**Assessment 1b: Bi-Weekly Report (Week 3 and 4)**

# Q1. Describe how OSPF would react to the attacker deactivating one of the network interfaces on the router

The OSPF's primary responsibility (Open Shortest Path First) is to enable routers connected with multiple networks and autonomous systems to build their routing tables every time the network topology is altered. It is achieved by sending an LSA (Link State Advertisement) messages between each other that information about the topology. However, if an attacker has compromised the router and deactivates a network interface on the router, it will have to look for a new link from the Link-state database to connect with the respective router. From the LSD, the router will construct the shortest path through the OSPF protocol and place itself as the root device within the network.

Moreover, when the router loses the network interface, the OSPF communicates the new link to the router that updates its routing table accordingly. Therefore, the attacker will modify the router by removing the shortest paths from its routing table that would further lead to a higher cost since the router will have to look for longer routes to get to the desired network; as a result, causing disruptions within the network topology. Having no existing links between routers linked to multiple systems would lead to partitioning attacks, where different LSAs are sent to its neighboring routers (Al-Musawi, B, Branch, P, Hassan, MF & Pokhrel, SR, 2020). Hence, this type of attack leads the attacker to remote overload links and driving no-data plane traces to track the attacker.

# Q2. Discuss the possible impacts on the network if the attacker were to repeatedly deactivate and reactivate one of the network interfaces on the router.

An attacker having persistent access to the router's network interface can severely impact the network topology. Deactivating and reactivating the router's network interfaces could lead the attacker to divert traffic away from original routes and, hence, perform severe attacks on the network. The attacks come in the form of denial of service and eavesdropping. Denial of service attacks is when the intruder tries to flood the network, degrading the network's ability to provide good quality of service to users.

The attacker's actions can lead to delivery failure of packets within the system, churning network routes that would cause performance degradation, network instability, and overloading links (Nakibly, G., Kirshon, A., Gonikman, D. and Boneh, n.d). Moreover, another possible initiated attack would be eavesdropping where an attacker can divert remote traffic through the network that the attacker has access to and, consequently, letting the attacker eavesdrop. Such traffic diversion motivates man-in-the-middle attacks and other impersonation attacks too.

# References

* Al-Musawi, B, Branch, P, Hassan, MF & Pokhrel, SR 2020, 'Identifying OSPF LSA falsification attacks through non-linear analysis,' Computer Networks, vol. 167, viewed 8 August 2020
* Nakibly, G., Kirshon, A., Gonikman, D. and Boneh, D. (n.d.). Persistent OSPF Attacks. [online] Available at: <https://crypto.stanford.edu/~dabo/pubs/papers/ospf.pdf>