INTRUSION DETECTION SYSTEM PROJECT REPORT

Data Communication & Network

Muhammad Faheem (42346)

Qalandar Shah (42687)

Daniyal Hussain (38233)

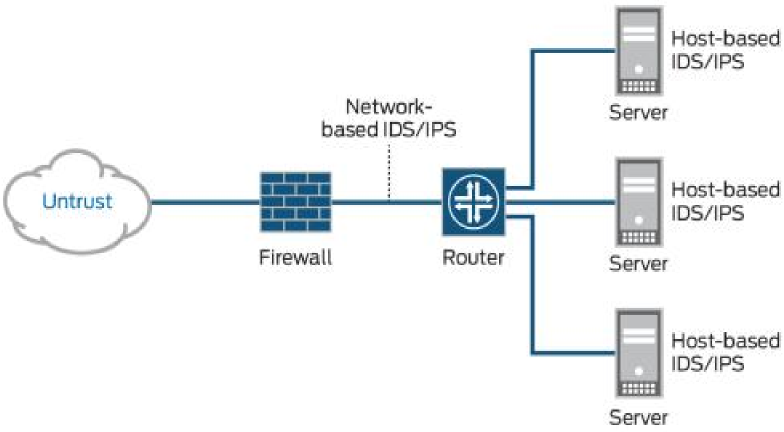
JUNE 15, 2025

IQRA UNIVERSITY
H-9 ISLAMABAD

Intrusion Detection System Project Report:

1. Introduction

With the rapid evolution of networking technologies and increased dependence on data communication networks (DCNs), ensuring network security has become a significant concern. An Intrusion Detection System (IDS) is a security mechanism designed to detect unauthorized access, abnormal traffic, and potential threats within a network. This project focuses on the development and understanding of an IDS tailored to the unique characteristics of DCNs.



2. Objective

The primary objectives of this project are:

- To study the fundamentals and importance of IDS in DCNs.
- To design a basic intrusion detection model using suitable algorithms.
- To detect common network attacks such as DoS, port scanning, spoofing, and brute force attacks.
- To simulate and evaluate the performance of the IDS.

2. Tools and Technologies Used

Tool / Technology	Purpose / Functionality
Cisco Packet Tracer	Network simulation and configuration of routers/switches
Command Line Interface (CLI)	Used to configure routers, apply IDS rules, and manage routing
SYSLOG Server	Logging and alert system for detected intrusions
HTTP Server	Web traffic simulation
FTP Server	File transfer service simulation
ICMP & Ping Tools	Network traffic generation for IDS testing
Dynamic Routing (RIP)	Enables automatic routing between networks
Securityk9 Package	Cisco IOS package for enabling IDS-related features on routers

3. Network Design / Project Description

Network Architecture

The project uses 3 networks interconnected using 3 Cisco 1941 routers and simulated with:

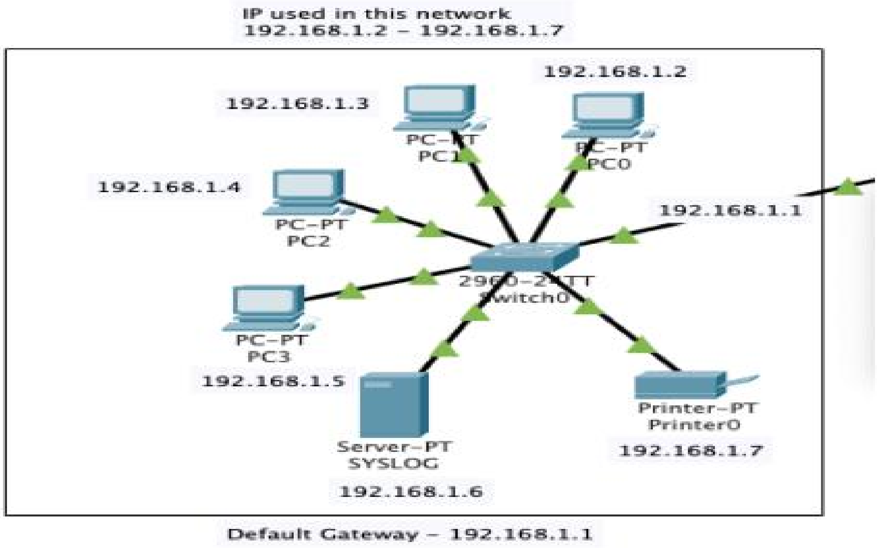
- SYSLOG server
- HTTP and FTP servers
- Multiple PCs, laptops, and printers

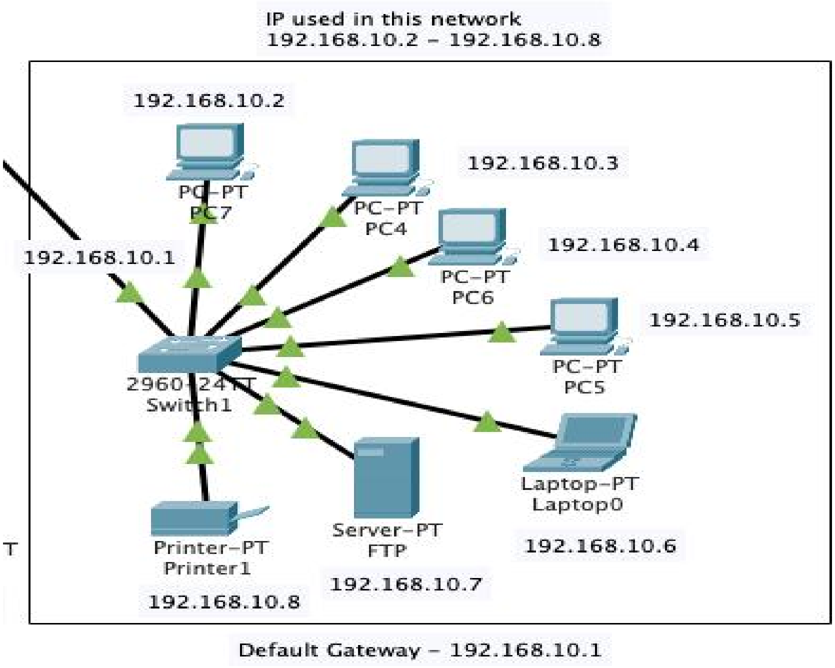
Each network was configured with:

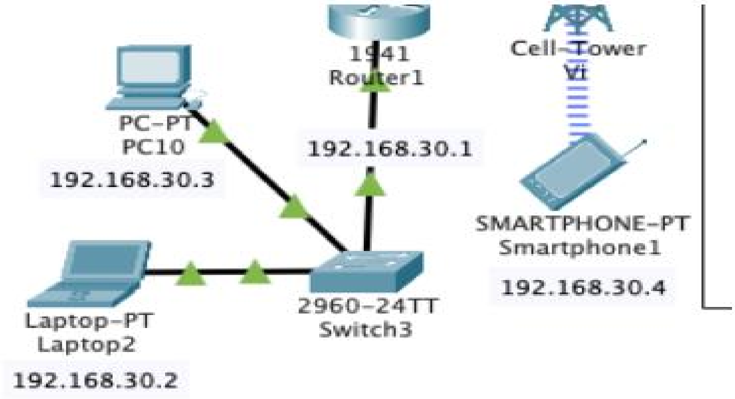
- IPv4 addressing
- Dynamic routing using RIP protocol
- Proper cabling (Straight-through and Serial DCE)

Software/Hardware

- Cisco Packet Tracer: for designing and simulating the network.
- Command Line Interface (CLI): for router configuration and IDS commands.







4. Implementation

Signature-Based Detection

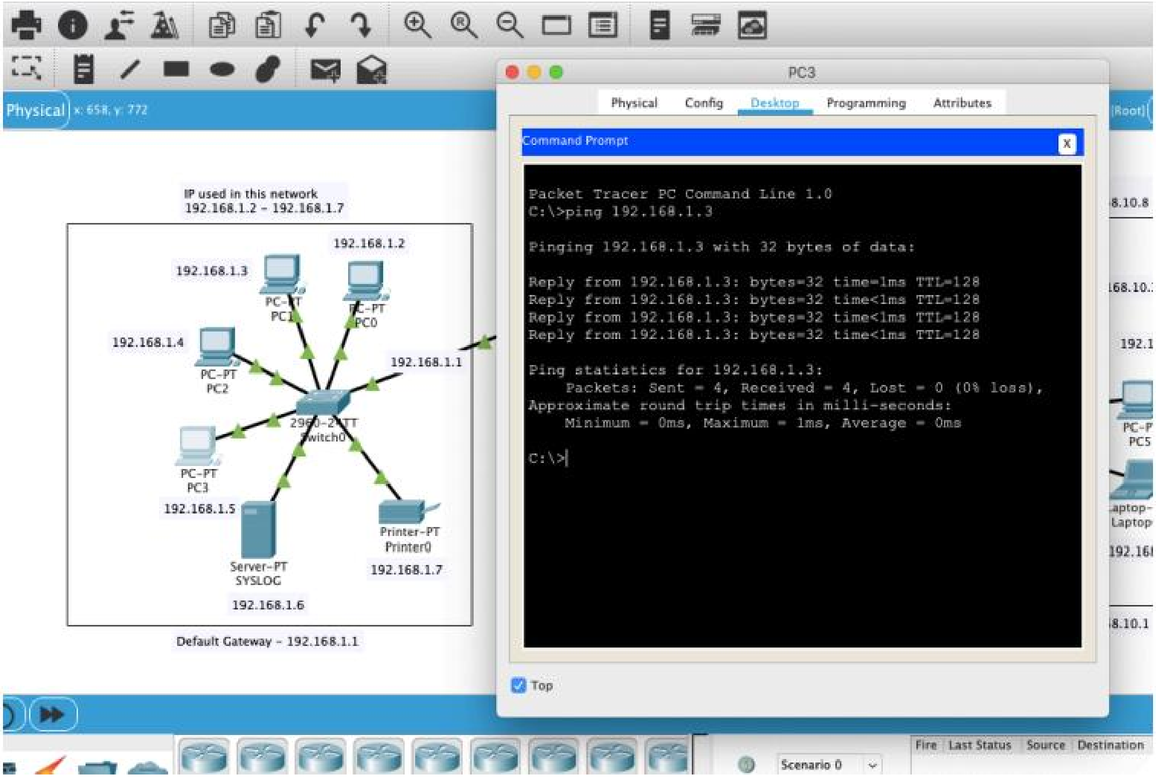
IDS was implemented on Router0, monitoring ICMP Echo Requests using Signature ID 2004. Only the detection and alerting action was configured (not prevention), distinguishing it from IPS.

Key Commands Used

- license boot module to enable securityk9.
- ip ips config location to define signature storage
- ip ips and ip ips signature-definition to define and enable detection rules
- logging host to send alerts to the SYSLOG server

Testing & Logging

- ICMP packets were sent across networks to simulate traffic.
- Detected malicious packets were logged in the SYSLOG server.
- FTP and HTTP servers were tested with custom configurations.



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

5. Challenges and Solutions

Challenges Encountered

- Initial IP configuration and routing issues.
- Configuration of services and servers.
- Understanding and applying complex CLI commands for IDS setup.

Future Enhancements

- Implementing Honeypot Systems.
- Integrating Intrusion Prevention System (IPS).
- Enhancing anomaly detection via machine learning.

6. Conclusion

This project successfully demonstrated the implementation of a Network-based Intrusion Detection System using Cisco Packet Tracer. It involved:

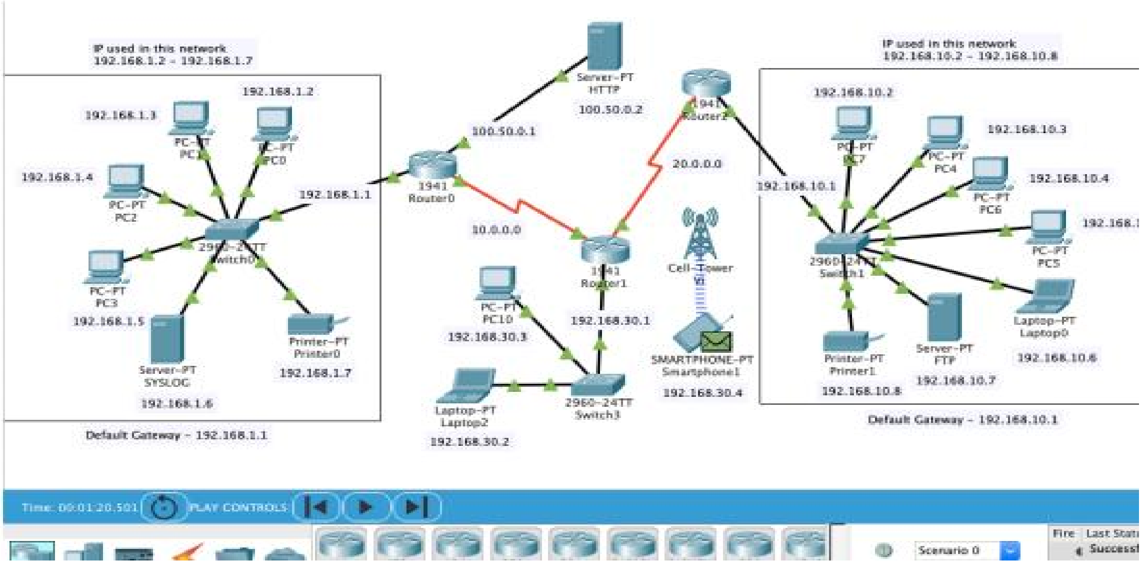
- Designing a network with 3 LANs.
- Configuring routers, servers, and hosts.
- Implementing and testing IDS with signature-based detection.

The project was a valuable learning experience in network security and Cisco-based configuration.

7. References

- Cisco Networking Academy. **"Introduction to Networks".**
- Checkpoint: What is an IDS?
- Intrusion Detection Taxonomy
- Books on signature-based and host-based IDS

Simulated Network Topology for IDS Implementation :



IP used in this network
192.168.1.2 - 192.168.1.7
192.168.1.3
PC-PT
PC1
192.168.1.2
PC-PT
PC0
192.168.1.4
PC-PT
PC2
192.168.1.1
2960-24TT
Switch0
PC-PT
PC3
192.168.1.5
Server-PT
SYSLOG
192.168.1.6
Printer-PT
Printer0
192.168.1.7
Default Gateway - 192.168.1.1
1941
Router0
100.50.0.1
Server-PT
HTTP
100.50.0.2
10.0.0.0
1941
Router1
1941
Router2
20.0.0.0
PC-PT
PC10
192.168.30.3
192.168.30.1
Laptop-PT
Laptop2
192.168.30.2
2960-24TT
Switch3
Cell-Tower
SMARTPHONE-PT
Smartphone1
192.168.30.4
IP used in this network
192.168.10.2 - 192.168.10.8
192.168.10.2
PC-PT
PC7
192.168.10.3
PC-PT
PC4
192.168.10.4
PC-PT
PC6
192.168.10.1
192.168.1
PC-PT
PC5
2960-24TT
Switch1
Printer-PT
Printer1
192.168.10.8
Server-PT
FTP
192.168.10.7
Laptop-PT
Laptop0
192.168.10.6
Default Gateway - 192.168.10.1
Time: 00:01:20.501
PLAY CONTROLS
Scenario 0
Fire
Last Stat
Successf