**Lateral VLAN Segmentation Bypass**

If direct access to a switch is available, VLAN segmentation can be bypassed. This involves reconfiguring the connected port to trunk mode, establishing virtual interfaces for target VLANs, and setting IP addresses, either dynamically (DHCP) or statically, depending on the scenario (**for further details check** [**https://medium.com/@in9uz/cisco-nightmare-pentesting-cisco-networks-like-a-devil-f4032eb437b9**](https://medium.com/@in9uz/cisco-nightmare-pentesting-cisco-networks-like-a-devil-f4032eb437b9)**).**

Initially, identification of the specific connected port is required. This can typically be accomplished through CDP messages, or by searching for the port via the **include** mask.

**If CDP is not operational, port identification can be attempted by searching for the MAC address**:

SW1(config)# show mac address-table | include 0050.0000.0500

Prior to switching to trunk mode, a list of existing VLANs should be compiled, and their identifiers determined. These identifiers are then assigned to the interface, enabling access to various VLANs through the trunk. The port in use, for instance, is associated with VLAN 10.

SW1# show vlan brief

**Transitioning to trunk mode entails entering interface configuration mode**:

SW1(config)# interface GigabitEthernet 0/2

SW1(config-if)# switchport trunk encapsulation dot1q

SW1(config-if)# switchport mode trunk

Switching to trunk mode will temporarily disrupt connectivity, but this can be restored subsequently.

Virtual interfaces are then created, assigned VLAN IDs, and activated:

sudo vconfig add eth0 10

sudo vconfig add eth0 20

sudo vconfig add eth0 50

sudo vconfig add eth0 60

sudo ifconfig eth0.10 up

sudo ifconfig eth0.20 up

sudo ifconfig eth0.50 up

sudo ifconfig eth0.60 up

Subsequently, an address request is made via DHCP. Alternatively, in cases where DHCP is not viable, addresses can be manually configured:

sudo dhclient -v eth0.10

sudo dhclient -v eth0.20

sudo dhclient -v eth0.50

sudo dhclient -v eth0.60

Example for manually setting a static IP address on an interface (VLAN 10):

sudo ifconfig eth0.10 10.10.10.66 netmask 255.255.255.0

Connectivity is tested by initiating ICMP requests to the default gateways for VLANs 10, 20, 50, and 60.

Ultimately, this process enables bypassing of VLAN segmentation, thereby facilitating unrestricted access to any VLAN network, and setting the stage for subsequent actions.

## References

* <https://medium.com/@in9uz/cisco-nightmare-pentesting-cisco-networks-like-a-devil-f4032eb437b9>