FYI

Attackväg 1 och 2 är de primära jag valt men lade till attackväg 3 också om du anser att det behövs. Den är ju dock mer på applikationslagret.

Attackväg 1 VLAN Hopping

Physical Layer

Angriparen ansluter via WiFi eller en fysisk port. Switchporten läcker nätverksinformation via CDP, såsom vilka VLAN som finns och vilket native VLAN som är konfigurerat.

Endast anslutning via fysisk port

Data-Link Layer

Om switchporten av misstag står i trunk-läge kan angriparen skicka taggade 802.1Q-paket och fritt välja vilket VLAN trafiken ska tillhöra, exempelvis VLAN 99

Om porten har DTP aktiverat så kan angriparen sätta sin enhet i trunkmode och då kommer switchens port att förhandlas fram till en trunkport. Angriparen får då åtkomst till alla VLAN som är allowed på trunken.

Om porten är i access mode och DTP är avstängt så kan angriparen dubbel-tagga sina paket.
Den yttre taggen matchar native VLAN, och den inre taggen anger målets VLAN. Den första switchen tar bort den yttre taggen, och nästa switch placerar paketet i fel VLAN.

Oavsett metod lyckas angriparen nu skicka 802.1Q-trafik som behandlas som giltig av switchen. Trafiken placeras i ett annat VLAN än angriparen egentligen tillhör, exempelvis admin- eller server-VLAN.

Network - Application Layer

Efter VLAN-hoppet befinner sig angriparen i ett VLAN som normalt är isolerat, exempelvis admin- eller server-VLAN. Därmed får angriparen direkt åtkomst till känsliga interna system som inte är nåbara från angriparens ursprungliga VLAN.

Datan stulen eller ändrad.

Confidentiality: Hög, angriparen får direkt åtkomst till databasen.

Integrity: Hög, data kan ändras, raderas eller manipuleras.

Availability: Medel, risk för störningar eller driftstopp om kritiska system påverkas