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

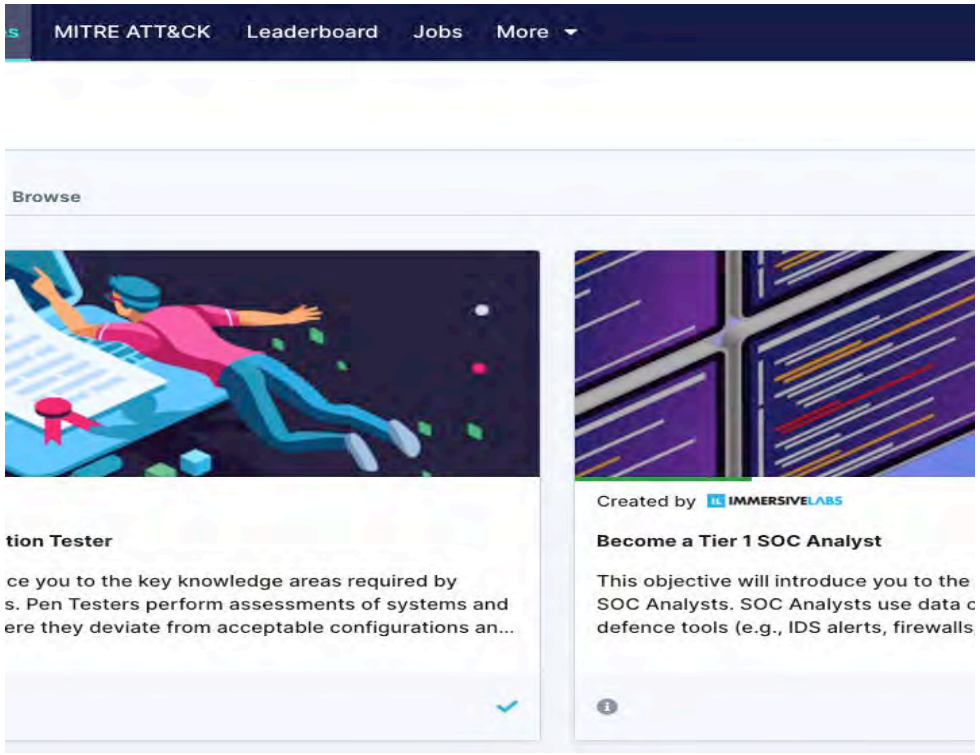
- Not an official endorsement from National University

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)

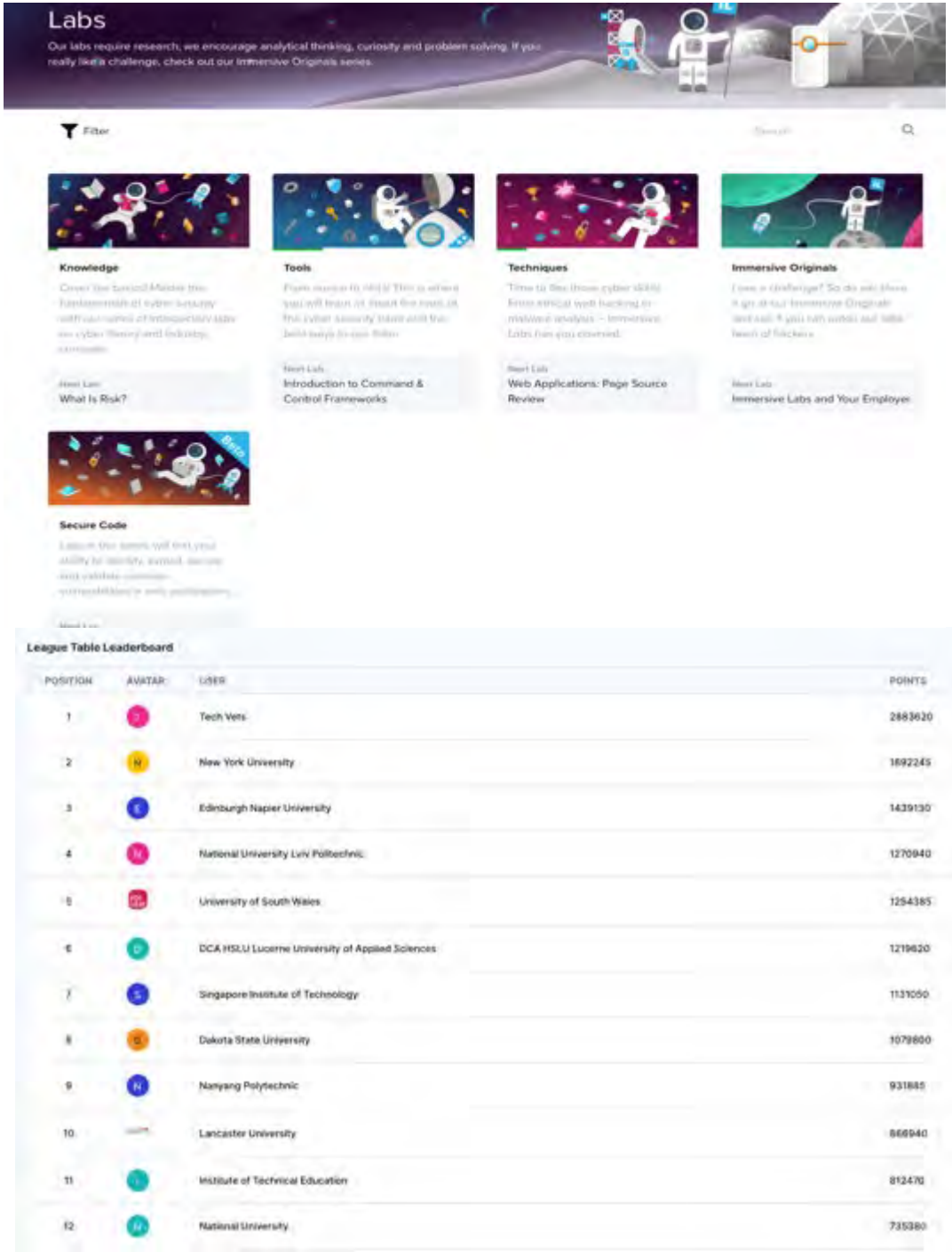
Immersive Labs Digital Cyber Academy

- 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



Clipboard | Tasks | Network | Info

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

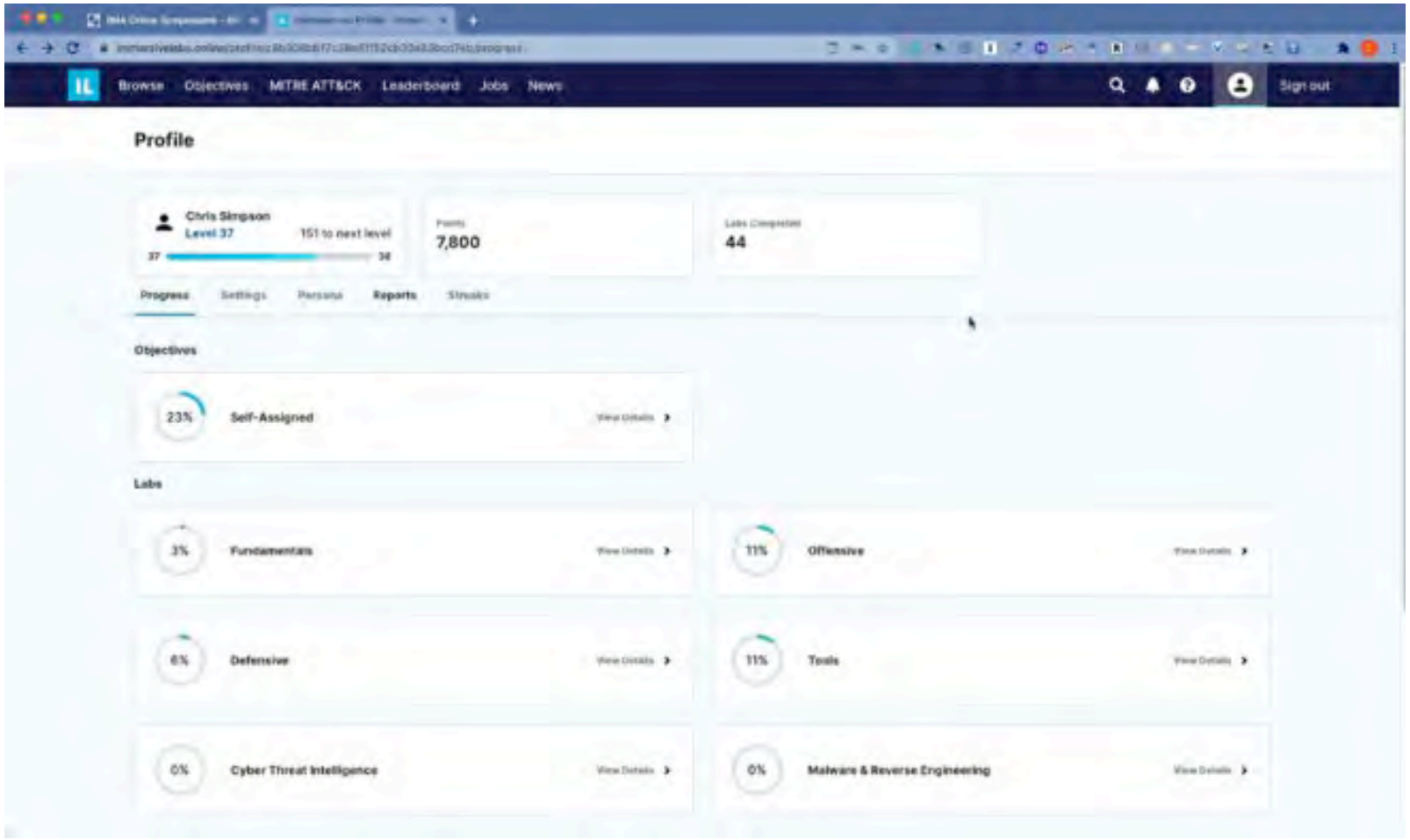
What is the server name sought in the first DNS request that is issued by the client?

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?

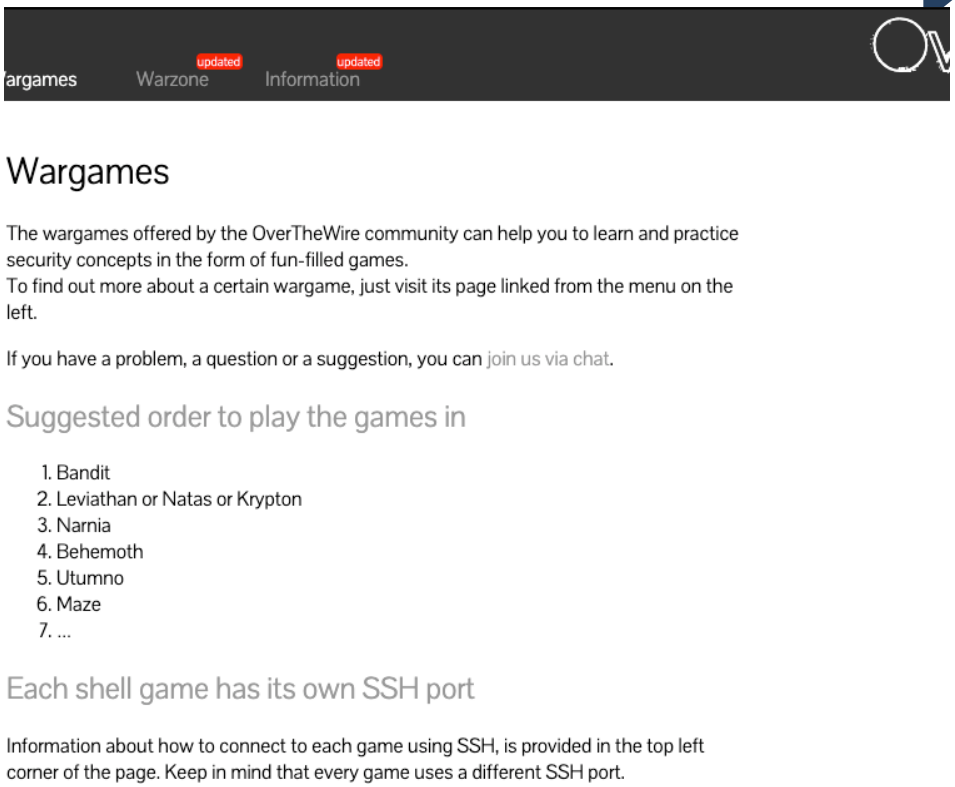

Browse
Objectives
MITRE ATT&CK
Leaderboard
Jobs
News
Sign out
Profile
Chris Simpson
Level 37
151 to next level
37
38
7,800
44
Progress
Settings
Persona
Reports
Streaks
Objectives
23%
Self-Assigned
Labs
3%
Fundamentals
11%
Offensive
6%
Defensive
11%
Tools
0%
Cyber Threat Intelligence
0%
Malware & Reverse Engineering

Reporting

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



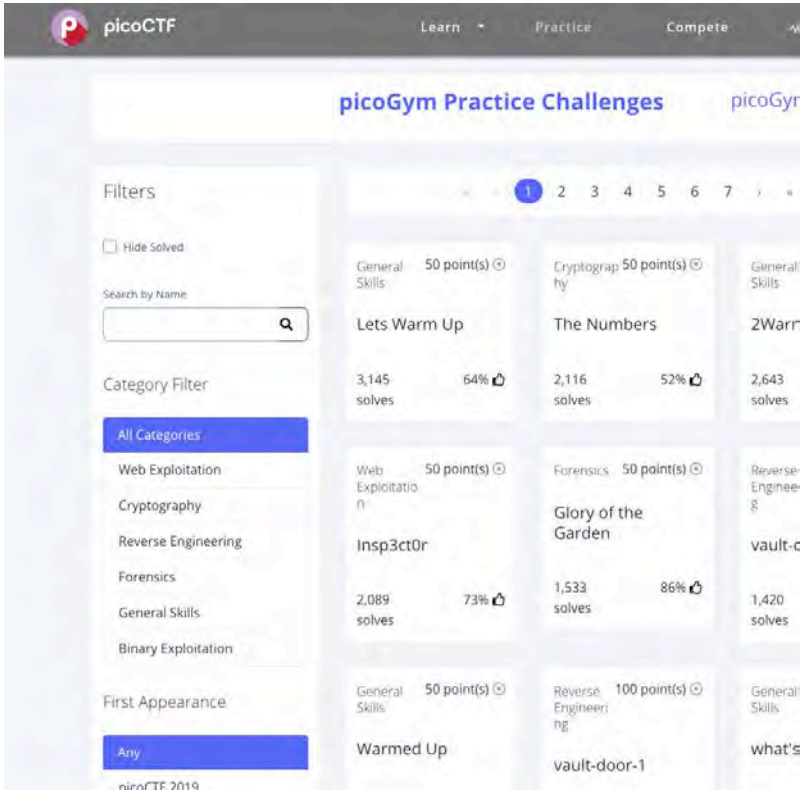
Bandit Demo

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

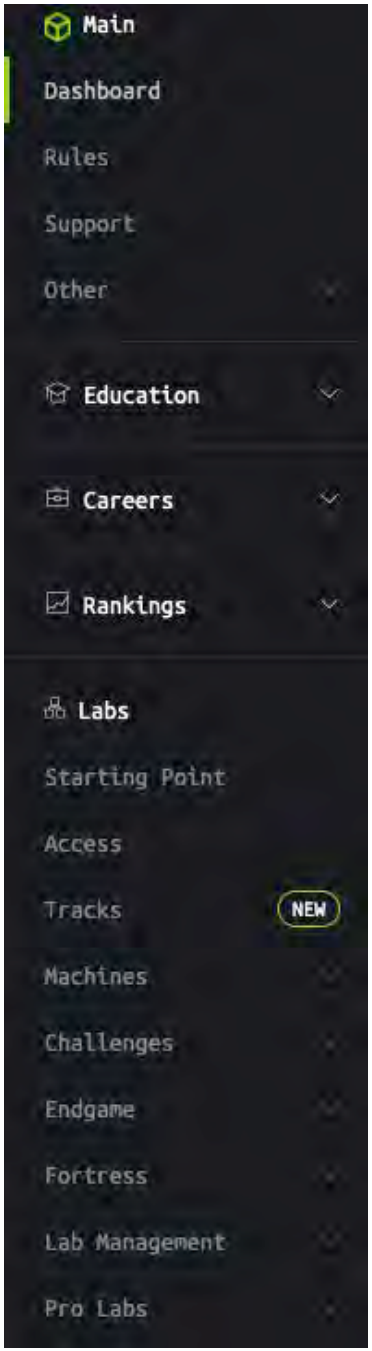


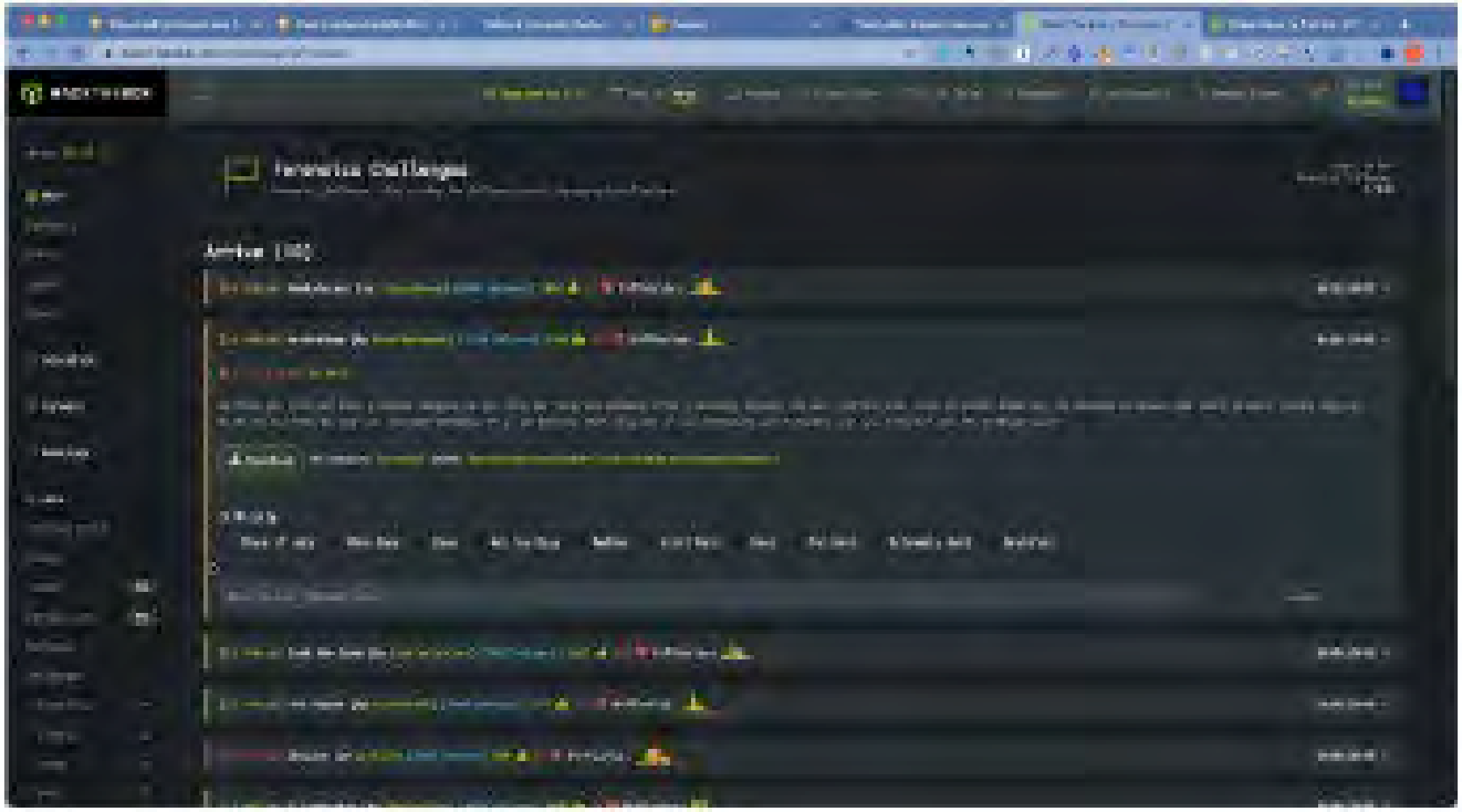
PicoCTF

- 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





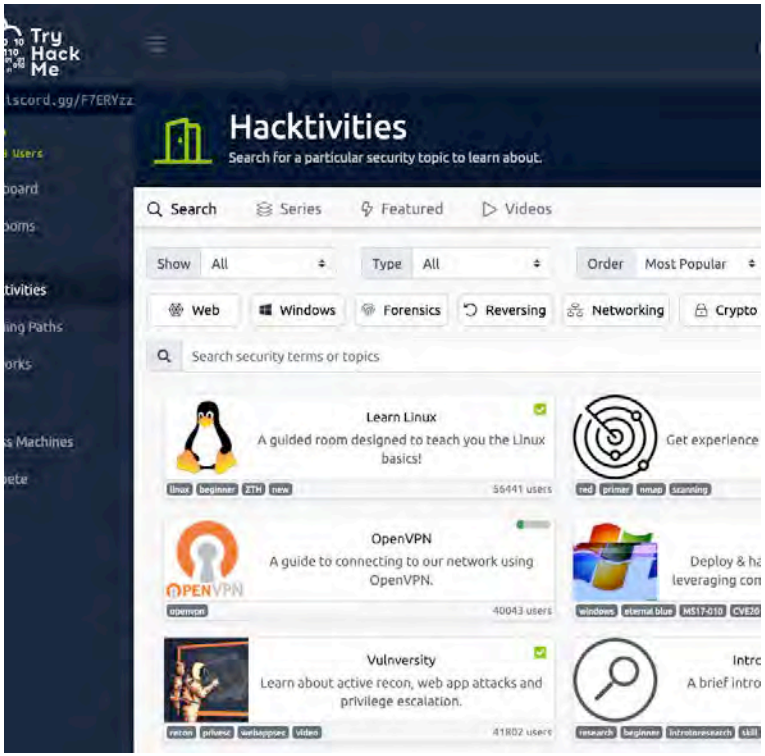

Hack The Box
VPN Connection
Machines
Challenges
Pro Labs
195
2164
789
0.406

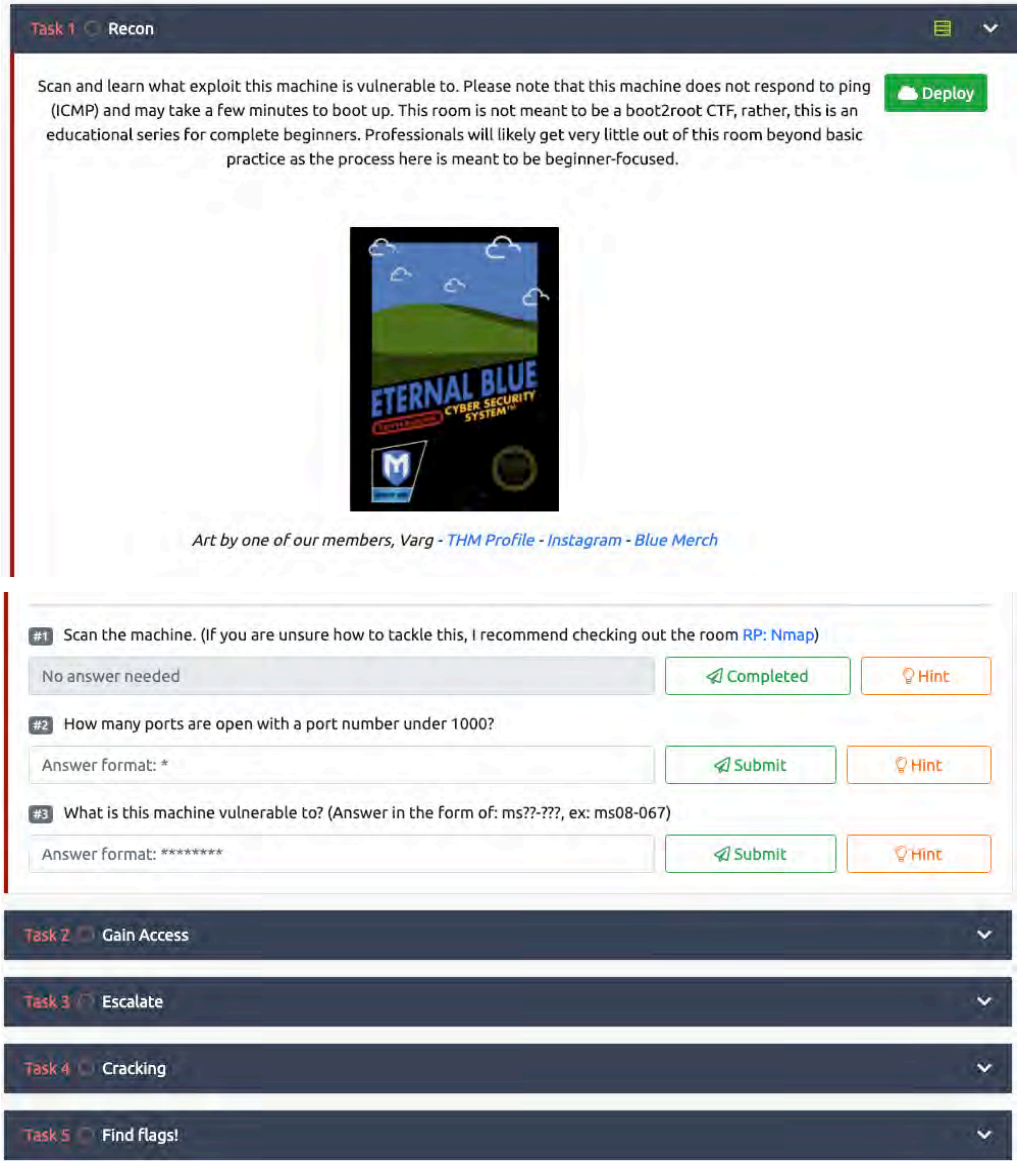
Videos and Tutorials

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

TryHackMe

- Community Built
- Variety of topics
- Room Concept
- East 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
ETERNAL BLUE
CYBER SECURITY SYSTEM
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

Try Hack Me

Hacktivities

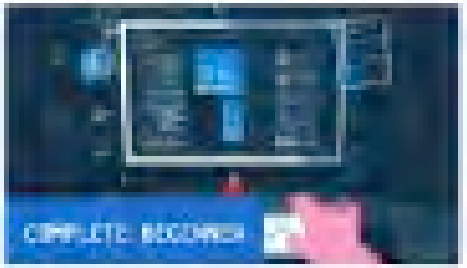
378

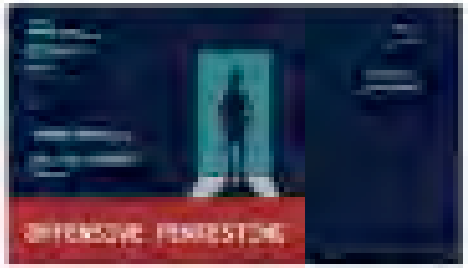
Overview

All Rooms

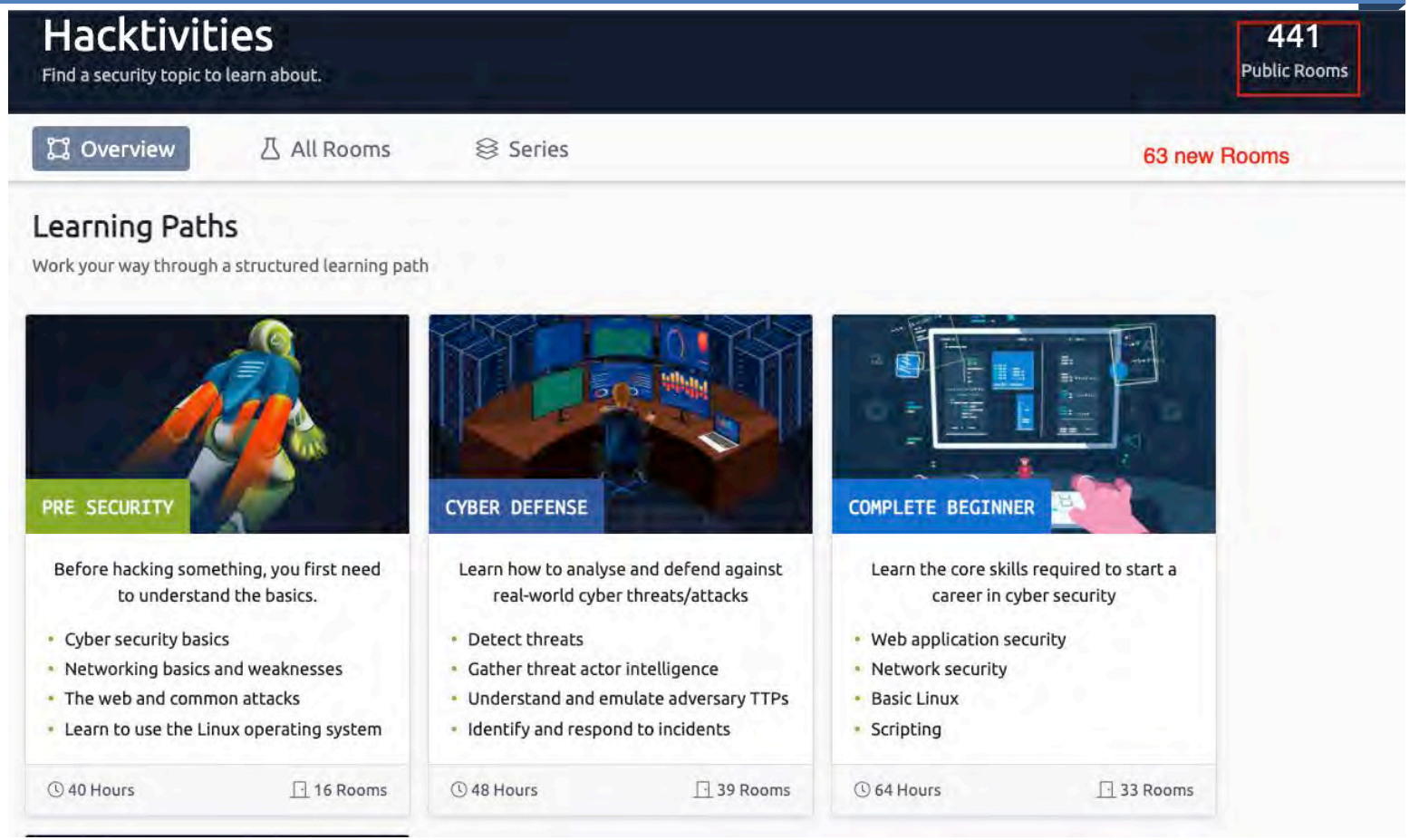
Series

Learning Paths



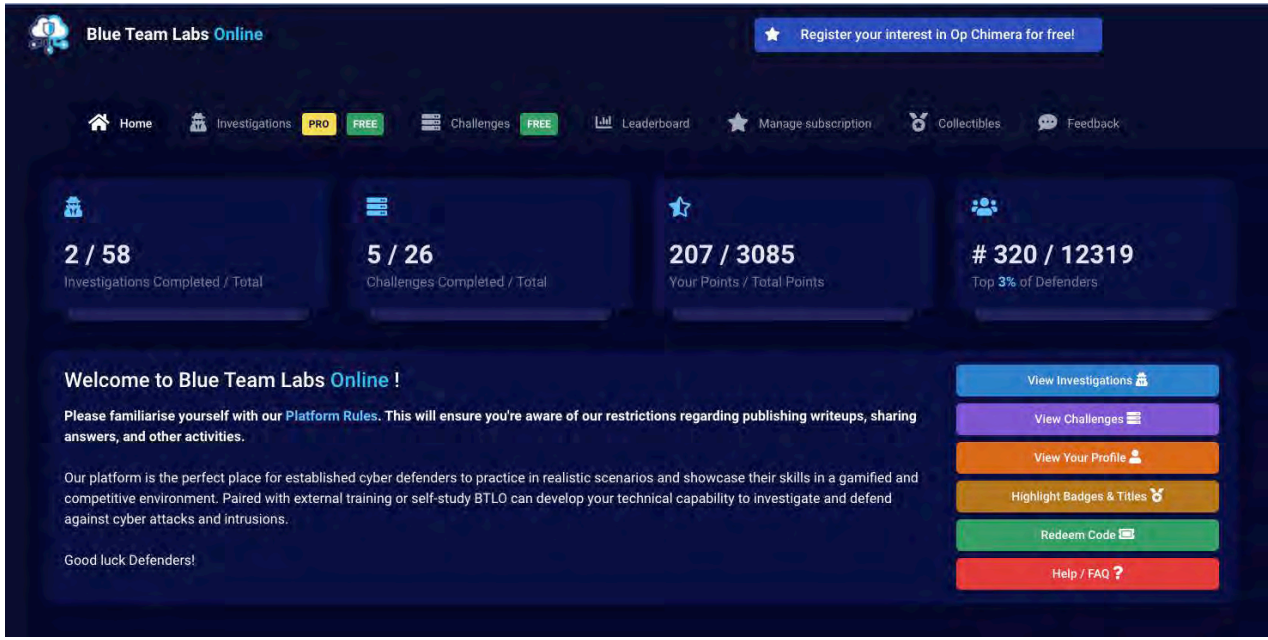


Pre Security

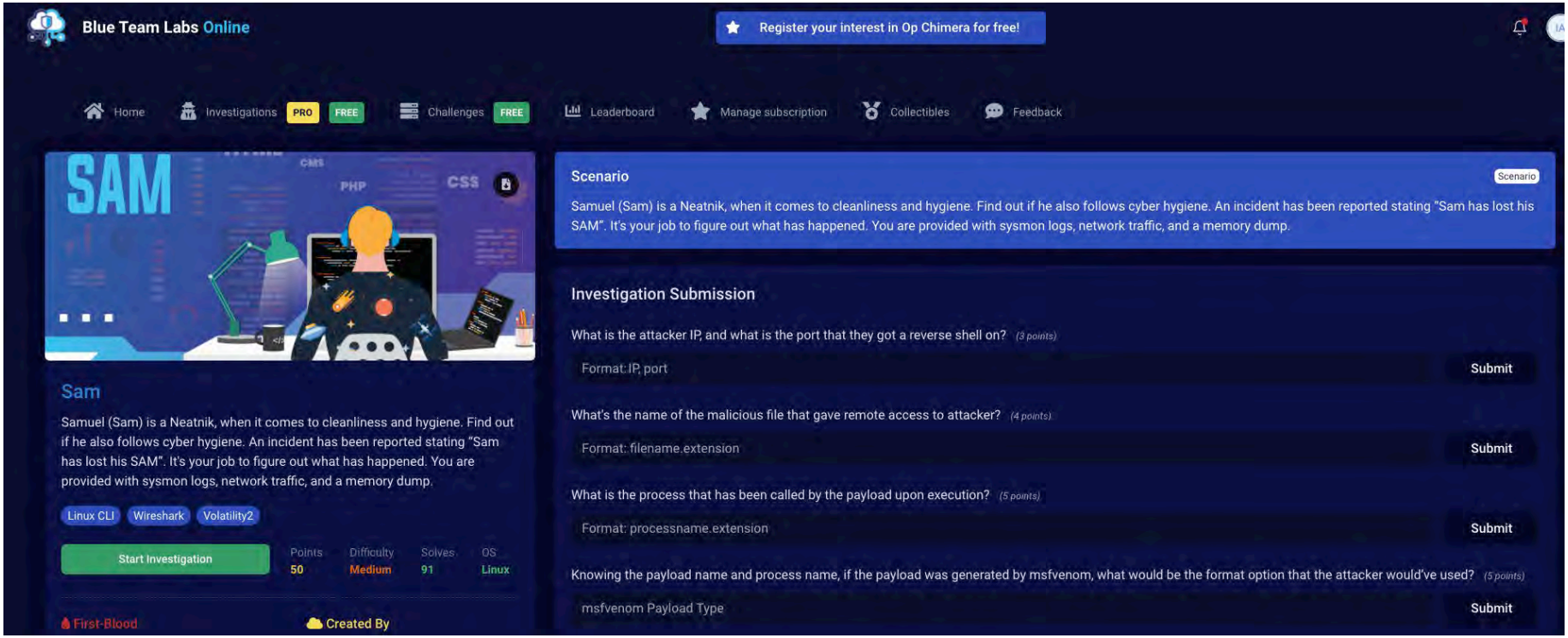


Blue Team Labs (Hack the Box for Blue Teams)

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



Blue Team Labs



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

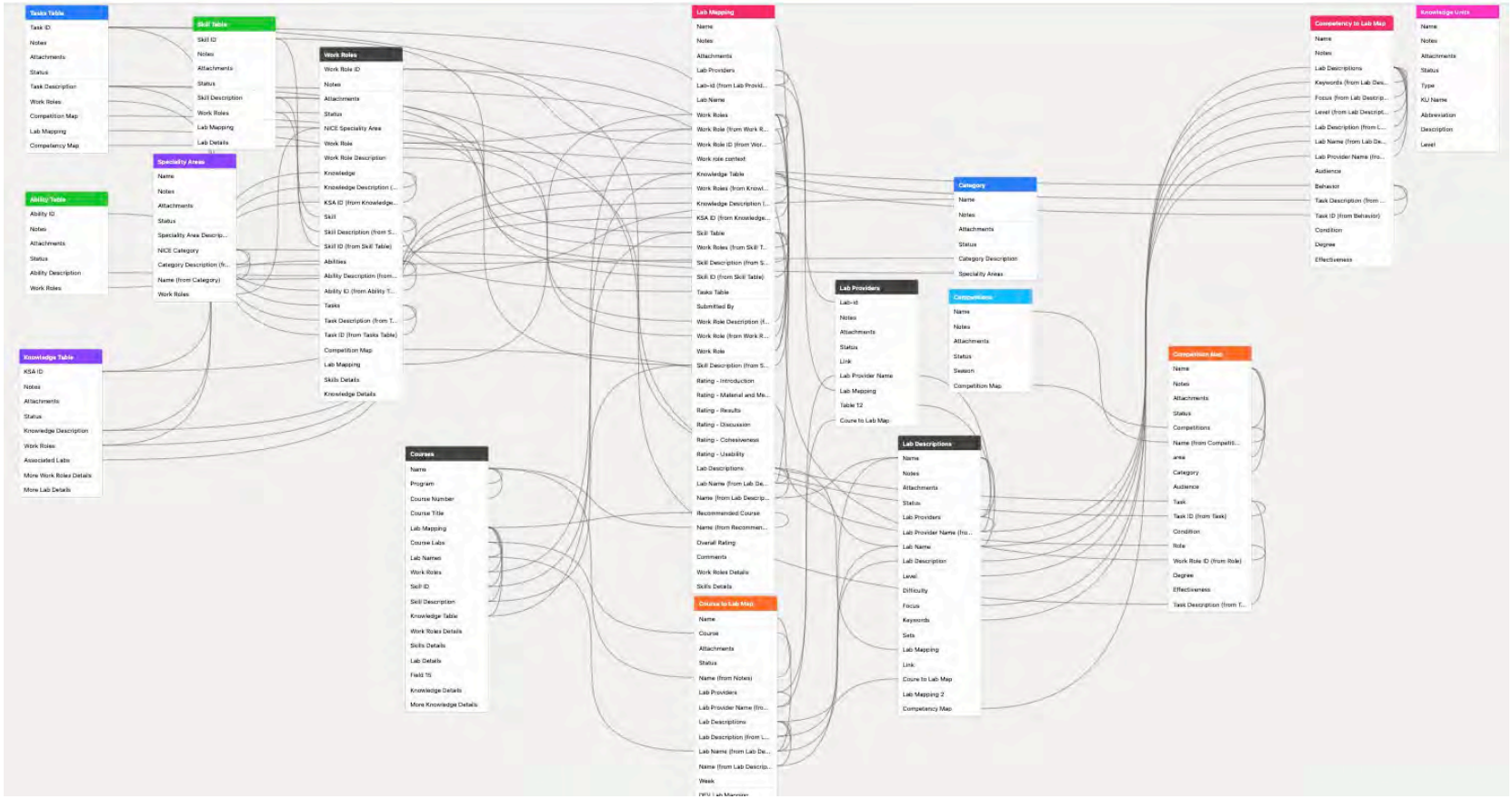
TABLES USE ROWS AND COLUMNS

EASY TO CONNECT TABLES

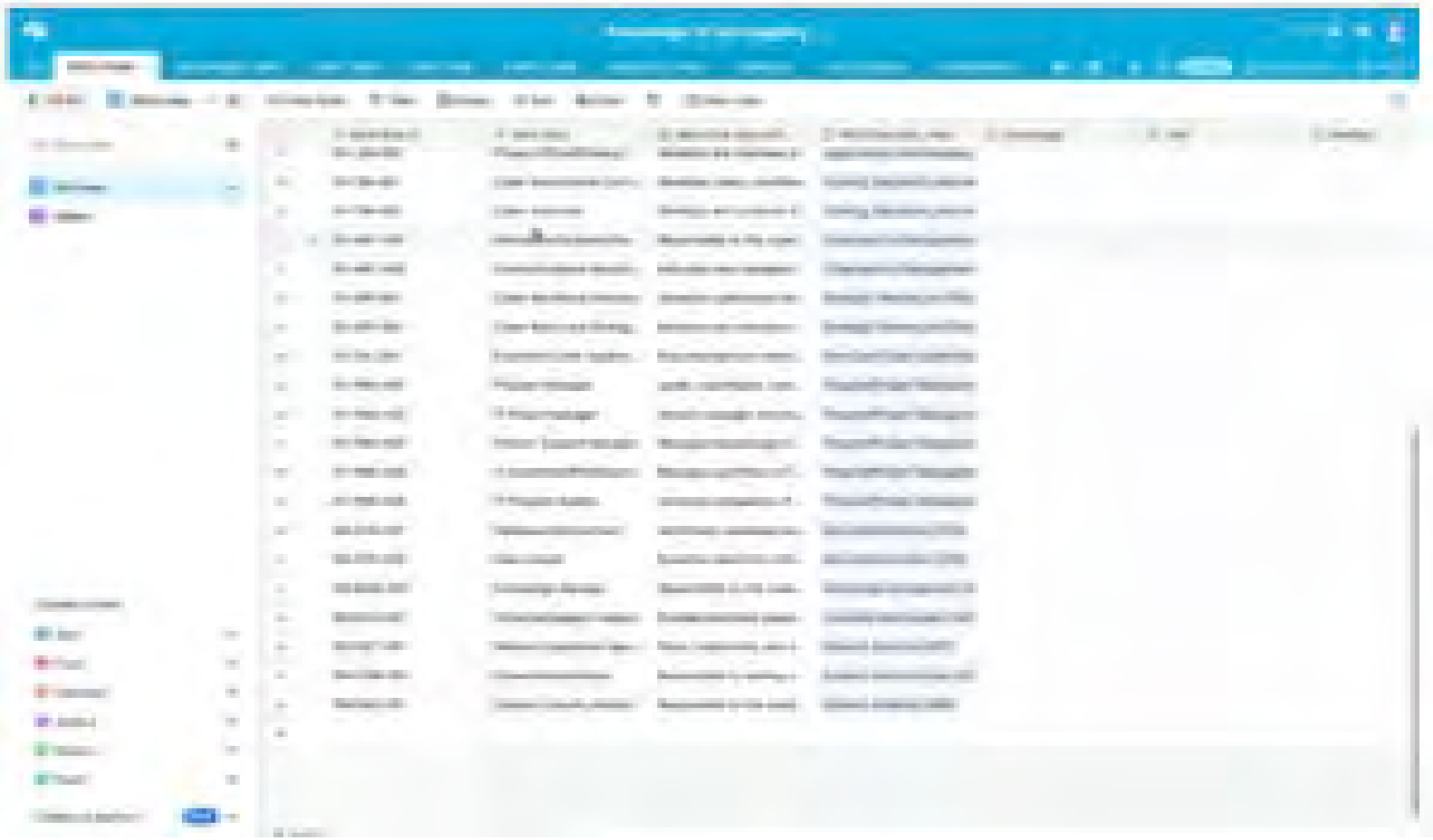
DOESN'T REQUIRE DETAILED DATABASE PLANNING

CAPABILITY TO CREATE FORMS

Database Design



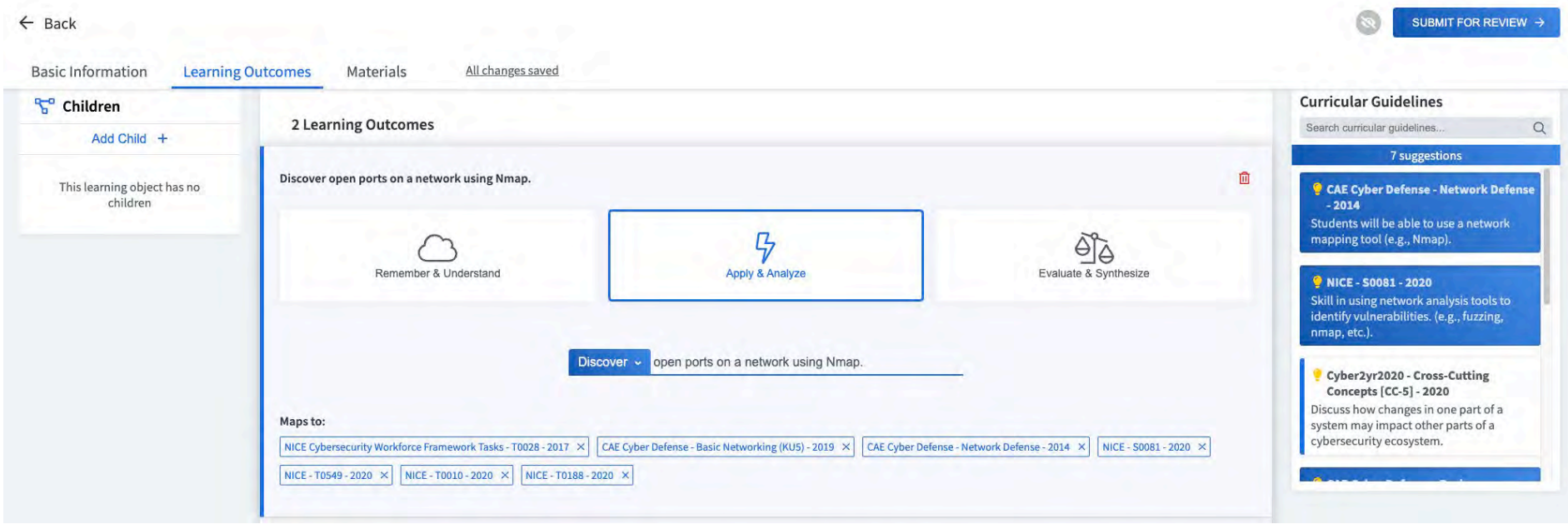
Airtable Demo



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



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

CARD
The CAE Resource Directory

https://www.caeresource.directory/

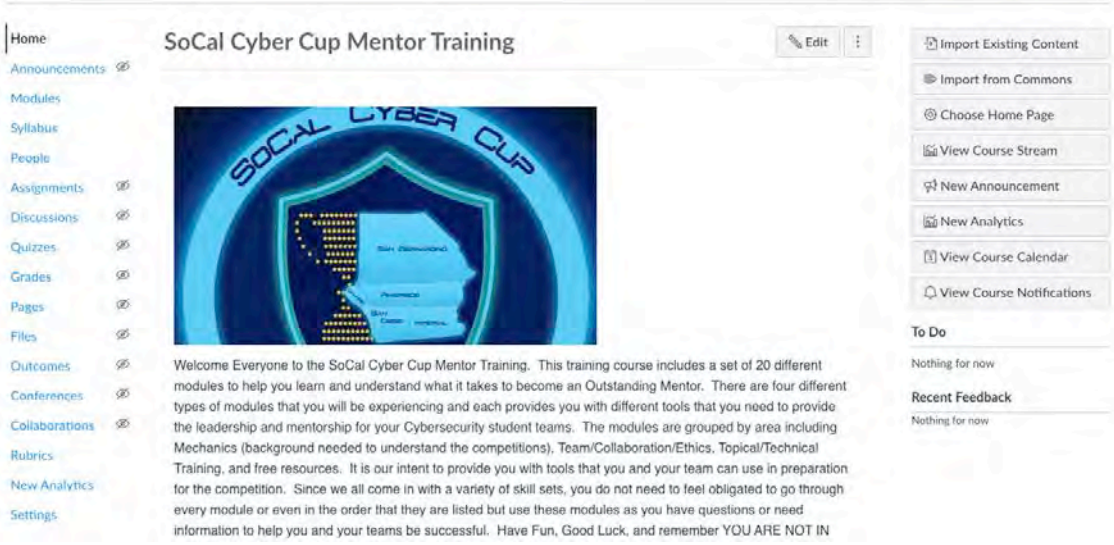
Some Other Takeaways

- 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



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/