pencegahan terhadap *DHCP Rogue* yang digunakan pada *DHCP Alert* yang dikombinasi *Firewall Filter Rule* pada *Bridge Mikrotik,* dengan didapatnya hasil sistem yang dapat dideteksi dan dicegah dengan *DHCP Rogue* di dalam jaringan *DHCP* berbasis *IPv4*(Kadafi & Khusnawi, 2015). Pada penggunaan *DHCP Rogue* dapat melakukan filtering pada trafik yang dapat mencegah adanya *DHCP Server* dari perangkat yang illegal, yang dapat mengganggu dalam lancarnya jaringan didalam satu jaringan.

2.2.14 Jenis ancaman dalam system keamanan DHCP Server

Pada jenis keamanan, terdapat beberapa *system* ancaman pada jaringan *DHCP Server* yang membuat orang lain tidak bertanggungjawab dalam hal membuat kerusakan jaringan computer perusahaan. Berikut beberapa dari ancaman yang harus diperhatikan:

1. *DHCP Snooping*

   Penyerangan pada DHCP Server kata lain bisa disebut DHCP Snooping cara kerjanya dengan menggunakan *switch* yang didaftarkan melalui port yang sah sebagai DHCP Server dan menggunakan sebagai umpan.

2. *IP/mac Spoofing*

   Jenis serangan yang digunakan pada *IP/MAC* dapat dikombinasikan kedua menggunakan status palsu lalu mengirimkan paket di target jaringan yang dapat mengakses jaringan dan hak akses yang sesuai dengan posisi alamat yang dituju pada *IP/MAC* yang terdaftar.

3. *DHCP Flooding*

   DHCP Flooding digunakan dalam meminta megirimkan dengan jumlah yang banyak pada *DHCP Server* pada peretas. Pada *DHCP Server* secara otomatis akan membagikan alamat IP yang sedang diminta dan keterbatasan tertentu yang menghabiskan alamat IP dari dalam *DHCP Server.* Hal ini dapat berakibat pengguna yang sedang meminta alamat IP pada *DHCP Server* tidak dapat alamat IP dikarenakan alamat IP di *DHCP Server* sudah kehabisan yang sudah diminta oleh peretas. Sehingga pengguna tidak dapat terhubung dalam jaringan.