Alumno: Rodrigo Vila

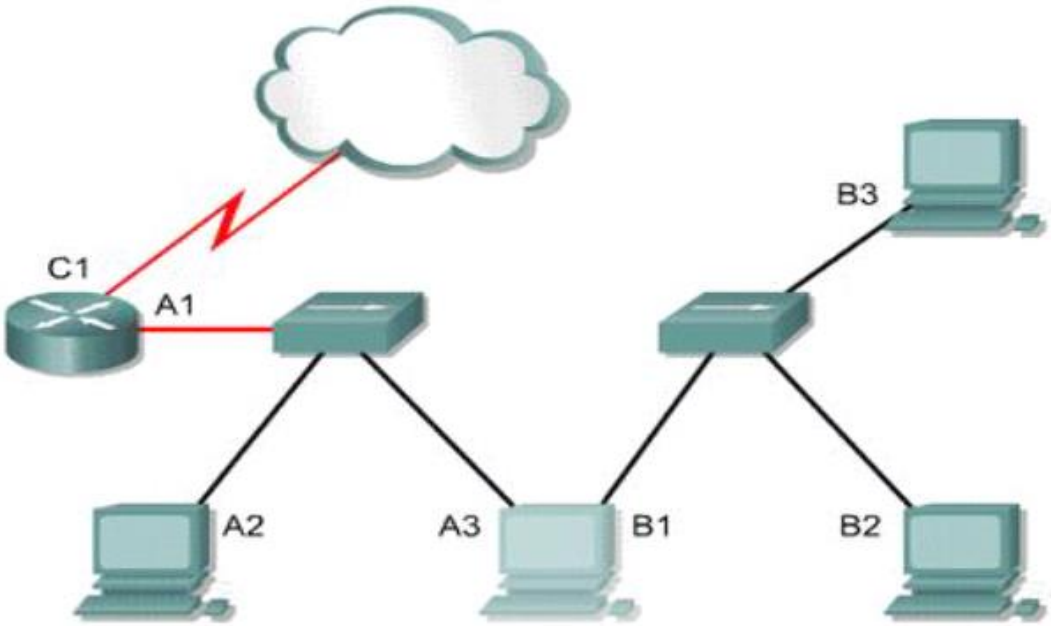
Ejercicios Modulo 2 Unidad 4 - Experto Universitario en Seguridad de la Información

¿Qué ejemplo de nuestra vida cotidiana, podríamos poner como "plan de contingencia"?

Un ejemplo de plan de contingencia en nuestra vida cotidiana podría ser tener un juego de llaves de repuesto en caso de que perdamos las originales. Siempre es prudente tener una copia de las llaves de casa o del auto guardada en un lugar seguro o confiarlas a una persona de confianza en caso de emergencia. Esto nos ayuda a estar preparados para situaciones inesperadas, como perder las llaves principales o quedarnos encerrados fuera de casa.

Ejercicio Número 1 Unidad 4

Observando el siguiente esquema de topología, cuantas situaciones o incidencias ¿podríamos poner como posibles problemas?



Según este diagrama algunos posibles problemas o incidencias podrian ser:

Fallos de hardware:

- Fallo del router: si el router falla, todos los dispositivos conectados a él perderán la conectividad de red
- Fallo del switch: si un switch falla, todos los dispositivos conectados a ese switch

perderán la conectividad de red.

- Fallo del dispositivo: si alguno de los dispositivos de la red falla, ya no podrá comunicarse con otros dispositivos de la red. Y si los dispositivos fallan al ser una topologia estilo "arbol" o similar, los dispositivos subyacentes tambien veran su conectividad interrumpida.

Problemas de conectividad:

- Fallos de cables: si alguno de los cables que conectan los dispositivos en la red falla, los dispositivos conectados a esos cables perderán la conectividad de la red.
- Errores de configuración: si alguno de los dispositivos de la red está configurado incorrectamente, es posible que no pueda comunicarse con otros dispositivos de la red.

Algunos ejemplos de perdida de conectividad podrian ser ocacionados por los siguientes ejemplos:

- Si se interrumpe la red desde la Nube a C1
- Si se interrumpen todas las conexiones presentes, ya que al ser una topologia tipo Árbol, al interrumpirse una conexion afecta a todos los dispositivos subyacentes.

Planes de Contingencia:

Los planes de contingencia a implementar deben incluir procedimientos para identificar y solucionar problemas, así como para restaurar la conectividad de la red en caso de una interrupción.

Algunos ejemplos específicos de medidas de planificación de contingencias que se pueden tomar:

- Copias de seguridad periódicas: realizar copias de seguridad periódicas de todos los datos de la red para poder restaurarlos en caso de una falla del hardware u otro desastre resultaria indispensable.
- Fuentes de energía redundantes: instalar fuentes de energía redundantes, como generadores o sistemas de alimentación ininterrumpida (UPS), para garantizar que los dispositivos continúen funcionando durante los cortes de energía.
- Monitoreo de red: utilizar herramientas de monitoreo de red para identificar y solucionar problemas antes de que causen interrupciones.
- Plan de recuperación ante desastres: desarrollar un plan de recuperación ante desastres que describa los pasos que se tomarán en caso de una interrupción importante y capacitar al personal de IT sobre éstos procedimientos.

Al tomar estas precauciones, la organización puede minimizar el riesgo de tiempo de inactividad de la red y garantizar que sus redes puedan satisfacer las necesidades de sus usuarios. Pero como dato mas importante a resaltar, yo implementaria una topologia diferente

que no sea tan vulnerable a fallos de conectividad, como malla o estrella extendida.

Consigna: A2 siempre tiene que llegar al equipo B3.

Interconectar y configurar los routers:

Se pueden configurar rutas estáticas en los switch (suponiendo que son L3) para dirigir específicamente el tráfico de A2 hacia B3 a través de un camino específico. Esto implica definir manualmente la ruta que debe seguir el tráfico para asi evitar interrupciones en la conexion si los cables A3 y B1 fallan.

Se debe especificar la dirección IP de destino (B3) y la interfaz de salida del switch S1 que conduce al dispositivo de red intermedio (en este caso, el switch S2).

Enrutamiento dinámico:

Se podrian configurar métricas de enrutamiento (se me ocurre por ejemplo con un balanceador de carga) personalizadas para favorecer la ruta que pasa por el switch S2. Esto garantizaria que el tráfico de A2 a B3 siempre elija la ruta más favorable a través de S2, incluso si hay otras rutas disponibles.

Redundancia de enlaces:

Se pueden establecer enlaces redundantes entre los dispositivos de red para proporcionar rutas alternativas en caso de que un enlace falle. Esto implica conectar los dispositivos con múltiples cables (en fin, reemplazando la topologia por las antes mencionadas como por ejemplo malla o estrella extendida).

Ejercicio Número 2 Unidad 4

Realizar una búsqueda en Internet y verificar cuántos posibles ataques distintos a correos electrónicos se pueden encontrar.

En caso de conocer alguno, subir un ejemplo explicando en modo resumen, una captura, una descripción.

Tips:

PHISHING: uno de los más conocidos y utilizados, se aprovechan de los desconocimientos de los usuarios, donde el atacante logra incentivando o forzando a que la víctima realice un click en un proceso, lo cual puede llevar a obtener datos de importancia.

Los posibles ataques a correos electrónicos son numerosos y en constante evolución debido al desarrollo de nuevas tecnologías y técnicas por parte de los atacantes. Algunos de los ataques comunes incluyen phishing, spear phishing, spoofing de correo electrónico, ataques de ingeniería social, ataques de ransomware a través del correo electrónico, y ataques de malware adjunto. Además, los ataques pueden variar en su nivel de sofisticación y enfoque, desde simples intentos de engañar al destinatario para que revele información confidencial hasta ataques más complejos que involucran el compromiso de cuentas de correo electrónico y la manipulación de sistemas de correo electrónico. En resumen, la cantidad de posibles ataques es significativa y en constante cambio a medida que surgen nuevas amenazas y vulnerabilidades.

Procedo a enumerar 5 de los ataques mas conocidos:

1 - Flood a correo electrónico: Es una forma de ataque de denegación de servicio (DDoS, por sus siglas en inglés) que se dirige específicamente a los servidores de correo electrónico. En este tipo de ataque, el objetivo es inundar el servidor de correo electrónico con una gran cantidad de tráfico de correo electrónico malicioso o no deseado, lo que provoca una sobrecarga en los recursos del servidor y lo hace incapaz de manejar solicitudes legítimas de correo electrónico.

El ataque de Flood a correo electrónico puede llevarse a cabo de varias maneras, pero generalmente implica el envío masivo de correos electrónicos desde múltiples direcciones IP, a menudo utilizando botnets o redes de computadoras comprometidas controladas por el atacante. Estos correos electrónicos pueden contener contenido malicioso, como archivos adjuntos infectados o enlaces a sitios web comprometidos, o simplemente pueden ser mensajes no deseados en grandes cantidades.

El objetivo principal de este tipo de ataque es abrumar al servidor de correo electrónico objetivo con una carga de trabajo excesiva, lo que hace que se vuelva lento o inaccesible para los usuarios legítimos que intentan enviar o recibir correos electrónicos. Además de causar interrupciones en el servicio, el ataque de Flood a correo electrónico también puede agotar los recursos del servidor, como el ancho de banda y la capacidad de procesamiento, lo que puede afectar negativamente a otros servicios y usuarios que dependen del mismo servidor.

Los ataques de Flood a correo electrónico pueden ser difíciles de mitigar debido a la naturaleza distribuida de los ataques y a la capacidad de los atacantes para cambiar constantemente las direcciones IP y las tácticas utilizadas. Los administradores de sistemas suelen implementar medidas de seguridad, como filtros de correo no deseado y sistemas de detección de intrusiones, para ayudar a protegerse contra este tipo de ataques, pero la prevención completa puede ser un desafío.

2 - Spoofing de correo electrónico: En este tipo de ataque, los atacantes falsifican la dirección de correo electrónico del remitente para hacer que el correo electrónico parezca que proviene de una fuente confiable. Esto se puede utilizar para engañar a los destinatarios y llevar a cabo ataques de phishing u otros tipos de estafas.

3 - Ataques de ransomware a través del correo electrónico: Los atacantes pueden distribuir ransomware a través del correo electrónico mediante el envío de archivos adjuntos maliciosos o enlaces a sitios web comprometidos. Una vez que el ransomware se ejecuta en el sistema de la víctima, cifra archivos y exige un rescate para su liberación.

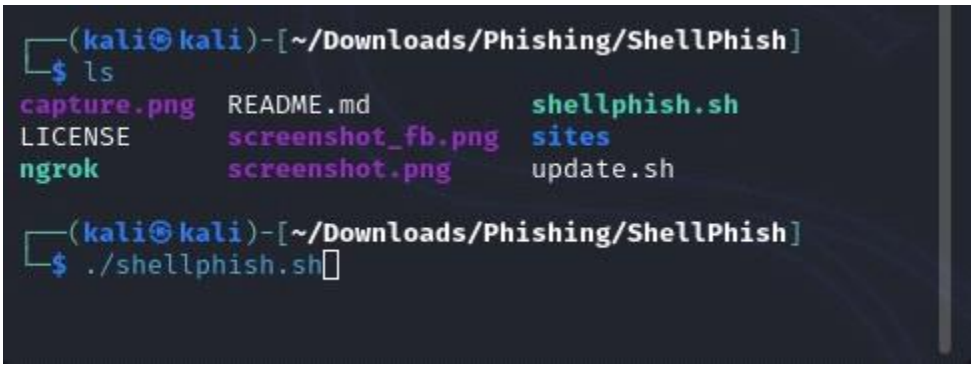
4 - Ataques de ingeniería social: Estos ataques implican el uso de técnicas psicológicas para engañar a los usuarios y obtener acceso no autorizado a información confidencial. Los atacantes pueden enviar correos electrónicos diseñados para manipular a los destinatarios y persuadirlos para que revelen información sensible o realicen acciones que beneficien al atacante.

5 - Ataques de malware adjunto: Los correos electrónicos pueden contener archivos adjuntos maliciosos, como documentos de Microsoft Office infectados, archivos PDF o archivos ejecutables, que pueden instalar malware en el sistema de la víctima cuando se abren. Este malware puede robar información, dañar archivos o tomar el control del sistema de la víctima para realizar actividades maliciosas.

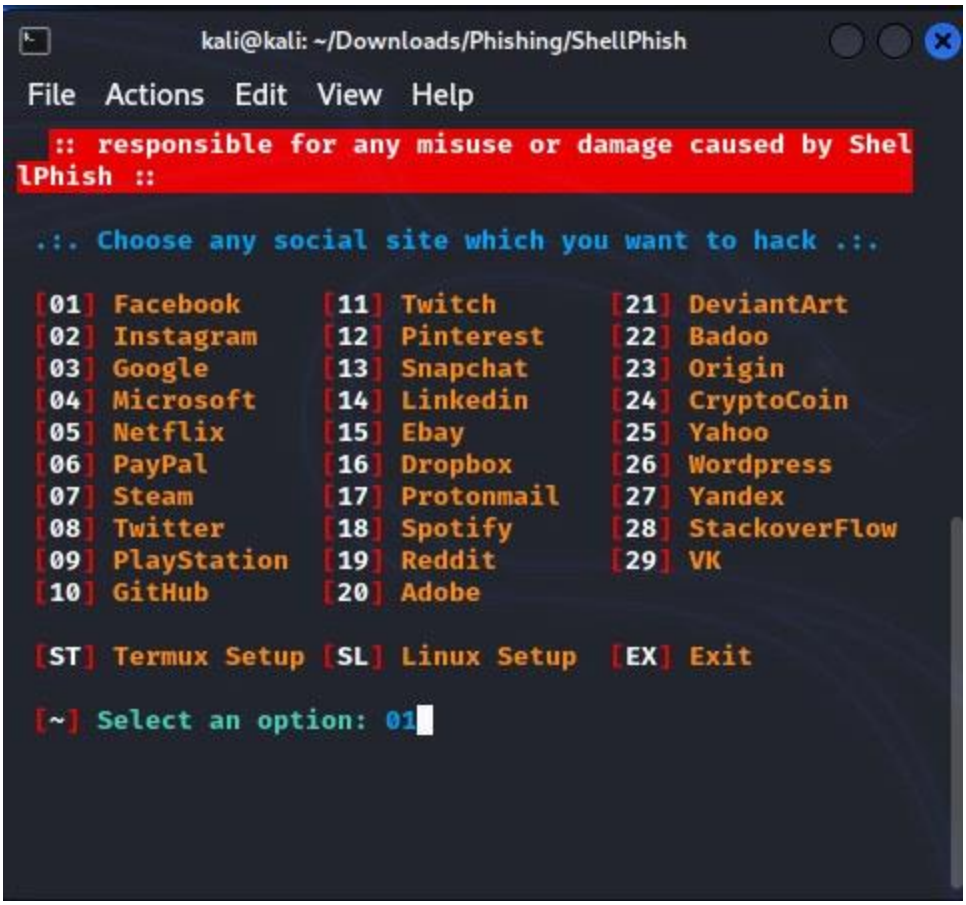
Como ejemplo, aprovecho esta consigna para exponer una investigacion reciente que realicé sobre la modalidad "Phishing" aprovechando las herramientas que me dio esta cursada sobre el sistema operativo Kali Linux. **A modo de "disclaimer" aclaro que el siguiente ejercicio se realizó solo con fines de investigación educativa y cualquier uso de lo aquí expuesto resulta ageno a mi responsabilidad.**

Utilizando la herramienta "Shellpish" procedo a realizar el siguiente laboratorio:

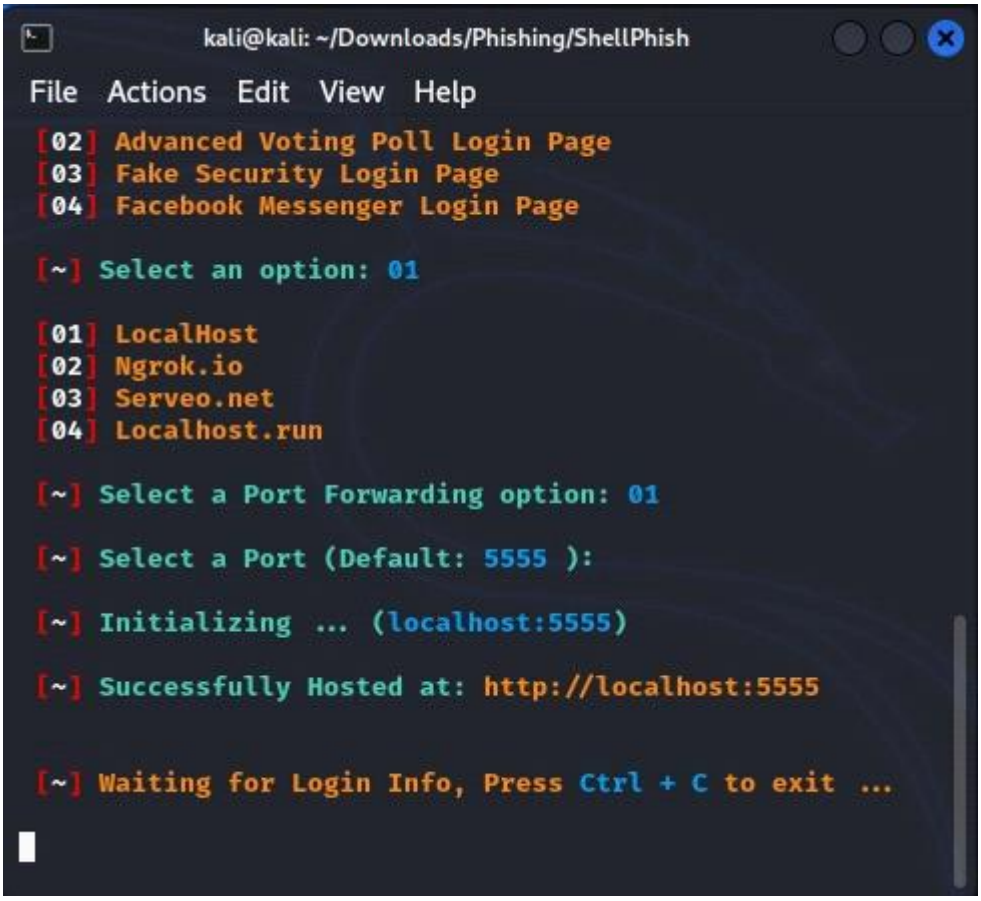
Paso 1 - Ejecuto la herramienta:



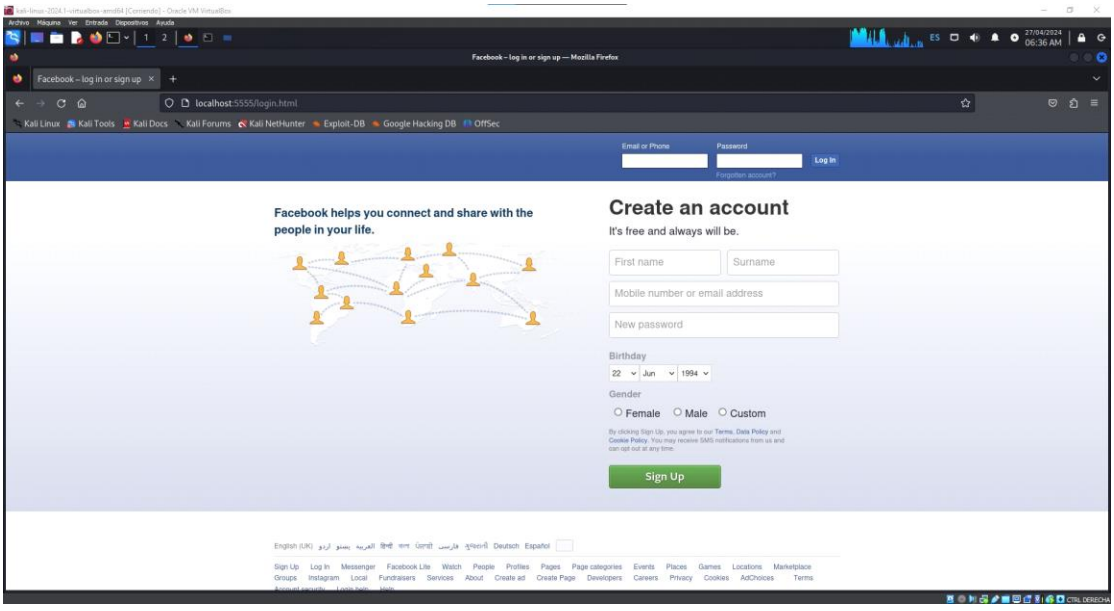
Paso 2 - Selecciono la plataforma a simular:



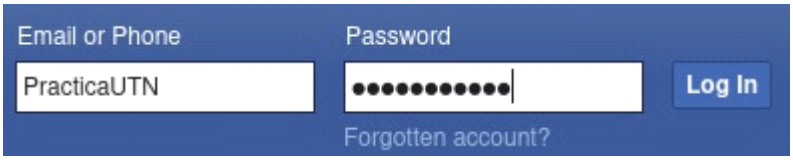
Paso 3 - Genero mi servidor donde se alojara la simulación. (En este caso localhost ya que no busca ser un tutorial sino una demostración). En cuyo caso hipotetico si quisiera exponerlo a internet eligiria "ngrok" por ejemplo, una herramienta similar a xampp en Windows y se me generaria un link el cual enviaria a la supuesta "victima":



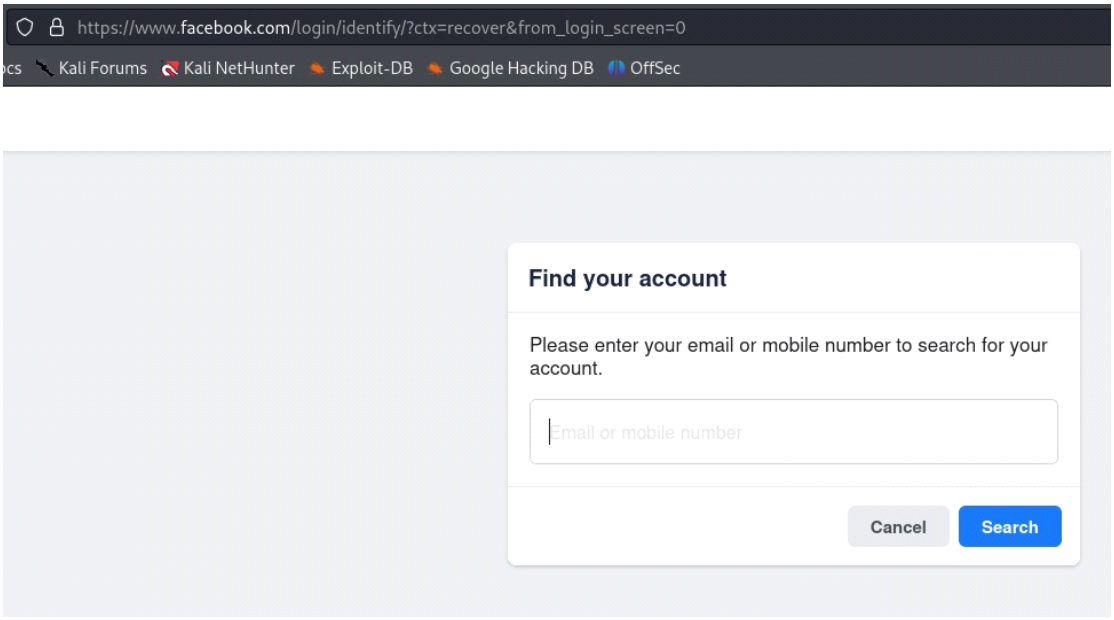
Paso 4 - Ingreso a la URL "trampa" donde se encuentra el sitio de phishing:



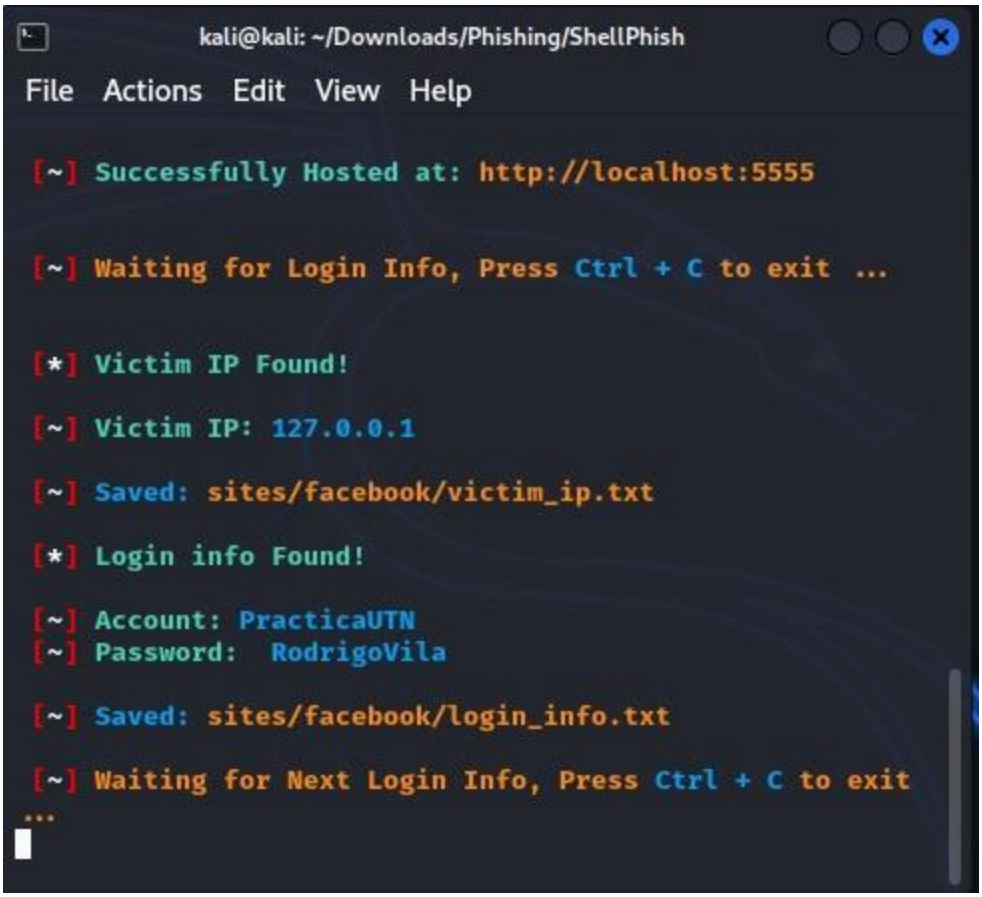
Paso 5 - El usuario "victima" introduce sus credenciales:



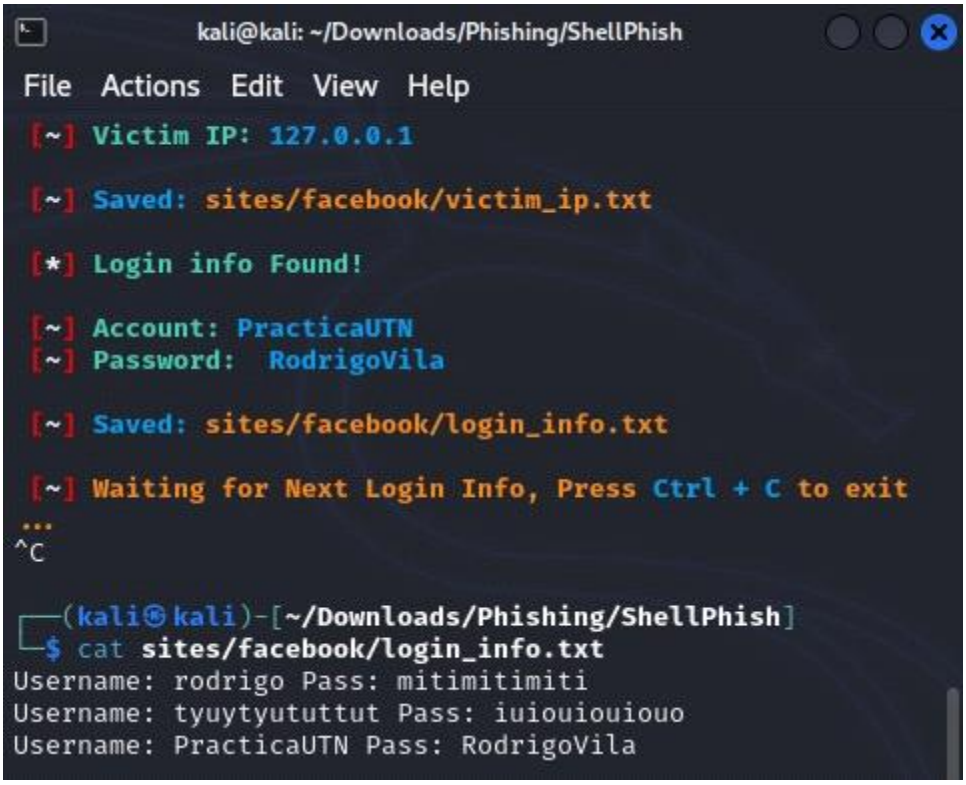
Paso 6 - Cuando el usuario procede a intentar loguear es redirigido a otro sitio, generalmente un sitio oficial de error o la URL original de la simulación.:



Paso 7 - Ya es demasiado tarde para la victima, el atacante ha recibido sus credenciales y hasta su numero de IP:



Nota: Generalmente estos sitios son enviados masivamente por email o a victimas seleccionadas de la organización objetivo. Creando asi una "base de datos" de credenciales para el atacante:



El mensaje de correo suele estar acompañado de metodologias combinadas como spoofing, ingenieria social, redirecciones, enmascaramientos, etc. con el objetivo de engañar a las personas.

Rodrigo Vila.-