

NETWORK INTRUSION DETECTION SYSTEM

Deepthi. I , Meera Vanathi M, Thavamitha AM
22011103010, 22011103028, 22011103060
Dr.S.Vidhusha



Protecting Your Network from Cyber Threats

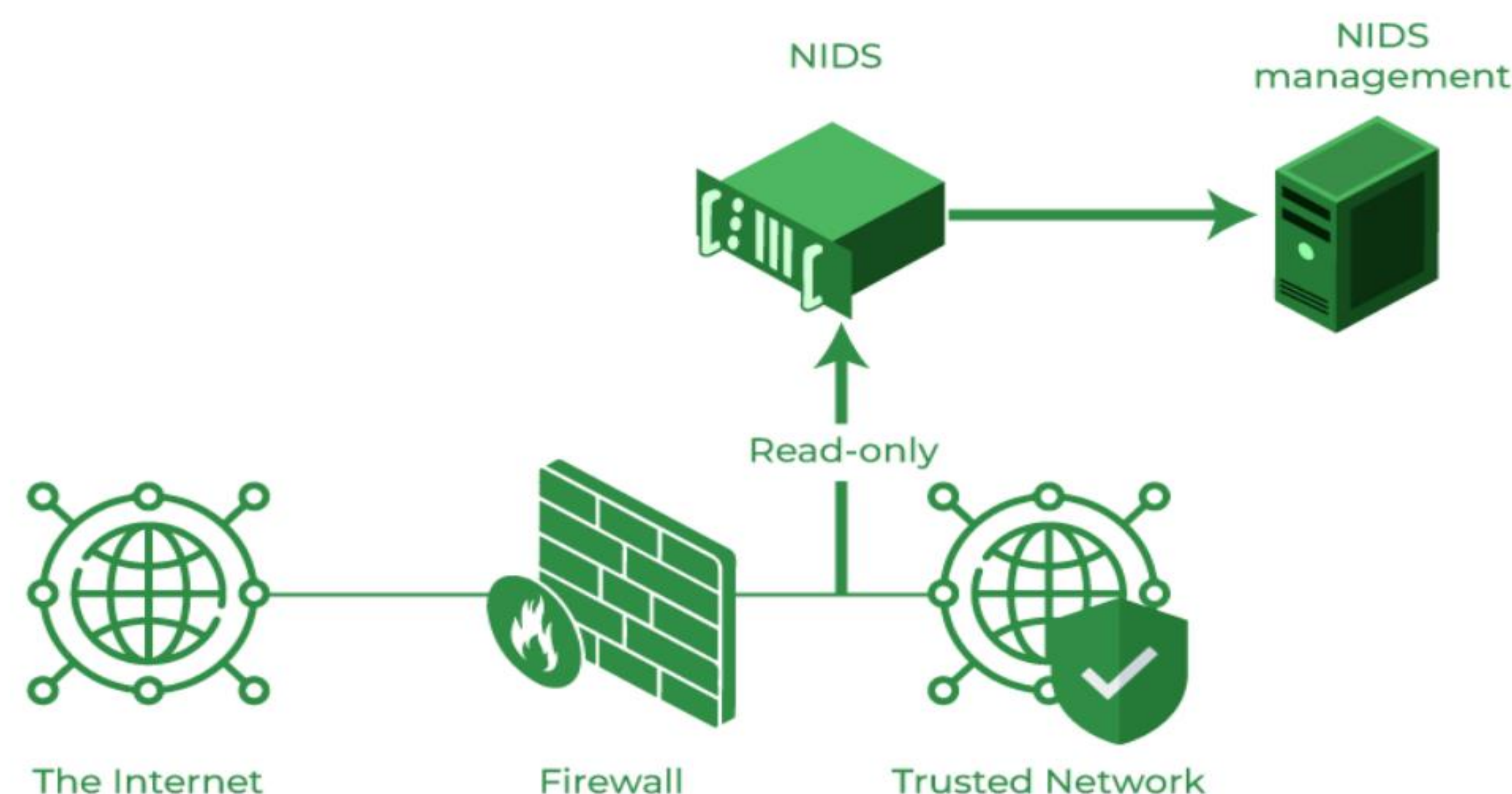
"We live in an age where security is the responsibility of all, not just a few."

Fortify your digital realm with our cutting-edge Network Intrusion Detection System (NIDS). It's your unwavering sentinel, protecting your data from hidden threats and elevating your network security to new heights. NIDS - your impenetrable shield in the cybersecurity battle.

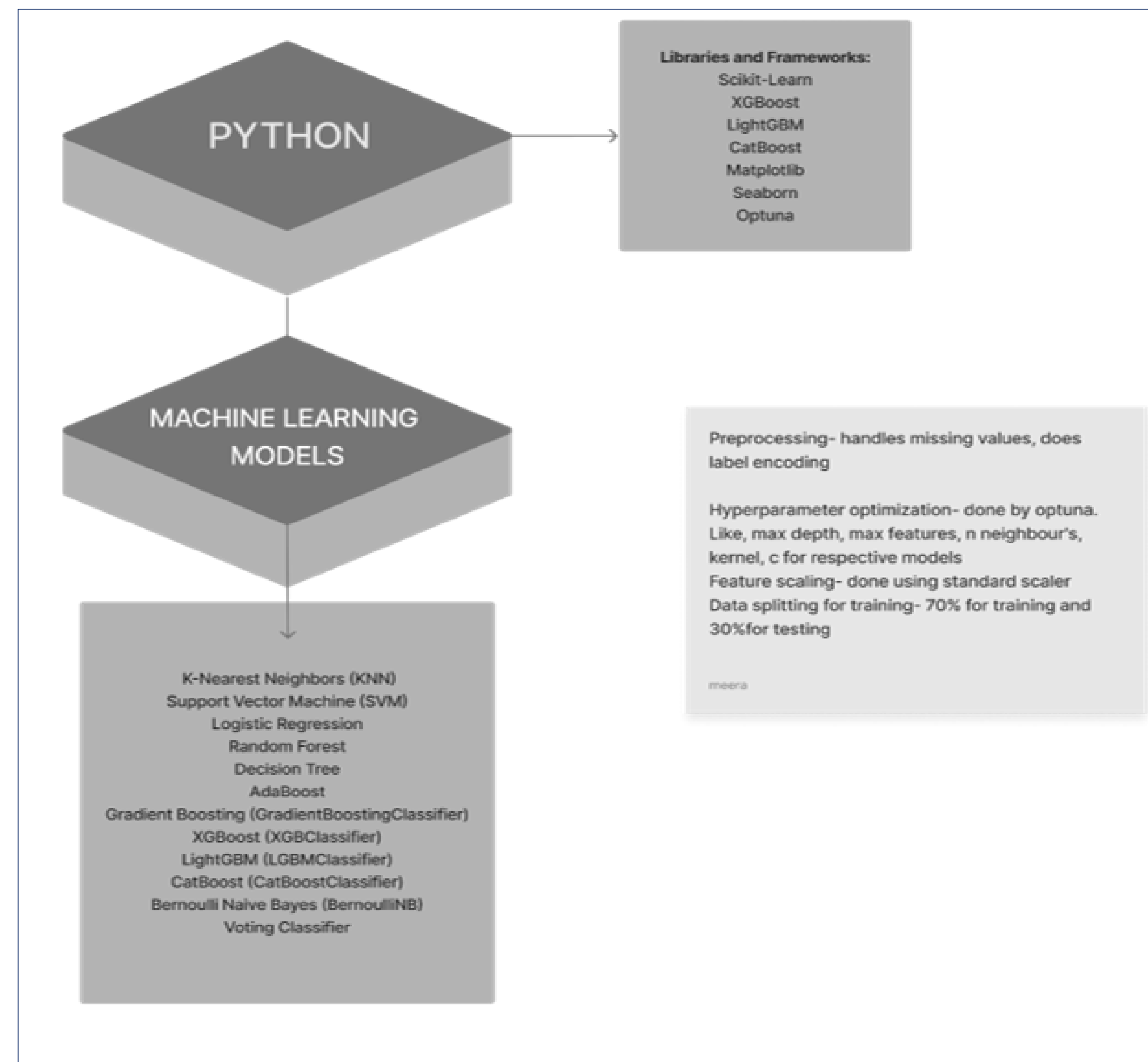
What is NIDS?

- A Network Intrusion Detection System (NIDS) is a crucial cybersecurity tool designed to monitor network traffic for suspicious activity and security threats.
- It acts as an extra layer of protection for your organization's digital assets.
- It differentiates malicious/anomaly network packets from every other usual packets.

NIDS: The Digital Guardian



Tech Stack



Data Collection

- IPsum: A threat intelligence feed comprised of 30+ publicly available lists of suspicious/malicious IP addresses. It ranks IPs by blacklist occurrences, reducing false positives in monitored traffic. Used in rule-based NIDS for enhanced security.
- For ml based NIDS, The dataset consists of a wide variety of intrusions simulated in a military network environment. It created an environment to acquire raw TCP/IP dump data for a network by simulating a typical US Air Force LAN. The LAN was focused like a real environment and blasted with multiple attacks.

Future Improvements

Zero Trust Security
IoT and Cloud Integration

Result And Conclusion

```
Start Capture Stop Capture
Packet 1 -
Source: 10.18.160.192 (Unknown)
Destination: 224.0.0.251 (mdns.mcast.net) - Protocol: UDP
Packet 2 -
Source: 10.18.168.56 (Unknown)
Destination: 224.0.0.251 (mdns.mcast.net) - Protocol: UDP
Packet 3 -
Source: 10.18.164.211 (Unknown)
Destination: 224.0.0.251 (mdns.mcast.net) - Protocol: UDP
Packet 4 -
Source: 10.18.173.92 (MSI)
Destination: 10.101.1.10 (Unknown) - Protocol: UDP
Packet 5 -
Source: 10.18.173.92 (MSI)
Destination: 10.101.1.10 (Unknown) - Protocol: UDP
Packet 6 -
Source: 10.18.218.165 (MAC-918308)
Destination: 239.255.255.250 (Unknown) - Protocol: UDP
Packet 7 -
Source: 10.18.224.234 (Unknown)
Destination: 239.255.255.250 (Unknown) - Protocol: UDP
Packet 8 -
Source: 10.18.159.72 (Unknown)
Destination: 255.255.255.255 (Unknown) - Protocol: UDP
Packet 9 -
Source: 10.18.159.72 (Unknown)
Destination: 255.255.255.255 (Unknown) - Protocol: UDP
```