Alejandro Fernández Perera

Analizamos la red en busca de hosts y los puertos abiertos para la maquina a la que queremos atacar, vemos que al analizar la red vemos una ip con dos servicios abiertos procedemos a sacar mas información añadiéndole el parámetro -A a el nmap.

Texto

Descripción generada automáticamente

Analizamos la ip de la maquina que queremos atacar en busca de puertos abiertos y los servicios que hay lanzados y vemos que tenemos el 22 con servicio ssh y el puerto 80 que tiene un servicio http apache

Texto

Descripción generada automáticamente

Probamos conectarnos por ssh pero nos pide password así que descartamos probaremos con el otro servicio.

Pasamos con el puerto 80 http que contiene el servicio apache2, cuando nos conectamos vemos la página default de apache2, lo primero que haremos será realizar una enumeración de directorios para ello utilizaremos dirb aunque podríamos usar también herramientas como wfuzz, gobuster o dirbuster.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Realizamos la búsqueda de directorios con dirb y le pasamos el diccionario common.txt, vemos que ha encontrado index.html y server status pero no nos da nada interesante, seguiremos probando con diferentes diccionarios, si fuera una pagina desconocida probaría a hacer un spider pero en este caso sabemos que no tiene enlaces internos en la página de apache2.

Texto

Descripción generada automáticamente

Probaremos con otro diccionario llamado megabeast.txt y como vemos aquí, ya nos muestra otro directorio llamado scarecrow.

Texto

Descripción generada automáticamente

Lo que nos encontramos en este directorio es muy interesante, un login.php y un personal\_secret\_admin\_page.php

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Accedemos a personal\_secret\_admin\_page.php pero nos devuelve esto, no podemos acceder porque no somos admins

Texto

Descripción generada automáticamente con confianza baja

Observamos la request por abajo pero no vemos nada interesante así que probaremos con el login.php

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

En login.php nos encontramos un input que nos dice si el usuario existe o no, lo que nos da acceso a hacer una enumeración de usuarios, también podemos observar que acepta xml, comprobaremos si hay posible xxe o sql injection, la prueba de enumración nos llevaría mucho tiempo así que empezaremos por el xxe y sqlInjection.

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza baja

Hacemos las pruebas básicas de sql injection

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

El sql injection no es inyectable así que pasaremos al xxe

Llevamos la petición al reapeter y lanzamos una petición post donde el valor auth sea un xml, probamos posibles tags que pueda aceptar y damos con el correcto que es user.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Ahora que sabemos que tenemos acceso haremos una lectura de ficheros.

Texto

Descripción generada automáticamente

Hacemos una lectura de etc password y tachan funciona.

Vamos a intentar leer el login.php, para poder lograrlo lo convertiremos a base 64 para poder obtener el resultultado y después lo descodificaremos.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Texto

Descripción generada automáticamente

No vemos nada interesante, así que haremos lo mismo para la otra pagina personal\_secret\_admin\_page.php y veremos que encontramos

Hacemos el mismo proceso que anteriormente y obtenemos el código base de personal\_secret\_admin\_page.php.

Texto, Carta

Descripción generada automáticamente

Podemos observar que utiliza una blacklist como filtro y que solo acepta conexiones desde la mima ip, sabemos que una blacklist nos dice los elementos que no admite así que sabemos los que si admite, gracias a este código sabemos que podemos intentar una inyección de comando ya que sabemos que esta esperando un parámetro ip, pero lo tenemos que hacer teniendo en cuenta la blacklist y viendo un poco nos damos cuenta que el parámetro %0a no se se encuentra en la blacklist.

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

Vemos que al hacer la petición desde el propio servidor con la inyección xxe nos da la página de sesión de el administrador ahora que tenemos acceso porque lo estamos haciendo desde la ip local trataremos de ejecutar comandos.

Le pasamos nuestra ip como parámetros y vemos como nos hace ping a nuestro dispositivo.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Ahora trataremos de evadir los filtros para intentar inyectar un comando en el parámetro, utilizaremos el carácter %0a que nombremos anteriormente para intentar evadirlo.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Probamos un comando básico y vemos que hemos conseguido ejecución de comandos, ahora intentaremos subir una webshell o tirar una reverseShell.

Abrimos un servidor http con Python en la que alojaremos nuestra webshell y después ejecutaremos el comando desde el xxe.

Usaremos la herramienta weebly para tirar nuestra webshell ya que es una forma más cómoda y eficiente de interactuar con la victima

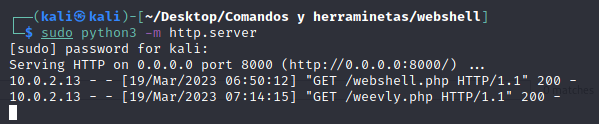
Para ello generaremos una webshell con weebly y la subiremos.

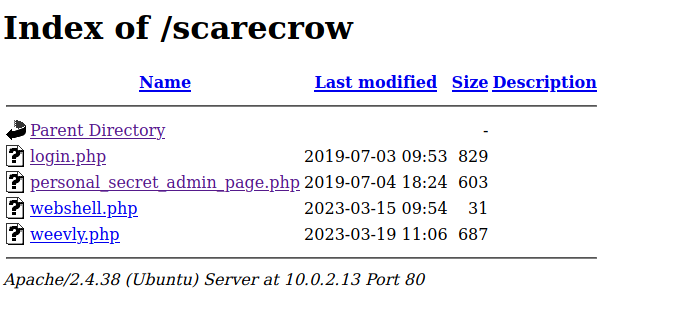


Ahora intentaremos subir el archivo

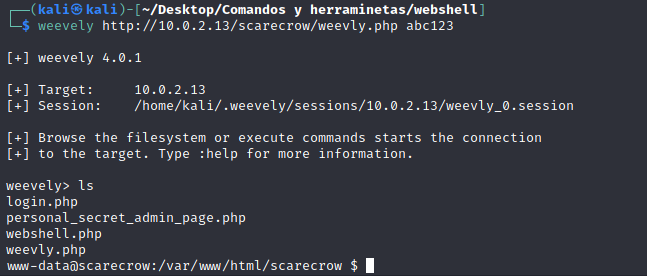
Después de hacer muchas pruebas vemos que haciendo doble encoding en el espacio la petición llega , y comprobamos en el servidor Python para ver si la request ha sido exitosa y se ha llegado a realizar y posteriormente comprobamos en la carpeta scarecrow que la subida se ha realizado con exito.





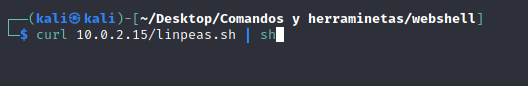


La webshell se ha subido con éxito así que ahora intetaremos establecer conexión con weevly.

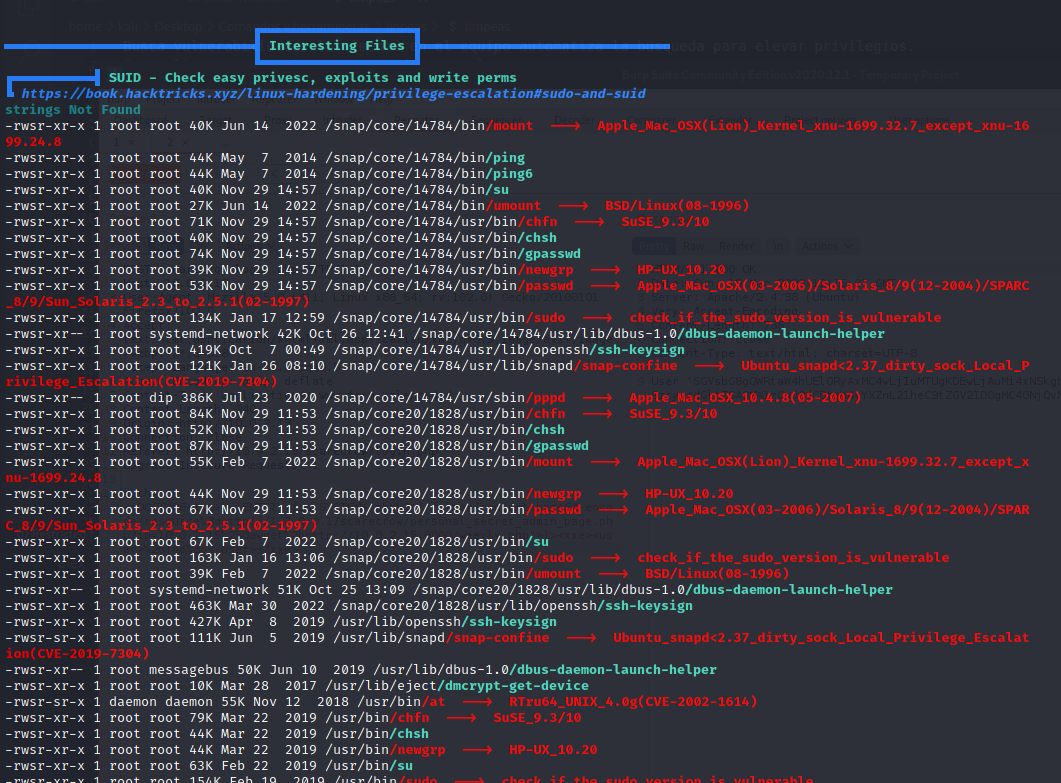


Y.. conseguido ya lo tenemos, ahora tenemos acceso al sistema de una forma mucha más cómoda.

Ahora lo que intentaremos será elevar privilegios para ello ejecutaremos linpeas en el ordenador de la victima. Para ello abrimos otro servidor Python http en la ubicación de la script que queremos subir y una vez hecho realizamos la petición del archivo desde la maquina victima

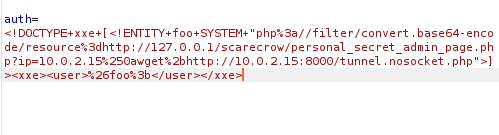


Una vez ejecutado nos da muchísima información buscaremos a ver si nos da algo interesante.



No consigo encontrar nada útil con la información del linpeas así que voy a ver si con regeorge desde dentro analizo la red y encuentro algo.

Subimos el archivo para tunelizar el tráfico



Ejecutamos reGeroge y especificamos la ubicación del archivo php.



Después configuramos el archivo proxychains4.conf y especificamos el puerto del regeroge y lanzamos el comando para hacer un scaneo a la red interna.





Los resultados nos dicen que no hay ningún otro dispositivo en la red que contenga puertos abiertos y que los puertos de la maquina actual son los mismos que habíamos visto desde el escaneo desde fuera.

Como esto no ha llegado a ningún lado seguiré tratando de elevar privilegios

Explorando por el sistema la única carpeta que encuentro que me llame la atención es paw-sk4-experiments pero es inaccesible, si enumeramos su interior vemos que hay una imagen llamada personal\_backup.jpeg pero no consigo acceso, vere si consigo alguna manera de acceder a ella.





Intento buscar archivos con permiso de administrador que tenga yo acceso de ejecución pero no encuentro nada útil.

