Project Part 1: Network Survey

Purpose

This project provides you an opportunity to solve a comprehensive problem in firewall and VPN implementation at various levels. You will play the role of an employee participating in the network security update planning process in a specific business situation.

Required Source Information and Tools

The following tools and resources will be needed to complete this project:

- A Web browser and access to the Internet to perform research for the project
- Access to the NetWitness Investigator application
- Packet trace files, vulnerability scans, and associated reports (provided by your instructor via email during Unit 1)
  - general_comm.pcap
  - encrypted_comm.pcap
  - nmap_scan.xml
  - topology_fisheye_chart.pdf
  - nessus_report.html

Learning Objectives and Outcomes

- You will be able to apply core competencies learned throughout the course to a single project.
- You will be able to analyze and apply knowledge of firewalls, VPNs, network diagrams, and defense measures.
- You will be able to demonstrate logical reasoning and decision-making skills.

Deliverables

The project is divided into two smaller assignments and one major assignment. Details for each deliverable can be found in this document. Refer to the course Syllabus for submission dates.

Project Part 1: Network Survey

Introduction

Network defenses rely first on understanding the current configuration of hosts, services, and protocols in use within the organization. Before it is possible to plan to change anything, you must first understand what is present and where it is located within the network. The initial phase of any network security realignment process involves identifying existing resources.

Scenario

You have been working as a technology associate in the information systems department at Corporation Techs. The Corporation Techs' management is concerned that they are losing business to a competitor whose bids are too accurately just under the bids offered by Corporation Techs—by an exact amount. A security firm was contracted to conduct a review of Corporation Techs' systems, identifying unauthorized access to the Web server as a potential source of compromise due to the shared reporting and public Web site functions. The packet trace and vulnerability scans gathered during this review are available for your use.

The Web server provides public access to the organization's static Web site for contact information, while sales team members in the field transfer contract and bid documents using a site secured with a logon and password. Corporation Techs has budgeted for new networking hardware but does not want to add additional servers due to cooling issues. Your manager has asked you to create a security plan that will prevent unauthorized access, while making sure that both public and secured Web access remain available.

Tasks

The data and information you need to complete this part of the project are provided to you. (See the Required Source Information and Tools section at the beginning of this document.) In this part of the project, you need to conduct a survey of the existing hosts, services, and protocols within Corporation Techs' network. Specifically, you need to:

1. Access the PCAP data using NetWitness Investigator.
2. Identify hosts within the Corporation Techs’ network.
3. Identify protocols in use within the Corporation Techs’ network.
4. Develop a list of hosts and services provided by each.
5. Create a professional report detailing the information above as the initial document for development of the network security plan.

Write the network survey results as detailed in the instructions above.

Place your report in the assigned Dropbox to be graded

Evaluation Criteria and Rubrics for this assignment

Evaluation Parameters	Percentage Weight
Did the student demonstrate an understanding of the competencies covered to date?	**30**
Did the student include all hosts identified within the provided packet trace?	**30**
Did the student include all services and protocols identified within the provided packet trace and align them with the proper host?	**30**
Did the student create a professional, well-developed draft with proper grammar, spelling, and punctuation?	**10**
Total	100%