1. **FOUNDATIONS OF CYBERSECURITY:**

In this course, you will learn the primary job responsibilities and core skills of those who work in the field of cybersecurity. You will explore the eight Certified Information Systems Security Professional (CISSP) security domains, various security frameworks and controls, as well as a foundational security model called the confidentiality, integrity, and availability (CIA) triad. You will also be introduced to some common tools used by security analysts that help protect organizations and people alike.

1. [**Foundations of Cybersecurity**](https://www.coursera.org/learn/foundations-of-cybersecurity/home/week/1)— *(current course)* Explore the cybersecurity profession, including significant events that led to the development of the cybersecurity field and its continued importance to organizational operations. Learn about entry-level cybersecurity roles and responsibilities.

**NO LABS DONE IN THIS COURSE**

1. **Play It Safe: Manage Security Risks:**

By the end of this course, you will develop a greater understanding of the eight Certified Information Systems Security Professional (CISSP) security domains, as well as specific security frameworks and controls. You’ll also be introduced to how to use security tools and audits to help protect assets and data. These are key concepts in the cybersecurity field, and understanding them will help you keep organizations, and the people they serve, safe from threats, risks, and vulnerabilities.

1. [**Play It Safe: Manage Security Risks**](https://www.coursera.org/learn/manage-security-risks/home/week/1)— *(current course)* Identify how cybersecurity professionals use frameworks and controls to protect business operations and explore common cybersecurity tools.

**NO LABS DONE IN THIS COURSE**

1. **Connect and Protect: Networks and Network Security**

By the end of this course, you will develop a greater understanding of network architecture, operations, intrusion tactics, common types of network vulnerabilities and attacks, and how to secure networks. You’ll also be introduced to common network protocols, firewalls, virtual private networks (VPNs), and system hardening practices.

1. [**Connect and Protect: Networks and Network Security**](https://www.coursera.org/learn/networks-and-network-security/home/week/1)— *(current course)* Gain an understanding of network-level vulnerabilities and how to secure networks.

**NO LABS DONE IN THIS COURSE**

1. **Tools of the Trade: Linux and SQL**

By the end of this course, you will develop a greater understanding of the basics of computing that will support your work as a security analyst. You will learn foundational concepts related to understanding operating systems, communicating with the Linux operating system through commands, and querying databases with Structured Query Language (SQL). These are key concepts in the cybersecurity field and understanding them will help you keep organizations secure.

1. [**Tools of the Trade: Linux and SQL**](https://www.coursera.org/learn/linux-and-sql/home/week/1)— *(current course)* Explore foundational computing skills, including communicating with the Linux operating system through the command line and querying databases with SQL.

**Module 2: Activity: Install software in a Linux distribution**

**Introduction**

In this lab, you’ll learn how to install and uninstall applications in Linux. You’ll use Linux commands in the Bash shell to complete this lab. You’ll also use the Advanced Package Tool (APT) package manager to install and uninstall the Suricata and tcpdump applications.

**What you’ll do**

You have multiple tasks in this lab:

* Confirm APT is installed in Bash--- **$apt**
* Install Suricata with APT— **$sudo apt install suricata**
* Uninstall Suricata with APT- **$sudo apt remove suricata**
* Install tcpdump with APT- **$sudo apt install tcpdump**
* List all the installed applications- **$apt list --installed**
* Reinstall Suricata with APT- $**sudo apt install suricata**

**Module 2: Activity: Examine input and output in the shell**

**Introduction**

In this lab, you’ll use the **echo** command to examine how input is received and how output is returned in the shell. You’ll also use other Linux commands in the Bash shell to explore more about input and output and other basic functions of the shell.

**What you’ll do**

You have multiple tasks in this lab:

* Generate output in the shell the **echo** command - **$echo hello**
* Perform basic calculations the **expr** command - **$expr 32 – 8, expr 3500 \* 12**
* Clear the shell window the **clear** command- **$clear**

**Module 3: Activity: Find files with Linux commands**

**Introduction**

In this lab, you’ll learn how to navigate Linux file structure, locate files, and read file contents. You’ll use Linux commands in the Bash shell to complete these steps.

**What you’ll do**

You have multiple tasks in this lab:

* Find your current working directory and display its contents-- **$pwd, $ls,$ls-l**
* Navigate to a directory and list subdirectories- $**cd /ex1/ex2**
* Display the contents of a file- **$cat “filename”**
* Display the first 10 lines of a file- **$head -n (number of lines you want) “filename”**

**Module 3: Activity: Filter with grep**

**Introduction**

In this lab, you’ll learn how to use the **grep** command and piping to search for files and return specific information. You’ll get information from different files, including server log files and user data files. You’ll use Linux commands in the Bash shell to complete these steps.

**What you’ll do**

You have multiple tasks in this lab:

* Search for error messages in a file- **$grep 'error' server\_logs.txt**
* Search for files that contain a specific string- **$ls | grep “Q1”**- Gives all the files that has Q1 name in it
* Search for information in user files- **$grep “String that you want to search for” “file name”**

**Eg: $grep “Human Resources” “Q1\_added\_users.txt”**

**Module 3: Activity: Manage files with Linux commands**

**Introduction**

In this lab, you’ll learn how to manage and modify files in a Linux file structure. You’ll use Linux commands in the Bash shell to complete these steps. You’ll also use the nano text editor to add text to a file.

**What you’ll do**

You have multiple tasks in this lab:

* Create a new directory- **$mkdir logs (Logs is the directory name)**
* Remove a directory- **$rmdir temp (Temp directory is removed)**
* Move a file and delete a file- **$mv “File name” (file path), $rm “file name”**
* Create a file and add text using nano- **$touch “file name that u want to give”, $nano “file name”**

**After entering the text, you can use “Ctrl+x” to exit and Yes to confirm.**

**Module 3: Activity: Manage authorization**

**Introduction**

In this lab, you’ll learn how to examine and manage file permissions. These skills can be used when configuring user authorization. You’ll use Linux commands in the Bash shell to complete this lab. While completing this lab please take screenshots or write down the commands you use in the Bash shell.

**What you’ll do**

You have multiple tasks in this lab:

* Check permissions for files in a directory- **$ls -l(Consists of permissions for owner, Group & Others), $ls -a(Gives the list of all the hidden files)**
* Check for incorrect file permissions and change permissions as needed

To change the permissions:

* 1. Chmod o-w project.txt(It removes the write permission for other users for the file “Project.txt”)
  2. Chmod g+r project.txt( It gives the read permission for the group users for the file “Project.txt”)
* Remove unauthorized access to a directory

**Module 3: Activity: Add and manage users with Linux commands**

**Introduction**

In this lab, you’ll learn how to add users and manage user access in a system. These skills can be used when working with authentication technology. You’ll use Linux commands in the Bash shell to complete this lab.

**What you’ll do**

You have multiple tasks in this lab:

* Add a new employee:

The useradd command is used to create a new user, and sudo is used to run the command with administrative privileges. Depending on the system, you might need superuser access. Eg: **$sudo useradd “name**

The usermod command modifies the user properties, and the -g option is used to set the **primary group** of the user. This command assigns research\_team as the primary group for researcher9.

Eg: $sudo usermod -g research\_team(Team name) researcher 9 (employee name)

* Change ownership of a file

sudo chown researcher9 /home/researcher2/projects/project\_r.txt

The chown command changes the ownership of a file or directory. In this command:

* + sudo is used to execute the command with administrative privileges.
  + chown researcher9 sets researcher9 as the new owner of the specified file.
  + /home/researcher2/projects/project\_r.txt is the full path to the file you want to change ownership of.

After running this command, researcher9 will be the new owner of the project\_r.txt file.

* Add the new employee to a new group

sudo usermod -a -G sales\_team researcher9

Explanation:

* + sudo: Run the command with administrative privileges.
  + usermod: Command to modify a user account.
  + -a: Append the user to the specified group(s) (used with -G).
  + -G sales\_team: Specifies the secondary group to which you are adding the user.

Using -a ensures that researcher9 is **added** to the sales\_team group **without removing** them from any other existing groups, including their primary group (research\_team).

* Delete the employee from the system

sudo userdel researcher9 is the command which will delete the user

**Module 4: Activity: Perform a SQL query**

**Introduction**

In this lab, you’ll learn how to retrieve information from a database using SQL. You’ll be using the MariaDB shell to run your SQL queries.

**What you’ll do**

You have multiple tasks in this lab:

* Return information on employee devices
* Examine login attempts
* Sort the data returned from a query

**Module 4: Activity: Filter a SQL query**

**Introduction**

In this lab, you’ll apply basic filters to SQL queries to retrieve information from a database. You’ll use SQL to get specific information about employees, their machines, and the departments they’re in. You’ll be using the MariaDB shell to run SQL queries.

**What you’ll do**

You have multiple tasks in this lab:

* Return information on machines and their operating systems
* Filter for machines with a specific operating system
* Filter for employees in specific departments
* Filter for employees who use specific machines

**Module 4: Activity: Apply more filters in SQL**

**Introduction**

In this lab, you’ll apply more filters to SQL queries to retrieve information from a database. You’ll use common operators in SQL to filter by specific dates and times. You’ll be using the MariaDB shell to run your SQL queries.

**What you’ll do**

You have multiple tasks in this lab:

* Filter for login attempts made after a certain date
* Filter for login attempts made in a certain date range
* Filter for login attempts made at a certain time
* Filter for login attempts by ID

**Module 4: Activity: Filter with AND, OR, and NOT**

**Introduction**

In this lab, you’ll use the AND, OR, and NOT operators in SQL to filter for information. You’ll use SQL to get specific information about employees, their machines, and the departments they’re in. You’ll be using the MariaDB shell to run SQL queries.

**What you’ll do**

You have multiple tasks in this lab:

* Filter for login attempts that occurred after hours
* Filter for login attempts on specific dates
* Filter for login attempts from specific locations
* Filter for information on employees in specific departments
* Filter for information on employees not in a specific department

**Module 4: Activity: Complete a join**

**Introduction**

In this lab, you’ll use INNER JOIN, LEFT JOIN, and RIGHT JOIN in SQL to retrieve information from two different tables. You’ll use these different types of SQL joins to join data from separate machines, employees, and login attempts tables. You’ll be using the MariaDB shell to run SQL queries.

**What you’ll do**

You have multiple tasks in this lab:

* Use an inner join to find information on employees and their machines
* Use a left join and right join to find information on employees and their machines
* Use an inner join to find information on employees and their login attempts

1. **Assets, Threats & Vulnerabilities:**

By the end of this course, you’ll build an understanding of the wide range of assets organizations must protect. You’ll explore many of the most common security controls used to protect valuable assets from risk. You’ll also discover the variety of ways assets are vulnerable to threats by adopting an attacker mindset.

1. [**Assets, Threats, and Vulnerabilities**](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/home/week/1)— *(current course)* Learn about the importance of security controls and developing a threat actor mindset to protect and defend an organization’s assets from various threats, risks, and vulnerabilities.

**Module 2: Activity: Decrypt an encrypted message**

**Introduction**

In this lab, you'll complete a series of tasks to obtain instructions for decrypting an encrypted file. Encryption of data in use, at rest, and in transit is critical to security functions. You'll use the Linux skills you have learned to uncover the clues needed to decode a classical cipher, restore a file, and reveal a hidden message.

**What you’ll do**

You have multiple tasks in this lab:

* List the contents of a directory
* Read the contents of files
* Use Linux commands to revert a classical cipher back to plaintext
* Decrypt an encrypted file and restore the file to its original state

*The tr command translates text from one set of characters to another, using a mapping. The first parameter to the tr command represents the input set of characters, and the second represents the output set of characters. Hence, if you provide parameters “abcd” and “pqrs”, and the input string to the tr command is “ac”, the output string will be “pr".*

1. **Sound the Alarm: Detection and Response**

By the end of the course, you will have hands-on practice using resources like network protocol analyzers, intrusion detection systems (IDS), and security information event management (SIEM) tools to capture network packets and analyze log data.

1. [**Sound the Alarm: Detection and Response**](https://www.coursera.org/learn/detection-and-response/home/week/1)— *(current course)* Understand the incident response lifecycle and practice using tools to detect and respond to cybersecurity incidents.

**Module 2: Activity: Analyze your first packet**

**Introduction**

In this lab activity, you'll learn how to open and analyze a packet capture file using Wireshark.

**What you’ll do**

You have multiple tasks in this lab:

* Open a packet capture file using Wireshark
* Examine packet information
* Apply display filters

**Module 2: Activity: Capture your first packet**

**Introduction**

In this lab activity, you'll capture and analyze live network traffic using tcpdump. You'll use Linux commands in the Bash shell to complete these steps.

**What you’ll do**

You have multiple tasks in this lab:

* Identify available network interfaces
* Use tcpdump to capture live network traffic
* Save network traffic to a packet capture file
* Filter the packet capture data