ACCESO NO AUTORIZADO MEDIANTE ATAQUE MITM, EXPLOTACIÓN DE RECURSO NFS, Y CLAVES SSH EXPUESTAS

Jesús Díaz Expósito

INDICE

1. INICIO

Este informe documenta los hallazgos de una actividad de análisis ofensivo realizada sobre una red interna. El objetivo ha sido evaluar el nivel de exposición y riesgo de compromiso de los sistemas presentes, en concreto una máquina con sistema operativo Linux Lubuntu.

Se ha llevado a cabo un ejercicio de intrusión desde otra máquina Kali conectada a la misma red, simulando el comportamiento de un actor malicioso con acceso limitado, pero capaz de interceptar tráfico y analizar recursos compartidos.

El propósito es identificar posibles vulnerabilidades explotables y ofrecer recomendaciones de mitigación para reducir la superficie de ataque.

2. RESUMEN EJECUTIVO

2.1. INTRODUCCIÓN

Este informe ejecutivo proporciona una visión general del compromiso de seguridad detectado en la red interna de la organización. Se ha conseguido el acceso completo a una máquina Linux Lubuntu a través de la obtención de credenciales privadas no protegidas y el análisis del tráfico de red, lo que evidencia debilidades en la configuración y protección de los recursos internos.

2.2. ALCANCE Y LIMITACIONES

2.2.1. Alcance

- **Sistemas evaluados**:
  - Máquina Lubuntu Linux (actua como servidor web con Apache en puerto 32013/TCP)
  - Máquina cliente.
  - Máquina atacante Kali Linux conectada a la misma red.
- **Técnicas empleadas**:
  - Intercepción de tráfico no cifrado (MITM).
  - Acceso a carpetas compartidas.
  - Uso de claves privadas para acceso remoto a la máquina Lubuntu.

2.2.2. Metodología

Se ha trabajado bajo un enfoque de caja negra, sin credenciales iniciales ni conocimiento del entorno.

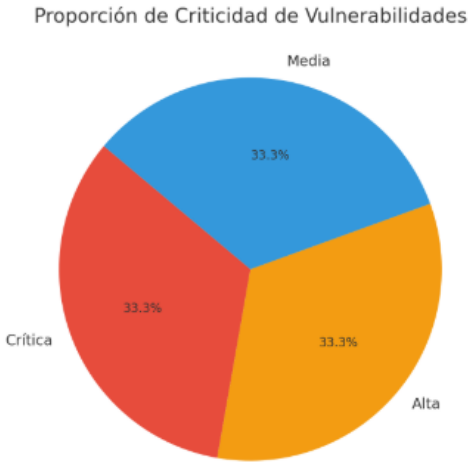
2.2.3. Limitaciones

- No se ha realizado una auditoría completa de otros sistemas o servicios.
- No se han ejecutado técnicas de escalado de privilegios ni persistencia sobre la máquina comprometida.
- La actividad se limitó a un entorno de red al que el atacante tenía acceso previo.

2.3. RESUMEN Y CRITICIDAD DE LAS VULNERABILIDADES

Vulnerabilidad	Tipo	Criticidad	Descripción breve
Clave privada SSH expuesta	Gestión de credenciales	Crítica	Acceso total al sistema mediante clave robada
Tráfico no cifrado (MITM)	Configuración de red	Alta	Permite interceptar información sensible
Apache en puerto no estándar	Ocultamiento por oscuridad	Media	Puede dificultar detección, pero no es protección

2.3.1 Gráfica de criticidad



3. RESUMEN TÉCNICO

3.1. INTRODUCCIÓN

Esta sección detalla el procedimiento técnico seguido durante la intrusión, describiendo paso a paso las acciones realizadas, las herramientas utilizadas y las técnicas ofensivas asociadas. La explotación se basó en el análisis de tráfico de red y la obtención de una clave privada SSH utilizada para comprometer el sistema Lubuntu Linux.

3.2. METODOLOGÍA OWASP

3.2.1. Análisis detallado

Según el OWASP Top 10, indicando su entorno afectado y criticidad, se han identificado las siguientes vulnerabilidades:

- **Login sin HTTPS:** El formulario de autenticación expone credenciales en texto plano, lo que corresponde con *Fallas Criptográficas (A02)* por no cifrar datos sensibles en tránsito.
- **Captura de credenciales vía MITM:** Refuerza la falla anterior y también puede vincularse con *Fallas de Identificación y Autenticación (A07)* si el sistema no implementa protección contra sesiones inseguras.

- **Port Knocking para abrir servicios:** Si el sistema permite abrir puertos críticos sin autenticación fuerte esto se corresponde con *Pérdida de Control de Acceso (A01)*.
- **NFS sin restricciones y clave privada expuesta:** El uso de componentes mal configurados o desactualizados (como NFS sin restricciones) se corresponde con *Componentes Vulnerables y Obsoletos (A06)*. Además, exponer claves privadas sin integridad ni cifrado puede corresponderse con *Fallas de Integridad de Software y Datos (A08)*.
- **Acceso remoto vía SSH con clave robada:** Aunque el acceso se logra por medios externos, el hecho de que la clave estuviera accesible sin protección refuerza las vulnerabilidades anteriores.

3.2.2. Tabla resumen

Vulnerabilidad OWASP	Entorno afectado	Criticidad OWASP
A02:2021 – Cryptographic Failures	Comunicación entre cliente y servidor (sin HTTPS)	Alta
A07:2021 – Identification and Authentication Failures	Aplicación web (formulario de login en Apache)	Alta
A01:2021 – Broken Access Control	Sistema operativo / servicios	Crítica
A06:2021 – Vulnerable and Outdated Components	NFS sin permisos / clave privada expuesta	Alta
A08:2021 – Software and Data Integrity Failures	SSH / sistema operativo	Alta

3.3. CLASIFICACIÓN DE TÉCNICAS SEGÚN MITRE

Podemos mapear los pasos realizados en la explotación con las tácticas y técnicas del marco MITRE ATT&CK. Este marco clasifica el comportamiento de los atacantes en tácticas (objetivos) y técnicas (métodos) observados en ataques reales.

3.3.1. Tácticas MITRE involucradas

1. **Acceso inicial** – Entrada al sistema por login vulnerable.
2. **Acceso a credenciales** – Captura de credenciales por red y acceso a claves privadas.
3. **Descubrimiento** – Identificación de puertos y recursos compartidos.
4. **Evasión de defensas** – Port knocking para evitar detección.
5. **Movimiento lateral** – Uso de SSH para pivotar dentro del sistema.

3.3.2. Tabla resumen

Táctica MITRE	Técnica MITRE	Código MITRE	Descripción
Initial Access	Exploit Public-Facing Application	T1190	El formulario de login expuesto en HTTP puede ser explotado para obtener acceso.
Credential Access	Network Sniffing	T1040	Uso de Wireshark para interceptar credenciales en texto plano.
Discovery	Network Service Discovery	T1046	Escaneo de servicios para identificar puertos abiertos
Defense Evasion	Traffic Signaling: Port Knocking	T1205.001	Técnica para abrir puertos mediante secuencia específica.
Lateral Movement	Remote Services: SSH	T1021.004	SSH abierto tras port knocking permite moverse lateralmente.
Discovery	Network Share Discovery	T1135	Exploración de unidades NFS sin permisos.
Credential Access	Unsecured Credentials. Private keys	T1552.004	Robo de claves SSH desde unidad NFS montada.
Initial Access	Valid Accounts: Cloud Accounts	T1078.004	Uso de credenciales válidas para acceso SSH.

3.3.3. Relevancia y criticidad

- T1040 y T1552.004 son altamente críticas, ya que permiten comprometer credenciales.
- T1205.002 (Port Knocking) es sofisticada y difícil de detectar.
- T1078.004 (uso de claves robadas) es común en ataques persistentes avanzados (APT).

3.4. DESARROLLO TÉCNICO

3.4.1 Metodología empleada

Se aplicaron técnicas apoyadas en herramientas como:

- **nmap**: detección de puertos abiertos y servicios.
- **ettercap**: ataque MITM con ARP spoofing.
- **Wireshark**: captura y análisis de tráfico.
- **Acceso a carpeta compartida** (vía NFS) y análisis de ficheros internos.
- **OpenSSH**: acceso remoto mediante clave privada.

3.4.2. Proceso de explotación (paso a paso)

Escaneo de red

Usamos `arp-scan` para identificar las máquinas ubicadas en la red:

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan 10.0.3.0/24 -v
[sudo] contraseña para kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:b4:a1:05, IPv4: 10.0.3.6
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.3.1        52:54:00:12:35:00       (Unknown: locally administered)
10.0.3.2        52:54:00:12:35:00       (Unknown: locally administered)
10.0.3.3        08:00:27:8e:2e:9e       (Unknown)
10.0.3.15       08:00:27:15:1f:29       (Unknown)
10.0.3.16       08:00:27:83:db:df       (Unknown)
—       Pass 1 complete
—       Pass 2 complete

5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.942 seconds (131.82 hosts/sec). 5 responded
```

Las dos máquinas identificadas son:

Nombre de la máquina	Dirección IP	Dirección MAC
Retillo	10.0.3.15	08:00:27:15:1f:29
Lubuntu	10.0.3.16	08:00:27:83:db:df

Escaneo de puertos

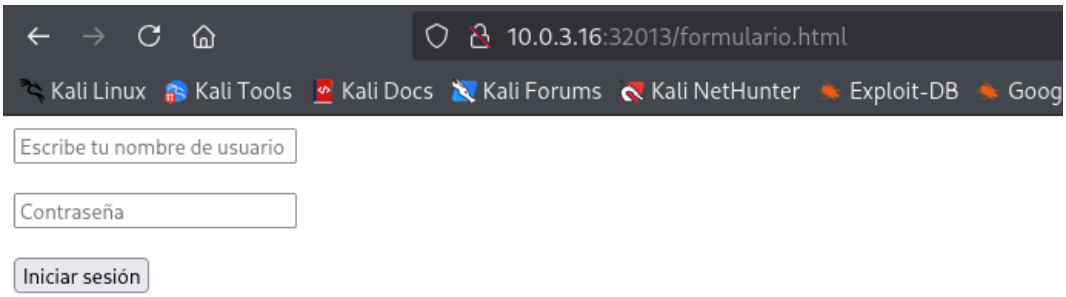
Usamos `nmap` para escanear ambas máquinas. Se comprueba que en la máquina *Retillo* no constan puertos abiertos:

```
┌──(kali㉿kali)-[~]
└─$ nmap 10.0.3.15 -sV -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-10 07:42 EDT
Nmap scan report for 10.0.3.15
Host is up (0.00036s latency).
All 65535 scanned ports on 10.0.3.15 are in ignored states.
Not shown: 65535 closed tcp ports (reset)
MAC Address: 08:00:27:15:1F:29 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.13 seconds
```

Sin embargo, en la máquina Lubuntu se detecta el puerto 32013/tcp abierto y corresponde al servicio HTTP y la versión Apache httpd 2.4.29:

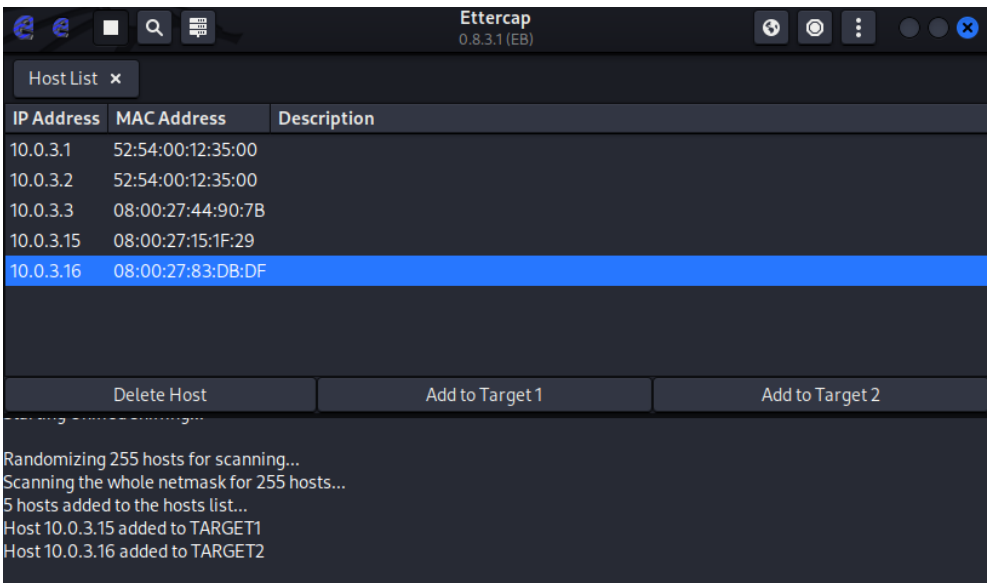
```
┌──(kali㉿kali)-[~]
└─$ nmap 10.0.3.16 -p- -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-09 13:22 EDT
Nmap scan report for 10.0.3.16
Host is up (0.044s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
32013/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
MAC Address: 08:00:27:83:DB:DF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.29 seconds
```

Si desde el navegador usamos como url: `10.0.3.16:32013`, este nos lleva a un formulario de login donde se solicita introducir credenciales de acceso:



Intercepción de tráfico (MITM)

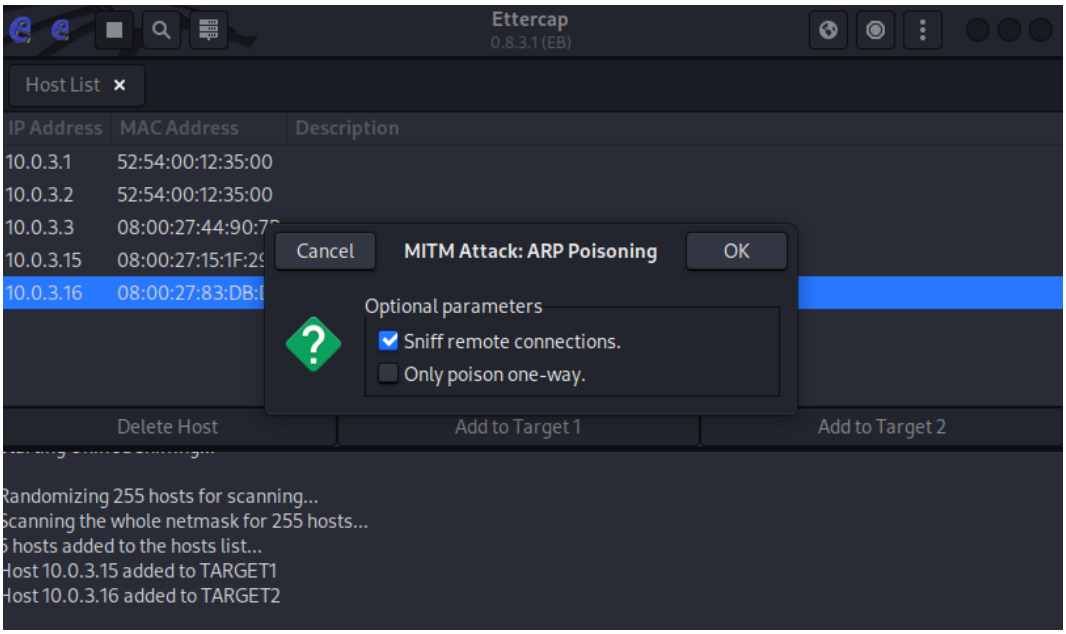
Se habilita un ataque MITM (Man in the middle) desde la máquina atacante, permitiendo interceptar y capturar tráfico transferido en texto plano entre las máquinas de la red (*Retillo* y *Lubuntu*).



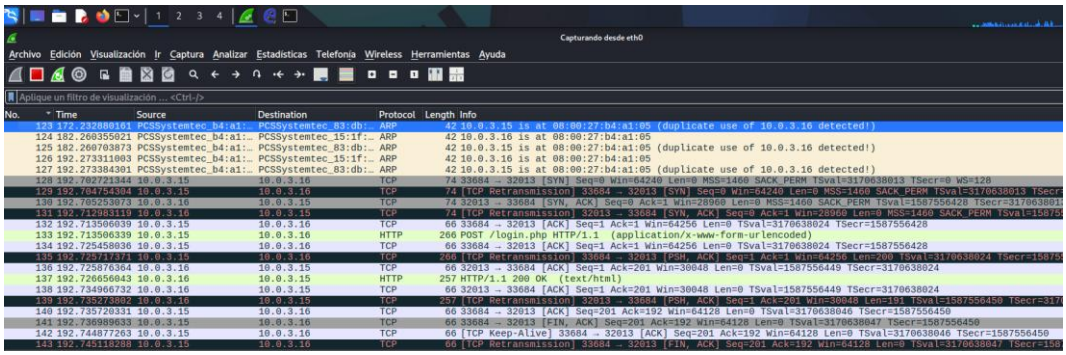
Para ello, se usa la herramienta ettercap. Primeramente, se efectua un escaneo de hosts y se añaden las máquinas 10.0.3.15 (Retillo) y 10.0.3.16 (Lubuntu)

como Target 1 y Target 2 respectivamente.

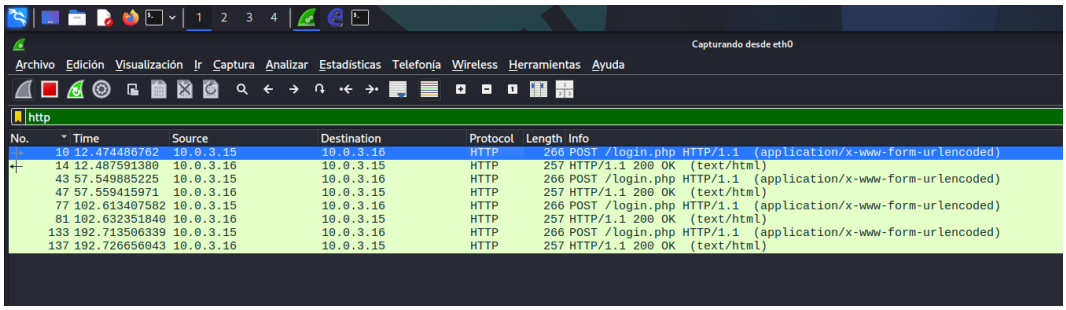
A continuación, desde ettercap, se realiza el ataque MITM mediante ARP poisoning o ARP spoofing (*envenenamiento o suplantación de ARP*): se envian mensajes ARP falsos a la red para asociar la dirección MAC del atacante con la IP del host atacado, y así cualquier tráfico dirigido a la dirección IP de ese host, será erróneamente enviado al atacante, en lugar de a su destino real.



Con la herramienta Wireshark previamente abierta, comenzamos a capturar el tráfico existente:



Se observa que existe tráfico HTTP entre las máquinas 10.0.3.15 (Retillo) y 10.0.3.16 (Lubuntu). Son peticiones del cliente y respuestas del servidor. Se filtra en Wireshark por HTTP para que se visualice mejor:

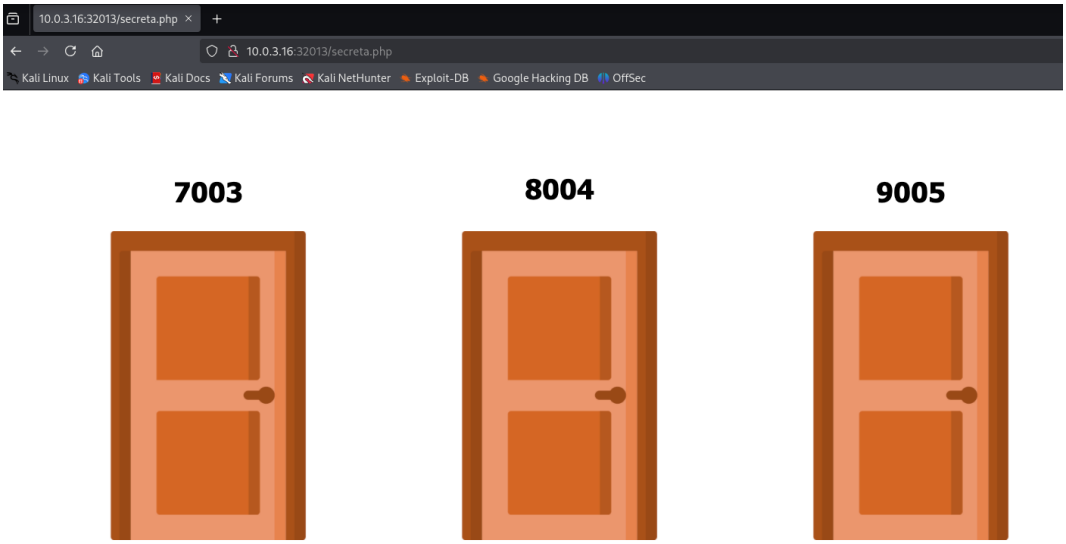


Analizando detalladamente el tráfico HTTP capturado se puede observar que se envían unas credenciales en texto plano y sin cifrar: `usuario=admin & palabra_secreta=LaBarbacoa`.

```
POST /login.php HTTP/1.1
Host: 10.0.3.16:32013
User-Agent: curl/7.68.0
Accept: */*
Content-Length: 42
Content-Type: application/x-www-form-urlencoded

usuario=admin & palabra_secreta=LaBarbacoa
HTTP/1.1 200 OK
Date: Tue, 08 Jul 2025 22:52:48 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 43
Content-Type: text/html; charset=UTF-8

El usuario o la contrase..a son incorrectos
```

Uso de credenciales de acceso capturadas

Se prueban las credenciales de acceso obtenidas (user: `admin`, pass: `LaBarbacoa`) en la aplicación web presente en 10.0.3.16:32013 y se consigue acceso, mostrándose a continuación la siguiente página:

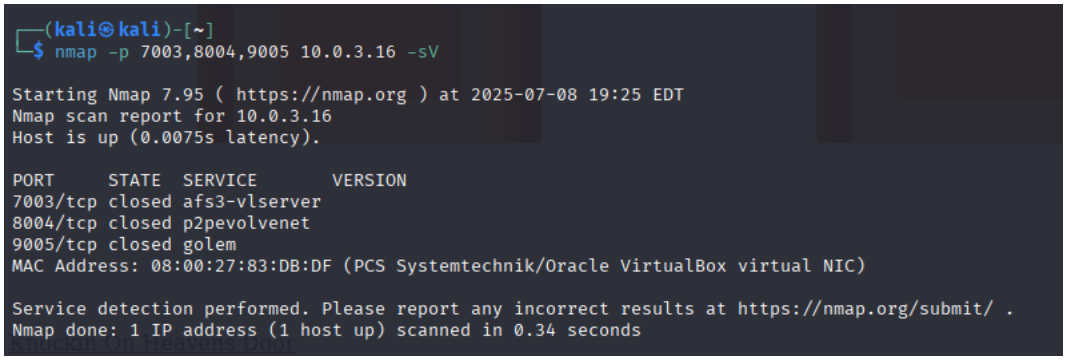


Se muestran tres puertas numeradas y en la parte inferior un enlace a Youtube de una canción titulada *"Knocking on heavens door"*, lo que da una pista sobre el siguiente paso en la explotación, que sería usar port knocking.

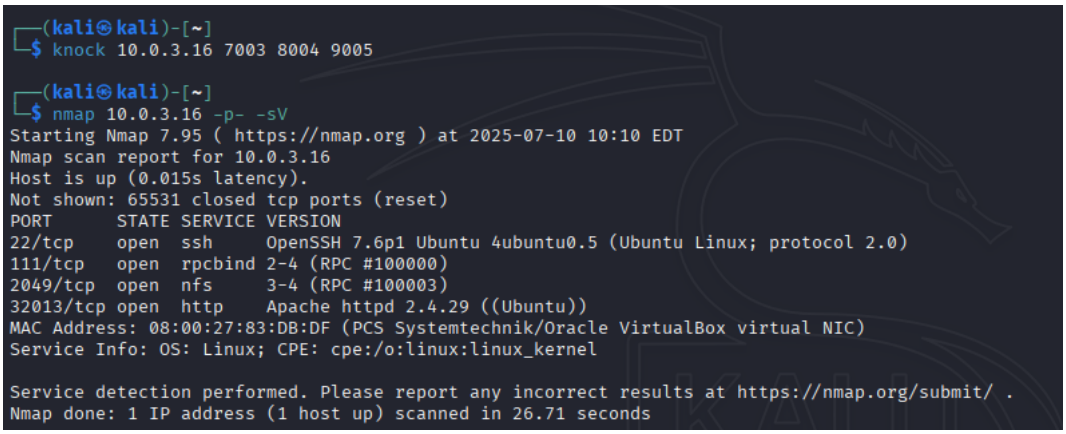
Uso de port knocking

El port knocking (*golpeo de puertos*) es una técnica de seguridad de redes que permite ocultar servicios en un servidor abriendo puertos específicos solo después de recibir una secuencia predefinida de intentos de conexión a puertos cerrados. Básicamente, se trata de "llamar" a un puerto específico con una secuencia de conexiones a otros puertos cerrados, y si la secuencia es correcta, el firewall abre el puerto deseado para la conexión legítima.

En este caso, la secuencia de puertos cerrados son 7003, 8004 y 9005:

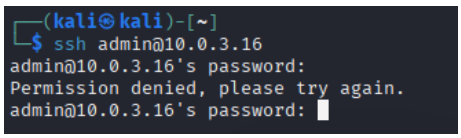


Para aplicar el port knocking usamos el comando `knock` a los tres puertos cerrados, y a continuación, al escanear de nuevo con nmap, se encuetran nuevos puertos abiertos en la máquina 10.0.3.16 (Lubuntu): 22/tcp ssh, 111/tcp rpcbind y 2049/tcp nfs:



Acceso a recurso compartido

El primer intento podría ser acceder vía SSH, una vez abierto dicho puerto, con las credenciales obtenidas anteriormente en la aplicación web (user: `admin`, pass: `LaBarbacoa`), pero el resultado es infructuoso:

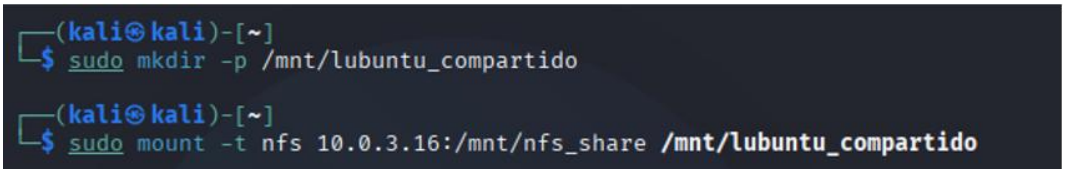


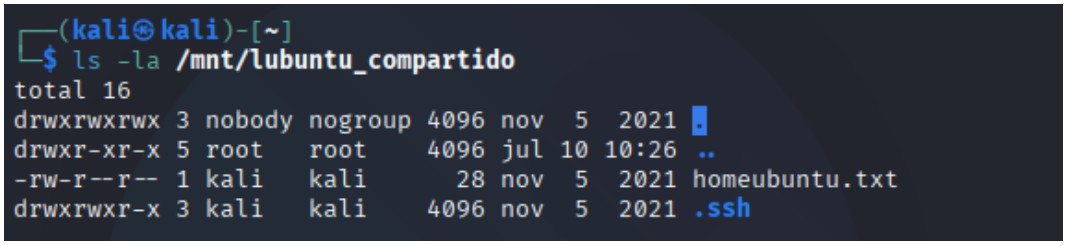
Por tanto, se exploran otras opciones, y en este caso se hace uso del puerto 2049/tcp con NFS (*network file system o sistema de archivos de red*), que es un protocolo que permite a varios dispositivos conectados a una misma red acceder y compartir archivos como si estuvieran en su propio disco duro.

Se prueba con el comando `showmount -e 10.0.3.16`, para comprobar qué recursos están disponibles vía NFS en el servidor Lubuntu, y se encuentra lo siguiente:

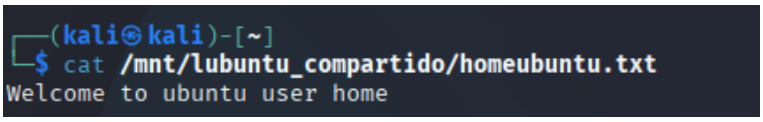
El servidor tiene activo un recurso NFS exportado públicamente: `/mnt/nfs_share *`, y el asterisco indica que cualquier cliente puede montar dicho recurso. Por tanto, a continuación, se monta el recurso:

- Se crea un punto de montaje local en la máquina Kali: `sudo mkdir -p /mnt/lubuntu_compartido`
- Se monta el recurso: `sudo mount -t nfs 10.0.3.16:/mnt/nfs_share /mnt/lubuntu_compartido`
- Se accede al recurso: `ls -la /mnt/lubuntu_compartido`

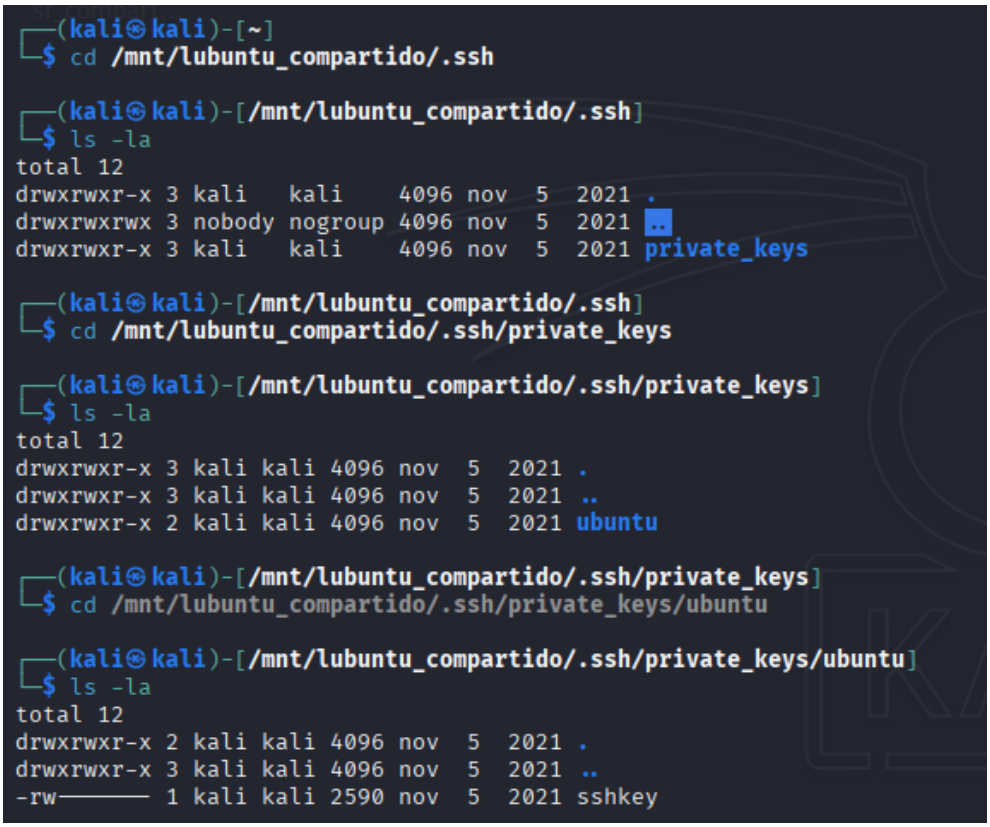




Al realizar cat al archivo `homeubuntu.txt` nos muestra que el recurso compartido es del usuario `ubuntu`:



Se obtiene un usuario y se necesita una contraseña, por lo que se debe explorar la estructura de directorios del recurso compartido:



Se localiza una clave privada en la ruta `/mnt/lubuntu_share/.ssh/private_keys/ubuntu/sshkey`

```
┌──(kali㉿kali)-[/mnt/lubuntu_compartido/.ssh/private_keys/ubuntu]
└─$ cat /mnt/lubuntu_compartido/.ssh/private_keys/ubuntu/sshkey
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAvAIfgoXmljQsH/jMSHeSmw1GSwVnfBgbETzNO8Ybpis2KCI7ZfIl
OodKX80zYFztSvkkmFSWp2qsRHKDCSM9E8x+Fm3JwdQLXxQzqBhxGTggXDWUJzfN5E2SDV
ZUv9ln3VW43ApmbsA/0dMIOyQejFyT8RyrvXNGTNGoUOtb7ke+Skmz+3SRkckP7GSV+mGZ
lvPallVspR0T/z31+aopm3Eq5h3PhjEzeF8Mf7uhMzCUon9NcfP7BFDR5VJb6J6CPJA8fY
5+T4g8ZisLffN2yxB57Dwy+qiykd66EzKAa4Xbv9U18pVAwVCWYsvwpoTsPJQBmlHw3gsN
rQIc7NBVQKhVAQ87JTnjfEaWYQntGVQ+xaECrzcJXMwRtoHZk5R5+sr2nNM3r+DgoPP5Hp
i/KV2uJ1+HpPXhhtk6YU9AWFAI3wAJRj845Torpaubng3rS2Ql8TDeflBwtWvc6eXxGtSS
3aqc3iJKI2yHfcbrUHLNBB7+6Iq3zTFc9TcXxoA5AAAFgIqhhRKKoYUSAAAAB3NzaC1yc2
EAAAGBALwCH4KF5pY0LB/4zEh3kpsNRksFZ3wYGxE8zTvGG6YrNigiO2XyJTqHSl/NM2Bc
7Ur5JJhUlqdqrERygwkjPRPMfhZtycHUC18UM6gYcRk4IFw1lCc3zeRNkg1WVL/ZZ91VuN
wKZm7AP9HTCDskHoxck/Ecq71zRkzRqFDrW+5HvkpJs/t0kZHJD+xklfphmZbz2pZVbKUd
E/899fmqKZtxKuYdz4YxM3hfDH+7oTMwlKJ/TXHz+wRQ0eVSW+iegjyQPH2Ofk+IPGYrC3
3zdssQeew8MvqospHeuhMygGuF27/VNfKVQMFQlmLL8KaE7DyUAZpR8N4LDa0CHOzQVUCo
VQEPOyU543xGlmEJ7RlUPsWhAq83CVzMEbaB2ZOUefrK9pzTN6/g4KDz+R6Yvyldridfh6
T14YbZOmFPQFhQCN8ACUY/OOU6K6Wrm54N60tkJfEw3n5QcLVr3Onl8RrUkt2qnN4iSiNs
h33G61ByzQQe/uiKt80xXPU3F8aAOQAAAAMBAAEAAAGBAK3eSMWsj1LZbPUkYceizTIXVK
qMlOduY5nNYP+mdmt2Ct+SyNu+1C8MbvuqCZlUVx6+ydkWYTzyqd2jCQuqSxHES9byMWPP
dbS4Og16jR2Fime8JQcf1IkOM8Oh0z6ZEDTg0dSsyY4ivOKPB02qWZX1B9wzZ6AMuzbPrZ
koEByMvK52+rvRUc5A4zj6zLiBCklPuxbMaW1JNvUVmCUL+O6H+eRWLVUsqyzmuehm3O06
QDsG/9giikGzfGlXgSffbXwd2u0NgPipYmuoSeQS0eebJIp3DPZA/JVwtt0zpT52rZ8BDS
EG12yCMAGnn0oSdjfE0lxWql6mFNhN+agbjHHb5zXLbcThWA0o8miWQzCHMM6/0t5Jg4Ww
rSiKxm0treraOaGSbXYLeHlU1Nn9kP0ZqoEYxcHdxC+bfOPc70zpFVgkDkCZiic2qoKhDO
EdDpHf/2siwVNuv+2xONKOdqB8wlvc3cY5WDiGzlrTI/na0odoF+I4NOYra8aaBUUnAQAA
AMEA3ERKP9MlJxY2jIyZ2Dmo/op1zde/rcc8tAkqV+1S6eW2j5XOHJA35nX2UB5Y02lCAd
CcYAgCWOs88OBhid/EPRjZHqS9GJ4HHG72uCBDoXe6GvEVrY1232y1A33KmUDD8E1qNGf+
R+nKcaucPfBOygU/TMTZq81uQZXXkjtFFDjOHyRUr34nv8uEVw9m0e7/X1Kbc+6X3A1M/Q
n9Knz9i7InbRpY73g/xDIDo0LVBoJkUpKRnxV8cvJPYsn+W5PyAAAAwQDiJg+54epFQYMK
Fjh4Hp7nCBrYSovTQmzklI4rpbCtQCDqARGAAoQ7bJO3KxYeerpV1YS/QPggmqG1JunnKX
7RrlRwlM7K61IgrFrGGDudEsWCyh9xdkKxDguabWFA3s12zm0qmfnG2bKiHh2uHbFrsvTN
vLBHsXFOhD69Y+TD5LNsi/lb6EF8yJtBJnZH6049MyVntCC+7pnnMs990i9RCCu6k6ndgb
Hty/tA9QJ++F5tLQWJX0/iFS4Gbt8hg88AAADBANTTPCB++AkEG/C3Vc8aoU7kXdZ2jhep
XnPJ+/9t+92DLaH/v73pALLtWfhNLu8YQC97rJBIXEP+IEiJfA1m0YLPdHXFscIMfFif6V
oHZ6hGeBZM4POQPqHKPoBnzYKbm6bTBdCEVE/IRGmO+LUQ52B+fk5EvQexoALxlbrJwZY1
ZNm/DQ6qc8FgupeQKexClL9UV4kSlcfUYEg0Bht9JVc7oWx8noMZCC9HT4rNltqsqRsocr
SGaJngGEjG0cnVdwAAAAlrYWxpQGthbGk=
-----END OPENSSH PRIVATE KEY-----
```

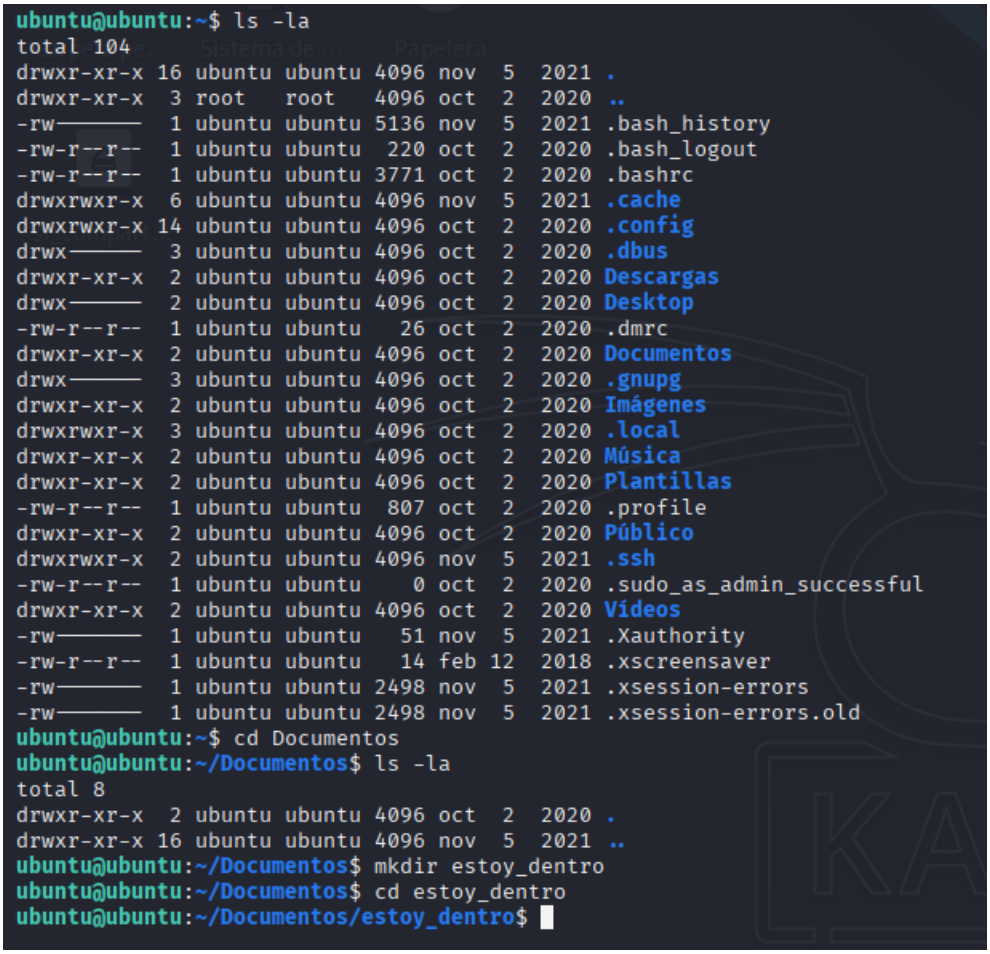
Este archivo corresponde a una clave privada SSH sin passphrase.

Acceso remoto a la máquina Lubuntu

Usando la clave privada obtenida, se logró establecer una conexión remota como el usuario legítimo `ubuntu`, mediante el comando: `ssh -i sshkey ubuntu@10.0.3.16`

```
┌──(kali㉿kali)-[/mnt/lubuntu_compartido/.ssh/private_keys/ubuntu]
└─$ ssh -i sshkey ubuntu@10.0.3.16
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-20-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


Pueden actualizarse 593 paquetes.
385 actualizaciones son de seguridad.

Last login: Wed Jul  9 01:53:43 2025 from 10.0.3.6
ubuntu@ubuntu:~$
```

Y una vez dentro, permite la ejecución completa de comandos en el sistema comprometido:



CONCLUSIONES

La evaluación ha revelado varias deficiencias críticas en la seguridad del entorno auditado:

1. **Gestión inadecuada de credenciales sensibles**, como claves privadas SSH sin protección, disponibles en rutas accesibles desde otras máquinas.
2. **Tráfico susceptible a intercepción**, lo que permite a un atacante con acceso a la red recopilar información crítica sin necesidad de explotar vulnerabilidades complejas.
3. **Falta de controles de aislamiento y segmentación**, que posibilita el acceso a recursos que deberían estar protegidos.

Estas debilidades han permitido obtener control total sobre el sistema interno, por lo que se recomienda implementar medidas de mitigación, como las siguientes:

- Cifrado de todas las comunicaciones internas (HTTPS, SSH, VPN).
- Protección de claves privadas con passphrase y control de acceso a rutas sensibles.
- Monitorización de accesos y comparticiones de red.
- Segmentación de redes y aplicación de políticas de mínimos privilegios.