**Network Security**

**Existed System**

DHCP Snooping:

**Attack→** In a DHCP starvation attack, the attacker sends a high number of DHCP DISCOVER packets with spoofed source MAC addresses. When the DHCP server begins responding, the available IP Addresses in the DHCP pool is quickly depleted, rendering the server useless. In addition, an attacker can then run a DHCP spoofing attack by setting up a rogue DHCP server to respond to new DHCP requests, which allows for seeing the traffic, relaying traffic to a gateway and even changing the destination to a malicious website.

Arp Snooping:

ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker’s MAC address with the IP address of a legitimate computer or server on the network. Once the attacker’s MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address. ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol.

Proposed System

**Mitigation→** DHCP snooping is used to validate DHCP messages received from untrusted sources and to filter out those deemed invalid. For example if response packet received is (DHCPACK, DHCPNAK, or DHCPOFFER packet) on untrusted interface. It does this by building a DHCP snooping binding database which contains info about untrusted hosts with leased IP addresses.