

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



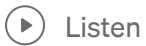
TryHackMe: WebOSINT



JJ's Blog · [Follow](#)

Published in Nerd For Tech

6 min read · Feb 24, 2021



... More

Conducting basic open source intelligence research on a website

You can access the room through this link: <https://tryhackme.com/room/webosint>



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.

<Spoiler alert> 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

No Answers needed

Task 2 : Whois Registration

Whois Site,

1) lookup.icann.org.

2) Whois Data

This should tell you the current hosting company used and name servers. Looking at the raw data option will show further details.

lookup.icann.org/lookup

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

RepublicOfKoffee.com

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: 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

DNSSEC Information

1. What is the name of the company the domain was registered with?
Ans : Namecheap Inc
2. What phone number is listed for the registration company? (do not include country code or special characters/spaces)
Ans : 6613102107
3. What is the first nameserver listed for the site?
Ans : DNS1.REGISTRAR-SERVERS.COM
4. What is listed for the name of the registrant?
Ans : redacted for privacy
5. What country is listed for the registrant?
Ans : Panama

Task 3 : Ghosts of Websites Past

1. What is the first name of the blog's author?
Ans : Steve

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

Ans : Gwangju,south korea

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

Ans : Gwangju, South Korea

Open in app ↗

Medium

Search



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.

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

Ans : 173.248.188.152

ViewDNS.info

Tools API Research Data

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 RepublicOfKoffee.com.

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

Ads by Google Find IP Location Locate IP Address IP Geolocation

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

Ans : Shared

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

Ans : 4



The screenshot shows the ViewDNS.info website interface. The 'Tools' tab is selected, and the 'IP History' section is active. It displays a table of historical IP addresses for the domain RepublicOfKoffee.com. The table has four columns: IP Address, Location, IP Address Owner, and Last seen on this IP. There are four entries in the table, showing a progression from 2016 to 2021. Below the table, there are buttons for 'Find IP Location', 'Locate IP Address', and 'IP Geolocation'.

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

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**

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

Ans : NS2.HEAT.NET

lookup.icann.org/lookup

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

Name servers of heat.net

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

Ans : 72.52.192.240

Tools API Research Data

[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 heat.net.

IP Address	Location	IP Address Owner	Last seen on this IP
208.117.87.195	Reston - United States	Atlantic.Net - Ashburn, VA	2021-02-20
74.116.2.147	United States	Express Web Systems, Inc.	2019-06-19
72.52.192.240	Lansing - United States	Liquid Web, L.L.C	2011-12-19

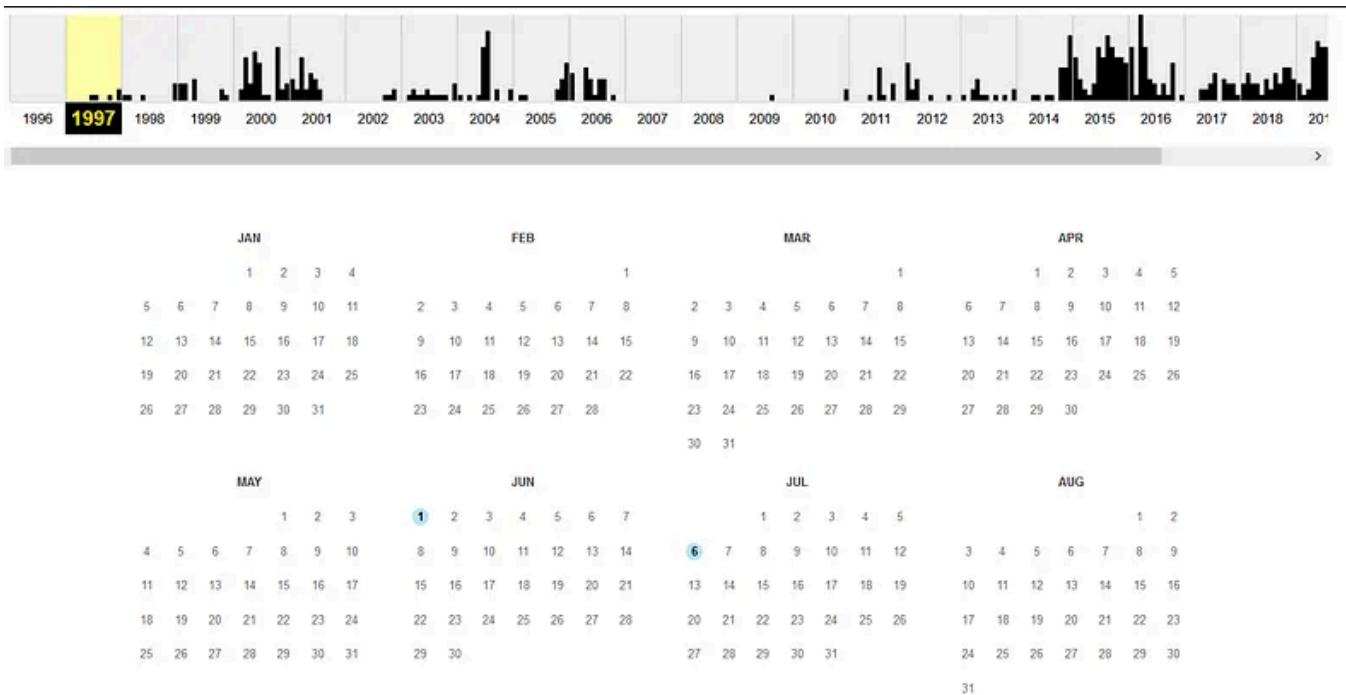
IP History

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

Ans : shared

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

Ans : 06/01/97



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

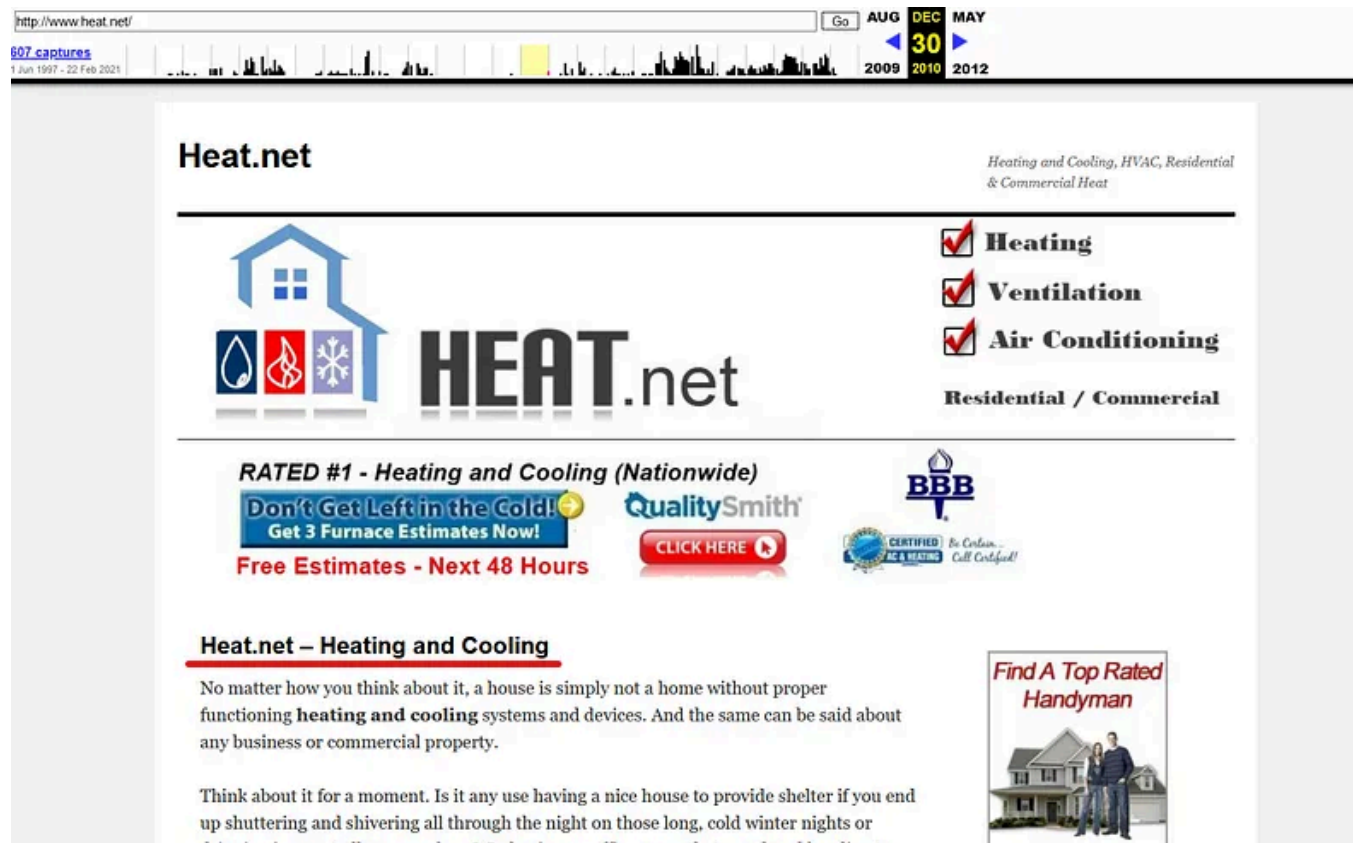
Ans : After years of great online gaming, it's time to say good-bye.

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

Ans : SegaSoft

7. What does the first header on the site on the last capture of 2010 say?

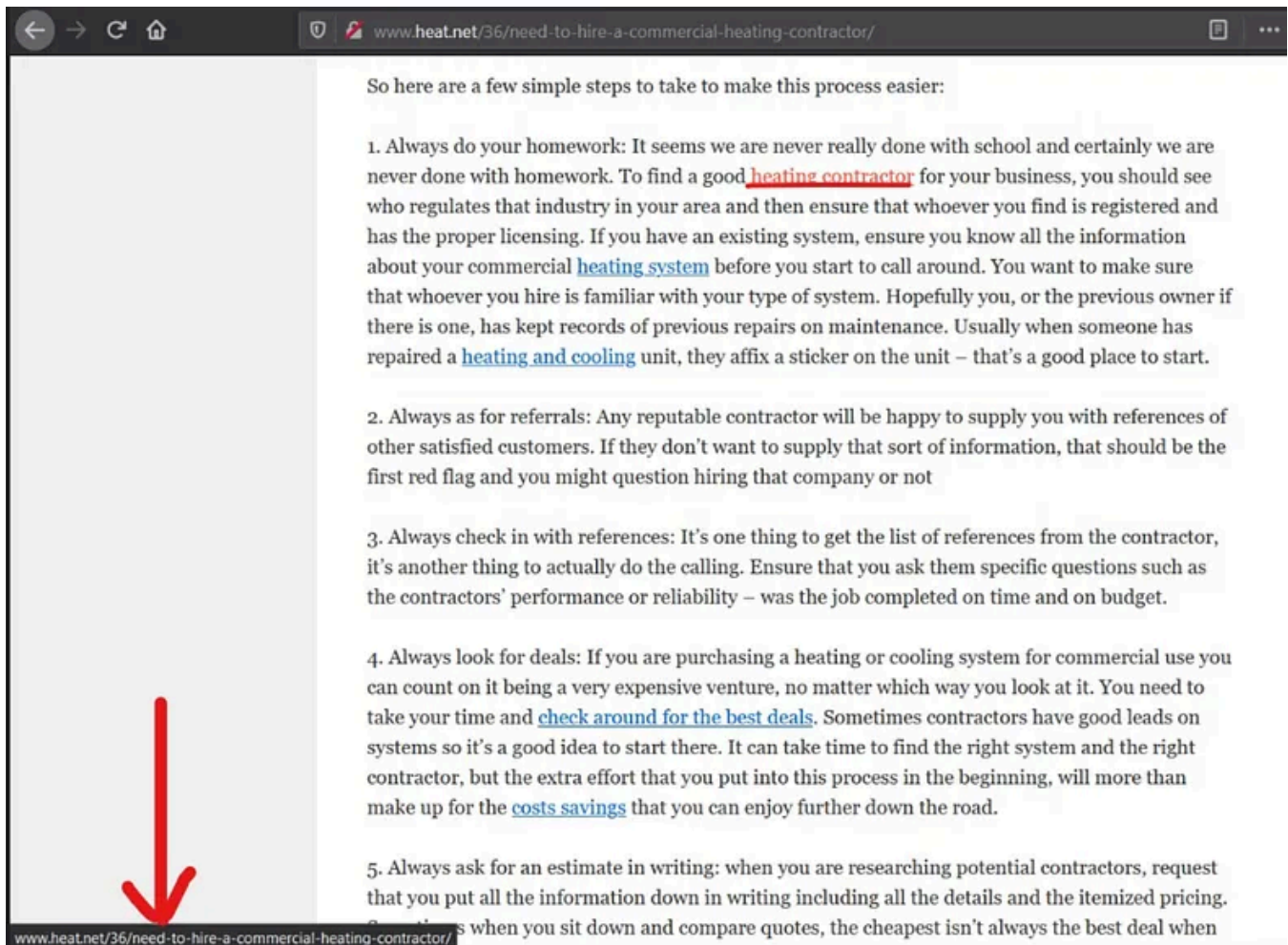
Ans : Heat.net — Heating and Cooling



Task 6 : Taking A Peek Under The Hood Of A Website

Go to this site : <http://www.heat.net/36/need-to-hire-a-commercial-heating-contractor/>

Point out the cursor on the links. it'll tell you site is belong from this domain or else.



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

Ans : 5

2. How many external links are in the text of the article?

Ans : 1

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

Ans : [purchase.org](#)

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

Goto [URL](#) -> Page Source -> Find -> Analytics

Ans : UA-251372-24

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

Ans : nay

6. Does the link to this website have any obvious affiliate codes embedded with it?

Yay or Nay

Ans : nay

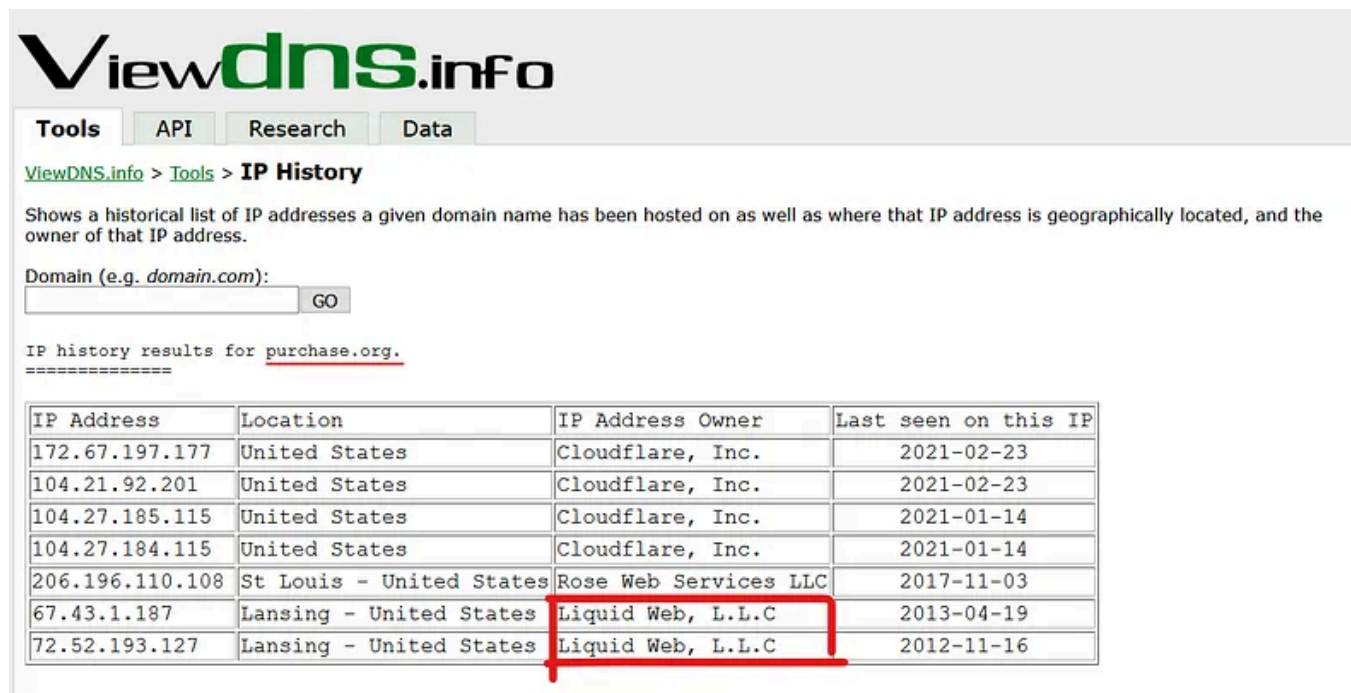
Task 7 : Final Exam: Connect the Dots

In this task, we need to find a connection between our target site i.e. heat.net and the external link.

The external link that we find is purchase.org

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

Ans : Liquid Web, L.L.C



ViewDNS.info

Tools API Research Data

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

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 ... 😊😊

@WebOSINT TryHackMe @osint



Follow

Published in Nerd For Tech

11.6K Followers · Last published 1 day ago

NFT is an Educational Media House. Our mission is to bring the invaluable knowledge and experiences of experts from all over the world to the novice. To know more about us, visit <https://www.nerdfortech.org/>.



Follow

Written by JJ's Blog

223 Followers · 86 Following

Intel | Research | Darkweb | Mystery | Infosec

No responses yet



What are your thoughts?

Respond

More from JJ's Blog and Nerd For Tech



In Nerd For Tech by JJ's Blog

Mysterious Side of the Internet

Deep—Deeper—Deepest !

May 13, 2021



571



3





In Nerd For Tech by Saravanan M

Don't use div—Have Some Empathy

How mindlessly using <div> can make some life harder.



Sep 28, 2024



212



9



In Nerd For Tech by Dick Dowdell

The Problem with Microservices

How to keep a really good idea from going badly wrong

Dec 1, 2024



175



3





In InfoSec Write-ups by JJ's Blog

Maveris OSINT CTF 2024 Writeup

OSINT CTF

Aug 26, 2024 🖱 11



See all from JJ's Blog

See all from Nerd For Tech

Recommended from Medium



 In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp


Discover the impact of training on teams and organisations

★ Nov 5, 2024 🖱 60



Day 11
Answers

cyberw1ng.medium.com

 In System Weakness by Karthikeyan Nagaraj

Advent of Cyber 2024 [Day 11] Writeup with Answers | TryHackMe Walkthrough

If you'd like to WPA, press the star key!

★ Dec 11, 2024 🖱 855 💬 1



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



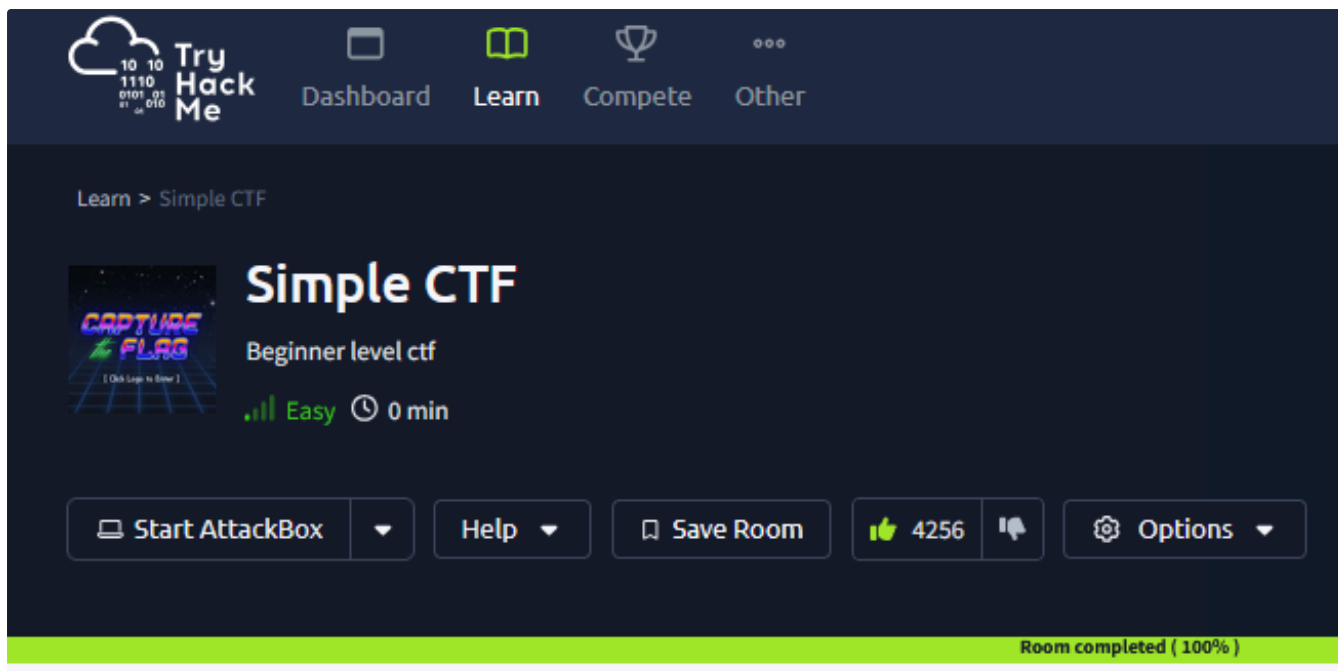
IritT

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





 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



 Jasper Alblas


TryHackMe: Cyborg - Walkthrough

Hi! It's been a while, but I am back!

Oct 14, 2024  2  1





 Atharva

TryHackMe—Whiterose Writeup

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

Nov 12, 2024  16



See more recommendations