Intrusion Detection
COMP 435
Fall 2017
Prof. Cynthia Sturton

Data Buddies Survey

What is it?
- Anonymous survey provided by CRA open now through Oct. 31st

Why is it important?
- Your feedback gives department real-time data on curriculum, pedagogy, student support and cultural climate from student POV

What’s in it for you?
- Completion of survey means raffle entry and chance to win Amazon gift card (dept to raffle more than $1K in gift cards)
- ***Check your email for more details***

Undergraduate Survey

Graduate Survey

Assignment 1 Grades

- Average (Mean) Score: 89.2%
- Median Score: 95%
- Standard Deviation: 17.89
1. Information gathering
2. Initial access
3. Privilege escalation
4. Data collection
5. Maintaining access
6. Covering tracks

Case Study: Target Breach

1. Reconnaissance
Case Study: Target Breach

1. Reconnaissance

2. Initial Access

3. Privilege escalation

4. Data collection

5. Maintaining access

6. Covering tracks
Points to Consider with the Target Breach

- Security perimeter
- Benign data
- Warnings

Intrusion Detection Systems (IDS)

- Not intrusion prevention!
- Host based IDS (HIDS)
- Network based IDS (NIDS)
- Hybrid IDS

Goals of Intrusion Detection

- Be quick
- Collect data
- Deter attacks
Base Rate Fallacy

If the base rate of incidence is low, then most alarms will be false alarms.

Threat

Users become habituated to ignoring alarms.

Conditional Probability

\[
P(A|B) = \frac{P(A \cap B)}{P(B)}
\]

\[
= \frac{P(B|A)P(A)}{P(B)}
\]

In-class Exercise
Methods of Analysis

- Anomaly detection
- Heuristic

Host-based Intrusion Detection Systems (HIDS)

- Detects external and internal threats
- Antivirus software