Module 4

Estimating the length of a connection chain to detect stepping-stone intrusion can largely reduce false-positive detection error. In this module, the following approaches are suggested to include. Yung’s approach can use the ratio between the time gap to the adjacent host and the one to the victim host to detect stepping-stone. Step-function approach can estimate the length of a connection accurately, but only applicable to a local area network, other than to the Internet. RTT data mining can be used to estimate the length of a connection chain accurately and be applicable to the Internet traffic. Crossover packets can be used to relatively tell how long a whole connection chain is from the victim side.