Hacking Ético Interno

Informe Ejecutivo / Técnico

TABLA DE CONTENIDOS

1. Introducción

El presente informe documenta el análisis de vulnerabilidades realizado sobre la máquina virtual Metasploitable 2, utilizando diversas herramientas de escaneo y metodologías estándar de seguridad. Este ejercicio tiene como objetivo identificar vulnerabilidades críticas, altas y medias, explicando su impacto y posibles medidas de mitigación. El trabajo se efectuó en un entorno controlado con una red configurada exclusivamente para este fin.

---

2. Objetivo

Identificar y analizar vulnerabilidades presentes en la máquina virtual Metasploitable 2 para comprender los riesgos asociados a cada fallo de seguridad y proponer recomendaciones que mitiguen dichos riesgos en entornos reales.

---

3. Alcance

Este análisis se limita al entorno de prueba configurado con las siguientes características:

- Máquinas virtuales aisladas mediante red "Host-Only".
- Uso exclusivo de herramientas de software libre o evaluación en Kali Linux.
- Escaneo de puertos, servicios y vulnerabilidades en la máquina objetivo (IP: 10.0.2.4).

No se consideraron otros equipos ni redes externas en el análisis.

---

4. Metodología de Trabajo

1. **Entorno de Trabajo:**
    - VM con Kali Linux (IP: 10.0.2.15/24).
    - VM con Metasploitable 2 (IP: 10.0.2.4).
2. **Herramientas Utilizadas:**
    - **Nmap:** Descubrimiento y enumeración de puertos.
    - **Nikto:** Escaneo de vulnerabilidades en aplicaciones web.
    - **Skipfish:** Generación de reportes automatizados.
3. **Fases:**
    - Identificación de servicios activos.

- Clasificación de vulnerabilidades según criticidad.
- Propuesta de medidas de mitigación.

---

5. Informe Ejecutivo

El análisis identificó múltiples vulnerabilidades en el sistema objetivo, destacando las siguientes:

- Acceso anónimo al servicio FTP (puerta trasera).
- Exposición de configuraciones sensibles en phpinfo.php.
- Uso de versiones obsoletas en Apache y MySQL.
- Directorios indexados y expuestos al acceso externo.

Se recomiendan actualizaciones de software, configuraciones seguras y deshabilitar servicios innecesarios para reducir riesgos.

---

6. Fortalezas y Debilidades

Fortalezas:

- Entorno diseñado para propósitos educativos.
- Múltiples servicios activos para simular entornos reales.

Debilidades:

- Uso de versiones antiguas y vulnerables de software.
- Configuraciones predeterminadas sin medidas de seguridad adicionales.
- Exposición de archivos sensibles y directorios indexados.

---

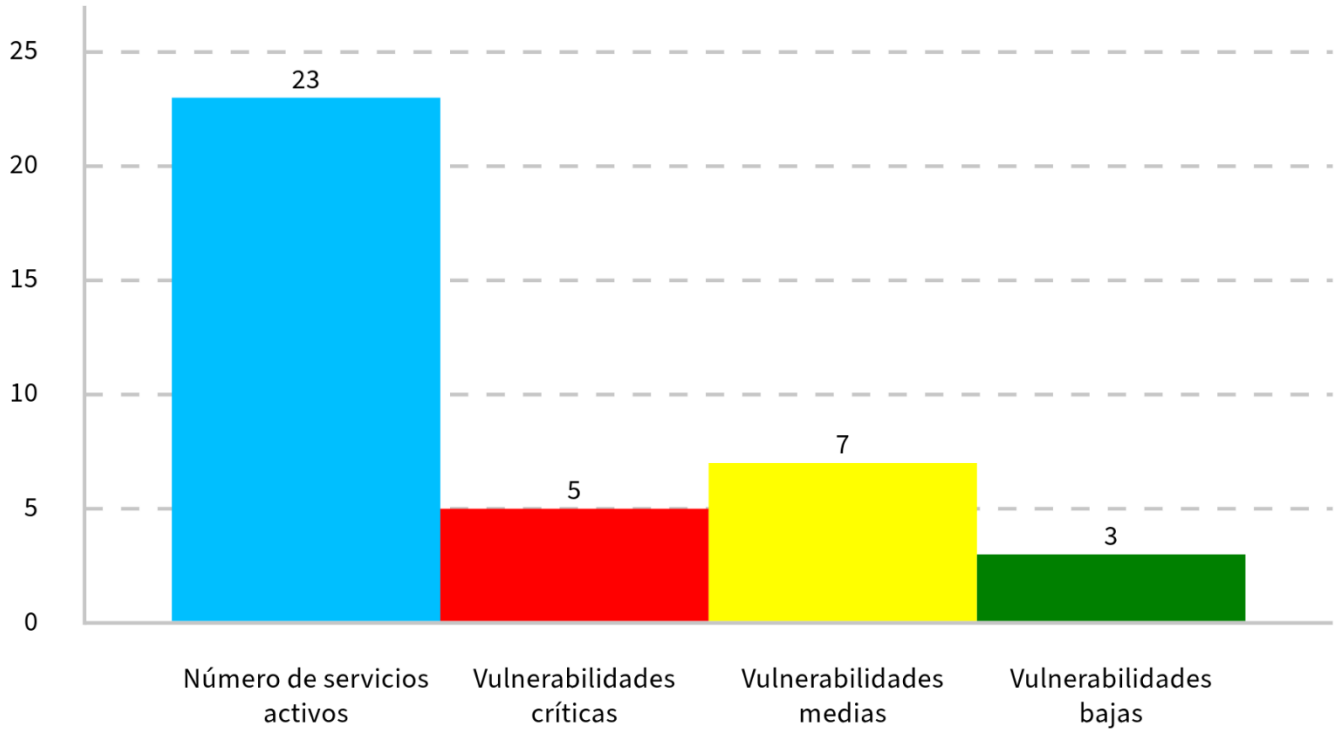
7. Análisis de Vulnerabilidades Detectadas – Riesgos – Recomendaciones

Tabla Resumen de Vulnerabilidades

Vulnerabilidad	Riesgo	Recomendación
phpMyAdmin expuesto	Compromiso completo del sistema	Restringir acceso o desinstalar
Backdoor en FTP (vsftpd 2.3.4)	Acceso remoto no autorizado	Deshabilitar el servicio FTP
Método TRACE activo	Exposición a ataques de Cross-Site Tracing (XST)	Deshabilitar el método TRACE
phpinfo.php accesible	Filtración de configuraciones sensibles	Restringir acceso mediante autenticación
Directorios indexados	Divulgación de información	Deshabilitar la indexación
Apache desactualizado	Vulnerabilidad a ejecución remota de código	Actualizar a una versión compatible y segura
MySQL desactualizado	Escalada de privilegios	Migrar a una versión moderna

8. Estadísticas

- **Número de servicios activos:** 23.
- **Vulnerabilidades críticas:** 5.
- **Vulnerabilidades medias:** 7.
- **Vulnerabilidades bajas:** 3.



9. Informe Técnico

El informe técnico incluye los detalles completos del análisis, junto con las capturas de pantalla y los comandos utilizados. Se adjunta como referencia en el anexo n° 14.

10. Resultados Obtenidos por Información Interna

El escaneo identificó vulnerabilidades relacionadas con configuraciones predeterminadas y software desactualizado, propias de la naturaleza de Metasploitable 2.

11. Enumeración de Vulnerabilidades a Través de Cada Herramienta Utilizada

- **Nmap:** Enumeración de puertos y servicios activos.
- **Nikto:** Vulnerabilidades en aplicaciones web y configuraciones inseguras.
- **Skipfish:** Reporte automatizado con vulnerabilidades adicionales.

---

12. Hoja de Revisión

Fecha	Revisado por	Comentarios
01/12/2024	Rodrigo Ezequiel Vila	Informe finalizado y revisado

---

13. Acuerdo de Confidencialidad

Toda la información contenida en este informe se considera confidencial y se utiliza exclusivamente con fines educativos. No debe ser compartida, distribuida o reproducida sin el consentimiento del autor.

---

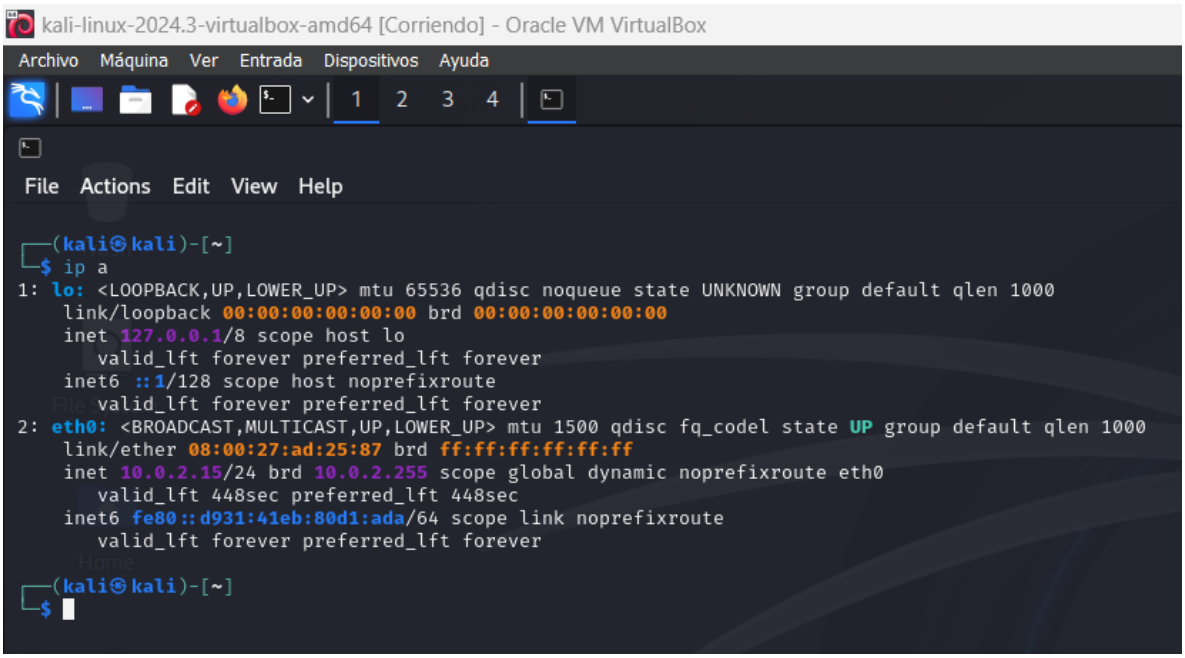
14. Procedimiento Paso a Paso

Desarrollo paso a paso del procedimiento:

1. Primero verifico mi ip para determinar el rango de ip que debo escanear para localizar la maquina con Metasploitable 2:

Ejecuto el comando: ip a

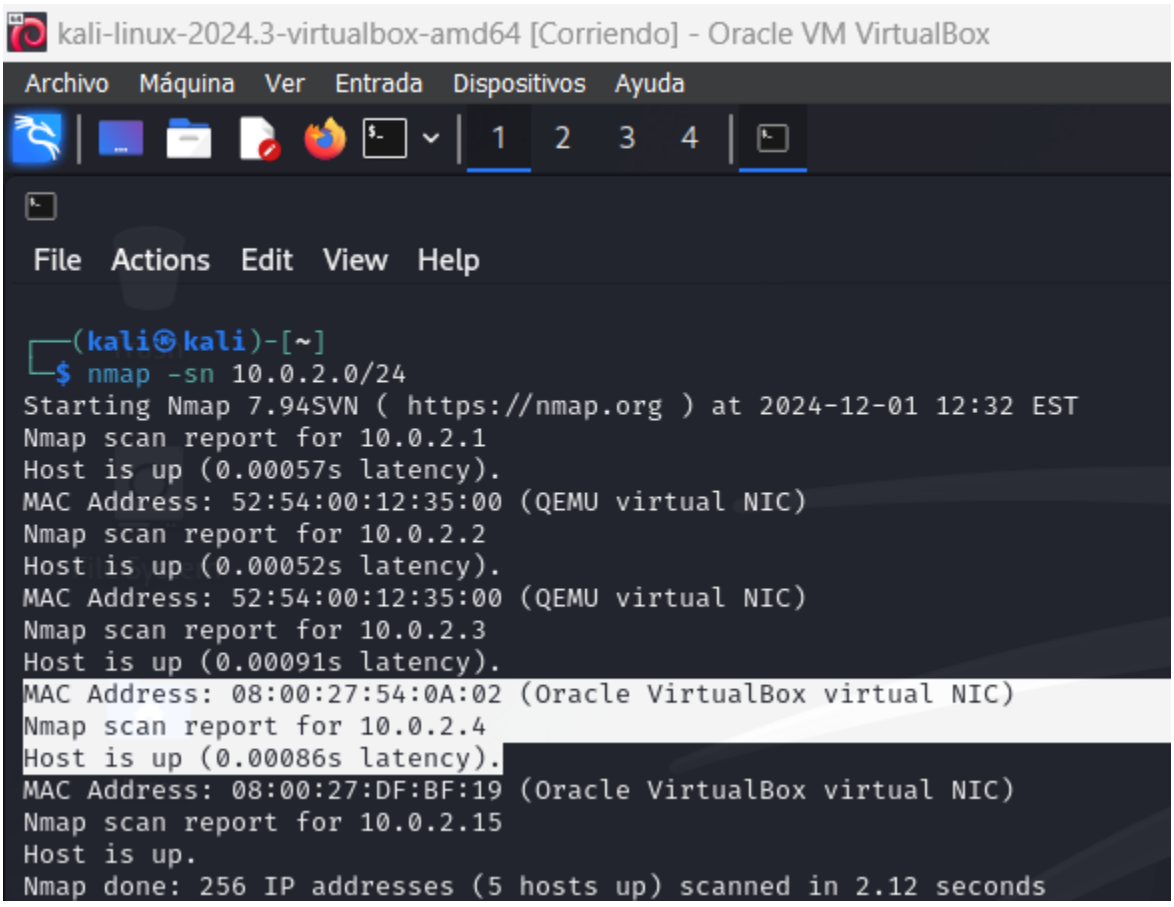
Mi ip es 10.0.2.15/24 lo que me indica que debo escanear el rango de ip 10.0.2.0/24



2. Utilizo Nmap para identificar dispositivos activos:

nmap -sn 192.168.1.0/24

(-sn: Realiza un escaneo de ping para identificar dispositivos activos en la red.)



Encuentro 2 dispositivos VirtualBox, uno corresponde a la VM con Kali Linux que estoy utilizando y el segundo, por deducción corresponde a la VM con Metasploitable 2, cuya IP es 10.0.2.4

3. Realizo un escaneo completo para identificar los servicios activos y sus versiones:

nmap -A 10.0.2.4

(-A: Habilita detección de sistema operativo, servicios y scripts NSE básicos.)

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 12:38 EST
Nmap scan report for 10.0.2.4
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.15
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2024-12-01T17:38:54+00:00; -6s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME,
DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/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
| sslv2:
```

| SSLv2 supported

| ciphers:

| SSL2_DES_192_EDE3_CBC_WITH_MD5

| SSL2_DES_64_CBC_WITH_MD5

| SSL2_RC4_128_WITH_MD5

| SSL2_RC2_128_CBC_WITH_MD5

| SSL2_RC4_128_EXPORT40_WITH_MD5

|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5

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 33296/tcp mountd

| 100005 1,2,3 60078/udp mountd

| 100021 1,3,4 43114/udp nlockmgr

| 100021 1,3,4 55083/tcp nlockmgr

| 100024 1 34284/udp status

|_ 100024 1 38064/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

514/tcp open tcpwrapped

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: 9

| Capabilities flags: 43564

| Some Capabilities: LongColumnFlag, Speaks41ProtocolNew, SwitchToSSLAfterHandshake, SupportsCompression, ConnectWithDatabase, SupportsTransactions, Support41Auth

| Status: Autocommit

|_ Salt: +EXj,<(QB7.|J>5-$kni

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/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: 2024-12-01T17:38:54+00:00; -6s 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-server-header: Apache-Coyote/1.1

|_http-title: Apache Tomcat/5.5

|_http-favicon: Apache Tomcat

MAC Address: 08:00:27:DF:BF:19 (Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Network Distance: 1 hop

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

| smb-security-mode:

| account_used: <blank>

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

| smb-os-discovery:

| OS: Unix (Samba 3.0.20-Debian)

| Computer name: metasploitable

| NetBIOS computer name:

| Domain name: localdomain

| FQDN: metasploitable.localdomain

|_ System time: 2024-12-01T12:38:46-05:00

|_smb2-time: Protocol negotiation failed (SMB2)

|_clock-skew: mean: 1h14m54s, deviation: 2h30m01s, median: -6s

TRACEROUTE

HOP RTT ADDRESS

1 1.46 ms 10.0.2.4

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 24.27 seconds

Puertos y Servicios Identificados:

1. **Puerto 21 (FTP):**
    - **Servicio:** vsftpd 2.3.4
    - **Observación:** Permite acceso anónimo (¡muy inseguro!).
    - **Vulnerabilidad conocida:** La versión 2.3.4 tiene una vulnerabilidad de puerta trasera (backdoor), explotable para acceso remoto.
2. **Puerto 22 (SSH):**
    - **Servicio:** OpenSSH 4.7p1
    - **Observación:** Versión antigua y vulnerable a ataques como fuerza bruta o exploits específicos.
3. **Puerto 23 (Telnet):**
    - **Servicio:** Linux telnetd
    - **Observación:** Telnet no encripta las conexiones, lo que lo hace susceptible a ataques de intercepción (sniffing).
4. **Puerto 25 (SMTP):**
    - **Servicio:** Postfix smtpd
    - **Observación:** Certificados SSL/TLS caducados, posibilidad de ataques de tipo man-in-the-middle.
5. **Puerto 53 (DNS):**
    - **Servicio:** ISC BIND 9.4.2
    - **Observación:** No se indica vulnerabilidad directa, pero el servicio de DNS puede ser objetivo de ataques de denegación de servicio (DoS) o manipulación de tráfico DNS.

6. **Puerto 80 (HTTP):**
    - **Servicio:** Apache httpd 2.2.8
    - **Observación:** Versión vulnerable a varios ataques, incluida la ejecución remota de código (RCE) a través de fallos en módulos.
7. **Puerto 111 (RPCbind):**
    - **Servicio:** rpcbind 2
    - **Observación:** El servicio RPC se encuentra en ejecución, lo que lo hace susceptible a ataques de desbordamiento de búfer y explotación de vulnerabilidades de NFS.
8. **Puerto 139 (NetBIOS-SSN):**
    - **Servicio:** Samba smbd 3.X - 4.X
    - **Observación:** La versión es vulnerable a ataques como el famoso EternalBlue.
9. **Puerto 445 (NetBIOS-SSN):**
    - **Servicio:** Samba smbd 3.0.20-Debian
    - **Observación:** La versión es vulnerable a ataques como el famoso EternalBlue.
10. **Puerto 512 (Exec):**

- **Servicio:** netkit-rsh rexecd
- **Observación:** El servicio rexecd permite la ejecución remota sin autenticación adecuada, lo que puede ser aprovechado por atacantes para obtener acceso a la máquina.

11. **Puerto 513 (Login):**

- **Servicio:** login
- **Observación:** Servicio antiguo y vulnerable a ataques de acceso no autorizado.

12. **Puerto 514 (TCPWrapped):**

- **Servicio:** tcpwrapped
- **Observación:** Puede indicar que el servicio está envuelto en un servicio de seguridad, pero aún es vulnerable dependiendo de la configuración interna.

13. **Puerto 1099 (Java-RMI):**

- **Servicio:** GNU Classpath grmiregistry
- **Observación:** El servicio de Java RMI puede ser vulnerable a ataques de ejecución remota de código (RCE).

14. **Puerto 1524 (Backdoor):**

- **Servicio:** bindshell
- **Observación:** Un backdoor clásico configurado intencionadamente en Metasploitable 2.

15. **Puerto 2049 (NFS):**

- **Servicio:** NFS 2-4 (RPC #100003)

- **Observación:** El servicio NFS tiene vulnerabilidades conocidas que permiten el acceso no autorizado a archivos compartidos.

16. **Puerto 2121 (FTP):**

- **Servicio:** ProFTPD 1.3.1
- **Observación:** La versión de ProFTPD en Metasploitable 2 tiene vulnerabilidades conocidas que permiten la ejecución remota de código.

17. **Puerto 3306 (MySQL):**

- **Servicio:** MySQL 5.0.51a
- **Observación:** Versión antigua con vulnerabilidades conocidas.

18. **Puerto 5432 (PostgreSQL):**

- **Servicio:** PostgreSQL DB 8.3.0 - 8.3.7
- **Observación:** Versión vulnerable a ataques de inyección SQL y acceso no autorizado.

19. **Puerto 5900 (VNC):**

- **Servicio:** VNC (protocol 3.3)
- **Observación:** La versión de VNC es vulnerable a ataques de fuerza bruta o de tipo man-in-the-middle.

20. **Puerto 6000 (X11):**

- **Servicio:** X11
- **Observación:** El servicio X11 puede ser explotado por atacantes para obtener acceso a la interfaz gráfica de la máquina.

21. **Puerto 6667 (IRC):**

- **Servicio:** UnrealIRCd
- **Observación:** La versión que viene en Metasploitable tiene un backdoor conocido.

22. **Puerto 8009 (AJP13):**

- **Servicio:** Apache Jserv (Protocol v1.3)
- **Observación:** Puede estar expuesto a ataques de inyección o denegación de servicio, aunque no se reportan vulnerabilidades inmediatas.

23. **Puerto 8180 (HTTP):**

- **Servicio:** Apache Tomcat/Coyote JSP engine 1.1
- **Observación:** La versión es muy antigua y vulnerable a diversas fallas de seguridad, como ejecución remota de código.

4. Realizo el escaneo de vulnerabilidades. Hay mucho para elegir pero decido centrarme en la herramienta Nikto y el puerto 80 dado que es el puerto más comúnmente asociado con aplicaciones web. La mayoría de las aplicaciones web y servicios HTTP escuchan en este puerto.

Ejecutamos el escaneo al puerto 80 de la maquina Metasploitable 2:

nikto -h http://10.0.2.4:80

Resultados resumidos del analisis:

Información General:

- **IP objetivo**: 10.0.2.4
- **Servidor web**: Apache/2.2.8 (Ubuntu) DAV/2
- **PHP**: Versión PHP/5.2.4-2ubuntu5.10.
- **Tiempo de ejecución**: 32 segundos, 8910 solicitudes.

Resultados de Vulnerabilidades Detectadas:

1. **Cabeceras HTTP faltantes o inseguras**:
    - **X-Frame-Options**: No está presente, lo que deja al servidor vulnerable a ataques de *clickjacking*.
    - **X-Content-Type-Options**: No configurado, lo que podría permitir que el agente de usuario renderice el contenido de una manera diferente a su tipo MIME esperado.
2. **Cabeceras inusuales**:
    - **tcn**: Se detectó un encabezado poco común con el valor "list", que puede ser un error o información no deseada.
3. **Vulnerabilidades en Apache**:
    - El servidor **Apache/2.2.8** está desactualizado. La última versión conocida es **Apache/2.4.54**, y la **2.2.34** llegó al fin de vida (EOL), lo que significa que no recibirá actualizaciones de seguridad.
4. **Métodos HTTP inseguros**:
    - El **método TRACE** está activo, lo que puede permitir ataques de **Cross-Site Tracing (XST)**. Esto permite que un atacante pueda realizar ataques XSS o interceptar cabeceras HTTP.

5. **phpinfo.php**:
    - Se encontró un archivo phpinfo.php, lo cual es peligroso porque revela información detallada sobre la configuración del servidor y su entorno de ejecución.
6. **Indexado de directorios**:
    - **/doc/** y **/test/**: Directorios con *indexing* habilitado, lo que permite que los atacantes vean el contenido del directorio.
    - **/icons/**: También tiene indexación habilitada y contiene un archivo README, que es un archivo predeterminado de Apache y puede contener información sensible.
7. **Archivos sensibles revelados**:
    - **phpMyAdmin**: Se detectaron varias rutas relacionadas con **phpMyAdmin**, como changelog.php, ChangeLog, y Documentation.html, lo que indica que el servidor tiene phpMyAdmin instalado y es accesible sin restricciones. Esto es un riesgo significativo, ya que phpMyAdmin es una herramienta para gestionar bases de datos MySQL y debe estar protegida o restringida.
    - **Archivo wp-config.php**: Se detectó la ruta **#wp-config.php#**, que generalmente contiene las credenciales de conexión a la base de datos de WordPress, lo que es una grave vulnerabilidad si se puede acceder.
8. **Vulnerabilidades PHP**:
    - Se encontraron múltiples rutas de **PHP** con cadenas de consulta específicas que pueden revelar información sensible sobre la configuración del sistema. Estos casos están relacionados con el **OSVDB-12184**.

Resumen de riesgos:

- **Alta gravedad**:
    - **phpMyAdmin** expuesto y accesible sin protección.
    - **phpinfo.php** expuesto, revelando detalles sensibles del sistema.
    - **Método TRACE activo**, lo que permite ataques de **XST**.
    - **Versiones antiguas de Apache** que ya no reciben actualizaciones de seguridad.
- **Media gravedad**:
    - **Directorios indexados**, lo que podría permitir la exploración de archivos sensibles.
    - **Cabeceras HTTP faltantes o inseguras**, lo que podría aumentar la superficie de ataque (aunque no necesariamente se pueden explotar directamente).
- **Baja gravedad**:
    - **Cabeceras inusuales** y **archivos predeterminados de Apache** que podrían no ser relevantes, pero aún así brindan información sobre la configuración del servidor.

Recomendaciones:

- **Actualizar Apache** a una versión segura que esté en soporte.
- **Deshabilitar el método TRACE** para evitar posibles ataques de XST.

- **Eliminar o proteger** los archivos y directorios sensibles como phpinfo.php, wp-config.php, y el acceso a **phpMyAdmin**.
- **Configurar adecuadamente las cabeceras HTTP** para mitigar ataques como *clickjacking* y *content sniffing*.
- **Deshabilitar la indexación de directorios** para evitar la exposición de contenido sensible.

Bueno, he categorizado manualmente y bajo mi propio criterio las vulnerabilidades en grave, media y alta gravedad. Ahora realizaré un escaneo con una herramienta que genere reporte automático ya categorizado y lo compararemos.

La herramienta de la que hablo es la que vimos en clase llamada “skipfish”. Procedemos:

Creamos una carpeta para guardar el reporte que se generará:

```
┌──(kali㉿kali)-[~]
└─$ mkdir Meta2
```

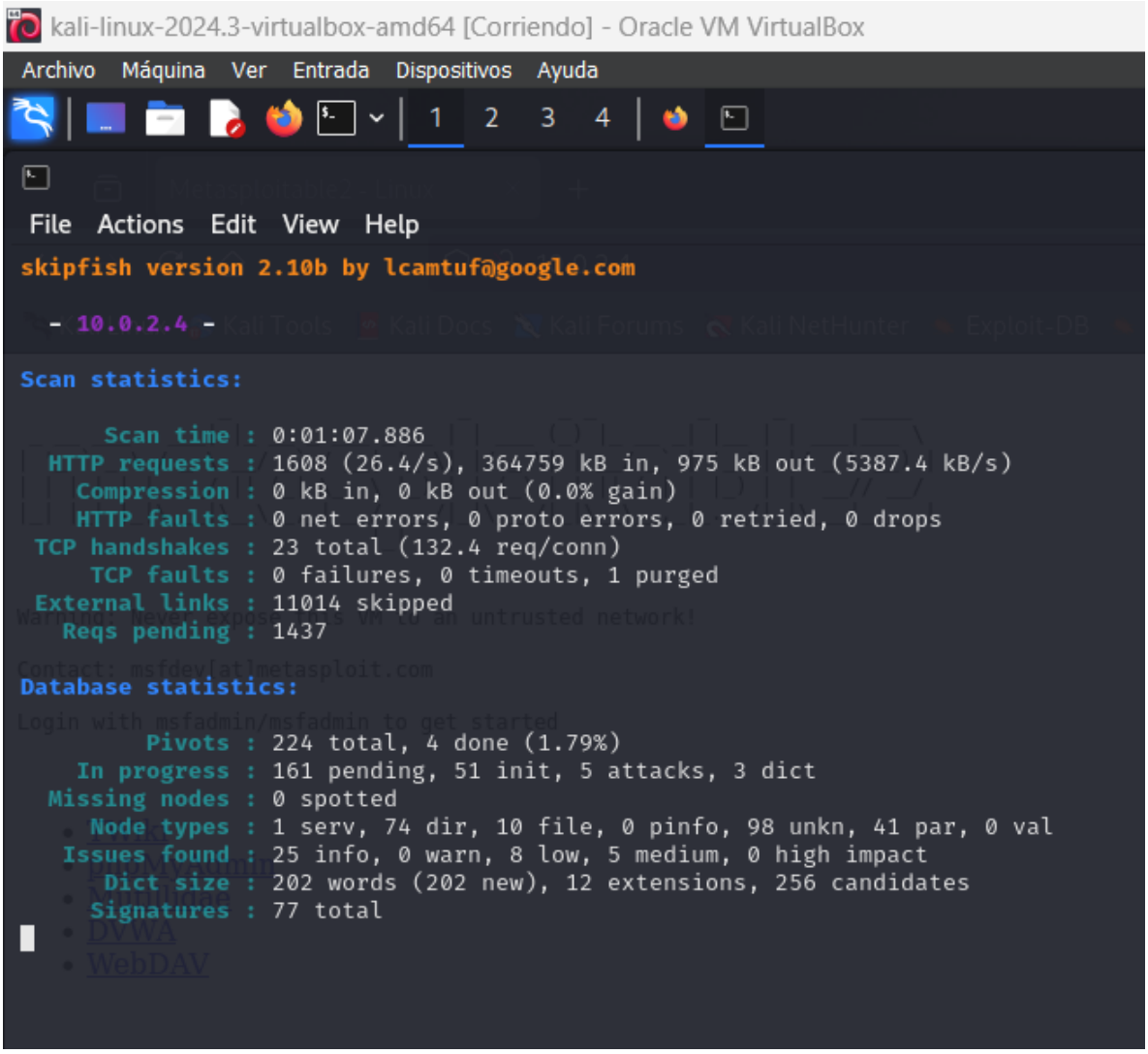
Ejecutamos el escaneo:

```
┌──(kali㉿kali)-[~]
└─$ skipfish -k 0:5:00 -o /home/kali/Meta2/ http://10.0.2.4:80
```

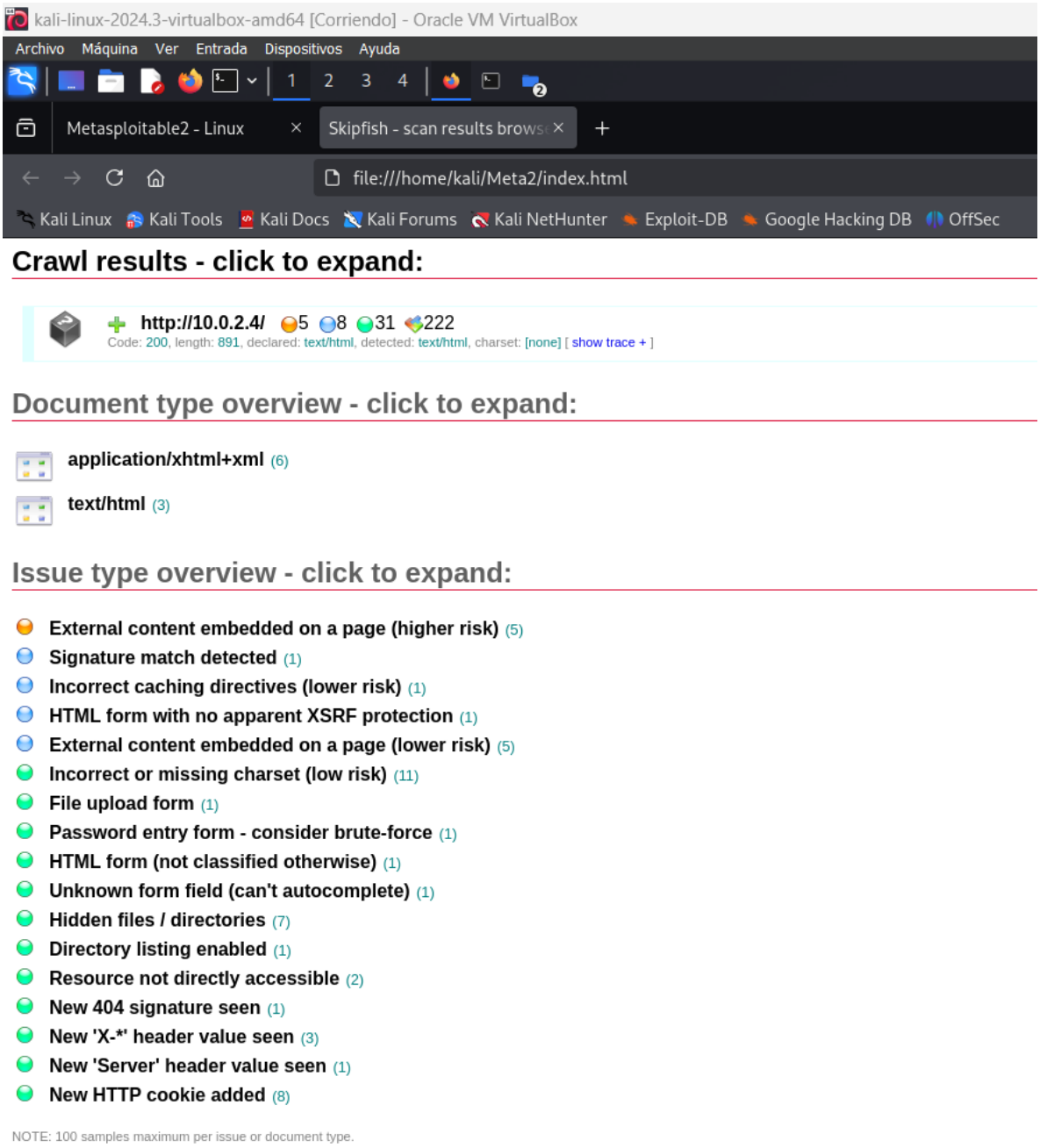
-k indica el tiempo del escaneo

-o indica el destino del reporte

Escaneo en proceso:



Resumen generado automáticamente con un tiempo de 5 minutos de escaneo:



Nota Final

Este informe se ha desarrollado con fines educativos y está basado en un entorno controlado diseñado para simular vulnerabilidades comunes. Los hallazgos y recomendaciones aquí documentados no representan una amenaza real, sino una guía para comprender la importancia de la seguridad informática en sistemas reales. Se sugiere seguir las mejores prácticas de seguridad en cualquier implementación de TI.

Rodrigo Ezequiel Vila.-