

HACKING CON PYTHON

La Guía Completa Para Principiantes De Aprendizaje De Hacking Ético Con Python Junto Con Ejemplos Prácticos



MILES PRICE

ÍNDICE

[Introducción](#)

[Capítulo 1: El Hacking básica](#)

[Capítulo 2: La Formación De Tu Hack](#)

[Capítulo 3: Encontrando una Contraseña](#)

[Capítulo 4: Los ataques Spoof](#)

[Capítulo 5: Hackear una conexión de red](#)

[Capítulo 6: Encontrar y ocultar las direcciones IP](#)

[Capítulo 7: Mobilede Hacking](#)

[Capítulo8: El Las mejores herramientas de hacking para uso](#)

[Capítulo 9: Cómo mantener a su propia red de seguridad](#)

[Conclusión](#)

Capítulo 4: Ataca Spoof

Gracias a <https://toschprod.wordpress.com/2012/01/31/mitm-4-arp-spoofing-exploit/> para el código en este capítulo.

Cuando se hacen trizas una red, la única cosa que realmente necesita es buenas habilidades de investigación. Hay que ser capaz de subirse a una red y tener un buen aspecto sin que nadie sepa que estás ahí. A veces, un hacker acceder a un sistema y sentarse allí, en silencio y observando y otras veces, ellos estarán allí bajo la apariencia de otra persona, alguien que está autorizado para estar en la red, por lo que se les permita permanecer allí. Para ello, los hackers utilizan técnicas de suplantación de identidad.

Spoofing es una técnica que consiste en el engaño, utilizado por los hackers que quieren hacerse pasar por otra persona, otro sitio web o software. Esto permite que el hacker para conseguir a través de los protocolos de seguridad que de otro modo les impediría acceder a la información que buscan. Hay un montón de diferentes técnicas de suplantación de identidad, incluyendo:

- **IP Spoofing** - esto implica el hacker enmascarar u ocultar su dirección IP. Normalmente, ésta será la dirección IP del ordenador que está utilizando para el corte y la razón de enmascaramiento es para que la red es engañado en la creencia de que este equipo es el que la red debería estar hablando con. La red se acaba de asumir que el equipo está destinado a ser allí y permitirá que las comunicaciones pasan por el hacker. La manera de hacer esto es a través de la imitación de la dirección IP o el intervalo de direcciones IP, asegurando que el dispositivo del usuario remoto pasa los controles para el criterio establecido por el administrador de red.

Lo que sucede aquí es que la red tiene la intención de ataque confía en ti, lo que le permite la entrada y el acceso a toda la información que desea. La red permitirá que los paquetes de información llegan a su sistema, ya que considera que son el receptor principal. Se puede hacer una de dos cosas con estos paquetes - sólo vista a través de ellos o hacer cambios antes de ser enviados al receptor correcto. Nadie va a ser cualquier enterarse de que otra persona está interceptando la información.

datos - la mejor proviene de MaxMind, una compañía que rastrea todas las direcciones IP en todo el mundo, junto con alguna información que va con cada uno de ellos, esta información podría incluir el país, el código de área, el código postal, incluso la ubicación GPS de la dirección.

1. Para buscar la dirección IP que desea, debe utilizar de manera Kali abrirlo y luego iniciar una nueva terminal. A partir de ahí, puede escribir este comando en el indicador para descargar la base de datos MaxMind - kali> wget-N-
[1 http://geolite.maxmind.com/download/geoip/database/GeoLiteCity.dat.gz](http://geolite.maxmind.com/download/geoip/database/GeoLiteCity.dat.gz)
2. Esto descargará en formato comprimido de manera descomprimir escribiendo el siguiente comando - kali> gzip-dGeoLiteCity.dat.gz
3. A continuación, usted debe descargar Pygeoip. Esto le ayudará a descifrar el contenido de MaxMind como está escrito en el script en Python. Puede descargar esta en una de dos maneras - ya sea directamente a la computadora o puede obtener Kali que lo haga por usted. Para utilizar Kali, escriba este comando en el símbolo - Kali> wget <http://pygeoip.googlecode.com/files/pygeoip-0.1.2.zip>
4. Una vez más, esto va a ser un archivo comprimido y, a descomprimirla, escriba el siguiente comando en el símbolo - kali> pygeoip-0.1.3.zip de descompresión.
5. Usted también necesitará algunas otras herramientas para ayudarle con lo que vas a hacerlo, utilizando Kali, escriba los siguientes comandos para descargarlos todos:
 - Kali> cd / pygeoip-0.1.3
 - Kali> w get http://SVN.python.org/proyectos/caja_de_arena/trunk/setuptools/ez_setup.py
 - Kali> w HTTP GET: /pypi.python.org/packages/2.5/s/setuptools/setuptools-0.6c11-py2.5.egg
 - Kali> mv setuptools0.6c11py2.5.eggsetuptools-0.3a1py2.5.

