AUDITORIA DE SEGURIDAD DE MOVISTAR

El ser capaz de romper la seguridad no te hace un hacker, ni tampoco, el ser capaz de cambiar una llanta te hace un ingeniero automotriz.

Elaborado Por: Andrea Giner Pastor

Fecha 25/10/2023

Tutor: Marco Antonio Lozano Solano

Análisis de las Vulnerabilidades

ÍNDICE

1. Auditoría Externa
   - 1.1 Identificación de Empleados
   - 1.2 Identificación de departamentos
   - 1.3 Localización Física
   - 1.4 Portal Corporativo
   - 1.5 Extranet
   - 1.6 Servicios Online
   - 1.7 Identidad en redes sociales
   - 1.8 Direcciones IP y Servicios Asociados
2. Cronograma (Diagrama de Gantt)
3. Ataque de ingeniería social
   - 3.1 Identificación de vectores
   - 3.2 Creación de señuelo
4. Plan de mejora para disminuir las debilidades
5. Resumen
6. Referencias bibliográficas

Introducción

Las vulnerabilidades informáticas son como una puerta abierta que permite el acceso remoto a los equipos de la empresa de personas no autorizadas, las cuales son susceptibles de llevar a cabo operaciones no permitidas y de un elevado riesgo para la ciberseguridad, tales como robo información, instalación de malware, acceso a cuentas bancarias, etc.

Tipos de vulnerabilidades y amenazas:

- **Amenazas de Malware**
- **Vulnerabilidades del Sistema**
- **Amenaza de ataque de denegación de servicio**
- **Vulnerabilidades producidas por contraseñas**
- **Vulnerabilidades producidas por usuarios**
- **Ataques por Inyección**

En estos primeros puntos vamos a realizar una auditoría externa para ver las vulnerabilidades o fallas que pueda tener la empresa Movistar.

- **Información de la Empresa:**

  - **Razón Social: Telefónica, SA**
  - **CIF: A28015865**
  - **Objeto Social: Se dedica a la instalación y explotación de servicios telefonicoscesion del estado el 21-12-1946.**
  - **Forma Jurídica: Sociedad Anónima**
  - **Actividad: Sociedades de cartera (holdings)**
  - **Actividad CNAE: 6420 - Actividades de las sociedades holding**
  - **Fecha de constitución: 19-4-1924**
  - **Fecha último cambio: 30-4-2023**

1.Auditoría Externa

Una auditoria externa es un análisis que realiza un auditor ajeno a la empresa sobre los procesos que desarrolla la misma, para comprobar que se realizan de manera adecuada y cumpliendo los requisitos legales establecidos.

1.1. Identificación de los Empleados

- **Aitor Goyenechea:** director de publicidad, marca y patrocinios telefónica/movistar España.

  - **Reside:** En Madrid
  - **número de teléfono es:** 659092397,
  - **correo electrónico es:**

    - aitor.goyenechea@telefonica.com,
    - agoyenechea@hotmail.com

  - **redes sociales:**

  LinkedIn: https://twitter.com/Aitor_goy

  https://www.facebook.com/aitor.goyenechea.7
  https://www.instagram.com/aitor_goy/

- **José María Álvarez – Pallete:** presidente ejecutivo telefónico S.A.

  - **Vive**: Londres – manhattan, aunque el nació en Barcelona.
  - **Nació**: el 12 de diciembre de 1963.
  - En momentos este casado.
  - **Sus redes sociales son:**

  https://www.facebook.com/carlozalmontes,
  https://www.instagram.com/jmalvpal/

https://twitter.com/jmalvpal?lang=ca

- **Pablo Ordorica:** Comunicación y Marketing en Movistar team.

  - **Vive:** en Madrid, pero nació en Asturias - Gijón.
  - **El correo electrónico es:** ordorica92@gmail.com .
  - **Sus redes sociales son:** https://www.instagram.com/pablo_ordorica/, https://www.facebook.com/p/Pablo-Ordorica-100063919997938/ , https://twitter.com/pablo_0rdorica?lang=ca, https://www.tiktok.com/@pablo_ordorica, https://www.linkedin.com/in/pablo-ordorica/?originalSubdomain=es,

    https://www.youtube.com/channel/UCyyYBUYGPvmf59fh6ld5c-g , https://www.twitch.tv/search?term=pablo%20ordorica.
  - **Su cumpleaños es:** el 6 de febrero.

- **Sebastián Unzué:** COO en Abarca Sports – General Manager Movistar Team Women.

  - En estos momentos reside en España en la comunidad de Madrid.
  - Tiene 31 años nació el 13 de septiembre.
  - Sus redes sociales son:

    - **LinkedIn**
    - **Instagram**
    - **Twitter**

Aunque no pertenece a movistar nos puede servir puede ser un canal de acceso para lanzar un ataque.

- **Chema Alonso:** Chief digital officer en telefónica.
  - Él es español, vive en Madrid en pozuelo de Alarcón.
  - Nació el 17 de junio de 1975 ahora mismo tiene 48 años.
  - Sus redes sociales son:

https://www.facebook.com/Chema.Alonso.Maligno/?locale=ca_ES

https://twitter.com/chemaalonso

https://www.instagram.com/chemaalonso/

http://www.calicoelectronico.com/

https://www.tiktok.com/@chema_alonso

https://www.youtube.com/user/Chemai64?sub_confirmation=1

https://www.tiktok.com/@chema_alonso

https://telegram.me/Elladodelmal

1.2. Identificación de departamentos

- **Comercial Empresas**
- **Comercial Clientes**
- **Servicio Atención**
- **Departamento de innovación**
- **Departamento de marketing**
- **Dirección de operaciones**
- **Departamento de comunicación y relaciones**

- **Departamento jurídico**
- **Departamento de finanzas**
- **Departamento de normativa Interna**
- **Departamento de recursos humanos**
- **Departamento de prensa y relaciones Institucionales**

1.3 .Localización Física

La empresa telefónica tiene sus plataformas de operación en: **España**, **Argentina**, **Brasil**, **Centroamérica**, **chile**, **Colombia**, **estados unidos**, **marruecos**, **México**, **Perú**, **Puerto rico**, **república checa**, **Uruguay** y **Venezuela**.

Telefónica, S.A. es una empresa multinacional de telecomunicaciones, con sede central en Madrid. Es la cuarta compañía de telecomunicaciones más importante de Europa y la decimotercera a nivel mundial.

La marca de telefónica se reserva exclusivamente para el papel institucional de la empresa. Para la comercialización de sus productos y servicios, la compañía tiene 3 marcas principales: Movistar para España e Hispanoamérica, para toda Europa y Brasil. Para llevar a cabo la auditoría externa de la sede física en España tendremos en cuenta:

- Dirección y contacto:

  Sede corporativa:

  - **Domicilio Social:** Calle gran vía, 28-5, Madrid
  - **Código Postal:** 28013
  - **Localidad:** Madrid
  - **Provincia**: Madrid
  - **Teléfono principal:** 900111004
  - **Otros teléfonos**: 914823733, 917548002

- **Fax**: 914829199
- **Email:** secretaria.delconsejo@telefonica.com
- **Web Principal:** https://www.telefonica.es/
- **Otras Webs:** https://www.wayra.es/ https://www.telefonica.com/

Dirección y contacto

Sede corporativa

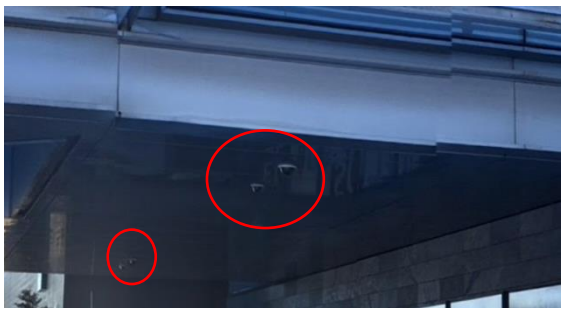
- **Domicilio Social:** RONDA DE LA COMUNICACION (EDIF. SUR 3)
- **Teléfono:** 911995152
- **Código Postal:** 28050
- **Localidad:** Madrid
- **Provincia:** Madrid
- **Otros teléfonos**: 910640907, 914258594, 900111004.
- **Fax:** 914234011
- **Web Principal:** **http://www.movistar.es/**
- **Otras Webs:** **http://www.o2online.es/** , **http://www.tuenti.es/**

No se podría realizar un ataque porque está lleno de cámaras de seguridad.

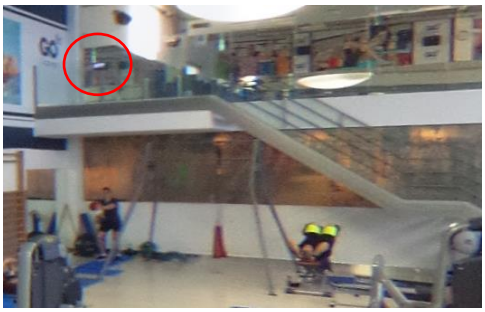
Cámara de seguridad

Cámara de Seguridad

Cámaras de Seguridad



Cámara de seguridad



1.4 Portal Corporativo

El portal corporativo de movistar es movistar.es
https://www.movistar.es/

La página corporativa de movistar es:
https://www.telefonica.com/es/nosotros/marcas/movistar/

Título: Jquery 3.6.4	
CVE: N/A	**Criticidad:** N/A
Descripción:	
El servicio identificado no tiene vulnerabilidades conocidas	

Título: Wordpress < 5.2.11	
CVE: CVE-2022-0254	**Criticidad:** N/A
Descripción:	
bmarshall511/wordpress_zero_spam es un WordPress Zero Spam que hace que bloquear el spam y los visitantes maliciosos sea muy fácil. Las versiones afectadas de este paquete son vulnerables a la inyección SQL debido a una desinfección y escape inadecuados de los parámetros ordery orderbyantes de usarlos en una declaración SQL en el panel de administración.	

1.5 Extranet

No hemos identificado la extranet en movistar

1.6 servicios online

Título: Jquery 1.11.1	
CVE: CVE-2020-11022	**Criticidad:** 6.1 (media)
Descripción:	
En versiones de jQuery mayores o iguales a 1.2 y anteriores a 3.5.0, pasar HTML de fuentes no confiables, incluso después de desinfectarlo, a uno de los métodos de manipulación DOM de jQuery (es decir, .html(), .append() y otros) puede ejecutarse. código no confiable. Este problema está solucionado en jQuery 3.5.0.	

Título: Next.js 13.4.2	
CVE: N/A	**Criticidad:** N/A
Descripción:	
El servicio identificado no tiene vulnerabilidades conocidas	

Título: core.js 2.6.12	
CVE: N/A	**Criticidad:** N/A
Descripción:	
El servicio identificado no tiene vulnerabilidades conocidas	

3.3 Identidad en redes sociales

- Facebook: https://www.facebook.com/movistar.es
- X: https://twitter.com/movistar_es
- Youtube: https://www.youtube.com/c/movistarespana
- Instagram: https://www.instagram.com/movistar_es/?hl=es

1.8Direcciones IP y Servicios Asociados

DATOS DEL TITULAR

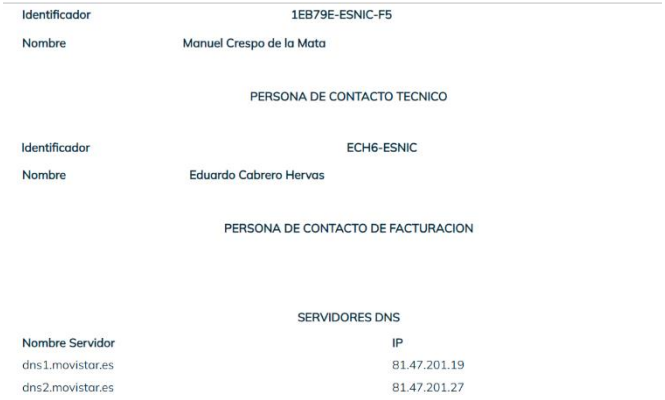
Nombre del Dominio	movistar.es
Identificador	18D108-ESNIC-F5
Titular	Telefonica SA
Fecha de Alta	20-06-2003
Fecha de Renovación	20-06-2024
Agente Registrador	ACENS TECHNOLOGIES S.L.

PERSONA DE CONTACTO ADMINISTRATIVO

Identificador	1EB79E-ESNIC-F5
Nombre	Manuel Crespo de la Mata

PERSONA DE CONTACTO TECNICO

Identificador	ECH6-ESNIC
Nombre	Eduardo Cabrero Hervas



Identificador	1EB79E-ESNIC-F5
Nombre	Manuel Crespo de la Mata

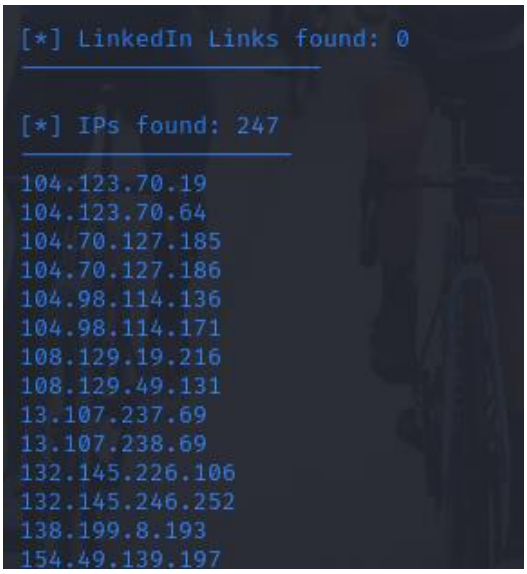
PERSONA DE CONTACTO TECNICO

Identificador	ECH6-ESNIC
Nombre	Eduardo Cabrero Hervas

PERSONA DE CONTACTO DE FACTURACION

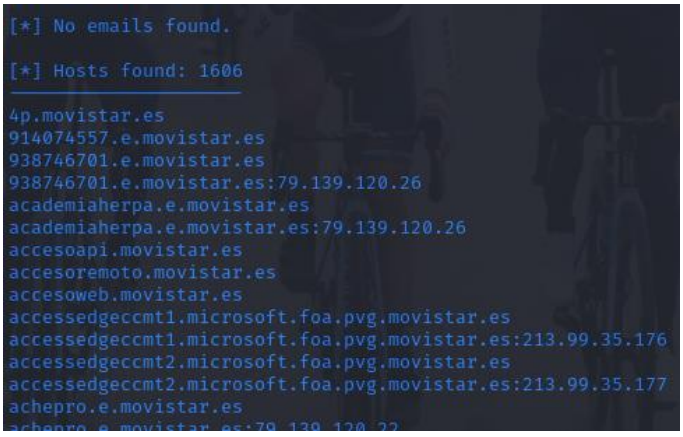
SERVIDORES DNS

Nombre Servidor	IP
dns1.movistar.es	81.47.201.19
dns2.movistar.es	81.47.201.27



```
[*] LinkedIn Links found: 0

[*] IPs found: 247
104.123.70.19
104.123.70.64
104.70.127.185
104.70.127.186
104.98.114.136
104.98.114.171
108.129.19.216
108.129.49.131
13.107.237.69
13.107.238.69
132.145.226.106
132.145.246.252
138.199.8.193
154.49.139.197
```

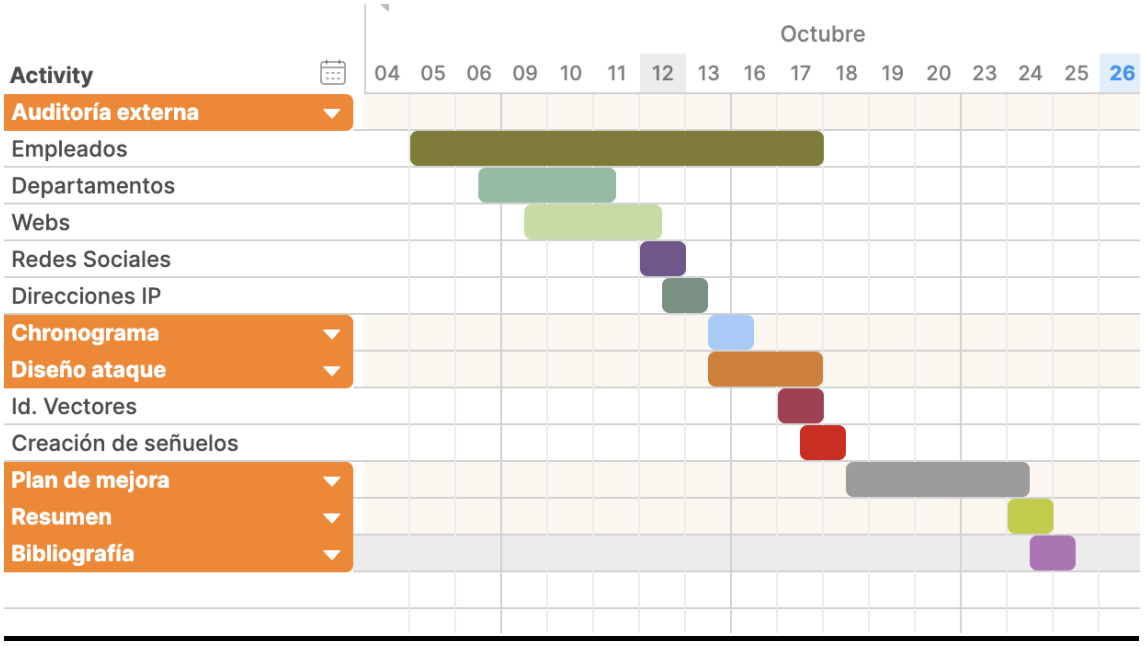


```
[*] No emails found.

[*] Hosts found: 1606
4p.movistar.es
914074557.e.movistar.es
938746701.e.movistar.es
938746701.e.movistar.es:79.139.120.26
academiaherpa.e.movistar.es
academiaherpa.e.movistar.es:79.139.120.26
accesoapi.movistar.es
accesoremoto.movistar.es
accesoweb.movistar.es
accessedgeccmt1.microsoft.foa.pvg.movistar.es
accessedgeccmt1.microsoft.foa.pvg.movistar.es:213.99.35.176
accessedgeccmt2.microsoft.foa.pvg.movistar.es
accessedgeccmt2.microsoft.foa.pvg.movistar.es:213.99.35.177
achepro.e.movistar.es
```


[*] Interesting Urls found: 42
http://seguros.movistar.es/
http://www.movistar.es/ne/pub/seg00/control/
http://www.movistar.es/ne/pub/seg00/control/NEAA00JSCSS?ac=aS&cn=1&co=1659&ns=745925&en=15038&nm=10
http://www.movistar.es/ne/pub/seg00/control/NEAA00JSCTS?ac=tr&ta=0&cn=1&co=1659&nm=10&en=15038&ns=745925
http://www.movistar.es/ne/pub/seg00/control/NEAA00JSCTS?ac=tr&ta=0&cn=1&co=1659&nm=15&en=15264&ns=745925
http://www.movistar.es/ne/pub/seg00/control/NEAA00JSCTS?ac=tr&ta=0&cn=1&co=1659&nm=19&en=15264&ns=745925
http://www.movistar.es/ne/pub/seg00/control/NEAA00JSCTS?ac=tr&ta=0&cn=1&co=1659&nm=2&en=14423&ns=745925
http://www.movistar.es/ne/pub/seg00/control/NEAA00JSCTS?ac=tr&ta=0&cn=1&co=1659&nm=21&en=14117&ns=745925
http://www.movistar.es/ne/pub/seg00/control/NEAA00JSCTS?ac=tr&ta=0&cn=1&co=1659&nm=29&en=15265&ns=745925

2.Cronograma (Diagrama de Gantt)



3. Ataque de ingeniería social

El mayor problema de las organizaciones en relación con la protección de sus activos, suele ser la falta de capacitación de los empleados relativa a los incidentes que llevan a cabo los ciberdelincuentes y la dificultad para identificarlos como tal.

En el caso de la empresa Movistar, se ha encontrado numerosa información que podría usarse para llevar a cabo un ataque de ingeniería social. En los subpuntos siguientes se hará un desglose de los vectores que se podrían emplear así como el tipo de señuelo.

3.1 Identificación de vectores

Se conoce como vector de ataque, aquellos posibles canales que un ciberdelincuente o atacante puede emplear para intentar materializar un ciberincidente. Entre los más habituales encontramos el correo electrónico, el teléfono, la mensajería instantánea, página web y la falta de actualizaciones de seguridad en los sistemas.

En el caso de la empresa propuesta y en base a la información recopilada en la auditoría externa podemos concretar los siguientes vectores que podría emplear un atacante:

- Correo electrónico: mediante técnicas OSINT se han recopilado varias direcciones que un atacante podría suplantar, escribir un mensaje malicioso o usar cualquier tipo de señuelo que permita este vector.
- Teléfonos: técnicas OSINT se han identificado varios teléfonos que podrían usarse para llevar a cabo un ataque de tipo Vishing o simplemente suplantar a alguien.
- Página web: aunque de manera directa no se ha encontrado ninguna vulnerabilidad en la página web del formulario de acceso, sí que podría suplantarse con algún tipo de aplicación que permita clonar la web y publicarla en un servidor malicioso, para capturar contraseñas o información confidencial.

3.2 Creación de señuelo

Una vez identificados los vectores de ataque, es hora de determinar qué tipo de señuelo podría usar el atacante:

Vector	Señuelo
Correo electrónico	Infectar un archivo PDF y enviárselo a alguna de las personas de las que tenemos su dirección de mail, diseñando un mensaje sobre el que la víctima pueda caer en el engaño.

Correo electrónico/página web	Enviar un correo electrónico con un mensaje convincente para el cambio de una contraseña, y en el que se incluya un enlace a un servidor malicioso en el que está publicada una página falsa del servicio de acceso a movistar. Este señuelo puede ser tanto para empleados como para clientes.
Teléfono (voz)	Mediante la información recopilada, un atacante podría hacerse pasar por alguien de la compañía o de un tercero de confianza (como un servicio técnico o similar). Tratando de engañar a la víctima para obtener información confidencial, o que esta lleve a cabo alguna acción que involucre al usuario.
Teléfono (SMS)	El atacante podría diseñar un mensaje de texto convincente, que incluyera un enlace para la descarga de un malware o para dirigir a la víctima a un sitio web malicioso.

4.Plan de mejora para disminuir las debilidades

En relación con la información que hemos identificado, relativo a la información de empleados, se recomienda que éstos limiten la publicación de información personal para evitar ataques. Esto también sería de aplicación para la información de la empresa en cuanto a los departamentos y la gente que trabaja en ellos.

En cuanto a la protección física, podemos afirmar que está bien protegida, no se puede decir lo mismo de los servicios web. Las aplicaciones analizadas enumeran las tecnologías disponibles y sus versiones, permitiendo a un atacante la búsqueda de información acerca de dichas tecnologías. Se recomienda limitar la publicación de dicha información.

Por último, se ha identificado bastante información relacionada con direcciones IP y servicios asociados. En este caso, se recomienda revisar si los servicios encontrados es necesario que sean visibles o si por el contrario se han de despublicar.

Con carácter general y a modo de recomendaciones, para reducir las posibles vulnerabilidades y amenazas se podría seguir lo siguiente:

- Requerir que los empleados utilicen contraseñas únicas.
- Añadir números y símbolos a una contraseña para mayor seguridad.

- Crear reglas que requieran que los empleados creen contraseñas complejas y únicas de al menos 12 caracteres; y cambiarlas si existe alguna razón para pensar que han sido vulneradas.
- Realizar copias de seguridad periódicas.
- Llevar una correcta gestión de las contraseñas.
- Mantener nuestros sistemas informáticos siempre actualizados.
- Monitorear constantemente los avisos de las ultimas vulnerabilidades conocidas.
- Que los empleados realicen de forma activa formaciones sobre como proteger la red y su seguridad en los diferentes dispositivos electrónicos como puede ser ordenadores de trabajo, móviles, tablets, etc.

5. Resumen

Para reducir estos tipos de daños lo que recomendaría es no poner mucha información en redes sociales si no es necesario luego hacer formaciones relacionados con este ámbito de la Seguridad desde el colegio para prevenir ciertas cosas como puede ser phishing, suplantar identidad o páginas web, etc.
Ya que para el atacante es muy útil esta información que subimos a Internet para hacer un mal uso de ellas. Ya que en la nueva tecnología nada está a salvo, aunque reforcemos la seguridad con contraseñas robustas este ámbito siempre está en constante actualización y por ello siempre los atacantes intentar atacar con todo tipo de programas maliciosos.
Dentro del plan de mejora se han indicado las cuestiones a seguir para mejorar la seguridad en Movistar.

6.Referencias Bibliográficas

Toda la información que está aquí en este proyecto o trabajo lo he sacado de estas paginas webs o URL:

- Wikipedia
- Redes Sociales (Facebook, Instagram, LinkedIn, Twitter, twicht, tik tok, etc.)
- La página de movistar
- Google maps
- Escáneres para realizar el reconocimiento del sistema, identificación de vulnerabilidades y análisis y verificación de las vulnerabilidades.
- Kali con el terminal de comandos para averiguar a través de comandos la ip y la url de los sitios web.