Lab09

Network Trace analysis and Attacks: First Part2

[You must not attack any network without authorization! There are also severe legal consequences for unauthorized interception of network data.]

Introduction

This project will introduce you to common network protocols, the basics behind analyzing network traces from both offensive and defensive perspectives, and several local network attacks.

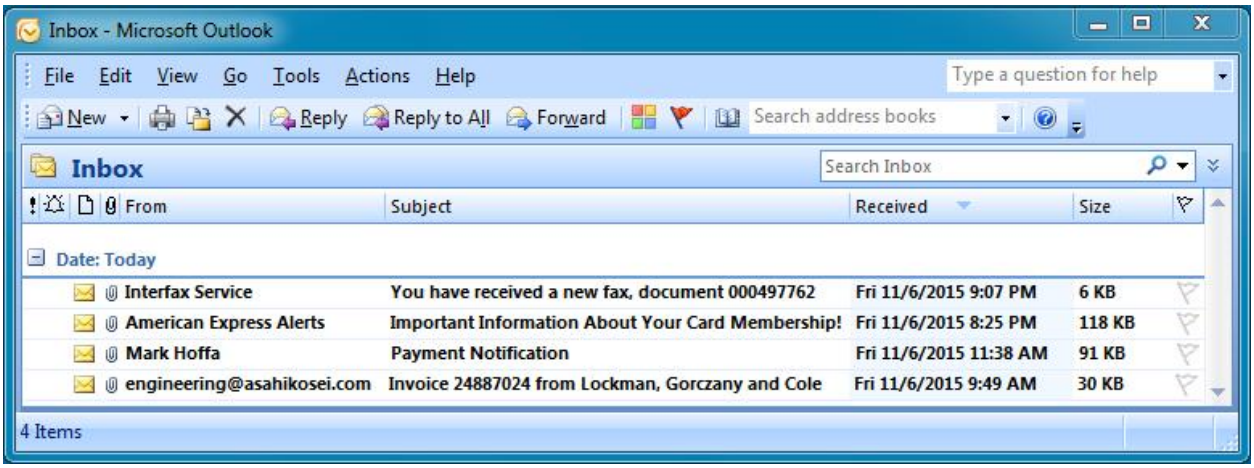
Objectives

• Gain exposure to core network protocols and concepts.

• Understand offensive techniques used to attack local network traffic.

9.1 Incident Response through Packet Analysis (25 points)

Suppose, you work as a security consultant for a private company. One fine day, the system administrator reported a security breach to you. The mail server has gone crazy and one of the employee's bank account has been compromised. In order to find out how the incident happened he submitted to you a packet capture and a collection of email attachments from that employee's computer because he believes this is a phishing attack that kicked off when the employee either opened email attachment or clicked a link contained in the emails.



Your task will be to submit a report which answers the following questions:

9.1.1 Date and approximate time of the infection.

9.1.2 The infected computer's IP address.

9.1.3 The infected computer's MAC address.

9.1.4 The infected computer's host name.

9.1.5 Which email the employee opened.

Please provide screen shots/commands that you used to conclude about the above questions.

9.2 Decrypting wifi (10)

You are given a capture of WPA traffic which was encrypted using the password "Induction" and SSID "Coherer". Use wireshark to decrypt this.

9.3 Breaking WiFi (extra credit “will be helpful: Trustme”)

At room 318 there is a wifi access point. Your task will be to break into this. The