Python, hacking y sec-tools desde las trincheras

Daniel García (cr0hn)

<spam>Me</me>

https://www.linkedin.com/in/garciagarciadaniel

https://twitter.com/ggdaniel

- Auditor de seguridad y hacking ético.
- Programador Python.
- Organizador de “saraos”.

- Creador de más de 15 herramientas de seguridad.
- Trabajo en Abirtone.
  - Formación especializada:
    - Hacking y seguridad.
    - Programación segura.
    - Hacking con Python y creación de herramientas de seguridad con Python.
  - Asesoramiento a empresas.
  - Auditoría de seguridad en código fuente.
  - Herramientas de seguridad, monitorización y hacking a medida.

De qué va este taller

- Seguridad y hacking en redes usando como base Scapy.
- Hacking web con Python.
- Creación de varias herramientas de hacking.

Materiales del taller

Todos los ejemplos y materiales de la charla pueden ser encontrados en:

https://github.com/abirtone/cybercamp-2015

Hacking de redes con Scapy

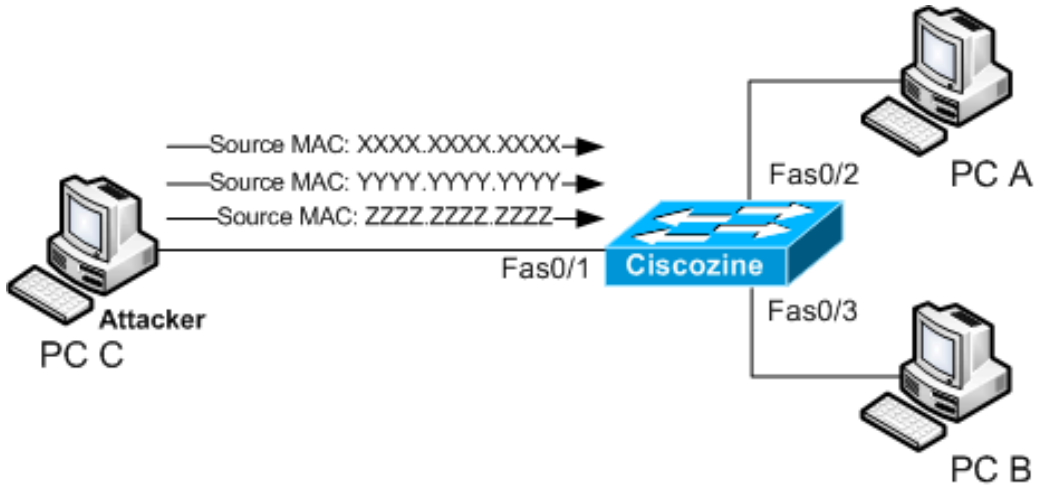
Estudio de Scapy

- Creación de paquetes.
- Envío de información.
- Recepción.
- PCAP.
- Sniffing.
- Flooding.
- Fuzzing

¡Demo time!

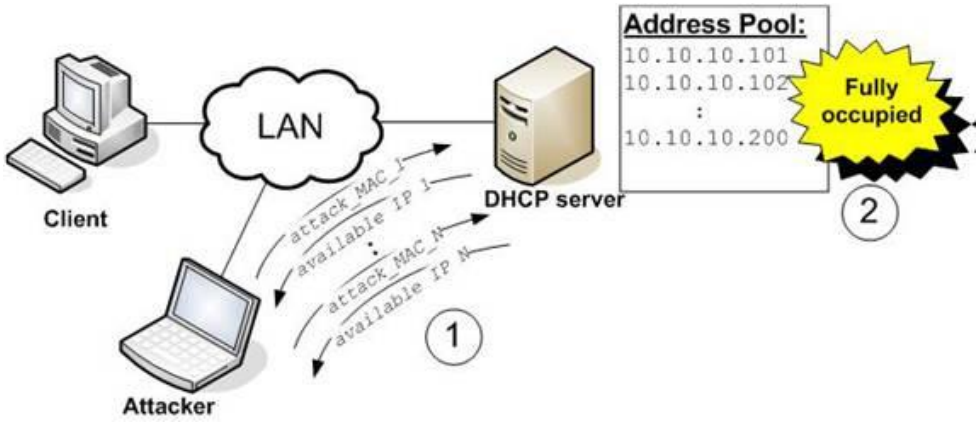
Implementando ataques en Scapy

- ARP flood



- DHCP Starvation

¡Demo time!



Usando Scapy para hacer herramientas

Creación de un escáner de puertos mono-hilo y multi-hilo.

¡Demo time!

“Profesionalizando” nuestras herramientas

Organización y metodología

- OMSTD: http://omstd.readthedocs.org
- STB: https://github.com/abirtone/STB
- STT: https://github.com/abirtone/STT

Transformando nuestras herramientas

- Escaneador de puestos re-usable.
- Usando nmap desde Python.

¡Demo time!

Un sistema de plugins sencillo

- Nos permitirá crear ataques o funcionalidades independientes y llamarlas bajo demanda.
- Existen muchas formas de crear un sistema de plugins.
- Crearemos un sistema muy sencillo de plugins con los ataques:
  - MAC flood.
  - DHCP starvation.

¡Demo time!

Herramientas para la web

Un fuzzer web

- Descubridor de directorios por fuerza bruta.
- Uso de URL del proyecto fuzzdb.
- Detección de páginas de error por defecto:
  - La app será capaz de generar una página de error aleatoria y comparar el contenido de cada URL buscada con la página de error. Si el contenido de ambas tiene un ratio de diferencia de un 60%, se consideran páginas diferentes -> la añadimos a la lista de URL descubiertas.

¡Demo time!

https://cybercamp.es **#CyberCamp15** **@CyberCampEs**

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD