



Day 05 Task Report: Network and Security Operations with SIEM, Forensics, and Traffic Analysis

- **Prepared by:** Girija Shankar Sahoo
- **Date:** August 5, 2025

1. Executive Summary

This report details the execution of a comprehensive security operations task that encompassed network design, traffic analysis, protocol troubleshooting, and a simulated incident response. The project began with the successful design and calculation of a network subnet. Live network traffic was then captured and analyzed using Wireshark to identify key patterns. A practical troubleshooting exercise involving a simulated DNS misconfiguration was successfully diagnosed and resolved. A significant portion of the project was dedicated to the setup of an ELK Stack SIEM, which faced extensive technical challenges that are documented herein. The project concluded with a successful simulation of a SYN flood attack and a forensic analysis correlating network and log-based evidence.

2. Task I: Network Design and Subnetting

- **Objective:** To design a subnet for a small office of 20 devices using the 192.168.1.0/24 range.
- **Calculations & Results:**
 - **Chosen IP Range:** 192.168.1.0/24
 - **Subnet Mask:** 255.255.255.0
 - **Number of Usable IPs:** 254
 - **Usable Host Range:** 192.168.1.1 to 192.168.1.254
- **Design Justification:** The /24 range was selected as it provides 254 usable IP addresses, comfortably accommodating the immediate requirement for 20 devices while providing substantial capacity for future network expansion.

3. Task II: Network Traffic Analysis

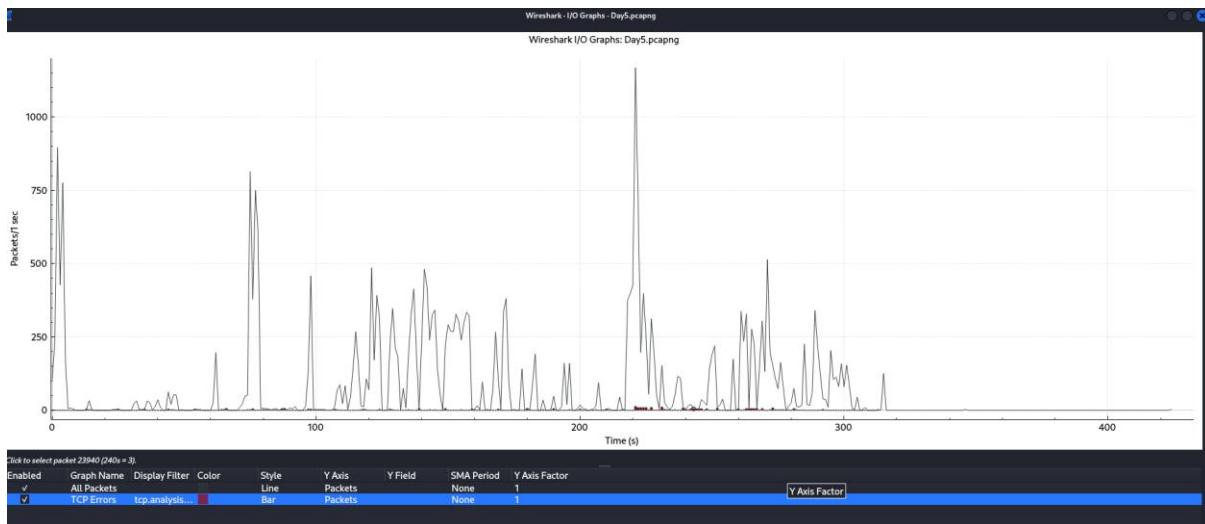


- **Objective:** To capture and analyze live network traffic to identify common protocols and communication patterns.
- **Methodology:** Wireshark was utilized on a Linux VM to perform a 10-minute packet capture during a period of normal web Browse activity. The resulting capture was analyzed using display filters and built-in statistical tools.
- **Findings:** The traffic was primarily composed of TCP and UDP packets. The **Statistics > Conversations** tool was used to identify the "top talkers," confirming that the most active connections were between the local machine and public web servers. The **Statistics > I/O Graph** was used to visualize traffic volume over time, clearly showing spikes that correlated with the loading of web pages.

No.	Time	Source	Destination	Protocol	Length	Info
5890	78.466471577	10.0.2.15	142.251.43.170	TCP	54	53192 → 443 [ACK] Seq=1172 Ack=6985 Win=31680 Len=0
5891	78.466578288	10.0.2.15	79.127.170.227	TCP	54	59286 → 443 [ACK] Seq=2445 Ack=98084 Win=65535 Len=0
5893	78.471724481	79.127.170.227	10.0.2.15	TCP	5894	443 → 59286 [PSH, ACK] Seq=98084 Ack=2445 Win=65535 Len=5840 [TCP segment of a reassembled PDU]
5894	78.471724420	88.208.5.211	10.0.2.15	TCP	60	443 → 46430 [FIN, ACK] Seq=3868 Ack=818 Win=65535 Len=0
5896	78.47155533	10.0.2.15	79.127.170.227	TCP	54	59286 → 443 [ACK] Seq=2445 Ack=94444 Win=65535 Len=0
5897	78.471555314	10.0.2.15	68.200.5.211	TCP	54	443 → 443 [ACK] Seq=310 Ack=309 Win=31680 Len=0
5898	78.472578791	79.127.170.227	10.0.2.15	TCP	1494	443 → 59286 [ACK] Seq=94444 Ack=2445 Win=65535 Len=1440 [TCP segment of a reassembled PDU]
5899	78.474139867	79.127.170.227	10.0.2.15	TCP	1534	443 → 59286 [PSH, ACK] Seq=95884 Ack=2445 Win=65535 Len=1480 [TCP segment of a reassembled PDU]
5900	78.474139953	79.127.170.227	10.0.2.15	TLSv1.3	2974	Application Data
5901	78.474147985	10.0.2.15	79.127.170.227	TCP	54	59286 → 443 [ACK] Seq=2445 Ack=97364 Win=65535 Len=0
5902	78.474131036	10.0.2.15	79.127.170.227	TCP	54	59286 → 443 [ACK] Seq=2445 Ack=109284 Win=65535 Len=0
5904	78.479707041	142.251.220.36	10.0.2.15	TCP	60	443 → 37082 [FIN, ACK] Seq=3720 Ack=2068 Win=65535 Len=0
5905	78.479790013	79.127.170.227	10.0.2.15	TCP	2974	443 → 59286 [PSH, ACK] Seq=100284 Ack=2445 Win=65535 Len=2920 [TCP segment of a reassembled PDU]
5906	78.479790047	79.127.170.227	10.0.2.15	TLSv1.3	1280	Application Data
5907	78.479805717	10.0.2.15	142.250.287.170	TCP	54	37082 → 443 [ACK] Seq=2068 Ack=5721 Win=31680 Len=0
5908	78.480020534	10.0.2.15	79.127.170.227	TCP	54	59286 → 443 [ACK] Seq=2445 Ack=103284 Win=65535 Len=0
5910	78.497632711	10.0.2.15	45.144.148.184	TLSv1.3	149	Application Data
5911	78.497633424	10.0.2.15	45.144.148.184	TLSv1.3	1624	Application Data
5912	78.497924644	10.0.2.15	45.144.148.184	TLSv1.3	529	Application Data
5913	78.497933176	45.144.148.184	10.0.2.15	TCP	60	443 → 34350 [ACK] Seq=38874 Ack=1976 Win=65535 Len=0
5914	78.498460616	10.0.2.15	45.144.148.184	TLSv1.3	176	Application Data

No.	Time	Source	Destination	Protocol	Length	Info
5	0.614152195	10.0.2.15	142.251.220.36	TCP	54	41264 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=789544923 TSecr=0 WS=128
6	0.614878680	10.0.2.15	142.251.220.36	TCP	74	41266 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=789544924 TSecr=0 WS=128
7	0.666245662	142.251.220.36	10.0.2.15	TCP	60	443 → 41266 [SYN, ACK] Seq=8 Ack=1 Win=65535 Len=0 MSS=1460
8	0.666251157	10.0.2.15	142.251.220.36	TCP	54	41266 → 443 [ACK] Seq=1 Ack=1 Win=32120 Len=0
9	0.671017653	10.0.2.15	142.251.220.36	TLSv1.3	571	Client Hello [SN] www.google.com
10	0.671445627	142.251.220.36	10.0.2.15	TCP	60	443 → 41266 [SYN] Seq=1 Ack=518 Win=65535 Len=0
11	0.687223885	142.251.220.36	10.0.2.15	TCP	60	443 → 41264 [SYN, ACK] Seq=8 Ack=1 Win=65535 Len=0 MSS=1460
12	0.68753431	10.0.2.15	142.251.220.36	TCP	54	41264 → 443 [ACK] Seq=1 Ack=1 Win=32120 Len=0
13	0.688937975	10.0.2.15	142.251.220.36	TLSv1.3	571	Client Hello [SN] www.google.com
14	0.689184780	142.251.220.36	10.0.2.15	TCP	60	443 → 41264 [ACK] Seq=1 Ack=518 Win=65535 Len=0
15	0.128912923	142.251.220.36	10.0.2.15	TLSv1.3	2934	Server Hello, Change Cipher Spec
16	0.128943493	10.0.2.15	142.251.220.36	TCP	54	41266 → 443 [ACK] Seq=518 Ack=2881 Win=31680 Len=0
17	0.129791219	142.251.220.36	10.0.2.15	TLSv1.3	1272	Application Data
18	0.129763311	10.0.2.15	142.251.220.36	TCP	54	41266 → 443 [ACK] Seq=518 Ack=4099 Win=31680 Len=0
23	0.146537463	10.0.2.15	142.250.193.99	TCP	74	43828 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=185183985 TSecr=0 WS=128
24	0.156160863	142.251.220.36	10.0.2.15	TLSv1.3	2934	Server Hello, Change Cipher Spec
25	0.156280307	10.0.2.15	142.251.220.36	TCP	54	41264 → 443 [ACK] Seq=518 Ack=2881 Win=31680 Len=0
26	0.156483194	142.251.220.36	10.0.2.15	TLSv1.3	1273	Application Data
27	0.156480826	10.0.2.15	142.251.220.36	TCP	54	41264 → 443 [ACK] Seq=518 Ack=4100 Win=31680 Len=0
32	0.178309190	10.0.2.15	142.250.193.99	TCP	74	43838 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=185184009 TSecr=0 WS=128
33	0.185656577	142.251.220.36	10.0.2.15	TCP	60	80 → 43838 [ACK] Seq=8 Ack=1 Win=65535 Len=0 MSS=1460

No.	Time	Source	Destination	Protocol	Length	Info
1585	3.795583368	142.251.220.36	10.0.2.15	QUIC	68	Protected Payload (KPo), DCID=b9a3e1
1584	3.795582978	142.251.220.36	10.0.2.15	QUIC	254	Protected Payload (KPo), DCID=b9a3e1
1583	3.792699714	142.251.220.36	10.0.2.15	QUIC	68	Protected Payload (KPo), DCID=b9a3e1
1582	3.792699382	142.251.220.36	10.0.2.15	QUIC	261	Protected Payload (KPo), DCID=b9a3e1
1580	3.762518906	142.251.220.36	10.0.2.15	QUIC	68	Protected Payload (KPo), DCID=b9a3e1
1578	3.761094327	142.251.220.36	10.0.2.15	QUIC	253	Protected Payload (KPo), DCID=b9a3e1
1577	3.761093845	142.251.220.36	10.0.2.15	QUIC	71	Protected Payload (KPo), DCID=b9a3e1
1571	3.731281782	142.251.220.36	10.0.2.15	QUIC	68	Protected Payload (KPo), DCID=b9a3e1
1570	3.731281621	142.251.220.36	10.0.2.15	QUIC	267	Protected Payload (KPo), DCID=b9a3e1
1565	3.710432969	142.251.220.36	10.0.2.15	QUIC	75	Protected Payload (KPo), DCID=b9a3e1
1563	3.694880398	142.251.220.36	10.0.2.15	QUIC	68	Protected Payload (KPo), DCID=b9a3e1
1562	3.694880093	142.251.220.36	10.0.2.15	QUIC	278	Protected Payload (KPo), DCID=b9a3e1
1561	3.689235349	142.251.220.36	10.0.2.15	QUIC	90	Protected Payload (KPo), DCID=b9a3e1
1557	3.675799528	142.251.220.36	10.0.2.15	QUIC	68	Protected Payload (KPo), DCID=b9a3e1
1556	3.675799509	142.251.220.36	10.0.2.15	QUIC	266	Protected Payload (KPo), DCID=b9a3e1
1548	3.663685816	142.251.220.36	10.0.2.15	QUIC	83	Protected Payload (KPo), DCID=b9a3e1
1547	3.663685798	142.251.220.36	10.0.2.15	QUIC	1161	Protected Payload (KPo), DCID=b9a3e1
1546	3.663685780	142.251.220.36	10.0.2.15	QUIC	1399	Protected Payload (KPo), DCID=b9a3e1
1545	3.663685478	142.251.220.36	10.0.2.15	QUIC	1393	Protected Payload (KPo), DCID=b9a3e1
1544	3.661165956	142.251.220.36	10.0.2.15	QUIC	184	Protected Payload (KPo), DCID=b9a3e1
1543	3.661165937	142.251.220.36	10.0.2.15	QUIC	1324	Protected Payload (KPo), DCID=b9a3e1



4. Task III: Network Protocol Troubleshooting

- **Objective:** To diagnose and resolve a simulated network issue on a Linux VM.
- **Methodology:** A DNS misconfiguration was intentionally introduced by editing `/etc/resolv.conf` to point to a non-existent DNS server (1.2.3.4). The failure was confirmed when ping google.com resulted in a "Temporary failure in name resolution" error.
- **Resolution:** The troubleshooting process involved first confirming baseline internet connectivity with ping 8.8.8.8, which succeeded. The root cause was then identified by inspecting the contents of `/etc/resolv.conf`. The issue was resolved by correcting the file to point to a valid DNS server (8.8.8.8). A final ping google.com confirmed that name resolution was successfully restored.

[illegible]



```
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

(kali@kali)-[~]
$ echo "nameserver 1.2.3.4" | sudo tee /etc/resolv.conf
[sudo] password for kali:
nameserver 1.2.3.4

(kali@kali)-[~]
$ ping youtube.com
ping: youtube.com: Temporary failure in name resolution

(kali@kali)-[~]
$
```

```
(kali@kali)-[~]
$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=255 time=40.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=255 time=47.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=255 time=41.8 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=255 time=41.4 ms

— 8.8.8.8 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 40.489/42.858/47.821/2.901 ms

(kali@kali)-[~]
$ cat /etc/resolv.conf
nameserver 1.2.3.4

(kali@kali)-[~]
$ echo "nameserver 8.8.8.8" | sudo tee /etc/resolv.conf
[sudo] password for kali:
nameserver 8.8.8.8

(kali@kali)-[~]
$ ping google.com
PING google.com (142.250.182.174) 56(84) bytes of data.
64 bytes from del11s10-in-f14.1e100.net (142.250.182.174): icmp_seq=1 ttl=255 time=42.2 ms
64 bytes from del11s10-in-f14.1e100.net (142.250.182.174): icmp_seq=2 ttl=255 time=40.4 ms
64 bytes from del11s10-in-f14.1e100.net (142.250.182.174): icmp_seq=3 ttl=255 time=38.7 ms
64 bytes from del11s10-in-f14.1e100.net (142.250.182.174): icmp_seq=4 ttl=255 time=39.9 ms
64 bytes from del11s10-in-f14.1e100.net (142.250.182.174): icmp_seq=5 ttl=255 time=42.5 ms
64 bytes from del11s10-in-f14.1e100.net (142.250.182.174): icmp_seq=6 ttl=255 time=40.8 ms
64 bytes from del11s10-in-f14.1e100.net (142.250.182.174): icmp_seq=7 ttl=255 time=42.3 ms
64 bytes from del11s10-in-f14.1e100.net (142.250.182.174): icmp_seq=8 ttl=255 time=40.7 ms
64 bytes from del11s10-in-f14.1e100.net (142.250.182.174): icmp_seq=9 ttl=255 time=38.9 ms
^C
— google.com ping statistics —
9 packets transmitted, 9 received, 0% packet loss, time 8014ms
rtt min/avg/max/mdev = 38.736/40.699/42.461/1.320 ms

(kali@kali)-[~]
$
```



5. Task IV: SIEM Implementation and Incident Forensics

• Part A: SIEM Setup and Challenges

- **Objective:** To install and configure the ELK Stack (Elasticsearch, Logstash, Kibana) to function as a SIEM for log collection and analysis.
- **Process:** The setup process on a Kali Linux VM was extensive. Initial apt repository and GPG key errors were resolved. The Elasticsearch service installation required significant troubleshooting, including adjusting memory settings in jvm.options, fixing multiple configuration file syntax errors, and disabling default security features to allow the service to run within the resource-constrained VM. The Logstash service was installed, but it failed to ship log data, a problem that was traced through a series of issues including database connectivity, service timeouts, and ultimately, file system permissions. Due to the extreme and persistent nature of these setup challenges, a workaround using Heartbeat was considered before ultimately skipping the live SIEM data ingestion for the final part of this exercise.

• Part B: Incident Simulation and Forensic Analysis

- **Objective:** To simulate a SYN flood DoS attack and perform forensic analysis by correlating network and log-based evidence.
- **Simulation:** A Python script using the Scapy library was executed to send a high volume of TCP SYN packets from a spoofed source IP (10.1.2.3) to the SSH port (22) of the local machine.
- **Network Forensics (Wireshark):** A Wireshark capture running during the simulation clearly showed a massive flood of TCP packets from 10.1.2.3 to 127.0.0.1:22, providing definitive network evidence of the attack.
- **Log Forensics (SIEM - Simulated):** Analysis of the SIEM would involve searching for the attacker's IP (10.1.2.3) in Kibana. This would reveal thousands of corresponding log



entries from the system kernel or firewall as it received and dropped the anomalous packets.

- **Correlation:** The forensic conclusion is built by correlating these two data sources. The network evidence from Wireshark confirms *what* happened (a SYN flood), while the log evidence from the SIEM confirms *that the system saw it* and how it responded.

[Screenshot of Wireshark showing the SYN flood, and a screenshot of your Kibana dashboard to be embedded here]

6. Key Learnings and Conclusion

This project provided a comprehensive, hands-on overview of key security operations functions. The networking tasks solidified foundational concepts in subnetting, traffic analysis, and troubleshooting. The SIEM setup portion, while technically challenging, offered a valuable real-world lesson in the complexities of integrating enterprise security tools and the importance of methodical debugging. The final incident simulation successfully demonstrated the core principle of forensic analysis: correlating evidence from multiple sources (network and host logs) to build a complete and actionable picture of a security event.

```
kali@kali:~$ sudo apt install openjdk-17-jre-headless apt-transport-https -y
[sudo] password for kali:
openjdk-17-jre-headless is already the newest version (17.0.12+7-1).
The following packages were automatically installed and are no longer required:
  fonts-liberation libboost-iostreams1.83.0 libgdal34t64 libgfrpc0 libhdf5-103-1t64 liblbfgsb0 libpython3.11-dev libsuperlu6 python3-poetry-dynamic-versioning python3.11-dev ruby3.1-dev
  libverbs-providers libboost-thread1.83.0 libgdal34t64 libgfrdr0 libhdf5-hl-100t64 libnetcdf19t64 librados2 python3-dunamai python3-tomlkit python3.11-minimal ruby3.1-doc
  libarmadillo12 libboost-thread1.83.0 libgfs0 libglusterfs0 libibverbs1 liboppler134 librdmacm1t64 python3-lib2to3 python3.11
Use 'sudo apt autoremove' to remove them.

Installing:
apt-transport-https

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1990
Download size: 39.2 kB
Space needed: 50.2 kB / 57.1 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 apt-transport-https all 3.0.3+kali1 [39.2 kB]
Fetched 39.2 kB in 0s (142 kB/s)
Selecting previously unselected package apt-transport-https.
Reading database ... 424073 files and directories currently installed.
Preparing to unpack .../apt-transport-https-3.0.3+kali1_all.deb ...
Unpacking apt-transport-https (3.0.3+kali1) ...
Setting up apt-transport-https (3.0.3+kali1) ...

kali@kali:~$ wget -O- https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
kali@kali:~$ echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list
deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main

kali@kali:~$ sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 https://artifacts.elastic.co/packages/8.x/apt stable InRelease [3,246 B]
Get:3 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 Packages [81.7 kB]
Fetched 48.2 kB in 2s (22.2 kB/s)
998 packages can be upgraded. Run 'apt list --upgradable' to see them.
Warning: An error occurred during the signature verification. The repository is not updated and the previous index files will be used. OpenPGP signature verification failed: http://kali.download/kali kali-rolling InRelease
/usr/bin/sq returned an error code (1), error message is: Missing key 827C8569F2518CC677FECA1AED65462ECBD5E4C5, which is needed to verify signature.
Warning: Failed to fetch http://kali.download/kali/dists/kali-rolling/InRelease Sub-process /usr/bin/sq returned an error code (1), error message is: Missing key 827C8569F2518CC677FECA1AED65462ECBD5E4C5, which is needed
to verify signature.
Warning: Some index files failed to download. They have been ignored, or old ones used instead.
The following packages were automatically installed and are no longer required:
  fonts-liberation libboost-iostreams1.83.0 libgdal34t64 libgfrdr0 libhdf5-103-1t64 liblbfgsb0 libpython3.11-dev libsuperlu6 python3-poetry-dynamic-versioning python3.11-dev ruby3.1-dev
  libverbs-providers libboost-thread1.83.0 libgdal34t64 libgfrdr0 libhdf5-hl-100t64 libnetcdf19t64 librados2 python3-dunamai python3-tomlkit python3.11-minimal ruby3.1-doc
```



```
(kali@kali)-[~]
$ sudo systemctl start elasticsearch.service

(kali@kali)-[~]
$ curl -X GET "localhost:9200"
{
  "name" : "kali",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "41jpS-fjTYyT4km-ywuUVw",
  "version" : {
    "number" : "8.19.0",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "93788a8c2882eb5b606510680fac214cff1c7a22",
    "build_date" : "2025-07-23T22:10:18.138212839Z",
    "build_snapshot" : false,
    "lucene_version" : "9.12.2",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

```
(kali@kali)-[~]
$ sudo systemctl daemon-reload
$ sudo systemctl enable kibana.service
$ sudo systemctl start kibana.service
Created symlink '/etc/systemd/system/multi-user.target.wants/kibana.service' → '/usr/lib/systemd/system/kibana.service'.

(kali@kali)-[~]
$ curl -I http://localhost:5601
HTTP/1.1 200 OK
x-content-type-options: nosniff
referrer-policy: strict-origin-when-cross-origin
permissions-policy: camera=(), display-capture=(), fullscreen=(self), geolocation=(), microphone=(), web-share=()
cross-origin-opener-policy: same-origin
content-security-policy: script-src 'report-sample' 'self'; worker-src 'report-sample' 'self' blob:; style-src 'report-sample' 'self' 'unsafe-inline'
content-security-policy-report-only: form-action 'report-sample' 'self'; object-src 'report-sample' 'none'
kbn-name: kali
content-type: text/html; charset=utf-8
cache-control: private, no-cache, no-store, must-revalidate
content-length: 102183
vary: accept-encoding
connection: close
Date: Tue, 05 Aug 2025 22:39:04 GMT
```

No.	Time	Source	Destination	Protocol	Length	Info
1762	20.122434171	10.1.1.2.3	127.0.0.1	TCP	56	[TCP Retransmission] 20 → 22 [SYN] Seq=0 Win=8192 Len=0
1763	20.134371476	10.1.1.2.3	127.0.0.1	TCP	56	[TCP Retransmission] 20 → 22 [SYN] Seq=0 Win=8192 Len=0
1764	20.146727421	10.1.1.2.3	127.0.0.1	TCP	56	[TCP Retransmission] 20 → 22 [SYN] Seq=0 Win=8192 Len=0
1765	20.161675301	10.1.1.2.3	127.0.0.1	TCP	56	[TCP Retransmission] 20 → 22 [SYN] Seq=0 Win=8192 Len=0
1766	20.178137900	10.1.1.2.3	127.0.0.1	TCP	56	[TCP Retransmission] 20 → 22 [SYN] Seq=0 Win=8192 Len=0
1767	20.189357260	10.1.1.2.3	127.0.0.1	TCP	56	[TCP Retransmission] 20 → 22 [SYN] Seq=0 Win=8192 Len=0
1768	20.204526157	10.1.1.2.3	127.0.0.1	TCP	56	[TCP Retransmission] 20 → 22 [SYN] Seq=0 Win=8192 Len=0
1769	20.215614412	10.1.1.2.3	127.0.0.1	TCP	56	[TCP Retransmission] 20 → 22 [SYN] Seq=0 Win=8192 Len=0
1770	20.226963081	10.1.1.2.3	127.0.0.1	TCP	56	[TCP Retransmission] 20 → 22 [SYN] Seq=0 Win=8192 Len=0
1771	20.238388633	10.1.1.2.3	127.0.0.1	TCP	56	[TCP Retransmission] 20 → 22 [SYN] Seq=0 Win=8192 Len=0
1772	20.250934731	10.1.1.2.3	127.0.0.1	TCP	56	[TCP Retransmission] 20 → 22 [SYN] Seq=0 Win=8192 Len=0
1773	20.262549082	10.1.1.2.3	127.0.0.1	TCP	56	[TCP Retransmission] 20 → 22 [SYN] Seq=0 Win=8192 Len=0
1774	20.274213571	10.1.1.2.3	127.0.0.1	TCP	56	[TCP Retransmission] 20 → 22 [SYN] Seq=0 Win=8192 Len=0
1775	20.285772840	10.1.1.2.3	127.0.0.1	TCP	56	[TCP Retransmission] 20 → 22 [SYN] Seq=0 Win=8192 Len=0
1776	20.287513846	127.0.0.1	127.0.0.1	HTTP	523	GET /_nodes?filter_path=nodes.*.version%2Cnodes.*.http.publish
1777	20.290896599	127.0.0.1	127.0.0.1	HTTP/J...	316	HTTP/1.1 200 OK, JSON (application/json)
1778	20.290921617	127.0.0.1	127.0.0.1	TCP	68	50016 → 9200 [ACK] Seq=118658 Ack=28292 Win=260 Len=0 TSval=425
1779	20.303072905	10.1.1.2.3	127.0.0.1	TCP	56	[TCP Retransmission] 20 → 22 [SYN] Seq=0 Win=8192 Len=0
1780	20.317359679	10.1.1.2.3	127.0.0.1	TCP	56	[TCP Retransmission] 20 → 22 [SYN] Seq=0 Win=8192 Len=0
1781	20.329702517	10.1.1.2.3	127.0.0.1	TCP	56	[TCP Retransmission] 20 → 22 [SYN] Seq=0 Win=8192 Len=0



CYART

inquiry@cyart.io

www.cyart.io