# Switch Security

Rohith Perumalla | 3/12/17

This past week I learned about a few ways to protect networking switches. Networking switches are used to extend networks and connect hosts to a network, but sometimes can be exploited to steal data or MAC addresses. Some ways hackers attempt to exploit networks include: packet sniffing, port flooding, DHCP starvation, or Denial of Service. Packet sniffing is used to capture any data that is in plain text and can be prevented by using SSH which encrypts plain text data being transmitted across the internet. Port Flooding overwhelms a switch with fake MAC addresses until the switch broadcasts the whole MAC address table across the networking, this can be prevented with the use of port security or DHCP snooping. Port security helps mitigate MAC address flooding attacks, and DHCP Snooping help identify potential flooding attempts and leading to them being shut down before any adverse effects occur. Sometimes hackers attempt to get information from a switch by overwhelming it with interruptions from an authorized user's access to a computer network, and some even use a virus to spread code among other computers to have a distributed denial of service coming from multiple sources to aggrandize the impact of the DoS to attack a switch. Telnet DoS's can be prevented with security patches or SSH. Some hackers even try brute forcing which basically tries every possible combination of characters until a combo works, this can be prevented with a strong password. Overall there are many ways for a hacker to get what they are looking for but there are equally as many ways to stay protected from malicious hackers.