Proactive Botnet Detection: Through Characterization of Distributed Denial of Service Attacks

By Dr Thomas S Hyslip

Createspace, United States, 2015. Paperback. Book Condition: New. 280 x 216 mm. Language: English . Brand New Book ***** Print on Demand *****.In this quantitative quasi-experimental study two distributed denial of service attacks were captured and the characteristics of the attacks were used to detect botnets by identifying egressing distributed denial of service attack packets at the source of the attack. A sample Dark DDoSer botnet was constructed and used to launch a distributed denial of service attack. The characteristics of the distributed denial of service attacks were used as the independent variables in a quasi-experiment where network traffic was monitored with Snort to detect DDoS packets. The dependent variable for the experiment was false positive alerts for the DDoS packets. The findings showed that the characteristics of a distributed denial of service attack can be used to pro-actively detect botnets through egress monitoring.

READ ONLINE
[1.77 MB]

Reviews

Good eBook and beneficial one. It really is simplified but unexpected situations from the 50 percent from the ebook. You can expect to like the way the blogger publish this ebook.
-- Bridie Stracke DDS

Complete information! Its such a excellent study. It is filled with knowledge and wisdom I realized this publication from my dad and i advised this publication to find out.
-- Geovanny Grimes