# EJEMPLOS PRÁCTICOS EN EL LABORATORIO DE CYBERSEGURIDAD - UPEC

## PRACTICAL EXAMPLES IN THE CYBERSECURITY LABORATORY - UPEC

RECIBIDO 01/10/2020 - ACEPTADO 14/12/2020

DOI: https://doi.org/10.32645/13906925.1002

**MARCO ANTONIO YANDÚN VELASTEGUÍ**

- Universidad Politécnica Estatal del Carchi
- Magister en Auditoría de Tecnologías de la Información
- marco.yandun@upec.edu.ec
- https://orcid.org/0000-0001-5627-9838

**JAIRO VLADIMIR HIDALGO GUIJARRO**

- Universidad Politécnica Estatal del Carchi
- Magister en Redes de Comunicaciones
- jairo.hidalgo@upec.edu.ec
- https://orcid.org/0000-0001-8165-0192

Cómo citar este artículo:
Yandún, M., & Hidalgo, J. (Julio - diciembre de 2020). "Ejemplos prácticos en el Laboratorio de Cyberseguridad - Upec". *Sathiri: sembrador, 15(2)*, 273-289. https://doi.org/10.32645/13906925.1002

## Resumen

*En la actualidad, por medio del internet, existen personas que buscan vulnerar los sistemas o aplicaciones, para ello utilizan diferentes ciberataques, se puede mencionar varias técnicas como Session Hijack, o ataque de suplantación y herramientas como John the Ripper, estos son los ataques más utilizados por los hackers para obtener la sesión de los usuarios conectados en la red. Este tipo de ataque se lo realiza a través de la red aprovechando las debilidades del sistema o aplicativo, ya que se conoce que la información sensible se transporta entre sesiones, para ello se utiliza el envenenamiento ARP con el Sniffer que permiten capturar y visualizar todo el tráfico de la red, obteniendo así el puerto y protocolo que se están utilizando para la conexión. En el presente documento se realizaron las prácticas en el laboratorio de CyberSeguridad UPEC, este laboratorio fue implementado como parte del Proyecto de investigación "La seguridad y el servicio informático en el Gobierno Provincial del Carchi (Ecuador) y las Alcaldías Municipales de Pasto, Ipiales y Túquerres (Colombia)". Las prácticas mostraron la intercepción de sesión a un usuario que se encuentra conectado a la máquina virtual de Centos utilizando Telnet, que es un protocolo que permite acceder a otra máquina y utilizarla remotamente desde la máquina virtual de Windows 7. Kali Linux fue utilizada como el atacante y realizó un escaneo de la red, aplicando "un envenenamiento" para luego acceder a la conexión, probando así la facilidad con la que se puede hacer la sustracción de sesión a los usuarios que se encuentran conectados, por lo que se recomendó usar protocolos de encriptación de los encabezados para que no sea tan fácil acceder a la conexión de la víctima.*

***Palabras claves:*** *Cyber ataque, Session Hijack, John the Ripper, Laboratorio CyberSeguridad-UPEC.*

## Abstract

*Currently through the internet there are people who seek to violate systems or applications, for this they use different cyberattacks, several techniques such as Session Hijack, or spoofing attack and tools such as John the Ripper, these are the most used attacks hackers to obtain the session of users connected to the network. This type of attack is carried out through the network, taking advantage of the weaknesses of the system or application, since it is known that sensitive information is transported between sessions, for this purpose, ARP poisoning is used with the Sniffer that allows to capture and visualize all the network traffic, thus obtaining the port and protocol that are being used for the connection. In this document, the practices were carried out in the UPEC Cybersecurity laboratory, this laboratory was implemented as part of the research project "Security and computer service in the Provincial Government of Carchi (Ecuador) and the Municipal Mayors of Pasto, Ipiales and Túquerres (Colombia) "The practices showed the interception of a session to a user who is connected to the Centos virtual machine using Telnet, which is a protocol that allows access to another machine and to use it remotely from the Windows 7 virtual machine. Kali Linux was used as the attacker and carried out a network scan and applied "poisoning" to then access the connection, thus testing the ease with which session subtraction can be done to users who are connected, so it is He recommended using encryption protocols for the headers so that it is not so easy to access the victim's connection.*

***Keywords:*** *Cyber attack, Session Hijack, John the Ripper, CyberSeguridad-UPEC laboratory.*

**Cómo citar este artículo:**
**Yandún, M., & Hidalgo, J. (Julio - diciembre de 2020). "Ejemplos prácticos en el Laboratorio de Cyberseguridad - Upec". *Sathiri: sembrador, 15(2),* 273-289. https://doi.org/10.32645/13906925.1002**

## 1. Introducción

Hoy en día los seres humanos dependemos mucho de las comunicaciones por medio de la conexión a internet para realizar varias actividades, según Amaro, Andrade, Macías y Rodríguez (2017).

> Con tener una computadora con conexión a internet hace que el ciberespacio sea un espacio atractivo para atacar y se convierta en un campo de batalla porque por medio de estos materiales es fácil acceder, robar y borrar información de otro ordenador se encuentre ubicado en cualquier parte del mundo con el fin de causar daño, físico, económico, durante el año 2012 donde Amaro cita a Stem (2013) se ha contabilizado 115, 000 víctimas por ciberataques a diario por 288 mil millones de dólares anuales, lo que muchos países como EEUU, China, Rusia han invertido en crear y desarrollar agencias que se dediquen a la defensa y ataque del ciberespacio todo por lo económico mientras se tengan conexión a internet.

Según indican Martínez, Niño y Viniegra (2019):

> En el año 2017 comienza mundialmente un ciberataque con un malware o software malicioso denominado WannaCry, que afecto a varias empresas españolas bloqueando las redes de comunicación y pidiendo un rescate para la liberación del sistema, donde este software malicioso fue tema de interés por parte de investigadores sobre su análisis tecnológico, donde se reconoce que este tipo de ataque no es nuevo y su efecto fue conocido por los precedentes presentados por google en el año 2010, lo que la investigación se basa en la documentación verídica y tiene dos procedimientos a realizarse, el diseño muestra de este malware se realiza a través de los datos de difusión, cuantitativa y cualitativa realizando el ciberataque y analizando los resultados así obteniendo reputación posita, neutro y negativa, dando como conclusión que la crisis son imprevistas por su esencia afectando a la compañía, dando a conocer los porcentajes 69% de mayor magnitud y en enfoque positivo el 20%, dando una rápida solución al ciberataque y la colaboración con todos los agentes implicados dando conocer las debilidades de la empresa lo que provocó que la compañía desaparezca en relación con el ciberataque.

Con la llegada de la tecnología de la información también aparecen nuevos sistemas de delincuencia en términos informáticos. Urueña (2015) indica que:

> El Cyber delincuente utiliza varias técnicas las cuales se aplican individualmente o de forma combinada donde se pueden mencionar los virus informáticos, el envío masivo de correo no deseado o Spam, el envío o instalación de archivos espías o Keylogers, el uso de troyanos para el control remoto de los sistemas, entre otros.

El trabajo de Anuj Kumar Baitha, *titulado Session Hijacking and Prevention Technique,* menciona que el secuestro de sesión o Session Hijacking es utilizado para el acceso no autorizado a sitios web de redes sociales y bancas, es por ello que el trabajo mencionado anteriormente proporciona información acerca del ataque, como los tipos de ataque que pueden realizarse, las herramientas que pueden utilizarse, la metodología del ataque y propone algunos mecanismos de seguridad. Como conclusiones, se obtuvo que algunas personas y expertos en seguridad aún no son conscientes de la existencia de este tipo de ataques y de las medidas que deben ser tomadas para evitarlos (Baitha, 2018).

**Cómo citar este artículo:**
**Yandún, M., & Hidalgo, J. (Julio - diciembre de 2020). "Ejemplos prácticos en el Laboratorio de Cyberseguridad - Upec". *Sathiri: sembrador, 15(2),* 273-289. https://doi.org/10.32645/13906925.1002**

En la misma línea de investigación, Jain, Sahu y Tomar (2015) publican su paper titulado "Session Hijacking: Threat Analysis and Countermeasures", referente al robo de sesión mostrando los nuevos riesgos a los que se enfrenta la información financiera y la identidad afectando así a la integridad de la víctima. Ellos también manifiestan que la información sensible del usuario se transporta constantemente entre sesiones y los hackers están realizando sus mejores técnicas para robarlos. Estos autores muestran que el secuestro de sesiones es una de las principales amenazas de las aplicaciones web y se proporciona medidas para este tipo de ataque (Jain, Sahu & Tomar, 2015).

Herrera menciona que existen varios peligros al conectarse a una red WiFi, los cuales muchas personas desconocen, estas pueden estar ubicadas en parques, centros comerciales e instituciones mientras que otras personas aprovechan su conocimiento técnico para vulnerar la seguridad de los individuos. Se constató que los usuarios no poseen protección al momento de navegar en internet, ya que la mayoría de las redes son vulnerables a ataques como Hijacking, envenenamiento ARP, ataque DOS, Sniffing, Spoofing. La mayor parte de la población desconoce el peligro de utilizar una red Wifi, las personas realizan pagos por internet sin tener activado el firewall, es por esto que el nivel de conocimiento en las redes WiFi es medio–bajo (Herrera, 2015).

En la temática que se está tratando, Armas (2017) indica que el proyecto presenta el análisis de vulnerabilidades del sistema de nombre de dominio DNS, con la ayuda del análisis de resultados se verá la conveniencia de utilizar mecanismos de protección y así evaluar su efectividad. Los resultados de los ataques fueron exitosos, por lo cual se han colocado medidas de protección como, por ejemplo, a los ataques de DNS Hijacking realiza un ataque MITM, el cual se lo puede impedir mediante tablas ARP estáticas, esto en el lado del usuario. Los ataques efectuados contra los servidores DNS afectan a otros servicios de internet como el correo electrónico, ya que no se pueden adquirir las direcciones IP.

Todo esto se logra por la forma como están constituidas las redes de computadores, según su arquitectura, topología, protocolos y métodos de acceso. Hidalgo y Yandún (2019) explican: "Protocolos de comunicación: es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para trasmitir información por medio de cualquier tipo de variación con una magnitud física (pág. 33).

Con el uso del Laboratorio de CyberSeguridad de la UPEC, se desarrollaron prácticas referentes a intercepción de sesión de usuarios, modificaciones de tablas de registro ARP. Para demostrar las vulnerabilidades de las conexiones, se utilizó máquinas virtuales con sistemas operativos Windows para clientes y Linux para atacantes, y se recomienda el cifrado del canal de comunicación para evitar este tipo de ataques.

## 2.- Materiales y Métodos – revisión literaria.

En primer lugar, se indica que el tipo de investigación aplicada en el presente trabajo es Explicativa y Experimental. Es Explicativa porque se indicó la razón por la que las sesiones de usuarios son interceptadas e incluso sus sesiones sustraídas y utilizadas por los atacantes; y es Experimental porque se realizaron las pruebas prácticas en la red de computadores y el escenario de estas pruebas fue el laboratorio de CyberSeguridad de la UPEC.

La intención del ataque informático es aprovechar las debilidades que se encuentras innatas en las aplicaciones, sistemas, protocolos, hardware, etc. Con el fin de causar daño y conseguir un beneficio económico o reconocimiento (De la Hoz, 2015).

Además, Auquilla y Espin (2019), mencionan a Acens (2017), quien afirma que un ciberataque se puede definir como una serie de operaciones que ponen en riesgo un sistema o aplicativo, entre estos ataques se puede encontrar el secuestro de sesión que roban la identidad del usuario manipulando los paquetes y protocolos que se utilizan para la conexión entre el cliente y el servidor para la realización de actividades fraudulentas.

Cómo citar este artículo:
Yandún, M., & Hidalgo, J. (Julio - diciembre de 2020). "Ejemplos prácticos en el Laboratorio de Cyberseguridad - Upec". *Sathiri: sembrador, 15(2),* 273-289. https://doi.org/10.32645/13906925.1002

Por otro lado, Pulla (2019) indica que el secuestro de sesión es un ataque combinado, en el que se captura y se altera el tráfico de red utilizando técnicas de Spoofing con la finalidad de redireccionar la conexión al atacante; dicho en otras palabras, es el acceso no autorizado de personas con fines maliciosos atacando la integridad del servicio. En seguridad, es difícil combatir este tipo de ataque.

Otro autor menciona que Session Hijacking se refiera a la intrusión con fines maliciosos a una sesión establecida entre cliente y servidor. Se comprende como sesión a la conexión entre el usuario y servidor utilizando dos dispositivos, esta conexión es iniciada, sostenida y finalizada. Este tipo de ataques también pueden ser considerados como ataques de suplantación (Fernández, 2019).

Vila (2017) afirma que Session Hijack es un ataque que tiene como objetivo acceder a la conexión de la víctima sin las credenciales de la misma. Para realizar este ataque, primero se realiza un envenenamiento ARP para visualizar el tráfico de la red, una vez capturado nuestro objetivo se empieza a husmear en el tráfico de la víctima con el fin de capturar las cookies de sesión y rehusarlas en un navegador.

Armas (2017) señala que el Hijacking es uno de los ataques más comunes, como por ejemplo el Hijacking DNS el cual consiste en interceptar el intento de un usuario DNS para redirigir a la persona a una página web diferente, una vez dentro del sitio pueden ser víctimas de ataque de phishing.

Otro tipo de Hijacking es el secuestro de sesión, este consiste en robar una sesión de un usuario que esté conectado a otro ordenador, pero a la misma red, así el atacante podrá obtener información sensible de la víctima y tener control del dispositivo (Herrera, 2015).

Olivares (2018) explica que, debido a su baja seguridad, el Hijacking puede dejar expuestos los métodos de conexión no cifrados, como sucede, por ejemplo, con Telnet, pero, a pesar de esto, el Hijacking puede dejar obsoletas todas las autentificaciones por dirección IP. También, Melgar (2015) muestra que bastantes veces el servidor se encuentra en nuestra propia red LAN, lo cual es utilizado por los hackers con la intención de secuestrar las direcciones DNS redirigiendo a los DNS falsos e inyectar malware en el PC.

Para González Paz, Beltrán Casanova y Fuentes Gari (2016), los ataques activos significan crear flujos de datos de transmisión, sus objetivos pueden ser maliciosos como suplantación de identidad o dar de baja un sitio web. Algunos de estos ejemplos son el ataque del hombre en el medio, secuestro de sesión (Hijacking), denegación de servicio (DOS).

Los tipos de ataques informáticos también tienen relación al aprendizaje autónomo, aplicación de redes neuronales y el análisis de tráfico de datos en las redes de comunicaciones, tal como mencionan Hidalgo y Yandún (2020).

## Secuestro de sesión con Session Hijacking

## Telnet Session Hijacking

Para la realización de la práctica se debe tener instalado Kali Linux, Centos y Windows XP en la máquina virtual. De esta manera, Kali Linux será el atacante, el servidor que se utilizará es el de Centos y el usuario atacado será XP.

Kali Linux realizará un ataque mediante ARP poisoning utilizando Ettercap para lograr obtener las credenciales de la sesión de telnet iniciadas por Windows, usando el servidor Centos. El atacante romperá la conexión del usuario Windows XP. Por último, el atacante dejara un nuevo directorio de inicio para las víctimas.

Cómo citar este artículo:
Yandún, M., & Hidalgo, J. (Julio - diciembre de 2020). "Ejemplos prácticos en el Laboratorio de Cyberseguridad - Upec". *Sathiri: sembrador, 15(2),* 273-289. https://doi.org/10.32645/13906925.1002

**Requisitos:** Instalar Kali Linux, Centos y Windows XP en Virtual Vox.

**Procedimiento.**

**Descargar e instalar** el servidor telnet en Centos para que el usuario Windows XP se pueda Conectar.

# yum install –y telnet* utilice este comando para descargar todos los paquetes del servidor

# systemctl start telnet.socket

#systemctl enable telnet.socket

Para activar el Puerto ingresamos los siguientes comandos.

```
[root@localhost ~]# firewall-cmd --permanent --add-port=23/tcp
success
[root@localhost ~]# firewall-cmd --reload
success
```

Por ultimo ingresamos el comando # ipadd para conocer la dirección Ip del servidor que será 192.168.1.100

```
[root@localhost ~]# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast sta
00
    link/ether 08:00:27:3d:b5:c5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 brd 192.168.1.255 scope global dynamic enp0s3
       valid_lft 85361sec preferred_lft 85361sec
    inet6 fe80::53de:8790:13ff:2df/64 scope link
       valid_lft forever preferred_lft forever
3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue stat
```

**Accesos.** - el usuario de Windows XP utilizará sesión en el servidor de Centos. Para ello activamos las opciones de Telnet.

>Inicio > Ejecutar > services.msc> aceptar

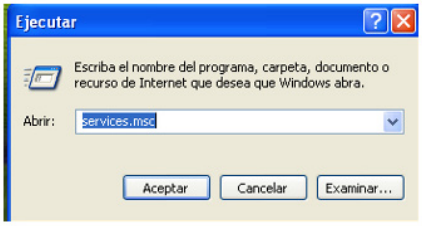


**Figura 1:** *Windows Xp Ejecutar*

Cómo citar este artículo:
Yandún, M., & Hidalgo, J. (Julio - diciembre de 2020). "Ejemplos prácticos en el Laboratorio de Cyberseguridad - Upec". *Sathiri: sembrador, 15(2),* 273-289. https://doi.org/10.32645/13906925.1002

Buscar Telnet y habilitar el servicio

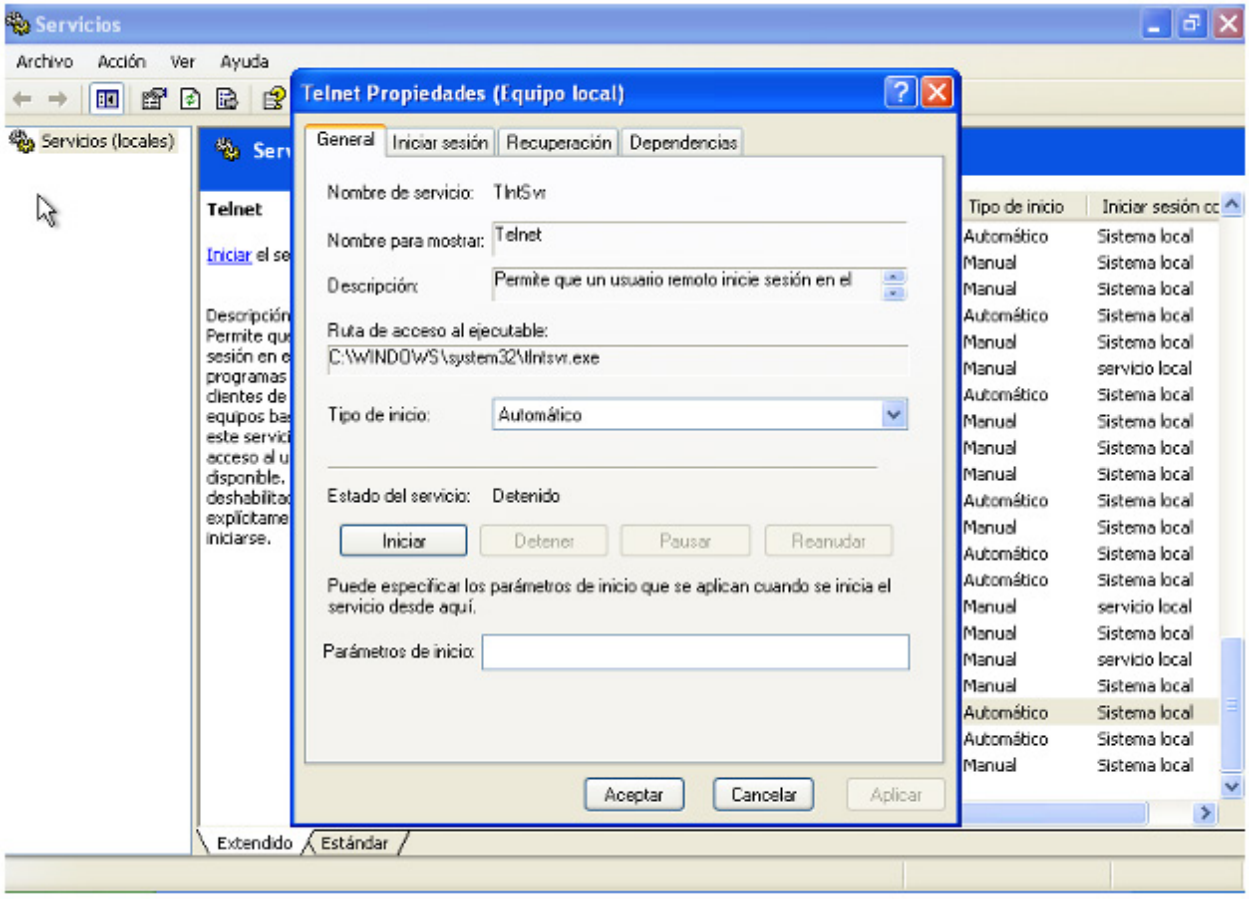


**Figura 2**: *Services.msc Activar Telnet.*

Para establecer la conexión con Centos, Ingresar al cmd y colocar Telnet seguido de la dirección IP del servidor, enter.

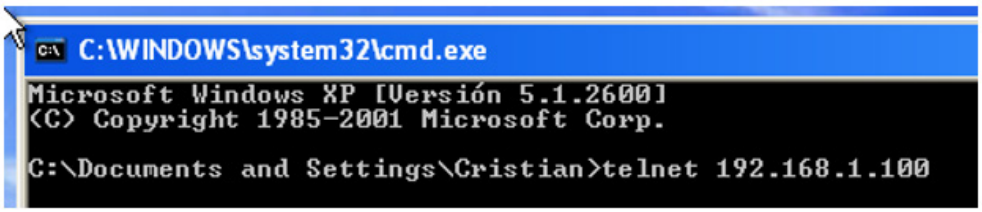


**Figura 3**: *Windows XP CMD.*

Cómo citar este artículo:
Yandún, M., & Hidalgo, J. (Julio - diciembre de 2020). "Ejemplos prácticos en el Laboratorio de Cyberseguridad - Upec". *Sathiri: sembrador, 15(2),* 273-289. https://doi.org/10.32645/13906925.1002

**IP de Windows XP** Para conocer la dirección de Windows XP presionamos en el CMD el comando ipconfig /all

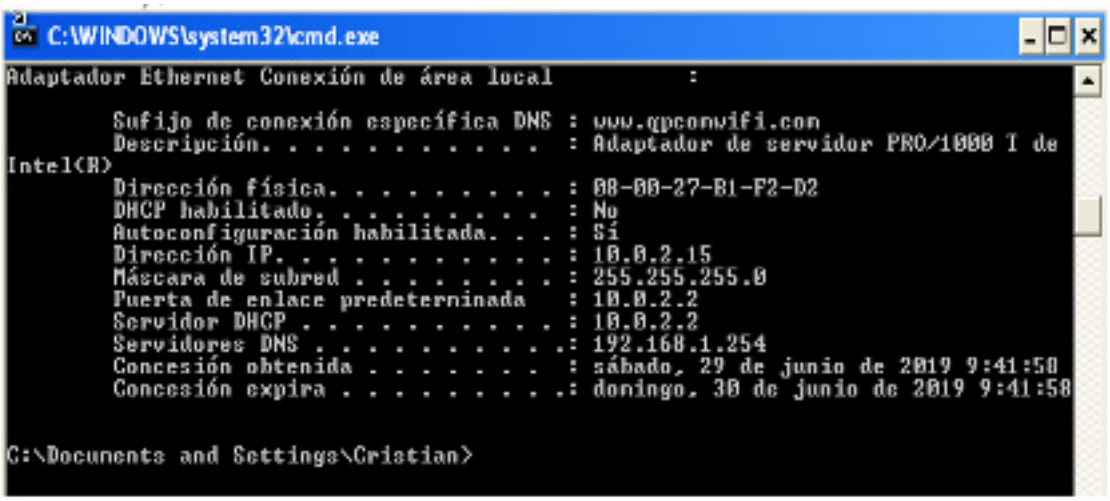


**Figura 4**: *Comando ip config.*

Ingresamos el nombre y la contraseña para acceder al servidor. De esta manera el usuario Windows XP se encuentra conectado a Centos por Telnet.

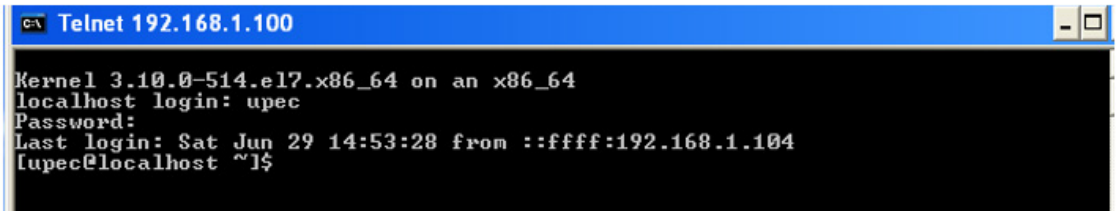


**Figura 5**: *Conexión a Telnet.*

Ahora ya tenemos conexión con el servidor.

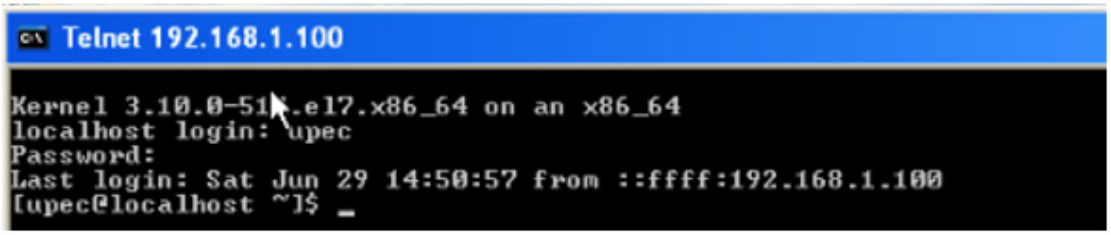


**Figura 6**: *Conexión con el servidor.*

Ingresar al entorno de Kali Linux > Aplicaciones >Ettercap > Sniff > Unifled Sniffing Luego, Hosts > Scan for Hosts para escanear todas las subredes y host anfitrión.

Cómo citar este artículo:
Yandún, M., & Hidalgo, J. (Julio - diciembre de 2020). "Ejemplos prácticos en el Laboratorio de Cyberseguridad - Upec". *Sathiri: sembrador, 15(2),* 273-289. https://doi.org/10.32645/13906925.1002

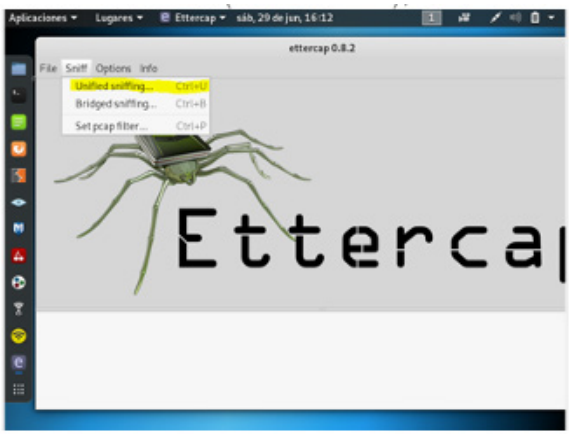


**Figura 7**: *Linux Ettercap.*


**Figura 8:** *Ettercarp, Escaneo de Host.*

Presionamos Hosts List para mostrar los hosts descubiertos.

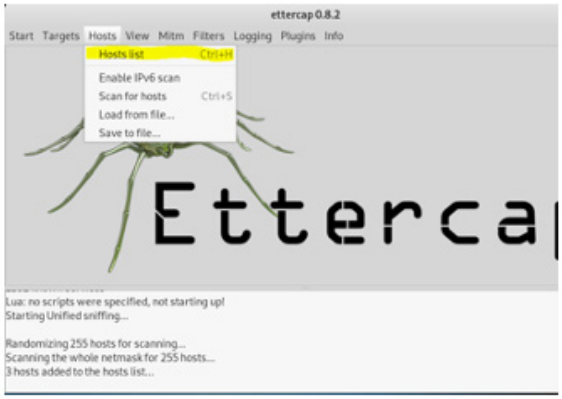


**Figura 9:** *Ettercap Host*

Cómo citar este artículo:
Yandún, M., & Hidalgo, J. (Julio - diciembre de 2020). "Ejemplos prácticos en el Laboratorio de Cyberseguridad - Upec". *Sathiri: sembrador, 15(2)*, 273-289. https://doi.org/10.32645/13906925.1002

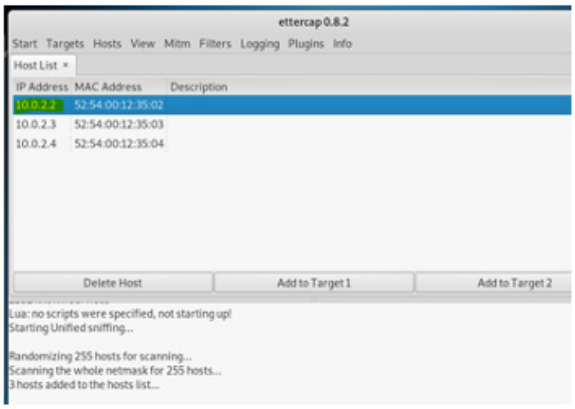


**Figura 10**: *Lista de host Descubiertos.*

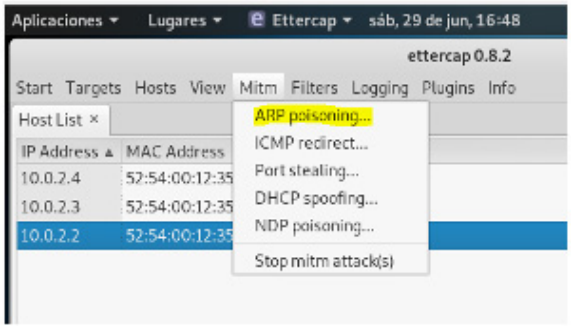


**Figura 11:** *Ettercap-Mitm.*

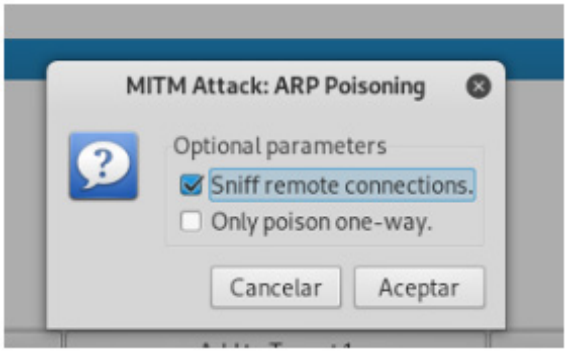


**Figura 12:** *ARP poisoning.*

En otro espacio, Ejecutar Wireshark y agregar un filtro en la parte superior para mostrar el tráfico de ARP.

Se puede observar cómo se envían los ARP desde Kali Linux con direcciones MAC incorrectas para las máquinas virtuales de Centos y Windows XP. Ahora cualquier dispositivo de la subred que intente enviar paquetes a Centos o XP serán engañadas y enviarán el paquete a Kali.

Cómo citar este artículo:
Yandún, M., & Hidalgo, J. (Julio - diciembre de 2020). "Ejemplos prácticos en el Laboratorio de Cyberseguridad - Upec". *Sathiri: sembrador, 15(2)*, 273-289. https://doi.org/10.32645/13906925.1002

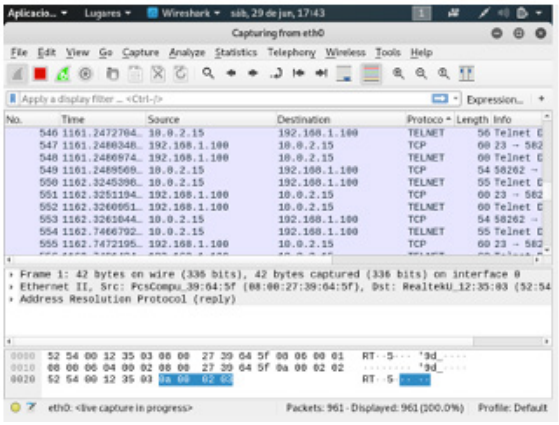


**Figura 13**: *Wireshark.*

Descargar Shijack del siguiente link https://packetstormsecurity.com/


**Figura 14:** Link de Descarga.

Para descomprimir el archivo # tar xvf shijack.tgz
# cd Shijack para ingresar a la carpeta descomprimida.

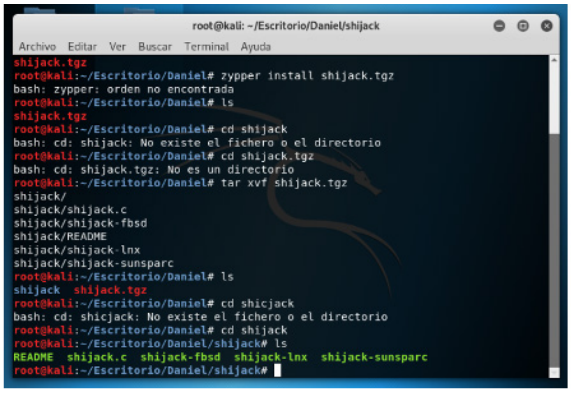


**Figura 15:** Instalación de Shijack.

Luego escribimos es código #./ shijack-lnx eth0 la ip de destino el puerto acompañado de la ip del servidor y el puerto 23 que es el de telnet.

Cómo citar este artículo:
Yandún, M., & Hidalgo, J. (Julio - diciembre de 2020). "Ejemplos prácticos en el Laboratorio de Cyberseguridad - Upec". *Sathiri: sembrador, 15(2),* 273-289. https://doi.org/10.32645/13906925.1002

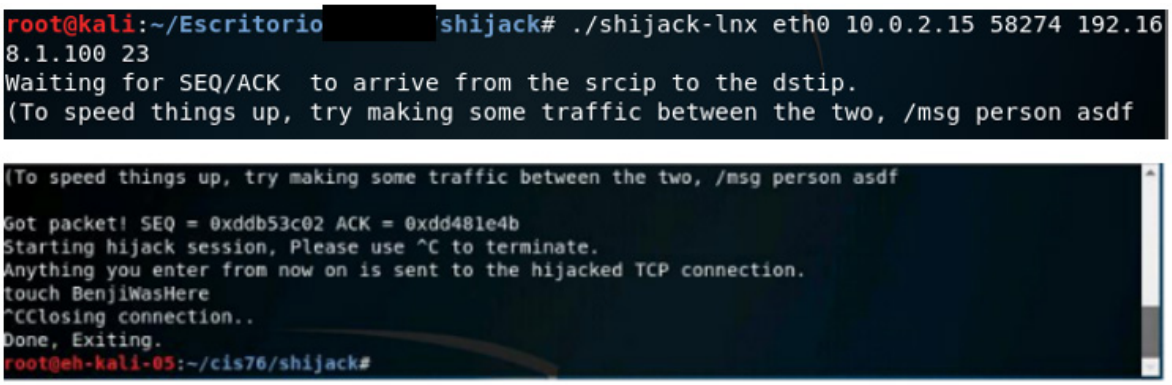


**Figura 16**: *Secuestro de la IP.*

En la sesión real con Windows muestra que la conexión se ha perdido de esta forma se realizó con éxito la práctica de captura de sesión.

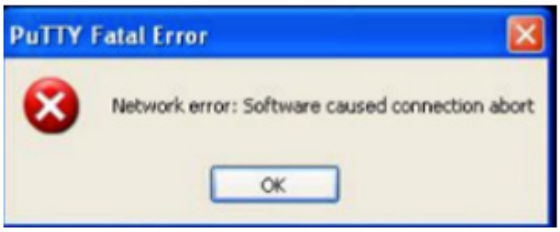


**Figura 17**: *Pérdida de conexión.*

**Cyber Ataque con John the Ripper.**

Desde una la máquina virtual VMWare, al sistema operativo de Kali Linux clic en cmd.

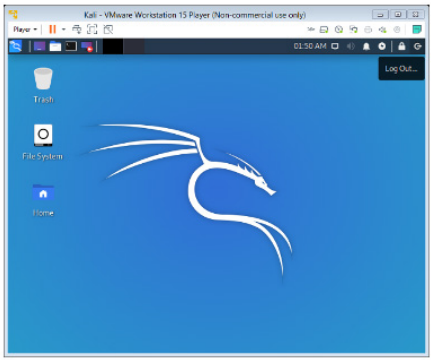

**Figura 18:** *Pantalla de Kali Linux.*

Generar e ingresa credenciales usuario y contraseña para realizar la práctica.

Cómo citar este artículo:
Yandún, M., & Hidalgo, J. (Julio - diciembre de 2020). "Ejemplos prácticos en el Laboratorio de Cyberseguridad - Upec". *Sathiri: sembrador, 15(2)*, 273-289. https://doi.org/10.32645/13906925.1002

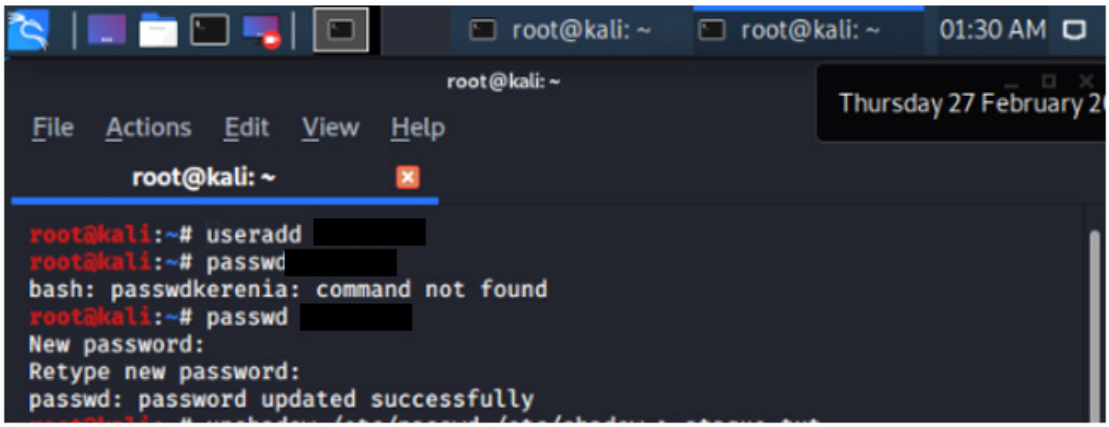


**Figura 19**: *Creación de un usuario y contraseña.*

Escribimos el comando nano passwd para poder ver la contraseña encriptada del usuario.

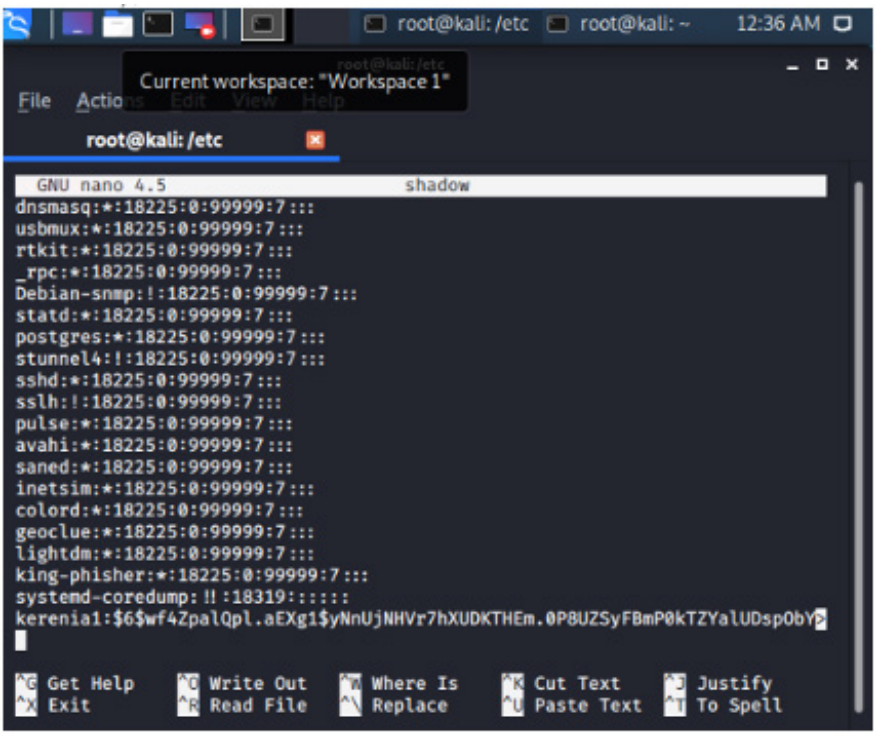


**Figura 20:** *Se muestra la clave encriptada dentro del sistema.*

Ejecutando el comando unshadow /etc/passwd /etc/shadow > ataque.txt, esto sirve para unir las dos carpetas de passwd y shadow, el cual se agrega a la carpeta de /root /.john

Cómo citar este artículo:
Yandún, M., & Hidalgo, J. (Julio - diciembre de 2020). "Ejemplos prácticos en el Laboratorio de Cyberseguridad - Upec". *Sathiri: sembrador, 15(2),* 273-289. https://doi.org/10.32645/13906925.1002

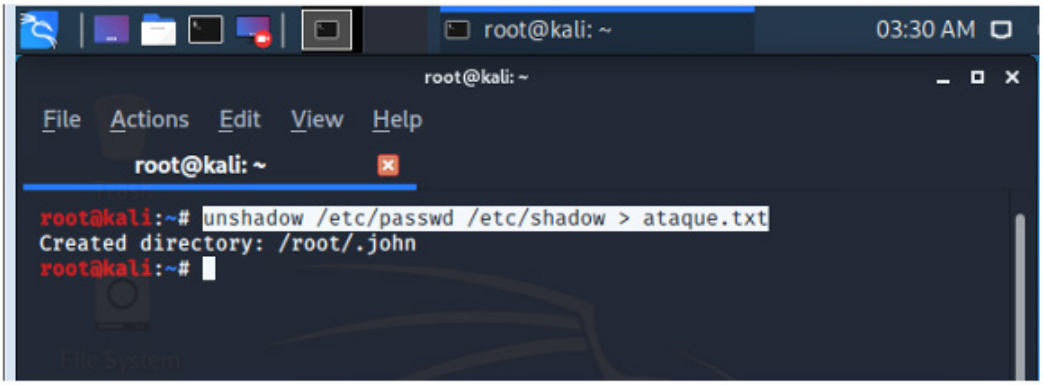


**Figura 21**: *Para crear los archivos de usuario.*

Ejecutar el comando John the Ripper con el siguiente formato John –format=sha512crypt ataque.txt, donde observamos que este craquea la contraseña.

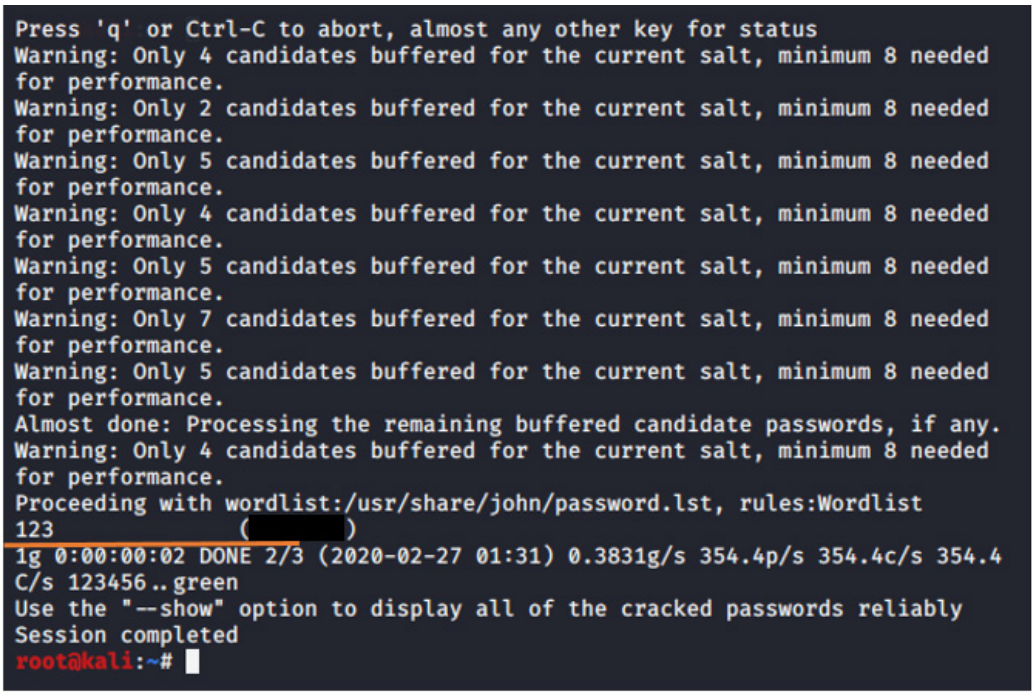


**Figura 22**: *Utilizando John the Ripper.*

## 3. Resultados y discusión.

Utilizando Ettercap se pudo husmear todo el tráfico de la red, y se obtuvo la ip de la víctima, y con la ayuda de Wireshark se pudo obtener el puerto por el cual la máquina de Windows XP se estaba conectando al entorno de Centos.

El secuestro de sesión Telnet fue realizada con éxito, la sesión iniciada en la máquina virtual de Centos desde Windows fue interrumpida usando Ettercap y Wireshark en el entorno de Kali Linux.

Cómo citar este artículo:
Yandún, M., & Hidalgo, J. (Julio - diciembre de 2020). "Ejemplos prácticos en el Laboratorio de Cyberseguridad - Upec". *Sathiri: sembrador, 15(2),* 273-289. https://doi.org/10.32645/13906925.1002

Se pudo observar que la herramienta John the Ripper sirvió para encontrar la contraseña del usuario, el cual puede desencriptar con gran facilidad, puesto que el archivo de la contraseña la muestra cifrada, siguiendo varios procedimientos como es el ingreso de varios comandos para la unión de los archivos passwd y shadown después de haber creado el usuario y contraseña, se verifica la contraseña mostrando tal como fue ingresada al principio.

Se realiza la práctica donde el comando John de Ripper puede descifrar las contraseñas de un determinado usuario, se demuestra un ciberataque.

Al no utilizar Windows, un puerto no seguro es más probable el robo de sesión, ya que las credenciales que utiliza no se encuentran encriptadas. Entonces, al utilizar el entorno de Kali Linux para husmear el tráfico es fácil observar las credenciales que utiliza el usuario para ingresar a Centos.

En un ambiente controlado como el laboratorio de CyberSeguridad de la UPEC, se generaron las pruebas y se observaron los datos de los usuarios de forma legible; y cuando se realizaban cambios en las configuraciones de los dispositivos de comunicación se observaba un nivel medio de protección, pero que no era suficiente para proteger datos sensibles, lo recomendable debe ser el cifrado de canal de comunicación para que los tipos de ataques y las herramientas usadas puedan atacar o incluso interceptar los datos, para que estos sean ilegible y no se pueda causar daño.

## 4. Conclusiones.

Las practicas realizadas en el laboratorio de Cyber Seguridad de la UPEC, son parte del proyecto de investigación “LA SEGURIDAD Y EL SERVICIO INFORMÁTICO EN EL GOBIERNO PROVINCIAL DEL CARCHI (ECUADOR) Y EN LAS ALCALDÍAS MUNICIPALES DE PASTO, IPIALES Y TÚQUERRES (COLOMBIA)”, y por lo tanto son demostrativas y tienen el propósito de generar medidas para mitigar estos tipos de Cyber ataques, instrucciones y afectaciones a la seguridad de la empresa.

En el ataque de intercepción de sesión se puede observar que los datos que la víctima recibía fueron interrumpidos por el atacante. De esta manera el atacante puede interceptar los datos utilizando la cuenta de otro usuario causando daño o robando información sensible.

Este tipo de ataque puede generar gran pérdida de información sensible para algunas empresas debido a que se realiza determinando las subredes de la red, el atacante puede filtrarse, eliminar una conexión crear otra, o simplemente esperar que la víctima reciba información importante.

Se puede concluir que John de Ripper es una de muchas herramientas que se utiliza para un ciberataque poniendo en riesgo la confidencialidad de las credenciales de un usuario, los ciberataques se consideran un delito informático para obtener información importante, sea de instituciones como de personas para obtener un objetivo referente a la economía.

## 5. Recomendaciones.

Tomar en cuenta muy seriamente las amenazas externas e internas, así como las vulnerabilidades existentes en el ámbito de manejo y resguardo de la información.

Gestionar de forma adecuada el riesgo informático realizando las matrices que incluyan la probabilidad y el impacto físico, de imagen, económico, que tendría la materialización de amenazas y vulnerabilidades.

De acuerdo a la matriz de riesgo, se deben generar los controles para mitigar las amenazas y vulnerabilidades implementado medidas de seguridad a nivel de Políticas, Hardware y Software.

Cómo citar este artículo:
Yandún, M., & Hidalgo, J. (Julio - diciembre de 2020). "Ejemplos prácticos en el Laboratorio de Cyberseguridad - Upec". *Sathiri: sembrador, 15(2),* 273-289. https://doi.org/10.32645/13906925.1002

## 6.- Referencias bibliográficas:

Amaro, J., Andrade, M., Macías, M. y Rodríguez, C. (2017) Ciberataque un paso de la Ciberguerra. Recuperado el 28 de agosto del 2017 de: http://148.236.18.55/bitstream/20.500.12107/1688/1/250-1792-A.pdf

Armas, X. (2017). Análisis de Seguridad del Sistema DNS (Domain Name Sistema), (tesis de pregrado). Escuela Politécnica Nacional, Quito, Ecuador Recuperado el 22 de julio del 2019, de: https://bibdigital.epn.edu.ec/bitstream/15000/17310/1/CD-7804.pdf

Auquilla, G & Espín, D (2019). Análisis de los mecanismos de defensa contra el ciberataque smtp spoofing en la infraestructura de red ipv4 (Trabajo de Titulación), Universidad Nacional De Chimborazo, Ecuador. Recuperado el 24 de julio de 2019, de: http://190.15.135.60/bitstream/51000/5576/1/UNACH-EC-ING-SIT-COMP-2019-0007.pdf

Baitha, A. (2018), Session Hijacking and Prevention Technique, International Journal of Engineering & Technology, 7, Recuperado el 22 de julio de 2019, de: https://www.researchgate.net/publication/325117343_Session_Hijacking_and_Prevention_Technique

BBC, Tecnología (2015) Así se realizó uno de los mayores ciberataques de la historia. Recuperado el 11 de noviembre del 2015, de: https://www.bbc.com/mundo/noticias/2015/11/151111_tecnologia_ciberataque_financiero_estados_unidos_il

Diario El Comercio. (2019). Ecuador denuncia 40 millones de ciberataques tras retiro de asilo a Assange. Recuperado el 15 de abril del 2019, de: https://www.elcomercio.com/actualidad/ecuador-denuncia-millones-ciberataques-assange.html

De la Hoz, E (2015). Sistemas de detección de intrusos con Mapas autorganizativos probabilísticos y optimización (Tesis doctoral), Universidad de Granada. Recuperado el 24 de julio de 2019, de: http://digibug.ugr.es/bitstream/handle/10481/43551/26117319.pdf?sequence=6&isAllowed=y

Fernández, E. (2019). Seguridad en APIs, Universitat Oberta de Catalunya (UOC) Universitat Oberta de Catalunya (UOC), Recuperado el 24 de julio de 2019, de: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/95147/6/efernandezcasaTFM0619memoria.pdf

Gascón, M. (2019) Los ciberataques más sonados de la historia: brechas de ciberseguridad de grandes empresas. Recuperado el 02 de diciembre del 2019, de: https://www.20minutos.es/noticia/4071984/0/los-ciberataques-mas-sonados-de-la-historia-brechas-de-ciberseguridad-en-las-grandes-empresas/

González Paz, A., Beltrán Casanova, D., & Fuentes Gari, E. R. (2016). Propuesta de Protocolos de Seguridad para la Red Inalámbrica Local de la Universidad de Cienfuegos. Universidad y Sociedad [seriada en línea], 8 (4). pp. 130- 137. Recuperado el 24 de julio del 2019, de: http://rus.ucf.edu.cu/

Herrera, A. (2015). Las Redes Wifi en Sitios de Mayor Concurrencia de Usuarios en la Ciudad de Esmeraldas (tesis de pregrado). Pontificia Universidad Católica Del Ecuador, Esmeraldas, Ecuador Recuperado el 22 de julio del 2019, de: https://repositorio.pucese.edu.ec/bitstream/123456789/553/1/HERRERA%20IZQUIERDO%20LUIS%20ALBERTO.pdf

Hidalgo J., Yandún M. (2019), Administración de Redes LAN, Ejercicios Prácticos con GNS3 ISBN 978-9942-914-66-8, https://doi.org/10.32645/9789942914668

**Cómo citar este artículo:**
**Yandún, M., & Hidalgo, J. (Julio - diciembre de 2020). "Ejemplos prácticos en el Laboratorio de Cyberseguridad - Upec". *Sathiri: sembrador, 15(2),* 273-289. https://doi.org/10.32645/13906925.1002**

Hidalgo J., Yandún M. (2020) Application of Classification Algorithms in the Generation of a Network Intrusion Detection Model Using the KDDCUP99 Database. In: Ahram T., Karwowski W., Vergnano A., Leali F., Taiar R. (eds) Intelligent Human Systems Integration 2020. IHSI 2020. Advances in Intelligent Systems and Computing, vol 1131. Springer, Cham. https://doi.org/10.1007/978-3-030-39512-4_70

Jain, V., Sahu, D. R., & Tomar, D. S. (2015). Session Hijacking: Threat Analysis and Countermeasures. In Int. Conf. on Futuristic Trends in Computational Analysis and Knowledge Management. Recuperado el 22 de julio de 2019, de : https://www.researchgate.net/profile/Vineeta_Jain4/publication/277307339_Session_Hijacking_Threat_Analysis_and_Countermeasures/links/5566bb1008aec22682ff202e.pdf

Martínez, L., Niño, J y Viniegra, L. (2019) La transparencia como variable reputacional de la comunicación de crisis en el contexto mediático del ciberataque wannacry. Recuperado el 09 de enero del 2019, de: http://www.seeci.net/revista/index.php/seeci/article/view/549/pdf_313

Melgar, E (2015). Desarrollo de un conjunto de aplicaciones para detección de ataques en redes IPv4/IPv6 utilizando Python (tesis de pregrado). Escuela Superior Politécnica del Litoral (ESPOL), Guayaquil, Ecuador Recuperado el 23 de julio del 2019, de: https://pdfs.semanticscholar.org/cd3f/77425dc7d358cc591ae764d5985912c5819b.pdf

Mendaño, L. (2016). Implementación de técnicas de hacking ético para el descubrimiento y evaluación de vulnerabilidades de la red en una cartera de estado. Quito. Recuperado el 25 de julio de 2019, de: http://bibdigital.epn.edu.ec/handle/15000/16836

Olivares, Javier. (2018). Seguridad Informática Hacking Ético. Ciudad de Barcelona: Cornella de Llobregat Recuperado el 24 de julio del 2019, de: https://books.google.com.ec/books?hl=es&lr=&id=efAmg9f8XtQC&oi=fnd&pg=PA23&dq=que+es+el+TCP+hijacking+2018&ots=CUEODieVZp&sig=h7hiv316gvmFf-tbYZrjgmSxV1g#v=onepage&q=HIJACKING&f=false

Pulla, J. (2019). Implementación de mecanismos de control aplicables a una red que mitiguen el secuestro de sesiones en el protocolo TCP (Examen complexivo). Universidad Técnica de Machala. Ecuador. Recuperado el 24 de julio de 2019, de: http://repositorio.utmachala.edu.ec/bitstream/48000/13609/1/ECUAIC-2019-SIS-DE00011.pdf

León, F. y Olmedo, J. (2018) Analysis of cyber attacks carried out in Latin América. Recuperado el 15 de septiembre del 2018, de: http://201.159.222.115/index.php/innova/article/view/837/779

Urueña, F. (2015) Ciberataques la mayor amenaza actual Recuperado el 16 de enero del 2015, de http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf

Velasco, R. (2015) John the Ripper crackea contraseña de usuarios en Linux. Recuperado el 25 de abril del 2015, de: https://www.redeszone.net/seguridad-informatica/john-the-ripper-crackear-contrasenas/

Velázquez, A. (2017) La responsabilidad internacional del estado como consecuencia de los ciberataques utilizados como métodos de combate a la luz del derecho internacional humanitario. (Tesis de posgrado). Universidad Pontificia Comillas, Madrid. Recuperado en abril del 2017, de: https://dialnet.unirioja.es/servlet/tesis?codigo=123917

Vila, R. (2017). Redes WIFI ¿Realmente se pueden proteger? Universitat Oberta de Catalunya (UOC) Universitat Oberta de Catalunya (UOC), Recuperado el 24 de julio de 2019, de: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72948/6/jvilariosTFG0118Memoria.pdf

**Cómo citar este artículo:**
**Yandún, M., & Hidalgo, J. (Julio - diciembre de 2020). "Ejemplos prácticos en el Laboratorio de Cyberseguridad - Upec". *Sathiri: sembrador, 15(2),* 273-289. https://doi.org/10.32645/13906925.1002**