Trabajo práctico 1: De todo un poco

Precalentamiento

Los ejercicios de este precalentamiento **no se entregan**. Esto es una guía para dejar todo listo para los próximos TPs.

Crear cuenta y armar grupos

Armar el grupo (entre 5 y 7 personas). Deben registrarse en cryptohack.org , hacer una cuenta compartida por grupo.

Setear entorno

Cryptohack nos ofrece un docker con todas las dependencias instaladas. Docker nos permite levantar el entorno ya configurado en un container.

1. Si no tienen docker instalado, pueden descargarlo de acá: https://www.docker.com/products/docker-desktop En el caso de Windows, incluir WSL en la instalación
2. Ejecutar docker, necesitamos que corra de fondo
3. Abrir una terminal y en cualquier directorio ejecutar:

```
docker run -p 127.0.0.1:8888:8888 -it hyperreality/cryptohack:latest
```

La primera vez va a demorar porque necesita descargar toda la imagen, las siguientes levanta más rápido.

4. Una vez levantado, al final nos va a decir “The Jupyter Notebook is running at: http://(2aeed6e8e141 or 127.0.0.1):8888/”. Traducción: entrar con un navegador a http://127.0.0.1:8888/

Con esto levantamos todo un entorno de Jupyter Notebook en el navegador, donde podemos ejecutar python de forma interactiva.

Cuando terminamos, podemos cerrar la instancia de docker desde la terminal con ctrl+C.

CRIPTOGRAFÍA

Familiarizándonos con la plataforma

Estos son ejercicios muy básicos para familiarizarse con el entorno local y la plataforma de Cryptohack. No hace falta entregarlos.

Resolver los tres ejercicios de la categoría Introduction:

- Finding flags
- Great snakes
- Network attacks

TP en sí

Estos ejercicios sí se entregan. ¡No se olviden de entregarlos!

1. Listar los integrantes del grupo y el username de Cryptohack del grupo.

El trabajo práctico consiste en resolver los siguientes ejercicios de la categoría General. Por cada uno deberán entregar la **flag** encontrada y una **breve explicación** de cómo la encontraron. Imaginen que se lo explican a alguien que nunca lo resolvió y tiene que poder resolverlo con sólo su explicación. No hace falta entregar el código.

Encoding

De la sección encoding, hacer todos:

2. ASCII
3. Hex
4. Base64
5. Bytes and Big Integers
6. Encoding Challenge

XOR

De la sección XOR, hacer todos:

7. XOR Starter
8. XOR Properties
9. Favourite byte
10. You either know, XOR you don't — Pista: miren bien la key
11. Lemur XOR — Tip: Image de PIL y numpy pueden ser útiles

CRIPTOGRAFÍA

Mathematics

De la sección Mathematics, hacer todos.

Tip: probablemente quieran chequear algunas funciones de Crypto.Util.number

12. Greatest Common Divisor
13. Extended GCD
14. Modular Arithmetic 1
15. Modular Arithmetic 2
16. Modular Inverting

Data formats

De la sección Data Formats, hacer todos:

17. Privacy-Enhanced Mail? Tip: chusmeen las librerías Crypto.PublicKey
18. CERTainly not
19. SSH Keys
20. Transparency A veces es cuestión de googlear...