INFORME AUDITORÍA HACKING ÉTICO

Máquina virtual y Dominio de IMF

**XX/XX/2021**

**1. Introducción**

**1.1 Objetivo**

El objetivo de este informe es documentar el proceso y los resultados de dos fases del reto CTF. La primera fase consiste en el reconocimiento y escaneo de la organización IMF, mientras que la segunda fase implica la realización de un hacking ético a una máquina virtual estilo CTF.

**1.2 Alcance**

El alcance del análisis incluye:

* **Fase 1: Reconocimiento y Escaneo:** Recolección de información pública sobre IMF y detección de puertos y servicios abiertos en los servidores asociados con IMF.
* **Fase 2: Hacking Ético:** Ejecución de un hacking ético sobre una máquina virtual estilo CTF para identificar y explotar vulnerabilidades.

**2. Fase de Reconocimiento y Escaneo**

**2.1 Metodología**

La fase de reconocimiento se enfocó en la recopilación de información pública disponible sobre IMF utilizando diversas herramientas de OSINT (Open Source Intelligence).

**2.2 Herramientas Utilizadas**

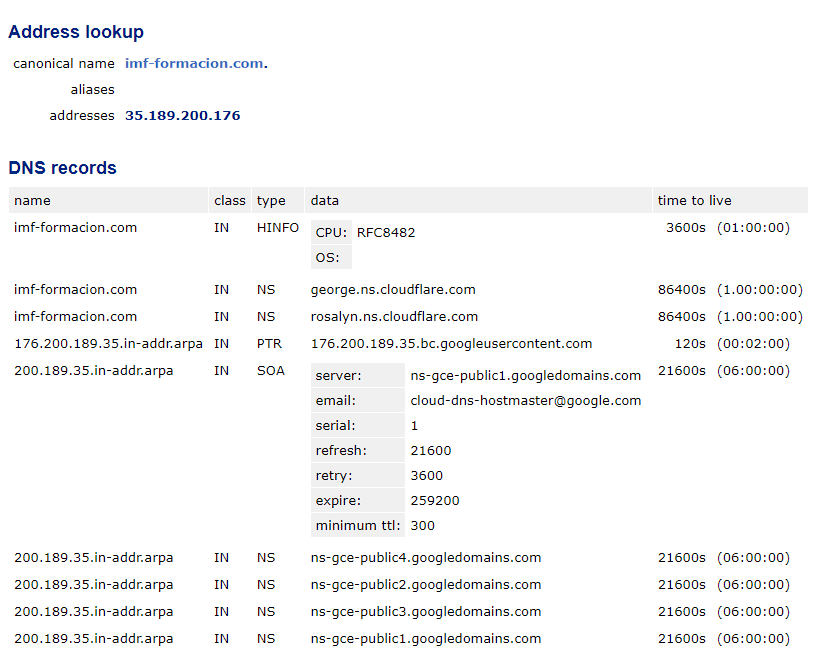
* **CentralOps:** Una herramienta de análisis de dominios que proporciona información detallada sobre los registros DNS, servidores de nombres, direcciones IP y otros datos relacionados con un dominio.
* **DNSdumpster:** Una herramienta de búsqueda de patrones de correos electrónicos que analiza los registros DNS para identificar patrones de correos electrónicos asociados con un dominio o empresa.
* **Maltego:** Una herramienta de inteligencia de código abierto que se utiliza para recopilar información pasiva sobre una organización o dominio, buscando en repositorios públicos como DNS, WHOIS, redes sociales y otras fuentes de información abierta.

**2.3 Resultados del Reconocimiento**

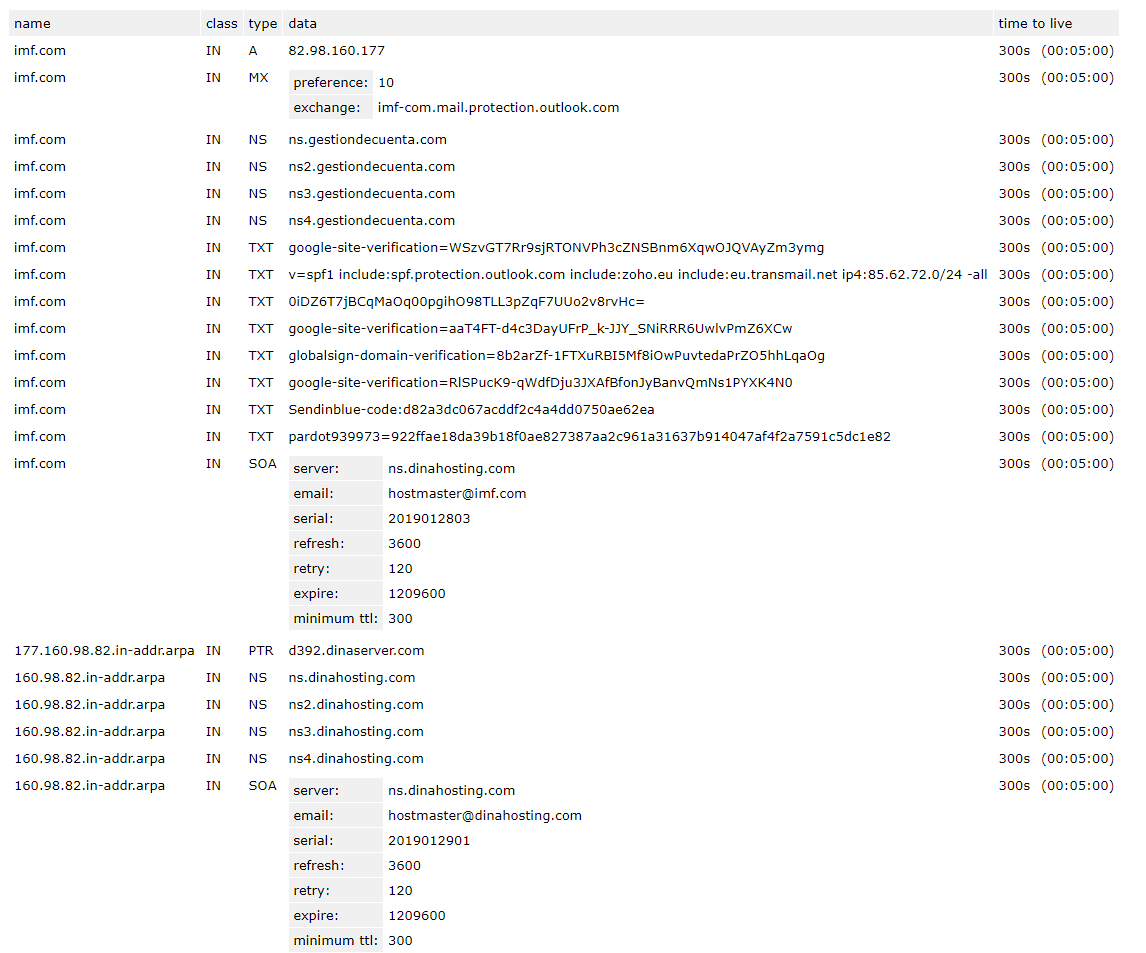
**2.3.1 Información General**

* **Nombre Completo de la Organización:** IMF Smart Education
* **Sitio Web Principal:** www.imf-formacion.com
* **Localización de la Sede:** Madrid, España

**2.3.2 Análisis de DNS con CentralOps**

Se realizó un análisis de dominios utilizando la herramienta CentralOps sobre los dominios imf-formacion.com e imf.com, obteniendo los siguientes resultados.

El resultado de la consulta DNS muestra que el nombre de dominio imf-formacion.com está alojado en los servidores de Google Cloud DNS y está configurado con dos servidores de nombres: george.ns.cloudflare.com y rosalyn.ns.cloudflare.com. Además, se encontró que el dominio tiene un registro HINFO que indica que el sistema operativo es RFC8482 y la CPU es RFC8482. Finalmente, se observó que el dominio utiliza un servidor SOA ns-gce-public1.googledomains.com con el correo electrónico cloud-dns-hostmaster@google.com

****

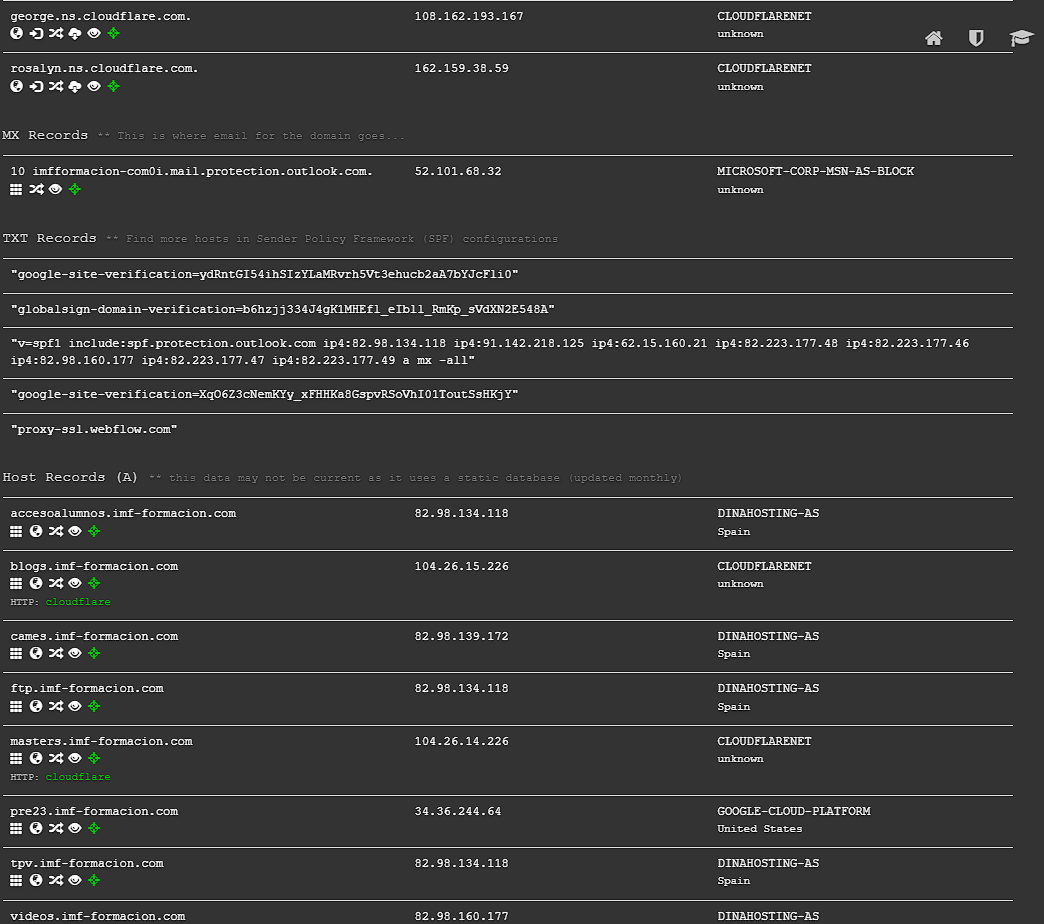
En esta tabla de registros DNS se muestra la configuración de nombres de dominio para el sitio web imf.com. La tabla lista varios registros DNS, incluyendo registros A, MX, NS, SOA y TXT, que proporcionan información sobre la dirección IP del sitio web, los servidores de correo electrónico, los servidores de nombres, la configuración de seguridad y la autenticación del dominio.

Los registros A y MX indican que el sitio web imf.com se encuentra en la dirección IP 82.98.160.177 y que los correos electrónicos se envían a través del servidor imf-com.mail.protection.outlook.com. Los registros NS indican que los servidores de nombres para el dominio son ns.gestiondecuenta.com, ns2.gestiondecuenta.com, ns3.gestiondecuenta.com y ns4.gestiondecuenta.com.

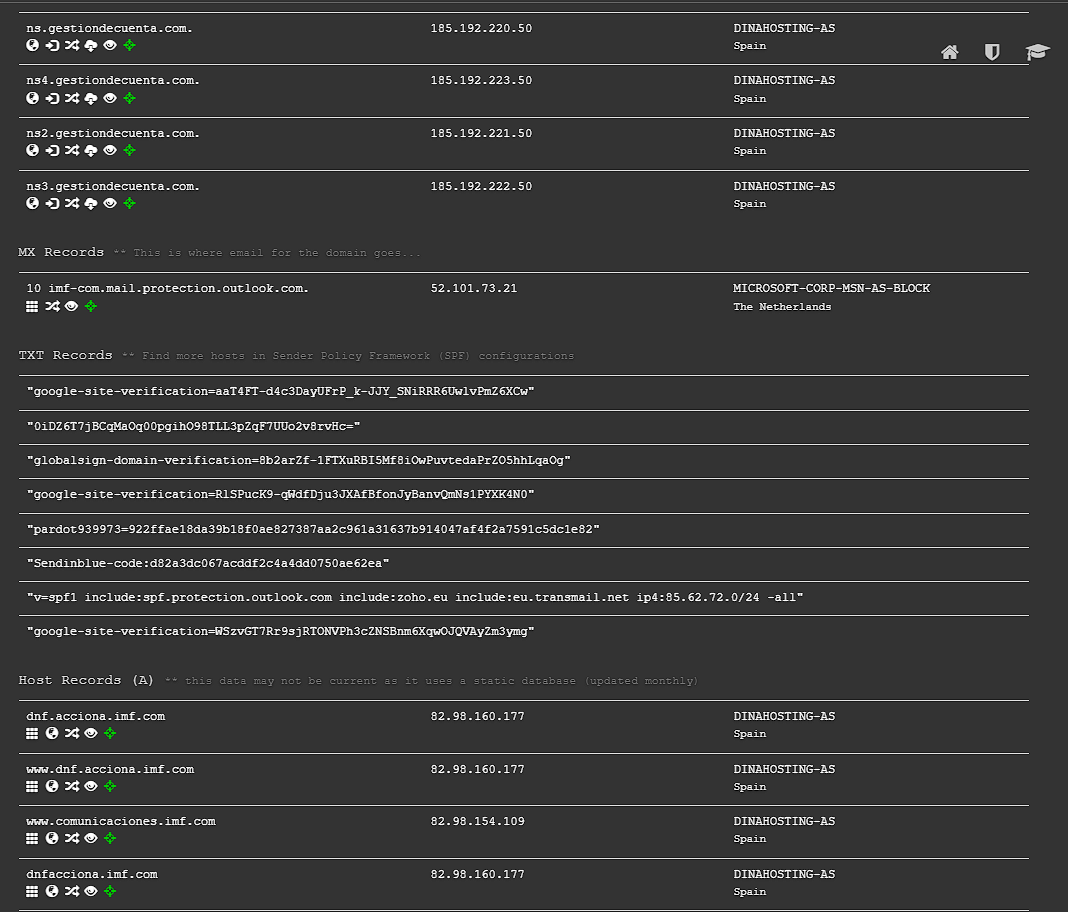
Los registros SOA proporcionan información sobre la configuración de seguridad del dominio, incluyendo la dirección de correo electrónico del administrador del dominio y la frecuencia de actualización de los registros DNS. Los registros TXT proporcionan información adicional sobre la autenticación del dominio, incluyendo claves de verificación de sitio de Google y otros proveedores de servicios.

**2.3.3 Análisis de DNS con DNSdumpster**

Se llevó a cabo un análisis de DNS utilizando la herramienta DNSdumpster sobre los dominios imf-formacion.com e imf.com, lo que arrojó los siguientes resultados.



La imagen muestra información de registros DNS para el dominio imf-formacion.com. La información incluye registros MX, TXT y A. Los registros MX muestran el servidor de correo electrónico para el dominio, mientras que los registros TXT muestran la configuración de SPF. Los registros A muestran las direcciones IP asociadas a los distintos subdominios del dominio. Notablemente, se encontraron subdominios diferentes en comparación con la respuesta de la herramienta CentralOps, como accesoalumnos.imf-formacion.com, blogs.imf-formacion.com, cames.imf-formacion.com, entre otros, lo que sugiere una estructura de subdominios más compleja de lo esperado.



La lista de registros DNS muestra una variedad de sitios web relacionados con la organización IMF, cada uno con su propia dirección IP y proveedor de hosting. La mayoría de los sitios web están alojados en servidores con direcciones IP que pertenecen a la red DINAHOSTING-AS, que se encuentra en España. Esto sugiere que la organización IMF tiene una presencia importante en España y que utiliza a DINAHOSTING-AS como proveedor de hosting para muchos de sus sitios web. Algunos de los sitios web, como error.imf.com y formacion.imf.com, tienen direcciones IP que se encuentran en la misma red, lo que sugiere que están relacionados entre sí.

La imagen también proporciona información sobre las tecnologías utilizadas por algunos de los sitios web. Por ejemplo, se muestra que algunos sitios web utilizan Microsoft-IIS/10.0 como servidor web, lo que sugiere que están utilizando tecnologías de Microsoft para hospedar sus sitios web. Además, se menciona que algunos sitios web utilizan ASP.NET, un framework de desarrollo web de Microsoft, lo que sugiere que están utilizando tecnologías de Microsoft para desarrollar y ejecutar sus aplicaciones web.

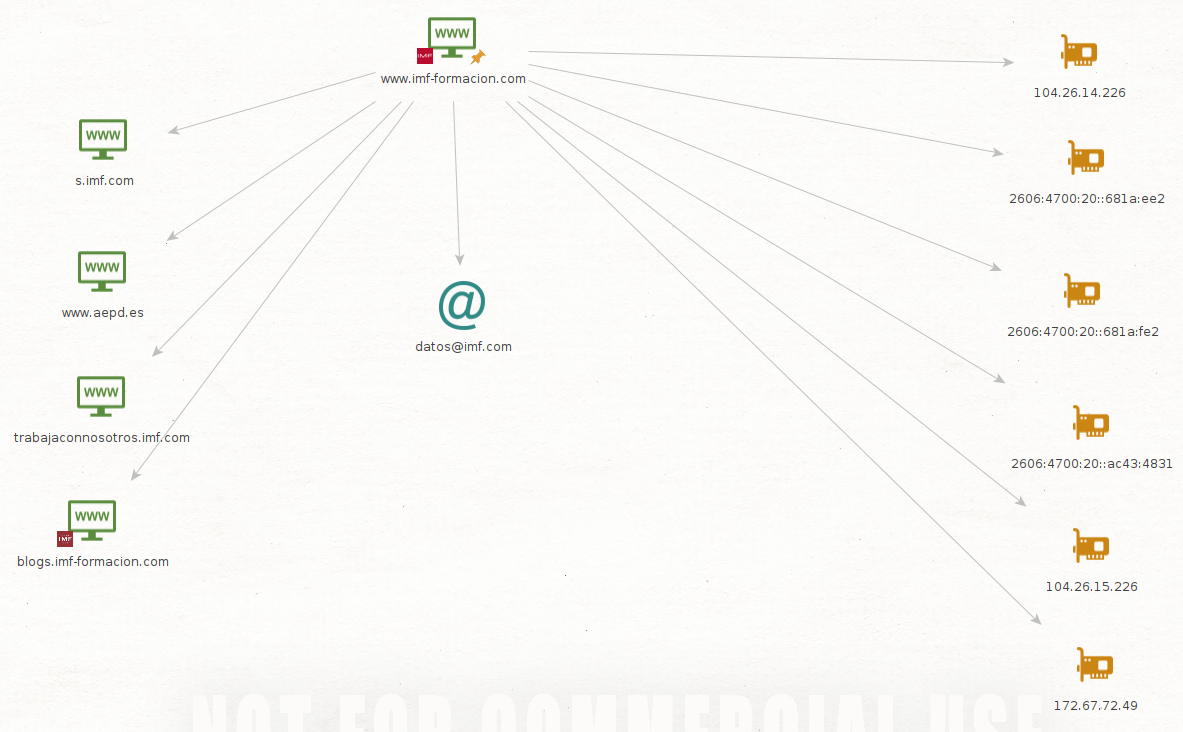
El escaneo DNS de imf.com detectó la existencia de más subdominios que los inicialmente identificados.

Tabla

Descripción generada automáticamente

**2.3.4 Recolección de información con Maltego**

Se empleó la herramienta Maltego para realizar una recolección de información relacionada con el dominio imf-formacion.com, lo que permitió descubrir nueva información, incluyendo nuevos dominios y un correo electrónico.

La imagen muestra una representación gráfica de la información recopilada, con sitios web en el lado izquierdo, direcciones IP (IPv4 e IPv6) en el lado derecho y un correo electrónico en el centro.

**Dominios identificados**

* **www.aepd.es**: Este dominio pertenece a la Agencia Española de Protección de Datos.

**Direcciones IP**

* **IPv4**:
  + 104.26.14.226
  + 104.26.15.226
  + 172.67.72.49
* **IPv6**:
  + 2606:4700:20::681a:ee2
  + 2606:4700:20::681a:fe2
  + 2606:4700:20::ac43:4831

**Correo electrónico**

* datos.imf.com

**Subdominios identificados**

* **s.imf.com**: Este subdominio del dominio imf.com redirige al dominio imf-formacion.com, al igual que el dominio imf.com.
* **trabajaconnosotros.imf.com**: Este subdominio del dominio imf.com nos lleva a una página de ofertas de trabajo de IMF Smart Education.
* **blogs.imf-formacion.com**: Este subdominio del dominio principal que estamos auditando nos lleva a un blog.

**2.4 Metodología de Escaneo**

La fase de escaneo se enfocó en la detección de puertos y servicios abiertos en los servidores asociados con IMF. No se realizaron pruebas de vulnerabilidades ni escaneos web activos.

**2.5 Herramientas Utilizadas**

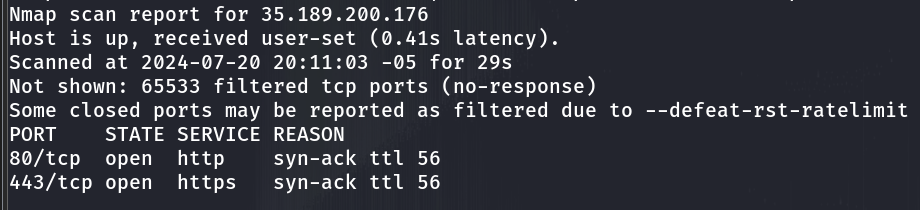
* **Nmap:** Escaneo de puertos y detección de versiones de servicios.

**2.6 Resultados del Escaneo**

El siguiente comando que se muestra es un escaneo de puertos utilizado para identificar los puertos abiertos en el servidor 35.189.200.176 que corresponde al dominio imf-formacion.com



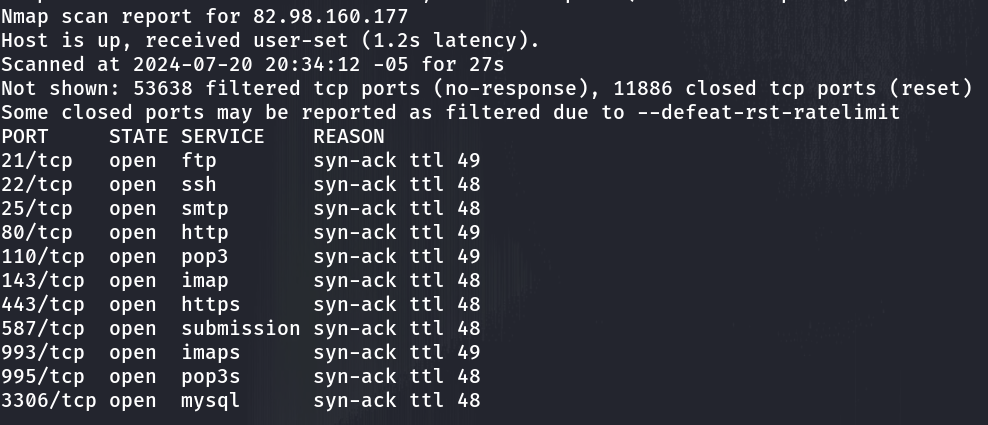
Los puertos 80 y 443 están abiertos. El puerto 80 ofrece el servicio http y el puerto 443 ofrece el servicio https.



Con el siguiente comando se hace un escaneo de puertos utilizado para identificar los puertos abiertos en el servidor 82.98.160.177 que corresponde al dominio imf.com



El escaneo de Nmap realizado en la dirección IP 82.98.160.177 ha encontrado los siguientes puertos abiertos



**3. Fase de Hacking Ético**

**3.1 Metodología**

La fase de hacking ético se centró en identificar y explotar vulnerabilidades en una máquina virtual estilo CTF. Esta fase implica realizar un análisis exhaustivo para encontrar vectores de ataque y ejecutar exploits para ganar acceso a la máquina, ademas se debe de encontrar 10 flags que están repartidas por todo el sistema.

**3.2 Herramientas Utilizadas**

* **Nmap:** Escaneo de puertos y detección de servicios.
* **Gobuster:** Fuerza bruta de directorios y archivos.
* **Metasploit:** Ejecución de exploits y post-explotación.
* **John the Ripper:** Cracking de contraseñas.
* **Burp Suite:** Análisis de aplicaciones web.
* **Hydra:** Ataques de fuerza bruta en servicios de autenticación.

**3.3 Resultados del Hacking Ético**

**3.3.1 Vector de Ataque Inicial**

* **Servicio Identificado:** HTTP en puerto 80
* **Exploit Utilizado:** [Ejemplo: SQL Injection en una página de login]

**3.3.2 Escalación de Privilegios**

* **Técnica Utilizada:** [Ejemplo: Kernel exploit para obtener privilegios de root]

**3.3.3 Post-Explotación**

* **Acciones Realizadas:**
  + Extracción de archivos sensibles.
  + Creación de un usuario persistente para acceso futuro.
  + Análisis de logs para identificar otros posibles vectores de ataque.

**4. Conclusión**

El análisis de seguridad realizado sobre la organización IMF y la máquina virtual estilo CTF permitió recopilar una cantidad significativa de información y explotar vulnerabilidades de manera efectiva. Este informe documenta los pasos seguidos, las herramientas utilizadas y los resultados obtenidos, proporcionando una visión clara y detallada del proceso y los hallazgos del análisis de seguridad.