VLAN Hopping

VLAN hopping is a security threat , a method of attacking networked resources on a Virtual LAN (VLAN). The basic concept behind all VLAN hopping attacks is where a user can gain access to a VLAN not assigned to the switch port to which the user connects..

There are two primary methods of VLAN hopping: switch spoofing and double tagging. Both attacks can be easily mitigated with proper switchport configuration

The first and most commonly used VLAN hopping method is where the attacker makes his workstation act as a trunk port

To overcome this kind of VLAN hopping attack, you must follow below steps

1. Ensure that ports are not set to negotiate trunks automatically.
Switch(config-if)# switchport nonegotiate
2. Ensure that ports that are not meant to be trunks are explicitly configured as access ports
Switch(config-if)# switchport mode access
The second way an attacker can hop VLANs is by using double tagging. With double tagging, the attacker inserts a second 802.1q tag in front of the existing 802.1q tag. This relies on the switch stripping off only the first 802.1q tag and leaving itself vulnerable to the second tag. This is not as common a method of VLAN hopping as using trunking.

Mitigation

Simply do not put any hosts on VLAN 1 (The default VLAN). i.e., assign an access VLAN other than VLAN 1 to every access port
Switch(config-if)# switchport access vlan 2
Change the native VLAN on all trunk ports to an unused VLAN ID.
Switch(config-if)# switchport trunk native vlan 999
Explicit tagging of the native VLAN on all trunk ports.
Switch(config-if)# switchport trunk native vlan tag

Example
As an example of a double tagging attack, consider a secure web server on a VLAN called VLAN1. Hosts on VLAN1 are allowed access to the web server; hosts from outside the VLAN are blocked by layer 3 filters.

An attacking host on a separate VLAN, called VLAN2, creates a specially formed packet to attack the web server. It places a header tagging the packet as belonging to VLAN2 on top of another header tagging the packet as belonging to VLAN1. When the packet is sent, the switch on VLAN2 sees the VLAN2 header and removes it, and forwards the packet.

The VLAN2 switch expects that the packet will be treated as a standard TCP packet by the switch on VLAN1. However, when the packet reaches VLAN1, the switch sees a tag indicating that the packet is part of VLAN1, and so bypasses the layer 3 handling, treating it as a layer 2 packet on the same logical VLAN. The packet thus arrives at the target server as though it was sent from another host on VLAN1, ignoring any layer 3 filtering that might be in place.

Via :Wikipedia