

# Mamá, yo quiero ser hacker

Manuel Rivas | [@0xmrvias](https://twitter.com/0xmrvias)



# Índice

- 1. About Me**
- 2. ¿Que es el Pentesting?**
- 3. Metodologías**
- 4. Fases y herramientas**
- 5. Entrenamiento**
- 6. Manos a la obra**

# About Me

- Ethical Hacker & Computer Security Lover
- Profesor de Formación Profesional (IES Rafael Alberti)
- Máster en seguridad de las TIC
- Máster en Cloud Security
- Security Research at Cloud competency Center (NCI College)



# Índice

- 1. About Me**
- 2. ¿Que es el Pentesting?**
- 3. Metodologías**
- 4. Fases y herramientas**
- 5. Entrenamiento**
- 6. Manos a la obra**

# Disclaimer

- Las técnicas mostradas en este taller tienen fines educativos.
- Sólo está permitido el uso de herramientas intrusivas en entornos controlados, o con autorización previa.
- Si hace uso de las mismas, en sistemas y redes ajenos o públicos, será bajo bajo su responsabilidad.



# ¿Pentesting?



# ¿Qué es el Pentesting?

- El Pentesting es una abreviatura formada por dos palabras “penetration” y “testing”.
- Es una práctica/técnica que consiste en atacar diferentes entornos o sistemas con la finalidad de encontrar y prevenir posibles fallos en el mismo.

# Tipos de Pentesting



## CAJA BLANCA

El auditor conoce información sobre la infraestructura, aplicación o sistemas que debe atacar, se dispone de un usuario con permisos limitados y, en algunos casos, se tendría acceso al código fuente. Se realiza en las oficinas del cliente o mediante VPN proporcionada por el cliente.

Ej: Empleado desleal, empleado que quiere dañar la reputación de la empresa.



## CAJA GRIS

El auditor conoce información parcial sobre la infraestructura, aplicación o sistema que debe atacar. Esta modalidad de Pentesting se trata de una mezcla de las otras dos.



## CAJA NEGRA

El auditor no conoce información alguna de la infraestructura, aplicación o sistemas que debe atacar. Únicamente el nombre de la empresa y el alcance definido.

Ej: Ciberdelincuente o empresa de la competencia que quiere dañarle o hacerse con información importante de sus clientes.

# Índice

- 1. About Me**
- 2. ¿Qué es el Pentesting?**
- 3. Metodologías**
- 4. Fases y herramientas**
- 5. Entrenamiento**
- 6. Manos a la obra**

# Metodologías de Pentesting



# Metodologías de Pentesting



# Metodologías de Pentesting



# Índice

1. ~~About Me~~
2. ~~¿Qué es el Pentesting?~~
3. ~~Metodologías~~
4. Fases y herramientas
5. Entrenamiento
6. Manos a la obra

# Fases y herramientas



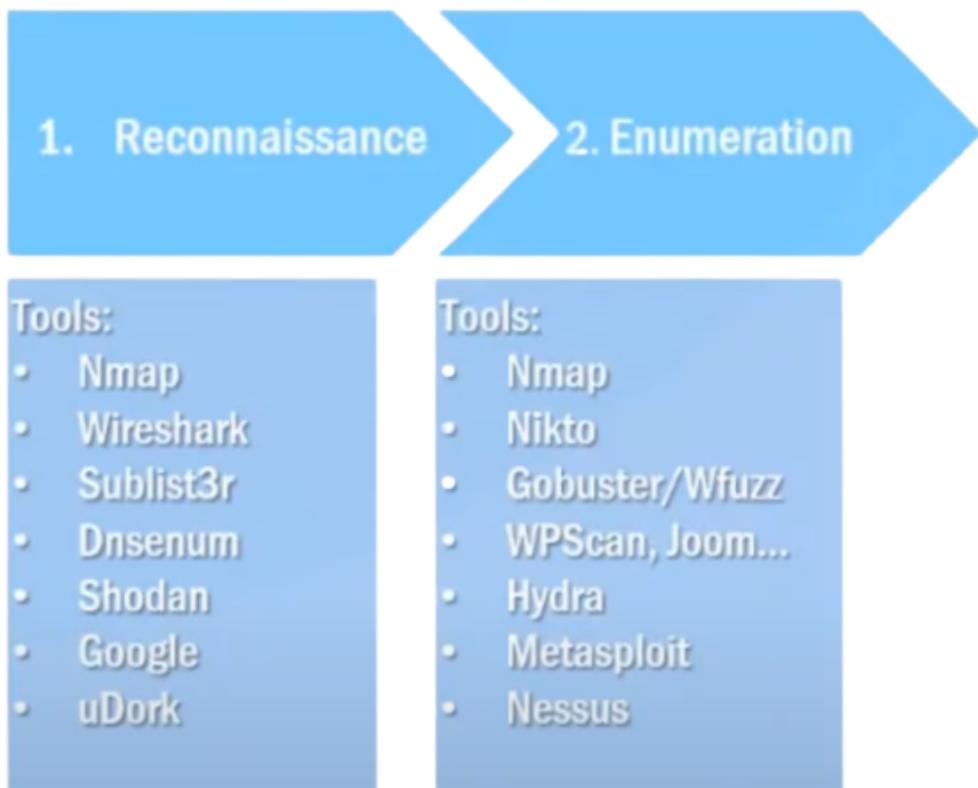
# Fases y herramientas

## 1. Reconnaissance

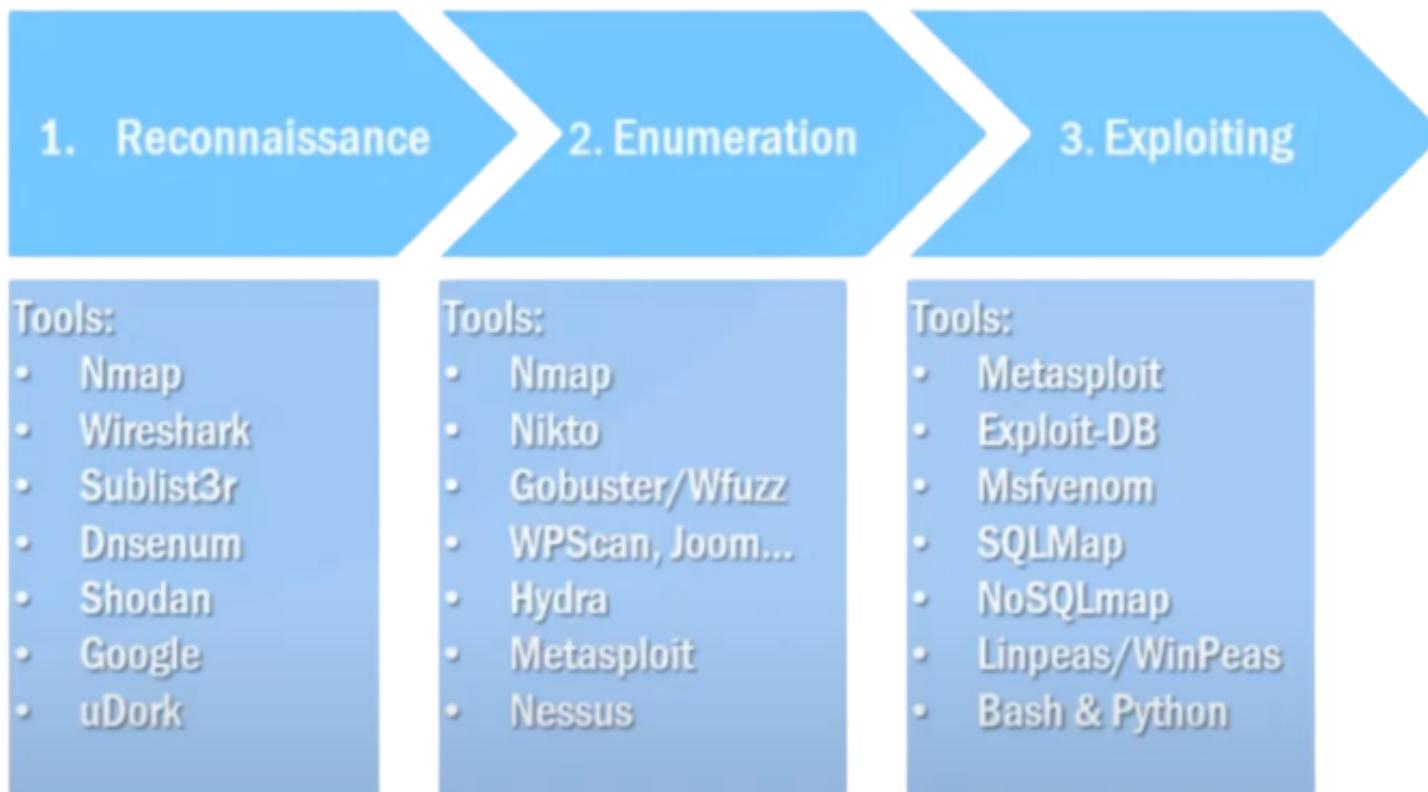
Tools:

- Nmap
- Wireshark
- Sublist3r
- Dnsenum
- Shodan
- Google
- uDork

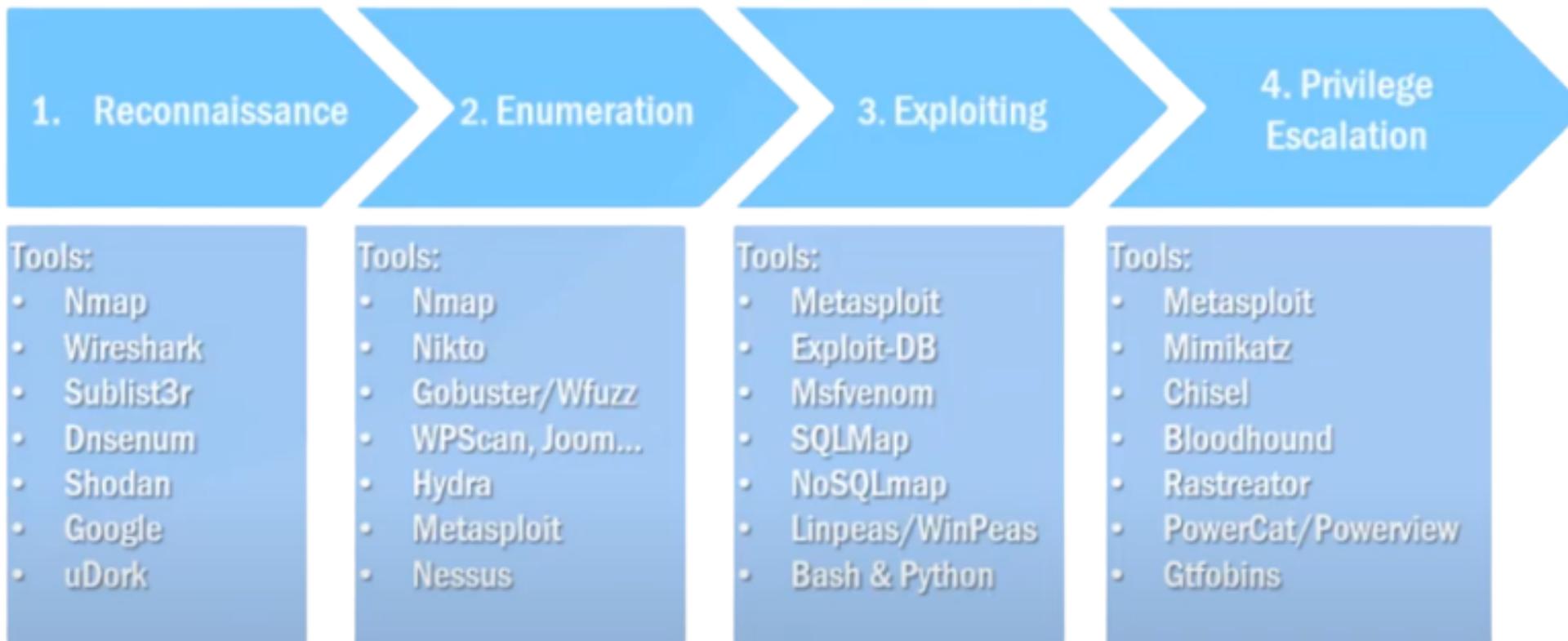
# Fases y herramientas



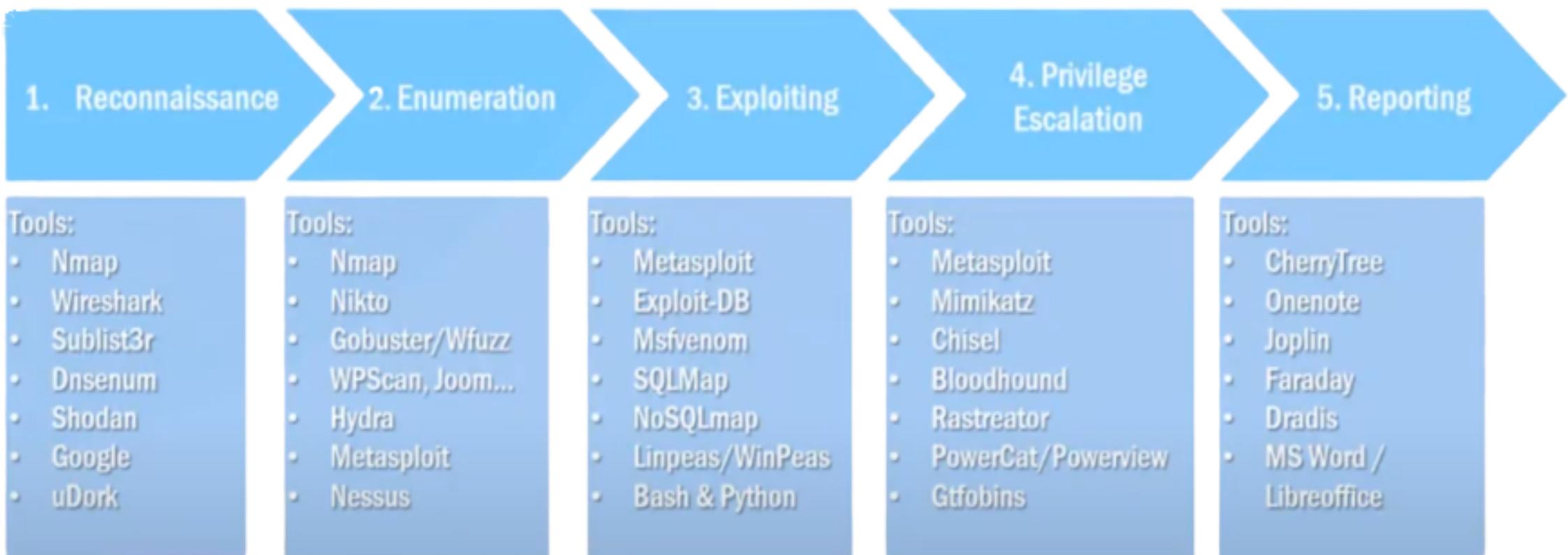
# Fases y herramientas



# Fases y herramientas



# Fases y herramientas



# Índice

1. ~~About Me~~
2. ~~¿Qué es el Pentesting?~~
3. ~~Metodologías~~
4. ~~Fases y herramientas~~
5. Entrenamiento
6. Manos a la obra

# Entrenamiento



**Easy/Medium level**  
(Genial para empezar)



**Medium/Hard**  
(Ideal para mejorar)

*NEVER  
give up!*

$$V = (C + H) * A$$

# "El ciberespacio, amenazas y oportunidades"



# "CYBEROLYMPICS"



<https://www.is4k.es/programas/cyberolympics>

# "El ciberespacio, amenazas y oportunidades"

## IES Rafael Alberti gana segundo 'oro' consecutivo en Las Olimpiadas de Ciberseguridad

El centro, se ha proclamado vencedor, por segundo año consecutivo, de las V Olimpiadas de Ciberseguridad 2019 para centros educativos de España (las CyberOlympics), organizadas por el Instituto Nacional de Ciberseguridad (INCIBE).



Alumnos de IES Rafael Alberti recogiendo el premio | Descubre la FP

# "El ciberespacio, amenazas y oportunidades"

## Premio 12ENISE

### NUEVA EDICIÓN 2019

Estás visitando la sección del premio 12ENISE correspondiente al pasado evento (2018).

Accede a la [edición del premio 13ENISE \(2019\)](#).

Felicidades al I.E.S. Rafael Alberti de Cádiz, ganadores del Premio ENISE con su proyecto El ciberespacio: Amenazas y Oportunidades. Deseamos que disfruten del material tecnológico para el centro valorado en 2.500€.



# "El ciberespacio, amenazas y oportunidades"

## **IES Rafael Alberti obtiene el premio nacional de la Agencia Española de Protección de Datos**

El centro ha sido reconocido con el Premio de Protección de Datos 2019 a las 'Buenas prácticas educativas en privacidad y protección de datos personales para un uso seguro de internet', que otorga anualmente la Agencia Española de Protección de Datos (AEPD).



IES Rafael Alberti de Cádiz | Descubre la FP

# "El ciberespacio, amenazas y oportunidades"

El equipo español que participará en la competición europea de ciberseguridad en Bucarest comienza su formación en León

Publicado el 01/07/2019



Los 15 mejores talentos de España, en materia de ciberseguridad, han recibido formación técnica y de soft skills necesarios para el desempeño de la selección en la competición

# "El ciberespacio, amenazas y oportunidades"

**Un estudiante gaditano, seleccionado para el Campeonato Europeo de Ciberseguridad**



🕒 Publicado: Viernes, 12 Octubre 2018 01:42

✍ Escrito por Redacción



Jose Manuel Otero Oliveira, estudiante del ciclo de grado medio de informática del IES Rafael Alberti, formará parte del equipo español que participará en el "European Cyber Security Challenge 2018". El mayor campeonato técnico a nivel europeo en materia de ciberseguridad, y donde el equipo español se ha alzado con la victoria en los dos últimos años, se celebra la próxima semana, del 14 al 17 de octubre, en Londres.

# "El ciberespacio, amenazas y oportunidades"



# "El ciberespacio, amenazas y oportunidades"



# EL ÉXITO NO LLEGA POR CASUALIDAD

ES TRABAJO DURO, PERSEVERANCIA,  
APRENDIZAJE, SACRIFICIO Y SOBRE TODO,  
AMOR POR LO QUE HACES

- PELE



# Índice

1. ~~About Me~~
2. ~~¿Qué es el Pentesting?~~
3. ~~Metodologías~~
4. ~~Fases y herramientas~~
5. ~~Entrenamiento~~
6. Manos a la obra

# Manos a la obra



; Happy Hacking !





Manuel Rivas | [@0xmrvs](https://twitter.com/0xmrvs)