**تمرین 2 :**

**حملات مربوط به لایه 2:**

1. دسترسی از یک VLAN به VLAN دیگر در لایه دو امکان پذیر نیست و تنها در لایه سه با استفاده از روتر و VLAN Routing این امکان فراهم می شود. VLAN Hopping نوعی از حملات است که توسط آن هکر می تواند در لایه دو شبکه از یک  VLAN به VLAN دیگر دسترسی پیدا کند. این حملات به دو شیوه Switch spoofing و Double Tagging قابل اجراست.
2. **Switch Spoofing**

در این حمله هکر تلاش می کند یک سوئیچ اشتباه را به شبکه اضافه کرده و یک Trunk ایجاد کند. اگر حمله موفق باشد ترافیک VLAN های مختلف از این سوییچ عبور خواهد کرد و امکان بازبینی و تغییرات اطلاعات را برای هکر ایجاد می کند. این حمله بر اساس خصوصیات دینامیک Trunk ها در سوئیچ می باشد. اگر Trunking دینامیک غیر فعال شود و اینترفیس های غیر Trunk برای Trunk شدن برنامه ریزی نشوند این حمله بی اثر می شود.

1. **Double Tagging**

مشابه حملات جعل (Spoofing) دیگر، در جعل DHCP هکر سعی در جازدن خود به جای دیگریست. در اینصورت باید بعنوان سرور DHCP قانونی خود را جا بزند. بدلیل اینکه DHCP در بیشتر شبکه ها برای تخصیص آدرس ها و دیگر اطلاعات به کاربرها استفاده می شود از دست دادن کنترل این بخش از شبکه می تواند بسیار خطرناک باشد. در حملات جعل DHCP یا DHCP Spoofing، هکر یک سرور DHCP جعلی را جاگذاری می کند. هنگامیکه کاربران درخواست تخصیص IP به سرور می دهند، سروری که سریعترین جواب را بدهد استفاده می شود. اگر کاربر از سرور جعلی که هکر جاگذاری کرده است جواب بگیرد، سرور جعلی می تواند هر آدرسی به آن تخصیص دهد و همینطور اینکه چه دستگاهی به عنوان Gateway استفاده می شود را کنترل کند. یک حمله خوب طراحی شده میتواند ترافیک کاربران را به سمت سرور جعلی هدایت کرده و به سمت Gateway دلخواه بفرستد. این حمله بسیار پنهان است بدین معنی که هکر به راحتی و بصورت پنهان میتواند به سرقت اطلاعات ادامه دهد.

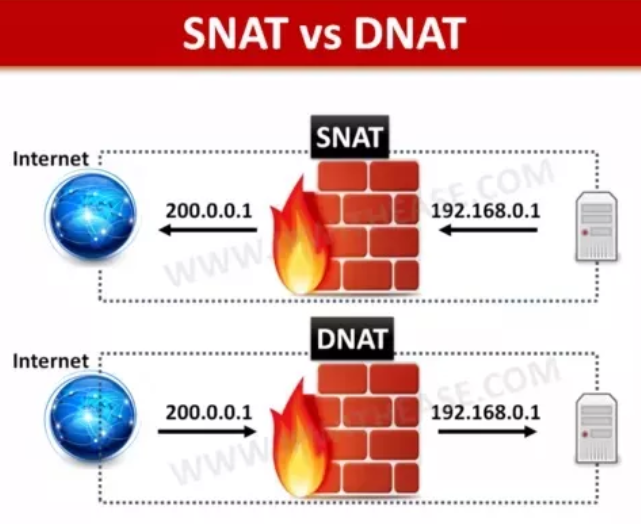
**تمرین 5:**

**NAT :** Network Address Translation : تبدیل Private IP به Public IP

با توجه به محدودیت تعداد IP ها ، ضرورت تبدیل IP های داخلی به IP که در شبکه اینترنت قابل مسیریابی باشد، با این پروتکل فراهم می شود .

Source NAT : مسیر رفت از شبکه داخلی به اینترنت

Destination NAT : مسیر بازگشت از اینترنت به شبکه داخلی



Static NAT : نگاشت یک به یک میان یک IP private و یک Public IP

Dynamic NAT : نگاشت یک به چند : یعنی تعدادی Private IP به یکIP Public تبدیل می شوند. (pool )

PAT : نگاشت یک به چند + پورت های متفاوت ) در این حالت یک IP public می تواند 65535 Private IPرا با پورت های متفاوت مدیریت کند. )