Assignment - 1

5 – Points

Assigned: 3rd Sep 2024

Deadline: 13th Sep 2024

CS 5323: PRINCIPLES OF CYBER SECURITY

Assignment - 1

- Students should submit one PDF file on Canvas (As you can only upload one file) containing the following:
- Assignment-1 Discussion is also enabled on Canvas (Discussion – Left menu)
- Use clear headings for the assignment. Making it helpful for the grader
- Plagiarism above 15% will be penalized by a deduction of 1 point.

Common Vulnerabilities and Exposures (CVEs)

- Students need to submit a brief understanding of how these (5 CVEs on the next slide) attacks work and how can they be mitigated (Total 50-100 words).
- Each of the 5 CVEs belong to different type of attack (i.e. Remote Code Execution, Microsoft Exchange, Command Line Execution, Authentication Bypass by Spoofing).
- Assignment pdf are to be submitted on canvas. The file should contain your name and abc123 in it.

Common Vulnerabilities and Exposures (CVEs)

- CVE's (description of each CVEs is worth 1 points i.e. 0.5 points for attack vector + 0.5 points for mitigation)
  - Remote Code Execution
    - Apache Log4j (CVE-2021-44228)
    - Microsoft Exchange (CVE-2021-26855)
  - Command Line Execution
    - Cisco Hyperflex (CVE-2021-1497)
  - Command Injection
    - Hikvision Webserver (CVE-2021-36260)
  - Authentication Bypass by Spoofing
    - Apache (CVE-2022-24112)

- Resource:
  - https://www.cisa.gov/uscert/ncas/alerts/aa22-279a
  - https://www.cvedetails.com/
  - https://cve.mitre.org/index.html