KringleCON 2020

- **Unescape Tmux**

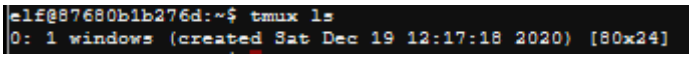
Descriere:

```
Can you help me?I was playing with my birdie (she's a Green Cheek!) in something
called **tmux**,then I did something and it disappeared!Can you help me find her?
We were so **attach**ed!!
```

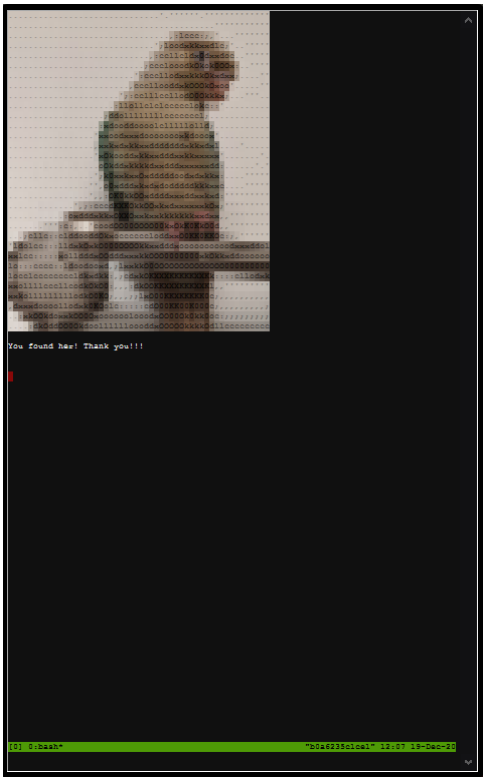
Rezolvare:

Din descrierea challenge-ului ne putem da seama ca suntem intr-un mediu in care este deschisa o sesiune Tmux pe care trebuie sa o accesam.

Am folosit comanda `tmux ls` pentru a vedea sesiunile deschise.



De aici am folosit comanda `tmux attach -t 0` pentru a ma concta la sesiunea deschisa, iar aici am gasit flag-ul.



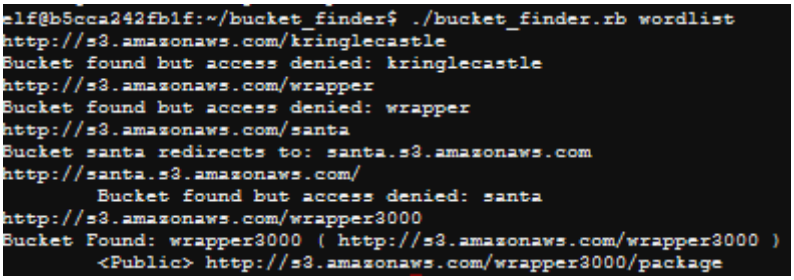
- **Investigate S3 Bucket**

Descriere:

```
Can you help me? Santa has been experimenting with new wrapping technology, and
we've run into a ribbon-curling nightmare!
We store our essential data assets in the cloud, and what a joy it's been!
Except I don't remember where, and the Wrapper3000 is on the fritz!
Can you find the missing package, and unwrap it all the way?
```

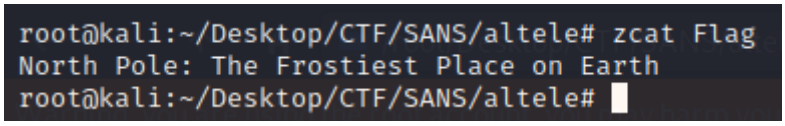
Rezolvare:

Am inceput prin a citi fisierul de TIPS, unde mi se specifica faptul ca in cazul in care am nevoie de editarea unui fisier pot sa folosesc nano sau vim, deci clar trebuia sa editez ceva. Un al doilea TIP era ca tot ce imi trebuie se afla in acel terminal. Am intrat in directorul bucket_finder, unde am gasit un script de ruby si un wordlist. Cum in descriere ni se precizeaza faptul ca nu mai gaseste Wrapper3000, am adaugat in wordlist si acest bucket, am rulat scriptul si am gasit un link ce ducea catre un bucket aws.



De aici am descarcat pachetul local, unde am gasit un base64 care era de fapt un fisier zip. In acel zip se afla o arhiva bz2, in care se afla una 7z, iar in cea 7z se afla un fisier pe care comanda file mi-l arata ca fiind "compress'd data 16 bits".

Am cautat sa vad cu ce as putea sa ii fac decompresia si am gasit utilitarul zcat, pe care l-am folosit si am scos flag-ul.



Flag: North Pole: The Frostiest Place on Earth

- **Uncover Santa's Gift List**

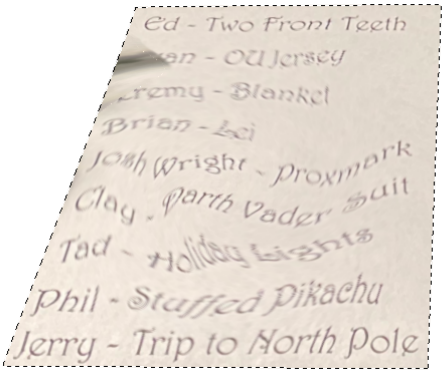
Descriere:

```
There is a photo of Santa's Desk on that billboard with his personal gift list.
What gift is Santa planning on getting Josh Wright for the holidays? Talk to
Jingle Ringford at the bottom of the mountain for advice.
```

Rezolvare:

Am primit poza asta ca challenge:

Aparent, din cerinta, trebuia sa ne dam seama ce va primi Josh Wright de Craciun, dar din cate se vede, nici macar nu stim daca are numele pus pe lista. Am facut putin research si am gasit un filtru asemanator in GIMP. Am intrat in utilitar, am incarcat poza, am decupat partea care ma interesa si am aplicat filtrul Whirl and Pinch pe poza. Nu a iesit cea mai clara scrisoare, dar macar am putut vedea ce va primi Josh.



Flag: proxmark

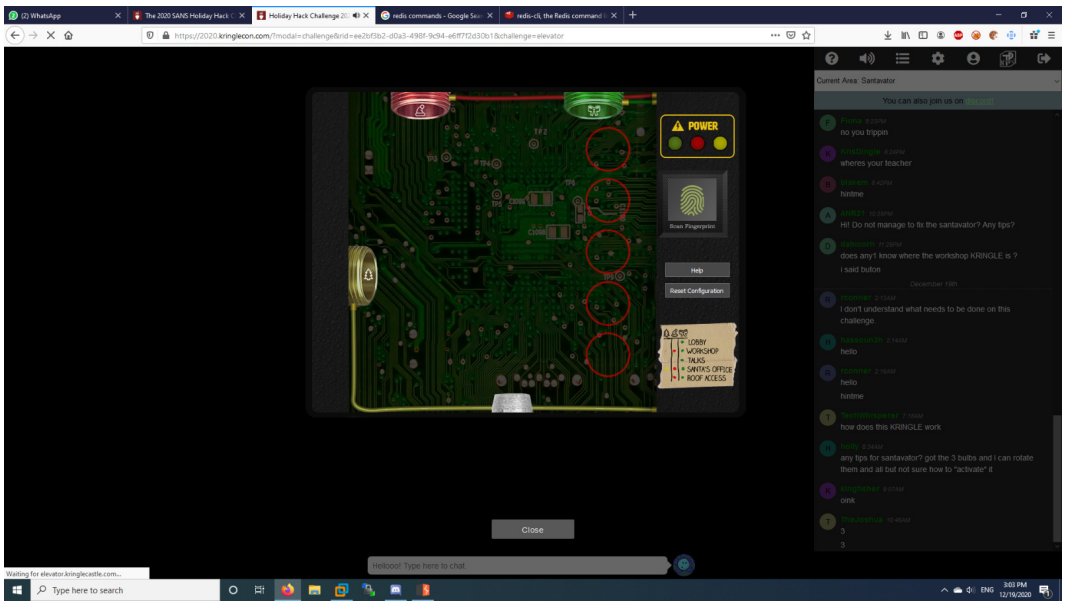
- **Operate the Santavator**

Descriere:

Talk to Pepper Minstix in the entryway to get some hints about the Santavator.

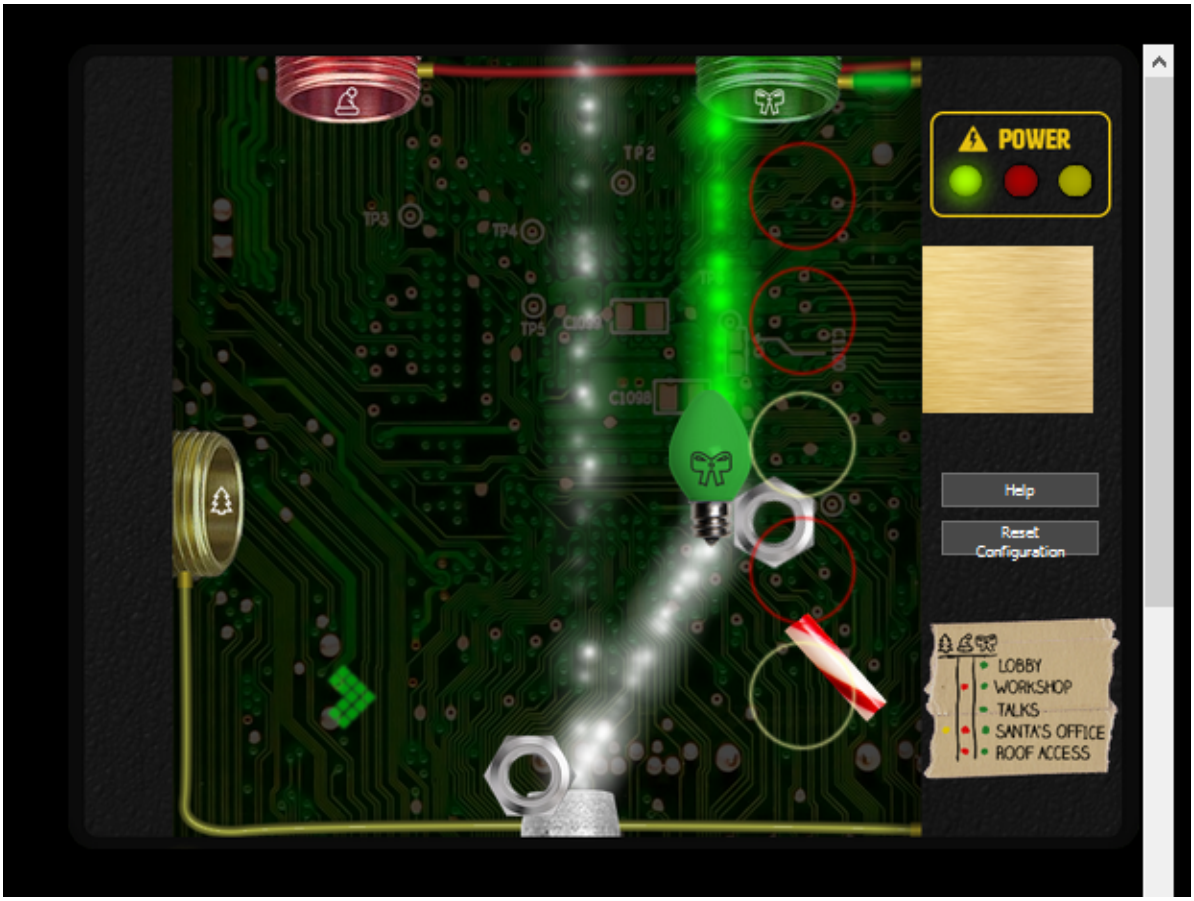
Rezolvare:

Am intrat in lift si am observat ca nici mcar unul din butoane nu functiona. Am dat refresh de cateva ori si am vazut ca peste interfata liftului si incarca un "cover" ce reprezenta interfata cu placa ce controla butoanele liftului. Am intrat in inspect element si am verificat sa vad ce e mai exact cu acea placa.



Aparent nu era niciun fir care sa duca curent intre butoane si sursa de electricitate. L-am lasat momentan asa si am continuat sa ma plimb pe harta. Am gasit o acadea, 2 suruburi si un bec, iar cand am vazut becul am revenit la lift, in ideea ca ma pot folosi de el.

Am intrat iarasi in inspect element, am sters cover-ul pentru a avea acces la circuite si am redirectionat curentul folosindu-ma de cele 2 piulite si de catre becul verde catre butonul ce activa etajul Talks, iar asa am luat achivement-ul.



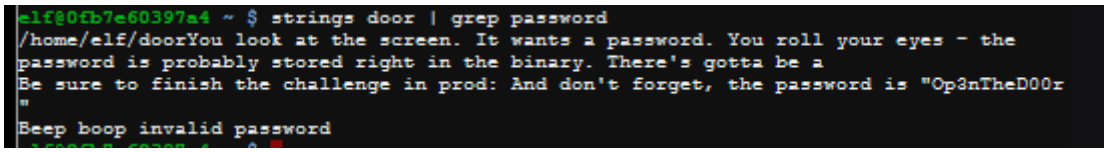
- **Usa de la SpekerUNPrep**

Descriere:

```
The door is controlled by ./door, but it needs a password! If you can figure
out the password, it'll open the door right up!
```

Rezolvare

Am primit un binar "door" ce astepta ca input o parola. Am incercat sa il scot din acel terminal emulat, dar nu avea conexiune la internet, deci nu era chiar posibil. Am incercat sa ma uit pe server, sa vad daca gasesc vreo parola in vre-un fisier, dar nimic. Dupa un timp m-am gandit sa dau pur si simplu strings pe binar si sa caut dupa "password" si aparent, a mers. (Aici am gasit si butonul de la etajul 1.5)



- **Regex Game**

Descriere:

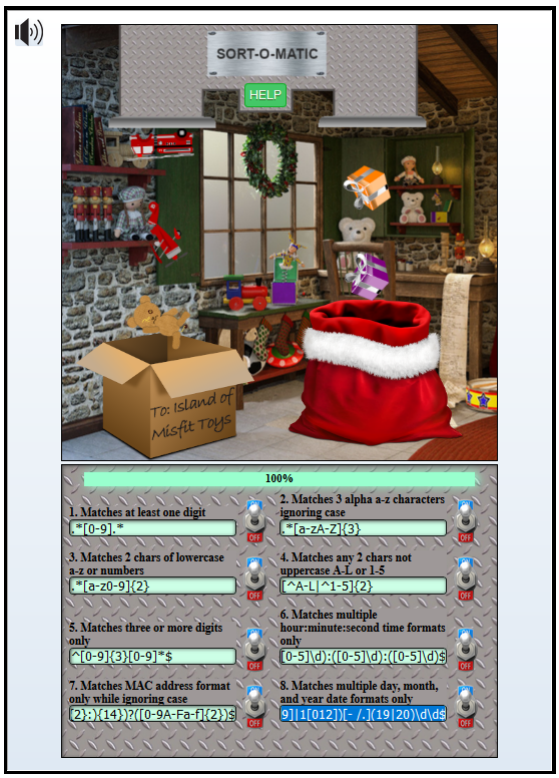
The SORT-O-MATIC is responsible for separating properly wrapped presents from disfunctional misfit presents. Properly wrapped presents are put into Santa's gift bag while the misfit toys are dropped into a box with a portal to the Island of Misfit Toys.

The SORT-O-MATIC's configuration works using regular expressions. When all eight regular expressions match the desired values the SORT-O-MATIC will properly sort presents.

Rezolvare:

In primul rand trebuia sa luam butonul de la SpekerUNPrep pentru putea urca la etajul 1.5, locul in care Mos Craciun facea jucariile. De aici se gaseau destul de multe obiecte pe jos, iar un task cerea rezolvarea unor regex-uri pentru a repara masina de jucarii.

1. Matches at least one digit : `.*[0-9].*`
2. Matches 3 alpha a-z characters ignoring case : `.*[a-zA-Z]{3}`
3. Matches 2 chars of lowercase a-z or numbers: `.*[a-z0-9]{2}`
4. Matches any 2 chars not uppercase A-L or 1-5: `[^A-L|^1-5]{2}`
5. Matches three or more digits only: `^[0-9]{3}[0-9]*$`
6. Matches multiple hour:minute:second time formats only: `^([0-5]\d):([0-5]\d):([0-5]\d)$`
7. Matches MAC address format only while ignoring case: `^([0-9A-Fa-f]{2}:){5}(([0-9A-Fa-f]{2}:){14})?([0-9A-Fa-f]{2})$`
8. Matches multiple day, month, and year date formats only: `^(0[1-9]|[12][0-9]|3[01])[-/.](0[1-9]|1[012])[- /.](19|20)\d\d$`



- **Linux Primer**

Descriere:

```
The North Pole 🍭 Lollipop Maker:
All the lollipops on this system have been stolen by munchkins. Capture munchkins
by following instructions here and 🍭's will appear in the green bar below. Run
the command "hintme" to receive a hint.
```

Rezolvare:

Aici nu o sa fac dau prea multe detalii, a fost un challenge in care trebuia sa cautam printr-o structura de fisiere cuvantul 'munchkin', ori cu `grep munchkin -io -r *` , ori cu find, nimic special.

- **Point-of-Sale Password Recovery**

Descriere:

```
Help Sugarplum Mary in the Courtyard find the supervisor password for the point-
of-sale terminal. What's the password?
```

Rezolvare:

Am primit un installer PXE care, dupa ce l-am instalat, mi-a scos o aplicatie santa-shop.exe si inca ceva fisiere. Am incercat sa caut parola prin strings, pentru ca decompilat era cam imposibil, executabilul avand 100mb, dar fara succes. Am cautat in folderul resources si am gasit un fisier app.asar. Am cautat pe google despre asta si am gasit ceva util pe https://medium.com/how-to-electron/how-to-get-source-code-of-any-electron-application-cbb5c7726c37. Am urmat pasii si am reusit sa dezasamblez fisierul asar, in care se afla codul sursa al unui site, respectiv backend-ul aplicatiei, in care am gasit si parola.

```
const SANTA_PASSWORD = 'santapass';
```

Flag: santapass

- **33.6 kbps:**

Descriere:

Am primit o imagine cu un telefon si niste butoane care scoteau niste sunete tare dubioase.

Rezolvare:

Am stat o gramada de timp sa imi dau seama cum as putea folosi notitele lasate langa telefon. Dupa ceva timp am dat click pe elf-ul de langa task si deasupra lui a aparut un numar de telefon. Cum nu am fost inspirat sa fac screenshot inainte, voi pune doar numarul aici :)) - 7568347. Daca sunam la numarul asta astepta sa vorbim. Am verificat codul javascript, iar acolo am vazut ca trebuia trimisa o ordine a mesajelor de pe biletel pentru a putea termina misiunea. In timp ce dadeam click pe mesaje, daca era cel corect, receptorul ramanea deschis, iar o variabila phase crestea, altfel, se inchidea.

M-am uitat in cod pentru a vedea cand cresc variabilele, am notat separat butoanele care declansau apelarea functiilor, am apasat pe butoane in ordinea corecta si bingo! Un nou achievement deblocat.

Ordinea butoanelor:

```
btnrespCrEsCl -baaDEEbrr
ack - aaah
cm_cj - WEWE..
l1_l2_info - beDURR..
trn schh...
```

- **Open HID Lock**

Descriere:

Trebuia sa deschid o usa al carui sistem de securitate se baza pe cartele RFID

Rezolvare:

Datorita challenge-ului 33.6 kbps am primit ca hint numele unui elf ce se gasea in curtea din fata a castelului. Dupa ce am pierdut cam o ora sa inteleg ce se intampla in acest challenge, pentru ca nu avea niciun sens la inceput, am inteles ca trebuie sa copiez o cartela RFID a unui elf cu ajutorul unui Proxmark3 emuator.

Am gasit elful, am dat comanda `lf hid read` pentru a-i putea copia cartela, iar apoi am mers sa deschid usa folosind comanda lf hid sim -r.

```
[magicdust] pm3 --> lf search

[=] NOTE: some demods output possible binary
[=] if it finds something that looks like a tag
[=] False Positives ARE possible
[=]
[=] Checking for known tags...
[=]

#db# TAG ID: 2006e22f13 (6025) - Format Len: 26 bit - FC: 113 - Card: 6025

[+] Valid HID Prox ID found!

[magicdust] pm3 --> lf hid read

#db# TAG ID: 2006e22f13 (6025) - Format Len: 26 bit - FC: 113 - Card: 6025
[magicdust] pm3 -->
```

- **Splunk Challenge**

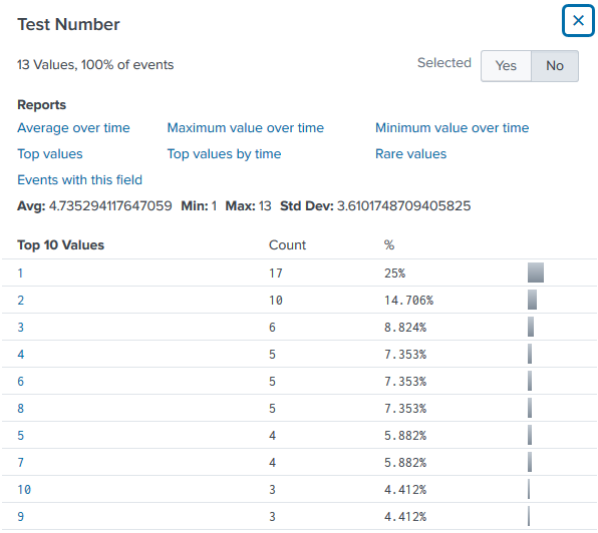
Descriere:

```
Access the Splunk terminal in the Great Room. What is the name of the adversary
group that Santa feared would attack KringleCon?
```

Rezolvare:

1. How many distinct MITRE ATT&CK techniques did Alice emulate?
2. What are the names of the two indexes that contain the results of emulating Enterprise ATT&CK technique 1059.003? (Put them in alphabetical order and separate them with a space)
3. One technique that Santa had us simulate deals with 'system information discovery'. What is the full name of the registry key that is queried to determine the MachineGuid?
4. According to events recorded by the Splunk Attack Range, when was the first OSTAP related atomic test executed? (Please provide the alphanumeric UTC timestamp.)
5. One Atomic Red Team test executed by the Attack Range makes use of an open source package authored by frgnca on GitHub. According to Sysmon (Event Code 1) events in Splunk, what was the ProcessId associated with the first use of this component?
6. Alice ran a simulation of an attacker abusing Windows registry run keys. This technique leveraged a multi-line batch file that was also used by a few other techniques. What is the final command of this multi-line batch file used as part of this simulation?
7. According to x509 certificate events captured by Zeek (formerly Bro), what is the serial number of the TLS certificate assigned to the Windows domain controller in the attack range?

   R1: 13



Test Number

13 Values, 100% of events — Selected: Yes / No

Reports

Average over time | Maximum value over time | Minimum value over time

Top values | Top values by time | Rare values

Events with this field

Avg: 4.735294117647059 **Min:** 1 **Max:** 13 **Std Dev:** 3.6101748709405825

Top 10 Values	Count	%
1	17	25%
2	10	14.706%
3	6	8.824%
4	5	7.353%
6	5	7.353%
8	5	7.353%
5	4	5.882%
7	4	5.882%
10	3	4.412%
9	3	4.412%

R2: t1059.003-main t1059.003-win

Query: `index=t1059.003*`

R3: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography

Query: `index=*  MachineGUID`

```
11/30/20 11/30/2020 08:42:59 PM
8:42:59.000 PM ... 29 lines omitted ...
        Creator Process ID:     0x1284
        Creator Process Name:   C:\Windows\System32\cmd.exe
        Process Command Line:   REG  QUERY HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography /v MachineGuid
```

R4: 2020-11-30T17:44:15Z

Query: `index=attack OSTAP`

R5: 3648

Query: `index=* *WindowsAudioDevice-Powershell-Cmdlet*`

R6: quser

Query: `index=* *.bat`

Am cautat pe pagina de github a atomic-red-team T-ul ce are legatura cu Registry Key, apoi am cautat codul sursa al T1547.001, iar de aici am gasit acest Discovery.bat.

https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1547.001/T1547.001.yaml

https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/ARTifacts/Misc/Discovery.bat

R7: 55FCEEBB21270D9249E86F4B9DC7AA60

Query: `index=* sourcetype=bro*`

Final: The Lollipop Guild

Enc: 7FXjP1lyfKbyDK/MChyf36h7

Ca hint am primit RFC 7465, deci era criptat cu RC4, iar cheia era pusa intr-un clip pus pe canalul de youtube al KringleCon: https://www.youtube.com/watch?v=RxVgEFt08kU&list=PLjLd1hNA7YVwqXqaBJfbXqkFb7LKw3r31&index=5

- ## Defeat Fingerprint Sensor

Descriere:

```
Bypass the Santavator fingerprint sensor. Enter Santa's office without Santa's
fingerprint.
```

Rezolvare:

Challenge-ul parea destul de simplu, trebuia sa urc la etajul la care doar Mos Craciun avea acces. Dupa ce am rezolvat challenge-ul HID door am putut sa joc deghizat ca Mos Craciun, asa cum am reusit sa rezolv challenge-ul cu Splunk. Dupa asta m-am dus la lift, am urcat la etajul secret, dar.. nu parea a fi calea spre rezolvarea challenge-ului. M-am schimbat inapoi in skin-ul meu si am incercat sa urc asa, dar nu puteam, pentru ca nu aveam amprenta mosului.

Am cautat in javascript, sa vad ce ar trebui sa fac pentru a trece de acel senzor, iar acolo, spre deosebire de restul butoanelor, am gasit o verificare in plus intr-un "if", se verifica daca functia hasToken("besanta"). Am incercat sa bypass-ez acest lucru, sa fac POST direct la pagina la care se facea POST in cazul in care se trecea de if, dar ca raspuns primeam doar un hash. Am mai cautat prin cod, dar nimic.
Dupa ceva timp, mi-am instalat chrome dev tools, iar de acolo am putut modifica bucata de cod javascript care facea verificarea. Am sters acel hasToken("besanta") si am putut urca la etajul secret si fara amprenta mosului.

- ## Can Bus Investigation

Descriere:

```
In your home folder, there's a CAN bus capture from Santa's sleigh. Some of the
data has been cleaned up, so don't worry - it isn't too noisy. What you will see
is a record of the engine idling up and down. Also in the data are a LOCK signal,
an UNLOCK signal, and one more LOCK. Can you find the UNLOCK? We'd like to encode
another key mechanism.
```

Rezolvare:

Am primit in terminal un elf file care verifica argv[1], in cazul in care trimiteam stringul bun, challenge-ul era gata. Trebuia sa gasesc pachetul malitios dintr-o captura de trafic vcan0. Cum nu am nici cea mai mica idee despre vcan0 am cautat cate ceva pe google, dar nu am gasit ceva ce m-ar putea ajuta. Dupa asta am revenit la cerinta si am observat ca mi se cerea un pachetul malitios, deci practic era un pachet diferit de toate celelalte.

Am dat `cat` pe fisier pentru a incerca sa il analizez si am observat foarte mult trafic ce avea id-ul 244, asa ca am incercat sa il analizez fara acest trafic, folosindu-ma de comanda `cat candump.log | grep -v 244` . Toate pachetele ramase erau de forma 188#00000000 sau de forma 19B#000000000000, doar unul singur era diferit, deci clar acesta era cel malitios. Arata asa: 19B#00000F000000, iar timestamp-ul lui era 1608926671.122520, asa ca raspunsul era 122520. Am trimis stringul ca argument la binar si am rezolvat challenge-ul.

Flag: 122520

- **Broken Tag Generator**

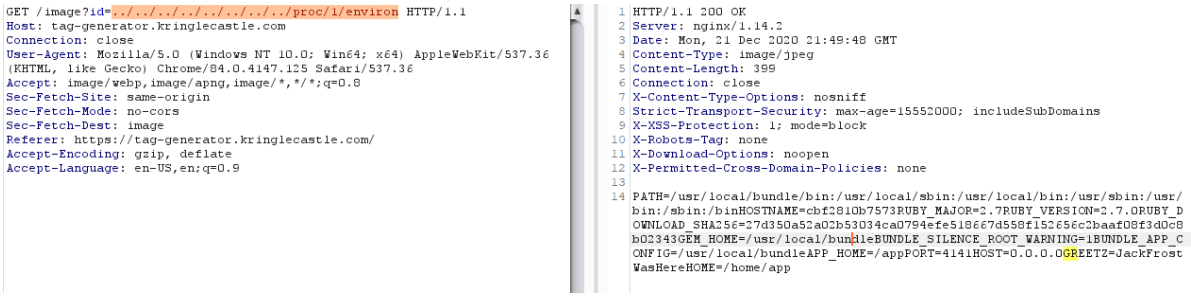
Descriere:

```
Help Noel Boetie fix the Tag Generator in the Wrapping Room. What value is in the environment variable GREETZ? Talk to Holly Evergreen in the kitchen for help with this.
```

Rezolvare:

Am primit un site in care imi puteam genera o felicitare de Craciun. Foarte dragut :D. Dar nu cred ca asta era scopul challenge-ului, asa ca am incercat sa vad ce pot exploata in el. Mi-a sarit in ochi functionalitatea de upload de poze. Am incercat sa uploadez poze cu php injectat, zip-uri cu directory traversal, dar nimic. Dupa un timp am vazut ca mi se genereaza fisierele uplaodate corect in /tmp/nume_generat, nume pe care il dadeam ca parametru de GET la /image?id=. Dupa ce am incercat fara succes sa injectez cod php pentru RCE am incercat un LFI in parametrul de GET si.. a mers.

Jumatate de problema era rezolvata, aveam acces sa citesc fisierele de pe server, iar acum trebuia sa gasesc o modalitate de a citit si variabila de mediu GREETZ. Avand in vedere ca variabilele de mediu sunt salvate in /proc/1/environ, am incercat LFI aici si a mers.



Payload: `../../../../../../../../proc/1/environ`

Flag: JackFrostWasHere