Abstract

Eight sites participated in the second DARPA off-line intrusion detection evaluation in 1999. Three weeks of training and two weeks of test data were generated on a test bed that emulates a small government site. More than 200 instances of 58 attack types were launched against victim UNIX and Windows NT hosts. False alarm rates were low (less than 10 per day). Best detection was provided by network-based systems for old probe and old denial-of-service (DoS) attacks and by host-based systems for Solaris user-to-root (U2R) attacks. Best overall performance would have been provided by a combined system that used both host- and network-based intrusion detection. Detection accuracy was poor for previously unseen new, stealthy, and Windows NT attacks. Ten of the 58 attack types were completely missed by all systems. Systems missed attacks because protocols and TCP services were not analyzed at all or to the depth required, because signatures for old attacks did not generalize to new attacks, and because auditing was not available on all hosts.