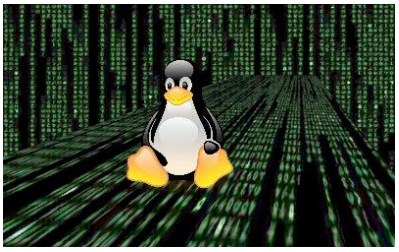
CYB-532 Spring 2021
Securing and Administering Linux Systems

Dates: 01/25-05/14/2021	**Mode:** • Online asynchronous	**Location:** http://blackboard.valpo.edu
Instructor: Sonja Streuber	**Office Hours:** M-F 8am – 8pm CST on Google Chat and by appointment	**Contact:** sonja.streuber@valpo.edu

Introduction



Welcome to CYB-532 Securing and Administering Systems in Linux Environments! This course discusses the secure administration of Linux server and client systems. The course will focus on security strategies in implementing Linux systems. Hands-on skill labs focus on Linux firewall design, the installation, configuration, and maintenance of Linux server environments. This course also examines common vulnerabilities and other security issues in Linux operating systems.

NOTE: This is **NOT** a Linux for Beginners course. It presumes that you are able to confidently use the command line to navigate around the file system, evaluate permissions, and write basic scripts.

Learning Objectives

Students who successfully complete this course will gain strong hands-on skills to administer and secure servers in two or more Linux distributions to follow enterprise-standard CIA best practices. Students will be able to:

- Configure various firewalls and network protocols
- Set up discretionary and mandatory access controls with multiple techniques
- Secure partitions, directories, and files using various encryption technologies
- Scan, audit, and harden Linux systems
- Set up logging and log security
- Configure and use various methods for vulnerability scanning and intrusion detection

Course Format

The format for this course is ONLINE ASYNCHRONOUS. This means that you will be working through the materials at your own pace with on-demand instructor support. However, the weekly deadlines for work submission apply as posted below.

Each Sunday evening, a communication from the instructor on Blackboard outlines the goals and tasks for the week. Generally, the work rhythm in this course is as follows:

- Monday: First weekly module--readings and videos with content-based quiz, Perusall annotations, Flipgrid, or other activity, due on Blackboard by 11:59 pm CST. Estimated time: 2 hours

- Wednesday: Second weekly module--readings and videos with application-based quiz and/ or collaborative coding assignment or discussion post, due on Blackboard by 11:59 pm CST. Estimated time: 2-3 hours
- Friday: Third weekly module--weekly lab assignment due on Blackboard by 11:59 pm CST. Estimated time: 3 hours.

ATTENDANCE POLICY: Attendance in this course is evaluated based on timely submission of assignments.

Textbooks & Materials

- **Textbook:**
  - Tevault, Donald (2020). *Mastering Linux Security and Hardening*. **SECOND EDITION**. Packt. ISBN 978-1-83898-177-8
- **Tools**:
  - A large-enough computer system to hold two complete Virtual Machines
  - Oracle Virtualbox at https://www.virtualbox.org
  - CentOS 7 and CentOS 8 at https://www.centos.org/download/
  - Ubuntu 20 Server at https://ubuntu.com/download/server
  - Cygwin at https://cygwin.com/install.html
  - Various free, open-source vulnerability scanning applications such as Snort, SecurityOnion, Lynis, OpenVAS, Kali, and more.

- **Other Resources:**
  - Buchanan, C., & Ramachandran, V. (2017). *Kali linux wireless penetration testing beginner's guide* - third edition (Third;3; ed.). GB: Packt Publishing. http://tinyurl.com/yacb4yk6
  - LaCroix, J. (2018). *Mastering ubuntu server* - second edition (2nd ed.) Packt Publishing. http://tinyurl.com/y8nedw33
  - Brash, R., & Naik, G. (2018). *Bash cookbook* (1st ed.) Packt Publishing. http://tinyurl.com/y8gvw5u6
  - Pelz, O. (2018). *Fundamentals of linux: Explore the essentials of the linux command line*. UK: Packt Publishing. http://tinyurl.com/y7o7urmb
  - LinkedIn Learning at Valparaiso University. Access at https://www.linkedin.com/learning/login-ent?redirect=https%3A%2F%2Fwww.linkedin.com%2Flearning%2F

Workload and Grading

Because this 3-credit course aims to build advanced practical skills, it requires SIGNIFICANT hands-on work. Plan on spending 8-9 hours a week on studying and applying the material

You will be completing the following tasks each week:

1. **Monday Moves (10 points each = 150 points)**. After studying the first module of the week, you will complete a short assessment that allows you to demonstrate your understanding of what you have just studied. That can be commenting on assigned reading or video viewing in Perusall

or Flipgrid, a quiz in Blackboard, researching a topic and posting it on the Discussion Board, or even posting a video of you performing an exercise--or a combination of these. Monday Work varies from week to week, but always focuses on the assigned materials. It CANNOT be made up and is due by 11:59 pm CST on the Monday of the week in which it is given.

2. **Wednesday Work (10 points each = 150 points)**. Typically, Wednesday Work consists of one or two short administration problems to help you explore and practice your new skills for any of the end-of-week labs. This is collaborative and shared work, often in a Discussion-thread or Flipgrid format. Wednesday Work CANNOT be made up and is due by 11:59 pm CST on the Wednesday of the week in which it is given.
3. **Friday Fun (10 points each=150 points)**: Some weeks contain a lab assignment about a theoretical, practical, or programming problem. This will extend the collaborative work from Wednesday and is most often in the form of a YouTube video recorded with Screencast-o-Matic or Screencastify. Solutions must be posted on Blackboard by 11:59 pm CST on FRIDAY. NO EMAIL SUBMISSIONS ACCEPTED.
4. **Final Exam (100 points)**: The final exam will be a comprehensive study of an assigned incident with remediation demonstration. It is a "take home exam." You will use Screen-Cast-O-Matic or Screencastify and your webcam to record your solution path and upload the file to YouTube. The YouTube settings must be as follows: Video must be unlisted, Title must include your name, the name of the case, and the name of this semester. Description must show a two-sentence summary of the central issue in your case. The due date for the Final Lab is as shown in Important Semester Dates.

Students can earn up to 280 points in this independent study. There will be no extra credit assignments.

Letter Grade Conversion:

A	A-	B+	B	B-	C+	C	C-	D+	D	D-	F
> 93%	90-93%	87-89.9%	83-86.9%	80-82.9%	77-79.9%	73-76.9%	70-72.9%	67-69.9%	63-66.9%	60-62.9%	< 60%

Assignment Submission, Late Work, and Academic Honesty

- **Assignment Submission:** All Assignments must be submitted on Blackboard. **BECAUSE OF FERPA LEGISLATION, I cannot accept any emailed assignments.**
- **Late Work:** Work is considered late if not posted to Blackboard by 11:59 pm CST of the day on which it is due. **Late work will lose 50% of the grade. If more than 1 week late, submitted work will earn only 1 point.**
- **Academic Honesty:** This course upholds the Valparaiso University Honor Code, which permits students to do their academic work in an atmosphere of responsible freedom. For you, this means that **all work you submit for this course must be your own**.
    - If you decide to include anyone else's words or code (from blogs, webpages, coding forums like GitHub or Stackoverflow, purchased solutions, etc.), you must:
        1. Give a clear **source citation** (including the exact location from which you copied these words or lines of code)

2. Include an **explanation in your own words** of what the cited passage means or what the copied code does, why it works, and why it is better than your own.

When the definition of unauthorized aid is in question, it is **your responsibility** to clarify your understanding of it with the instructor. Ignorance is not a valid excuse for violations of the Honor Code. Students should report suspected violations to the Honor Council.

In addition, you must write and sign with your name the following statement on all course work:

I have neither given nor received, nor have I tolerated others' use of unauthorized aid.

For more information about Valparaiso University's Academic Honor Code, case review cycles, and potential penalties, please refer to http://www.valpo.edu/student/honorcouncil/index.php

Any work in noncompliance the Valparaiso University Honor Code will receive 0 points and be referred to the Graduate School for adjudication.

Schedule

Week	Start Date (2021)	Topic	Applicable Materials and Tools (includes LinkedIn Learning courses where applicable)	Graded Work Due • M=Mon 11:59 pm CST • W= Wed 11:59 pm CST • F=Fri 11:59 pm CST
1	1/25	Course Introduction	Tevault Chapter 1	Monday Moves = M Wednesday Work = W Friday Fun = F
2	1/31	Running Linux in a Virtual Environment and Keeping Linux Updated	Tevault Chapter 1	Monday Moves = M Wednesday Work = W Friday Fun = F
3	2/07	Securing User Accounts	Tevault Chapter 2	Monday Moves = M Wednesday Work = W Friday Fun = F
4	2/14	Securing Your Server with a Firewall (1)	Tevault Chapter 3	Monday Moves = M Wednesday Work = W Friday Fun = F
5	2/21	Securing Your Server with a Firewall (2)	Tevault Chapter 4	Monday Moves = M Wednesday Work = W Friday Fun = F
6	2/28	Encryption Technologies	Tevault Chapter 5	Monday Moves = M Wednesday Work = W Friday Fun = F
7	3/07	SSH Hardening	Tevault Chapter 6	Monday Moves = M Wednesday Work = W Friday Fun = F
8	3/14	Mastering Discretionary Access Control	Tevault Chapter 7	Monday Moves = M Wednesday Work = W Friday Fun = F
9	3/21	Access Control Lists and Shared Directory Management	Tevault Chapter 8	Monday Moves = M Wednesday Work = W Friday Fun = F
10	3/28	Implementing Mandatory Access	Tevault Chapter 9	Monday Moves = M Wednesday Work = W Friday Fun = F

		Control with SELinux and AppArmor		
11	4/07	Kernel Hardening and Process Isolation	Tevault Chapter 10	Monday Moves = M Wednesday Work = W Friday Fun = F
12	4/11	Scanning, Auditing, and Hardening	Tevault Chapter 11	Monday Moves = M Wednesday Work = W Friday Fun = F
13	4/18	Logging and Log Security	Tevault Chapter 12	Monday Moves = M Wednesday Work = W Friday Fun = F
14	4/25	Vulnerability Scanning and Intrusion Detection	Tevault Chapter 13	Monday Moves = M Wednesday Work = W Friday Fun = F
15	5/02	Security Tips and Tricks	Tevault Chapter 14	Monday Moves = M Wednesday Work = W Friday Fun = F
FINAL	5/11	Take-Home Final due at the end of the Special Period--Professional on Tuesday, 5/11 at 10:00 am CST. **No late submissions will be considered.**		**Course Final Exam**

APPENDIX A: University Policies

Diversity and Inclusion

Valparaiso University aspires to create and maintain a welcoming environment built on participation, mutual respect, freedom, faith, competency, positive regard, and inclusion. This course will not tolerate language or behavior that demeans members of our learning community based on age, ethnicity, race, color, religion, sexual orientation, gender identity, biological sex, disabilities (visible and invisible), socio-economic status, or national origin. The success of this class relies on all students' contribution to an anti-discriminatory environment where everyone feels safe, welcome, and encouraged to engage, to explore, and ultimately, "to embark on a rewarding personal and professional journey" (Pres. Heckler).

Title IX

Valparaiso University strives to provide an environment free of discrimination, harassment, and sexual misconduct (sexual harassment, sexual violence, dating violence, domestic violence, and stalking). If you have been the victim of sexual misconduct, we encourage you to report the incident. If you report the incident to a University faculty member or instructor, she or he must notify the University's Title IX Coordinator about the basic facts of the incident. Disclosures to University faculty or instructors of sexual misconduct incidents are not confidential under Title IX. Confidential support services available on campus include: Sexual Assault Awareness & Facilitative Education Office "SAAFE" (219-464-6789), Counseling Center (219-464-5002), University Pastors (219-464-5093), and Student Health Center (219-464-5060). For more information, visit http://www.valpo.edu/titleix/ .

Access and Accommodation Services

The Access & Accommodations Resource Center (AARC) is the campus office that works with students to provide access and accommodations in cases of diagnosed mental or emotional health issues, attentional or learning disabilities, vision or hearing limitations, chronic diseases, or allergies. You can contact the office at aarc@valpo.edu or 219.464.5206. Students who need, or think they may need, accommodations due to a diagnosis, or who think they have a diagnosis, are invited to contact AARC to arrange a confidential discussion with the AARC office. Further, students who are registered with AARC **are required to contact their professor(s) if they wish to exercise the accommodations** outlined in their letter from the AARC.

Academic Support

To get help, use the Academic Success Center (ASC) online directory (valpo.edu/academicsuccess) or contact the ASC (academic.success@valpo.edu) to help point you in the right direction for academic support resources for this course. Valpo's learning centers offer a variety of programs and services that provide group and individual learning assistance for many subject areas. These learning centers include:

- Tutoring Lab: Serves the academic needs of undergraduate and graduate students – tutors offer suggestions on organization of papers, assist in research and citations, and help in understanding difficult assignments. Additional one on one tutoring is also available.
- Writing Center: Writing Consultants provide proofreading and editing assistance for papers and assignments.

Class Cancellations

Notifications of class cancellations will be made through Blackboard with as much advance notice as possible. It will be both posted on Blackboard and sent to your Valpo e-mail address. If you don't check your Valpo e-mail account regularly or have it set-up to be forwarded to your preferred e-mail account,

you may not get the message. Please check Blackboard and your Valpo e-mail (or the e-mail address it forwards to) before coming to class.

Emergencies

VU's Emergency Notification System (ENS) uses multiple forms of communication, including e-mail, building alarms, outdoor sirens, message boards, computer alerts, Twitter, and public address messaging. Please review the specific procedures for this class found in Blackboard. Remember: "Siren inside, GO outside; Siren outside, GO inside." To evacuate, gather your personal belongings quickly and proceed to the nearest exit. Do not use the elevator. To shelter in place, move away from the windows and stay low to the ground; lock or barricade the door if there is a threat of violence.

APPENDIX B: Learning Objectives

Student Learning Objectives—Valparaiso University

1. Demonstrate theoretical and practical knowledge as well as the intellectual skills and creative capacities pertinent to their respective fields of study.
2. Solve both conceptual and applied problems by integrating broad-based knowledge, evidence-based reasoning, and informational literacy.
3. Practice experiential, interdisciplinary, and collaborative learning in both academic and co-curricular pursuits.
4. Communicate effectively in oral, written, and digital forms in increasingly complex contexts.
5. Engage in cross-cultural dialogue and experiences with the requisite knowledge to succeed in a diverse, global community.
6. Develop character, integrity, and wisdom as they discern their vocations and prepare to ethically lead and serve church and society.

httpF://www.valpo.edu/institutional-effectiveness/files/2017/08/University-wide-SLOs.pdf

Student Learning Objectives—Computer Science Majors (Undergraduate)

1. To understand and practice methods of inquiry and strategies of interpretation within the student's field of study.
    a. Students will master several programming environments.
    b. Students will learn to identify and isolate problems.
2. To master the knowledge and skills pertinent to the student's field of study.
    a. Students will acquire an extensive technological vocabulary.
    b. Students will become comfortable with a wide range of technology environments.
3. To effectively articulate the ideas, concepts, and methods through written and oral presentation.
    a. Students will be taught how to make formal oral presentations and be required to give 6 such presentations during their program.
    b. Students will write numerous thorough papers requiring extensive research. They will be required to use the services of the writing center.
4. To understand the connection between their knowledge and skills on one hand and their professional identity, responsibilities, and demands on the other.
    a. Students will understand the implications of legal and professional regulations as they relate to information technology.
    b. Students will study how technology can be made available to people that are traditionally less advantaged.
5. To integrate knowledge and methods of their study with cognates and other disciplines.
    a. Students will learn techniques of modeling data from other disciplines.
    b. Students will study human factors in IT.
6. To practice ethical and cultural sensitivity as it relates to professional and personal responsibility.
    a. Students will examine a wide range of ethical issues related to technology and the potential side effects on people and the environment.
    b. Students will explore the relationship between IT and ethnic and cultural diversity.

Student Learning Objectives—Graduate School

1. Students will understand and practice methods of inquiry and strategies of interpretation within the student's field of study.
2. Students will master the knowledge and skills pertinent to the student's field of study.
3. Students will effectively articulate the ideas, concepts, and methods through written and oral presentation.
4. Students will understand the connection between their knowledge and skills on the one hand and their professional identity, responsibilities, and demands on the other.
5. Students will integrate knowledge and methods of their study with cognates and other disciplines.
6. Students will study, reflect upon, and practice ethical behavior and cultural sensitivity as they relate to professional and personal responsibility.

Student Learning Objectives—Information Technology Program (Graduate)

1. To understand and practice methods of inquiry and strategies of interpretation within the student's field of study.
   1A. Students will master several programming environments.
   1B. Students will learn to identify and isolate problems.
2. To master the knowledge and skills pertinent to the student's field of study.
   2A. Students will acquire an extensive technology related vocabulary.
   2B. Students will become comfortable using a wide range of technology environments.
3. To effectively articulate the ideas, concepts, and methods through written and oral presentation.
   3A. Students will be taught how to make formal, oral presentations and be required to give 6 such presentations during their program.
   3B. Students will write numerous, thorough papers requiring extensive research. They will be required to use the services on the writing center.
4. To understand the connection between their knowledge and skills on one hand and their professional identity, responsibilities, and demands on the other.
   4A. Students will understand the implications of legal and professional regulations as they relate to information technology.
   4B. Students will study how technology can be made available to people that are traditionally less advantaged.
5. To integrate knowledge and methods of their study with cognates and other disciplines.
   5A. Students will learn techniques of modeling data from other disciplines.
   5B. Students will study human factors in IT.
6. To practice ethical and cultural sensitivity as it relates to professional and personal responsibility.
   6A. Students will examine a wide range of ethical issues related to technology and the potential effects on people and the environment.
   6B. Students will explore the relationship between IT and ethnic and cultural diversity.

APPENDIX

Student Learning Objectives—Graduate School

1. Students will understand and practice methods of inquiry and strategies of interpretation within the student's field of study.
2. Students will master the knowledge and skills pertinent to the student's field of study.
3. Students will effectively articulate the ideas, concepts, and methods through written and oral presentation.
4. Students will understand the connection between their knowledge and skills on the one hand and their professional identity, responsibilities, and demands on the other.
5. Students will integrate knowledge and methods of their study with cognates and other disciplines.
6. Students will study, reflect upon, and practice ethical behavior and cultural sensitivity as they relate to professional and personal responsibility.

Student Learning Objectives—Information Technology Program

1. To understand and practice methods of inquiry and strategies of interpretation within the student's field of study.
   1A. Students will master several programming environments.
   1B. Students will learn to identify and isolate problems.
2. To master the knowledge and skills pertinent to the student's field of study.
   2A. Students will acquire an extensive technology related vocabulary.
   2B. Students will become comfortable using a wide range of technology environments.
3. To effectively articulate the ideas, concepts, and methods through written and oral presentation.
   3A. Students will be taught how to make formal, oral presentations and be required to give 6 such presentations during their program.
   3B. Students will write numerous, thorough papers requiring extensive research. They will be required to use the services on the writing center.
4. To understand the connection between their knowledge and skills on one hand and their professional identity, responsibilities, and demands on the other.
   4A. Students will understand the implications of legal and professional regulations as they relate to information technology.
   4B. Students will study how technology can be made available to people that are traditionally less advantaged.
5. To integrate knowledge and methods of their study with cognates and other disciplines.
   5A. Students will learn techniques of modeling data from other disciplines.
   5B. Students will study human factors in IT.
6. To practice ethical and cultural sensitivity as it relates to professional and personal responsibility.
   6A. Students will examine a wide range of ethical issues related to technology and the potential effects on people and the environment.
   6B. Students will explore the relationship between IT and ethnic and cultural diversity.