

★ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



Web OSINT WriteUp-TryHackMe



DimigraS · [Follow](#)

9 min read · Aug 18, 2021



Listen



Share



More

Open Source Intelligence Gathering plays a vital role for security researchers, Ethical Hackers, Pentesters, Security Analysts, and of course Black Hat Hackers. OSINT helps in collecting and analyzing information from publically available resources for intelligence purposes.

To get an idea of what Open Source Intelligence Gathering looks like, we are going to walk through the TryHackMe room “[Web OSINT](#)”. This room targets gathering

information related to websites. So without further ado let's dive in.

(Task 1)-When A Website Does Not Exist

What's the first thing you do when you are given the name of a business to check out? Fire up the ol' web browser, find the website and check it out, right?

What if the website, or even the entire business, no longer exists?

That does NOT mean it's the end of the road.

OSINT researchers may still be able to connect the dots and find useful information on such organizations.

Your job is to find as much information as you can about the website RepublicofKoffee.com.

The website doesn't exist, and if it does by the time you read this, the website in its current form is not our target.

One way to collect information about a website without directly visiting it is to simply do a search for it.

Note: Sometimes plugging a website into the search bar will send you directly to the site. Avoid this by putting the site in quote marks. Also note that this will only return results where the full domain name is written out on the website.

Go ahead and google "RepublicOfKoffee.com" with and without quote marks, just to see what happens.

#1 Click To Complete

ANSWER: No answer needed

(Task 2)-Whois Registration

Just because nothing shows up when you visit 'RepublicOfKoffee.com,' doesn't mean that someone doesn't own the domain. In fact, if there is any kind of landing page at all, even a spammy one, then you can be sure that someone does, in fact, own it. But is it currently owned by the same person that used it for the time period we are interested in? We may or may not be able to figure that out, but it's worth a look.

We can confirm current registration status with a whois lookup.

A 'whois' lookup is the most basic form of domain recon available. There are multiple websites that will do it for you as well.

Personally, I recommend just going directly to lookup.icann.org. This should tell you the current hosting company used and name servers. Looking at the raw data option will show further details.

We're looking for any data we might be able to use as pivot points. Maybe an email address? Or better yet, a physical address or phone number?

Technically these are required in order to register any domain, but most domain registrars offer some kind of privacy protection for a trivial fee, if not free.

Anyway, let's see what we can find out!

Domain Information
Name: REPUBLICOFKOFFEE.COM
Registry Domain ID: 2582024072_DOMAIN_COM-VRSN
Domain Status: clientTransferProhibited
Nameservers: DNS1.REGISTRAR-SERVERS.COM DNS2.REGISTRAR-SERVERS.COM
Dates
Registry Expiration: 2022-01-01 17:33:07 UTC
Created: 2021-01-01 17:33:07 UTC

Registrar Information
Name: NAMECHEAP INC

#1 What is the name of the company the domain was registered with?

ANSWER: Namecheap Inc

#2 What phone number is listed for the registration company? (do not include country code or special characters/spaces)

ANSWER: 6613102107

#3 What is the first nameserver listed for the site?

ANSWER: DNS1.REGISTRAR-SERVERS.COM

#4 What is listed for the name of the registrant?

ANSWER: redacted for privacy

#5 What country is listed for the registrant?

ANSWER: Panama

(Task 3)-Ghosts of Websites Past

Don't be discouraged when your initial searches on a website turn up empty.

That's where Archive.org and the Internet Wayback Machine come into play.

Do yourself a favor and install the archive.org browser extension that will automatically pull up an option to search for a site on the Wayback Machine when it fails to load in the web browser.

Either with the browser extension, or just by going to archive.org and searching for it, see what snapshots are available of our target domain, RepublicOfKoffee.com.

Looking at the historical information available for the site, you should be able to answer the following questions without too much trouble.

#1 What is the first name of the blog's author?

ANSWER: Steve

#2 What city and country was the author writing from?

ANSWER: Gwangju, south korea

#3 [Research] What is the name (in English) of the temple inside the National Park the author frequently visits?

ANSWER: Gwangju, South Korea

(Task 4)-Digging into DNS

So far we've gathered some good info about the content that was on our target website, even though it hasn't been live for several years.

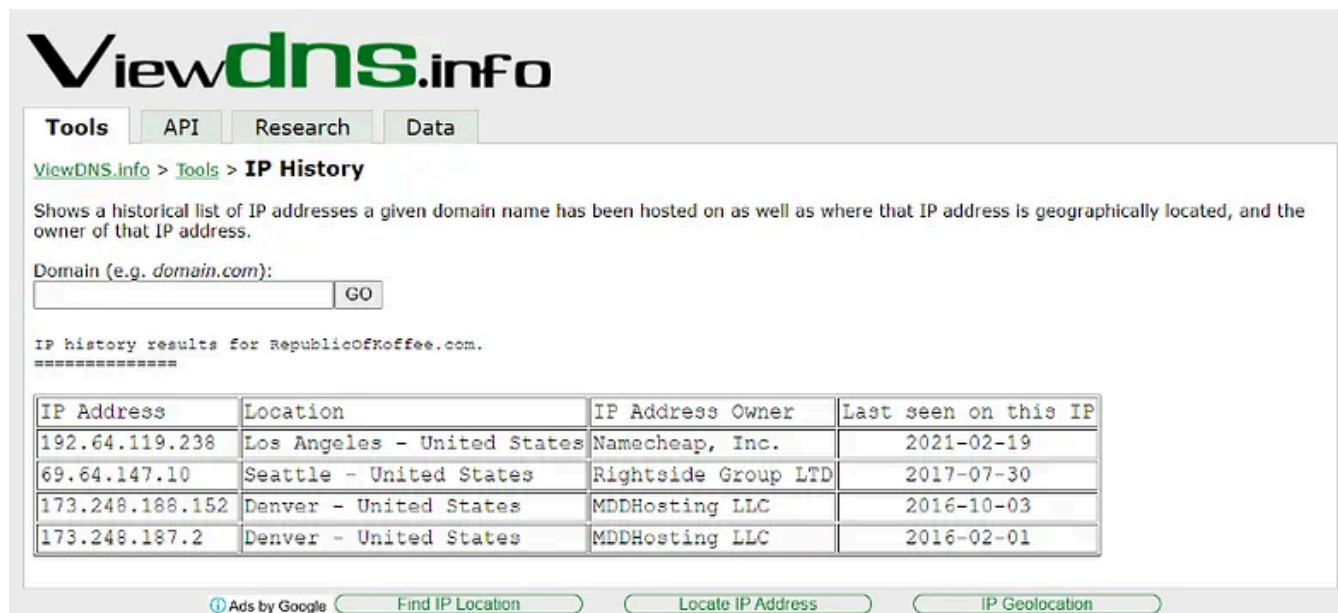
But what about technical details?

That's where ViewDNS.info comes in.

ViewDNS.info provides a convenient UI for looking up registration information on a target website. Using this information, it may be possible to draw certain conclusions that are not clearly spelled out, such as whether the website is hosted

on a shared or dedicated IP address. The answer to this question can imply things about the website's budget as well as traffic.

Take a look at the search options available and see if you can answer these questions.



The screenshot shows the ViewDNS.info website interface. At the top is the logo 'ViewDNS.info'. Below it are navigation tabs: 'Tools' (selected), 'API', 'Research', and 'Data'. The main heading is 'ViewDNS.info > Tools > IP History'. A description states: 'Shows a historical list of IP addresses a given domain name has been hosted on as well as where that IP address is geographically located, and the owner of that IP address.' There is a search input field labeled 'Domain (e.g. domain.com):' with a 'GO' button. Below this, it says 'IP history results for RepublicOfKoffee.com.' followed by a table of results.

IP Address	Location	IP Address Owner	Last seen on this IP
192.64.119.238	Los Angeles - United States	Namecheap, Inc.	2021-02-19
69.64.147.10	Seattle - United States	Rightside Group LTD	2017-07-30
173.248.188.152	Denver - United States	MDDHosting LLC	2016-10-03
173.248.187.2	Denver - United States	MDDHosting LLC	2016-02-01

At the bottom of the page, there are four buttons: 'Ads by Google', 'Find IP Location', 'Locate IP Address', and 'IP Geolocation'.

#1 What was RepublicOfKoffee.com's IP address as of October 2016?

ANSWER: 173.248.188.152

#2 Based on the other domains hosted on the same IP address, what kind of hosting service can we safely assume our target uses?

ANSWER: Shared

#3 How many times has the IP address changed in the history of the domain?

ANSWER: 4

(Task 5)-Taking Off The Training Wheels

Congratulations on making it this far.

You'll need all of the skills you've learned so far for this task.

All I have for you, is a domain: **heat.net**

The screenshot shows the ICANN Lookup website interface. At the top, there's a navigation bar with links like WHOIS, POLICIES, INVOLVED, COMPLAINTS, and CENTER. The main heading is "Domain Name Registration Data Lookup". Below this, there's a search bar where "heat.net" has been entered. To the right of the search bar is a "Lookup" button. Below the search bar, there's a disclaimer: "By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN Privacy Policy, and agree to abide by the website Terms of Service and the Domain Name Registration Data Lookup Terms of Use." Below the disclaimer is a section titled "Domain Information" with a dark blue header. This section contains the following details: Name: HEAT.NET, Registry Domain ID: 4878759_DOMAIN_NET-VRSN, Domain Status: clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited, Nameservers: NS1.HEAT.NET and NS2.HEAT.NET (the latter is highlighted with a red box), and Dates.

lookup.icann.org/lookup

WHOIS POLICIES INVOLVED COMPLAINTS CENTER

Domain Name Registration Data Lookup

Enter a domain name [Frequently Asked Questions \(FAQ\)](#)

heat.net Lookup

By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN [Privacy Policy](#), and agree to abide by the website [Terms of Service](#) and the [Domain Name Registration Data Lookup Terms of Use](#).

Domain Information

Name: HEAT.NET

Registry Domain ID: 4878759_DOMAIN_NET-VRSN

Domain Status:
[clientDeleteProhibited](#)
[clientRenewProhibited](#)
[clientTransferProhibited](#)
[clientUpdateProhibited](#)

Nameservers:
NS1.HEAT.NET
NS2.HEAT.NET

Dates

#1 What is the second nameserver listed for the domain?

ANSWER: NS2.HEAT.NET

#2 What IP address was the domain listed on as of December 2011?

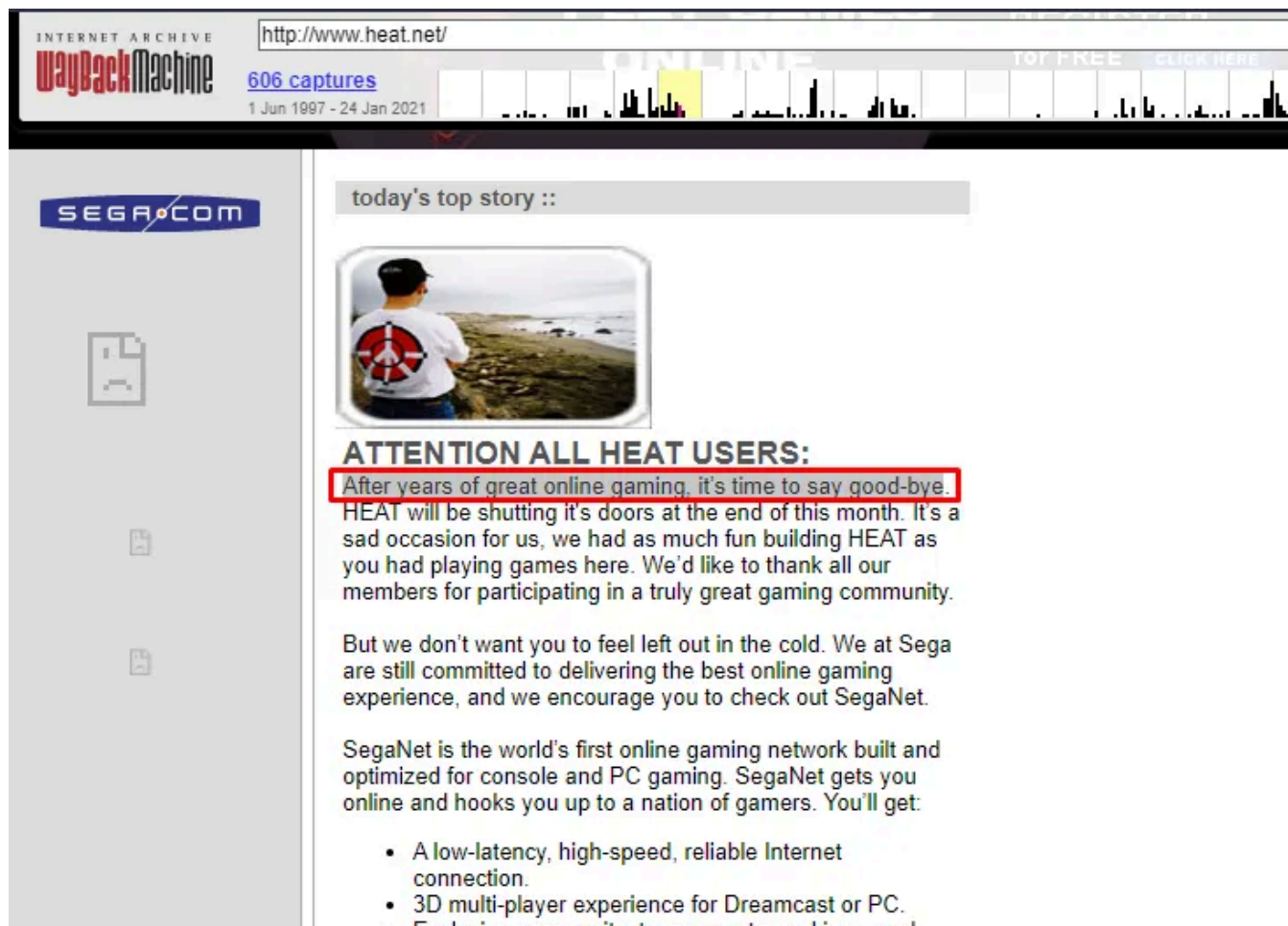
ANSWER: 72.52.192.240

#3 Based on domains that share the same IP, what kind of hosting service is the domain owner using?

ANSWER: shared

#4 On what date did was the site first captured by the internet archive? (MM/DD/YY format)

ANSWER: 06/01/97



#5 What is the first sentence of the first body paragraph from the final capture of 2001?

ANSWER: After years of great online gaming, it's time to say good-bye.

#6 sing your search engine skills, what was the name of the company that was responsible for the original version of the site?

ANSWER: SegaSoft

#7 hat does the first header on the site on the last capture of 2010 say?

ANSWER: Heat.net — Heating and Cooling

(Task 6)-Taking A Peek Under The Hood Of A Website

Isn't it kind of interesting how the website disappeared for a period of time and came back?

Clearly the purpose of the site is different now. Let's roll up our sleeves and figure out what's going on.

First, do you have any gut feelings about this site? What is your overall impression? Does it *feel* like a legitimate source of information?

Why?

You might consider some of the following points:

- Language — What grade level is the writing? Does it seem to be written by a native English speaker?
- UX — Is it user friendly? Is the design modern?
- What pages does the site have?

I can tell you that this website conforms well to antiquated search engine optimization (SEO) best practices. You can read more about [SEO best practices on ahrefs](#) if you like before you continue.

Technical Research

Often, clues about a website and its creator/owner may be unintentionally left behind in the source code of the website. Pretty much every web browser will have a method of doing this. It is well worth taking the time to become acquainted with how this works in your browser of choice. For Chrome on MacOS, you'll go to the top menu bar and choose View > Developer > View Source.

Note: This also works on sites you visit within Archive.org's Wayback Machine.

Once the source code of the page loads, it's time to look around. You don't have to understand HTML, CSS, or Javascript to read notes that the developers left behind for themselves. In HTML, comments begin with the characters `<!--` . Here's an example of what a forgotten comment might look like in practice:

```
<!--Don't forget to email Bob Loblaw when the site goes live at bob@fakeemail.com-->
```

As easy as that may be to read, if it was buried inside a gigantic page full of code it could still be easy to miss.

Technical Research

Often, clues about a website and its creator/owner may be unintentionally left behind in the source code of the website. Pretty much every web browser will have a method of doing this. It is well worth taking the time to become acquainted with

how this works in your browser of choice. For Chrome on MacOS, you'll go to the top menu bar and choose View > Developer > View Source.

Note: This also works on sites you visit within Archive.org's Wayback Machine.

Once the source code of the page loads, it's time to look around. You don't have to understand HTML, CSS, or Javascript to read notes that the developers left behind for themselves. In HTML, comments begin with the characters `<!--`. Here's an example of what a forgotten comment might look like in practice:

```
<!--Don't forget to email Bob Loblaw when the site goes live at bob@fakeemail.com-->
```

← How Do Heating and Cooling Systems Work? Save Money on Your Commercial Heating Bill →

Need to Hire a Commercial Heating Contractor?

Posted on December 21, 2010 by admin

Even though this might seem like yet another daunting task in a long list, it really is not that difficult to find the perfect person who will help you with your **commercial heating** needs. Just as with any other contractor for any other important job, you need to follow a few basic steps to make sure you don't get taken advantage of or wasting unnecessary time and money.

So here are a few simple steps to take to make this process easier:

1. Always do your homework: It seems we are never really done with school and certainly we are never done with homework. To find a good [heating contractor](#) for your business, you should see who regulates that industry in your area and then ensure that whoever you find is registered and has the proper licensing. If you have an existing system, ensure you know all the information about your commercial [heating system](#) before you start to call around. You want to make sure that whoever you hire is familiar with your type of system. Hopefully you, or the previous owner if there is one, has kept records of previous repairs on maintenance. Usually when someone has repaired a [heating and cooling](#) unit, they affix a sticker on the unit – that's a good place to start.
2. Always ask for referrals: Any reputable contractor will be happy to supply you with references of other satisfied customers. If they don't want to supply that sort of information, that should be the first red flag and you might question hiring that company or not
3. Always check in with references: It's one thing to get the list of references from the contractor, [but you should actually do the calling](#). Ensure that you ask them specific questions such as

www.heat.net/39/save-money-on-your-commercial-heating-bill/

#1 How many internal links are in the text of the article?

ANSWER: 5

#2 Website in the article's only external link (that isn't an ad)

ANSWER: 1

#3 Website in the article's only external link (that isn't an ad)

ANSWER: purchase.org

#4 Try to find the Google Analytics code linked to the site

ANSWER: A-251372-24

#5 Is the Google Analytics code in use on another website? Yay or nay

ANSWER: NAY

#6 Does the link to this website have any obvious affiliate codes

ANSWER: NAY

(Task 7)-Final Exam: Connect the Dots

Experienced OSINT researchers will tell you that chasing rabbit holes all day and night without being able to make some solid connections is not OSINT.

OSINT refers to the patterns that start to emerge as we connect the dots in the analysis of the data.

Congrats! you found that our target, heat[.]net, links to an interesting external site. A question remains though: *Why???*

There is no affiliate code in the link, so there is no obvious financial connection between the two. Maybe there's another kind of connection.

This is your final exam, and there is exactly one question.

Get busy!

[ViewDNS.info](#) > [Tools](#) > **IP History**

Shows a historical list of IP addresses a given domain name has been hosted on as well as where that IP address is geographically located, and the owner of that IP address.

Domain (e.g. domain.com):

GO

IP history results for purchase.org.

=====

IP Address	Location	IP Address Owner	Last seen on this IP
172.67.197.177	United States	Cloudflare, Inc.	2021-02-23
104.21.92.201	United States	Cloudflare, Inc.	2021-02-23
104.27.185.115	United States	Cloudflare, Inc.	2021-01-14
104.27.184.115	United States	Cloudflare, Inc.	2021-01-14
206.196.110.108	St Louis - United States	Rose Web Services LLC	2017-11-03
67.43.1.187	Lansing - United States	Liquid Web, L.L.C	2013-04-19
72.52.193.127	Lansing - United States	Liquid Web. L.L.C	2012-11-16

#1 Use the tools in Task 4 to confirm the link between the two sites. Try hard to figure it out without the hint

ANSWER: Liquid Web, L.L.C

(Task 8)-Debriefing

Click to complete

No Answer needed.

(Task 9)-Wrap-up

A little web OSINT knowledge can go a long way in online investigations. A few examples of where it comes into play include any kind of business OSINT, online scams, or even political journalism. If you would like to see a prime example of this kind of research being put into practice, I highly recommend checking out NixIntel's expose [linking antifa.com to Russia](#), which is an amazing case study.

Make sure to check out the other OSINT boxes out there such as:

- The [Searchlight IMINT Room](#) and [Geolocation](#) for Geolocation and Image Analysis
- The [Google Dork](#) room for advanced search engine operators
- The [OhSINT](#) room for a little extra IMINT practice

There are also two fantastic podcasts that every OSINT practitioner should regularly listen to. The [OSINT Curious](#) podcast and [The Privacy, Security, & OSINT Show](#).

Finally, a solid paid option for OSINT training that won't break the bank is [TheOSINTion](#). If you enjoyed the content of this room you would LOVE the [Business OSINT](#) course they offer. I have no affiliation with the course other than being a satisfied customer.

Thanks for reading.

Tryhackme

Web

Osint



Follow

Written by DimigraS

35 Followers · 2 Following

Cyber security

No responses yet



What are your thoughts?

Respond

More from DimigraS



 DimigraS

Pentesting Fundamentals-TryHackMe

Learn the important ethics and methodologies behind every pentest the room Pentesting Fundamentals of Tryhackme let's get started.

Sep 9, 2021



4



DimigraS

TryHackMe—Security Engineer Path

What is security engineering?

Feb 12, 2024



DimigraS

Hack the Box: Illumination

A quick snack from hack the box let's get the challenge.

May 20, 2023



 DimigraS

Encryption- Crypto 101 WriteUp—TryHackMe

I tried to prepare a write-up for the “Encryption—Crypto 101” room on tryhackme.

Jul 31, 2021  50



See all from DimigraS

Recommended from Medium

Open in app 

Medium



Search





In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations



Nov 5, 2024



60



In System Weakness by Sunny Singh Verma [SuNnY]

Silver Platter TryHackMe Motion Graphics Writeup | Beginner Friendly | Detailed Walkthrough |...

A Detailed motion Graphics writeup for TryHackMe room Silver Platter

★ Jan 13 🖱 50



Lists



Staff picks

804 stories · 1587 saves



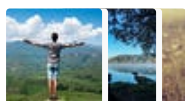
Stories to Help You Level-Up at Work

19 stories · 925 saves



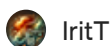
Self-Improvement 101

20 stories · 3244 saves



Productivity 101

20 stories · 2740 saves



IritT

CyberChef: The Basics — Crypto 101 — Defensive Security Tooling- Cryptography-TryHackMe Walkthrough

This room is an introduction to CyberChef, the Swiss Army knife for cyber security professionals.

Nov 2, 2024



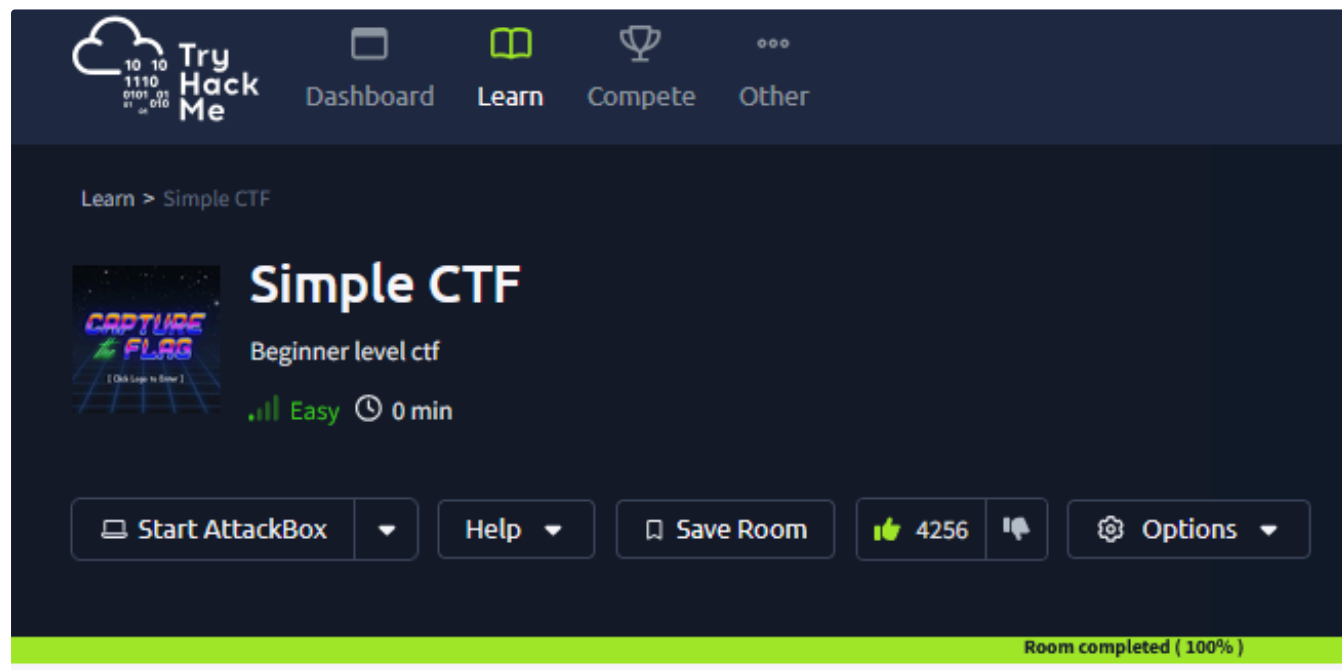


Berat Arslan

TryHackMe - U.A. High School Writeup

“U.A. High School” CTF named is one of the “easy” rooms in THM.

Aug 25, 2024 🖱 87



In InfoSec Write-ups by Momal Naz


TryHackMe | Simple CTF | Walkthrough | By HexaHunter

Step-by-step guide to solving the Simple CTF room for beginners.

Sep 9, 2024 🖱 5





 Atharva

TryHackMe—Whiterose Writeup

Complete step-by-step writeup for TryHackMe challenge room Whiterose!

Nov 12, 2024  16



See more recommendations