Machine Learning for Cybersecurity

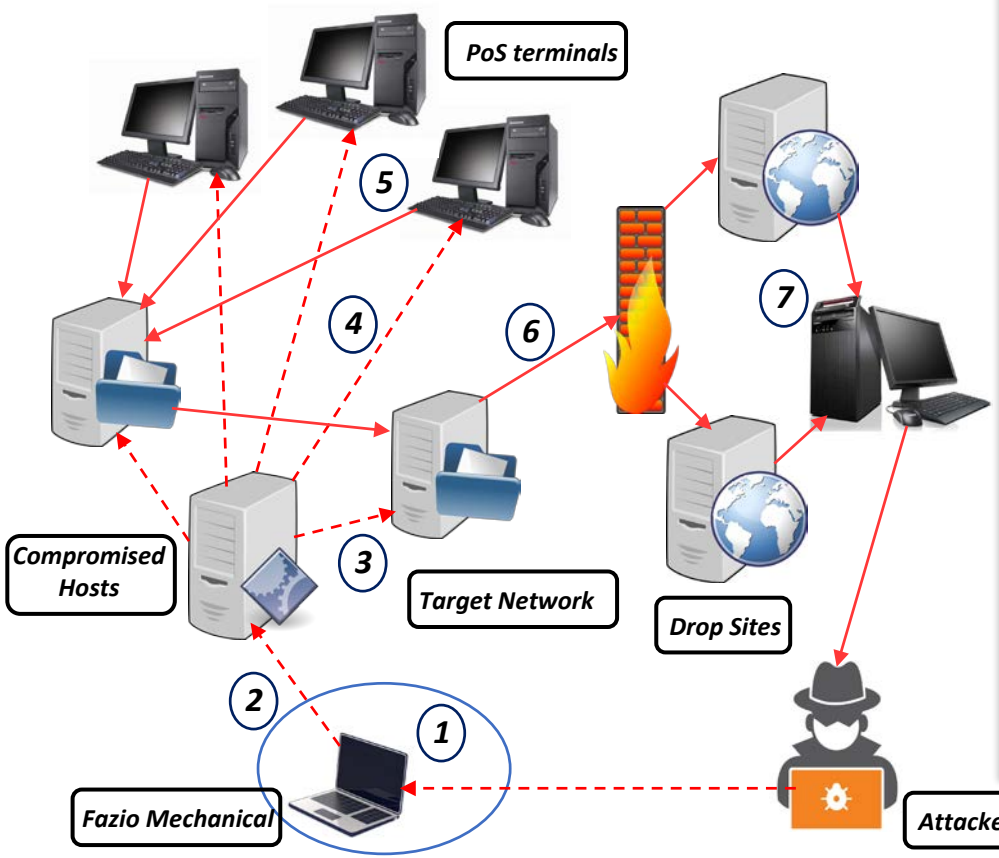
- What you will learn:
  - How to use machine learning algorithms to implement cybersecurity concepts
  - How to implement machine learning algorithms such as clustering, k-means, regression and ensemble methods
  - How to use Python libraries - NumPy, and Scikit-learn
  - Understand how to combat malware, detect spam, and cyber anomalies
  - How to use TensorFlow in the cybersecurity domain and implement real-world examples

- Course Grade will be based upon homework/projects (60%) and a final project (40%)
- Pre-requisite: Good Python programming experience
- Recommended Laptop: GPU laptop (GTX 1080 or equivalent) with 16GB memory; or CPU laptop with 64GB memory

Machine Learning for Cybersecurity

TARGET

data breach *Credit/debit card details of 41 million customers were stolen*



Stages of Target data breach:

1. Phishing attack against Fazio Mechanical Service
2. Accessed the Target network
3. Gained access to vulnerable machines
4. Installed malware on Point of Service terminals
5. Collected card information from Point of Service
6. Moved data out of the Target network
7. Aggregated stolen card and person data

Machine Learning for Cybersecurity

- Course content

1. Basics for Machine Learning for Cybersecurity
2. Time Series Analysis and Ensemble Modeling
3. Segregating Legitimate and Lousy URLs
4. Knocking down CAPTCHAs
5. Using Data Science to Catch Email Fraud and Spam
6. Efficient Network Anomaly Detection Using k-means

Machine Learning for Cybersecurity

course content continued…

7. Decision Tree and Context-Based Malicious Event
8. Catching Impersonators and Hackers Red Handed
9. Changing the Game with TensorFlow
10. Financial Fraud and How Deep Learning can Mitigate It
11. Case Studies