1. Definición del Alcance

**Objetivo**: Identificar vulnerabilidades de la página web que puedan ser explotadas por atacantes.

**Activos Críticos**: Servidores de bases de datos y servidores de aplicaciones web.

2. Planificación

**Herramientas a Utilizar**: Nmap para el escaneo de puertos, Burpsuite para realizar pruebas de penetración web, sqlmap para descubrir vulnerabilidades de inyección sql, GoBuster para realizar fuerza bruta contra directorios,

3. Evaluación de Riesgos

**Escaneo de Puertos y Servicios**: Utilizar Nmap para identificar servicios expuestos y puertos abiertos en los dispositivos de red.

4. Identificación de Riesgos

**Acceso FTP anónimo** permitido que debería ser revisado y posiblemente restringido.

Las **versiones de los servicios son detalladas**, lo que puede facilitar la identificación de vulnerabilidades conocidas asociadas a esas versiones específicas.

La interfaz de administración puede ser accesible sin medidas de seguridad adecuadas.

Configuraciones potencialmente inseguras en las cookies HTTP.

5. Informe

Para comenzar a vulnerar la máquina, lo primero que deberemos de hacer será utilizar la herramienta **nmap** para conocer la ip y los puertos que se encuentran abiertos.



Con este pequeño comando, lo que haremos será:

nmap: Es el programa que se está ejecutando.

-sCV: Esta es una combinación de dos opciones:

-sC: Ejecuta scripts predeterminados de Nmap que son seguros y están diseñados para detectar información adicional y vulnerabilidades comunes en los servicios encontrados.

-sV: Intenta determinar la versión de los servicios que se están ejecutando en los puertos abiertos.

-Pn: Esta opción le dice a Nmap que no realice un descubrimiento de hosts antes de realizar el escaneo. Normalmente, Nmap primero intenta descubrir qué hosts están activos antes de escanearlos, pero con -Pn Nmap asumirá que todos los hosts están activos y procederá al escaneo. Es útil si los hosts bloquean las peticiones de ping que normalmente se utilizan para el descubrimiento.

-p 1-10000: Define el rango de puertos a escanear, desde el puerto 1 hasta el puerto 10,000.

-T5: Establece el nivel de temporización a 5, que es el más rápido y agresivo. Aunque puede terminar más rápido, también es más probable que genere tráfico de red y registros que pueden ser detectados fácilmente por sistemas de prevención de intrusiones.

10.0.2.0/24: Especifica el rango de direcciones IP que serán escaneadas. En este caso, todas las direcciones en la subred 10.0.2.0 con una máscara de red de 24 bits (es decir, desde 10.0.2.1 hasta 10.0.2.254).

Y el resultado que nos arroja es el siguiente

Texto

Descripción generada automáticamente

Con esto podemos ver que la ip 10.0.2.15 tiene el puerto 21, 22 y 7080 abierto.

El atacante podría conectarse de manera anónima al equipo a través de ftp ya que ftp-anon está permitido, además de eso, también podemos apreciar que se esta ejecutando un servicio FTP con vsftpd versión 3.0.3.

El puerto 22 está abierto y está ejecutando OpenSSH versión 7.2p2 que permite realizar comunicaciones seguras y cifradas a través de la red usando el protocolo SSH.

Las huellas digitales ssh-hostkey de claves RSA y ECDSA sirven para identificar la identidad del servidor.

El puerto 7080 está ejecutando un servidor web Apache versión 2.4.48 con diferentes tecnologías como OpenSSL o PHP.

El título de la página HTTP es "Admin Panel", lo cual podría indicar una interfaz de administración accesible.

Los detalles del servidor (http-server-header) confirman la versión de Apache y los módulos instalados.

Se mencionan las flags de las cookies HTTP (http-cookie-flags), indicando que la cookie de sesión PHP no tiene la bandera httponly establecida, lo que podría ser una vulnerabilidad ya que permite que la cookie sea accesible a través de scripts del lado del cliente como JavaScript, aumentando el riesgo de ataques como XSS.

Texto

Descripción generada automáticamente

Para conectarnos a la aplicación web lo único que deberemos de poner es la ip y el puerto que se encuentra abierto **10.0.2.15:7080**

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

Esta es la interfaz de inicio de sesión en la cual no conocemos las credenciales ni de usuario ni de contraseña, por lo que podemos probar a usar un fragmento de código para hacer inyección sql y así poder acceder al interior de la página.

Para ello usaremos la herramienta burpsuite que interceptara la petición y gracias a esto podremos modificar los parámetros que creamos convenientes.

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

Introducimos valores aleatorios pero validos y le damos a login.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Y dentro de esta pagina modificaremos tanto el correo como la contraseña añadiendo el fragmento “ ‘ or ‘1’=’1’ -- - “ o “ ‘ or true -- - “

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Y le damos al botón de arriba a la izquierda que pone “Forward”

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

Y nos saldrá esta pantalla la cual indica que hemos realizado el inicio de sesión de manera exitosa sin saber ni el correo ni la contraseña, solo a través de inyección sql.

Interfaz de usuario gráfica

Descripción generada automáticamente

Dentro de este panel de control podemos observar varias opciones, citas, doctores, pacientes y servicios.

Haciendo un poco de búsqueda no hay un apartado en especifico en el que se pueda subir archivos o modificar parámetros para poder tirar una reverse Shell, para ello vamos a indagar un poco más a ver si hay alguna manera de acceder.

Para ello vamos a usar la herramienta de **GoBuster,** que nos ayudara a localizar archivos y directorios que se encuentren ocultos y no sean accesibles de manera directa.

Captura de pantalla de computadora

Descripción generada automáticamente

Usando ese diccionario nos detecta “files” y “pages” como recursos ocultos, vamos a probar a acceder a ver si podemos localizar alguna vulnerabilidad.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

A simple vista no detectamos mucho ni se puede hacer mucha cosa, por lo que vamos a seguir investigando.

Texto

Descripción generada automáticamente

Al inspeccionar el código fuente de la pagina web, vemos que hay una línea comentada la cual tiene una redireccion a un sitio llamado “setting.php”, vamos a probar a acceder a ella escribiendo esa dirección en la url.

Captura de pantalla de computadora

Descripción generada automáticamente

La imagen muestra una interfaz de usuario para la configuración de un sistema de gestión hospitalaria, específicamente se observa un formulario para configurar detalles de la empresa, como el nombre, la dirección de correo electrónico, el sitio web, la dirección y otros ajustes como el símbolo de la moneda, la activación de la interfaz de usuario, el impuesto por defecto, etc. Además, hay una opción para subir un logotipo de la empresa la cual podemos aprovechar para subir una reverse Shell, para ello lo primero que tendremos que hacer será poner en escucha la maquina atacante a través de un puerto para podernos conectar mas adelante.

Texto

Descripción generada automáticamente

Ponemos en escucha la maquina a través del puerto 4444 y accedemos a la siguiente [pagina web](https://www.revshells.com/) que nos creara una reverse Shell en código php

Captura de pantalla de computadora

Descripción generada automáticamente

Donde el parámetro de ip será modificado por la ip de la maquina atacante y el puerto será por el que nos queramos conectar a la máquina.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Seleccionamos la reverse Shell con el nombre que le hayamos dado, en mi caso reverse.php.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Como podemos ver, en la parte superior de la pantalla acaban de aparecer diferentes iconos que tiene la pagina por defecto, deberemos de inspeccionarlos para poder acceder a la ruta en la cual se encuentran guardados, para ello haremos click derecho, inspeccionar y buscaremos el nombre del archivo que acabamos de subir.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Como se puede apreciar en esta imagen, se ha subido correctamente al servidor, también probe con “tunnel.nosocket.php” y funciona igual de bien, pero en este caso el que nos interesa es el “reverse.php”

Interfaz de usuario gráfica, Sitio web

Descripción generada automáticamente

Lo pegamos en la url y a simple vista parecera que no ocurre nada pero si nos vamos a la terminal donde habíamos puesto el puerto a la escucha obtendremos lo siguiente.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

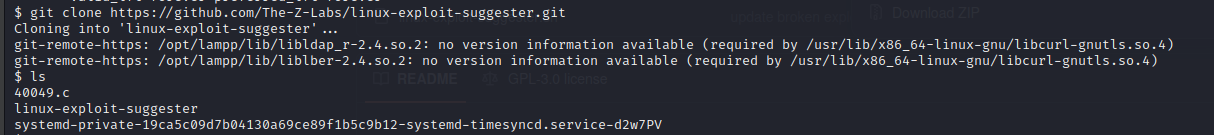
Hemos conseguido establecer una conexión a través de una reverse Shell, así que ahora lo que queda es obtener privilegios de administrador o root.

Imagen que contiene Texto

Descripción generada automáticamente

Si hacemos un id podemos ver que el identificador del usuario es 1 y el nombre es Daemon, el grupo principal es 1 con el nombre de Daemon y los grupos a los que pertenece este usuario es al 1 con nombre Daemon igual.

Para obtener las diferentes vulnerabilidades que tiene la maquina vamos a usar una herramienta que se llama [linux-exploit-suggester](https://github.com/The-Z-Labs/linux-exploit-suggester), esta herramienta ayuda a detectar deficiencias de seguridad en sistemas basados en Linux, para ello examina tanto las configuraciones de compilación del kernel como los ajustes en tiempo de ejecución.



Lo clonamos y vemos que se haya creado de manera correcta.

Una vez creado accedemos al directorio y ejecutamos el programa.

Texto

Descripción generada automáticamente

Aquí se nos desplegaran varias opciones como la versión de kernel, arquitectura, distribución, etc.

Texto

Descripción generada automáticamente

Buscaremos este apartado que normalmente suele ser el necesario para hacer la escalada de privilegio.

Buscaremos en internet por un posible script a través del cve y nos clonaremos en nuestra maquina victima el proyecto [CVE-2021-4034](https://github.com/berdav/CVE-2021-4034).

Texto

Descripción generada automáticamente

Tras haberlo clonado, accederemos al interior de la carpeta, compilaremos el programa con el comando make y ejecutaremos el proyecto, así de esta manera habremos conseguido escalar privilegios y ser root.

Por otro lado, desde el login se puede emplear fuerza bruta para conseguir el nombre de la base de datos.

Interfaz de usuario gráfica, Aplicación, Tabla

Descripción generada automáticamente

Aquí lo que hacemos es calcular el tamaño que se va a extraer “1’ or (select length(database()))=4 -- -“

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Con “1' or substring(database(),1,1)='d' -- -“ iremos iterando en el valor que queramos para ir obteniendo los nombres de las bases de datos que nosotros busquemos.

Interfaz de usuario gráfica

Descripción generada automáticamente

En este caso obtenemos que la primera letra de la primera base de datos es la **C** ya que la pagina nos devuelve una longitud diferente al resto.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

La letra que la sigue es la L, y así hasta completar el nombre de la base de datos que seria clinic\_db