A Practical Approach and Mitigation Techniques on Application Layer DDoS Attack in Web Server

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
18. www.nginx.com
Index Terms

Computer Science          Information Sciences

Keywords

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