INTRODUCCIÓN METASPLOIT

Metasploit **es el framework más común usado en seguridad informática para tareas de creación o ejecución de *exploits*.**

1.

VULNERABILIDADES

VULNERABILIDADES

Tipos de vulnerabilidades

- De software
  - Inyección SQL
  - XSS
  - Desbordamiento de buffer …
- De hardware
- Red de comunicaciones

VULNERABILIDADES ETAPAS

- *Nacimiento*: defectos provenientes de la creación del producto por parte del desarrollador. Defecto = Vulnerabilidad cuando se puede aprovechar para romper la seguridad del sistema.

- *Descubrimiento*: Momento en el que un descubridor se percata de la existencia de dicha vulnerabilidad.

VULNERABILIDADES ETAPAS

- *Comunicación*: el descubridor revela la vulnerabilidad. Puede ser de forma privada o sacarla a la luz (publicada ante todo el mundo).

- *Corrección*: El desarrollador del producto analiza la vulnerabilidad, localiza el problema y lo corrige con un parche o nueva versión.

- *Publicación*: La vulnerabilidad se da a conocer de forma extendida, puede que mediante un comunicado para las actualizaciones.

VULNERABILIDADES ETAPAS

- Automatización de la explotación: creación de una herramienta para explotar la vulnerabilidad. Dicha herramienta o script se le conoce como ***exploit***. Peligro ante expertos e inexpertos.

- Muerte: Número de sistemas vulnerables es insignificante. Herramienta retirada, parche para solucionarla muy extendido o falta de interés para explotarla.

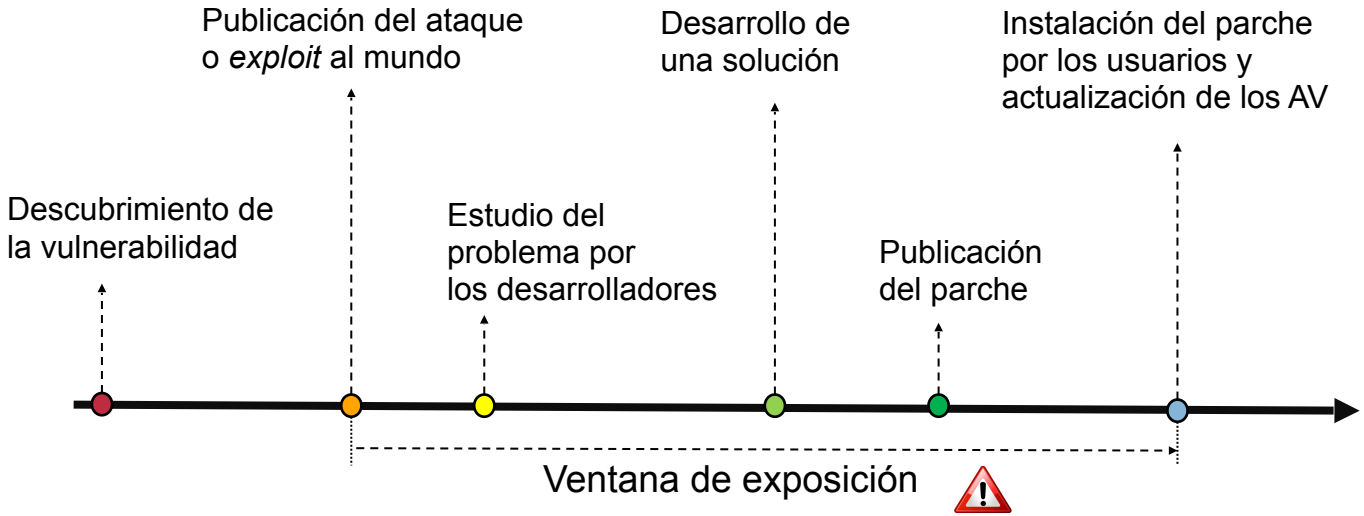
VULNERABILIDADES CASO I

Corrección y publicación puede suceder al mismo tiempo.

- El descubridor de la vulnerabilidad es el desarrollador del producto.
- Evitan que terceros las aprovechen y se generen problemas de seguridad y reputación.
- Es importante un equipo de *testing* y *desarrollo* con buena formación en seguridad

VULNERABILIDADES CASO II

Si se publica la vulnerabilidad y *exploit* antes de que se corrija la misma surge un ***Zero-day***



VULNERABILIDADES CASO III

¿Descubrimiento a la vez que el nacimiento?

- ***¡Vulnerabilidad intencionada!***
- Funcionan a modo de *backdoor* o *caballo de Troya*.
- NSA, FBI o grandes multinacionales suelen estar detrás.
- Posible objetivo > captar información y datos

2.

METASPLOIT

INTRODUCCIÓN

Framework más famoso usado por profesionales de seguridad informática para creación y ejecución de exploits

- Gran comunidad detrás (popularidad)
- Tareas automatizadas en descubrimiento y explotación (+ v3.0)
- Subdividido en componentes y módulos que pueden crecer con nuevas funcionalidades

PENTESTER

- Identificar y obtener información (Puertos y servicios)
- ¿Existen vulnerabilidades en dichos sistemas o servicios? = Se intentan explotar

Dos tipos de *pentesting*:

- Solo descubrimiento de vulnerabilidades
- Con ejecución de exploits aprovechando las vulnerabilidades encontradas

POTENCIAL DE METASPLOIT

- Posibilidad de que los usuarios creen sus propios *exploits*, *payloads* o *encoders*.
- Útil para desarrolladores, *pentesters* y *sysadmins*.
- Puede usar herramientas de terceros como *Nmap* o *Nessus*.
- Integrado en Kali
- +10.000 exploits y herramientas auxiliares

3.

HERRAMIENTAS AUXILIARES Y MÓDULOS

HERRAMIENTAS AUXILIARES

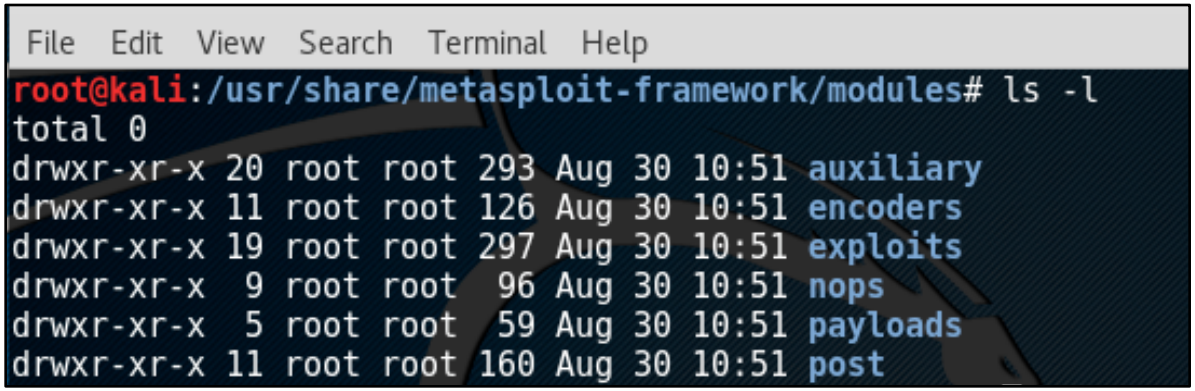
- *Msfpayload*: Gestión de *shellcodes*, desde su creación, ejecución y consulta.

- *Msfencode*: Para evadir sistemas antimalware o IDS/IPS intentando dificultar que estos detecten la ejecución del *payload*.

- *Msfvenom*: Integra en una única tarea las ventajas de *msfpayload* y *msfencode*.

MÓDULOS

Localizados dentro de Kali en el directorio de instalación de Metasploit.



MÓDULOS

- *Auxiliary*: Herramientas a usar en una prueba de intrusión: escaneos, denegación de servicios, *sniffers* o *fuzzers* entre otras.

- *Encoders*: Herramientas para ofuscar el código de las *shellcodes*, para evadir los sistemas antivirus y que no descubran el payload.

MÓDULOS

- *Exploits*: El más importante por tener todos los exploits publicados en el framework, listos para configurarlos y ejecutarlos.

- *Payloads*: Dispone de todos los payloads disponibles en el framework organizados por tipos, sistemas operativos y tecnologías.