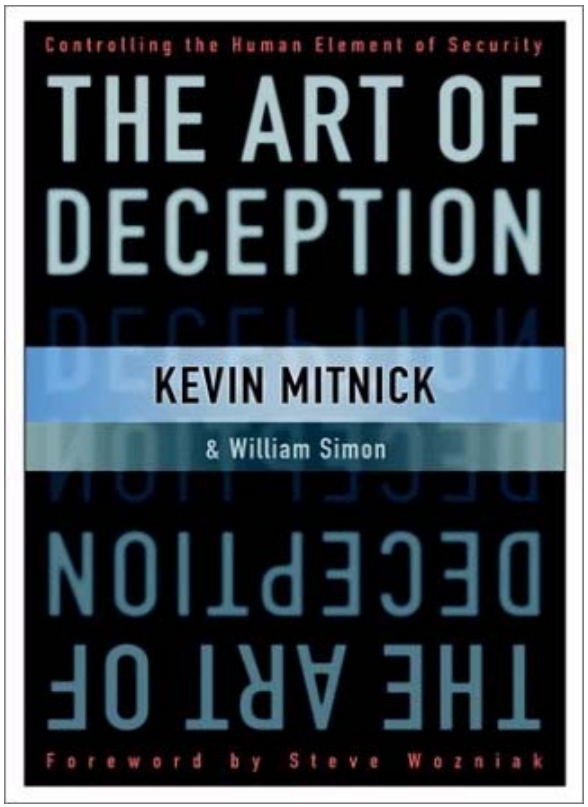
Un buen Ingeniero Social debe investir tiempo elaborando un pretexto denominado el “Vector de Ataque”, para luego formular un fantasía creíble con todos los detalles.

Este ataque debe ser lo suficientemente creíble para no tener percepciones negativas o crearlos en los receptores finales, y de esta manera no activar alarmas durante el proceso de hacer realidad la fantasía.

* http://en.wikipedia.org/wiki/Social_engineering_%28security%29

Ingeniería Social (Cont.)

La Ingeniería Social utiliza la influencia y persuasión para engañar a la gente convenciéndola o manipulándola para creer en alguien el cual no es el Ingeniero Social. Como resultado, el Ingeniero Social es capaz de aprovecharse de la gente para obtener información con o sin el uso de la tecnología.



* https://www.mitnicksecurity.com/

Human Security Testing - OSSTMM

Human Security (HUMSEC) es una subsección de PHYSSEC e incluye Psychological Operations (PSYOPS). Evaluar este canal requiere interacción con personas en posiciones vigilantes de activos.

Este canal abarca a las personas involucradas, principalmente al personal operativo dentro del alcance objetivo o framework. Mientras algunas servicios consideran esto simplemente como “Ingeniería Social”, el objetivo del verdadero cumplimiento de la prueba de seguridad en este canal es probar la concientización de seguridad del personal y medir la brecha con la norma estándar de seguridad delineada en la política de la empresa, regulaciones de la industria o legislación regional.

El analista requerirá tener diversas herramientas y métodos para completar algunas tareas y asegurar la no sospecha entre el personal. De esta manera no se invalidarán las pruebas debido a un descubrimiento temprano aumento de paranoia. También puede ser pertinente limitar las pruebas a sujetos de un departamento u otro limite.

* http://www.isecom.org/research/osstmm.html

Verificación de Confianza - HUMSEC - OSSTMM

Tergiversación: Utiliza la tergiversación como un miembro de soporte “interno” o personal de entrega desde dentro del alcance sin credenciales.

Fraude: Utiliza una representación fraudulenta como un miembro de la gerencia u otro personal clave.

Desorientación: Utiliza la tergiversación como un miembro de soporte o personal de entrega desde fuera del alcance.

Phishing: Accede a información controlada personal o activos físicos a través todos los canales descubiertos para el personal dentro del alcance, con el uso de una pasarela fraudulenta donde el personal es consultado para proporcionar credenciales.

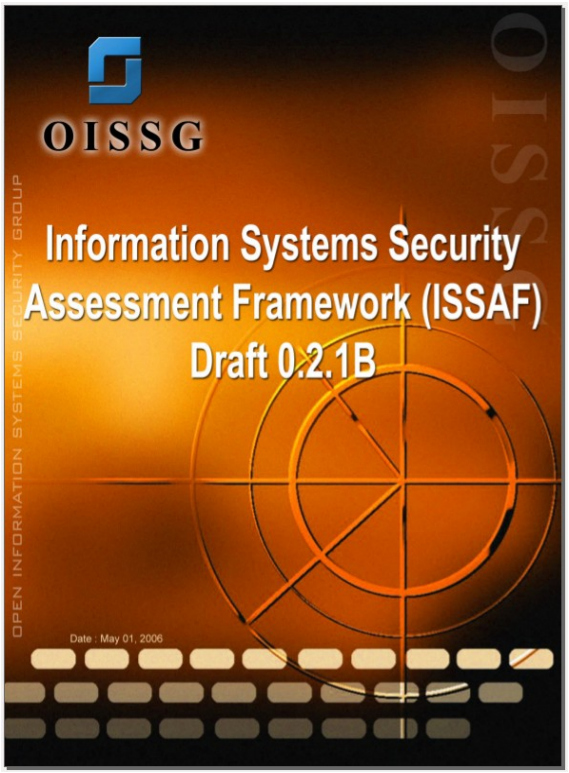
Abuso de Recursos: Toma activos fuera del alcance de una fuente confiable y conocida o través del propio alcance hacia otro personal sin credenciales establecidas o requeridas.

In Terrorem: Incitar al temor, revuelta, violencia o caos, mediante la desorganización del personal usando rumor y otros abusos psicológicos.

Metodología - ISSAF

Para los Empleados:

- Manejar información sensible
- Almacenamiento de contraseña
- Surfear sobre el hombro
- Revelar Contraseñas por teléfono
- Acceso físico a las estaciones de trabajo



Para Soporte:

- Hacerse pasar como un usuario
- Hacerse pasar como personal de vigilancia

Bucear en la basura.
Ingeniería social inversa

OISSG
Open Information Systems Security Group

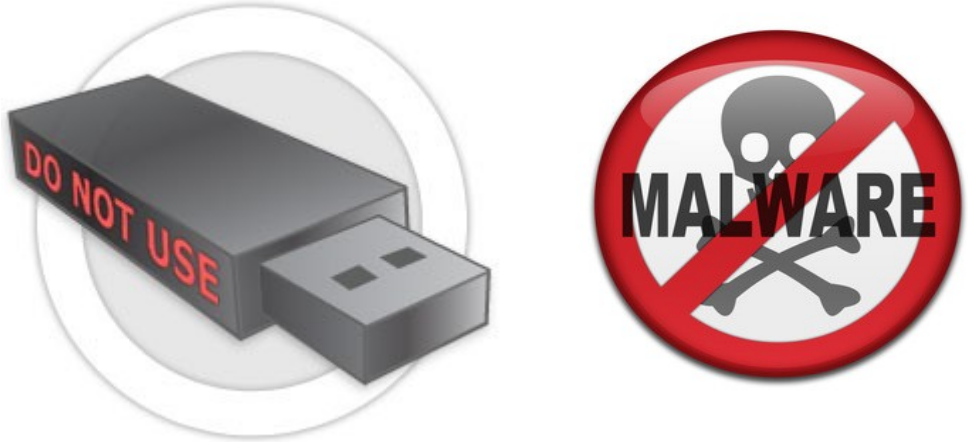
* https://www.facebook.com/OISSG

Cebo

Este ataque utiliza medios de computadoras para inducir a la victima en la instalación de malware. Como dejar un CD o USB en un lugar público. Esta ataque se aprovecha de la curiosidad humana natural cuando se presenta lo desconocido.

Caso: El empleado de una organización mantiene el medio de cómputo abandonado, para luego utilizarlo en el sistema de la organización, como su computadora.

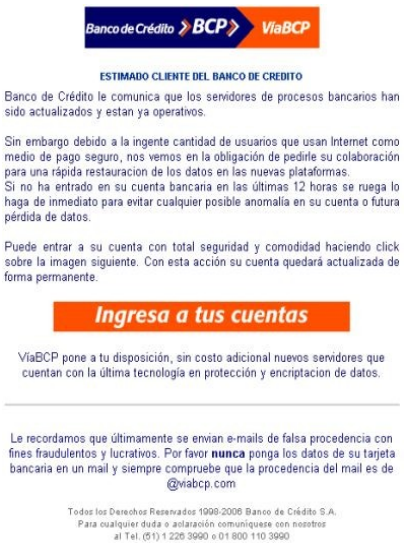
Este medio contendrá malware, el cual puede crear una puerta trasera en la computadora de la victima. Este malware intentará conectarse hacia el sistema del atacante proporcionando acceso dentro de la red corporativa.



Phishing

Estos ataques frecuentemente se asocian a correos electrónicos falsificados, los cuales solicitan a un usuario conectarse hacia un sitio web ilegítimo. Estos sitios simulan ser la página de un banco, una red social, correo electrónico, etc. Este sitio web falso tratará de ser lo más idéntico al sitio real, con la esperanza de hacer creer a la victima de su legitimidad, para poder capturar información sensible como números de cuenta, contraseñas, correos, códigos de seguridad, entre otra información.

Estos ataques también se realizan mediante un teléfono. Donde la víctima recibe un SMS o llamada directa, solicitándole información sensible, permitiendo al atacante suplantar a la victima.



Pretexto

Es un método de inventar un escenario para convencer a las victimas en divulgar información no debida. Es utilizada frecuentemente contra organizaciones reteniendo datos del cliente, como bancos, compañías de tarjetas de crédito, etc. Se solicitará información desde la organización suplantando a un cliente usualmente desde un teléfono.

Se aprovecha de la debilidad en las técnicas de identificación utilizadas en las transacciones por voz. Pues es imposible una identificación física. Algunas veces se solicita información persona para verificación, como fecha de nacimiento, nombres y apellidos, etc. Pero esta información podría ser obtenida a través de sitios webs o búsquedas en la basura.

Social-Engineer Toolkit

Social-Engineer Toolkit es una herramienta open source orientada a las Pruebas de Penetración alrededor de la Ingeniería Social. SET es el estándar para Pruebas de Penetración con Ingeniería Social y es apoyada fuertemente dentro de la comunidad de seguridad.

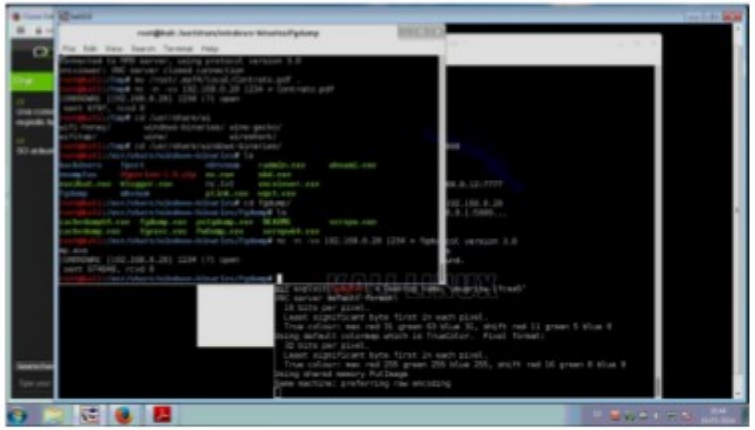
SET permite automatizar técnicas complejas y hacer los ataques creíbles. Las capacidades de SET pueden ser explotadas si la persona utilizándolo tiene los conocimientos para hacerlo. El comprender como personalizar y utilizar todas las capacidades de SET permitirá alcanzar altas probabilidades de éxito en ataques de Ingeniería Social.

* https://www.trustedsec.com/social-engineer-toolkit/

Curso Virtual de Hacking Ético

Curso Virtual de Hacking Ético

2015



Grupo Sábado:
10, 17, 24 y 31 de Enero del 2015
De 3:30pm a 7:15pm (UTC -05:00)

Grupo Domingo:
11, 18, 25 de Enero y 1 de Febrero del 2015
De 9:00am a 12:45pm (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:

Más Información: http://www.reydes.com/d/?q=Curso_de_Hacking_Etico
E-mail: **caballero.alonso@gmail.com** / Sitio Web: http://www.reydes.com

Cursos Virtuales

Todos los Cursos Virtuales dictados están disponibles en Video.

Curso Virtual de Hacking Ético

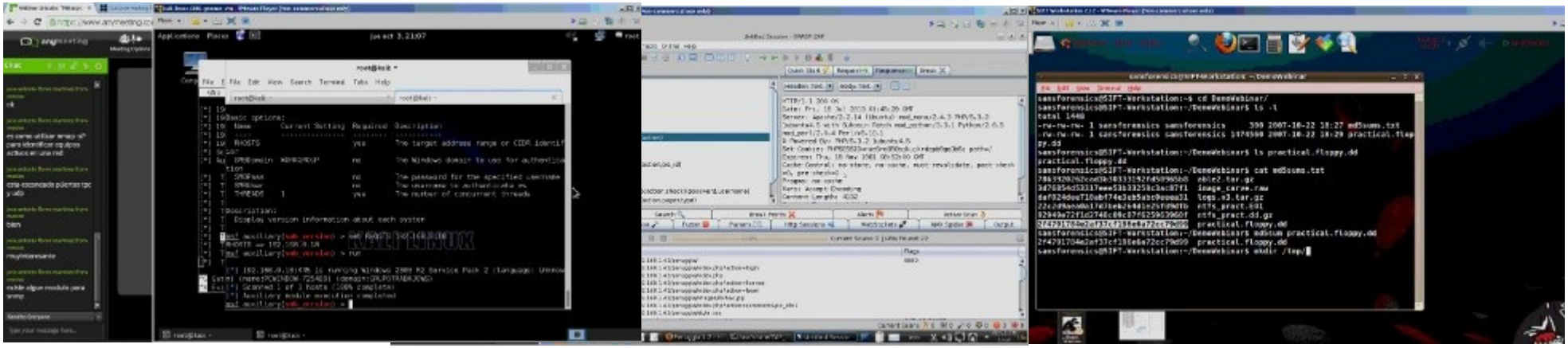
http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web

http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

Curso Virtual de Informática Forense

http://www.reydes.com/d/?q=Curso_de_Informatica_Forense



Más Contenidos

Videos de 22 Webinars Gratuitos sobre Hacking Ético, Hacking Aplicaciones Web e Informática Forense.

http://www.reydes.com/d/?q=videos

Diapositivas utilizadas en los Webinars Gratuitos.

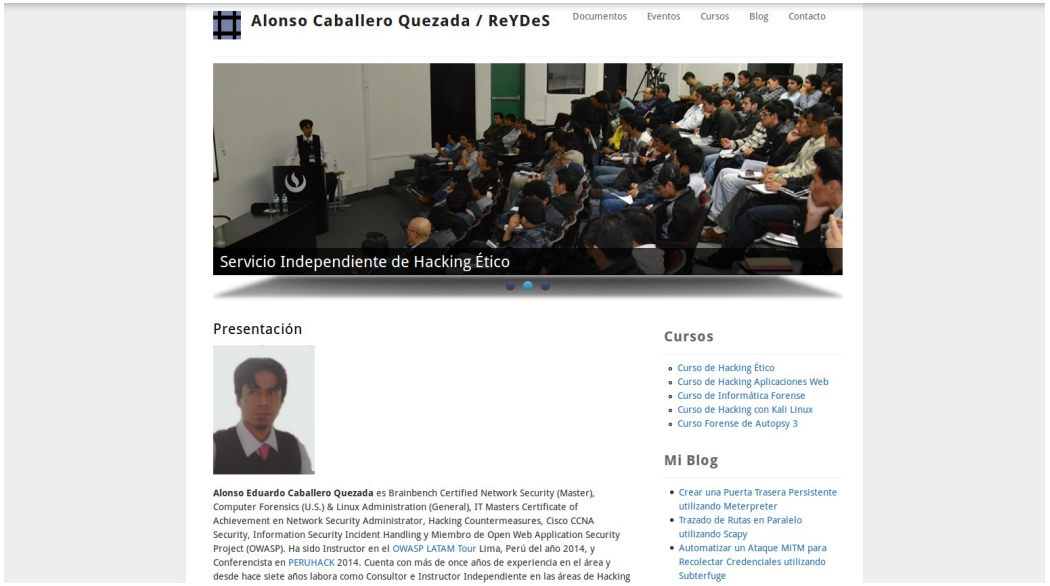
http://www.reydes.com/d/?q=node/3

Artículos y documentos publicados

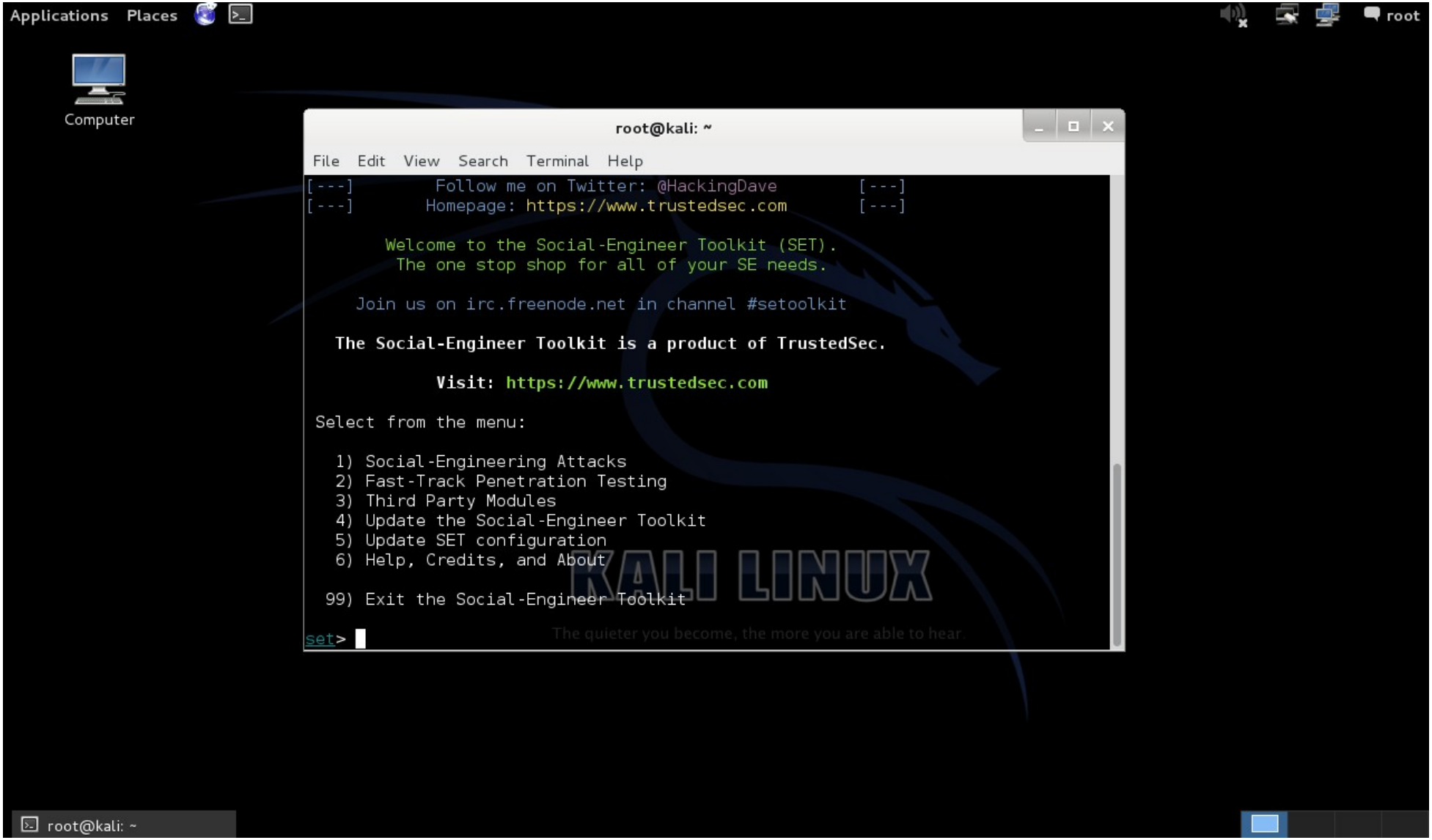
http://www.reydes.com/d/?q=node/2

Mi Blog sobre temas de mi interés.

http://www.reydes.com/d/?q=blog/1



Demostraciones



Ingeniería Social

¡Muchas Gracias!

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Jueves 8 de Enero del 2015