LIST OF FIGURES

Figure 2. 1 ELK Architecture 14
Figure 3. 1 NDLC Methods 16
Figure 3. 2 System Model 19
Figure 3. 3 Intrusion Prevention System Flowchart 21
Figure 3. 4 Adding The OISF PPA 22
Figure 3. 5 Install Suricata 22
Figure 3. 6 Suricata Enable Service 22
Figure 3. 7 Suricata Stop Service 23
Figure 3. 8 Community-id Setting 23
Figure 3. 9 Nfqueue Configuration 24
Figure 3. 10 IPS Mode Using Nfqueue 24
Figure 3. 11 NFQUEUE Rules 24
Figure 3. 12 UFW Status 25
Figure 3. 13 SQL Injection Rules 26
Figure 3. 14 Cross-Site Scripting (XSS) Rules 27
Figure 3. 15 Command Injection Rules 27
Figure 3. 16 Diagram Flow ELK Stack 31
Figure 3. 17 Docker Satatus 31
Figure 4. 1 SQL Injection Curl 35
Figure 4. 2 SQL Injection Detection Logs in Suricata 35
Figure 4. 3 XSS Curl 35
Figure 4. 4 XSS Detection Logs in Suricata 36
Figure 4. 5 Command Injection Curl 36
Figure 4. 6 Command Injection Detection Logs in Suricata 36
Figure 4. 7 JSON log from Suricata (SQL Injection) 37
Figure 4. 8 Elasticsearch Log (SQL Injection) 37
Figure 4. 9 JSON log from Suricata (XSS) 38
Figure 4. 10 Elasticsearch Log (XSS) 38
Figure 4. 11 JSON log from Suricata (Command Injection) 38
Figure 4. 12 Elasticsearch Log (Command Injection) 39
Figure 4. 13 Discover in Elasticsearch 40
Figure 4. 14 Visualize in Elasticsearch 40

Figure 4. 15 DVWA Security Level 42
Figure 4. 16 DVWA Vulnerability...42
Figure 4. 17 Discover view in Kibana (SQL Injection) 48
Figure 4. 18 Discover view in Kibana (XSS) 53
Figure 4. 19 Discover view in Kibana (Command Injection)....................................58
Figure 4. 20 Discover View in Kibana Indicating All Attack 59
Figure 4. 23 Normal Network Traffic 78
Figure 4. 24 During Attack Traffic...79