Universidad Nacional Autónoma de México

Facultad de Ciencias

Criptografía y Seguridad

Práctica 4: SSH-Multiverse

Fecha de entrega: 26/09/2022

Equipo:

Criptonianos

Acosta Arzate Rubén - 317205776

Bernal Marquez Erick - 317042522

Deloya Andrade Ana Valeria - 317277582

Marco Antonio Rivera Silva - 318183583

1. Introducción

De acuerdo a la especificado en la práctica. SSH (Secure Shell) es un protocolo utilizado para establecer una conexión segura y cifrada entre dos dispositivos a través de una red. Se usa comúnmente para el acceso remoto y la administración de servidores y otros equipos en red. Una de las características clave de SSH es su uso del cifrado para proteger los datos a medida que se transmiten entre dispositivos. Esto ayuda a evitar el acceso no autorizado o que se intercepte información confidencial.

SSH es un objetivo común para los actores de amenazas porque proporciona una puerta de acceso. El objetivo de esta práctica es conocer y practicar los ataques de diccionario, aprovechando el descuido de los usuarios y una mala implementación de una política para establecer contraseñas seguras. De la misma manera, se plantea como un repaso de herramientas que hemos estudiado previamente.

En esta historia ficticia se plantea el ataque a un servidor donde muy probablemente se encuentren los examenes, calificaciones, prácticas y tareas de los alumnos. Por lo tanto nos da curiosidad entrar a dicho servidor, la única pista que se nos proporciona es que tenemos un usuario en el servidor y que nuestra contraseña está entre las más famosas, las cuales se encuentran en el archivo *rockyou.txt* de *Kali Linux*

2. Desarrollo

2.1. Reconocimiento

Lo primero que hicimos fue hacer un reconocimiento de los puertos por medio de la herramienta **nmap**. En especifico usamos el comando **nmap 3.85.60.57** para saber que puertos estaban abiertos y que servicios ofrecían.

Figura 1: Ejecución de nmap

Después escaneamos todos los puertos, es decir del 1 al 65535 para estar seguros de analizar todo. Para ello usamos el comando **nmap -p 1-65535 3.85.60.57**.

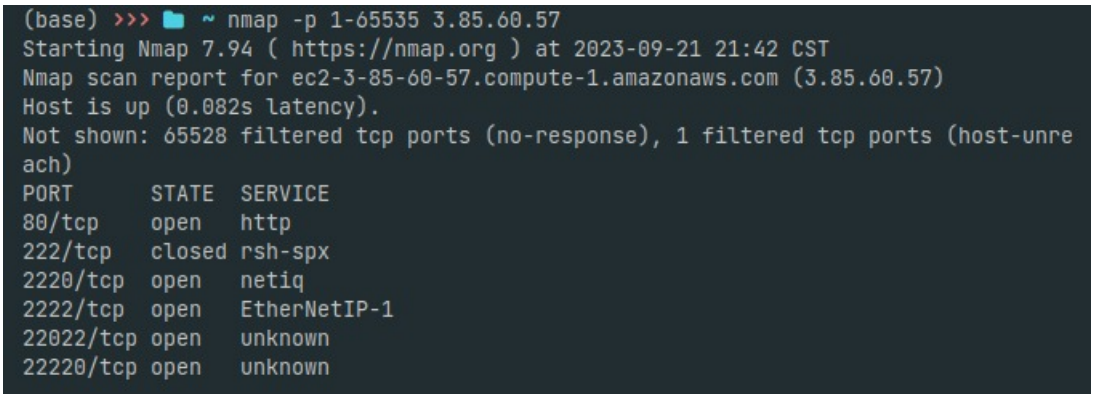

Figura 2: Ejecución de nmap

Pudimos observar que nos mostraba varios puertos pero no nos decía qué versión usaban, por lo que tuvimos que usar el siguiente comando **nmap -Pn -sV -p88,2220,2222,22022,22220 3.85.60.57**

```
(base) >>> ~ nmap -Pn -sV -p80,2220,2222,22022,22220 3.85.60.57
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 22:33 CST
Nmap scan report for ec2-3-85-60-57.compute-1.amazonaws.com (3.85.60.57)
Host is up (0.071s latency).

PORT      STATE    SERVICE      VERSION
80/tcp    open     http         Apache httpd
2220/tcp  open     netiq?
2222/tcp  filtered EtherNetIP-1
22022/tcp open     ssh          OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
22220/tcp open     ssh          OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
1 service unrecognized despite returning data. If you know the service/version, pl
ease submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-s
ervice :
SF-Port2220-TCP:V=7.94%I=7%D=9/21%Time=650D1912%P=x86_64-pc-linux-gnu%r(Ge
SF:nericLines,5,"Nlr\r\n");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 161.78 seconds
(base) >>> ~
```

Figura 3: Ejecución de nmap

Una vez que pudimos ver los puertos que estaban abiertos ya sabíamos a donde podríamos hacer el ataque por diccionario, en particular nos interesaban los puertos 22022 y 22220 ya que debíamos entrar por medio de ssh. Sin embargo, la contraseña podría ser cualquiera, para ello se nos proporcionó la pista de que nuestra contraseña era de las mas utilizadas las cuales se encuentran en el famoso documento *rockyou.txt* pero aun así sería demasiado tardado probar una por una, incluso si nos las dividíamos entre todos los miembros del equipo, por lo cual decidimos seguir buscando pistas relacionadas al servidor.

Pensamos que si era un servidor entonces podíamos acceder a él a través de una pagina web por medio de la IP, para nuestra sorpresa nos mostraba un archivo html en el que venía un mensaje cifrado con

clave PGP y un párrafo diciéndonos que la llave se encontraba en la carpeta donde subimos nuestras llaves públicas para la práctica 2 de correo cifrado.

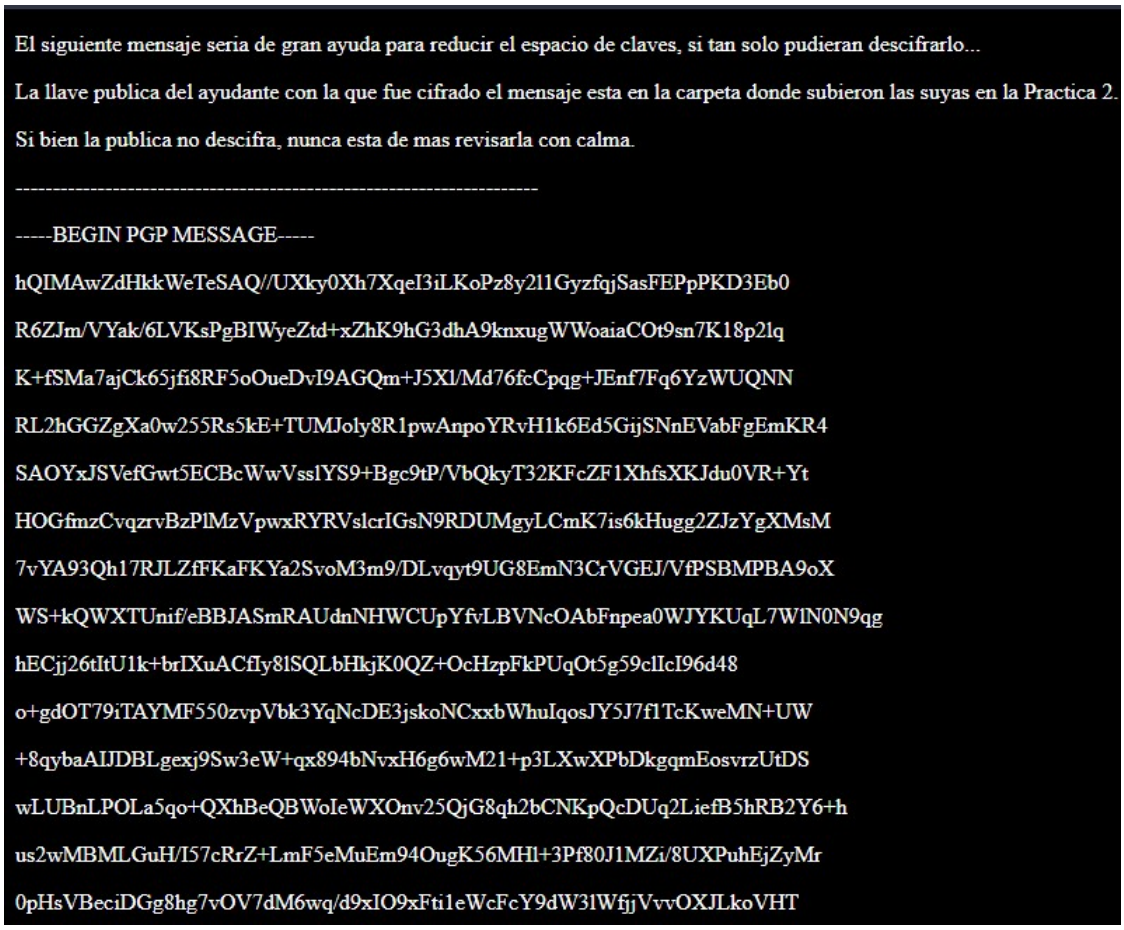

Figura 4: html del servidor

Buscamos la carpeta con las llaves y pudimos ver un archivo con el nombre de Ivan, por lo que procedimos a abrirlo y ahí estaba escrita su llave para un mensaje PGP con un comentario hasta abajo que decía que a veces, por accidente, se compartían las llaves privadas. Es entonces cuando nos dimos cuenta que la llave nos servirá para descifrar el mensaje que había en el servidor.

```
c0Bhoj3++VjyXo6QuMIN7EEbUqNAdIll1NzpHOL1TO1I+1QhDWE6d1n/8rTfLtuG
Wa1Brdeszh8/2aMPQncc/KGoKNigOGSn+tvyEKoBxeVAHnwWNQKfdeHWODwySiAX
kUiaoyYzqCF8Qz/kADWM2FSYdfvJWf6MBOAkSvDtJryPdKPHVmfk6+50CduU6Hp4
C2n7J3yzzQheubeeLxSP89BVJhhrox4uUUSTn7If4cC3mLr3XZqcrjelWVqt06TN
Ib/mxFoANj1zxoQVG4OuiQI8BBgBCgAmFiEErDuN6dCec3QH91ATUGRAoYPSGtcF
AmT//hMCGwwFCQANLwAACgkQUGRAoYPSGtfKBA/9FZnxNVgXl0/K3zOWihyDPPKe
dgtc7g81D6AA9xTxJd32Fejay/a4qOlOgMdUKxS7uyrsxFd7eDMHTW7FJ1TMWToB
IRODMfp7KrIK1nNR1NbCSHr89L6XYimE9DpDEIdhvrw3COSPgoaVnf5ZzRgYYGUy
Xewlpk1TAxijFw01uS335pSlqlaQ9pWpMR2BEFrmWqpwV/bbzs12vUJrys683DnH
QjIQFg94xKZP4zWeYkSmJu458toO64+dnp4vlW7luc4rqI0hy7UXWmMysFBzrPRK
qGHdS4+LqPn2YQKHLFwHxN96uRqWM5kkUHNPvJ2MEhOxEpbXqk866BpGDiVcXcWR
jXjZJmd14DDuQMEIwsZ4NV1gw7AkcVGymoL0hg9Gds/41KoblNjsREujW+5PSQKj
p/2bRHO5f5M9ZmSgYSvmf7MWKvEoVV84vpkdD1qZUs/DzgLG2tLkm4H5W2rmM8Wh
zTnspH5Tg/gKBZIjlKYCYYjROYIuCAdMblhCpWV3ujgmR0I6OxULzDpic9IVybV+
Ewy/UM0vK0OFf8qaZlR6w+7/shPs1Dxakw/ADhpdw2OIip+36tlckpgcRIFVAyLq
LAFcCrsTunIl1pM8ggH0xdpyJis5s/obl7ru5yEIwt9Z8SmBUDJQGGnoYYNY/viu
yMyJ6efhZCCj+7rVNPqwBgAAZ3BnAA==
=4tFz
-----END PGP PRIVATE KEY BLOCK-----


Los errores humanos son un factor muy importante a tomar en cuenta,
en este caso representado como subir la llave privada en vez de la
llave pública. Importen de manera correcta esta llave privada para
poder descfirar el mensaje y así reducirán considerablemente el trabajo.
```

Figura 5: Obteniendo la clave

Acto seguido, procedimos a descifrar el texto con ayuda de la página web *Online PGP Encryption Decryption*. El texto descifrado es

```
imsseguros:x:U*********
criptonianos:x:p***********
shieldedcodesmiths:x:b*******
hashheroes:x:1******
dragoncode:x:1*****
unsecure:x:j******
criptidos:x:a*********
criptopanas:x:M*********
```

```
fosildinamita:x:k************
criptosocialoutcast:x:2*******
enigmaforce:x:c******
unitario:x:a******
mrmaui:x:x*******
davidshiro:x:o******
```

```
Los asteriscos indican la longitud de la contraseña la cual inicia después de :x:.
Esto es, pueden ver el primer carácter de su contraseña.
De esta manera se reduce drásticamente el número de posibles contraseñas.
```

Esto nos proporcionaba la pista de que nuestra contraseña empieza con la letra p y tiene como longitud 12 carácteres. Hicimos un script de python para filtar las posibles llaves y las colocamos en un nuevo archivo de texto llamado *posiblesCriptonianos.txt* y así proceder con el ataque por diccionario. De esta manera pudimos reducir las posibles llaves del archivo *rockyou.txt* de varios millones de posibilidades a alrededor de 25,000 posibles llaves.

```
1  with open('rockyou.txt', 'r', encoding='latin1') as f:
2      diccionario = f.readlines()
3  posibles = []
4  for i in diccionario:
5      if i[0] == "p" and len(i) == 12:
6          posibles.append(i)
7  with open("posiblesCriptonianos.txt", "w") as f:
8      for contra in posibles:
9          f.write(contra)
10     print('Done')
```

2.2. Ataque por diccionario

Al tener dos puertos ssh abiertos debiamos probar ambos para ver por cual podíamos entrar, por suerte bastó con intentar el primer puerto *22022*. Una vez que tenemos nuestro archivo de posibles contraseñas, usamos la herramienta *hydra* con nuestro usuario que encontramos en la hoja de cálculo de los equipos, en específico usamos el comando **hydra -I -V -l criptonianos -P posiblesCriptonianos.txt -t 6 ssh://3.85.60.57:22022**.

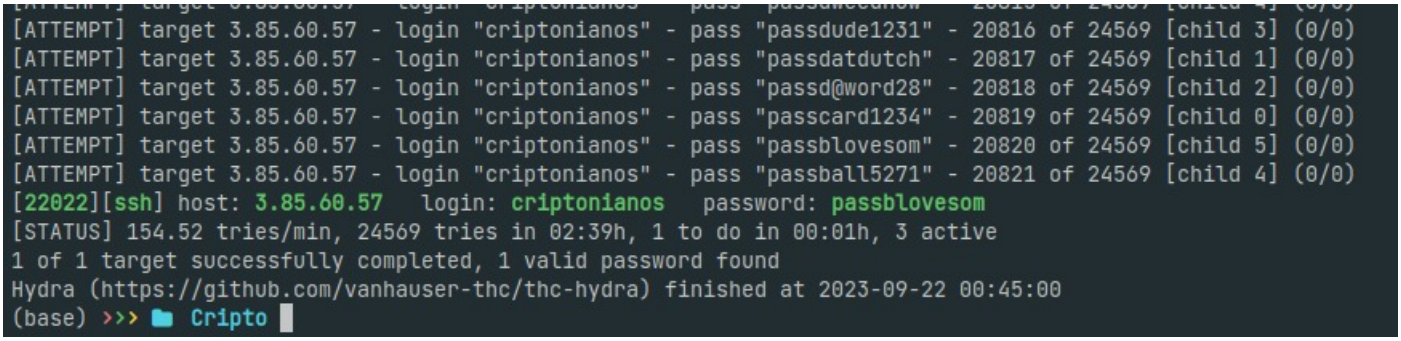

Figura 6: Ejecución de Hydra

Después de ejecutar el comando empezó a realizar las posibles combinaciones, para nuestro caso tardó aproximadamente 2 horas con 10 minutos, mientras que si hubiéramos usado el archivo *rockyou.txt* completo nos hubiéramos tardado días. Una vez que *hydra* logró encontrar la contraseña correcta, pudimos proceder a intentar acceder al servidor por medio de ssh.

2.3. Acceso por SSH

Procedimos a intentarnos conectar al servidor con nuestro usuario y contraseña utilizando el comando **ssh criptonianos@3.85.60.57 -p 22022** con el cual especificamos el puerto que queremos usar. Sin embargo, teníamos un problema ya que el servidor nos rechazaba la conexión.

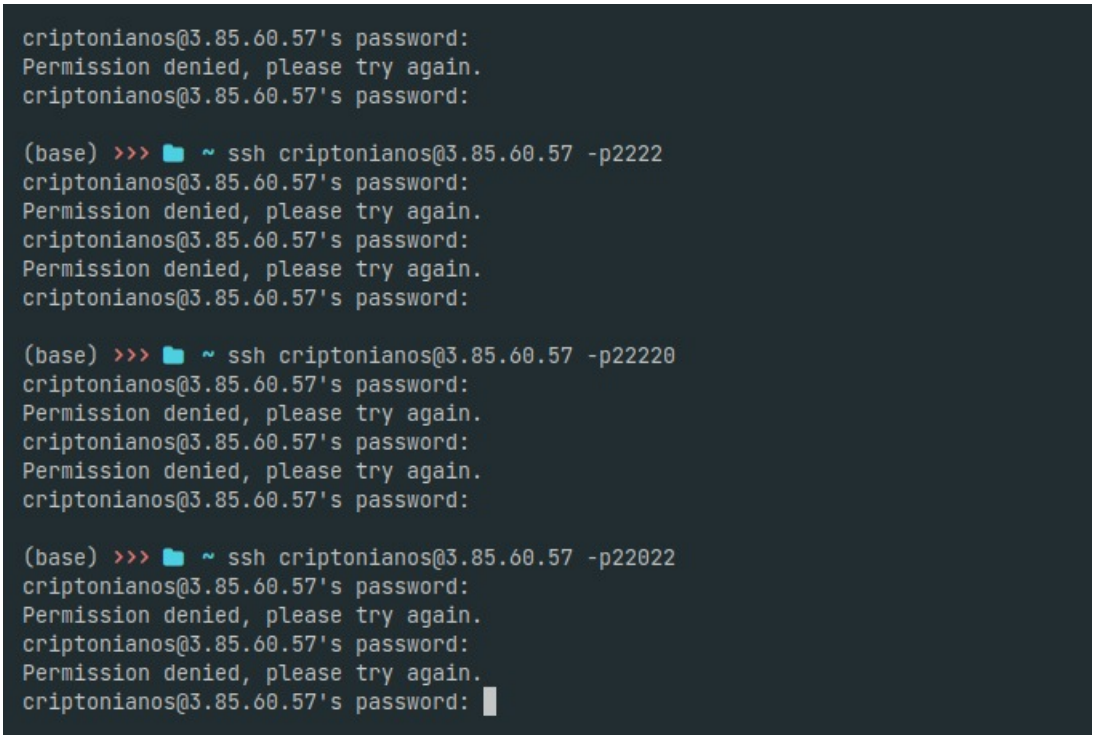

Figura 7: Intentos de entrar al server por ssh

Por suerte esto era problema del servidor, a lo que el ayudante nos ayudó para checar qué estaba pasando. Una vez solucionado ese problema pudimos acceder de forma exitosa al servidor.

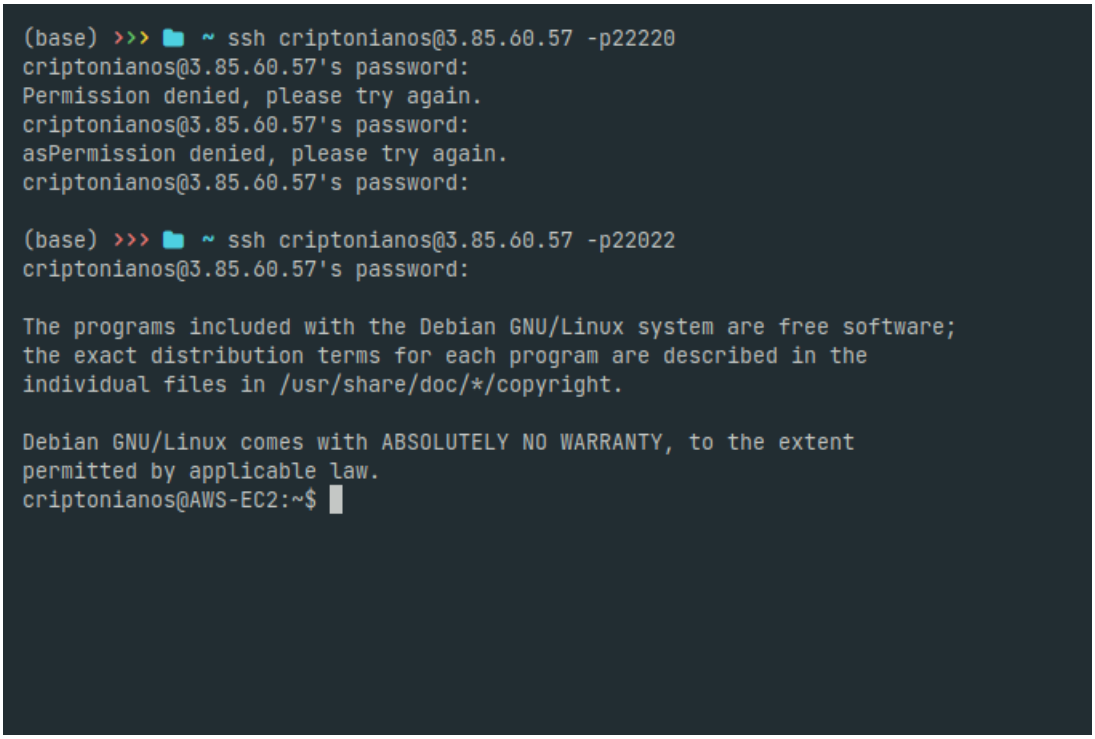

Figura 8: Conexión exitosa al servidor por medio de ssh

Una vez dentro procedemos a dejar nuestro rastro en el servidor:

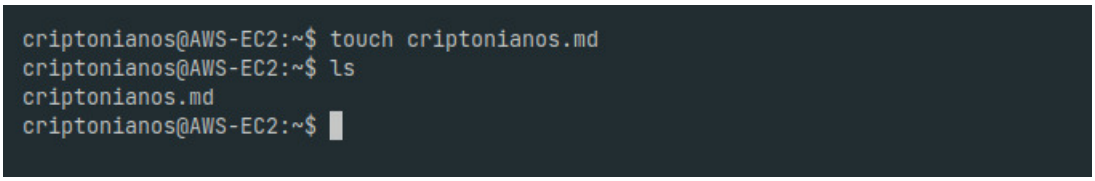

Figura 9: Rastro dejado en el servidor

2.4. Bandera

Durante nuestra investigación en busca de más información y con el objetivo de acceder al servidor, logramos descubrir la bandera al examinar el código fuente de la página HTML que se encuentra alojada en el servidor.

```
  11xZikFu3kHw/bZRxGaEmxY+x4pdAOEhP4Q/SMSAS4vIGKkbfd4r6JtBgnMAmzcJ</p>
  <p style="color:#FFFFFF">
  E6q1zuyGraSchD0azS12P8R7Q8alEsS1Bj/Dt5dNRLoPPQLMNXQg</p>
  <p style="color:#FFFFFF">=k6zQ</p>
  <p style="color:#FFFFFF">-----END PGP MESSAGE-----</p>
  <!--â€" Muchas veces y por malas practicas suelen salir a produccion
  sitiosâ€"-->
  <!--â€" que tienen como comentarios usuarios y contraseÃ±as â€"-->
  <!--â€" o demas informacion que no deberia estar ahi â€"-->
  <!--â€" En nuestro caso sera una bandera â€"-->
  <!--â€" FlagCyS2024-1{SiempreRevisaElHTML} â€"-->
 </body>
</html>
```

Figura 10: Bandera de la práctica

2.5. Extra: Post Explotación

Nuestra idea para la post-explotación del servidor fue minar criptomonedas *duino coin* ya que son criptomodenas basadas en mineria más limpia (cuanto menos potente y energía ocupe el equipo minando, mayor sería la ganancia.), Sin embargo, después de un tiempo de haber entrado el servidor nos desconectaba (durabamos en conexión aproximadamente 1 o 2 minutos), por lo que la instalación completa no pudo ser realizada.

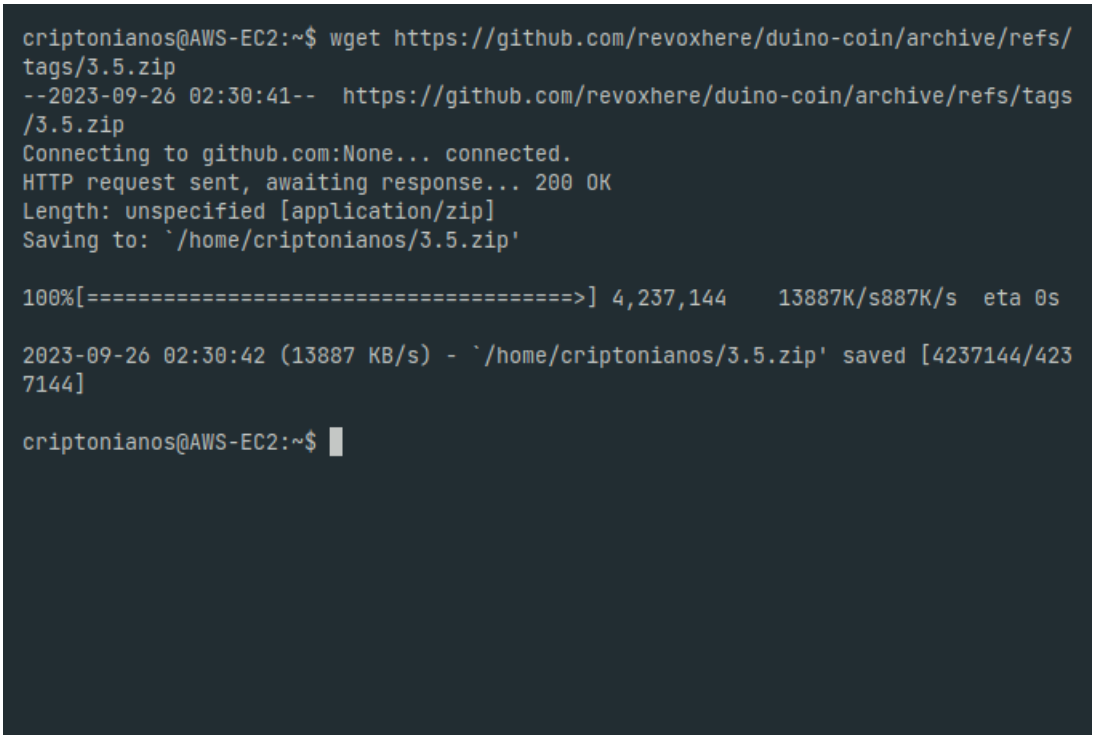

Figura 11: Intento de minar criptomonedas

2.6. Problemas

Tuvimos algunos problemas como que a veces se cayó el servidor, escaneamos mal puertos o simplemente la conexión del servidor era temporal y la sesión no guardaba nuestros avances. Así incluimos capturas de estos intentos en el reporte.

Además este tipo de ataques se consideran activos, es decir, que dejan algún rastro en las bitácoras del servidor, por lo cual todos los intentos se habrán quedado guardados en el servidor.

3. Punto extra (OSINT)

Utilizando únicamente fuentes abiertas y usando la información de manera responsable (siguiendo las buenas prácticas vistas en clase "OSINT de manera responsable" y nunca con la intención de hacer daño [Doxing]) buscar aspectos relevantes de cualquiera de sus ayudantes: David Silva, Cecilia Villatoro e Ivan Galindo. Dicha información en ningún caso deberá ser compartida con terceros.

A continuación mostraremos los descubrimientos obtenidos en base a la investigación que realizamos, explicaciones de cómo fue el proceso, además de las páginas y redes sociales de donde obtuvimos dicha información.

Aunque el desarrollo del punto extra fue éxitoso, por motivos de seguridad y respeto a la privacidad de las personas en el curso, no haremos pública la información obtenida a través de tecnicas *OSINT*.

4. Conclusiones

4.1. Práctica

Pudimos ver como nuestros equipos tales como servidores o computadoras personales son susceptibles a ataques por diccionario cuando nuestras políticas no cumplen con buenos estándares de seguridad, por ejemplo utilizar contraseñas más usadas, limitar las IP's del servidor, limitar los intentos de inicio de sesión, configuración de puertos, autenticación por SSH en lugar de contraseñas, etc.

Además, comprendimos la importancia hacer un reconocimiento al servidor con el objetivo de minimizar esfuerzos en cuanto al ataque de diccionario. Por otro lado también vimos el poder de las herramientas que usamos y sabemos que siempre deben de ser usadas con responsabilidad.

4.2. Parte Extra (OSINT)

Muchas veces creemos que nuestra información en internet está protegida o nadie la puede consultar al poner nuestros perfiles en *privado*. Al realizar la parte extra de la práctica (OSINT) nos dimos cuenta que esto no es suficiente, ya que hasta la más mínima pista como fotos, nicknames, correos, etc, nos puede dar suficiente información como para seguir buscando en otras fuentes con las herramientas correctas. No hace falta un ataque a nosotros mismos para comprobar los riesgos que esto conlleva, basta ver los casos en que una celebridad sube una foto a sus redes sin mencionar dónde se encuentra e inmediatamente la gente en internet se da a la tarea de investigar con base a los detalles que se logren apreciar en la foto para finalmente terminar averiguando qué lugar es.

No solo las fotos o publicaciones actuales puede revelar información, sino también las publicaciones que hicimos en el pasado, las cuales muchas veces pasan por alto olvidándonos por completo de la información que puede haber ahí.

Si bien siempre habrá información en internet acerca de varias cosas, incluidos nuestros datos personales, existen formas de mitigar este impacto. Un buen ejercicio es investigarnos a nosotros mismos para ver qué es lo qué podemos obtener y a partir de ahí poner medidas de limiten esta información tal como perfiles privados, nicknames distintos, ocultar pistas que puedan revelar información en nuestras fotos, etc.

5. Referencias

- *Online PGP Encryption Decryption tool using pgp public private keys.* (2018). https://8gwifi.org/pgpencdec.jsp
- *NMAP Documentation - free security scanner for network exploration & security audits.* (s.f). https://nmap.org/docs.html