Design and Simulation of an Intrusion Detection System Using Cisco Packet Tracer

Aarathy R Babu
AM.EN.U4ECE22002
Department of Electronics and Communication Engineering
Amrita Vishwa Vidyapeetham, Amritapuri
am.en.u4ece22002@am.students.amrita.edu

Aswathi H S
AM.EN.U4ECE22010
Department of Electronics and Communication Engineering
Amrita Vishwa Vidyapeetham, Amritapuri
am.en.u4ece22010@am.students.amrita.edu

Harshit Kumar
AM.EN.U4ECE22017
Department of Electronics and Communication Engineering
Amrita Vishwa Vidyapeetham, Amritapuri
am.en.u4ece22017@am.students.amrita.edu

Sruthi Balakrishnan P
AM.EN.U4ECE22046
Department of Electronics and Communication Engineering
Amrita Vishwa Vidyapeetham, Amritapuri
am.en.u4ece22046@am.students.amrita.edu

Krishnapriya V B
AM.EN.U4ECE22052
Department of Electronics and Communication Engineering
Amrita Vishwa Vidyapeetham, Amritapuri
am.en.u4ece22052@am.students.amrita.edu

***Abstract*—This paper discusses the design and simulation of a Network-based Intrusion Detection System (NIDS) with the use of Cisco Packet Tracer. The main goal is to improve network security through the detection and reporting of unauthorized or malicious activities in real time. The simulation will have three interconnected LANs, each having PCs, servers, switches, and routers set up using dynamic routing protocols. The IDS is installed on the edge router, which makes it scan ICMP traffic and use pre-defined IPS signatures to identify anomalies. Identified events are written to a central Syslog server, allowing administrators to monitor potential threats without interfering with the network. The project illustrates the hands-on application of a lightweight IDS architecture on a virtual platform and focuses on packet inspection, signature setup, and alert management as key factors towards protecting contemporary digital networks. The project is a model for applying IDS on the real world and can further be modified to integrate intrusion prevention and sophisticated detection methods.**

I. Introduction

In the present scenario of a globalized world, cyber threats have become highly advanced in nature, creating a huge threat to networks and data systems. With organizations increasingly dependent on digital platforms, there is now a high demand for strong network monitoring and defense. An Intrusion Detection System (IDS) is a key security system that detects suspicious or unapproved activity within network traffic and alerts administrators in case of detection.

IDSs are broadly categorized as Host-based Intrusion Detection Systems (HIDS) and Network-based Intrusion Detection Systems (NIDS). HIDS works at the host level by monitoring a single machine, whereas NIDS works at the network level, observing traffic passing through routers and switches. This project aimed to develop a NIDS using Cisco Packet Tracer to mimic real-time monitoring in a multi-network scenario.

The system is capable of identifying possible intrusions like ICMP-based attacks with signature-based detection. The network layout includes several subnets that are routed through routers, with services such as HTTP, FTP, and SYSLOG spread across the network. The IDS is being set up on the router with Cisco IOS commands and is being combined with a Syslog server for logging security alerts. This configuration illustrates how fundamental networking concepts and simple security settings can be utilized to establish an early-warning defense system.

This project not only solidifies fundamental concepts of IP addressing, routing, and protocol setup but also covers practical elements of intrusion detection, security rule enforcement, and event logging to a central repository.

II. System Design and Architecture

The proposed Intrusion Detection System (IDS) is simulated in Cisco Packet Tracer to emulate a secure and monitored network environment. The overall design comprises three

interconnected local area networks (LANs), each containing multiple end devices and servers, with communication facilitated through Cisco routers and switches. The IDS is deployed on the edge of the primary network to analyze inbound traffic and detect potential threats using predefined signatures.

A. Network Topology Overview

The architecture includes:

- **Three LANs** with static IPv4 addressing schemes:
  - Network 1: 192.168.1.0/24
  - Network 2: 192.168.10.0/24
  - Network 3: 192.168.30.0/24
- **Three Cisco 1941 routers** are used to interconnect the LANs via serial and Ethernet interfaces.
- **Layer-2 switches** facilitate intra-network communication.
- **Servers** for Syslog, HTTP, and FTP functions are strategically placed in the network.

Each router interface and device is manually configured to ensure deterministic communication across the network.

B. Key Devices and Roles

- **PCs and Laptops:** Simulate client and user endpoints.
- **SYSLOG Server:** Collects and logs IDS alerts for administrative review.
- **HTTP Server:** Hosts a sample webpage accessible via the network.
- **FTP Server:** Enables file transfer services using credentials.
- **Routers:** Perform inter-network routing and host the IDS configuration.
- **Switches:** Connect local devices within each subnet.

C. IP Addressing and Routing

Static IP addresses are assigned to all devices to ensure consistent identification and routing paths. Dynamic routing protocols are configured between routers to automate inter-network communication. The addressing scheme includes both Class A and Class C addresses for internal and router-to-router communication.

D. Intrusion Detection Configuration

The IDS is implemented on Router 0 by enabling Cisco's `securityk9` feature set and applying signature-based rules. Key configurations include:

- **IPS Signature ID 2004** for detecting ICMP Echo Requests (ping).
- Activation of **logging mechanisms** to forward alerts to the SYSLOG server.
- Use of **signature definition commands** to enable and monitor specific types of traffic.

This architecture ensures that all ICMP traffic entering Network 1 through Router 0 is inspected, and suspicious activity is logged centrally.

E. Cables and Interfaces

- **Straight-through cables** connect PCs, servers, and switches.
- **Serial DCE cables** connect routers using Serial interfaces for WAN simulation.

Proper interface configuration and clock rate settings are ensured for seamless communication.

This system architecture provides a secure and observable environment suitable for studying the behavior of an IDS and how it interacts with real-time network traffic in a simulated setup.

III. Implementation

The implementation phase involves setting up the network topology, configuring IP addresses, enabling routing protocols, and deploying the Intrusion Detection System (IDS) using Cisco IOS commands. The project is executed in Cisco Packet Tracer, a versatile network simulation tool that allows configuration, testing, and visualization of traffic flow across the network.

A. Network Topology Setup

The topology consists of three local networks connected via routers, with devices placed and interconnected as follows:

- End devices (PCs, laptops) are connected to switches using **copper straight-through cables**.
- Switches are connected to routers through Ethernet ports.
- Routers are interconnected via **serial DCE cables** to simulate wide area links.

Each network includes a specific set of devices:

- **Network 1:** Four PCs, a Syslog server, a printer, and a switch.
- **Network 2:** Four PCs, an FTP server, a laptop, and a printer.
- **Network 3:** A PC, a laptop, and a switch.

B. IP Address and Routing Configuration

Each device is assigned a static IP address within its subnet. The router interfaces are configured with matching IP addresses and subnet masks. Dynamic routing is enabled using protocols like **RIP or EIGRP** to ensure automatic route propagation between the routers.

Sample configuration steps:

```
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 no shutdown

router rip
 network 192.168.0.0
 network 10.0.0.0
```

C. Server Configuration

- **Syslog Server:** All services except the `SYSLOG` service are disabled to focus on logging incoming alerts from the IDS.
- **HTTP Server:** A custom webpage is hosted and accessible from any client in the network using the server IP `100.50.0.2`.
- **FTP Server:** An FTP account is created with username `harsh` and password `123`, enabling file transfers within the network.

D. IDS Deployment on Router

The IDS is deployed on **Router 0** (interface GigabitEthernet 0/0) to monitor incoming ICMP traffic. The Cisco IOS `securityk9` feature set is activated to enable IDS functionality. Signature-based detection is implemented using IPS rule configuration.

Key command sequence:

```
license boot module
c1900 technology-package securityk9
reload
mkdir flash:ids
ip ips config location flash:ids
ip ips IDS_RULE
interface g0/0
 ip ips IDS_RULE out
 logging host 192.168.1.4
```

The **ICMP Echo Request signature (ID 2004)** is enabled to detect ping-based traffic. The IDS generates alerts for any matching traffic and forwards logs to the Syslog server.

E. Testing and Verification

Connectivity is validated using `ping` tests between devices in different networks. IDS functionality is tested by simulating ICMP traffic from external networks. The alerts generated are verified at the Syslog server. Additional simulation tools within Packet Tracer are used to trace packet flow and analyze detection efficiency.

This implementation successfully integrates core networking concepts with basic intrusion detection functionality, simulating a secure and monitored network scenario in a controlled environment.

IV. Device Configuration

Each device in the network was manually configured with a static IPv4 address appropriate to its respective subnet. This approach ensured consistent addressing, simplified routing, and made it easier to monitor and track traffic for intrusion detection.

A. IP Addressing Scheme

Devices in each network were assigned IPs from distinct private address ranges:

- **Network 1 (192.168.1.0/24)**
  - PC1: 192.168.1.2
  - SYSLOG Server: 192.168.1.4
  - Default Gateway: 192.168.1.1
- **Network 2 (192.168.10.0/24)**
  - FTP Server: 192.168.10.2
  - PC5: 192.168.10.3
  - Default Gateway: 192.168.10.1
- **Network 3 (192.168.30.0/24)**
  - Laptop: 192.168.30.2
  - PC: 192.168.30.3
  - Default Gateway: 192.168.30.1

Other router-to-router interfaces used Class A addresses (e.g., 10.0.0.0, 20.0.0.0) to facilitate backbone communication between the three networks.

B. Server Setup

- The **Syslog server** was configured to only run logging services and collect alerts generated by the IDS.
- The **HTTP server** was assigned IP `100.50.0.2` and hosted a sample webpage.
- The **FTP server** was set up with basic credentials (username: `harsh`, password: `123`) and allowed file upload/download within the network.

C. Router Interface Configuration

Router interfaces were manually assigned IPs matching their respective networks. Dynamic routing was enabled to support seamless communication between networks. Each router interface was named and enabled accordingly, ensuring all connected networks could communicate through intermediate paths.

D. Addressing Policy

To maintain clarity and ease of administration:

- Each subnet had its own default gateway on the router.
- IP addresses were assigned sequentially.
- Subnet masks were consistently set to `255.255.255.0`.

This structured addressing and configuration enabled effective routing, simplified monitoring, and accurate packet inspection for the IDS system.

V. Results and Observatio

The Intrusion Detection System (IDS) simulated in Cisco Packet Tracer was considered a success and confirmed that not only did the networks function properly and communicate across all three networks, also, the IDS operated correctly. The original testing of the networks was based on the use of ICMP pinging the devices, which verified that they were communicating across each configured network, and those that were intended to communicate could be found. All hosts and servers replied as they ought to, verifying appropriate IP addressing and dynamic routing were functional between subnets. The configuration of the IDS was done on Router 0, and if it detected an event, it generated an alert based on the signature defined in its configuration. ICMP Echo Requests

were sent to each host and server, which generated alerts from the IDS, the signature (ID 2004) relied on to generate alerts was correctly forwarded to the Syslog server. The IDS was able to detect suspicious traffic and generate alerts, this was performed in the successful operation of the IDS as expected and to determine it did indeed truly detect and report traffic once again within the expectations of a detection-based system (not blocking it). The Syslog server recorded the alerts in near real-time with their corresponding message detail, the provided logs clearly presented the alerts to the administrator, and the alerts from the Syslog server were sufficient detail to be of use to the administrators. The next successful step was to test the IDS and network by extending the network with a broader range of devices and to verify the IDS operated without issues successfully. The IDS was confirmatively successful in the above tests and continued to operate without reported issues and its continued detection of intrusions was confirmed as well without any degradation of performance on the devices and the service they provided. The next logical test was to show simulated link failure of a number of devices and show a negotiated device failure, showing that there was continued detection of Ingress traffic from the subjective view of the system, and equally continued connectivity, should links, or devices fail, by means of the successful negotiation provided by dynamic routing. In summary, this simulation was able to successfully provide the administrator a working example of how effective and useful a basic signature-based IDS can provide to their multi-network devices.

VI. Conclusion

This project was able to successfully illustrate the design and simulation of a Network-based Intrusion Detection System (NIDS) via Cisco Packet Tracer. Through the setup of a multi-network environment made up of routers, switches, end devices, and servers, the system was capable of successfully monitoring and detecting anomalous network activity, in this case ICMP-based traffic. The IDS was configured through signature-based detection rules and shared with a Syslog server for consolidated alert logging. With different tests, the system showed consistent connectivity, correct alert generation, and solid scalability. Although the IDS was restricted to detection and logging, the project gave a solid foundation in understanding fundamental concepts of networking and security. The implementation shows how simulation tools can be applied for prototyping security solutions in the virtual space. Future developments can involve the incorporation of intrusion prevention capabilities (IPS), anomaly-based detection, and cloud-based log inspection to build a more comprehensive and intelligent security infrastructure.