Bringing Offensive Cyber Operations Together

Final Presentation for CSC 840
Kurt Jarvis

Introduction

This semester was a focus on multiple topics that were pieces of different aspects to offensive cyber operations. If you made it past chapter 5, you are probably committed to execution but how do we make it all work together to improve security? Here are the questions to ask yourself:

- How do I methodically go from no access to maximum access?
- How do I ensure that I don't miss anything?
- How do I estimate effort and timelines?
- How do I explain this to the consumer?
- How do I explain this to the team who is going to fix it?

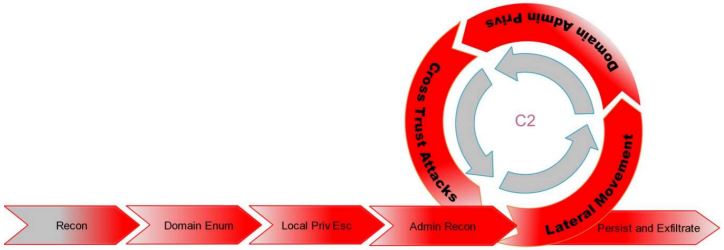
So can I identify the weakness in the architecture…usually.

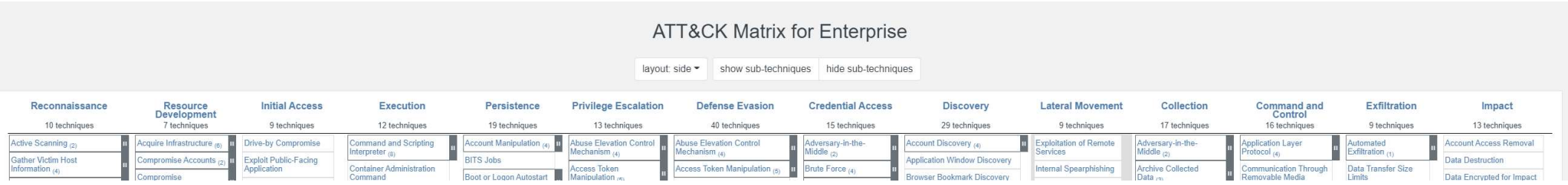
Can I establish an entry-point…probably.

Can I impose my will on your product….you better hope not!

Letting the Methodologies work together

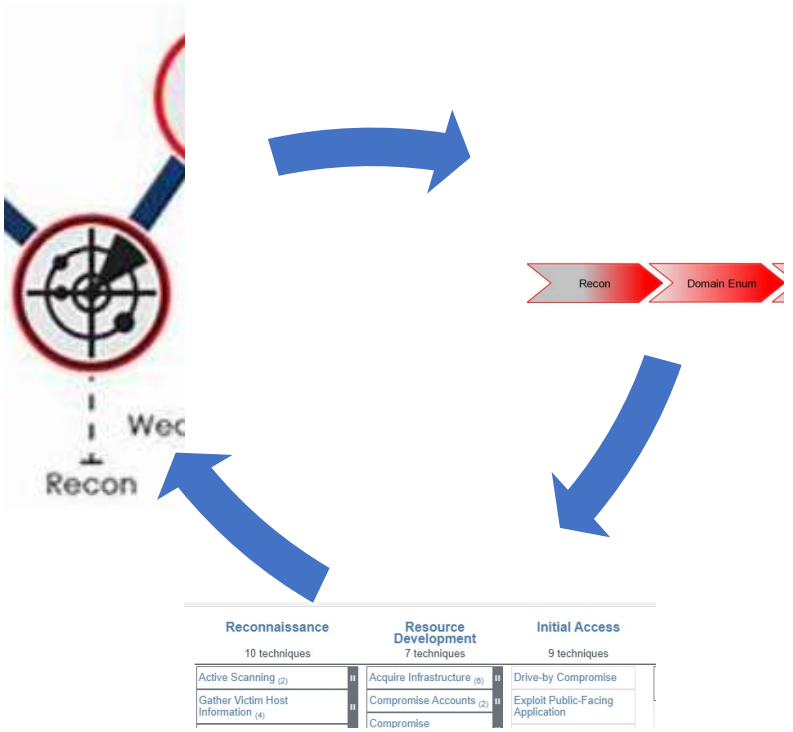
- Lockheed Martin Kill Chain (How do I break this down into steps)
- Privilege Escalation Methodology (What am I trying to do)
- MITRE ATT&CK (What are the techniques to get me where I wanna go)





Break Down the Steps Together

- These are the steps, but how do we get there?
  - What do we need to do?
  - What are we looking for?
  - What techniques are there?
  - What technical implementation do I chose?



Demo Time!

- Conducting Recon
  - https://attack.mitre.org/#
    - Gather Victim Host Information
    - Search Open Technical Databases
    - Active Scanning
  - Exploit-db: https://www.exploit-db.com/
  - Nvd: https://nvd.nist.gov/
  - Change logs

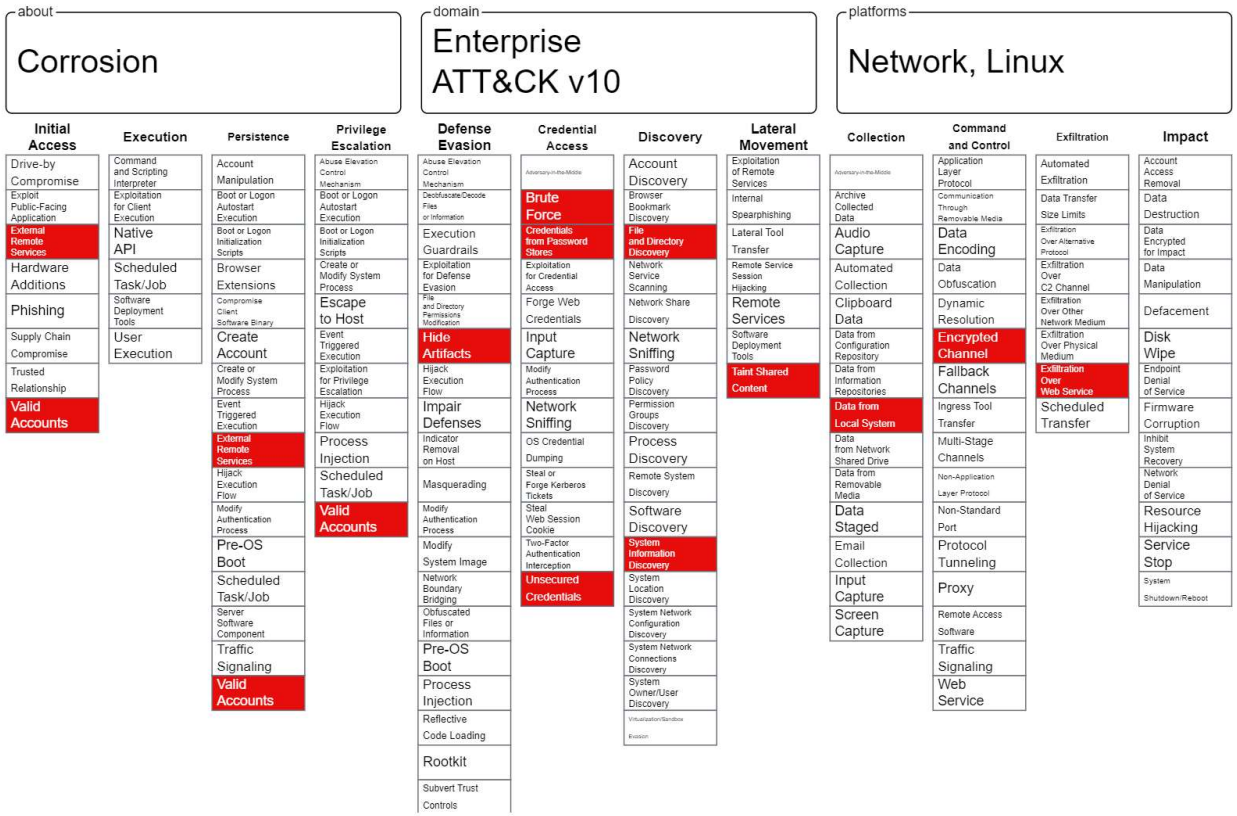
My full write-up for this vulnhub box: https://artilleryred.medium.com/vulnhub-writeup-of-corrosion-7a5859ce84d8

Results for the Excursion

What can I give the Blue Team?
- Risk Management
- How can I get better?

Did I use a C2?
- Teamwork
- Pre-built exploits
- Stealthiness

Did I cover my tracks?
- Auditibility
- Tools
- Purple-teaming



Where to Navigate Next?

- Are you proficient at the technologies today? The technology stack is very deep and is only growing:
  - Cloud
  - Containerization
  - Kubernetes
  - IoT
  - LiFi
  - Embedded/Real-Time Operating Systems
  - CANBUS

- MITRE D3FEND
  - When they get better, we have to get better!