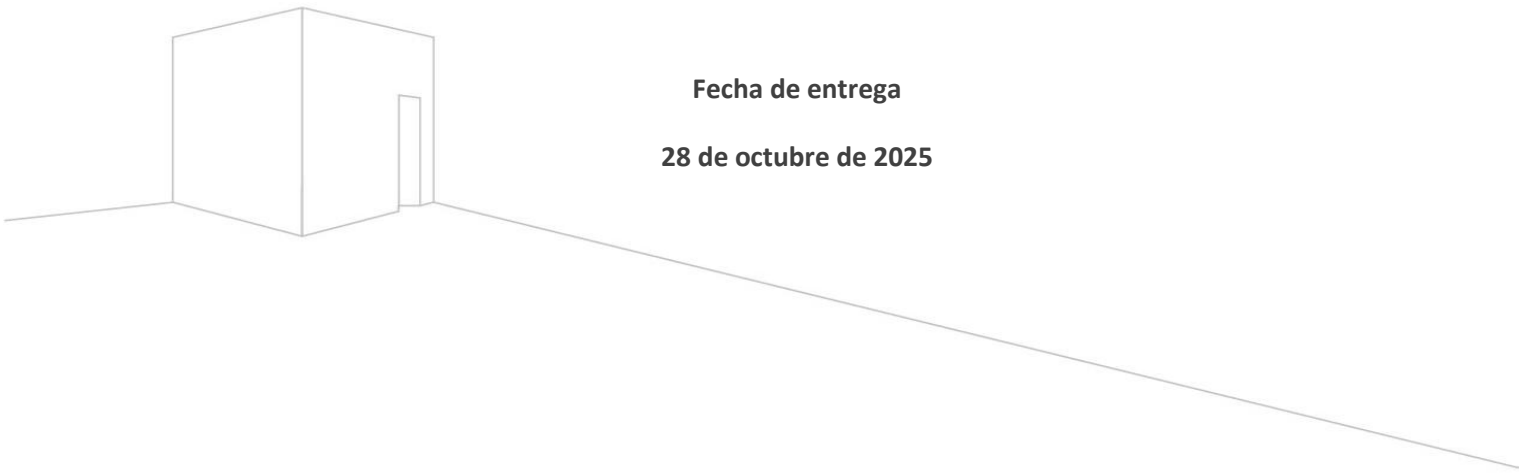
Evaluación Sumativa Numero 2

Asignatura: Seguridad de la información

Sección: T12062/IEI(1)-170-N6/D

Nombre del académico: ROBERTO ALVEAL ORTEGA

Nombre de los integrantes del grupo: Daniel Jara



Fecha de entrega

28 de octubre de 2025

Introducción

El presente informe tiene como finalidad presentar una evaluación de seguridad total, conforme a los criterios definidos en la Unidad de Aprendizaje N° 2. Este trabajo se compone de un análisis de riesgos teórico a partir de un caso práctico y de la práctica de pruebas de intrusión, llevado a cabo en un laboratorio controlado.

Primera parte. Se examinará el caso de la compañía DATAGLOBAL , identificando sus activos críticos, amenazas y vulnerabilidades que forman parte de su infraestructura IaaS y de su equipo de desarrollo remoto, finalizando con la matriz de riesgo resultante.

Segunda parte. Se recoge el desarrollo de dos laboratorios prácticos. El primero de ellos es una simulación de ataque de Ingeniería Social (Phising) y el segundo es un análisis de vulnerabilidades sobre un sistema objetivo (Metasploitable2). Este contiene escaneo de red, identificación de vulnerabilidades, verificación segura y un plan de mitigación.

Actividad 1: análisis de Riesgos

1.- Actividades para auditoria de DATAGLOBAL:

Realizaríamos las siguientes actividades de auditoría para obtener la información correcta sobre las amenazas y vulnerabilidades de DATAGLOBAL:

Revisión de Políticas de Control de Acceso: Dado que 15 desarrolladores tienen acceso a todas ellas, es importante entrevistar al gerente y al supervisor para determinar quién tiene acceso a qué. Hay que revisar la política del “mínimo privilegio”/ “menos privilegios posibles”.

Análisis de Configuración de IaaS: Realizar una auditoría técnica de la configuración de la seguridad de las tres plataformas en la nube que utilizan, lo que significa realizar la revisión de permisos IAM, reglas de firewall (grupos de seguridad) y exposición de las bases de datos. *

Auditoría de Red Empresarial: Analizar la red de oficina donde los desarrolladores se conectan los miércoles. Hay que escanear esta red para encontrar vulnerabilidades, dado que un equipo infectado puede comprometer como mínimo los servidores de prueba.

Revisión de Herramientas de Desarrollo: Evaluación del “amplia variedad de herramientas” que utiliza el equipo (local y en la nube) para verificar que no existan configuraciones inseguras (p.ej. claves de API expuestas en repositorios).

2.- Activos críticos de la empresa:

Los principales 3 activos importantes de DATAGLOBAL son:

Las Bases de Datos (BD): Contienen la información de los clientes y la información acerca de las soluciones web. La confidencialidad y la integridad de estas Bases de Datos es fundamental para el negocio y para las relaciones de confianza con nuestros clientes.

Las Aplicaciones Web: Son el principal producto que se vende a los clientes. La disponibilidad de las aplicaciones y su correcto funcionamiento son el soporte del negocio, y, en consecuencia, la base de los ingresos de DATAGLOBAL.

La Infraestructura IaaS: Es la infraestructura donde residen las aplicaciones y bases de datos, (servidores + redes + almacenamiento). Un compromiso de la infraestructura IaaS es un compromiso de la empresa.

3.- Matriz de probabilidad-impacto:

A continuación, se puede observar una matriz compuesta por la probabilidad del daño y del impacto para los riesgos detectados en DATAGLOBAL.

Riesgo	Probabilidad	Impacto	Nivel de Riesgo	
Acceso no autorizado a IaaS por credenciales filtradas		**Alta** (15 desarrolladores con acceso total [41], trabajando en remoto [42]y usando múltiples herramientas [43]).	**Crítico** (Pérdida de confidencialidad e integridad de todas las BD y aplicaciones).	**Crítico**
Infección de Malware en la red de la oficina		**Media** (El equipo se reúne solo una vez por semana[44], pero usan sus equipos personales sin control centralizado).	**Alto** (Compromiso de los servidores de prueba, que podría escalar a producción si usan las mismas credenciales).	**Alto**
Fuga de datos por un desarrollador interno		**Media** (No hay indicios de malicia, pero el acceso total de 15 personas [45] facilita un error humano o una acción maliciosa).	**Crítico** (Robo de propiedad intelectual o datos de clientes).	**Crítico**

Actividad 2: amenazas y vulnerabilidades

1.- Esquema de ataque por software malintencionado:

Un desarrollador trabajando de forma alejada y usando su propio equipo, usado para muchas de las herramientas de la nube a la vez, es uno de los vectores de ataque primarios. A continuación esquematizamos un ataque:

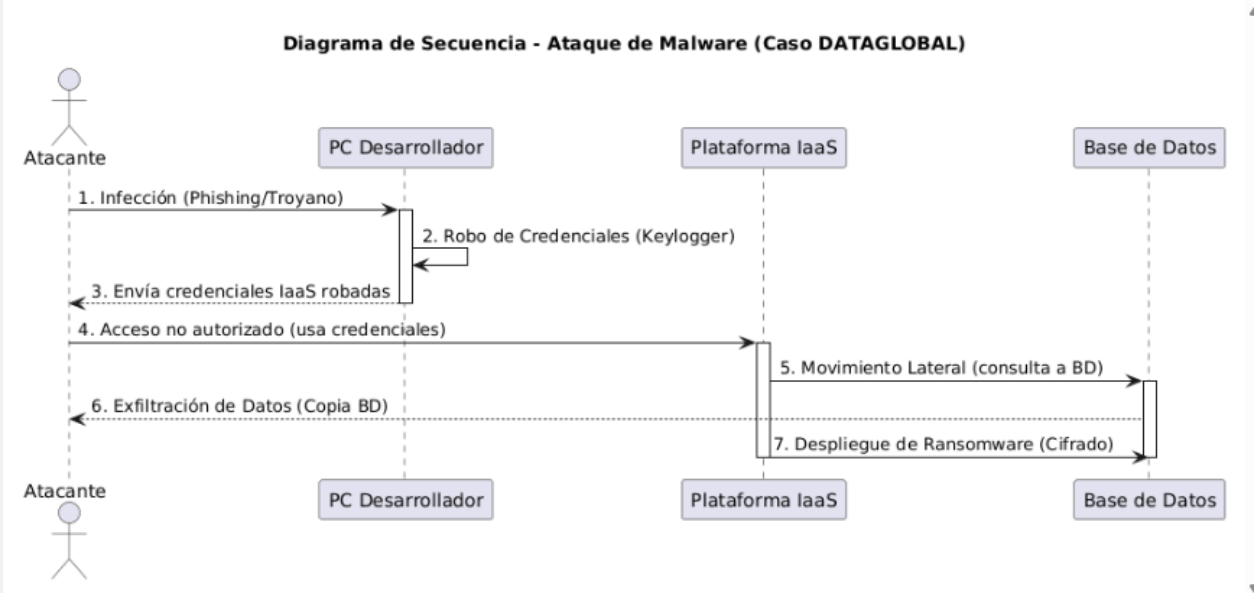
1. Infección Inicial: El desarrollador recibió un correo de Phishing (el de la Actividad 3) o descargó una herramienta de desarrollo no oficial que contiene un troyano. Se sigue ejecutando el software malicioso en su equipo local.

2. Robo de credenciales: El troyano va a permanecer escondido y va a empezar a controlar todo lo que hace el desarrollador. Le va a robar las credenciales de acceso a la plataforma IaaS (Infraestructura como Servicio) de DATAGLOBAL.

3. Acceso no autorizado: Con las credenciales robadas, el atacante va a hacer uso de ellas para acceder a distancia al panel de control de la IaaS de la empresa.

4. Movimiento Lateral y Exfiltración: Una vez dentro, el atacante tiene acceso a las tres plataformas, a bases de datos y a aplicaciones y va a copiar (exfiltrar) bases de datos de clientes a un servidor externo.

5. Despliegue de Ransomware: El atacante va a hacer uso de su acceso total para cifrar las aplicaciones web, así como las bases de datos con el objetivo de maximizar el daño y pedir un rescate. Se va a interrumpir la continuidad operacional de DATAGLOBAL y de sus clientes.



2.- Medidas de minimización o reducción:

Con el fin de reducir o minimizar el impacto de un ataque de software maligno como se ha descrito anteriormente en el anterior punto, se deben aplicar las siguientes medidas:

El Principio de Mínimo Privilegio: Esta es la medida más urgente. Los 15 desarrolladores no deben tener acceso ilimitado. Deben definirse roles en IaaS para que un desarrollador solo pueda tener acceso a los recursos de la plataforma sobre la cual trabaja.

Autenticación de Múltiples Factores (MFA): Implementar MFA obligatorio de todos los accesos a la consola de IaaS y a las herramientas en la nube, evitando así que un atacante pueda acceder solo con la contraseña robada.

Segmentación de Red: Las tres plataformas IaaS deben estar en redes (VPC) diferentes e incluso aisladas entre sí; si un atacante compromete la Plataforma 1, esta segmentación evitaría que pudiera "saltar" fácilmente en la Plataforma 2 o 3.

3.- Acciones por compromiso con GitHub:

En caso de que se presuma que una actualización publicada a través de GitHub ha puesto en riesgo la infraestructura, se deben llevar a cabo las siguientes acciones priorizadas en los servidores web:

Desconectar el Servidor de Forma Inmediata: La acción inicial consiste en desvincular el servidor web comprometido de la red pública y de la interna (modificar las reglas del firewall) para frenar cualquier comunicación saliente del malware (por ejemplo, exfiltración de datos) y prevenir ataques a otros servidores.

Revertir la Actualización (Rollback): Emplear el historial de Git para deshacer el "commit" (la actu alización) perjudicial. Reinstalar la versión estable y limpia más reciente del código.

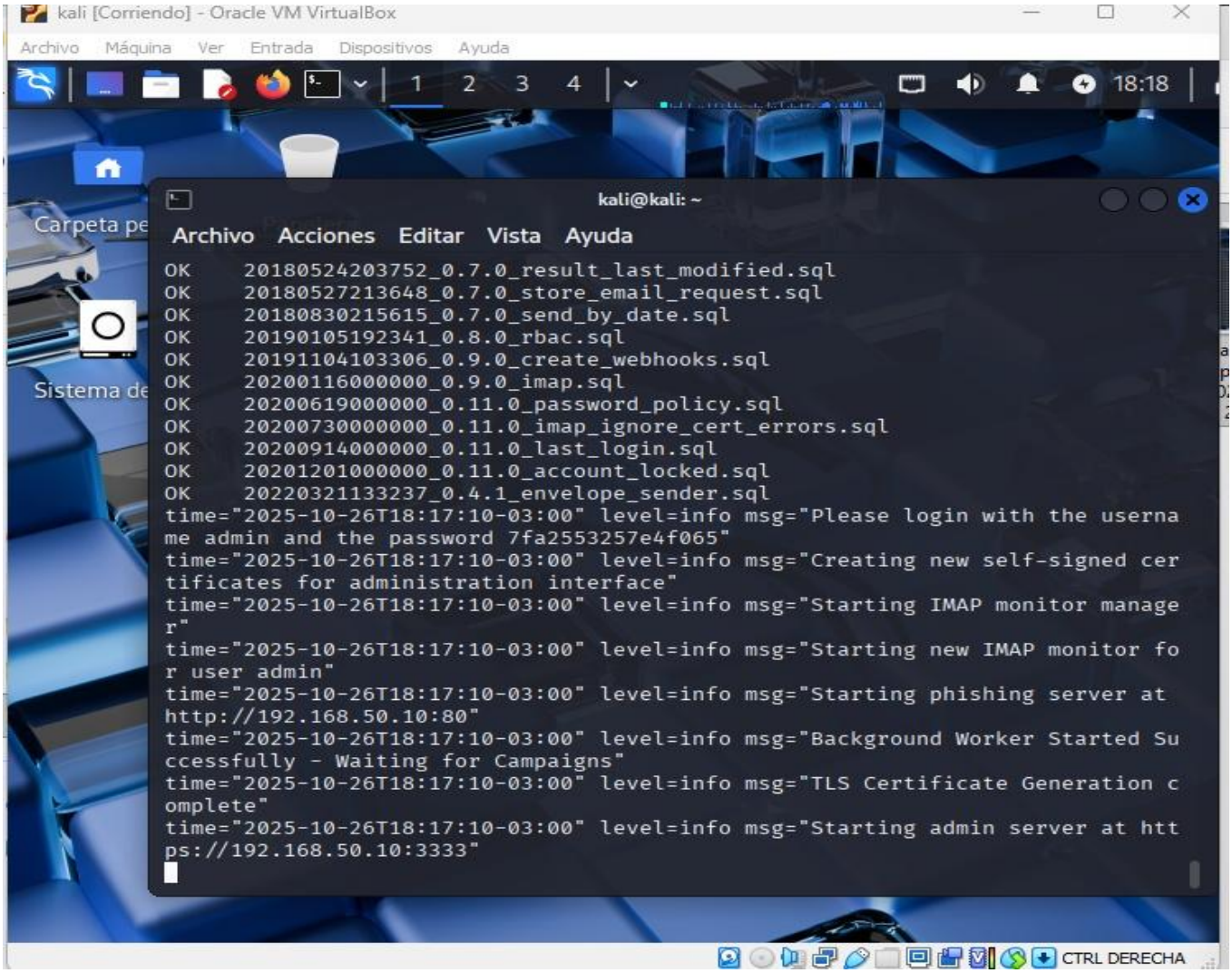
Rotación de Todas las Credenciales: Suponer que todas las "claves secretas" (contraseñas de API, contraseñas de bases de datos, claves SSH) que se encontraban en el servidor han sido sustraída s. Es necesario anular y crear nuevas credenciales para cada uno de los servicios con los que el servidor se conectaba.

Actividad 3: ingeniería social

La meta de esta actividad fue llevar a cabo una simulación controlada de un ataque de Phishing en un entorno de laboratorio aislado (intnet) para ilustrar cómo un atacante puede obtener las credenciales de un usuario y los peligros que esto conlleva. El vector seleccionado fue un correo electrónico de Phishing que imitaba al equipo de soporte

Configuración del Entorno de Pruebas (GoPhish)

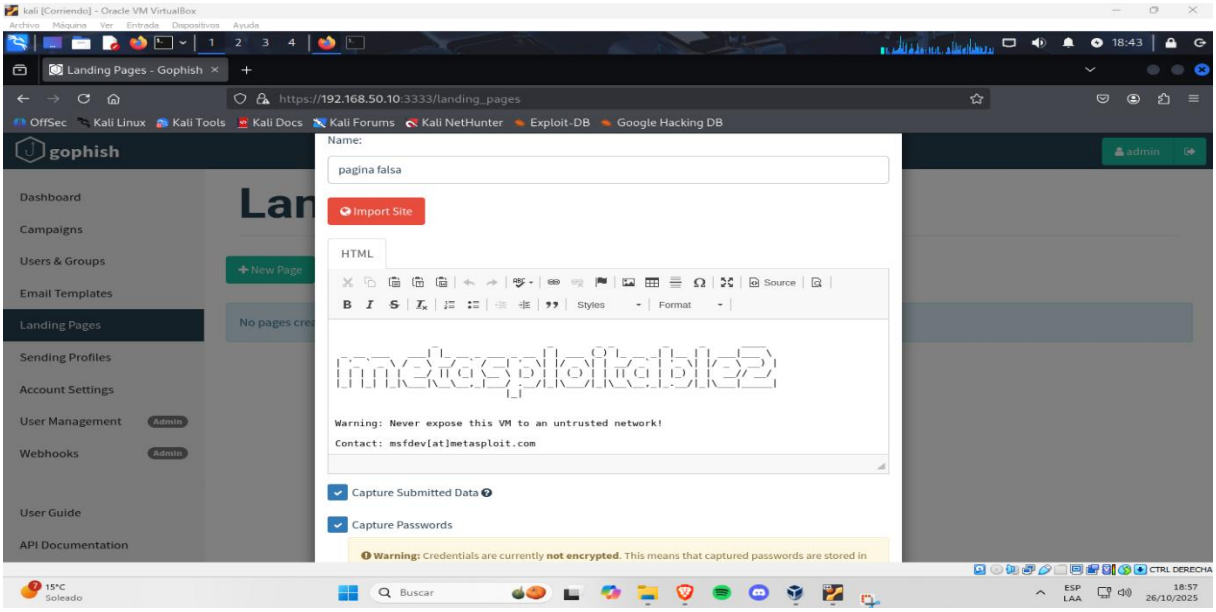
La simulación se llevó a cabo con la herramienta GoPhish, que fue instalada en la máquina Kali Linux (IP 192.168.50.10). Se estableció la herramienta para funcionar en la red local, teniendo el panel de administración en el puerto 3333 y el servidor de phishing en el puerto 8080, como se muestra en la siguiente imagen de la terminal al iniciar el servicio:



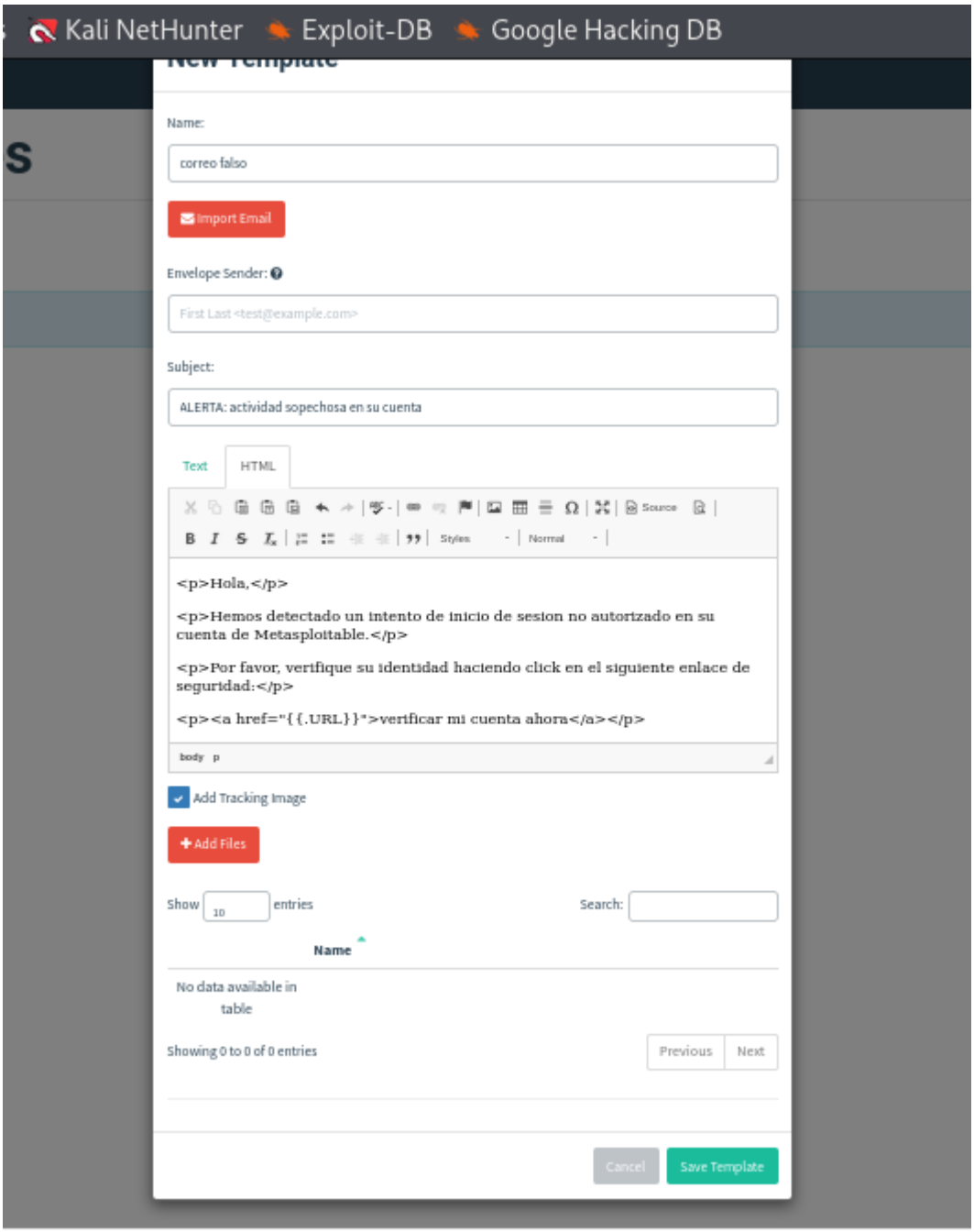
Modelos (Mensaje y Langing page)

Se diseñaron las dos plantillas esenciales para el ataque, según lo que indica la pauta:

1.- Plantilla de Langing page (Página Falsa): Se diseñó una página que replicaba el sitio de phpMyAdmin de la computadora objetivo (importando la URL http://192.168.50.20/phpMyAdmin/).
Se seleccionaron las opciones "Capture Submitted Data" y "Capture Passwords" para almacenar las credenciales que la víctima proporcione.



2.- Plantilla de Mensaje (Correo Fraudulento): Se creó un correo con el tema "AVISO: Actividad dudosa en su cuenta". El cuerpo del mensaje (consultar captura) contiene la variable {{.URL}}, que GoPhish sustituye por el enlace de seguimiento exclusivo

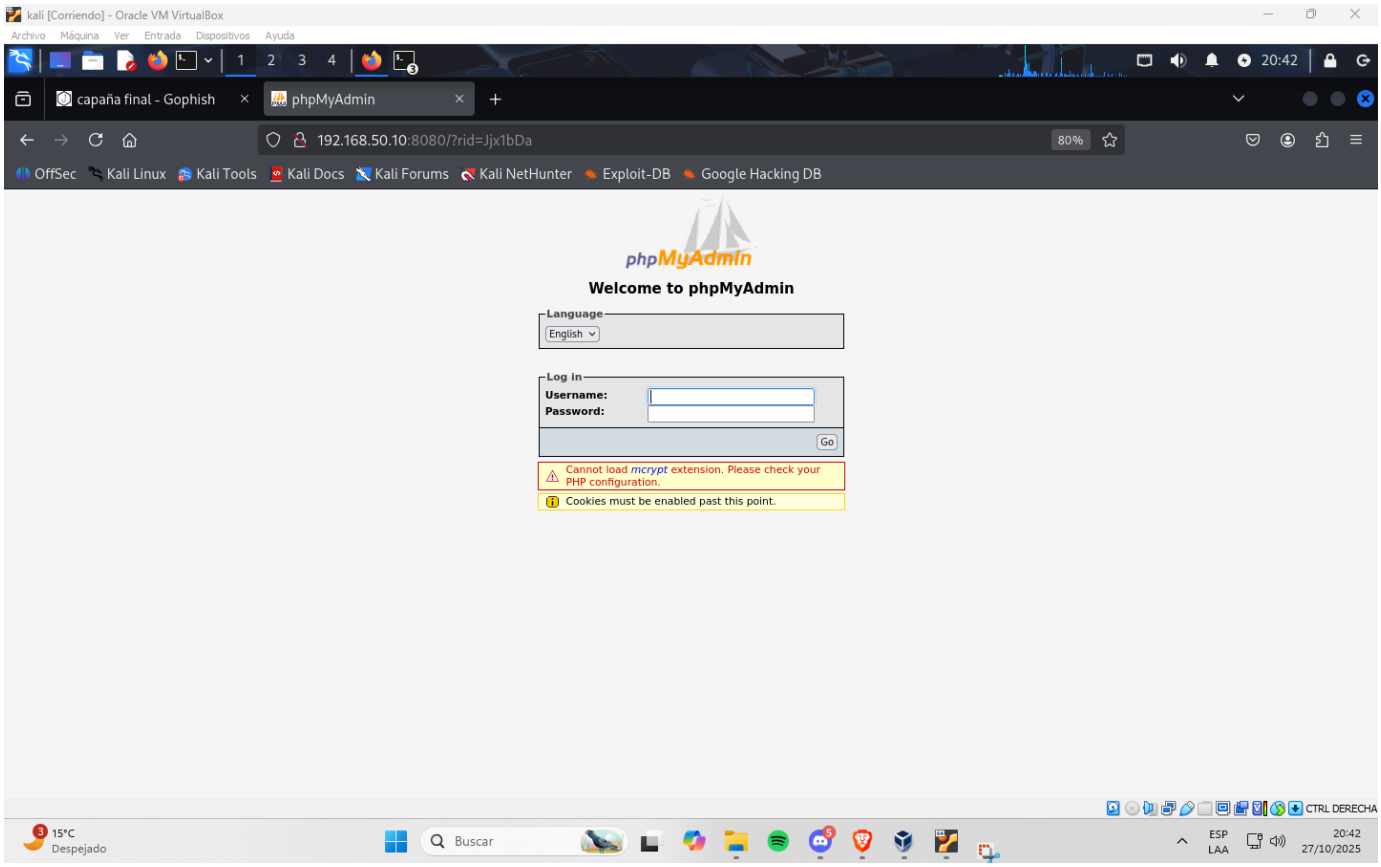


secuencialidad y Apoyo al Ataque:

El ataque se ve favorecido por factores humanos, como la confianza o el pánico, que impulsan al usuario a actuar sin comprobar. La sucesión del ataque fue esta:

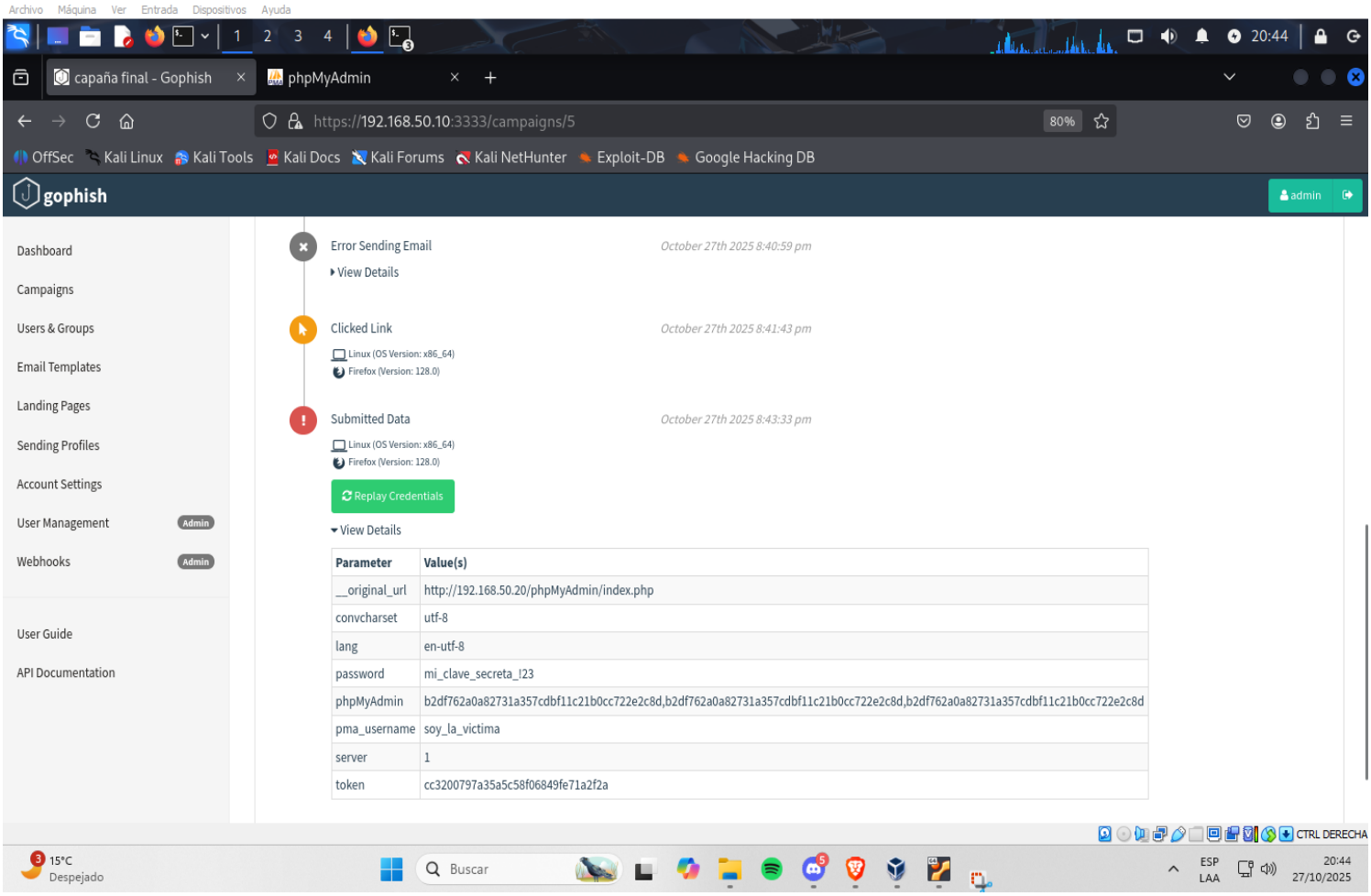
1.- Se inicia la campaña a través de GoPhish. Se emula el clic de la víctima al abrir el enlace de seguimiento único (http://192.168.50.10:8080/?rid=...).

2.- La víctima es conducida a la página fraudulenta de phpMyAdmin.



3.- El usuario, pensando que su cuenta está amenazada, contribuye al ataque al ingresar sus credenciales (soy_la_victima / mi_clave_secreta_123), tal como se demostró en el laboratorio.

4.- GoPhish logra capturar estos datos, como se muestra en la captura del panel de resultados a continuación, donde se pueden ver las credenciales obtenidas.



Peligros para la Sostenibilidad Operativa y Estrategias Preventivas.

Peligros: El peligro principal es la sustracción de las credenciales de un usuario. Si este usuario posee privilegios (como el acceso a DATAGLOBAL IaaS), el efecto es grave: sustracción de bases de datos, toma de servidores (Ransomware) y paralización completa de la continuidad operacional.
Acciones Preventivas:

Capacitación (Factor Humano): Instruir a los trabajadores para que reconozcan mensajes de correo electrónicos sospechosos, desconfíen de enlaces urgentes y nunca ingresen credenciales desde un correo electrónico.

Filtros de Correo (Técnico): Establecer filtros de correo (Spam/Anti-Phishing) que evalúen los enlaces y la reputación del emisor.

Autenticación de Dos Factores (2FA): Es la estrategia más eficiente. A pesar de que el intruso obtenga la contraseña, no podría entrar sin el segundo factor (por ejemplo, código del móvil).

Actividad 4: Hacking a Metasploitable2

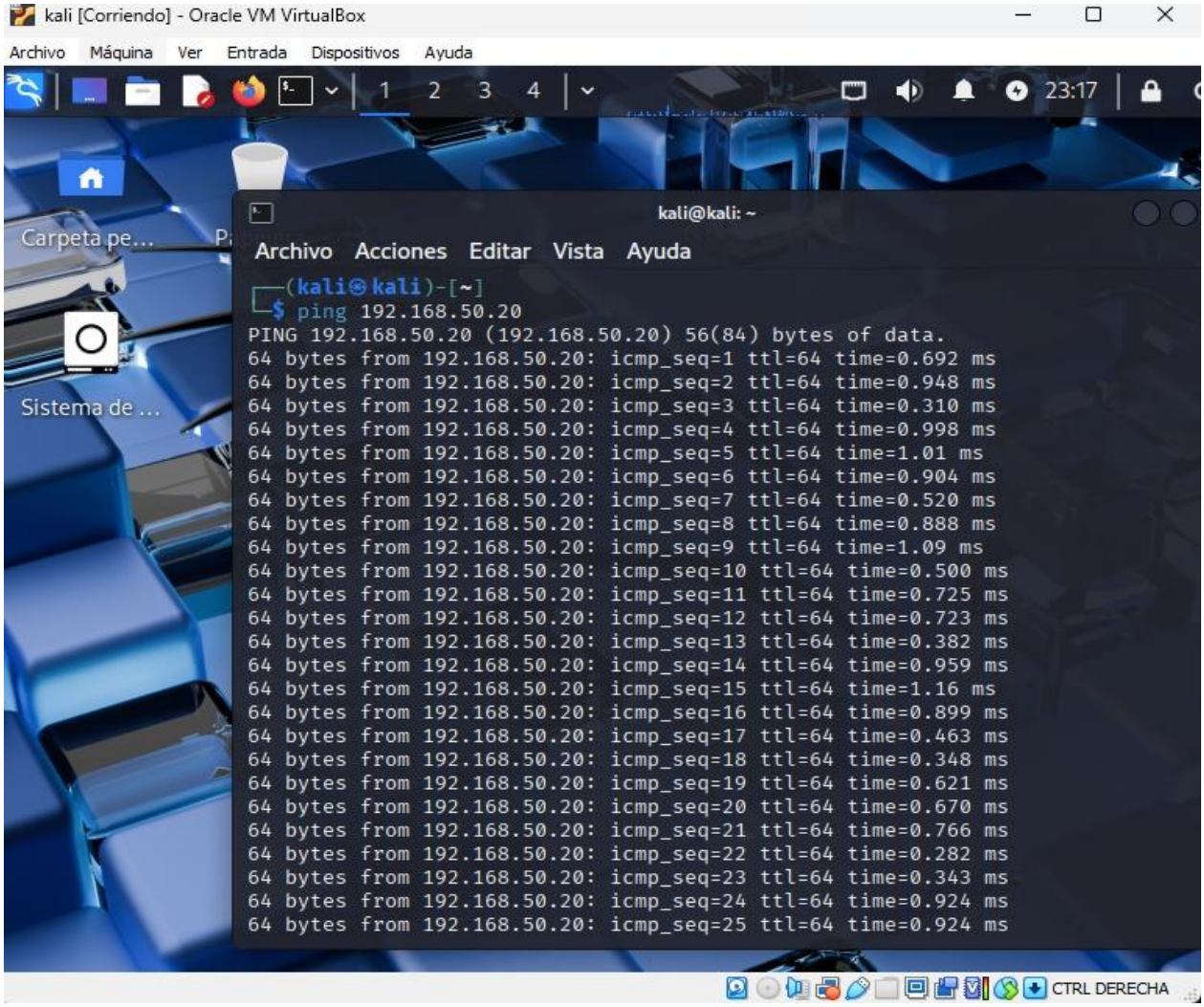
1.- configuración del laboratorio:

Para esta tarea, se estableció el laboratorio en un entorno de red separado (intnet) en VirtualBox, de acuerdo a lo que se indica en la pauta. El ambiente está compuesto por:

Máquina Ofensiva: Kali Linux (IP: 192.168.50.10)

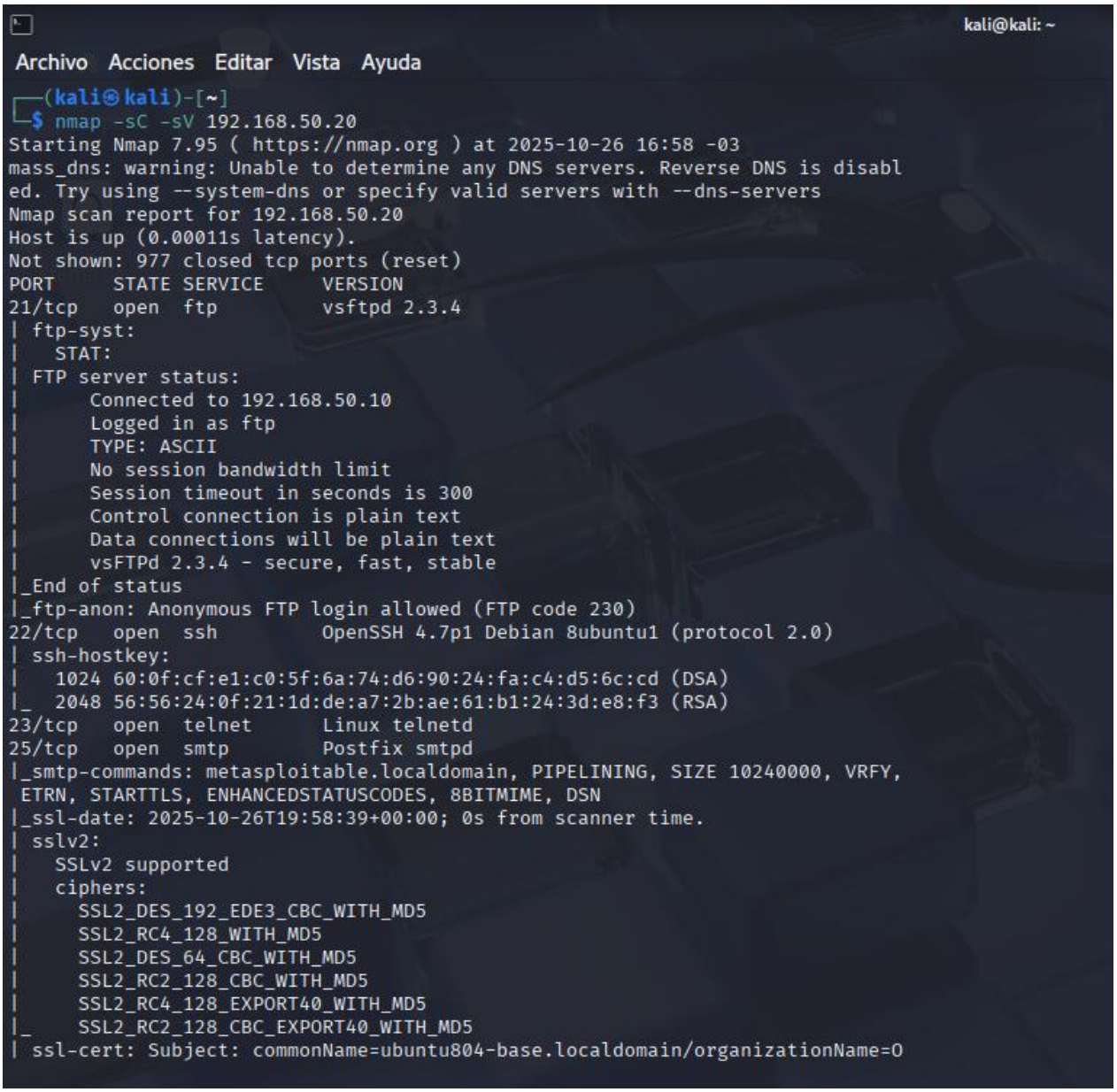
Máquina Afectada: Metasploitable2 (IP: 192.168.50.20)

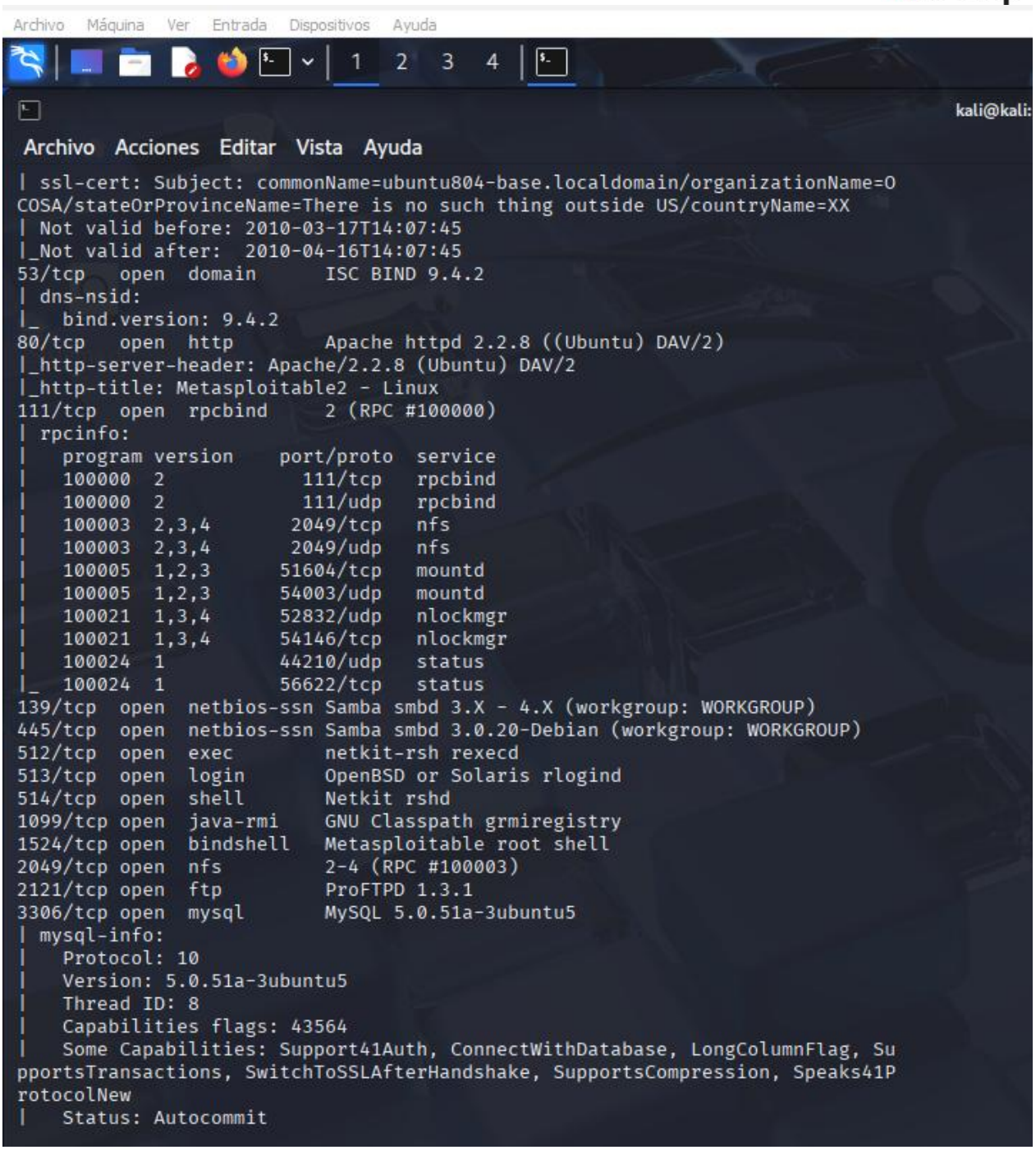
La conexión entre las dos máquinas se comprobó con éxito a través de un ping desde Kali a Metasploitable2, como se muestra en la captura siguiente:

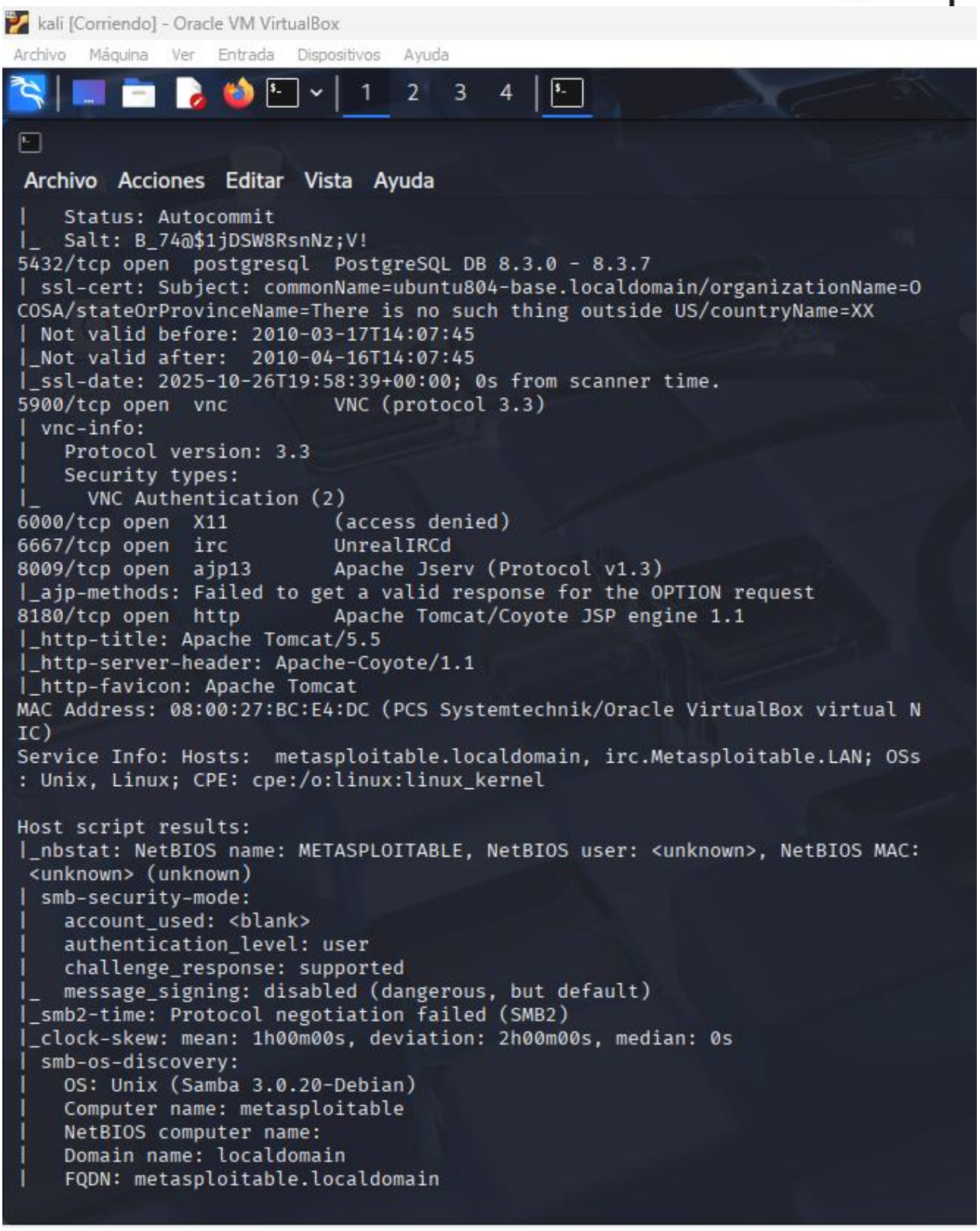


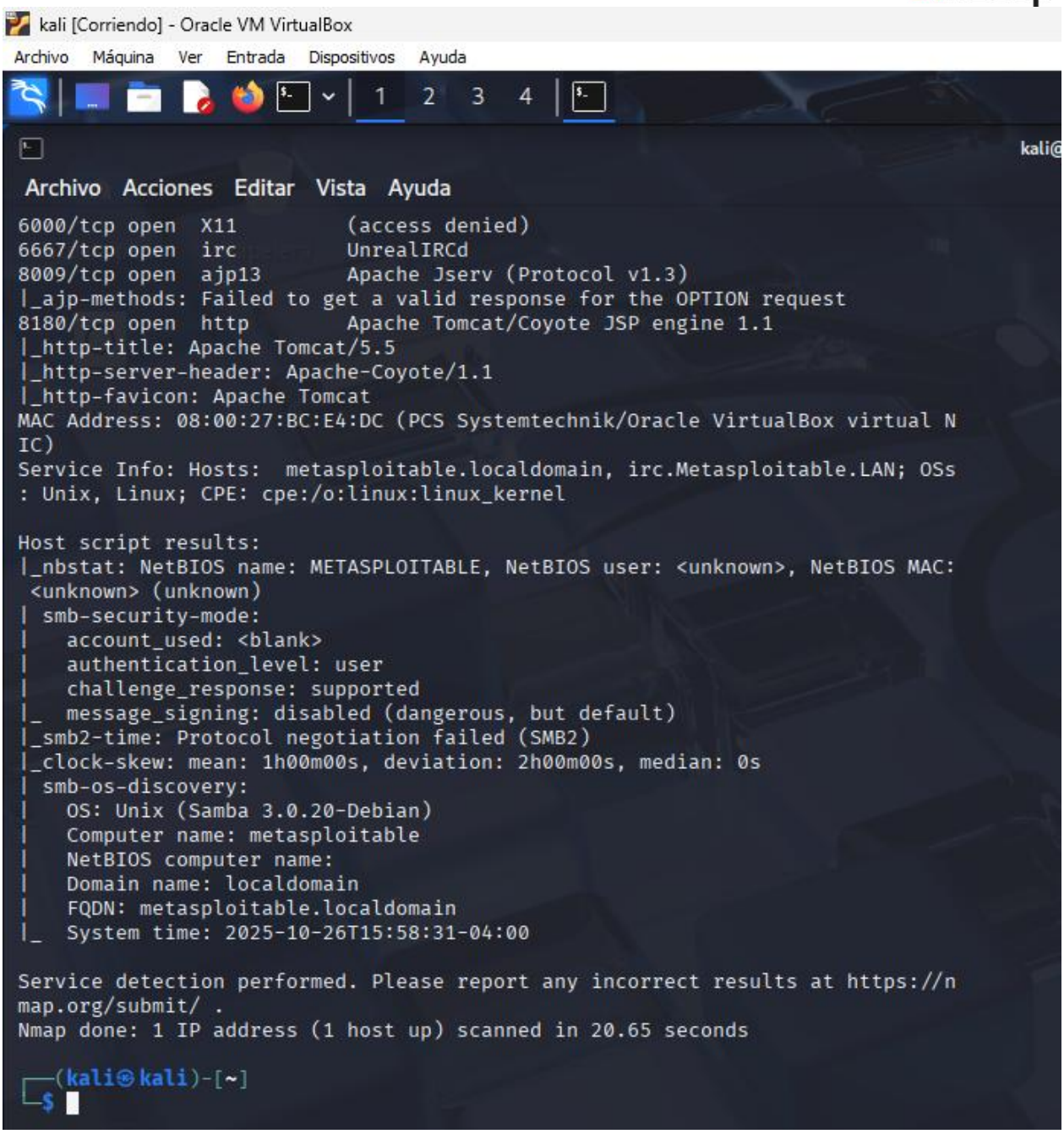
3.- Exploración de red (nmap):

Se realizó un escaneo de servicios y versiones (nmap -sC -sV) en la máquina objetivo. Los resultados, que se presentan a continuación, mostraron una gran cantidad de puertos accesibles y servicios con versiones antiguas y susceptibles




Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
kali@kali:
Archivo Acciones Editar Vista Ayuda
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
53/tcp open domain ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2 111/tcp rpcbind
| 100000 2 111/udp rpcbind
| 100003 2,3,4 2049/tcp nfs
| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 51604/tcp mountd
| 100005 1,2,3 54003/udp mountd
| 100021 1,3,4 52832/udp nlockmgr
| 100021 1,3,4 54146/tcp nlockmgr
| 100024 1 44210/udp status
|_ 100024 1 56622/tcp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login OpenBSD or Solaris rlogind
514/tcp open shell Netkit rshd
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 8
| Capabilities flags: 43564
| Some Capabilities: Support41Auth, ConnectWithDatabase, LongColumnFlag, Su
pportsTransactions, SwitchToSSLAfterHandshake, SupportsCompression, Speaks41P
rotocolNew
| Status: Autocommit


kali [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
Archivo Acciones Editar Vista Ayuda
| Status: Autocommit
|_ Salt: B_74@$1jDSW8RsnNz;V!
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2025-10-26T19:58:39+00:00; 0s from scanner time.
5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security types:
|_ VNC Authentication (2)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
MAC Address: 08:00:27:BC:E4:DC (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h00m00s, deviation: 2h00m00s, median: 0s
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain


kali [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
kali@
Archivo Acciones Editar Vista Ayuda
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
MAC Address: 08:00:27:BC:E4:DC (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h00m00s, deviation: 2h00m00s, median: 0s
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2025-10-26T15:58:31-04:00
Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.65 seconds
(kali㉿kali)-[~]
$

3.- Detección de vulnerabilidades:

De acuerdo con los resultados del escaneo nmap, se detectan los siguientes 3 hallazgos críticos, tal como lo requiere la pauta:

Hallazgo 1 (FTP - Puerto 21): El servicio vsftpd 2.3.4 se encuentra activo. Esta versión particular es reconocida por incluir una vulnerabilidad de puerta trasera (backdoor) (CVE-2011-2523), la cual posibilita la ejecución remota de comandos.

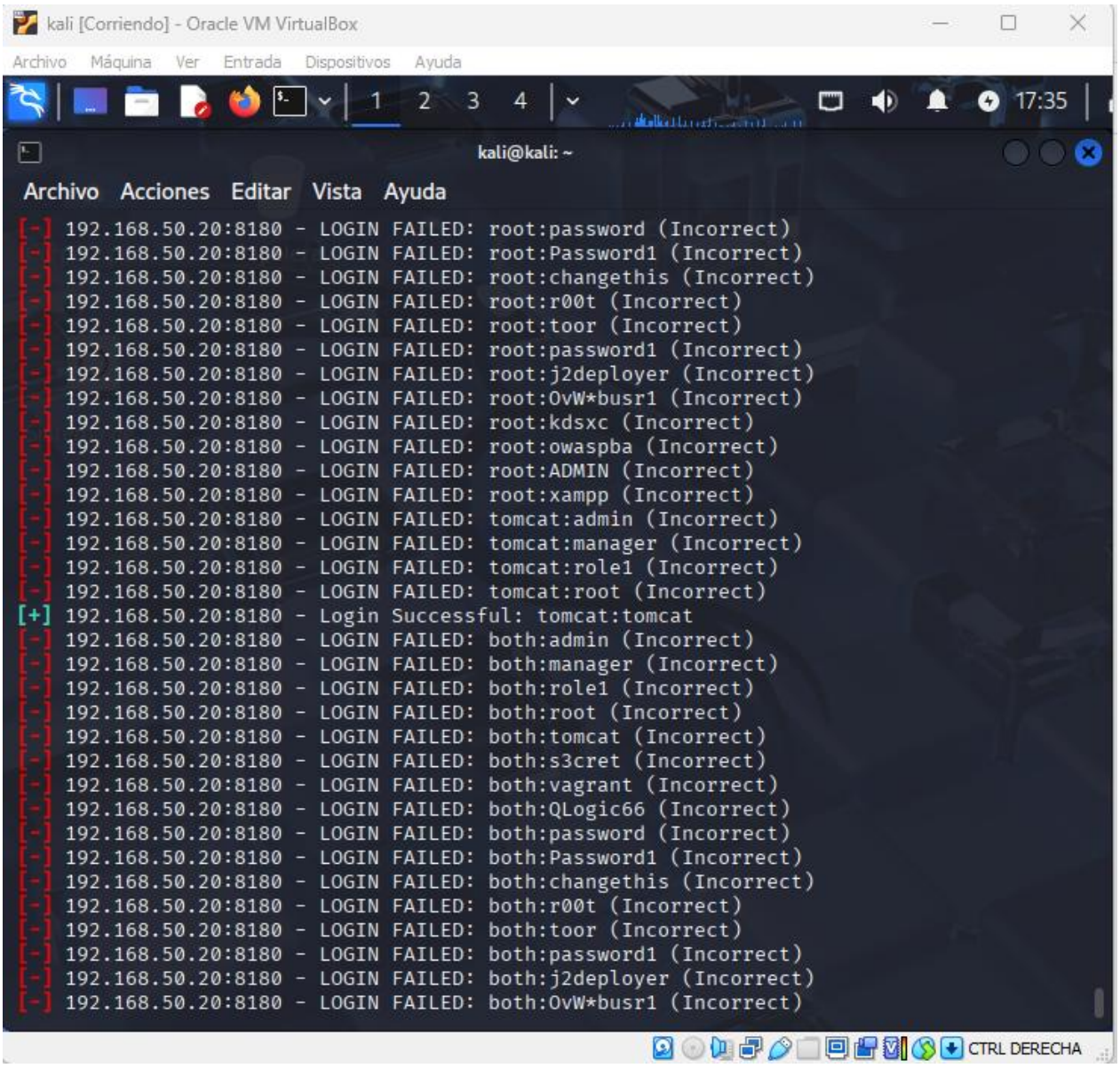
Hallazgo 2 (Telnet - Puerto 23): El servicio telnetd de Linux está disponible. Telnet es un protocolo vulnerable que envía todas las credenciales (nombre de usuario y contraseña) en texto sin cifrar, lo que permite que un atacante en la red las capture con facilidad.

Hallazgo 3 (Tomcat - Puerto 8180): El servicio Apache Tomcat 5.5 se encuentra en funcionamiento. Esta versión está desactualizada y el panel de control (/manager) suele ser susceptible a credenciales predeterminadas o débiles, lo que permite a un atacante cargar archivos dañinos

4.- Comprobación

Se eligió el Hallazgo 3 (Apache Tomcat) para realizar la verificación segura. Se empleó el módulo auxiliar auxiliary/scanner/http/tomcat_mgr_login de Metasploit para buscar credenciales predeterminadas.

El escáner verificó con éxito que el servicio presenta vulnerabilidades, detectando credenciales de administrador predeterminadas: tomcat:tomcat



5.- Efecto en la continuidad operativa:

La exposición de credenciales de administrador (tomcat:tomcat) en el servidor Apache Tomcat tiene un impacto Crítico y afecta de manera directa a los 3 pilares de la seguridad (Tríada CIA):

Integridad: Un intruso que tiene acceso al panel de administrador puede cargar un archivo dañino (como una "web shell") y obtener control total del servidor. Es posible cambiar el código de las aplicaciones, modificar datos y secuestrar el sistema.

Confidencialidad:

A través del servidor comprometido, el atacante tiene la capacidad de acceder a archivos de configuración y sustraer las contraseñas de acceso a las bases de datos. Esto le daría la capacidad de extraer toda la información confidencial de la compañía y sus clientes.

Disponibilidad:

El agresor puede paralizar el servicio de Tomcat, "eliminar" las aplicaciones implementadas o llevar a cabo un ataque de Ransomware desde el servidor, ocasionando una interrupción total del servicio y perjudicando la continuidad operativa.

6.- Reducción de impactos:

Para reducir este riesgo particular, se deben ejecutar las siguientes acciones específicas:

Modificar Credenciales:

Ingresar al archivo de configuración de usuarios de Tomcat (usualmente tomcat-users.xml) y alterar de inmediato la contraseña del usuario "tomcat". La contraseña nueva tiene que ser fuerte y exclusiva.

Implementar Mínimo Privilegio:

Suprimir o desactivar la cuenta "tomcat" si no es absolutamente esencial. Si es necesario, otorgarle un rol sin derechos de despliegue (manager-gui) y establecer cuentas distintas para funciones administrativas.

Actualizar el Servicio:

La versión 5.5 de Tomcat ya no es válida y ya no cuenta con soporte. Es necesario organizar la migración inmediata a una versión actualizada y corregida (por ejemplo, Tomcat 9 or 10).

Limitar Acceso:

El panel de control (puerto 8180) no debe estar accesible a toda la red. Es necesario establecer un firew all local (iptables) o directrices de grupo de seguridad (en IaaS) para que únicamente la IP del administra dor del sistema tenga acceso a ese puerto.

Conclusión

Durante esta Evaluación Sumativa, se llevó a cabo un examen de seguridad exhaustivo que incluyó tanto la valoración teórica de riesgos como la realización de ataques controlados en un entorno de pruebas.

Durante la fase inicial, el estudio del caso DATAGLOBAL mostró que las inadecuadas políticas de acceso (por ejemplo, 15 desarrolladores con acceso total) y la ausencia de segmentación de red generan riesgos significativos para la continuidad operativa de una empresa.

En la etapa práctica, la Actividad 4 evidenció la sencillez con la que un atacante puede localizar y confirmar vulnerabilidades críticas en sistemas obsoletos. El escaneo realizado con nmap junto con la verificación posterior a través de Metasploit confirmó la existencia de credenciales por defecto (tomcat:tomcat), un descubrimiento que posibilitaría a un atacante obtener control total del servidor.

Finalmente, la Actividad 3 (Ingeniería Social) resultó ser muy importante, mostrando que el componente humano es frecuentemente el punto más vulnerable. A través de la simulación de Phishing con GoPhish, se consiguió replicar un sitio y obtener con éxito las credenciales de una víctima (mi_clave_secreta_123), demostrando el alto peligro de este tipo de ataques.

Este informe establece que la seguridad de la información debe ser un esfuerzo en múltiples capas, integrando controles técnicos sólidos (actualizaciones, firewalls, MFA) junto con una formación continua del personal (prevención de Phishing), para resguardar efectivamente los activos de una organización