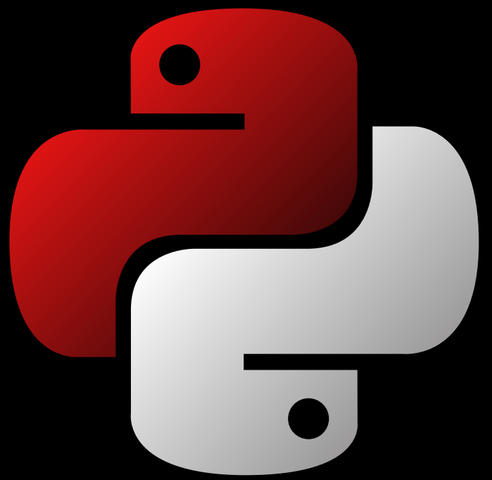
DEEPSEC ACADEMY

DeepSec Pentesting Web Python Course



Sockets

¿Que es Nmap?

Es un programa de codigo abierto que sirve para efectuar rastreo de puertos aunque influye diferentes funcionalidades que le permiten obtener mucha información valiosa de una red

Sockets

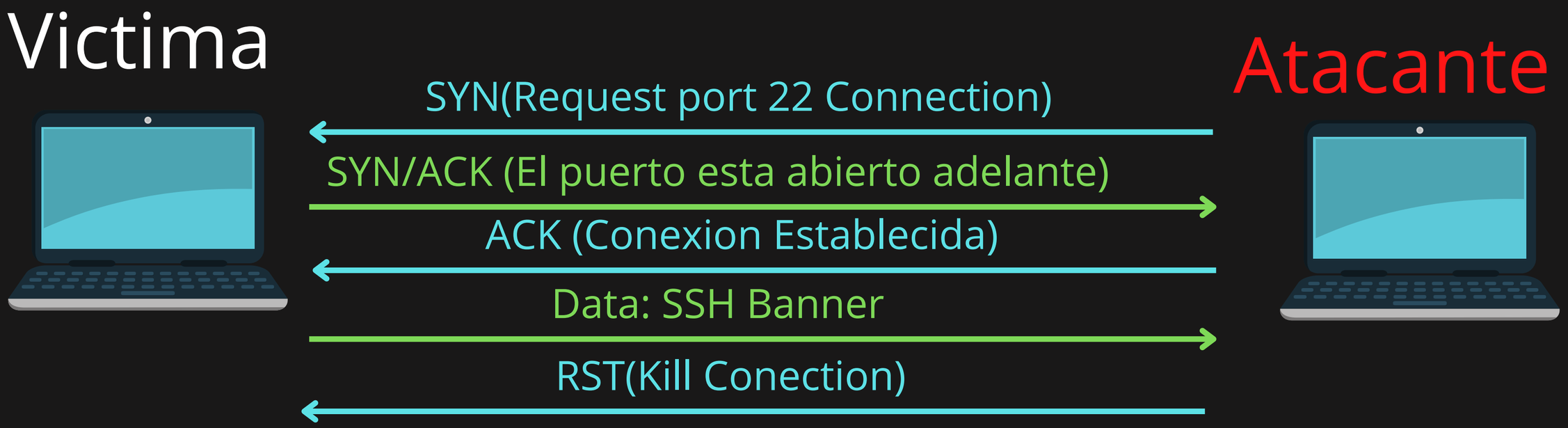
Tipos de Escaneo con NMAP

- sT (TCP Connect Scan): Es la opción que se suele utilizar para detectar si un puerto esta abierto o cerrado, pero tambien suele ser el mecanismo mas auditado y vigilado por sistemas de deteccion de intrusos. Con esta opcion, un puerto se encuentra abierto si el servidor responde con un paquete que contenga el flag ACK al enviar un paquete con el flag SYN

Sockets

Tipos de Escaneo con NMAP

- sT (TCP Connect Scan)



Sockets

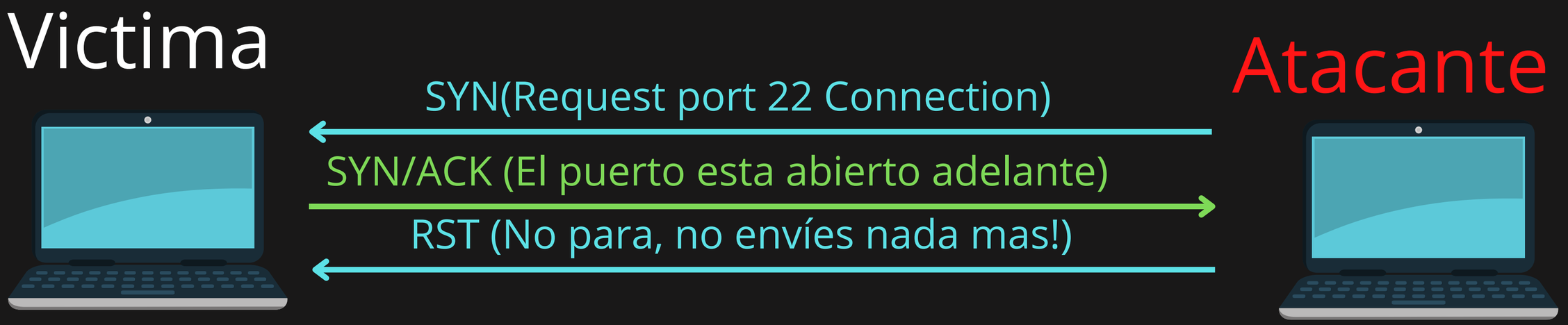
Tipos de Escaneo con NMAP

- sS (TCP Stealth Scan): Tipo de escaneo basado en el TCP Connect Scan con la diferencia de que la conexion en el puerto indicado no se realiza de forma completa. Consiste en comprobar el paquete de respuesta del objetivo ante un paquete con el flag SYN habilitado. Si el objetivo responde con un paquete que tiene el flag RST, entonces se puede comprobar si el puerto esta abierto o cerrado

Sockets

Tipos de Escaneo con NMAP

- sS (TCP Stealth Scan)



Sockets

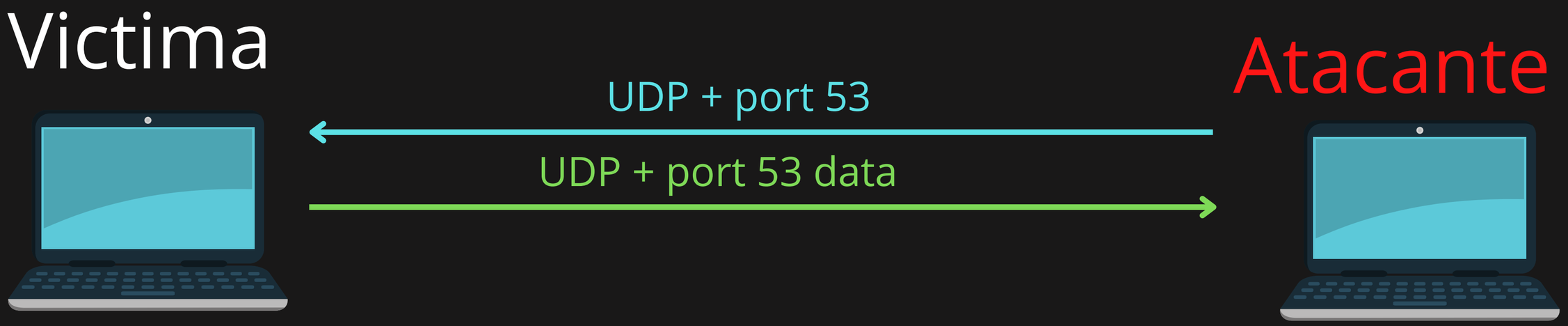
Tipos de Escaneo con NMAP

- sU (UDP Scan): Tipo de escaneo basado en el protocolo UDP donde no se lleva a cabo un proceso de conexion, sino que simplemente se envia un paquete UDP para determinar si el puerto esta abierto. Si la respuesta es otro paquete UDP, significa que el puerto esta abierto. En el caso de que el puerto no este abierto se recibira un paquete ICMP del tipo 3(destino inalcanzable)

Sockets

Tipos de Escaneo con NMAP

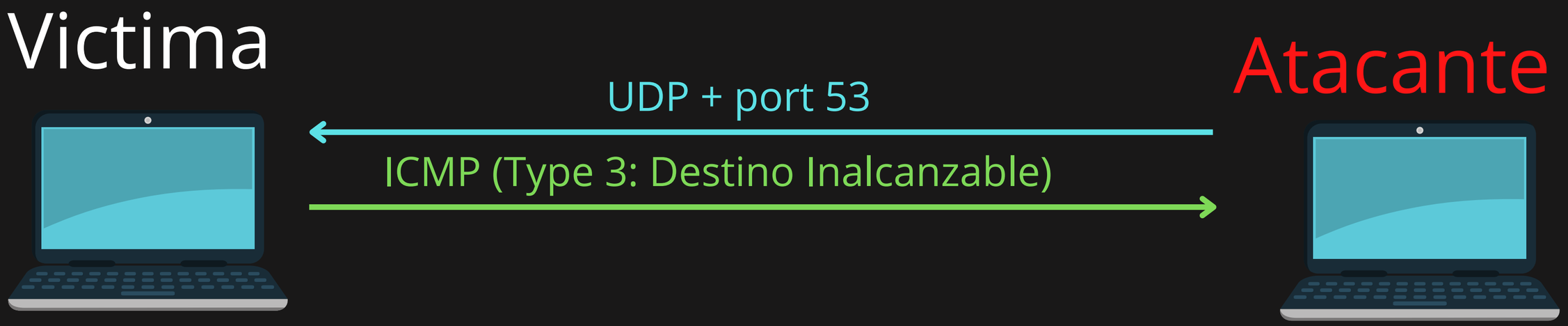
- sU (UDP Scan):



Sockets

Tipos de Escaneo con NMAP

- sU (UDP Scan):



Sockets

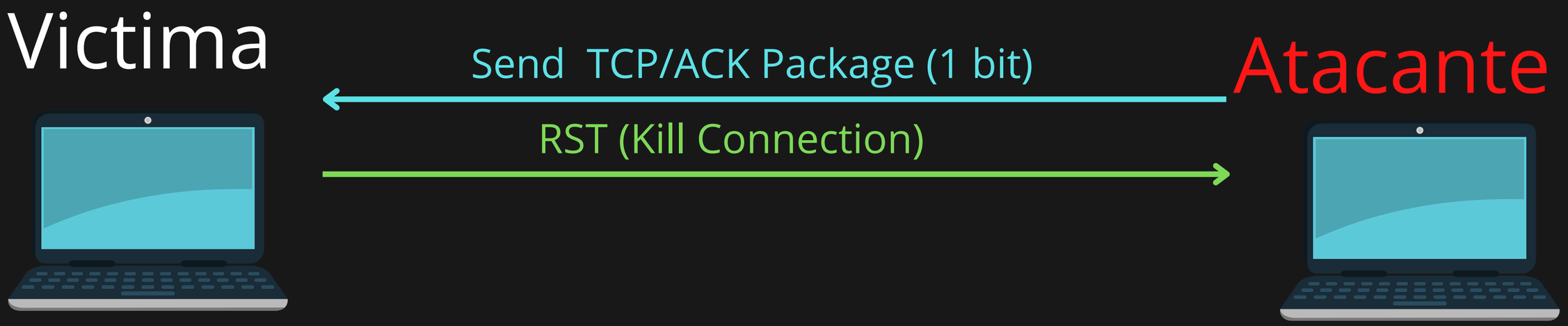
Tipos de Escaneo con NMAP

- sA (TCP ACK Scan): Tipo de escaneo que permite saber si nuestra maquina objetivo tiene algun tipo de firewall en ejecución. Lo que hace este escaneo es enviar un paquete con el flag ACK activado y se envía a la maquina objetivo. En el caso de que la maquina remota responda con un paquete que tenga el flag RST activado, se puede determinar que el puerto no se encuentra filtrado por ningún firewall. En el caso de que el no responda o lo haga con un paquete ICMP del tipo 3 se puede determinar que hay un firewall filtrando los paquetes enviados en el puerto indicado.

Sockets

Tipos de Escaneo con NMAP

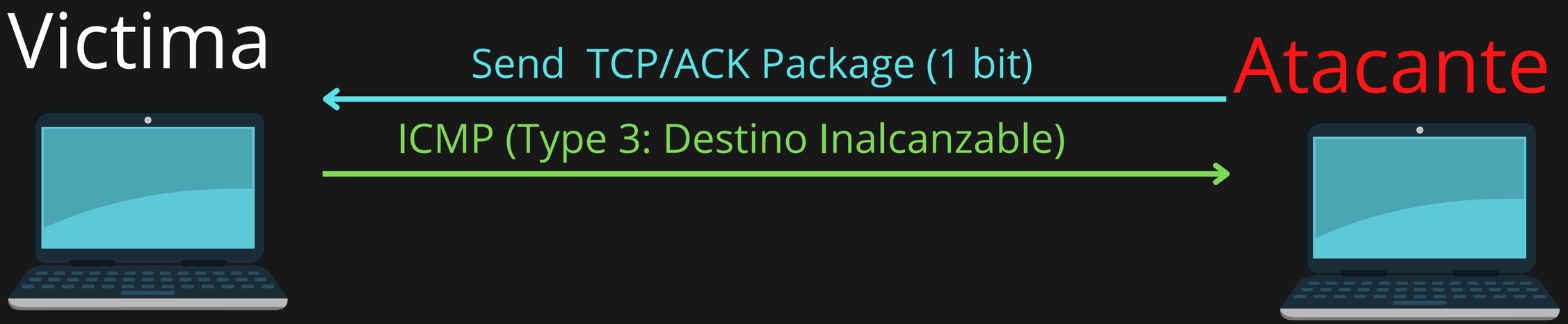
- sA (TCP ACK Scan):



Sockets

Tipos de Escaneo con NMAP

- sA (TCP ACK Scan):



Sockets

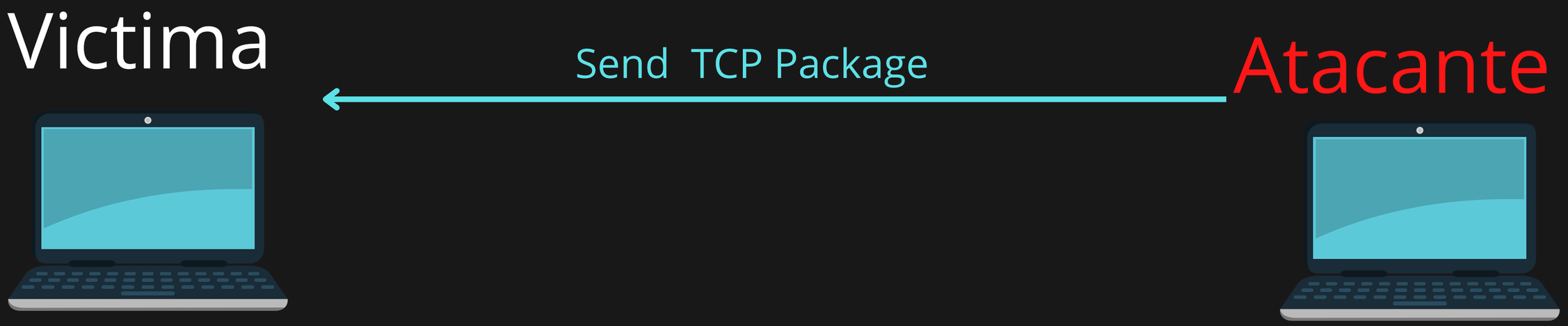
Tipos de Escaneo con NMAP

- sN (TCP NULL Scan): Tipo de escaneo que envia un paquete TCP a la maquina objetivo sin ningun flag. Si la maquina remota no emite nunguna respuesta, se puede determinar que el puerto se encuentra abierto. Si la maquina remota devuelve un flag RST, podemos decir que el puerto se encuentra cerrado

Sockets

Tipos de Escaneo con NMAP

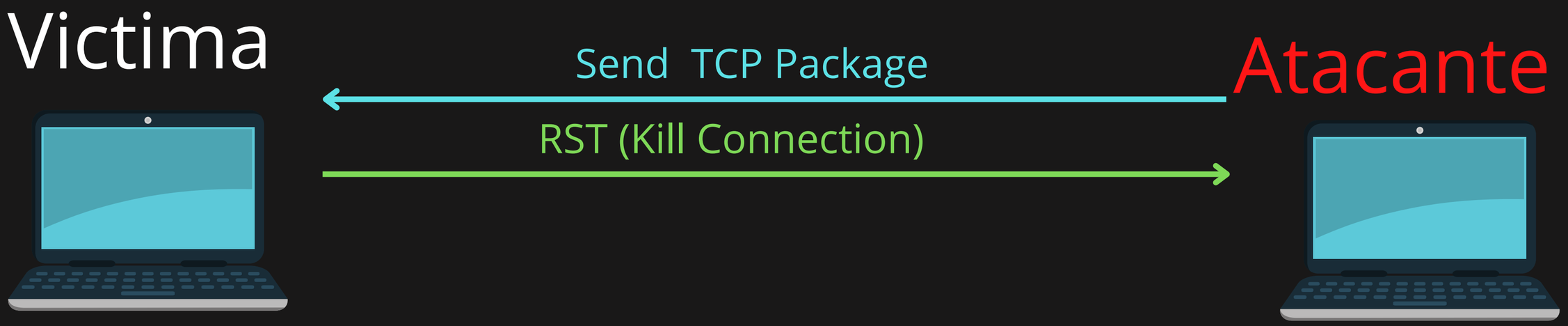
- sN (TCP NULL Scan):



Sockets

Tipos de Escaneo con NMAP

- sN (TCP NULL Scan):



Sockets

API Nmap en Python

En python podemos hacer uso de nmap a través de la librería python-nmap la cual nos permite manipular fácilmente los resultados de un escaneo.

```
> pip install python-nmap
```

Sockets

API Nmap en Python

En python podemos hacer uso de nmap a través de la librería python-nmap la cual nos permite manipular fácilmente los resultados de un escaneo.

```
> pip install python-nmap
```

¡Muchas gracias!