

CYBE 466: Host Based Cyber Defense

Instructor: David Krovich Email: dmkrovich@mail.wvu.edu

Office: The Internet

Office Hours: During Live Sessions and by Appointment

Pre-Requisites: Grade of C- or higher in CS453

Course Description: An in depth study of the strategies available to defend hosts (clients, IoT devices, servers) against cyber attacks.

Technology Requirements

- A computer capable of running Virtualbox with a minimum of 8GB of ram. 16GB or more is recommended.
- Video teleconferencing capabilities including both audio and video.

Expected Learning Outcomes: At the end of the course students will be able to:

- Configure host based access control methods such as user account management, file permissions, and host based network firewalls
- Install, configure, and defend core internet services such as sshd, named, and httpd.
- Analyze host health and integrity via log monitoring, filesystem monitoring, connection monitoring, and process status monitoring.
- Inherit and defend previously configured host systems

Topics Covered

- 1) Operating System Installation
- 2) Account Management
- 3) Remote Access (ssh,vnc, rdesktop)
- 4) Windows Active Directory
- 5) Operating System Hardening
- 6) Process monitoring

- 7) Network connection monitoring
- 8) Firewalls
- 9) File Sharing (NFS, CIFS, ftpd)
- 10) DNS
- 11) Web Server/Application Security
- 12) Database Server Security
- 13) Intrusion Detection
- 14) CLI / Scripting
- 15) Log Monitoring
- 16) Backup and restore
- 17) IoT Management

Class Readings:

- Mike O'Leary *Cyber Operations: Building, Defending, and Attacking Modern Computer Networks*
- William (Chuck) Easttom, II *Network Defense and Countermeasures: Principles and Practices, 3rd Edition*
- Orin Thomas *Windows Server 2016 Inside Out*
- Rothwell, W., & Kinsey, D. (2019). *Linux essentials for cybersecurity*

Grading:

- Engagement: 100 points

There will be 10 engagement assignments during the course of the semester. Each engagement assignment will be worth 10 points.

- 6 homeworks: 600 points

There will be 6 homework assignments during the course of the semester. Each homework assignment will be worth 100 points each.

- 1 Test: 100 points

There will be one timed test around midterm. You will need to have a camera to take the test.

- Final: 200 points

Final will be comprehensive

- **Grading Scale:**

- A = 900 to 1000
- B = 800 to 899
- C = 700 to 799
- D = 600 to 699
- F = < 600

Academic Integrity:

The integrity of the classes offered by any academic institution solidifies the foundation of its mission and cannot be sacrificed to expediency, ignorance, or blatant fraud. Therefore, instructors will enforce rigorous standards of academic integrity in all aspects and assignments of their courses. For the detailed policy of West Virginia University regarding the definitions of acts considered to fall under academic dishonesty and possible ensuing sanctions, please see the West Virginia University [Academic Standards Policy](#) below. Should you have any questions about possibly improper research citations or references, or any other activity that may be interpreted as an attempt at academic dishonesty, please see your instructor before the assignment is due to discuss the matter.

Inclusivity Statement

The West Virginia University community is committed to creating and fostering a positive learning and working environment based on open communication, mutual respect, and inclusion.

If you are a person with a disability and anticipate needing any type of accommodation in order to participate in your classes, please advise your instructors and make appropriate arrangements with [the Office of Accessibility Services](#).

More information is available at the [Division of Diversity, Equity, and Inclusion](#) as well.