David Thomsen

A paragraph in your own words on potential security issues related to OSPF if authentication is not used

OSPF is one of the most common protocols used in networking so it is well known to both attackers and users. This means that without authentication, they are easily breached by an outside attacker. Without authentication, a rogue user can set up a rogue router within the network and gather information from within the network. By adding an additional layer of security to the network, it lowers the chance of an outside attacker getting inside the network and messing with it.

A paragraph in your own words on how OSPF authentication works and the most common methods

There are three types of authentications that OSPF uses which are None, Password Authentication, and MD5 Authentication. MD5 being the safest, as it uses an MD5 algorithm and is not exchanged by peers. MD5 is similar to a common password, but it is encrypted so that it can not be read by an outside attacker. It is applied in cisco by using the command: ip ospf message-digest-key 1 md5 password and it will be what is added to my OSPF file.

https://logrhythm.com/blog/monitoring-ospf-neighbors-for-eavesdropping/

http://ce.sc.edu/cyberinfra/docs/onr_projects/Routing%20Hijacking/submittedWork/OSPF_Hijacking.pdf

https://community.cisco.com/t5/networking-knowledge-base/ospf-authentication/ta-p/3131640