IJRIT International Journal of Research in Information Technology, Volume 1, Issue 11, November, 2013, Pg. 459-468

International Journal of Research in Information Technology (IJRIT)

www.ijrit.com ISSN 2001-5569

Network (In) Security through IP Packet Filtering

Anshul Bhatia[1], Gaurav sharma[2] and Arjun anand[3]

[1]Student, Information Technology, Maharishi Dayanand University
New Delhi, Delhi, India
Anshulbhatia45@gmail.com

[2]Student, Information Technology, Maharishi Dayanand University
New Delhi, Delhi, India
sharma.gaurav21007@gmail.com

[3]Student, Information Technology, Maharishi Dayanand University
New Delhi, Delhi, India
arjunanand38@gmail.com

Abstract

Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The architecture of the internet, when modified can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. The businesses create an "intranet" to remain connected to the internet but secured from possible threats.

Used properly, packet filtering is a useful tool for the security-conscious network administrator, but its effective use requires a thorough understanding of its capabilities and weaknesses, and of the quirks of the particular protocols that filters are being applied to. This paper examines the utility of IP packet filtering as a network security measure, briefly contrasts IP packet filtering to alternative network security approaches such as application-level gateways, describes what packet filters might examine in each packet, and describes the characteristics of common application protocols as they relate to packet filtering. There are currently two fundamentally different networks, data networks and synchronous network comprised of switches. The internet is considered a data network. Since the current data network consists of computer-based routers, information can be obtained by special programs, such as "Trojan horses," planted in the routers. The synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers. That is why security is emphasized in data networks, such as the internet,and other networks that link to the internet.

Keywords: packet filtering works , packet examples , packet filtering caveats and packet filtering rules.

Full text: https://sites.google.com/a/ijrit.com/papers/home/V1I1141.pdf