

حمله Double Tagging چیست؟

Double Tagging یا **VLAN Double Tagging** یکی از روش‌های حمله در شبکه‌های VLAN است که در آن مهاجم با قرار دادن دو برچسب (Tag) روی یک فریم اترنت، تلاش می‌کند بسته را به VLAN دیگری ارسال کند. این حمله یکی از انواع حملات **VLAN Hopping** محسوب می‌شود.

پیش‌نیاز

فرض کنید شبکه به شکل زیر است:

کامپیوتر مهاجم

|
|

Access Port

|

Switch 1

|

===== Trunk =====

|

Switch 2

|

VLAN 20 (سرور)

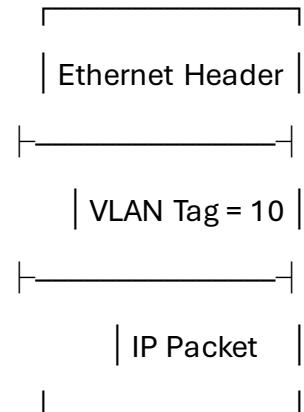
فرضیات:

- مهاجم در **VLAN 10** قرار دارد.
- **Native VLAN** نیز برابر **10** است.
- بین دو سوئیچ یک لینک **Trunk** وجود دارد.

تگ VLAN چیست؟

در استاندارد **IEEE 802.1Q**، هنگام عبور یک فریم از لینک Trunk، یک تگ به آن اضافه می‌شود.

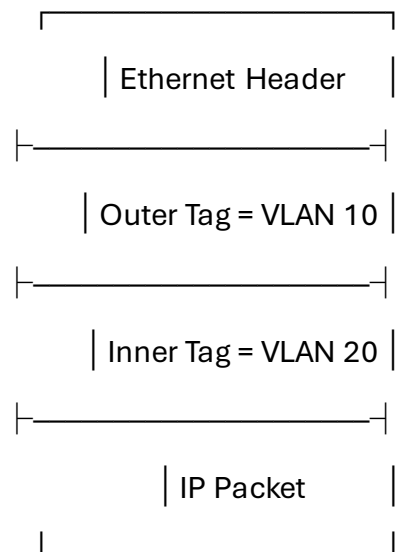
نمونه یک فریم معمولی:



در حالت عادی فقط یک Tag وجود دارد.

در حمله Double Tagging چه اتفاقی می‌افتد؟

مهاجم یک فریم با دو تگ VLAN ایجاد می‌کند.



- **Outer Tag** مربوط به Native VLAN است.

- **Inner Tag** مربوط به VLAN هدف است.

مرحله اول

مهاجم این فریم را ارسال می کند.

Outer Tag = 10

Inner Tag = 20

مرحله دوم

فریم وارد **Switch 1** می شود.

چون **Outer Tag** برابر Native VLAN است، هنگام خروج از لینک **Trunk**، سوئیچ آن را حذف می کند.

قبل از خروج:

Tag 10

Tag 20

بعد از خروج:

Tag 20

مرحله سوم

فریم وارد **Switch 2** می شود.

Switch 2 فقط یک Tag مشاهده می کند:

VLAN 20

در نتیجه تصور می کند این فریم متعلق به **VLAN 20** است و آن را داخل همان **VLAN** ارسال می کند.

مسیر حمله

مهاجم



Tag10

Tag20



Switch 1



حذف Tag10



Tag20



Switch 2



ارسال به VLAN20



سرور

چرا این حمله امکان پذیر است؟

علت اصلی، رفتار **Native VLAN** است.

در لینک‌های Trunk، فریم‌های Native VLAN معمولاً بدون Tag ارسال می‌شوند.

به همین دلیل:

۱. سوئیچ اول تصور می‌کند اولین Tag مربوط به Native VLAN است.

۲. آن را حذف می‌کند.

۳. Tag دوم باقی می‌ماند.

۴. سوئیچ دوم آن را به عنوان VLAN مقصد معتبر می‌شناسد.

آیا ارتباط دوطرفه برقرار می‌شود؟

معمولاً خیر.

این حمله اغلب یک طرفه است.

مهاجم VLAN20 —————▶

اما پاسخ معمولاً به مهاجم بازمی‌گردد.

به همین دلیل بیشتر برای حملاتی مانند موارد زیر استفاده می‌شود:

- ارسال بسته‌های مخرب
- ARP Spoofing
- DHCP Attack
- STP Attack
- Denial of Service (DoS)

شرایط لازم برای موفقیت حمله

برای موفق بودن حمله باید همه شرایط زیر برقرار باشند:

- مهاجم در Native VLAN قرار داشته باشد.

- بین سوئیچ‌ها لینک **Trunk** وجود داشته باشد.
 - **Native VLAN** بدون Tag ارسال شود.
 - سوئیچ‌ها از استاندارد **802.1Q** استفاده کنند.
- اگر یکی از این شرایط برقرار نباشد، حمله موفق نخواهد شد.

روش‌های جلوگیری

۱. از **VLAN 1** به عنوان **Native VLAN** استفاده نکنید.

بهتر است مثلاً:

Native VLAN = 999

باشد و هیچ کاربری داخل آن قرار نگیرد.

۲- **Native VLAN** را **Tag** کنید.

در سوئیچ‌های سیسکو:

```
vlan dot1q tag native
```

۳- **Native VLAN** را تغییر دهید.

```
interface GigabitEthernet0/1
```

```
switchport mode trunk
```

```
switchport trunk native vlan 999
```

۴- فقط **VLAN** های موردنیاز را روی **Trunk** مجاز کنید.

```
switchport trunk allowed vlan 10,20,30
```

۵- پورت‌های بدون استفاده را خاموش کنید.

interface range Fa0/10-24

shutdown

۶- قابلیت Port Security را فعال کنید.

switchport port-security

۷- از DHCP Snooping و Dynamic ARP Inspection استفاده کنید.

این قابلیت‌ها از سوءاستفاده مهاجم پس از ورود بسته به VLAN مقصد جلوگیری می‌کنند.

تفاوت Switch Spoofing و Double Tagging

Double Tagging

استفاده از دو Tag

نیازمند Native VLAN

معمولاً ارتباط یک طرفه

Switch Spoofing

سوءاستفاده از DTP

نیازمند DTP

ارتباط دوطرفه

مهاجم خود را Switch معرفی می‌کند مهاجم روی Access Port قرار دارد

جمع‌بندی

حمله Double Tagging یکی از حملات شناخته‌شده VLAN Hopping است که از نحوه پردازش Native VLAN در استاندارد 802.1Q سوءاستفاده می‌کند. در این حمله، مهاجم با قرار دادن دو تگ VLAN روی یک فریم، باعث می‌شود سوئیچ اول تگ بیرونی را حذف کند و سوئیچ دوم تگ داخلی را به عنوان VLAN مقصد بپذیرد.

در شبکه‌های امروزی، اگر تنظیمات امنیتی مانند تغییر Native VLAN ، Tag کردن Native VLAN ، محدود کردن VLAN های مجاز روی Trunk و غیرفعال کردن DTP به درستی اعمال شوند، احتمال موفقیت این حمله بسیار کم خواهد بود.