Print

Lab 4 of 6: Intrusion Detection Systems (IDS), Intrusion Protection Systems (IPS), and Honeypots

Submit your assignment to the Dropbox located on the silver tab at the top of this page.

(See the Syllabus section "Due Dates for Assignments & Exams" for due dates.)

iLAB OVERVIEW

Scenario/Summary

In this lab, you will explore at least one IDS, IPS, or Honeypot currently offered by product vendors and cloud service providers. You will be making a security recommendation, related to the protection of a target network of your choice.

There are a few different paths you may take in this lab, so let's address some of the distinguishing features and definitions that are out there.

IDS and IPS Overview

- An intrusion detection system (IDS) generally detects and logs known intrusions or anomalous network activity. Generally, no real-time protection actually occurs, therefore false-positives create little or no damage. Optionally, suspicious network traffic can be routed to an alternate network, such as a honeypot.
- An intrusion protection system (IPS) generally detects, logs, and then blocks known intrusions or anomalous network activity. False-positives are an issue and will result in a self-inflicted denial of service condition. Optionally, suspicious network traffic can be routed to an alternate network, such as a honeypot.

Honeypot Overview

- Honeypots come in several broad categories. The most common labels we apply to them are research honeypots, active honeypots, and offensive honeypots. They are designed to do what their label suggests, and here is a brief summary.

Note: Seek qualified legal advice before deploying any type of honeypot.

- Research honeypots generally collect and analyze data about the attacks against a decoy-network. They can also route the attacker to new decoy-networks, to gather more details about the potential attacks. The data gathered are used to understand the attacks and strengthen the potential target networks.
- Active honeypots have many of the features found in a research honeypot, but they also hold special content that, once taken by the attackers, can be used as evidence by investigators and law enforcement. For example, active honeypots may have database servers containing a fake bank account or credit card information.
- Offensive honeypots are configured with many of the features of the active honeypots, with one interesting and dangerous addition: they are designed to damage the attacker. When used outside of your own network, this type of honeypot can result in vigilantism, attacks against false-targets, and may result in criminal charges against the honeypot operators. Offensive honeypots are not recommended for non-law-enforcement organizations. However, when used fully within your own network, this technique can detect and neutralize the attacker.

Any of the above services can be implemented on a privately managed network, or through a cloud service. The selection of one platform over another will generally determine where the specific protection occurs—on your network or in the cloud.

The reason for this lab is to give you an understanding of how special network technology can be used as a security research tool, while also providing varying degrees of protection.

Deliverables

Document Authoring Guidelines

Each section will vary in size based on the requirements. Drive yourself to create a useful document for the direction you have selected.

Lab Document Framework

- **The Target Network:** Indicate the type of activities and data that it supports in a few sentences. For example, it is the website for an educational institution that holds personal academic and financial information, or it is the network used to control devices in a chemical plant. Use your imagination, but select something that is real and meaningful to you.
- **The Protection System:** Select one from the presented list (Step 2), or choose your own protection technology, if it is highly relevant.
- **The Body of the Management Briefing Document:** See the guidance in Step 3. It is generally about 4 to 10 paragraphs.

- **Citations and Resources Used in this Report:** Tell us where you received external guidance and ideas. If you have presented original ideas, then give yourself credit, and tell us why you believe it is correct.

Delivering Your Lab Document

Organize your materials into a single comprehensive document. Name your document(s) such that the course ID, your full name, and this lab's name are referenced. For example, include SEC572_FirstName_LastName_Lab4 in the file's name. Your document must be readable with Microsoft Word 2007(or prior) or a standard PDF file viewer.

Submit your assignment to the Week 4 Dropbox located on the silver tab at the top of this page. (See the Syllabus section "Due Dates for Assignments & Exams" for due date information.)

Use the Dropbox comment area to give your instructor an introduction, or state any special information.

Required Software

Access the software at https://lab.devry.edu.
Steps: 1, 2, and 3

iLAB STEPS

Step 1

Back to Top

Broadly outline the target network. Indicate the type of activities and data that it supports in a few sentences.

Step 2

Back to Top

Select the protection system. Choose from one of the following.

- Intrusion detection system (IDS)
- Intrusion protection system (IPS)
- Research honeypot
- Active honeypot
- Offensive honeypot

Step 3

Back to Top

Create a management briefing document that will inform senior decision makers about their options, vendors, products, relevant examples, and issues associated with your selected protection (from Step 2). If cost can be identified, then please include that information as well. It is generally about 4 to 10 paragraphs.

Suggested Resources

Back to Top

Your textbook and other related textbooks

The DeVry Online Library

Professional Journals and Security Website

News Media Releases

Security Vendor and Contributor Websites (See the examples below, but be aware that URLs do change without notice.)

- https://www.google.com/search?q=intrusion detection system reviews
- http://www.bing.com/search?q=intrusion protection system reviews
- https://www.google.com/#q=Research Honeypots
- https://www.google.com/#q=Active Honeypots
- http://www.bing.com/search?q=Offensive Honeypot
- http://www.f5.com/
- http://www.snort.org/

Grading Rubric

Back to Top

Category	**Points**	**%**	**Description**
Structure	2.5	5	Use of applicable and creative layouts
Documentation and Formatting	7.5	15	Appropriate citations or referenced sources and formats of characters or content
Lab or Case Analysis	20	40	Accurate and complete delivery of lab tasks
Executive or Management Quality Content	20	40	Provides an appropriate value to managers in the setting of the lab's scope
Total	50	100	A quality lab document will meet or exceed all of the above requirements.

Back to Top