

TEAM CHALLENGE

SPRING 10 – RETO OBIOBÁ

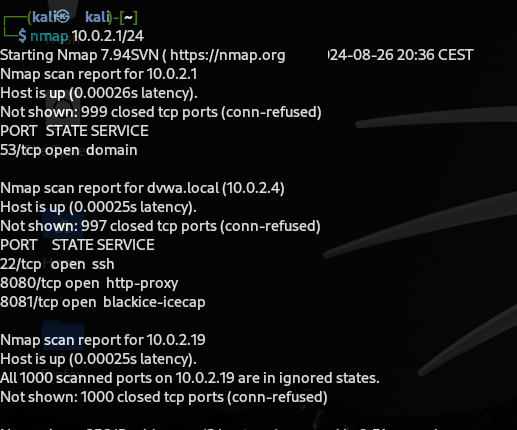
EXPLOTACIÓN VULNERABILIDADES

MAQUINA ODIOBA

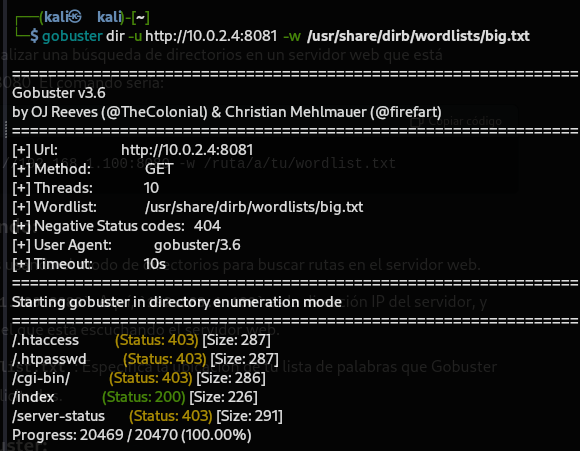
INTRODUCCIÓN

Para este ejercicio se han usado diversas aplicaciones y servicios para encontrar vulnerabilidades que permitan el acceso no autorizado al sistema, exponiendo únicamente los que han resultado positivos para conseguir tal fin, los cuales son:

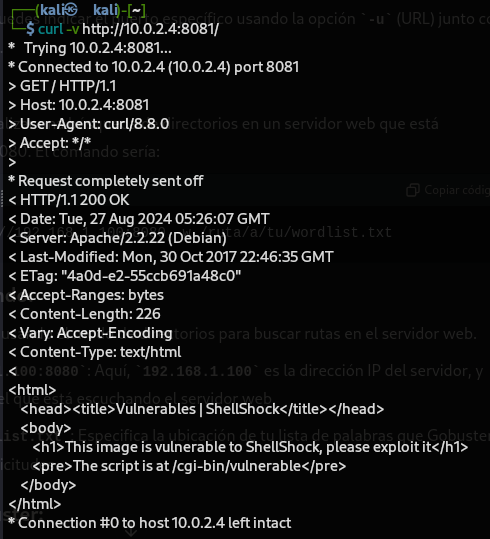
* 1.- EXPLORACIÓN IP DEL OBJETIVO

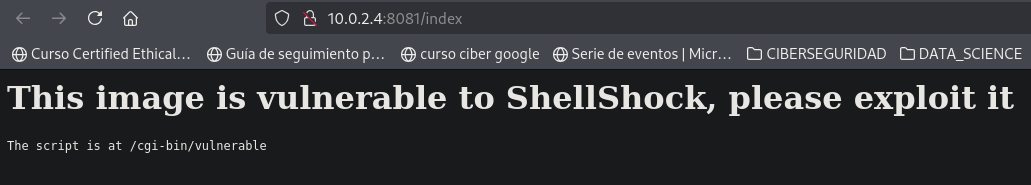


* En este caso se ha usado la aplicación nmap, la cual es una herramienta potente de escáner con multitud opciones. En este caso simplemente se ha usado para buscar las IP activas en el rango de IPs 10.0.2.1/24, siendo la 10.0.2.4 la del objetivo.
* 2.- EXPLORACIÓN WEB
* En primer lugar, se ha usado la aplicación Gobuster, herramienta diseñada para descubrir directorios, archivos, subdominios y otros puntos de entrada ocultos en servidores web, al hacer solicitudes repetitivas fuerza bruta, basadas en listas de palabras.



* En segundo lugar, se ha utilizado la aplicación Curl, herramienta CLI que permite la transferencia de datos desde o hacia un servidor, utilizando diversos protocolos (HTTP, HTTPS, FTP, entre otros), siendo muy versátil para realizar solicitudes web y obtener respuestas directamente desde la terminal.

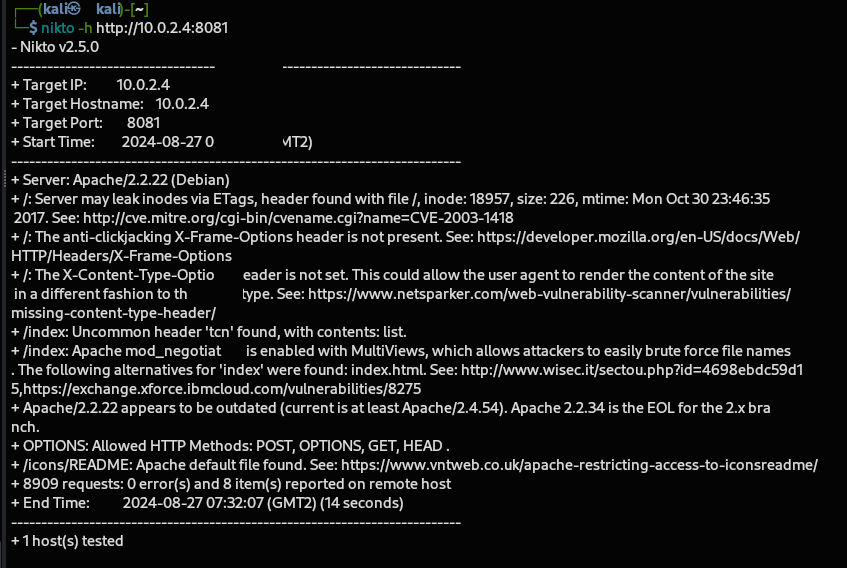




* En este caso, en uno de los directorios ocultos y menos evidentes a usar desde la interfaz pública del sitio web, se ha hallado información o pista importante para una posterior explotación, indicando claramente que el script *“/cgi-bin/vulnerable”* presenta una vulnerabilidad conocida como “ShellShock”.

El directorio */cgi-bin/* es la ubicación estándar donde se ubican los scripts CGI - Common Gateway Interface (Interfaz de puerta de enlace común), los cuales se ejecutan en el servidor en respuesta a las peticiones de los clientes, devolviendo a éste el resultado del script solicitado. Esta mecánica de funcionamiento es, a menudo, se convierte en punto de ataque en vulnerabilidades que permiten la ejecución de código arbitrario mediante la inyección de scripts maliciosos, como puede ser la “ShellShock”

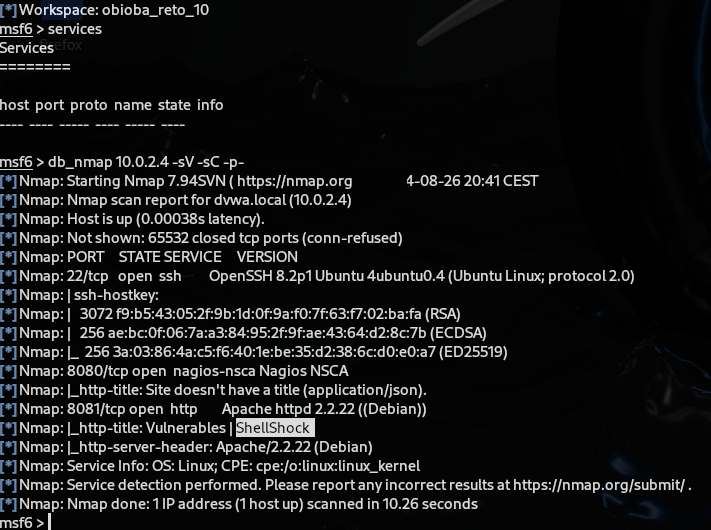
* En tercer lugar, se ha utilizado la aplicación Nikto, otra herramienta de escaneo de vulnerabilidades web de código abierto que ayuda a identificar fallos de seguridad en servidores web proporcionando una visión general de posibles puntos débiles (archivos y directorios sensibles, versiones antiguas no actualizadas, configuraciones inseguras y otras vulnerabilidades más comunes) que podrían ser explotados por atacantes malintencionados.

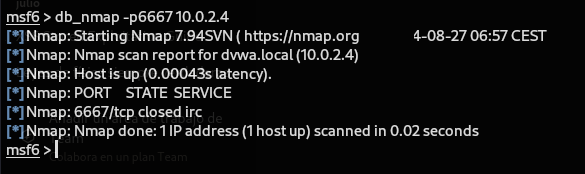


* Como se puede ver, ha encontrado una posible vulnerabilidad con un CVE-2003-1418 relacionado con las etiquetas Etags (Entity Tags), las cuales se usan para identificar las versiones asignadas a un recurso en el servidor web. Cuando un cliente solicita un recurso, el servidor usa los Etags para determinar si la versión almacenada en la cache de ese recurso es la misma que esta en el servidor, ayudando todo esto la sincronización del cliente y servidor y optimizando el uso de la caché.

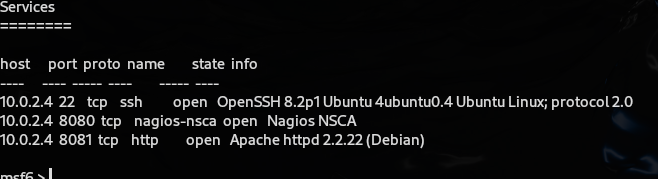
Se ha realizado una búsqueda en Metaexploit del CVE, así como por la descripción o nombre del identificador, con resultado infructuoso.

* Además, el directorio */índex/* es vulnerable a ataques por fuerza bruta.
* 3.- FASE DE EXPLOTACIÓN

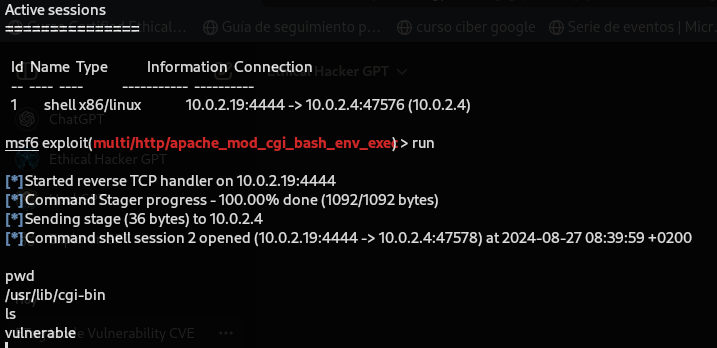


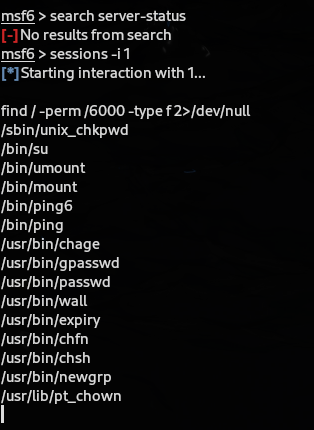






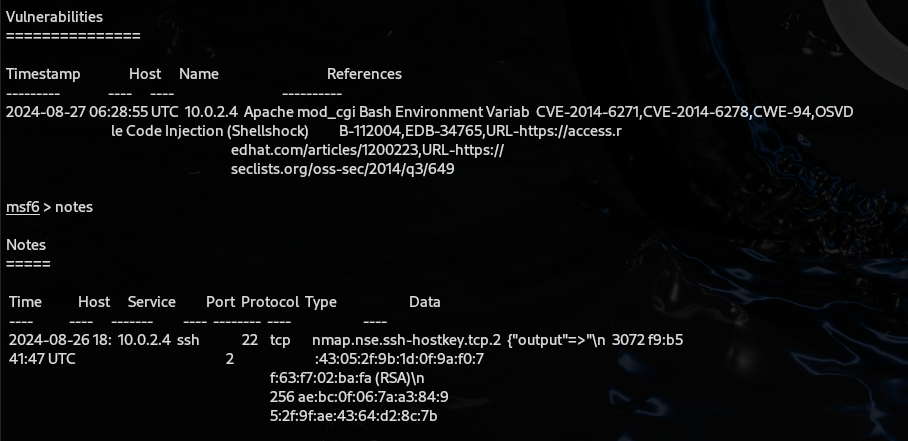




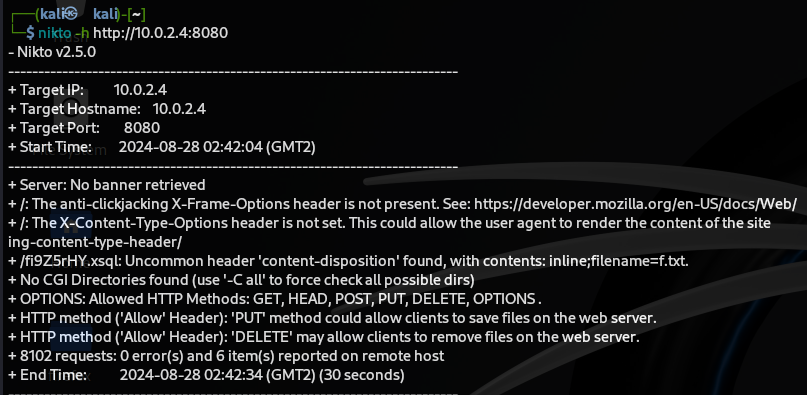


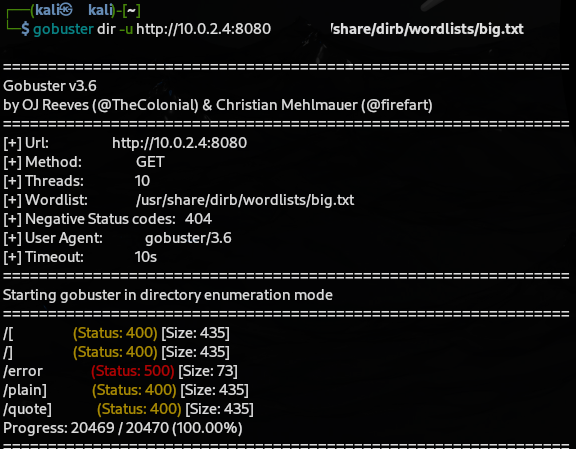
RESUMEN:





Puerto 8080





**Nagios NSCA (Nagios Service Check Acceptor)** es un componente de Nagios, una popular herramienta de monitoreo de redes y sistemas. NSCA permite a los servidores y dispositivos enviar resultados de verificación pasivos (como estado de servicios o dispositivos) al servidor Nagios central, que luego procesa y actúa sobre esos resultados. Normalmente, NSCA se comunica de forma segura con el servidor Nagios a través de una conexión cifrada.

**¿Para qué sirve en un puerto HTTP-Proxy?**

Cuando NSCA está asociado con un puerto HTTP-Proxy, como el 8080, es posible que esté siendo utilizado para recibir y procesar informes de estado o resultados de monitoreo desde dispositivos remotos a través de un proxy HTTP. Este uso a través de un proxy puede ser parte de una configuración más compleja donde los dispositivos no pueden comunicarse directamente con el servidor Nagios y necesitan enrutar sus mensajes a través de un proxy.

