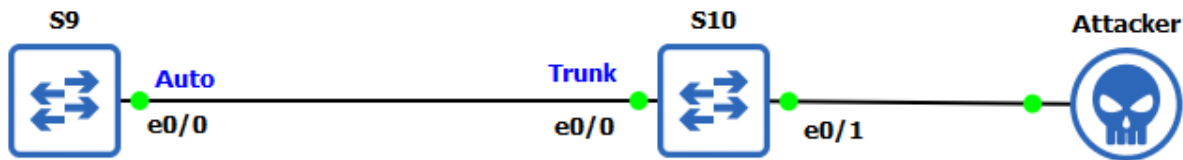


## VLAN Hopping Attack:

- o Attacker connects to a VLAN to gain access to traffic on other VLANs.
- o Attacker send spoofed trunk negotiation & interface configured as a trunked.
- o Disable any automated trunk negotiation (DTP) on Cisco Switches.
- o Never leave a port in "dynamic desirable", "dynamic auto" or "trunk" mode.
- o Hardcode all the access ports as access port and disable DTP everywhere.
- o Shutdown all the interfaces in Cisco Switches which are not in use.



Open Yersinia from Terminal type `root@kali:~# yersinia -G` and lunch attack.



The screenshot shows the Yersinia GUI. On the left, a 'Protocols' table shows the number of packets for various protocols:

Protocols	Packets
CDP	6
DHCP	0
802.1Q	0
802.1X	0
DTP	25
HSRP	0
ISL	4
MPLS	0
STP	163

The main window shows a 'Choose protocol attack' dialog with 'DTP' selected. Below it, a 'Choose attack' dialog is open, showing 'enabling trunking' as the selected attack type. A 'Last seen' log on the right shows timestamps for the attack.

```
s10#show interfaces trunk
```

```
Port      Mode      Encapsulation  Status  Native vlan
Et0/0    desirable n-802.1q      trunking  1
Et0/1    auto      n-802.1q      trunking  1
```