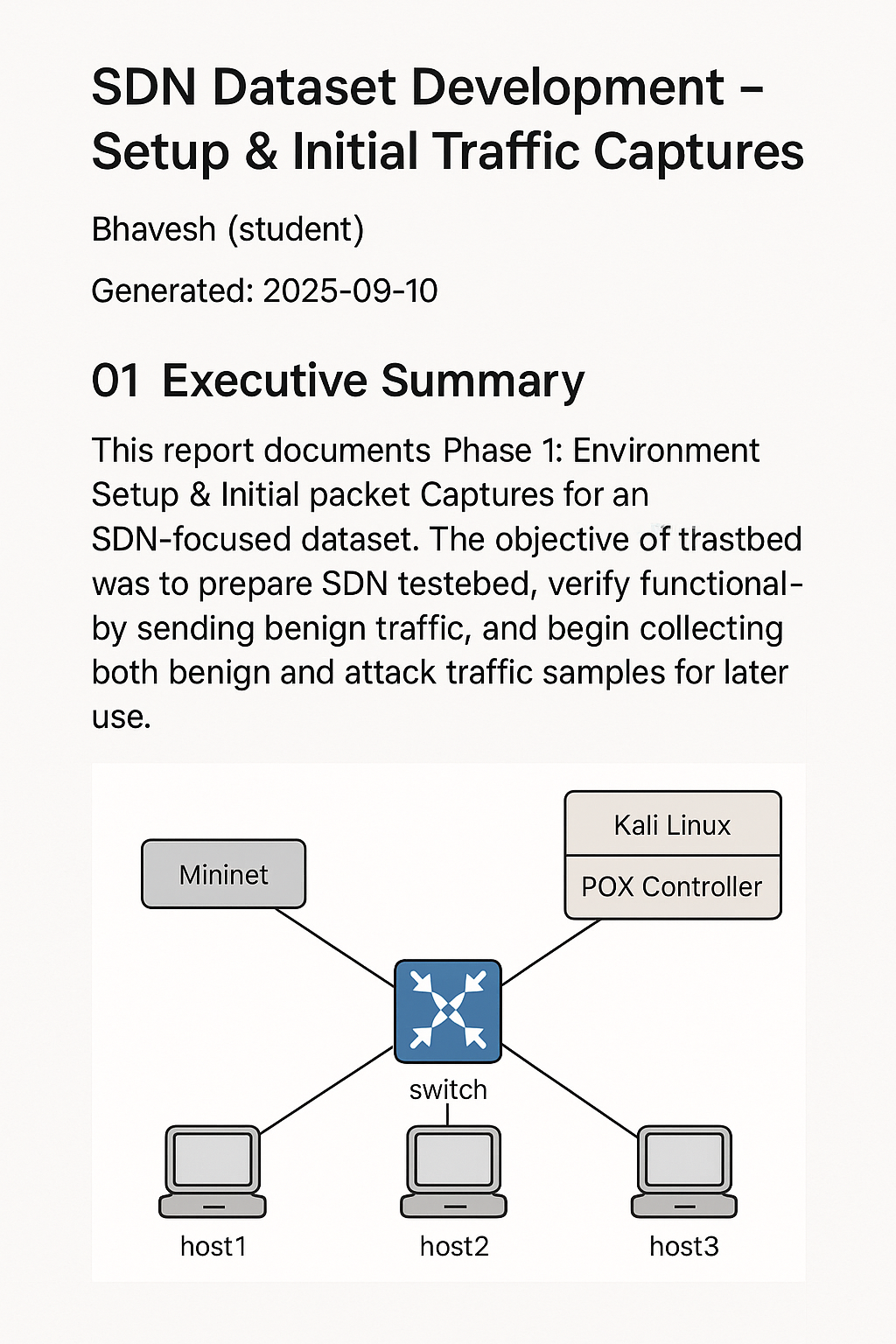
**Title:** SDN Dataset Development – Setup & Initial Traffic Captures

## 01 Executive Summary

This report documents **Phase 1: Environment Setup & Initial Packet Captures** for an SDN-focused dataset. The objective of this phase was to prepare the SDN testbed (Mininet + Kali + POX), verify functionality by sending benign traffic, and begin collecting both benign and attack traffic samples for later use.

Key completed tasks:

* **Testbed setup:** Dual-VM environment with POX controller on Kali and Mininet topology on Ubuntu.
* **System specifications:**
  + **Kali VM:** 8 GB RAM, 4 processors, 80 GB disk, bridged networking.
  + **Ubuntu VM (20.x):** 4 GB RAM, 8 processors, 20 GB disk, bridged networking.
* **Benign traffic capture:** Successfully sent ICMP (ping) packets between Mininet hosts and captured packets.
* **Attack traffic capture:** Captured traffic for ARP spoof, SYN flood, and Port scan.
* **Dataset structure:** Organized folders for storing benign and malicious .pcap files.



## 02 Introduction

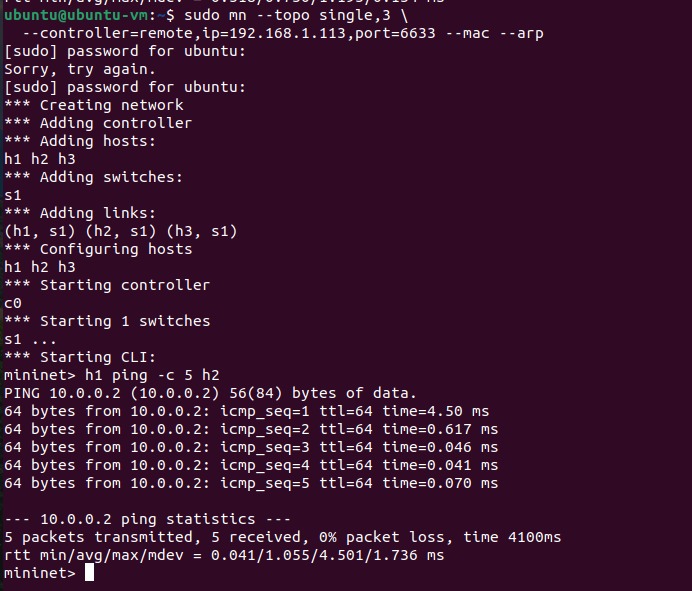
The purpose of this project is to build a labeled dataset for SDN security research, including both benign traffic and common network attacks. This dataset will later be used to analyze attack behaviors, extract IoCs, and explore ML-based intrusion detection approaches.

## 03 Completed Setup & Captures

### SDN Testbed

* **Tools used:**
  + Mininet (network emulation, Ubuntu VM)
  + POX controller (SDN control, Kali VM)
  + Kali Linux (attacker tools)
  + Wireshark (packet capture)
* **Topology created:** Single switch with 3 hosts

**sudo mn --topo single,3**



### 

### Virtual Machine Specifications

**Kali Linux VM (Controller + Attacker):**

|  |  |
| --- | --- |
| **Components** | **Specification** |
| Memory: | 8 GB |
| Processors: | 4 Core |
| Disk: | 80 GB |
| Network Adapter: | Bridged (Automatic) |
| OS: | Kali Linux Rolling 2024.4 (x64) |

**Ubuntu VM (Mininet Testbed):**

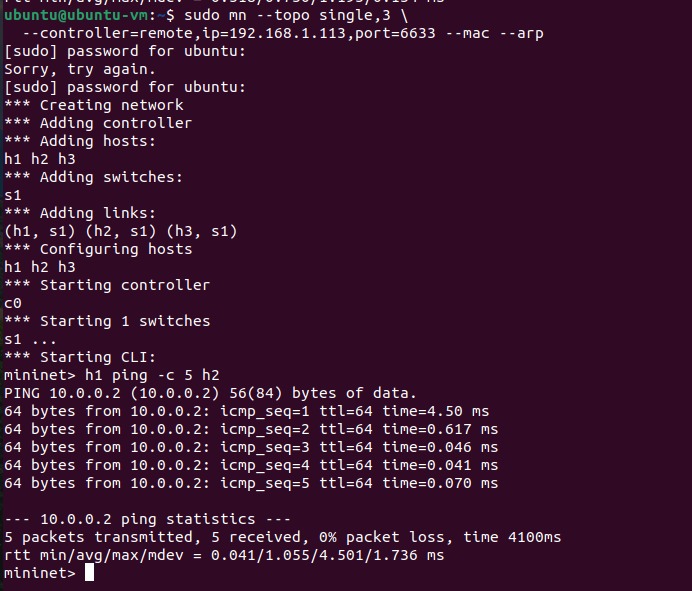
|  |  |
| --- | --- |
| **Components** | **Specification** |
| Memory: | 8 GB |
| Processors: | 4 Core |
| Disk: | 80 GB |
| Network Adapter: | Bridged (Automatic) |
| OS: | Kali Linux Rolling 2024.4 (x64) |

### Benign Traffic

* Sent ICMP packets from h1 → h2

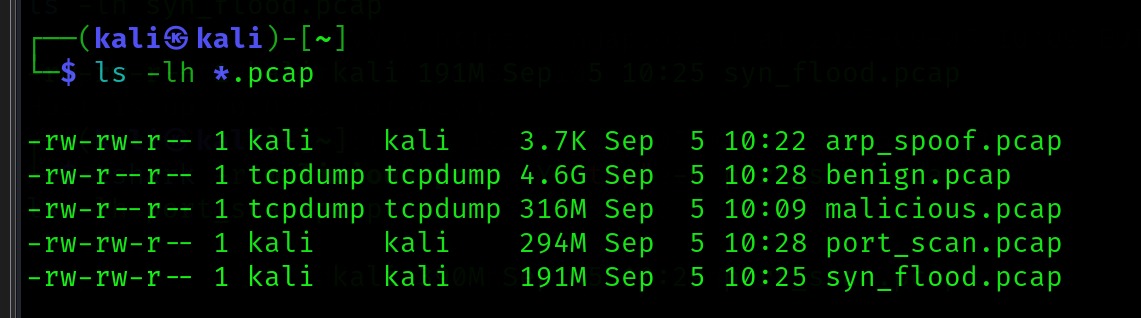
h1 ping 10.0.0.2

* Verified delivery with successful ping replies.
* Captured packets on h2-eth0 interface using Wireshark.
* Saved benign capture file for analysis.

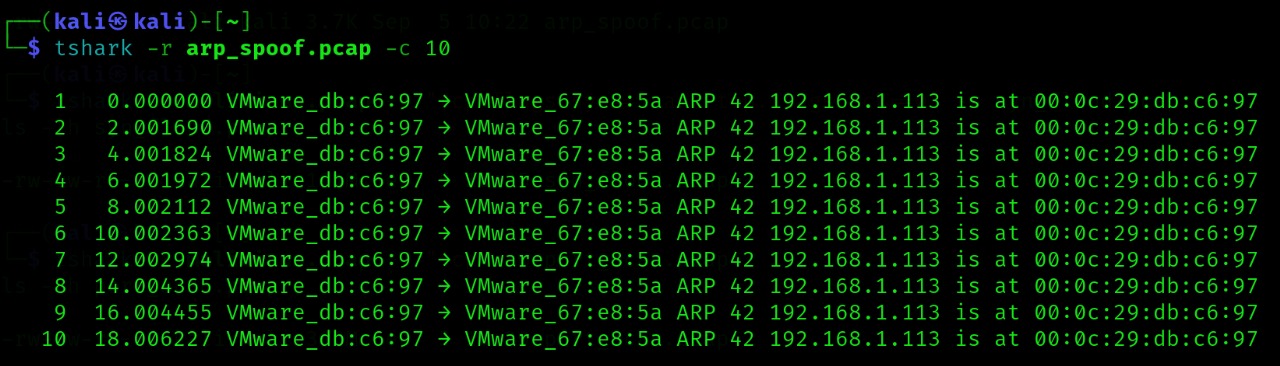


### Attack Traffic

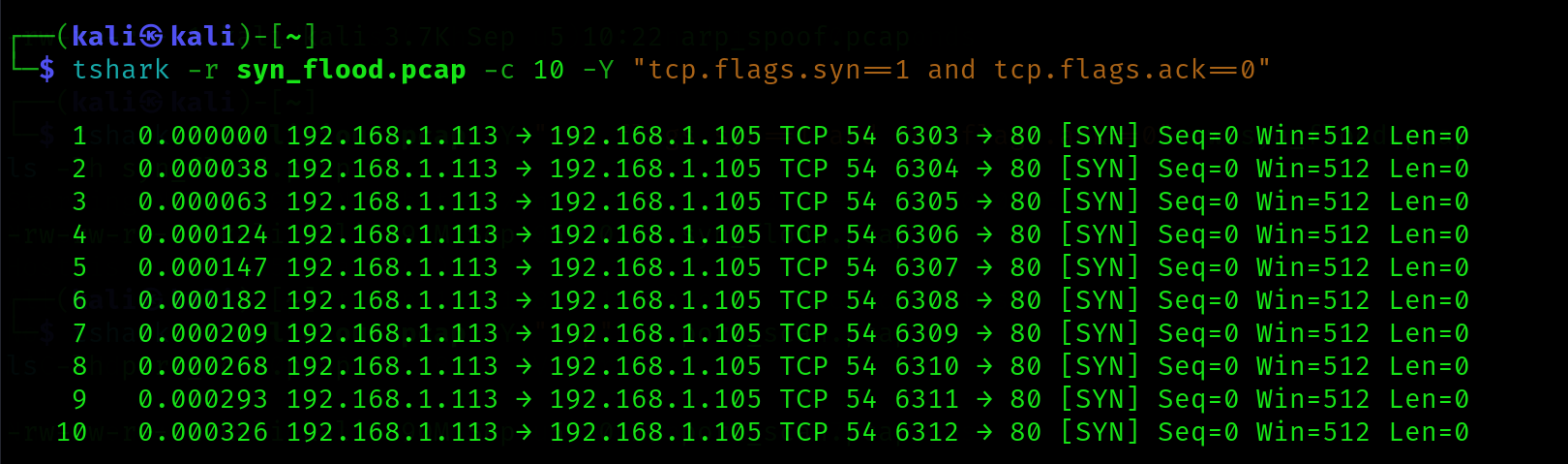
* Captured traffic for:
  + **ARP spoofing**
  + **SYN flood**
  + **Port scan**
* Stored attack .pcap files separately.



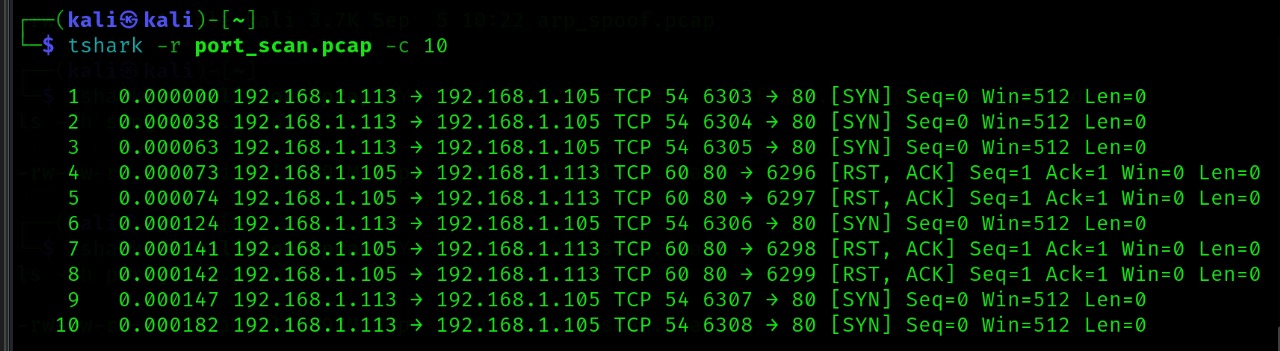
**ARP spoofing**



**SYN flood**



**Port scan**



### Dataset Structure

* ~/sdn\_dataset/pcaps/benign/
* ~/sdn\_dataset/pcaps/attacks/arp\_spoof/
* ~/sdn\_dataset/pcaps/attacks/syn\_flood/
* ~/sdn\_dataset/pcaps/attacks/port\_scan/

## 04 Observations

* Mininet topology successfully created and functional.
* ICMP traffic confirmed connectivity between hosts.
* Wireshark verified traffic capture.
* Dataset folders initialized for systematic storage of benign and attack traffic.
* Dual VM setup (Kali + Ubuntu) confirmed working with bridged networking.

## Appendix

### Useful Commands

# Mininet topology creation

sudo mn --topo single,3

# Ping test

h1 ping 10.0.0.2

# Capture traffic on host interface

h2 tcpdump -i h2-eth0 -w ~/sdn\_dataset/pcaps/benign/icmp\_ping.pcap &

### Notes

* All captures performed in an isolated lab environment.
* No real systems impacted.