University of Utah
School of Computing
CS 6967: Security Operations

Lab 5 Response Outline

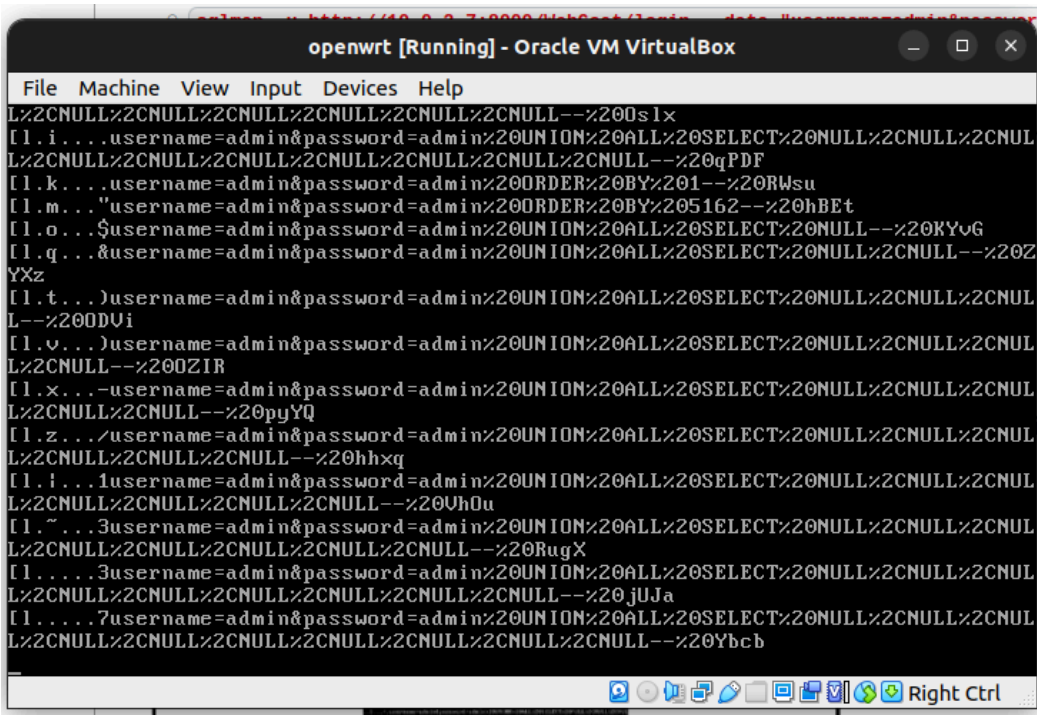
Lab 5: Intrusion Detection: Snort

Test 1: Check Traffic Sent From SQLMap to WebGoat

Summary of test experience:

This test requires screening the traffic made from Kali's SQLMap to WebGoat. Here I used, in the OpenWrt router, tcpdump, which can analyze network data packets to check whether any tcp packets are in the traffic. Then, I ran an SQLMap attack on the WebGoat's login page to find any SQL vulnerabilities. The task finally was to monitor this SQLMap attack from the OpenWrt router's terminal.

Screenshot of test results:



Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

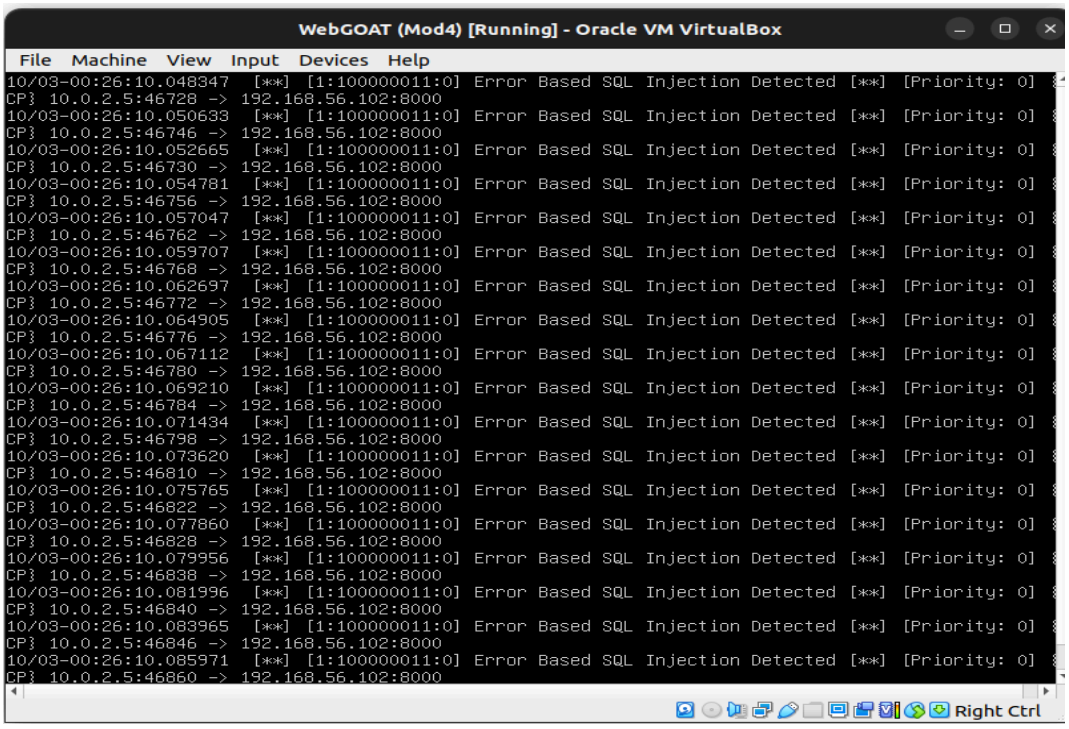
From the above image, it's seen that tcpdump at the OpenWrt router's terminal could capture packets going from Kali's SQLMap to the WebGoat server, thus completing the test successfully.

Test 2: Detect SQL Injection Attacks With Snort

Summary of test experience:

In Test 2, any SQL injection attacks on the WebGoat Server must be detected. For this, I used, in the WebGoat, Snort as a network intrusion detector. I faced some network issues while installing Snort in the WebGoat server. But luckily, it's resolved after a whole restart. Then I added two snort rules to detect anomaly-based tcp intrusion. Finally, I ran the SQLMap attack on the WebGoat's login page from the Kali Linux to test it out.

Screenshot of test results:



Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

The above screenshot shows that Snort could capture the SQL attack and raise alerts with the message "**Error Based SQL injection Detected**" which I set in the rules.