530 PROJECT PROPOSAL

<Cybersafe: A Network Security Workshop>

<Rajesh Sharma Indrakanti, Raksha Ravindra Deshpande>

<Fall 2023>

PROJECT DESCRIPTION

<The project aims to develop an interactive-based demonstration on the network security and TCP/IP network model. That assists in the fundamental concepts of network security among the target audience. The project will involve a workshop which includes TCP/IP and OSI differences, how packet travels from one router to another, demonstration on Buffer flow using Kali Linux. The project significance lies in addressing the challenges of networks security awareness and knowledge It reduces the possibility of security breaches and accidents by helping people establish a solid foundation in network safety practices through the review and reteaching of key concepts. The targeted category, "Reteaching," is an excellent fit for the objectives of reiterating key information, enabling people to make knowledgeable decisions about network security, and eventually improving an organization's or individual's overall security posture. Because the project's material will be easily understood, it can be completed in the allotted time.>

TARGET AUDIENCE

<Beginners with little to no networking experience>

AUDIENCE SKILL LEVEL

<Basics of networking>

LEARNING OBJECTIVES

After a participant views or interacts with the project, they should be able to …

Objective 1 – <Security Fundamentals>
Objective 2 – <Understand Network Threats >
Objective 3 – <Security Awareness >

RELEVANCE OF TOPIC

<Certainly, an in-depth understanding of the TCP/IP network model, network layers, and issues covered in the network security course is necessary to ensure that the networking basics workshop is successful. The application, transport, network, and data connection layers of the TCP/IP paradigm serve as the basis for networking theory and the methods used to transfer data across networks. In this workshop we will discuss

regarding the layers, TCP/IP and OSI differences we will mainly concentrate on the security awareness that should be given to the audience and spread the awareness which is the most important when it comes to network security. The course goals are well aligned with participant ability to use best practices to improve network security and better understand the significance of these concepts to network security.>

Research and Supporting Materials

<Introduction to Network Security – Douglas Jacobson. Web Application Vulnerabilities – Steven Palmer>

Already enrolled in Professor Jacobson's 530 course, all that remains is to review the textbook and access online tutorials in order to gain a deeper understanding of the demonstration of network attacks and vulnerabilities.

Required resources

Target audience, a small classroom, power point for the presentation, Kali Linux tool, word document for the report, YouTube

References

[1]. < Grubb, S. (2021). How cybersecurity really works: A Hands-On Guide for Total Beginners. National Geographic Books.>

[2]. < Palmer, S. (2011). Web application vulnerabilities: Detect, Exploit, Prevent. Elsevier. >

Project Timeline

< Week 1: Specify the goals of the workshop, the intended audience, and the learning objectives. An area equipped with the amenities needed Prepare the content outline and workshop agenda.

Week 2: Develop workshop materials in week two, including exercises, presentations, and hands-on activities. necessary setup of the tools. Documents to support the argument. Set a final time and agenda for the workshop.

Week3: Gather the necessary supplies and tools for the classroom carrying out the workshop. Make sure the workshop's audience is engaged. Promote group activities and practical experience.

Week 4: Get audience input on how the workshop was delivered. fulfillment of learning goals. Answer the audience's questions. Forward the audience the information and resources for follow-up.

Task Dependencies & Potential Issues

<Venue Availability, Technical Issues, Low registration Numbers.>

Expected Outcomes, Evaluation, and Assessment

< The anticipated outcomes would be Improved comprehension, practical abilities, threat awareness, and tool efficiency. Materials that we give will be evaluated and assessed, and comments will be provided. >

Personal Learning Goals

<after this workshop, our initial objective would be to enhance our understanding of fundamental security concepts and gain practical experience in the field. Additionally, our interaction and communication abilities would be enhanced. In addition, we would increase our understanding of current security trends and threats.>