Poster Abstract

Ben Mixon-Baca

The struggle for information assurance is an on going battle between the white hats (good hackers) and the black hats (bad hackers). The white hats must continually attempt to stay one step a head of the black hats by fully understanding the details of how the technologies they are using behaves. Similarly, the black hats are ever persistent in their study of systems, in an attempt to find the smallest behavior that may lead to information disclosure or otherwise compromise a system. In researching operating systems behavior to better understand the means by which an attacker might be able to leverage behavior, Xu Zhang discovered an anomaly specific to the Linux operating system network stack. In particular, he noted that a specific field in the TCP header was behaving in a way that could be used by an adversary to infer the state of a serves listening socket while minimizing their exposure to the server. He noted that if an attacker wished, they could send packets with varying source IP addresses but with the same port number to a given server and under certain conditions, the sequence number field initialized by the server in the TCP header would go unchanged for long streams of packets. This is significant to a black hat hacker because it can allow her infer the state of other connections being handle by the server. It is significant to the white hat hacker because it can allow her to configure her systems setting in such a way that this side channel does not disclose the kind of information that the black hat may find valuable. The topics of this poster are, what causes this behavior and can it be used with the idle scan developed by Roya Ensafi as an effective side channel. Additionally, this poster will provide a brief summary of how the results of this behaviors origins have effected current research.