Caden Keese, Miles Maloney, Kanan Boubion, Scott Spinali, Maxon Crumb
COMP 365
Assignment 4

Attack Tree:

Key:
🟩 Easy 🟥 Difficult

🟩 Compromise Client Data

- 🟩 1. Compromise Confidentiality
  - 🟩 1.1. Steal username and password
    - 🟩 1.1.1. Shoulder Surfing
    - 🟩 1.1.2. Sticky notes
    - 🟥 1.1.3. Phishing
    - 🟥 1.1.4. Spear Phishing
    - 🟩 1.1.5. Keylogger
      - 🟩 1.1.5.1. Physical access
    - 🟥 1.1.6. Coercion
- 🟩 2. Compromise Integrity
  - 🟩 2.1. Change user data
    - 🟩 2.1.1. Steal username and password
      - 🟩 2.1.1.1. Social engineering
        - 🟩 2.1.1.1.1. Shoulder Surfing
        - 🟩 2.1.1.1.2. Sticky notes
        - 🟥 2.1.1.1.3. Phishing
        - 🟥 2.1.1.1.4. Spear Phishing
        - 🟩 2.1.1.1.5. Keylogger
          - 🟩 2.1.1.1.5.1. Physical access to keyboard
        - 🟥 2.1.1.1.6. Coercion
- 🟩 3. Compromise Non-repudiation
  - 🟩 3.1. Corruption of usage log
    - 🟥 3.1.1. Gain root access to the OS
    - 🟩 3.1.2. Access to storage medium
      - 🟩 3.1.2.1. Physical access
- 🟩 4. Compromise Availability
  - 🟩 4.1. Encrypt/delete data
    - 🟩 4.1.1. Install malware

4.1.1.1. Social engineering

4.1.1.1.1. USB in a parking lot

4.1.1.1.2. Phishing attack

4.1.1.1.2.1. Spear phishing

4.1.1.2. Trojan horse

4.1.1.3. Exploit zero-day vulnerability

4.2. Physical Destruction

4.2.1. Physical access

ADTool A-D tree:
*See attached file

Propositional interpretation of tree:
*Compromise non-repudiation (attack-defense tree branch)

(((user negligence) ∧ (encrypted hard drive)) ∨ ¬(encrypted hard drive)) ∨ (gain root access)