حمله BGP Neighbor

حمله به همسایه BGP یکی از روش های مهاجمان برای ایجاد اختلال در عملکرد شبکه است. در چنین حملاتی، مهاجم سعی می کند تا با ایجاد اختلال در ارتباطات BGP، ترافیک شبکه را به نفع خود هدایت کند.

این می تواند با استفاده از روش های مختلفی انجام شود، از جمله:

1. ایجاد اختلال در لایه 2 که مانع از دسترسی به طرف مقابل می شود.
2. مشکلات در لایه 3: آدرس IP اشتباه در یکی از روترها.
3. فیلتر کردن پورت TCP 179 (BGP) با استفاده از لیست دسترسی.
4. تنظیم آدرس IP اشتباه برای روتر همسایه BGP.

برای مقابله با این نوع حملات، می توان از روش های مختلفی استفاده کرد. به عنوان مثال، می توان از تکنیک های مانند فیلتر کردن مسیر، استفاده از روش های احراز هویت قوی، و ایجاد محدودیت های مناسب برای ترافیک BGP استفاده کرد[3](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-16/irg-xe-16-book/configuring-bgp-neighbor-session-options.html). [همچنین، می توان از ابزارهای نظارتی استفاده کرد تا تغییرات غیرمنتظره در جدول مسیریابی را شناسایی کند1](https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/).