ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA TELECOMUNICACIONES

IMPLEMENTACIÓN DE UN HONEYPOT UTILIZANDO KIPPO PARA MITIGAR LAS ACCIONES NO AUTORIZADAS DE LOS INTRUSOS AL PROTOCOLO SSH

Trabajo de Integración Curricular

Tipo: Proyecto Técnico

Presentado para optar al grado académico de:

INGENIERO EN TELECOMUNICACIONES

AUTOR:

FERNANDO JOSUEE ERAZO RIVERA

Riobamba – Ecuador

2023

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA TELECOMUNICACIONES

IMPLEMENTACIÓN DE UN HONEYPOT UTILIZANDO KIPPO PARA MITIGAR LAS ACCIONES NO AUTORIZADAS DE LOS INTRUSOS AL PROTOCOLO SSH

Trabajo de Integración Curricular

Tipo: Proyecto Técnico

Presentado para optar al grado académico de:

INGENIERO EN TELECOMUNICACIONES

AUTOR: FERNANDO JOSUEE ERAZO RIVERA

DIRECTOR: ING. MARCO VINICIO RAMOS VALENCIA

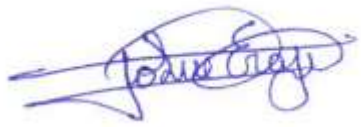
Riobamba – Ecuador

2023

Yo, Fernando Josuee Erazo Rivera, declaro que el presente Trabajo de Integración Curricular es de mi autoría y los resultados del mismo son auténticos. Los textos en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Integración Curricular; el patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 23 de agosto de 2023



Fernando Josuee Erazo Rivera
060542570-1

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA TELECOMUNICACIONES

El Tribunal del Trabajo de Integración Curricular certifica que: El Trabajo de Integración Curricular; tipo: Proyecto Técnico, **IMPLEMENTACIÓN DE UN HONEYPOT UTILIZANDO KIPPO PARA MITIGAR LAS ACCIONES NO AUTORIZADAS DE LOS INTRUSOS AL PROTOCOLO SSH**, realizado por el señor: **FERNANDO JOSUEE ERAZO RIVERA**, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Integración Curricular, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal Autoriza su presentación.

	FIRMA	**FECHA**
Ing. Dr. C. Pedro Severo Infante Moreira **PRESIDENTE DEL TRIBUNAL**		2023-08-23
Ing. Msc. Marco Vinicio Ramos Valencia **DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR**		2023-08-23
Ing. Oswaldo Geovanny Martinez Guashima **ASESOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR**		2023-08-23

DEDICATORIA

Dedico esta tesis a todos aquellos que, como yo, sienten una pasión por la seguridad informática y la ciberdefensa. En particular, agradezco a mi familia por su inquebrantable apoyo y comprensión durante el proceso de investigación. También quiero dedicar a mi tutor por su guía y sabiduría, y a mis amigos y colegas por su apoyo y aliento en cada paso del camino. Por último, dedico este trabajo a la comunidad de investigadores de Honeypot, cuyo trabajo es esencial para proteger nuestros sistemas y redes de los ataques maliciosos. Espero que mi proyecto técnico contribuya de alguna manera a la lucha contra el cibercrimen y la defensa de la seguridad en línea.

Fernando Josuee Erazo Rivera

AGRADECIMIENTO

Quiero agradecer a todas las personas que hicieron posible la realización de esta tesis. En primer lugar, a mi tutor, por su paciencia, orientación y apoyo constante durante todo el proceso de investigación. También agradezco a mis amigos y compañeros de clase, por su colaboración, ayuda y motivación constante. A mi familia, por su amor incondicional y apoyo inquebrantable en todas mis decisiones. Por último, agradezco a todas las personas que de alguna manera contribuyeron a este trabajo, por compartir su conocimiento y experiencia en el tema de estudio. Este trabajo no hubiera sido posible sin el apoyo y la colaboración de todas estas personas, y les agradezco de todo corazón su valiosa contribución.

Fernando Josuee Erazo Rivera

ÍNDICE DE CONTENIDO

CAPITULO III

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE ANEXO

RESUMEN

El objetivo de este proyecto técnico fue implementar un honeypot utilizando Kippo para mitigar las acciones no autorizadas de los intrusos al protocolo SSH, para lo cual se diseñó y desarrolló un escenario de pruebas mediante 3 máquinas virtuales como son: Kali Linux, Centos y Windows 7, configuradas correctamente con distintos sistemas operativos, los cuales fueron los encargados de realizar los ataques y un sistema operativo basado en Linux en el cual fue instalado el honeypot. Los ataques ejecutados y los registros analizados fueron llevados a cabo mediante el estándar de ejecución de pruebas de penetración (PTES), esta metodología de seguridad es una de las más usadas porque contiene fases y etapas que garantizan que todos los detalles se recopilen de manera eficiente y que el profesional de penetración tenga una idea clara de las acciones realizadas; se inició desde el reconocimiento donde se buscó y recopiló la mayor cantidad de información acerca del servidor SSH que va a ser vulnerado, luego se realizó un escaneo obteniendo la información detallada de toda la red, es decir los sistemas operativos, puertos y servicios que están activos, de esta manera se obtuvo acceso al servidor evadiendo los mecanismos de protección y teniendo el control de todos los datos. Todas las acciones quedaron registradas y almacenadas en un archivo, posteriormente se realizó el análisis de los datos obtenidos en los cuales se pudo observar las acciones que el intruso ejecutó en el servidor. Mediante estas acciones se ejecutó algunas recomendaciones como, por ejemplo: crear contraseñas más seguras y claves SSH, cambiar el puerto SSH que viene por defecto, bloquear automáticamente los ataques que llegan por fuerza bruta, deshabilitar el servidor OpenSSH en computadores personales y sobre todo mantener siempre actualizado SSH. De esta manera se concluye que al aplicar estas recomendaciones en el servidor SSH, este disminuye considerablemente los ataques y así se logra que se pueda mitigar las acciones no autorizadas de los intrusos al protocolo SSH. Se recomienda tener conectividad entre las 3 máquinas virtuales e instalar correctamente el honeypot Kippo.

Palabras clave: <SEGURIDAD INFORMÁTICA>, <ESTÁNDAR PTES>, <PRUEBAS DE PENETRACIÓN>, <LINUX (SOFTWARE)>, <VULNERABILIDADES INFORMÁTICAS>, <PROTOCOLO SSH>, <MITIGACIÓN DE VULNERABILIDADES>, <PYTHON (SOFTWARE)>.

SUMMARY / ABSTRACT

The objective of this technical project was to implement a honeypot using Kippo to mitigate the unauthorized actions of intruders to the SSH protocol, for which a test scenario was designed and developed using 3 virtual machines such as: Kali Linux, Centos and Windows 7, correctly configured with different operating systems, which were responsible for carrying out the attacks and a Linux-based operating system in which the honeypot was installed. The attacks executed and the logs analyzed were carried out using the Penetration Test Execution Standard (PTES), This security methodology is one of the most used because it contains phases and stages that guarantee that all the details are collected efficiently and that the penetration professional has a clear idea of the actions carried out; started from the reconnaissance where the most information about the SSH server to be compromised was searched and collected, later a scan was carried out obtaining detailed information of the entire network, that is, the operating systems, ports and services that are active, in this way access to the server was obtained, evading the protection mechanisms and having control of all the data. All the actions were registered and stored in a file, later the analysis of the data obtained was carried out, in which it was possible to observe the actions that the intruder carried out on the server. Through these actions, some recommendations were carried out, such as: creating more secure passwords and SSH keys, changing the SSH port that comes by default, automatically blocking attacks that arrive by brute force, disabling the OpenSSH server on personal computers and, above all, maintaining always updated SSH. In this way, it is concluded that by applying these recommendations in the SSH server, it considerably reduces the attacks and thus it is possible to mitigate the unauthorized actions of the intruders to the SSH protocol. It is recommended to have connectivity between the 3 virtual machines and to correctly install the Kippo honeypot.

Keywords: <COMPUTER SECURITY>, <PTES STANDARD>, <PENETRATION TESTING>, <LINUX (SOFTWARE)>, <COMPUTER VULNERABILITIES>, <SSH PROTOCOL>, <VULNERABILITY MITIGATION>, <PYTHON (SOFTWARE)>.

MSc. Wilson G. Rojas
NOMBRE Y FIRMA PROFESOR
C.I 0602361842

INTRODUCCIÓN

Los sistemas de detección de intrusos vienen siendo una herramienta muy importante para las personas encargadas de administrar la seguridad de redes, algunas personas piensan que un IDS ("Intrusion Detection System") es la solución para proteger a la red de personas no autorizadas causando una irreal sensación de seguridad en la red, se debe tener en cuenta que un detector de intrusos no es más que una medida de seguridad para proteger la red.(Torres Garcia y Zambrano Nuñez 2011, p. 16). Unas de las ventajas que presentan estos sistemas es de proveer de información detallada y necesaria para conocer de las vulnerabilidades que presenta la red antes de que sean explotadas y así lograr desarrollar una seguridad adecuada.

Hoy en día existen muchas redes que se encuentran interconectadas entre sí por medio del internet teniendo así acceso a cualquier máquina que se encuentre conectada a la red, de esta forma existe un índice alto de intrusos que entran a estas redes con la finalidad de causar daños o lo más peligroso aún, el robo de información valiosa y personal; por lo que es muy necesario aumentar la seguridad de estos sistemas. (Castro Guerrero 2011, p. 11)

Uno de los problemas o amenazas que se han generado es el de GoScanSSH, el cual es "una nueva variedad de malware que se ha estado dirigiendo a servidores SSH basados en Linux expuestos a Internet desde junio de 2017. El malware intenta obtener una credencial SSH válida a través de un ataque de lista de palabras e intenta infectar el host. Tras iniciar sesión con éxito, se entrega nuevo malware que infecta el host y el proceso se repite". (ssh.com 2021c)

Otra amenaza es sobre : BothanSpy y Gyrfalcon que "son supuestas herramientas de piratería de la CIA que tienen como objetivo varias implementaciones de SSH (Secure Shell) con el objetivo de robar nombres de usuario, contraseñas, claves SSH y frases de contraseña de claves SSH . Son herramientas que se usan después de que ya se ha obtenido acceso a la máquina de destino, generalmente la computadora de escritorio/portátil de un usuario, y se usan para robar credenciales que luego se pueden usar para propagar el ataque a servidores y otros sistemas". (wikileaks 2017)

Bothanspy se dirige al cliente ssh en Microsoft Windows mientras que Gyrfalcon apunta al cliente openssh en plataformas Linux.

Entre los incidentes relacionados al protocolo ssh se da en abril de 2020, la OMS (Organización Mundial de la Salud) anunció que "se accedió sin autorización a algunas de las cuentas de sus

empleados. Este caso no es una violación perse, ya que las credenciales utilizadas para el acceso ilegal formaban parte de una enorme base de datos de credenciales recopiladas a partir de varias filtraciones".(ssh.com 2021b)
Sin embargo, algunos empleados de la OMS habían utilizado las credenciales de inicio de sesión de la empresa en servicios de terceros que fueron violados, y los piratas informáticos utilizaron la información reutilizada para obtener acceso.

Por lo escrito anteriormente, los honeypots KIPPO muestran una alternativa para poder mitigar dichas amenazas e incidentes. Se dice que los Honeypot son trampas que están destinados a ser atacadas. Es por eso que KIPPO es un Honeypot, "destinado a capturar información detallada sobre ataques de intrusos, con sistemas, aplicaciones y servicios virtuales a ser comprometidos teniendo en cuenta que no son reales (los cuales no se encuentran en producción) y con costos muy por debajo en comparación con otros tipos de Honeypots ya que no utiliza mucho hardware, beneficiando a todo servidor que este expuesto al mundo exterior". (Castro Guerrero 2011, p. 11)

CAPÍTULO I

1. DIAGNÓSTICO DEL PROBLEMA

En este capítulo se realiza interrogantes sobre la importancia y necesidad de implementar un honeypot para mitigar que intrusos no autorizados accedan al protocolo ssh, de la misma manera se ejecuta su respectiva justificación y las consecuencias que puede causar un acceso de dichos intrusos, además se explica el objetivo principal y específicos.

1.1 Formulación del problema

¿Es importante y necesario implementar un honeypot utilizando KIPPO para mitigar las acciones no autorizadas de los intrusos al protocolo SSH?

1.2 Sistematización del problema

¿Existen mecanismos de defensa para la seguridad de redes?
¿Cuál es el problema con los mecanismos de defensa en la seguridad de redes?
¿Qué metodologías me permiten realizar un escaneo de vulnerabilidades en la red?
¿Cuál es el propósito de implementar un honeypot?
¿Por qué utilizar KIPPO?
¿Se puede utilizar KIPPO para la detección de otras vulnerabilidades?
¿Por qué es importante saber qué acciones realizan los intrusos no autorizados al protocolo SSH?
¿Cuáles son las consecuencias de los ingresos no autorizados al protocolo SSH?

1.3 Justificación del trabajo de titulación

1.3.1 Justificación teórica

Existen varios mecanismos de defensa para la seguridad de redes como son los firewalls, redes privadas virtuales (VPNs), listas de control de acceso, sistemas de detección de intrusos (IDS), etc. Algunos de los problemas más frecuentes que se pueden dar en estos mecanismos de seguridad son cuando estos no están configurados de la manera correcta, y de este modo consiguen proporcionar una inexistente sensación en la seguridad.(Castro Guerrero 2011, p. 11)

Uno de los problemas que se presentan en los mecanismos de defensa de seguridad de redes por ejemplo en un IDS o también llamado Sistema de Detección de intrusos es que a menudo se presentes falsos positivos, esto ocurre cuando algunos datos que son normales diariamente en el tráfico coincidan con un ataque conocido y de esta manera puedan generar alertas y pensar que se está recibiendo un ataque de algún intruso no autorizado.(Castro Guerrero 2011, p. 21)

Para realizar análisis o escaneo de vulnerabilidades de la seguridad de redes o sistemas, existen algunas metodologías o estándares, tales como: Proyecto de seguridad de aplicaciones web abiertas (OWASP), el Manual de metodología de prueba de seguridad de código abierto (OSSTMM), el Marco de evaluación de seguridad de los sistemas de información (ISSAF) y el Estándar de ejecución de pruebas de penetración (PTES), las cuales la mayoría siguen la misma metodología, pero sus fases se denominan de forma distinta.

El propósito de implementar un honeypot es activar un servidor y llenarlos de archivos tentadores, logrando que sea difícil pero no imposible de penetrarlo, de esta manera atrae a los atacantes (como la miel) esperando que los intrusos aparezcan, de esta manera se observa los movimientos y las acciones de los intrusos, obteniendo así información sobre las estrategias de ataque.

En este proyecto se utilizará KIPPO ya que "es un honeypot de interacción media a través de SSH diseñado para registrar ataques de fuerza bruta y, lo más importante, toda la interacción Shell realizada por el atacante". (GitHub 2022)
Además, Kippo no sirve para detectar otras vulnerabilidades, este programa detecta intrusos y se encarga de registrar los ataques y las acciones generados mediante una conexión SSH.

Es muy importante conocer las acciones que realizan los intrusos no autorizados al protocolo SSH ya que al tener un servidor Linux estamos expuestos a ataques de acceso remoto y SSH es el protocolo utilizado para tener acceso a esos servidores, además una vez conocidas estas acciones que realizan los atacantes se puede dar recomendaciones para conseguir mitigar este problema.

Las consecuencias de ingresos de intrusos no autorizados a un servidor mediante el protocolo SSH son graves ya que pueden manejar por completo la computadora mediante intérpretes de comandos, robar, copiar o secuestrar información valiosa como datos personales y redirigir el tráfico para poder ejecutar otros programas.

1.3.2 Justificación aplicativa

Para la realización de este proyecto primero se deberá conocer toda la información necesaria e importante acerca del protocolo ssh, así como la aplicación correcta de un honeypot para que funcione de manera eficiente.

Posteriormente, se va a aplicar la metodología de seguridad más adecuada para este tipo de proyecto, junto con su respectiva herramienta de testeo que brindará toda la información de vulnerabilidades en el protocolo ssh,

Después, se va a desarrollar un escenario de pruebas tal y como se observa en la ilustración 1-1 el cual, en una sola computadora física, a través de la ayuda de 3 máquinas virtuales, se instalará distintos sistemas operativos los cuales serán los encargados de realizar los ataques y de esta manera observar las vulnerabilidades que tiene el servidor SSH,

Además, se va a implementar un honeypot KIPPO que permitirá analizar los resultados de los atacantes mediante los registros guardados en la base de datos y de esta manera establecer recomendaciones los cuales nos permitirá disminuir los ataques al protocolo ssh y así mitigar las acciones no autorizadas de los intrusos al protocolo ssh.

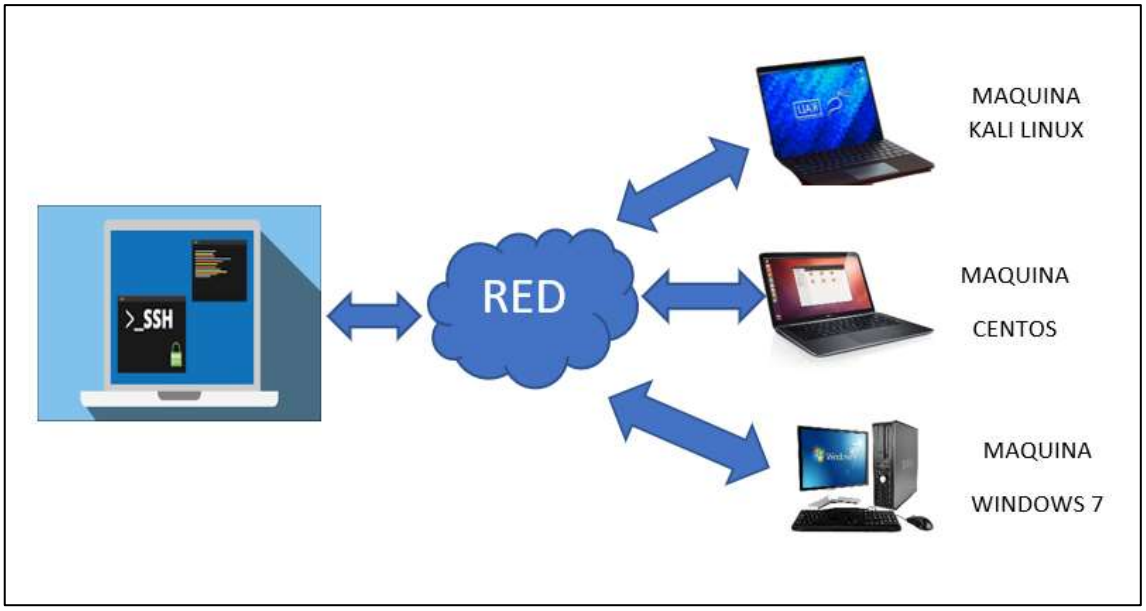


Ilustración 1-1: Arquitectura de la red

Realizado por: Erazo, J, 2022

1.4 Objetivos

1.4.1 Objetivo general

Implementar un honeypot utilizando KIPPO para mitigar las acciones no autorizadas de los intrusos al protocolo SSH.

1.4.2 Objetivos específicos

- Conocer la información necesaria de las vulnerabilidades del protocolo SSH en accesos no autorizados, y la aplicación correcta de un honeypot.
- Aplicar las metodologías de seguridad y herramientas de testeo en el análisis de vulnerabilidades en accesos no autorizadas a SSH.
- Desarrollar un escenario de pruebas que permita realizar los ataques y observar las vulnerabilidades mediante la implementación de la honeypot KIPPO.
- Analizar los resultados obtenidos con KIPPO y establecer recomendaciones para evitar futuras intrusiones en el protocolo SSH.

CAPÍTULO II

2. MARCO TEÓRICO

Este capítulo expone toda la información necesaria e importante que se debe conocer acerca de un honeypot y su correcta aplicación, así como conceptos básicos sobre el protocolo ssh, metodologías de seguridad y herramientas de testeo para el análisis de vulnerabilidades.

2.1 Ssh

SSH, Secure Shell, "es un enfoque popular, potente y basado en software para la seguridad de la red". (Barrett, Silverman y Byrnes, 2005, p. 1)

Cada vez que una computadora envía datos a la red, SSH los cifra (codifica) automáticamente. Luego, cuando los datos llegan a su destinatario, SSH los descifra (decodifica) automáticamente. El resultado es un cifrado transparente: los usuarios pueden trabajar con normalidad, sin saber que sus comunicaciones están cifradas de forma segura en la red. Además, SSH utiliza algoritmos de encriptación seguros y modernos y es lo suficientemente eficaz como para encontrarse en aplicaciones de misión crítica en las principales corporaciones.(Barrett, Silverman y Byrnes, 2005, p. 1-2)

Ssh crea un canal en una computadora remota con cifrado de extremo a extremo para así poder ejecutar el Shell, además ssh no tiene una seguridad completa, pero cabe recalcar que nada lo es, lo cual no protegerá de intrusos o ataques, sin embargo, proporciona autenticación, encriptación y es fácil de usar.(Barrett, Silverman y Byrnes, 2005, p. 3)

Hoy en día, el protocolo se utiliza para administrar más de la mitad de los servidores web del mundo y habitualmente en todas las computadoras Linux o Unix, ya sea físicamente o mediante la nube. Los administradores y especialistas en seguridad de la información lo saben utilizar para configurar, dirigir, mantener y operar la mayoría de los firewalls, conmutadores, enrutadores y servidores en los millones de redes y entornos de misión crítica de nuestro mundo digital. También está integrado en muchas soluciones de administración de sistemas y transferencia de archivos.

El nuevo protocolo reemplazó varias herramientas y protocolos heredados, incluidos telnet, ftp, FTP / S, rlogin (inicio de sesión remoto), rsh (Shell remoto) y rcp (copia remota).

2.1.1 Características de Ssh

- **Inicios de sesión remotos seguros**

Ssh inicia sesión remota segura mediante el cliente ssh, es decir el cliente se autentica en el servidor SSH de un ordenador remoto por medio de una conexión encriptada, consiguiendo que la contraseña y el nombre de usuario estén encriptados antes de salir de la computadora local, después el servidor ssh inicia la sesión de manera cifrada viajando entre el cliente y servidor.

Es así como ssh evita los problemas que tenía telnet, el cual también permitía iniciar sesión de manera remota en una computadora desde otra, pero lamentablemente telnet y softwares similares transmiten las contraseñas y el nombre de usuario en texto sin formato, lo cual hace vulnerable a que una persona maliciosa pueda interceptar. (Barrett, Silverman y Byrnes 2005, p. 5-7)

- **Transferencia segura de archivos**

Cuando se usa ssh, los archivos se pueden transferir de manera segura entre computadores con un comando de copia segura llamado scp que al ser transmitido el archivo se cifra automáticamente, a diferencia de cuando se utiliza un programa como ftp, al no proporcionar una solución segura en los paquetes que viajan por la red pueden ser interceptados fácilmente por terceros.(Barrett, Silverman y Byrnes, 2005, p. 7)

- **Ejecución remota segura de comandos**

Los clientes ssh pueden ejecutar un solo comando remoto para muchas computadoras en una red local, los cuales viajan por la red de manera cifrada.(Barrett, Silverman y Byrnes, 2005, p. 7)

- **Claves y agentes**

Ssh tiene diversos mecanismos de autenticación, y el más seguro son las claves en vez de contraseñas. Una clave es “una pequeña cantidad de bits que identifica de manera única a un usuario de SSH. Por seguridad, una clave se mantiene encriptada; se puede usar solo después de ingresar una frase de contraseña secreta para descifrarlo”.(Barrett, Silverman y Byrnes, 2005, p. 8)

De esta manera ssh puede autenticarse en todas las cuentas de la computadora sin la necesidad de ingresar repetidamente o memorizar varias contraseñas, ya que por razones de seguridad a veces los usuarios prefieren poner distintas contraseñas para todas las cuentas disponibles.

- **Control de acceso**

Ssh permite que otras personas puedan usar distintas cuentas de computadora para realizar ciertos propósitos, por ejemplo revisar correos electrónicos en el computador de otra personas sin revelar o cambiar la contraseña.(Barrett, Silverman y Byrnes, 2005, p. 8)

2.2 OpenSsh

"OpenSSH es una implementación de código abierto del protocolo SSH . Está basado en la versión gratuita de Tatu Ylonen y desarrollado por el equipo de OpenBSD y la comunidad de usuarios".(ssh.com, 2021a)

2.3 Claves ssh

"SSH proporciona un mecanismo de autenticación basado en claves criptográficas, denominado autenticación de clave pública. La clave privada correspondiente a una clave autorizada sirve como autenticación para el servidor".(ssh.com, 2021a)

Estas claves vienen siendo contraseñas muy seguras ya que vienen cifradas con una contraseña en forma de frase donde solo el usuario conoce, sin embrago estas claves son utilizadas en automatización y casi no tienen estas frases, Las claves de usuario se utilizan para autenticar usuarios y las claves de hosts para autenticar hosts. (ssh.com, 2021a)

"Las claves SSH reemplazaron la autenticación insegura .rhosts que era vulnerable a ataques activos a nivel de red. Reemplazar .rhosts mejoró enormemente la seguridad de Internet y los sistemas de información empresarial".(ssh.com, 2021a)

Sin embargo, OpenSSh se remitió de manera gratuita en muchos de los sistemas operativos y esto llevó a falta de políticas por lo cual los administradores no llegaron a prestar atención suficiente y por lo tanto no son tan utilizadas ya que para algunos las claves ssh brindan el mismo nivel de acceso que los nombres de usuarios y contraseñas. (ssh.com, 2021a)

2.4 Honeypot

"Es un programa que tiene la apariencia de un servicio atractivo, un conjunto de servicios, un sistema operativo completo o incluso una red completa, pero en realidad es un compartimento herméticamente cerrado construido para atraer y contener a un atacante".(Joshi y Sardana, 2011, p. 7)
Otros autores definen a un honeypot como: "un recurso de seguridad cuyo valor radica en ser probado, atacado o comprometido."(Spitzner, 2002, p. 58)
Este sistema está colocado para que un atacante encuentre el sistema y lo explote. Sin embargo, lo que el atacante generalmente ignora es que el honeypot no contiene datos reales de valor y está aislado de otros dispositivos de red. Los defensores de redes pueden usar la información de registro detallada recopilada por el señuelo para derivar herramientas, tácticas y procedimientos utilizados por el atacante.(Sanders y Smith, 2014, p. 317)

2.4.1 Clasificación de los honeypots

- **Honeypots interacción baja**

"Un honeypot de baja interacción está basado en software y está diseñado para emular uno o más servicios".(Sanders y Smith, 2014, p. 319)
Además, son los más simples para instalar, configurar, implementar y mantener, ya que tiene un diseño simple como se muestra en la ilustración 1-2, con lo cual el atacante se limita a interactuar con los servicios designados anteriormente. Por ejemplo, estos honeypots podrían emular servidores Unix con servicios como FTP y Telnet.(Mohammed y Rehman, 2016, p. 108)
De hecho, la función principal de este clase de honeypots es de escaneos no autorizados o conexiones no autorizadas y capturar toda actividad de un atacante obteniendo una ventaja el cual, el atacante tiene restricciones para atacar otros host desde el honeypot.(Mohammed y Rehman, 2016, p. 109)

También están diseñados para capturar comportamientos conocidos. El atacante actúa de cierta manera y el honeypot responde de una manera predeterminada. Los honeypots de interacción baja no son buenos para interactuar o descubrir comportamientos o ataques desconocidos o inesperados.(Spitzner, 2002, p. 93)

El nivel de interacción que brindan depende del servicio que se está emulando y del software en sí. Por ejemplo, Kippo es un honeypot de interacción baja que imita el servicio SSH. Permite que un atacante inicie sesión en este servicio e incluso navegar por un sistema de falsos archivos. Sin

embargo, nunca permite que un atacante acceda a un componente real del sistema operativo subyacente.(Sanders y Smith, 2014, p. 319)

- **Honeypots interacción alta**

Brindan un sistema operativo real para atacar, lo que atrae al hacker informático y, por otro lado, expone el sistema a un gran riesgo. Estos honeypots son utilizados especialmente para fines investigativos, ya que ofrecen acceso completo y la posibilidad de acumular información sobre el ataque. A demás, son difíciles de implementar porque se debe utilizar muchas herramientas para ejecutarlos, requieren mucho tiempo y conllevan un nivel de riesgo alto.(Joshi y Sardana, 2011, p. 17)

Los honeypots de interacción alta ofrecen gran cantidad de información de los atacantes, dan acceso al atacante a un sistema operativo real en el que no se emula ni se restringe nada y así identificar nuevas vulnerabilidades, pero una vez que los malos tienen acceso a uno de estos honeypots, tienen un sistema completamente operativo para interactuar, lo que les da la capacidad de hacer lo que quieran, como atacar otros sistemas o capturar la actividad de producción. Se debe realizar una gran cantidad de trabajo para mitigar estos riesgos.(Spitzner, 2002, p. 96)

Un honeypot de interacción alta en realidad está configurado para reflejar un sistema de producción, y está diseñado para dar a un atacante el dominio completo de un sistema operativo en caso de que se sienta tentado a comprometerlo. Este sistema se configurará para utilizar un amplio registro del sistema de archivos, y también estará sujeto a un conjunto muy exhaustivo de reglas y supervisión de IDS.(Sanders y Smith, 2014, p. 319)

- **Honeypots interacción media**

Los honeypots de interacción media ofrecen a los atacantes más capacidad de interacción que los honeypots de interacción baja, pero menos funcionalidad que las soluciones de interacción alta como se observa en la ilustración 1-2. Pueden esperar cierta actividad y están diseñados para dar ciertas respuestas más allá de lo que daría un honeypot de baja interacción.(Spitzner, 2002, p. 94)

Estos honeypots no tienen un entorno de sistema operativo real ni implementan todos los detalles del protocolo de aplicación. Tienen una capa de virtualización. Simplemente proporcionan respuestas que el hacker espera.

“Kippo es un honeypot de interacción media porque es un software que simula un servicio, pero también simula un sistema de archivos falso con el que un atacante puede interactuar”. (Sanders y Smith, 2014, p. 319)

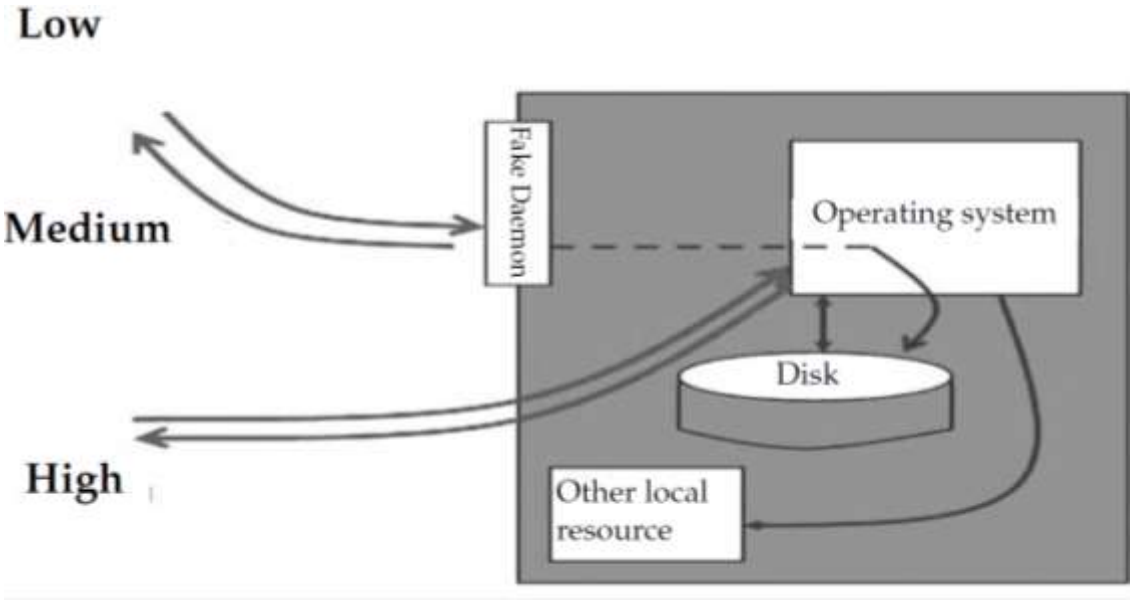


Ilustración 1-2: Clasificación de los Honeypots

Fuente: (Joshi y Sardana 2011, p. 16)
Realizado por: Erazo, J, 2022

2.4.2 Tipos de honeypots

- **Honeypots físicos**

Es una sola máquina que ejecuta un sistema operativo real y servicios reales, donde el honeypot está conectado a una red y es accesible a través de una sola dirección IP. Los honeypots físicos siempre están conectados con el concepto de honeypots de interacción alta. Los honeypots físicos son menos prácticos en escenarios reales debido a la vista limitada de su dirección IP única y al alto costo que implica mantener una granja de honeypots físicos. Honeynets son un ejemplo de honeypots físicos.(Joshi y Sardana, 2011, p. 19)

- **Honeypots virtuales**

Por lo general, se implementan utilizando una sola máquina física que aloja varios honeypots virtuales. Los honeypots virtuales son más rentables para monitorear grandes espacios de direcciones IP y emular grandes direcciones IP al mismo tiempo.(Joshi y Sardana, 2011, p. 19)
Usamos el término virtual porque los diferentes sistemas operativos tienen la apariencia de estar ejecutándose en sus propias computadoras independientes, que no son máquinas reales. Estas soluciones son posibles gracias al software de virtualización que permite ejecutar varios sistemas operativos al mismo tiempo, en el mismo hardware.

Las ventajas de un honeypot virtual son los costos reducidos y una administración más sencilla, ya que todo se combina en un solo sistema, en lugar de necesitar muchas computadoras para implementar.(Mohammed y Rehman, 2016, p. 14-15)
Hoy en día, existen muchas opciones de herramientas para virtualización entre las que podemos sugerir: VMWare, VirtualBox, entre otros.

2.5 Kippo

"Kippo es un honeypot de interacción media que simula un servidor SSH y está diseñado para detectar intentos de fuerza bruta y registrar la interacción del atacante con un entorno de shell simulado".(Sanders y Smith, 2014, p. 328)
Kippo es útil porque el protocolo SSH se usa comúnmente para administrar dispositivos basados en Unix.

2.5.1 Características de Kippo

- Sistema de archivos falso con la capacidad de agregar/eliminar archivos. Se incluye un sistema de archivos falso completo que se asemeja a una instalación de Debian 5.0
- Posibilidad de agregar contenidos de archivos falsos para que el atacante pueda 'catear' archivos como /etc/passwd. Solo se incluyen contenidos de archivo mínimos
- Registros de sesión almacenados en un formato compatible con UML para una fácil reproducción con los tiempos originales
- Al igual que Kojoney, Kippo guarda los archivos descargados con wget para su posterior inspección.
- Astucia; ssh finge conectarse en algún lugar, exit realmente no sale, etc.(GitHub, 2022)

2.5.2 Requisitos

- Un sistema operativo (probado en Debian, CentOS, FreeBSD y Windows 7)
- Python 2.5+
- Twisted 8.0 a 15.1.0
- PyCrypto
- Interfaz Zope(GitHub, 2022)

2.5.3 ¿Cómo ejecutarlo?

- Edite kippo.cfg a su gusto e inicie el honeypot ejecutando:

./start.sh

- start.sh es un script de shell simple que ejecuta Kippo en segundo plano usando twistd. Se pueden proporcionar opciones de inicio detalladas ejecutando twistd manualmente. Por ejemplo, para ejecutar Kippo en primer plano:

twistd -y Kippo.tac -n

- Por defecto, Kippo escucha las conexiones ssh en el puerto 2222. Puede cambiar esto, pero no lo cambie a 22 ya que requiere privilegios de root. Utilice el reenvío de puertos en su lugar.(GitHub, 2022)

Archivos de interés:

- dl/ - los archivos descargados con wget se almacenan aquí
- log/kippo.log - salida de registro/depuración
- log/tty/ - registros de sesión
- utils/playlog.py - utilidad para reproducir registros de sesión
- utils/createfs.py - usado para crear fs.pickle
- fs.pickle - sistema de archivos falso
- honeyfs/ - contenido del archivo para el sistema de archivos falso - siéntase libre de copiar un sistema real aquí(GitHub, 2022)

2.6 Nmap

"Nmap (abreviatura de Network Mapper) es una herramienta para recopilar información de red".(Rahalkar y Jaswal 2019, p. 16)

Sirve tanto para la recopilación y enumeración de información. A simple vista, puede parecer una herramienta bastante pequeña y sencilla. Sin embargo, es tan completo que nos puede brindar una descripción general rápida de qué puertos están abiertos y qué servicios se están ejecutando en nuestra red de destino. (Rahalkar y Jaswal 2019, p. 16)

Los propósitos en los cuales se le puede utilizar son los siguientes:

- Descubrimiento de host
- Detección de servicios
- Enumeración de versiones
- Escaneo de vulnerabilidades
- Pruebas de evasión de cortafuegos

Nmap cuenta con muchos parámetros para configurar los cuales se lo presenta en la tabla 1-2:

Tabla 1-2: Parámetros de la herramienta de testeo Nmap

PARÁMETRO	SIGNIFICADO
-sT	Realiza una exploración de conexión
-sU	Realiza un escaneo para detectar puertos UDP abiertos
-sP	Realiza un escaneo de ping simple
-A	Realiza un análisis agresivo
-sV	Realiza la detección de la versión del servicio
-v	Imprime salida detallada
-p 1-1000	Escanea puertos en el rango del 1 a 1000
-o	Realiza detección de sistema operativo
-iL	Escanea todos los hosts del archivo especificado
-ox	Salida de los resultados del escaneo en formato XML
-oG	Salida de los resultados del escaneo en formato greppable

Fuente: (Rahalkar y Jaswal 2019, p. 91)

Realizado por: Erazo, J, 2022

2.7 Metodologías de Penetración

Las pruebas de penetración siguen una metodología o estándar, existen varias metodologías como, por ejemplo: Proyecto de seguridad de aplicaciones web abiertas (OWASP), el Manual de metodología de prueba de seguridad de código abierto (OSSTMM), el Marco de evaluación de seguridad de los sistemas de información (ISSAF) y el Estándar de ejecución de pruebas de penetración (PTES), las cuales la mayoría siguen la misma metodología, pero sus fases se denominan de forma distinta.

2.7.1 Owasp

OWASP significa Open Web Application Security Project, o en español proyecto de seguridad de aplicaciones web abiertas; proporciona metodologías y listas de las 10 mayores debilidades de seguridad que se presentan en las aplicaciones web como se muestra en la ilustración 2-2. Esta

lista es usada por las profesionales que se dedican a penetrar las aplicaciones web y es lo que la mayoría de las empresas buscan cuando contratan profesionales de penetración para probar sus aplicaciones web. Esta es también la forma más común y frecuente de pruebas de penetración.(Singh 2019, p. 20)

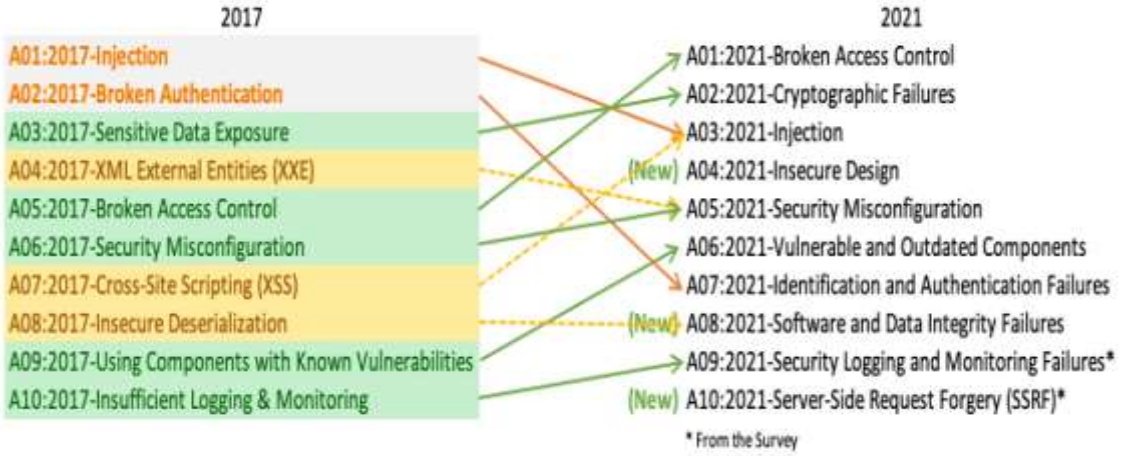


Ilustración 2-2: Top 10 OWASP

Realizado por: Erazo, J, 2022

También se caracteriza por ser una asociación de profesionales con ideas similares que lanzan software y documentación que se basa en el conocimiento en la seguridad de las aplicaciones, cubriendo temas como:

- “Recopilación de la información
- Pruebas de gestión de la configuración e implementación
- Pruebas de gestión de la identidad
- Pruebas de autenticación
- Pruebas de autorización
- Pruebas de gestión de sesiones
- Pruebas de validación de la entrada
- Manejo de los errores
- Criptografía
- Pruebas de lógica de negocios
- Pruebas del lado del cliente” (Sharma y Singh 2018, p. 6)

2.7.2 Osstmm

Osstmm "Es un manual revisado por pares de pruebas y análisis de seguridad que da como resultados hechos verificados. Estos hechos proporcionan información procesable que puede mejorar considerablemente su seguridad operativa".(Herzog 2010, p. 1)

Se utiliza para realizar pruebas de seguridad exhaustivas y está diseñado para ser repetible y consistente. Está abierto a las contribuciones de todos los evaluadores de seguridad, lo que fomenta pruebas de seguridad mucho más precisas, procesables y productivas.(Singh y Sharma 2020, p. 9)

La Osstmm incluye las siguientes secciones clave:

- **Métricas de seguridad operativa**

Se ocupa de lo que debe protegerse y de la exposición de la superficie de ataque. Esto se puede medir creando un RAV (una descripción fáctica imparcial de la superficie de ataque).(Singh y Sharma 2020, p. 10)

- **Análisis de confianza**

La confianza se mide como las interacciones entre objetivos dentro del alcance que cualquier persona puede explotar con malas intenciones. Para cuantificar la confianza, necesitamos comprender y realizar análisis para tomar decisiones más racionales y lógicas.(Singh y Sharma 2020, p. 10)

- **Pruebas de seguridad humana**

La Seguridad Humana (HUMSEC) es una subsección de la Seguridad Física (PHYSSEC) e incorpora las Operaciones Psicológicas (PSYOPS). Probar este aspecto de la seguridad requiere comunicación con personas que tienen acceso físico a los activos protegidos, por ejemplo, un guardián.(Singh y Sharma 2020, p. 10)

- **Pruebas de seguridad física**

Se refiere a la seguridad del material dentro del dominio físico. Probar este canal demanda una interacción no comunicativa con barreras y humanos (guardianes) colocados dentro de los activos. (Singh y Sharma 2020, p. 11)

- **Pruebas de seguridad inalámbrica**

Spectrum Security (SPECSEC) es la clasificación de seguridad que contiene Electronics Security (ELSEC), Signals Security (SIGSEC) y Emanations Security (EMSEC). Probar este canal requiere que el analista esté cerca del objetivo. (Singh y Sharma 2020, p. 11)

- **Pruebas de seguridad de telecomunicaciones**

La seguridad de las telecomunicaciones es un subconjunto de ELSEC, que describe las telecomunicaciones de la organización a través de cables. Probar este canal cubre la interacción entre el analista y los objetivos. (Singh y Sharma 2020, p. 11)

- **Pruebas de seguridad de la red de datos**

Las pruebas relacionadas con el aspecto de seguridad de la seguridad de la red de datos (seguridad de las comunicaciones (COMSEC) requieren la interacción con las personas que tienen acceso a los datos operativos que se usan para controlar el acceso a la propiedad. (Singh y Sharma 2020, p. 11)

- **Normativas de cumplimiento**

Depende del lugar y del tipo de gobierno, industria y negocio vigente actualmente, y de la legislación de apoyo. En pocas palabras, el cumplimiento es un conjunto de políticas generales que están definidas por la legislación o la industria, y estas políticas son obligatorias. (Singh y Sharma 2020, p. 11)

- **Informes con el informe de auditoría de prueba de seguridad (STAR)**

El propósito de realizar un informe de auditoría para prueba de seguridad (STAR) es servir como resumen ejecutivo, indicando la superficie de ataque de los objetivos ensayados dentro de un alcance particular. (Singh y Sharma 2020, p. 12)

2.7.3 Issaf

En la metodología (ISSAF) también llamado marco de evaluación de seguridad de los sistemas de información, el profesional de penetración imita los pasos de hacking con algunas fases adicionales.

Las fases por las que pasa son las siguientes:

- "Recopilación de la información
- Mapeo de la red

- Identificación de las vulnerabilidades
- Penetración
- Obtención de acceso y escalada de privilegios
- Enumeración
- Comprometer a los usuarios/sitios remotos
- Mantenimiento del acceso
- Cubriendo las pistas”

“Su objetivo es evaluar la política y el proceso de seguridad de la información de una organización con respecto a su cumplimiento con los estándares de la industria de TI, junto con las leyes y los requisitos reglamentarios”.(Singh y Sharma 2020, p. 13)

2.7.4 Ptes

Es el estándar más usado porque cubre todo lo relacionado con una prueba de penetración.
Ptes se divide en siete secciones:

- **Compromiso previo**

Estas acciones deben llevarse a cabo antes de que comience una actividad, como definir el alcance de la actividad, que generalmente implica mapear las IP de la red, las aplicaciones web, las redes inalámbricas, etc.(Singh y Sharma 2020, p. 15)

- **Recopilación de la información**

Este es un proceso que se utiliza para recopilar la mayor cantidad de información posible sobre el objetivo. Esta es la parte más crítica del pentesting, ya que cuanta más información tengamos, más vectores de ataque podemos planificar para realizar la actividad. En caso de una actividad de caja blanca, toda esta información ya se proporciona al equipo de pruebas.(Singh y Sharma 2020, p. 15)

- **Modelado de amenazas**

El modelo de modelado de amenazas depende de la cantidad de información recopilada. Dependiendo de eso, la actividad se puede dividir y luego realizar utilizando herramientas automatizadas, ataques lógicos, etc(Sharma y Singh 2018, p. 8)

- **Análisis de vulnerabilidad**

Este es un proceso de descubrimiento de fallas que pueden ser utilizadas por un atacante. Estas fallas pueden ser cualquier cosa, desde puertos abiertos/configuración incorrecta del servicio hasta una inyección de SQL. Hay muchas herramientas disponibles que pueden ayudar a realizar un análisis de vulnerabilidad.(Sharma y Singh 2018, p. 9)

- **Explotación**

Este es un proceso de obtener acceso al sistema evadiendo el mecanismo de protección en el sistema basado en la evaluación de vulnerabilidad. Los exploits pueden ser públicos o de día cero.(Sharma y Singh 2018, p. 9)

- **Post-explotación**

Este es un proceso donde el objetivo es determinar la criticidad del compromiso y luego mantener el acceso para uso futuro. Esta fase debe seguir siempre las reglas del compromiso que es proteger al cliente y protegernos a nosotros mismos (cubrir las pistas según los requerimientos de la actividad).(Singh y Sharma 2020, p. 17)

- **Informe o Reporte**

Esta es una de las fases más importantes, ya que la reparación de todos los problemas depende totalmente de los detalles presentados en el informe(Singh y Sharma 2020, p. 17)

En el informe debe estar presente tres elementos esenciales:

1. La criticidad del error
2. Los pasos necesarios para reproducir el error
3. Sugerencias

CAPÍTULO III

3. MARCO METODOLÓGICO

Este capítulo muestra las configuraciones del servidor Linux, asimismo de las 3 máquinas virtuales que servirán como intrusos, la instalación correcta del honeypot Kippo y los ataques realizados por cada una de las máquinas virtuales como son: Kali Linux, Centos y Windows 7, aplicando metodologías de seguridad o estándares de testeo con sus respectivas herramientas en los accesos no autorizadas a ssh.

Para realizar este proyecto técnico, es necesario implementar una red virtual, para lo cual se utiliza una computadora con las siguientes características:

- Procesador Intel core i7 séptima generación
- Memoria RAM de 12 Gb
- Disco duro de 1 Tb
- CPU 2.70 Ghz
- Tarjeta de red de 100Mbps

Las máquinas virtualizadas utilizadas necesitan de los siguientes requerimientos (ver tabla 1-3):

Tabla 1-3: Requerimientos para configurar máquinas virtuales

SISTEMA OPERATIVO	DISCO DURO	MEMORIA RAM
Ubuntu 18.04.4	20 GB	2GB
Kali Linux 2017.1	20 GB	2GB
Centos 8.2	20 GB	2GB
Windows 7	60 GB	2GB

Realizado por: Erazo, J, 2022

Las máquinas virtuales se debe crear en un software de virtualización llamado vmware, este debe estar instalado y configurado correctamente, posteriormente se empieza a crear las 4 máquinas virtuales, una con sistema operativo ubuntu en el cual va a ser implementado el honeypot KIPPO y servirá como servidor ssh (ver anexo D), una máquina kali linux que realiza un ataque por fuerza bruta llamado ncrack (ver anexo E), una maquina con sistema operativo Centos cuyos ataques son realizados mediante los nombres y contraseñas que generalmente se utilizan en los servidores ssh (ver anexo F), y por último una máquina con Windows 7 que realiza ataques que simula ser originados por ingeniería social (ver anexo G).

3.1 Configuración del servidor Ssh Linux

Después de haber realizado la instalación del sistema operativo Ubuntu, procedemos con la configuración del servidor ssh, para lo cual es necesario instalar el paquete openssh-server; para ello ingresamos a un terminal y mediante una conexión a internet se descarga y posteriormente se instala el software, introducimos el siguiente comando:

sudo apt-get install openssh-server

Con este comando se instala un servidor ssh que se muestra en la ilustración 1-3.
Después es necesario reiniciar el servidor ssh con el siguiente comando:

sudo /etc/init.d/ssh restart

A continuación, se procede a configurar un servidor dhcp, el cual tiene como finalidad lograr una conexión de red virtual y casi real entre el servidor ssh y las máquinas virtuales existentes, para esto se le asigna en un rango de direcciones ip determinadas, se asignan parámetros como la puerta de enlace, la dirección ip, la máscara de subred, el broascast, las interfaces, etc

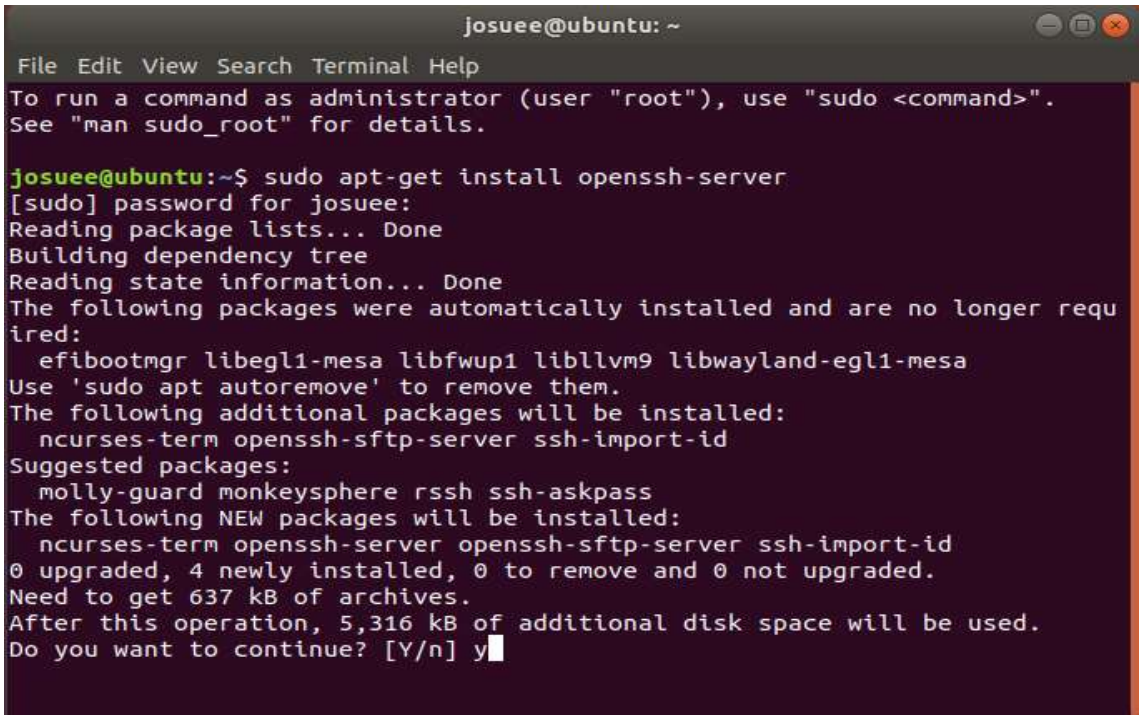


Ilustración 1-3: Instalación de openssh-server

Realizado por: Erazo, J, 2022

Primero se configura las interfaces de red con el comando:

sudo nano /etc/network/interfaces

Al ejecutar este comando se abrirá una ventana donde se tendrá que ingresar los datos como se muestra en la ilustración 2-3 y se guardarán dichos cambios.

luego, se configura el archivo dhcp.conf con el siguiente comando:

sudo nano /etc/dhcp/dhcpd.conf

se realiza las configuraciones necesarias tal y como lo está en la ilustración 3-3, todas estas direcciones ip y demás configuraciones depende del administrador que vaya a implementar, es decir ya queda a elección de cada administrador.

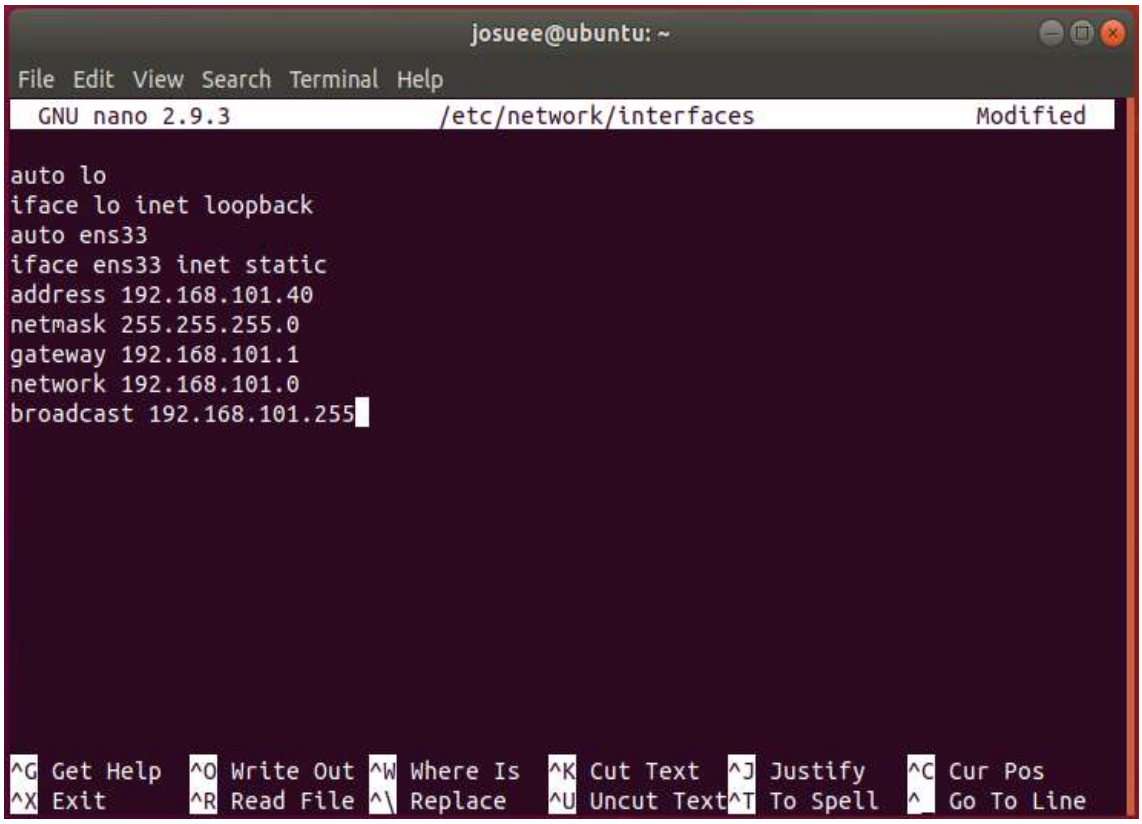


Ilustración 2-3: Configuración de las interfaces

Realizado por: Erazo, J, 2022

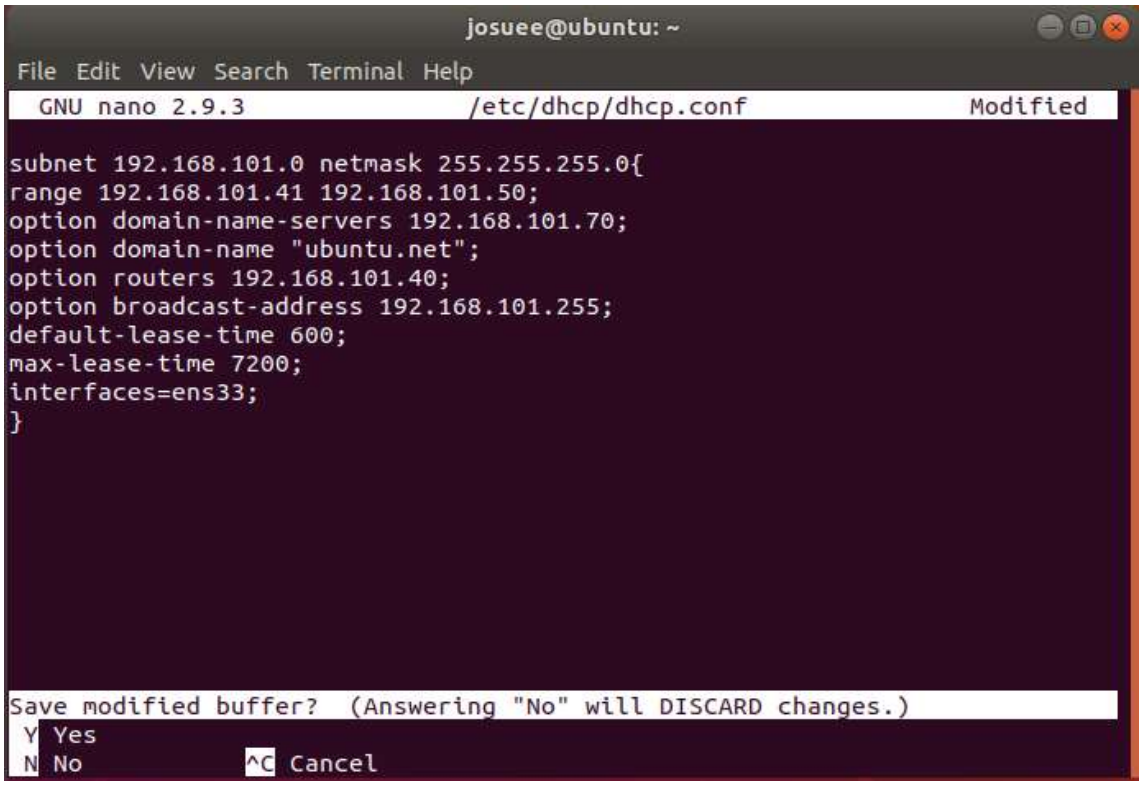


Ilustración 3-3: Configuración del servidor DHCP

Realizado por: Erazo, J, 2022

Una vez realizado estos pasos es necesario guardar y reiniciar las configuraciones para que estos tengan efecto, para esto ingresamos los siguientes comandos:

```
sudo /etc/init.d/networking restart
```

Luego es necesario actualizar el software para poder seguir con la instalación del dhcp-server, para lo cual se ejecutan los siguientes comandos como se visualiza en la ilustración 4-3:

```
sudo apt update
sudo apt -y install isc-dhcp-server
```

Por último, es necesario ejecutar algunos comandos extras para que las interfaces de red se configuren correctamente como se visualiza en la ilustración 5-3:

```
sudo invoke-rc.d networking stop
sudo invoke-rc.d networking start
```

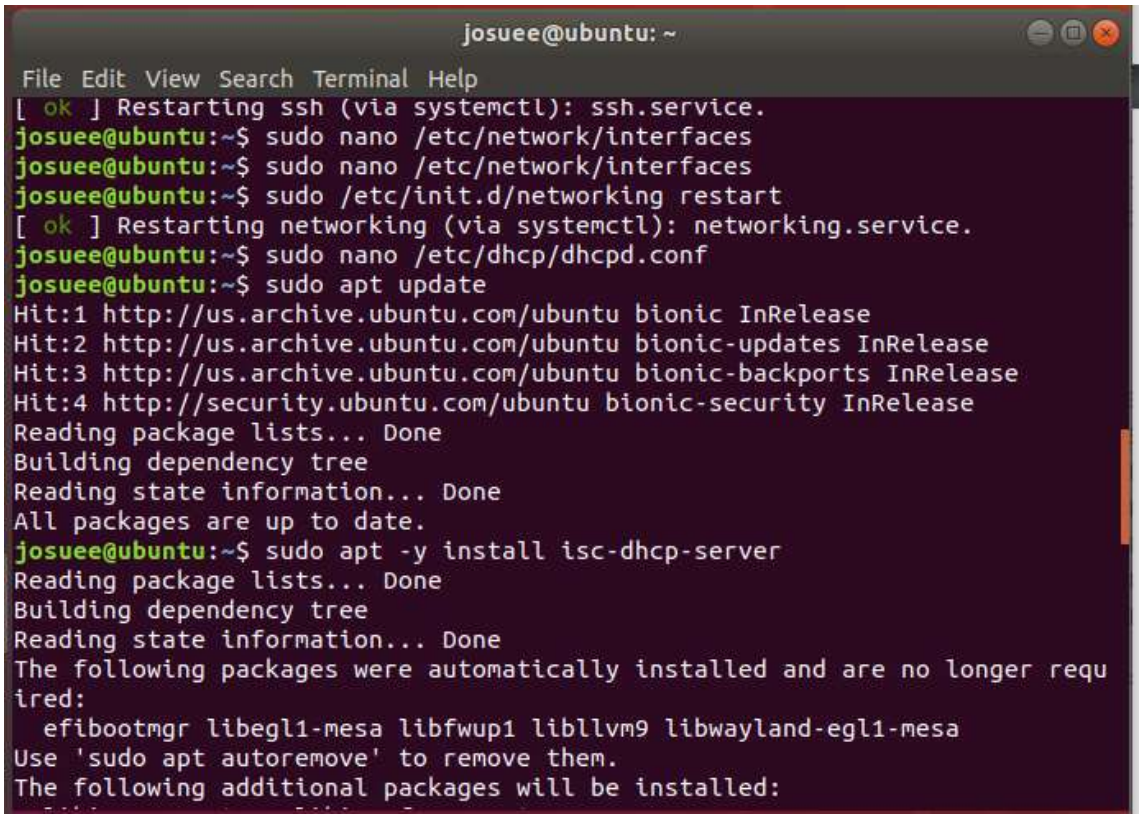


Ilustración 4-3: Configuraciones para reiniciar las interfaces de red e instalar servidor dhcp

Realizado por: Erazo, J, 2022

Una vez completada todas las configuraciones anteriores, se inicia el servidor dhcp con el comando:

sudo /etc/init.d/isc-dhcp-server start

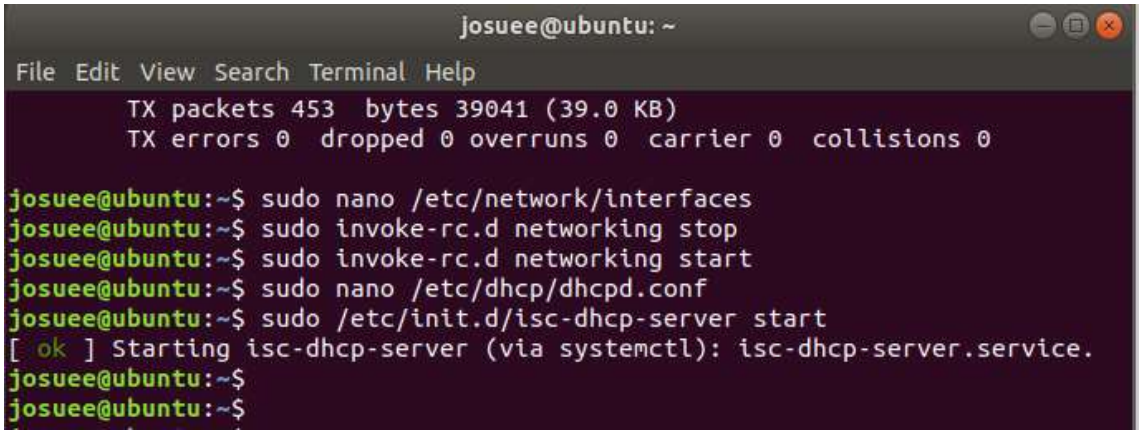


Ilustración 5-3: Comandos extras para el correcto funcionamiento de las interfaces

Realizado por: Erazo, J, 2022

Con esto se tiene listo y preparado nuestro servidor ssh, logrando conectividad entre todas las máquinas virtuales y permitiendo a los intrusos acceder a este servicio.
Tener en cuenta que para descargar las actualizaciones o algunos comandos que no vienen instalados, se debe tener una conexión a internet, sin esto no se puede hacer nada.

3.2 Configuración de las máquinas atacantes al servidor

3.2.1 Configuración de Máquina Virtual Kali Linux

Una vez instalado (ver anexo E), se empieza a verificar que exista conectividad con el servidor Ubuntu, para ello se realiza ping como se muestra en la ilustración 6-3 y se comprueba la dirección ip con el comando: nmcli

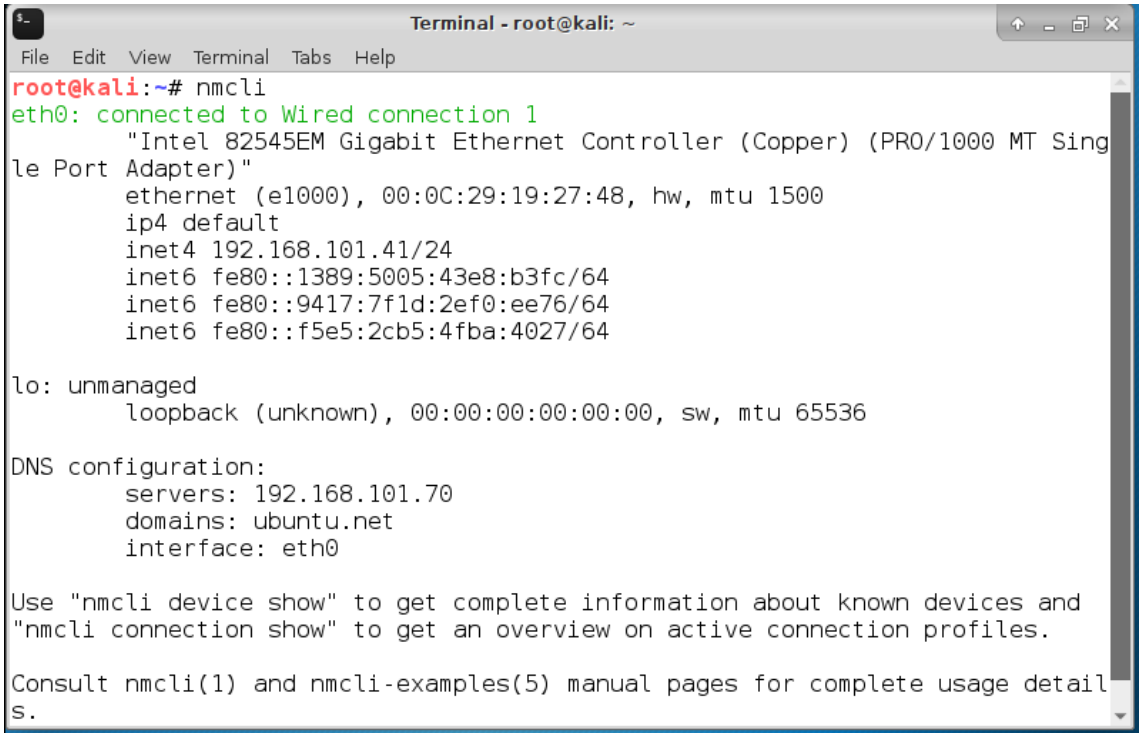


Ilustración 6-3: Comprobación dirección ip de la máquina virtual Kali Linux

Realizado por: Erazo, J, 2022

No se necesita configurar ningún cliente ssh, ya que por defecto viene instalado, se ingresa el nombre de usuario y la dirección del servidor:

ssh josuee@192.168.101.40 (nombre_usuario@direcion_servidor)

se ingresa la contraseña y de esta manera se provee una conexión al servidor ssh, el cual se encuentra configurado correctamente tal como se muestra en la ilustración 7-3.

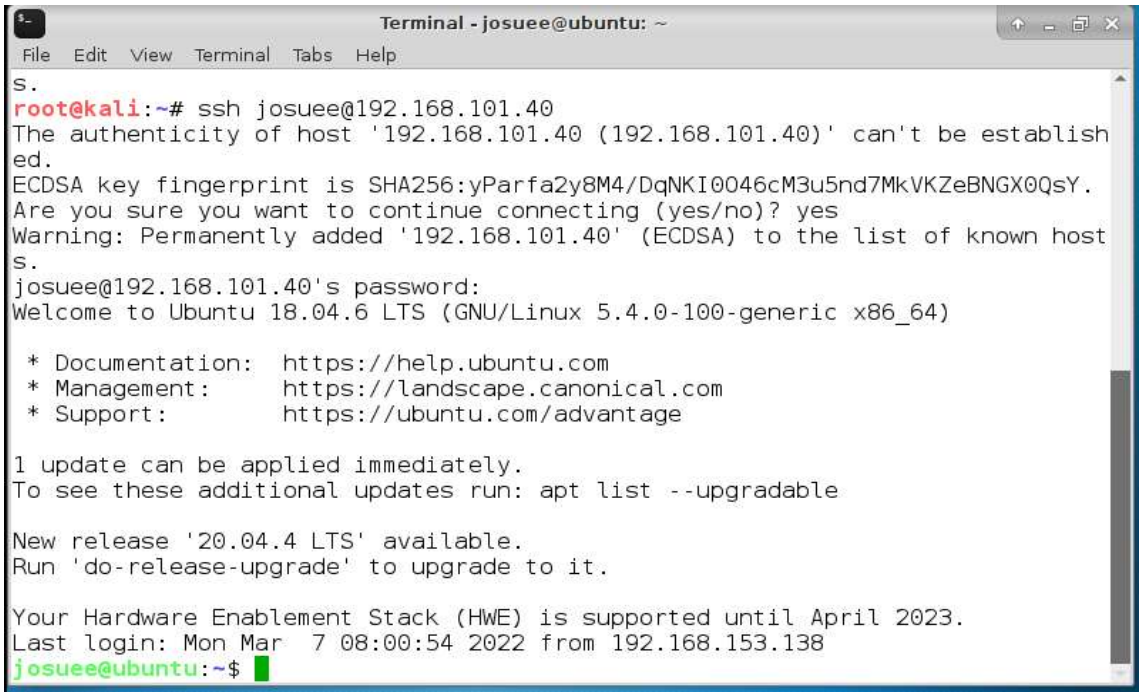


Ilustración 7-3: Verificación conexión con el servidor ssh en Kali Linux

Realizado por: Erazo, J, 2022

3.2.2 Configuración de la Máquina Virtual Centos

Una vez instalado (ver anexo F), se empieza a verificar que exista conectividad con el servidor Ubuntu, para ello se realiza ping y se comprueba la dirección ip con el comando: ifconfig
Tal como se muestra en la ilustración 8-3.

No se necesita configurar ningún cliente ssh, ya que por defecto viene instalado, se ingresa el nombre de usuario y la dirección del servidor:

ssh josuee@192.168.101.40 (nombre_usuario@direcion_servidor)

se ingresa la contraseña y de esta manera se provee una conexión al servidor ssh, el cual se encuentra configurado correctamente.

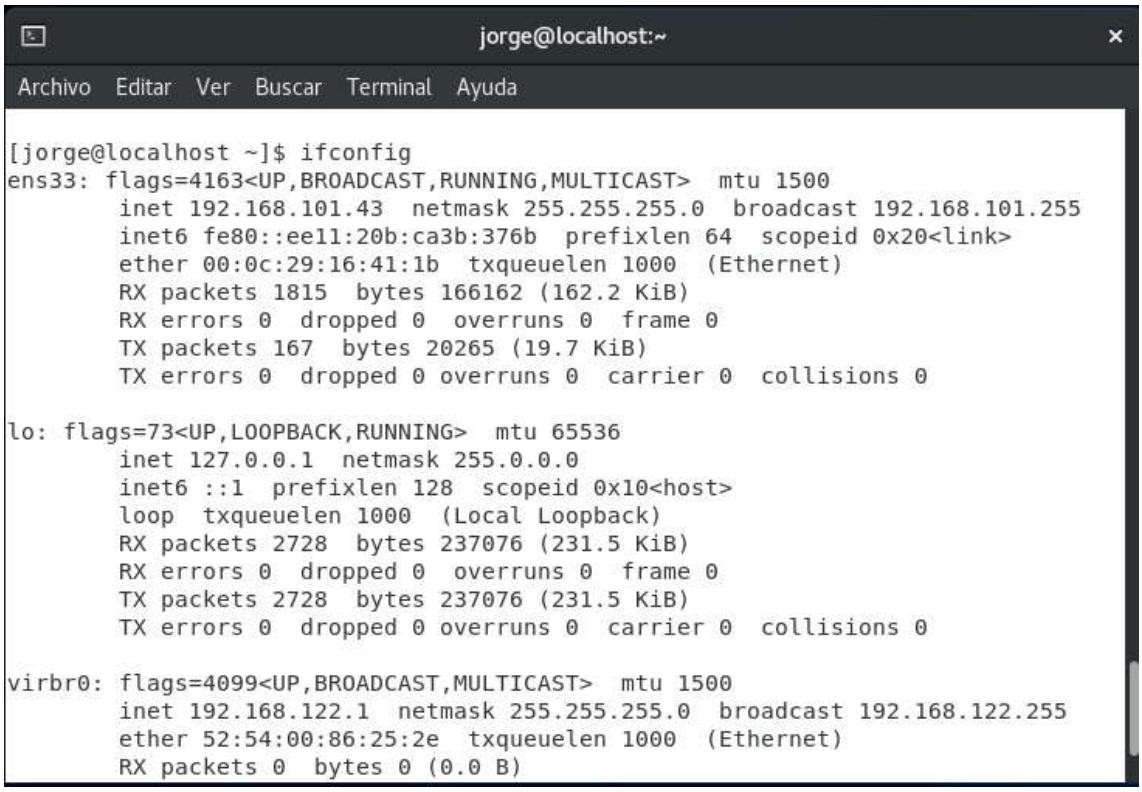


Ilustración 8-3: Comprobación dirección ip de la máquina virtual centos

Realizado por: Erazo, J, 2022

3.2.3 Configuración de la Máquina Virtual Windows 7

Una vez instalado (ver anexo G), se empieza a verificar que exista conectividad con el servidor Ubuntu, para ello se realiza ping y se comprueba la dirección ip.

Para esta máquina virtual es necesario utilizar un programa de cliente ssh llamado Putty que permite acceder al sistema Linux en modo texto desde sistemas operativos Windows. Se configura la dirección ip del servidor al cual va a ser conectado y su puerto, en este caso es el 22 para ssh, tal como se muestra en la ilustración 9-3.

Dando clic en open se abre un editor de comandos donde se va a ingresar el usuario y contraseña como muestra la ilustración 10-3.

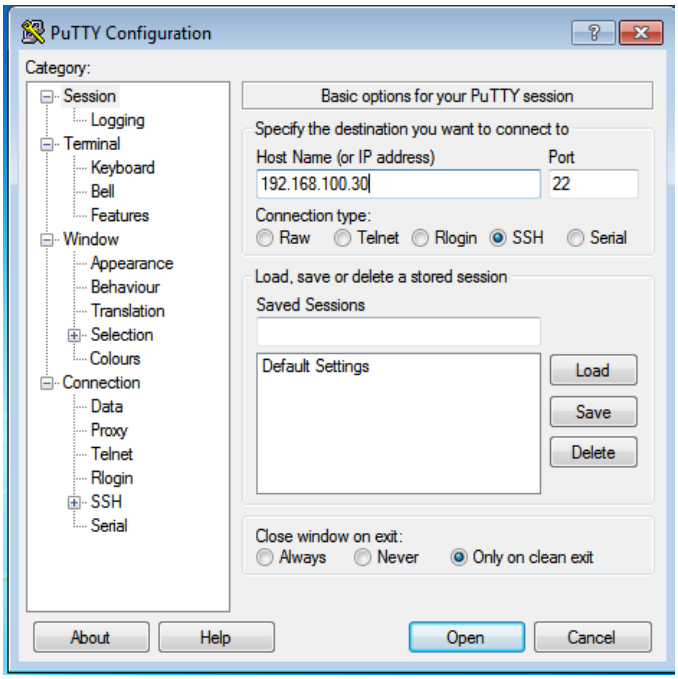


Ilustración 9-3: Configuración para la conexión al servidor ssh mediante putty

Realizado por: Erazo, J, 2022

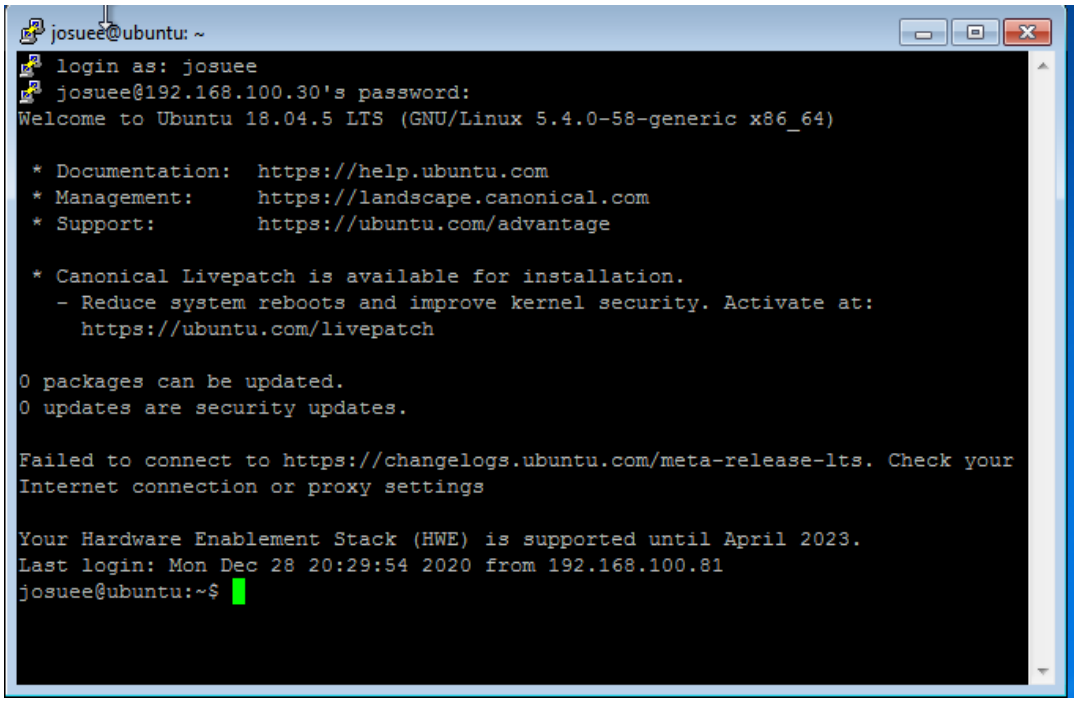


Ilustración 10-3: Conexión ssh desde Windows 7

Realizado por: Erazo, J, 2022

3.3 Implementación de honeypot Kippo

“Kippo requiere varios paquetes de python para ejecutarse. La mejor manera de instalarlos es el uso de pip, para lo cual es necesario instalar paquetes del sistema operativo, en este caso debian, para ello ejecutamos el siguiente comando:” (Github, 2022b).

sudo apt-get install build-essential -python-dev libmysqlclient-dev python-virtualenv python-pip

tal como muestra la ilustración 11-3.

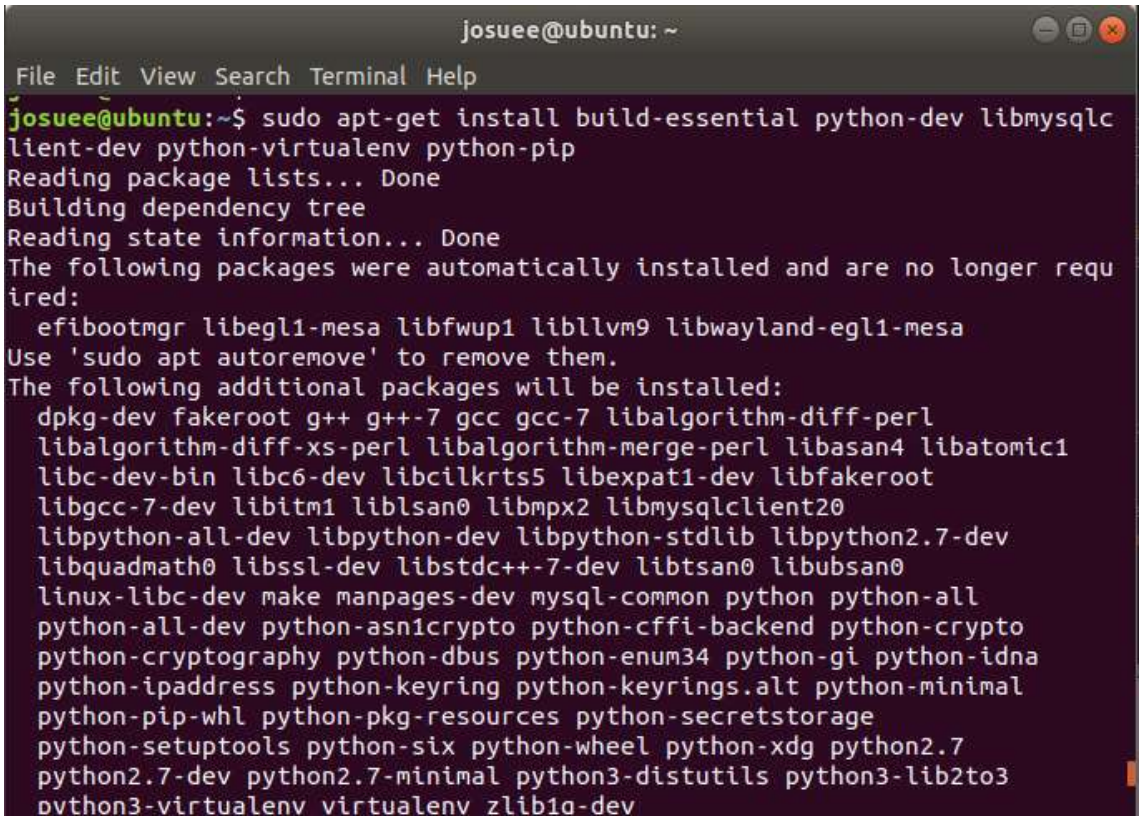


Ilustración 11-3: Instalación de paquetes necesarios para la ejecución de Kippo

Realizado por: Erazo, J, 2022

después, se debe crear un entorno virtual (ver ilustración 12-3) el cual crea entornos Python aislados con el comando:

virtualenv env

luego se debe activar el entorno virtual con el comando:

. ./env/bin/actívate

A continuación, se instala los paquetes Python necesarios (ver figura 13-3) ejecutando los comandos:(Github, 2022b)

pip install twisted==15.1.0

pip install pyasn1

pip install pycrypto

Adicional, se pueden agregar paquetes para características específicas (ver figura 14-3) como:

pip install MySQL-python

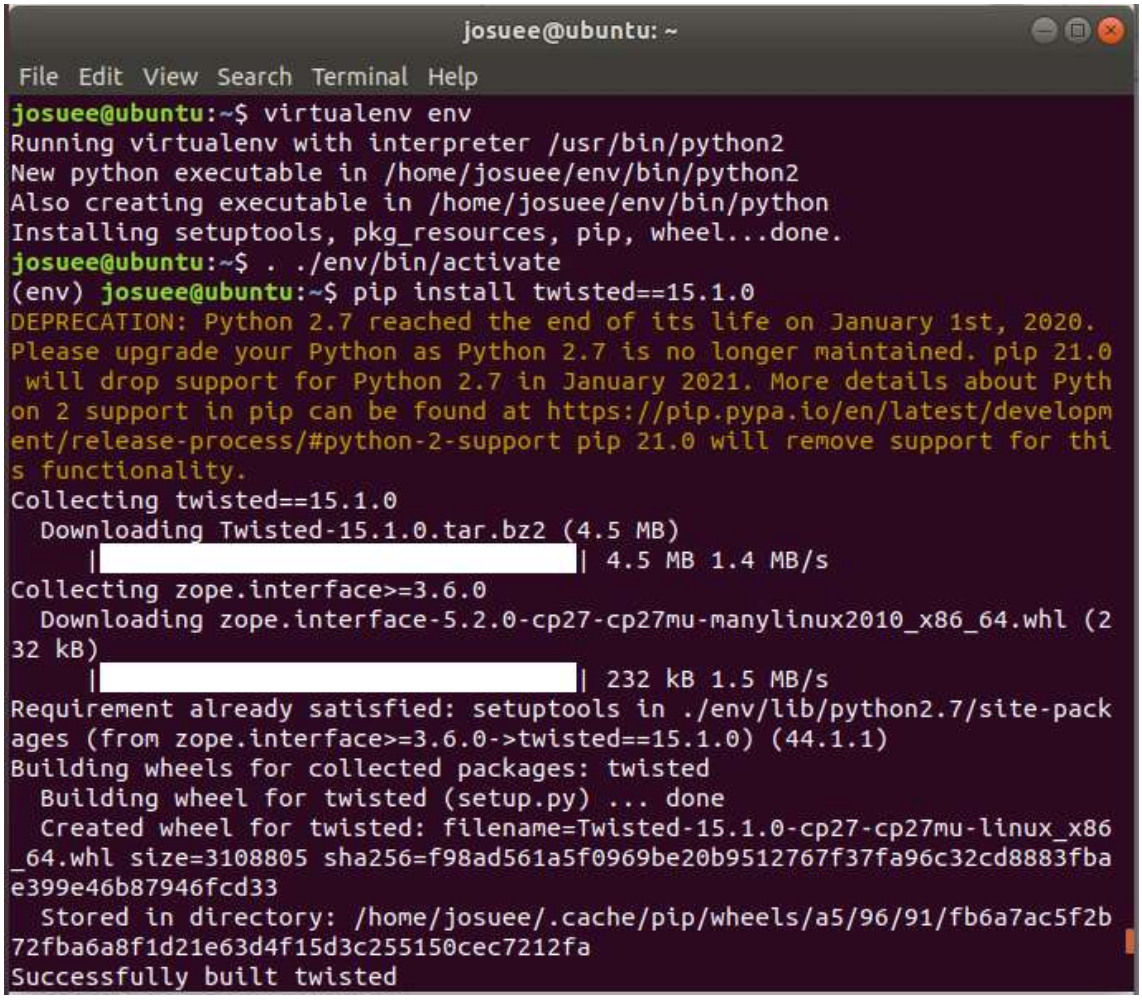


Ilustración 12-3: Configuración del entorno virtual

Realizado por: Erazo, J, 2022

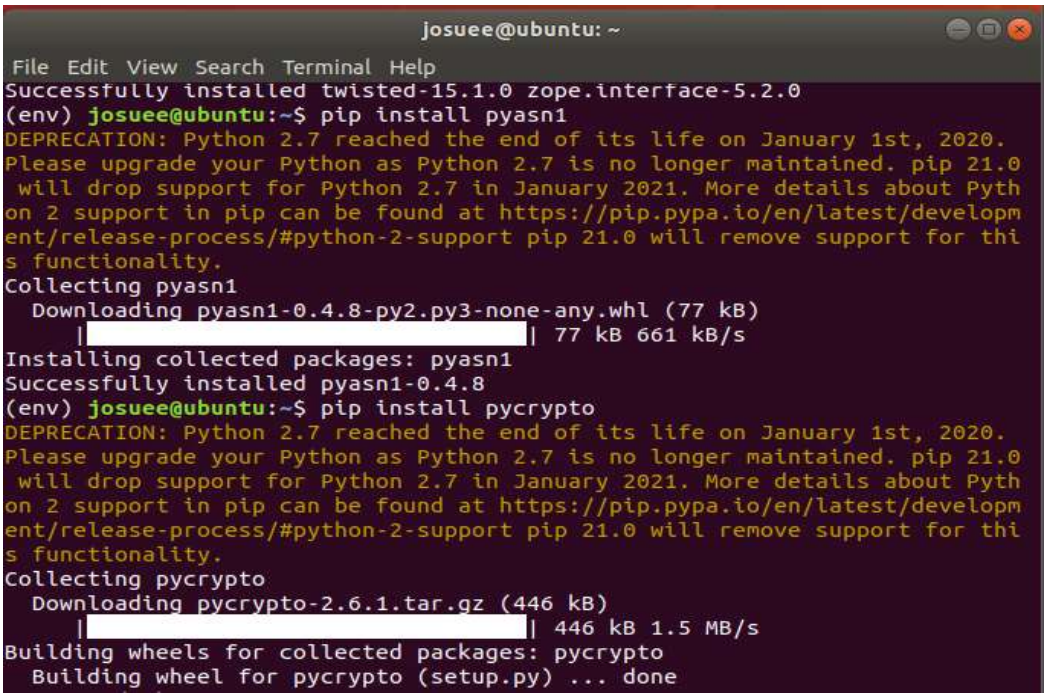


Ilustración 13-3: Instalación de paquetes Python necesarios

Realizado por: Erazo, J, 2022

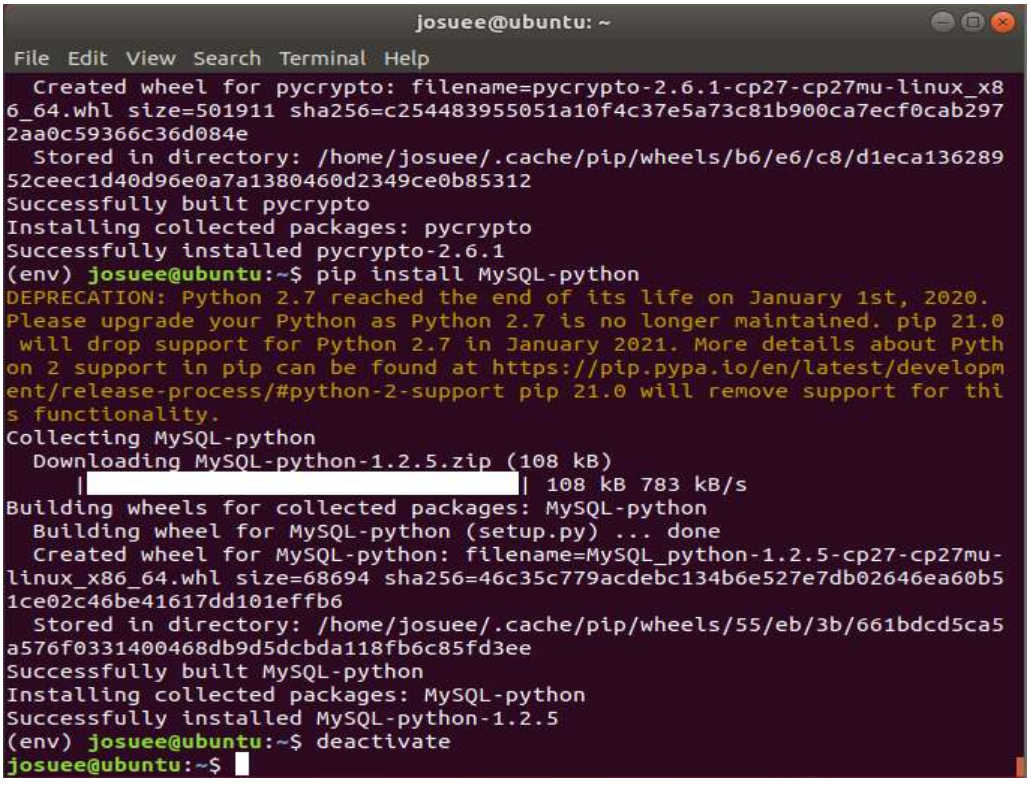


Ilustración 14-3: Instalación de MySQL-python

Realizado por: Erazo, J, 2022

luego es recomendable desactivar el entorno virtual con el comando:

deactivate

después de las configuraciones y paquetes instalados anteriormente, se procede con la instalación de Kippo, para lo cual ejecutamos los siguientes comandos (ver ilustración 15-3):

sudo apt install git
git clone https://github.com/desaster/kippo.git

con estos comandos clonamos el código de Kippo desde un repositorio(Github, 2022b), tal y como se muestra en la ilustración 16-3.

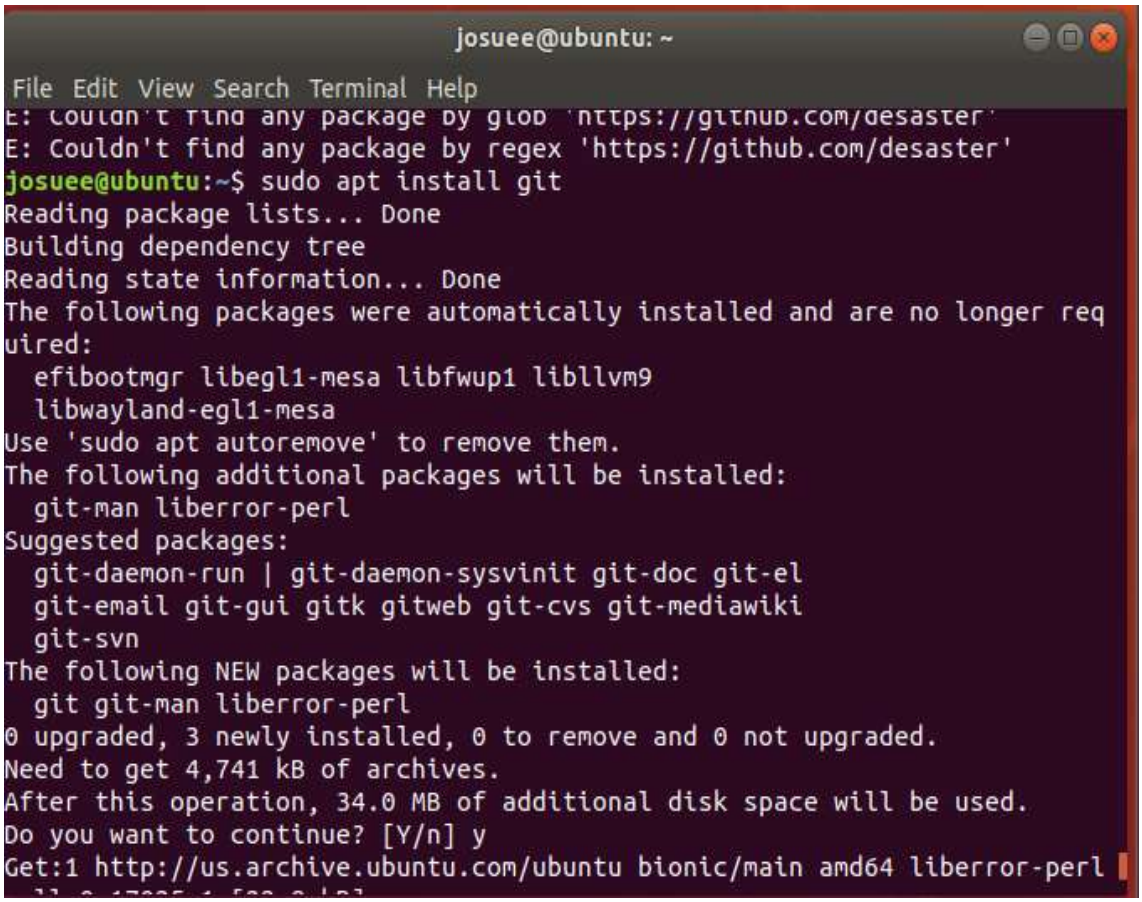


Ilustración 15-3: Instalación del comando git para la clonación de Kippo

Realizado por: Erazo, J, 2022

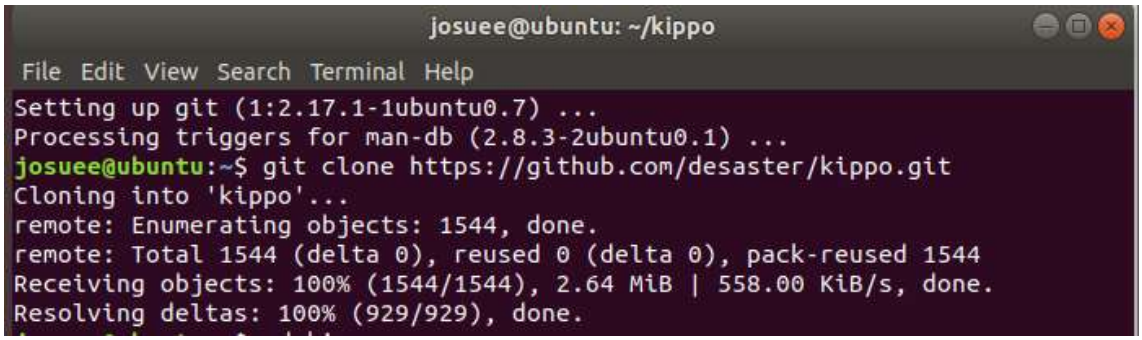


Ilustración 16-3: Clonación e instalación de Kippo

Realizado por: Erazo, J, 2022

Esta clonación sirve para obtener todo el código de Kippo con el cual se tiene acceso a toda la configuración, los comandos para utilizar en la emulación, los registros, directorios, carpetas que sirven para engañar a los intrusos, una vez clonado el código de Kippo en la máquina virtual Ubuntu, se debe realizar algunas configuraciones adicionales para que funcione correctamente Kippo (ver ilustración 17-3), estos comandos son los siguientes:

cd kippo
sudo mv kippo.cfg.dist kippo.cfg
sudo chmod -R 777 /home

Ilustración 17-3: Configuración de comandos adicionales para correcto funcionamiento de Kippo

Realizado por: Erazo, J, 2022

Por defecto, Kippo escucha las conexiones ssh en el puerto 2222, cuando se utiliza windows 7 no existe ningún problema porque el puerto 22 está libre, pero en Linux se encuentra restringido para usar como root, por lo cual se puede cambiar mediante un reenvío de puertos tal como se muestra en la ilustración 18-3 con el comando:

sudo iptables -t nat -A PREROUTING -p tcp --dport 22 -j REDIRECT --to-port 2222

por último, se guarda esa configuración con el comando (Github, 2022a)

sudo iptables-save

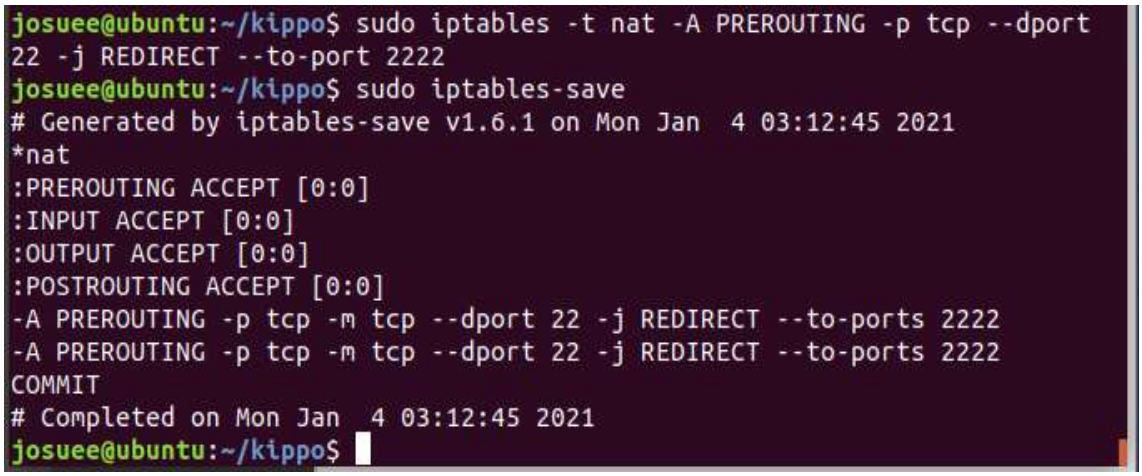


Ilustración 18-3: Ejecución de reenvío de puertos para que el puerto 22 sea accesible

Realizado por: Erazo, J, 2022

Con esto ya se puede iniciar Kippo correctamente, es necesario que cuando queramos iniciar Kippo, se lo haga desde el entorno virtual creado anteriormente, para lo cual ejecutamos los siguientes comandos (ver ilustración 19-3):

. ./env/bin/activate
cd kippo
./start.sh

Para la realización de pruebas de funcionamiento se debe conectar desde un terminal de la máquina virtual Ubuntu hacia el servidor Kippo en el puerto 2222, el cual tiene como nombre de usuario root, y la contraseña 123456. Para ello se aplica el siguiente comando:

ssh 127.0.0.1 -p 2222 -l root

y se puede observar la conexión hacia un supuesto servidor ssh tal como lo muestra la ilustracion 20-3.

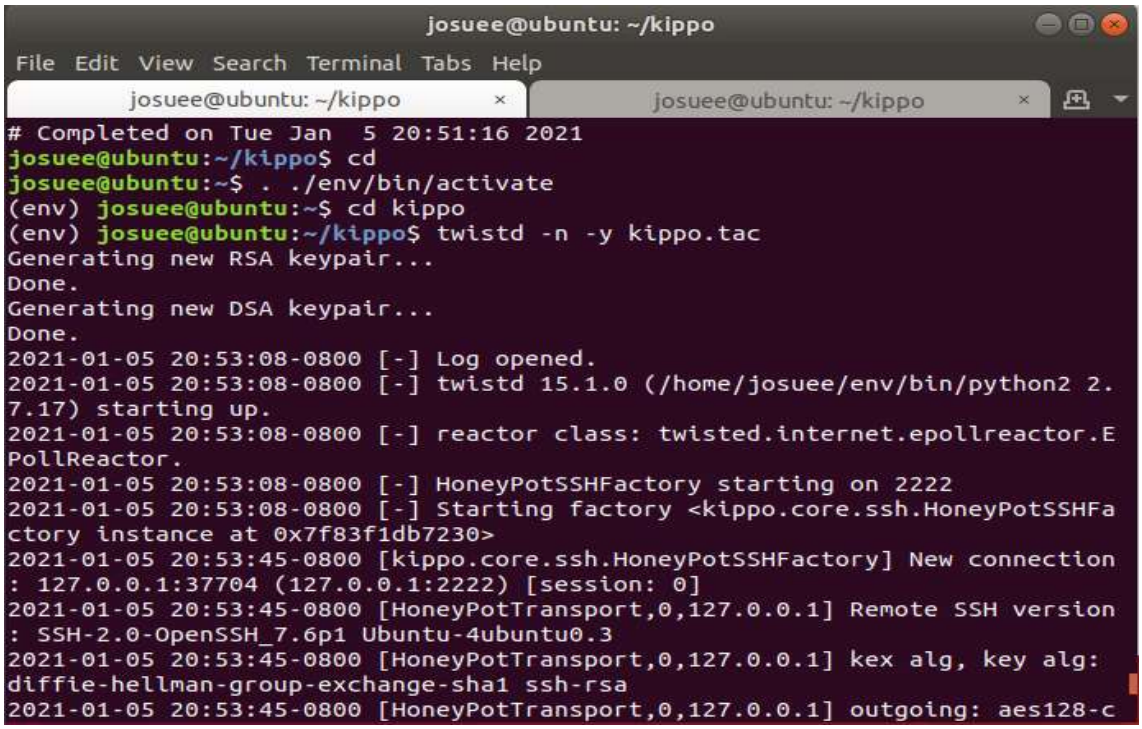


Ilustración 19-3: Inicialización de Kippo en primer plano

Realizado por: Erazo, J, 2022

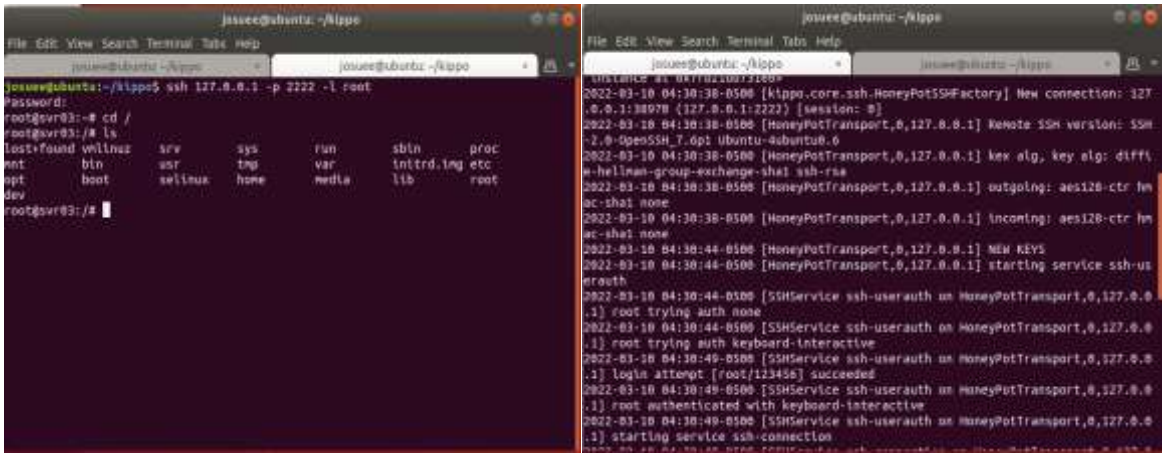


Ilustración 20-3: Conexión al servidor ssh que ofrece el honeypot Kippo

Realizado por: Erazo, J, 2022

Como se observa en la ilustración 20-3 en la parte derecha, también se puede proporcionar opciones de inicio detalladas ejecutando twistd manualmente. Por ejemplo, para ejecutar Kippo en primer plano se utiliza el siguiente comando:

twistd -y kippo.tac -n

3.4 Metodología de seguridad usada

La metodología de seguridad usada en este proyecto va a ser el estándar de ejecución de pruebas de penetración, ya que es el más utilizado y cubre casi todo lo relacionado con las pruebas de penetración. Para esto se debe seguir diferentes fases, los cuales garantizan que todos los detalles sobre el trabajo y el objetivo se recopilen de manera eficiente y que el profesional de penetración tenga una comprensión clara de la tarea.

Además, se tomará en cuenta mucho las etapas de las pruebas de penetración con sus respectivas herramientas de testeo como se observa en la ilustración 21-3.

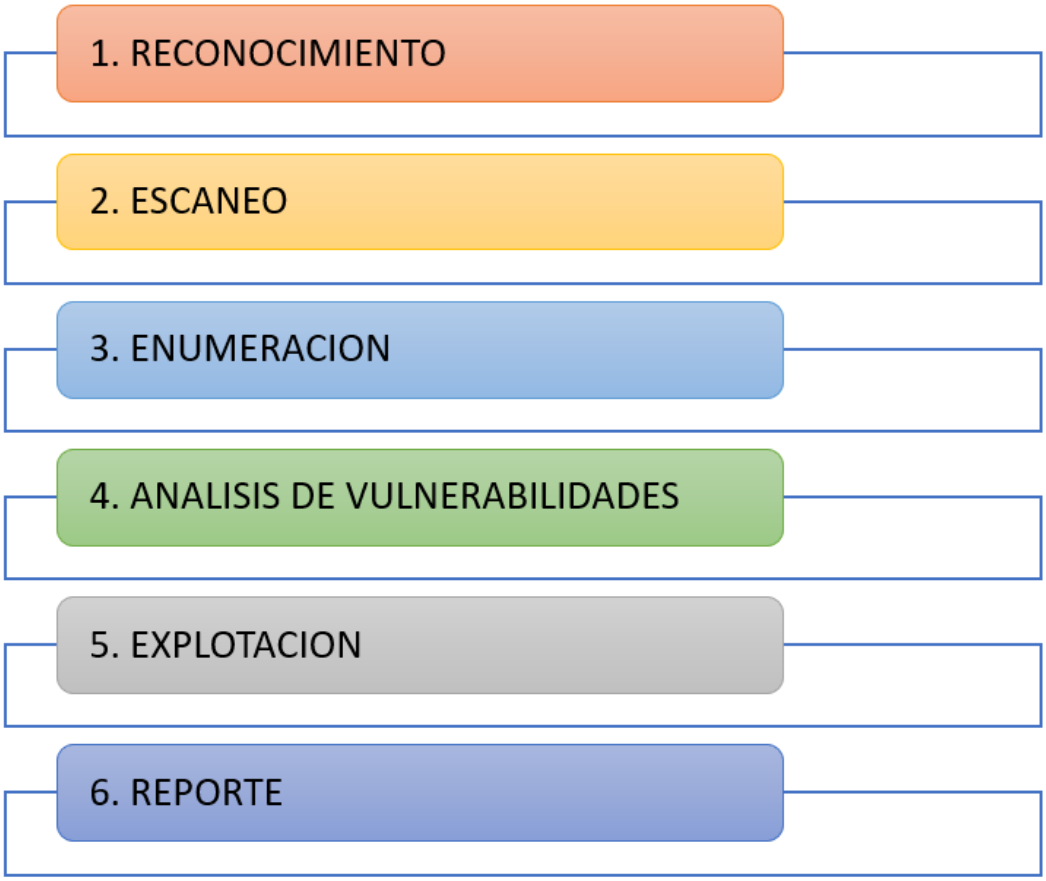


Ilustración 21-3: Etapas de las pruebas de penetración

Realizado por: Erazo, J, 2022

Esta metodología va a ser aplicada en la prueba de ataques de fuerza bruta mediante Kali Linux que se encuentra a continuación;

3.5 Pruebas de ataques

3.5.1 Ataque fuerza bruta mediante máquina virtual Kali Linux

Kali Linux ha sido elegido para realizar el ataque de fuerza bruta ya que es una distribución Linux muy completa y contiene una variedad de herramientas de testeo, este ataque se lo realiza mediante una herramienta de fuerza bruta llamado ncrack que utiliza diccionarios para combinar cada uno de los usuarios con cada una de las contraseñas y de esta manera obteniendo al final las correctas.

- **Compromiso previo**

La prueba de penetración se inicia con la fase del compromiso previo que incluye a la etapa de reconocimiento, aquí se busca y recopila la mayor cantidad de información acerca del servidor ssh que va a ser vulnerado y por consiguiente atacado, se debe conocer el puerto en el que trabaja estos tipos de servidores, es decir el puerto 22, las llaves ssh y el proceso del servidor o también llamado openssh.

- **Recopilación de la información**

En la fase de recopilación de la información que incluye la etapa de escaneo, se realiza un escaneo de red sobre el objetivo en base a la información obtenida en la etapa de reconocimiento, es decir se busca los sistemas operativos, puertos y servicios que están activos.

Para ello se va a utilizar la herramienta Nmap que viene incluido en Kali Linux, el cual se realiza un escaneo a la dirección ip del servidor a cuál va a ser atacado mediante el comando:

```
Nmap -sV -p- -T5 192.168.101.40
```

Este comando realiza un escaneo de los puertos, servicios y versiones de la dirección ip donde se encuentra el servidor ssh tal como se muestra en la ilustración 22-3.

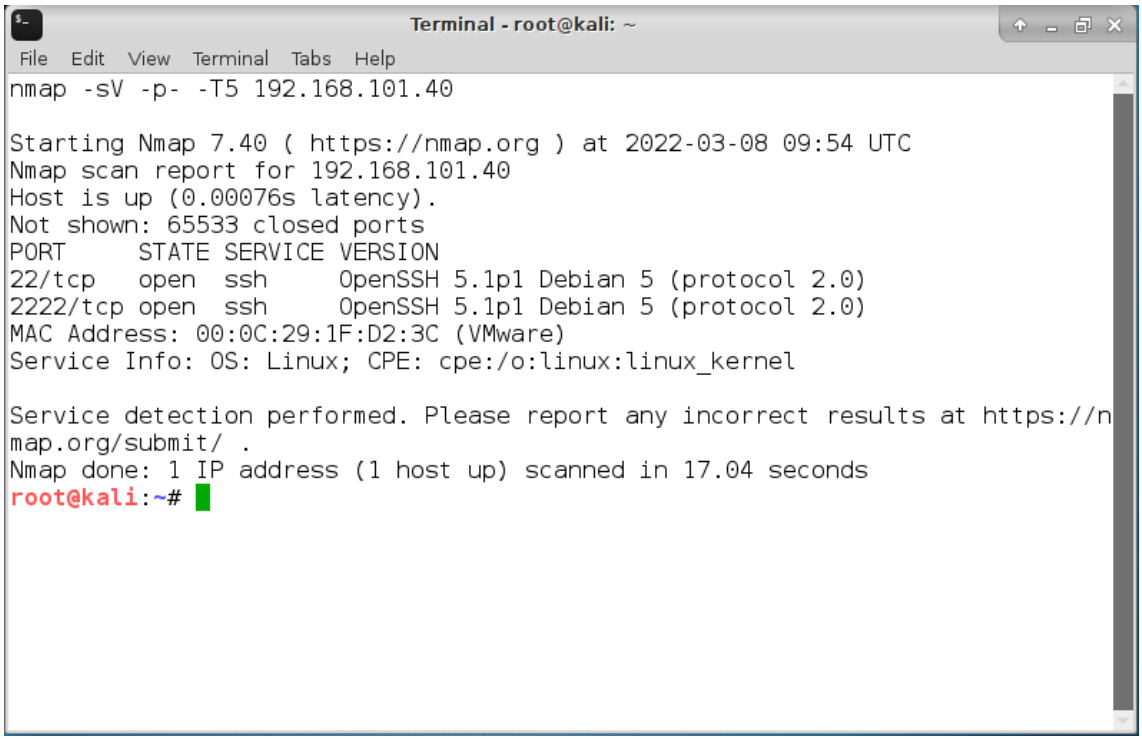


Ilustración 22-3: Escaneo de puertos, servicios y versiones del servidor ssh

Realizado por: Erazo, J, 2022

- **Modelado de amenazas**

En la fase de modelado de amenazas donde se incluye la etapa de enumeración, se obtiene la información detallada (ver figura 23-3) del objetivo que se encuentra bajo ataque interactuando profundamente con los puntos de entrada que ofrece. Esta etapa ayudará al intruso a identificar los vectores de ataque los cuales son métodos para que el atacante tenga acceso al sistema, en este caso el método encontrado para atacar al servidor es mediante el protocolo ssh.

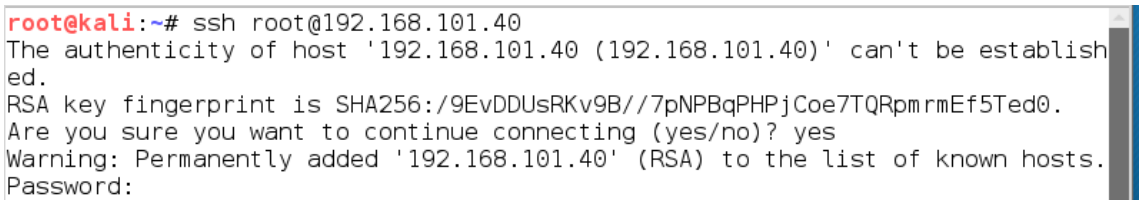


Ilustración 23-3: Información del protocolo ssh con conexión exitosa.

Realizado por: Erazo, J, 2022

- **Análisis de vulnerabilidades**

En la fase de análisis de vulnerabilidades se identifican y categorizan las vulnerabilidades asociadas al objetivo que está siendo atacado, utilizando como base toda la información recopilada en los anteriores pasos. Este es un proceso para descubrir fallas y sean utilizadas por el atacante, en este caso encontramos la vulnerabilidad de ataque por fuerza bruta, que permite realizar la penetración a este servidor ssh tal como se muestra en la ilustración 24-3.

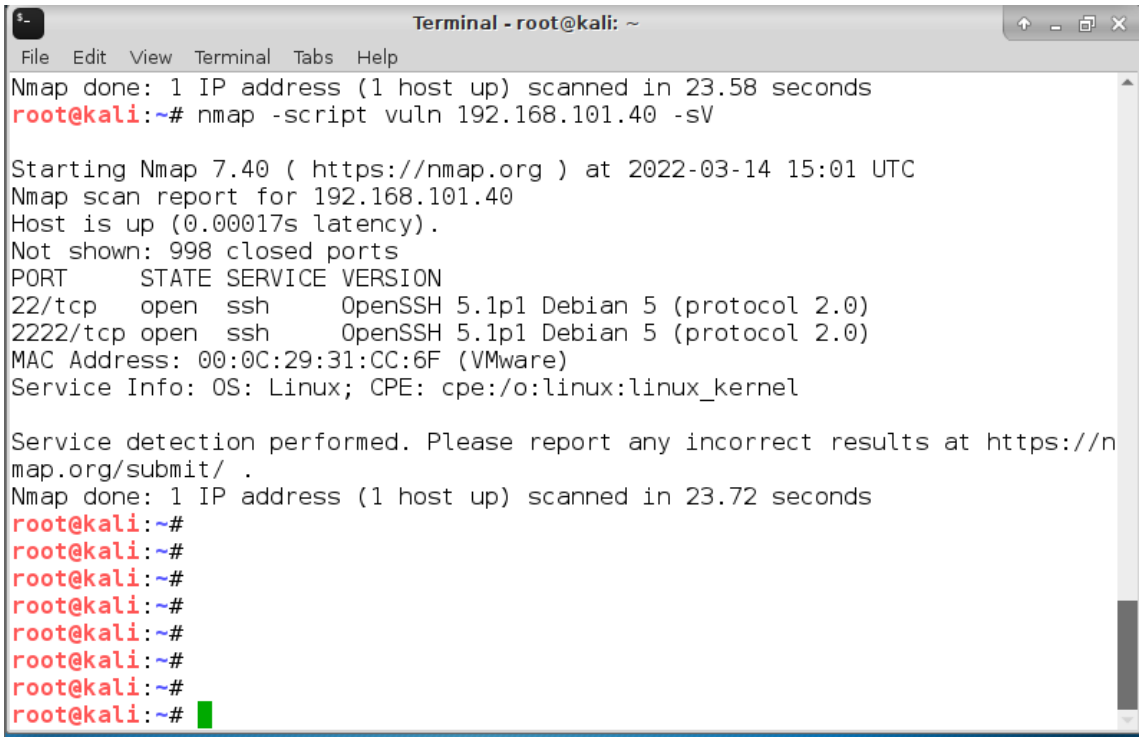


Ilustración 24-3: Análisis de vulnerabilidad del servidor ssh

Realizado por: Erazo, J, 2022

- **Explotación**

En la fase de explotación se obtiene acceso al sistema evadiendo así los mecanismos de protección basados en la evaluación de las vulnerabilidades, para esto se ejecuta el ataque de fuerza bruta mediante diccionario.

Para realizar esta fase, primero se debe crear un diccionario en Kali Linux con los comandos que se muestran en la ilustración 25-3.

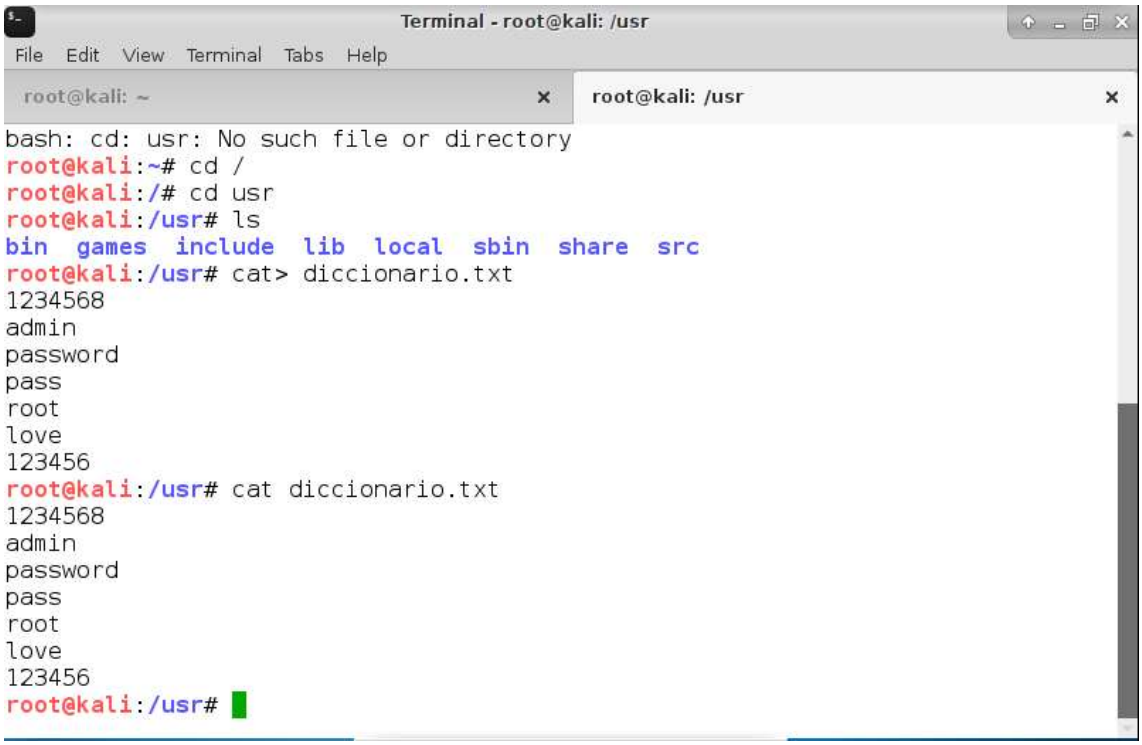


Ilustración 25-3: Creación del diccionario para realizar el ataque por fuerza bruta

Realizado por: Erazo, J, 2022

Una vez creado el diccionario se empieza con la ejecución del ataque mediante la fuerza bruta para obtener el nombre de usuario y contraseña del servidor ssh, para eso aplicamos el comando tal como se muestra en la ilustración 26-3:

Ncrack -p22 -U ´/usr/diccionario.txt´ -P ´usr/diccionario.txt´ 192.168.101.40 -f -v

Este comando indica la ejecución del ataque de fuerza bruta en el puerto 22, buscando el nombre de usuario y la contraseña en el archivo diccionario, la dirección ip donde se encuentra el servidor ssh, además que se detenga cuando encuentre la combinación correcta y que muestre el resultado de la operación.

Después de realizar este código y terminar el ataque de fuerza bruta, se obtiene como resultado el usuario y la contraseña del servidor ssh.

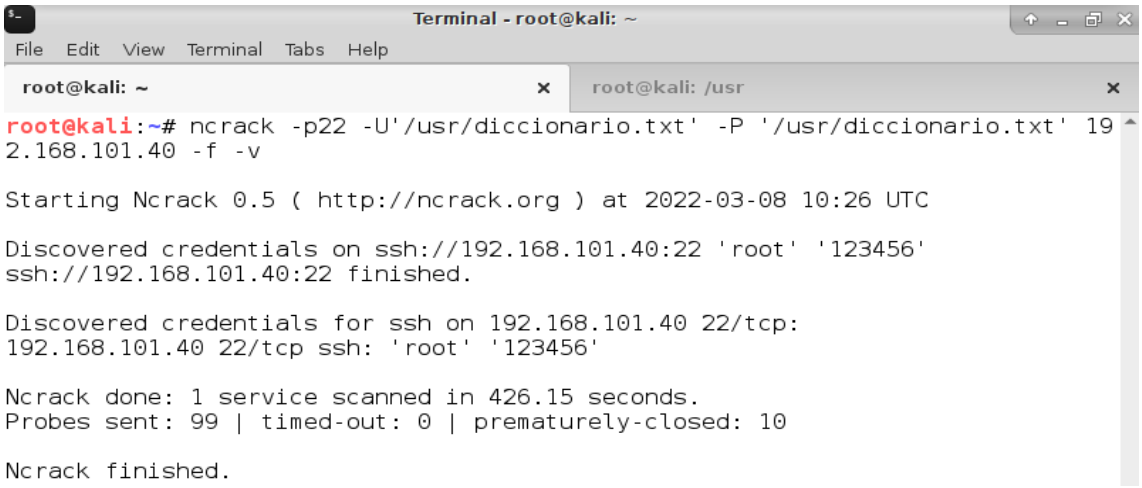


Ilustración 26-3: Ejecución del ataque de fuerza bruta mediante la herramienta ncrack

Realizado por: Erazo, J, 2022

- **Post Explotación**

En la fase de post explotación se aprovecha para acceder a los datos o propagarse a otros sistemas dentro de la red. el objetivo principal suele ser demostrar el impacto que la vulnerabilidad y el acceso obtenido pueden tener para la organización.

En este caso se ingresa al servidor ssh mediante el usuario y contraseña encontrados anteriormente mediante el ataque de fuerza bruta tal como se muestra en la ilustración 27-3.

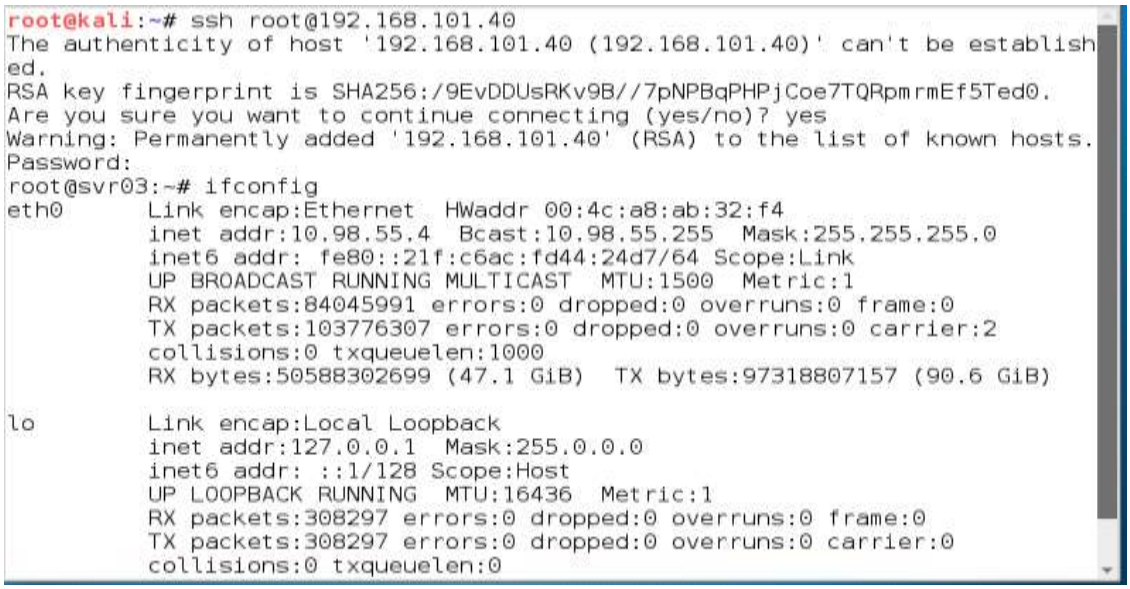


Ilustración 27-3: Conexión al servidor ssh mediante el usuario y contraseña encontrada

Realizado por: Erazo, J, 2022

Una vez ya estando adentro del sistema se puede comenzar a espiar la información que tiene, como mirar los archivos y carpetas como muestra la ilustración 28-3.

También se puede crear carpetas, borrar, copiar archivos en otros directorios como muestra la ilustración 29-3 y agregar usuarios al sistema como se muestra en la ilustración 30-3.

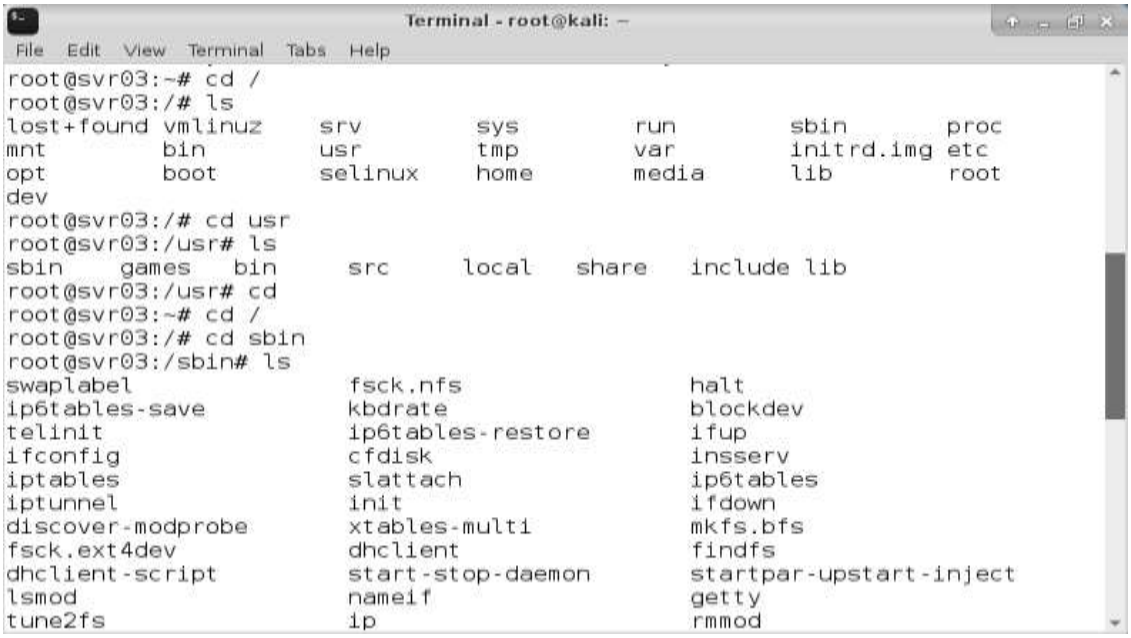


Ilustración 28-3: Exploración interna de los directorios del servidor ssh desde Kali Linux

Realizado por: Erazo, J, 2022

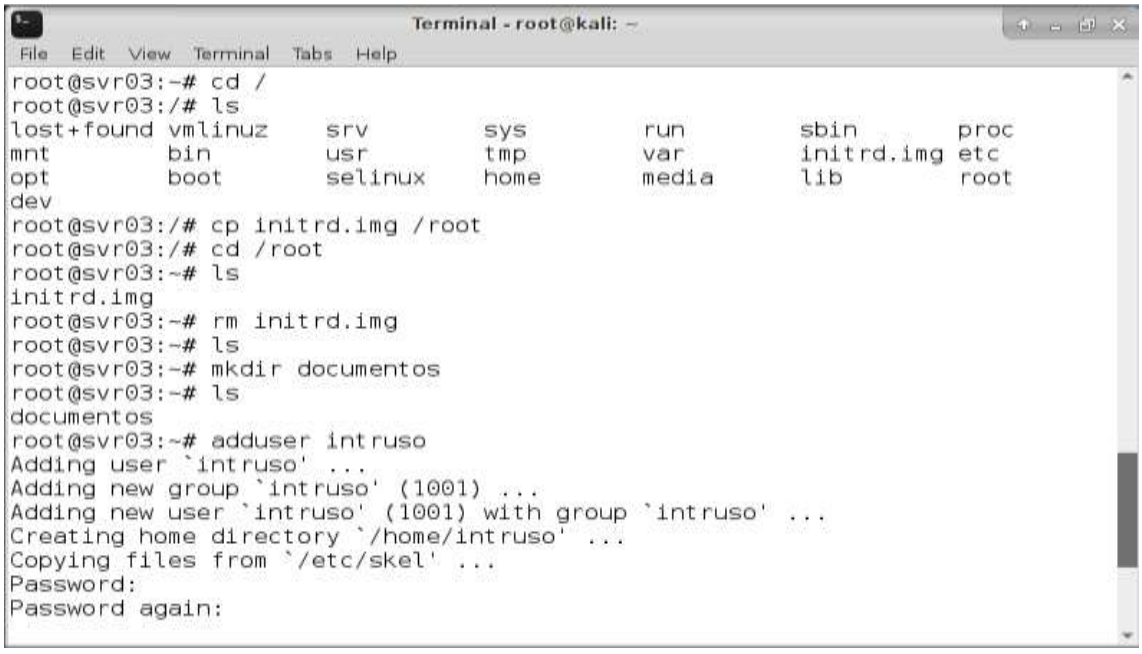


Ilustración 29-3: Comandos para copiar y borrar archivos o agregar usuarios al servidor ssh

Realizado por: Erazo, J, 2022

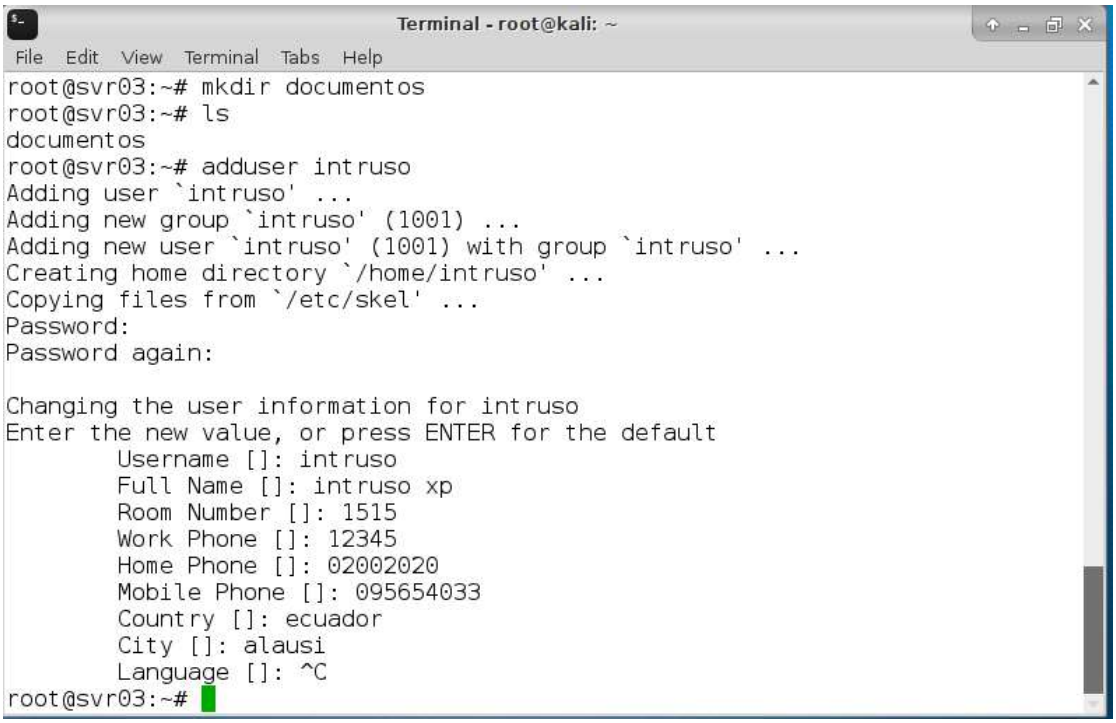


Ilustración 30-3: Datos ingresados para el nuevo usuario creado

Realizado por: Erazo, J, 2022

También se puede generar llaves públicas como se muestra en la ilustración 31-3.

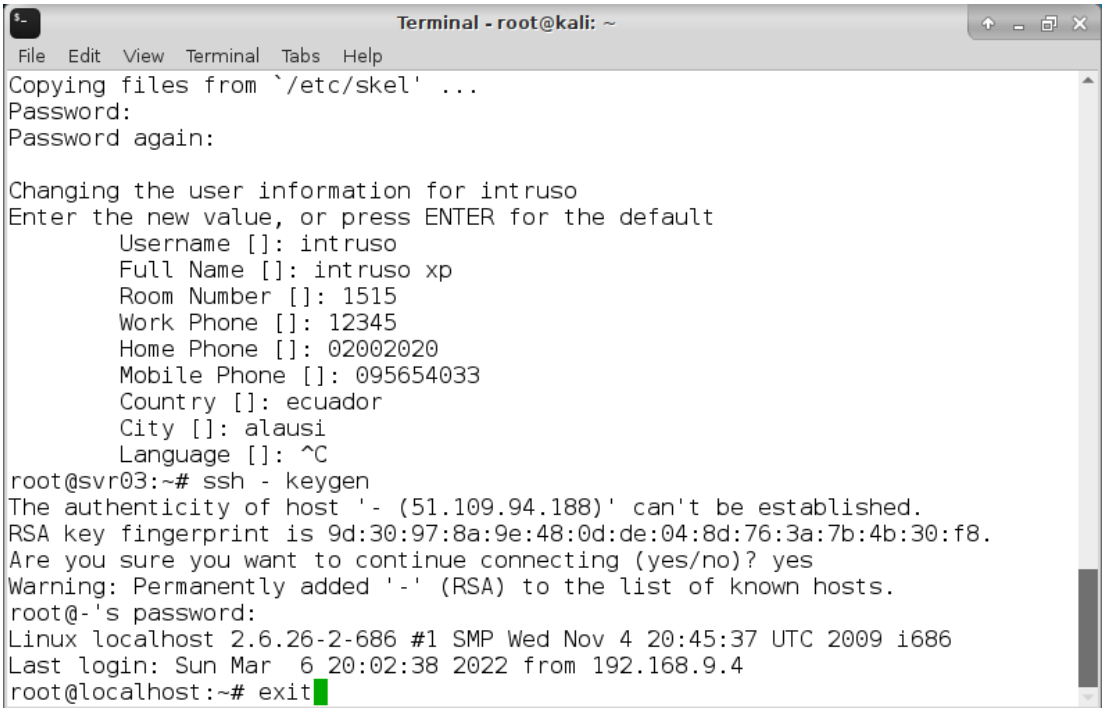


Ilustración 31-3: Ataque para la creación de llaves públicas en el servidor ssh

Realizado por: Erazo, J, 2022

Lo interesante de haber instalado Kippo y las ventajas que tiene, es que el atacante al desconectarse del servidor ssh, Kippo simula una desconexión y de esta manera el atacante puede seguir realizando acciones no autorizadas a este servidor tal como se muestra en la ilustración 32-3.

Todas estas acciones que realiza el atacante quedan registradas en el honeypot Kippo, y es así de esta manera que luego en los registros se analiza todas las acciones no autorizadas de los intrusos al protocolo ssh.

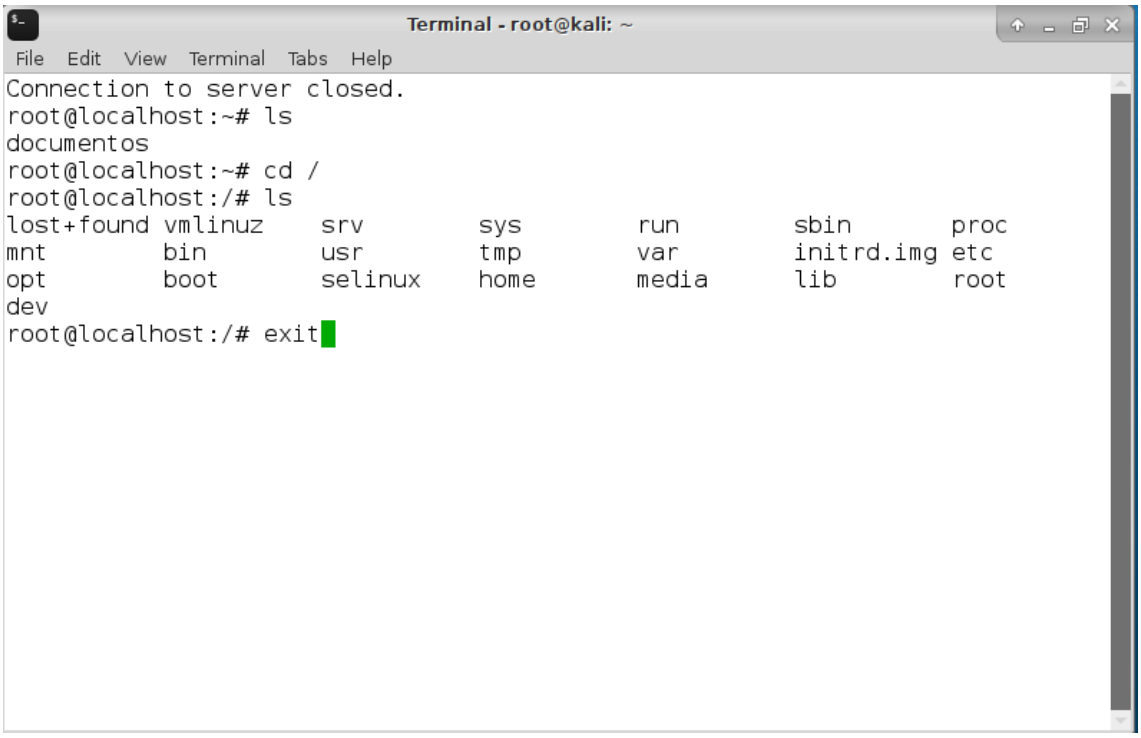


Ilustración 32-3: Exploración de archivos después de haber salido del servidor ssh desde Kali Linux

Realizado por: Erazo, J, 2022

- **Informe o Reporte**

El informe o reporte será los análisis de los registros de los ataques y las recomendaciones para mitigar los accesos no autorizados al protocolo ssh que se encuentra en el capítulo IV.

3.5.2 Ataque manual mediante máquina virtual Centos

Se utiliza una máquina virtual Centos, esta distribución linux tiene una plataforma manejable y muy consistente que se adapta a una extensa variedad de implementaciones teniendo una base sólida de construcción y sirve para comunidades de código abierto.

El ataque que se utiliza en esta máquina virtual se lo va a realizar mediante los nombres de usuarios y contraseñas que comúnmente son utilizadas por los usuarios o administradores de sistemas. Este ataque es uno de los más comunes utilizados por los intrusos no autorizados ya que de esta manera intentan vulnerar al servidor mediante usuarios y contraseñas ingresadas aleatoriamente.

Para empezar con el ataque, se ingresa al terminal de la máquina virtual centos, una vez ahí, se debe conectar con el servidor ssh mediante un nombre de usuario y contraseña aleatoriamente, para esto utilizamos como ejemplo el siguiente comando:

ssh josuee@192.168.101.40

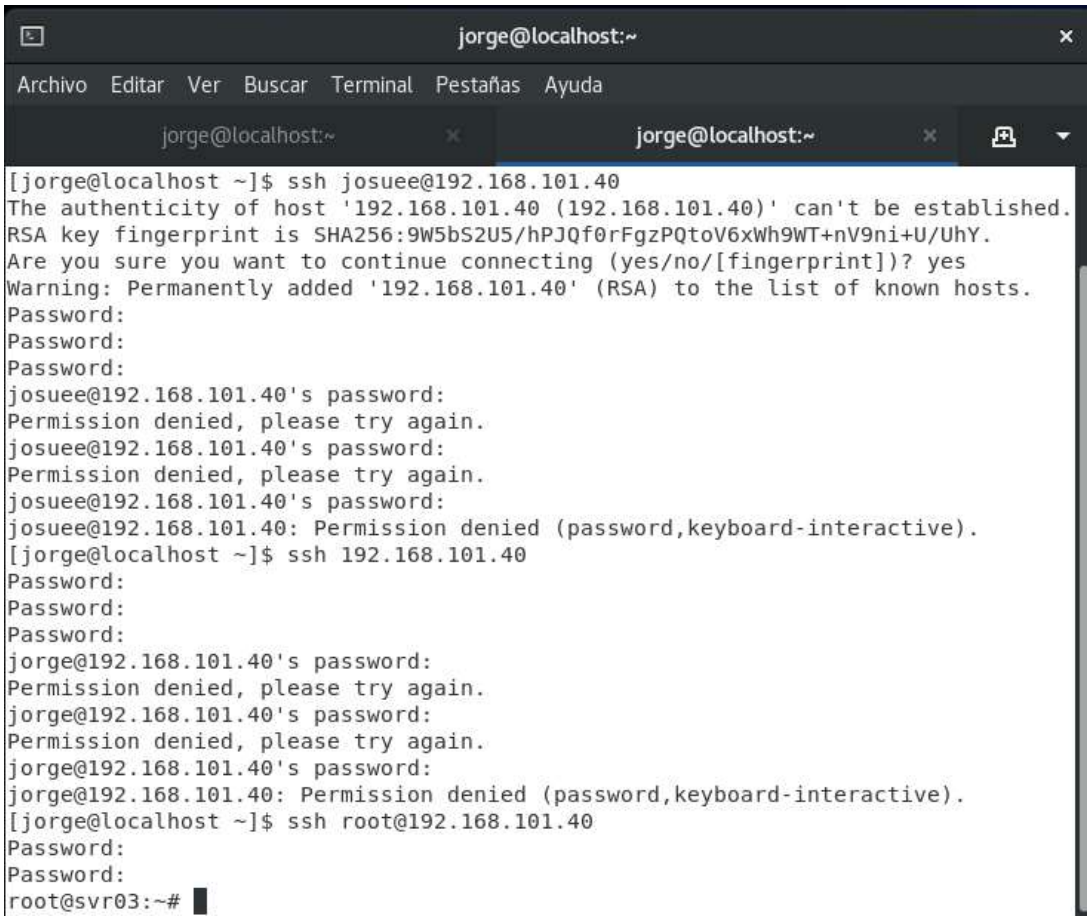


Ilustración 33-3: Ataque mediante usuarios y contraseñas comúnmente utilizadas

Realizado por: Erazo, J, 2022

Como se observa en la ilustración 33-3, se ha utilizado primero un nombre de usuario llamado josuee con una contraseña aleatoria y se ha denegado el acceso al servidor ssh, después es usado el nombre de usuario por defecto y con las contraseñas aleatorias y vuelve a negar el acceso al servidor, por último se intenta con el nombre de usuario root y una contraseña cualquiera y no se conecta, pero al ingresar la contraseña correcta que es 123456, este automáticamente inicia sesión en el servidor ssh de manera exitosa.

Con esto el atacante ingresa al sistema y puede realizar todas las acciones no autorizadas que quiera, como por ejemplo puede empezar a espiar la información, puede observar y leer todas las carpetas y archivos que se encuentran ahí, además que puede explorar y navegar por cada directorio que tiene el sistema, esto lo podemos notar en la ilustración 34-3.

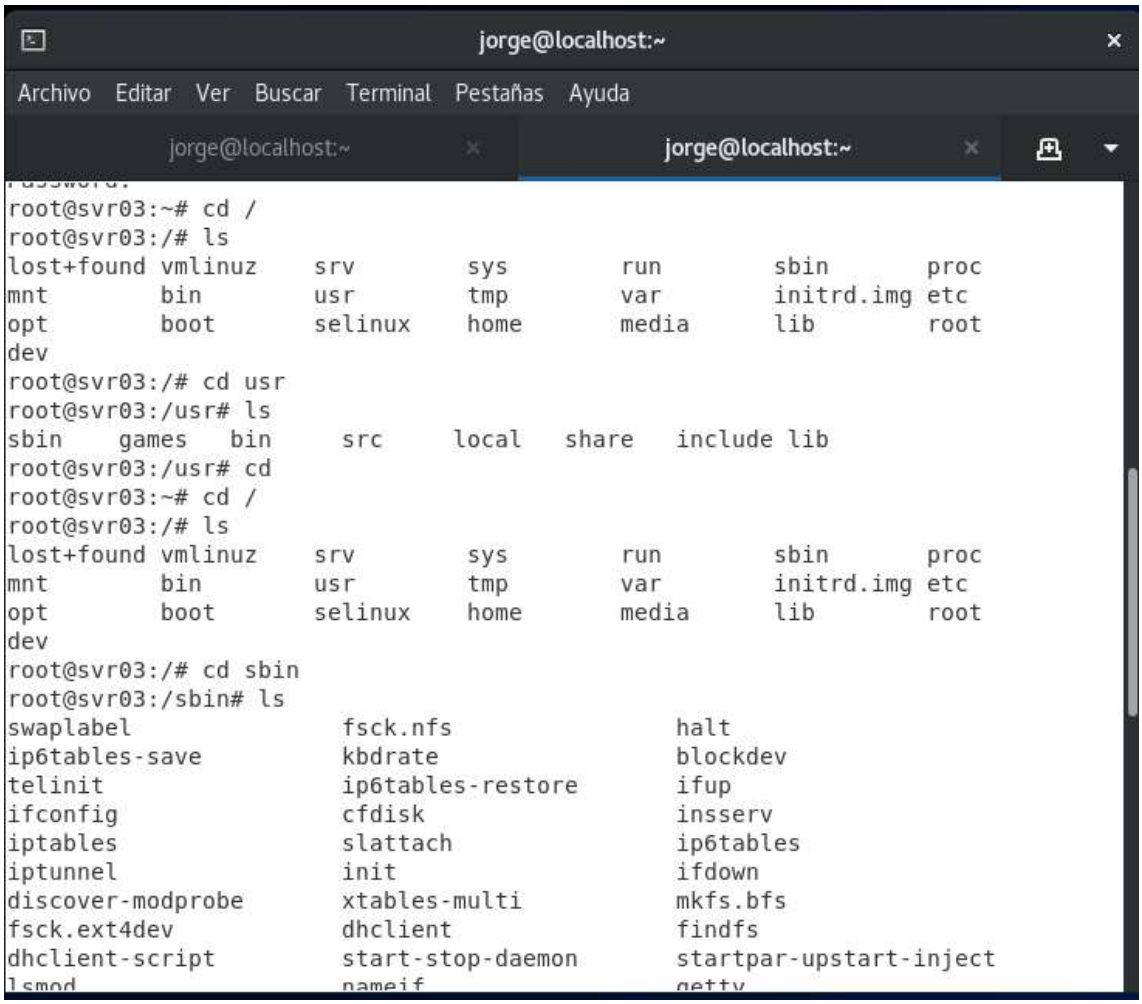


Ilustración 34-3: Exploración interna por los directorios del servidor ssh desde Centos

Realizado por: Erazo, J, 2022

Lo interesante de haber instalado Kippo y las ventajas que tiene, es que el atacante al desconectarse del servidor ssh, Kippo simula una desconexión y de esta manera el atacante puede seguir realizando acciones no autorizadas a este servidor (ver ilustración 35-3).

Todas estas acciones que realiza el atacante quedan registradas en el honeypot Kippo, y es así de esta manera que luego en los registros se analiza todas las acciones no autorizadas de los intrusos al protocolo ssh.

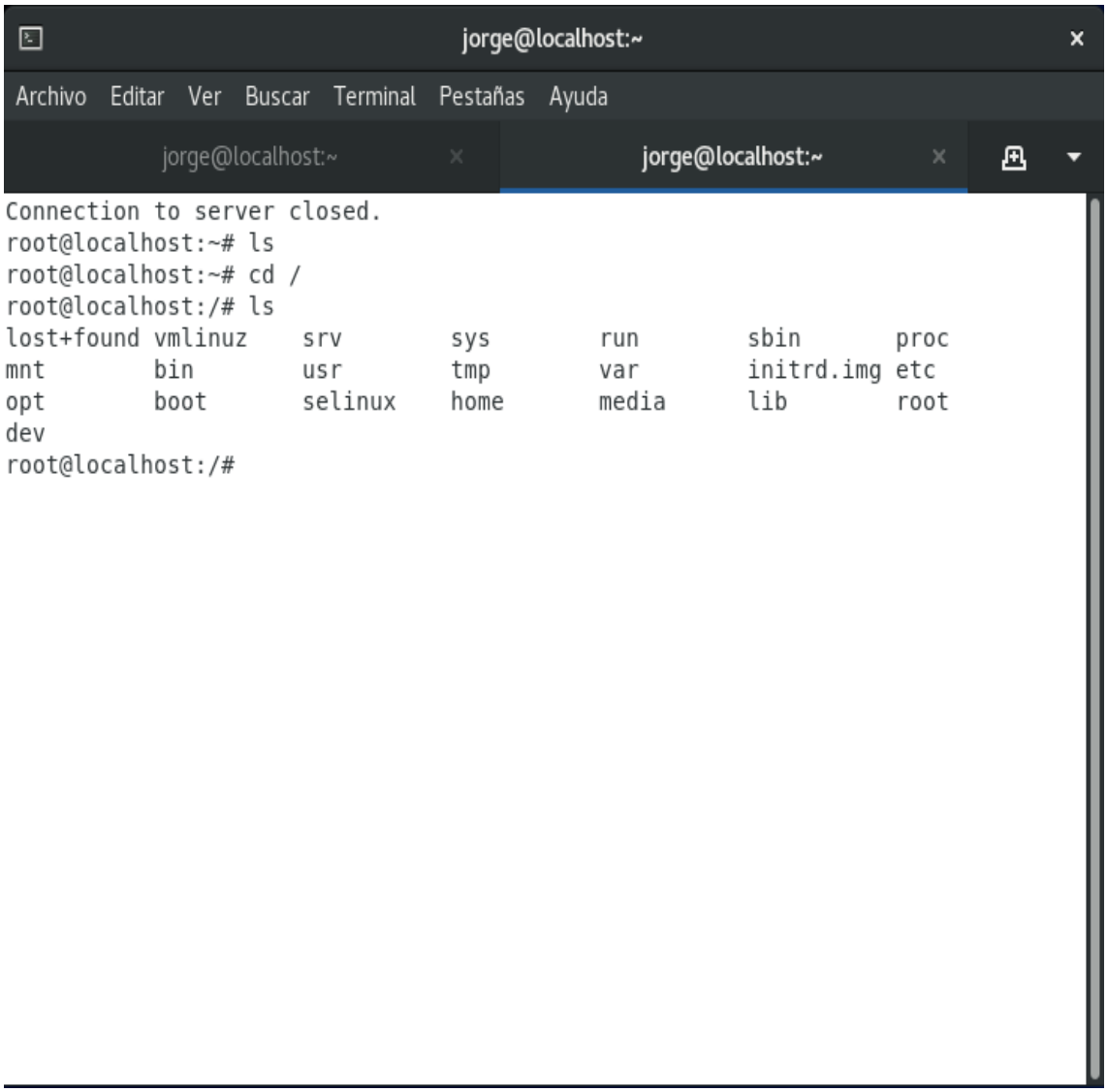


Ilustración 35-3: Exploración de archivos después de haber salido del servidor ssh desde Centos

Realizado por: Erazo, J, 2022

3.5.3 Ataque de ingeniería social mediante máquina virtual Windows 7

Windows 7 ha sido elegido para realizar este ataque ya que es uno de los sistemas operativos más utilizados en oficinas o empresas en donde es común que sucedan estos tipos de ataques.

En este caso se da uso de la ingeniería social, el cual el intruso hace todo lo necesario y posible para conseguir la contraseña y el nombre de usuario del servidor, todo esto se puede obtener mediante ataques de phishing, es decir hacerse pasar por otras personas y enviar correos electrónicos falsos para que estos sean respondidos por el usuario y de esta manera obtener las credenciales, también se usan llamadas telefónicas o virus que son insertadas en lo discos extraíbles de los usuarios o trabajadores de alguna institución, etc.

En este ataque, se simula haber obtenido el usuario y la contraseña a partir de un ataque de ingeniería social, para iniciar con el ataque primero se debe ejecutar el cliente ssh en Windows 7 mediante un programa llamado Putty, se ingresa la dirección ip del servidor y el puerto por donde va a ser vulnerado, en este caso el puerto es el número 22 tal como se muestra en la ilustración 36-3.

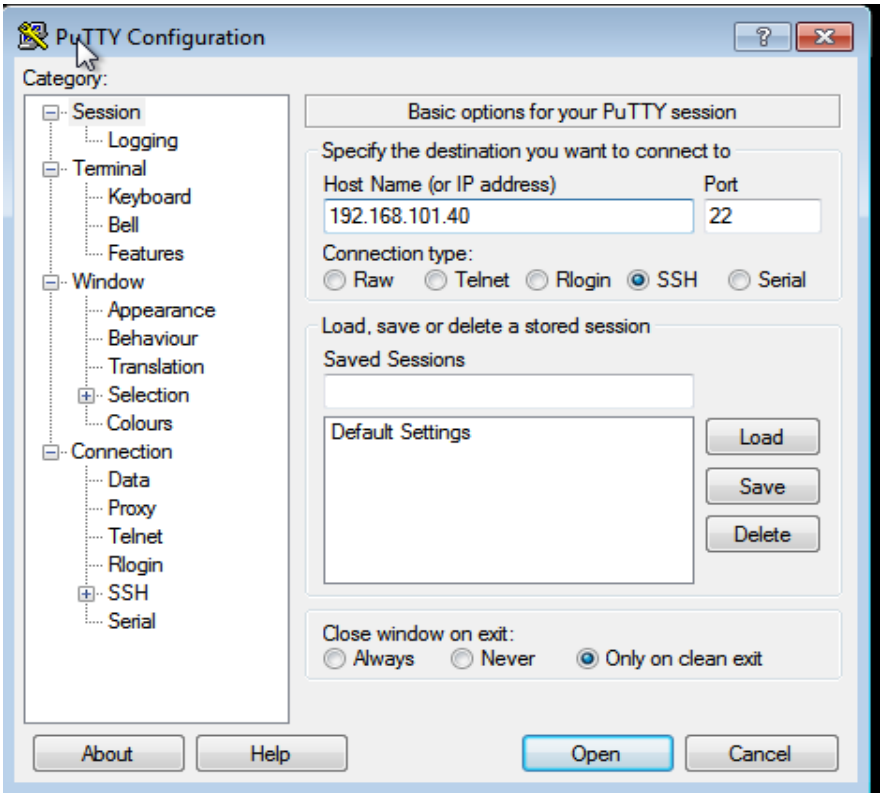


Ilustración 36-3: Inicio de sesión ssh mediante programa putty en Windows 7

Realizado por: Erazo, J, 2022

A continuación, al dar clic en open se abre una ventana que muestra la llave por la cual se conecta al servidor mediante el protocolo ssh, esta debe ser aceptada para iniciar la sesión (ver ilustración 37-3).

Se ingresa el nombre el nombre de usuario y contraseña, y de esta manera ya está el intruso dentro del servidor para realizar cualquier tipo de acciones.

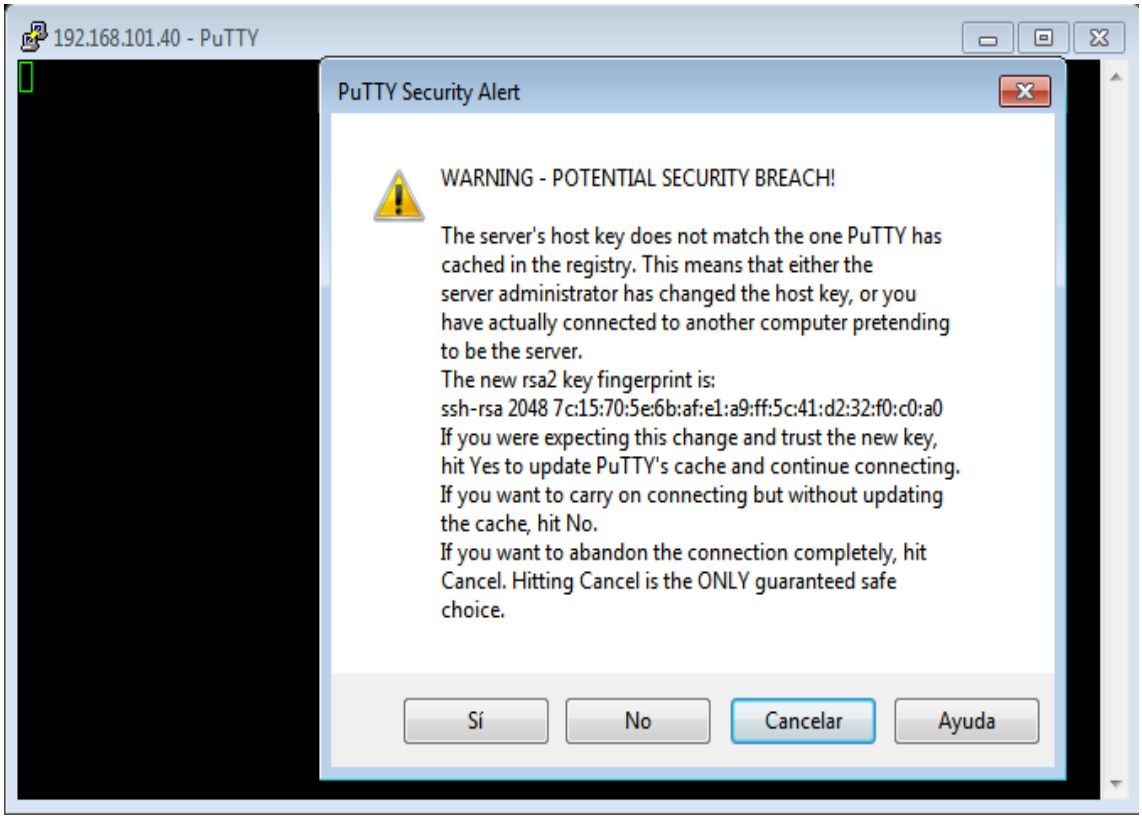


Ilustración 37-3: Aceptación de la llave generada por el servidor ssh

Realizado por: Erazo, J, 2022

Una vez que el atacante ingresa al sistema ya puede realizar todas las acciones no autorizadas que quiera, como por ejemplo puede empezar a espiar la información, puede observar y leer todas las carpetas y archivos que se encuentran ahí, además que puede explorar y navegar por cada directorio que tiene el sistema, tal como lo muestra en la ilustración 38-3.

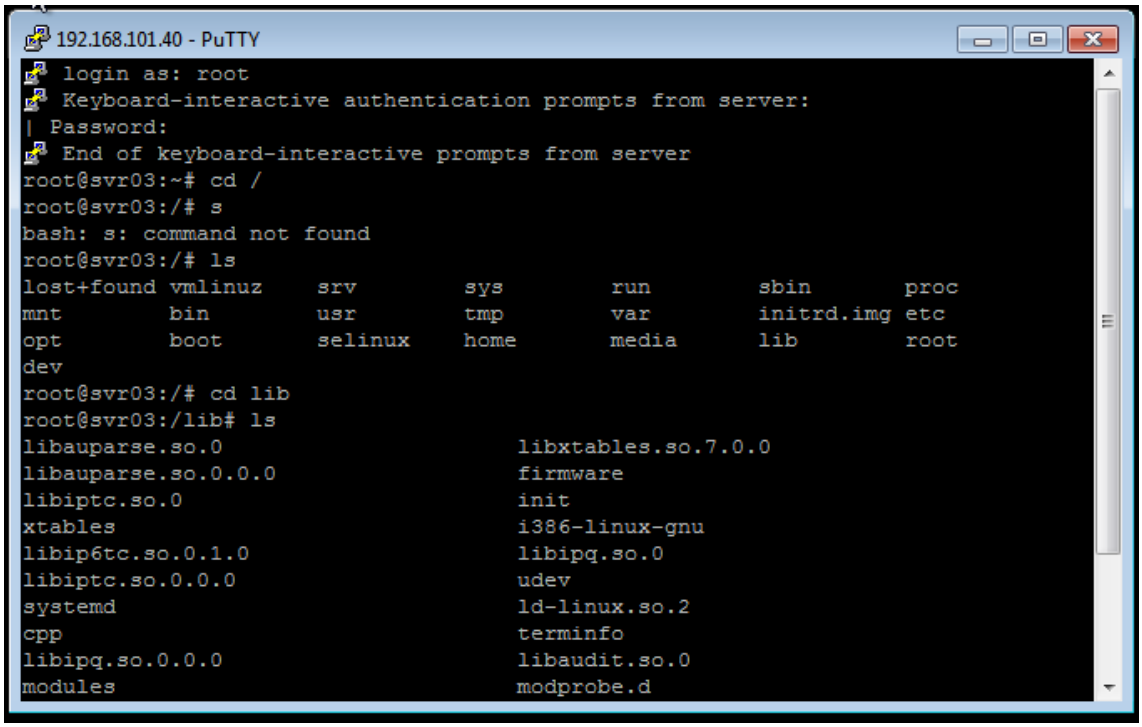


Ilustración 38-3: Exploración interna por los directorios del servidor ssh desde Windows 7

Realizado por: Erazo, J, 2022

CAPÍTULO IV

4. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 Análisis de los registros

Después de haber realizado los ataques al servidor ssh, estos archivos denominados “Kippo.log” quedan registrados en el honeypot Kippo en una carpeta con el nombre de “log”, en este archivo se almacenan todos los datos del día, la hora y la fecha en la que el atacante ingresa al servidor, así como las acciones no autorizadas de los intrusos mediante el protocolo ssh como por ejemplo las conexiones que utiliza, las direcciones ip del atacante y el puerto por donde ingresa al servidor. Todos estos registros se muestran a continuación, tanto para los ataques realizados mediante fuerza bruta por diccionario desde la máquina virtual de Kali linux, para los ataques realizados mediante usuarios y contraseñas usadas comúnmente desde la máquina virtual de centOs y para los ataques realizados mediante ingeniería social desde la máquina virtual de Windows 7.

4.1.1 Análisis de ataque de la máquina virtual Kali Linux

A continuación, se muestran unas tablas con código de colores y su significado de los datos encontrados en el registro de las acciones no autorizadas de los intrusos mediante el ataque de fuerza bruta de diccionario y por consiguiente también se muestra unas figuras que exponen los datos encontrados en el registro.

Tabla 1-4: Código de colores con su significado del ataque de fuerza bruta

	Dirección y puerto del atacante
	Dirección y puerto del servidor
	Numero de sesiones intentadas por el atacante
	Versión remota de SSH o software que utiliza el atacante
	Inicio fuerza bruta mediante Ncrack
	Nombre del servidor que ingresa el atacante
	Contraseña del servidor que ingresa el atacante
	Estado de la conexión

Realizado por: Erazo, J, 2022

```
2022-03-08 05:26:14-0500 [-] Starting factory <kippo.core.ssh.HoneyPotSSHFactory instance at
0x7f5ca1a5b1e0>
2022-03-08 05:26:26-0500 [kippo.core.ssh.HoneyPotSSHFactory] New connection:
192.168.101.41:32876 (192.168.101.40:2222) [session: 0]
2022-03-08 05:26:26-0500 [HoneyPotTransport,0,192.168.101.41] Remote SSH version: SSH-2.0-
OpenSSH_7.1
2022-03-08 05:26:26-0500 [HoneyPotTransport,0,192.168.101.41] kex alg, key alg: diffie-hellman-group
exchange-sha1 ssh-rsa
2022-03-08 05:26:26-0500 [HoneyPotTransport,0,192.168.101.41] outgoing: aes128-ctr hmac-sha1
none
2022-03-08 05:26:26-0500 [HoneyPotTransport,0,192.168.101.41] incoming: aes128-ctr hmac-sha1
none
2022-03-08 05:26:31-0500 [HoneyPotTransport,0,192.168.101.41] NEW KEYS
2022-03-08 05:26:31-0500 [HoneyPotTransport,0,192.168.101.41] starting service ssh-userauth
2022-03-08 05:26:31-0500 [SSHService ssh-userauth on HoneyPotTransport,0,192.168.101.41] admin
trying auth password
2022-03-08 05:26:31-0500 [SSHService ssh-userauth on HoneyPotTransport,0,192.168.101.41] login
attempt [admin/admin] failed
2022-03-08 05:26:32-0500 [-] admin failed auth password
2022-03-08 05:26:32-0500 [-] unauthorized login:
2022-03-08 05:26:33-0500 [SSHService ssh-userauth on HoneyPotTransport,0,192.168.101.41] admin
trying auth password
2022-03-08 05:26:33-0500 [SSHService ssh-userauth on HoneyPotTransport,0,192.168.101.41] login
attempt [admin/1234567] failed
2022-03-08 05:26:34-0500 [-] admin failed auth password
2022-03-08 05:26:34-0500 [-] unauthorized login:
2022-03-08 05:26:34-0500 [SSHService ssh-userauth on HoneyPotTransport,0,192.168.101.41] admin
trying auth password
2022-03-08 05:26:34-0500 [SSHService ssh-userauth on HoneyPotTransport,0,192.168.101.41] login
attempt [admin/root] failed
2022-03-08 05:26:35-0500 [-] admin failed auth password
2022-03-08 05:26:35-0500 [-] unauthorized login:
2022-03-08 05:26:35-0500 [SSHService ssh-userauth on HoneyPotTransport,0,192.168.101.41] admin
trying auth password
2022-03-08 05:26:35-0500 [SSHService ssh-userauth on HoneyPotTransport,0,192.168.101.41] login
attempt [admin/123456] failed
2022-03-08 05:26:36-0500 [-] admin failed auth password
2022-03-08 05:26:36-0500 [-] unauthorized login:
2022-03-08 05:26:36-0500 [SSHService ssh-userauth on HoneyPotTransport,0,192.168.101.41] admin
trying auth password
2022-03-08 05:26:36-0500 [SSHService ssh-userauth on HoneyPotTransport,0,192.168.101.41] login
attempt [admin/password] failed
2022-03-08 05:26:37-0500 [-] admin failed auth password
2022-03-08 05:26:37-0500 [-] unauthorized login:
2022-03-08 05:26:37-0500 [HoneyPotTransport,0,192.168.101.41] connection lost
```

Ilustración 1-4: Registro de los datos guardados en Kippo sobre el ataque mediante fuerza bruta

Realizado por: Erazo, J, 2022

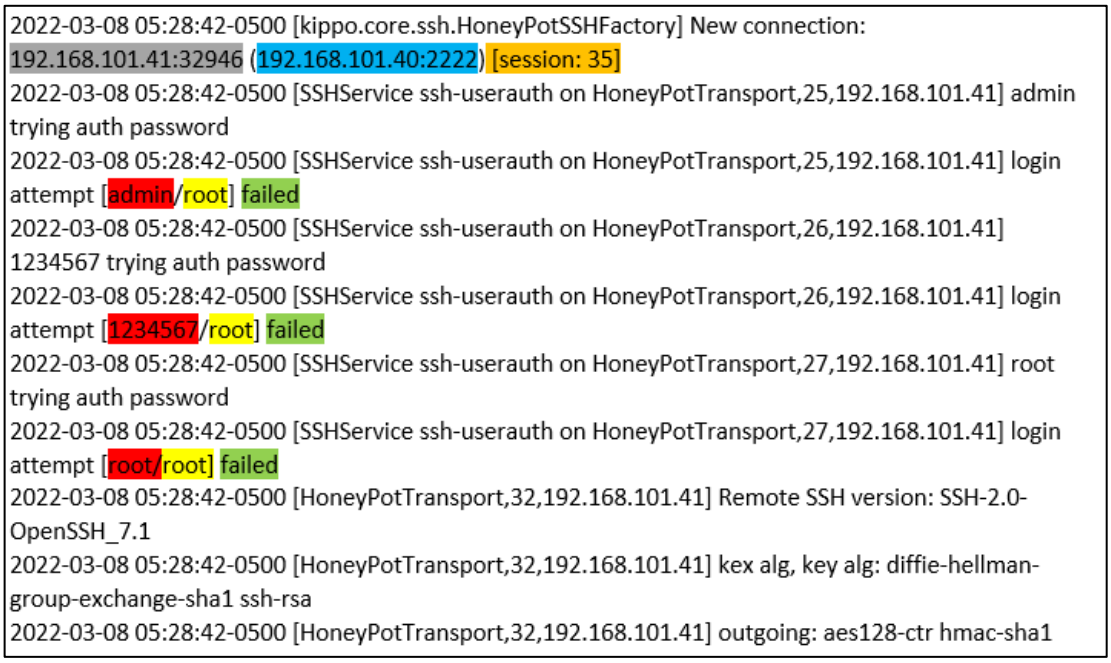


Ilustración 2-4: Registro de los datos guardados en Kippo sobre el ataque mediante fuerza bruta

Realizado por: Erazo, J, 2022

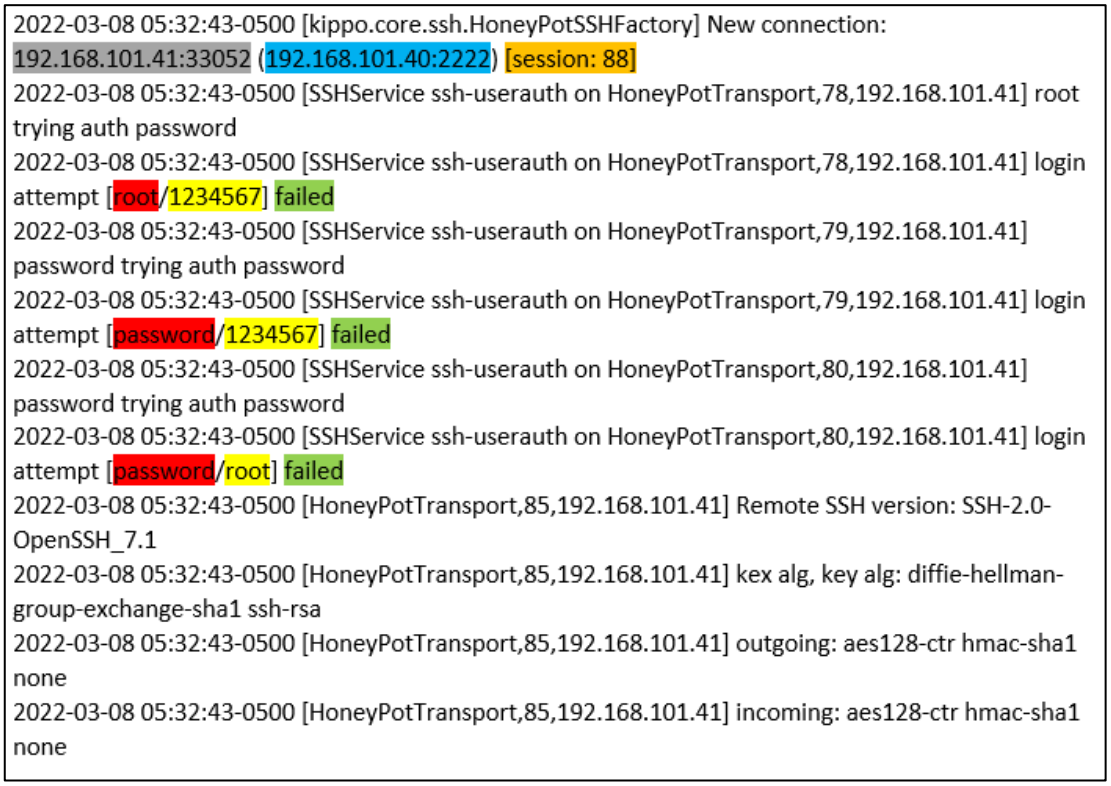


Ilustración 3-4: Registro de los datos guardados en Kippo sobre el ataque mediante fuerza bruta

Realizado por: Erazo, J, 2022

En las ilustraciones 1-4, 2-4, 3-4 y tomando en cuenta a la tabla 1-4 se puede observar la dirección ip y puerto desde donde se realizó el ataque por fuerza bruta mediante el color gris, de la misma manera la dirección ip y puerto del servidor ssh con el color celeste, así como el número de sesiones que intentó el atacante para encontrar el usuario y contraseña incorrecta mediante el color anaranjado, además el inicio del ataque de fuerza bruta con el color crema y por último todas las combinaciones que se hizo entre los usuarios y contraseñas que se encontraban en el diccionario, de esta manera se puede tomar un ejemplo;

En la ilustración 1-4 se puede observar que se realiza la combinación de un usuario llamado "admin" que se encuentra pintado de color rojo y de una contraseña llamado "root" que se encuentra pintado de color amarrillo, el cual proporciona un estado de fallido que se encuentra pintado de color verde.

En la ilustración 2-4 y 3-4 también se logra observar algunas combinaciones de usuarios y contraseñas las cuales dan como fallido.

En cambio, en la ilustración 4-4 y tomando en cuenta la tabla 2-4 se puede observar que después de 98 sesiones, se realiza la combinación de un usuario llamado "root" que se encuentra pintado de color rojo y de una contraseña llamado "123456" que se encuentra pintado de color amarrillo, el cual proporciona un estado de éxito que se encuentra pintado de color verde, así de esta manera se puede observar que después de generar y comparar usuarios y contraseñas del diccionario mediante el ataque de fuerza bruta, este se detiene automáticamente y queda registrado en el honeypot Kippo.

Tabla 2-4: Código de colores con su significado del ataque de fuerza bruta exitoso

	Dirección y puerto del atacante
	Dirección y puerto del servidor
	Numero de sesiones intentadas por el atacante
	Versión remota de SSH o software que utiliza el atacante
	Nombre del servidor que ingresa el atacante
	Contraseña del servidor que ingresa el atacante
	Estado de la conexión

Realizado por: Erazo, J, 2022

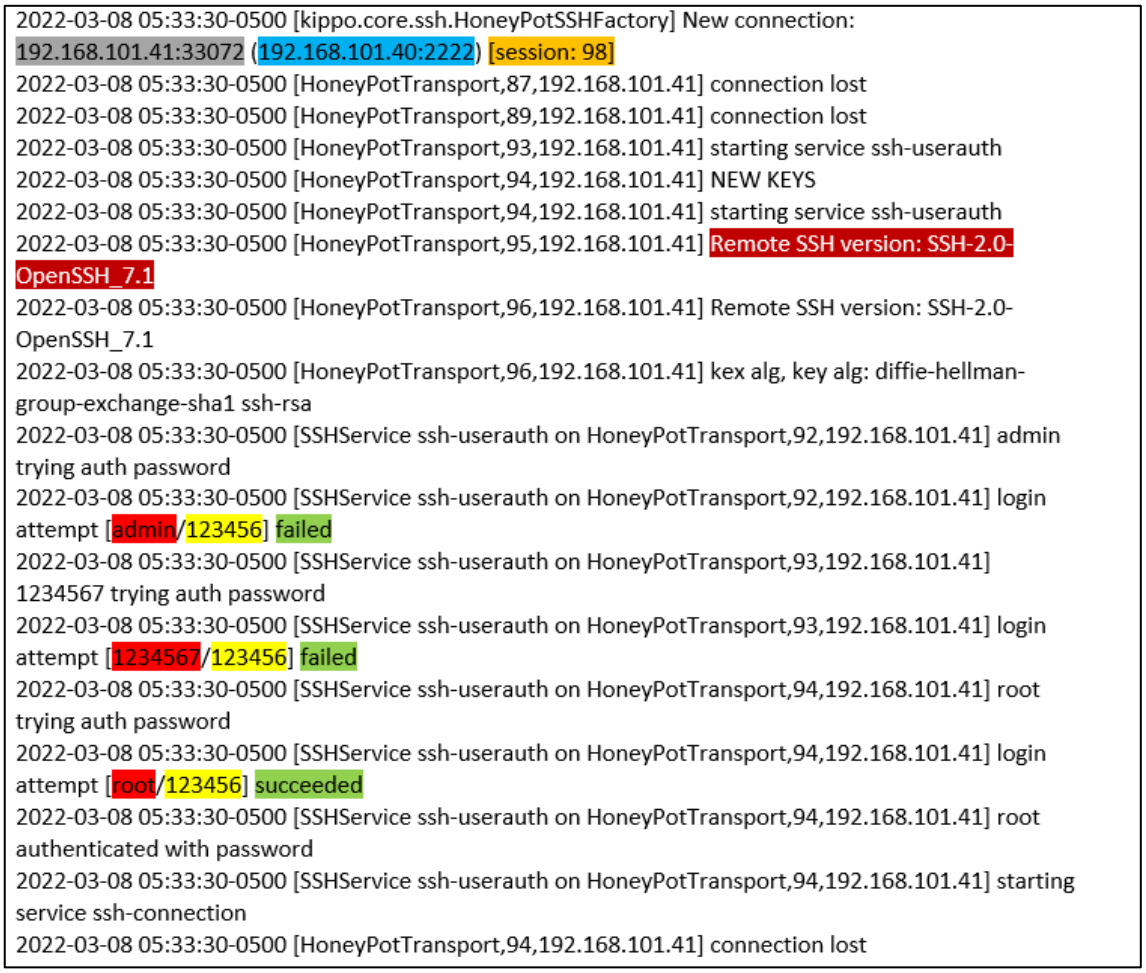


Ilustración 4-4: Registro de los datos guardados en Kippo sobre el ataque mediante fuerza bruta exitoso

Realizado por: Erazo, J, 2022

Tabla 3-4: Código de colores con su significado al ingresar al servidor mediante el ataque de fuerza bruta

	Dirección y puerto del atacante
	Dirección y puerto del servidor
	Numero de sesiones intentadas por el atacante
	Versión remota de SSH o software que utiliza el atacante
	Nombre del servidor que ingresa el atacante
	Contraseña del servidor que ingresa el atacante
	Estado de la conexión
	Dirección de registro de movimientos

Realizado por: Erazo, J, 2022

```
2022-03-08 06:07:46-0500 [kippo.core.ssh.HoneyPotSSHFactory] New connection:
192.168.101.41:45470 (192.168.101.40:2222) [session: 1]
2022-03-08 06:07:46-0500 [HoneyPotTransport,1,192.168.101.41] Remote SSH version: SSH-2.0-
OpenSSH_7.4p1 Debian-10
2022-03-08 06:07:46-0500 [HoneyPotTransport,1,192.168.101.41] kex alg, key alg: diffie-hellman-group-
exchange-sha1 ssh-rsa
2022-03-08 06:07:46-0500 [HoneyPotTransport,1,192.168.101.41] outgoing: aes128-ctr hmac-sha1
none
2022-03-08 06:07:46-0500 [HoneyPotTransport,1,192.168.101.41] incoming: aes128-ctr hmac-sha1
none
2022-03-08 06:07:53-0500 [HoneyPotTransport,1,192.168.101.41] NEW KEYS
2022-03-08 06:07:53-0500 [HoneyPotTransport,1,192.168.101.41] starting service ssh-userauth
2022-03-08 06:07:53-0500 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.41] root
trying auth none
2022-03-08 06:07:53-0500 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.41] root
trying auth keyboard-interactive
2022-03-08 06:07:56-0500 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.41] login
attempt [root/123456] succeeded
2022-03-08 06:07:56-0500 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.41] root
authenticated with keyboard-interactive
2022-03-08 06:07:56-0500 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.41] starting
service ssh-connection
2022-03-08 06:07:56-0500 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,1,192.168.101.41] Opening TTY log: log/tty/20220308-060756-6968.log
```

Ilustración 5-4: Registro de los datos guardados en Kippo sobre el inicio de sesión en el servidor ssh

Realizado por: Erazo, J, 2022

Como se observa en la ilustración 5-4 al iniciar sesión con el usuario y contraseña exitoso, este registra la dirección en donde se guarda todos los movimientos que realizó el intruso, esta dirección se encuentra pintado de color azul, el cual fue añadido a la tabla 3-4.

En la ilustración 6-4 y tomando en cuenta la tabla 4-4, se puede observar de color verde el registro de los datos de todas las acciones que realizó el intruso cuando ingresó de forma exitosa al servidor como por ejemplo la exploración y lectura de directorios.

En la ilustración 7-4 se puede observar la creación y eliminación de archivos que realizó el intruso cuando estaba dentro de los directorios como por ejemplo el comando adduser intruso.

Tabla 4-4: Código de colores con su significado ingresado cuando se explora el servidor ssh

	Comando ingresado por el atacante

Realizado por: Erazo, J, 2022

```
2022-03-08 06:08:53-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] CMD: cd /
2022-03-08 06:08:53-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] Command found: cd /
2022-03-08 06:08:55-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] CMD: ls
2022-03-08 06:08:55-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] Command found: ls
2022-03-08 06:09:15-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] CMD: cd usr
2022-03-08 06:09:15-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] Command found: cd usr
2022-03-08 06:09:28-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] CMD: ls
2022-03-08 06:09:28-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] Command found: ls
2022-03-08 06:09:32-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] CMD: cd
2022-03-08 06:09:32-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] Command found: cd
2022-03-08 06:09:35-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] CMD: cd /
2022-03-08 06:09:35-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] Command found: cd /
2022-03-08 06:09:41-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] CMD: cd sbin
2022-03-08 06:09:41-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] Command found: cd sbin
2022-03-08 06:09:43-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] CMD: ls
2022-03-08 06:09:43-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] Command found: ls
2022-03-08 06:10:35-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] CMD: cd
2022-03-08 06:10:35-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] Command found: cd
2022-03-08 06:10:46-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] CMD: cd /
2022-03-08 06:10:46-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] Command found: cd /
2022-03-08 06:10:50-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] CMD: ls
2022-03-08 06:10:50-0500 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,1,192.168.101.41] Command found: ls
```

Ilustración 6-4: Registro de los datos guardados en Kippo sobre la exploración de directorios en el servidor ssh mediante el ataque de fuerza bruta

Realizado por: Erazo, J, 2022

```
2022-03-08 06:11:03-0500 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,1,192.168.101.41] CMD: cp initrd.img /root
2022-03-08 06:11:03-0500 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,1,192.168.101.41] Command found: cp initrd.img /root
2022-03-08 06:11:10-0500 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,1,192.168.101.41] CMD: cd /root
2022-03-08 06:11:10-0500 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,1,192.168.101.41] Command found: cd /root
2022-03-08 06:11:15-0500 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,1,192.168.101.41] CMD: ls
2022-03-08 06:11:15-0500 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,1,192.168.101.41] Command found: ls
2022-03-08 06:11:29-0500 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,1,192.168.101.41] CMD: rm initrd.img
2022-03-08 06:11:29-0500 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,1,192.168.101.41] Command found: rm initrd.img
2022-03-08 06:11:32-0500 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,1,192.168.101.41] CMD: ls
2022-03-08 06:11:32-0500 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,1,192.168.101.41] Command found: ls
2022-03-08 06:11:46-0500 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,1,192.168.101.41] CMD: mkdir documentos
2022-03-08 06:11:46-0500 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,1,192.168.101.41] Command found: mkdir documentos
2022-03-08 06:11:48-0500 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,1,192.168.101.41] CMD: ls
2022-03-08 06:11:48-0500 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,1,192.168.101.41] Command found: ls
2022-03-08 06:12:10-0500 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,1,192.168.101.41] CMD: adduser intruso
```

Ilustración 7-4: Registro de los datos guardados en Kippo de la eliminación y creación de archivos

Realizado por: Erazo, J, 2022

Como se muestra a continuación en la tabla 5-4 el código de colores tiene significados nuevos el cual se muestra pintado en la ilustración 8-4 donde el color verde significa el comando ingresado por el atacante cuando intenta crear llaves ssh y el color amarrillo significa los datos que ingresa el atacante para su respectiva creación de las llaves ssh.

Tabla 5-4: Código de colores con su significado explorados por el atacante mediante la fuerza bruta

	Comando ingresado por el atacante
	Datos ingresados por el atacante

Realizado por: Erazo, J, 2022

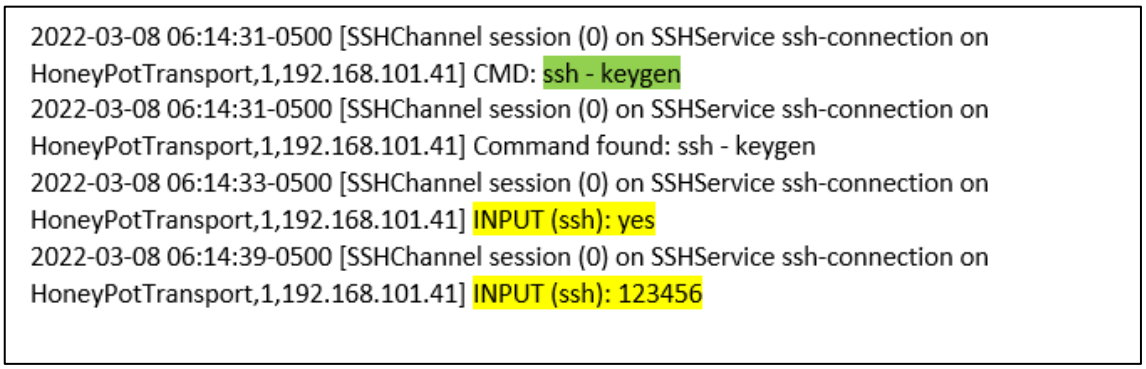


Ilustración 8-4: Registro de los datos guardados en Kippo sobre la creación de llaves ssh mediante el ataque de fuerza bruta

Realizado por: Erazo, J, 2022

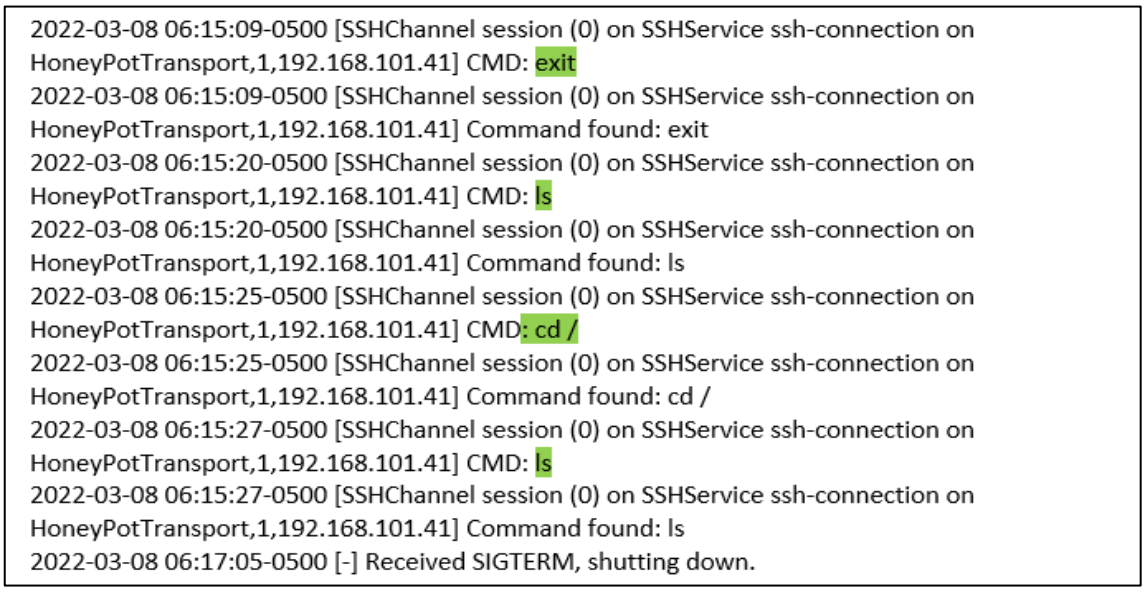


Ilustración 9-4: Registro de los datos guardados en Kippo de la exploración de archivos cuando se cierra sesión ssh mediante el ataque de fuerza bruta

Realizado por: Erazo, J, 2022

4.1.2 Análisis de ataque de la máquina virtual Centos

A continuación, se muestran unas tablas orientativas del significado de los datos encontrados en el registro de las acciones no autorizadas de los intrusos mediante el ataque de usuarios y contraseñas utilizadas comúnmente y por consiguiente también se muestra unas figuras que exponen los datos encontrados en el registro.

Tabla 6-4: Código de colores con su significado en el análisis del ataque de contraseñas comúnmente utilizadas

	Dirección y puerto del atacante
	Dirección y puerto del servidor
	Numero de sesiones intentadas por el atacante
	Versión remota de SSH o software que utiliza el atacante
	Nombre del servidor que ingresa el atacante
	Contraseña del servidor que ingresa el atacante
	Estado de la conexión

Realizado por: Erazo, J, 2022

En las ilustraciones 10-4, 11-4 y tomando en cuenta a la tabla 6-4 se puede observar la dirección ip y puerto desde donde se realizó el ataque por usuarios y contraseñas que comúnmente son utilizadas en servidor ssh pintadas de color gris, de la misma manera la dirección ip y puerto del servidor ssh con el color celeste, así como el número de sesiones que intentó el atacante para encontrar el usuario y contraseña incorrecta mediante el color anaranjado

En la ilustración 10-4 se puede observar que se realiza la combinación de un usuario llamado “josuee” que se encuentra pintado de color rojo y de una contraseña llamado “root” que se encuentra pintado de color amarrillo, el cual proporciona un estado de fallido que se encuentra pintado de color verde.

En cambio, en la ilustración 12-4 se puede observar que después de 2 sesiones, se realiza la combinación de un usuario llamado “root” que se encuentra pintado de color rojo y de una contraseña llamado “123456” que se encuentra pintado de color amarrillo, el cual proporciona un estado de éxito que se encuentra pintado de color verde.

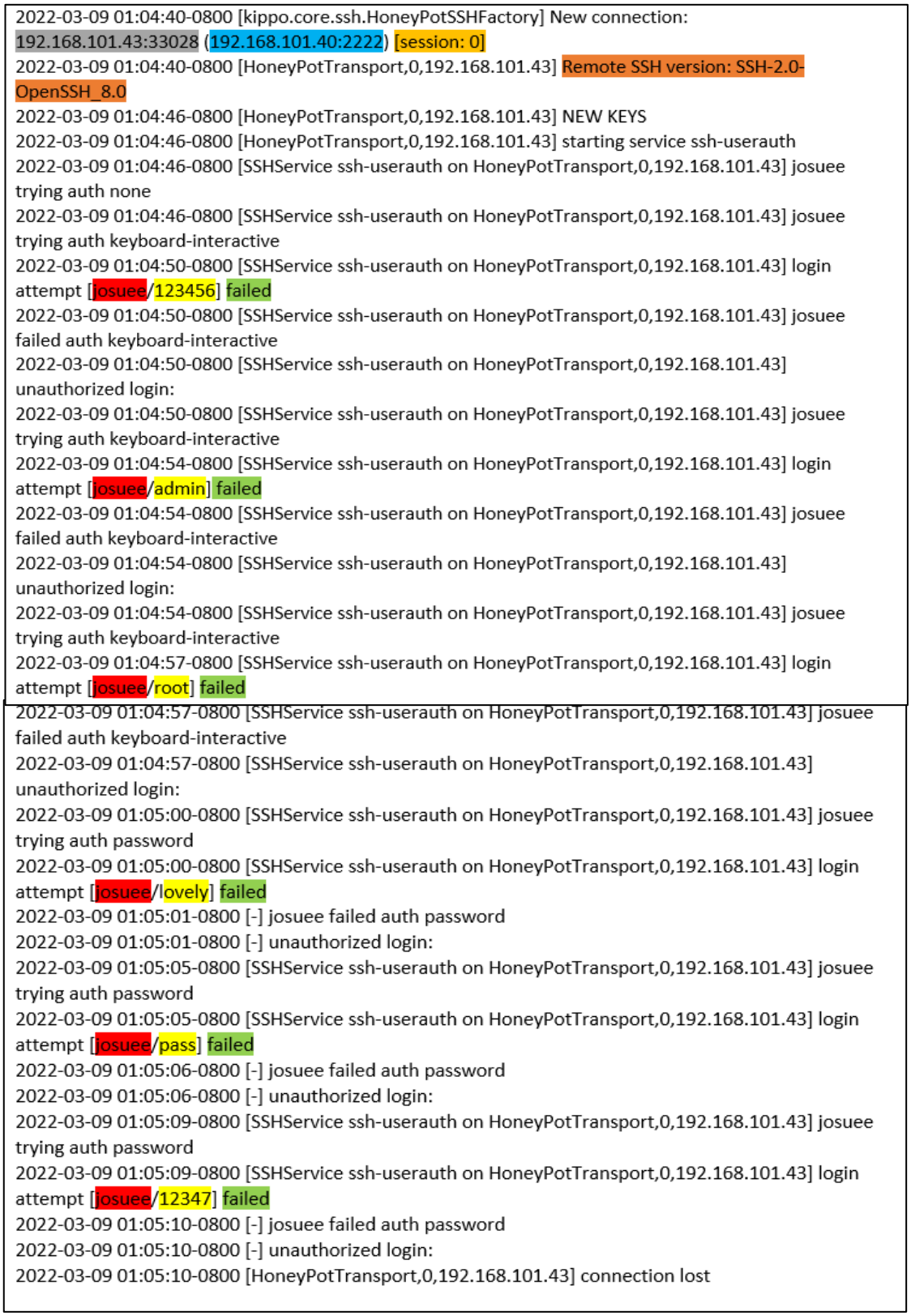


Ilustración 10-4: Registro de los datos guardados en Kippo de los ataques mediante usuarios y contraseñas comúnmente utilizadas

Realizado por: Erazo, J, 2022

```
2022-03-09 01:05:52-0800 [kippo.core.ssh.HoneyPotSSHFactory] New connection:
192.168.101.43:33030 (192.168.101.40:2222) [session: 1]
2022-03-09 01:05:52-0800 [HoneyPotTransport,1,192.168.101.43] Remote SSH version: SSH-2.0-
OpenSSH_8.0
2022-03-09 01:05:55-0800 [HoneyPotTransport,1,192.168.101.43] NEW KEYS
2022-03-09 01:05:55-0800 [HoneyPotTransport,1,192.168.101.43] starting service ssh-userauth
2022-03-09 01:05:55-0800 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.43] jorge
trying auth none
2022-03-09 01:05:55-0800 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.43] jorge
trying auth keyboard-interactive
2022-03-09 01:05:59-0800 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.43] login
attempt [jorge/google] failed
2022-03-09 01:05:59-0800 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.43] jorge
failed auth keyboard-interactive
2022-03-09 01:05:59-0800 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.43]
unauthorized login:
2022-03-09 01:05:59-0800 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.43] jorge
trying auth keyboard-interactive
2022-03-09 01:06:02-0800 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.43] login
attempt [jorge/2146657] failed
2022-03-09 01:06:02-0800 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.43] jorge
failed auth keyboard-interactive
2022-03-09 01:06:02-0800 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.43]
unauthorized login:
2022-03-09 01:06:02-0800 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.43] jorge
trying auth keyboard-interactive
2022-03-09 01:06:04-0800 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.43] login
attempt [jorge/root] failed
2022-03-09 01:06:04-0800 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.43] jorge
failed auth keyboard-interactive
2022-03-09 01:06:04-0800 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.43]
unauthorized login:
2022-03-09 01:06:06-0800 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.43] jorge
trying auth password
2022-03-09 01:06:06-0800 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.43] login
attempt [jorge/admin] failed
2022-03-09 01:06:07-0800 [-] jorge failed auth password
2022-03-09 01:06:07-0800 [-] unauthorized login:
2022-03-09 01:06:11-0800 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.43] jorge
trying auth password
2022-03-09 01:06:11-0800 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.43] login
attempt [jorge/adminroot] failed
2022-03-09 01:06:12-0800 [-] jorge failed auth password
2022-03-09 01:06:12-0800 [-] unauthorized login:
2022-03-09 01:06:13-0800 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.43] jorge
trying auth password
2022-03-09 01:06:13-0800 [SSHService ssh-userauth on HoneyPotTransport,1,192.168.101.43] login
attempt [jorge/t] failed
2022-03-09 01:06:14-0800 [-] jorge failed auth password
2022-03-09 01:06:14-0800 [-] unauthorized login:
2022-03-09 01:06:14-0800 [HoneyPotTransport,1,192.168.101.43] connection lost
```

Ilustración 11-4: Registro de los datos guardados en Kippo de los ataques mediante usuarios y contraseñas comúnmente utilizadas 2

Realizado por: Erazo, J, 2022

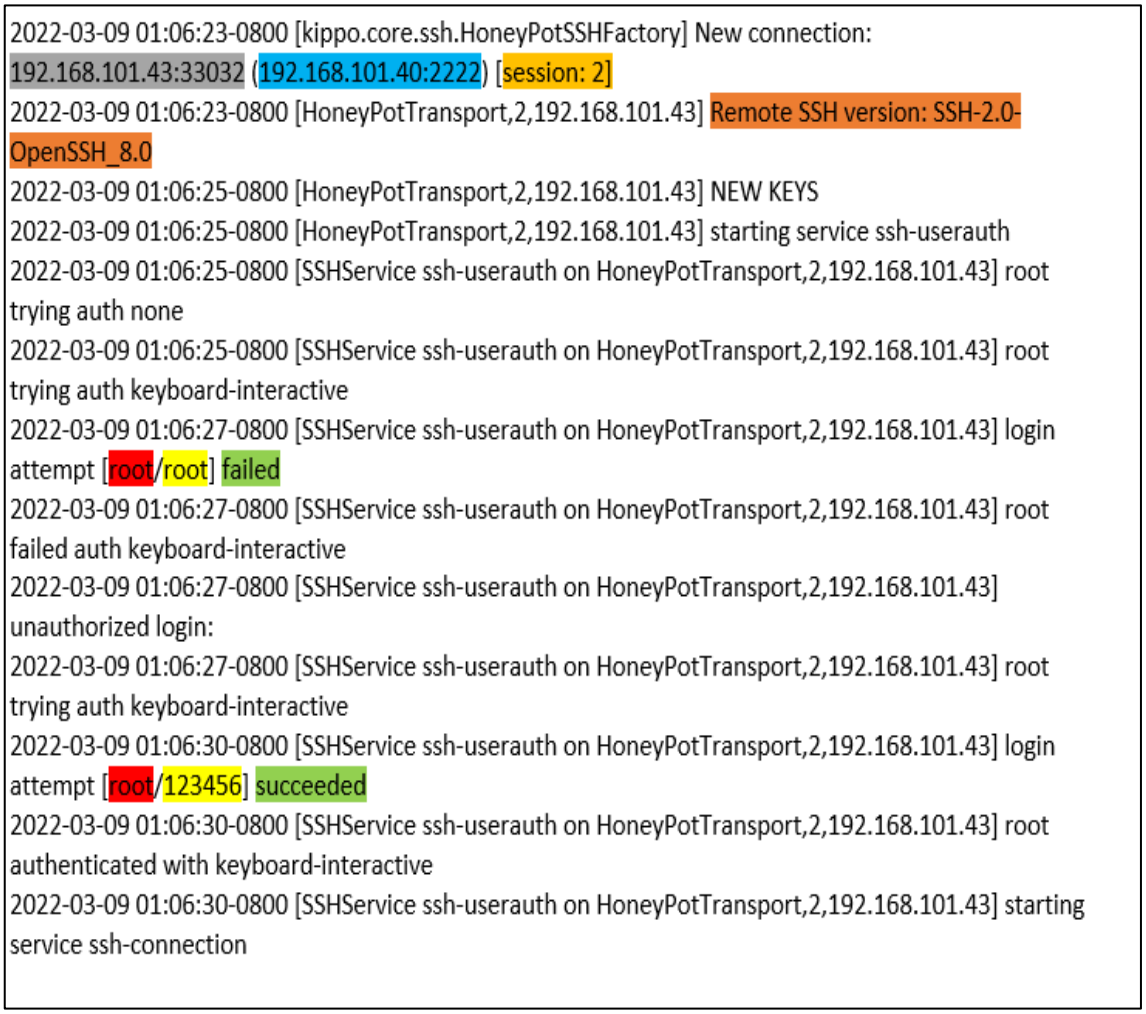


Ilustración 12-4: Registro de los datos guardados en Kippo de los ataques mediante usuarios y contraseñas comúnmente utilizadas exitoso

Realizado por: Erazo, J, 2022

Como se observa en la ilustración 13-4 al iniciar sesión con el usuario y contraseña exitoso que comúnmente se utilizan en los servidores ssh, este registra la dirección en donde se guarda todos los movimientos que realizó el intruso, esta dirección se encuentra pintado de color azul, el cual fue añadido a la tabla 7-4.

En la ilustración 13-4, 14-4, se puede observar de color verde el registro de los datos de todas las acciones que realizó el intruso cuando ingresó de forma exitosa al servidor como por ejemplo la exploración y lectura de directorios.

Tabla 7-4: Código de colores con su significado explorados por el atacante mediante usuarios y contraseñas comúnmente utilizadas

	Comando ingresado por el atacante
	Dirección del registro en nuestro computador

Realizado por: Erazo, J, 2022

```
2022-03-09 01:06:30-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] getting shell
2022-03-09 01:06:30-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] Opening TTY log: log/tty/20220309-010630-7518.log
2022-03-09 01:06:31-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] /etc/motd resolved into /etc/motd
2022-03-09 01:08:07-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] CMD: cd /
2022-03-09 01:08:07-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] Command found: cd /
2022-03-09 01:08:09-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] CMD: ls
2022-03-09 01:08:09-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] Command found: ls
2022-03-09 01:08:14-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] CMD: cd usr
2022-03-09 01:08:14-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] Command found: cd usr
2022-03-09 01:08:16-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] CMD: ls
2022-03-09 01:08:16-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] Command found: ls
2022-03-09 01:08:21-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] CMD: cd
2022-03-09 01:08:21-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] Command found: cd
2022-03-09 01:08:26-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] CMD: cd /
2022-03-09 01:08:26-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] Command found: cd /
2022-03-09 01:08:30-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] CMD: ls
HoneyPotTransport,2,192.168.101.43] CMD: exit
```

Ilustración 13-4: Registro de los datos guardados en Kippo sobre la exploración de directorios en el servidor ssh mediante el ataque de contraseñas y usuarios comúnmente utilizados

Realizado por: Erazo, J, 2022

```
2022-03-09 01:09:45-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] Command found: exit
2022-03-09 01:09:52-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] CMD: ls
2022-03-09 01:09:52-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] Command found: ls
2022-03-09 01:09:56-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] CMD: cd /
2022-03-09 01:09:56-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] Command found: cd /
2022-03-09 01:09:58-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] CMD: ls
2022-03-09 01:09:58-0800 [SSHChannel session (0) on SSHService ssh-connection on
HoneyPotTransport,2,192.168.101.43] Command found: ls
```

Ilustración 14-4: Registro de los datos guardados en Kippo de la exploración de archivos cuando se cierra sesión ssh mediante el ataque de usuarios y contraseñas comúnmente utilizadas

Realizado por: Erazo, J, 2022

4.1.3 Análisis de ataque de la máquina virtual Windows 7

A continuación, se muestran unas tablas orientativas del significado de los datos encontrados en el registro de las acciones no autorizadas de los intrusos mediante el ataque que simula ser originado por ingeniería social y luego también se muestra unas figuras que exponen los datos encontrados en el registro.

Tabla 8-4: Código de colores con su significado en el análisis del ataque mediante ataque ingeniería social

	Dirección y puerto del atacante
	Dirección y puerto del servidor
	Numero de sesiones intentadas por el atacante
	Versión remota de SSH o software que utiliza el atacante
	Nombre del servidor que ingresa el atacante
	Contraseña del servidor que ingresa el atacante
	Estado de la conexión
	Dirección de registro de movimientos

Realizado por: Erazo, J, 2022

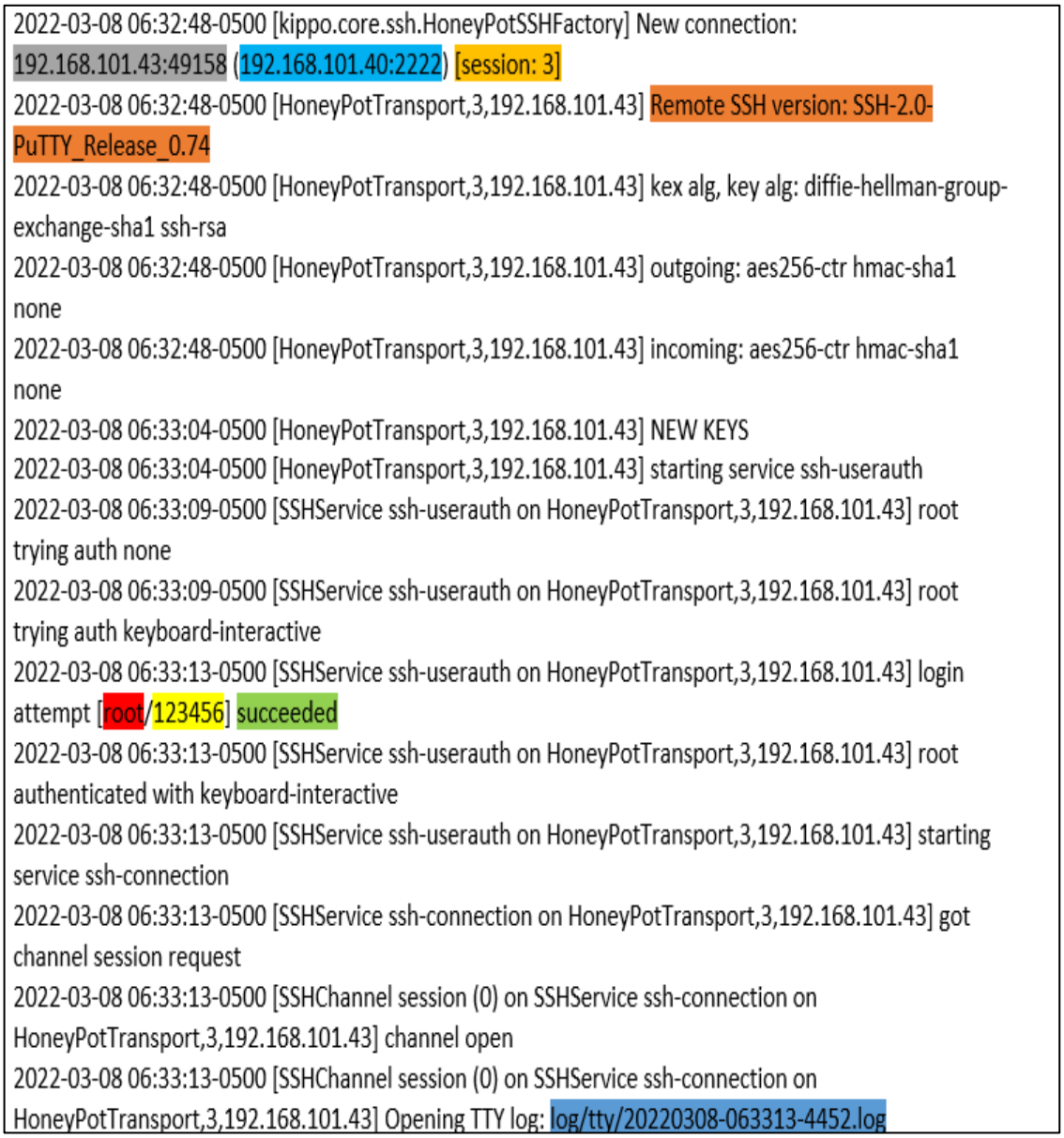


Ilustración 15-4: Registro de los datos guardados en Kippo de los ataques mediante ingeniería social

Realizado por: Erazo, J, 2022

Tabla 9-4: Código de colores con su significado explorados por el atacante mediante ataque ingeniería social.

	Comando ingresado por el atacante

Realizado por: Erazo, J, 2022

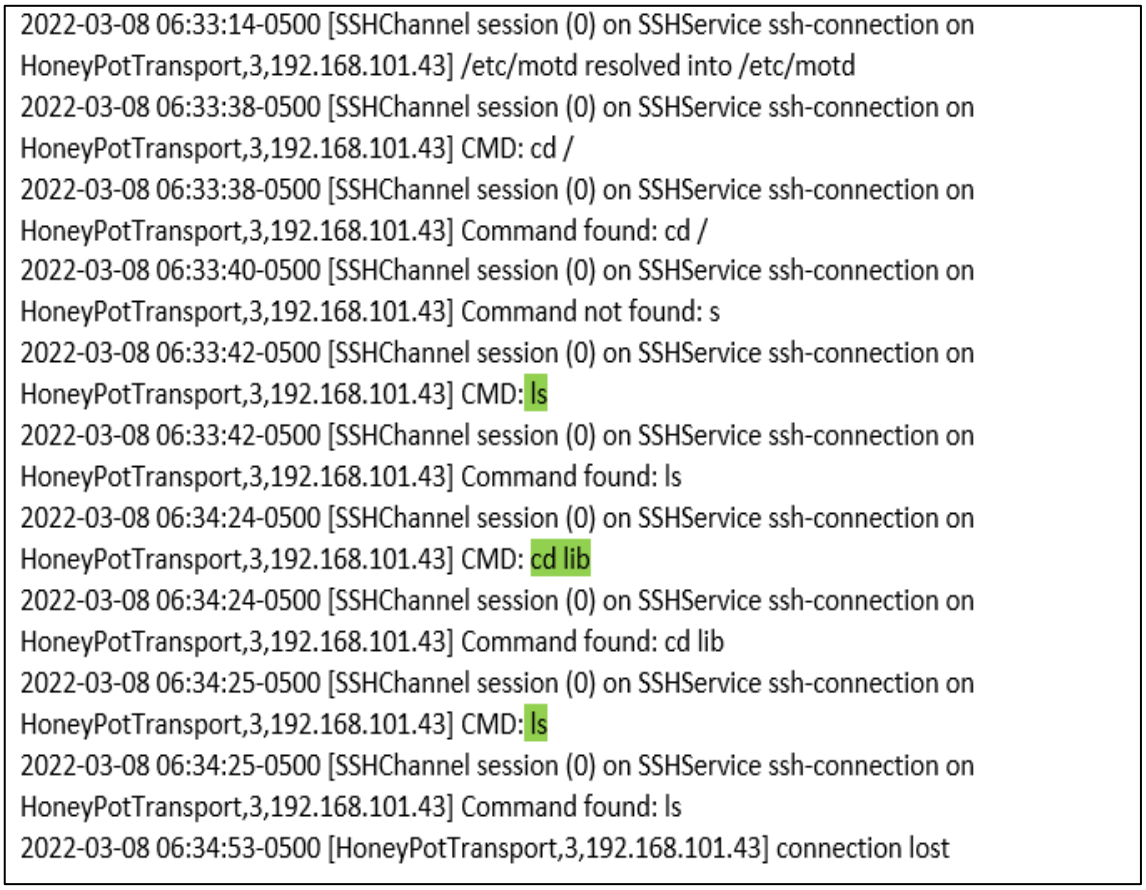


Ilustración 16-4: Registro de los datos guardados en Kippo sobre la exploración de directorios en el servidor ssh mediante el ataque de ingeniería social

Realizado por: Erazo, J, 2022

En la ilustración 15-4 se puede observar que después de 3 sesiones, se realiza la combinación de un usuario llamado “root” que se encuentra pintado de color rojo y de una contraseña llamado “123456” que se encuentra pintado de color amarrillo, el cual proporciona un estado de éxito que se encuentra pintado de color verde. También registra la dirección en donde se guarda todos los movimientos que realizó el intruso, esta dirección se encuentra pintado de color azul, el cual fue añadido a la tabla 9-4.

En la ilustración 16-4 y tomando en cuenta la tabla 9-4, se puede observar de color verde el registro de los datos de todas las acciones que realizó el intruso cuando ingresó de forma exitosa al servidor como por ejemplo la exploración y lectura de directorios.

4.2 Recomendaciones para mitigar el acceso no autorizado al protocolo ssh

Todas las recomendaciones que se van a realizar a continuación se desarrollan en el servidor ssh, para realizar los ataques y demostrar que estas recomendaciones disminuyen los ingresos no autorizados se los hace desde cualquier máquina virtual, en este caso se va a realizar desde la máquina virtual Kali linux, la arquitectura de la red se muestra en la Ilustración 1-1.

- **Crear contraseñas más seguras**

Esta recomendación es la más básica que se debe aplicar para mitigar las acciones no autorizadas de los atacantes al protocolo ssh, hoy en día se recomienda mucho que todos los usuarios sean capaces de crear contraseñas más seguras las cuales deben incluir letras tanto mayúsculas como minúsculas, además deben contener símbolos, números y pasado los 8 caracteres.
Para crear contraseñas nuevas se debe ingresar el código que se observa en la ilustración 17-4.
Lo más importante es evitar usar contraseñas que sean comunes, por ejemplo: 12345678

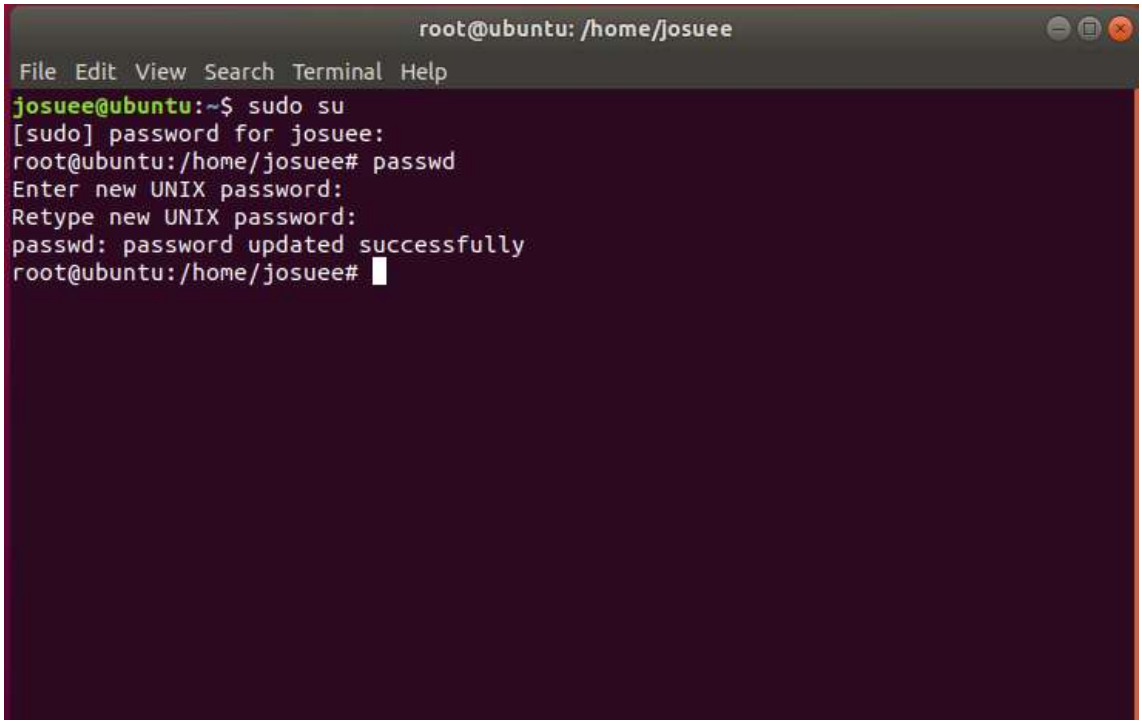


Ilustración 17-4: Código para cambiar la contraseña en el servidor SSH

Realizado por: Erazo, J, 2022

Al momento de cambiar la contraseña es posible que puedan volver a descifrar la misma, por eso es recomendable cambiarlo cada 3 meses.
Para verificar la demostración del acceso negado al servidor ssh ver la ilustración 21-4.

- **Iniciar sesiones ingresando claves ssh**

A pesar de que existen contraseñas bien seguras con caracteres especiales, puede ocurrir el riesgo de que algún día se logre romper la contraseña mediante un ataque, es por lo que la mejor solución es reemplazar los inicios de sesión que se basan en claves o llaves, que además permiten establecer una sesión más rápida e inmediata y permite realizar tareas automatizadas como transferencia de archivos.

Para esto se debe crear una clave ssh con el comando como se observa en la ilustración 18-4:

ssh-keygen

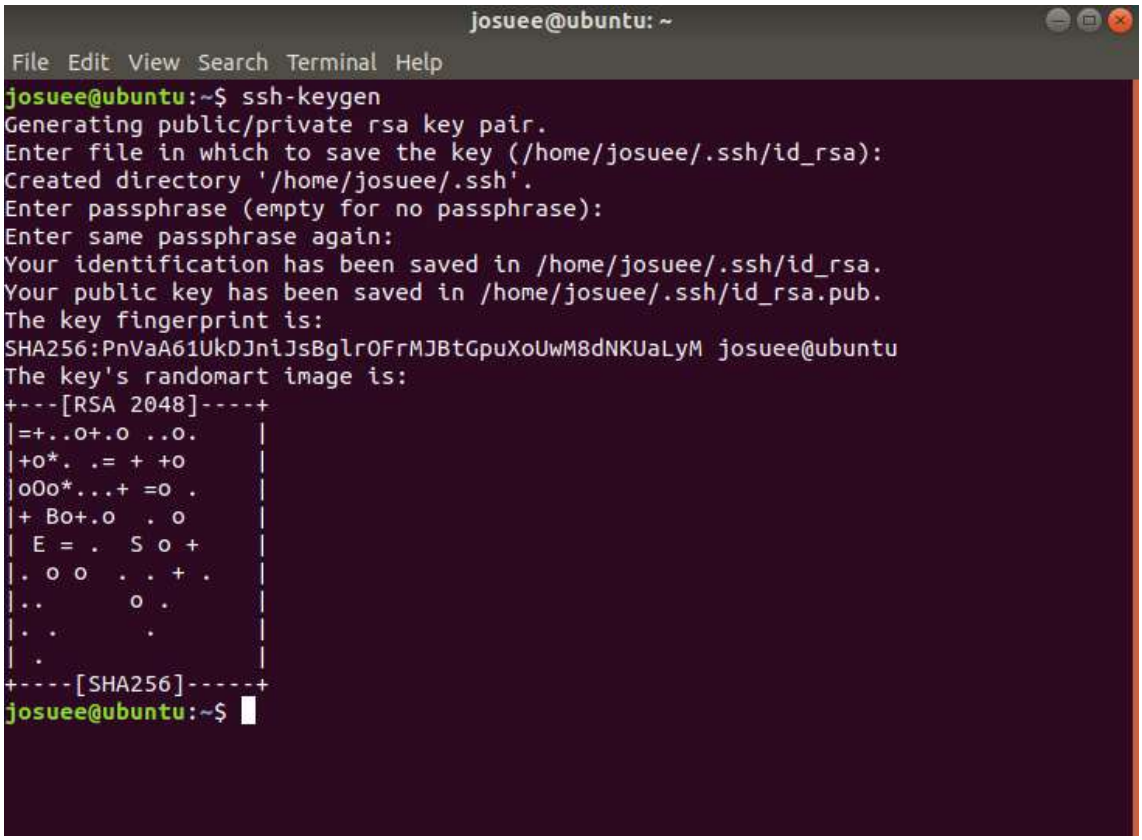


Ilustración 18-4: Código exitoso para la creación de llaves ssh

Realizado por: Erazo, J, 2022

Para verificar la demostración del acceso negado al servidor ssh ver la ilustración 21-4.

- **Deshabilitar el reenvío de puertos**

Al deshabilitar el reenvío de puertos se evita que el intruso no autorizado ingrese al puerto 22 mediante otro puerto que esté registrado en el reenvío.

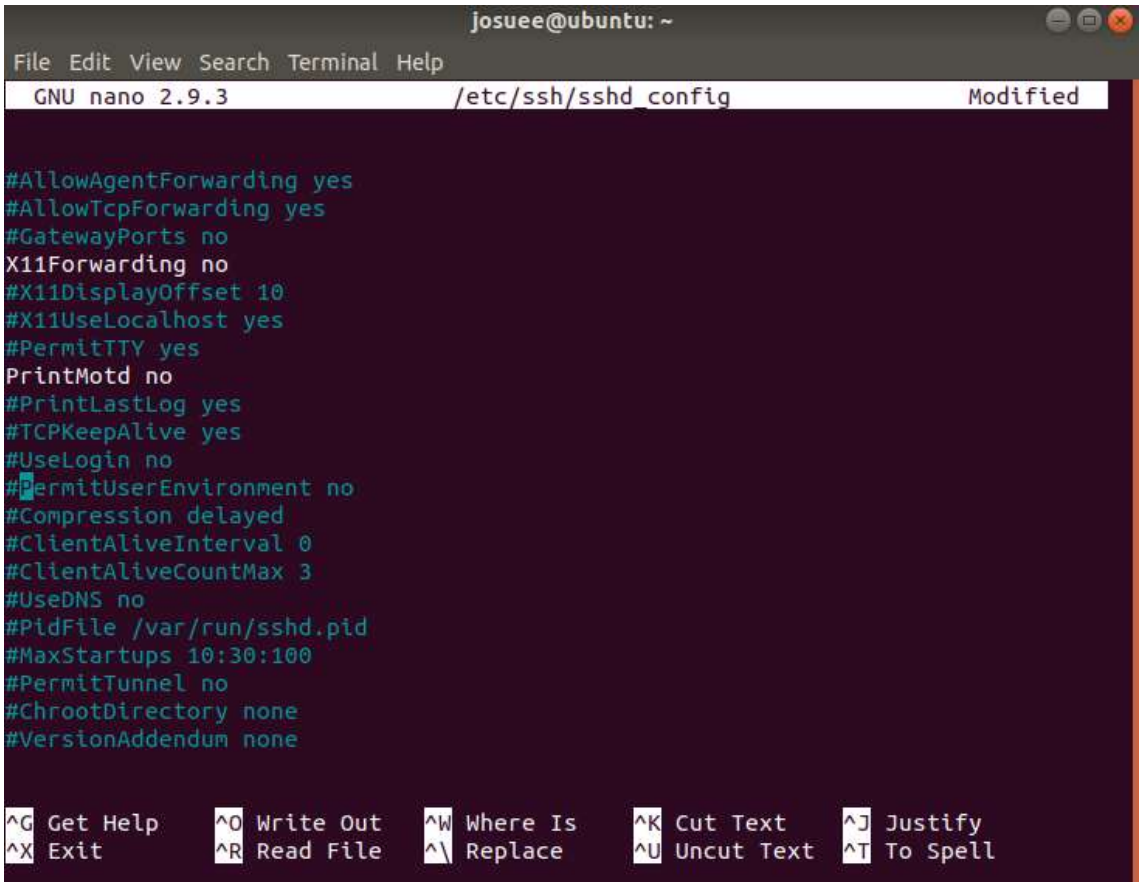


Ilustración 19-4: Código para la deshabilitar el reenvío de puertos**.**

Realizado por: Erazo, J, 2022

Para deshabilitar el reenvío de puertos se debe poner la palabra NO en después de la palabra x11Forwarding como se observa en la ilustración 19-4.

Para verificar la demostración del acceso negado al servidor ssh ver la ilustración 21-4.

- **Poner límite en los intentos de autenticación**

Esta es una excelente forma de mitigar los accesos no autorizados ya que se limita al atacante a realizar una cierta cantidad de inicios de sesión fallidos, es decir no podrá lograr utilizar todas las combinaciones del diccionario que está siendo utilizado.
MaxAuthTries es una herramienta que puede ayudar a lograr esta recomendación para lo cual aplicamos el siguiente comando:

nano -w /etc/ssh/sshd_config

y en la variable anterior mencionada se debe poner el valor de 3: MaxAuthTries 3 como se observa en la ilustración 20-4.

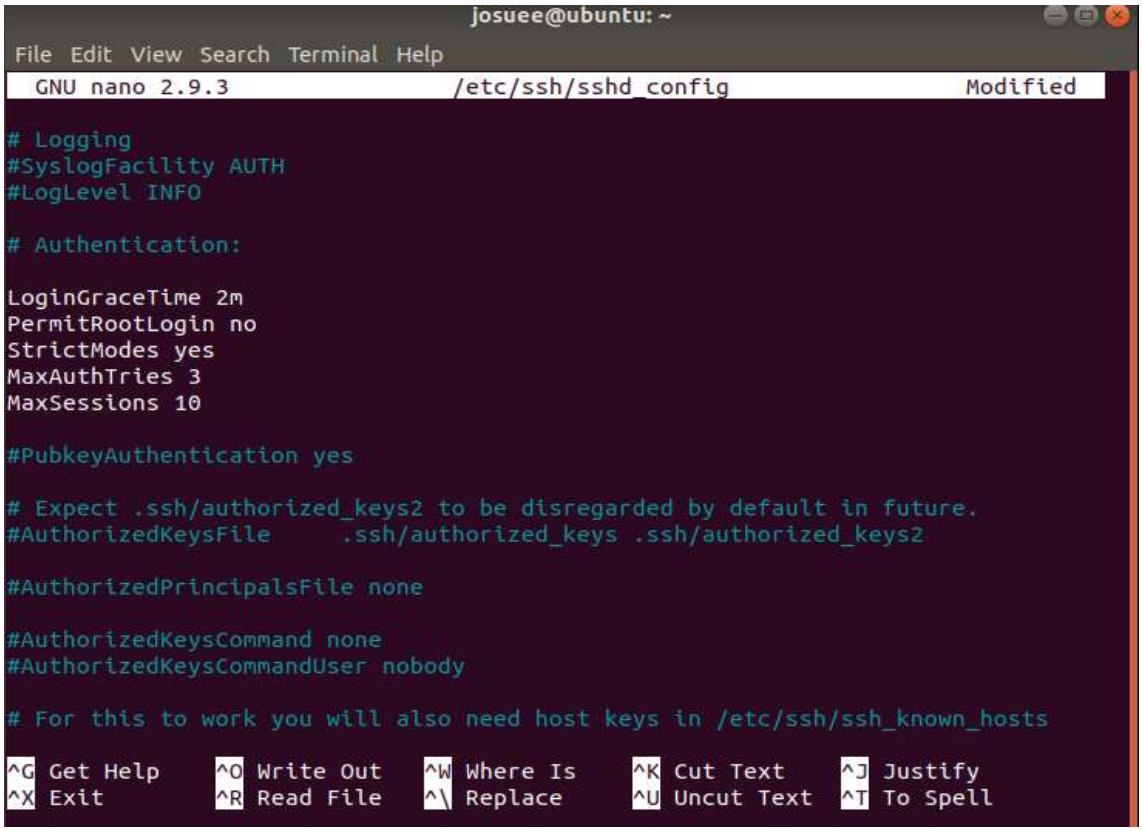


Ilustración 20-4: Código para poner límites en los intentos de autenticación

Realizado por: Erazo, J, 2022

Para verificar la demostración del acceso negado al servidor ssh ver la ilustración 21-4.

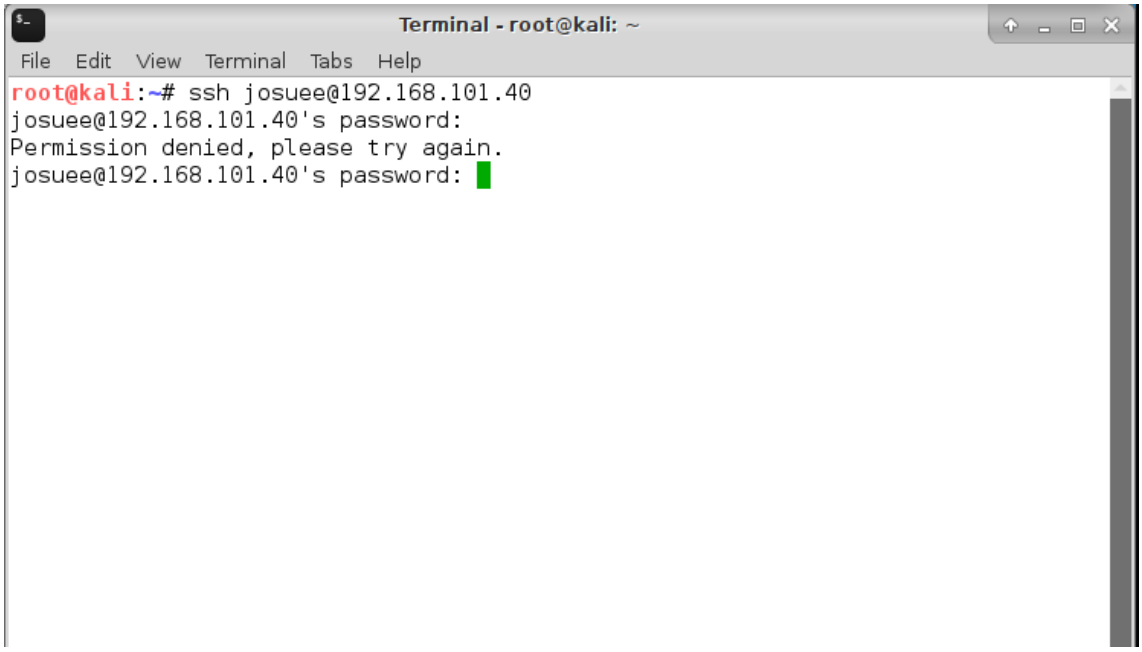


Ilustración 21-4: Acceso negado al servidor ssh desde la máquina virtual Kali Linux.

Realizado por: Erazo, J, 2022

- **Deshabilitar el inicio de sesión de forma root**

A pesar de tener configurado el puerto 22 de forma predeterminada, en la mayoría de los servidores ssh tienen la forma de iniciar sesión mediante root, esto es muy peligroso porque el atacante puede usar esta forma para acceder al puerto 22 y comenzar a realizar los ataques por fuerza bruta y peor aun cuando la contraseña de autenticación es débil.

Es por esto que se debe editar el archivo de configuración de ssh con el comando:

nano -w /etc/sshd_config

Luego se busca la variable PermitRootLogin y le ponemos la palabra No como se observa en la ilustración 22-4.

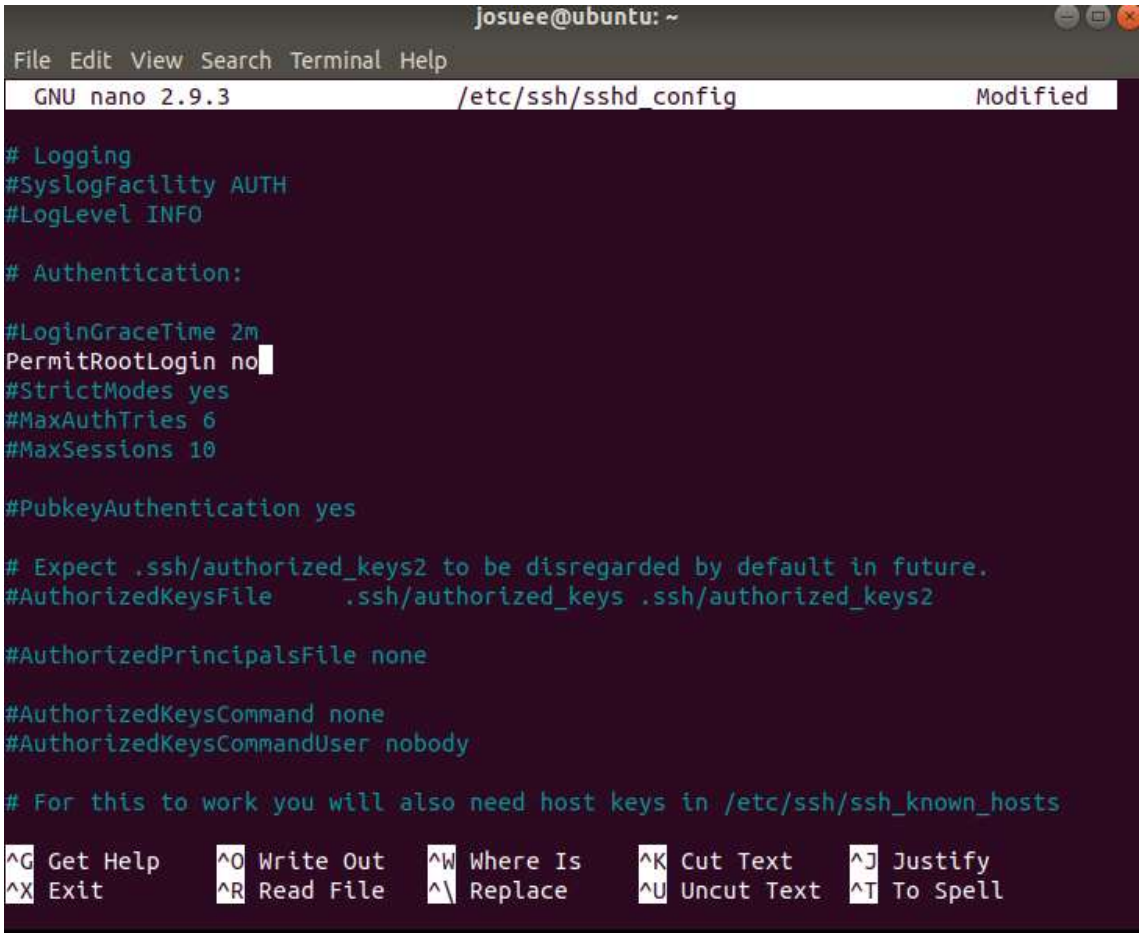


Ilustración 22-4: Código para deshabilitar el inicio de sesión de forma root

Realizado por: Erazo, J, 2022

Para verificar la demostración del acceso negado al servidor ssh ver la ilustración 21-4.

- **Bloquear automáticamente los ataques que llegan mediante fuerza bruta**

Si se llega a dar cuenta que tuvo un ataque de fuerza bruta, la mejor manera de detenerlo es bloqueando la dirección IP por donde están realizando el ataque, para saber de dónde proviene el ataque se tiene que revisar los registros y luego bloquear mediante el firewall.
Debido al costo del software no fue posible la adquisición para la demostración.

- **Cambiar el puerto ssh que viene por defecto**

Esta recomendación es una de las más antiguas y seguras que se debe realizar ya que los servidores ssh vienen dado por defecto en el puerto 22 y esto es conocido por muchos intrusos no autorizados y también por las herramientas de testeo que lanzan ataques de diccionario o también llamado fuerza bruta, al cambiarlo por otro como por ejemplo 685 como se observa en la ilustración 23-4, se evita que los atacantes ingresen al sistema mediante el puerto 22 y sea difícil de encontrar el nuevo puerto.

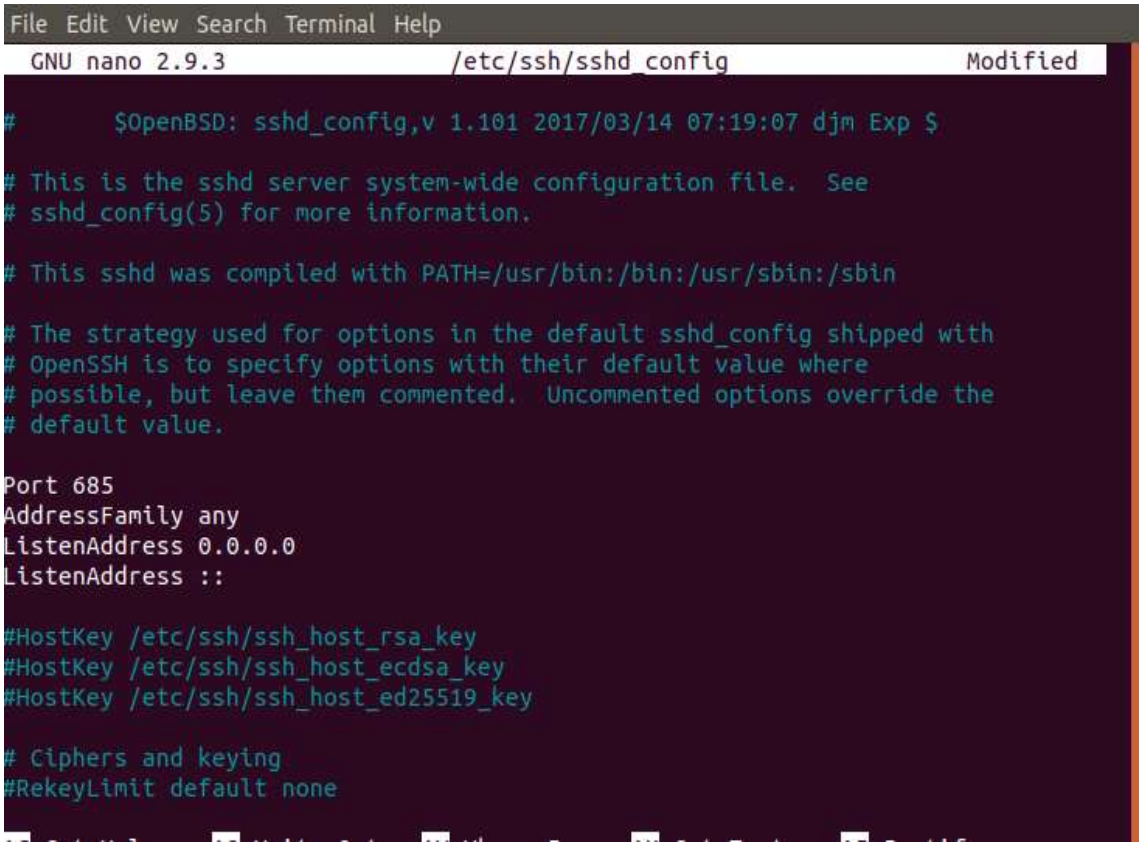


Ilustración 23-4: Código para cambiar el puerto ssh que viene por defecto.

Realizado por: Erazo, J, 2022

Para verificar que el puerto ssh está cambiado, se realiza un ingreso al servidor ssh y sale un mensaje de conexión rechazada como se observa en la ilustración 24-4.

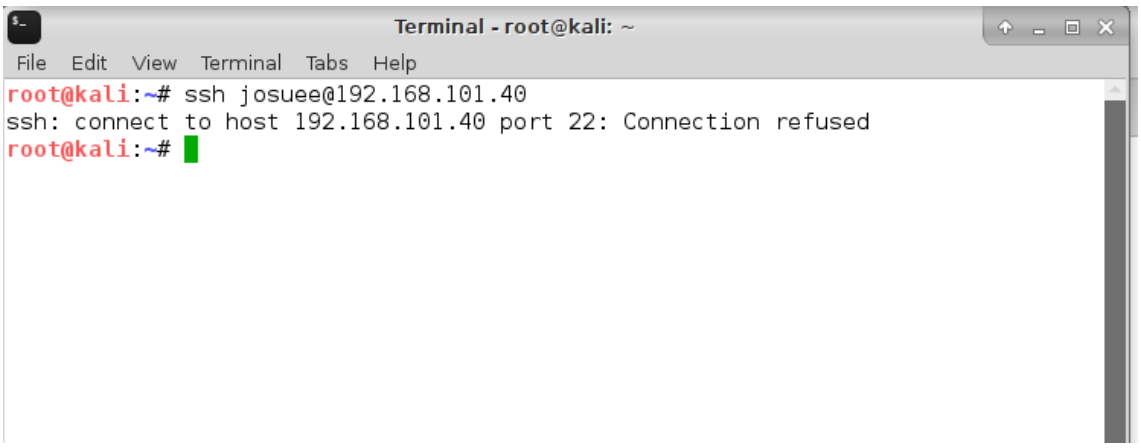


Ilustración 24-4: Acceso negado al servidor SSH por cambio de puerto

Realizado por: Erazo, J, 2022

- **Filtrar el puerto ssh en el firewall**

Es recomendable filtrar el puerto ssh mediante un firewall de software ya que es una de las cosas más básicas que se debe configurar cuando se instala un sistema operativo o servidor, por ejemplo, un firewall muy conocido es el CSF que es fácil de instalar y filtrar los puertos.
Lo primero es editar el archivo csf.conf con el comando: nano -w /etc/csf/csf.conf
Luego se busca las variables con el comando:

#Allow incoming TCP ports
TCP_IN = « 23,80,685 »

Agregamos nuestro puerto ssh a esta lista de puertos y con eso ya está filtrado.
Debido al costo del software no fue posible la adquisición para la demostración.

- **Deshabilitar el servidor openssh en computadores personales**

Es recomendable deshabilitar el servidor ssh en algunas distribuciones Linux que vienen habilitadas de manera predeterminada, esto puede causar muchos problemas ya que tiene habilitado el inicio de sesión mediante root y se escucha en el puerto 22.
Por ejemplo, en sistemas operativos basados en Linux se puede aplicar el siguiente comando como se observa en la ilustración 25-4:

sudo apt-get remove opensss-server

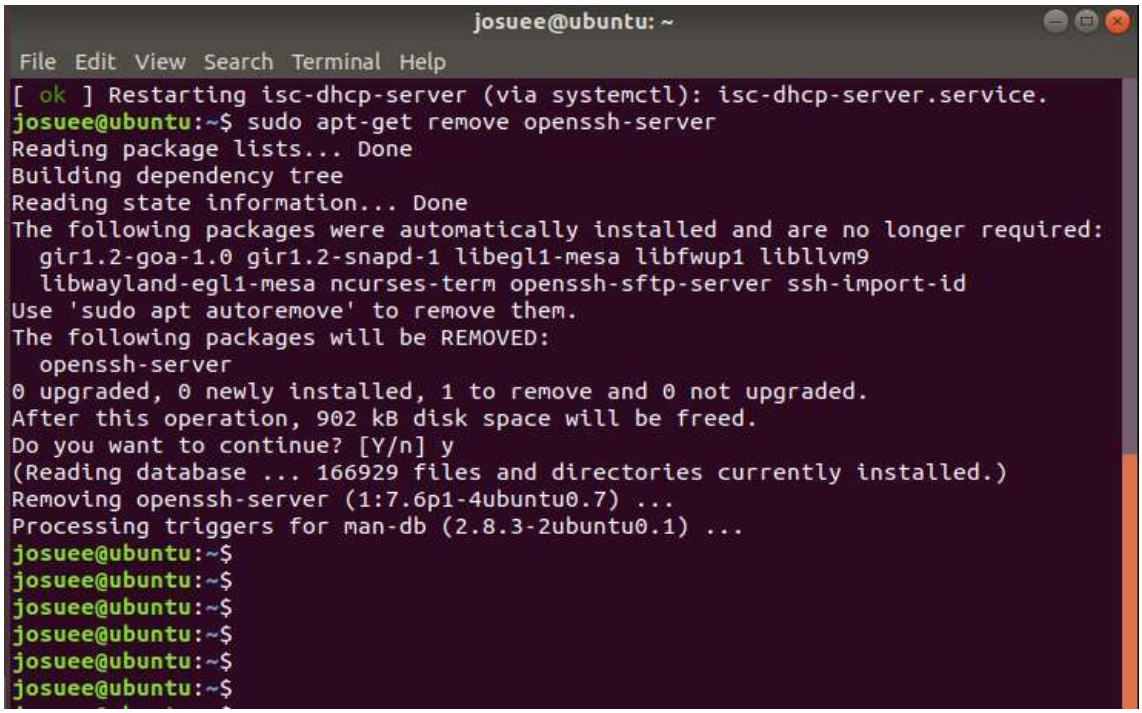


Ilustración 25-4: Código para remover el servidor openssh en computadores personales.

Realizado por: Erazo, J, 2022

Para verificar que el servidor openssh está deshabilitado, se realiza un escaneo de la red el cual muestra que no existe ningun servidor ssh ni tampoco un puerto 22 como se observa en la ilustración 26-4.

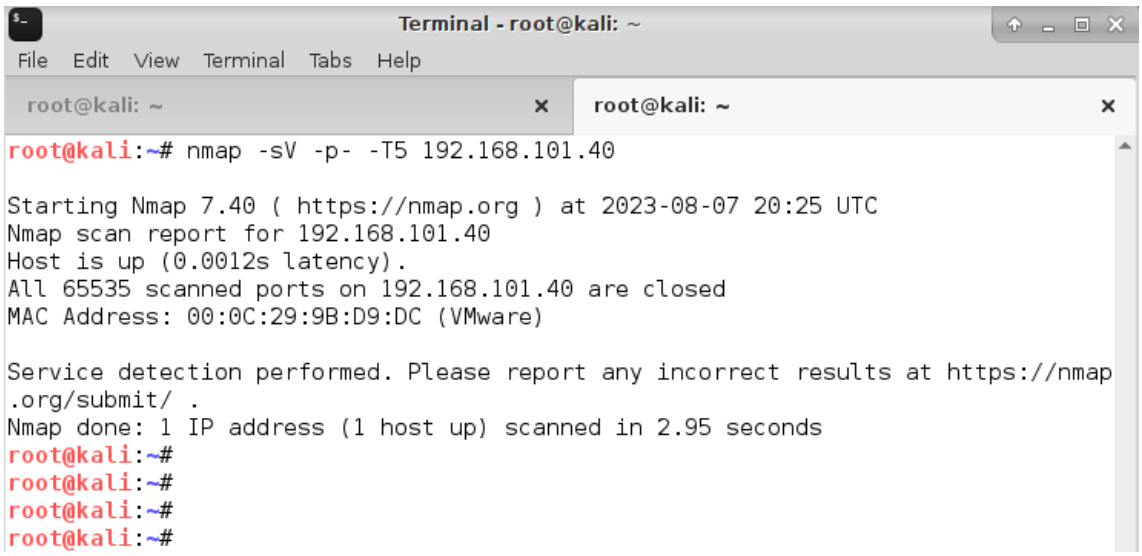


Ilustración 26-4: Escaneo de la red para verificar que no está activo el servidor openssh

Realizado por: Erazo, J, 2022

- **Mantener siempre actualizado ssh**

Y, por último, una recomendación básica, mantener siempre actualizado los paquetes del servidor ssh y el openssh

En distribuciones Linux se puede aplicar el siguiente comando como se observa en la ilustración 27-4:

apt-get update openssh-server

con esto se mantiene siempre protegido al servidor ssh contra nuevas vulnerabilidades.

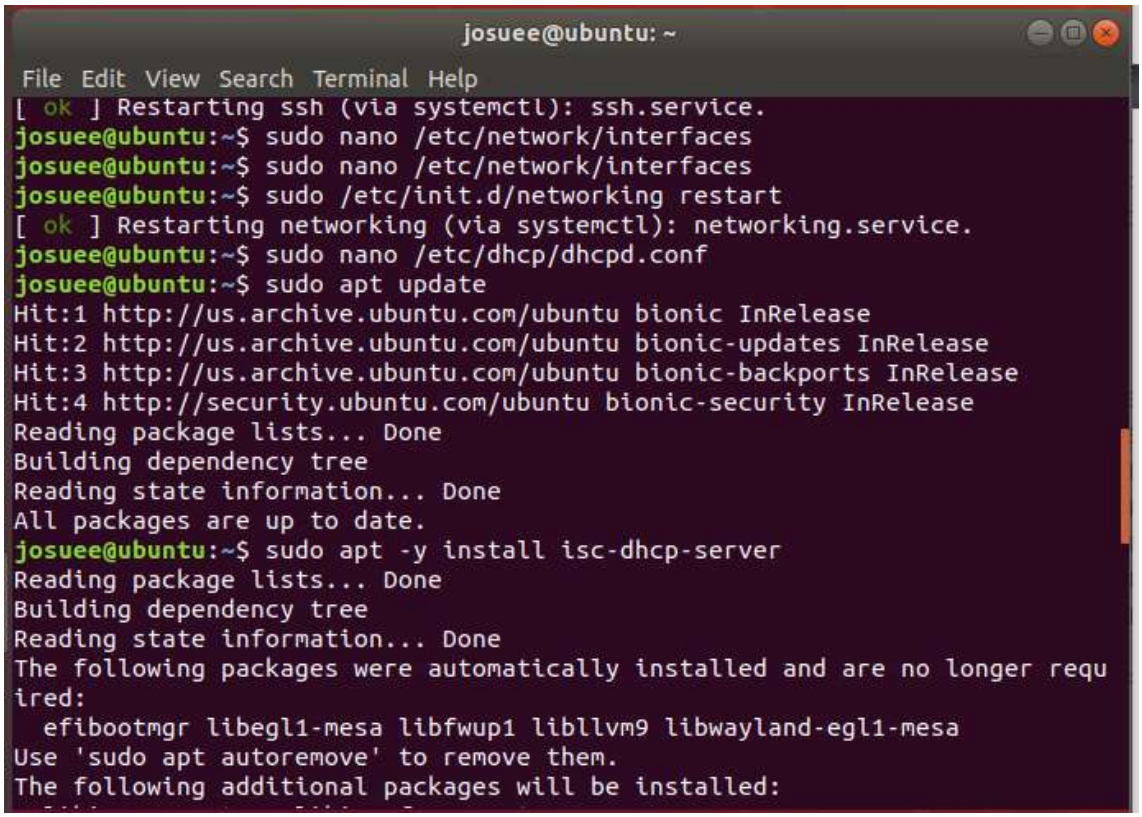


Ilustración 27-4: Código para actualizar el servidor ssh

Realizado por: Erazo, J, 2022

Al aplicar todas estas recomendaciones se puede llegar a disminuir futuras intrusiones y de esta manera se mitiga las acciones no autorizadas de los intrusos al protocolo ssh.

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Se ha implementado con éxito un honeypot mediante Kippo, además, a través de pruebas de testeo y ataques por hacking se logró realizar recomendaciones para de esta manera mitigar las acciones no autorizadas de los intrusos al protocolo ssh.

Para mitigar el acceso al protocolo ssh, es necesario crear contraseñas más seguras y claves ssh, cambiar el puerto ssh que viene por defecto, bloquear automáticamente los ataques que llegan por fuerza bruta, deshabilitar el servidor openssh en computadores personales y sobre todo mantener siempre actualizado ssh.

Se obtuvo toda la información necesaria de las vulnerabilidades del protocolo ssh en accesos no autorizados, de la misma manera conceptos básicos de un honeypot y la correcta configuración de Kippo, además de la investigación de algunas metodologías de seguridad que son utilizadas en la rama de la ciberseguridad.

Para la aplicación de este proyecto técnico, entre las metodologías investigadas, se utilizó el estándar de ejecución de pruebas de penetración, el cual es más utilizado y cubre casi todo lo relacionado con las pruebas de penetración, así como también sus respectivas herramientas de testeo.

Se diseñó y desarrolló un escenario de pruebas con el cual se realizó los ataques; consiguiendo de esta manera observar las vulnerabilidades que presenta nuestro servidor, llegando a la conclusión que los honeypots pueden ser usados con el propósito de detectar y disminuir los ataques, ayudando a los administradores de redes y seguridad recopilar información necesaria sobre las amenazas para defenderse de los atacantes.

Al tener instalado y configurado correctamente el honeypot Kippo en el servidor, este garantiza que todas las acciones realizadas por el atacante queden registradas y almacenadas en un archivo, posteriormente se realiza el análisis de los datos obtenidos lo cuales son fáciles de interpretar y así observar todo lo que el intruso ejecutó en el servidor, para de esta manera establecer varias

recomendaciones para disminuir ataques y que futuros intrusos ingresen mediante el protocolo ssh.

Los ataques más conocidos y ejecutados al protocolo ssh son: los ataques por fuerza bruta o también llamado por diccionario, así como también los ataques que son realizados mediante los usuarios y contraseñas que generalmente son usados en los servidores ssh, y por último ataques que son originados por ingeniería social.

5.2 Recomendaciones

Para la creación de los entornos virtuales utilizados en este proyecto es necesario seguir los pasos tal y como se muestran en este documento, de esta manera su ejecución será exitosa sin ningún problema.

Verificar que las máquinas virtuales instaladas tengan conectividad y estén haciendo ping entre todas, además se debe tener en cuenta que para descargar las actualizaciones o algunos comandos que no vienen instalados en el servidor ubuntu, es necesario una conexión a internet.

Para un correcto manejo en la instalación del honeypot Kippo, se debe tener conocimiento sobre Python que es uno de los lenguajes de programación más usados actualmente, así como también conocer comandos básicos utilizados en las herramientas de testeo o configuraciones de redes.

Instalar correctamente Kippo en el servidor Ubuntu, ya que, si el honeypot no funciona de la manera esperada, todas las acciones de los atacantes no quedan registradas en los archivos, y este no podría ser visualizado por el administrador de seguridad; por lo tanto, sería perjudicial porque los intrusos estarían pasando desapercibidos haciendo daño a los datos de los servidores.

Cambiar el último objetivo específico para que se refleje con el objetivo principal que se trata de mitigar las acciones no autorizadas de los intrusos al protocolo ssh.

BIBLIOGRAFÍA

BARRETT, D.J., SILVERMAN, R.E. y BYRNES, R.G., 2005. *SSH, the Secure Shell The Definitive Guide*. Second. United States of America: O'Reilly Media, Inc. ISBN 0-596-00895-3.

CASTRO GUERRERO, C.A., 2011. *Implementación de un honeypot mediante KIPPO para detectar acciones de un atacante al ganar acceso por SSH para mejorar la seguridad en la red de un servidor*. S.l.: universidad del azuay.

GITHUB, 2022. desaster/kippo. [en línea]. Disponible en: https://github.com/desaster/kippo.

GITHUB, 2022a. Making Kippo Reachable. [en línea]. Disponible en: https://github.com/desaster/kippo/wiki/Making-Kippo-Reachable.

GITHUB, 2022b. Running Kippo. [en línea], Disponible en: https://github.com/desaster/kippo/wiki/Running-Kippo.

HERZOG, P., 2010. *OSSTMM 3 The Open Source Security Testing Methodology Manual* [en línea]. S.l.: ISECOM. Disponible en: https://www.isecom.org/OSSTMM.3.pdf.

JOSHI, R.. y SARDANA, A., 2011. *Honeypots A New Paradigm to Information Security*. USA: Science Publishers. ISBN 978-1-57808-708-2.

MOHAMMED, M. y REHMAN, H., 2016. *Honeypots and Routers Collecting Internet Attacks*. USA: Taylor & Francis Group. ISBN 13: 978-1-4987-0220-1.

RAHALKAR, S. y JASWAL, N., 2019. *The Complete Metasploit Guide*. Birmingham-UK: Packt Publishing. ISBN 978-1-83882-247-7.

SANDERS, C. y SMITH, J., 2014. *Applied Network Security Monitoring Collection, Detection, and Analysis*. USA: Syngress. ISBN 978-0-12-417208-1.

SHARMA, H. y SINGH, H., 2018. *Hands-On Red Team Tactics A practical guide to mastering Red Team operations*. Birmingham-UK: Packt Publishing. ISBN 978-1-78899-523-8.

SINGH, G.D., 2019. *Learn Kali Linux 2019 Perform powerful penetration testing using Kali Linux, Metasploit, Nessus, Nmap, and Wireshark*. Birmingham-UK: Packt Publishing. ISBN 978-1-78961-180-9.

SINGH, H. y SHARMA, H., 2020. *Hands-On Web Penetration Testing with Metasploit* [en línea]. Birmingham: Packt Publishing. ISBN 978-1-78995-352-7. Disponible en: https://learning.oreilly.com/library/view/hands-on-web-penetration/9781789953527/.

SPITZNER, L., 2002. *Honeypots: Tracking Hackers*. S.l.: Addison Wesley Professional. ISBN 0-321-10895-7.

SSH.COM, 2021a. OpenSSH: SSH key management needs attention. [en línea]. Disponible en: https://www.ssh.com/academy/ssh/openssh.

SSH.COM, 2021b. Password and credentials related breaches. [en línea]. Disponible en: https://www.ssh.com/academy/password-credential-breaches.

SSH.COM, 2021c. SSH threat advisory: GoScanSSH. *2021* [en línea]. Disponible en: https://www.ssh.com/academy/attack/goscanssh.

TORRES GARCIA, D.F. y ZAMBRANO NUÑEZ, P.S., 2011. *implementacion de un sistema de detección y analisis de intrusiones no autorizadas utilizando honeypots caso practico desitel-espoch*. S.l.: escuela superior politecnica de chimborazo.

WIKILEAKS, 2017. BothanSpy y Gyrfalcon. *2017* [en línea]. Disponible en: https://wikileaks.org/vault7/#BothanSpy.

ANEXOS

ANEXO D: CONFIGURACIÓN E INSTALACIÓN MÁQUINA VIRTUAL UBUNTU 18.04.4

Para la configuración e instalación de la máquina virtual Ubuntu se realizan los siguientes pasos: Se crea una máquina virtual, seleccionamos la configuración recomendada y por último se selecciona desde donde va a ser instalada, ya sea desde un dvd o una imagen iso (ver ilustración 1-0).

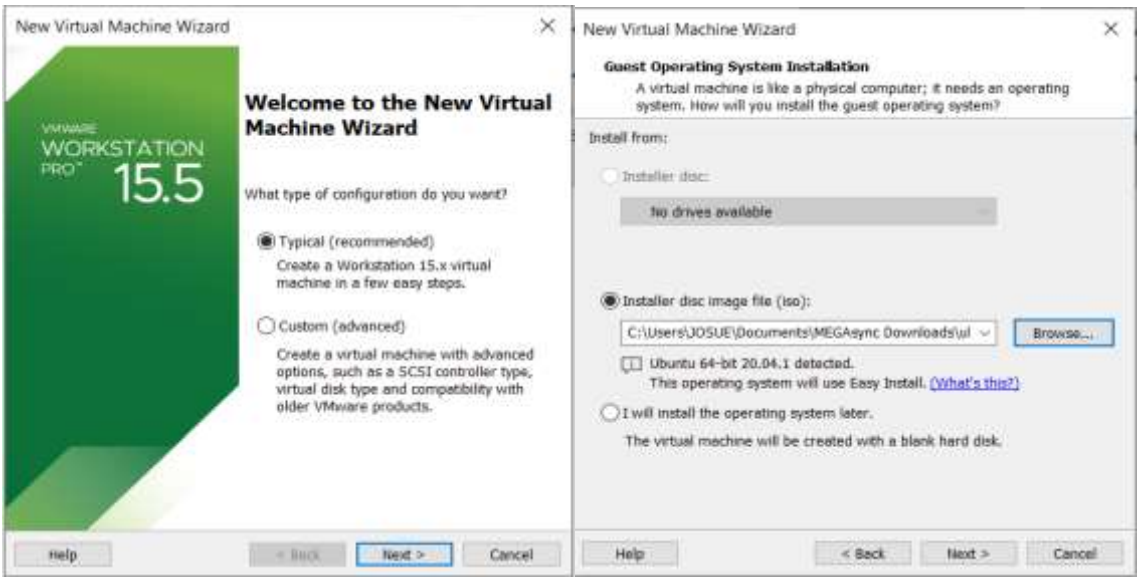


Ilustración 1-0: Selección del tipo de máquina virtual y método de instalación de Ubuntu

Realizado por: Erazo, J, 2022

Se selecciona el nombre de usuario y la contraseña (ver ilustración 2-0):

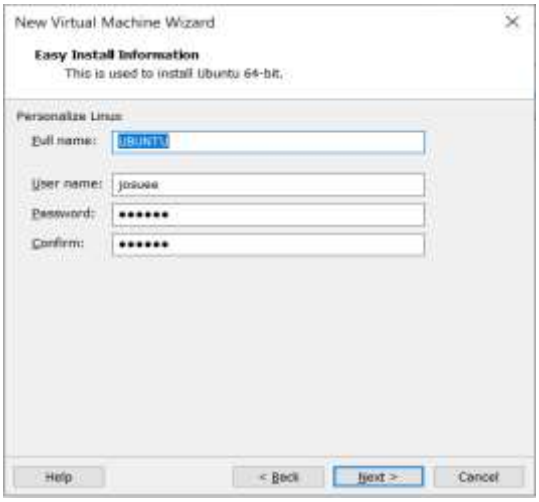


Ilustración 2-0: Nombre, usuario y contraseña de la máquina virtual Windows 7

Realizado por: Erazo, J, 2022

Por último, se selecciona el tamaño del disco duro y se verifica las configuraciones de red, en este caso será adaptador brigded (puente) que viene por defecto, de esta manera tenemos una conexión de ping hacia todas las máquinas virtuales existentes, después aplastar el botón finish (ver ilustración 3-0).

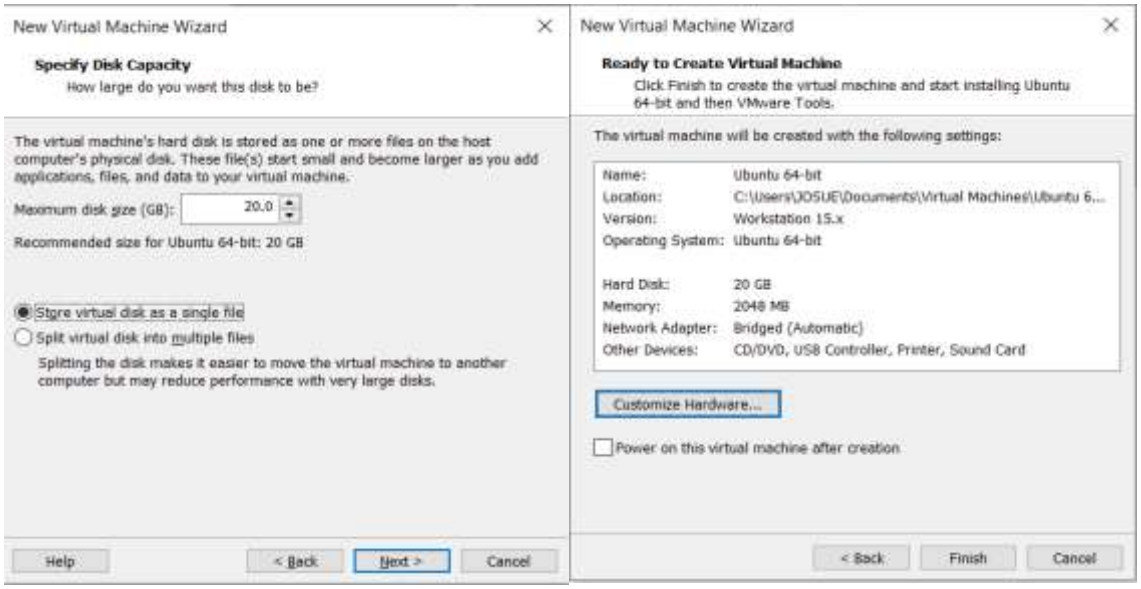


Ilustración 3-0: Capacidad de disco y resumen de configuración de la máquina virtual de Ubuntu

Realizado por: Erazo, J, 2022

Se espera un momento a que cargue el sistema operativo el cual se instala automáticamente

Al final ingresamos el usuario y contraseña creada anteriormente para iniciar sesión (ver ilustración 4-0).

Ilustración 4-0: Pantalla de inicio de sesión de la máquina virtual Ubuntu

Realizado por: Erazo, J, 2022

ANEXO E: CONFIGURACIÓN E INSTALACIÓN MÁQUINA VIRTUAL KALI LINUX

Para la configuración e instalación de la máquina virtual Kali Linux se realizan los siguientes pasos:

Se crea una máquina virtual, seleccionamos la configuración recomendada y por último se selecciona desde donde va a ser instalada, ya sea desde un dvd o una imagen iso (ver ilustración 5-0).

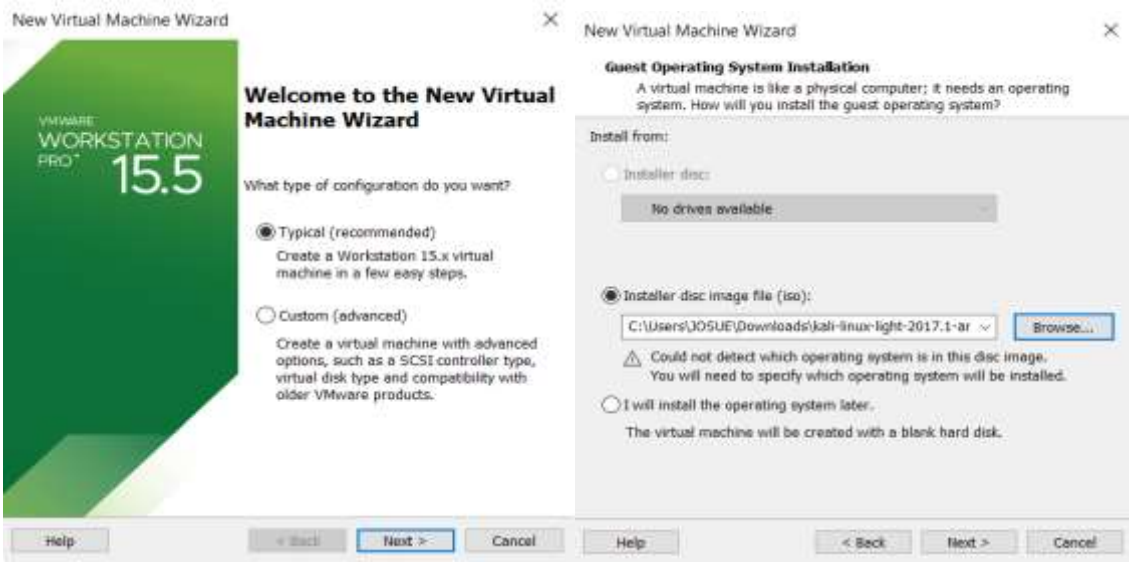


Ilustración 5-0: Selección del tipo de máquina virtual y método de instalación de Kali Linux

Realizado por: Erazo, J, 2022

Se selecciona el tipo de sistema operativo y la versión, además se le da un nombre a la máquina virtual que será creada y su ubicación en el disco duro (ver ilustración 6-0).

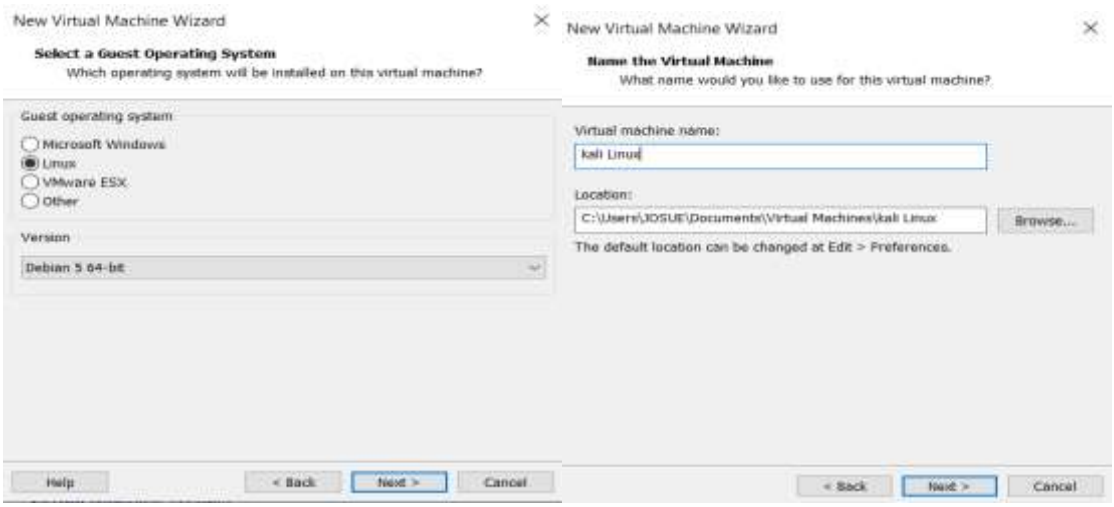


Ilustración 6-0: Selección versión de sistema operativo y nombre de la máquina virtual

Realizado por: Erazo, J, 2022

Después, se selecciona el tamaño del disco duro y se verifica las configuraciones de red, en este caso será adaptador brigded (puente) que viene por defecto, de esta manera tenemos una conexión de ping hacia todas las máquinas virtuales existentes y también es esencial para las direcciones del servidor dhcp que será utilizado, después aplastar el botón finish (ver ilustración 7-0).

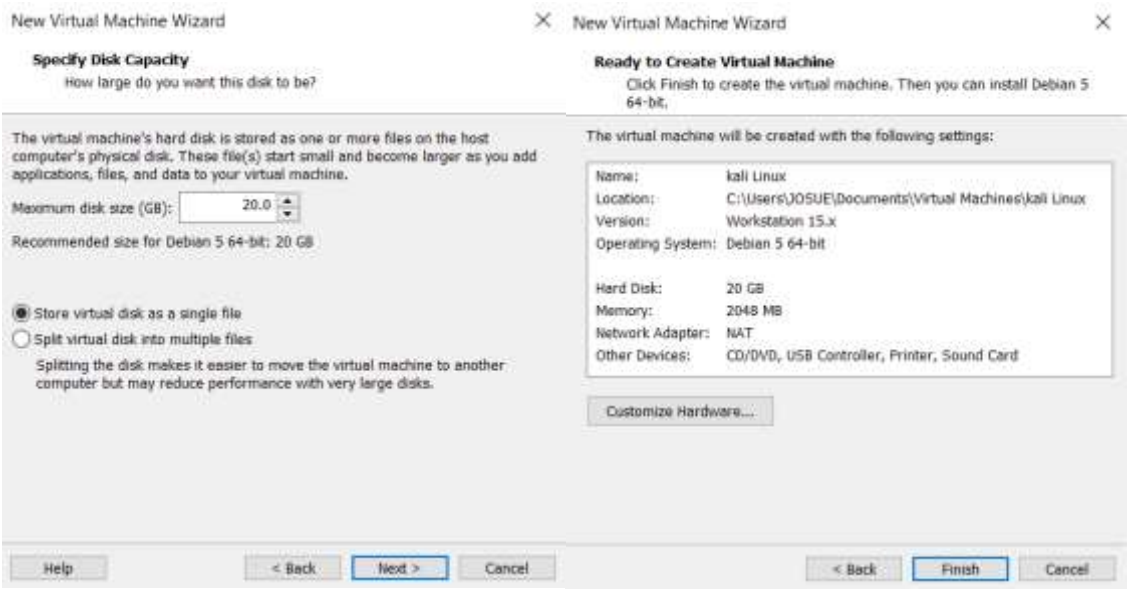


Ilustración 7-0: Capacidad de disco y resumen de configuración de la máquina virtual Kali Linux

Realizado por: Erazo, J, 2022

Por último, se elige la versión en la cual queremos iniciar el sistema operativo e ingresamos los datos de inicio de sesión (ver ilustración 8-0):

Usuario: root

Contraseña: toor

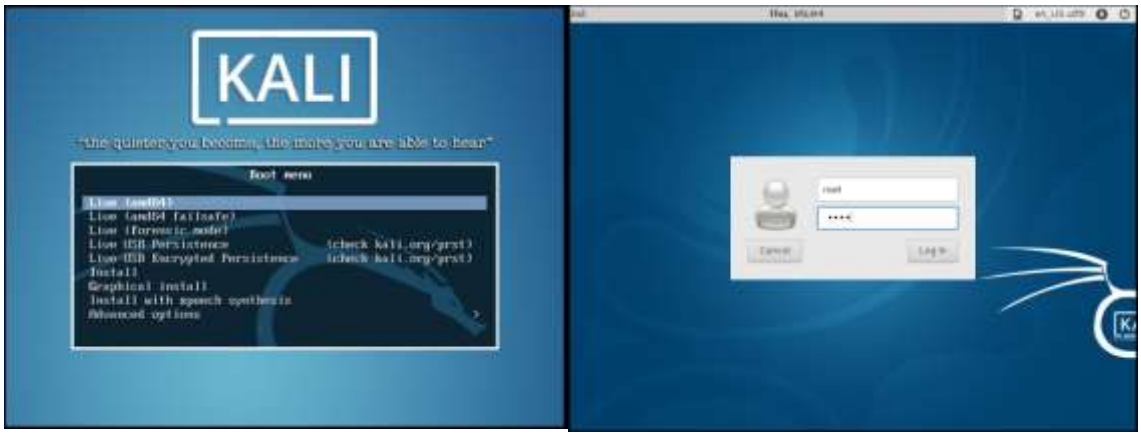


Ilustración 8-0: Elección de versión de Kali Linux y Pantalla de inicio de sesión

Realizado por: Erazo, J, 2022

ANEXO F: CONFIGURACIÓN E INSTALACIÓN MÁQUINA VIRTUAL CENTOS

Para la configuración e instalación de la máquina virtual centOs se realizan los siguientes pasos: Se crea una máquina virtual, seleccionamos la configuración recomendada y por último se selecciona desde donde va a ser instalada, ya sea desde un dvd o una imagen iso (ver ilustración 9-0).

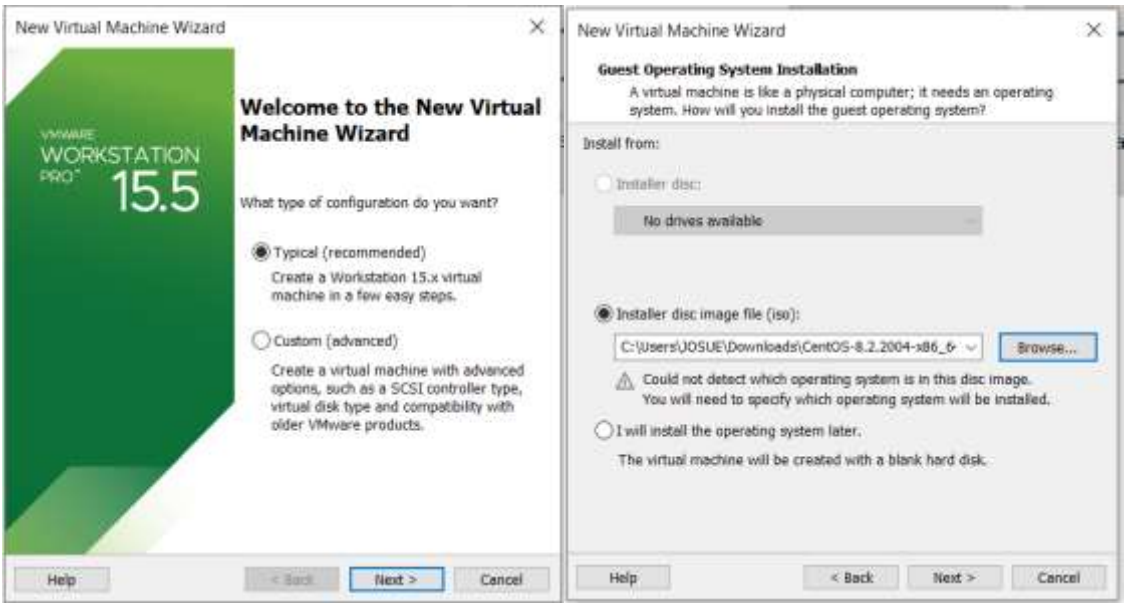


Ilustración 9-0: Selección del tipo de máquina virtual y método de instalación de Kali Linux

Realizado por: Erazo, J, 2022

Luego, se ingresa el nombre de usuario y la contraseña que servirá como inicio de sesión, además se ingresa el nombre y ubicación de la máquina virtual que va a ser creada (ver ilustración 10-0).

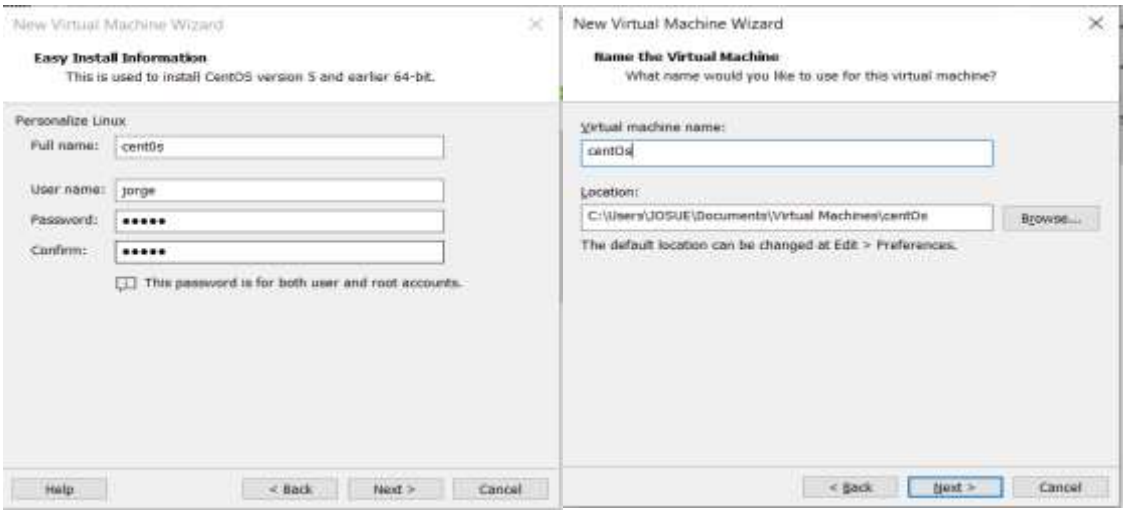


Ilustración 10-0: Ingreso de nombre de usuario y contraseña de creación de Kali Linux

Realizado por: Erazo, J, 2022

Por último, se selecciona el tamaño del disco duro y se verifica las configuraciones de red, en este caso será adaptador brigded (puente) que viene por defecto, de esta manera tenemos una conexión de ping hacia todas las máquinas virtuales existentes y también es esencial para las direcciones del servidor dhcp que será utilizado, después aplastar el botón finish (ver ilustración 11-0).

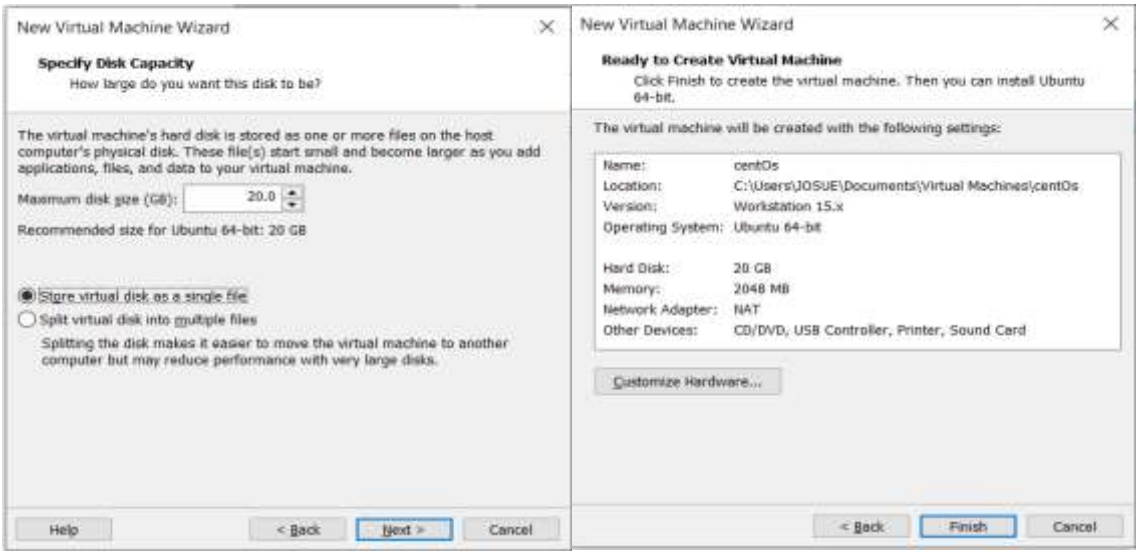


Ilustración 11-0: Capacidad de disco y resumen de configuración de la máquina virtual Kali Linux

Realizado por: Erazo, J, 2022

A continuación, se ejecuta el sistema operativo y la instalación se realiza automáticamente. Elegimos el idioma y país donde será instalado el sistema operativo (ver ilustración 12-0).

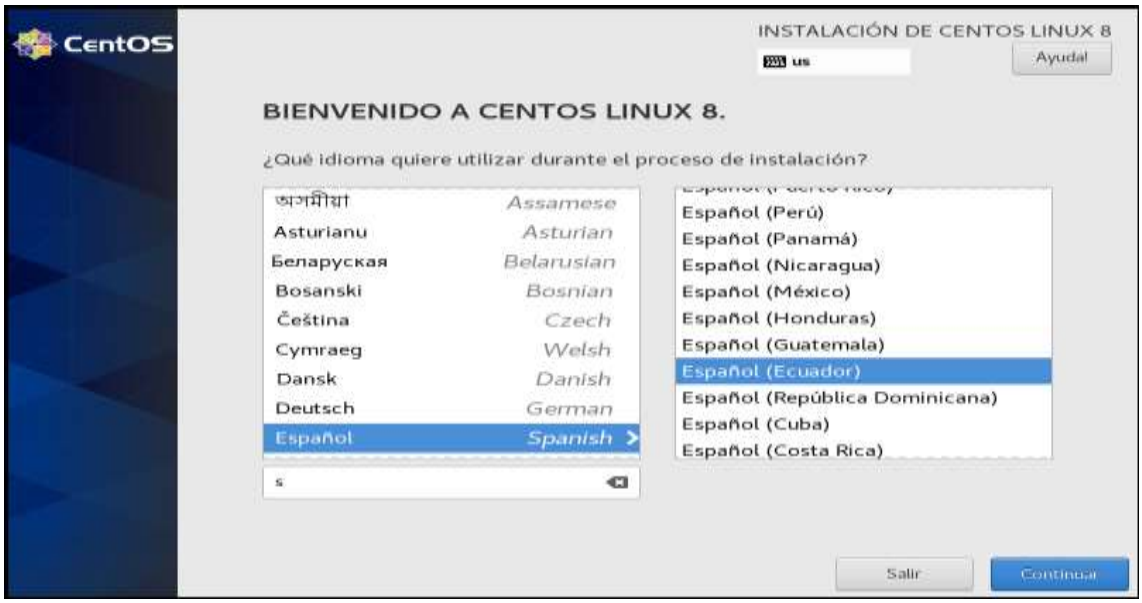


Ilustración 12-0: Selección de idioma y país para la instalación

Realizado por: Erazo, J, 2022

Por último, se realiza algunas configuraciones adicionales para que esté instalado correctamente (ver ilustración 13-0).

Ilustración 13-0: Configuraciones adicionales para la instalación de centos

Realizado por: Erazo, J, 2022

Para ingresar al sistema operativo se utiliza los siguientes datos:
Usuario: jorge
Contraseña: jorge

ANEXO G: CONFIGURACIÓN E INSTALACIÓN MÁQUINA VIRTUAL WINDOWS 7

Para la configuración e instalación de la máquina Windows se realizan los siguientes pasos:
Se crea una máquina virtual, seleccionamos la configuración recomendada y por último se selecciona desde donde va a ser instalada, ya sea desde un dvd o una imagen iso (ver ilustración 14-0).

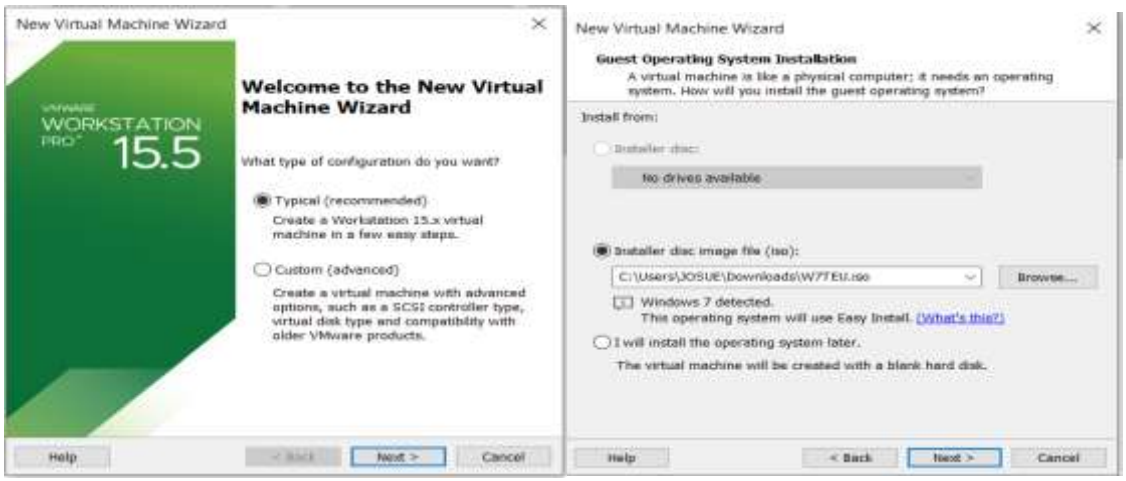


Ilustración 14-0: Selección del tipo de máquina virtual y como será instalado el sistema operativo

Realizado por: Erazo, J, 2022

A continuación, se introduce la llave del producto de la versión de Windows que va a ser utilizada, se selecciona el nombre de usuario y contraseña deseada (ver ilustración 15-0), en este caso:

Usuario: LEONARDO

Contraseña: leonardo

Se selecciona el nombre de la máquina virtual, que por defecto viene dado en Windows 7

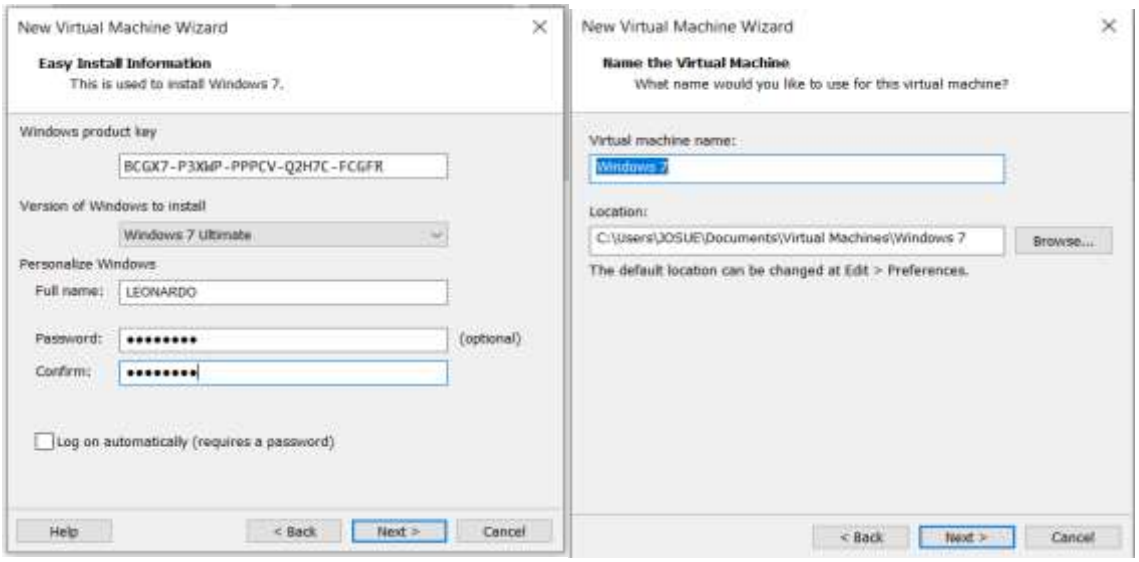


Ilustración 15-0: Nombre, usuario y contraseña de la máquina virtual Windows 7

Realizado por: Erazo, J, 2022

Por último, se selecciona el tamaño del disco duro y se verifica las configuraciones de red, en este caso será adaptador brigded (puente) que viene por defecto, de esta manera tenemos una conexión

de ping hacia todas las máquinas virtuales existentes y también es esencial para las direcciones del servidor dhcp que será utilizado, después aplastar el botón finish (ver ilustración 16-0).

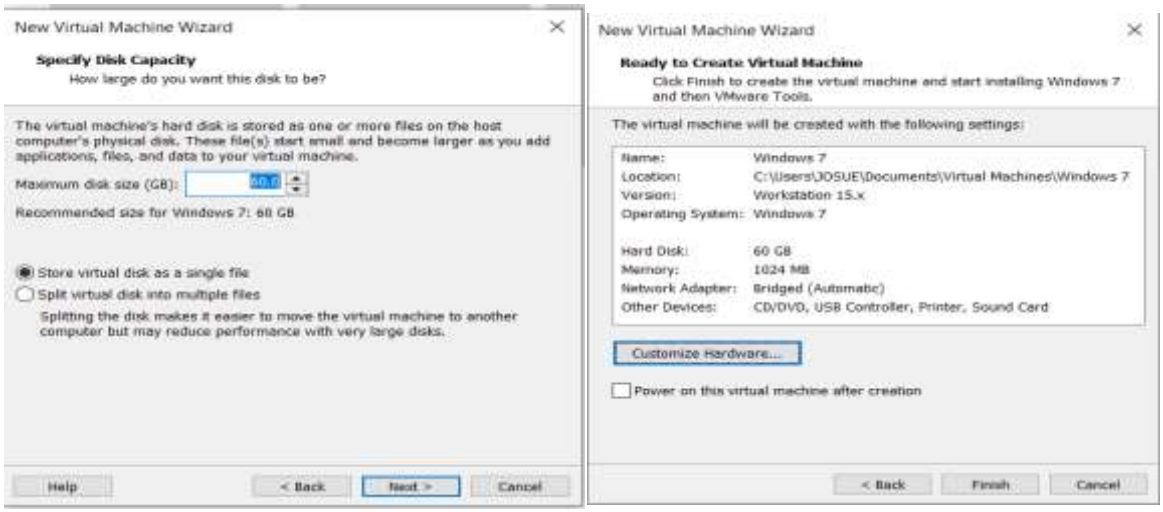


Ilustración 16-0: Capacidad del disco y resumen de configuración de la máquina virtual Windows 7

Realizado por: Erazo, J, 2022

Se elige el sistema operativo a ser instalado, se espera unos minutos hasta que copie todos los archivos de instalación y termine de instalar (ver ilustración 17-0).

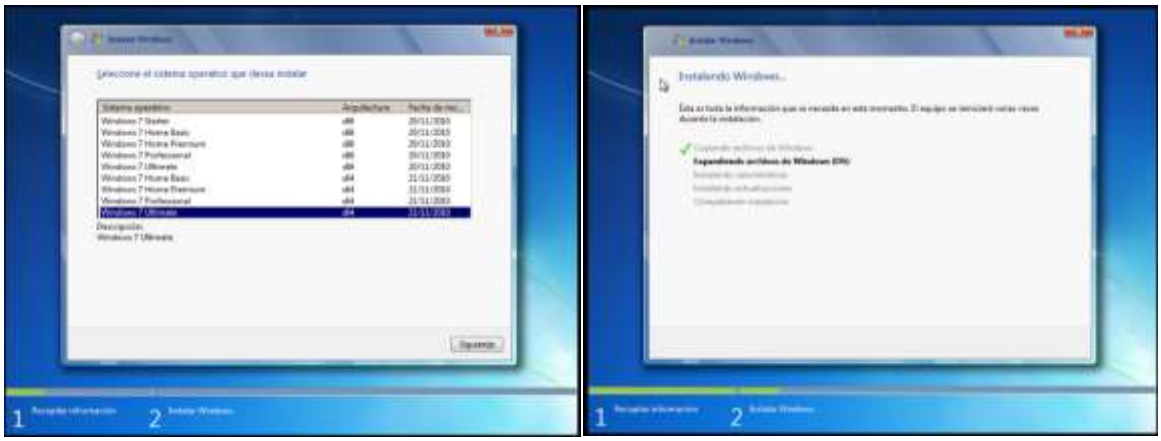


Ilustración 17-0: Instalación de Windows 7

Realizado por: Erazo, J, 2022

Una vez terminada la instalación se ingresa el nombre de usuario y contraseña configurada y está listo para ser utilizada.

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE

UNIDAD DE PROCESOS TÉCNICOS

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 19 / 05 / 2023

INFORMACIÓN DEL AUTOR
Nombres – Apellidos: Fernando Josuee Erazo Rivera
INFORMACIÓN INSTITUCIONAL
Facultad: Informática y Electrónica
Carrera: Telecomunicaciones
Título a optar: Ingeniero en Telecomunicaciones
f. Analista de Biblioteca responsable: Ing. Fernanda Arévalo M.

0646-DBRA-UPT-2023