

GenCyber 2024 Pre-Camp Engagement

1: Review the NICE Framework Work Roles and KSAs

2: Review RPi Videos and Documentation

3: Complete the GenCyber Survey



NICE Framework Work Roles and KSAs

- Created by NIST (National Institute of Standards and Technology).
- Uses a common language to define and organize different jobs (Work Roles) in cybersecurity.
- Describes what knowledge (K) and skills (S) and abilities (A) are needed for these roles.
- Helps make sure that everyone in cybersecurity can talk to each other and understand each other.
- Important for training people and making sure they are ready to do cyber security jobs well.
- [NICE Framework Work Roles Weblink](#) (with all work roles to explore)

Key Work Roles

Click each work role title to find out more:

[Exploitation Analyst](#): This role involves finding gaps in information gathering and access, which can be closed using cyber collection/preparation. It uses approved tools and techniques to enter specific computer networks.

[Secure Software Assessor](#): This role involves checking the security of new or existing computer programs and software to find any problems and give clear advice on what to do next.

[Cyber Defense Analyst](#): This role involves looking at data from different cybersecurity tools to reduce risks.

[Systems Administrator](#): This role involves creating and managing parts of a computer system while following rules about security. It includes installing and updating hardware and software, managing user accounts, backing up and recovering information, and making sure security measures are in place.

[Cyber Defense Forensics Analyst](#): This role involves studying digital clues from computer security problems to find helpful information that can fix weaknesses in systems and networks.

[AI/ML Specialist](#): This role involves creating and improving applications and tools that use artificial intelligence. Your goal is to make sure these programs help achieve important goals effectively.

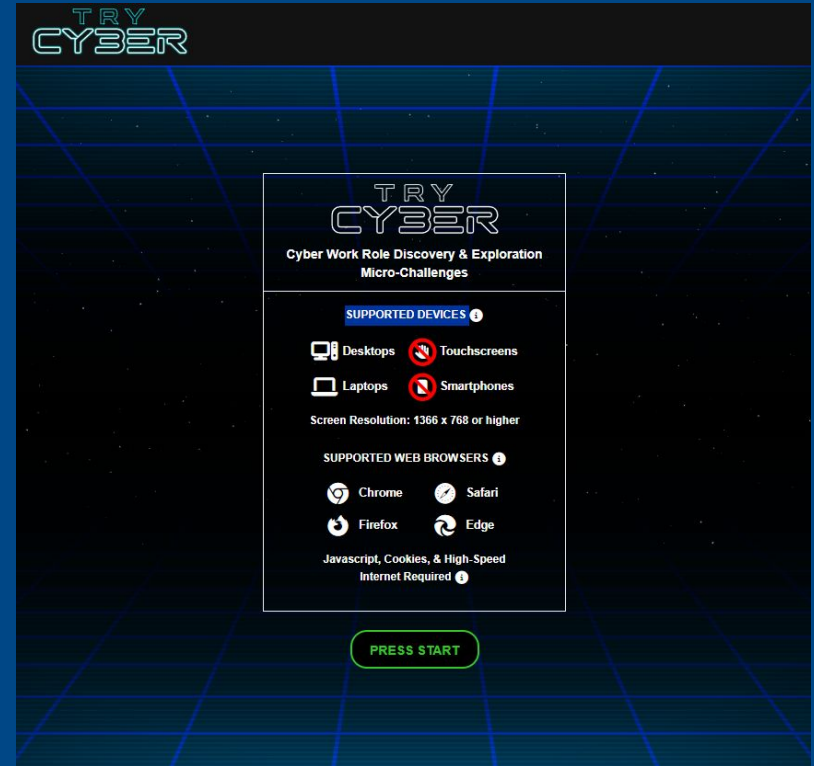
TRY CYBER

TRY CYBER is a guided simulator of work roles with mini-challenges to simulate real tasks for the work roles.

[TRY CYBER Link](#)

For extra guidance, check out the next slides:

Slides [5](#), [6](#)



TRY CYBER Challenges for Work Roles

Click the corresponding pictures on the site to do a challenge for each work role

Exploitation Analyst:

Vulnerability Assessment Analyst

Difficulty: ☆ ☆

Help Itzel perform a security audit on one of the university's workstations. [NICE Framework T0549]

Mentor



Secure Software Assessor:

Technical Support Specialist Adv.

Difficulty: ☆ ☆

Help Tomás resolve support tickets related to locked user accounts. [NICE Framework T0468]

Mentor



Cyber Defense Analyst:

Cyber Defense Analyst

Difficulty: ☆ ☆ ☆

Assist Noah in analyzing suspicious network traffic and identifying threats. [NICE Framework T0023]

Mentor



Systems Administrator:

Systems Administrator

Difficulty: ☆

Assist Skyla in managing system privileges by adding users to privileged groups. [NICE Framework T0144]

Mentor



Cyber Defense Forensics Analyst:

Forensics Analyst

Difficulty: ☆ ☆

Help Indigo scan digital evidence for malicious software. [NICE Framework T0285]

Mentor



AI/ML Specialist:

Data Analyst

Difficulty: ☆ ☆

Help Ivy identify troubling trends in the intrusion prevention software's logs. [NICE Framework T0349]

Mentor



TRY CYBER Navigation

The TRY CYBER interface is shown with a dark theme. On the left is a sidebar with icons for Trash, Home, Terminal Emulator, and Materials. The main area displays a Linux desktop environment. On the right is a vertical navigation panel with three tabs: Info, Chat, and Report. The Info tab is active, showing a welcome message and instructions. Three callout boxes with arrows point to the tabs: a blue box for Info, a red box for Chat, and a yellow box for Report.

TRY CYBER

26 Jun, 00:13

TIME REMAINING: 19 MINUTES End Challenge

Info

Welcome to Your Challenge Workspace!

We are excited you are here and interested in trying out this cyber work role!

This is the **Info Tab** of the **Main Panel**.

From this workspace, you will be able to:

- Interact with a cyber work role mentor
- Attempt the micro-challenge
- Track your micro-challenge progress
- End your micro-challenge attempt

Should you require credentials for anything within the provided Linux VM, use the following:

Username: `playerone`

Password: `password123`

Note: The provided password is NOT an example of a secure password and is only provided for ease of use.

Interacting With the Mentor

You can interact with your cyber work role mentor via a scripted text chat. You can access the chat interface by opening the **Chat Tab** of the **Main Panel**.

Attempting the Micro-Challenge

Each micro-challenge contains **two tasks**, which will be assigned to you by the work role mentor within the **Chat**

Chat

Report

Terminal Emulator

Trash

Home

Materials

The info tab always appears with basic information about the challenge

The chat tab always appears with the directions and interactive guidance of the "mentor"

The report tab may appear for you to "type" in your report requested by your mentor

T	L	✓	Report Entry for bruteforce-1.pcap
A	I		
S	S		
K	T	✓	Report Entry for bruteforce-2.pcap

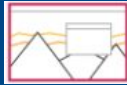
Raspberry Pi Videos and Documentation

Click each link to review the following documentation:

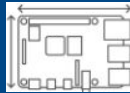
1. [Getting Started](#)



2. [Raspberry Pi OS](#)

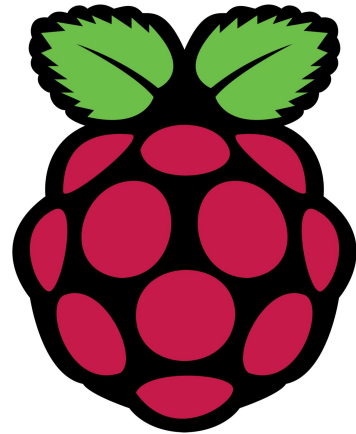


3. [Raspberry Hardware](#)



Here's the link if you want to explore more:

[Raspberry Pi \(RPi\) Website](#)



GenCyber Survey

Complete the
Google Form to
show off what
you learned!

GenCyber Pre-Engagement Survey

Complete the survey to show what you learned

kida.ibe@gmail.com [Switch account](#)

Not shared

* Indicates required question

What is your full name? *

Your answer

Which cybersecurity roles interested you the most? (List your top 3) *

Your answer

Name one Knowledge, one Skill, and one Ability for Exploitation Analysis (Exploitation Analyst) *

Your answer

Name one Knowledge, one Skill, and one Ability for 1 Software Security Assessment (Software Security Assessor).

Your answer

