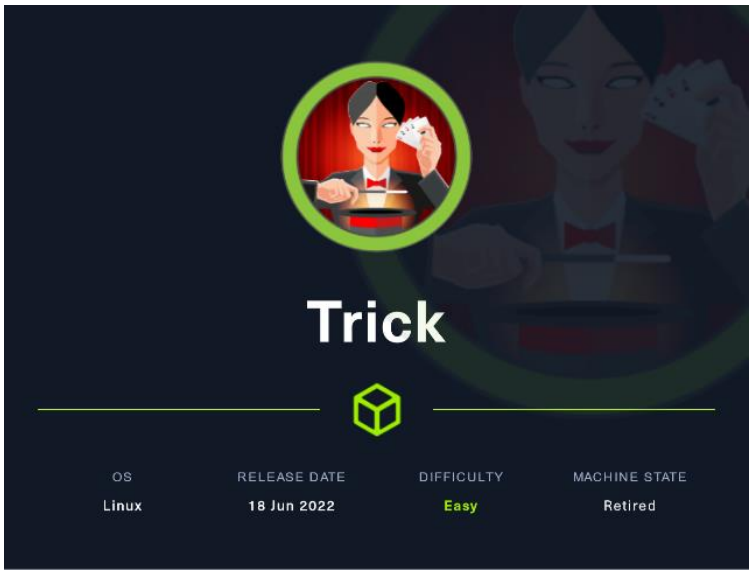
Máquina Trick



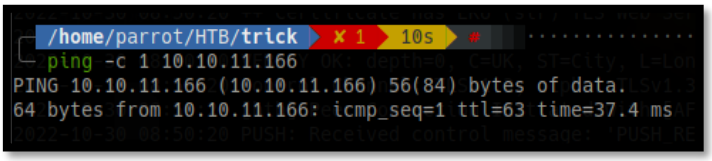
31 Octubre 2022

Hack The Box
Creado por: dandy_loco

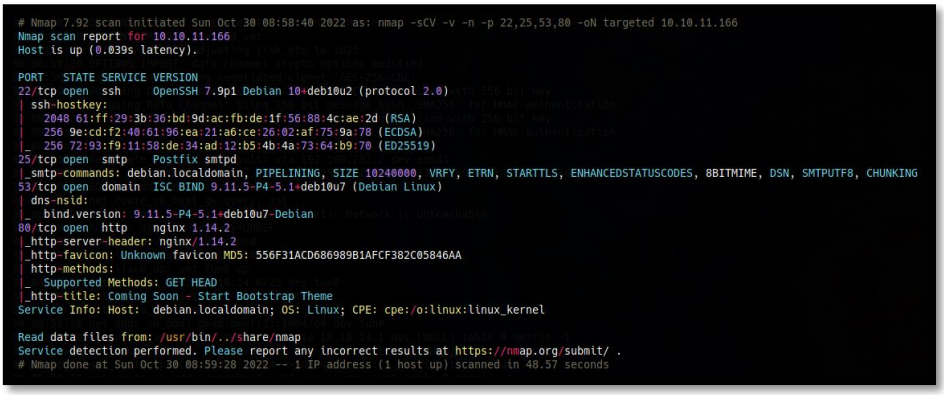
HACKTHEBOX

1. Enumeración

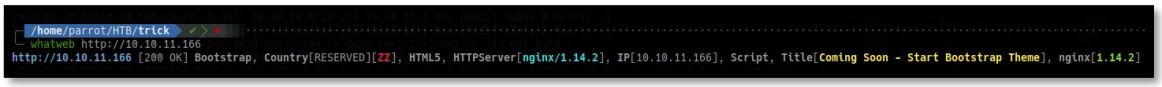
Realizamos un PING a la máquina víctima para comprobar su TTL. A partir del valor devuelto, nos podemos hacer una idea del sistema operativo que tiene. En este caso podemos deducir que se trata de una máquina Linux.



Realizamos un escaneo exhaustivo de los puertos abiertos, con sus correspondientes servicios y versiones asociados.

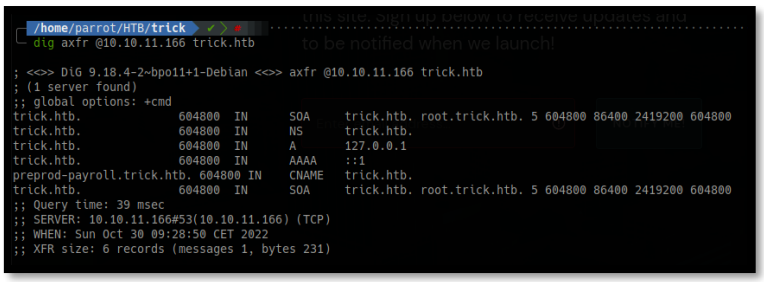


Analizamos las tecnologías que usa el servicio web que corre por el puerto 80.



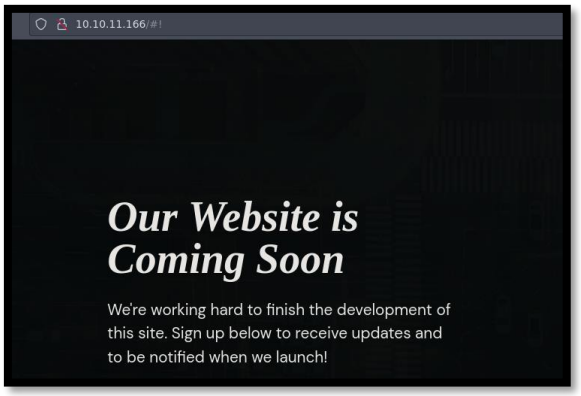
Vemos que la máquina víctima tiene expuesto el servicio de DNS. Vamos a ver si podemos hacer un ataque de transferencia de zona. En HackTheBox, todos los dominios suelen ser el nombre la máquina y terminados en .htb. Por tanto, analizaremos el dominio trick.htb.

```
1. dig axfr @10.10.11.166 trick.htb
```

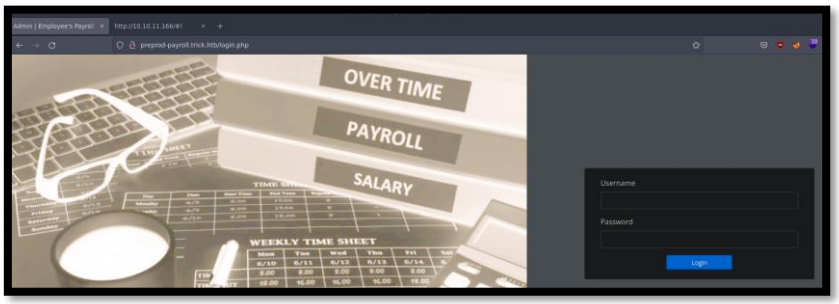


Descubrimos una entrada DNS preprod-payroll.trick.htb. Lo tendremos en cuenta para más adelante.

Abrimos la página web, con nuestro navegador. Revisamos también su código fuente, aunque no vemos nada que nos llame la atención.

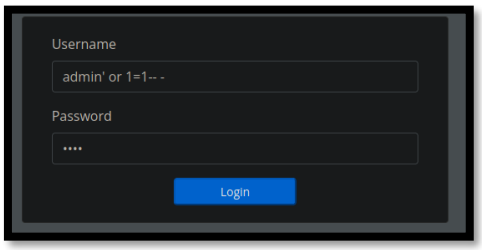


Realizamos una búsqueda por fuerza bruta de directorios con la IP, pero no encontramos nada de interés. Vamos a acceder a la web, pero esta vez con el fqdn preprod-payroll.trick.htb, que anteriormente tendremos que haber metido en el fichero hosts de nuestra máquina atacante.



2. Análisis de vulnerabilidades

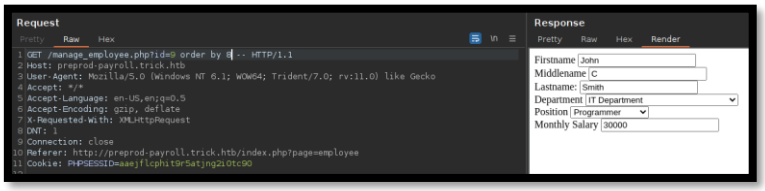
Miramos si podemos hacer una inyección de SQL con “admin’ or 1=1 -- -“, y efectivamente ganamos acceso a la aplicación, como usuario “Administrator”.



En el título de la web, vemos que la aplicación se llama “Recruitment Management System”.

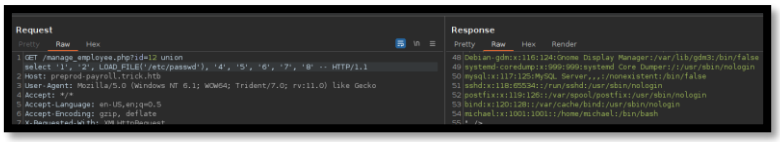
Revisamos si existen exploits para esta aplicación.

Nos llama la atención el del SQL Injection. En el exploit, nos hace referencia a una opción llamada “vacancy” que no tenemos. Pero podemos realizar un ataque similar con la opción de modificación de los datos del empleado. Usando el parámetro “order by”, detectamos que tenemos 8 columnas.

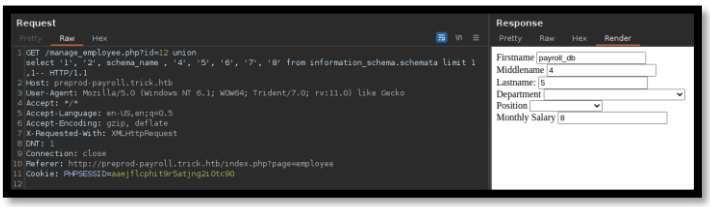


Detectamos sobre qué campos podemos escribir.

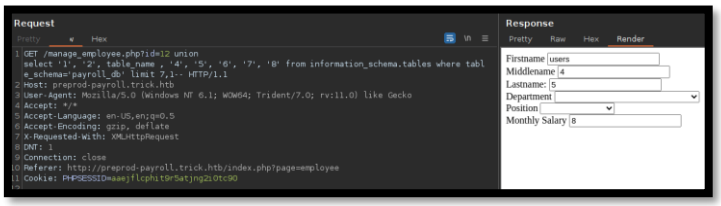
Intentamos leer el fichero “/etc/passwd”. Conseguimos obtener el usuario del sistema llamado “michael”.



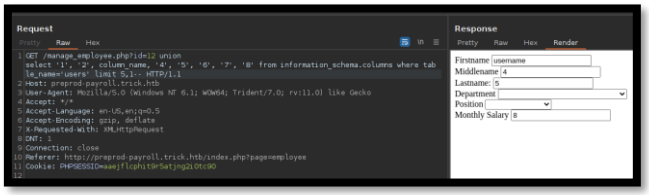
Seguimos enumerando, esta vez, consultamos las bases de datos del sistema. Solo hay una base de datos llamada “payroll_db”.



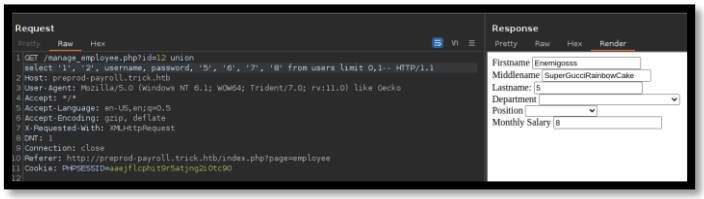
Detectamos como se llama la tabla de usuarios.



Localizamos las columnas de usuario y password.



Obtenemos unas credenciales. Solo tenemos un usuario en esa tabla.



1. Clave: SuperGucciRainbowCake

Intentamos conectarnos con el usuario “michael” y la anterior clave por ssh pero no funciona. Como tenemos un servidor Nginx, vamos a enumerar los sitios configurados. Para ello intentamos leer la configuración por defecto que está en el fichero “/etc/nginx/sites-enabled/default”.

Descubrimos una nueva URL “preprod-marketing.trick.htb”. Metemos la nueva entrada en el /etc/hosts, y revisamos la web. En esta web, vemos que se acontece un LFI.

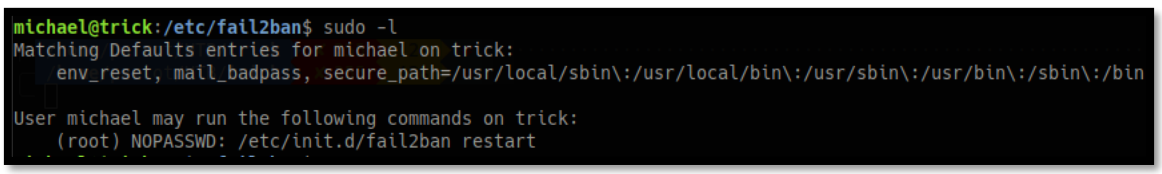
3. Explotación y acceso

Intentamos conseguir la id_rsa del usuario.

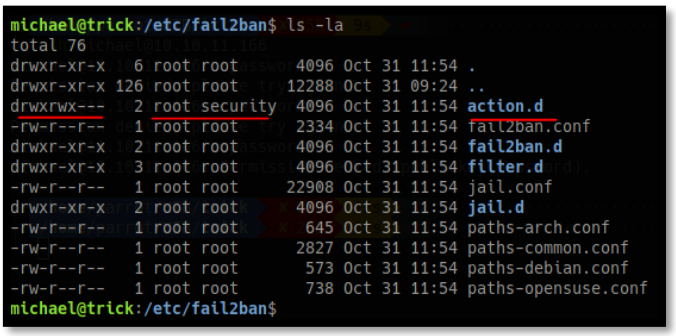
Intentamos conectarnos por ssh con el usuario “michael”.

4. Escalada de privilegios

Miramos a qué grupos pertenecemos que privilegios sudo tenemos.



Revisamos los privilegios y vemos qué permisos tenemos en el directorio de la aplicación fail2ban. Tenemos todos los permisos sobre el directorio por el grupo al que pertenecemos (security).



Buscamos como abusar del servicio de fail2ban:

```
https://youssef-ichioui.medium.com/abusing-fail2ban-misconfiguration-to-escalate-privileges-on-linux-826ad0cdafb7
```

Copiamos el fichero *iptables-multiport.conf* en /tmp/, lo modificamos para que, cuando se vaya a producir un "ban", la acción ejecutada añada permisos SUID a la bash.

Borramos el fichero original de */etc/fail2ban/action.d/iptables-multiport.conf* (recordar que el usuario tiene permisos para maniobrar en el directorio, pero no modificar los propios ficheros) y copiamos nuestro fichero en esa ruta. Reiniciamos con "*sudo /etc/init.d/fail2ban restart*" el servicio para que aplique las configuraciones.

Intentamos sucesivos intentos erróneos de conectarnos por SSH, para que se ejecute nuestra acción. Revisamos si se han cambiado los permisos de bash y escalamos privilegios de root.