Práctico 2 - Pentesting

Deadline parte ENTREGABLE: 15 de Octubre 23:59
Sugerencia: Trabajar desde la máquina virtual con Kali instalada en el TP0.

- Para practicar:
    - https://drive.google.com/file/d/1CBiLVfB0T2PeI33tGxp8jv9kDRPX0gm7/view?usp=sharing
    - https://www.vulnhub.com/

Parte entregable

1. **[SOLO ALUMNOS DE CARRERAS DE FAMAF]**
   Realizar la fase de reconocimiento y enumeración sobre la red pública de la Facultad de Matemática, Astronomía, Física y Computación.

Alcance:

Red pública: la clase C donde se encuentra **www.famaf.unc.edu.ar**

- Se deberá realizar el reconocimiento de la información pública de las diferentes fuentes estudiadas en clases (OSINT, SHODAN, ...)

- Se deberá realizar el escaneo y enumeración de la red, hosts, puertos, servicios y versiones.

- Se deberá completar el formulario para registrar la IP desde la cual se realizará la evaluación.

- Cualquier vulnerabilidad encontrada deberá ser reportada inmediatamente.

- Periodo de trabajo permitido: 30/09/20 al 13/10/20.

No estará permitido:
- Realizar escaneos/tests intrusivos que prueben explotar vulnerabilidades.

El no cumplimiento de esta premisa puede implicar la desaprobación de este trabajo y otras sanciones correspondientes.

1. **[SOLO ALUMNOS DE CARRERAS EXTERNAS A FAMAF]**
   Realizar la fase de reconocimiento y enumeración sobre la/las redes pública/s de los siguientes dominios:

Alcance:

Dominios:

- *.playstation.net
- *.sonyentertainmentnetwork.com
- *.api.playstation.com

- Se deberá investigar la información pública de las diferentes fuentes estudiadas en clases (OSINT, SHODAN, ...)

- Se deberá realizar el escaneo y enumeración de la red, hosts, puertos, servicios y versiones.

- [opcional] Podrán cambiar de dominio/s avisando previamente al docente (en común acuerdo) y solo por dominios con política de escaneo y enumeración abiertas.

---

2. **[PARA TODOS]** Descargar la máquina virtual de evaluación del siguiente enlace:

   https://drive.google.com/file/d/0B5ZJif86MN7SbVhrMXdiZ2NFVUE/view

a. Realizar las distintas fases de un test de intrusión sobre dicha máquina virtual intentando explotar la máxima cantidad de vulnerabilidades y alcanzar el máximo nivel de privilegios posible. Realizar un informe detallando el proceso realizado.
b. Realizar un informe que describa las vulnerabilidades encontradas, el riesgo de cada una y las mitigaciones para corregirlas.