حملات vLan: vLan یک گروه منطقی از منابع شبکه است که توسط پورت‌های تعریف شده توسط مدیر به یک سوئیچ متصل می‌شود. حملات vLan معمولاً از دو نوع هستند:

Mac Spoofing

مهاجم ، MAC آدرس خود را برابر سرور موجود در شبکه قرار می دهد و به سمت سوئیچ ترافیک ارسال می کند. سوئیچ با دریافت این ترافیک و بررسی MAC آدرس مبدا بسته ، فکر می کند که پورت متصل به سرور تغییر کرده در نتیجه جدول MAC خود را تغییر می دهد و از این پس ترافیکی که مقصد آن سرور است را روی پورت 2 ارسال می کند و این ترافیک تحویل مهاجم می شود و به این صورت مهاجم به اطلاعات ارسالی دیگر سیستم ها دسترسی پیدا می کند.

Mac Flooding

مهاجم جدول CAM سوئیچ را با MAC آدرس های جعلی پر می کند. بعد از اینکه جدول پر شد. از این پس سوئیچ بدلیل پر شدن جدول Cam خود نمی تواند MAC جدید را یاد بگیرد درنتیجه سوئیچ بسته های دریافتی که آدرس مقصد آنها در جدول CAM ندارد را روی تمام پورت های خود ارسال می کند.

حملات Trunking دراین گونه از حملات از طریق لینک Trunk سیگنال‌ها و دستورات مختلف برای هر سوئیچ یا روتر ارسال می شوند. حملات Trunking عمدتاً از دو نوع هستند:

[Switch Spoofing](https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKPREA4/vlan1-and-vlan-hopping-attack)

این اکسپلویت فقط زمانی می‌تواند موفق شود که یک سوییچ واقعی به‌گونه‌ای پیکربندی شده باشد که اجازه برقراری اتصال trunk را بدهد. این اتفاق زمانی می‌افتد که یکی از اینترفیس‌های سوییچ روی حالت «Dynamic Desirable»، «Dynamic Auto» یا «Trunk» تنظیم شده باشد.

در حمله switch spoofing حمله‌کننده آدرس MAC یک دستگاه را تغییر می‌دهد تا به عنوان یک پورت سوئیچ مجاز عمل کند و به شبکه هدف دسترسی پیدا کند.

[Double Tagging](https://www.computernetworkingnotes.com/ccna-study-guide/vlan-basic-concepts-explained-with-examples.html)

حمله‌کننده دو برچسب VLAN به یک بسته داده اضافه می‌کند. برچسب خارجی متعلق به VLAN خود حمله‌کننده است و برچسب داخلی متعلق به VLAN قربانی. این حمله فقط در صورتی کار می‌کند که کامپیوتر حمله‌کننده به VLAN اصلی پورت trunk متصل باشد. وقتی بسته دو برچسبه به سوئیچ می‌رسد، سوئیچ فقط برچسب خارجی را می‌بیند و آن را حذف می‌کند، سپس بسته را به تمام پورت‌های متصل به VLAN اصلی ارسال می‌کند.

ARP Poisoning

نوعی از حمله است از حملات( mitm (men in the middle است که هکر با آدرس مک جعلی خود را به عنوان gateway جا زده و اطلاعات را شنود (sniff) می کند.

VLAN Hopping

به مهاجمان اجازه می‌دهد هرگونه محدودیت لایه 2 را که برای جداکردن هاست‌ها ساخته شده، دور بزنند.