CASO PRÁCTICO: RECONOCIMIENTO DE UNA ORGANIZACIÓN

Objetivo:

Realizar un reconocimiento completo de una organización y extraer toda la información sensible.

Contenido:

- Técnicas de Footprinting
- Técnicas de Fingerprinting
- Técnicas OSINT

Detalles:

En esta práctica el alumno aplicará las técnicas y utilizará las diferentes herramientas vistas durante el módulo.

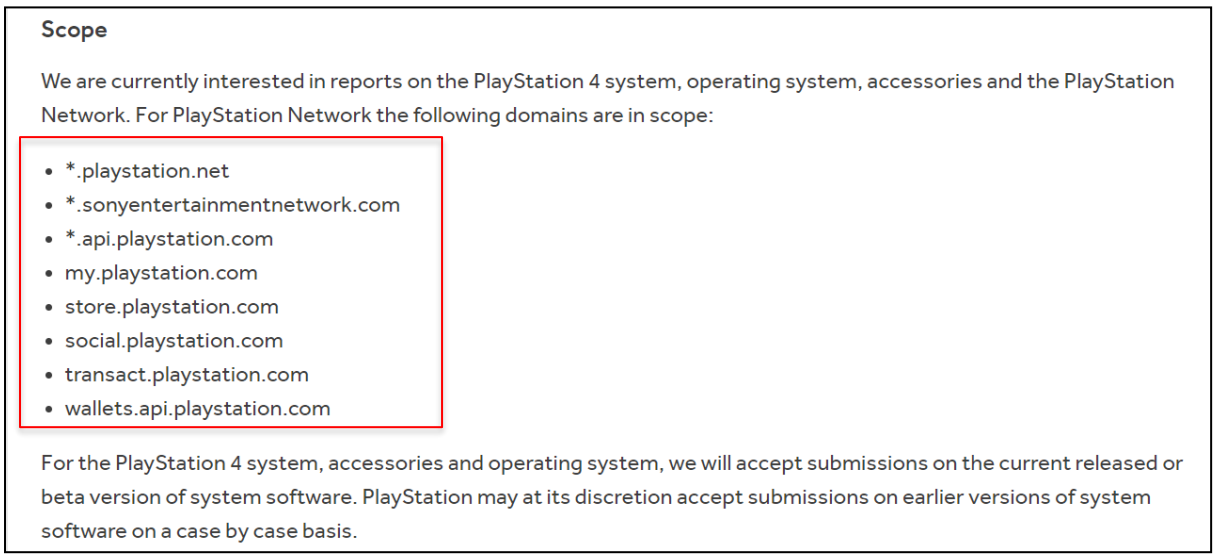
Preparación

El alumno deberá elegir una organización que esté dentro del programa de hackerone.

- Crear una cuenta en https://hackerone.com/
- Elegir una organización con varios dominios en el scope.
- Elegir una organización con subdominios en el scope.
- Comprobar detalladamente que está permitido atacar dichos dominios.

Por ejemplo, el scope de Playstation cumple los requisitos:

https://hackerone.com/playstation



Scope

We are currently interested in reports on the PlayStation 4 system, operating system, accessories and the PlayStation Network. For PlayStation Network the following domains are in scope:

- *.playstation.net
- *.sonyentertainmentnetwork.com
- *.api.playstation.com
- my.playstation.com
- store.playstation.com
- social.playstation.com
- transact.playstation.com
- wallets.api.playstation.com

For the PlayStation 4 system, accessories and operating system, we will accept submissions on the current released or beta version of system software. PlayStation may at its discretion accept submissions on earlier versions of system software on a case by case basis.

Desarrollo

El objetivo es obtener la máxima información posible de la organización elegida. Esto incluye, pero no limita:

- Dominios relacionados (dentro del scope).
- Información de cada dominio.
- Análisis de vulnerabilidades.
- Correos corporativos.

Evaluación

Es obligatorio la entrega de un informe para considerar como APTA la práctica. Este informe ha de contener:

- Los resultados más importantes del reconocimiento de la organización.
- Detalles de las herramientas y los comandos utilizados. Paso a paso para que puedan ser repetidos.
- Otros ficheros suplementarios donde se almacenen los resultados. Para facilitar que el informe principal no esté lleno de cientos de páginas con tablas.
- Prima más el contenido y la estructura que la apariencia del informe.