



## Bringing Offensive Cyber Operations Together

**Final Presentation for CSC 840**  
**Kurt Jarvis**



Bringing Offensive Cyber Operations Together



# 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!



**Bringing Offensive Cyber Operations Together**



# 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)



ATT&CK Matrix for Enterprise

layout: side show sub-techniques hide sub-techniques

| Reconnaissance  | Resource Development  | Initial Access   | Execution   | Persistence  | Privilege Escalation   | Defense Evasion  | Credential Access                              | Discovery   | Lateral Movement  | Collection  | Command and Control   | Exfiltration  | Impact  |
|---|---|--|---|--|--|--|--|---|---|---|---|---|---|
| 10 techniques   | 7 techniques  | 9 techniques   | 12 techniques   | 19 techniques  | 13 techniques  | 40 techniques  | 15 techniques                                  | 29 techniques   | 9 techniques  | 17 techniques   | 16 techniques   | 9 techniques  | 13 techniques   |
| Active Scanning (2)<br>Gather Victim Host Information (4) | Acquire Infrastructure (6)<br>Compromise Accounts (2)<br>Compromise | Drive-by Compromise<br>Exploit Public-Facing Application | Command and Scripting Interpreter (6)<br>Container Administration Command | Account Manipulation (4)<br>BITS Jobs<br>Boot or Logon Autostart | Abuse Elevation Control Mechanism (4)<br>Access Token Manipulation (5) | Abuse Elevation Control Mechanism (4)<br>Access Token Manipulation (5) | Adversary-in-the-Middle (2)<br>Brute Force (4) | Account Discovery (4)<br>Application Window Discovery<br>Browser Bookmark Discovery | Exploitation of Remote Services<br>Internal Spearphishing | Adversary-in-the-Middle (2)<br>Archive Collected Data (3) | Application Layer Protocol (4)<br>Communication Through Removable Media | Automated Exfiltration (1)<br>Data Transfer Size Limits | Account Access Removal<br>Data Destruction<br>Data Encrypted for Impact |

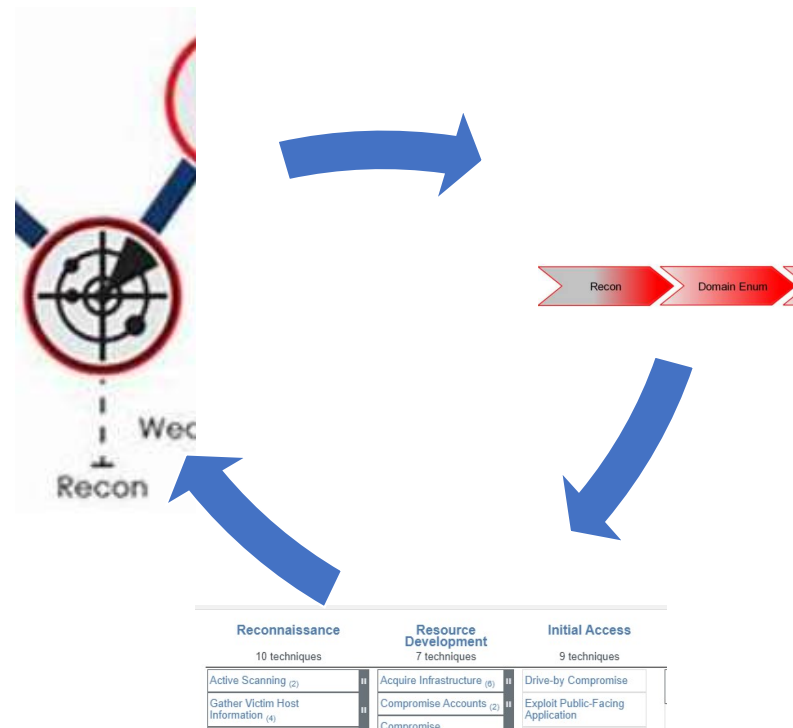


## Bringing Offensive Cyber Operations Together



# 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?



Bringing Offensive Cyber Operations Together



# 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>



Bringing Offensive Cyber Operations Together



# 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?

- Auditability
- Tools
- Purple-teaming

| about                             |                                   |   |                                      | domain                                      |  |  |                                  | platforms                            |                                       |  |                            |
|-----------------------------------|-----------------------------------|---|--------------------------------------|---|--|--|----------------------------------|--------------------------------------|---------------------------------------|--|----------------------------|
| Corrosion                         |                                   |   |                                      | Enterprise<br>ATT&CK v10                    |  |  |                                  | Network, Linux                       |                                       |  |                            |
| Initial Access                    | Execution                         | Persistence                                 | Privilege Escalation                 | Defense Evasion                             | Credential Access                      | Discovery                              | Lateral Movement                 | Collection                           | Command and Control                   | Exfiltration                           | Impact                     |
| Drive-by Compromise               | Command and Scripting Interpreter | Account Manipulation                        | Abuse Elevation Control Mechanism    | Abuse Elevation Control Mechanism           | Abuse Elevation Control Mechanism      | Account Discovery                      | Exploitation of Remote Services  | Archive Collected Data               | Application Layer Protocol            | Automated Exfiltration                 | Account Access Removal     |
| Exploit Public-Facing Application | Exploitation for Client Execution | Boot or Logon Autostart Execution           | Boot or Logon Autostart Execution    | Deobfuscate/Decode Files or Information     | Brute Force                            | Browser Bookmark Discovery             | Internal Spearphishing           | Automated Collection                 | Communication Through Removable Media | Data Transfer                          | Data Destruction           |
| External Remote Services          | Native API                        | Boot or Logon Initialization Scripts        | Boot or Logon Initialization Scripts | Execution Guardrails                        | Credentials from Password Storage      | File and Directory Discovery           | Lateral Tool Transfer            | Clipboard Data                       | Data Encoding                         | Data Size Limits                       | Data Destruction           |
| Hardware Additions                | Scheduled Task/Job                | Browser Extensions                          | Create or Modify System Process      | Exploitation for Defense Evasion            | Exploitation for Credential Access     | Network Service Scanning               | Remote Service Session Hijacking | Data from Configuration Repositories | Data Obfuscation                      | Exfiltration Over Alternative Protocol | Data Encrypted for Impact  |
| Phishing                          | Software Deployment Tools         | Compromise Client Software Binary           | Escape to Host                       | File and Directory Permissions Modification | Forge Web Credentials                  | Network Share Discovery                | Remote Services                  | Data from Information Repositories   | Dynamic Resolution                    | Exfiltration Over C2 Channel           | Data Manipulation          |
| Supply Chain Compromise           | User Execution                    | Create Account                              | Event Triggered Execution            | Hide Artifacts                              | Input Capture                          | Network Sniffing                       | Software Deployment Tools        | Data from Local System               | Encrypted Channel                     | Exfiltration Over Physical Medium      | Defacement                 |
| Trusted Relationship              |                                   | Create or Modify System Process             | Hijack Execution Flow                | Hijack Execution Flow                       | Modify Authentication Process          | Password Policy Discovery              | Taint Shared Content             | Data from Network Shared Drive       | Fallback Channels                     | Exfiltration Over Web Service          | Disk Wipe                  |
| Valid Accounts                    |                                   | Event Triggered Execution                   | Process Injection                    | Impair Defenses                             | Network Sniffing                       | Permission Groups Discovery            |                                  | Data from Removable Media            | Ingress Tool Transfer                 | Scheduled Transfer                     | Endpoint Denial of Service |
|                                   |                                   | External Remote Services                    | Scheduled Task/Job                   | Indicator Removal on Host                   | OS Credential Dumping                  | Process Discovery                      |                                  | Data Staged                          | Multi-Stage Channels                  |  | Firmware Corruption        |
|                                   |                                   | Hijack Execution Flow                       | Valid Accounts                       | Masquerading                                | Steal or Forge Kerberos Tickets        | Remote System Discovery                |                                  | Email Collection                     | Non-Application Layer Protocol        |  | Inhibit System Recovery    |
|                                   |                                   | Modify Authentication Process               |                                      | Modify Authentication Process               | Steal Web Session Cookie               | Software Discovery                     |                                  | Input Capture                        | Non-Standard Port                     |  | Network Denial of Service  |
|                                   |                                   | Pre-OS Boot                                 |                                      | Modify System Image                         | Two-Factor Authentication Interception | System Information Discovery           |                                  | Screen Capture                       | Protocol Tunneling                    |  | Resource Hijacking         |
|                                   |                                   | Scheduled Task/Job                          |                                      | Network Boundary Bridging                   | Unsecured Credentials                  | System Location Discovery              |                                  |                                      | Proxy                                 |  | Service Stop               |
|                                   |                                   | Server Software Component Traffic Signaling |                                      | Obfuscated Files or Information             |  | System Network Configuration Discovery |                                  |                                      | Remote Access Software                |  | System Shutdown/Reboot     |
|                                   |                                   | Valid Accounts                              |                                      | Pre-OS Boot                                 |  | System Network Connections Discovery   |                                  |                                      | Traffic Signaling                     |  |                            |
|                                   |                                   |   |                                      | Process Injection                           |  | System Owner/User Discovery            |                                  |                                      | Web Service                           |  |                            |
|                                   |                                   |   |                                      | Reflective Code Loading                     |  | Uniquification/Randomization           |                                  |                                      |                                       |  |                            |
|                                   |                                   |   |                                      | Rootkit                                     |  | Execution                              |                                  |                                      |                                       |  |                            |
|                                   |                                   |   |                                      | Subvert Trust Controls                      |  |  |                                  |                                      |                                       |  |                            |

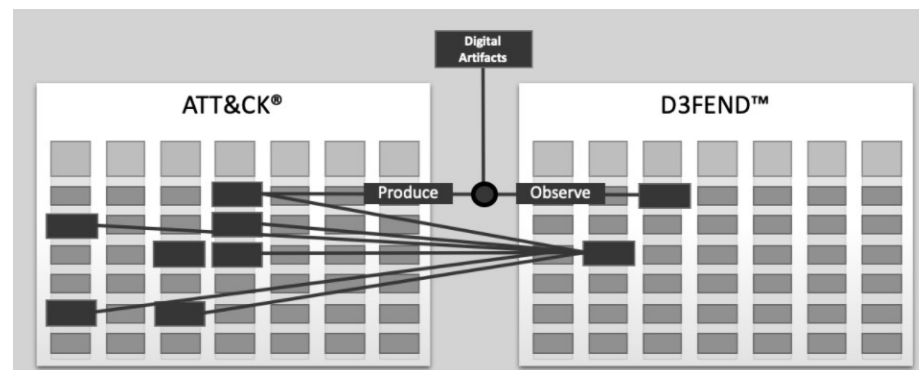


## Bringing Offensive Cyber Operations Together



## 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!



Bringing Offensive Cyber Operations Together