Abstract

Computer worm detection has been a challenging and often elusive task. This is partly because of the difficulty of accurately modeling either the normal behavior of computer networks or the malicious actions of computer worms. This paper presents a literature review on the worm detection techniques, highlighting the worm characteristics leveraged for detection and the limitations of the various detection techniques. The paper broadly categorizes the worm detection approaches into content signature based detection, polymorphic worm detection, anomaly based detection, and behavioral signature based detection. The gap in the literature in the techniques is indicated and is the main contribution of the paper.
victims of an internet worm. In the proceedings of the internet Measurement Workshop
- Staniford, S. , Paxson, V. , & Weaver, N. 2002. How to Own the Internet in Your Spare Time. In USENIX Security Symposium, 149-167

Index Terms

Computer Science    Security

Keywords

Computer worm    computer worm detection    intrusion detection    detection techniques