Abstract

Denial of Service (DoS) or Distributed Denial of Service (DDoS) is a powerful attack which prevents the system from providing services to its legitimate users. Several approaches exist to filter network-level attacks, but application-level attacks are harder to detect at the host base firewall. Filtering in application level can be computationally expensive and difficult to scale, while DDoS attacks still creating bogus positives that block legitimate users. In this paper, the authors show application layer DoS attack for HTTP web server using some open source DoS attack tools and also suggest some realistic mechanisms that can protect a web server from application-level DoS attacks especially while attacks targeting the resources including CPU, sockets, memory of the victim server. The authors propose a new DDoS defense mechanism that protects http web servers from application-level DDoS attacks based on the reverse proxy. The attack flow detection mechanism detects attack flows based on the symptom or stress at the server, since it is getting more difficult to identify bad flows only based on the incoming traffic patterns. A popular software known as Wireshark which is a network protocol analyzer is
used to capture the packets during a DoS attack from the victim server Ethernet interface to
detect the attacking host IP address and analysis the types of attack. We evaluate the
performance of the proposed scheme via experiment.

References

2. www.arbornetworks.com
   attacks that mimic flash crowds,” in Proc. of NSDI, Boston, MA, 2005.
   2007.
11. A. Kuzmanovic, E. Knightly, “Low-rate TCP-targeted denial of service attacks (the shrew
    vs. the mice and elephants),” in Proc. of ACM SIGCOMM, pp. 75-86, 2003.
13. H. Sun, J. Lui, D. Yau, “Defending against low-rate TCP attacks: dynamic detection and
    2711-2727, 2010.
18. www.nginx.com
    Techniques," "South Asian network Operators Group (SANOG) -23 Conference, Thimpu,
    Bhutan, 2014.
Index Terms

Computer Science

Information Sciences

Keywords

HTTP, TCP, Slowloris, OWASP, OSI layer attack; Nginx, fail2ban, IPtables.