Ethical Hacking

CONTENIDO

- Que es un Ethical Hacking?
- En que consiste un Test de Intrusión?
- Alcance
- Metología de Ethical Hacking
- Etapas y Herramientas
- Descubrimiento y Exploración
- Ingenieria Social

DEFINICIÓN

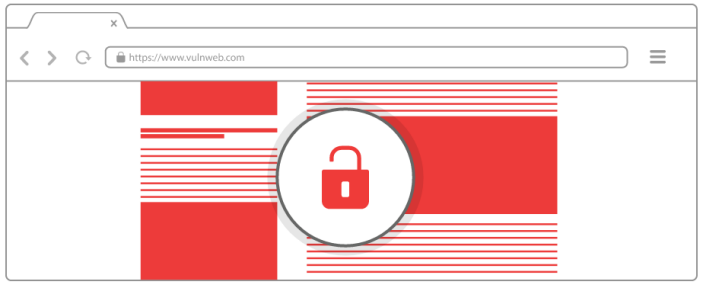
Conjunto de metodologías y técnicas pasivas e intrusivas que recrean un ataque informático en un ambiente controlado.

CONSISTE

Descubrir vulnerabilidades y vectores de ataques, para su posterior mitigación.

ANÁLISIS DE RIESGO

PLAN DE ACCIÓN



EXPOSICIÓN DE VULNERABILIDADES

MITIGACIÓN DE VULNERABILIDADES

Quienes realizan un Test de Intrusión

- Personas con amplios conocimientos sobre plataformas utilizadas en el mercado y las vulnerabilidades asociadas a las mismas.
- Personas formadas con conocimiento sobre Seguridad Informática y de la Información.
- Personas con formación y experiencia en técnicas y el uso de las herramientas de ethical hacking

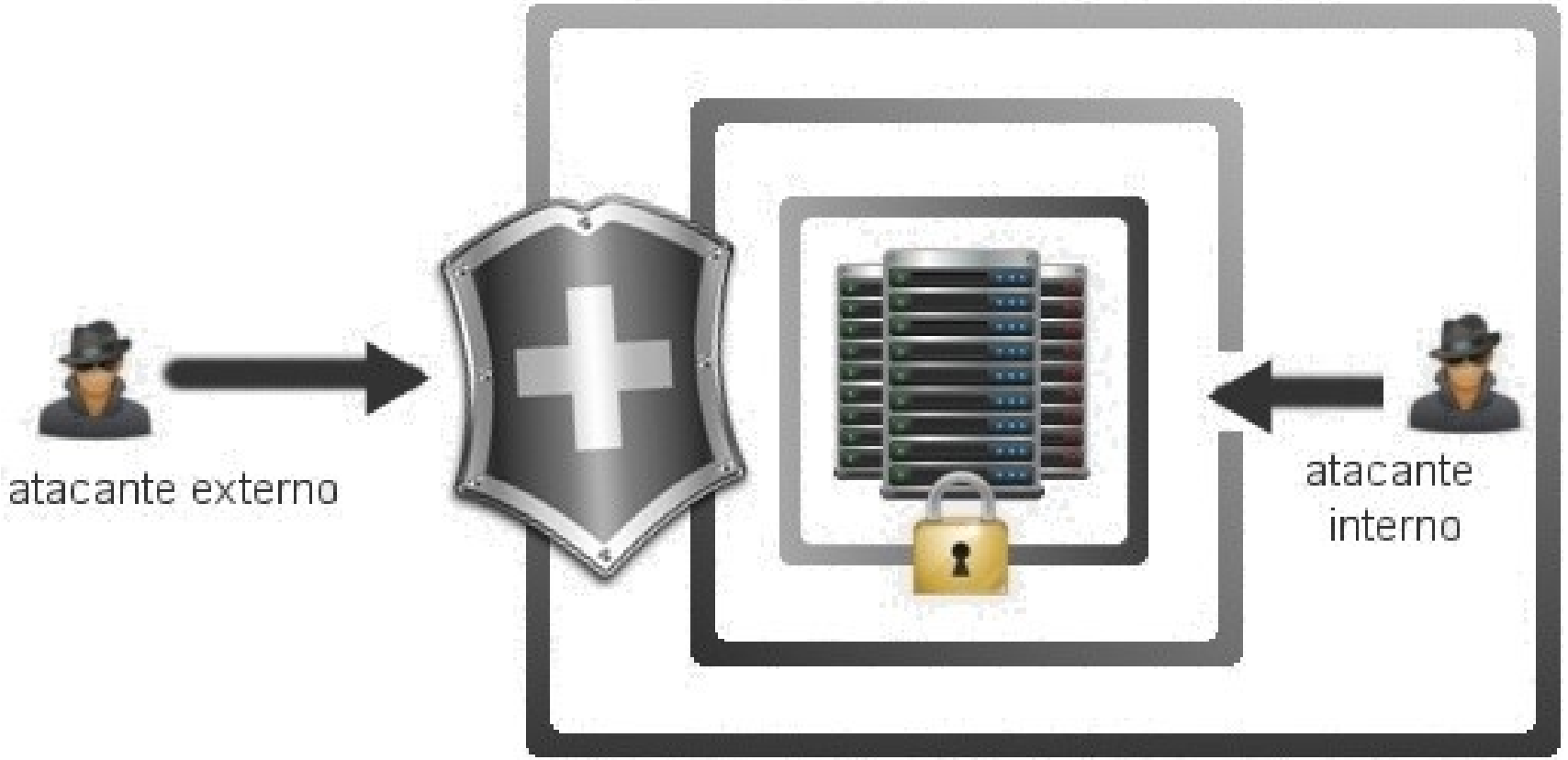
GARANTIZAR

Tipo de Hackers

ETAPAS

1. Definición del alcance
2. Descubrimiento y Exploración
3. Análisis de vulnerabilidades
4. Intrusión
5. Presentación de Informes

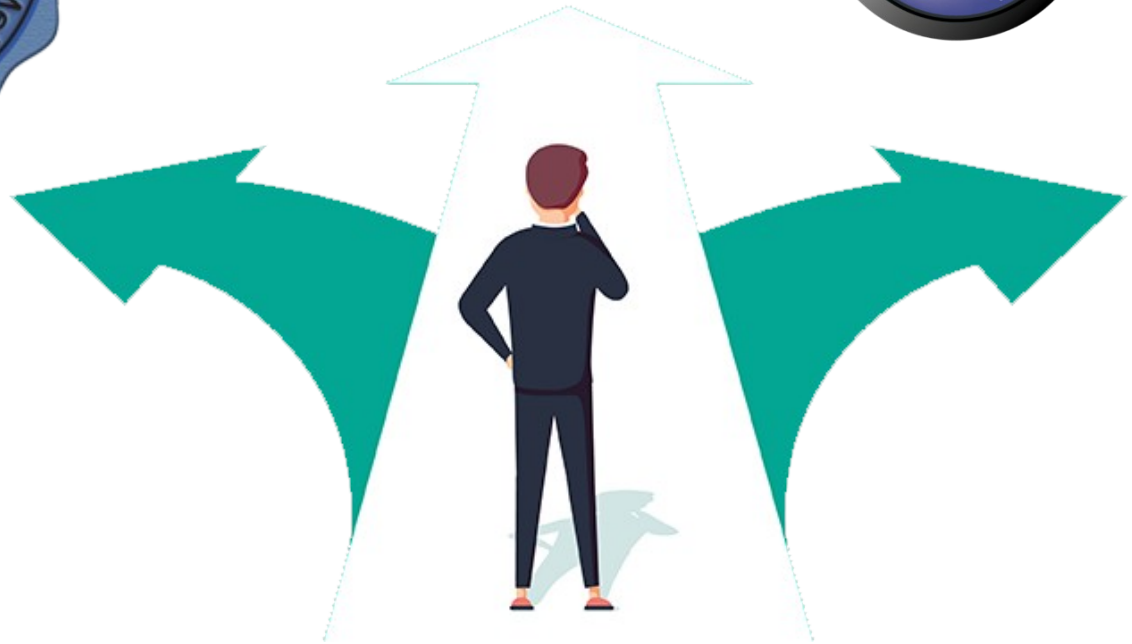
Tipo de amenazas



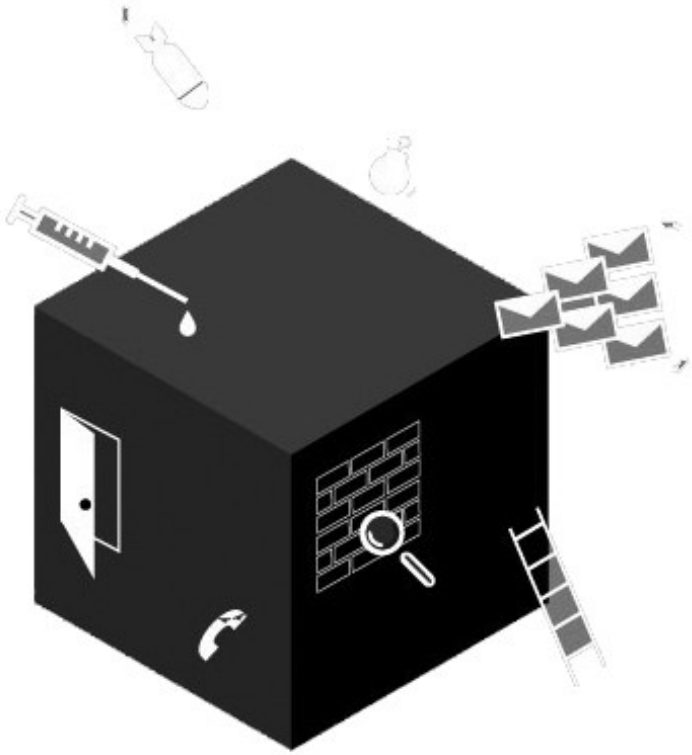
Definición del alcance

Se definen objetivos tales como Pool de direcciones IP Públicas, nombre de dominio, URL, Organización, escenarios, metodologías, herramientas, etc.

METODOLOGÍAS



TIPO DE PRUEBAS



BLACK BOX

GRAY BOX

WHITE BOX

DESCUBRIMIENTO Y EXPLORACIÓN

Descubrimiento y Exploración

Se realizan tareas a fin de recabar datos asociados al objetivo mediante el uso de herramientas y técnicas de recolección de información (Information Gathering).

Por donde empezar?

Descubrimiento

Obtener la mayor cantidad de información del objetivo.

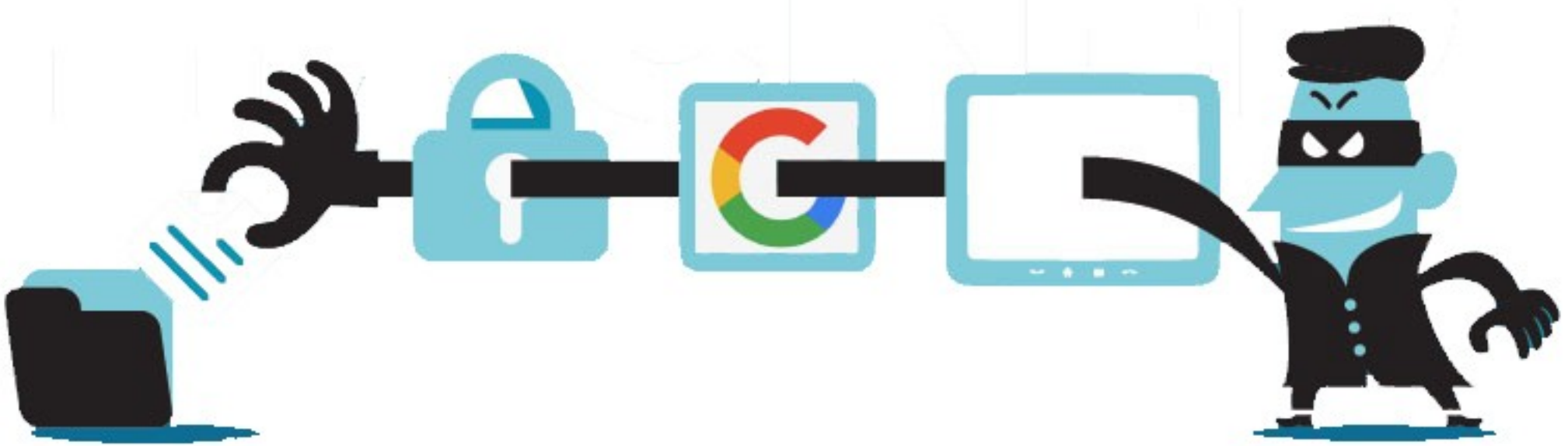
Herramientas de acceso público

- Motores de búsqueda
- Sitio Institucional del Objetivo

HACKING CON GOOGLE

Los “dorks” o “google dorks” son técnicas utilizadas para realizar filtros a través del motor de búsqueda de google, el principal objetivo consiste en obtener resultados mas acotados y obtener en algunos casos información que podría no encontrarse resguardada de manera apropiada.

HACKING CON GOOGLE



SITIOS WEB CON INFORMACION PUBLICA

- SHODAN
- ARCHIVE.ORG
- NETCRAFT
- REDES SOCIALES
- PILP
- WHOIS

METADATOS

ExifTool

NAVEGACION DEL SITIO WEB

Secure | view-source:https://[redacted]

```
            theme: "light",
            lang: "en",
            customStylesheetID: "genesys_widgets_custom",
            plugins: [
                  "cx-webchat",
                  "cx-webchat-service",
                  "cx-send-message",
                  "cx-send-message-service",
                  "cx-search",
                  "cx-knowledge-center-service",
                  "cx-chat-deflection",
                  "cx-channel-selector",
                  "cx-stats-service",
                  "cx-call-us",
                  "cx-sidebar"
            ]
      },
      webchat: {
          <!--  dataURL: "http://10.20.27.110:9080/genesys/2/chat/chat-IPS", -->
            dataURL: "https://[redacted]genesys/2/chat/chat-IPS",
            apikey: "",
            userData: {},
            autoInvite: {
                  enabled: true,
                  timeToInviteSeconds: 5,
                  inviteTimeoutSeconds: 30
            },
            chatButton: {
                  enabled: false,
                  openDelay: 1000,
                  effectDuration: 300,
                  hideDuringInvite: true
            },
            uploadsEnabled: false,
            emojis: true
      },
      sendmessage: {
          <!--  dataURL: "http://10.20.27.110:9080/genesys/2/email/SendMessage", -->
            dataURL: "https://[redacted]genesys/2/email/SendMessage",
            apikey: "",
```

[redacted]/concrete/src/noexiste

Not Found

The requested URL /concrete/src/noexiste was not found on this server.

Apache/2.2.15 (CentOS) Server at [redacted] Port 80

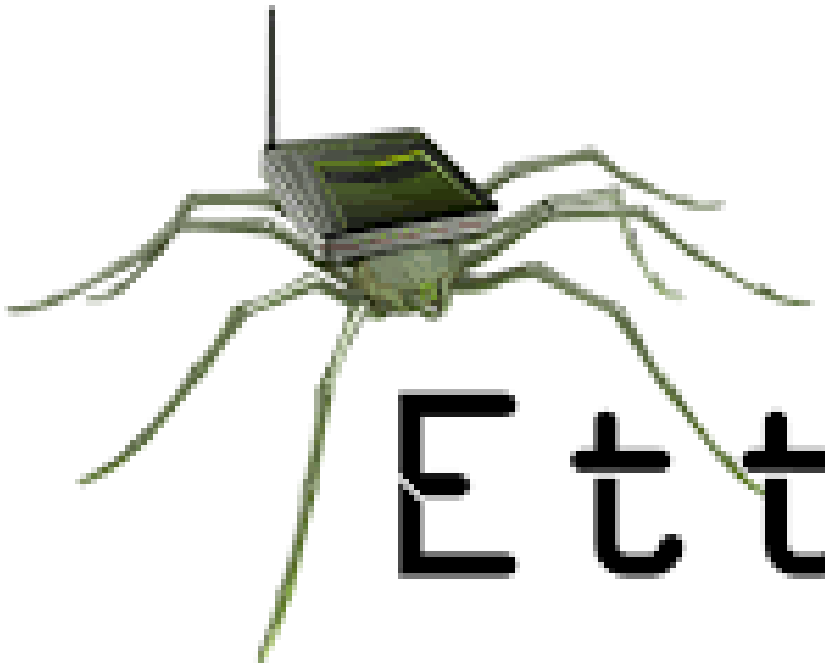
```
root@debi:# printf "GET / HTTP/1.0\r\n\r\n" | nc -v www.i          30
DNS fwd/rev mismatch: w          py != m          /.py
www          y [201.217.50.26] 80 (http) open
HTTP/1.1 200 OK
Date: Tue, 30 Jul 2019 12:44:18 GMT
Server: Apache/2.2.17 (EL)
Last-Modified: Mon, 29 Jan 2018 15:12:34 GMT
ETag: "25000a-56c-563ebacf8bc80"
Accept-Ranges:  none
Content-Length: 1388
Connection: close
Content-Type: text/html; charset=ISO-8859-1
```

Descubrimiento y Exploración

Técnicas

- Ingeniería social
  - Trashing
  - Spam
  - Llamadas telefónicas
- Footprinting
  - Netcraft
  - Archive
  - Pilp
  - Shodan
  - Google Dorks
- Fingerprinting
  - nmap
  - dnsenum

INGENIERIA SOCIAL CON

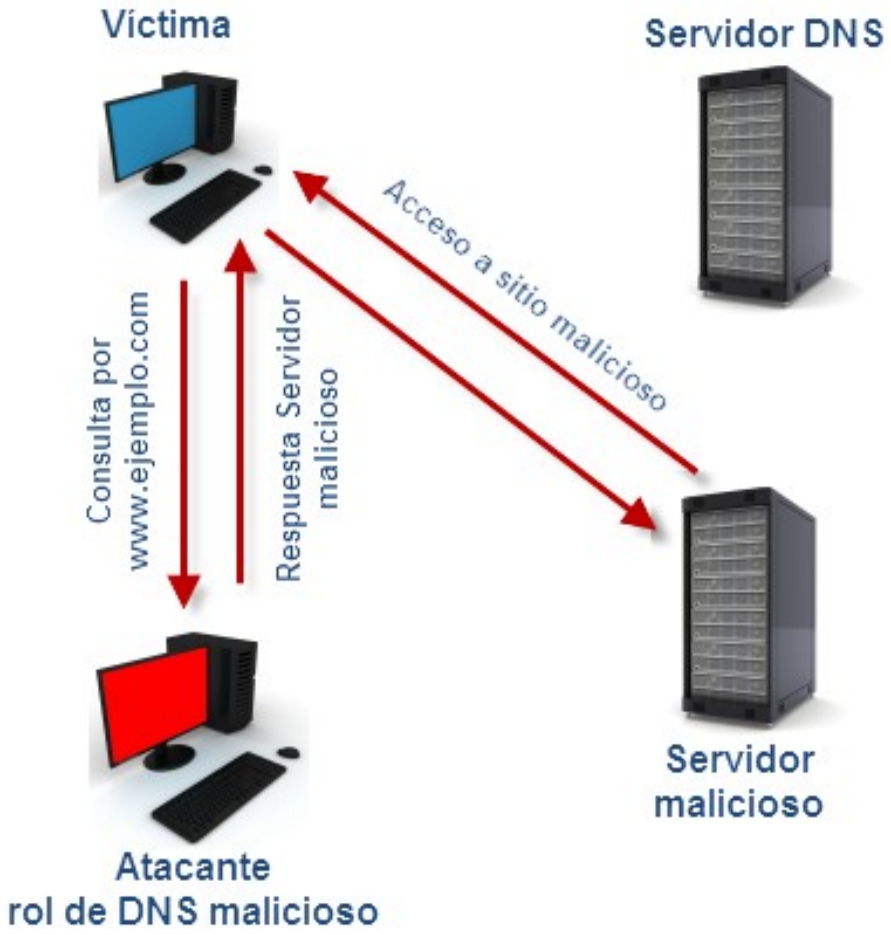


Ettercap

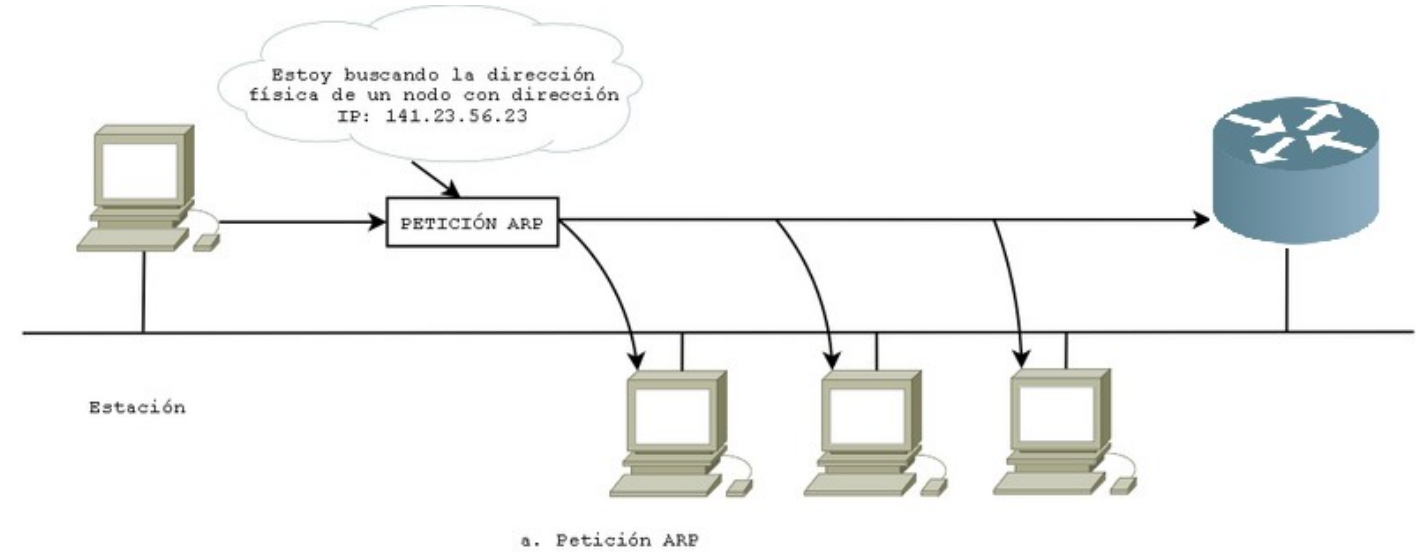
ENVENENAMIENTO ARP | DNS SPOOF | INGENIERIA SOCIAL

DNS CICLO LEGÍTIMO

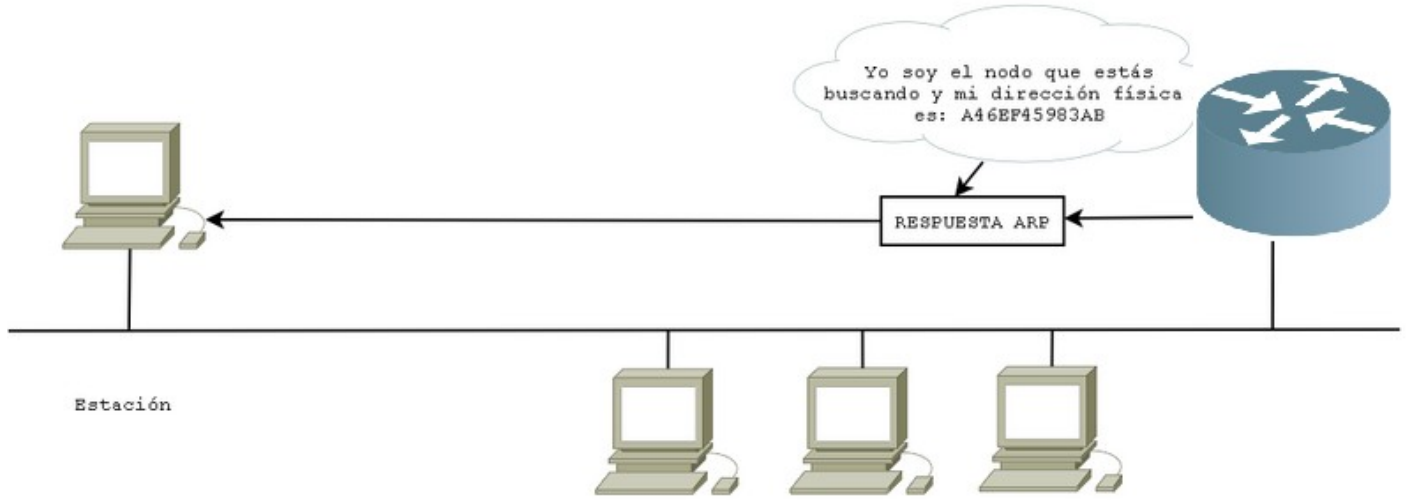
DNS CICLO MALICIOSO



ARP CICLO LEGITIMO

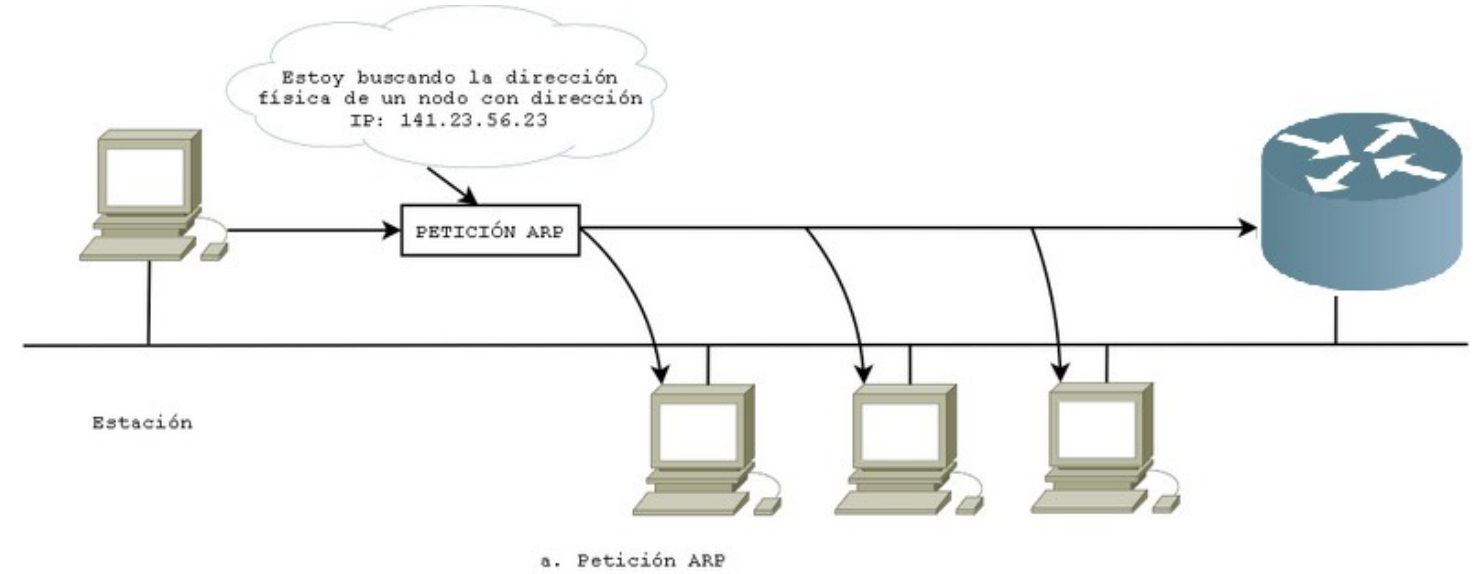


a. Petición ARP



b. Respuesta ARP

ARP CICLO MALICIOSO



a. Petición ARP

b. Respuesta ARP

DEMO