Module 1

In this module, it covers the concepts of stepping-stone and its intrusion, as well as the basic techniques to detect stepping-stone intrusion. The way to use SSH to establish a connection chain is introduced. There are basically two types of technique to detect stepping-stone intrusion: host-based and connection chain-based. Host-based detection technique compares the incoming connections with outgoing ones of a host to decide if the host is used as a stepping-stone. Connection chain-based technique estimates the length of a connection chain from a sensor to the victim to judge if a host is used as a stepping-stone.