REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

FACULTAD DE CIENCIAS E INGENIERÍAS FÍSICAS Y FORMALES

PROGRAMA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"Implementación de una Infraestructura de Voto Electrónico utilizando Privoxy bajo el esquema TOR (The Onion Routing)"

TESIS PRESENTADA POR EL BACHILLER:

CHRISTIAN ALONSO VEGA CERVANTES,

PARA OPTAR POR EL TÍTULO PROFESIONAL DE

INGENIERO DE SISTEMAS

AREQUIPA-PERÚ

2013

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

AGRADECIMIENTO

A Dios por haberme regalado la vida e irradiar luz en mi camino y permitirme llegar a este momento tan especial de mi vida.

A mi casa de estudio Universidad Católica de Santa María por haberme acogido en sus aulas durante mi formación profesional.

A mis docentes por ser mi guía en la culminación de mis estudios.

Y a mi orientadora **Ing. Karina Rosas** y **Ing. Jorge Martínez** por su dedicación a lo largo del desarrollo de la tesis.

Gracias a la gente que en algún momento me ha hecho perder la cabeza, a los que más tarde me han tenido que ayudar a buscarla, a los que han conseguido que me centre y avance y a todas las neuronas que han quedado en el camino.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

DEDICATORIA

No hay palabras que puedan describir mi profundo agradecimiento hacia mi linda familia, **Juana Cervantes de Vega y José Vega Huayna**, a quienes les dedico este trabajo ya que durante todos estos años confiaron en mí e hicieron posible este momento.

También a mis grandes hermanos que también fueron como mis mejores amigos: **José Luis Vega y Marco Antonio Vega,** por estar a mi lado, apoyándome y aconsejándome.

A Dios por oír mis oraciones todas las noches.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

PRESENTACIÓN

Señor Director del Programa Profesional de Ingeniería de Sistemas.
Señores Miembros del jurado Dictaminador.

De conformidad con las disposiciones del Reglamento de Grados y Títulos del Programa Profesional de Ingeniería de Sistemas, pongo a vuestra disposición el presente trabajo de investigación titulado: **"Implementación de una infraestructura de Voto Electrónico utilizando Privoxy bajo el esquema TOR (The Onion Routing)"** el mismo que de ser aprobado me permitirá obtener el Título Profesional de Ingeniero de Sistemas.

Arequipa, Diciembre del 2012

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

RESUMEN

Cuando surge internet, comienza a ser blanco de ataques, robo de información y de violación a la privacidad, lo cual hoy, es un problema crítico que sufren todas las personas y/o organizaciones por eso la privacidad y la seguridad es un tema muy importante hoy en día, en la actualidad encontramos varios sistemas que nos permiten proteger nuestra privacidad y dar seguridad en nuestra navegación en la internet.

En la seguridad informática se tiene un dicho muy conocido "lo que no está permitido debe estar prohibido" el cual se debe considerar dentro de los términos de seguridad informática.

En este trabajo se hace un recuento de las tecnologías utilizadas para la implementación de una infraestructura de voto electrónico así como también se propone una nueva tecnología para la implementación de éstos sistemas, utilizando Privoxy bajo el esquema TOR (The Onion Routing), como un medio seguro para transmitir información.

Con esto se pretende aportar la suficiente información para quienes deseen conocer acerca del uso de Privoxy y TOR, además de plantear una solución a los problemas de la seguridad en la transmisión de información en redes no seguras.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

ABSTRACT

When there is internet, is becoming targets of attacks, information theft and privacy violation, which today is a critical problem experienced by all individuals and / or organizations for that privacy and security is a major issue today, now found several systems that allow us to protect our privacy and provide security in our internet browsing.

In computer security is a well known saying "what is not allowed to be prohibited" which should be considered in terms of security.

This paper gives an account of the technologies used for the implementation of electronic voting infrastructure as well as new technology is proposed for the implementation of these systems, under the scheme using Privoxy and TOR (The Onion Routing), as a means secure transmitted information.

This is intended to provide enough information for those who want to know about using Privoxy and TOR, and its proposed solution to the problems of security in information transmission in untrusted networks.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

INTRODUCCIÓN

Al transcurrir el tiempo, el mundo de la información a evolucionado y el uso de las computadoras ha ido creciendo debido a su capacidad de volumen de almacenamiento y a su velocidad de procesamiento de información, actualmente se ha logrado que se utilicen sistemas informáticos en casi todos los sectores sociales, empresariales facilitando la vida diaria de las personas e incluso llegando a los gobiernos para colaborar con la democratización de los países.

Es por ello que la intención de éste proyecto es mostrar los principales problemas que se originan en la seguridad de las redes y mostrar una nueva forma de proteger el sistema de voto electrónico hacia éstas amenaza, utilizando Privoxy bajo el esquema TOR como una solución segura.

- CAPÍTULO I:
  Planteamiento Teórico: Se presenta las bases teóricas en donde se detallará las técnicas empleadas en el desarrollo de la metodología.
- CAPÍTULO II:
  Marco Teórico: Muestro el estado de arte relacionado al tema.
- CAPÍTULO III:
  Diseño e Implementación: Muestro la implementación de una infraestructura de voto electrónico utilizando Privoxy bajo el esquema TOR.
- CAPÍTULO IV:
  Evaluación de los Resultados: Presenta los resultados obtenidos así como las diferentes pruebas realizadas.

Para finalizar se muestran las conclusiones, los posibles trabajos futuros y recomendaciones obtenidas luego de realizar el proyecto.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

ÍNDICE

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

CAPÍTULO III: DISEÑO E IMPLEMENTACIÓN

CAPÍTULO IV: EVALUACIÓN DE LOS RESULTADOS

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

ÍNDICE DE FIGURAS

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

ÍNDICE DE TABLAS

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

CAPÍTULO I

PLANTEAMIENTO TEÓRICO

1.1. Título

Implementación de una infraestructura de Voto Electrónico utilizando Privoxy bajo el esquema TOR (The Onion Routing).

1.2. Identificación del Problema

El mundo de la información y la comunicación ha cambiado tanto que el modo en que adquirimos, almacenamos y diseminamos el conocimiento cada vez se parece menos a los modos usados tradicionalmente.

Es por eso que nuestra privacidad y la seguridad de nuestros datos se pueden ver afectadas. Cuantos más datos nuestros estén informatizados, más posibilidades existen que alguien que nosotros no hayamos previsto, pueda tener acceso a los mismos.

En los sistemas de voto electrónico actuales la privacidad, seguridad y confiabilidad del voto es muy importante. Lo que se propone es proteger la privacidad del votante así como también proveer seguridad y confiabilidad del voto electrónico.

Un informe divulgado por la empresa Kaspersky Lab, indica que en el 2010, el número de programas maliciosos diseñados para robar datos personales a usuarios se ha incrementado en más del 100%. Como si esto ya no fuera impactante, el

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

informe agrega que el número de nuevas firmas de Troyanos bancarios introducidos en las bases de datos de Kaspersky Lab ha superado los 25.000 en 2010, cinco veces más que en el 2006. Esto es tan preocupante que las cifras parecen equivocadas. [KPKY20]

1.3. Descripción del Problema

La seguridad y la privacidad ocupan un lugar importante en la vida de todo ciudadano común, con el desarrollo de aplicaciones más sofisticadas donde el usuario debe interactuar muchas horas con el computador ya sea para revisar su correo personal, cuentas bancarias o incluso realizar diferentes tipos de transacciones las cuales son confidenciales y no quieren que sean conocidos por personas extrañas, así como también los proveedores de internet (ISP) los cuales pueden saber exactamente los sitios a los que se conecto es por eso que este trabajo propone el uso de TOR y Privoxy para dar solución a este problema así como dar a conocer otras funciones que serán descritas más adelante.

1.4. Justificación

Esta propuesta pretende dar a conocer las ventajas el utilizar una nueva tecnología, para reducir algunas de las barreras citadas anteriormente en la implementación de una infraestructura de voto electrónico. El trabajo proporciona todos los conocimientos requeridos para aplicar esta nueva tecnología para mejorar la seguridad de aplicaciones que funcionan sobre internet.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

1.5. Objetivos

1.5.1. Objetivo General

Proporcionar una infraestructura utilizando Privoxy bajo el esquema TOR (The Onion Routing).

.

1.5.2. Objetivos Específicos

- Utilizar una tecnología poco conocida la cual asegura la confiabilidad de los datos.
- Garantizar el anonimato de los usuarios en el proceso de emisión del voto.
- Elaborar un esquema que permita utilizar Privoxy bajo el esquema TOR (The Onion Routing) como garantía de seguridad en la implementación de los sistemas de voto electrónico.

1.6. Hipótesis

Actualmente el navegar por la internet no es, para nada, una actividad anónima; prácticamente todo lo que se transmite, consulta o visita puede ser archivado e incluso cuantos más datos nuestros estén informatizados, más posibilidades existen de que alguien que nosotros no hayamos previsto, pueda tener acceso a los mismos, es probable que con el uso de esta nueva tecnología como Privoxy y TOR (The Onion Routing), se logre la navegación del usuario de forma anónima, aumentando el nivel de seguridad y privacidad de los usuarios cuando estos naveguen por la internet.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

1.7. Variables

1.7.1. Independientes

- TOR (The Onion Routing).
- Privoxy.

1.7.2. Dependientes

- Estructura de voto electrónico usando Privoxy bajo el esquema TOR.

Indicadores

- Anonimidad.
- Seguridad y Privacidad.
- Seguridad en el envío de información.

1.8. Alcances y Limitaciones

- La Implementación de una infraestructura de voto electrónico utilizando Privoxy bajo el esquema TOR tendrá fines académicos, por lo que será desarrollado utilizando diferentes herramientas, poniendo énfasis en la seguridad de la transmisión del voto.

1.9. Área Científica

1.9.1 Área: Ciencias físicas.

1.9.2 Línea: Calidad y servicio en redes de datos.

1.10. Tipo y nivel de investigación

1.10.1 Tipo: Aplicada.

1.10.2 Nivel: Descriptivo.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

1.11. Estado de Arte

1.11.1 Título:"TOR sistema de comunicación anónima"

Roger Dingledine -The Free Haven Project.

Objetivos:

- Analiza esta nueva tecnología para su respectivo uso, también se define los posibles usos en que puede ser utilizado y en que campos, así mismo se describe quienes utilizaron esta nueva tecnología por primera vez.

Conclusiones:

- TOR es una nueva tecnología poco conocida así mismo ofrece una seguridad a los datos utilizando un tipo de encriptación.
- Inicialmente utilizada por fuerzas armadas americanas.

Referencia: [TFHP21]

1.11.2 Título:"Seguridad del protocolo de autenticación TOR"

Facultad de ciencias de la computación de la Universidad de Waterloo.

Objetivos:

- Mostrar y analizar los componentes que utiliza la red TOR para proporcionar seguridad en el envío de datos, así mismo, la seguridad de la red TOR se deriva en parte por el hecho de que los diversos nodos en el

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

circuito o red operan en diferentes dominios administrativos.

Conclusiones:

- Se muestra que el protocolo de autenticación de TOR es seguro lo cual se recomienda utilizar TOR para navegar en el internet de forma anónima.

Referencia: [STUW22]

1.11.3 Título:" Las mediciones de rendimiento y estadísticas de Tor Servicios Ocultos"

Simposio Internacional sobre Aplicaciones y Internet.
Karsten Loesing, Werner Sandmann, Christian Wilms y Guido Wirtz Universidad de Bamberg.

Objetivos:

- Ofrecer una visión sobre las mediciones de latencia y obtener un análisis estadístico detallado. De esta manera, podemos obtener información valiosa que nos permiten dar ciertas afirmaciones estadísticos y para sugerir mejoras en el oculto servicio de protocolo y su aplicación.

Conclusiones:

- Se realizó mediciones de rendimiento de los servicios ocultos de Tor y estadísticamente analizados los datos se centran en el tiempo de respuesta como un parámetro importante orientados QoS.
- Por otra parte, se obtuvieron ideas que dieron lugar a recomendaciones sobre cómo mejorar el protocolo de

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

servicio oculto y su aplicación. La investigación adicional incluye el desarrollo de un modelo detallado, basado en las mediciones de los sub-pasos. Dicho modelo podría ser una base para el análisis matemático sofisticado, por ejemplo, a través de teoría de colas o simulación.

Referencia: [MTSO24]

Este análisis de antecedentes ayudó a esclarecer, fortalecer nuestros conceptos y dar a conocer que la tecnología que nosotros vamos a utilizar para dar solución a nuestro problema, proporciona un alto grado de privacidad y confiabilidad a nuestros datos.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

CAPÍTULO II

MARCO TEÓRICO

2.1 Voto Electrónico

En el marco de la automatización de los procesos electorales, significa el paso de los sistemas de votación basados en papel a aquellos sistemas electrónicos de votación (Electronic Voting Systems).

Las elecciones tienen un gran componente de procesos administrativos. En consecuencia, toda administración electoral busca modernizar sus procesos a través de la automatización de sus distintas etapas, tales como la captura de información, la consulta de archivos, los cálculos y la emisión de informes y principalmente la seguridad de dicha captura de información [CHG/1998].

Es necesario precisar que, en sentido estricto, la expresión automatización de los procesos electorales hace referencia a la aplicación de tecnología de procesamiento automático de datos para garantizar la transparencia de las elecciones y acelerar aquellos procesos en los que se manejan grandes volúmenes de datos [CZM/2001].

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

2.2 Oportunidades, riesgos y desafíos del voto electrónico

2.2.1 Oportunidades del voto electrónico

Existen argumentos a favor y en contra de la votación electrónica que justifican el uso de un método u otro. Por un lado, la tecnología para la votación electrónica puede poner en marcha un proceso que permita a las personas con discapacidades el votar por ellas mismas, de manera fácil y en secreto y otra que la votación electrónica permite que los electores voten en un distrito electoral distinto de aquel en que estén registrados, facilitando todo el proceso para quienes solían votar por correo.

2.2.2 Riesgos del voto electrónico a distancia

La intervención no autorizada de terceros en el proceso de votación así como en la etapa actual de la tecnología de la información, no existe garantía de que un programa no puede ser manipulado para permitir el almacenamiento y impresión de un documento diferente del que aparece en la pantalla.

En comparación con los procedimientos convencionales, es más difícil detectar y identificar el origen de los errores y de las fallas técnicas.

2.2.3 Desafíos del voto electrónico remoto

En el contexto del voto electrónico a distancia, se debe prestar especial atención al proceso que garantice el voto libre y secreto. Sólo los electores debidamente acreditados deben ser capaces de ejercer el voto, para lo

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

que su identidad debe ser corroborada por ejemplo, usando un NIP (Número de Identificación Personal-o una firma digital), al tiempo que se verifica que tenga derecho al voto. En un sistema de voto electrónico a distancia debe existir una distinción electrónica entre el voto y la identificación del votante. [SVES01]

2.3 EXPERIENCIAS INTERNACIONALES DE VOTO ELECTRÓNICO [GOBA03]

2.3.1. ALEMANIA

Alemania comenzó las pruebas de voto electrónico como proyecto piloto en 1999. Se implemento en las universidades (Osnabruck, Bermerhaven), a nivel local de asesoramiento (jóvenes de la comunidad y los consejos de la tercera edad), así como en los consejos de empleados públicos y privados.

2.3.2. INDIA

Desde 1998, la Comisión Electoral utilizó cada vez más máquinas de votación electrónica (MVE) en los centros de votación. En 2003, todas las elecciones estatales y elecciones secundarias se llevaron a cabo utilizando MVE. Animado por esa experiencia la comisión ha decidido utilizar solamente MVE para las elecciones de la Lok Sabha (Cámara Baja) de 2004.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

2.3.3. BRASIL

En las elecciones de 2000 y 2002 más de 400 mil máquinas de votación electrónica fueron utilizadas a nivel nacional en Brasil y los resultados fueron contados electrónicamente en cuestión de minutos después del cierre de las urnas.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

2.4 Países latino americanos y legislación referida al voto electrónico

PAÍS	¿EXIGE PAPELETA O BOLETA ELECTORAL?	¿PROHÍBE LA VOTACIÓN ELECTRÓNICA?	¿HACE REFERENCIA AL VOTO ELECTRÓNICO?
ARGENTINA	Uso de boletas. Reglamentarita.	No	No refiere.
BOLIVIA	Uso de boletas. Reglamentarita.	No	No refiere.
BRASIL	Uso de boletas.	No	El artículo 103 del código electoral señala el uso de cédulas de votación. El último inciso, sin embargo, deja abierta la posibilidad de utilizar mecanismos diversos, a condición de que se asegure el secreto del voto. Brasil promueve un mecanismo electrónico denominado «urna electoral».

COLOMBIA	Uso de boletas.	No	No refiere específicamente. Sin embargo, el artículo 58 del Código Electoral señala que «el gobierno procederá a tecnificar y sistematizar el proceso electoral especialmente en lo relacionado con la actualización de los censos, expedición de documentos de identificación, preparación y desarrollo de las elecciones.
CHILE	Uso de boletas.	No	No refiere.
ECUADOR	Uso de papeletas.	No	No refiere.
HONDURAS	Uso de papeletas.	No	No refiere
PANAMÁ	No hace referencia a papeletas. Cada elección se define el mecanismo.	No	No refiere
PERÚ	Uso de boletas. Reglamentaria.	No	No refiere

PARAGUAY	Reglamentaria en cuanto a los pasos de votación. Se da por descontado el uso de cédulas.	No	No refiere. Sin embargo, ya ha tenido una experiencia de votación electrónica en el año 2003 mediante ánfora electrónica.

Tabla 2.1 Legislación Referida al Voto Electrónico
Fuente: Elaboración propia

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

2.5 Nuevas formas de votación

2.5.1 Sistemas de voto electrónico mediante aparatos situados en los colegios electorales

Estos sistemas incorporan aparatos que se instalan en los colegios electorales. El votante sigue desplazándose hasta allí físicamente y cuenta con la asistencia y control del personal del recinto de votación. Esto implica que la etapa de identificación, autentificación y validación seguirá realizándose se forma convencional.

2.5.2 Esquema que utiliza canales anónimos

Se trata también de un esquema bastante seguro pero a la vez un poco complejo. Se intenta salvaguardar la identidad del votante ocultando el origen de los mensajes que recibe el servidor (igualmente, el votante debe poder identificarse mediante algún tipo de autorización emitida previamente).

Con este sistema ya se han realizado diversas experiencias piloto para aprobar su utilidad entre ellas, hay que destacar la de universidad Autónoma de Barcelona, en marzo de 2002.

2.6 Privoxy

Privoxy (Junkbuster Privacy Enhanching Proxy) es un filtro de contenido sencillo, hace mucho tiempo, existía la Internet Junkbuster, de codificadores anónimo y la corporación Junkbuster. Esto ahorró a muchos usuarios un gran dolor en los

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

primeros días de publicidad en la web y el seguimiento del usuario.
La versión 2.0.2, publicada en 1998, era (y es) la última versión oficial disponible de Corporations Junkbuster. Afortunadamente, había sido liberado bajo la GNU GPL, lo que permitió un mayor desarrollo de los demás [PR16]. Así Stefan Waldher comenzó el mantenimiento de una versión mejorada del software, para que con el tiempo un número de personas que contribuyeron a la creación de parches.

Ya podría reemplazar pancartas con una imagen transparente, y tuvo una primera versión, pero sigue siendo muy estrecha basada en el original, con todas sus limitaciones, tales como la falta de apoyo HTTP/1.1, flexible por configuración del sitio, o la modificación de contenidos. La última versión de este esfuerzo fue la versión 2.0.2-10, publicada en el 2000.

Privoxy funciona como proxy web, tiene capacidades avanzadas de filtrado para proteger la privacidad, modificar el contenido de las páginas web, administrar cookies, controlar accesos y eliminar anuncios, banners, ventanas emergentes y otros elementos indeseados del internet.

Privoxy tiene una configuración muy flexible y puede ser personalizado para adaptarse a las necesidades y gustos individuales. Privoxy es útil tanto para sistemas aislados como para redes multiusuario. Privoxy está basado en el programa Internet Junkbuster y está publicado bajo la licencia pública general GNU. Se ejecuta en Linux, Windows, Mac OS X, Amiga OS, BeOS y en muchas versiones de Unix. Casi cualquier navegador debería ser capaz de usar Privoxy con un mínimo de cambios. La versión estable más reciente es la 3.0.12. Una lista

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

de reglas para Privoxy bastante popular era la Neilvandyke. Acción de Neil Van Dyke, que cuenta con aproximadamente 7.500 reglas.

El uso de Privoxy en combinación con TOR alrededor del mundo para sortear la censura en internet en países como Irán, Arabia Saudita, los Emiratos Árabes Unidos y en China, para evitar el sistema de censura de Internet del gobierno chino llamada Gran Cortafuegos. Bajo estas restricciones, muchos sitios web resultan bloqueados por sus respectivos gobiernos incluyendo muchas redes sociales. [RPS17]

Ahora mencionaremos algunos del equipo Privoxy:

- ✓ Fabián Keil,
- ✓ David Schmidt.
- ✓ Hal Burgis.
- ✓ Mark Miller.
- ✓ Gerry Murphy.
- ✓ Lee Rian.
- ✓ Roland Rosenfeld,

Figura 2.1 Símbolo de Privoxy

Fuente: http://www.privoxy.org/

2.6.1 ¿Por qué se recomienda el uso de Privoxy?

Privoxy es sin duda una buena opción, especialmente para aquellos que quieren un mayor control y seguridad. Los

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

que tienen la voluntad de leer la documentación y la capacidad de ajustar su instalación serán los más beneficiados. Una de las fortalezas de Privoxy es que es altamente configurable que le da la capacidad de personalizar por completo la instalación.

Conocer, o al menos que tenga un interés en aprender sobre HTTP y otros protocolos de red, HTML, y "expresiones regulares" será una gran ventaja y nos ayudará a sacar el máximo partido de Privoxy.

2.6.2 ¿Cómo funciona Privoxy?

Privoxy es un proxy que se centra principalmente en la mejora de la privacidad, publicidad y la eliminación de basura y liberando al usuario de las restricciones impuestas a sus actividades. Sentado entre su navegador e Internet, que se encuentra en una posición perfecta para filtrar la información de salida personal que su navegador tiene fugas, así como basura entrante.

Utiliza una variedad de técnicas para hacer esto, todos los cuales están bajo su control total a través de los archivos de configuración y opciones. Al ser un proxy también hace más fácil compartir configuraciones entre varios navegadores y/o usuarios. [MP19]

2.6.3 Surgimiento de Privoxy a partir de Junkbuster

Aunque obsoleto, Junkbuster Corporations continúa ofreciendo su versión original de la Junkbuster de

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

Internet, por lo que publicar este software Junkbuster-derivadas de conformidad con el mismo nombre que llevó a la confusión. También hay posibles complicaciones legales del uso del nombre Junkbuster, que es una marca registrada de Junkbuster Corporations, sin embargo, no hay objeciones por parte de Junkbuster Corporations al proyecto Privoxy sí mismo, y que, de hecho, todavía comparten sus ideales y metas. Los desarrolladores creen que hay muchas mejoras sobre el código original y que es el momento de hacer una ruptura con el pasado y hacer un nombre por derecho propio.

Privoxy es el "Proxy Privacidad Mejora". Además, su modificación y supresión de contenido basura que da para el usuario permite tener más control, más libertad, y le permite navegar por la web.

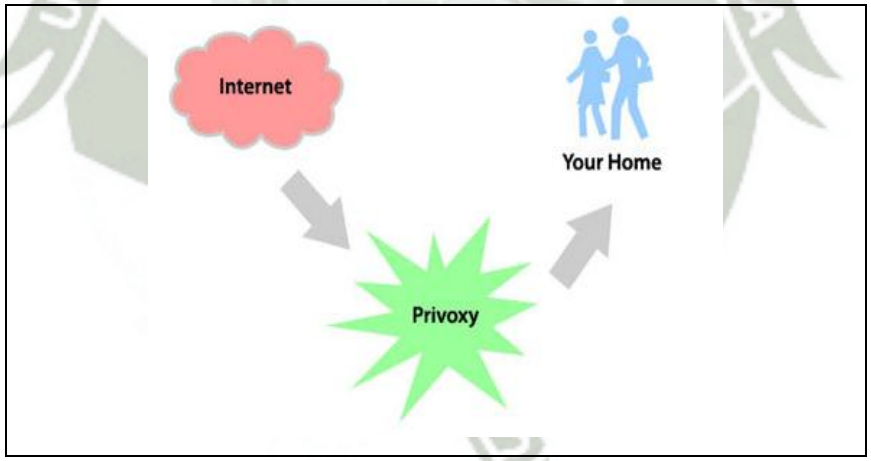


Figura 2.2 Diagrama de diseño con Privoxy

Fuente: http://www.privoxy.org/

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

2.6.4 Diferencias entre Privoxy y Junkbuster

Privoxy comienza donde Junkbuster lo dejó. El nuevo Privoxy aún bloquea anuncios y banners así mismo ayuda a proteger la privacidad. Sin embargo, la mayoría de estas características se han mejorado, y muchas otras nuevas se han añadido, todos en el mismo sentido. Algunas características de Privoxy incluyen:

- ✓ Compatible con IPv6, siempre que el sistema operativo lo hace también, y el script de configuración detecta.
- ✓ Se puede ejecutar como "interceptar" proxy, lo que evita la necesidad de configurar los navegadores de forma individual.
- ✓ Página web de filtrado (reemplazos de texto, elimina banners basados en el tamaño, invisibles "Web bugs" y molestias HTML, etc.)
- ✓ Soporte para Perl expresiones regulares compatibles con los archivos de configuración, y una sintaxis de configuración más sofisticada y flexible.

2.6.5 ¿Privoxy se puede ejecutar como un servidor en una red?

Sí, Privoxy se ejecuta como un servidor y puede ser fácilmente configurado para "servir" a más de un cliente.

2.6.6 Filtros

Privoxy distingue entre filtros y ficheros de acciones. Los filtros incluyen reglas, como una regla para eliminar banners de más de cierto tamaño. Los ficheros de acciones asocian reglas a direcciones. Estas pueden ser desde url a

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

comodines que representen fragmentos de direcciones pertenecientes a páginas de anuncios.

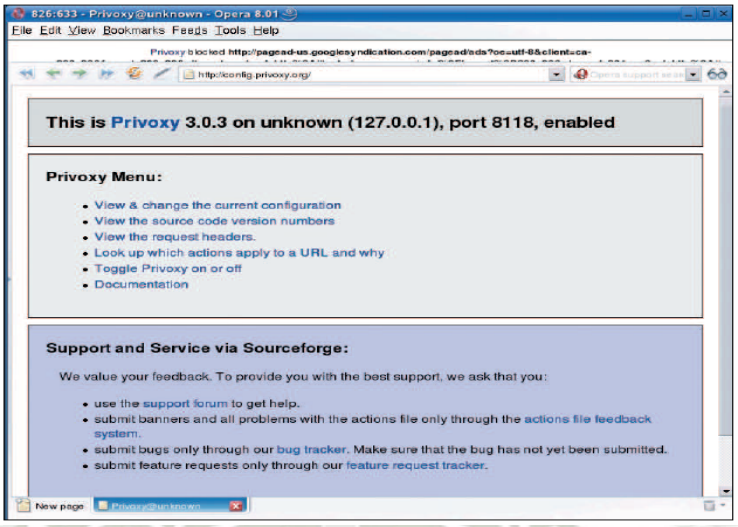


Figura 2.3 Ventana principal de Privoxy

Fuente: http://www.privoxy.org/

Privoxy es bastante discreto en el uso diario y apenas afectó a los tiempos de carga, incluso a las páginas grandes.

El programa mostrará la mayoría de los sitios web correctamente, incluso si se aplica la configuración de filtro Cautious. Si no, se puede ejecutar el comprobador de url que indica que reglas se aplican a la página actual. Desafortunadamente, el comprobador carece de una estructura clara, dejando al usuario con el problema de encontrar la regla responsable de bloquear su vista. [MGLF18]

2.7 Proxy

2.7.1 Definición de Proxy

Un proxy es un ordenador que intercepta las conexiones de red que un cliente hace a un servidor de destino existen

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

diferentes tipos de proxies con diferentes protocolos, como el proxy de FTP. Proxy patrón de diseño también es un patrón de diseño (programación) con el mismo esquema que el proxy de red.

Como se ve, proxy tiene un significado muy general, aunque siempre es sinónimo de intermediario.

VENTAJAS

- ✓ **Control**: Sólo el intermediario hace el trabajo real.
- ✓ **Ahorro**: Por tanto, sólo uno de los usuarios (el proxy) ha de estar equipado.
- ✓ **Velocidad:** el proxy puede hacer caché: guardar la respuesta de una petición para darla a otro usuario cuando la pida.
- ✓ **Filtrado:** El proxy puede negarse a responder.
- ✓ **Modificación:** Como intermediario, un proxy puede falsificar información.
- ✓ **Anonimato:** Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos.

DESVENTAJAS

- ✓ **Abuso**: Al estar dispuesto a recibir peticiones de muchos usuarios y responderlas.
- ✓ **Carga**: Un proxy ha de hacer el trabajo de muchos usuarios.
- ✓ **Intromisión**: Es un paso más entre el origen y destino, y algunos usuarios pueden no querer pasar por el proxy.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

- ✓ **Incoherencia**: Si hace de caché, es posible que se equivoque.
- ✓ **Irregularidad**: El hecho de que el proxy represente a más de un usuario da problemas en muchos escenarios, en concreto los que presuponen una comunicación directa entre un emisor y un receptor como TCP/IP.

2.7.2 Proxy de web / Proxy cache de web

Se trata de un proxy para una aplicación específica como acceso a la web. Aparte de la utilidad general de un proxy, proporciona una caché para las páginas web y los contenidos descargados, que es compartida por todos los equipos de la red.

2.7.3 Proxies transparentes

Un proxy transparente combina un servidor proxy con NAT (Network Address Translation) de manera que las conexiones son direccionadas dentro del proxy sin configuración por parte del cliente, y habitualmente sin que el propio cliente conozca de su existencia. Este es el tipo de proxy que utilizan los proveedores de servicios de internet (ISP).

2.7.4 Reverse Proxy / Proxy inverso

Un reverse proxy es un servidor proxy instalado en el domicilio de uno o más servidores web. Todo el tráfico entrante de Internet y con el destino de uno de esos servidores web pasa a través del servidor proxy. Hay varias razones para instalar un “reverse proxy”, ventajas seguridad, cifrado y distribución de carga.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

2.7.5 Proxy NAT (Network Address Translation)

Otro mecanismo para hacer de intermediario en una red es el NAT (Network Address Translation) conocida como enmascaramiento de IPs. Es una técnica mediante la cual las direcciones fuente o destino de los paquetes IP son reescritas, sustituidas por otras (de ahí el "enmascaramiento").

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

2.8 Comparación de Privoxy, Proxy otros

	Privoxy	**Proxy**	**FreeProxy**	**AnalogX Proxy**	**Squid**
Características	Para aquellos que quieren un mayor control y seguridad. Es altamente configurable. La configuración se puede hacer con un navegador Web	Intercepta las conexiones de red. El más famoso es el servidor proxy web. Proxy (patrón de diseño) donde tiene sentido un intermediario.	Permite crear usuarios y grupos. Posee filtro de contenidos y url. Restringe acceso a grupo de sitios por usuarios, importa listas (url o IP) de prohibición, emite 4 tipos de informes de accesos y visitas a sitios.	Simple, pequeño, y fácil de usar. Se puede registrar sin costo. Datos seguros entre un servidor Proxy y un cliente.	Tiene mecanismo de autentificación y control de acceso (por IP, por usuario y por periodo). Posee web-caché. Funcionamiento sobre plataformas Linux y Windows. Filtrado de contenidos (por palabras y páginas

					web). Restricción de acceso a sitios de red.
Desventajas		Recibe peticiones de muchos usuarios. Es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente.	El manual sólo se encuentra en inglés.		No permite uso de modo transparente en Windows. Hay que configurar el uso del Proxy en cada cliente.

Requerimientos	Windows 98/ME/NT /2000/XP	Windows 98/ME/NT /2000/XP	Windows (98, NT, 2000, XP and Server 2003).	Windows (Windows 98 /ME/NT/ 2000/ XP).	Windows 2000 Professional y Server, XP Professional, 2003 Server, Vista, 2008 Server. Antivirus actualizado.
Especificación Técnica	Licencia: Gratis (GPL) Idiomas: Inglés Tamaño: 270 KB		Licencia: Gratis (GPL) Idiomas: Inglés Tamaño:4,16MB	Licencia: Gratis (GPL) Idiomas:Inglés Tamaño:270KB	Licencia: Gratis (GPL) Idioma: Inglés Tamaño: 3,85 MB

Tabla 2.2 Comparación de Privoxy, Proxy otros

Fuente: Elaboración propia

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

2.9 TOR (The Onion Routing)

Es una implementación libre de un sistema de encaminamiento llamado Onion Routing que permite a sus usuarios comunicarse en Internet de manera anónima. Originado en el US Naval Research Laboratory y hasta noviembre de 2005 patrocinado por la Electronic Frontier Foundation(EFF), TOR es desarrollado por Roger Dingledine y Nick Mathewson junto con otros desarrolladores. [TFHP21]

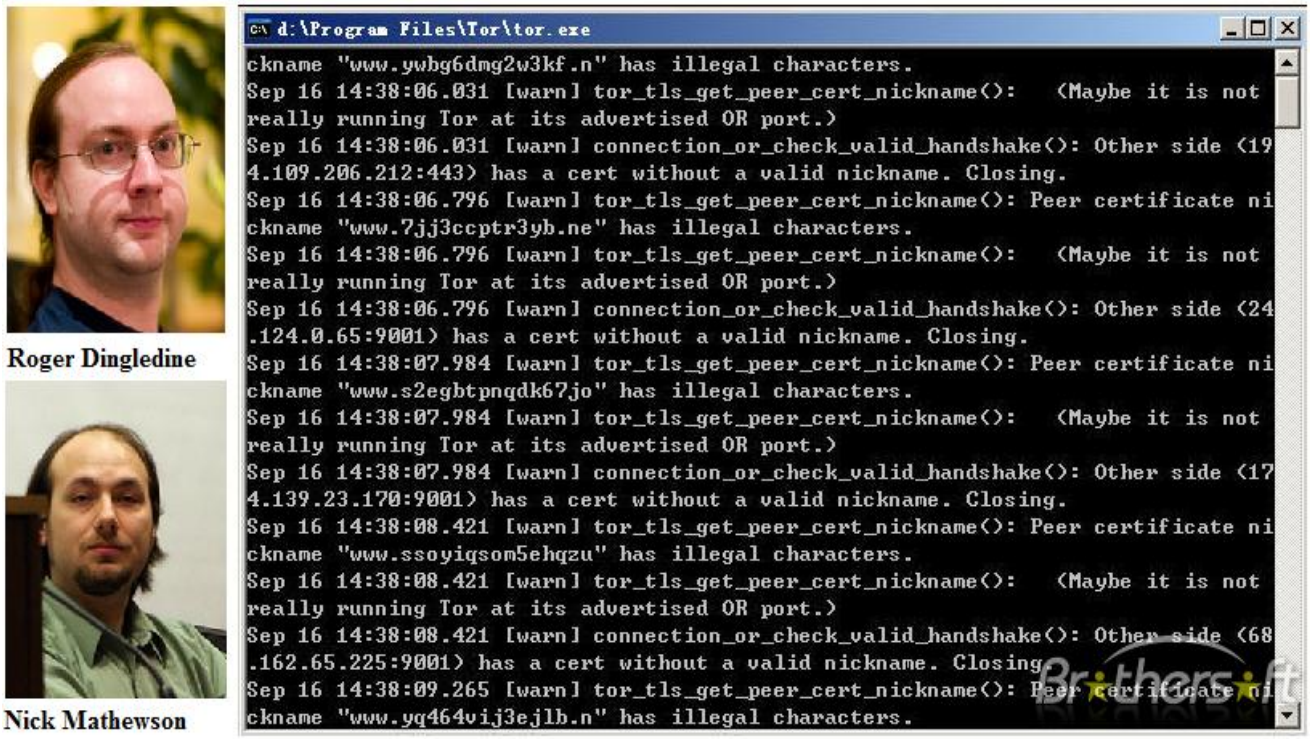


Figura 2.4 Autores de TOR (The Onion Routing)
Fuente: Elaboración propia

Es una red de túneles virtuales que permiten a las personas mejorar su privacidad y seguridad en internet. La EFF (Electronic Frontier Foundation) lo usa para mantener las libertades civiles activas en internet. Uno puede navegar por diversos sitios sin dejar huella. Como lo usa tanto el ejército como los civiles por igual, no se puede calcular que cantidad de tráfico generado por el uno o el otro.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

TOR provee un canal de comunicación anónimo y está diseñado para ser resistente a ataques de análisis de tráfico (trafico análisis). Por lo tanto, usando TOR es posible realizar una conexión a un equipo sin que éste o ningún otro tengan posibilidad de conocer el número de IP de origen de la conexión. [RSNB13]

TOR es usualmente combinado con Privoxy para acceder a páginas web de forma anónima y segura. Privoxy es un proxy HTTP diseñado para proteger la privacidad en la navegación por el Internet. La interfaz de TOR es un proxy SOCKS (usa el puerto 9050).

Es importante saber que TOR no es 100% fiable en lo que se refiere al cifrado de la información. Su función principal es asegurar el anonimato del usuario, de forma que no se pueda rastrear la información que envía.

Grupos como Indymedia recomiendan TOR para salvaguardar la privacidad de sus miembros y seguridad en línea. Grupos activistas como Electronic Frontier Foundation (EFF) recomiendan TOR como un mecanismo para mantener las libertades civiles online.

Corporaciones usan TOR como una forma segura de realizar un análisis competitivo, y para proteger documentación sensible de espías. También lo usan para reemplazar las tradicionales VPN (Red Privada Virtual), que revelan la cantidad exacta y el momento de la comunicación[SGMI08].

Una rama de la Marina de los EE.UU. usa TOR para reunir información de inteligencia, y uno de sus equipos usó TOR durante en el Medio Oriente recientemente. Las fuerzas del orden utilizan TOR para visitar sitios web sospechosos sin dejar direcciones IP del gobierno en sus registros web, y para la seguridad durante las operaciones.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

2.9.1 ¿Por qué necesitamos TOR?

Usar TOR te protege contra una forma habitual de vigilancia en Internet conocida como "análisis de tráfico". El análisis de tráfico puede ser utilizado para deducir quién está hablando a quién sobre una red pública.

Conocer el origen y el destino de su tráfico de Internet permite a otros seguir el rastro de tu comportamiento e intereses. Puede incluso amenazar tu trabajo y seguridad física revelando quién y dónde se encuentra.
Por ejemplo, si usted viaja al extranjero y te conectas al computador de tu empresa para revisar o enviar correo, puedes revelar inadvertidamente tu nacionalidad y tu afiliación profesional a cualquiera que vigile la red, incluso si la conexión está cifrada. [ACPM10]

TOR hace uso también de la criptografía para eso hay dos técnicas muy habituales para cifrar el contenido de un mensaje, denominadas asimétrica y simétrica. La primera está formada por dos claves distintas, una pública y otra privada. La pública la puede tener cualquier persona, y la privada solo la tienen personas autorizadas.

Ambas pueden cifrar y descifrar un mensaje, pero si cifro el mensaje con una clave, solo puedo descifrarlo con la otra clave. Supongamos que cifro un mensaje con la clave pública, si intento descifrar el texto cifrado con la clave pública, no obtendré nada, aparte de números y letras sin sentido; necesito la clave privada para descifrar el mensaje. Esto es reversible, es decir, también puedo cifrar un mensaje con la privada, pero solo podré descifrarlo con la pública. [STUW22]

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM
UNIVERSIDAD CATÓLICA DE SANTA MARÍA

¿Qué consigo con esto? Pues depende de cómo utilices las claves. Si utilizo la pública para cifrar y la privada para descifrar, tengo confidencialidad, solo el destinatario puede averiguar el contenido del mensaje. Pero si utilizo la privada para cifrar y la pública para descifrar, obtengo la autenticación del remitente y la integridad del mensaje, ya que solo la persona que dispone de la clave privada me ha podido enviar el mensaje. La criptografía simétrica utiliza solo una clave tanto para cifrar como para descifrar. Pero, ¿Qué tiene que ver la criptografía con TOR? Mucho. [MCHM07]

Como ya se ha dicho que para que el anonimato sea práctico, tengo que satisfacer varios requerimientos. El primero es la integridad del paquete y el segundo es asegurar la identidad del servidor. Para asegurar estos dos requerimientos, TOR se basa en un modelo de redes telescópicas o redes de cebolla de segundo orden.

Empecemos: las cebollas. Algunos se han preguntado por qué el símbolo de TOR es una cebolla, no es porque todos los desarrolladores sean vegetarianos, sino porque las cebollas tienen capas.

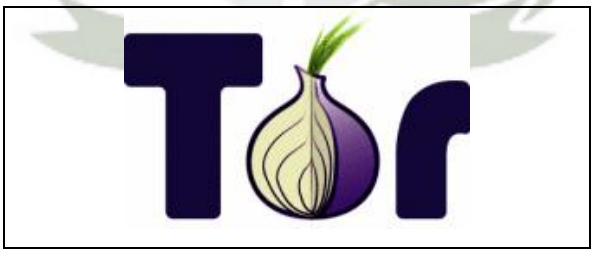


Figura 2.5 Símbolo TOR (The Onion Routing)
Fuente: https://www.torproject.org/

Una cebolla está formada por el núcleo y capas externas. En el campo de las redes de anonimato, el núcleo de la cebolla es el

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM
UNIVERSIDAD CATÓLICA DE SANTA MARÍA

paquete TCP, y las capas externas son envoltorios cifrados con clave simétrica. Es decir, supongamos que quiero hacer una petición de conexión a un servidor web, y que me conecto por TOR. Para proteger el paquete TCP, el cliente que se conecta a TOR genera *n* capas, siendo *n* el número de servidores intermedios por el cual pasará nuestro paquete de datos.

2.9.2 Ejemplo de la funcionalidad de TOR

Cada capa ha sido creada con una clave simétrica negociada entre cada servidor intermedio y el cliente. Una vez que el cliente ha generado la cebolla, se envía a través de la conexión TOR, y empieza a recorrer los diferentes servidores intermedios. Cada capa de la cebolla es "pelada" por el servidor intermedio correspondiente a medida que la cebolla va pasando por los servidores intermedios, de manera que la puerta de salida genera el paquete TCP original y se le envía al servidor que hospeda la página web. Veamos la siguiente imagen de redes cebolla para entenderlo mejor:

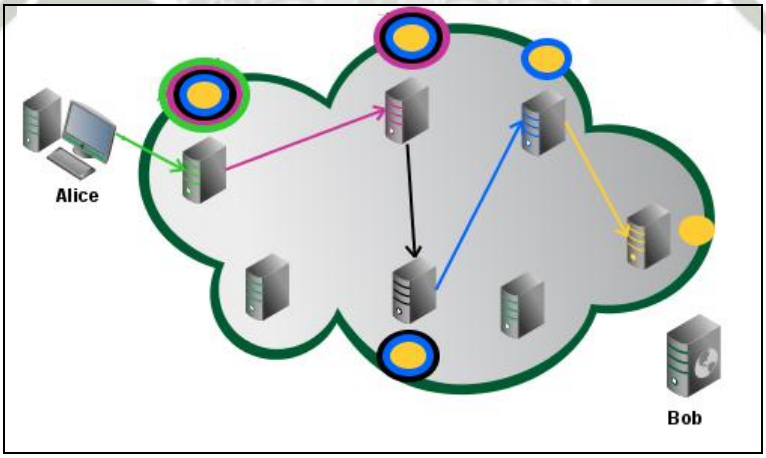


Figura 2.6 Red TOR 1 (The Onion Routing)
Fuente: https://www.torproject.org/

Alice es el cliente, la nube representa la red TOR y los ordenadores que están dentro de ella representan los servidores

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

intermedios. Podemos observar que Alice inicia la conexión con la puerta de entrada, que está coloreada de verde, Alice primero consulta a todos los servidores intermedios que va a utilizar el medio para acordar una clave simétrica con cada uno de ellos, y una vez que tiene todas las claves simétricas, genera la cebolla.

Después la envía y cada servidor intermedio retira la capa correspondiente. Al final del camino, el servidor coloreado de amarillo obtiene el paquete TCP original.

El funcionamiento es el siguiente. Primero conecto con la puerta de entrada, negocio con ella una clave y la utilizo para usarla como clave de sesión.

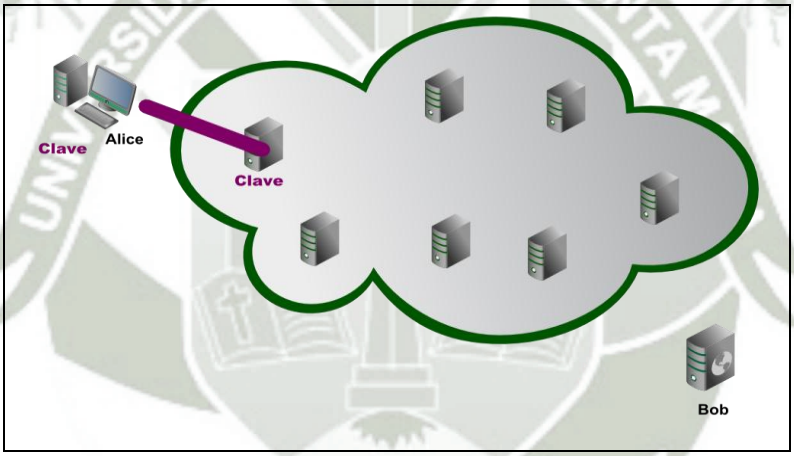


Figura 2.7 Red TOR 2 (The Onion Routing)
Fuente: https://www.torproject.org/

Después, con la conexión establecida, conecto a través de ésta con otro servidor, negocio la clave, y creo otro canal de comunicación anidado en el primero.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

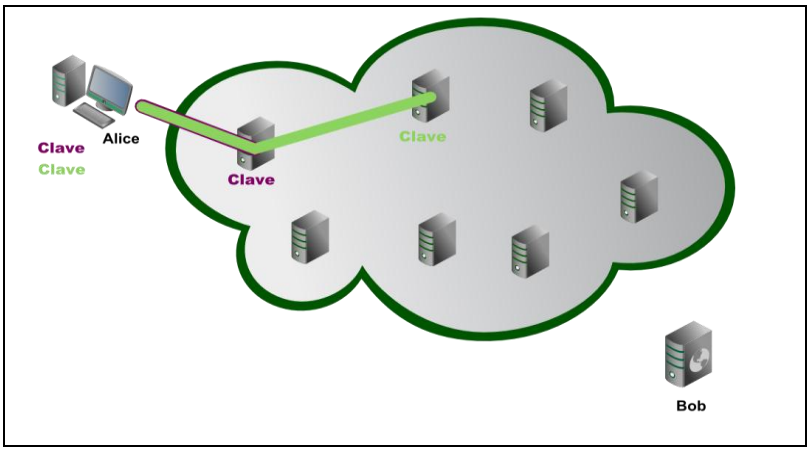


Figura 2.8 Red TOR 3 (The Onion Routing)
Fuente: https://www.torproject.org/

Así sucesivamente hasta que llego a la puerta de salida, la cual envía al servidor que hospeda la página web (Bob) el paquete TCP, sin saber la identidad de Alice, ya que solo conoce la identidad del servidor anterior a él.

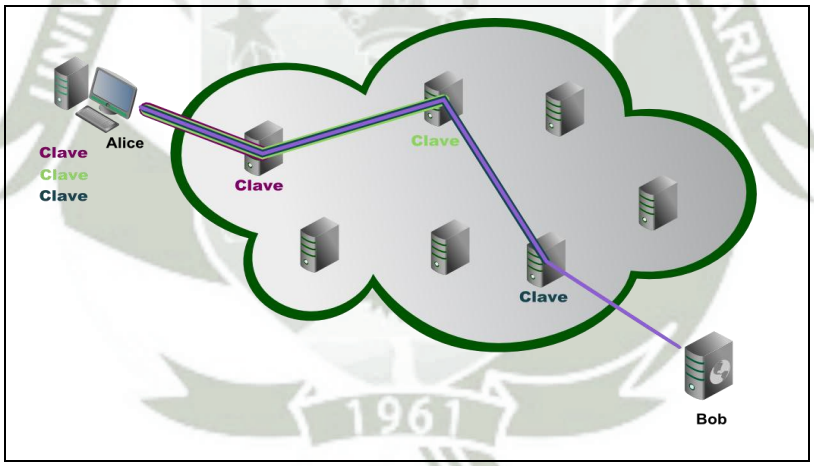


Figura 2.9 Red TOR 4 (The Onion Routing)
Fuente: https://www.torproject.org/

El esquema de la red telescópica, por tanto, crea un canal seguro sobre el que mandar los paquetes TCP. Este canal seguro está protegido por una clave simétrica generada entre el servidor intermedio correspondiente y el cliente. Ahora ¿Cómo se crean las conexiones? La respuesta nos la da el protocolo de seguridad

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

TLS. TLS (transporte layer security) es la evolución del protocolo SSL (secure sockets layer).

Estos dos protocolos aseguran canales de comunicación sobre Internet mediante claves simétricas. A través de este protocolo, genero un túnel entre dos servidores sobre el que envió la información. Es decir, TOR utiliza el protocolo TLS para establecer la conexión entre los diferentes servidores todavía falta una cosa bastante importante la autoridad de directorio.

Una autoridad de directorio es una base de datos que almacena todas las direcciones de todos los re-transmisores. En este momento hay seis autoridades de directorio, lo que forma una base de datos distribuida. Supongamos que tengo la base de datos y hay tres clientes que quieren acceder a ella, el servidor se empieza a sofocar, pero, ¿y si en vez de tres son trescientos? Puede que el servidor colapse.

Para evitarlo, se duplicó la base de datos y descentralizó el sistema, de tal forma que los trescientos se repartan entre los seis servidores. Eso es una base de datos descentralizada. Por tanto, el cliente accede a la autoridad de directorio, consulta la base de datos y crea el circuito TOR.

Por ejemplo: Imaginemos que una persona reside en un país cuyo gobierno censura ciertos sitios web. Quieres visitar esos sitios, porque crees que hay información útil almacenada en ellos, pero no puedes acceder porque tu gobierno opina que no debes hacerlo. Si conoces TOR, lo podrías usar, pero ¿y si el gobierno ha bloqueado totalmente la red TOR? ¿Lo pueden hacer? Sí, y de hecho numerosos gobiernos lo hacen actualmente.

Si alguien quiere bloquear TOR, solo tiene que bloquear el acceso a las autoridades de directorio, ya que sin las direcciones de los re-transmisores, no podemos construir un circuito TOR.

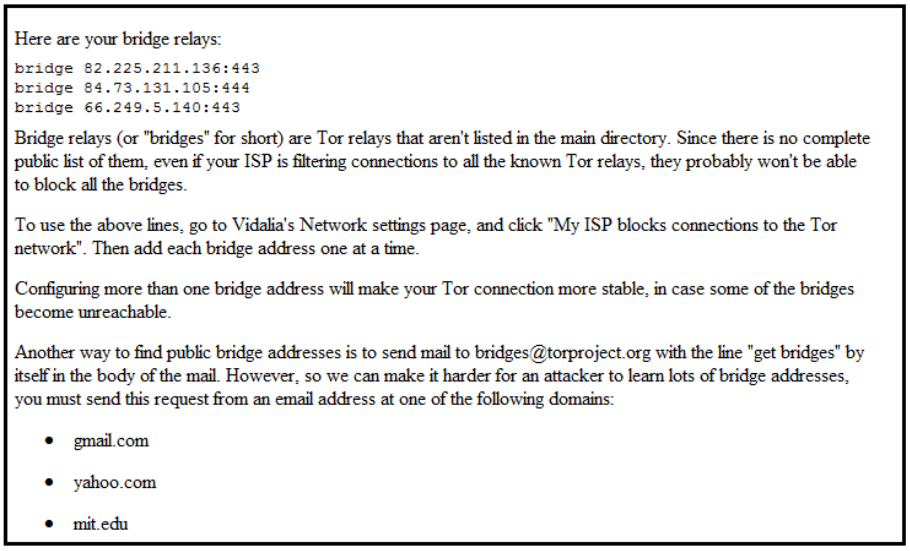
Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

Por tanto, si quiero evitar el bloqueo de TOR, tengo que buscar una alternativa a las autoridades de directorio: los bridges relays.

Los bridges relays son re-transmisores que no están listados en las autoridades de directorio. [ZJWY06]



Here are your bridge relays:

```
bridge 82.225.211.136:443
bridge 84.73.131.105:444
bridge 66.249.5.140:443
```

Bridge relays (or "bridges" for short) are Tor relays that aren't listed in the main directory. Since there is no complete public list of them, even if your ISP is filtering connections to all the known Tor relays, they probably won't be able to block all the bridges.

To use the above lines, go to Vidalia's Network settings page, and click "My ISP blocks connections to the Tor network". Then add each bridge address one at a time.

Configuring more than one bridge address will make your Tor connection more stable, in case some of the bridges become unreachable.

Another way to find public bridge addresses is to send mail to bridges@torproject.org with the line "get bridges" by itself in the body of the mail. However, so we can make it harder for an attacker to learn lots of bridge addresses, you must send this request from an email address at one of the following domains:

- gmail.com
- yahoo.com
- mit.edu

Figura 2.10 Algunos bridges relays
Fuente: https://www.torproject.org/

2.9.3 Servicios Ocultos

TOR también posibilita a los usuarios el ocultar su localización mientras ofrecen varias clases de servicios, tales como publicación web o un servidor de mensajería instantánea. Usar TOR "puntos de encuentro", otros usuarios de TOR pueden interconectarse a estos servicios ocultos sin conocer la identidad del otro de la red. Esta funcionalidad de servicio oculto permite a los usuarios de TOR configurar un sitio web donde la gente puede publicar material.

Aunque la característica más popular del TOR es facilitar anonimato a usuarios finales, puede también proporcionar

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

anonimato a servidores. Usando la red TOR, es posible a los servidores anfitrión ocultarse para que su localización y quienes los usen sean desconocidas. Estos servicios usan una dirección .onion en vez de otro TLD existente. A pesar de que no existe un seguimiento de estos sitios, algunos servidores proporcionan direcciones útiles. [DALJ15]

2.9.3.1 Servicios ocultos o de ubicación oculta

Ya vimos como logra un usuario conectado a TOR ser anónimo para el servicio (Bob) al que accede. Pero, ¿qué pasa si es Bob el que desea permanecer anónimo? Para esto existen los servicios ocultos o de ubicación oculta (location-hidden services). Mediante un servicio oculto, es posible ofrecer un servidor en la red TOR sin una IP que lo identifique, con la desventaja de que es necesario accederlo a través de TOR.

Cómo funcionan:
Supongamos que Bob quiere ofrecer un servidor web anónimo. Después de la configuración, TOR genera una par de claves pública/privada que identifican al servicio. Con la clave pública, genera un digest, que forma parte de la dirección del servicio ejemplo: l73fuoioj5hzznxc, junto con el pseudo dominio de nivel superior (pseudo TDL) .onion, dando como resultado la dirección por la que se accede al servicio: [XLNW11]

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

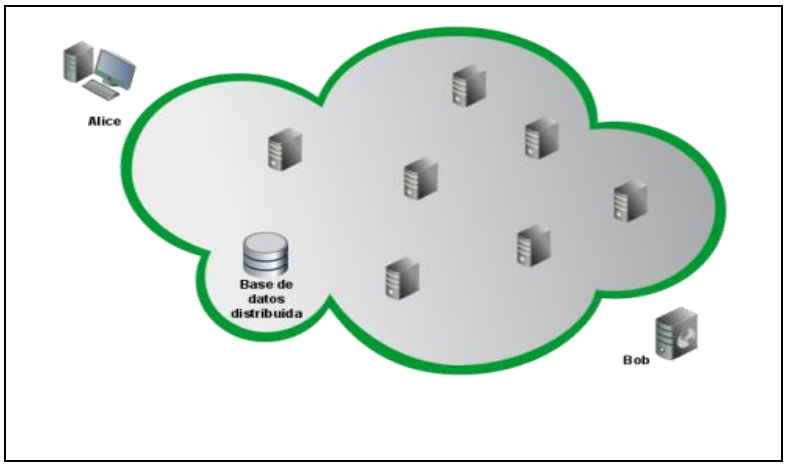


Figura 2.11 Red TOR 5 (The Onion Routing) inverso
Fuente: https://www.torproject.org/

Para lograr un alto desempeño del servicio en la red TOR, el primer paso es elegir, aleatoriamente, un grupo de routers de cebollas (Onion routers) para que sirvan de puntos de introducción y generar circuitos TOR (o sea, de 3 saltos, encriptados) a cada uno de ellos.

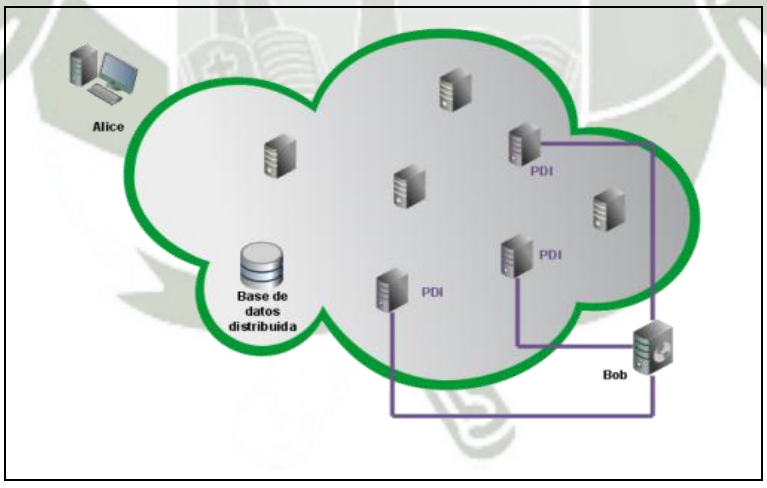


Figura 2.12 Red TOR 6 (The Onion Routing) inverso
Fuente: https://www.torproject.org/

El segundo paso es crear un descriptor del servicio, que incluye: la dirección .onion, el/los puertos por los que se accede al

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

servicio, una descripción opcional y la dirección, y firmado con la clave privada.

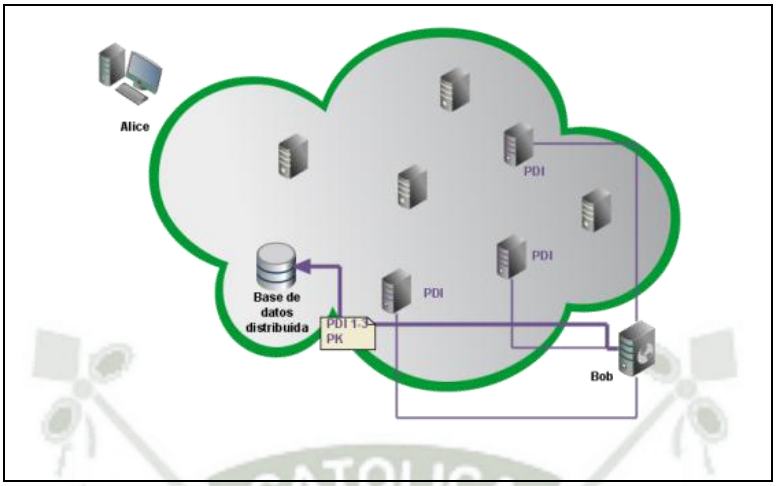


Figura 2.13 Red TOR 7 (The Onion Routing) inverso
Fuente: https://www.torproject.org/

Ahora un cliente (Alice) desea conectarse al servicio. Asumimos que ya conoce la dirección, tal vez porque la vio en un índice de servicios ocultos o Bob se la dijo. Como tercer paso, Alice descarga el descriptor del servicio de la base de datos distribuida y obtiene la dirección de los puntos de introducción.

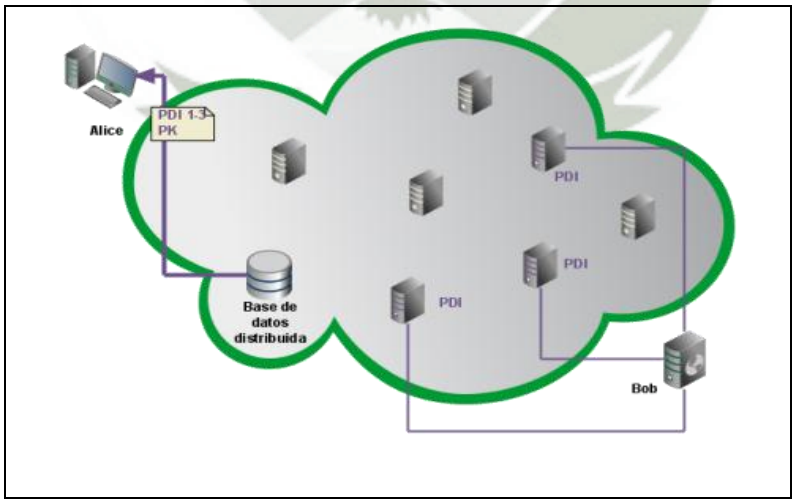


Figura 2.14 Red TOR 8 (The Onion Routing) inverso
Fuente: https://www.torproject.org/

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

Para el cuarto paso Alice ha creado un circuito TOR hasta un nodo cualquiera, pidiéndole que actúe como punto de encuentro.

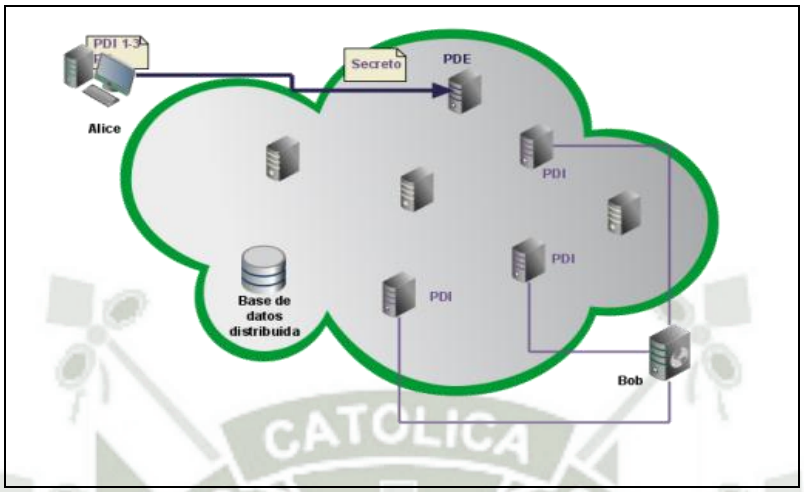


Figura 2.15 Red TOR 9 (The Onion Routing) inverso
Fuente: https://www.torproject.org/

Quinto paso: Ahora Alice crea un mensaje de introducción, encriptado con la clave pública del servicio oculto, que incluye la dirección del punto de encuentro y el secreto de un sólo uso, y le pide a alguno de los puntos que lo envíe al servicio oculto.

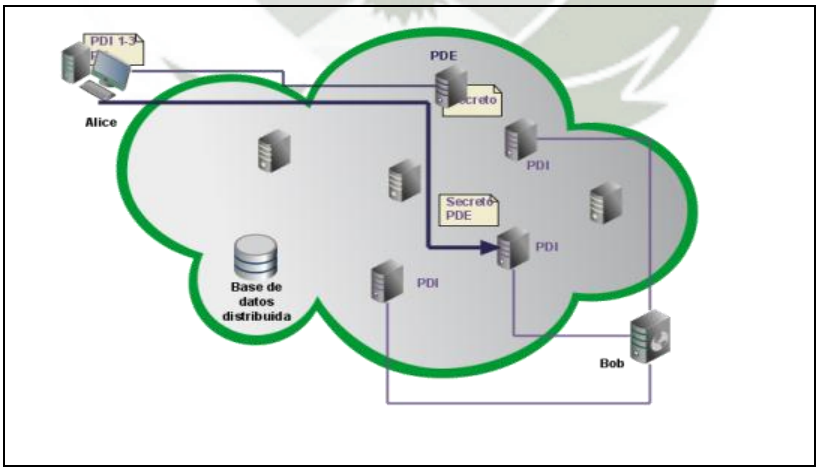


Figura 2.16 Red TOR 10 (The Onion Routing) inverso
Fuente: https://www.torproject.org/

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

En el sexto paso el servicio oculto desencripta el mensaje y obtiene la dirección del punto de encuentro y el secreto.

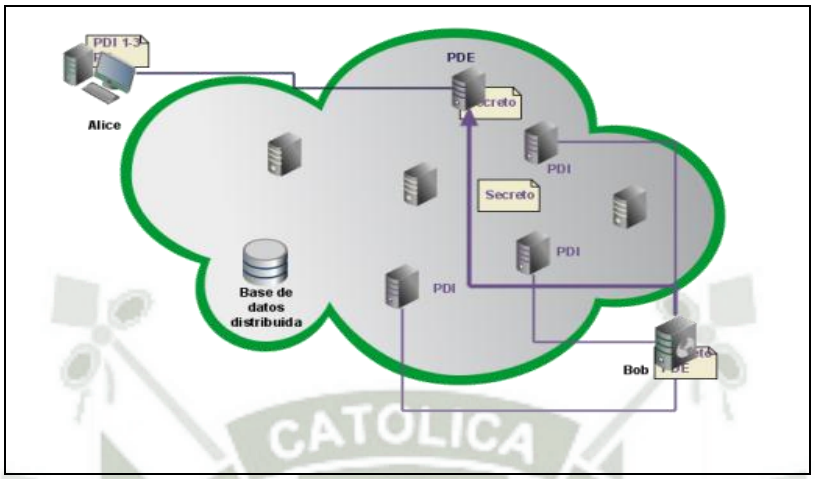


Figura 2.17 Red TOR 11 (The Onion Routing) Inverso
Fuente: https://www.torproject.org/

En el séptimo y último paso, el punto de encuentro notifica a Alice la conexión establecida y ambos pueden empezar a comunicarse a través de sus circuitos TOR de manera normal. El punto de encuentro simplemente reenvía los paquetes.

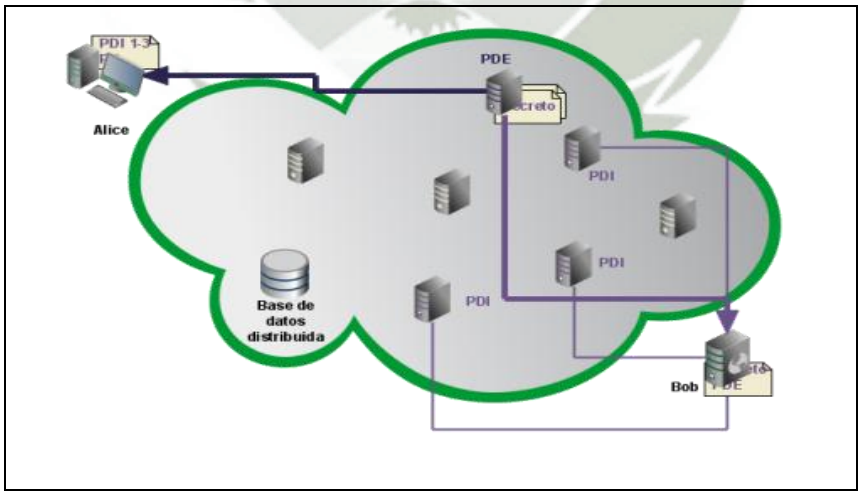


Figura 2.18 Red TOR 12 (The Onion Routing) inverso
Fuente: https://www.torproject.org/

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

Es importante aclarar que los puntos de introducción no son usados en la comunicación final para evitar que un sólo re-transmisor sea completamente responsable del servicio oculto.

2.10 Permaneciendo anónimo

TOR no puede solucionar todos los problemas de anonimato. Se centra únicamente en proteger el transporte de datos. Es necesario utilizar el software de apoyo específico del protocolo si no se quiere que los sitios que visita para ver su información de identificación. Por ejemplo, puedes utilizar proxy web como Privoxy mientras navegas para bloquear cookies y ocultar información sobre su tipo de navegador.

2.11 El futuro de TOR

Proporcionar una red de anonimato usable en la Internet hoy en día es un desafío permanente. Queremos que TOR que satisfaga las necesidades de los usuarios. También queremos mantener la red en funcionamiento de manera que maneje la mayor cantidad de usuarios posibles. Seguridad y facilidad de uso no tiene que estar en contradicción a medida que aumenta la usabilidad de TOR, ello atraerá más usuarios, lo que aumentará las posibles fuentes y destinos de cada comunicación, aumentando así la seguridad para todos.

2.12 A quienes protege TOR

a) Se protege sus comunicaciones de las empresas irresponsables. Todo a través de Internet, TOR se está recomendando a las personas recién preocupadas por su privacidad frente a la creciente violación y robo de los datos privados.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM
UNIVERSIDAD CATÓLICA DE SANTA MARÍA

b) Se protege a sus hijos en línea. Usted ha dicho a sus hijos que no deben compartir la información de identificación personal en línea, pero se pueden compartir su ubicación, simplemente por no ocultar su dirección IP.

2.13 Quienes utilizan TOR

1) Los militares usan TOR

- **Servicios Ocultos:** Cuando el Internet fue diseñado por el DARPA, su propósito principal era ser capaz de facilitar la distribución, comunicación robusta en el caso de las huelgas locales. Sin embargo, algunas funciones deben ser centralizadas, como los sitios de mando y control.
- **Reunión de Inteligencia:** El personal militar utiliza los recursos electrónicos de ejecución y seguimiento de los insurgentes. Ellos no quieren que el servidor web registra en un sitio web insurgentes para registrar una dirección militar, revelando así la vigilancia.

2) Los Periodistas

- Los periodistas ciudadanos en China utilizan TOR para escribir acerca de eventos locales para fomentar el cambio social y la reforma política.

3) Los oficiales de la policía usan TOR

- **Línea de vigilancia:** TOR permite a los funcionarios navegar por sitios web cuestionables sin dejar pistas reveladoras.
- **Operaciones Sting:** Del mismo modo, el anonimato permite a los agentes del orden a participar en línea "encubierta" de operaciones.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

4) Activistas denuncian irregularidades y el uso de TOR

- Activistas de derechos humanos usan TOR para reportar anónimamente los abusos de zonas de peligro. A nivel internacional, los derechos laborales de los trabajadores el uso de TOR y otras formas de guardar el anonimato en línea y sin conexión para organizar a los trabajadores de conformidad con la Declaración Universal de los Derechos Humanos. A pesar de que están dentro de la ley, no significa que sean seguros. TOR proporciona la capacidad para evitar la persecución sin dejar de levantar la voz.

- Human Rights Watch recomienda TOR en su informe, "competencia a la baja. Complicidad corporativa en la censura de Internet en China" El coautor del estudio, entrevistó a Roger Dingledine, líder del proyecto TOR, sobre el uso de TOR. Cubren TOR en la sección sobre la manera de romper el "Gran Firewall de China", y recomiendan que los trabajadores de derechos humanos en todo el mundo utilicen TOR para la navegación segura y las comunicaciones. "[SNS14]

- En el este de Asia, algunos sindicalistas utilizan el anonimato para revelar información sobre talleres clandestinos que producen bienes para los países occidentales y la organización de mano de obra local.

- TOR puede ayudar a los activistas y evitar la censura del gobierno o las empresas que dificulta la organización. En uno de esos casos, un proveedor canadiense bloqueó el acceso a un sitio web de la unión utilizados por sus propios empleados para ayudar a organizar una huelga.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

5) Los ejecutivos de negocios que usan TOR

- **Mantener las estrategias de forma confidencial:** Un banco de inversión, por ejemplo, no puede ser que desee fisgones de la industria para poder seguir lo que los sitios web de sus analistas están observando. La importancia estratégica de los patrones de tráfico, y la vulnerabilidad de la vigilancia de estos datos, está empezando a ser más ampliamente reconocido en varias zonas del mundo de los negocios.

- **Responsabilidad:** En una época en que la actividad empresarial irresponsable y no declarada ha socavado las empresas miles de millones de dólares, un ejecutivo de la administración quiere que todo el personal se sienta libre de divulgar la malversación interna. TOR facilita la rendición de cuentas interna antes de que se convierta en denuncia.

6)Los bloggers usan TOR

- Con frecuencia oímos hablar de los bloggers que son demandados por decir las cosas perfectamente legales en línea, en su blog.Se recomienda el FEP guía legal para bloggers.

- Global voices mantiene una guía de los blogs anónimos con Word press y TOR.

7) Profesionales de TI usan TOR

- **Para comprobar las normas IP basadas en Firewall:** Un firewall puede tener algunas políticas que sólo permiten ciertas direcciones IP o rangos. TOR se puede utilizar para

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

verificar las configuraciones utilizando una dirección IP fuera del bloque asignado de la empresa de investigación.

- **Para omitir sus propios sistemas de seguridad para la profesión:** Por ejemplo, una empresa puede tener una política estricta con respecto a los empleados el material se puede ver en Internet. Una revisión del registro revela una posible violación. TOR se puede utilizar para verificar la información sin excepción de su puesta en sistemas de seguridad de la empresa.

- **Para conectar de nuevo a los servicios implementados:** Un ingeniero de red puede usar TOR para conectarse de forma remota de nuevo a los servicios, sin la necesidad de una máquina externa y la cuenta de usuario, como parte de las pruebas operativas.

2.14 Propiedades de TOR

➢ Es una red sobrepuesta sobre Internet

La topología de TOR consiste en una cantidad de re-transmisores TOR (también llamados enrutadores de cebollas, nodos u OR), administrados por voluntarios, que mantienen conexiones TSL (sobre TCP/IP), permanentemente entre sí, para formar esta red.

➢ Protege contra ataques de análisis de tráfico

El objetivo de TOR, determinado por su modelo de amenazas, es proteger contra el análisis de tráfico.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

Básicamente, TOR dificulta que un atacante actuando como cliente descubra el destino de una conexión, que un atacante actuando como servidor descubra el origen de una conexión, y que un grupo de re-transmisores vinculen al cliente con los destinatarios de sus conexiones.

- **Promueve activamente la facilidad de uso**

Los desarrolladores de TOR enfatizan la facilidad de uso del sistema como medida para aumentar el anonimato.

- **Es multiplataforma**

Existen versiones tanto para los sistemas operativos GNU/Linux, los derivados de BSD, Mac OS X, y Windows (2000, XP, Vista, 7 y las Server Editions). Esta variedad de plataformas soportadas ayuda a que crezca la base de usuarios.

- **Está ampliamente documentado**

Tiene muy buena documentación, actualizada y variada y en diversos idiomas. Los protocoles intervinientes están completamente detallados, y los encargados del proyecto TOR mantienen una biblioteca actualizada de documentos sobre anonimato y seguridad.

2.15 Vulnerabilidades de TOR

Para romper el sistema de anonimato de TOR, hay cuatro grandes caminos que puedes tomar:

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

2.15.1 Inyectar código:

TOR protege al cliente con los servidores intermedios, pero no hay nada que proteja el servidor destino o la puerta de salida. Imaginemos que hay una persona que quiere averiguar las identidades de las personas que visitan una página.

Lo primero que hará será buscar el servidor que aloja la página y controlarlo activa o pasivamente. En definitiva, saber en todo momento lo que ocurre en el servidor para monitorear las peticiones y analizarlas posteriormente.

2.15.2 Analizar la red TOR:

Supongamos que alguien analiza todo el tráfico de la red TOR, y que en base a estudios estadísticos puede determinar que un cliente se ha conectado a un servidor externo por medio de una puerta de salida. ¿Es posible? Sí ¿En serio? Sí, numerosos países y operadoras de telefonía actualmente lo hacen.Se necesita una potencia de cálculo inmensa, aunque es menor si solo se estudian clientes TOR concretos, es decir, aquellos que accedan a unos servidores externos determinados o que pertenezcan a un país determinado.

Como mencionó, se necesita una capacidad de cálculo grande, pero es posible que empresas gigantes, que manejan miles de millones de dólares al año, acudan a esta técnica para revelar la identidad de ciertas personas. La única forma de luchar con este método desemboca en un peligro mayor aumentando la red TOR. Pero si aumentó la red TOR para dificultar las tareas de cálculo, mayor número de re-transmisores no serán confiables. [SAAK12]

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

CAPÍTULO III

DISEÑO E IMPLEMENTACIÓN

3. Objetivo

Proponer una implementación de infraestructura de voto electrónico utilizando Privoxy bajo el esquema TOR sustentando la elección y utilización de diferentes herramientas de anonimato y demostrando como éstas mejoran la seguridad en la navegación.

3.1 Diseño de la Infraestructura

Según lo expuesto anteriormente vamos a proponer un esquema de red que brindará mecanismos de control y seguridad para asegurar los requerimientos de nuestra red. A continuación se ilustra el diseño propuesto.

3.1.1 Descripción del diseño Propuesto

Observamos que en el diagrama de la figura 4.14 se ha realizado un diseño basado en la red TOR. A continuación se detallan las características más importantes del diseño:

- Se identifican dos bloques que corresponden a la red TOR y a la red de los votantes.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

- Para interconectar cada uno de estos bloques a la red TOR y a la red de los votantes se emplea un firewall independiente y para el acceso a internet se hace mediante un router el cual conecta el internet con la red TOR.

- Los votantes acceden a realizar su voto a través del firewall 1. De tal forma que el firewall 1 debe contener políticas de seguridad orientadas a proteger la red.

- Una vez realizado la votación dicho voto es encriptado y enviado a la red TOR una vez que el voto salga de la red TOR es dirigido al centro de almacenamiento (base de datos) por el cual deberá pasar por el Firewall 2 el cual también debe contener políticas de seguridad para proteger dicha red.

- Al contar con servidores de datos. Dichos servidores deberían contar con tarjetas de red para permitir la conectividad.

- En el diseño también se visualiza una nube conocida como la red TOR la cual cuenta con un nodo de entrada por donde se envía el paquete de datos y que luego va saltando de un servidor a otro dentro de la red y finalmente sale de la red TOR por un nodo de salida y de ahí se encamina a nuestro destino. El paquete de datos se encuentra cifrada desde nuestro ordenador hasta el nodo de salida que la desencripta antes de enviarla a nuestro destino.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

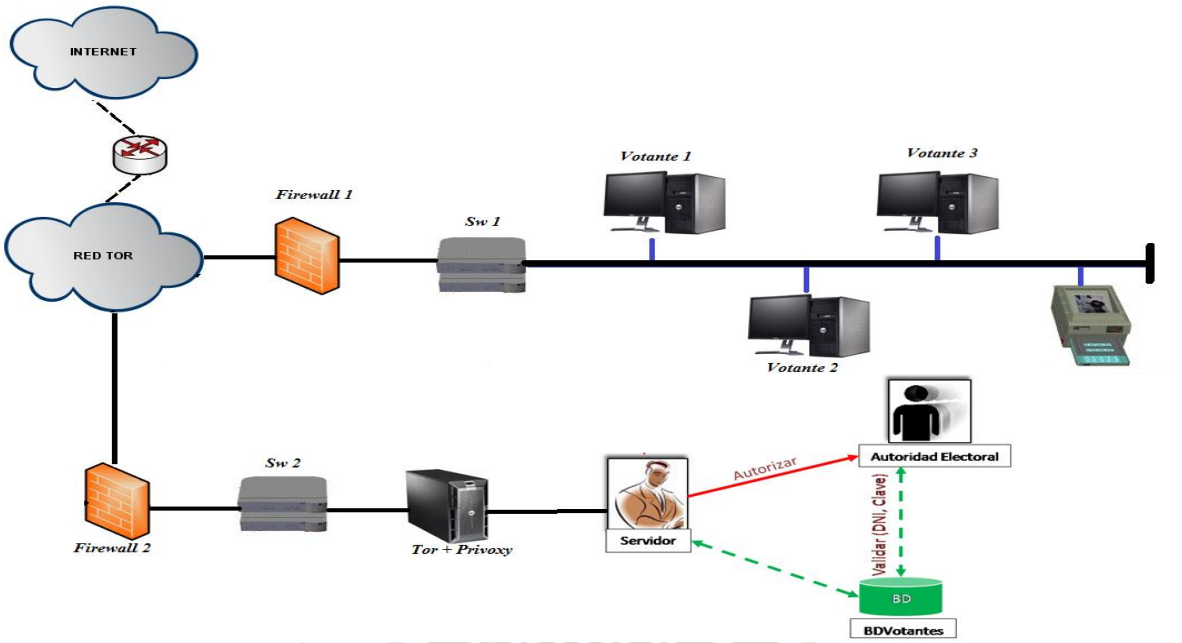


Figura 3.1 Diseño de la Infraestructura
Fuente: Elaboración propia

3.2 Herramientas Disponibles

Para la implementación del proyecto se ha decidido utilizar herramientas de software libre las cuales ayudan agilizar y de realizar la comunicación rápida. Dichas herramientas se describen a continuación:

- ✓ **FoxyProxy** es una extensión que cambia proxies automáticamente, en base a patrones de la URL. Dicho de otra manera, FoxyProxy automatiza el proceso manual de modificar los parámetros de las propiedades de conexión de Firefox.

  El cambio de servidor proxy depende de la página a cargar y de las reglas de selección definidas por el usuario. Los íconos animados indican cuando se encuentra en uso un servidor proxy. El reporte avanzado muestra cuando fue utilizado cada proxy.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

Figura 3.3 FoxyProxy

Fuente: http://www.foxyproxy.com

- ✓ **NoScript** es un plug-in gratuito que va a permitir controlar todo lo que se va a ejecutar al abrir una página web. NoScript bloquea la ejecución de Java script, Java, Flash, Silverlight, y otros plugins y contenidos de scripts. NoScript tiene un lista blanca (whitelist) para permitir la ejecución de scripts de ciertos sitios.

Figura 3.4 NoScript

Fuente: http://www.noscript.com

3.3 Implementación del diseño Propuesto

3.3.1 Instalación de TOR y Privoxy

Como ya hemos visto anteriormente cada vez que navegamos por internet o por la red siempre vamos

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

dejando rastros y estos rastros o huellas permiten a las grandes corporaciones privadas o gubernamentales crear un perfil de navegación nuestro.

Bueno a continuación se muestra la información sobre el kernel con el que se trabajó.

```
[root@localhost ~]# uname –a
Linux localhost.localdomain 2.6.28.1.fc10 #1 SMP Sat Jan 24 15:59:36
EDT 2009 i686 i686 i386 GNU/Linux
```

Ahora los pasos a seguir son:

- ✓ Descargar TOR y Privoxy en la raíz y lo procedemos descargarlos.

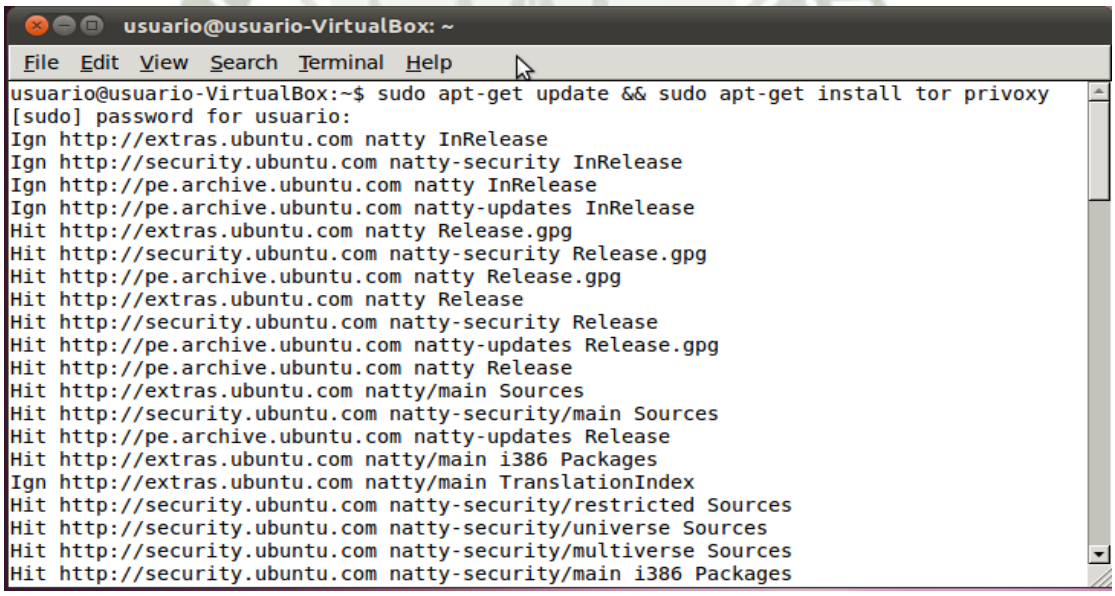


Figura 3.5 Instalación de TOR y Privoxy

Fuente: Elaboración propia

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

Ahora confirmamos la instalación.

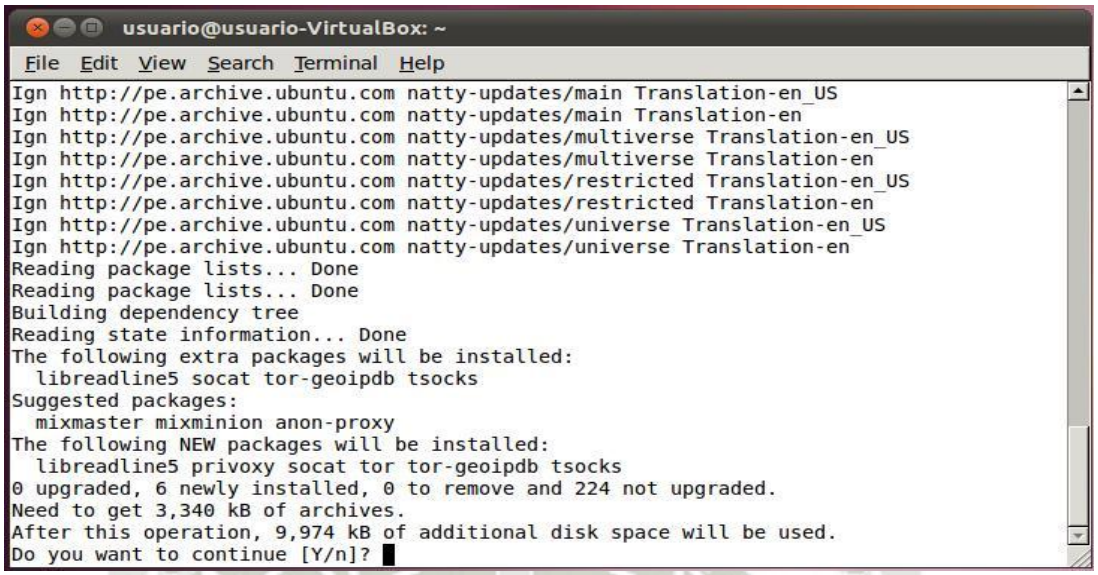


Figura 3.6 Confirmación de la instalación de TOR y Privoxy

Fuente: Elaboración propia

Ahora configuramos Privoxy agregamos la siguiente línea al inicio o al final del archivo es muy importante colocar el punto al final. Acá le estamos indicando a Privoxy que utilice la dirección local 127.0.0.1 y el puerto 9050. Tendrá que reiniciar Privoxy para que los cambios tengan efecto.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

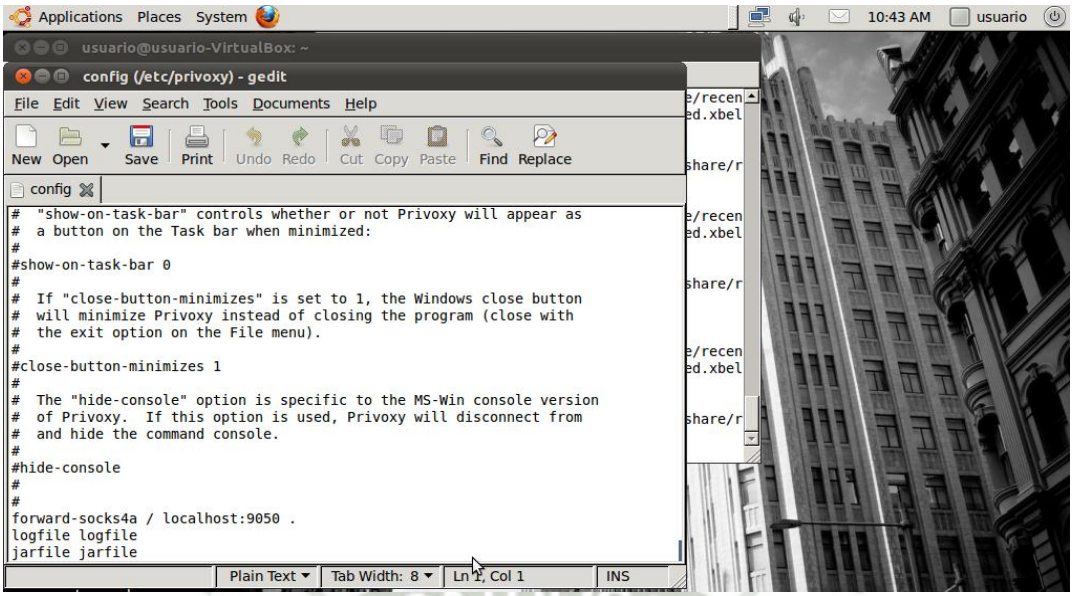


Figura 3.7 Configuración de Privoxy

Fuente: Elaboración propia

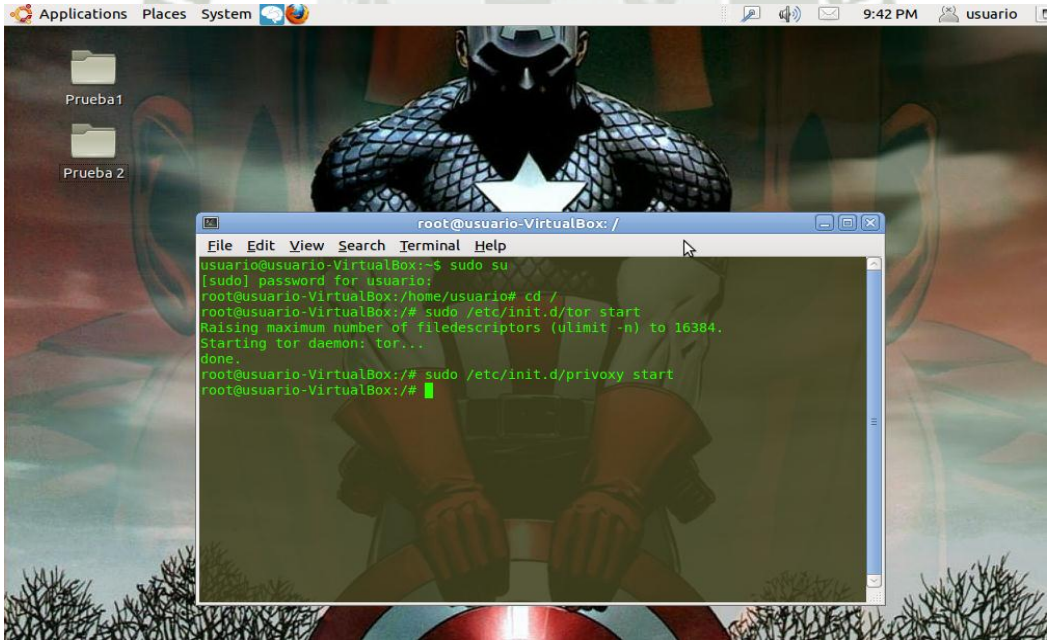


Figura 3.8 Reiniciar TOR y Privoxy

Fuente: Elaboración propia

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

Ahora nos falta realizar la configuración de nuestro navegador web (Firefox):

Para esto vamos a utilizar dos herramientas que son el FoxyProxy y el NoScript que ya se explicaron anteriormente.

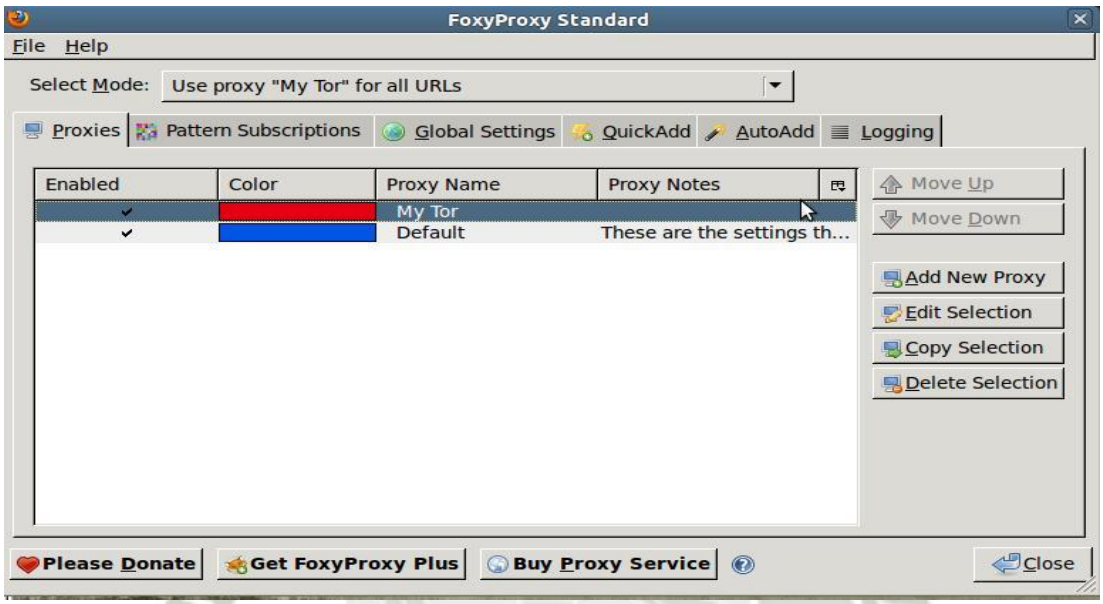


Figura 3.9 Instalación y Configuración de FoxyProxy

Fuente: https://addons.mozilla.org/en-US/firefox/addon/torbutton/

Estas herramientas se deben configurar con los siguientes valores ya que deben de apuntar hacia Privoxy, los valores a ingresar son la dirección 127.0.0.1 y puerto 9050.

La instalación y configuración de NoScript se realiza automáticamente. Para verificar si el anonimato funciona correctamente deben visitar la siguiente dirección:

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM
UNIVERSIDAD CATÓLICA DE SANTA MARÍA

http://torcheck.xenobite.eu/index.php

3.4 Servicio oculto para la página de votación dentro de la red TOR

Para empezar debemos configurar nuestra máquina TOR la cual ya no va ser una máquina de TOR sino va a ser ahora un servidor de la red TOR la cual va a almacenar nuestra página para realizar la votación esta configuración se realiza en el archivo /torrc.

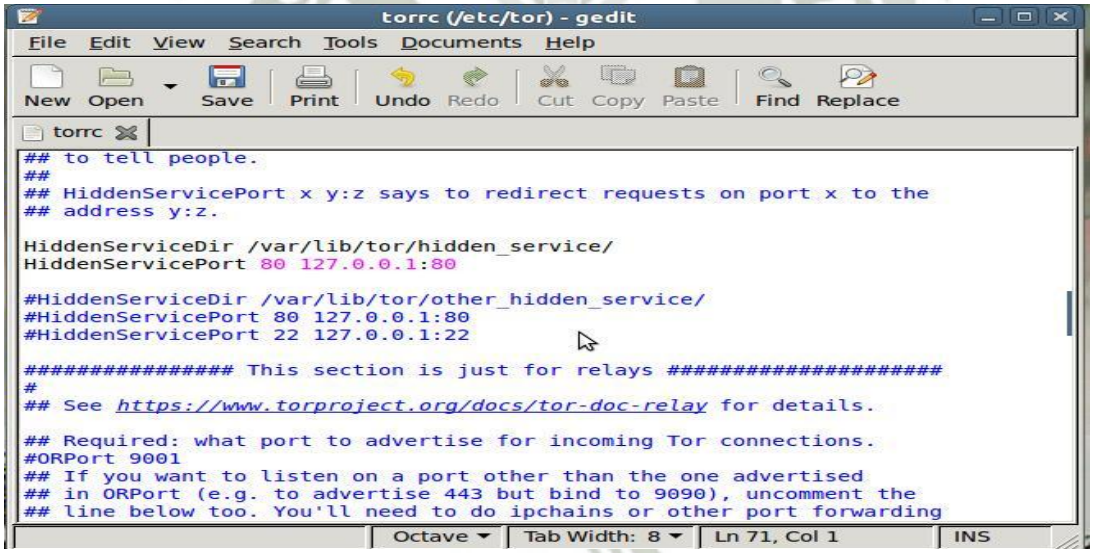


Figura 3.10 Configuración servicio oculto
Fuente: Elaboración propia

Ahora lo que sigue es configurar nuestro servidor web para eso utilizamos Apache.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

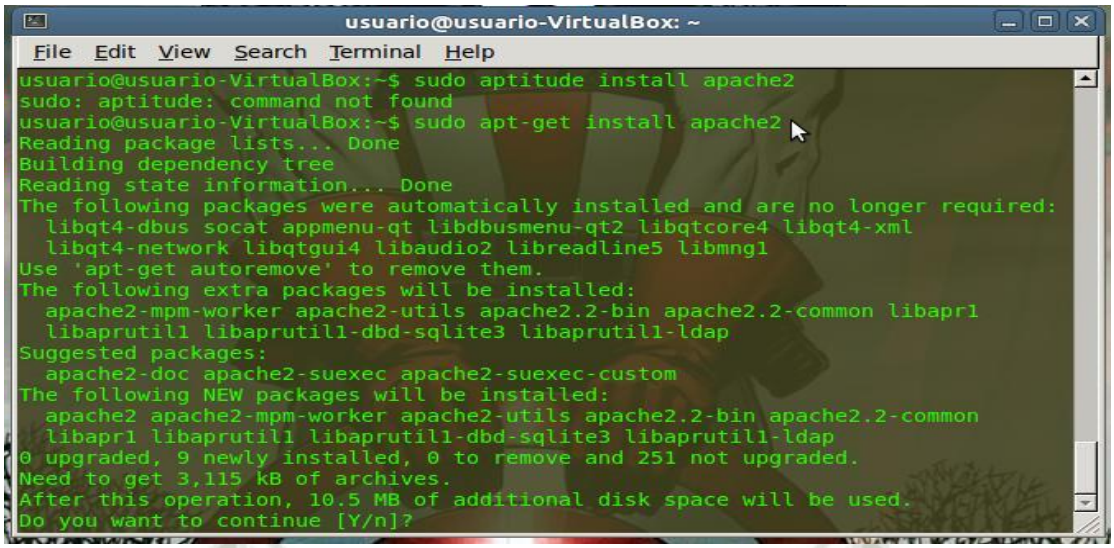


Figura 3.11 Instalación de Nuestro Servidor Web

Fuente: Elaboración propia

En este punto creamos la página de votación electrónica. Como se observa a continuación solo es una simulación ya que todos los componentes y herramientas utilizadas están desactivados es una página sencilla ya que nuestro objetivo sólo es la implementación de una infraestructura anónima.

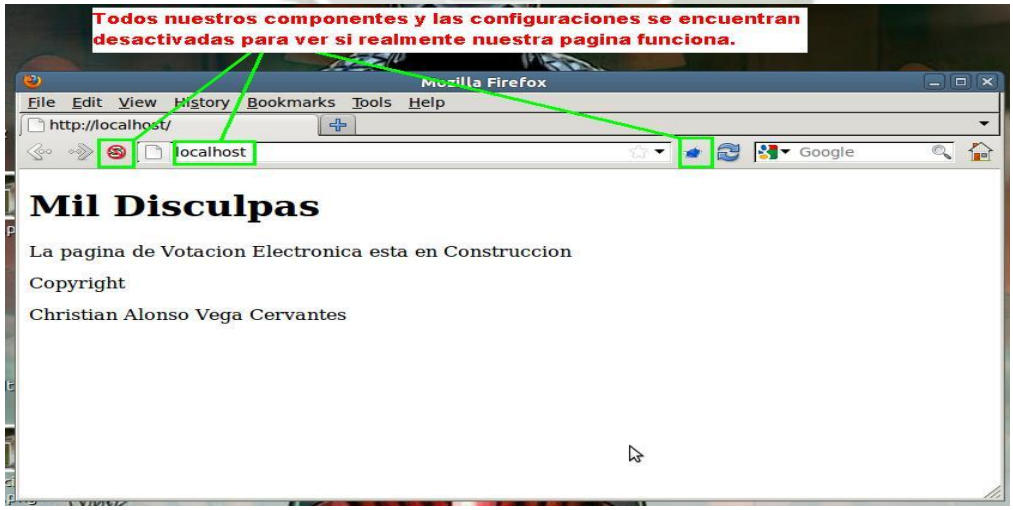


Figura 3.12 Verificación de nuestro servidor web

Fuente: Elaboración propia

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

Bueno ahora lo siguiente es cargar nuestra simulación de nuestra página al servidor oculto el cual pertenece a la red TOR y el cual nos dará la dirección .onion en la cual aparecerá nuestra página.

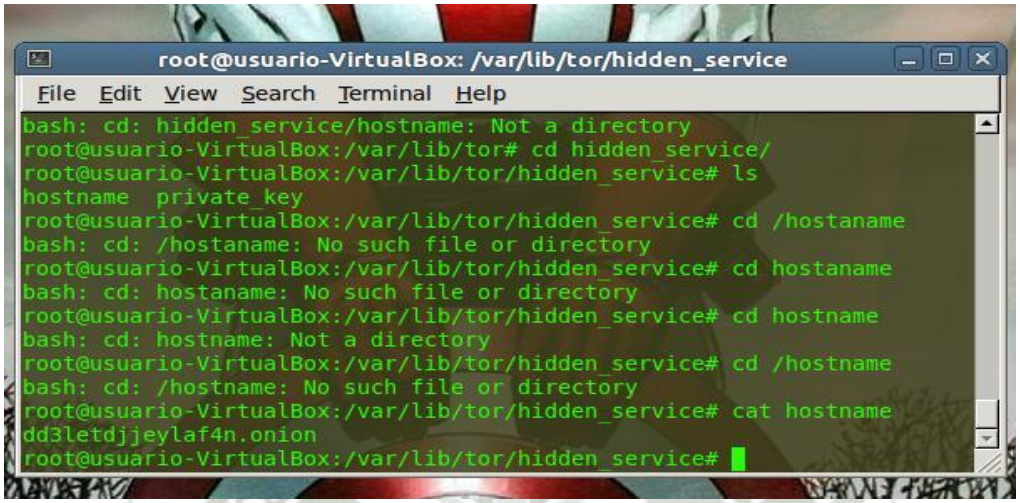


Figura 3.13 Dirección .onion de la página de Votación
[Fuente: Propia]

Ahora por último paso es activar todos los componentes como TOR, Privoxy, Apache, FoxyProxy y eso es todo.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

CAPÍTULO IV

EVALUACIÓN DE LOS RESULTADOS

4.1 EVALUACIÓN DE ANONIMIDAD

4.1.1 Prueba 1. Verificación de la IP de los Votantes

La primera prueba consiste en verificar la IP de las máquinas de los votantes o también llamadas urnas para verificar que las IP pertenezcan a la misma red configurada inicialmente.

El procedimiento es el siguiente: como se muestra la imagen 4.1

Figura 4.1 Imagen de TOR desactivado

Fuente: Elaboración propia

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

La IP con la que contamos es la 190.237.135.70 la cual es la IP que nos asignó el proveedor de internet de nuestra ciudad. La figura 4.2 muestra la nuestra localización de nuestra IP.

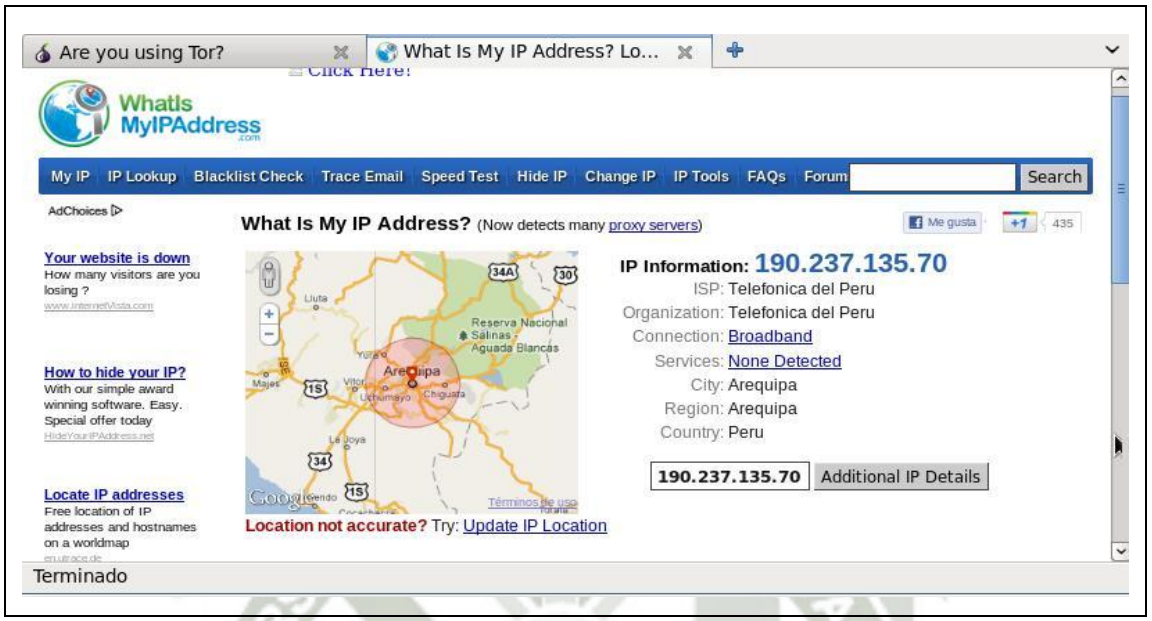


Figura 4.2 Imagen de la IP actual

Fuente: http://whatismyipaddress.com/

Con esto comprobamos que nuestra IP esta dentro del rango de nuestra ciudad y de nuestro país.

4.1.2 Prueba 2. Comprobación del cambio de IP

La prueba consiste en verificar que las máquinas de los votantes o urnas electrónicas estén con su IP cambiada para su navegación anónima y para que el elector pueda realizar su voto seguro sin que haya modificación de dicho voto en el proceso electoral realizado.

El procedimiento a seguir es:

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

Después de revisar la anterior información procedemos a activar TOR para que nuestra máquina configurada con TOR se conecte a la red TOR la cual nos asignará una IP de otro país o alguna ciudad del exterior con esta nueva IP se aumentará la seguridad y privacidad de nuestra máquina y a la vez permaneceremos anónimos en nuestra navegación por el internet como se muestra las imágenes 4.2 y 4.3.

Figura 4.3 Imagen de TOR activado

Fuente: Elaboración propia

La nueva IP asignada a la máquina es la 89.253.105.39 con la cual procederemos a realizar la votación anónima. A continuación se muestra la ubicación de la nueva IP asignada a la máquina. Como se observa en la imagen 4.4.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

Figura 4.4 Imagen de la IP nueva

Fuente: Elaboración propia

Como pueden observar en las figuras 4.2 y 4.4 la IP cambio de la siguiente manera:

190.237.135.70 ——> 46.105.27.26

Estas IPs pueden variar cada vez que se reinicie el sistema e incluso se puede obtener una IP que se encuentre libre o que ya teníamos registrada en anteriores conexiones.

También al navegar por internet debe de aparecer ya no el Google de Perú el típico www.google.com.pe sino debe de aparecer otro Google como: como se observa en la figura 4.5

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

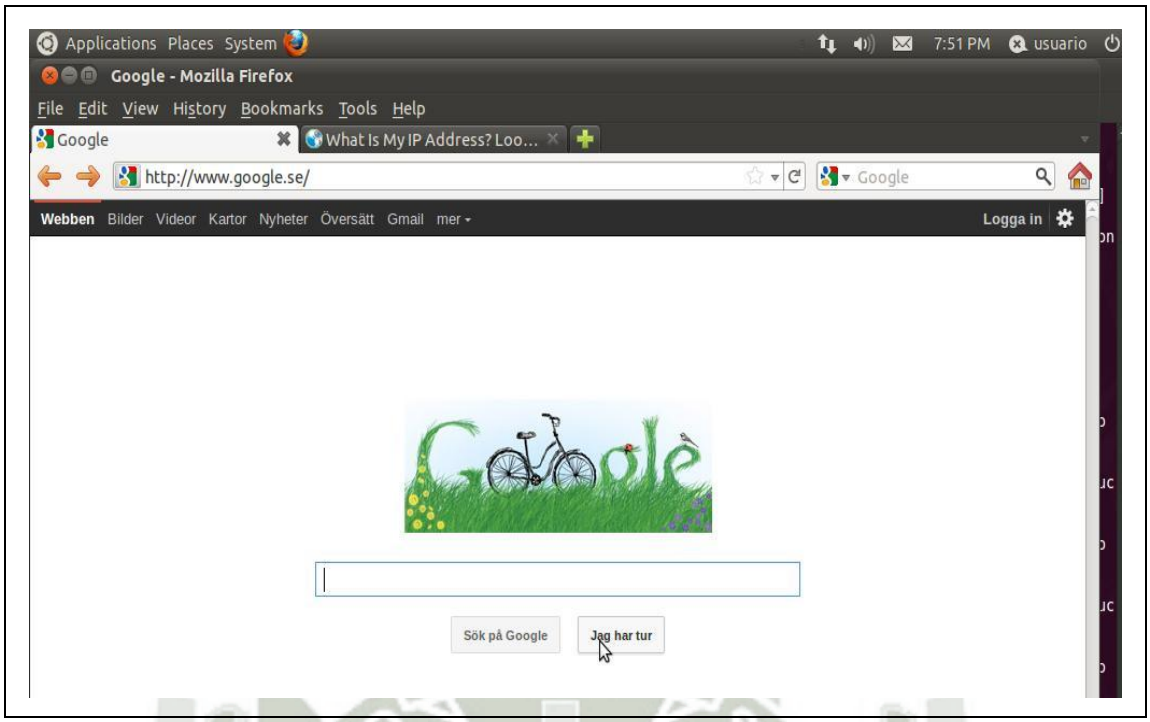


Figura 4.5 Imagen de nuestro nuevo Google de TOR
Fuente: Elaboración propia

4.2 EVALUACIÓN DE SEGURIDAD Y PRIVACIDAD

4.2.1 Prueba 3. Comprobación sí navegamos dentro de la red TOR

Esta prueba es muy importante ya que nos permitirá conocer si nuestra máquina o PC esta dentro de la red TOR la cual nos permitirá navegar anónimamente así como mostrar los servicios ocultos dentro de esta red internacional y las direcciones .onion. Como se muestra la imagen 4.6 y 4.7.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

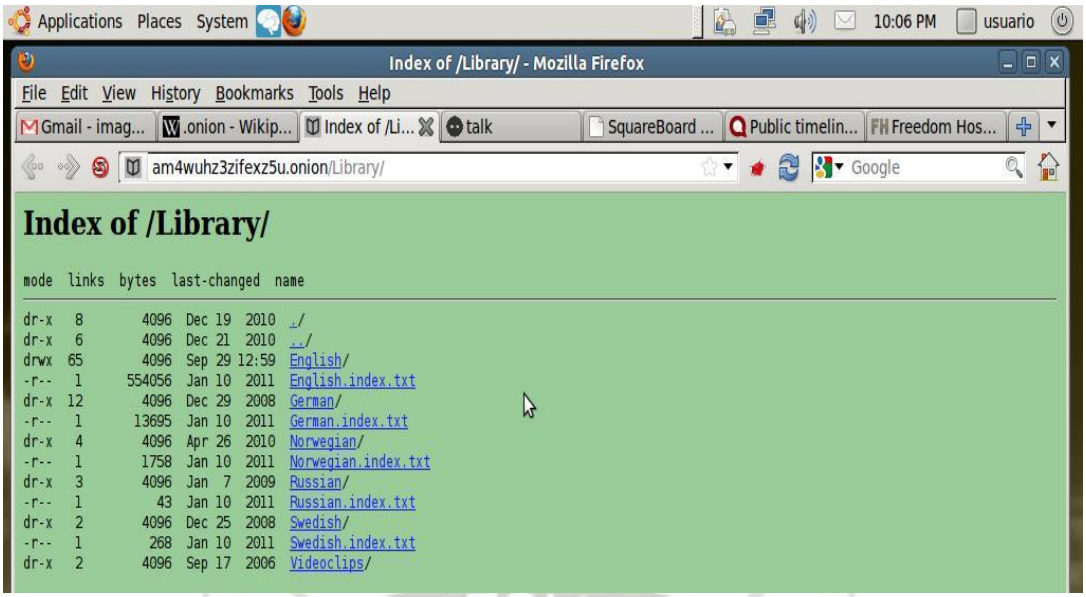


Figura 4.6 Imagen de servicios ocultos de la red TOR 1

Fuente: http://am4wuhz3zifex5u.onion

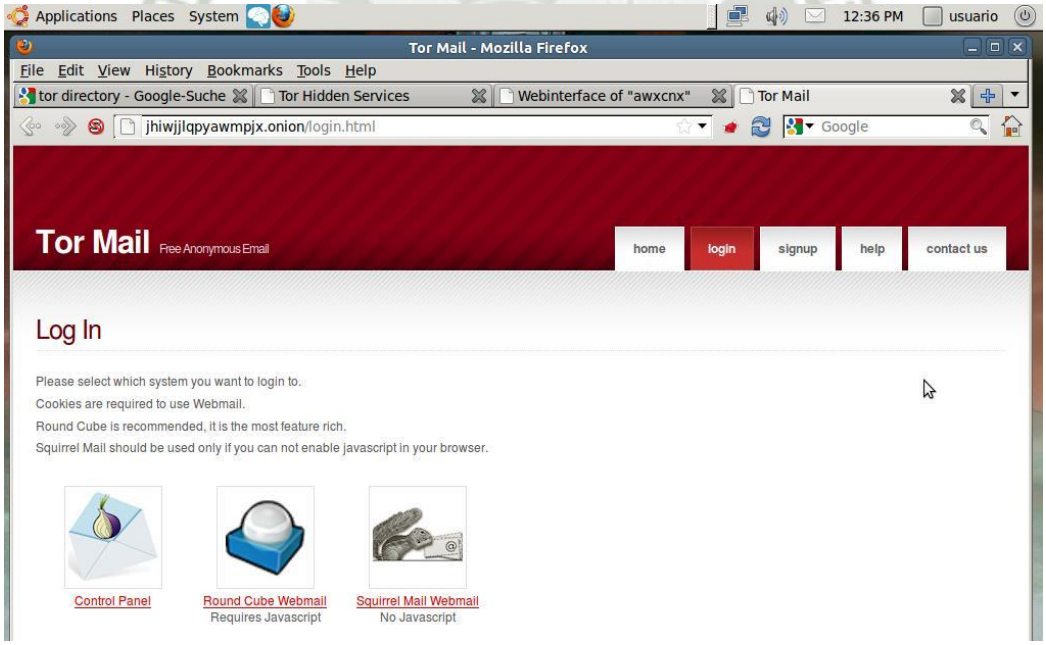


Figura 4.7 Imagen de servicios ocultos de la red TOR 2

Fuente: http://3g2upl4pq6kufc4m.onion

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

4.3 EVALUACIÓN DE SEGURIDAD EN EL ENVIÓ DE INFORMACIÓN

4.3.1 Prueba 4. Creación de nuestra página dentro de la red TOR para la realización de las votaciones

Esta prueba es para verificar si nuestra página de votación está alojada como un servicio oculto dentro de la red TOR. Para esto primero debemos colocar la dirección .onion ya mencionada en el anterior capítulo la cual es dd9letdjjeylaf4n.onion, como se observa en la figura 4.8

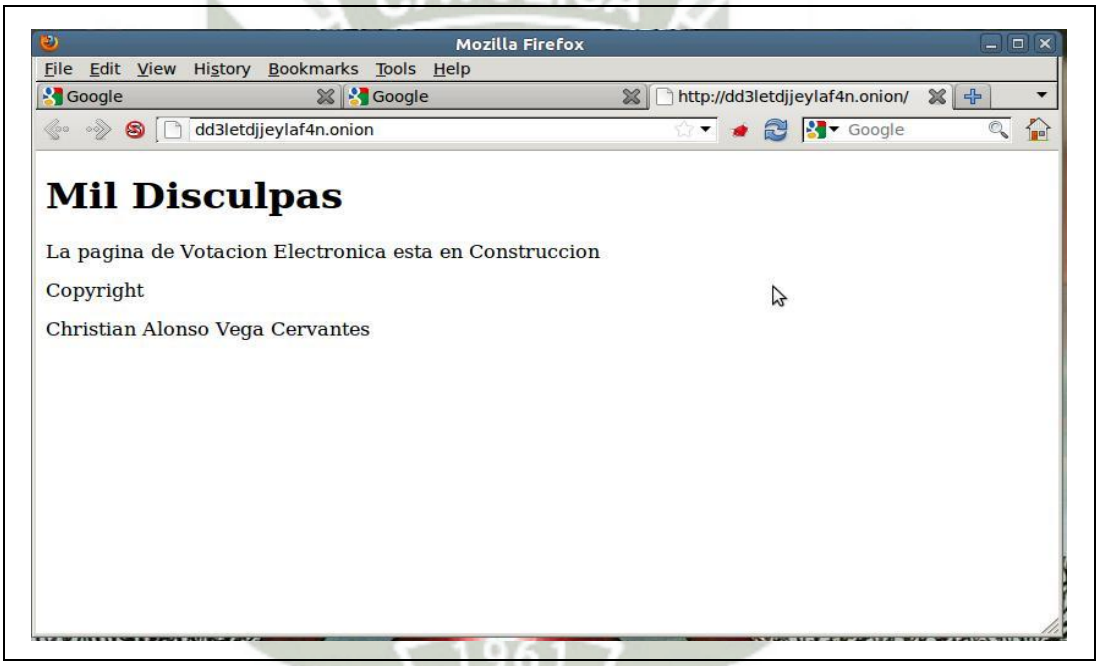


Figura 4.8 Imagen de la Votación Electrónica
Fuente: Elaboración propia

Con esto hemos logrado que nuestra página este dentro de la red TOR como un servicio oculto.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

4.3.2 Prueba 5. Comprobación de la simulación de la votación desde otro sistema operativo

Esta prueba consiste en comprobar si nuestro servicio oculta se puede visualizar desde otro sistema operativo en este caso lo probaremos desde Windows XP ya que toda la implementación y configuración del proyecto se encuentra en Ubuntu. Para eso al momento de que el votante realice su voto deberá aparecer como se observa en la figura 4.9.

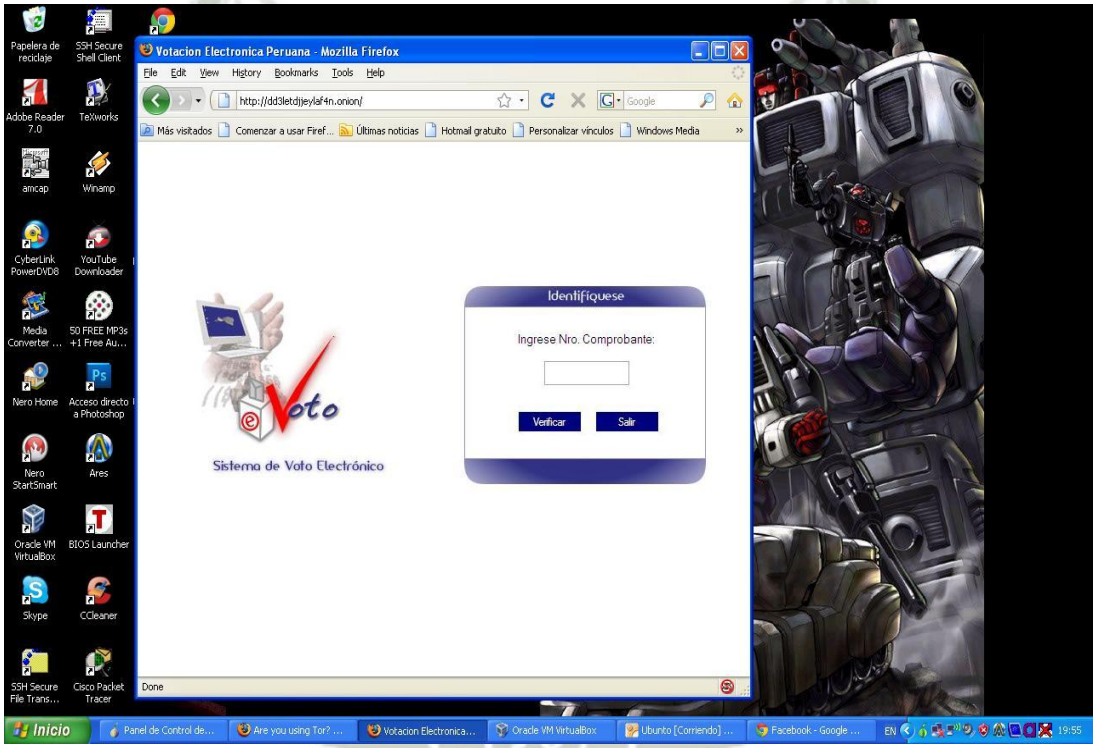


Figura 4.9 Página de la votación electrónica

Fuente: Elaboración propia

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

CONCLUSIONES

1. Para proteger los sistemas de votaciones de las amenazas actuales, se utilizó una metodología de seguridad informática mediante el empleo TOR y Privoxy, permitiendo una votación más segura.

2. El trabajo realizado alcanzó el objetivo general brindando seguridad y confiabilidad en el envió de datos así mismo se dio a conocer una nueva tecnología la cual ayuda a proteger la identidad del usuario cuando este navega por el internet.

3. Se pudo comprobar que la integración de las diferentes tecnologías y herramientas utilizadas hace que la identidad del usuario este protegida.

4. Este trabajo asegura que las IP de las urnas se encuentren anónimas antes de realizar el proceso electoral para así proteger los datos de los votantes.

5. Es indispensable contar con una tecnología que pueda garantizar un nivel de seguridad es por eso que se propuso este trabajo utilizando una nueva tecnología como es TOR y con el cual se alcanzó los objetivos deseados.

6. Se demostró también que los sistemas operativos abiertos tales como (Linux) tienen un entorno más manipulable y el cual pueden ser configurados a las necesidades de cada institución o persona que aquellos sistemas operativos cerrados como Windows por este motivo la implementación de este proyecto se realizó sobre Ubuntu.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

BIBLIOGRAFÍA

[ALD02] Aldegani, Gustavo. Seguridad Informática. MP Ediciones, Argentina. 2004. Página 22.

[AND09] Andreasson, Oskar. Iptables Tutorial 1.1.19. 2003. http://iptables-tutorial.frozentux.net/iptables-tutorial.html

[BOR03] Borghello, Cristian Fabián. Seguridad Informática sus Implicancias e Implementación. Tesis de Licenciatura en Sistemas, Universidad Tecnológica Nacional de Argentina. 2001.

[CHG/1998] Chang Mota, Roberto 1998, P.14, Instituto Iberoamericano de Derechos Humanos (IIDH).

[CZM/2001] Guzmán Rojas, Iván "La Automatización de los procesos electorales", diccionario electoral. San José de Costa Rica: IIDH/CAPEL, 2001.

[CC/2005] Cantijoch Cunill, 2005; http://ebookbrowse.com/cantijoch-cunill-voto-electronico-pdf-d305679158

[MZC/2000] Martínez Castaño, 2000; Tornadijo, 2003

[SVES01] Scytl: Voto Electrónico Seguro. Scytl: Secure Electronic Voting. [En línea] 2007. www.scytl.com.

[REJM05] Reniu, Josep M. Del papel a la Red: El Voto

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

Electrónico. La Vanguardia. 2005.

[GOBA03] Gobierno de Buenos Aires. Prueba Piloto de Voto Electrónico. [Publicación] Buenos Aires: Octubre 2005.

[RIAJ04] Rial, Juan. Posibilidades y Límites del Voto Electrónico. [Publicación] Perú: s.n., 2004.

[FIR21] Firewall: http://www.checkpoint.com/products/protect/firewall-1.html

[LIN22] Anónimo. Edición Especial. Linux Máxima Seguridad. La Guía Definitiva Para Proteger de Hackers sus Servidores
Linux. http://savannah.nongnu.org/projects/plex86

[ZJWY06] Zhen Ling, lunzhou Luo, Wei Yu, Ming Yang and Xinwen Fut "Extensive Analysis and Large-Scale Empirical Evaluation of TOR Bridge Discovery"

[MCHM07] Masoud Akhoondi, Curtis Yu, and Harsha V. Madhyastha
Department of Computer Science and Engineering
University of California, Riverside "LASTor: A Low-Latency AS-Aware TOR Client"

[SGMI08] Stjepan Groš, Marko Salkic, Ivan Šipka-Faculty of Electrical and Computing Engineering
University of Zagreb; Unska bb, 10000 Zagreb, Croatia
Protecting "TOR Exit Nodes from Abuse"

[ACPM10] Abdelberi Chaabane, Pere Manils, Mohamed Ali Kaafar; INRIA Rhone-Alpes Grenoble, France "Digging

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

into Anonymous Traffic: A Deep Analysis of the TOR Anonymizing Network”

[SAAK12] Sambuddho Chakravarty, Angelos Stavrou, Angelos D. Keromytis “Identifying Proxy Nodes in a TOR Anonymization Circuit”

[XLNW11] Xin Liu, Neng Wang “An Improved TOR Circuit-Building Protocol”, 2009

[RSNB13] Robin Snader and Nikita Borisov, Member, IEEE, “Improving Security and Performance in the TOR Network through Tunable Path Selection”, 2011

[SNS14] Souad Benmeziane, Nadjib Badache, Sihem Bensimessaoud “TOR Network Limits”,2011

[DALJ15] Dhiah el Diehn I. Abou-Tair, Lexi Pimenidis, Jens Schomburg, Benedikt Westermann “Usability Inspection of Anonymity Networks”,2009

[PR16] Privoxy: http://www.privoxy.org/

[RPS17] Ribut Pujo Siswanto “Abstract Developing a Proxy Server with Privoxy”, 2009

[MGLF18] Magazine Linux Filtros: http://www.linux-magazine.es/issue/12/Filtros.pdf/

[MP19] Manual User Privoxy: http://madbutcher.dyndns.org:8080/FTPRoot/ftp/Privoxy/Docs/privoxy-user-manual.pdf

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

[KPKY20] Revista Kaspersky: http:www.kaspersky.com/sp/about

[TFHP21] Roger Dingledine" TOR sistema de comunicación anónima".

[STUW22] "Seguridad del protocolo de autenticación TOR" Facultad de ciencias de la computación de la Universidad de Waterloo

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

ANEXO A

COMO ESCONDER NUESTRA IP EN INTERNET

1. COMO ESCONDER MI IP

Hay situaciones en las cuales queremos visitar un site sin dejar rastros en él, pero al acceder al lugar, la visita quedará registrada en un archivo log del servidor. Los visitantes frecuentes generan muchos registros. Estos registros pueden brindar información al administrador de la red, información que es enviada desde nuestra PC sin que nosotros nos enteremos, así que la mejor opción es navegar con un intermediario que entre a los sitios por nosotros.

Paso 1: Determinar Nuestra Dirección IP

Para averiguar nuestra propia dirección IP podemos ir a http://megawx.aws.com/support/faq/software/ip.asp. Cada computadora conectada a internet tiene un número identificador único llamado "dirección IP".

Paso 2: Navegar Anónimamente

Método 1: Anonymizer

Cualquiera puede navegar anónimamente con la ayuda de un excelente servicio llamado: "Anonymizer X"

http://www.anonymizer.com/3.html.

Anonymizer es una de las herramientas más populares para navegar anónimamente, pero no es la única. Continuamente

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

aparecen sitios que ofrecen servicios similares. Otra buena alternativa es JANUS (http://www.rewebber.de/) ubicado en Alemania. Es rápido, puede encriptar el URL, y además es gratuito. Además es capaz de encriptar los URLs (las direcciones de las páginas) de modo que puedan ser usadas como referencia al servidor. Todas las referencias en la respuesta del servidor son encriptadas también, antes de que lleguen al usuario."

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

ANEXO B

MI PROXY

ES ANÓNIMO

¿Mi proxy es realmente anónimo?

No todos los proxies son del todo anónimos. Algunos de ellos dejan que el administrador del sistema (del sitio visitado) averigüe la dirección IP desde la cual nos estamos conectando al proxy, o sea, nuestra dirección IP real. Una vez que se esté usando un proxy se puede hacerle una prueba de anonimato en la siguiente dirección: http://www.tamos.com/bin/proxy.cgi Si se recibe el mensaje "Proxy server is detected!" - entonces hay un agujero de seguridad en el proxy que estás usando, y el servidor web es capaz de averiguar tu verdadero IP. La información sobre tu verdadero IP va a aparecer en la página web. Si el mensaje que recibes es "Proxy server not detected" significa que se está navegando anónimamente.

Las herramientas pueden ser encadenadas. Por ejemplo, si estas usando el Proxy A, y se sabe las direcciones de otros dos proxies (Proxy B y Proxy C). La dirección que se solicitaría sería algo así como:

http://proxyB:puerto/http://proxyC:puerto/http://www.lapagina.com... como resultado, accederías a www.lapagina.com a través de 3 proxies anónimos: A (que está configurado en el browser) B y C (que están en el URL que se escribió).

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

ANEXO C

PLAN DE TESIS

1. Título

"Implementación de una infraestructura de Voto Electrónico utilizando Privoxy bajo el esquema TOR (The Onion Routing)".

2. Identificación del Problema

El mundo de la información y la comunicación ha cambiado tanto que el modo en que adquirimos, almacenamos y diseminamos el conocimiento cada vez se parece menos a los modos usados tradicionalmente.

Es por eso que nuestra privacidad y la seguridad de nuestros datos se pueden ver afectadas. Cuantos más datos nuestros estén informatizados, más posibilidades existen que alguien que nosotros no hayamos previsto, pueda tener acceso a los mismos.

En los sistemas de voto electrónico actuales la privacidad, seguridad y confiabilidad del voto es muy importante. Lo que se propone es proteger la privacidad del votante así como también proveer seguridad y confiabilidad del voto electrónico.

Un informe divulgado por la empresa Kaspersky Lab, indica que en el 2010, el número de programas maliciosos diseñados para robar datos personales a usuarios se ha incrementado en más del 100%. Como si esto ya no fuera impactante, el informe agrega que el número de nuevas firmas de Troyanos bancarios introducidos en las

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

bases de datos de Kaspersky Lab ha superado los 25.000 en 2010, cinco veces más que en el 2006.

La página de la EFF sobre privacidad tiene una buena discusión sobre el tema. En un mundo perfecto posiblemente no habría necesidad de permanecer anónimo; pero este mundo no es perfecto.

Existen razones económicas o políticas por las cuales puedes tener temor de denunciar abiertamente un hecho. Por ejemplo: puedes temer que alguien tome represalias contra ti o incluso atente contra tu vida, ya sea por criticar a un régimen autoritario o por denunciar algo que tu empresa o gobierno está haciendo en forma ilegal. La corte suprema de U.S.A. en 1995 resumía la importancia del anonimato así:

La protección de la expresión anónima es vital para el devenir democrático. Permitir a los disidentes esconder sus identidades los libera para expresar opiniones crítica o minoritarias... el anonimato es un escudo de la tiranía de la mayoría...

3. Descripción del Problema

La seguridad y la privacidad ocupan un lugar importante en la vida de todo ciudadano común, con el desarrollo de aplicaciones más sofisticadas donde el usuario debe interactuar muchas horas con el computador ya sea para revisar su correo personal, cuentas bancarias o incluso realizar diferentes tipos de transacciones las cuales son confidenciales y no quieren que sean conocidos por personas extrañas, así como también los proveedores de internet (ISP) los cuales pueden saber exactamente los sitios a los que se conecto es por eso que este trabajo propone el uso de TOR y Privoxy para dar solución a este problema así como dar a conocer otras funciones que serán descritas más adelante.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

4. Justificación

Esta propuesta pretende dar a conocer las ventajas el utilizar una nueva tecnología, para reducir algunas de las barreras citadas anteriormente en la implementación de una infraestructura de voto electrónico. El trabajo proporciona todos los conocimientos requeridos para aplicar esta nueva tecnología para mejorar la seguridad de aplicaciones que funcionan sobre internet.

Algunos dicen "**el que nada hace, nada teme**"

Un informe divulgado por la empresa Kaspersky Lab, indica que en el 2010, el número de programas maliciosos diseñados para robar datos personales a usuarios se ha incrementado en más del 100%.

Como si esto ya no fuera impactante, el informe agrega que el número de nuevas firmas de Troyanos bancarios introducidos en las bases de datos de Kaspersky Lab ha superado los 25.000 en 2010, cinco veces más que en 2006. Esto es tan preocupante que las cifras parecen equivocadas.

5. Objetivos

5.1. General

- Proporcionar una infraestructura utilizando Privoxy bajo el esquema TOR (The Onion Routing).

5.2. Específicos

- Mejorar el canal de comunicación haciéndolo anónimo.
- Mejorar de seguridad y privacidad en la navegación por internet.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

- Implementar un diseño resistente a ataques de análisis de tráfico (traffic analysis).

6. Alcances

6.1. Internos

- El usuario podrá navegar por el internet de forma anónima y segura.

- El envió de información fiable en lo que se refiere al cifrado de la información.

- Los usuarios podrán contar con el medio para poder expresarse anónimamente en un contexto en que algunos gobernantes piensan que tienen el derecho de monitorear nuestras acciones.

6.2. Externos

- Implementación de una infraestructura de Voto electrónico utilizando Privoxy bajo el esquema TOR (The Onion Routing)

- Mejorar la navegación por internet haciéndolo de forma anónima y envió de información de forma cifrada.

7. Hipótesis

Dado que hoy en día Navegar por internet no es, para nada, una actividad anónima; prácticamente todo lo que se transmite, consulta o visita puede ser archivado e incluso cuantos más datos

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

nuestros estén informatizados, más posibilidades existen de que alguien que nosotros no hayamos previsto, pueda tener acceso a los mismos, es probable que con la Implementación de una infraestructura de Voto electrónico utilizando Privoxy bajo el esquema TOR (The onion routing), se logre la navegación del usuario de forma anónima, aumentando el nivel de seguridad y privacidad de los usuarios cuando estos naveguen por el internet.

8. Variables

8.1. Independientes

- TOR (The onion routing).
- Privoxy.

8.2. Dependientes

- Infraestructura del voto electrónico.

9. Indicadores

- Anonimidad.
- Mejor Seguridad y Privacidad.
- Mejor seguridad en el envío de información.

10. Área de Investigación

El área de investigación es la de Redes y Telecomunicaciones.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

11. Tipo de Investigación

El tipo de investigación es exploratoria.

12. Nivel de Investigación

El nivel de investigación es experimental.

13. Marco Teórico

13.1 Voto Electrónico

Durante los últimos años el tema del voto electrónico ha comenzado a ocupar lugares cada vez más importantes en los discursos políticos. Este artículo muestra como la implementación de sistemas de voto electrónico transforma los procedimientos establecidos en las votaciones convencionales, y que tienen como objetivo salvaguardar los principios democráticos básicos que rigen los procesos electorales.

Además, existen algunas implicaciones políticas que deben tenerse en cuenta, especialmente las relativas a la participación electoral. Para la exposición de un estudio de caso para este fenómeno, se toman datos relativos en la que se pretende reflexionar sobre una pregunta clásica de esta cuestión: ¿están justificados los temores a la implementación de sistemas electrónicos de votación? Es en este marco en el que las nuevas tecnologías hacen su irrupción. En el caso de las votaciones electrónicas, la tecnología puede afectar a muchas de las fases del proceso electoral, desde la convocatoria hasta la proclamación de

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

resultados. No obstante, donde resulta más interesante observar esta incursión es en la fase de la emisión del voto, momento que viene estrictamente regulado hasta el detalle para que en ningún caso se vean vulnerados los principios democráticos básicos.

¿Cómo afecta la irrupción de la tecnología a los diferentes momentos que constituyen esta fase? ¿Cómo se ve transformado el proceso electoral con la implementación de elementos electrónicos que modifican el procedimiento habitual? Las elecciones constituyen una pieza fundamental en el funcionamiento de la democracia. Desde la aceptación del carácter popular de la soberanía y ante la necesidad práctica de ejercer el poder a través de representantes, la elección de estos por la comunidad constituye un acto que da sentido y define el carácter democrático del sistema. En el modelo ideal de democracia representativa se produciría una plasmación idéntica de los intereses y demandas de los ciudadanos en los diversos órganos de poder.

Los procesos electorales son el instrumento que debe garantizar la máxima concordancia entre estas posiciones los gobernantes/representantes y los gobernados/representados como si se tratase de un muestreo. El objetivo básico debe residir en que la selección realizada conduzca a una acción de gobierno coherente con las voluntades reales de aquellos que ostentan la soberanía, dando lugar también a la legitimidad que una transferencia de poder como esta requiere. Las elecciones van a condicionar pues el carácter democrático del sistema.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

13.2 Sistema de votación por Internet

El modo de voto por Internet puede usar lugares remotos (desde cualquier computadora habilitada) o puede usar los tradicionales con casillas computarizadas conectadas a Internet.

Algunas organizaciones usan Internet para elegir ejecutivos o miembros de directivos así como para otros tipos de elecciones. La votación tras Internet ha sido utilizada privadamente en algunas naciones y públicamente en los Estados Unidos, el Reino Unido (UK), Irlanda, Suiza y Estonia. En Suiza, donde ya es una parte establecida de los referendos local, los votantes son provistos de contraseñas, a través del servicio postal, para acceder a la papeleta.

La mayoría de los votantes en Estonia pueden emitir sus votos en elecciones locales y parlamentarias, si desean hacerlo, a través de Internet, por cuanto la mayoría de los inscriptos en los padrones tienen acceso a un sistema de voto electrónico; éste es el desarrollo más opulento en países de la Unión Europea.

Se hizo posible porque la mayoría de los estonios tienen una tarjeta de identidad nacional equipada con un microprocesador legible por computadora que pueden utilizar para acceder a la elección en red. Los votantes sólo necesitan una computadora, un lector electrónico de tarjetas, su tarjeta de identidad y su clave, y así votar desde cualquier rincón del mundo.

Los votos electrónicos estonios sólo pueden emitirse durante los días de votación anticipados. El día mismo de

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

la elección la gente debe dirigirse a los puestos de votación y llenar una papeleta de papel.

13.3 Sistemas de votación en red (Network Voting Systems)

En estos sistemas algunos o todos los datos del proceso electoral son transmitidos sobre una red de comunicaciones que no es, ni física ni lógicamente, utilizada sólo por los datos de la elección. Es decir, la red es generalmente una red pública (como Internet) o privada (como una red de cajeros automáticos).

La FEC dentro de sus estándares considera al sistema de votación en red de DRE (Public Network Direct Record Electronic Voting System) como un sistema de registro electrónico directo, pero con capacidad para transmitir los resultados de la votación ya sea en línea, en lotes o al final de la jornada electoral. Estos sistemas tienen dos distintas alternativas:

13.3.1 Sistema de votación en red asistido (Attended Network Voting System)

Es el sistema de votación presencial que interconecta varias computadoras que proporcionan soporte para el voto y para el escrutinio. En este caso el elector tiene que asistir a un centro de votación previamente determinado, se identifica ante el administrador, se le asigna una computadora y vota en ella.

Este sistema se puede establecer a través de una PC o de una computadora portátil (laptop) sea con pantalla sensible al tacto, ratón o teclado.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

En ese mismo orden, resultan también más amigables para el elector. En este sistema se requiere de una máquina administradora y varios terminales, un programa intenso de información y educación electoral, y un sistema de respaldo e infraestructura que pueden ser costosos. Como son máquinas convencionales sus costos son mayores que las del sistema anterior, pero se pueden utilizar en otras actividades no electorales.

13.3.2 Sistema de votación en red no asistido (Unattended Network Voting System)

Es un sistema de votación no presencial que se sirve de la plataforma de Internet, la red de redes. Es un sistema no asistido pues el elector no tiene que desplazarse a un lugar de votación sino que puede votar desde cualquier lugar en el que exista acceso a Internet.

La tecnología para encriptar información puede utilizarse para asegurar que la emisión del voto a través de Internet resulte segura y privada. Sin embargo, estos sistemas de voto generan muchas de las preocupaciones asociadas con los sistemas de voto en ausencia y por correo, incluyendo aquellas que se relacionan con el hecho de que la población sea influida o forzada a votar de determinada manera o con la posibilidad de que las personas puedan vender su derecho al voto.

Suele incluirse dos casos que no corresponden estrictamente al llamado voto electrónico. En algunos estados de EE. UU., el voto no se efectúa en una urna

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

sino a través de un mecanismo similar a una máquina tragamonedas: el votante, una vez identificado y autorizado su voto, accede a una cabina en la que, en dicha máquina, selecciona el voto deseado y lo emite. El recuento es automático y al finalizar la jornada electoral se obtienen directamente los resultados (Martínez Castaño, op. cit.). Sin embargo, la votación no se realiza a través de un dispositivo electrónico sino de uno mecánico.

Un segundo caso es el que hace referencia al voto convencional que se introduce en una máquina que cuenta los votos o de lectura óptica. Las máquinas de escrutinio eliminan la subjetividad implícita en la evaluación de la validez del voto y pueden asegurar un escrutinio imparcial, pero las máquinas no pueden definir la intención de un elector que haya hecho una marca extra en el papel o que no haya marcado el lugar correcto que la máquina lee. Esto puede invalidar un voto válido y genera un motivo de conflicto de integridad.

Los electores necesitan saber cómo usar y marcar correctamente una papeleta leída por una máquina para lo que se requiere un programa de educación electoral, sobre todo en países en los que son muchos los jóvenes que ingresan al cuerpo electoral. Estas máquinas también eliminan muchos de los errores humanos así como las oportunidades para manipular el proceso y la consolidación de resultados. Sin embargo, en este caso se trata de una máquina escrutadora, más no de un voto electrónico. Todo esto nos lleva a examinar la

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

factibilidad de estas propuestas desde distintos puntos de vista.

GRÁFICO 1
Sistemas de votación

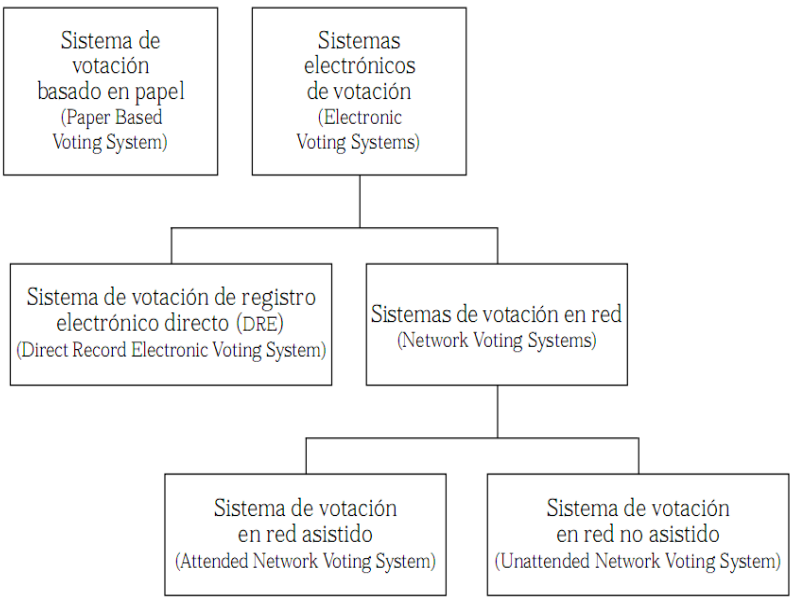


Figura 1 Sistemas de Votación

Fuente: http://blog.pucp.edu.pe

13.4 Privoxy

Privoxy es un proxy que está basado en el programa Internet Junkbuster y está publicado bajo la licencia pública general GNU.

Privoxy cuenta con capacidades avanzadas de filtrado para proteger la privacidad, modificar el contenido de las páginas web, administrar cookies, controlar accesos y eliminar anuncios, banners, ventanas emergentes y otros elementos indeseados de Internet.

Privoxy tiene una configuración muy flexible y puede adaptarse a las necesidades de cada usuario, ya que es una aplicación tanto para sistemas de redes autónomos como para multiusuario.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

Además, Privoxy utiliza el concepto de acciones con el fin de manipular el flujo de datos entre el navegador y los sitios remotos. Hay varias medidas disponibles con funciones específicas para bloqueo de sitios web, gestión de cookies, etc., estas acciones pueden ser invocadas por separado o combinadas.

Una lista de reglas para Privoxy bastante popular era la neilvandyke.action de Neil Van Dyke, que constaba de aproximadamente 7.500 reglas. Hoy en día el proyecto está abandonado. También se usa a Privoxy en combinación con TOR alrededor del mundo para sortear la censura en internet en países como Irán, Arabia Saudita, los Emiratos Árabes Unidos y en China, para evitar el sistema de censura de Internet del gobierno chino llamada Gran Cortafuegos. Bajo estas restricciones, muchos sitios web resultan bloqueados por sus respectivos gobiernos incluyendo muchas redes sociales, la wiki pedía y todos sus proyectos hermanos en China.

13.5 TOR

El 13 de agosto de 2004 en el 13 Simposio USENIX de Seguridad, Dingledine Roger, Nick Mathewson, y Syverson Pablo presentó TOR, router cebolla.
El código fuente de TOR se publica bajo la licencia BSD. A partir de abril de 2011.

TOR provee un canal de comunicación anónimo y está diseñado para ser resistente a ataques de análisis de tráfico. Por lo tanto, usando TOR es posible realizar una conexión a un equipo sin que este o ningún otro tenga posibilidad de conocer el número de IP de origen de la conexión.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

TOR es usualmente combinado con Privoxy para acceder a páginas web de forma anónima y segura. Privoxy es un proxy HTTP diseñado para proteger la privacidad en la navegación de internet. La interfaz de TOR es un proxy SOCKS (usualmente en el puerto 9050).

TOR o enrutamiento de cebolla es una técnica para la comunicación anónima en una red informática. Los mensajes son varias veces encriptado y enviada luego a través de nodos de la red varios llamados enrutadores cebolla. Cada router cebolla elimina una capa de cifrado para descubrir instrucciones de ruta, y envía el mensaje al siguiente router cuando se repite. Esto evita que los nodos intermedios conozcan el origen, destino y contenido del mensaje.

Una enrutamiento de cebolla (o simplemente cebolla) es una estructura de datos que "envuelve" un mensaje de texto con sucesivas capas de cifrado, de forma que cada capa puede ser 'abierto' (descifrado), como la capa de una cebolla el mensaje de texto original sólo se puede ver por la mayoría en:

-El remitente
-El último intermediario
-El receptor

Si hay cifrado de extremo a extremo entre el remitente y el destinatario, entonces ni siquiera el último intermediario puede ver el mensaje original, esto es similar a un juego de "pasar el paquete. Un intermediario que tradicionalmente se llama un nodo o un router. Para crear y transmitir una cebolla, los pasos siguientes medidas:

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

El remitente recoge los nodos de una lista proporcionada por un nodo especial llamado nodo de directorio (tráfico entre el remitente y el nodo de la guía también se puede cifrar o de otra manera anónima o descentralizada); los nodos seleccionados están ordenados para proveer un camino a través del cual el mensaje pueda dirigirse, este orden de los nodos se llama una cadena o un circuito.

Utilizando la criptografía de clave asimétrica, el remitente usa la clave pública de cada nodo elegido para envolver el mensaje de texto en las capas necesarias de cifrado: Las claves públicas se recuperan de una lista de una publicidad o por vía de negociación en el terreno para un uso temporal, y las capas se aplican en el orden inverso de la ruta del mensaje del emisor al receptor), con cada capa, el cliente incluye información para el nodo que corresponde con respecto al siguiente nodo al que debe ser la cebolla de transmisión.

Como la cebolla pasa a cada nodo de la cadena, una capa de cifrado se despega por el nodo de recepción (usando la clave privada que corresponde a la clave pública con la que la capa se ha cifrado), y luego la cebolla recién disminuida se transmite a entonces el nodo siguiente en la cadena. El último nodo de la cadena se despega en la última capa y transmite el mensaje original al destinatario. Con este enfoque significa que cada nodo de la cadena está muy bien consciente de sólo dos nodos:

-El nodo anterior de la que la cebolla se transmitió.
-El nodo de las actuaciones a que la cebolla siguiente debe ser transmitida.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

El peeling de distancia de cada capa de la cebolla hace que sea difícil o imposible de rastrear la cebolla sin poner en peligro un gran número de nodos.

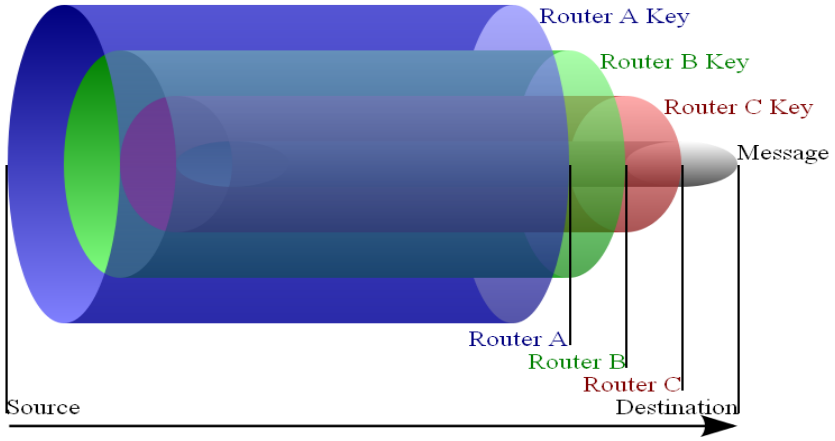


Figura 2 The Onion Routing

Fuente: http://highsec.es

13.6 Servicios ocultos

Aunque la característica más popular del TOR es anonimato de sus clientes, puede también proporcionar anonimato a los servidores. Usando la red del TOR, es posible a los servidores anfitrión ocultarse para que su localización y quienes los usen sean desconocidas.

Estos servicios usan una dirección .onion en vez de otro TLD existente. A pesar de que no existe un seguimiento de estos sitios, algunos servidores proporcionan direcciones útiles.

14 Universo y Muestra

Se aplicaran los métodos no parametritos en la abstracción de la muestra. Se tomara en cuenta a todas las personas, ello implica que se empleara la técnica del muestreo por cuotas el cual

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

consiste exclusivamente en aplicar encuestas, cuestionarios o entrevistas personales a las personas.

15 Esquema de la Tesis

Introducción
Justificación
Cap. 1. Generalidades
Cap. 2.Marco Teórico
Cap. 3.Modelo de la Implementación.
Cap. 4.Evaluacion
Conclusiones y Recomendaciones
Bibliografía
Anexos

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

ANEXO D

GLOSARIO

A

Adsl: Son las siglas de Asymmetric Digital Subscribe Line (Línea de Abonado Digital Asimétrica). Consiste en una línea digital de alta velocidad, apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado.

Administrador: Persona que se encarga de todas las tareas de mantenimiento de un sistema informático. Tiene acceso total y sin restricciones.

Anonimato: El anonimato es el estado de una persona siendo anónima, es decir, que la identidad de dicha persona es desconocida. Esto puede ser simplemente porque no se le haya pedido su identidad, como en un encuentro ocasional entre extraños, o porque la persona no puede o no quiere revelar su identidad.

Ataque: Intento de traspasar un control de seguridad.

Automatización: La automatización es un sistema donde se trasfieren tareas de producción, realizadas habitualmente por operadores humanos a un conjunto de elementos tecnológicos.

B

Base de datos: Conjunto de datos organizados de modo tal que resulte fácil acceder a ellos, gestionarlos y actualizarlos.

Blogger: Blogger es un servicio creado por Pyra Labs para crear y publicar una bitácora en línea. El usuario no tiene que escribir ningún código o instalar programas de servidor o de scripting. Blogger acepta para el alojamiento de las bitácoras su propio servidor (Blogspot) o el servidor que el usuario especifique (FTP o SFTP).

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

Bridges: Dispositivo de interconexión que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Este interconecta dos segmentos de red (o divide una red en segmentos) haciendo el pasaje de datos de una red para otra, con base en la dirección física de destino de cada paquete.

C

Cifrado: El cifrado es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

Cisco: Cisco Systems es una empresa multinacional con sede en San José (California, Estados Unidos), principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones

Claves Simétricas: Es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma.

Contingencia: Procedimientos alternativos al orden normal de una empresa, cuyo fin es permitir el normal funcionamiento de esta, aun cuando alguna de sus funciones se viese dañada por un accidente interno o externo.

Cortafuegos: Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Cookies: Es un fragmento de información que se almacena en el disco duro del visitante de una página web a través de su modo a petición

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

del servidor de la página. Esta información puede ser luego recuperada por el servidor en posteriores visitas. En ocasiones también se le llama "huella".

Criptografía: Criptografía proviene del griego y se puede traducir como “La manera de escribir raro” (crypto’s de extraño y graphos de escritura). Consiste en modificar los datos de un archivo para evitar así que los puedan leer personas no deseadas. Esta técnica ha tenido su principal aplicación en los ejércitos y en la diplomacia.

D

Darpa: (Defense Advanced Research Project Agency o DARPA). DARPA es una agencia del Departamento de Defensa del gobierno de los Estados Unidos, responsable del desarrollo de nuevas tecnologías usadas en el área militar.

Desencriptación/ Descifrado: Recuperación del contenido real de una información previamente cifrada.

DNS: Servidor de Nombres de Dominio. Servidor automatizado utilizado en el internet cuya tares es convertir nombres fáciles de entender a direcciones numéricas de IP.

E

Encriptación: La encriptación es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

EFF: Es una organización sin ánimo de lucro con sede en Estados Unidos con el objetivo declarado de dedicar sus esfuerzos a conservar los derechos de libertad de expresión, como los protegidos por la Primera Enmienda a la Constitución de Estados Unidos, en el contexto de la era digital actual.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

Enrutar: Es redirigir o encaminar una conexión a un equipo en concreto que dispone de un servicio específico o un software que necesita realizar conexiones por un puerto X.

F

Firma Digital: Esquema matemático que sirve para demostrar la autenticidad de un mensaje digital o de un documento electrónico. Una firma digital da al destinatario seguridad en que el mensaje fue creado por el remitente, y que no fue alterado durante la transmisión. Las firmas digitales se utilizan comúnmente para la distribución de software, transacciones financieras y en otras áreas donde es importante detectar la falsificación y la manipulación.

Firewall: Barrera de protección o procedimiento de seguridad que coloca un sistema de cómputo programado especialmente entre una red segura y una red insegura. Un sistema o combinación de sistemas que fija los límites entre dos o más redes y restringe la entrada y salida de la información.

FTP: (File Transfer Protocol: Protocolo de transferencias de archivos) Un conjunto de protocolos mediante el cual pueden transferirse archivos de una computadora a otra. FTP es también el nombre de un programa que usa los protocolos para transferir archivos de ida y vuelta entre computadoras.

G

GLP: Es una licencia creada por la Free Software Foundation a mediados de los 80, y está orientada principalmente a proteger la libre distribución, modificación y uso de software. Usado por Linux.

GNU: Es un acrónimo recursivo que significa GNU No es Unix (GNU is Not Unix). Puesto que en inglés "gnu" (en español "ñu") se pronuncia igual que "new", Richard Stallman recomienda pronunciarlo "guh-noo".

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

Gusanos: Son programas que se transmiten a sí mismos de una maquina a otra a través de una red. Se fabrican de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.

H

Hardware: Componentes electrónicos, tarjetas, periféricos y equipo que conforman un sistema de computación.

HTTP (Hyper Text Transfer Protocol): Es un protocolo de la capa de aplicaciones con la velocidad necesaria para sistemas de información hipermediales en un ambiente distribuido y colaborativo.

HTML: siglas de HyperText Markup Language (Lenguaje de Marcado de Hipertexto), es el lenguaje de marcado predominante para la elaboración de páginas web. Es usado para describir la estructura y el contenido en forma de texto, así como para complementar el texto con objetos tales como imágenes.

I

Implementación: Es la realización de una aplicación, o la ejecución de un plan, idea, modelo científico, diseño, especificación, estándar, algoritmo o política.

Internet: Conjunto de redes de ámbito mundial conectadas entre sí mediante el protocolo IP (Internet Protocol).

IP (Internet Protocol): Protocolo de comunicación sin conexión. Proporciona el servicio de envío de paquetes para los protocolos soportados TCP, UDP, ICMP. El IP tiene prestaciones para direccionamiento, especificación del tipo de servicio, fragmentación y rearmado, y seguridad.

IPV6: Es una versión del protocolo Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol versión 4

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

(IPv4) RFC 791, que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet.

IRC: Es un protocolo de comunicación en tiempo real basado en texto, que permite debates entre dos o más personas. Se diferencia de la mensajería instantánea en que los usuarios no deben acceder a establecer la comunicación de antemano, de tal forma que todos los usuarios que se encuentran en un canal pueden comunicarse entre sí, aunque no hayan tenido ningún contacto anterior.

ISP (Internet Service Provider): Compañía o individuo dedicado a vender acceso (servicio) a Internet.

J

Junbuster: Explicado en el marco teórico.

K

Keep-alive: Indica si se permiten o no las conexiones persistentes, es decir más de una petición por conexión. Puede tomar los valores On u Off. El valor predeterminado es On.

Kernel: se refiere al núcleo o kernel de un sistema operativo.

L

LAN (Local Area Network): red de área local. Red de datos de alta velocidad y bajo nivel de error que cubre un área geográfica relativamente pequeña.

LRU (Least Recently Used): El usado menos recientemente.

LFU (Least Frequently Used): El usado menos frecuentemente.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE TESIS UCSM
UNIVERSIDAD CATÓLICA DE SANTA MARÍA

M

Modem: Modulador-demodulador. El módem realiza la modulación y demodulación de las señales digitales producidas por el computador para adaptarlas a la red de telecomunicación. De esta forma, permite a la computadora transmitir información a través de una línea telefónica, fibra óptica u otro dispositivo. La velocidad de transmisión de los módem se mide en bits por segundo o en baudios.

N

NAT: Es un mecanismo utilizado por enrutadores IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados.

O

Ordenadores: Es una máquina electrónica que recibe y procesa datos para convertirlos en información útil.

P

Paquete: Un paquete corresponde a la capa de red del Modelo OSI, por ejemplo en el caso del protocolo IP. Siendo el paquete la unidad de datos de protocolo (PDU) de la capa de red.

Plugins: (del inglés "conectable"), add-on (agregado), complemento, conector o extensión.

Privoxy: Programa que funciona como proxy web, usado frecuentemente en combinación con TOR y Squid.

Protocolo: Conjunto de normas (lenguaje de reglas y símbolos) que rige cada tipo de comunicación entre dos computadoras (intercambio de información).

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

Proxy: entidad que, a fin de mayor eficiencia, esencialmente suple otra identidad.

Proxy cache: Permite incrementar la velocidad de acceso a Internet al mantener localmente las páginas más consultadas por los usuarios de una organización, evitando las conexiones directas con los servidores remotos.

R

Router: Dispositivo de capa de red que utiliza una o más métricas para determinar la ruta óptima por la cual se enviará el tráfico de la red. Ocasionalmente paquetes de una red a otra en base a la información de capa de red.

S

Script: Archivo de órdenes o archivo de procesamiento por lotes es un programa usualmente simple, que por lo regular se almacena en un archivo de texto plano.

Squid: programa que implementa un servidor proxy.

Socks: Es un protocolo de Internet que permite a las aplicaciones Cliente-servidor usar de manera transparente los servicios de un firewall de red. SOCKS es una abreviación de "SOCKetS".

Spam: correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

SSL (Secure Sockets Layers): Protocolo que provee una conexión segura entre dos Hosts.

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

U

UTMP: Fichero binario con información de cada usuario que está conectado en un momento dado.

T

TCP (Transmission Control Protocol): Protocolo orientado a conexión. Su función principal es proporcionar mecanismos que ofrezcan seguridad en el proceso de entrega de los paquetes a su destino, así como ordenar paquetes de información y evitar la petición de estos.

TCP/IP (Transfer Control Protocol/ Internet Protocol):
Arquitectura de red con un conjunto de protocolos que permiten compartir recursos a través de una red. Esta familia de protocolos es la más importante difundidos en la actualidad, por ser la base de Internet.

V

VPN: VPN no es más que una estructura de red corporativa implantada sobre una red de recursos de carácter público, pero que utiliza el mismo sistema de gestión y las mismas políticas de acceso que se usan en las redes privadas.

W

WAN: Redes que se extienden sobre un área geográfica extensa. Contiene una colección de máquinas dedicadas a ejecutar los programas de usuarios (hosts).

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis

REPOSITORIO DE
TESIS UCSM

UNIVERSIDAD
CATÓLICA
DE SANTA MARÍA

X

XDSL: Se conoce como **xDSL** a la familia de tecnologías de acceso a Internet de banda ancha basadas en la digitalización del bucle de abonado telefónico (el par de cobre). La principal ventaja de xDSL frente a otras soluciones de banda ancha (cable módem, fibra óptica, etc.)

Z

Publicación autorizada con fines académicos e investigativos
En su investigación no olvide referenciar esta tesis