D+D Exercise for Threat Intelligence
Materials:

- Dice
- Character Sheets
- Scenario/Powerpoint

- Combat = cyber warfare
- OSINT element
- Possible targets: Exxon Mobile
  - Snacks
  - Bit of a budget.
  - APTs
  - A diversity of APTs
  - Manual
  - Link a document.
  - 1-2 from China, Russia, NK, India, Iran, the NSA
  - Administrative: Anna

Character Sheets for each APT (20-30 minutes)

APT ~8
Cozy Bear: +1 SOPH +2 TTC (Russia)
Mustang Panda: +2 SOPH +1 TTC (China)
Labyrinth Chollima: +2 TTC +1 CHA (North Korea)
Ocean Buffalo: +1 SOPH +2 COMP (Vietnam)
Remix Kitten: +2 COMP +1 CHA (Iran)
Venomous Bear: +3 DEADL (Russia)
Wicked Panda: +1 COMP +1 RES +1 CHA (China)
The Equation Group: +1 RES +1 SOPH +1 DEADL (USA)

APT Sheet

- Description of APT
- Objectives
- Motives
- Passive cool APT buff
- Picture of APT

Character Sheet

- Stats:
  - Strength – Deadliness/Effectiveness
  - Dexterity – Computing Speed/Power
  - Constitution – Time-to-compromise
  - Intelligence – Sophistication
  - Wisdom – Available Resources (money, manpower...)
  - Charisma – Charisma

- Classes:
  - **Developer** - good at creating software tools
    - INT, DEX
    - Deadliness: Versatility/High Compromise Capability
    - Computing Speed: Malware development
    - Computing Speed: Stealth
  - **Social Engineer** - good at infiltrating and executing
    - CHA, CON
    - Charisma: Social Engineering
    - Charisma: Language Proficiency
    - Charisma: Diplomacy
    - Available Resources: Bribery
  - **Pentester** - good at hacking
    - INT, STR
    - Deadliness: Escalation/Lateral Movement
    - Time-to-compromise: Firewall/Endpoint Detection and Response (EDR)
    - Sophistication: Forensics
  - **Device Engineer** - good at creating and using physical tools
    - WIS, STR
    - Sophistication: Adaptability
    - Available Resources: Technological Innovation
  - **Infastructure/systems engineer** - can deploy any server/service
    - INT, CON
    - Deployability: Versatility/High Compromise Capability
    - Sophistication: Connection strength
    - Available Resource: Bitcoin

Scenario

- Give the players and ourselves latitude, and strike a balance there.
- Reward Creativity, give enough guidance to the DMs to accomplish our goals.

1. Decide how to approach and attack Exxon Mobile (Brute force Attack, OSINT/Recon → Social Engineering, Vulnerability Enumeration/Exploitation, Physical Penetration, Malware creation/use, infrastructure exploitation, blackmail, immoral/war crimes, etc.)
2. ???
3. ???
4. ???
5. ???
6. ???
7. ???
8. ???
9. Final fight with whatever (Social Engineering → CEO; Penetration → defending Cybersecurity/Blue Team; infrastructure → Power Grid; war crimes → the UN)

Goal: Obtain Sensitive information from ExxonMobil's headquarters/Server building
You only know the following:

1. The network is running an Active Directory.
    a. GitLab login is integrated with the AD.
2. Employees are permitted to use personal flash storage devices.
    a. All flash storage devices are scanned for known malware signatures.
3. The security camera system is down awaiting repairs.
4. Network switches in unsecured areas (around desks, conference rooms, etc.) do not have port security configured.
5. Visitors and contractors are common.

Constraints:

2. Custom malware and tools developed in-house are available
3. Unlimited resources (can build things within reason)
4. Unlimited cloud credits
5. All reasonable vectors are permitted
    a. Including physical and social engineering

Question/Objective: Based on this information and your resources alone, what is your initial plan for achieving your objective?