Intrusion Detection

COMP 435
Fall 2017
Prof. Cynthia Sturton

Data Buddies Survey

UNC DEPARTMENT OF COMPUTER SCIENCE

CRA Computing Research Association

Undergraduate Survey
http://bit.ly/CSundergraduate

Graduate Survey
http://bit.ly/CSgraduate

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

2

ELECTRONIC FRONTIER FOUNDATION DEFCON 919

FIGHTING BACK AGAINST DRM

WHEN: Monday, Oct 23 19:00 – 20:00
WHERE: Sitterson 014, UNC Chapel Hill

The 1998 Digital Millennium Copyright Act (DMCA) made it illegal to bypass digital locks or publish methods of doing so. Since then, digital rights management (DRM) technologies have begun to appear everywhere, from automobiles to home goods to medical devices. Today, modifying the software on your slow cooker might be illegal!

In this session, we'll talk about how DRM has impacted innovation and how hackers can fight back. We'll also discuss other methods that manufacturers have used to shut down secondary markets, including patents and license agreements.

Join us for a social hour afterwards, ask questions and connect to local groups dedicated to studying alternative applications of technology.

We are inclusive to everybody! All skill levels and backgrounds welcome!

More Information:
www.eff.org
dc919.net
Contact: eac@dc919.net

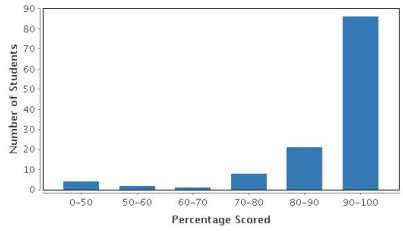
3

Assignment 1 Grades

- Average (Mean) Score: 89.2%
- Median Score: 95%
- Standard Deviation: 17.89

4

Assignment 1 Grades



Intrusions

Equifax data breach may affect nearly half the US population

Hackers steal sensitive personal information on as many as 143 million people from the credit reporting firm.

Every single Yahoo account was hacked - 3 billion in all

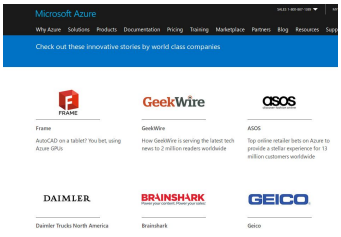
Target to Pay $18.5 Million to 47 States in Security Breach Settlement

Intrusions

1. Information gathering
2. Initial access
3. Privilege escalation
4. Data collection
5. Maintaining access
6. Covering tracks

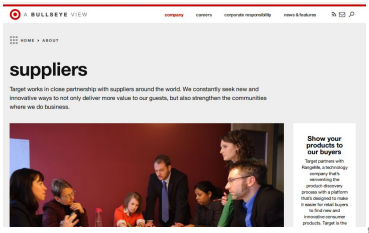
Case Study: Target Breach

1. Reconnaissance



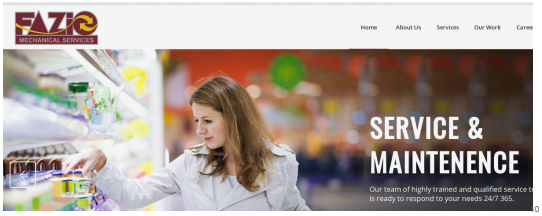
Case Study: Target Breach

1. Reconnaissance



Case Study: Target Breach

2. Initial Access

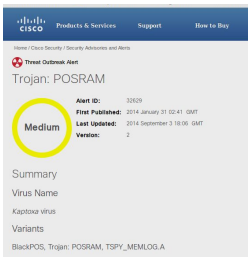


Case Study: Target Breach

3. Privilege escalation

Case Study: Target Breach

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

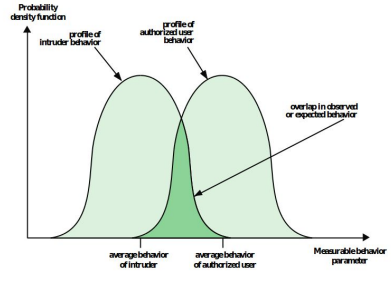


Figure 8.1 Profiles of Behavior of Intruders and Authorized Users

Computer Security: Principles and Practice, 3rd ed. William Stallings and Lawrie Brown. Pearson, 2015.

Base Rate Fallacy

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

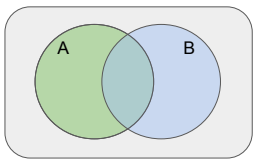
Threat

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

Network-based Intrusion Detection Systems (NIDS)

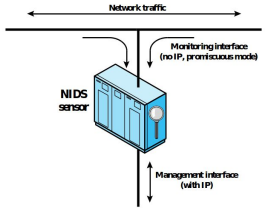


Figure 8.4 Passive NIDS Sensor

Computer Security: Principles and Practice, 3rd ed. William Stallings and Lawrie Brown. Pearson, 2015.

Honeypots

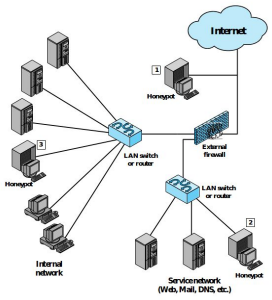


Figure 8.8 Example of Honeypot Deployment

Computer Security: Principles and Practice, 3rd ed. William Stallings and Lawrie Brown. Pearson, 2015.