****

**Computer Networks Project Proposal**

**SecureNet: Intrusion Detection System Implementation using Cisco Packet Tracer**

**Group Members:**

* Muhammad Talha Bilal (K21-3349)
* Ahmed Ali (K21-3212)
* Muhammad Taha Hassan (K21-4680)

**Objective:**

The objective of this project is to design and implement an Intrusion Detection System (IDS) using Cisco Packet Tracer. The IDS will monitor network traffic, detect suspicious activities or potential security breaches, and provide alerts to network administrators, enhancing the overall security posture of the network infrastructure.

**Introduction:**

In today's interconnected world, network security is of paramount importance to protect sensitive data and maintain the integrity of systems. An Intrusion Detection System (IDS) plays a critical role in identifying and responding to unauthorized access attempts, malicious activities, and other security threats. With the increasing complexity of cyber threats, having an effective IDS is essential for safeguarding network assets and maintaining operational continuity.

**Description:**

The project will involve configuring and simulating an IDS using Cisco Packet Tracer, a powerful network simulation tool. The IDS will analyze network traffic in real-time, employing various detection techniques to identify suspicious patterns or anomalies. Upon detection of potential intrusions, the IDS will generate alerts and notifications, enabling network administrators to take timely action to mitigate security risks.

Key features of the IDS include:

1. Network Traffic Monitoring: Continuous monitoring of network traffic to detect abnormal behavior and potential security breaches.
2. Signature-Based Detection: Utilizing signature-based detection techniques to identify known patterns of malicious activity, such as malware or denial-of-service attacks.
3. Anomaly-Based Detection: Employing anomaly-based detection algorithms to identify deviations from normal network behavior, indicating potential intrusions or unauthorized access attempts.
4. Alerting Mechanism: Generating alerts and notifications for detected intrusions, providing relevant information to facilitate incident response and mitigation efforts.
5. Integration with Cisco Devices: Seamless integration with Cisco networking devices, allowing for efficient deployment and management within Cisco-based network infrastructures.

**Network Topology:**

The network topology will consist of the following components:

* Client Devices: Representing end-user devices connected to the network, such as computers, laptops, and mobile devices.
* Cisco Routers and Switches: Serving as the network infrastructure components through which traffic flows, providing connectivity and routing capabilities.
* Intrusion Detection System (IDS): Deployed strategically within the network to monitor and analyze traffic for potential security threats.
* Server: Hosting critical applications and services accessed by network users.

**Conclusion:**

By implementing an Intrusion Detection System on Cisco Packet Tracer, we aim to enhance the security posture of network infrastructures by proactively identifying and responding to security threats. The project leverages the capabilities of Cisco Packet Tracer to simulate real-world network environments and test the effectiveness of the IDS in detecting and mitigating various types of intrusions. Through this project, we seek to empower network administrators with a powerful tool to safeguard their networks against evolving cyber threats.

Thank you for considering this project proposal. We are eager to receive your feedback and collaborate on the successful execution of this project.