Webinar Gratuito
Hacking Ético

V. 2

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

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

e-mail: ReYDeS@gmail.com

Jueves 30 de Octubre del 2014

¿Quién Soy?

- Consultor e Instructor Independiente en Hacking Ético, Informática Forense y GNU/Linux.
- Ex Integrante de RareGaZz y actual integrante de PeruSEC.
- Ex Redactor en la Revista Linux+ DVD (ES).
- Creador del II Reto Forense Digital Sudamericano - Chavín de Huantar 2012.
- Brainbench Certified Network Security, Brainbench Certified Computer Forensics (U.S.) & Brainbench Certified Linux Administration (General). CNHE, CNCF, CNHAW.
- Más de 11 años de experiencia en el área.
- @Alonso_ReYDeS
- pe.linkedin.com/in/alonsocaballeroquezada/

Hacking Ético, Pruebas de Penetración, etc.

Existen diversos términos o denominaciones, los cuales se utilizan de manera similar, generando algo de confusión. Por lo tanto se proceden a definir los siguientes términos.

- Hacking Ético
- Pruebas de Penetración
- Valoraciones de Seguridad (Valoraciones de Vulnerabilidades)
- Auditorias de Seguridad

*

Hacking Ético

Definición Tradicional de Hacking:

El termino se refiere a la exploración de la tecnología, intentando conocerla al nivel más profundo, para ser capaz de manipularla y hacer algo para lo cual no fue diseñada.

Definición “Mala” de Hacking:

Muchas personas piensas en el término como la irrupción en las computadoras y redes sin permiso.

Ético:

El uso del término “Ético”, implica la no connotación “Mala” del termino Hacking.

El Hacking Ético utiliza técnicas de ataque de computadora para encontrar fallas con el permiso del propietario del objetivo y con el propósito de mejorar la seguridad del objetivo.

*

Pruebas de Penetración

Las Pruebas de Penetración se orientan en encontrar vulnerabilidades de seguridad en el entorno objetivo, las cuales podrían permitir a un atacante a penetrar la red o computadoras, o robar información.

Esto se realiza utilizando técnicas y herramientas similares a las empleadas por los criminales y atacantes del mundo real.

El propósito de una Prueba de Penetración es comprometer los sistemas del objetivo y obtener acceso a la información, para poder determinar el impacto en la empresa.

El Hacking Ético es un termino amplio abarcando todas las técnicas de Hacking Éitco utilizados para propósitos buenos, mientra que las Pruebas de Penetración están más enfocadas en el proceso de encontrar vulnerabilidades en el entorno objetivo. Desde este punto de vista la Prueba de Penetración es un subconjunto del Hacking Ético.

*

Valoraciones de Seguridad

A las Valoraciones de Seguridad también se les denomina como “Valoraciones de Vulnerabilidades”. También estos términos son utilizados de manera similar al termino de Pruebas de Penetración, pero existen diferencias.

Las Pruebas de Penetración se enfocan en ingresar o robar datos. Penetrar el entorno objetivo explotando las vulnerabilidades descubiertas.

Las Valoraciones de Seguridad o de Vulnerabilidades se enfocan en encontrar vulnerabilidades de seguridad, frecuentemente sin explotarlas ni obtener ingreso.

Por lo tanto las Pruebas de Penetración son más profundas, con el objetivo de tomar control sobre los sistemas y robar datos, mientras que las valoraciones de seguridad y vulnerabilidades, implican el proceso de buscar fallas de seguridad. Estas valoraciones también incluyen frecuentemente revisión de políticas y procedimientos, las cuales no están incluidas en una Prueba de Penetración.

*

Auditorias de Seguridad

Las auditorias de Seguridad implican realizar una medición de las cosas contra un conjunto de estándares riguroso, previamente determinado y fijo. Estas auditorias son casi siempre hechas con listas de verificación detalladas.

Algunas organizaciones de Pruebas de Penetración y Hacking Ëtico han creado sus propias listas de verificación internas para temas requeridos de ser descubiertos durante una prueba, pero esas listas de verificación no son tan detalladas como una auditoria exhaustiva.

*

Definición de un Hacker Ético

Es una persona asignada para realizar Pruebas de Penetración, con el propósito de mejorar la postura de seguridad de la organización.

Es empleado por una organización para intentar penetrar en la infraestructura de red o sistemas de computadoras, utilizando los mismo métodos de un Hacker “Malicioso”, con el propósito de encontrar y solucionar las vulnerabilidades de seguridad en las computadoras.

Las Pruebas de Penetración realizadas por solicitud del propietario de los sistemas o redes objetivos, son totalmente legales.

*

Tipos de Hackers

1. Sombrero Blanco: Hackers Éticos los cuales utilizan sus conocimientos para propósitos defensivos. Son profesionales de seguridad utilizando sus conocimientos para ubicar debilidades e implementar medidas correctivas.

2. Sombrero Negro: Son Hackers “maliciosos” o Crackers quienes utilizan sus conocimientos para propósitos ilegales o maliciosos. Rompen o violan la integridad de los sistemas remotos con intenciones dañinas.

3. Sombrero Gris: Son Hackers trabajando de manera ofensiva o defensiva, dependiendo de la situación. Esta es la línea que divide a un Hacker y un Cracker. Muchos individuos caen en ambas categorías.

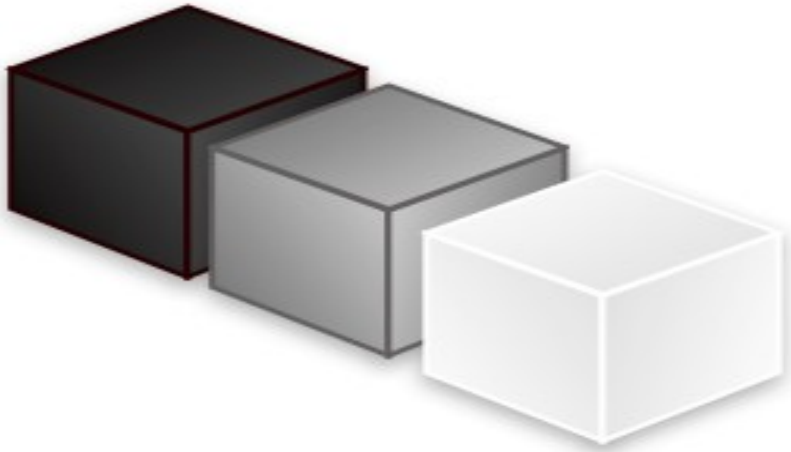
*

Tipos de Pruebas

1. Caja Negra: Realizar pruebas de seguridad sin un conocimiento previo sobre la infraestructura de red o sistemas a ser evaluados. Este tipo de pruebas simula el ataque de un Hacker malicioso externo al perímetro de seguridad de la empresa.

2. Caja Blanca: Realiza evaluaciones de seguridad con un conocimiento pleno de la infraestructura de la red, tal como lo tendría el administrador de la red.

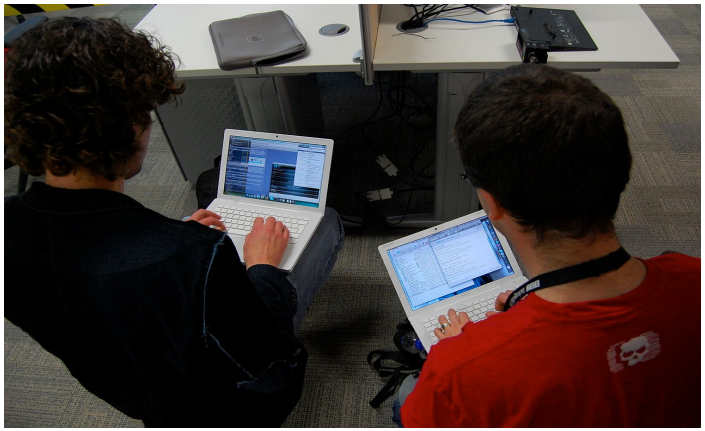
3. Caja Gris: Involucra realizar una evaluación de seguridad de manera interna. Este tipo de pruebas examina el alcance del acceso de un insider (interno) dentro de la red.

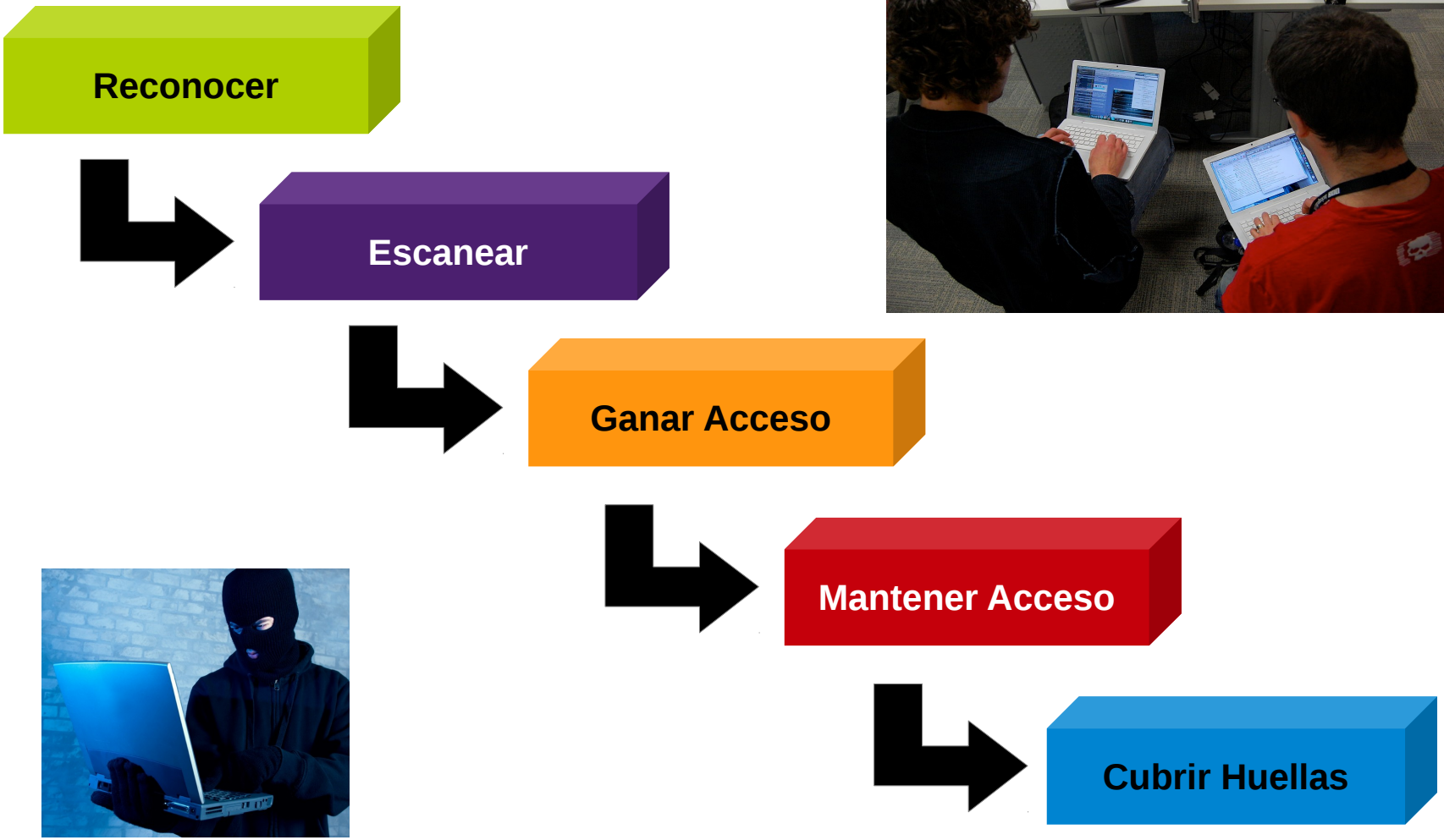


*

Fases de un Hacking Ético

Un Hacker Ético sigue una metodología similar a la utilizada por un Hacker “Malicioso”. Los fases o etapas son idénticas, sin importar las intenciones del Hacker.



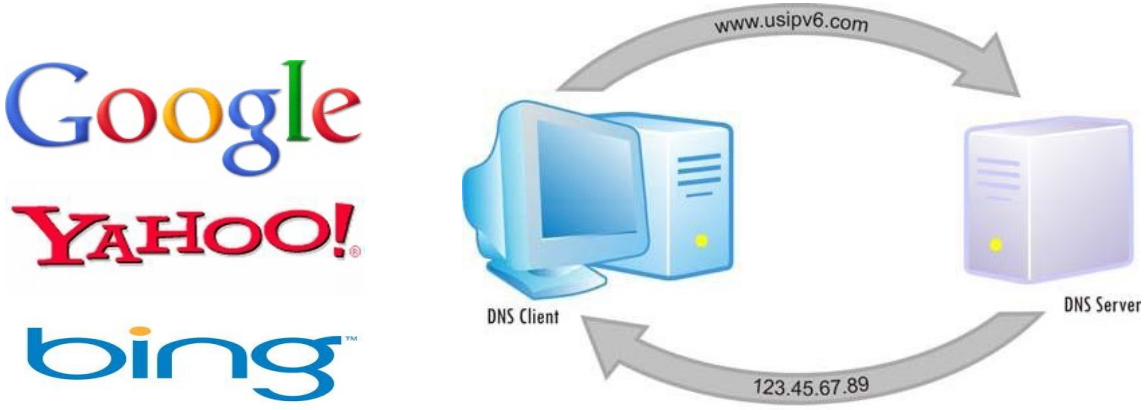


*

Reconocimiento

Reconocimiento Pasivo: Captura información relacionada al objetivo sin conocimiento del individuo o empresa. Este proceso se denomina captura de información. Algunos métodos son la búsqueda de basura e ingeniería social. El Sniffing en la red es también un mecanismo utilizado.

Reconocimiento Activo: Evalúa la red para descubrir hosts únicos, direcciones IP, y servicios en la red. Implica un mayor riesgo de detección que el reconocimiento pasivo. Proporciona indicios de los mecanismos de seguridad, pero el proceso también incrementa las posibilidades de ser detectado. Ambos tipos de reconocimiento permiten descubrir información útil a ser utilizado en un ataque.



*

Escaneo

Implica tomar la información descubierta durante la fase de Reconocimiento y utilizarla para examinar la red. Entre las herramientas que el Hacker utiliza durante la fase de Escaneo se incluyen:

1. Dialers (Marcadores)
2. Port Scanners (Escaners de Puertos)
3. Network Mappers (Mapeadores de red)
4. Sweepers (Barredores)
5. Vulnerability Scanners (Escaners de Vulnerabilidades)

Los Hackers buscan cualquier información útil para realizar el ataque; como por ejemplo el nombre de las computadoras, las direcciones IP, cuentas de usuario, etc.

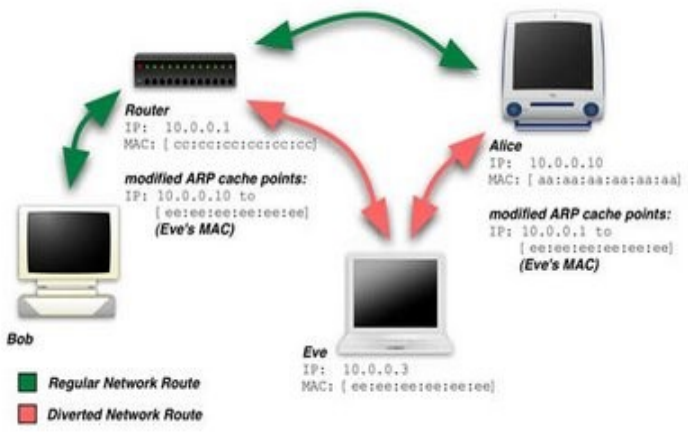
*

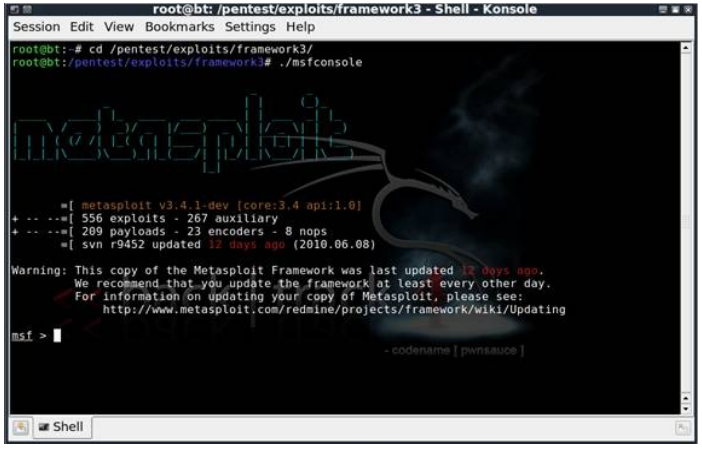
Ganar Acceso

Aquí se manifiesta el Hacking “Real”. Las vulnerabilidades descubiertas durante la fase de Reconocimiento y Escaneo ahora se explotan para ganar acceso.

El método de conexión que el Hacker utiliza para realizar la explotación puede ser una Red de Área Local (LAN, ya sea cableada o inalámbrica), acceso local al objetivo, Internet, o fuera de línea (off-line).

Algunas de las técnicas utilizadas incluyen, desbordamiento de buffer basados en pila, secuestro e interceptación de sesiones, etc.





*

Mantener Acceso

Cuando se gana el acceso, se desea mantener el acceso para realizar posteriores ataques y explotaciones. El Hacker “fortalece” el sistema de otros Hackers o del personal de seguridad, asegurando su acceso exclusivo con puertas traseras (backdoors), rootkits, troyanos u otros mecanismos.

Si el Hacker se apropia del sistema, puede utilizarlo como base para lanzar ataques hacia otros sistemas o redes. A este sistema también se le denomina un sistema zombi.

```
meterpreter > getuid
Server username: NT-AUTORITÄT\SYSTEM
meterpreter > use incognito
Loading extension incognito...success.
meterpreter > list_tokens
Usage: list_tokens <list_order_option>

Lists all accessible tokens and their privilege level

OPTIONS:

    -g        List tokens by unique groupname
    -u        List tokens by unique username


meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
NT-AUTORITÄT\LOKALER DIENST
NT-AUTORITÄT\NETZWERKDIENST
NT-AUTORITÄT\SYSTEM
PENTEST-3C73D9C\pentestuser

Impersonation Tokens Available
========================================
NT-AUTORITÄT\ANONYMOUS-ANMELDUNG
```

antidetection

Package: Brilliant Hacker defender Forever

Brilliant Hacker defender Forever has same features as Brilliant Hacker defender package with addition of Antivirus support and Antidetection engine support - both for 6 months. Only this package comes with support for new detectors not only for new versions of existing detectors. The package contains these features:

- Antivirus protection
- Antivirus support 6 months
- Source code
- Internal inifile
- Logoner
- Antidetection engine
  - F-Secure BlackLight 1.0.1017.0, 1.2.1003.0, 1.3.1015, 1.4.1003, 1.5.1002, 2.0.1008, 2.1.1010, 2.1.1012, 2.1.1013, 2.1.1018, 2.1.1019
  - F-Secure BlackLight Console 1.25.1006.0, 1.28.1006.0
  - Find Hidden Service 1.0, 1.1
  - Flister 0.1
  - IceSword 1.04, 1.06, 1.06b, 1.08, 1.10, 1.12
  - Kernel SC 1.3
  - Kernel PS 0.4, 1.0
  - KHS 0.1
  - Klister 0.4
  - KProcCheck 0.1, 0.2-beta1, 0.2-beta2
  - modGKEPEK 0.1, 0.2
  - Process Hunter
  - Process Magic V1.0 by WinEggDrop
  - RegdatXP 1.41, 1.42
  - RootkitRevealer v1.00, v1.01, v1.10, v1.20, v1.31, v1.32, v1.33, v1.40, v1.51, v1.53, v1.54, v1.55
  - RootKitShark 3.11, 3.22, 3.27
  - TaskInfo 6.0.1.134, 6.2.0.170
  - UnHackMe 1.0, 2.0, 2.5 beta, 2.5 beta2, 2.5, 3.0 beta
- Antidetection engine support 6 months

package price: 900 EUR

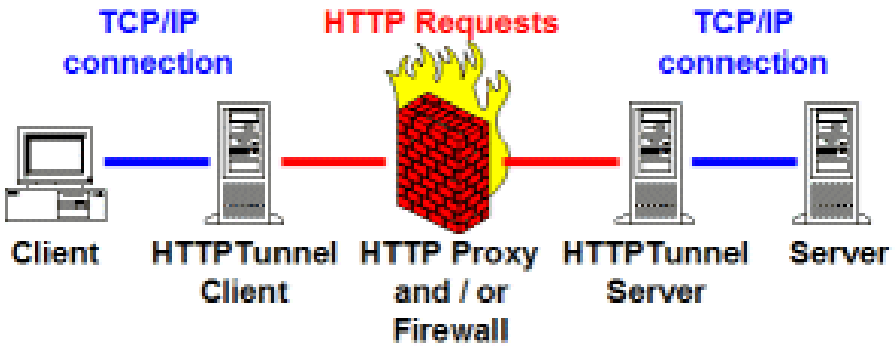
*

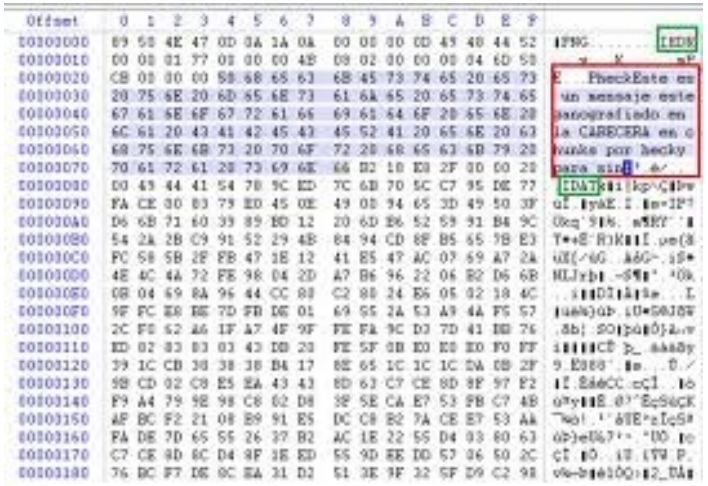
Cubrir Huellas

Cuando el Hacker ha ganado y mantiene el acceso en las redes y sistemas, desea cubrir sus huellas para evitar ser detectado por el personal de seguridad y utilizar el sistema comprometido, remover evidencia de su intrusión, o evitar acciones legales.

Se intenta eliminar los rastros del ataque, tales como archivos de registros (logs), o alarmas de los IDS o IPS.

Entre las actividades realizadas aquí se incluyen la esteganografía, utilizar protocolos “tunneling” y alterar los archivos de registros.





*

Procedimiento para realizar un Hacking Ético

Un Hacking Ético se realiza de una manera organizada y estructurada, como parte de una Prueba de Penetración o Auditoría de Seguridad. La intensidad y alcance de los sistemas y aplicaciones a ser evaluados son determinadas por las necesidades del cliente.

1. Hablar con el cliente, discutir las necesidades de las pruebas.
2. Preparar y firmar un documento de acuerdo de NO divulgación (Acuerdo de Confidencialidad) con el cliente.
3. Organizar al equipo de Hackers Éticos, y preparar los horarios de las pruebas.
4. Realizar las pruebas.
5. Analizar los resultados de las pruebas, y preparar un reporte.
6. Presentar el reporte al cliente.

*

Cursos Virtuales

Todos los Cursos 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 Información:

caballero.alonso@gmail.com

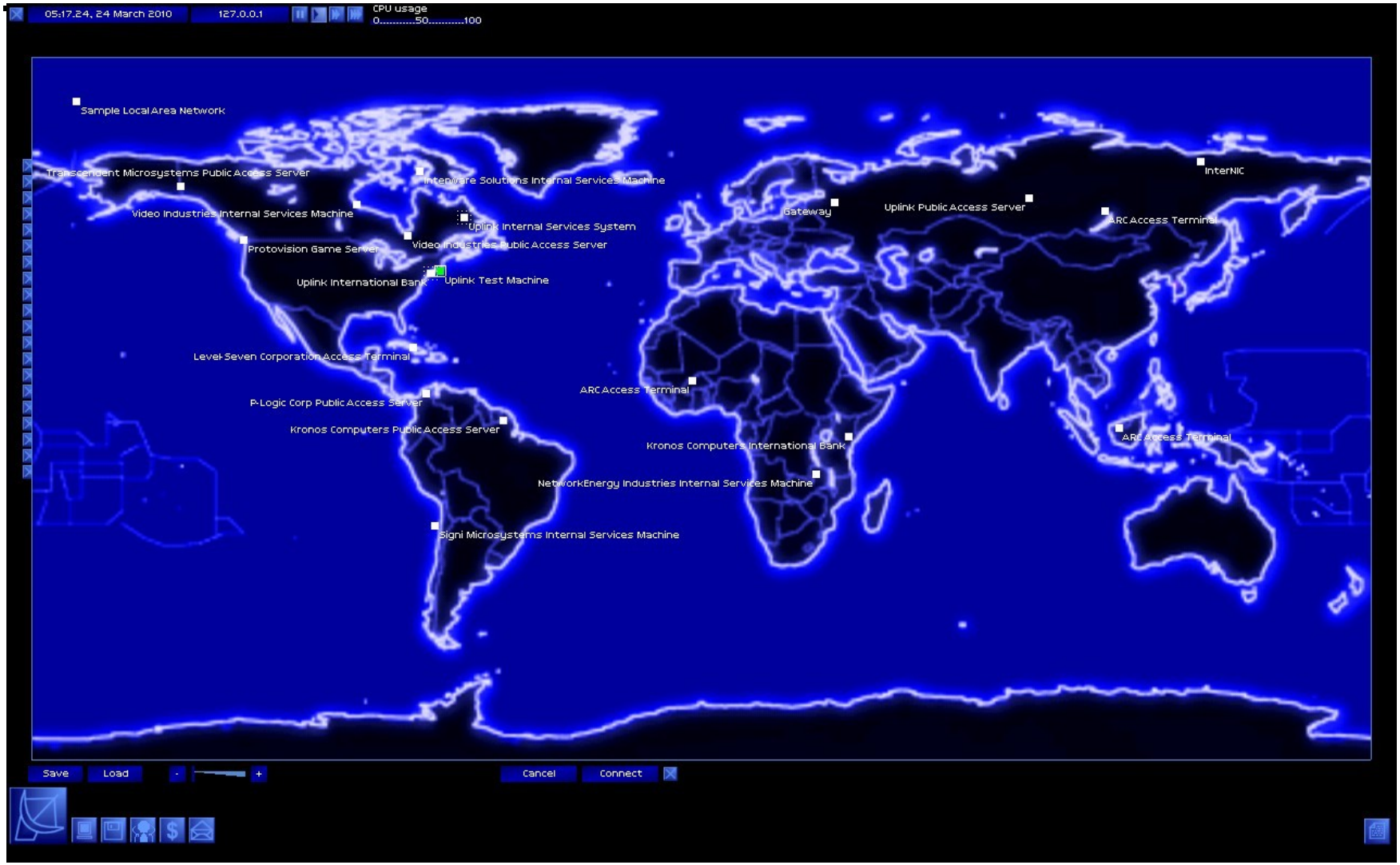
@Alonso_ReYDeS

http://pe.linkedin.com/in/alonsocaballeroquezada/

ReYDeS

http://www.reydes.com

Demostraciones



*

Más Material

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

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

Todas las diapositivas utilizadas en los Webinars Gratuitos las encuentran en la siguiente página.

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

Todos los artículos y documentos que he publicado.

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

Mi Blog sobre temas de mi interés.

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

¡Muchas Gracias!
Hacking Ético

V. 2

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

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

e-mail: ReYDeS@gmail.com

Jueves 30 de Octubre del 2014