Cybersecurity Lab Portfolio - Alen Guner

Lab: SQL Injection Detection via Web Logs (Apache + Zeek)

Objective:

Simulate a SQL injection attack on a vulnerable web application and detect it using Apache or Zeek logs. Build awareness of web-based attack patterns and log analysis techniques.

Tools Used:

- DVWA (Damn Vulnerable Web App) or bWAPP
- Apache Web Server
- Zeek (formerly Bro)
- SQLMap
- Optional: ELK Stack or Wazuh for log aggregation

Steps Taken:

1. Environment Setup:
- Deployed DVWA or bWAPP on a local server with Apache.
- Ensured logging was enabled for access and error logs.

2. Attack Simulation:
- Launched SQLMap against login and search forms in DVWA:
  sqlmap -u "http://target-ip/dvwa/vulnerable_page.php?id=1" --batch --level=5

3. Log Collection:
- Captured HTTP requests in Apache access logs and/or Zeek logs.
- Filtered for unusual patterns like `' OR 1=1--`, `UNION SELECT`, and HTTP 500 errors.

4. Analysis:
- Used grep and custom scripts to highlight suspicious query parameters.
- Mapped attacker IP, timestamp, request URL, and payload.

5. Alert Building:
- Created basic detection rules for SQLi signatures in log files.
- Optionally forwarded logs to Wazuh/ELK for visualization and correlation.

Outcome / What I Learned:

- Successfully detected SQL injection payloads in Apache/Zeek logs.
- Learned how to simulate, detect, and document common web attack vectors.
- Gained experience in building detection logic from raw logs.
- Understood attacker behavior through structured query patterns.

Keywords:

Cybersecurity Lab Portfolio - Alen Guner

SQL Injection, Web Security, Log Analysis, Apache, Zeek, DVWA, SQLMap, Detection Rules, SIEM, Wazuh