

# Final Capstone Project Report

KUNJ MODI - 100951290

# Topic 1 - Detection of DoS Attacks using Suricata

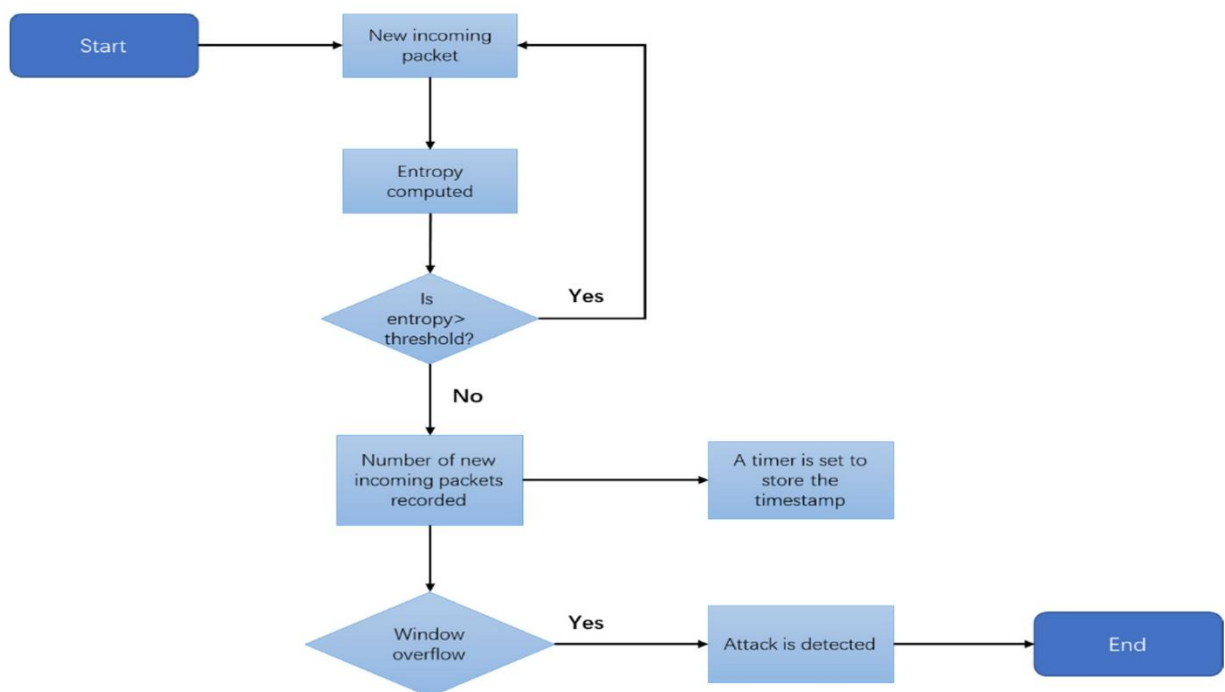
## 1. Introduction to the Project

This project's goal is to set up and use Suricata, an open-source, free intrusion detection system (IDS), to identify and stop denial-of-service (DoS) assaults on networks. To detect unusual network traffic patterns linked to DoS attacks such as SYN floods, UDP floods, and Ping of Death (PoD) attacks, Suricata will be configured with particular rules.

## 2. Prerequisite of the Project

- A basic understanding of DoS attack techniques and network protocols: Recognizing UDP, ICMP, TCP/IP, and the characteristics of DoS assaults.
- Knowledge of IDS/IPS principles: a fundamental knowledge of the function of intrusion detection and prevention systems in network security.
- Installing Suricata software on a server computer: Suricata needs to be set up and operational on a specified server.
- Resources for DoS attack simulation: Tools for creating DoS attack traffic include LOIC, hping3, and other like programs.
- An environment for testing networks: a secure setting for watching and simulating network attacks.

## 3. Network Diagram



## 4. Methodology

## 5. Challenges Faced in the Program

### 1. Ensuring Accurate Detection of DoS Attacks

- a. Rule Sensitivity: We needed to create rules that were sensitive enough to detect real DoS attacks quickly. However, overly sensitive rules could trigger alerts for benign activities, leading to false positives. For example, legitimate high traffic from multiple users could be mistaken for a DoS attack.
- b. Reducing False Positives: To mitigate this, we refined our rules iteratively. This involved adjusting thresholds, adding more context to rules, and testing them against various traffic patterns. We used a combination of existing community rules and custom rules tailored to our network's specific characteristics.
- c. Testing and Validation: Continuous testing was essential. We simulated various types of DoS attacks, including SYN floods, UDP floods, and Ping of Death, and monitored Suricata's performance.

```
3/8/2024 -- 16:29:40 - <Info> -- Loading distribution rule file /usr/share/suricata/rules/tls-events.rules
3/8/2024 -- 16:29:46 - <Info> -- Ignoring file e972a1a2078ddbc4fb8ff12f8ce8253c/rules/emerging-deleted.rules
3/8/2024 -- 16:29:50 - <Info> -- Loaded 51558 rules.
3/8/2024 -- 16:29:51 - <Info> -- Disabled 14 rules.
3/8/2024 -- 16:29:51 - <Info> -- Enabled 0 rules.
3/8/2024 -- 16:29:51 - <Info> -- Modified 0 rules.
3/8/2024 -- 16:29:51 - <Info> -- Dropped 0 rules.
3/8/2024 -- 16:29:51 - <Info> -- Enabled 136 rules for flowbit dependencies.
3/8/2024 -- 16:29:51 - <Info> -- Creating directory /var/lib/suricata/rules.
3/8/2024 -- 16:29:51 - <Info> -- Backing up current rules.
3/8/2024 -- 16:29:51 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 51558; enabled: 39215; added: 51558; removed 0; modified: 0
3/8/2024 -- 16:29:51 - <Info> -- Writing /var/lib/suricata/rules/classification.config
3/8/2024 -- 16:29:51 - <Info> -- Testing with suricata -T.
3/8/2024 -- 16:30:21 - <Info> -- Done.
kunj@kunj:~$ sudo systemctl start suricata
kunj@kunj:~$ sudo systemctl enable suricata
suricata.service is not a native service, redirecting to systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable suricata
kunj@kunj:~$
```

## 2. Configuring Suricata to Handle High Traffic Volumes

- a. Resource Allocation: We ensured that the server running Suricata had adequate CPU, memory, and disk I/O capabilities. This involved selecting appropriate hardware and optimizing the operating system settings to prioritize Suricata processes.
- b. Performance Tuning: Suricata's configuration settings, such as max-pending-packets and threading, were fine-tuned to improve performance. For example, enabling multiple threads and balancing them across CPU cores helped in processing packets faster.
- c. Load Balancing: In cases of extreme traffic, load balancing techniques were implemented. We distributed the network traffic across multiple Suricata instances using network load balancers, ensuring no single instance was overwhelmed.
- d. Packet Capture Optimization: Adjustments were made to the packet capture settings to ensure efficient data handling. This included using optimized network drivers and packet capture libraries like PF\_RING or AF\_PACKET.

```
root@kunj-VMware-Virtual-Platform:~# hping3 -S --flood -V 192.168.198.137
using ens33, addr: 192.168.198.129, MTU: 1500
HPING 192.168.198.137 (ens33 192.168.198.137): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

```
ap":0},"ftp":{"memuse":0,"memcap":0},"file_store":{"open_files":0}}
{"timestamp":"2024-08-03T17:35:45.787756-0400","flow_id":1112343510414342,"in_iface":"ens33","event_type":"flow","src_ip":
":192.168.198.129","src_port":36463,"dest_ip":"192.168.198.2","dest_port":53,"proto":"UDP","app_proto":"dns","flow":{"p
kts_toserver":1,"pkts_toclient":1,"bytes_toserver":100,"bytes_toclient":436,"start":"2024-08-03T17:30:35.652203-0400","e
nd":"2024-08-03T17:30:35.673586-0400","age":0,"state":"established","reason":"timeout","alerted":false}}
{"timestamp":"2024-08-03T17:35:51.772110-0400","flow_id":1883165139930388,"in_iface":"ens33","event_type":"flow","src_ip":
":192.168.198.137","src_port":58474,"dest_ip":"192.229.211.108","dest_port":80,"proto":"TCP","app_proto":"http","flow":
```

## 3. Balancing Between Detection Sensitivity and Network Performance

- a. Impact on Network Latency: Running an IDS like Suricata can introduce latency, especially when processing high volumes of traffic. It was crucial to minimize this impact to ensure that network performance remained within acceptable limits for users.

- b. Rule Optimization: We streamlined rule sets to include only those critical for detecting DoS attacks. Unnecessary or redundant rules were disabled to reduce processing overhead. For example, rules that were unlikely to detect DoS attacks were turned off.
- c. Traffic Filtering: Filtering out non-critical traffic before it reached Suricata helped reduce the load. This was achieved through firewall rules or upstream filtering devices that pre-processed traffic and only forwarded relevant packets to Suricata.

```
valid_lft 1638sec preferred_lft 1638sec
kunj@kunj:~$ sudo tail -f /var/log/suricata/eve.json
{"timestamp": "2024-08-03T17:33:05.578868-0400", "flow_id": "515897885203605", "in_iface": "ens33", "event_type": "dns", "src_ip": "192.168.198.137", "src_port": 37641, "dest_ip": "192.168.198.2", "dest_port": 53, "proto": "UDP", "pkt_src": "wire/pcap", "dns": {"type": "query", "id": 36721, "rrname": "dit.whatsapp.net", "rrtype": "A", "tx_id": 0, "opcode": 0}}
{"timestamp": "2024-08-03T17:33:05.580051-0400", "flow_id": "433280371522534", "in_iface": "ens33", "event_type": "dns", "src_ip": "192.168.198.137", "src_port": 51644, "dest_ip": "192.168.198.2", "dest_port": 53, "proto": "UDP", "pkt_src": "wire/pcap", "dns": {"version": 2, "type": "answer", "id": 51294, "flags": "8180", "qr": true, "rd": true, "ra": true, "opcode": 0, "rrname": "graph.whatsapp.net", "rrtype": "A", "rcode": "NOERROR", "answers": [{"rrname": "graph.whatsapp.net", "rrtype": "CNAME", "ttl": 5, "rdata": "static.whatsapp.net"}, {"rrname": "static.whatsapp.net", "rrtype": "CNAME", "ttl": 5, "rdata": "mmx-ds.cdn.whatsapp.net"}, {"rrname": "mmx-ds.cdn.whatsapp.net", "rrtype": "A", "ttl": 5, "rdata": "31.13.80.53"}], "grouped": {"A": ["31.13.80.53"], "CNAME": ["static.whatsapp.net", "mmx-ds.cdn.whatsapp.net"]}}}
{"timestamp": "2024-08-03T17:33:05.601512-0400", "flow_id": "515897885203605", "in_iface": "ens33", "event_type": "dns", "src_ip": "192.168.198.137", "src_port": 37641, "dest_ip": "192.168.198.2", "dest_port": 53, "proto": "UDP", "pkt_src": "wire/pcap", "dns": {"version": 2, "type": "answer", "id": 36721, "flags": "8180", "qr": true, "rd": true, "ra": true, "opcode": 0, "rrname": "dit.whatsapp.net", "rrtype": "A", "rcode": "NOERROR", "answers": [{"rrname": "dit.whatsapp.net", "rrtype": "CNAME", "ttl": 5, "rdata": "scontent.whatsapp.net"}, {"rrname": "scontent.whatsapp.net", "rrtype": "CNAME", "ttl": 5, "rdata": "mmx-ds.cdn.whatsapp.net"}, {"rrname": "mmx-ds.cdn.whatsapp.net", "rrtype": "A", "ttl": 5, "rdata": "31.13.80.53"}], "grouped": {"CNAME": ["scontent.whatsapp.net", "mmx-ds.cdn.whatsapp.net"], "A": ["31.13.80.53"]}}}
{"timestamp": "2024-08-03T17:33:05.629952-0400", "flow_id": "523895681294975", "in_iface": "ens33", "event_type": "tls", "src_ip": "192.168.198.137", "src_port": 37362, "dest_ip": "31.13.80.53", "dest_port": 443, "proto": "TCP", "pkt_src": "wire/pcap", "tls": {"sni": "graph.whatsapp.net", "version": "TLS 1.3", "ja3": {"hash": "b5001237acdf006056b409cc433726b0", "string": "771,4865-4867-4866-49195-49199-52393-52392-49196-49200-49162-49161-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-34-51-43-13-45-28-65282-30-31-32-33-34-35-36-37-38-39-40-41-42-43-44-45-46-47-48-49-50-51-52-53-54-55-56-57-58-59-60-61-62-63-64-65-66-67-68-69-70-71-72-73-74-75-76-77-78-79-80-81-82-83-84-85-86-87-88-89-90-91-92-93-94-95-96-97-98-99-100-101-102-103-104-105-106-107-108-109-110-111-112-113-114-115-116-117-118-119-120-121-122-123-124-125-126-127-128-129-130-131-132-133-134-135-136-137-138-139-140-141-142-143-144-145-146-147-148-149-150-151-152-153-154-155-156-157-158-159-160-161-162-163-164-165-166-167-168-169-170-171-172-173-174-175-176-177-178-179-180-181-182-183-184-185-186-187-188-189-190-191-192-193-194-195-196-197-198-199-200-201-202-203-204-205-206-207-208-209-210-211-212-213-214-215-216-217-218-219-220-221-222-223-224-225-226-227-228-229-230-231-232-233-234-235-236-237-238-239-240-241-242-243-244-245-246-247-248-249-250-251-252-253-254-255-256-257-258-259-260-261-262-263-264-265-266-267-268-269-270-271-272-273-274-275-276-277-278-279-280-281-282-283-284-285-286-287-288-289-290-291-292-293-294-295-296-297-298-299-300-301-302-303-304-305-306-307-308-309-310-311-312-313-314-315-316-317-318-319-320-321-322-323-324-325-326-327-328-329-330-331-332-333-334-335-336-337-338-339-340-341-342-343-344-345-346-347-348-349-350-351-352-353-354-355-356-357-358-359-360-361-362-363-364-365-366-367-368-369-370-371-372-373-374-375-376-377-378-379-380-381-382-383-384-385-386-387-388-389-390-391-392-393-394-395-396-397-398-399-400-401-402-403-404-405-406-407-408-409-410-411-412-413-414-415-416-417-418-419-420-421-422-423-424-425-426-427-428-429-430-431-432-433-434-435-436-437-438-439-440-441-442-443-444-445-446-447-448-449-450-451-452-453-454-455-456-457-458-459-460-461-462-463-464-465-466-467-468-469-470-471-472-473-474-475-476-477-478-479-480-481-482-483-484-485-486-487-488-489-490-491-492-493-494-495-496-497-498-499-500-501-502-503-504-505-506-507-508-509-510-511-512-513-514-515-516-517-518-519-520-521-522-523-524-525-526-527-528-529-530-531-532-533-534-535-536-537-538-539-540-541-542-543-544-545-546-547-548-549-550-551-552-553-554-555-556-557-558-559-560-561-562-563-564-565-566-567-568-569-570-571-572-573-574-575-576-577-578-579-580-581-582-583-584-585-586-587-588-589-590-591-592-593-594-595-596-597-598-599-600-601-602-603-604-605-606-607-608-609-610-611-612-613-614-615-616-617-618-619-620-621-622-623-624-625-626-627-628-629-630-631-632-633-634-635-636-637-638-639-640-641-642-643-644-645-646-647-648-649-650-651-652-653-654-655-656-657-658-659-660-661-662-663-664-665-666-667-668-669-670-671-672-673-674-675-676-677-678-679-680-681-682-683-684-685-686-687-688-689-690-691-692-693-694-695-696-697-698-699-700-701-702-703-704-705-706-707-708-709-710-711-712-713-714-715-716-717-718-719-720-721-722-723-724-725-726-727-728-729-730-731-732-733-734-735-736-737-738-739-740-741-742-743-744-745-746-747-748-749-750-751-752-753-754-755-756-757-758-759-760-761-762-763-764-765-766-767-768-769-770-771-772-773-774-775-776-777-778-779-780-781-782-783-784-785-786-787-788-789-790-791-792-793-794-795-796-797-798-799-800-801-802-803-804-805-806-807-808-809-810-811-812-813-814-815-816-817-818-819-820-821-822-823-824-825-826-827-828-829-830-831-832-833-834-835-836-837-838-839-840-841-842-843-844-845-846-847-848-849-850-851-852-853-854-855-856-857-858-859-860-861-862-863-864-865-866-867-868-869-870-871-872-873-874-875-876-877-878-879-880-881-882-883-884-885-886-887-888-889-890-891-892-893-894-895-896-897-898-899-900-901-902-903-904-905-906-907-908-909-910-911-912-913-914-915-916-917-918-919-920-921-922-923-924-925-926-927-928-929-930-931-932-933-934-935-936-937-938-939-940-941-942-943-944-945-946-947-948-949-950-951-952-953-954-955-956-957-958-959-960-961-962-963-964-965-966-967-968-969-970-971-972-973-974-975-976-977-978-979-980-981-982-983-984-985-986-987-988-989-990-991-992-993-994-995-996-997-998-999-1000-1001-1002-1003-1004-1005-1006-1007-1008-1009-1010-1011-1012-1013-1014-1015-1016-1017-1018-1019-1020-1021-1022-1023-1024-1025-1026-1027-1028-1029-1030-1031-1032-1033-1034-1035-1036-1037-1038-1039-1040-1041-1042-1043-1044-1045-1046-1047-1048-1049-1050-1051-1052-1053-1054-1055-1056-1057-1058-1059-1060-1061-1062-1063-1064-1065-1066-1067-1068-1069-1070-1071-1072-1073-1074-1075-1076-1077-1078-1079-1080-1081-1082-1083-1084-1085-1086-1087-1088-1089-1090-1091-1092-1093-1094-1095-1096-1097-1098-1099-1100-1101-1102-1103-1104-1105-1106-1107-1108-1109-1110-1111-1112-1113-1114-1115-1116-1117-1118-1119-1120-1121-1122-1123-1124-1125-1126-1127-1128-1129-1130-1131-1132-1133-1134-1135-1136-1137-1138-1139-1140-1141-1142-1143-1144-1145-1146-1147-1148-1149-1150-1151-1152-1153-1154-1155-1156-1157-1158-1159-1160-1161-1162-1163-1164-1165-1166-1167-1168-1169-1170-1171-1172-1173-1174-1175-1176-1177-1178-1179-1180-1181-1182-1183-1184-1185-1186-1187-1188-1189-1190-1191-1192-1193-1194-1195-1196-1197-1198-1199-1200-1201-1202-1203-1204-1205-1206-1207-1208-1209-1210-1211-1212-1213-1214-1215-1216-1217-1218-1219-1220-1221-1222-1223-1224-1225-1226-1227-1228-1229-1230-1231-1232-1233-1234-1235-1236-1237-1238-1239-1240-1241-1242-1243-1244-1245-1246-1247-1248-1249-1250-1251-1252-1253-1254-1255-1256-1257-1258-1259-1260-1261-1262-1263-1264-1265-1266-1267-1268-1269-1270-1271-1272-1273-1274-1275-1276-1277-1278-1279-1280-1281-1282-1283-1284-1285-1286-1287-1288-1289-1290-1291-1292-1293-1294-1295-1296-1297-1298-1299-1300-1301-1302-1303-1304-1305-1306-1307-1308-1309-1310-1311-1312-1313-1314-1315-1316-1317-1318-1319-1320-1321-1322-1323-1324-1325-1326-1327-1328-1329-1330-1331-1332-1333-1334-1335-1336-1337-1338-1339-1340-1341-1342-1343-1344-1345-1346-1347-1348-1349-1350-1351-1352-1353-1354-1355-1356-1357-1358-1359-1360-1361-1362-1363-1364-1365-1366-1367-1368-1369-1370-1371-1372-1373-1374-1375-1376-1377-1378-1379-1380-1381-1382-1383-1384-1385-1386-1387-1388-1389-1390-1391-1392-1393-1394-1395-1396-1397-1398-1399-1400-1401-1402-1403-1404-1405-1406-1407-1408-1409-1410-1411-1412-1413-1414-1415-1416-1417-1418-1419-1420-1421-1422-1423-1424-1425-1426-1427-1428-1429-1430-1431-1432-1433-1434-1435-1436-1437-1438-1439-1440-1441-1442-1443-1444-1445-1446-1447-1448-1449-1450-1451-1452-1453-1454-1455-1456-1457-1458-1459-1460-1461-1462-1463-1464-1465-1466-1467-1468-1469-1470-1471-1472-1473-1474-1475-1476-1477-1478-1479-1480-1481-1482-1483-1484-1485-1486-1487-1488-1489-1490-1491-1492-1493-1494-1495-1496-1497-1498-1499-1500-1501-1502-1503-1504-1505-1506-1507-1508-1509-1510-1511-1512-1513-1514-1515-1516-1517-1518-1519-1520-1521-1522-1523-1524-1525-1526-1527-1528-1529-1530-1531-1532-1533-1534-1535-1536-1537-1538-1539-1540-1541-1542-1543-1544-1545-1546-1547-1548-1549-1550-1551-1552-1553-1554-1555-1556-1557-1558-1559-1560-1561-1562-1563-1564-1565-1566-1567-1568-1569-1570-1571-1572-1573-1574-1575-1576-1577-1578-1579-1580-1581-1582-1583-1584-1585-1586-1587-1588-1589-1590-1591-1592-1593-1594-1595-1596-1597-1598-1599-1600-1601-1602-1603-1604-1605-1606-1607-1608-1609-1610-1611-1612-1613-1614-1615-1616-1617-1618-1619-1620-1621-1622-1623-1624-1625-1626-1627-1628-1629-1630-1631-1632-1633-1634-1635-1636-1637-1638-1639-1640-1641-1642-1643-1644-1645-1646-1647-1648-1649-1650-1651-1652-1653-1654-1655-1656-1657-1658-1659-1660-1661-1662-1663-1664-1665-1666-1667-1668-1669-1670-1671-1672-1673-1674-1675-1676-1677-1678-1679-1680-1681-1682-1683-1684-1685-1686-1687-1688-1689-1690-1691-1692-1693-1694-1695-1696-1697-1698-1699-1700-1701-1702-1703-1704-1705-1706-1707-1708-1709-1710-1711-1712-1713-1714-1715-1716-1717-1718-1719-1720-1721-1722-1723-1724-1725-1726-1727-1728-1729-1730-1731-1732-1733-1734-1735-1736-1737-1738-1739-1740-1741-1742-1743-1744-1745-1746-1747-1748-1749-1750-1751-1752-1753-1754-1755-1756-1757-1758-1759-1760-1761-1762-1763-1764-1765-1766-1767-1768-1769-1770-1771-1772-1773-1774-1775-1776-1777-1778-1779-1780-1781-1782-1783-1784-1785-1786-1787-1788-1789-1790-1791-1792-1793-1794-1795-1796-1797-1798-1799-1800-1801-1802-1803-1804-1805-1806-1807-1808-1809-1810-1811-1812-1813-1814-1815-1816-1817-1818-1819-1820-1821-1822-1823-1824-1825-1826-1827-1828-1829-1830-1831-1832-1833-1834-1835-1836-1837-1838-1839-1840-1841-1842-1843-1844-1845-1846-1847-1848-1849-1850-1851-1852-1853-1854-1855-1856-1857-1858-1859-1860-1861-1862-1863-1864-1865-1866-1867-1868-1869-1870-1871-1872-1873-1874-1875-1876-1877-1878-1879-1880-1881-1882-1883-1884-1885-1886-1887-1888-1889-1890-1891-1892-1893-1894-1895-1896-1897-1898-1899-1900-1901-1902-1903-1904-1905-1906-1907-1908-1909-1910-1911-1912-1913-1914-1915-1916-1917-1918-1919-1920-1921-1922-1923-1924-1925-1926-1927-1928-1929-1930-1931-1932-1933-1934-1935-1936-1937-1938-1939-1940-1941-1942-1943-1944-1945-1946-1947-1948-1949-1950-1951-1952-1953-1954-1955-1956-1957-1958-1959-1960-1961-1962-1963-1964-1965-1966-1967-1968-1969-1970-1971-1972-1973-1974-1975-1976-1977-1978-1979-1980-1981-1982-1983-1984-1985-1986-1987-1988-1989-1990-1991-1992-1993-1994-1995-1996-1997-1998-1999-2000-2001-2002-2003-2004-2005-2006-2007-2008-2009-2010-2011-2012-2013-2014-2015-2016-2017-2018-2019-2020-2021-2022-2023-2024-2025-2026-2027-2028-2029-2030-2031-2032-2033-2034-2035-2036-2037-2038-2039-2040-2041-2042-2043-2044-2045-2046-2047-2048-2049-2050-2051-2052-2053-2054-2055-2056-2057-2058-2059-2060-2061-2062-2063-2064-2065-2066-2067-2068-2069-2070-2071-2072-2073-2074-2075-2076-2077-2078-2079-2080-2081-2082-2083-2084-2085-2086-2087-2088-2089-2090-2091-2092-2093-2094-2095-2096-2097-2098-2099-2100-2101-2102-2103-2104-2105-2106-2107-2108-2109-2110-2111-2112-2113-2114-2115-2116-2117-2118-2119-2120-2121-2122-2123-2124-2125-2126-2127-2128-2129-2130-2131-2132-2133-2134-2135-2136-2137-2138-2139-2140-2141-2142-2143-2144-2145-2146-2147-2148-2149-2150-2151-2152-2153-2154-2155-2156-2157-2158-2159-2160-2161-2162-2163-2164-2165-2166-2167-2168-2169-2170-2171-2172-2173-2174-2175-2176-2177-2178-2179-2180-2181-2182-2183-2184-2185-2186-2187-2188-2189-2190-2191-2192-2193-2194-2195-2196-2197-2198-2199-2200-2201-2202-2203-2204-2205-2206-2207-2208-2209-2210-2211-2212-2213-2214-2215-2216-2217-2218-2219-2220-2221-2222-2223-2224-2225-2226-2227-2228-2229-2230-2231-2232-2233-2234-2235-2236-2237-2238-2239-2240-2241-2242-2243-2244-2245-2246-2247-2248-2249-2250-2251-2252-2253-2254-2255-2256-2257-2258-2259-2260-2261-2262-2263-2264-2265-2266-2267-2268-2269-2270-2271-2272-2273-2274-2275-2276-2277-2278-2279-2280-2281-2282-2283-2284-2285-2286-2287-2288-2289-2290-2291-2292-2293-2294-2295-2296-2297-2298-2299-2300-2301-2302-2303-2304-2305-2306-2307-2308-2309-2310-2311-2312-2313-2314-2315-2316-2317-2318-2319-2320-2321-2322-2323-2324-2325-2326-2327-2328-2329-2330-2331-2332-2333-2334-2335-2336-2337-2338-2339-2340-2341-2342-2343-2344-2345-2346-2347-2348-2349-2350-2351-2352-2353-2354-2355-2356-2357-2358-2359-2360-2361-2362-2363-2364-2365-2366-2367-2368-2369-2370-2371-2372-2373-2374-2375-2376-2377-2378-2379-2380-2381-2382-2383-2384-2385-2386-2387-2388-2389-2390-2391-2392-2393-2394-2395-2396-2397-2398-2399-2400-2401-2402-2403-2404-24
```

## 6. Conclusion: Lessons Learned in the Project

**Lesson 1:** Practical Experience with Suricata Configuration and Rule Creation: Gained hands-on experience in setting up and configuring Suricata for real-world use.

**Lesson 2:** In-depth Understanding of Different DoS Attack Patterns and Network Signatures: Developed a thorough understanding of various DoS attack methods and their network signatures.

**Lesson 3:** Enhanced Skills in Analyzing Security Logs and Mitigating Network Attacks: Improved ability to analyze security logs, identify attack patterns, and respond to network threats effectively.

## 7. Project Management - Listing the Work Done by Each Member of the Team

**Kunj Modi & Dhairya Soni:** Configured and installed Suricata on the server and set up the network testing environment.

**Jay Parekh:** Developed and refined detection rules for identifying DoS attack patterns such as SYN floods, UDP floods, and Ping of Death.

**Deep Patel:** Performed continuous testing and validation by simulating various DoS attacks and monitored Suricata's performance.

**Mohitkumar Patel:** Optimized Suricata's performance, including resource allocation, performance tuning, load balancing, and packet capture optimization.

## REFERENCES:

1. Suricata User Guide — Suricata 8.0.0-dev documentation. (n.d.).

<https://docs.suricata.io/en/latest/>

2. Odiye, I. O. (2024, June 10). Responding to network attacks with Suricata and Wazuh XDR.

Wazuh. <https://wazuh.com/blog/responding-to-network-attacks-with-suricata-and-wazuh-xdr/>

## Topic 2: SQL Injection Detection Using Zeek

### 1. Introduction to the Project

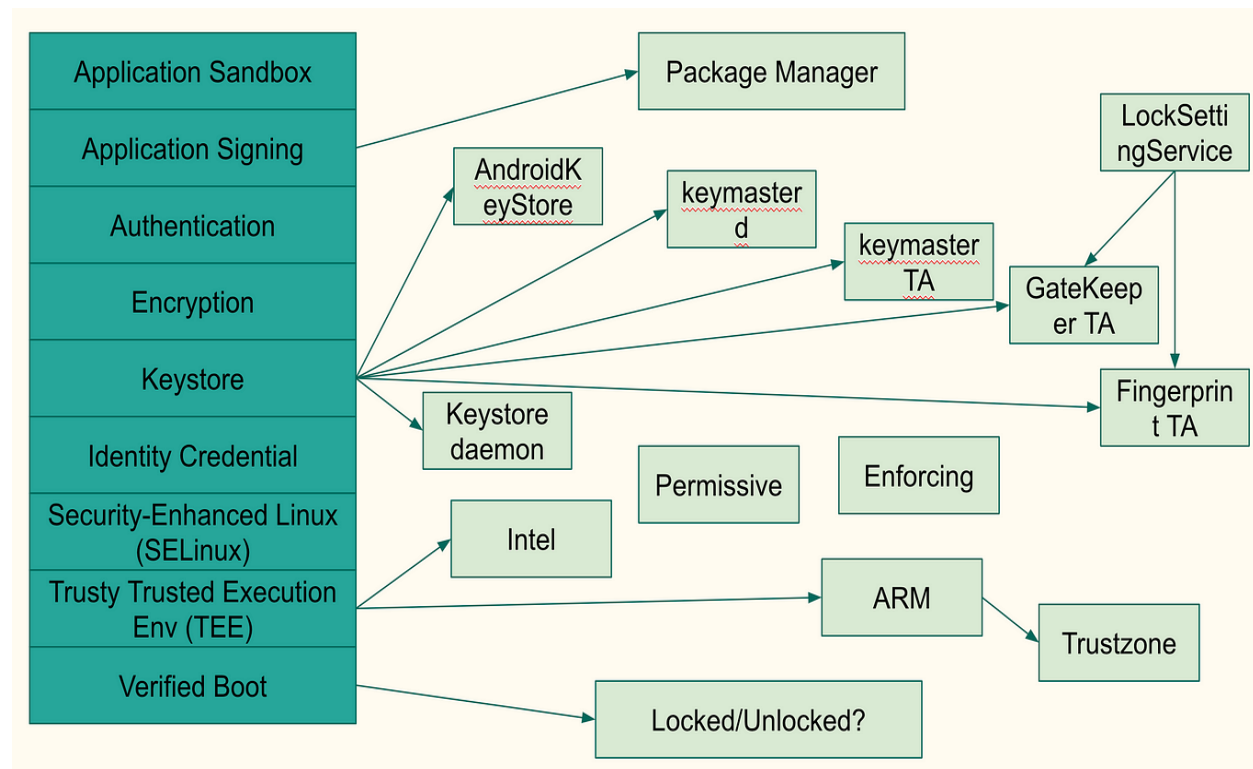
This study investigates the detection of SQL injection attempts directed towards web applications using Zeek, a network security monitoring tool. SQL injection is a common and serious attack vector that allows malicious SQL queries to be injected into user input fields, hence jeopardising the security of web applications. The aim of this research is to successfully identify and neutralise these assaults by utilising Zeek's capabilities.

### 2. Prerequisite of the Project

In order for this project to be completed successfully, the following conditions must be met:

- A basic understanding of the effects of SQL injection attacks.
- Knowledge of Zeek's (formerly called Bro) scripting features.
- Permission to test a web application that is susceptible to SQL injection.
- A monitoring system for Zeek installation and configuration.

### 3. Network Diagram



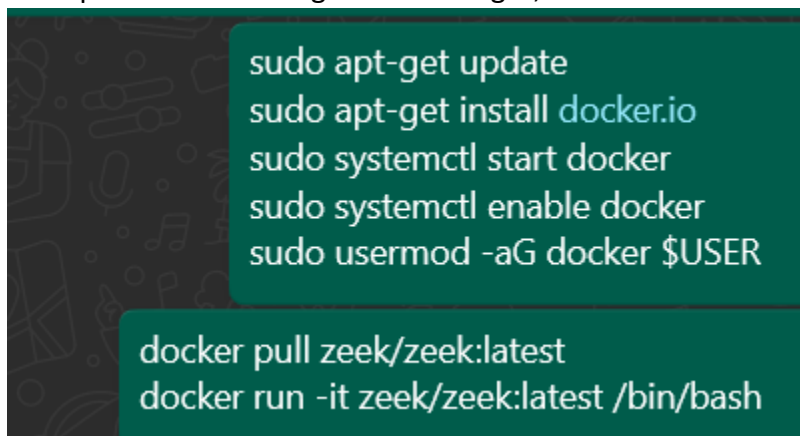
## 4. Methodology

### 4.1 First Task: Set Up Zeek on the Watching Computer

1. **Description:** Zeek needs to be set up on a specific monitoring computer in order to record and examine network data.
2. **Steps:**
  - a. Go to the official website and download the Zeek installation package.
  - b. Observe the operating system-specific installation guidelines.
  - c. Check Zeek's status and run it to confirm the installation.

### 4.2 Task 2: Set Up Zeek to Record and Examine Data

1. **Description:** To monitor traffic between the web server and the internet, configure Zeek.
2. **Steps:**
  - a. Add the network interfaces that the web server uses to the Zeek configuration files.
  - b. Configure the right alerting and logging settings.
  - c. To implement the configuration changes, restart Zeek.



```
sudo apt-get update
sudo apt-get install docker.io
sudo systemctl start docker
sudo systemctl enable docker
sudo usermod -aG docker $USER

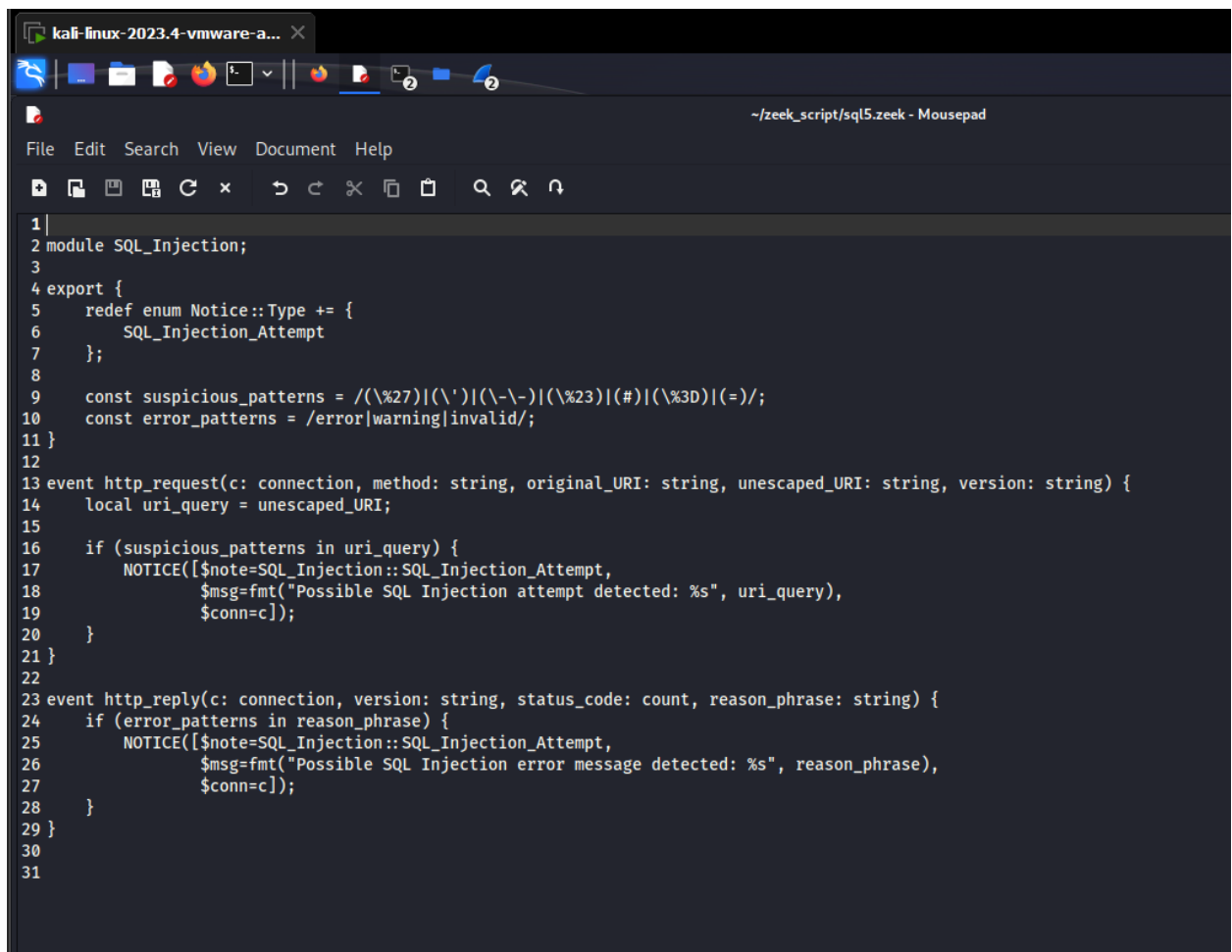
docker pull zeek/zeek:latest
docker run -it zeek/zeek:latest /bin/bash
```

### 4.3 Task 3: Create Zeek Scripts to Identify SQL Injection

1. **Description:** Create and modify Zeek scripts to find patterns of SQL injection in HTTP requests.
2. **Steps:**
  - a. Create or alter Zeek scripts to find particular SQL injection patterns, like functions, keywords, and encoding schemes.



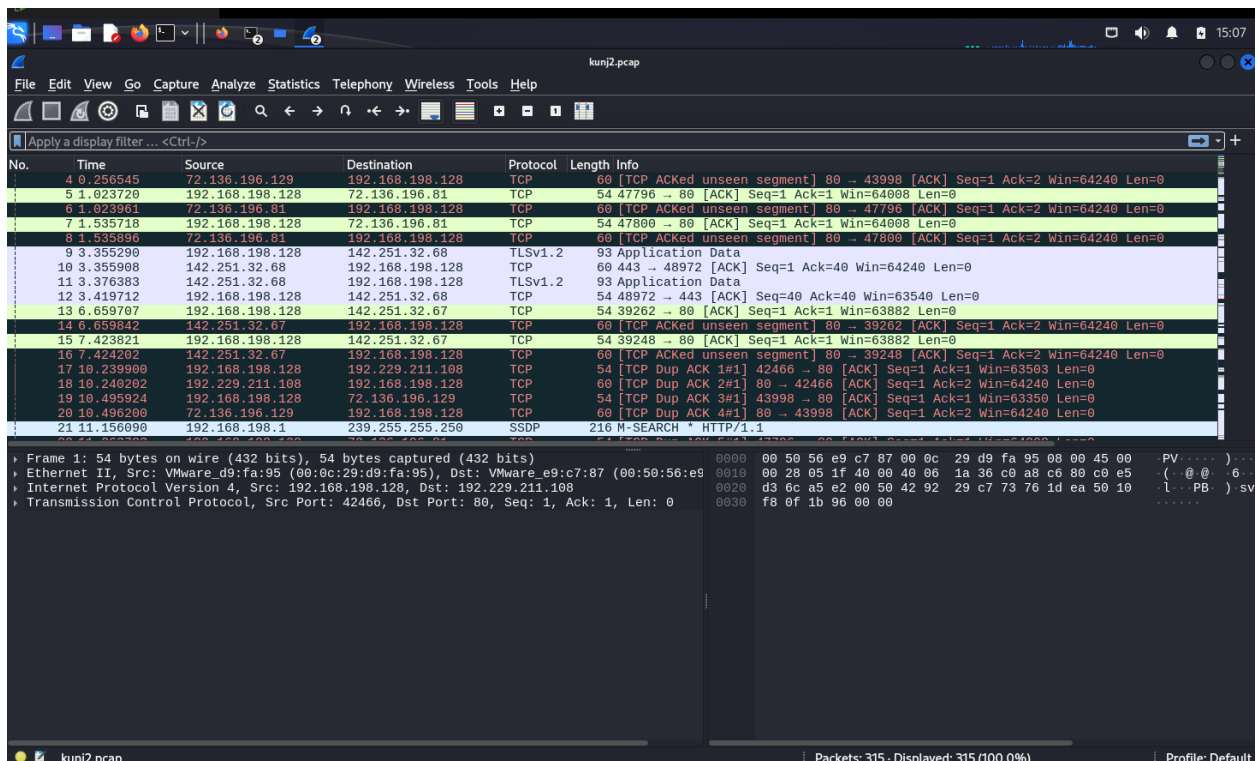
- b. Make sure these scripts correctly detect SQL injection attempts by testing them.
- c. For improved detection, make use of already-written scripts like detect-sqli. zeek.

A screenshot of a Kali Linux virtual machine window. The title bar reads 'kali-linux-2023.4-vmware-a...'. The desktop has several icons. A 'Mousepad' window is open, showing a Zeek script file named 'sql5.zeek'. The script defines a module 'SQL\_Injection' and exports a function to detect SQL injection attempts by analyzing HTTP requests and replies for suspicious and error patterns in the URI query and reason phrase. The script uses 'NOTICE' to log detected attempts and errors.

```
1|
2 module SQL_Injection;
3
4 export {
5   redef enum Notice::Type += {
6     SQL_Injection_Attempt
7   };
8
9   const suspicious_patterns = /(\\%27)|(\\'|)(\\-\\-)|(\\%23)|(#)|(\\%3D)|(=)/;
10  const error_patterns = /error|warning|invalid/;
11 }
12
13 event http_request(c: connection, method: string, original_URI: string, unescaped_URI: string, version: string) {
14   local uri_query = unescaped_URI;
15
16   if (suspicious_patterns in uri_query) {
17     NOTICE([$note=SQL_Injection::SQL_Injection_Attempt,
18             $msg=fmt("Possible SQL Injection attempt detected: %s", uri_query),
19             $conn=c]);
20   }
21 }
22
23 event http_reply(c: connection, version: string, status_code: count, reason_phrase: string) {
24   if (error_patterns in reason_phrase) {
25     NOTICE([$note=SQL_Injection::SQL_Injection_Attempt,
26             $msg=fmt("Possible SQL Injection error message detected: %s", reason_phrase),
27             $conn=c]);
28   }
29 }
30
31
```

#### 4.4 Task 4: Create Attacks via SQL Injection

- 1. **Description:** To mimic SQL injection attacks on a website that is vulnerable, use a testing tool.
- 2. **Steps:**
  - a. Find or develop a testing tool that can replicate SQL injection attacks.
  - e. Conduct deliberate assaults on the web application to potentially produce SQL injection traffic.
  - f. Keep an eye out for these fake attacks in Zeek's logs and alerts.



## 4.5 Task 5: Review and edit the Zeek logs

1. **Description:** Examine Zeek's logs and warnings to spot erratic traffic patterns and improve routines.
2. **Steps:**
  - a. Look for any patterns of SQL injection in the logs.
  - b. To increase detection accuracy, Zeek scripts should be adjusted and improved in light of the research.
  - c. Keep an eye on the scripts and update them frequently to accommodate new SQL injection methods.

```
(kali㉿kali)-[~/zeek_script]
$ sudo docker exec -it flamboyant_raman zeek -C -r /zeek/kunj2.pcap /zeek/sql6.zeek

Zeek has started!
```

## 5. Difficulties the Project Faces

**Challenge 1:** The first challenge is setting Zeek up to correctly record and examine pertinent traffic.

**Challenge 2:** Creating efficient Zeek scripts to identify different SQL injection patterns is the second challenge.

**Challenge 3:** Reducing the number of false positives while identifying SQL injection attempts.

**Challenge 4:** To ensure effective testing, simulate realistic attacks on the web application.

## **6. Conclusion: Project-Related Lessons Learnt**

**Lesson 1:** Comprehending the subtleties of SQL injection attacks and the different types of assaults.

**Lesson 2:** Learning how to analyse and spot SQL injection attempts using Zeek scripting.

**Lesson 3:** Understanding how crucial it is to continuously improve scripts in order to stay ahead of emerging attack strategies.

**Lesson 4:** Zeek implementation as a useful part of an all-encompassing web application security plan.

## **7. Project Management: Enumerating the Tasks Completed by Every Team Member**

**Kunj Modi & Dhairya Soni:** Setting up and configuring Zeek initially.

**Jay Parekh:** Writing Zeek scripts and modifying them to detect SQL Injection.

**Deep Patel:** Zeek log analysis and SQL injection attack simulation.

**Mohitkumar Patel:** Scripts are improved, and findings are documented.

## **REFERENCES:**

1. Github.com Zeek scripts

<https://github.com/zeek/zeek/blob/master/scripts/base/protocols/http/detect-sqli.zeek>

2. The Zeek Network Security Monitor. (n.d.-b). Zeek. <https://zeek.org/>

