IT417 Management of Information Security
Project Report and Presentation
Network Infrastructure Design

Design a secure network for the Strome College of Business. Assume the domain is SCB.odu.edu. It has three (3) wired subnets (labs, classrooms, faculty offices) with no more than 200 computers in each subnet, two domain controllers, NAS, and web server. Assume private IP addresses are used in the internal network. Knowing the layout of Constant Hall, assume all labs and classrooms are on the first floor and all faculty offices are on the same floor. Placement and choice of switches and routers will be your decision. Design a network infrastructure that primarily uses Microsoft Windows and Cisco products incorporating all the material covered in the course. You may choose other enterprise products based on your requirement

Specifically, provide a written report describing the existing and recommended network infrastructure focusing on the security blueprint. The report must be at least 25 pages (single line spacing) excluding the Title page, table of contents, bibliography, diagrams, and specifications.

You may create this report in Microsoft Word but **must submit as a PDF file.** Be sure to **include the names of all team members on the title page along with each member's contribution.**

Your report must have:

1. Title page
2. Table of contents
3. Your write-up must contain the following:
    a. Introduction to the problem with your mission statement and your explanation of how you intend to setup the network. Provide details including domain controllers, file servers, routers, switches, etc. in the introduction as well as in a network diagram.
    b. Describe each of the measures you have taken to provide information security covering
        i. Possible threats and attacks faced by the network
        ii. Planning, organization, risk analysis, and policies
            1. Create a threat-vulnerability-asset worksheet and assess the risk with the existing controls
        iii. Any measures you may take to ensure confidentiality and authenticity including encryption and VPNs. Be specific and justify its use/need.
        iv. Access control policies and implementation
        v. Firewalls policies and implementation
        vi. Intrusion detection systems policies and implementation
        vii. Host hardening including update policies and implementation
        viii. Security for software/applications (including web based) commonly used in a university environment including policies, configurations, and what and who may install software
        ix. Data protection measures including policies, technology, backup storage locations, and restoration/recovery measures.
        x. Assess the risk with the updated controls and cost benefit analysis
        xi. Incident response plans, disaster recovery plans
4. Bibliography

5. Specifications on all the appliances/software you are recommending in the above implementation

Each group may consist of a max of three members.