Curso de

Pentesting a Redes

Juan Pablo Caro

Contenido

1. Introducción y conceptos generales
2. Ataques a protocolos de red
3. Ingeniería Social
4. Ataques de denegación de servicio
5. Ataques a redes inalámbricas
6. Creación de reportes

Pre-requisitos

- Conceptos básicos de pentesting
- Manejo intermedio de Linux
- Conocimiento básico de redes
- Conocimiento básico de Sistemas Operativos
- Recomendable: nociones básicas de programación

Cursos sugeridos en Platzi

- Curso de Fundamentos de Pentesting
- Curso de Administración de Servidores Linux
- Curso de Introducción a la Seguridad Informática
- Curso de Redes de Internet

Recursos

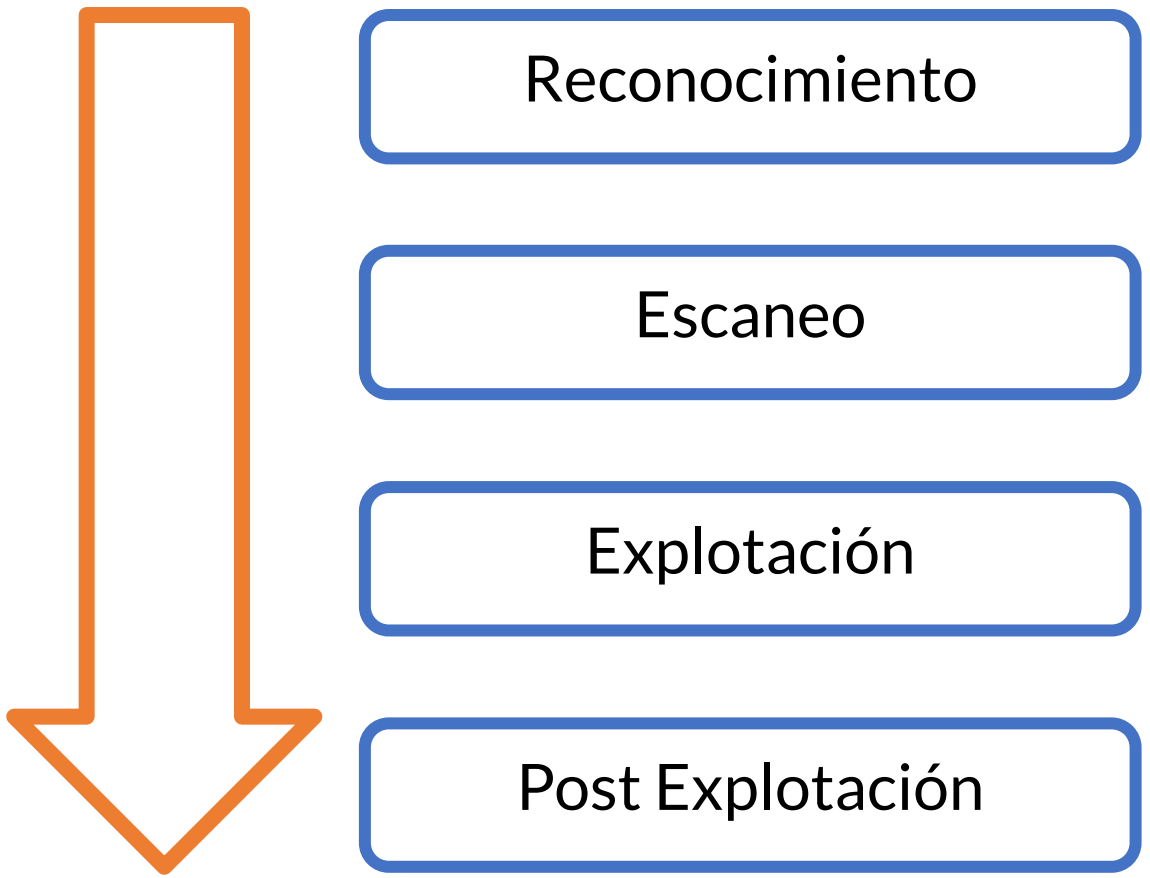
- Motor de máquinas virtuales (VirtualBox, VMWare)
- Sistemas operativos Linux
  - Kali
  - Debian
  - Metasploitable
  - Tiny Core
- Fuentes de consulta
  - https://www.pentest-standard.org/
  - https://www.offensive-security.com/

Modelo de ataques

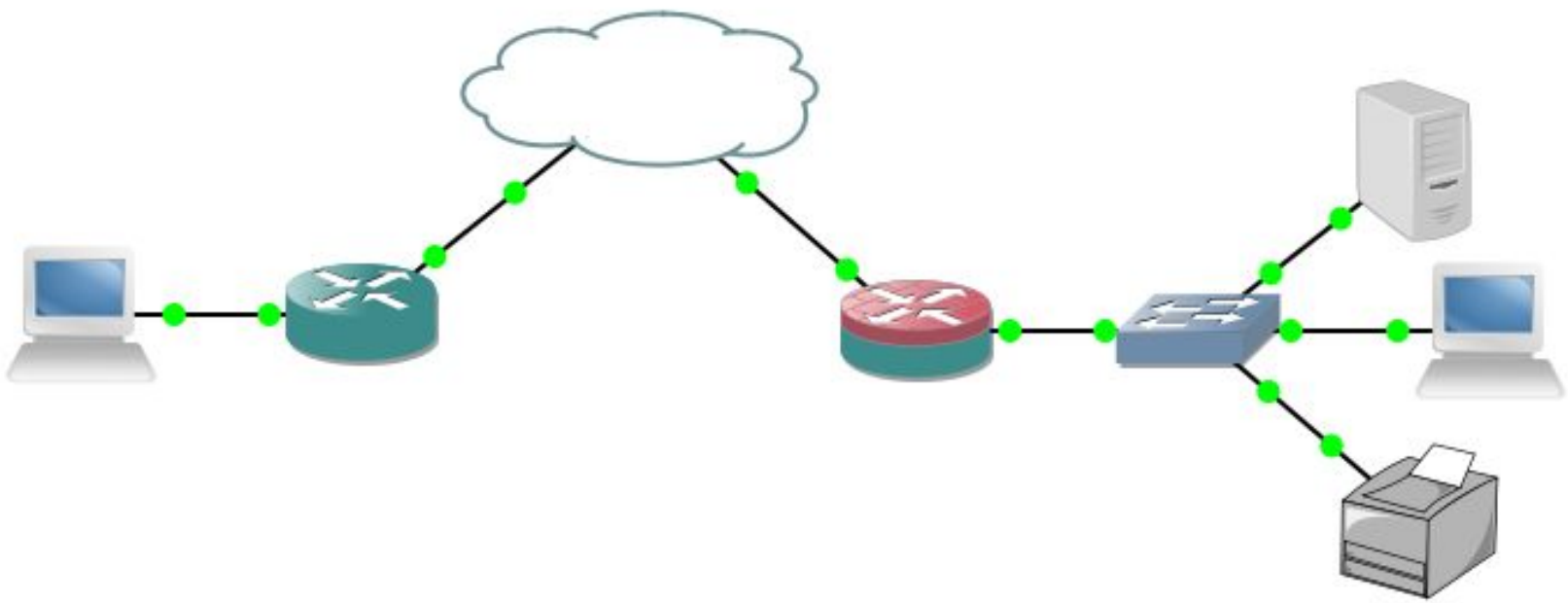
Conceptos clave de un proceso de Pentesting

- Acceso legal y autorizado
- Mejorar la seguridad de los sistemas de información
- Identificación y explotación de vulnerabilidades

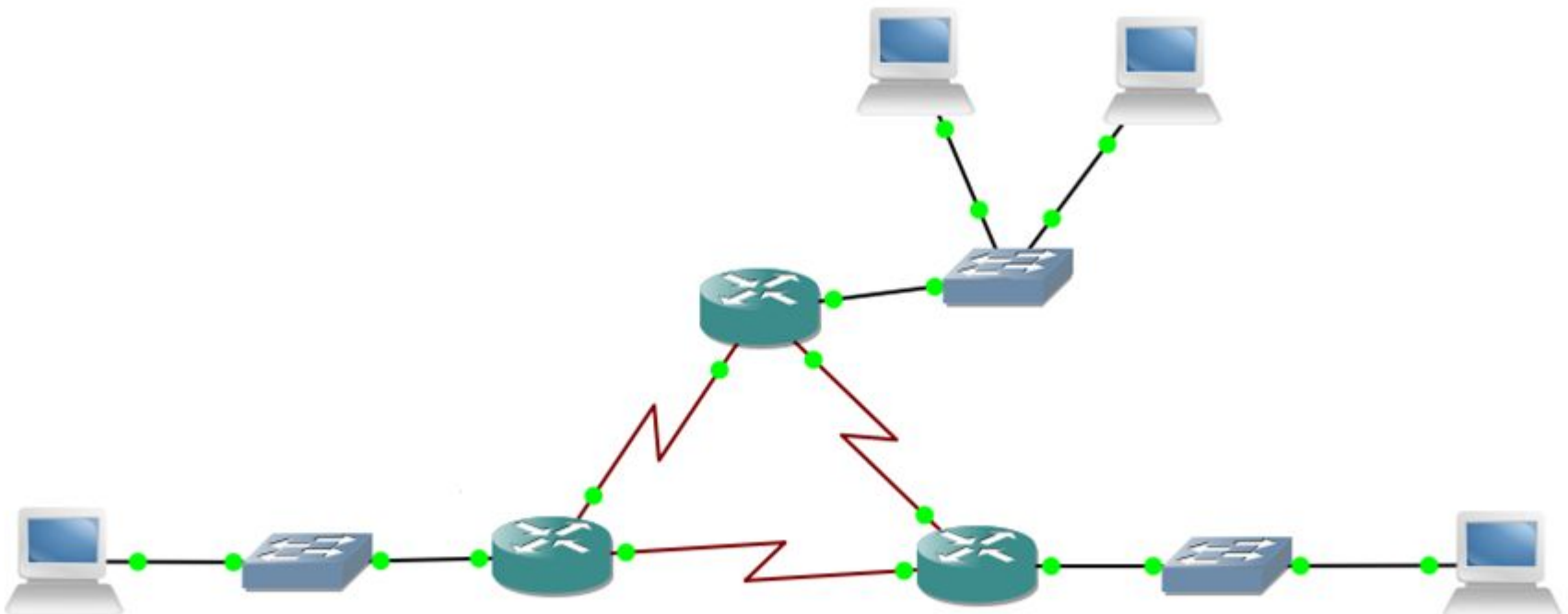
Etapas del Pentesting



Pivoting



Entornos de red



Direccionamiento dinámico

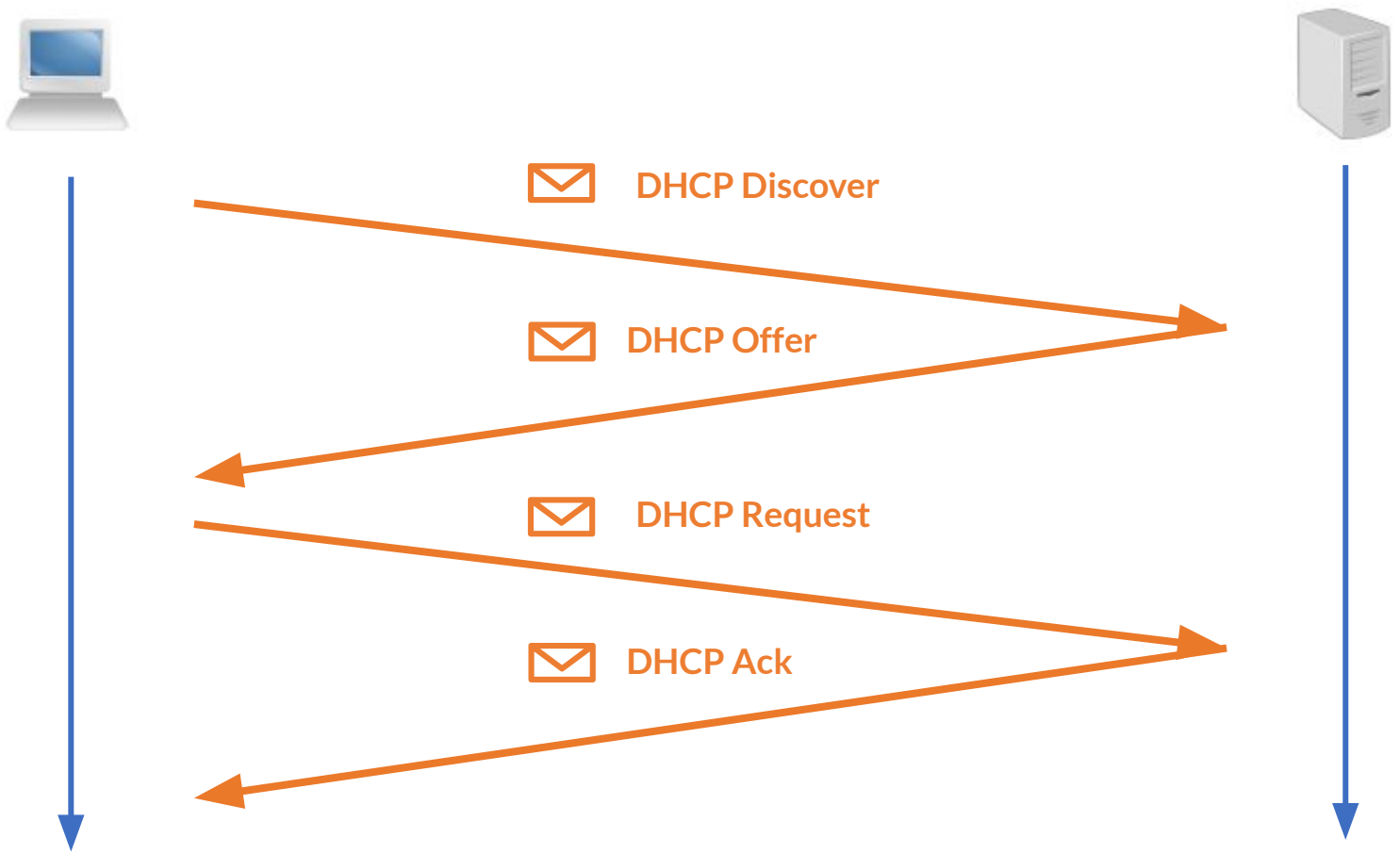
Direcciones estáticas

- Establecidas previamente para cada interfaz.
- Configuración manual de cada dispositivo.
- Disponibilidad limitada de direcciones.

Dynamic Host Configuration Protocol

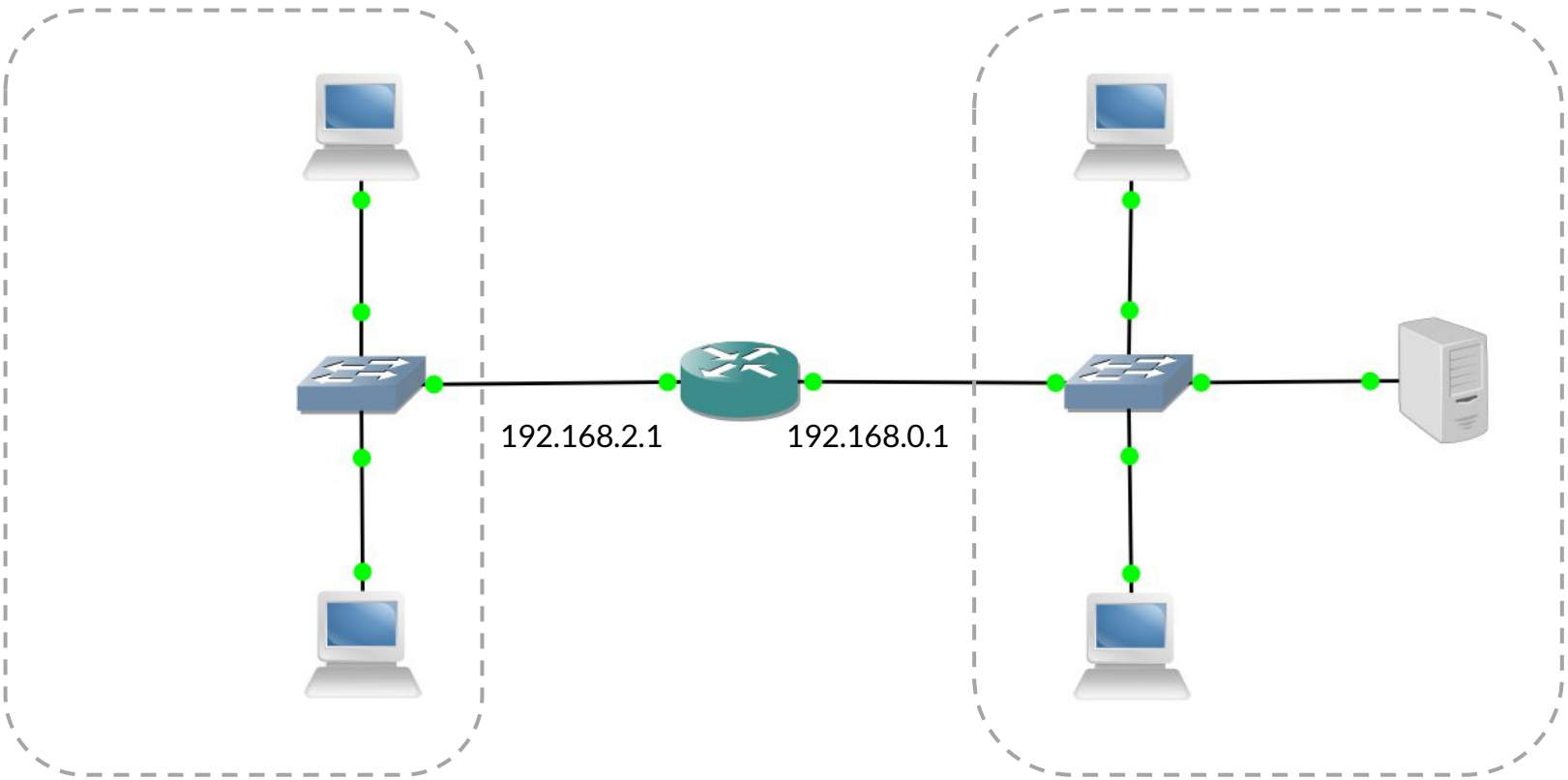
- Protocolo a través del cual un servidor asigna una dirección IP dinámicamente a un dispositivo en un segmento de red.

Secuencia de DHCP

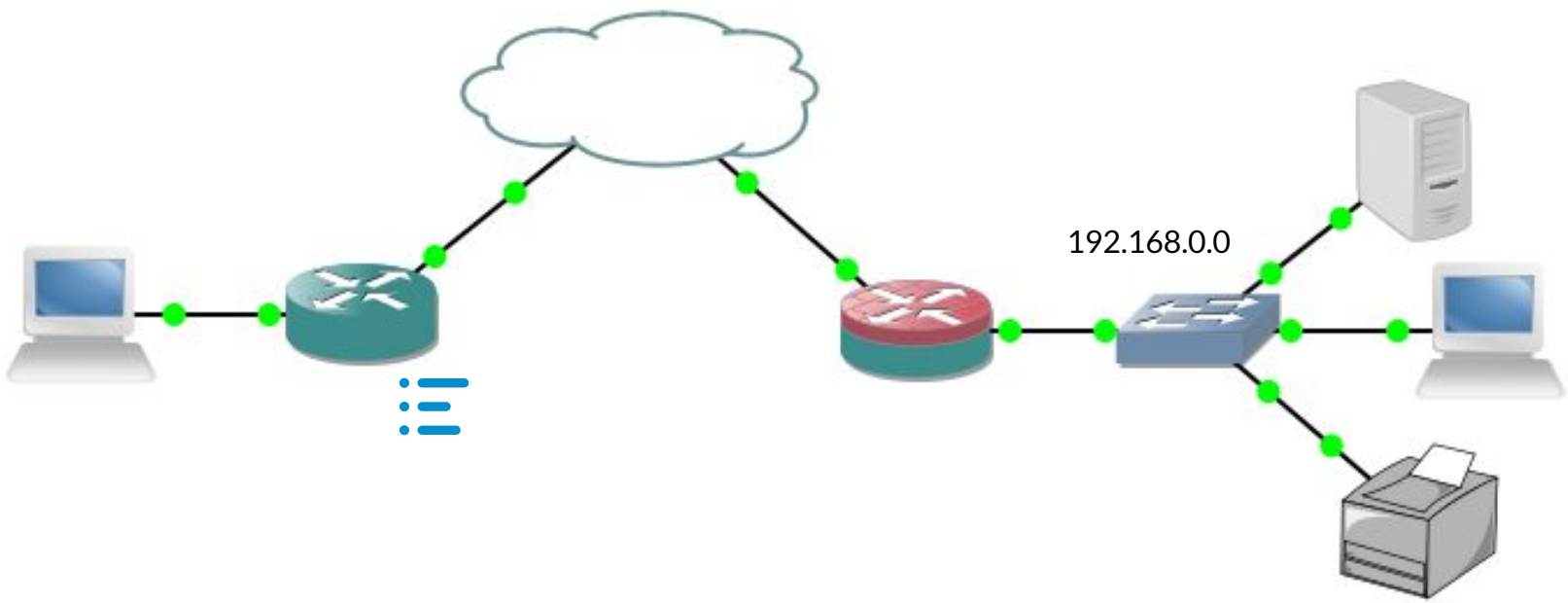


Protocolos de enrutamiento dinámico

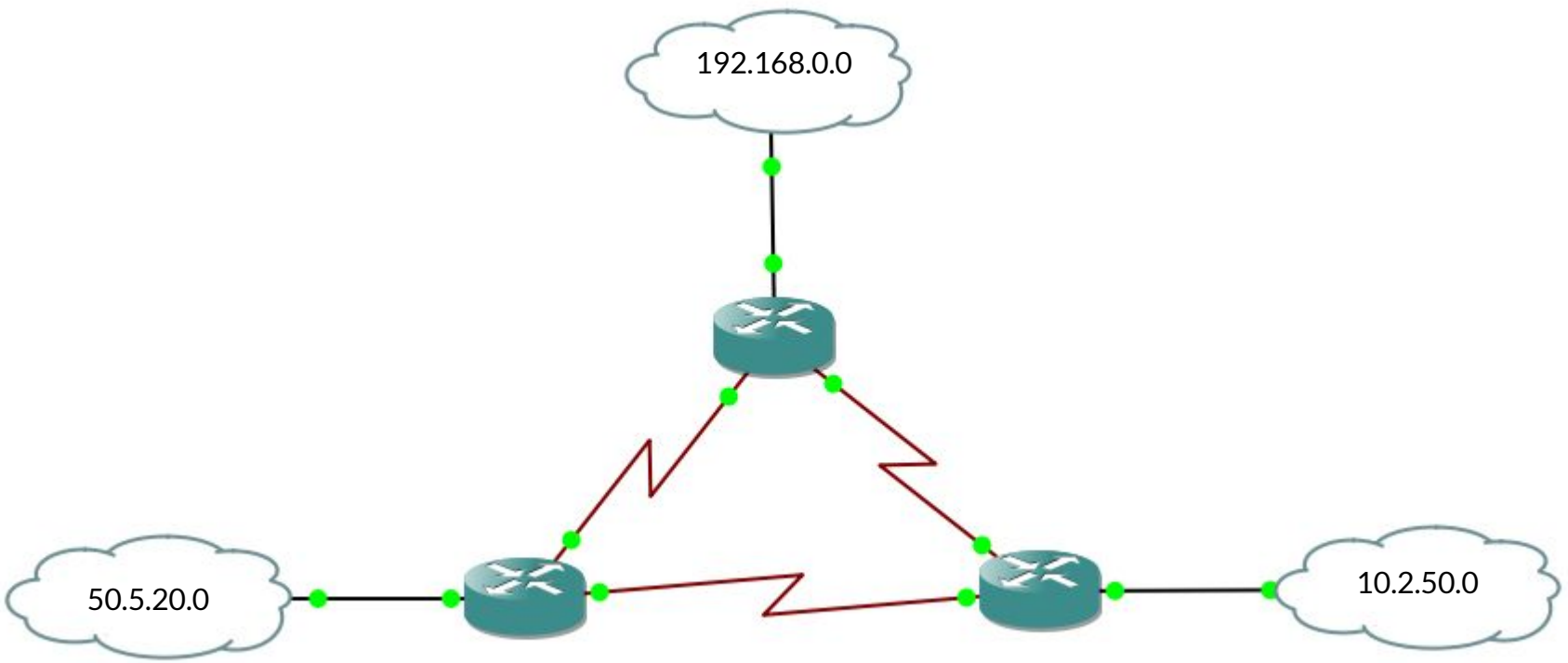
Enrutamiento entre segmentos



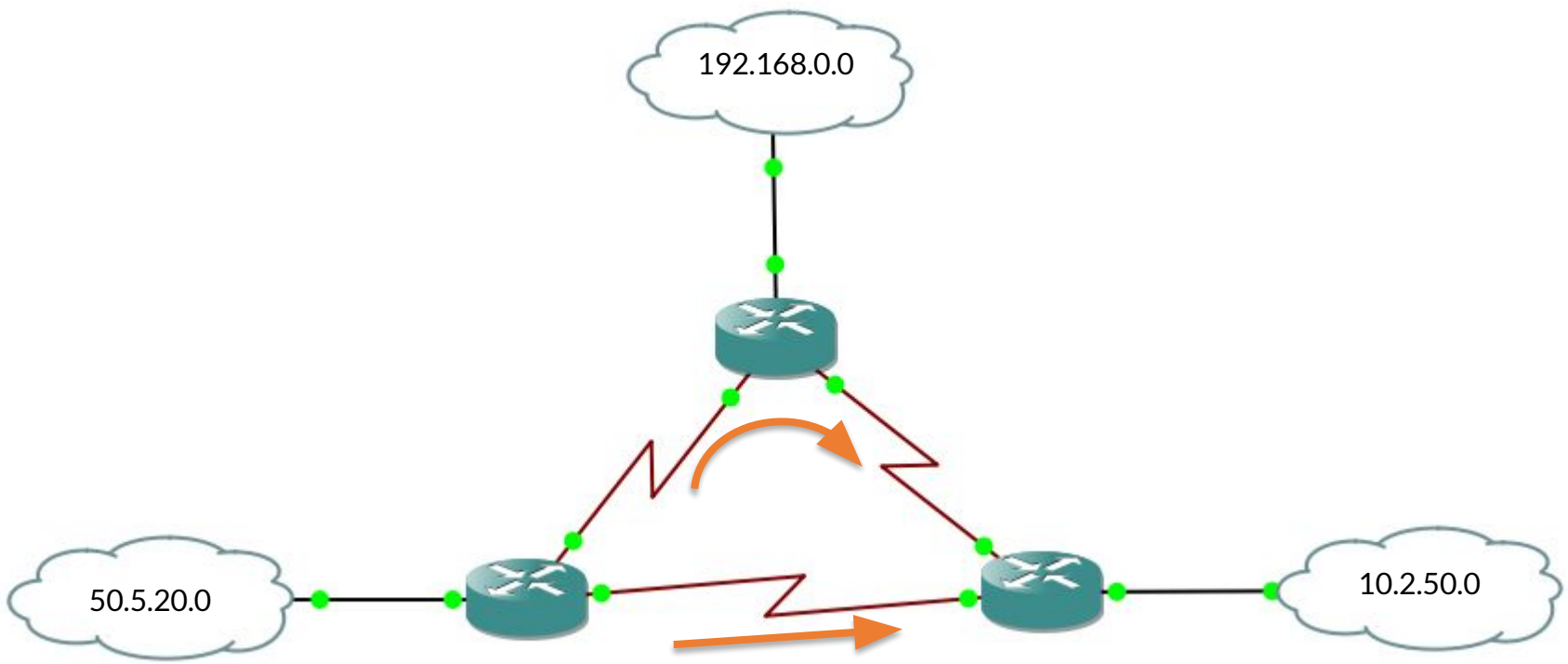
Tablas de enrutamiento



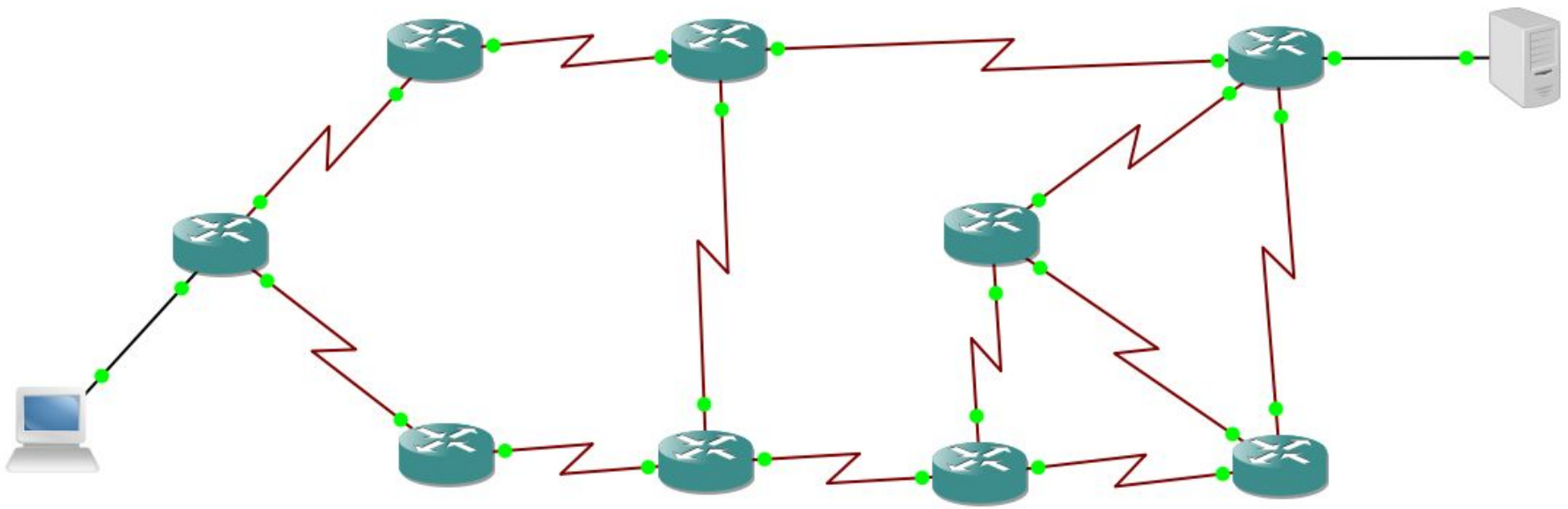
Tablas de enrutamiento



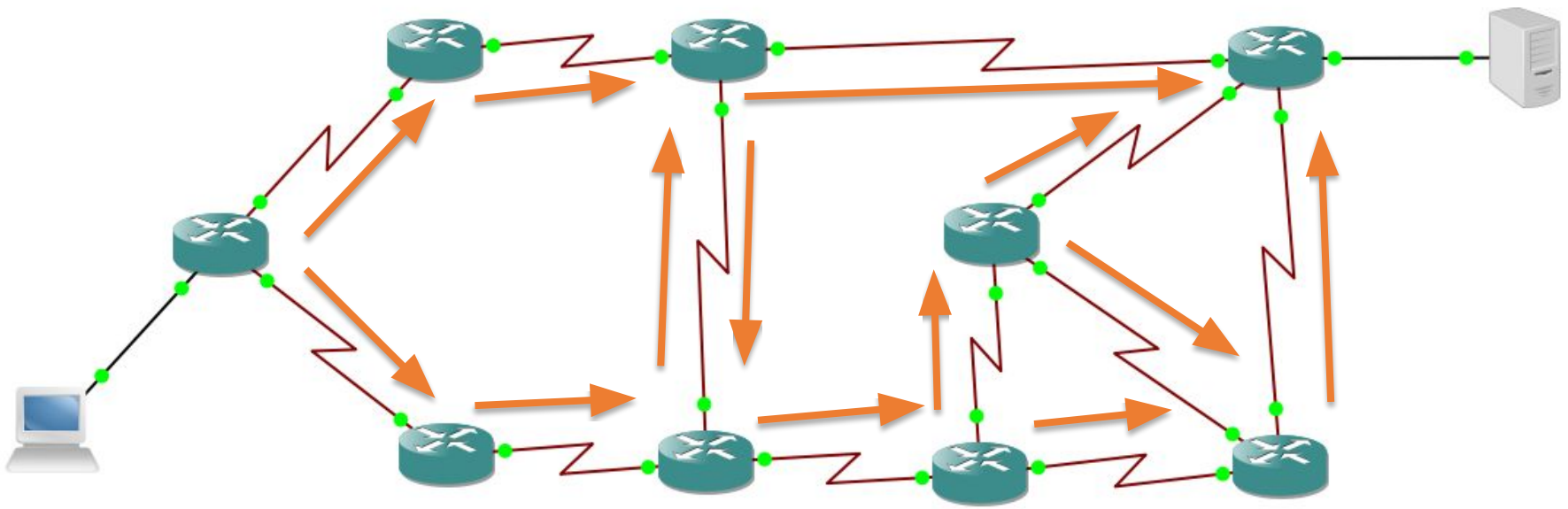
Tablas de enrutamiento



Tablas de enrutamiento



Tablas de enrutamiento



Protocolos de enrutamiento dinámico

1. Protocolos de vector-distancia

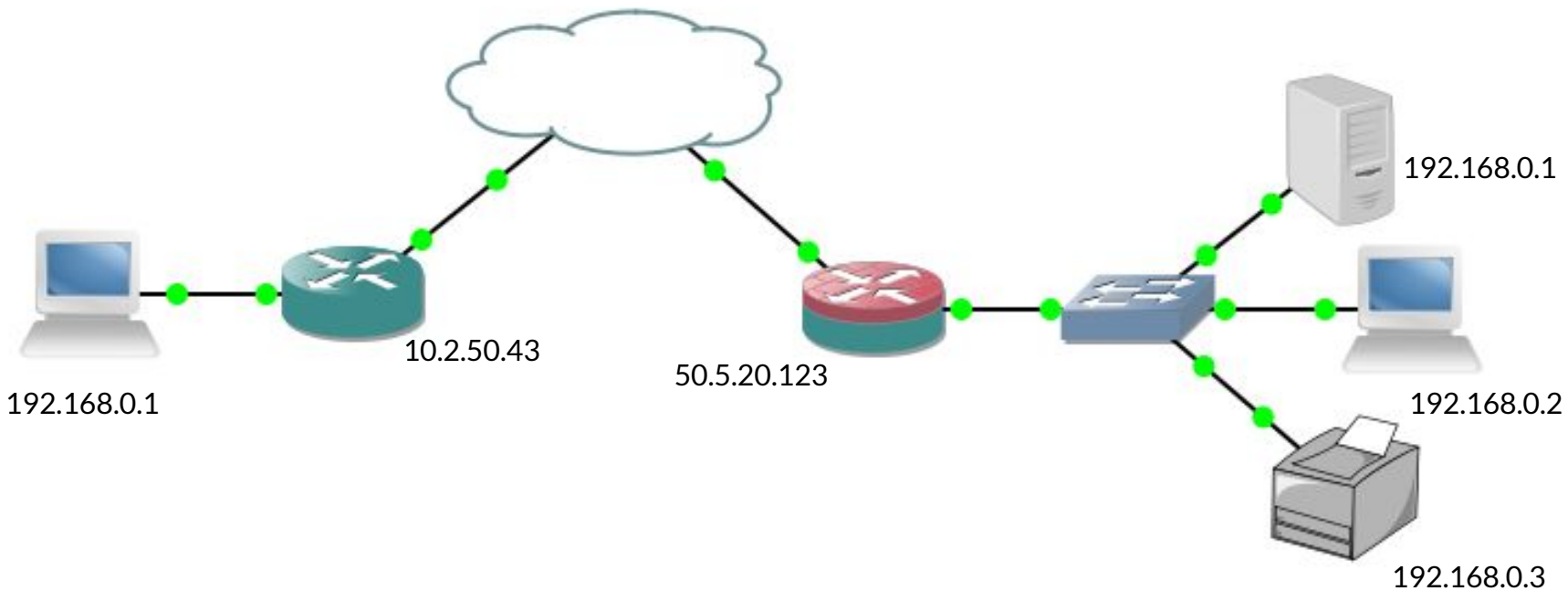
   Los enrutadores propagan las rutas como vectores de distancia (métrica) y dirección.

2. Protocolos de estado de enlace

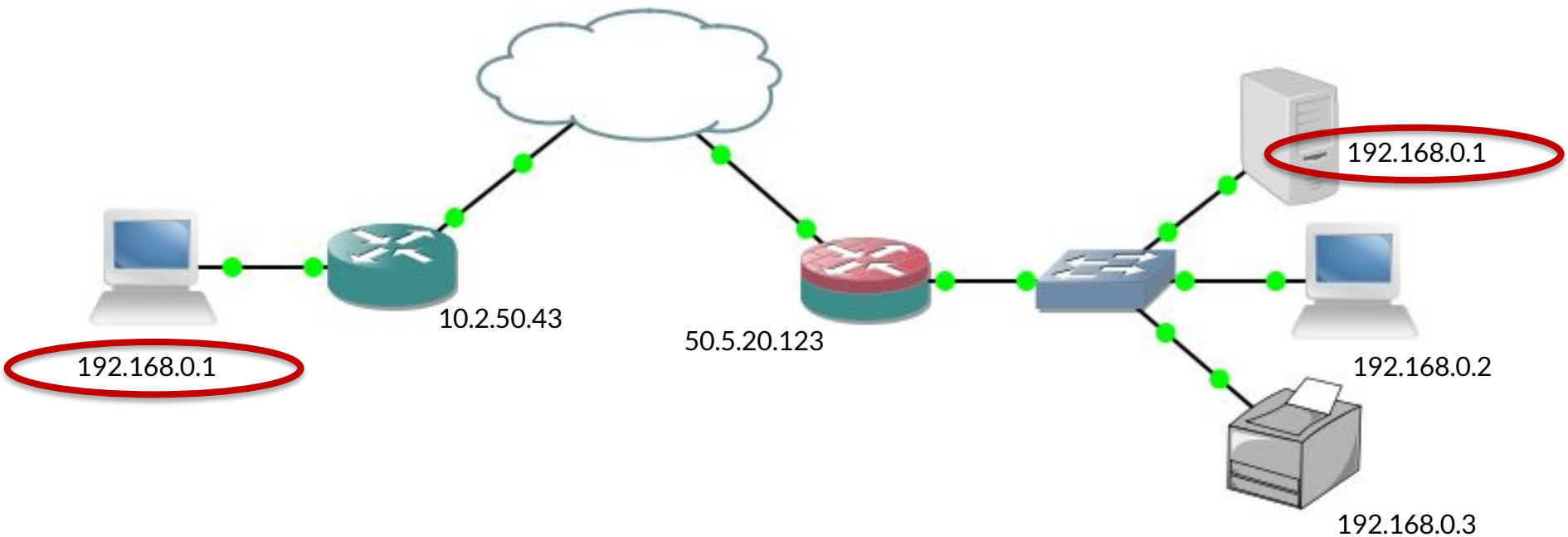
   Cuando un enrutador nuevo ingresa a la red, notifica a los enrutadores adyacentes e intercambia información de rutas con ellos.

Re direccionamiento y traducción

Traducción de direcciones



Traducción de direcciones



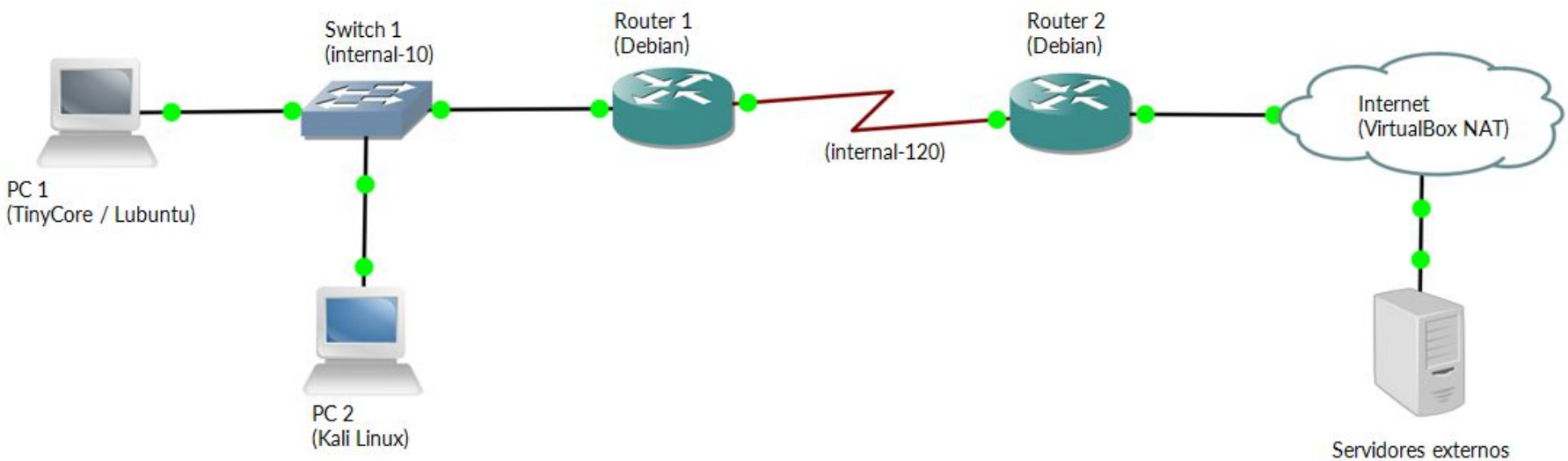
Network Address Translation (NAT)

Protocolo para traducción de direcciones IP en un dispositivo intermedio.

Existen dos tipos de NAT:

- Source NAT (SNAT)
- Destination NAT (DNAT)

Configuración de entorno



Servidores de nombres de dominio

Nombres de dominio

- Nombre de dominio: www.platzi.com
- Dirección IP pública: 104.20.54.150
- Es más fácil recordar nombres que direcciones.

Estructura de un nombre de dominio

Creación de un reporte

¿Qué información obtuvimos?

- Información base
- Vulnerabilidades
- Resultados de la explotación
- Puertas traseras

¿Qué tenemos de nuevo?

- Topología de la red
- Vulnerabilidades en protocolos
- Vulnerabilidades físicas
- Contraseñas y accesos a la red

Cómo ordenar la información

- Resumen ejecutivo
- Hallazgos principales
- Topología identificada
- Lista de acciones ejecutadas
- Recomendaciones

Curso de

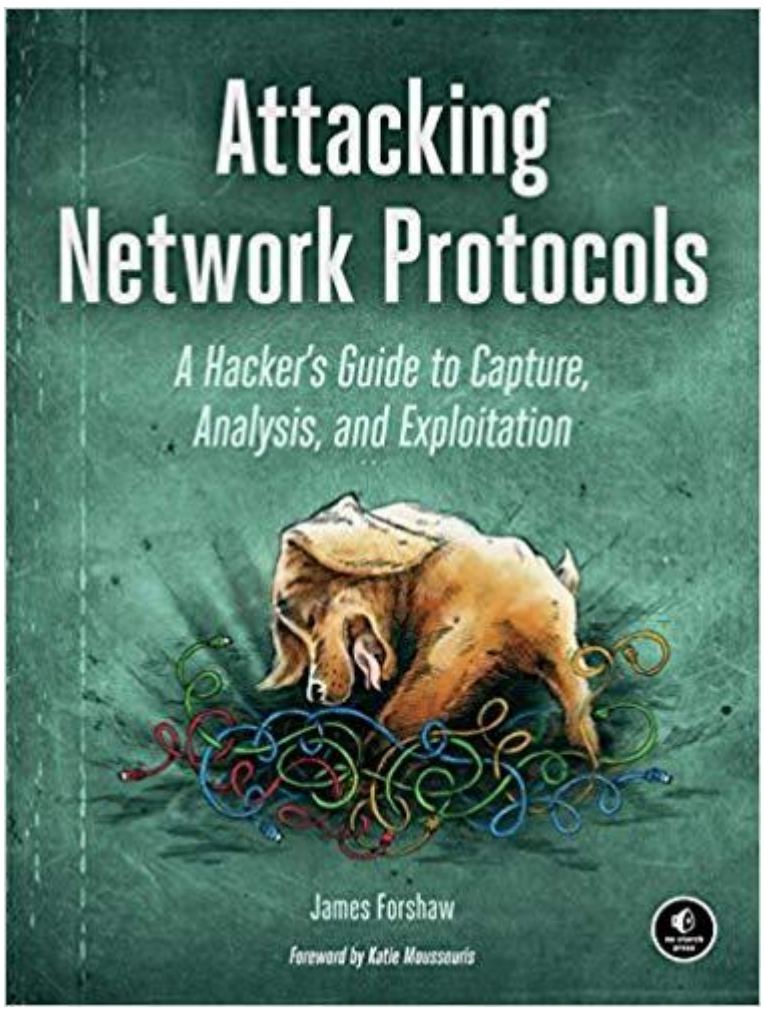
Pentesting a Redes

Juan Pablo Caro

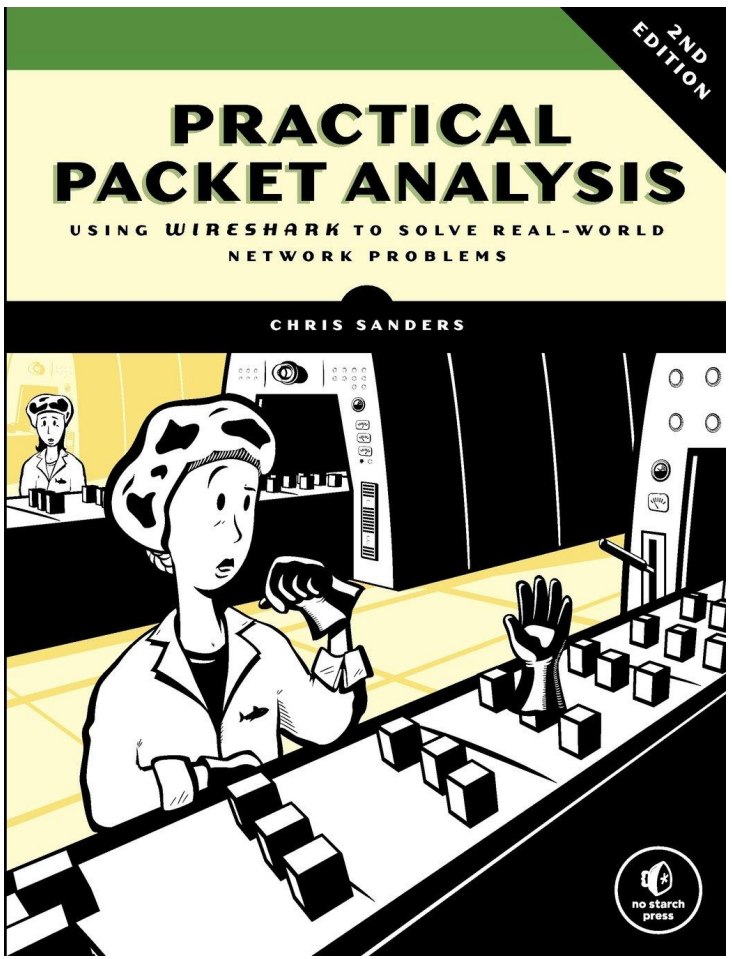
Fuentes de consulta

1. www.exploit-db.com
2. www.offensive-security.com
3. www.sans.org/security-resources/blogs
4. www.google.com

Bibliografía recomendada



Bibliografía recomendada



Bibliografía recomendada