

Mapping Low Cost and Open Source Labs to the NICE Workforce Framework and CAE KU's

Chris Simpson,
Director National University Center for
Cybersecurity

Agenda

- Background
- Examples of free labs and how we use them
- Mapping labs to the NICE Framework and KU's

Background

- Hands on labs are a critical component of any cybersecurity program and a requirement to become an NSA/DHS Center of Academic Excellence
- Several ways to deliver lab content
 - Develop and deploy labs on internal or outsourced infrastructure
 - Utilize labs from external lab providers
 - Utilize free grant resourced labs
 - Use free and open source labs
- Managing an internal lab environment is expensive

Challenges of Running an Internal Lab

- Help Desk
 - Academic vs Technical issues
 - Hours of operation
 - Student complete school work in the evening and on weekends
 - “Ticket Management”
- Admin access to systems
- Developing lab content
- Cost

Finding Outsourced Labs

- “Word of Mouth”
- Textbook Vendors
- Vendor booths
- Google

Challenges of Free Labs

- Downtime
- Support
- Updates
- No single vendor provides everything you need
- Publicly available answers
- Course coverage of lab content
- Faculty preparation
- Vendor lab changes

Free/Freemium Providers

- Not an official endorsement from National University

Providers

(No particular order)

Immersive Labs
(Free)

NICE Challenge
(Free)

Over the Wire
(Free)

PicoCTF (Free)

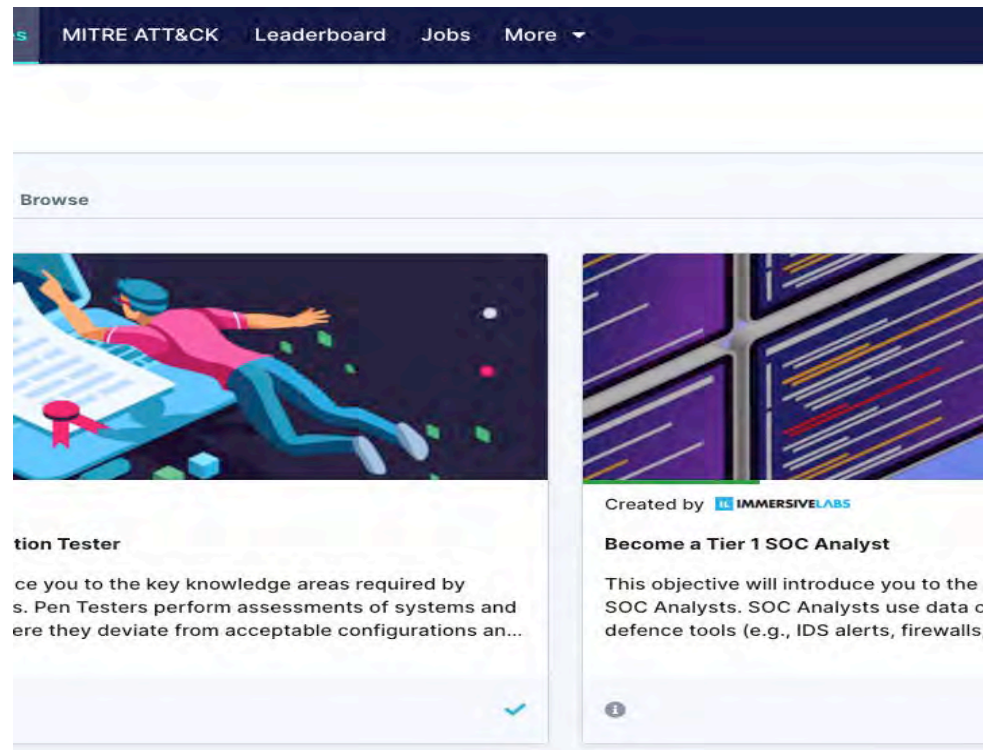
Hack The Box
(Freemium)

TryHackMe.com
(Freemium)

Blue Team Labs
(Freemium)

Immersive Labs Digital Cyber Academy

- Available to students, Veterans, and Neurodivergent community
- Question based, virtual machine based and scenario based labs



Immersive Labs

Badging

Large variety of topics

Novice to “Ninja”

Knowledge + Hands on

Rankings

The image displays the Immersive Labs website interface. At the top, a banner features the text "Labs" and "Our labs require research, we encourage analytical thinking, curiosity and problem solving. If you really like a challenge, check out our Immersive Originals series." Below the banner, there's a "Filter" button and a search icon. The main content area is divided into four columns, each representing a different category of labs:

- Knowledge:** Cover the fundamentals of cyber security with our series of introductory labs on cyber theory and industry scenarios.
Start Lab: What Is Risk?
- Tools:** From simple to advanced, this is where you will learn to master the tools of the cyber security world and the build your own tools.
Start Lab: Introduction to Command & Control Frameworks
- Techniques:** Time to flex those cyber skills! From ethical web hacking to malware analysis - Immersive Labs has you covered.
Start Lab: Web Applications: Page Source Review
- Immersive Originals:** (Love a challenge? So do we! These are our most Immersive Originals and are the ones that will test your skills to the limit.)
Start Lab: Immersive Labs and Your Employer

Below these categories, there's a "Secure Code" section with a description: "Learn the skills you'll need to be able to identify, exploit, secure and validate...".

At the bottom, there's a "League Table Leaderboard" table showing the top 12 teams:

POSITION	AVATAR	USER	POINTS
1		Tech Vets	2883620
2		New York University	1692245
3		Edinburgh Napier University	1439130
4		National University of Ireland Galway	1270940
5		University of South Wales	1254385
6		DCA HSLU Lucerne University of Applied Sciences	1219620
7		Singapore Institute of Technology	1137050
8		Dakota State University	1079600
9		Nanyang Polytechnic	931885
10		Lancaster University	860940
11		Institute of Technical Education	812470
12		National University	735380



Desktop

Applications



Trash



File System



Home



LabFiles



Terminator



Ghidra



Chromium

Lab Progress

13%

Tasks

1. Open the PCAP file located in the /labfiles/PCAPBasics/ directory.
2. Analyse the PCAP file, answer the questions and complete the lab.

Question 1 of 8

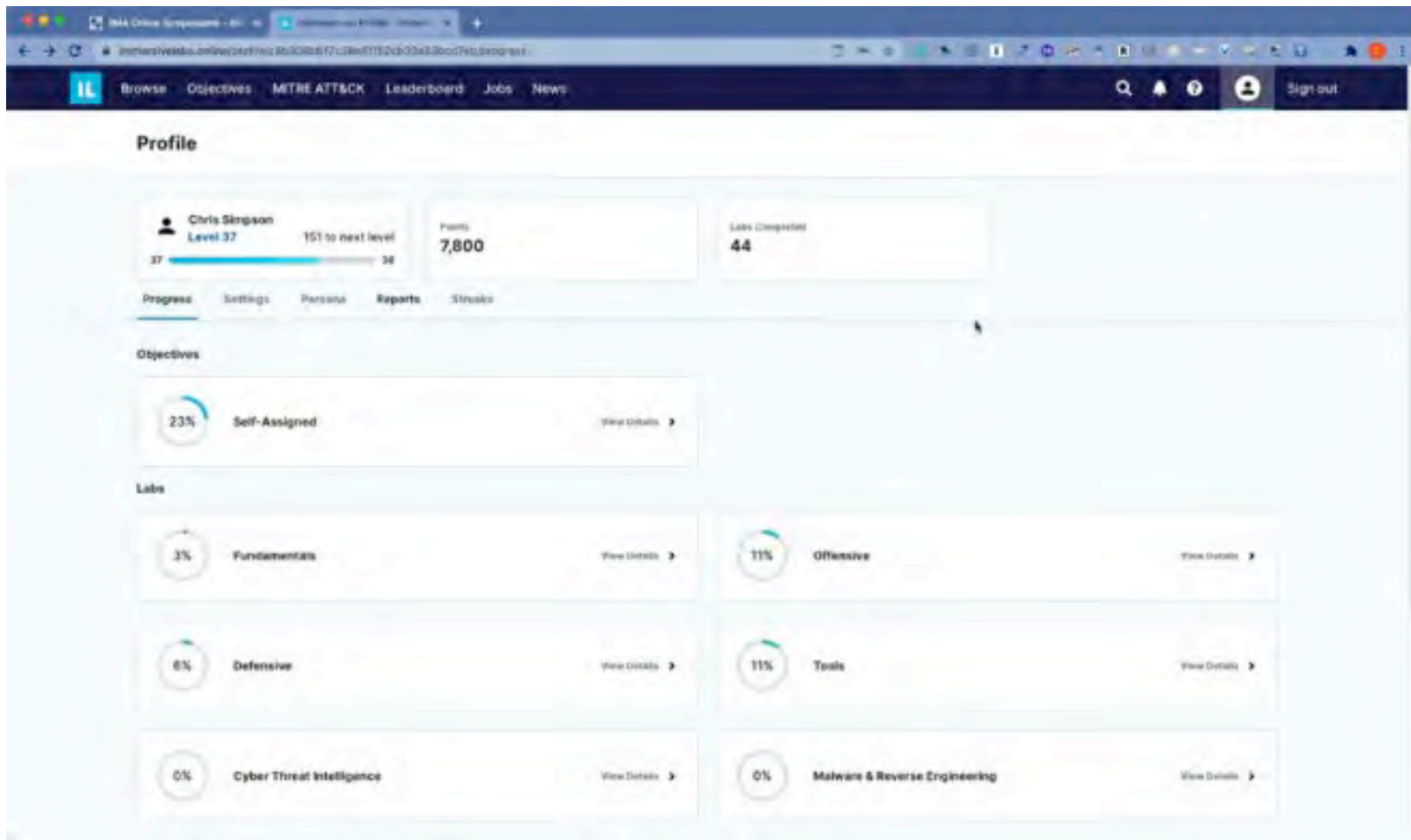
What is the server name sought in the first DNS request that is issued by the client?

Question 2 of 8

What is the first IP address returned in the DNS response for the domain in Q1?

Question 3 of 8

What is the browser user agent string that issued the search request?



Reporting

MITRE ATT&CK
The framework is a collection of attack techniques and tactics that are used by threat actors to compromise systems. The framework is designed to be flexible and scalable, allowing organizations to tailor it to their specific needs.

MITRE ATT&CK Framework Mapping

Personal View

Attack ID	Tactic	Technique	MITRE ATT&CK ID	MITRE ATT&CK Name	MITRE ATT&CK Description	MITRE ATT&CK Category	MITRE ATT&CK Subcategory	MITRE ATT&CK Platform	MITRE ATT&CK Version	MITRE ATT&CK Status	MITRE ATT&CK Last Updated
T1566	Phishing	Spearphishing Link	T1566.001	Spearphishing Link	Threat actors use spearphishing to deliver malicious links to specific individuals or groups within an organization.	Initial Access	Phishing	Windows	4.1	Active	2023-09-01
T1566	Phishing	Phishing	T1566.002	Phishing	Threat actors use phishing to deliver malicious links to a large number of individuals within an organization.	Initial Access	Phishing	Windows	4.1	Active	2023-09-01
T1566	Phishing	Spearphishing Attachment	T1566.003	Spearphishing Attachment	Threat actors use spearphishing to deliver malicious attachments to specific individuals or groups within an organization.	Initial Access	Phishing	Windows	4.1	Active	2023-09-01
T1566	Phishing	Phishing Attachment	T1566.004	Phishing Attachment	Threat actors use phishing to deliver malicious attachments to a large number of individuals within an organization.	Initial Access	Phishing	Windows	4.1	Active	2023-09-01
T1566	Phishing	Spearphishing	T1566.005	Spearphishing	Threat actors use spearphishing to deliver malicious links or attachments to specific individuals or groups within an organization.	Initial Access	Phishing	Windows	4.1	Active	2023-09-01
T1566	Phishing	Phishing	T1566.006	Phishing	Threat actors use phishing to deliver malicious links or attachments to a large number of individuals within an organization.	Initial Access	Phishing	Windows	4.1	Active	2023-09-01
T1566	Phishing	Spearphishing	T1566.007	Spearphishing	Threat actors use spearphishing to deliver malicious links or attachments to specific individuals or groups within an organization.	Initial Access	Phishing	Windows	4.1	Active	2023-09-01
T1566	Phishing	Phishing	T1566.008	Phishing	Threat actors use phishing to deliver malicious links or attachments to a large number of individuals within an organization.	Initial Access	Phishing	Windows	4.1	Active	2023-09-01
T1566	Phishing	Spearphishing	T1566.009	Spearphishing	Threat actors use spearphishing to deliver malicious links or attachments to specific individuals or groups within an organization.	Initial Access	Phishing	Windows	4.1	Active	2023-09-01
T1566	Phishing	Phishing	T1566.010	Phishing	Threat actors use phishing to deliver malicious links or attachments to a large number of individuals within an organization.	Initial Access	Phishing	Windows	4.1	Active	2023-09-01

Mapping to Mitre Att&ck

Over the Wire

- Community built labs
- Different games and levels
- Command line based
- Bandit great for learning Linux
- Under the Wire for PowerShell



Wargames

The wargames offered by the OverTheWire community can help you to learn and practice security concepts in the form of fun-filled games.

To find out more about a certain wargame, just visit its page linked from the menu on the left.

If you have a problem, a question or a suggestion, you can [join us via chat](#).

Suggested order to play the games in

1. Bandit
2. Leviathan or Natas or Krypton
3. Narnia
4. Behemoth
5. Utumno
6. Maze
7. ...

Each shell game has its own SSH port

Information about how to connect to each game using SSH, is provided in the top left corner of the page. Keep in mind that every game uses a different SSH port.



Bandit Demo

Bandit Demo

Introducing the picoGym



picoGym is a noncompetitive practice space where you can explore and solve challenges from previously released picoCTF competitions, find fresh never before revealed challenges, and build a knowledge base of cyber security skills in a safe environment.

Whether you are a cyber security professional, competitive hacker or new to CTFs you will find interesting challenges in the picoGym that you can solve at your own pace. Team picoCTF will regularly update this challenge repository so visit the picoGym often.

[Practice picoGym](#)

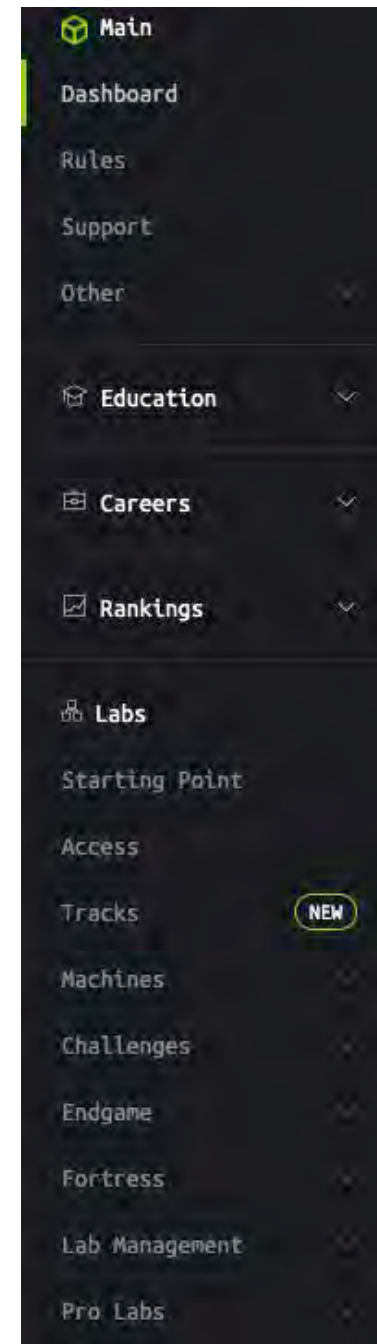
The screenshot shows the picoCTF picoGym Practice Challenges page. The header includes the picoCTF logo and navigation links: Learn, Practice, and Compete. The main heading is 'picoGym Practice Challenges'. On the left, there is a sidebar with filters: 'Hide Solved' (checkbox), 'Search by Name' (input field), 'Category Filter' (a list with 'All Categories' selected, and other categories like Web Exploitation, Cryptography, etc.), and 'First Appearance' (a dropdown with 'Any' selected). The main content area displays a grid of challenge cards. Each card shows the category, points, title, number of solves, and a percentage. For example, 'Lets Warm Up' is a General Skills challenge worth 50 points with 3,145 solves and a 64% completion rate. Other visible challenges include 'The Numbers', '2Warm', 'Insp3ct0r', 'Glory of the Garden', 'vault-c', 'Warmed Up', 'vault-door-1', and 'what's'.

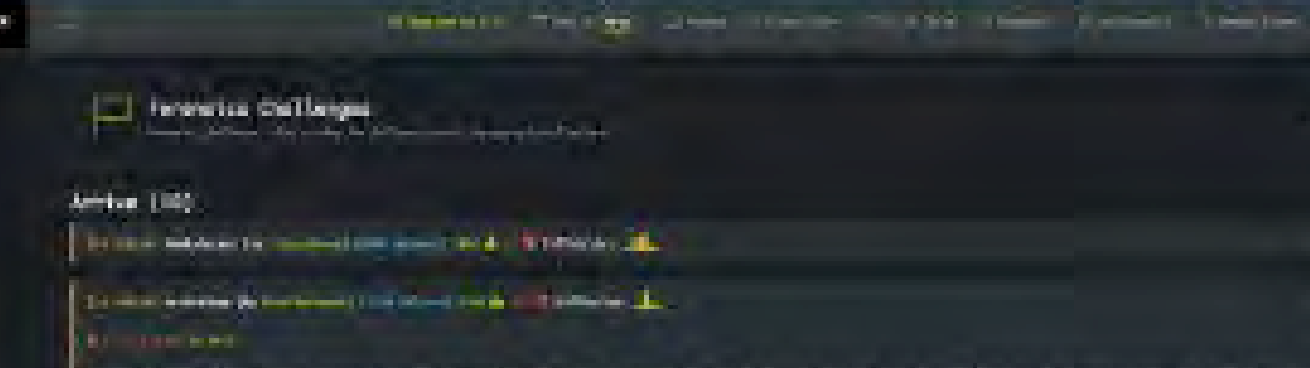
PicoCTF

- Designed by Carnegie Mellon
- Designed for high school students
- Great for anyone new to cybersecurity

Hack the Box

- Freemium model
- Vulnerable hosts
 - Active
 - Retired
- Challenges
- Scenarios
- "Hack" into hosts
- Linux and Windows
- Difficulty ratings
- Ranking system
- Active and Retired Machines
- Can share answers for retired machines
- Set of challenges
- Beginner to expert





The screenshot shows the AWS IAM console 'Users' page. The 'Users' list table is the primary focus, displaying the following data:

Name	Access Key ID	Status	Last Used	Last Sign-in Time
root		Active		2023-10-27 10:00:00
aws-logs		Active		2023-10-27 10:00:00

The 'root' user is highlighted in blue. The 'aws-logs' user is also visible below it. The table columns include Name, Access Key ID, Status, Last Used, and Last Sign-in Time. The 'root' user has a status of 'Active' and a last sign-in time of '2023-10-27 10:00:00'. The 'aws-logs' user has a status of 'Active' and a last sign-in time of '2023-10-27 10:00:00'.



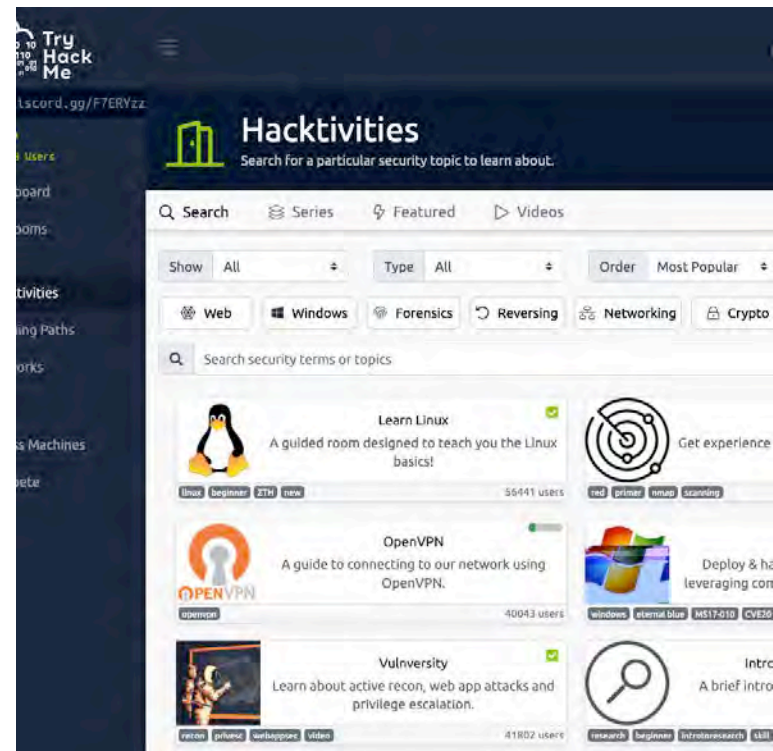
Videos and Tutorials

- Twitch.TV
 - https://www.twitch.tv/r00k_infosec/
- YouTube - Ippsec
- <https://www.youtube.com/channel/UCa6eh7gCkpPo5XXUDfygQQA>



TryHackMe


- Community Built
- Variety of topics
- Room Concept
- Easy to build your own VM and upload
- Clone and customize rooms



Task 1 Recon

Scan and learn what exploit this machine is vulnerable to. Please note that this machine does not respond to ping (ICMP) and may take a few minutes to boot up. This room is not meant to be a boot2root CTF, rather, this is an educational series for complete beginners. Professionals will likely get very little out of this room beyond basic practice as the process here is meant to be beginner-focused.

Deploy



Art by one of our members, Varg - [THM Profile](#) - [Instagram](#) - [Blue Merch](#)

#1 Scan the machine. (If you are unsure how to tackle this, I recommend checking out the room [RP: Nmap](#))

No answer needed

Completed

Hint

#2 How many ports are open with a port number under 1000?

Answer format: *

Submit

Hint

#3 What is this machine vulnerable to? (Answer in the form of: ms??-???, ex: ms08-067)

Answer format: *****

Submit

Hint

Task 2 Gain Access

Task 3 Escalate

Task 4 Cracking

Task 5 Find flags!

TryHackMe



TryHackMe
176 Rooms

1,000
Points

10 Members

1,000,000
Visits

1,000
Followers

99%

5.0



Hacktivities

The ultimate guide to learning

378

Points Scored

Overview

All Rooms

Settings

Learning Paths

Work your way through a structured learning path

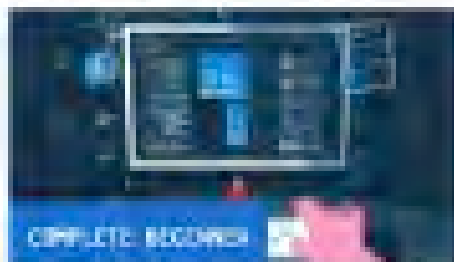


Learn how to analyse and defend against real world cyber threat intelligence

- Detect threats
- Gather threat actor intelligence
- Understand and simulate adversary TTPs
- Identify and respond to incidents

10 rooms

10 rooms

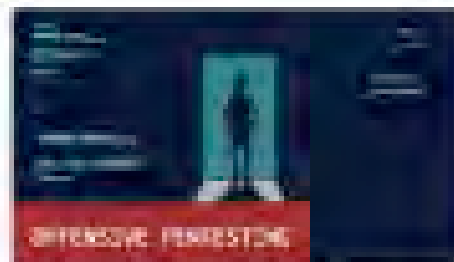


Learn the core skills needed to start a career in cyber security

- Web application security
- Network security
- Basic Linux
- Scripting

10 rooms

10 rooms



Prepare yourself for real world penetration testing

- Utilise industry standard tools
- Learn multiple attack scenarios
- Plan an offensive security
- Supporting exercises & resources

10 rooms

10 rooms

Pre Security

Hacktivities

Find a security topic to learn about.

441

Public Rooms

Overview

All Rooms

Series

63 new Rooms

Learning Paths

Work your way through a structured learning path



PRE SECURITY

Before hacking something, you first need to understand the basics.

- Cyber security basics
- Networking basics and weaknesses
- The web and common attacks
- Learn to use the Linux operating system

⌚ 40 Hours

📁 16 Rooms



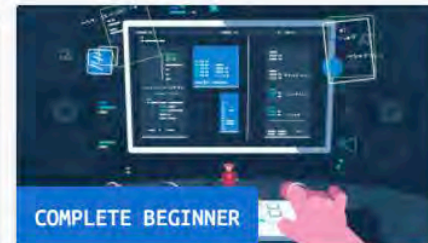
CYBER DEFENSE

Learn how to analyse and defend against real-world cyber threats/attacks

- Detect threats
- Gather threat actor intelligence
- Understand and emulate adversary TTPs
- Identify and respond to incidents

⌚ 48 Hours

📁 39 Rooms



COMPLETE BEGINNER

Learn the core skills required to start a career in cyber security

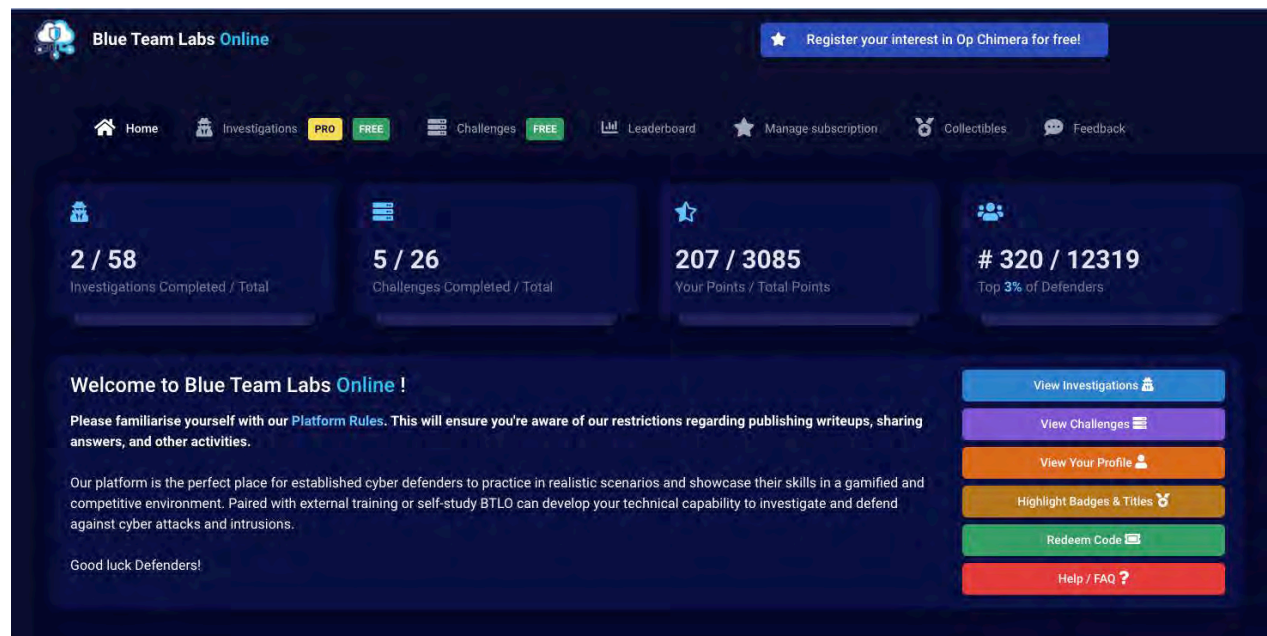
- Web application security
- Network security
- Basic Linux
- Scripting

⌚ 64 Hours


📁 33 Rooms

Blue Team Labs (Hack the Box for Blue Teams)


- Community Built
- Variety of topics
- Room Concept
- Ranks and badges
- Deploys VM's




Blue Team Labs

 Blue Team Labs Online


★ Register your interest in Op Chimera for free!

 Home


 Investigations


PRO


FREE


 Challenges


FREE

 Leaderboard

 Manage subscription

 Collectibles

 Feedback



Sam

Samuel (Sam) is a Neatnik, when it comes to cleanliness and hygiene. Find out if he also follows cyber hygiene. An incident has been reported stating "Sam has lost his SAM". It's your job to figure out what has happened. You are provided with sysmon logs, network traffic, and a memory dump.

Linux CLIWiresharkVolatility2

Start Investigation

Points	Difficulty	Solves	OS
50	Medium	91	Linux

🔥 First-Blood

☁ Created By

Scenario

Samuel (Sam) is a Neatnik, when it comes to cleanliness and hygiene. Find out if he also follows cyber hygiene. An incident has been reported stating "Sam has lost his SAM". It's your job to figure out what has happened. You are provided with sysmon logs, network traffic, and a memory dump.

Investigation Submission

What is the attacker IP, and what is the port that they got a reverse shell on? (3 points)

Format: IP, port

Submit

What's the name of the malicious file that gave remote access to attacker? (4 points)

Format: filename.extension

Submit

What is the process that has been called by the payload upon execution? (5 points)

Format: processname.extension

Submit

Knowing the payload name and process name, if the payload was generated by msfvenom, what would be the format option that the attacker would've used? (5 points)

msfvenom Payload Type

Submit



Deploy in the Cloud

- Use Devops tools to deploy labs in the cloud
- Examples
 - Detection Lab
 - Mordor
 - CyberRange

Nice Challenge

Excellent set of challenges

Mapped to NICE
Framework

Free

Reservations required

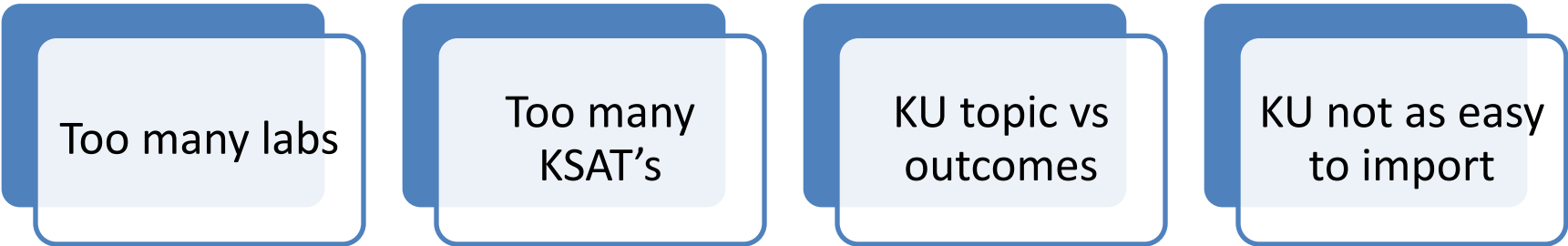
Mapping Labs To Objectives

Build a catalog of
labs mapped to the
NICE Framework
and CAE KU's

Student project
mapping
TryHackMe

Using AirTable

Some challenges to mapping labs



Too many labs

Too many
KSAT's

KU topic vs
outcomes

KU not as easy
to import

What is AirTable

CLOUD BASED
SPREADSHEET/DATABASE

A BASE IS A SET OF
TABLES

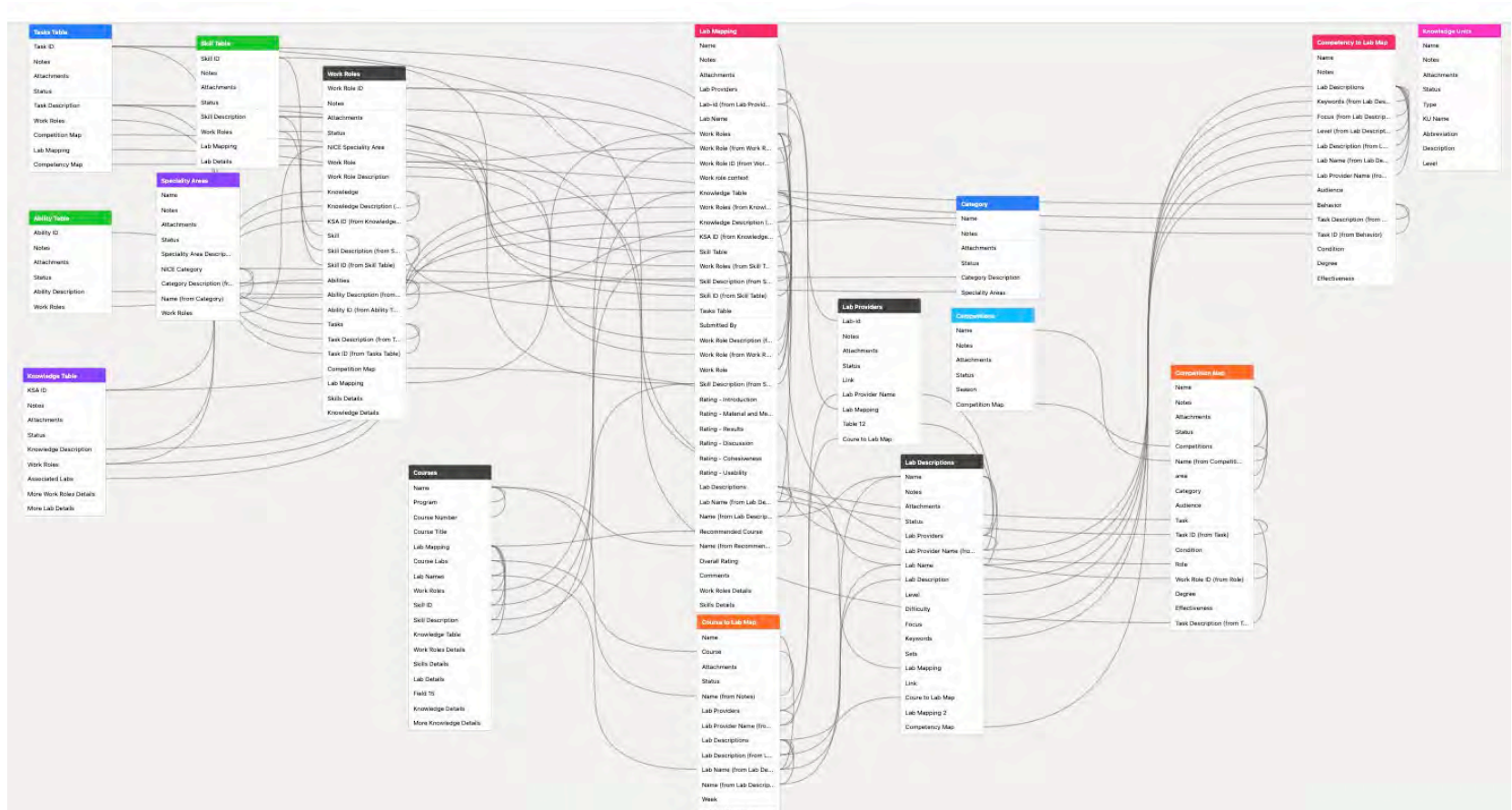
TABLES USE ROWS AND
COLUMNS

EASY TO CONNECT
TABLES

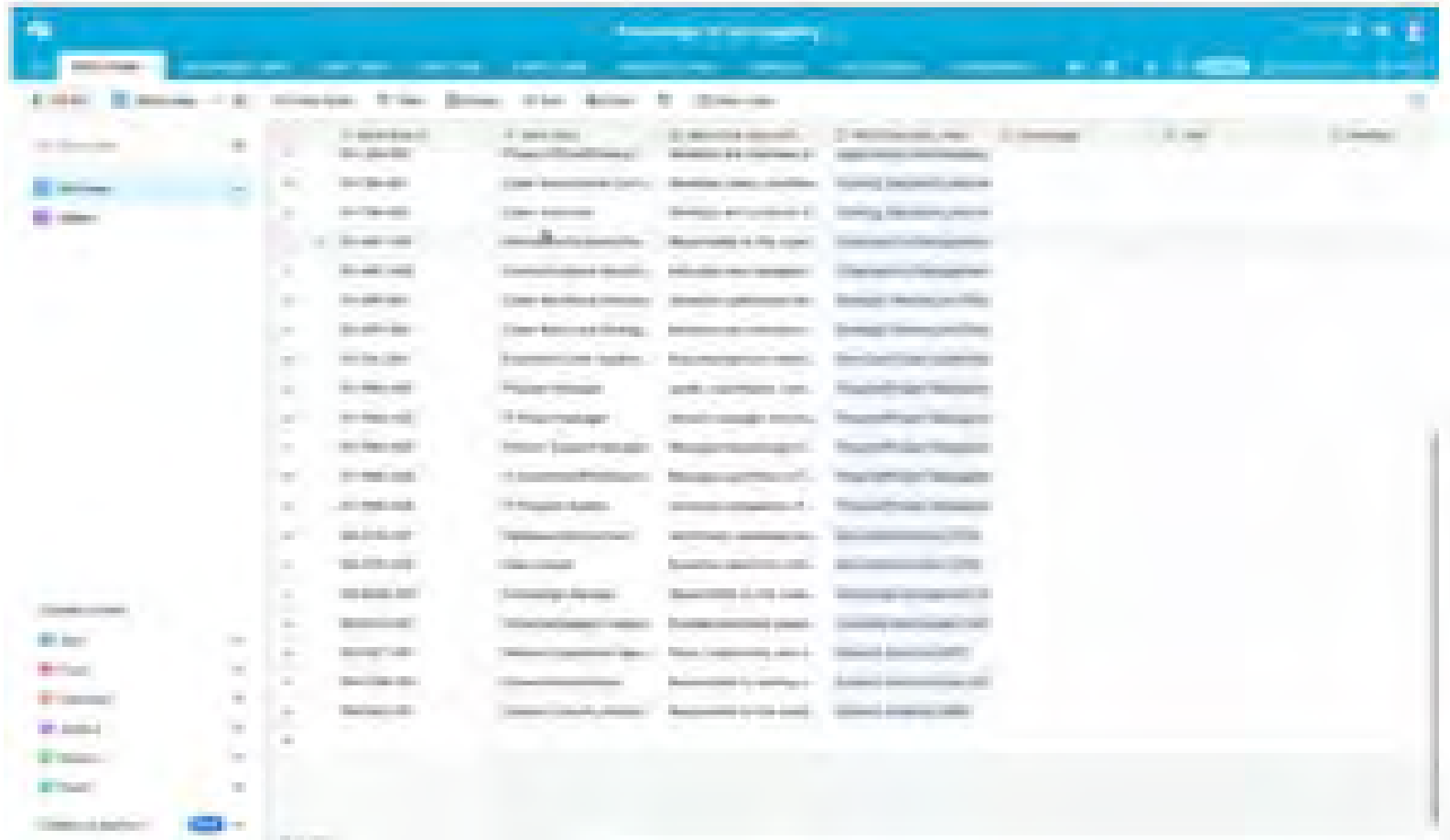
DOESN'T REQUIRE
DETAILED DATABASE
PLANNING

CAPABILITY TO CREATE
FORMS

Database Design



Airtable Demo



The screenshot displays the Airtable web interface. At the top, there is a blue navigation bar with the Airtable logo and a search bar. Below the navigation bar, a sidebar on the left contains a list of tables and views. The main area shows a table with the following columns: ID, Name, Email, Phone, and Address. The table contains 15 rows of data. The interface is clean and modern, with a light blue and white color scheme.

ID	Name	Email	Phone	Address
1	John Doe	john.doe@example.com	(123) 456-7890	123 Main St, New York, NY 10001
2	Jane Smith	jane.smith@example.com	(987) 654-3210	456 Elm St, Los Angeles, CA 90001
3	Bob Johnson	bob.johnson@example.com	(555) 111-2222	789 Oak St, Chicago, IL 60601
4	Alice Brown	alice.brown@example.com	(333) 444-5555	101 Pine St, San Francisco, CA 94101
5	Charlie Davis	charlie.davis@example.com	(222) 333-4444	202 Cedar St, Austin, TX 78701
6	Diana Prince	diana.prince@example.com	(111) 222-3333	303 Maple St, Seattle, WA 98101
7	Frank Miller	frank.miller@example.com	(444) 555-6666	404 Birch St, Denver, CO 80201
8	Grace Wilson	grace.wilson@example.com	(777) 888-9999	505 Spruce St, Portland, OR 97201
9	Harry Potter	harry.potter@example.com	(666) 777-8888	606 Ash St, Boston, MA 02101
10	Ivy Green	ivy.green@example.com	(555) 666-7777	707 Hickory St, Miami, FL 33101
11	Jack Black	jack.black@example.com	(444) 555-6666	808 Sycamore St, Phoenix, AZ 85001
12	Karen White	karen.white@example.com	(333) 444-5555	909 Walnut St, San Diego, CA 92101
13	Liam Neeson	liam.neeson@example.com	(222) 333-4444	1010 Chestnut St, Dallas, TX 75201
14	Mia Farrow	mia.farrow@example.com	(111) 222-3333	1111 Olive St, Houston, TX 77001
15	Noah Park	noah.park@example.com	(999) 888-7777	1212 Elm St, New Orleans, LA 70101



CLARK

Clark Center

- Digital repository for cybersecurity curriculum
- Built to store content
- Supports Bloom's Taxonomy
- Easy search for KSATs and KU's plus other frameworks
- Crowdsourced mapping
- Not for external labs
- <https://clark.center/>

Clark Center Example

[← Back](#)

Basic Information

Learning Outcomes

Materials

All changes saved

Children

Add Child +

This learning object has no children

2 Learning Outcomes

Discover open ports on a network using Nmap.

Remember & Understand

Apply & Analyze

Evaluate & Synthesize

Discover ▾ open ports on a network using Nmap.

Maps to:

NICE Cybersecurity Workforce Framework Tasks - T0028 - 2017 ×

CAE Cyber Defense - Basic Networking (KUS) - 2019 ×

CAE Cyber Defense - Network Defense - 2014 ×

NICE - S0081 - 2020 ×

NICE - T0549 - 2020 ×

NICE - T0010 - 2020 ×

NICE - T0188 - 2020 ×

SUBMIT FOR REVIEW →

Curricular Guidelines

Search curricular guidelines...

7 suggestions

CAE Cyber Defense - Network Defense - 2014

Students will be able to use a network mapping tool (e.g., Nmap).

NICE - S0081 - 2020

Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc.).

Cyber2yr2020 - Cross-Cutting Concepts [CC-5] - 2020

Discuss how changes in one part of a system may impact other parts of a cybersecurity ecosystem.

Centers of Academic Excellence in Cybersecurity Resource Directory (CARD)

- Categorized collection of cybersecurity education resources developed by members of the cybersecurity community
- No KU/KSAT mapping



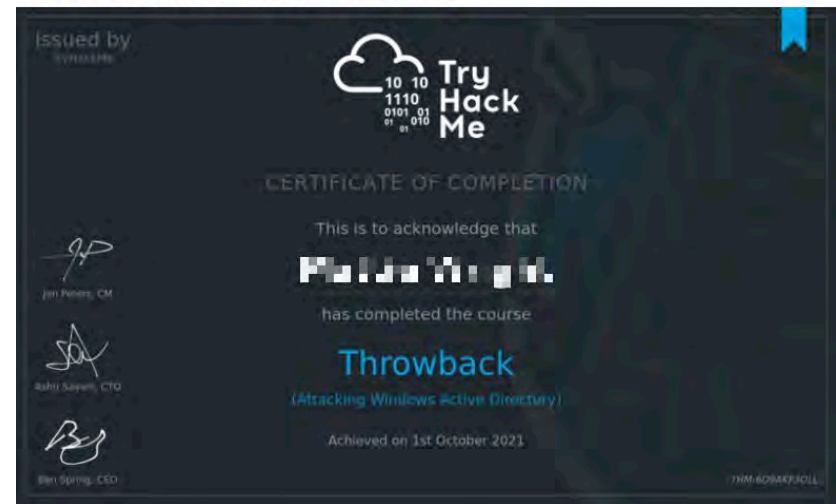
<https://www.caeresource.directory/>

Some Other Takeaways

- Students can share achievements
- Capstone projects
- Invitation to attend capstone
 - TryHackMe Throwback
 - Hack the Box Dante

Truly enjoyed the Throwback Network from TryHackMe! Awesome setup for learning network pentesting and attacking Windows Active Directory. Thank you [TryHackMe!](#)


[#tryhackme](#) [#throwback](#) [#thm](#) [#activedirectory](#) [#pentesting](#)



Cyber Competition Coach and Mentor Training

[Home](#)
[Announcements](#)
[Modules](#)
[Syllabus](#)
[People](#)
[Assignments](#)
[Discussions](#)
[Quizzes](#)
[Grades](#)
[Pages](#)
[Files](#)
[Outcomes](#)
[Conferences](#)
[Collaborations](#)
[Rubrics](#)
[New Analytics](#)
[Settings](#)

SoCal Cyber Cup Mentor Training



Welcome Everyone to the SoCal Cyber Cup Mentor Training. This training course includes a set of 20 different modules to help you learn and understand what it takes to become an Outstanding Mentor. There are four different types of modules that you will be experiencing and each provides you with different tools that you need to provide the leadership and mentorship for your Cybersecurity student teams. The modules are grouped by area including Mechanics (background needed to understand the competitions), Team/Collaboration/Ethics, Topical/Technical Training, and free resources. It is our intent to provide you with tools that you and your team can use in preparation for the competition. Since we all come in with a variety of skill sets, you do not need to feel obligated to go through every module or even in the order that they are listed but use these modules as you have questions or need information to help you and your teams be successful. Have Fun, Good Luck, and remember YOU ARE NOT IN

[Edit](#)
[Import Existing Content](#)
[Import from Commons](#)
[Choose Home Page](#)
[View Course Stream](#)
[New Announcement](#)
[New Analytics](#)
[View Course Calendar](#)
[View Course Notifications](#)
To Do
Nothing for now
Recent Feedback
Nothing for now



Questions?

Email: csimpson@nu.edu

Links

- <https://www.immersivelabs.com/digital-cyber-academies/>
- <https://overthewire.org/wargames/>
- <https://underthewire.tech/>
- <https://www.hackthebox.eu/>
- <https://www.picoctf.org/>
- <https://tryhackme.com/>
- <https://www.youtube.com/channel/UCa6eh7gCkpPo5XXUDfygQQA>
- https://www.twitch.tv/r00k_infosec/
- <https://www.detectionlab.network/>
- <https://mordordatasets.com/introduction.html>
- <https://medium.com/aws-cyber-range>
- <https://clark.center/home>
- <https://github.com/carnal0wnage/weirdAAL>
- <https://github.com/RhinoSecurityLabs/cloudgoat>
- <https://rhinosecuritylabs.com/aws/assume-worst-aws-assume-role-enumeration/>
- <https://airtable.com/>