Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.79 – 88

RESEARCH ARTICLE

A NEW IP TRACEBACK SCHEME TO AVOID LAUNCH ATTACKS

E.JANSI*[1]
M.Tech Student
Department of Computer Science and Engineering
PRIST University Pondicherry, India.
jansibtech15@gmail.com

BHARATHI.R*[2]
Assistant professor
Department of Computer Science and Engineering
PRIST University Pondicherry, India.
prist2009cse@gmail.com

E.PUSHPARAJ*[3]
Assistant Professor
Ranganathan Engineering College,
Coimbatore

ABSTRACT

The Internet has been widely applied in various fields; more and more network security issues emerge and catch people's attention. However, adversaries often hide themselves by spoofing their own IP addresses and then launch attacks. For this reason, researchers have proposed a lot of trace back schemes to trace the source of these attacks. Some use only one packet in their packet logging schemes to achieve IP tracking. Others combine packet marking with packet logging and therefore create hybrid IP trace back schemes demanding less storage but requiring a longer search. In this paper, we propose a new hybrid IP trace back scheme with efficient packet logging aiming to have a fixed storage requirement for each router (under 320 KB, according to CAIDA's skitter data set) in packet logging without the need to refresh the logged tracking information and to achieve zero false positive and false negative rates in attack-path reconstruction. In addition, we use a packet's marking field to censor attack traffic on its upstream routers. Lastly, we simulate and analyze our scheme, in comparison with other related research, in the following aspects: storage requirement, computation, and accuracy.

KEYWORDS: New hybrid IP trace back, CAIDA's, packet logging, packet marking

Full Text: http://www.ijcsmc.com/docs/papers/March2014/V3I3201411.pdf