CYBER DEFENSE ANALYST (CDA) COURSE RESOURCES

GENERAL RESOURCES

DOCUMENTATION

- Cybersecurity Resource and Reference Guide, February 28, 2022
  https://dodcio.defense.gov/Portals/0/Documents/Library/CSResourceReferenceGuide.pdf
- NIST SP 800-181r1, Workforce Framework for Cybersecurity (NICE Framework)
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf
- DoD Directive 8140.01, Cyberspace Workforce Management
  https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001p.pdf

WEBSITES AND OTHER RESOURCES

- DoD Cyber Workforce Framework Tool
  https://public.cyber.mil/wid/dcwf/

MODULE 4 – NETWORK TECHNOLOGIES

PORTS, PROTOCOLS, AND SERVICES (PPS)

- Network Services Learning Activity:
  - Commonly Used Network Services Learning Activity
- Network Services Learning Activity Resources:
  - PPS List (Excel Spreadsheet)
  - The Internet Assigned Numbers Authority (IANA):
    https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml
  - The Internet Engineering Task Force (IETF):
    https://www.rfc-editor.org/
  - Techopedia Dictionary:
    https://www.techopedia.com/dictionary
  - DoD Ports, Protocols, and Services Management:
    https://cyber.mil/ppsm/cal/ (CAC Required)

MODULE 6 – TECHNOLOGY MANAGEMENT

PACKET-LEVEL ANALYSIS FILTERS

- Wireshark Display Filters Walkthrough: Part 1
- Wireshark Display Filters Walkthrough: Part 2
- Wireshark Intrusion Analysis Walkthrough: Part 1
- Wireshark Intrusion Analysis Walkthrough: Part 2

MODULE 8 – CYBERSECURITY BASICS

INTRUSION DETECTION AND PREVENTION

- Network IDS Walkthrough

MODULE 12 – ATTACK DETECTION, ANALYSIS, AND RESPONSE

CLIENT-SIDE ATTACKS

- Client-Side Attacks and Detection: Analysis Exercise

SERVER-SIDE ATTACKS

- Service-Side Attacks and Detection: Analysis Exercise

WEB SERVER ATTACKS

- Web Server Attacks: Analysis Exercise

EXCESSIVE USER RIGHTS

- Excessive User Rights: Analysis Exercise

WORM ATTACKS

- Live Worm Propagation Attacks: Analysis Exercise