SANS 2022 Holiday Hack Challenge Write-up

Bonus

1/3/23

Author:

Jim Kirn

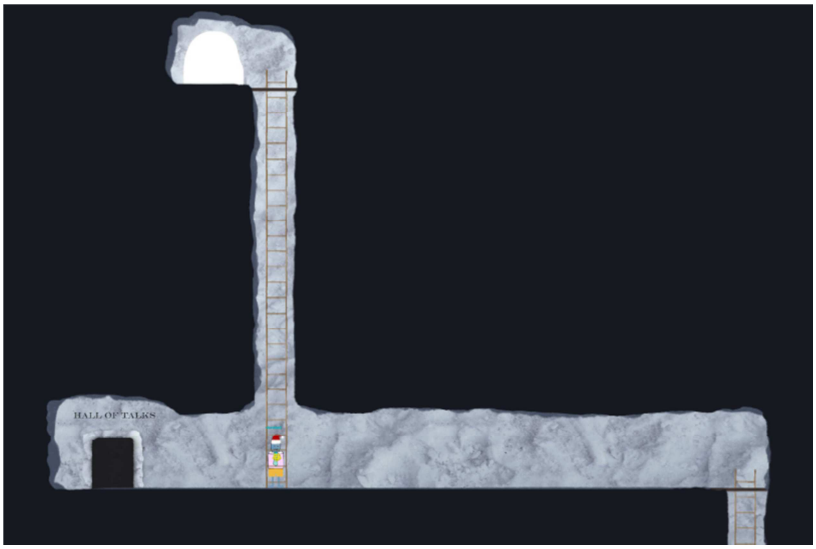
(**mrrobot**) in game, @infosecjim in Discord, @JimKirn on Twitter

Bonus Material

Several areas were not put into the SANS Writeup submission due to too much information. Although these items were useful for solving the challenges, it was felt that they did not need to be put into the final report.

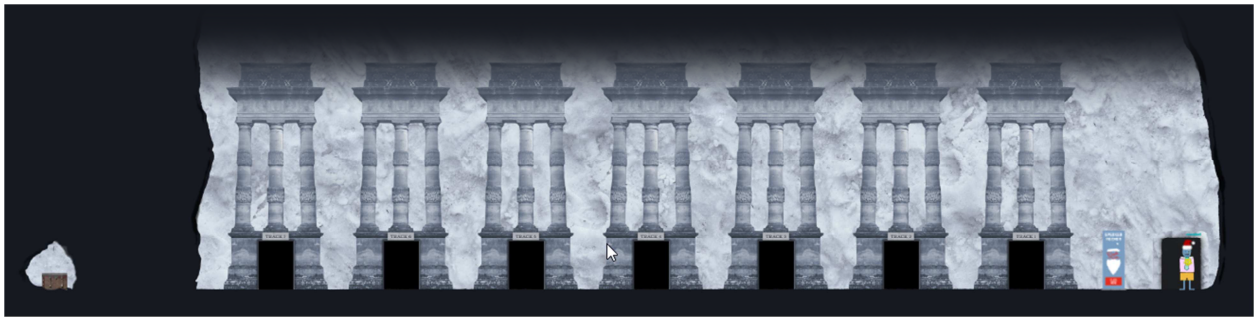
Cave

There were several "Treasure Chest Boxes" in the cave that gave you both KringleCoins and Hints. To enter the Cave you enter here:



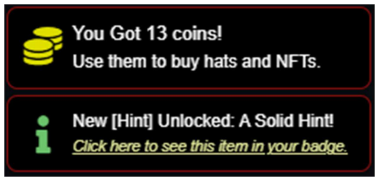
Box 1 – Hall of Talks

Once you go down the ladder and you will see the "Hall of Talks". Click to enter and you will see:



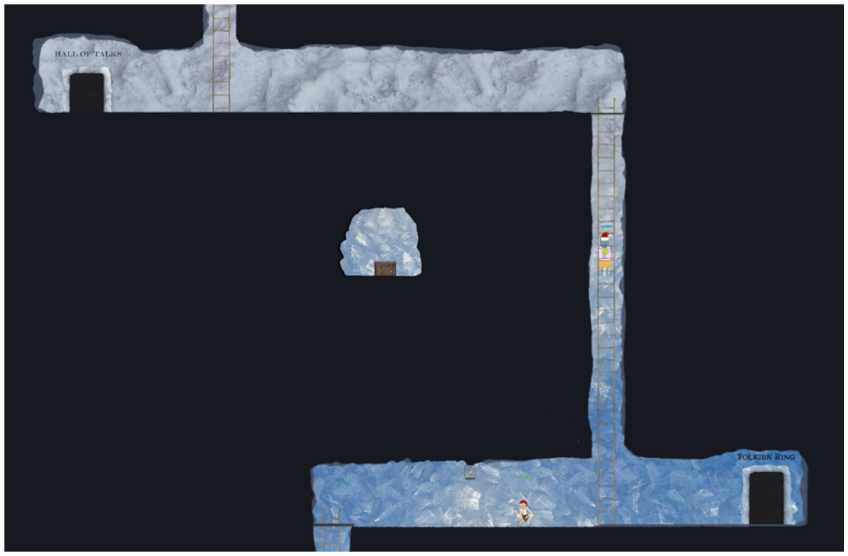
Navigate to the left and you can go through the wall to get to box 1. Click on it and you will see:

Click on “Take All Items” and you get:



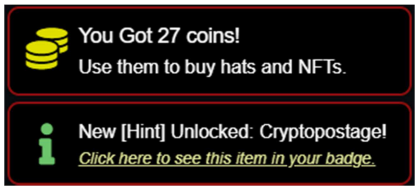
Box 2

As you keep going down the second ladder and you will see another box off to the left.



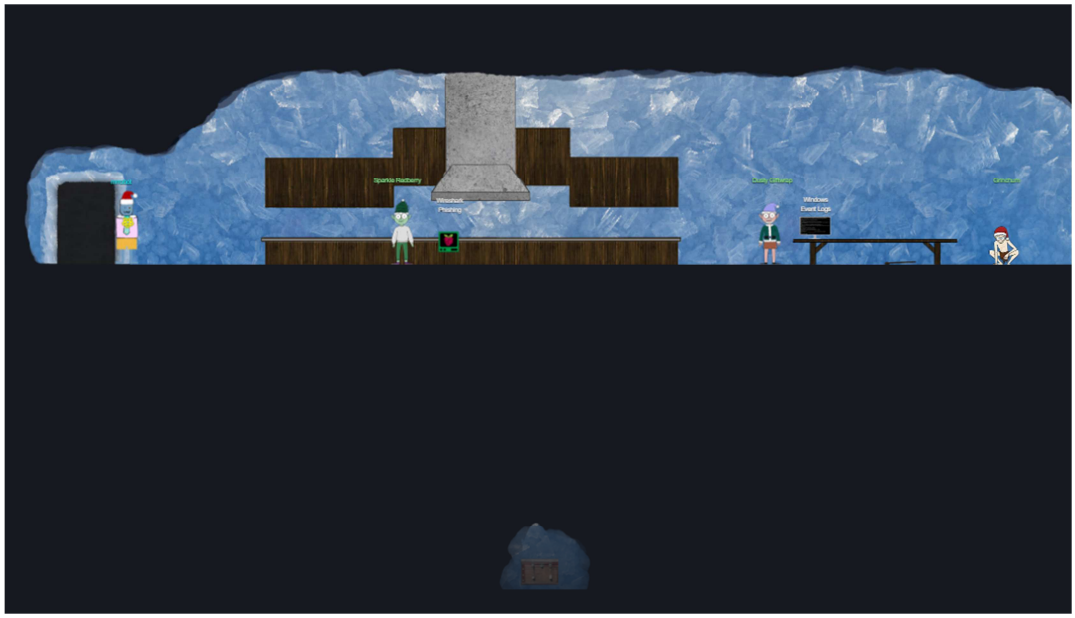
After navigating to the box you will see:

Click on “Take All Items” and you get:



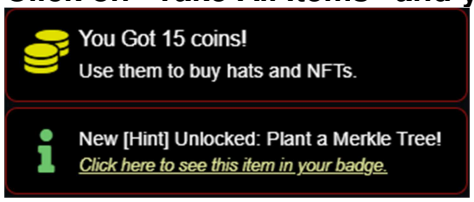
Box 3 – Tolkien Ring

At the bottom of the second ladder and you will see the “Tolkien Ring” entrance. Click to enter and you will see:



Change your zoom to 90%. Navigate to below the center of the table and you should be able to further navigate to box 3.

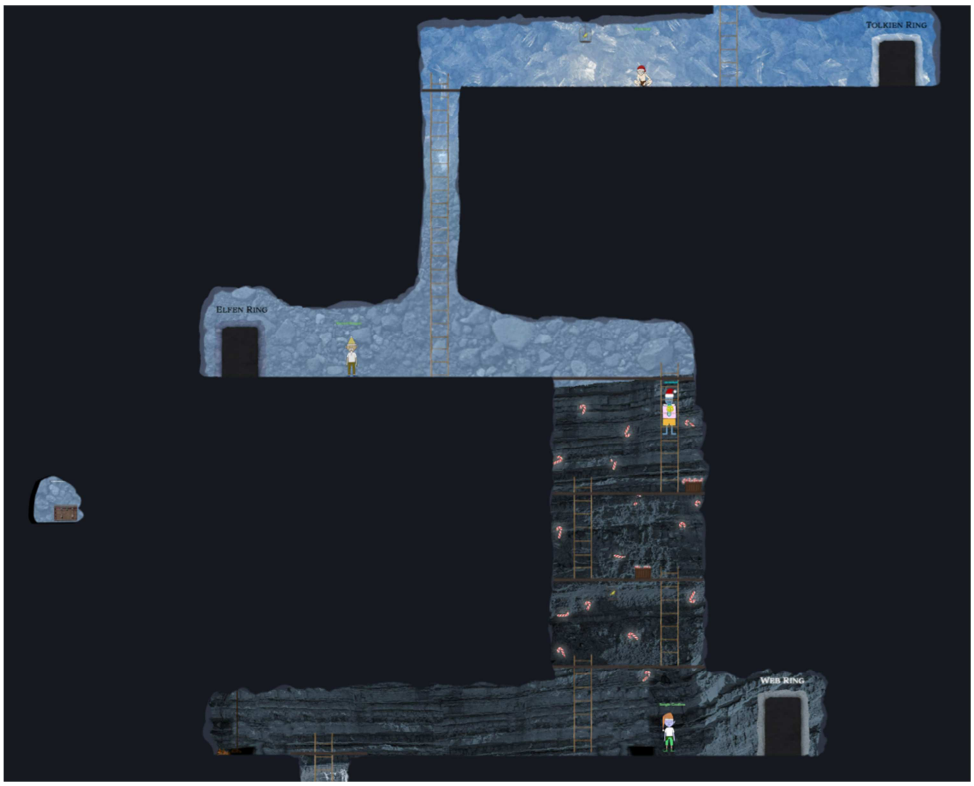
Click on “Take All Items” and you get:



Box 4

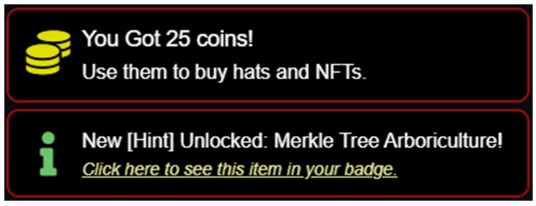
Exit the “Tolkien Ring” entrance. Go down the third ladder. To the right of the “Elfen Ring” entrance” will be a series of ladders leading down to the “Web

Ring”. Go down these ladders and to the far left is a rope you can climb to navigate to box 4.



Click to enter and you will see:

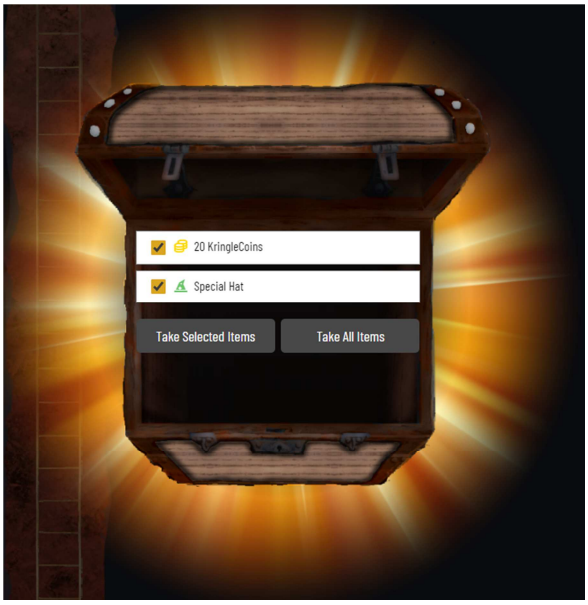
Click on “Take All Items” and you get:



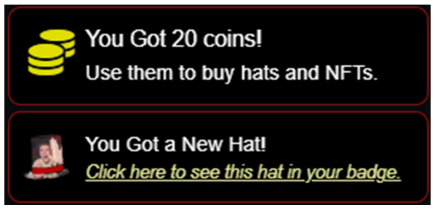
Box 5

Once you go down the ladder to the very bottom you will see the "Burning Ring of Fire" entrance. Make sure you are at 90% zoom level and start navigating to the right until you can get to box 5:

Click to enter and you will see:



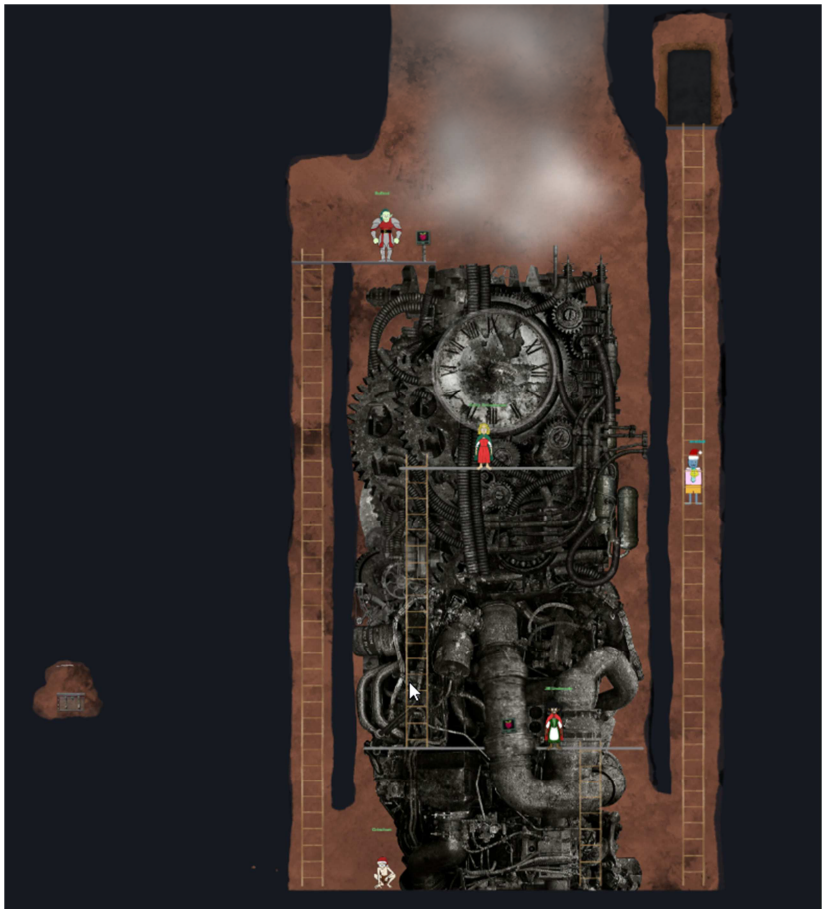
Click on “Take All Items” and you get:



Here is the “Special Hat”:

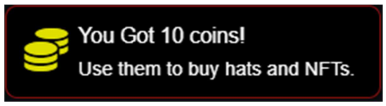
Box 6 – Cloud Ring

From the “Burning Ring of Fire” entrance, go back up and look for the “Cloud Ring” entrance. Click to enter and you will see:



Go to the bottom and then to the far left. Navigate through the wall to get to box 6.

Click on “Take All Items” and you get:



Hints

Get these by solving challenges:

AWS Whoami?

From: Jill Underpole
Terminal: AWS CLI 101
In the AWS command line (CLI), the Secure Token Service or STS has one very useful function.

AWS: get-caller-identity
https://awscli.amazonaws.com/v2/documentation/api/latest/reference/sts/get-caller-identity.html

IAM Privilege Escalation

From: Gerty Snowburrow
Terminal: AWS CLI 201
You can try s3api or lambda service commands, but Chris Elgee's talk on AWS and IAM might be a good start!

Chris Elgee, All I want for AWS is Allow * | KringleCon 2022
https://www.youtube.com/watch?v=t-xDvVUialo

(Attached) User Policies

From: Gerty Snowburrow
Terminal: AWS CLI 201
AWS inline policies pertain to one identity while managed policies can be attached to many identities.

AWS: Managed policies and inline policies
https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_managed-vs-inline.html

Merkle Tree Arboriculture

From: Hidden Chest - NPSL (Outside Elfen Ring)
Terminal: Bored Sporc Rowboat Society
You're going to need a Merkle Tree of your own. Math is hard. Professor Petabyte can help you out.

What is a Merkle Tree?
https://decentralizedthoughts.github.io/2020-12-22-what-is-a-merkle-tree/

Prof. Qwerty Petabyte, You Can Still Have Fun With Non-Fungible Tokens | KringleCon 2022
https://www.youtube.com/watch?v=Qt_RWBq63S8

Plant a Merkle Tree

Plant a Merkle Tree
From: Hidden Chest - Tolkien Ring
Terminal: Bored Sporc Rowboat Society

You can change something that you shouldn't be allowed to change. This repo might help!
https://github.com/QPetabyte/Merkle_Trees

Commiting to Mistakes

Commiting to Mistakes
From: Tinsel Upatree
Terminal: Jolly CI/CD
The thing about Git is that every step of development is accessible – even steps you didn't mean to take! `git log` can show code skeletons.

Switching Hats

Switching Hats
From: Tinsel Upatree
Terminal: Jolly CI/CD
If you find a way to impersonate another identity, you might try re-cloning a repo with their credentials.

Mount Up and Ride

From: Bow Ninecandle
Terminal: Prison Escape
Were you able to `mount` up? If so, users' `home/` directories can be a great place to look for secrets...

Over-Permissioned

From: Bow Ninecandle
Terminal: Prison Escape
When users are over-privileged, they can often act as root. When *containers* have too many permissions, they can affect the host!

Container is running in privileged mode
https://learn.snyk.io/lessons/container-runs-in-privileged-mode/kubernetes/

Built-In Hints

From: Sparkle Redberry
Terminal: Windows Event Logs
The hardest steps in this challenge have hints. Just type `hint` in the top panel!

Event Logs Exposé

From: Sparkle Redberry
Terminal: Windows Event Logs
New to Windows event logs? Get a jump start with Eric's talk!

Eric Pursley, Log Analyzing off the Land | KringleCon 2022
https://www.youtube.com/watch?v=5NZeHYPMXAE

Hat Dispensary

From: Wombley Cube
Terminal: Hat Vending
To purchase a hat, first find the hat vending machine in the Burning Ring of Fire. Select the hat that you think will give your character a bold and jaunty look, and click on it. A window will open giving you instructions on how to proceed with your purchase.

Wear It Proudly!

From: Wombley Cube
Terminal: Hat Vending
You should have been given a target address and a price by the Hat Vending machine. You should also have been given a Hat ID #. Approve the transaction and then return to the Hat Vending machine. You'll be asked to provide the Hat ID and your wallet address. Complete the transaction and wear your hat proudly!

Prepare to Spend

From: Wombley Cube
Terminal: Hat Vending
Before you can purchase something with KringleCoin, you must first approve the financial transaction. To do this, you need to find a KTM; there is one in the Burning Ring of Fire. Select *the Approve a KringleCoin transfer* button. You must provide the target wallet address, the amount of the transaction you're approving, and your private wallet key.

HTTS Git Cloning

From: Bow Ninecandle
Terminal: Clone with a Difference
There's a consistent format for Github repositories cloned via HTTPS. Try converting!

Git Clone
https://github.com/git-guides/git-clone

Lock Mechanism

From: Alabaster Snowball
Terminal: Boria Mine Door
The locks take input, render some type of image, and process on the back end to unlock. To start, take a good look at the source HTML/JavaScript.

Input Validation

From: Alabaster Snowball
Terminal: Boria Mine Door
Developers use both client- and server-side input validation to keep out naughty input.

OWASP: Input Validation Cheat Sheet
https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

Content-Security-Policy

From: Alabaster Snowball
Terminal: Boria Mine Door
Understanding how Content-Security-Policy works can help with this challenge.

OWSAP: Content Security Policy Cheat Sheet
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

Wireshark Top Talkers

From: Alabaster Snowball
Objective: Naughty IP
The victim web server is 10.12.42.16. Which host is the next top talker?

Naughty IP
https://2022.kringlecon.com/badge?section=objective&id=objBoriaPcapa

Wireshark : How to identify Top-talkers in Network
https://protocoholic.com/2018/05/24/wireshark-how-to-identify-top-talkers-in-network/

Wireshark String Searching

From: Alabaster Snowball
Objective: Credential Mining
The site's login function is at /login.html. Maybe start by searching for a string.

Credential Mining
https://2022.kringlecon.com/badge?section=objective&id=objBoriaPcapa

Wireshark: Finding Packets
https://www.wireshark.org/docs/wsug_html_chunked/ChWorkFindPacketSection.html

HTTP Status Codes

From: Alabaster Snowball
Objective: 404 FTW
With forced browsing, there will be many 404 status codes returned from the web server. Look for 200 codes in that group of 404s. This one can be completed with the PCAP or the log file.

404 FTW
https://2022.kringlecon.com/badge?section=objective&id=objBoriaPcapc

Instance Metadata Service

From: Alabaster Snowball
Objective: IMDS, XXE, and Other Abbreviations
AWS uses a specific IP address to access IMDS, and that IP only appears twice in this PCAP.

IMDS, XXE, and Other Abbreviations
https://2022.kringlecon.com/badge?section=objective&id=objBoriaPcapd

SANS: Cloud Instance Metadata Services (IMDS)
https://www.sans.org/blog/cloud-instance-metadata-services-imds-/

Cryptopostage

From: Hidden Chest - NPSL (Outside Tolkien Ring)
Objective: Blockchain Divination
Look at the transaction information. There is a From: address and a To: address. The To: address lists the address of the KringleCoin smart contract.

Blockchain Divination
https://2022.kringlecon.com/badge?section=objective&id=objContractAnalysis

A Solid Hint
From: Hidden Chest - Hall of Talks
Objective: Blockchain Divination
Find a transaction in the blockchain where someone sent or received KringleCoin! The *Solidity Source File* is listed as `KringleCoin.sol`. Tom's Talk might be helpful!

Blockchain Divination
https://2022.kringlecon.com/badge?section=objective&id=objContractAnalysis

Tom Liston, A Curmudgeon Looks at Cryptocurrencies | KringleCon 2022
https://www.youtube.com/watch?v=r3zj9DPC8VY

Significant Case
From: Hal Tandybuck
Objective: Glamtariel's Fountain
Early parts of this challenge can be solved by focusing on Glamtariel's WORDS.

Glamtariel's Fountain
https://2022.kringlecon.com/badge?section=objective&id=objMirror

Checkout Old Commits
From: Jill Underpole
Objective: Trufflehog Search
If you want to look at an older code commit with git, you can `git checkout CommitNumberHere`.

Trufflehog Search
https://2022.kringlecon.com/badge?section=objective&id=objTrufflehog

Trufflehog Tool
From: Jill Underpole
Objective: Trufflehog Search
You can search for secrets in a Git repo with `trufflehog git https://some.repo/here.git`.

Trufflehog Search
https://2022.kringlecon.com/badge?section=objective&id=objTrufflehog

Talks
All the talks are all located at https://www.youtube.com/@KringleCon

Welcome to the 2022 SANS Holiday Hack Challenge – Ed Skoudis
https://www.youtube.com/watch?v=4EStXLwBfFg

Log Analyzing off the Land – Eric Pursley
https://www.youtube.com/watch?v=5NZeHYPMXAE

All I want for AWS is Allow – Chris Elgee
https://www.youtube.com/watch?v=t-xDvVUialo

You Can Still Have Fun With Non-Fungible Tokens – Prof. Qwerty Petabyte
https://www.youtube.com/watch?v=Qt_RWBq63S8

A Curmudgeon Looks at Cryptocurrencies – Tom Liston
https://www.youtube.com/watch?v=r3zj9DPC8VY

Xmas Scanning with Nmap – Rajvi Khanjan Shroff
https://www.youtube.com/watch?v=O1vc5yDUeiE

Python's Nan-Issue – Mark Baggett
https://www.youtube.com/watch?v=lghzDTQBLNM

Javascript Obfuscation: Can You Deobfuscate Who's Naughty or Nice? – Melissa Bischoping
https://www.youtube.com/watch?v=d4pQyktLrow

Finding Rudolph: Why You Should Use IaC in the Cloud – Antoinette Stevens
https://www.youtube.com/watch?v=viuubNCrtrM

DevOps Faux Paws – Jared Folkins
https://www.youtube.com/watch?v=vIQY_FH1SVk

CTFs: Santa's Gift to Landing Your First (or Next) Cybersecurity Role – Chris Lemmon
https://www.youtube.com/watch?v=mDHvHBMOkj4

Other Hints

Identifying and retrieving TLS/SSL Certificates from a PCAP file using Wireshark
https://richardatkin.com/post/2022/01/15/Identifying-and-retrieving-certificates-from-a-PCAP-file-using-Wireshark.html

Container Breakout – Part 1
https://tbhaxor.com/container-breakout-part-1/

SVG Editor (Very helpful for solving the Lock terminal)
https://codepen.io/aerotwist/pen/njerWz

SVG Tutorial
https://developer.mozilla.org/en-US/docs/Web/SVG/Tutorial%7C%7C

Blockchain Explorer
https://prod-blockbrowser.kringle.co.in/

BSRS Gallery
https://boredsporcrowboatsociety.com/gallery.html
Last Sporc NFT = BSRS #000631 As of 1/3/2023