COM 5335: NETWORK SECURITY
Assignment 2

Background/Scenario

Network attacks have resulted in the loss of sensitive data and significant network downtime. When a network or the resources in it are inaccessible, worker productivity can suffer, and business income may be lost. Attackers have developed many tools over the years to attack and compromise the networks of organizations. These attacks take many forms, but in most cases, they seek to obtain sensitive information, destroy resources, or deny legitimate users access to resources.

To understand how to defend a network against attacks, an administrator must first identify network vulnerabilities. Specialized security audit software developed by equipment and software manufacturers can be used to help identify potential weaknesses. In addition, the same tools used by attackers can be used to test the ability of a network to mitigate an attack. After the vulnerabilities are known, steps can be taken to help mitigate the network attacks.

This assignment provides a structured research project that is divided into two parts: *Researching Network Attacks* and *Researching Security Audit Tools*.

- **Part 1**, you are required to individually research various network attacks that have actually occurred. Then, you must select one of these and describe how the attack was perpetrated and how extensive the network outage or damage was. You also need to investigate how the attack could have been mitigated or what mitigation techniques might have been implemented to prevent future attacks. You also required to submit your report based on a predefined form included in this assignment.

- **Part 2**, you are required to individually research the network security audit tools and investigate one that can be used to identify host or network device vulnerabilities. You create a one-page summary of the tool based on a predefined form included in this assignment.

References: CCNA Security 1.0 Student Lab Manual from Cisco Systems, Inc.

Objectives

Part I: Researching Network Attacks

- Research network attacks that have occurred.
- Select a network attack and create your own report describe what you have learnt from your self-study.

Part II: Researching Security Audit Tools

- Research network security audit tools.
- Select a tool and create your own report to describe what you have learnt from your self-study.

Deadline: Friday 29 November, 2019 (Midnight)

READ THIS FIRST

Plagiarism, paraphrasing and downloading large amounts of information from external sources, will not be tolerated and will be dealt with severely. Although you should make full use of any source material, which would normally be an occasional sentence and/or paragraph (referenced) followed by your own critical analysis/evaluation, you will receive no marks for work that is not your own. Your work may be subject to checks for originality which can include use of an electronic plagiarism detection service.

References: CCNA Security 1.0 Student Lab Manual from Cisco Systems, Inc.

Part 1. Researching Network Attacks

In Part 1 of this assignment, you research various network attacks that have actually occurred and select one on which to report. Fill in the form below based on your findings.

***Step 1**: Research various network attacks.*

List some of the attacks you identified in your research.

***Step 2**: Fill in the following form for the network attack selected.*

Name of attack:	
Type of attack:	
Dates of attacks:	
Computers/ Organizations affected:	
How it works and what it did:	
Mitigation options:	
References and info links:	

Part 2. Researching Security Audit Tools

In part 2 of this assignment, you research network security audit tools and investigate one that can be used to identify host or network device vulnerabilities. Fill in the report below based on your findings.

Step 1: *Research various security audit and network attack tools.*

List some of the tools that you identified in your search.

References: CCNA Security 1.0 Student Lab Manual from Cisco Systems, Inc.

Step 2: *Fill in the following form for the security audit or network attack tool selected.*

Name of tool:	
Developer:	
Type of tool (character-based or GUI):	
Used on (network device or computer host):	
Cost:	
Description of key features and capabilities of product or tool:	
References and info links:	

Step 3: *Reflection*

a. What is the prevalence of network attacks and what is their impact on an organization's operation? What are some key steps organizations can take to help protect their networks and resources?

b. Have you actually worked for an organization or know of one where the network was compromised? If so, what was the impact to the organization and what did they do about it?

c. What steps can you take to protect your own PC or laptop computer?