- Filename: eccouncil-ceh31250-v11-1-5-1-cyber-kill-chain.md
- Show Name: CEHv11 (312-50)
- Topic Name: Intro to Ethical Hacking
- Episode Name: Cyber Kill Chain

==========

Cyber Kill Chain

Objectives:

- List and define the 7 phases of the Cyber Kill Chain
- Identify and explain activities performed at each phase

- Tell us a little about the development of the cyber kill chain.
    - Developed by Lockheed-Martin around 2011
    - Researchers recognized a common attack pattern
        - Broke that pattern down into 7 phases
            - https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- So we have 7 phases, what is the first phase of the cyber kill chain?
    - Recon
        - Information gathering
            - Public info
                - technical and non-technical
- Phase 2 is Weaponization. Explain that idea.
    - Analyze info gathered in Recon
        - Find possibly exploitable vulnerabilities
            - Create malicious deliverable payload to exploit vulnerabilities
                - Custom malware
                - Off-the-shelf
                - Phishing campaign
- I'm guessing that once a payload is ready, we're on to Phase 3 Delivery?
    - Correct
    - Payload is delivered to target
        - email
        - usb
        - web
- How does the Exploitation Phase happen?
    - Clicks on malicious link
    - Goes to compromised web site
    - Executes malicious software binary
- Our next phase is Phase 5: Installation? What's being installed?
    - 'insider' malware will install more Malware
        - Backdoors

        - Malicious activity hiding
        - Maintaining access

- It would seem that the Attacker is now ready for the Command and Control phase?
    - Constant communication and control is established
    - Use encryption and other techniques to hide malicious communication
    - Attempt to Priv Esc
    - Continue to hide attacker's presence
- Phase 7 is called 'Actions and Objectives'. Can you elaborate on that title?
    - Whatever reason the attacker decided to attack can now be done
        - Cyber crime
        - Hacktivism
        - Blackmail
        - Political

...