Quick Demo Guide for BaDOS (L7 DOS)

created by sVen Mueller (s.mueller@f5.com)

This is a quick guide to run a BaDOS demo in UDF. To get more details and explanations check the BaDOS_Demo document and BaDOS-FAQ.

1) Start: “ASM Lab ISC FY18 + BaDOS” Blueprint in UDF
2) Login to the Kali Linux box
3) Run the Baslinetraffic script in a screen terminal
    a. # screen
    b. # ./basline_menu.sh
    c. choose 1
    d. de-attach by clicking Ctrl-a-d
    e. # screen
    f. # ./basline_menu.sh
    g. choose 2
4) Logon via RDP to the Windows box (admin:admin)
5) Start Chrome and open: http://localhost:3000 (admin:admin)
6) Choose Health and Mitigation Dashboard
7) Logon to Kali with another SSH session
8) Run the attack script
    a. # ./AB_DOS.sh
    b. choose 1
9) Check the Grafana Dashboard
10) Check the created Signature in the BIG-IP GUI (Security/DOS Protection/Siganture
11) When bad actors are detected
    a. Logon to BIG-IP via SSH
    b. Check logfiles
        i. *# tail -f /var/log/dosl7/dosl7d.log*
        ii. *# ./show_shun_list*