CyberDojo

THE SCHOOL OF CYBERDEFENSE

SRI SRI UNIVERSITY

PROBLEM STATEMENTS

Date – 11th January 2024

Confidential Document

Attention : This document contains confidential and privileged information for the intended recipient only. Any unauthorized disclosure, copying or distribution is prohibited. By accepting this document, you agree to maintain its confidentiality.

BTech – Semester 4 – Problem Statements

G 1. Hospital Network

Problem Statement:

Design and implement a secure and efficient network for a multi-specialty hospital. The network must interconnect departments like Emergency, Radiology, Pharmacy, and Administration. It should support:

- Secure data sharing between doctors and staff.
- VLAN segmentation to isolate sensitive medical records and IoT devices (e.g., patient monitors).
- Redundant paths for critical system uptime and disaster recovery.

Challenge: Ensure HIPAA compliance by implementing access control lists (ACLs), secure remote access for telemedicine, and robust network monitoring.

G 2. Bank Network

Problem Statement:

Build a highly secure network for a bank's headquarters and branches. The network must support:

- Encrypted communication for financial transactions between branches and the central server.
- VLANs to segment departments like Customer Service, Loans, and IT Operations.
- Implementation of a DMZ for hosting public-facing applications like online banking.

Challenge: Design robust failover mechanisms and firewall configurations to ensure 24/7 availability and prevent unauthorized access.

G 3. Manufacturing Network

Problem Statement:

Develop a scalable network for a manufacturing plant, integrating different units like Assembly, Quality Control, Logistics, and Administration. The network must support:

- Seamless communication between production lines and inventory systems.
- VLAN segmentation for secure communication between IoT devices, SCADA systems, and enterprise networks.
- Real-time monitoring to detect and respond to network issues without disrupting operations.

Challenge: Ensure high availability and protection against industrial cyber threats targeting OT systems.

G 4. University Network

Problem Statement:

Design a robust network for a university campus that connects departments, hostels, libraries, and administrative offices. The network must:

- Provide high-speed internet for students and faculty.
- Implement VLANs for department-based segmentation.
- Include a centralized authentication server for Wi-Fi access control.

Challenge: Incorporate scalable solutions to accommodate future growth, such as new buildings and users, while ensuring security against external threats.

G 5. Government and Defense Network

Problem Statement:

Create a secure and mission-critical network for a government agency with defense units. The network should support:

- Interconnection between departments such as Intelligence, Operations, and Public Relations.
- Data encryption for sensitive communication.
- Redundancy and failover mechanisms to ensure zero downtime during emergencies.

Challenge: Ensure compliance with strict government security standards while implementing network segmentation and real-time threat monitoring.

G 6. Oil and Gas Network

Problem Statement:

Design a resilient network for an oil and gas company, connecting their headquarters, refineries, and exploration sites. The network must:

- Enable communication between remote sites and centralized control systems.
- Segment and protect critical OT devices managing pipeline operations.
- Incorporate satellite links for remote and offshore sites.

Challenge: Address the unique challenges of latency in remote communication and implement security protocols to defend against industrial cyber threats.

G 7. Media Outlet Network

Problem Statement:

Build a network for a media outlet connecting their newsroom, editing studios, and broadcasting servers. The network must:

- Ensure seamless streaming of live content.
- Isolate different teams (e.g., editors, reporters, and broadcasting) using VLANs.
- Support cloud-based storage and retrieval of archived media files.

Challenge: Implement QoS to prioritize streaming traffic and maintain uninterrupted live broadcasts during peak network usage.

G 8. Airport Network

Problem Statement:

Develop a secure and efficient network for an international airport. The network must:

- Connect terminals, air traffic control, baggage handling systems, and administrative offices.
- Implement VLANs to segregate passenger Wi-Fi from operational systems.
- Ensure real-time data flow for flight information systems.

Challenge: Design a highly redundant network to ensure zero downtime for critical systems like air traffic control and flight tracking.

G 9. Retail Platform - E-Commerce Network

Problem Statement:

Create a network for an e-commerce platform, integrating their data center, warehouses, and customer service units. The network must:

- Support secure online transactions.
- Use a DMZ for public-facing applications like the e-commerce website and payment gateway.
- Segment the internal network for secure communication between inventory systems, sales teams, and IT.

Challenge: Implement redundancy to handle high traffic during peak sales events and ensure PCI-DSS compliance for payment security.

BTech – Semester 6 – Project Mentor Allocation

G 1 - SIEM Implementation & Use Cases

Implement a SIEM solution in a lab environment or for a small business. Configure log sources, correlation rules, and incident response procedures. Design and implement specific SIEM use cases using Splunk to detect and respond to common security threats, such as brute force attacks, malware infections, or unauthorized access.

G 2 - Automated Cyber Security Incident Triage

Develop an automated incident triage system that analyzes incoming alerts, categorizes them, and prioritizes them based on severity and potential impact

G 3 - Security Orchestration & Automation Response

Developing security orchestration and automation workflows using tools like SOAR platforms. These workflows should streamline incident response processes and improve efficiency.

G 4 - Cyber Security Metrics & Dashboard

Develop a cybersecurity metrics framework and a real-time dashboard for tracking key security performance indicators (KPIs) within an organization

BTech – Semester 8 – Project Mentor Allocation

G 1 - Advanced Active directory Defense and attack

Objective: Simulate and secure an enterprise-grade Active Directory (AD) setup.

Key Tasks:

- Red Team:
  - Perform reconnaissance using tools like BloodHound and ADRecon.
  - Execute attacks like Golden Ticket, DCShadow, or DCSync.
- Blue Team:
  - Harden AD security with least privilege principles and secure SPN configurations.
  - Monitor attack patterns using Sysmon and Splunk.
- Set up alerts for critical AD events (e.g., Event ID 4768 for Kerberos tickets).

G 2 - Automated Incident Response with SOAR Platform

Objective: Develop workflows for automating incident response using SOAR tools.

Key Tasks:

- Create automated playbooks for:
  - Malware detection and isolation.
  - Phishing email analysis and blocking.
  - Privileged account anomaly detection & many more
- Integrate APIs of tools like Shuffle, SentinelOne, or Wazuh for streamlined response.
- Simulate incidents and measure response times.

Outcome: Fully operational workflows and a comparative analysis of manual vs. automated response.

G 3 – Web Application Threat Simulation and WAF Configuration

Objective: Simulate real-world web application attacks and enhance security using a Web Application Firewall (WAF).

Key Tasks:

- Red Team:
  - Launch common OWASP Top 10 attacks (e.g., SQL Injection, XSS, Command Injection) against a vulnerable web application (e.g., DVWA, Juice Shop).
- Blue Team:
  - Set up and configure a WAF (e.g., ModSecurity, AWS WAF).
  - Create custom rules to detect and block simulated attacks.
  - Monitor and log traffic to identify anomalies and attack patterns.

Outcome: A secure web application with tailored WAF rules and incident response documentation.

G 4 - Threat Hunting and Malware Analysis in a simulated environment

Objective: Create a threat-hunting framework to detect and analyze malware in a controlled lab setup.

Key Tasks:

- Red Team:
  - Deploy a malware sample (e.g., ransomware or trojans) in a sandboxed lab environment.
  - Observe its behavior using tools like Procmon or Cuckoo Sandbox.
- Blue Team:
  - Use threat-hunting tools (e.g., Elastic SIEM, Splunk) to detect IOCs like file changes, registry modifications, or suspicious network traffic.
  - Develop response mechanisms to isolate and remediate malware infections.

Outcome: A threat-hunting guide with identified IOCs and steps for malware containment.