# Use of Free and Open Source Labs to Support Cybersecurity Education

Chris Simpson,

Director National University Center for Cybersecurity

# Agenda

- Background
- Examples of free labs and how we use them
- Tracking Objectives
- Sharing Objectives

# 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

# Goal

- Build a database that provides information on labs and learning outcomes, KST, KU’s, and competencies associated with those labs.

# 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

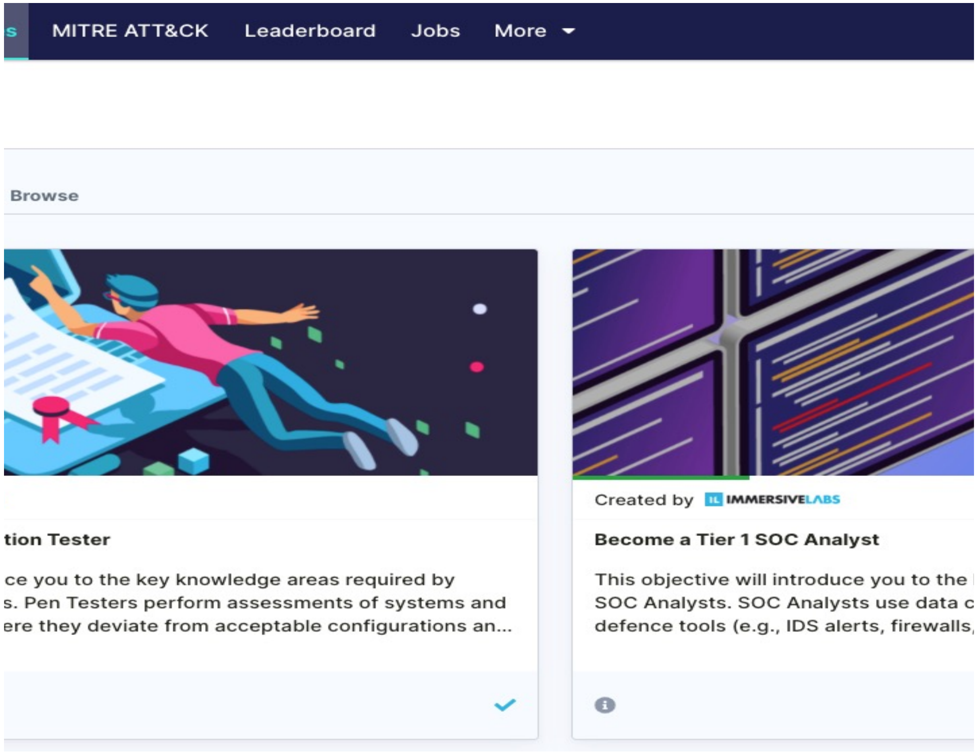
- Not an official endorsement from National University

# 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



tion Tester

ce you to the key knowledge areas required by s. Pen Testers perform assessments of systems and ere they deviate from acceptable configurations an...

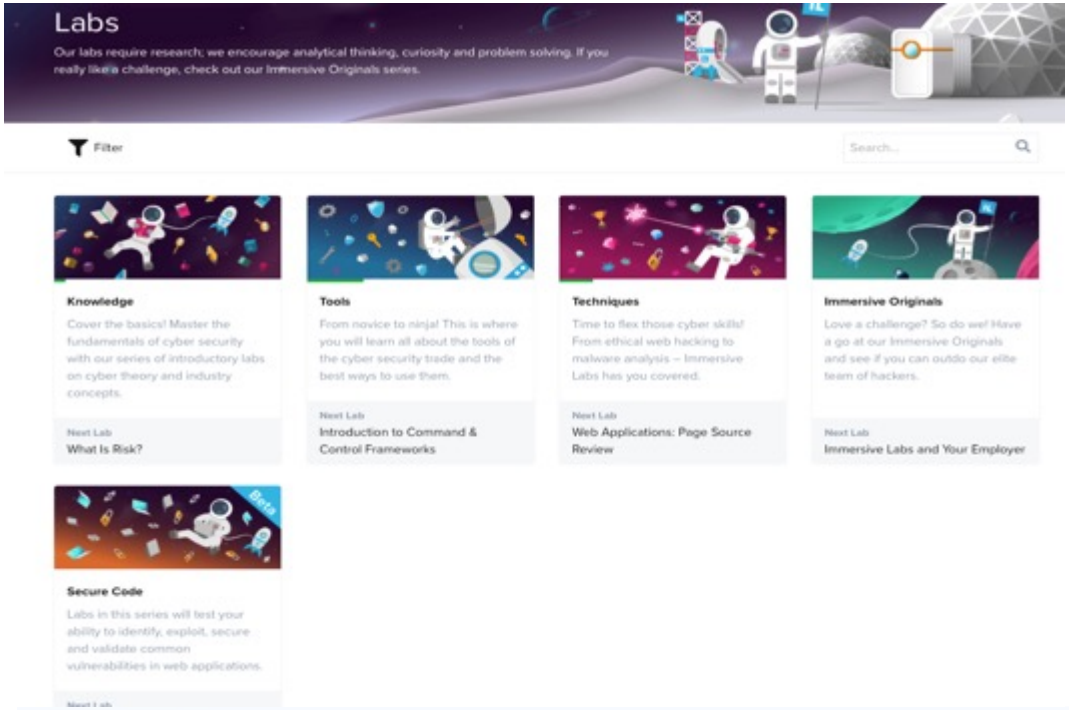
Created by IMMERSIVELABS

Become a Tier 1 SOC Analyst

This objective will introduce you to the SOC Analysts. SOC Analysts use data c defence tools (e.g., IDS alerts, firewalls,

# Immersive Labs

- Badging
- Large variety of topics
- Novice to “Ninja”
- Knowledge +  Hands on
- Rankings



## Labs

Our labs require research; we encourage analytical thinking, curiosity and problem solving. If you really like a challenge, check out our Immersive Originals series.

Filter

Search...

**Knowledge**

Cover the basics! Master the fundamentals of cyber security with our series of introductory labs on cyber theory and industry concepts.

Next Lab
What Is Risk?

**Tools**

From novice to ninja! This is where you will learn all about the tools of the cyber security trade and the best ways to use them.

Next 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.

Next Lab
Web Applications: Page Source Review

**Immersive Originals**

Love a challenge? So do we! Have a go at our Immersive Originals and see if you can outdo our elite team of hackers.

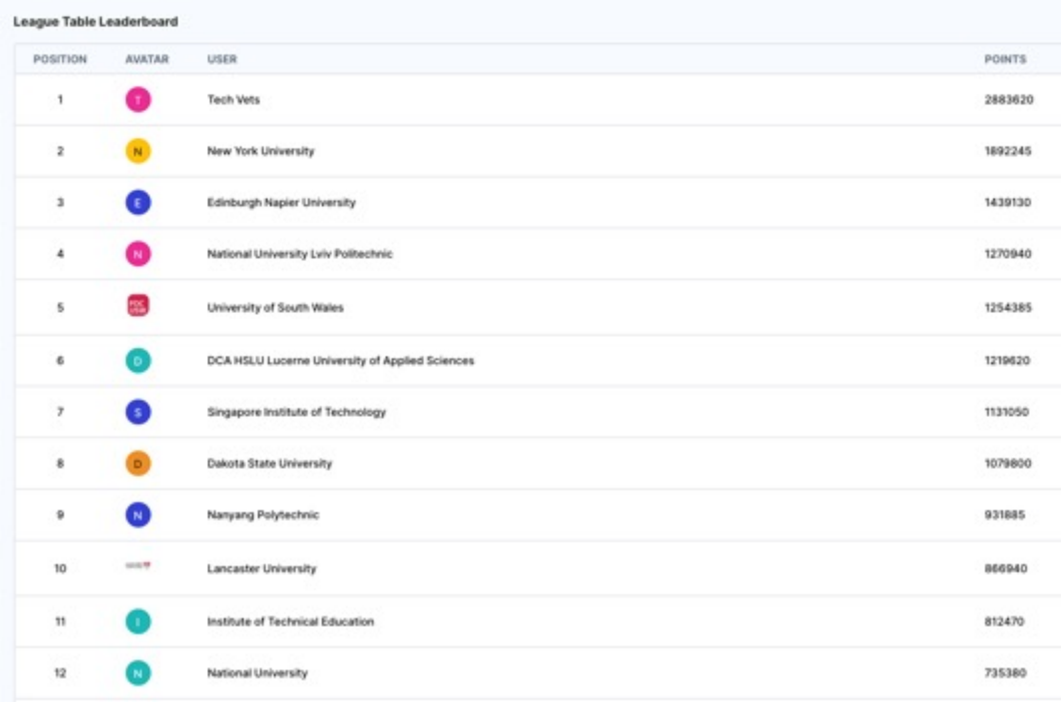
Next Lab
Immersive Labs and Your Employer

Beta

**Secure Code**

Labs in this series will test your ability to identify, exploit, secure and validate common vulnerabilities in web applications.

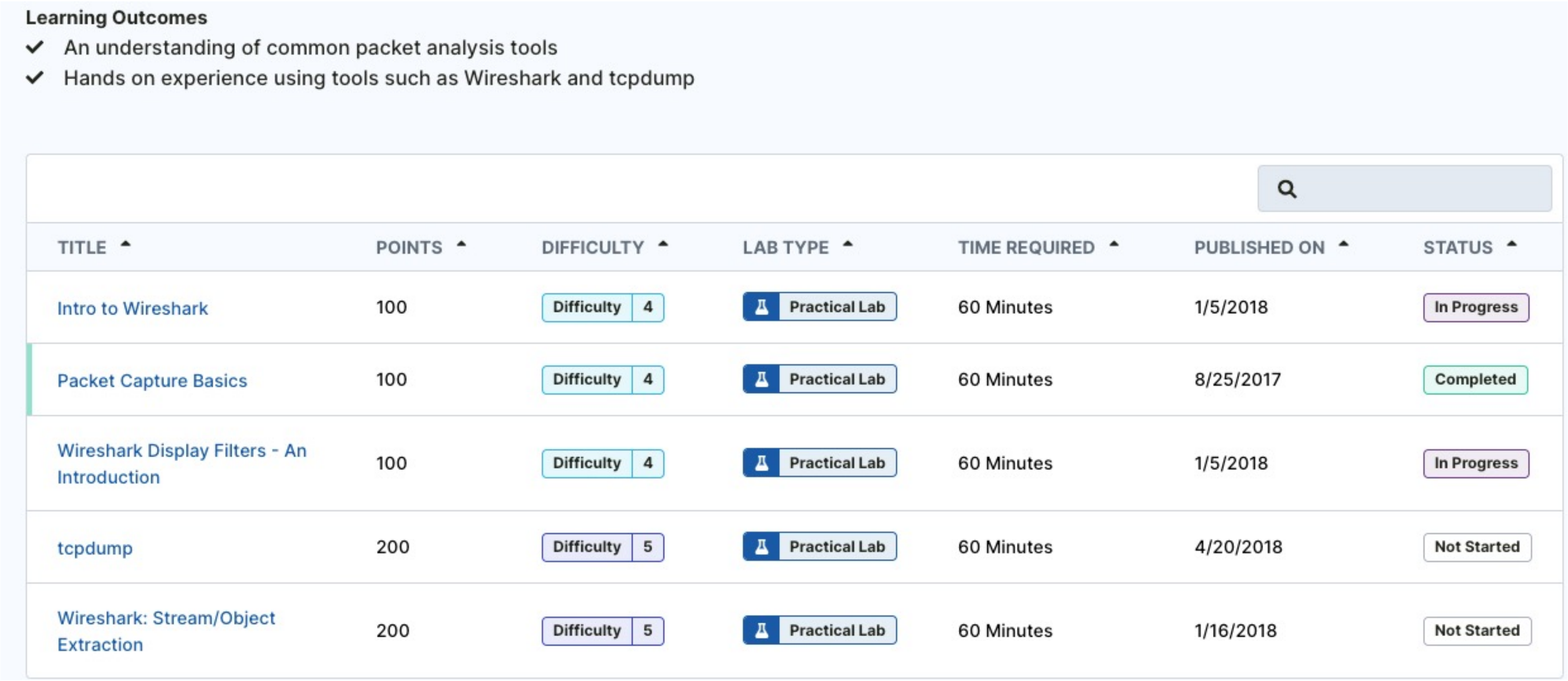
Next Lab



**League Table Leaderboard**

| POSITION | AVATAR | USER | POINTS |
|---|---|---|---|
| 1 | T | Tech Vets | 2883620 |
| 2 | N | New York University | 1892245 |
| 3 | E | Edinburgh Napier University | 1439130 |
| 4 | N | National University Lviv Politechnic | 1270940 |
| 5 |  | University of South Wales | 1254385 |
| 6 | D | DCA HSLU Lucerne University of Applied Sciences | 1219620 |
| 7 | S | Singapore Institute of Technology | 1131050 |
| 8 | D | Dakota State University | 1079800 |
| 9 | N | Nanyang Polytechnic | 931885 |
| 10 |  | Lancaster University | 866940 |
| 11 | I | Institute of Technical Education | 812470 |
| 12 | N | National University | 735380 |

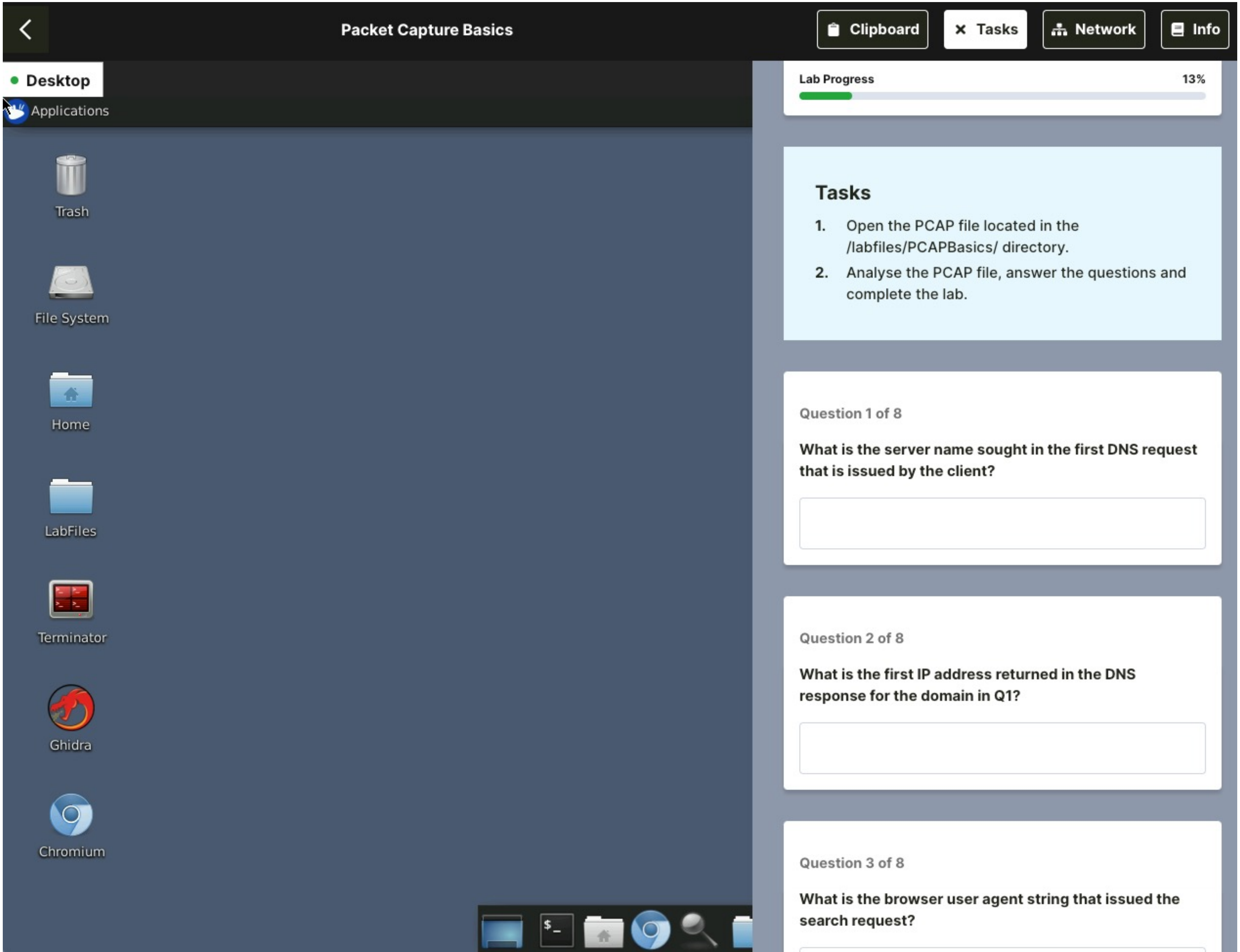
# Different difficulty Levels



**Learning Outcomes**

- ✓ An understanding of common packet analysis tools
- ✓ Hands on experience using tools such as Wireshark and tcpdump

| TITLE | POINTS | DIFFICULTY | LAB TYPE | TIME REQUIRED | PUBLISHED ON | STATUS |
|---|---|---|---|---|---|---|
| Intro to Wireshark | 100 | Difficulty 4 | Practical Lab | 60 Minutes | 1/5/2018 | In Progress |
| Packet Capture Basics | 100 | Difficulty 4 | Practical Lab | 60 Minutes | 8/25/2017 | Completed |
| Wireshark Display Filters - An Introduction | 100 | Difficulty 4 | Practical Lab | 60 Minutes | 1/5/2018 | In Progress |
| tcpdump | 200 | Difficulty 5 | Practical Lab | 60 Minutes | 4/20/2018 | Not Started |
| Wireshark: Stream/Object Extraction | 200 | Difficulty 5 | Practical Lab | 60 Minutes | 1/16/2018 | Not Started |



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

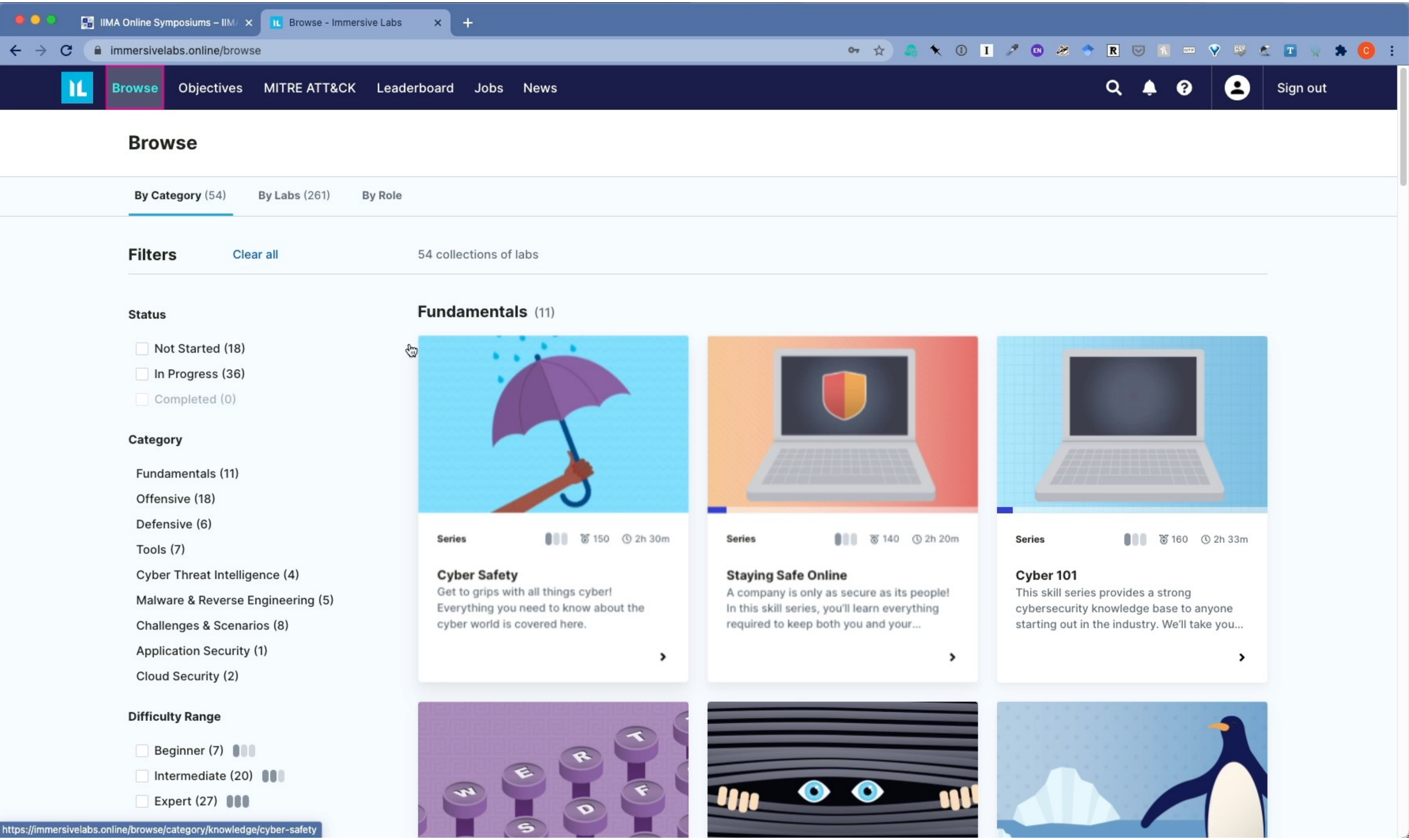
**What is the server name sought in the first DNS request that is issued by the client?**

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

**By Category** (54) | By Labs (261) | By Role

**Filters** Clear all

54 collections of labs

**Status**

- □ Not Started (18)
- □ In Progress (36)
- □ Completed (0)

**Category**

- Fundamentals (11)
- Offensive (18)
- Defensive (6)
- Tools (7)
- Cyber Threat Intelligence (4)
- Malware & Reverse Engineering (5)
- Challenges & Scenarios (8)
- Application Security (1)
- Cloud Security (2)

**Difficulty Range**

- □ Beginner (7)
- □ Intermediate (20)
- □ Expert (27)

**Fundamentals** (11)

Series 150 2h 30m

**Cyber Safety**

Get to grips with all things cyber! Everything you need to know about the cyber world is covered here.

Series 140 2h 20m

**Staying Safe Online**

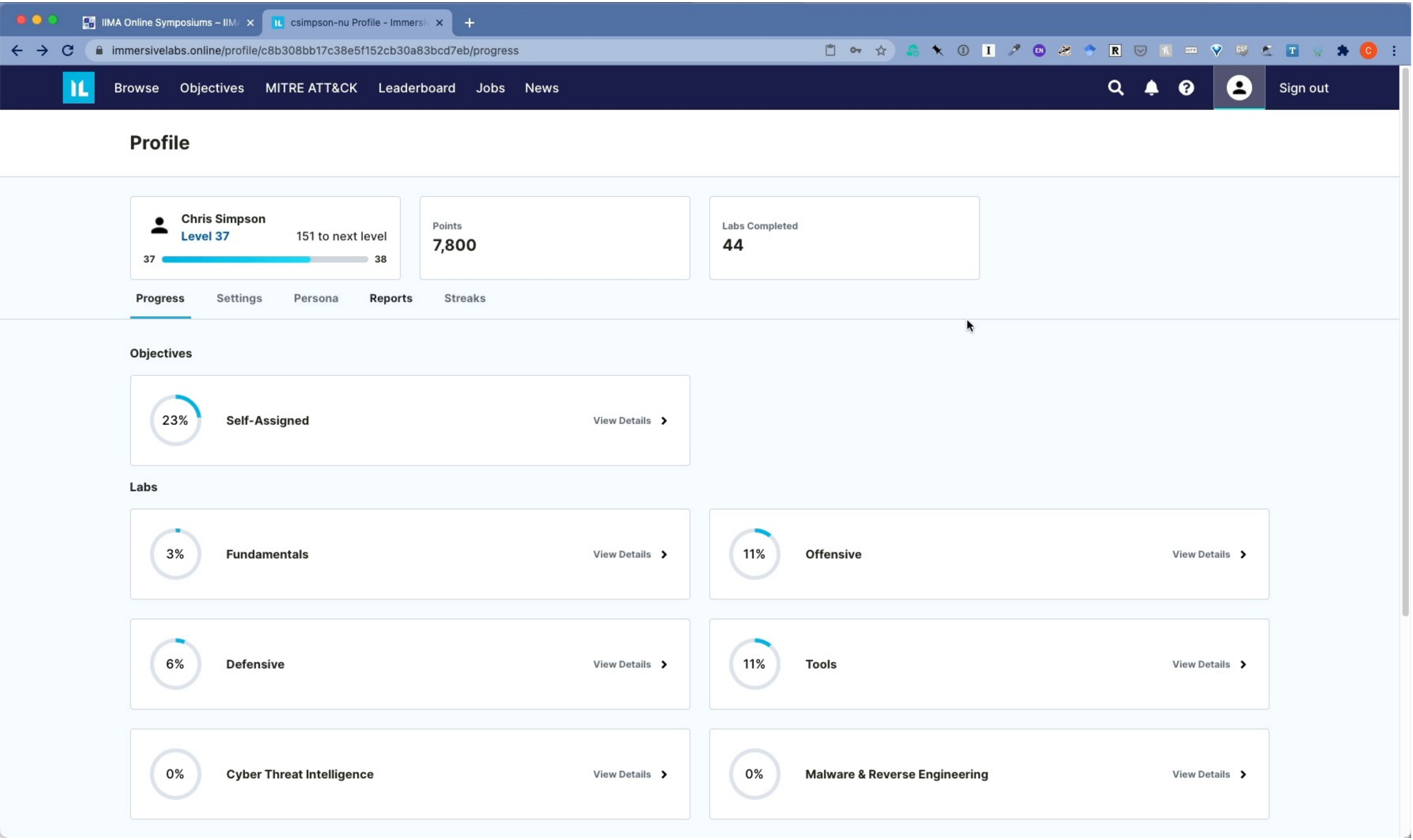
A company is only as secure as its people! In this skill series, you'll learn everything required to keep both you and your...

Series 160 2h 33m

**Cyber 101**

This skill series provides a strong cybersecurity knowledge base to anyone starting out in the industry. We'll take you...

https://immersivelabs.online/browse/category/knowledge/cyber-safety


IIMA Online Symposiums – IIM
csimpson-nu Profile - Immersi
immersivelabs.online/profile/c8b308bb17c38e5f152cb30a83bcd7eb/progress
Browse
Objectives
MITRE ATT&CK
Leaderboard
Jobs
News
Sign out
Progress
Settings
Persona
Reports
Streaks
View Details

## Profile

Chris Simpson
Level 37
151 to next level
37 38

Points
7,800

Labs Completed
44

### Objectives

23% Self-Assigned

### Labs

3% Fundamentals

11% Offensive

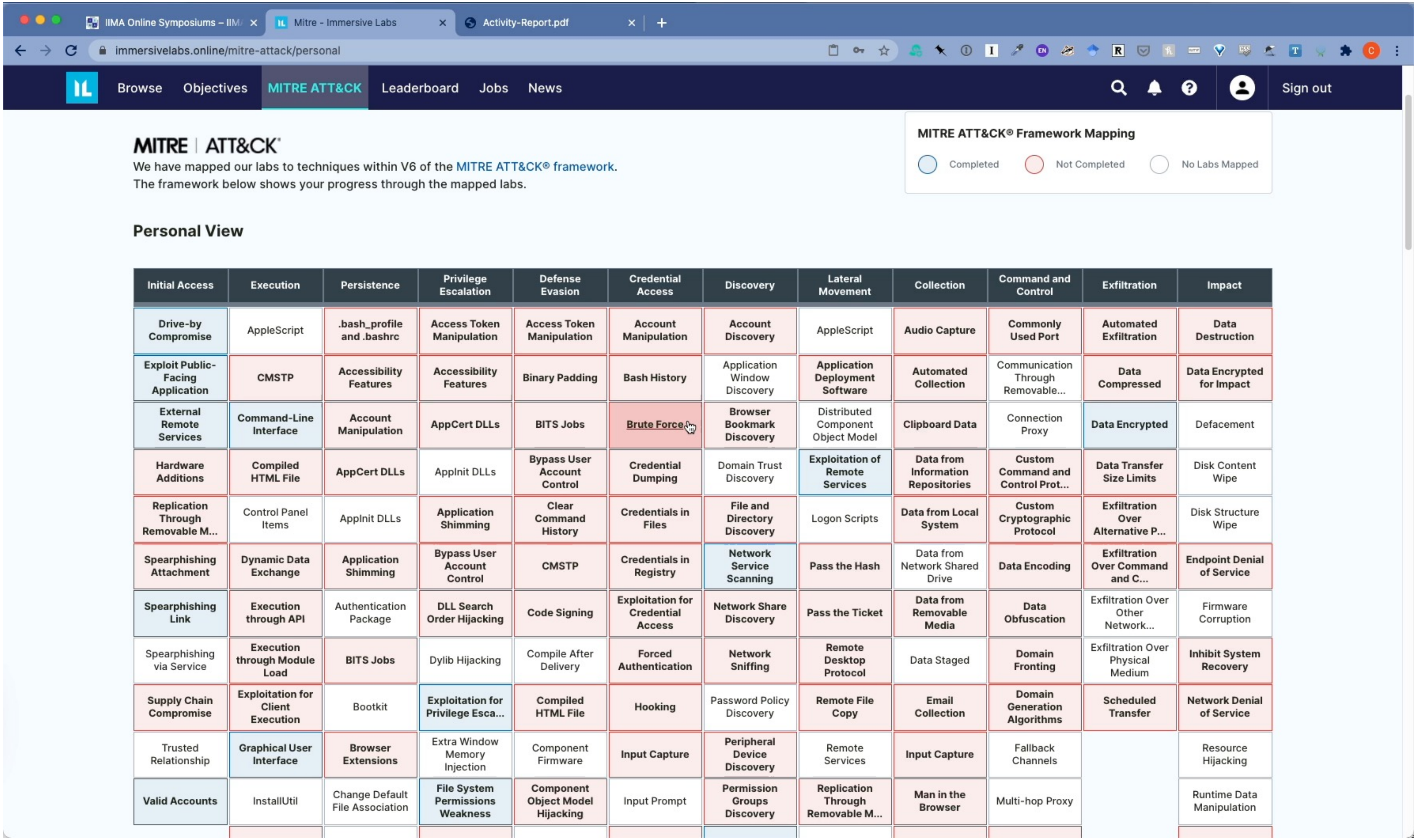
6% Defensive

11% Tools

0% Cyber Threat Intelligence

0% Malware & Reverse Engineering

# Reporting



MITRE | ATT&CK®

We have mapped our labs to techniques within V6 of the MITRE ATT&CK® framework.
The framework below shows your progress through the mapped labs.

MITRE ATT&CK® Framework Mapping

○ Completed ○ Not Completed ○ No Labs Mapped

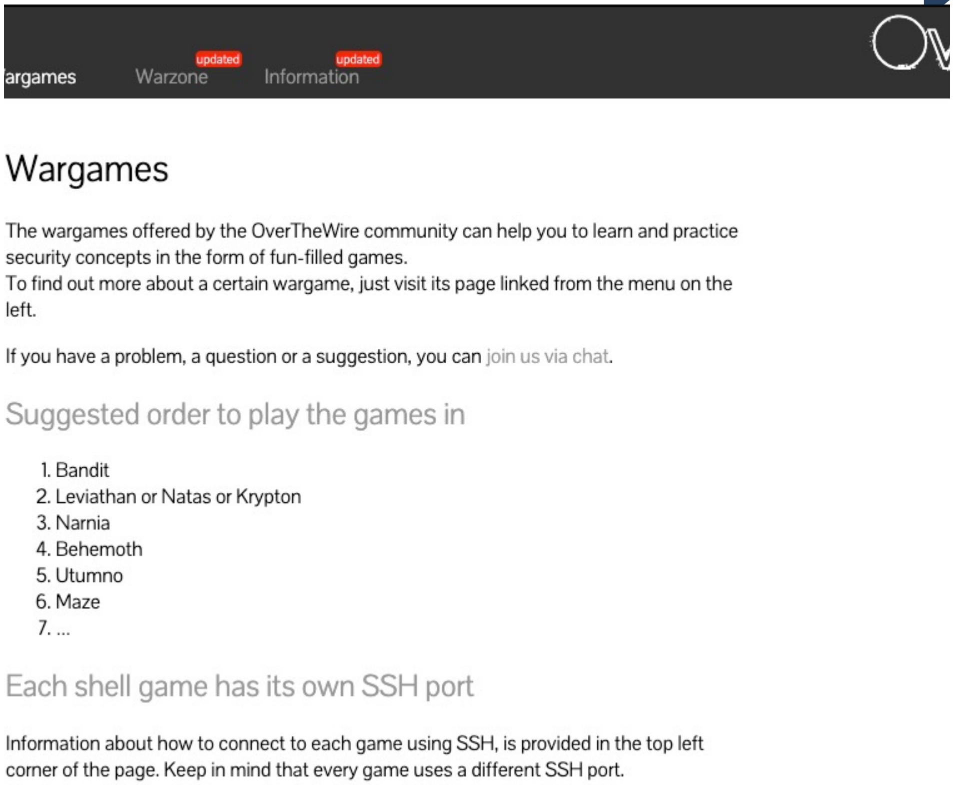
Personal View

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Drive-by Compromise | AppleScript | .bash_profile and .bashrc | Access Token Manipulation | Access Token Manipulation | Account Manipulation | Account Discovery | AppleScript | Audio Capture | Commonly Used Port | Automated Exfiltration | Data Destruction |
| Exploit Public-Facing Application | CMSTP | Accessibility Features | Accessibility Features | Binary Padding | Bash History | Application Window Discovery | Application Deployment Software | Automated Collection | Communication Through Removable... | Data Compressed | Data Encrypted for Impact |
| External Remote Services | Command-Line Interface | Account Manipulation | AppCert DLLs | BITS Jobs | Brute Force | Browser Bookmark Discovery | Distributed Component Object Model | Clipboard Data | Connection Proxy | Data Encrypted | Defacement |
| Hardware Additions | Compiled HTML File | AppCert DLLs | AppInit DLLs | Bypass User Account Control | Credential Dumping | Domain Trust Discovery | Exploitation of Remote Services | Data from Information Repositories | Custom Command and Control Prot... | Data Transfer Size Limits | Disk Content Wipe |
| Replication Through Removable M... | Control Panel Items | AppInit DLLs | Application Shimming | Clear Command History | Credentials in Files | File and Directory Discovery | Logon Scripts | Data from Local System | Custom Cryptographic Protocol | Exfiltration Over Alternative P... | Disk Structure Wipe |
| Spearphishing Attachment | Dynamic Data Exchange | Application Shimming | Bypass User Account Control | CMSTP | Credentials in Registry | Network Service Scanning | Pass the Hash | Data from Network Shared Drive | Data Encoding | Exfiltration Over Command and C... | Endpoint Denial of Service |
| Spearphishing Link | Execution through API | Authentication Package | DLL Search Order Hijacking | Code Signing | Exploitation for Credential Access | Network Share Discovery | Pass the Ticket | Data from Removable Media | Data Obfuscation | Exfiltration Over Other Network... | Firmware Corruption |
| Spearphishing via Service | Execution through Module Load | BITS Jobs | Dylib Hijacking | Compile After Delivery | Forced Authentication | Network Sniffing | Remote Desktop Protocol | Data Staged | Domain Fronting | Exfiltration Over Physical Medium | Inhibit System Recovery |
| Supply Chain Compromise | Exploitation for Client Execution | Bootkit | Exploitation for Privilege Esca... | Compiled HTML File | Hooking | Password Policy Discovery | Remote File Copy | Email Collection | Domain Generation Algorithms | Scheduled Transfer | Network Denial of Service |
| Trusted Relationship | Graphical User Interface | Browser Extensions | Extra Window Memory Injection | Component Firmware | Input Capture | Peripheral Device Discovery | Remote Services | Input Capture | Fallback Channels | | Resource Hijacking |
| Valid Accounts | InstallUtil | Change Default File Association | File System Permissions Weakness | Component Object Model Hijacking | Input Prompt | Permission Groups Discovery | Replication Through Removable M... | Man in the Browser | Multi-hop Proxy | | Runtime Data Manipulation |

# 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.

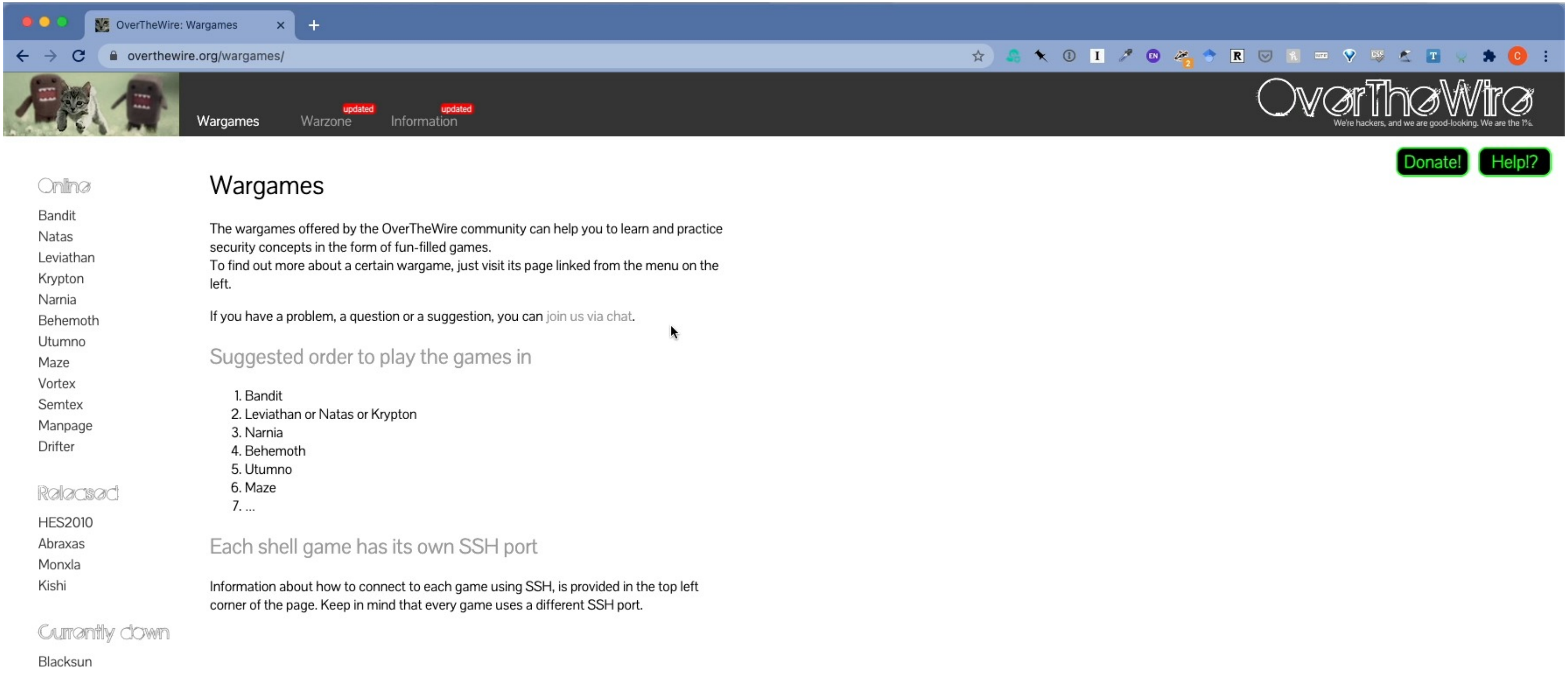
### Suggested order to play the games in

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.

# Over the Wire



Online

- Bandit
- Natas
- Leviathan
- Krypton
- Narnia
- Behemoth
- Utumno
- Maze
- Vortex
- Semtex
- Manpage
- Drifter

Released

- HES2010
- Abraxas
- Monxla
- Kishi

Currently down

- Blacksun

## 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.

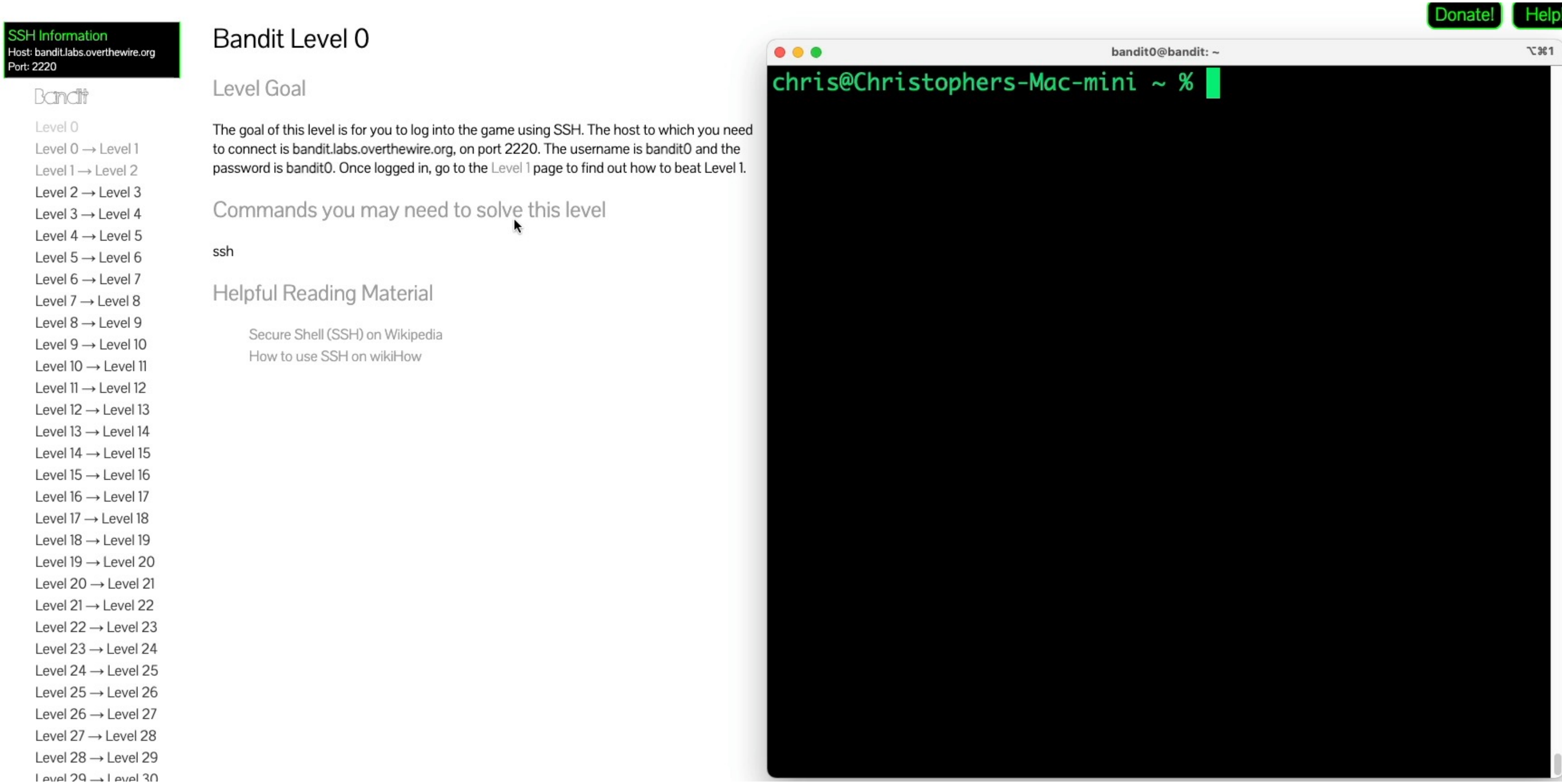
If you have a problem, a question or a suggestion, you can join us via chat.

### 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.



SSH Information
Host: bandit.labs.overthewire.org
Port: 2220

## Bandit Level 0

### Level Goal

The goal of this level is for you to log into the game using SSH. The host to which you need to connect is bandit.labs.overthewire.org, on port 2220. The username is bandit0 and the password is bandit0. Once logged in, go to the Level 1 page to find out how to beat Level 1.

### Commands you may need to solve this level

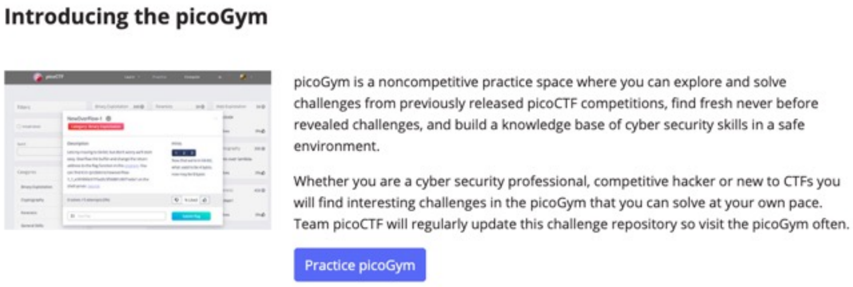
ssh

### Helpful Reading Material

Secure Shell (SSH) on Wikipedia
How to use SSH on wikiHow

```
chris@Christophers-Mac-mini ~ % 
```

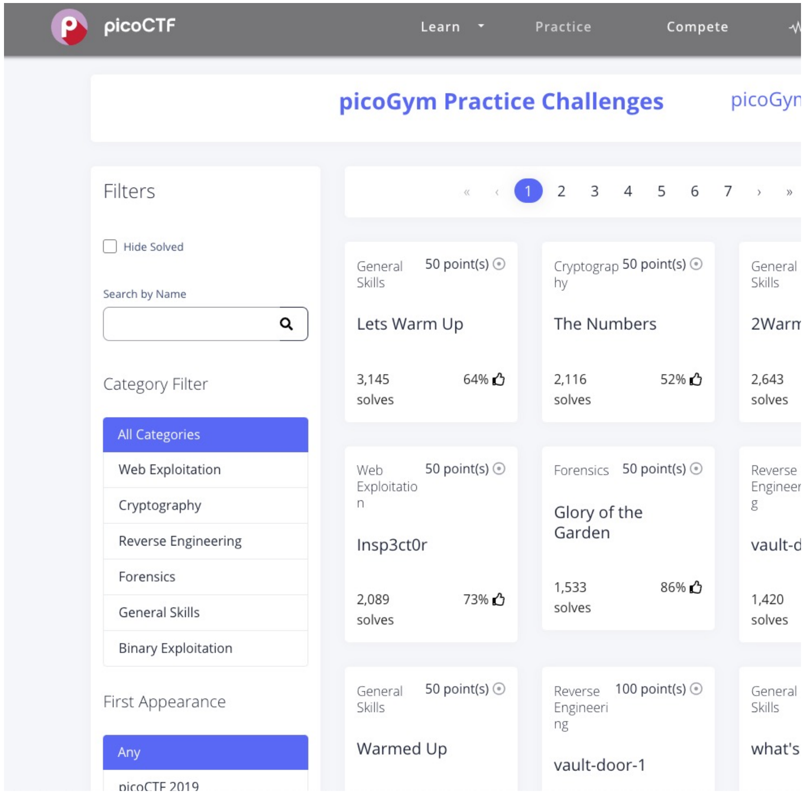
# Bandit Demo



### 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.



General Skills 50 point(s)
Lets Warm Up
3,145 solves 64%

Cryptography 50 point(s)
The Numbers
2,116 solves 52%

General Skills
2Warm
2,643 solves

Web Exploitation 50 point(s)
Insp3ct0r
2,089 solves 73%

Forensics 50 point(s)
Glory of the Garden
1,533 solves 86%

Reverse Engineering
vault-d
1,420 solves

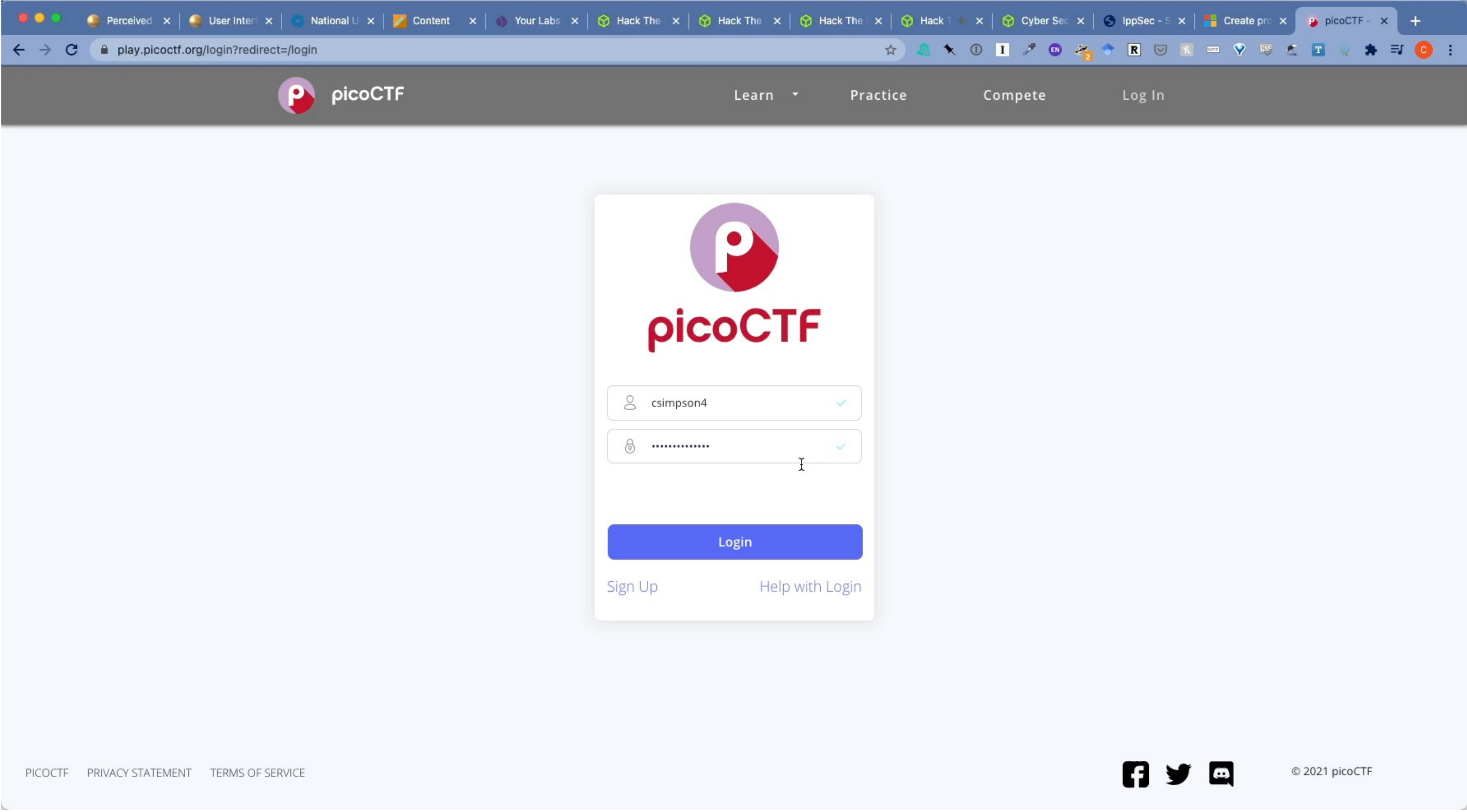
General Skills 50 point(s)
Warmed Up

Reverse Engineering 100 point(s)
vault-door-1

General Skills
what's

PicoCTF

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


Perceived
User Inter
National U
Content
Your Labs
Hack The
Hack The
Hack The
Hack T
Cyber Sec
IppSec - S
Create pro
picoCTF -
play.picoctf.org/login?redirect=/login
picoCTF
Learn
Practice
Compete
Log In
picoCTF

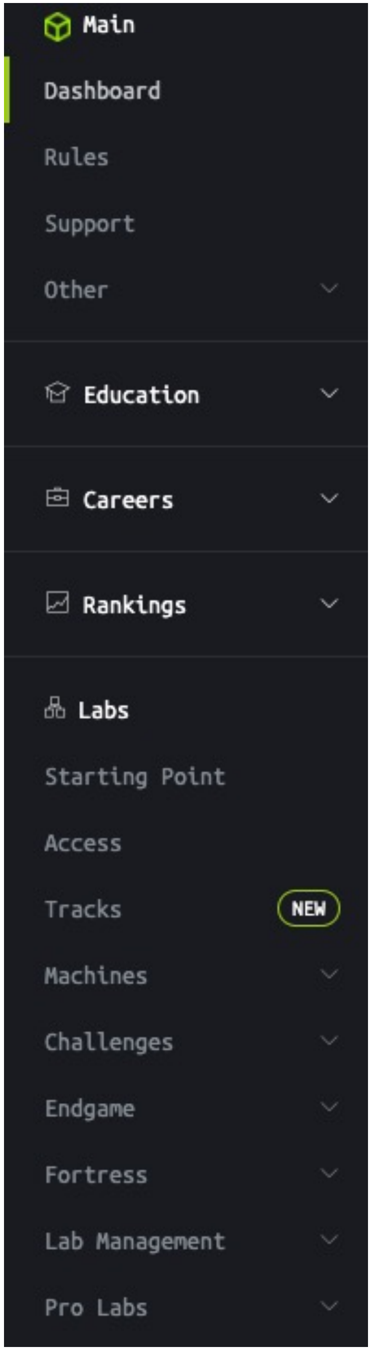
csimpson4

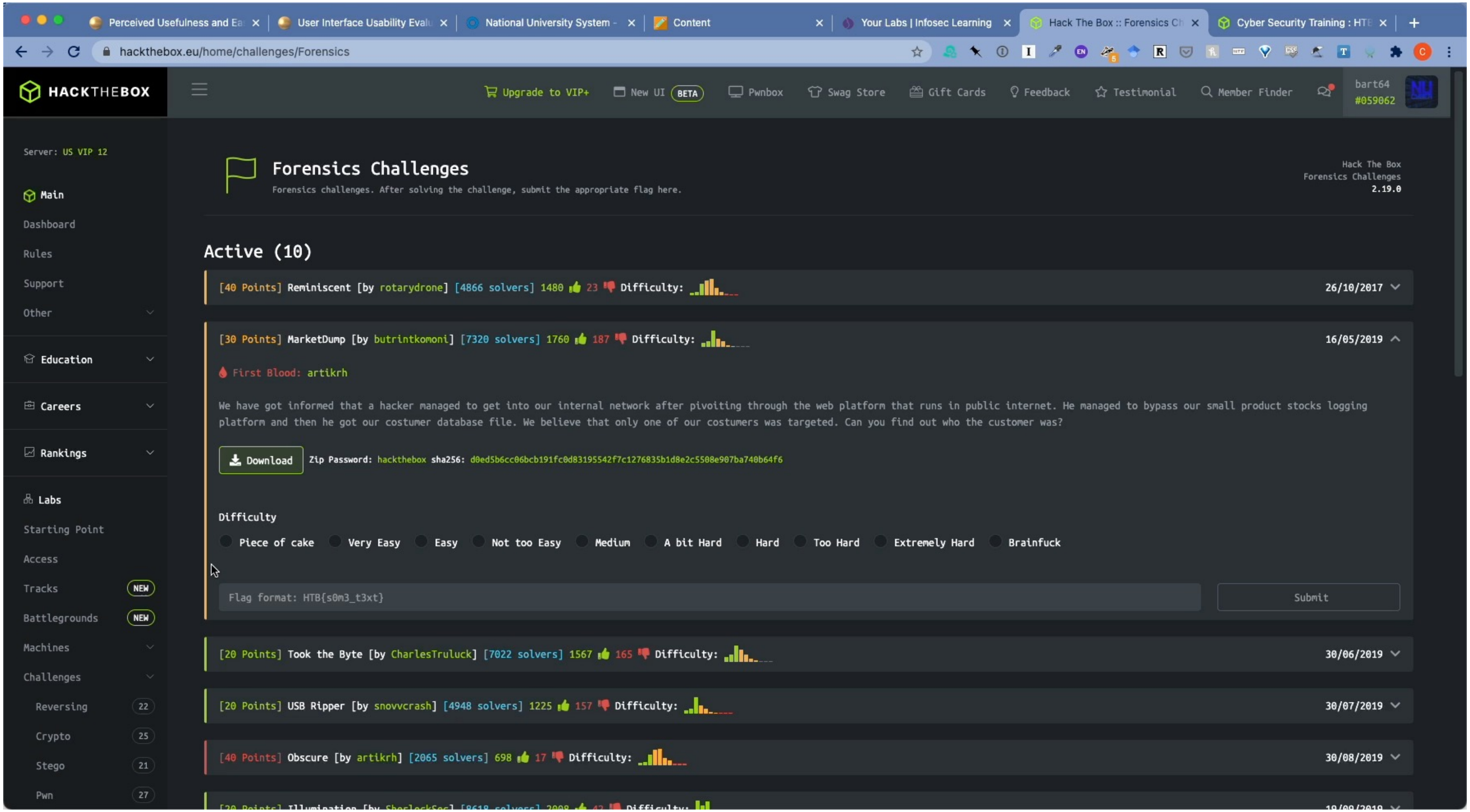
••••••••••••••

Login
Sign Up
Help with Login
PICOCTF
PRIVACY STATEMENT
TERMS OF SERVICE
© 2021 picoCTF

# 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





## Forensics Challenges

Forensics challenges. After solving the challenge, submit the appropriate flag here.

Hack The Box
Forensics Challenges
2.19.0

### Active (10)

[40 Points] Reminiscent [by rotarydrone] [4866 solvers] 1480 👍 23 👎 Difficulty: 26/10/2017

[30 Points] MarketDump [by butrintkomoni] [7320 solvers] 1760 👍 187 👎 Difficulty: 16/05/2019

First Blood: artikrh

We have got informed that a hacker managed to get into our internal network after pivoting through the web platform that runs in public internet. He managed to bypass our small product stocks logging platform and then he got our costumer database file. We believe that only one of our costumers was targeted. Can you find out who the customer was?

Download Zip Password: hackthebox sha256: d0ed5b6cc06bcb191fc0d83195542f7c1276835b1d8e2c5508e907ba740b64f6

Difficulty

○ Piece of cake ○ Very Easy ○ Easy ○ Not too Easy ○ Medium ○ A bit Hard ○ Hard ○ Too Hard ○ Extremely Hard ○ Brainfuck

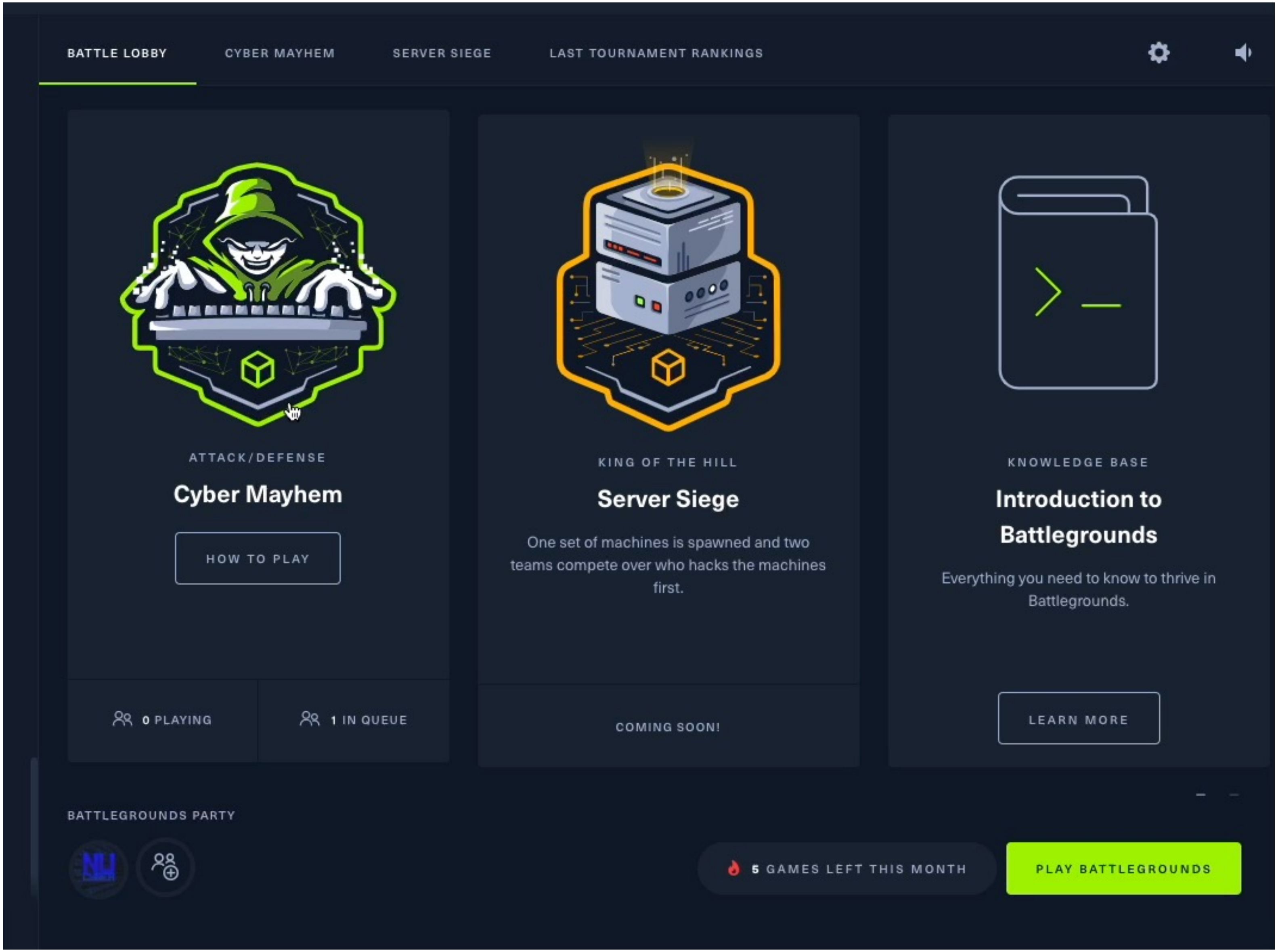
Flag format: HTB{s0m3_t3xt} Submit

[20 Points] Took the Byte [by CharlesTruluck] [7022 solvers] 1567 👍 165 👎 Difficulty: 30/06/2019

[20 Points] USB Ripper [by snovvcrash] [4948 solvers] 1225 👍 157 👎 Difficulty: 30/07/2019

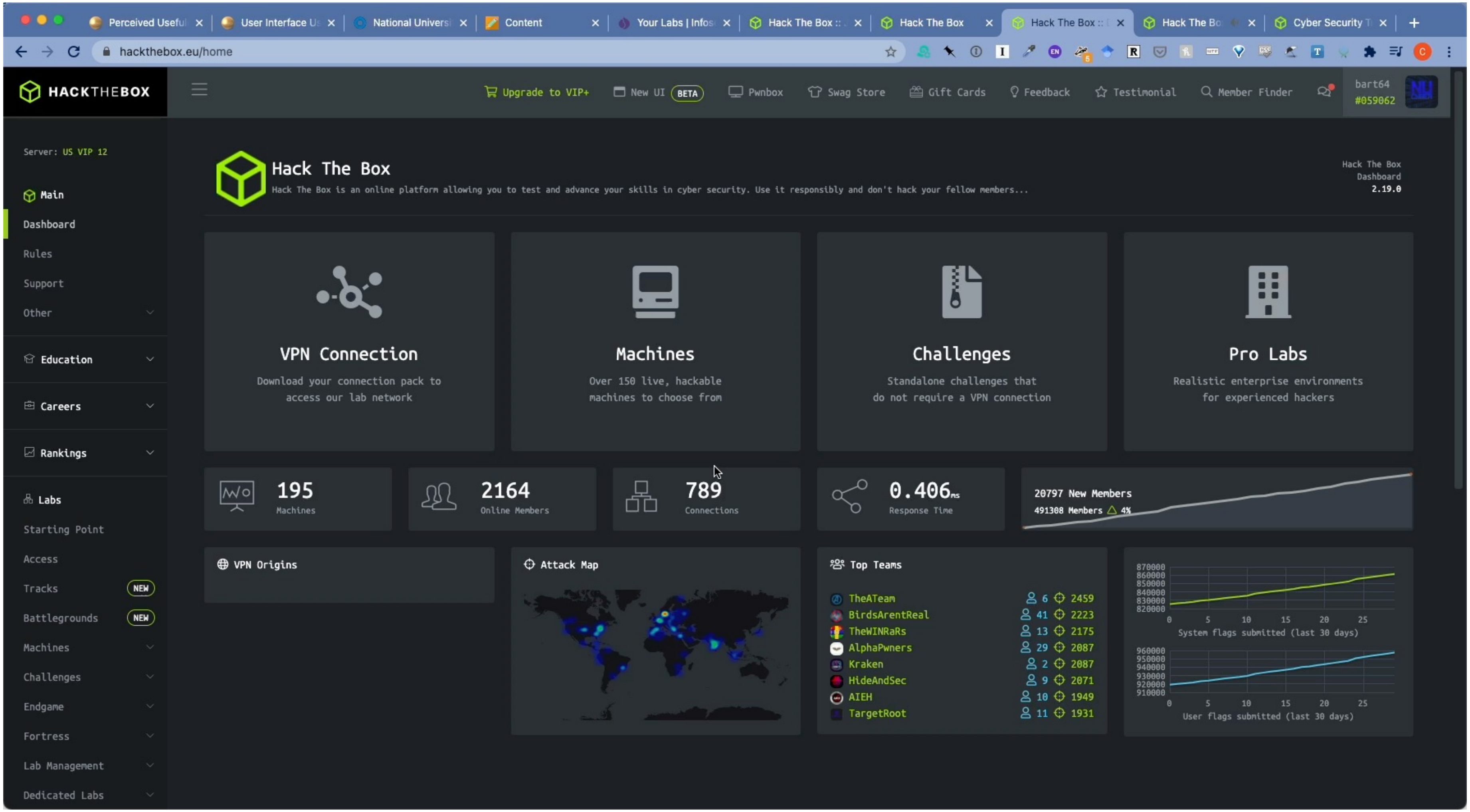
[40 Points] Obscure [by artikrh] [2065 solvers] 698 👍 17 👎 Difficulty: 30/08/2019

[20 Points] Illumination [by SherlockSec] [8618 solvers] 2008 👍 42 👎 Difficulty: 19/09/2019



One set of machines is spawned and two teams compete over who hacks the machines first.

Everything you need to know to thrive in Battlegrounds.



Server: US VIP 12

- Main
- Dashboard
- Rules
- Support
- Other
- Education
- Careers
- Rankings
- Labs
- Starting Point
- Access
- Tracks NEW
- Battlegrounds NEW
- Machines
- Challenges
- Endgame
- Fortress
- Lab Management
- Dedicated Labs

## Hack The Box

Hack The Box is an online platform allowing you to test and advance your skills in cyber security. Use it responsibly and don't hack your fellow members...

Hack The Box
Dashboard
2.19.0

**VPN Connection**
Download your connection pack to access our lab network

**Machines**
Over 150 live, hackable machines to choose from

**Challenges**
Standalone challenges that do not require a VPN connection

**Pro Labs**
Realistic enterprise environments for experienced hackers

195 Machines

2164 Online Members

789 Connections

0.406ms Response Time

20797 New Members
491308 Members △ 4%

VPN Origins

Attack Map

Top Teams

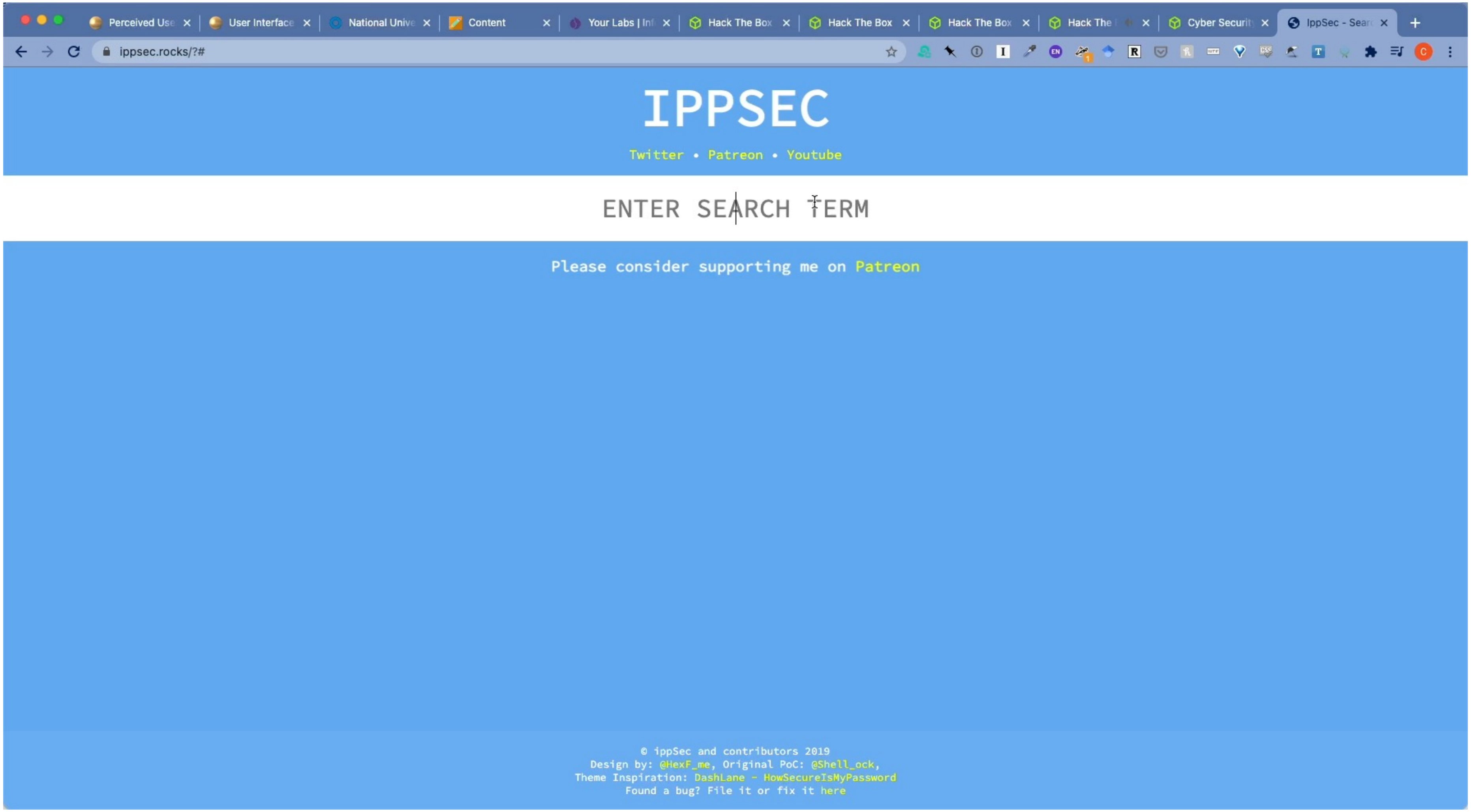
| | | |
|---|---|---|
| TheATeam | 6 | 2459 |
| BirdsArentReal | 41 | 2223 |
| TheWINRaRs | 13 | 2175 |
| AlphaPwners | 29 | 2087 |
| Kraken | 2 | 2087 |
| HideAndSec | 9 | 2071 |
| AIEH | 10 | 1949 |
| TargetRoot | 11 | 1931 |

System flags submitted (last 30 days)

User flags submitted (last 30 days)

# Videos and Tutorials

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



IPPSEC

Twitter • Patreon • Youtube

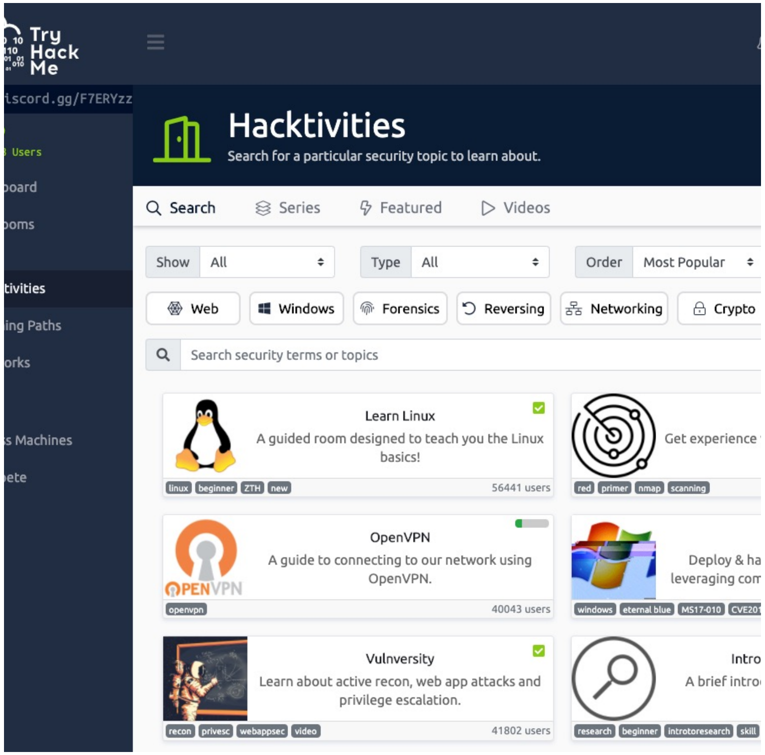
ENTER SEARCH TERM

Please consider supporting me on Patreon

© ippSec and contributors 2019
Design by: @HexF_me, Original PoC: @Shell_ock,
Theme Inspiration: DashLane - HowSecureIsMyPassword
Found a bug? File it or fix it here

# TryHackMe

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



Hacktivities

Search for a particular security topic to learn about.

Learn Linux

A guided room designed to teach you the Linux basics!

linux beginner ZTH new 56441 users

Get experience

red primer nmap scanning

OpenVPN

A guide to connecting to our network using OpenVPN.

openvpn 40043 users

Deploy & ha leveraging com

windows eternal blue MS17-010 CVE20

Vulnversity

Learn about active recon, web app attacks and privilege escalation.

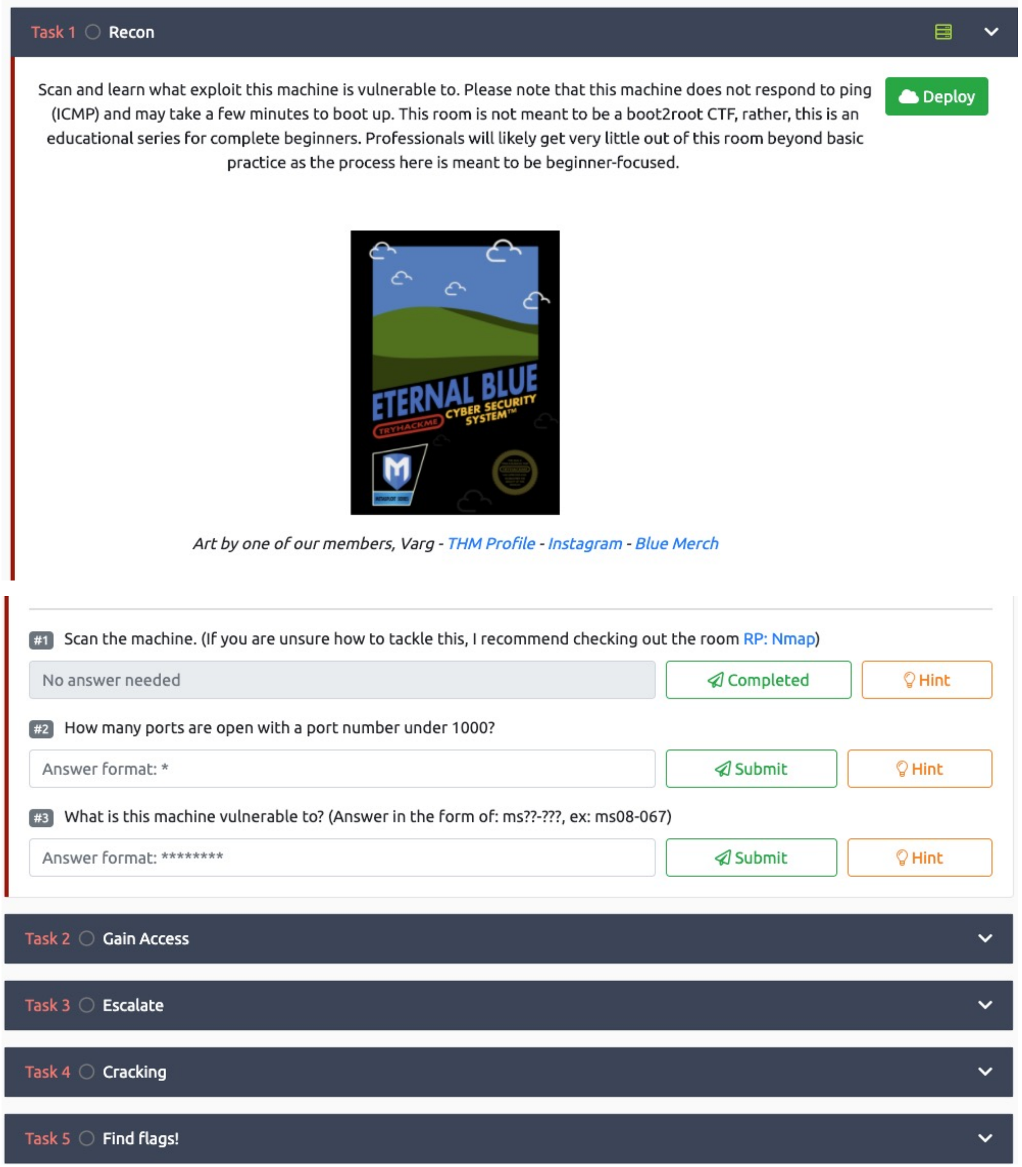
recon privesc webappsec video 41802 users

Intro

A brief intro

research beginner introtoresearch skill

# TryHackMe



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.

*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

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

Answer format: *

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

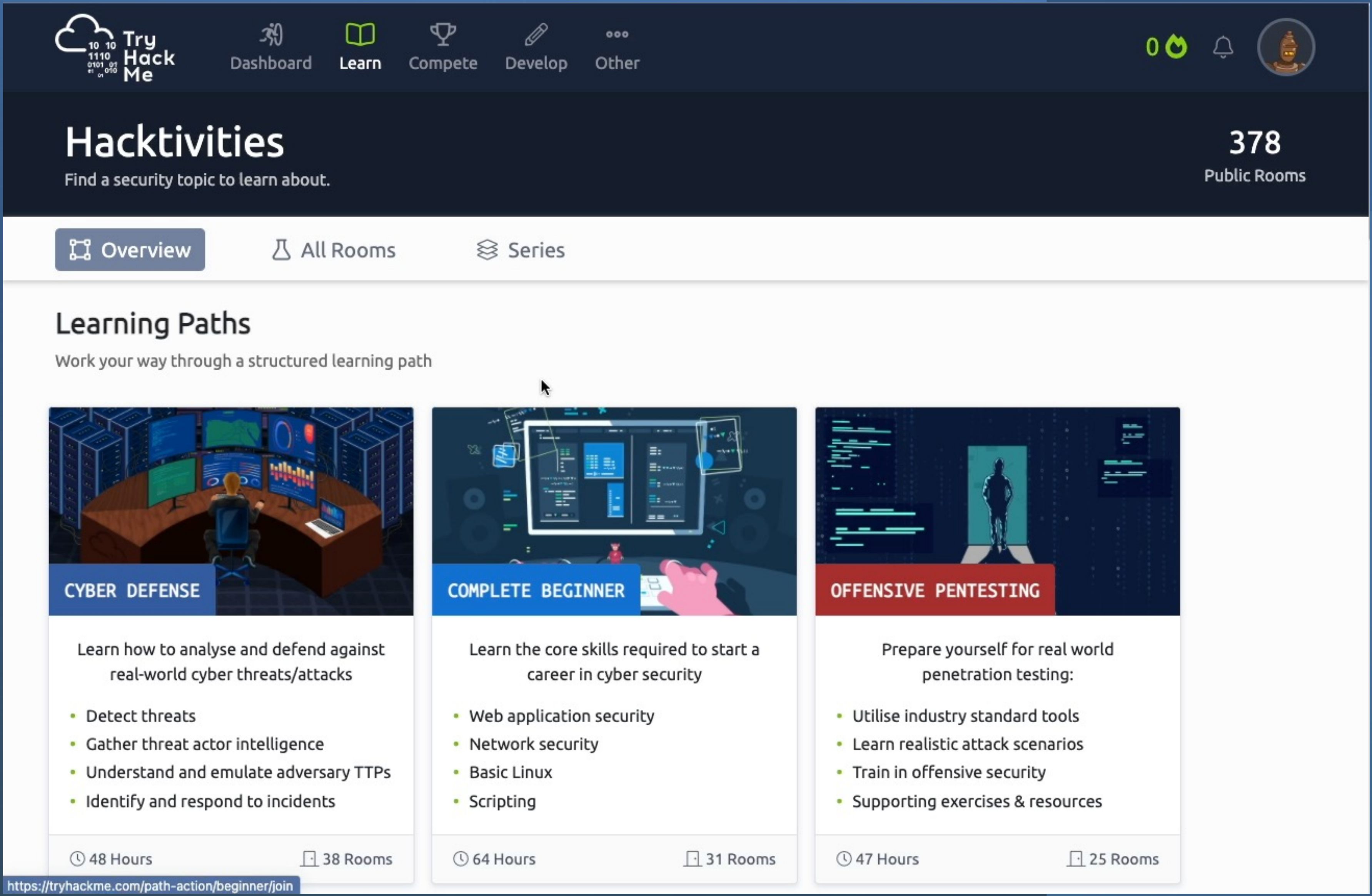
Answer format: ********

Task 2 ○ Gain Access

Task 3 ○ Escalate

Task 4 ○ Cracking

Task 5 ○ Find flags!



# Hacktivities

Find a security topic to learn about.

378
Public Rooms

## Learning Paths

Work your way through a structured learning path

**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 | 38 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 | 31 Rooms

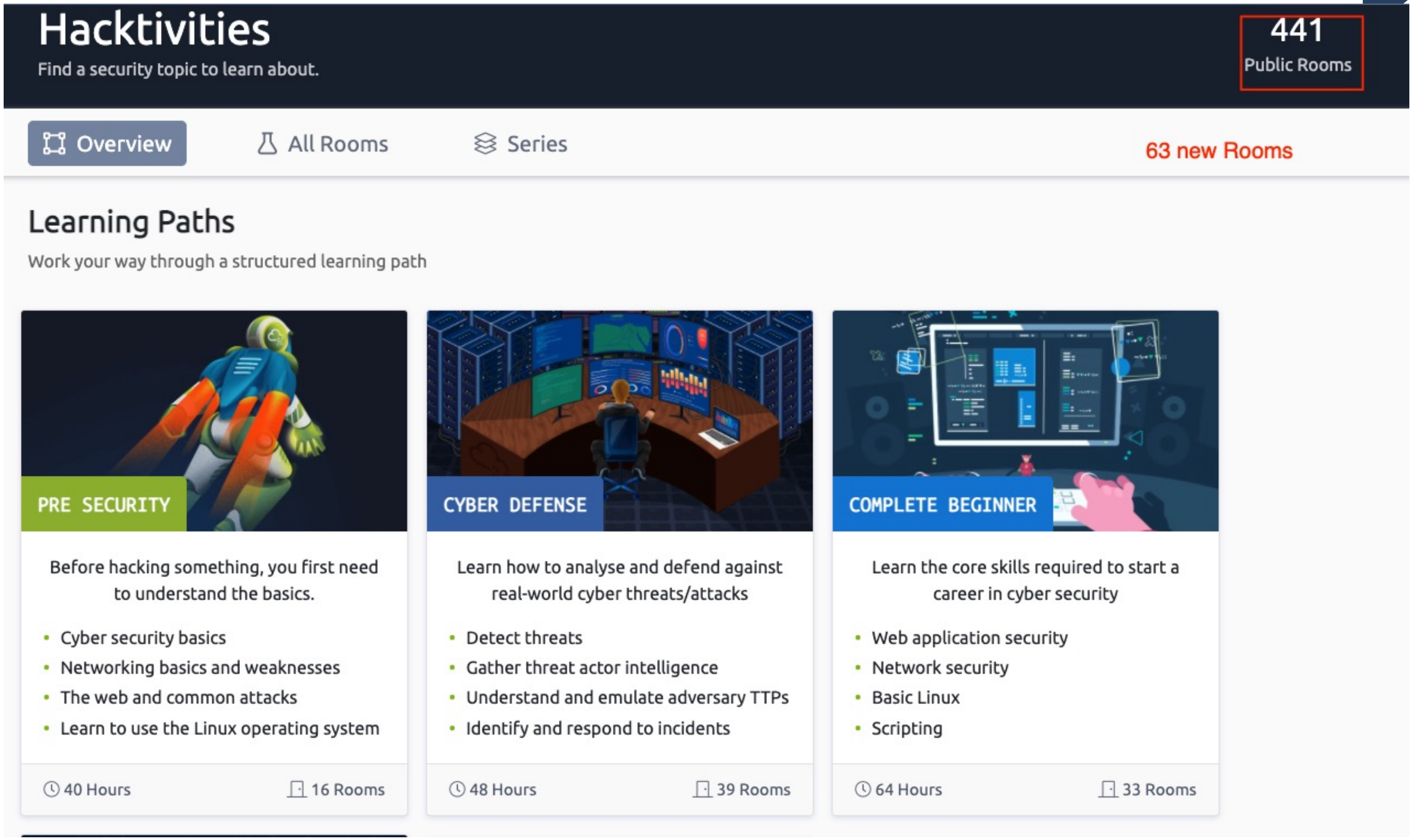
**OFFENSIVE PENTESTING**

Prepare yourself for real world penetration testing:

- Utilise industry standard tools
- Learn realistic attack scenarios
- Train in offensive security
- Supporting exercises & resources

47 Hours | 25 Rooms

# Pre Security



## Hacktivities

Find a security topic to learn about.

441
Public Rooms

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**

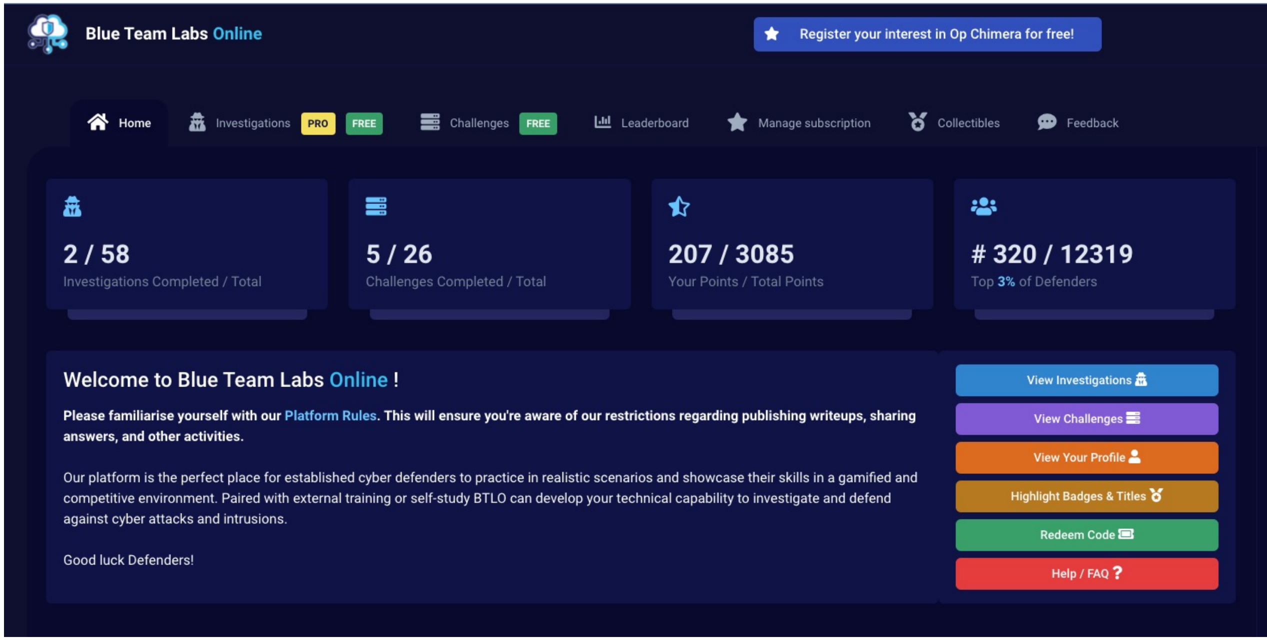
Learn the core skills required to start a career in cyber security

- 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



2 / 58
Investigations Completed / Total

5 / 26
Challenges Completed / Total

207 / 3085
Your Points / Total Points

# 320 / 12319
Top 3% of Defenders

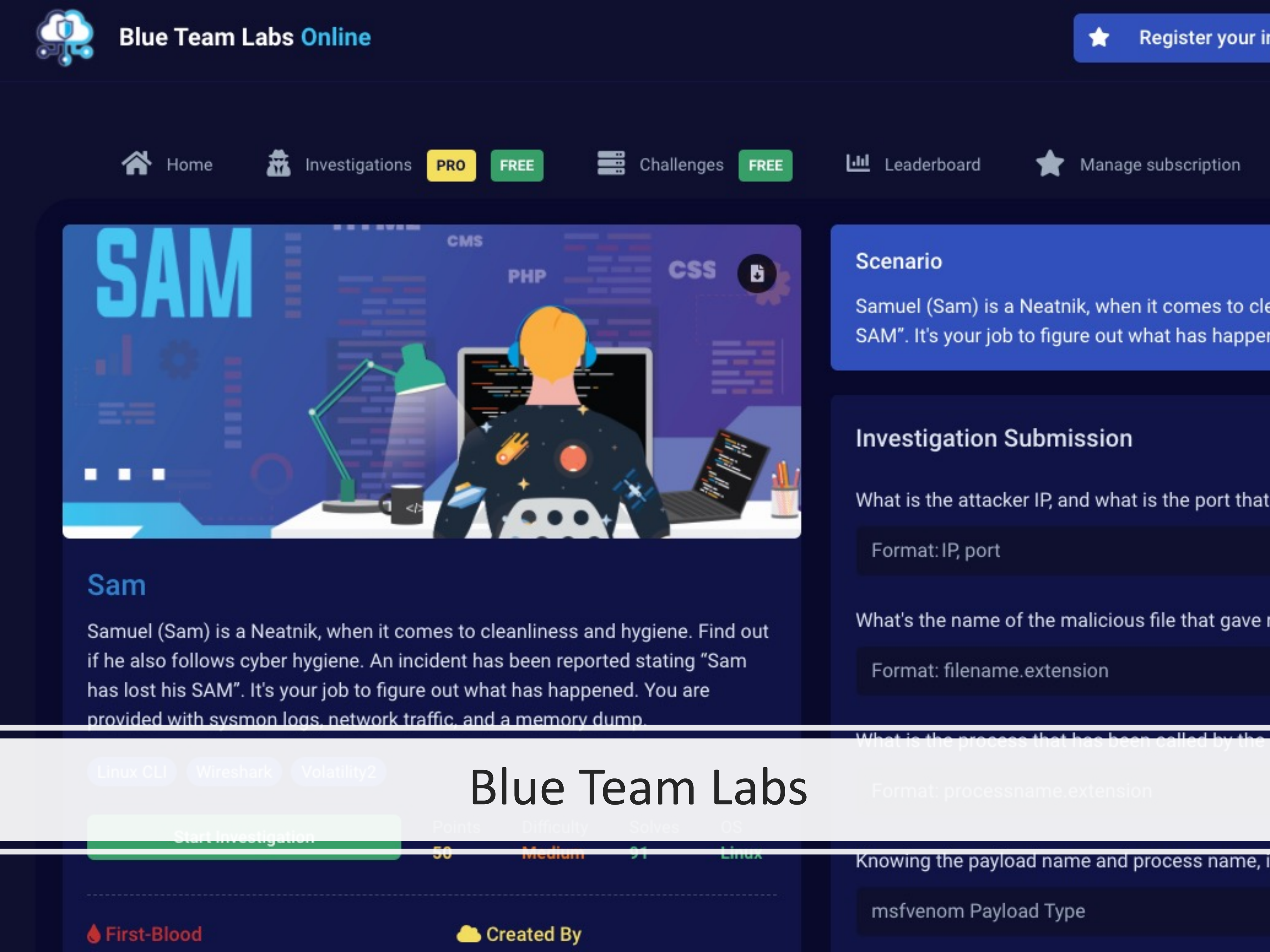
Welcome to Blue Team Labs Online !

**Please familiarise yourself with our Platform Rules. This will ensure you're aware of our restrictions regarding publishing writeups, sharing answers, and other activities.**

Our platform is the perfect place for established cyber defenders to practice in realistic scenarios and showcase their skills in a gamified and competitive environment. Paired with external training or self-study BTLO can develop your technical capability to investigate and defend against cyber attacks and intrusions.

Good luck Defenders!

# Blue Team Labs



## 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.

| Points | Difficulty | Solves | OS |
|---|---|---|---|
| 50 | Medium | 91 | Linux |

## Scenario

Samuel (Sam) is a Neatnik, when it comes to cle
SAM". It's your job to figure out what has happen

## Investigation Submission

What is the attacker IP, and what is the port that

Format: IP, port

What's the name of the malicious file that gave r

Format: filename.extension

What is the process that has been called by the

Format: processname.extension

Knowing the payload name and process name, i

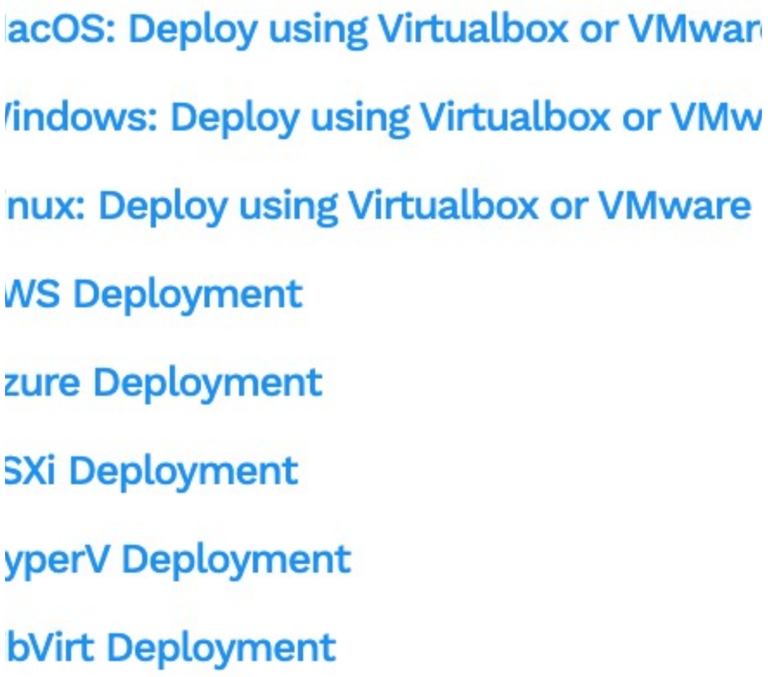
msfvenom Payload Type

# Deploy in the Cloud

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

# Detection Lab

- "DetectionLab is a repository containing a variety of Packer, Vagrant, Powershell, Ansible, and Terraform scripts that allow you to automate the process of bringing an ActiveDirectory environment online complete with logging and security tooling using a variety of different platforms.
- https://www.detectionlab.network/



acOS: Deploy using Virtualbox or VMwar

indows: Deploy using Virtualbox or VMw

nux: Deploy using Virtualbox or VMware

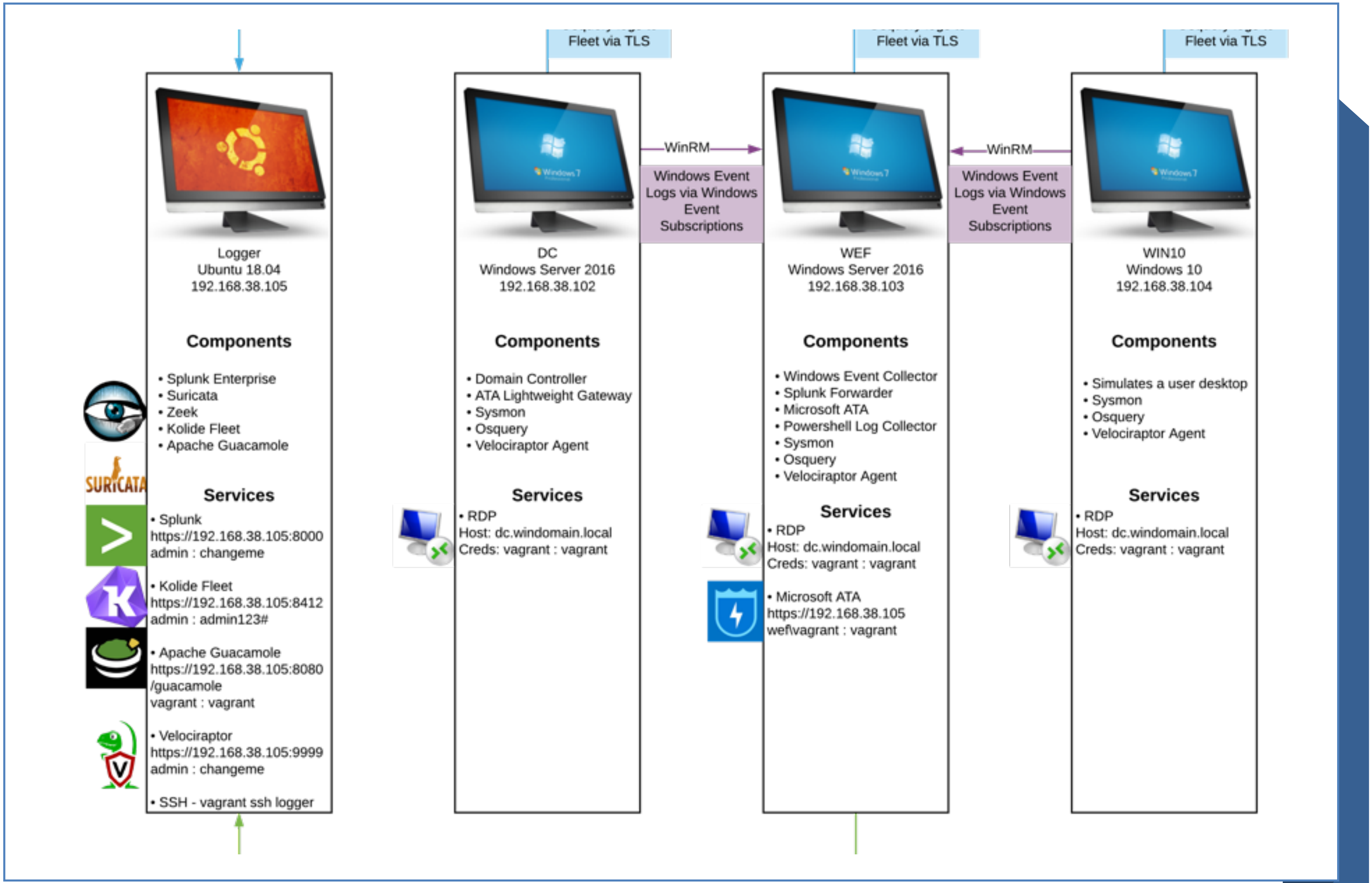
WS Deployment

zure Deployment

SXi Deployment

yperV Deployment

bVirt Deployment



Fleet via TLS

Fleet via TLS

Fleet via TLS

WinRM

Windows Event Logs via Windows Event Subscriptions

WinRM

Windows Event Logs via Windows Event Subscriptions

Logger
Ubuntu 18.04
192.168.38.105

**Components**

- Splunk Enterprise
- Suricata
- Zeek
- Kolide Fleet
- Apache Guacamole

**Services**

- Splunk
https://192.168.38.105:8000
admin : changeme
- Kolide Fleet
https://192.168.38.105:8412
admin : admin123#
- Apache Guacamole
https://192.168.38.105:8080
/guacamole
vagrant : vagrant
- Velociraptor
https://192.168.38.105:9999
admin : changeme
- SSH - vagrant ssh logger

DC
Windows Server 2016
192.168.38.102

**Components**

- Domain Controller
- ATA Lightweight Gateway
- Sysmon
- Osquery
- Velociraptor Agent

**Services**

- RDP
Host: dc.windomain.local
Creds: vagrant : vagrant

WEF
Windows Server 2016
192.168.38.103

**Components**

- Windows Event Collector
- Splunk Forwarder
- Microsoft ATA
- Powershell Log Collector
- Sysmon
- Osquery
- Velociraptor Agent

**Services**

- RDP
Host: dc.windomain.local
Creds: vagrant : vagrant
- Microsoft ATA
https://192.168.38.105
wef\vagrant : vagrant

WIN10
Windows 10
192.168.38.104

**Components**

- Simulates a user desktop
- Sysmon
- Osquery
- Velociraptor Agent

**Services**

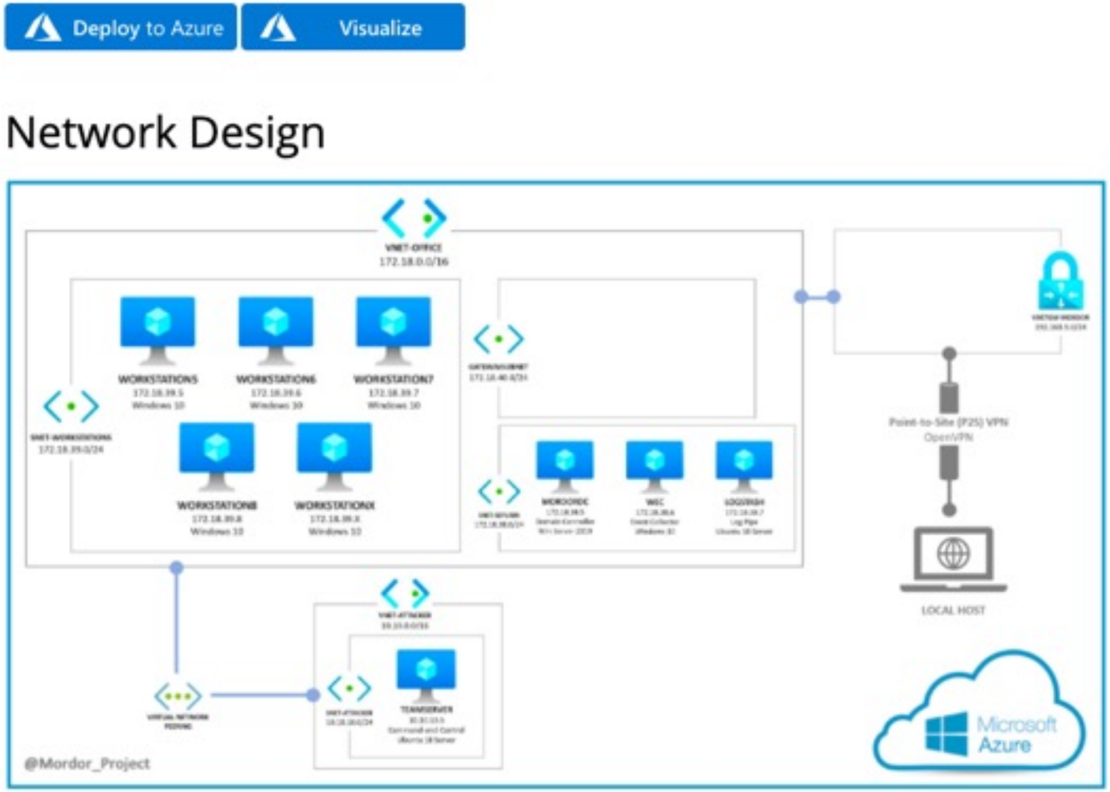
- RDP
Host: dc.windomain.local
Creds: vagrant : vagrant

# Project Mordor

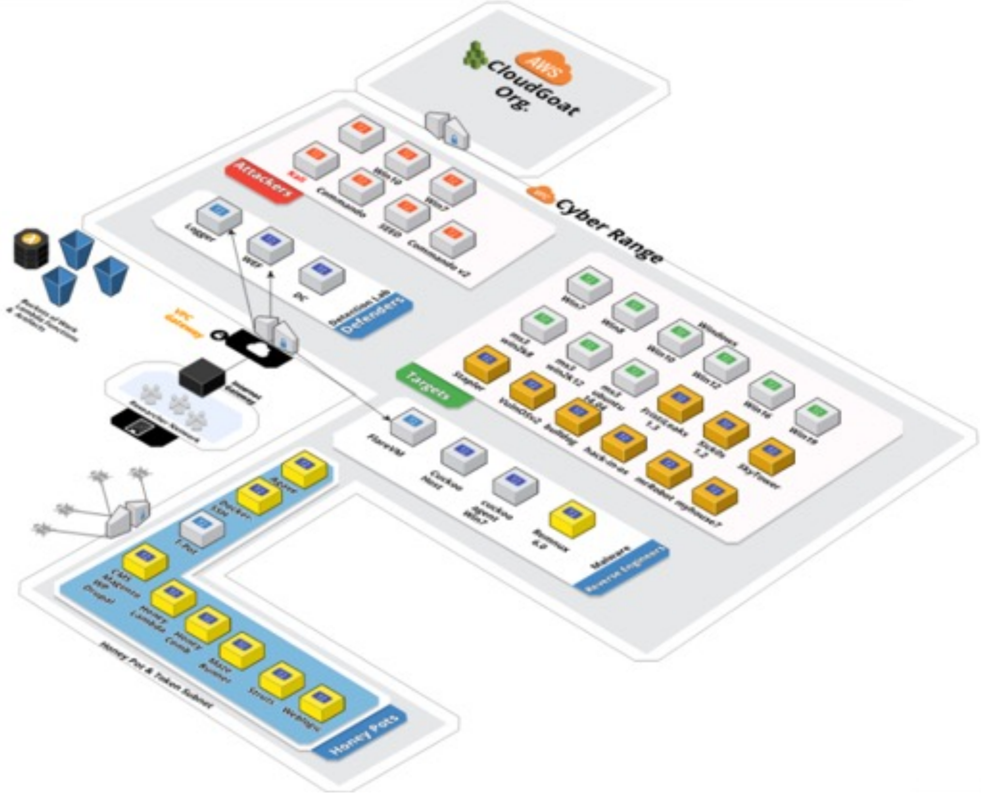
- The Mordor project provides pre-recorded security events generated by simulated adversarial techniques in the form of JavaScript Object Notation (JSON) files for easy consumption.
- The pre-recorded data is categorized by platforms, adversary groups, tactics and techniques defined by the Mitre ATT&CK Framework.
- The pre-recorded data represents not only specific known malicious events but additional context/events that occur around it.
- https://mordordatasets.com/introduction.html

Template for Azure deployment

# Project Mordor



## Network Design



# Cyber Range

- This project provides a bootstrap framework for a complete offensive, defensive, reverse engineering, & security intelligence tooling in a private research lab using the AWS Cloud.

- This project contains vulnerable systems and a toolkit of the most powerful open-source / community edition tools known to Penetration testers, Developers, Malware Analysts, Forensic/Reverse Engineers, ThreatHunters, & more.

# Nice Challenge

- Excellent set of challenges
- Mapped to NICE Framework
- Free
- Reservations required

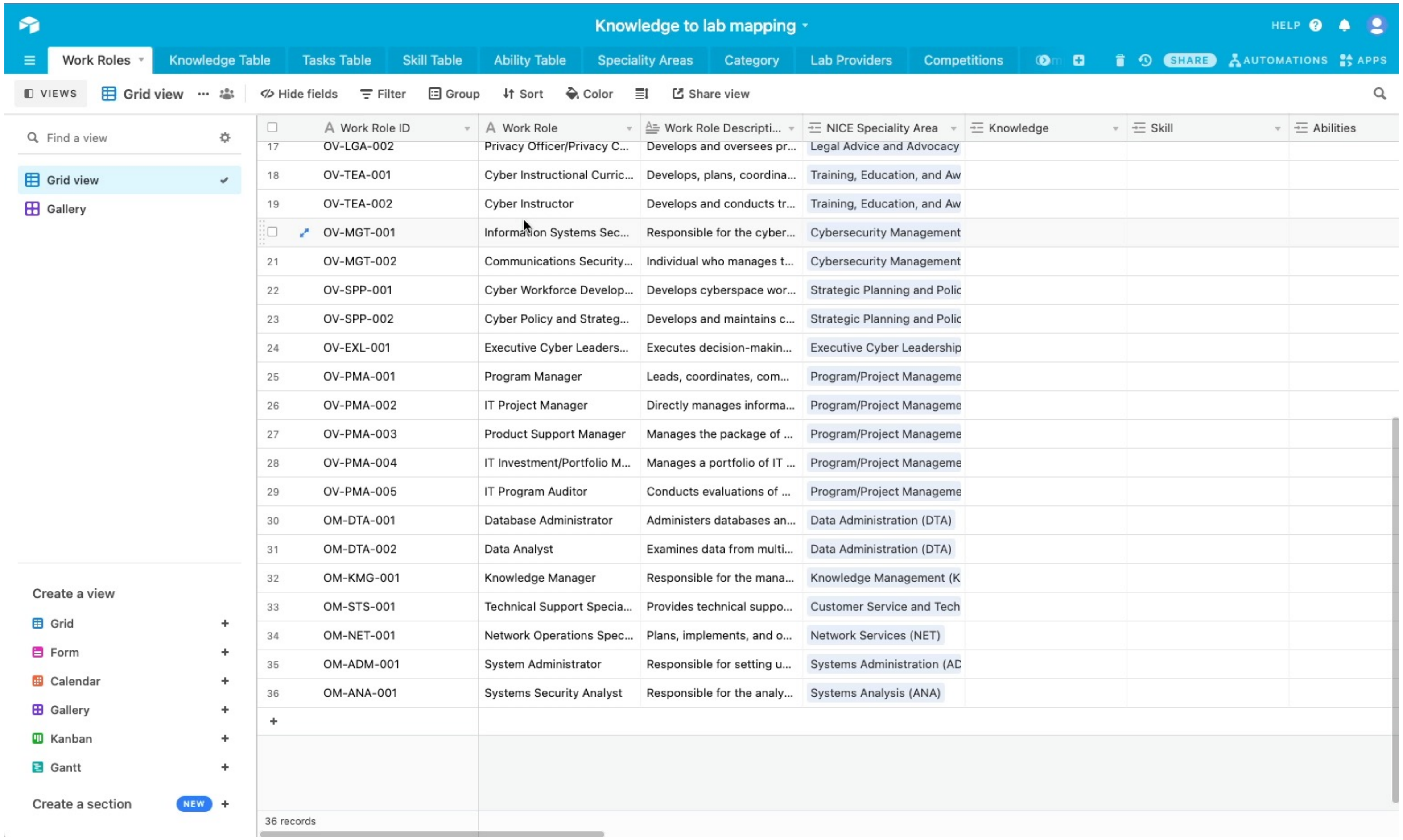
# Mapping Labs To Objectives

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

Student project mapping TryHackMe

Using AirTable

# Airtable Demo

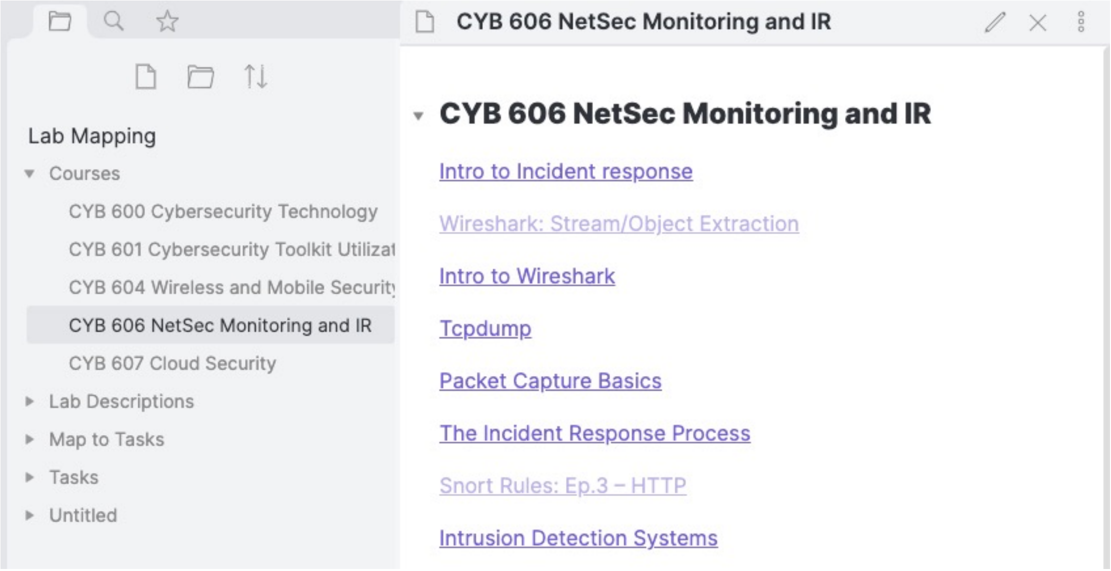


| | Work Role ID | Work Role | Work Role Descripti... | NICE Speciality Area | Knowledge | Skill | Abilities |
|---|---|---|---|---|---|---|---|
| 17 | OV-LGA-002 | Privacy Officer/Privacy C... | Develops and oversees pr... | Legal Advice and Advocacy | | | |
| 18 | OV-TEA-001 | Cyber Instructional Curric... | Develops, plans, coordina... | Training, Education, and Aw | | | |
| 19 | OV-TEA-002 | Cyber Instructor | Develops and conducts tr... | Training, Education, and Aw | | | |
| □ | OV-MGT-001 | Information Systems Sec... | Responsible for the cyber... | Cybersecurity Management | | | |
| 21 | OV-MGT-002 | Communications Security... | Individual who manages t... | Cybersecurity Management | | | |
| 22 | OV-SPP-001 | Cyber Workforce Develop... | Develops cyberspace wor... | Strategic Planning and Polic | | | |
| 23 | OV-SPP-002 | Cyber Policy and Strateg... | Develops and maintains c... | Strategic Planning and Polic | | | |
| 24 | OV-EXL-001 | Executive Cyber Leaders... | Executes decision-makin... | Executive Cyber Leadership | | | |
| 25 | OV-PMA-001 | Program Manager | Leads, coordinates, com... | Program/Project Manageme | | | |
| 26 | OV-PMA-002 | IT Project Manager | Directly manages informa... | Program/Project Manageme | | | |
| 27 | OV-PMA-003 | Product Support Manager | Manages the package of ... | Program/Project Manageme | | | |
| 28 | OV-PMA-004 | IT Investment/Portfolio M... | Manages a portfolio of IT ... | Program/Project Manageme | | | |
| 29 | OV-PMA-005 | IT Program Auditor | Conducts evaluations of ... | Program/Project Manageme | | | |
| 30 | OM-DTA-001 | Database Administrator | Administers databases an... | Data Administration (DTA) | | | |
| 31 | OM-DTA-002 | Data Analyst | Examines data from multi... | Data Administration (DTA) | | | |
| 32 | OM-KMG-001 | Knowledge Manager | Responsible for the mana... | Knowledge Management (K | | | |
| 33 | OM-STS-001 | Technical Support Specia... | Provides technical suppo... | Customer Service and Tech | | | |
| 34 | OM-NET-001 | Network Operations Spec... | Plans, implements, and o... | Network Services (NET) | | | |
| 35 | OM-ADM-001 | System Administrator | Responsible for setting u... | Systems Administration (AD | | | |
| 36 | OM-ANA-001 | Systems Security Analyst | Responsible for the analy... | Systems Analysis (ANA) | | | |

# How do we share?

# Obsidian

- Multi platform notetaking app with wiki like capability
- Based on Markdown



Lab Mapping

- Courses
  - CYB 600 Cybersecurity Technology
  - CYB 601 Cybersecurity Toolkit Utilizat
  - CYB 604 Wireless and Mobile Securit
  - CYB 606 NetSec Monitoring and IR
  - CYB 607 Cloud Security
- Lab Descriptions
- Map to Tasks
- Tasks
- Untitled

CYB 606 NetSec Monitoring and IR

## CYB 606 NetSec Monitoring and IR

Intro to Incident response

Wireshark: Stream/Object Extraction

Intro to Wireshark

Tcpdump

Packet Capture Basics

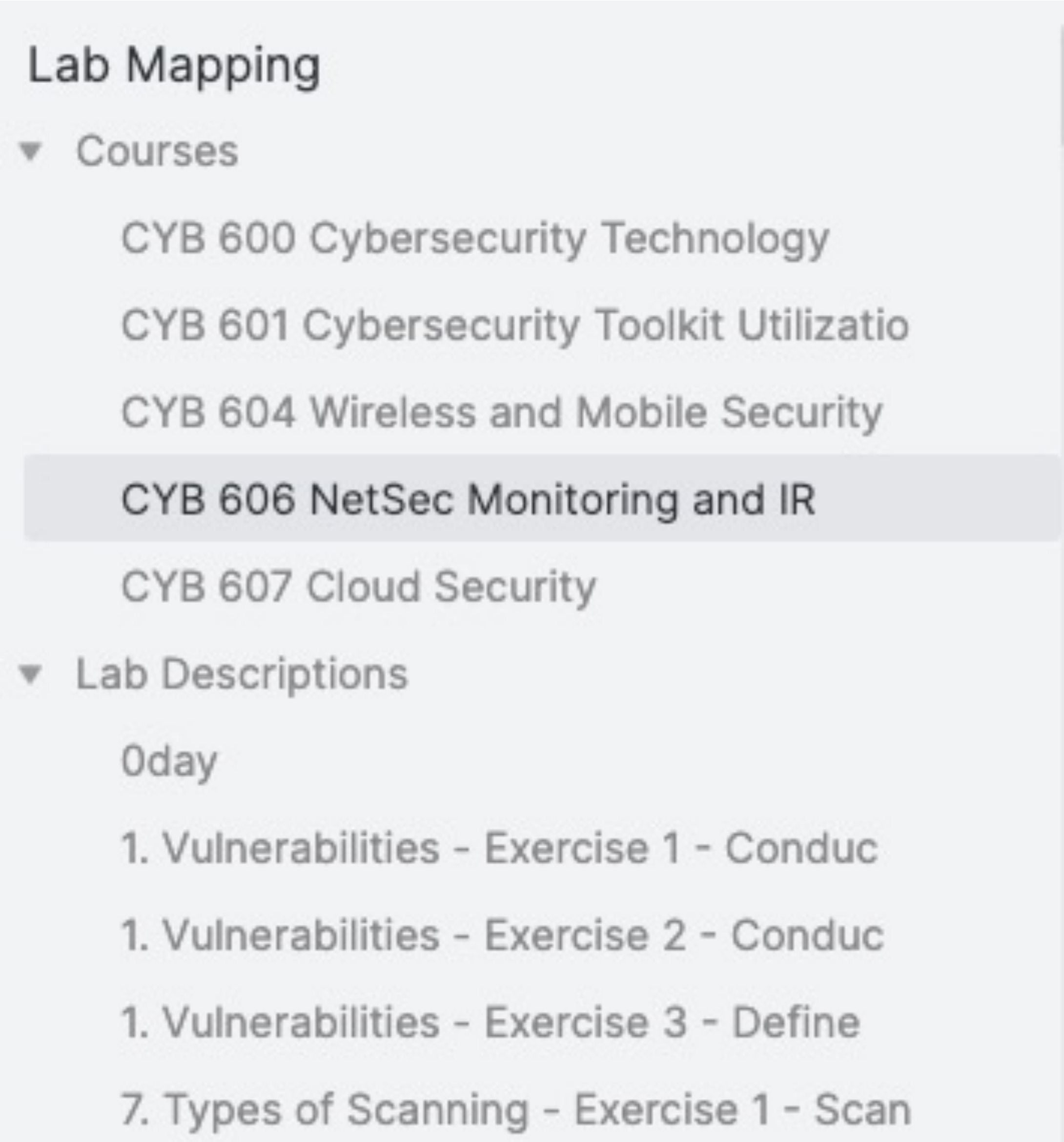
The Incident Response Process

Snort Rules: Ep.3 – HTTP

Intrusion Detection Systems

# Workflow

1. Build view in AirTable
2. Export view to CSV
3. Clean up columns
4. Run Python script that creates markdown files for each row
5. Copy to Obsidian



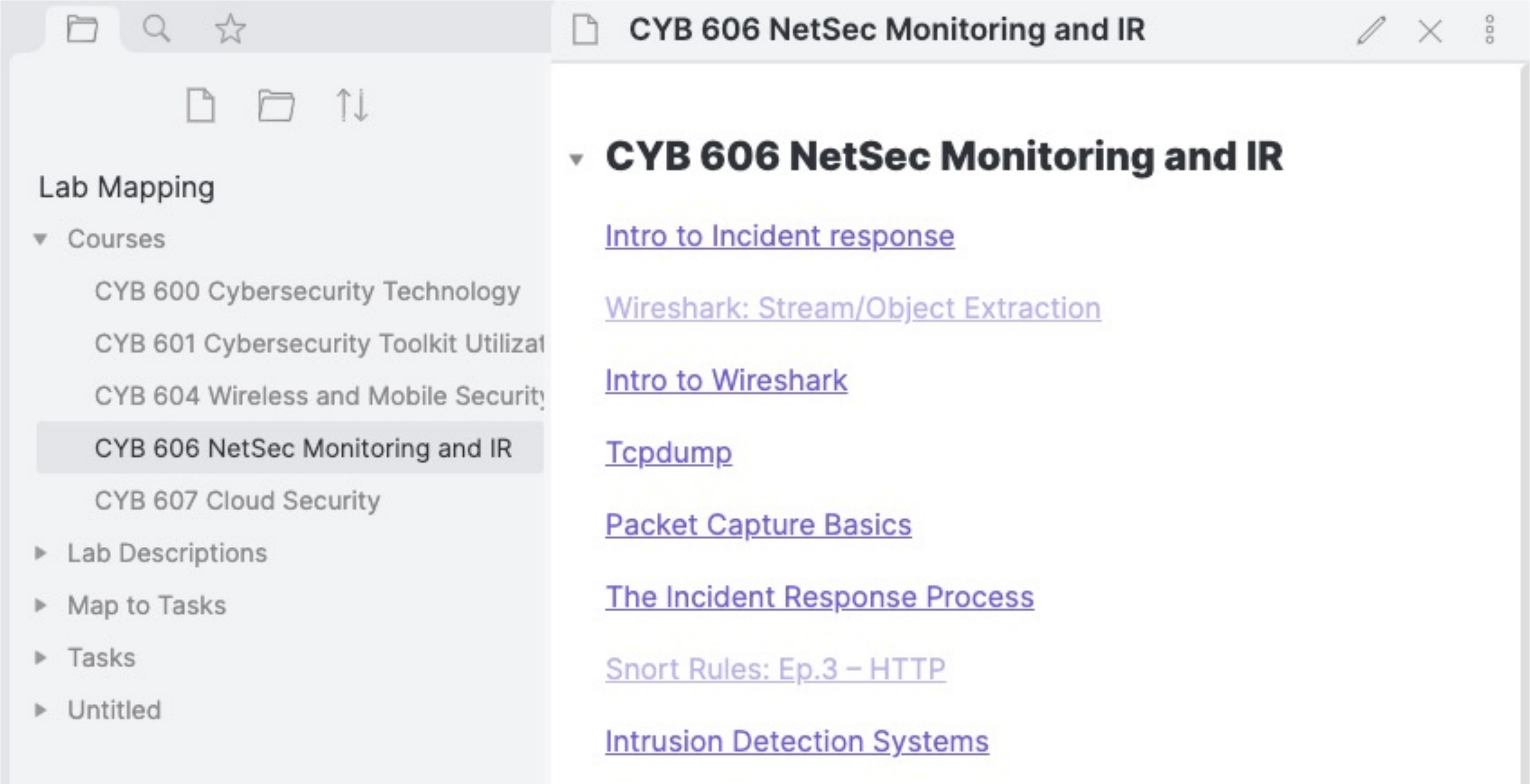
Lab Mapping

▼ Courses

- CYB 600 Cybersecurity Technology
- CYB 601 Cybersecurity Toolkit Utilizatio
- CYB 604 Wireless and Mobile Security
- CYB 606 NetSec Monitoring and IR
- CYB 607 Cloud Security

▼ Lab Descriptions

- 0day
- 1. Vulnerabilities - Exercise 1 - Conduc
- 1. Vulnerabilities - Exercise 2 - Conduc
- 1. Vulnerabilities - Exercise 3 - Define
- 7. Types of Scanning - Exercise 1 - Scan



Lab Mapping
Courses
CYB 600 Cybersecurity Technology
CYB 601 Cybersecurity Toolkit Utilizat
CYB 604 Wireless and Mobile Securit
CYB 606 NetSec Monitoring and IR
CYB 607 Cloud Security
Lab Descriptions
Map to Tasks
Tasks
Untitled

CYB 606 NetSec Monitoring and IR

CYB 606 NetSec Monitoring and IR

Intro to Incident response

Wireshark: Stream/Object Extraction

Intro to Wireshark

Tcpdump

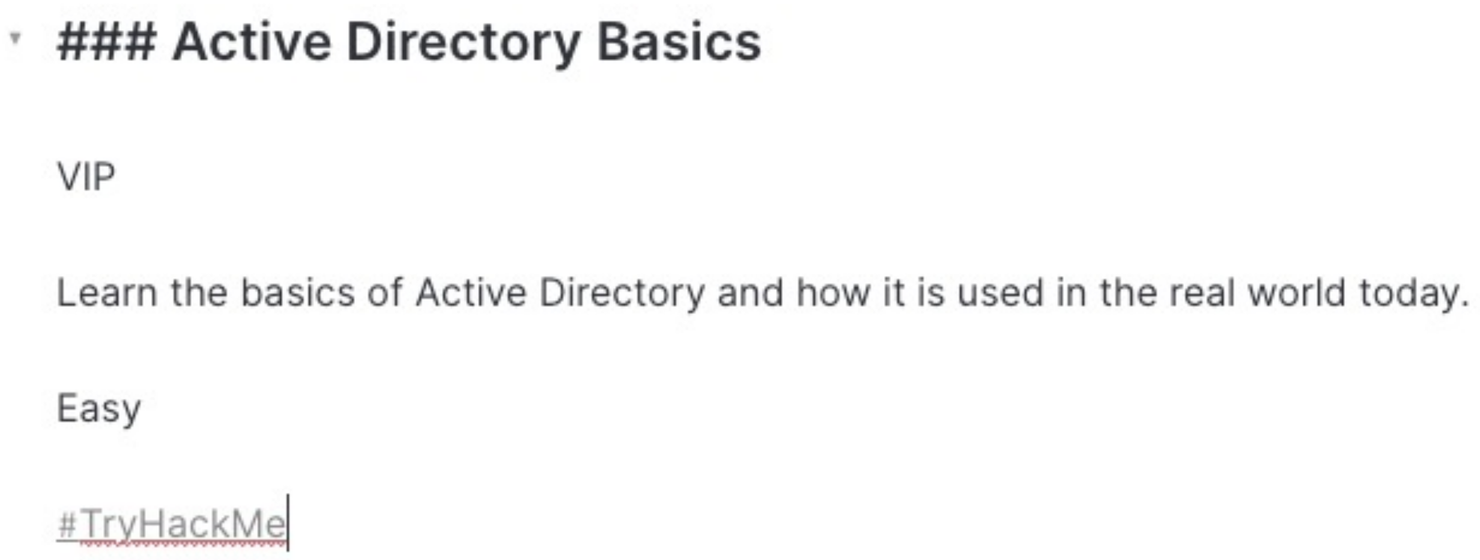
Packet Capture Basics

The Incident Response Process

Snort Rules: Ep.3 – HTTP

Intrusion Detection Systems

Course Page



### Active Directory Basics

VIP

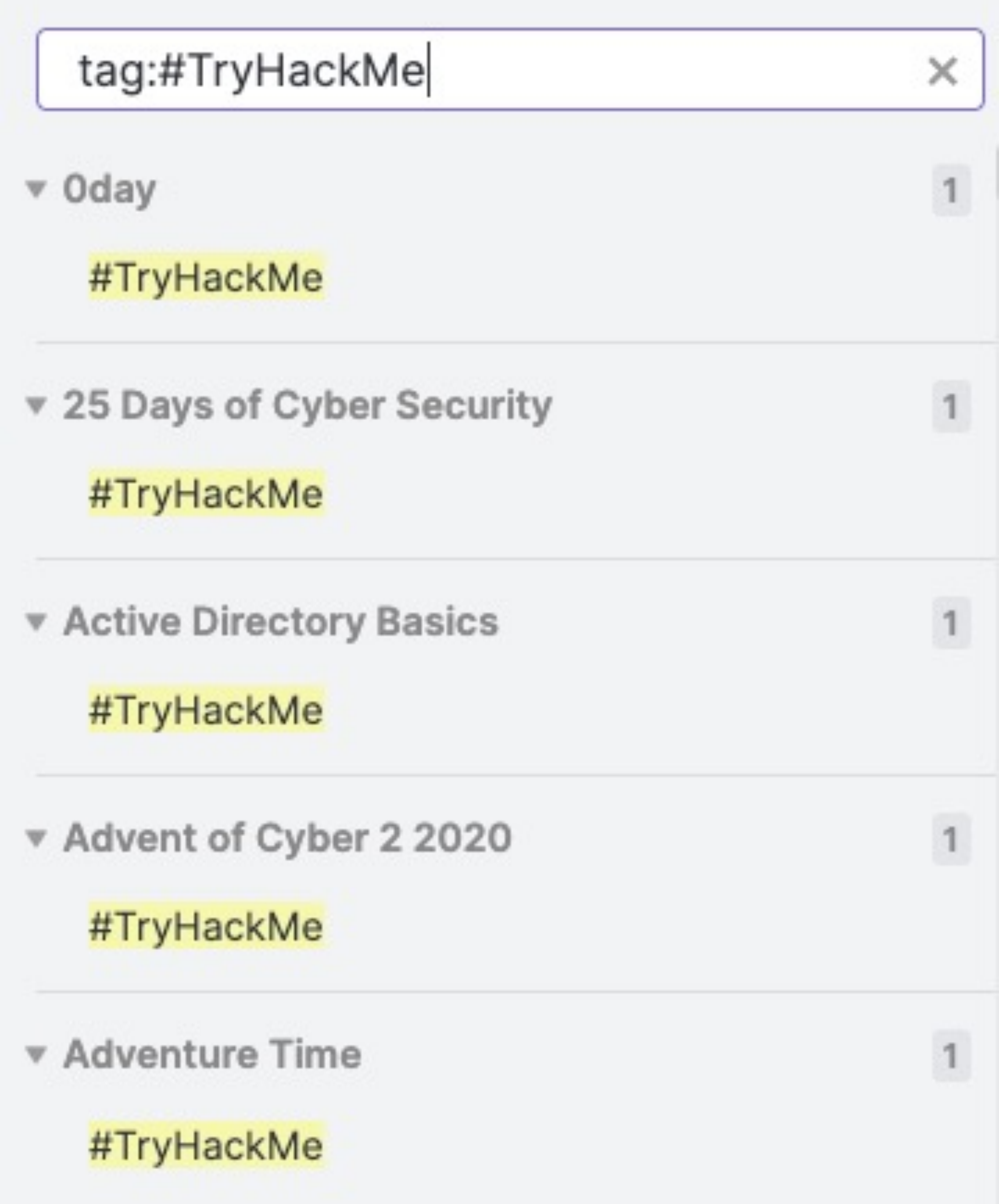
Learn the basics of Active Directory and how it is used in the real world today.

Easy

#TryHackMe

Lab Page

# Tags



tag:#TryHackMe

▾ 0day 1

#TryHackMe

▾ 25 Days of Cyber Security 1

#TryHackMe

▾ Active Directory Basics 1

#TryHackMe

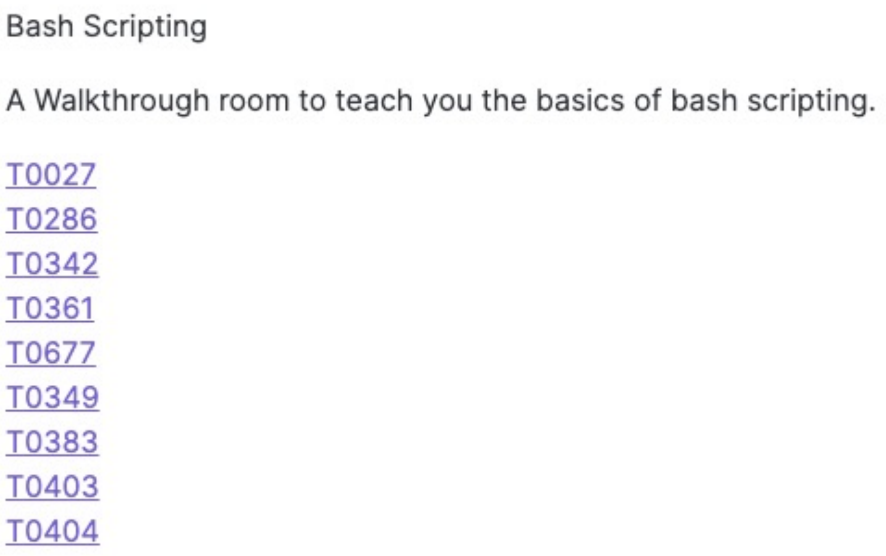
▾ Advent of Cyber 2 2020 1

#TryHackMe

▾ Adventure Time 1

#TryHackMe

# Labs to Tasks



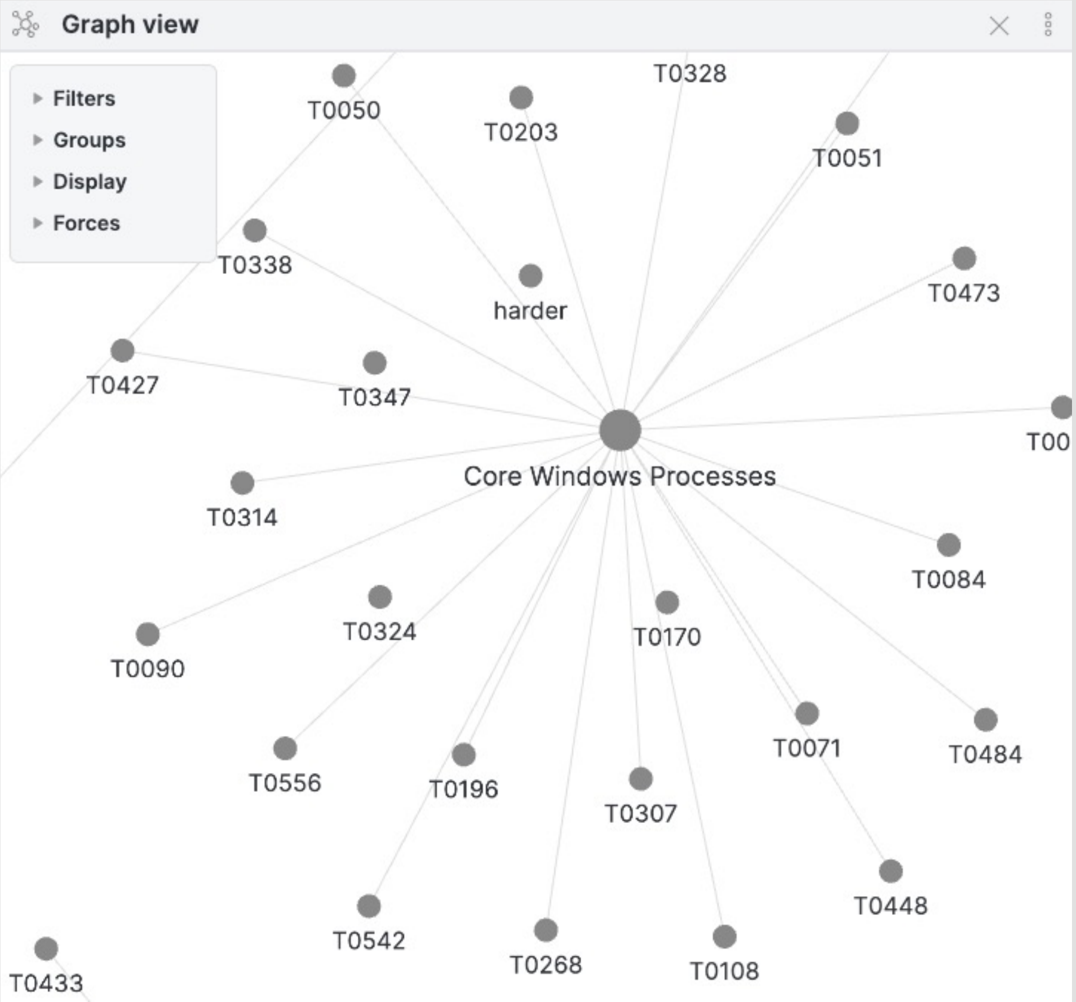
Bash Scripting

A Walkthrough room to teach you the basics of bash scripting.

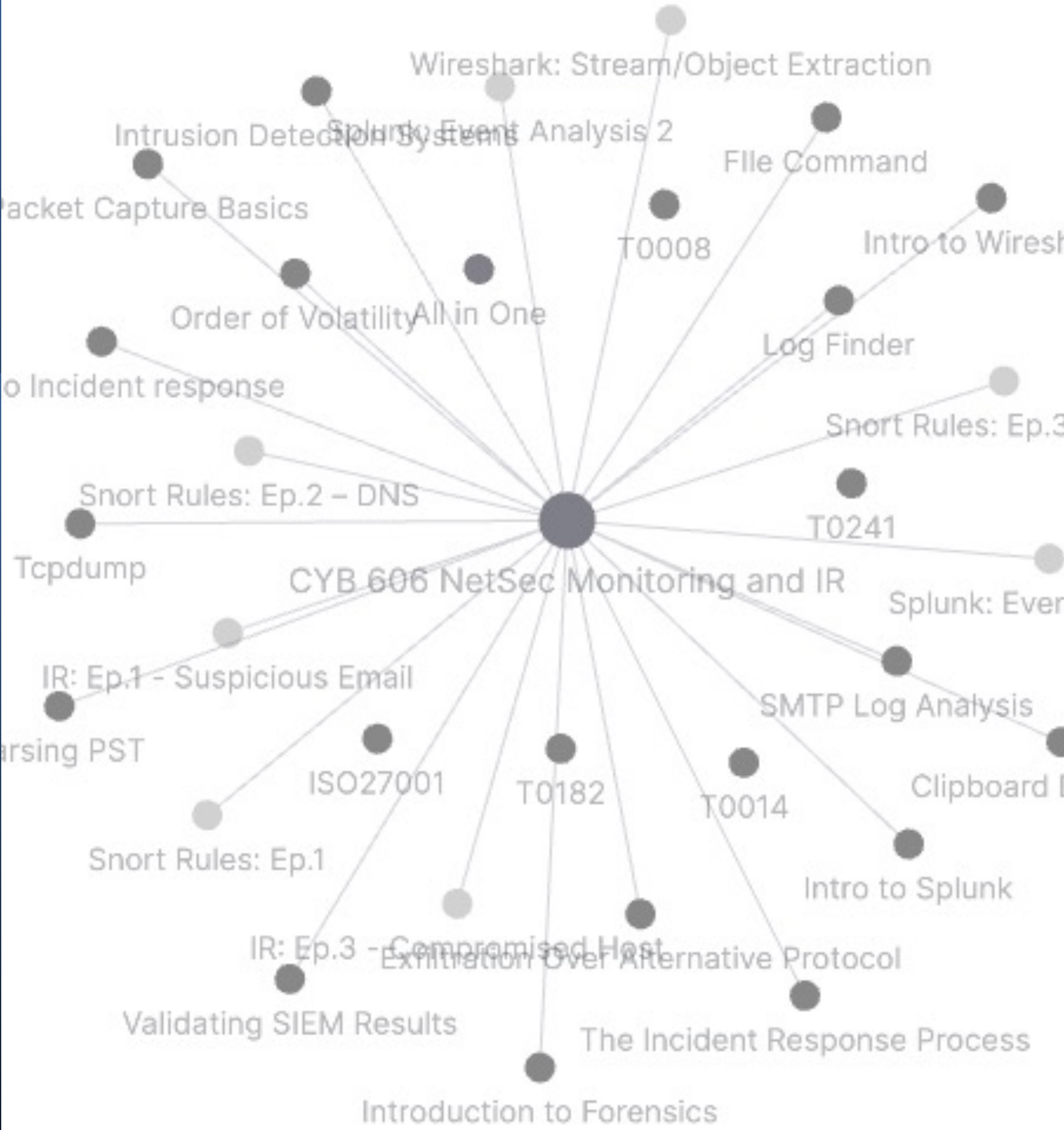
T0027
T0286
T0342
T0361
T0677
T0349
T0383
T0403
T0404

- Links go to tasks

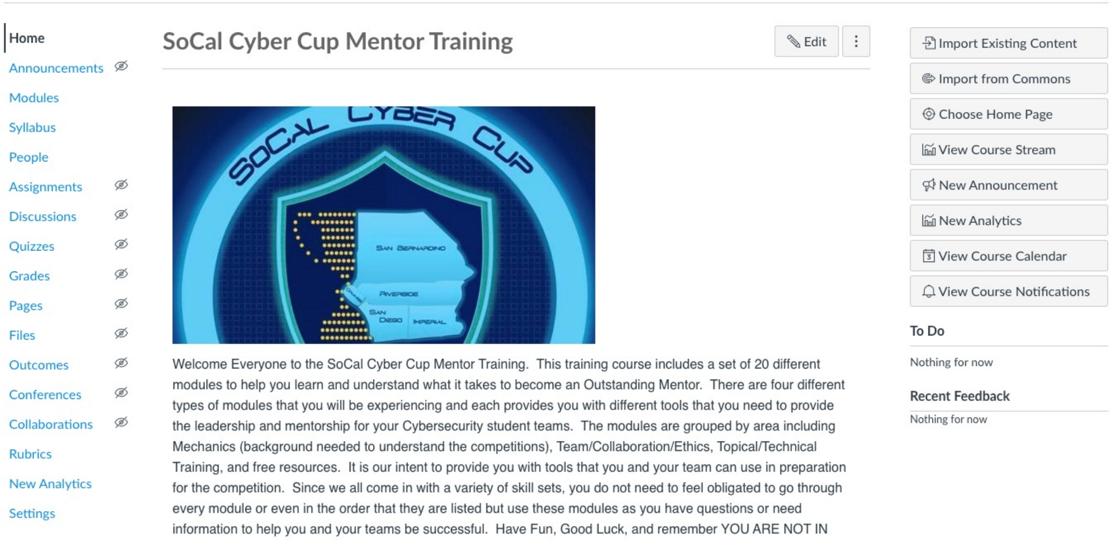
# Visualization



# Visualization



# Cyber Competition Coach and Mentor Training



## 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

# Questions?
# Volunteer to help?

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://obsidian.md/