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. ???

Skills

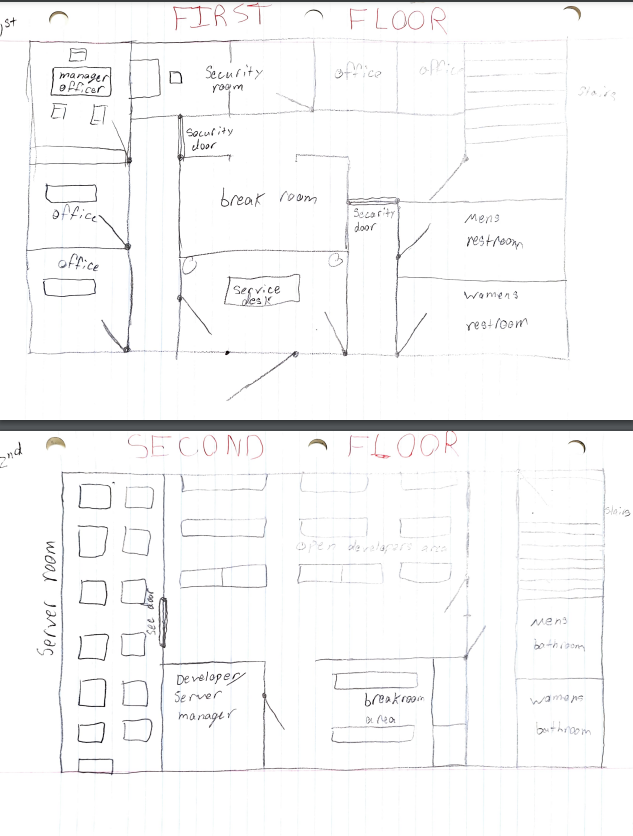
* Deadliness: **Versatility/High Compromise Capability**
* Deadliness: **Escalation/Lateral Movement**
* Computing Speed: **Malware development**
* Computing Speed: **Stealth**
* Computing Speed: **Connection strength**
* Time-to-compromise: **Firewall/Endpoint Detection and Response (EDR)**
* Sophistication: **Forensics**
* Sophistication: **Adaptability**
* Available Resources: **Bribery**
* Available Resources: **Technological Innovation**
* Available Resource: **Crypto-Currency**
* Charisma: **Social Engineering**
* Charisma: **Language Proficiency**
* Charisma: **Diplomacy**

Hacking/Penetration Scenario

\*Breakpoints Included\*

* OSINT should be done to find out some of the information that only we have in the scenario.
  + The security camera system is down awaiting repairs. **\*12\***
  + Network switches in unsecured areas (around desks, conference rooms, etc.) do not have port security configured. **\*12\***
  + Visitors and contractors are common. **\*8\***
  + Linux is not used anywhere within the Enterprise, except for one specific user on the system. The CEO himself has always been a diehard Linux user. **\*12\***
  + The hobbies of the CEO or other executive leadership include golf, skiing, and ostrich skin boots. **\*2\***
* If they use Mimikatz, they will find that the passwords are stored but they are hashed, so the WDigest Registry setting has been changed. **\*8\***
  + If they try to crack the hashes, they might be successful **\*13\***
* If they Port Scan an IP on the environment, they might alert the Incident Response/Triage Team, \*10\* and find that the computer that they are working with is likely Windows 7. **\*12\***
  + They can look up common exploits for Windows 7. **\*2\***
  + If they use EternalBlue, they find that the computer is in fact vulnerable to it, and upon exploiting the vulnerability, they gain Authority access. **\*8\***
* If they create a spearphishing attack, they will find that the executive leadership utilizes a specific trusted email address for internal communication. **\*14\***
* If they register a series of new domains for attack infrastructure, they might unintentionally provide a new fingerprint for further pivoting exposing the group to greater visibility, **\*10\*** but they will have greater resources to leverage in their future attacks.
* If they launch ransomware, they will be paid with an increase in crypto-currency or they will not be paid and the FBI will get involved – the Baltimore Office.
* If they compromise the third-party authentication provider (think RSA hack 2011), the group is able to penetrate the system and exfiltrate intellectual property data related to the drilling equipment. The third-party authentication provider denies the legitimacy of the hack and attempts to sue Exxon. The group is able to sell the blueprints to Iraq for a lot crypto-currency.

Physical/Social Engineering Scenario



War Crimes Scenario

Haha Good Luck!

Players are given:

Goal: Obtain Sensitive information from ExxonMobil’s Headquarters/Server Building

You only know the following:

1. The network is running an Active Directory.

2. Employees are permitted to use personal flash storage devices.

Constraints:

1. Custom malware and tools developed in-house are available.

2. Unlimited cloud credits.

3. All 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?

Goal: Obtain Sensitive information from ExxonMobil’s Headquarters/Server Building

The following is important to know about the directory:

1. The network is running an Active Directory.

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.**

6. **Linux is not used anywhere within the Enterprise, except for one specific user on the system. The CEO himself has always been a diehard Linux user.**

7.

Constraints:

1. Custom malware and tools developed in-house are available

2. Unlimited cloud credits

3. All 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?