WEEK 12: FLAWS AWS

Report by Hapidael Mumbi

CS-CNS06-24062

Introduction

In this lab we learn about cloud security, focusing on Amazon Web Services (AWS).

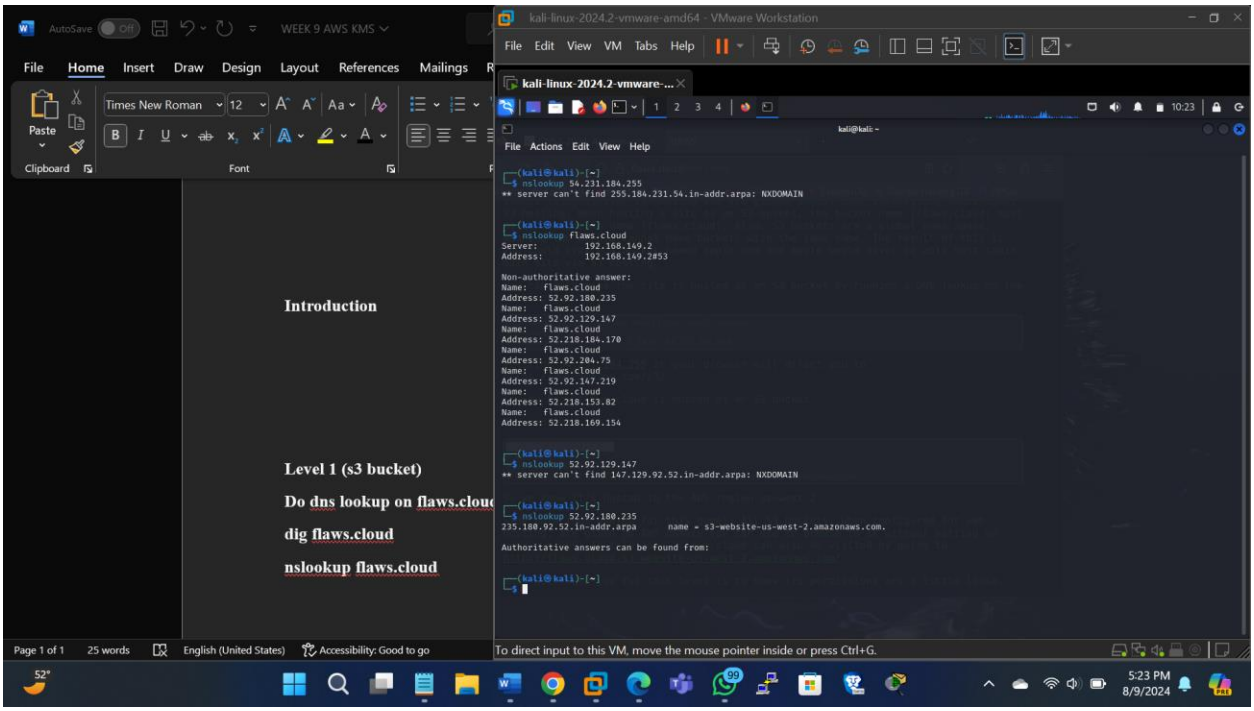
simulate common security misconfigurations and vulnerabilities in cloud environments. The lab introduces us to various aspects of cloud security, helping us understand how attackers might exploit weaknesses and how to prevent such attacks. Each level in the lab demonstrates a specific type of vulnerability, providing.

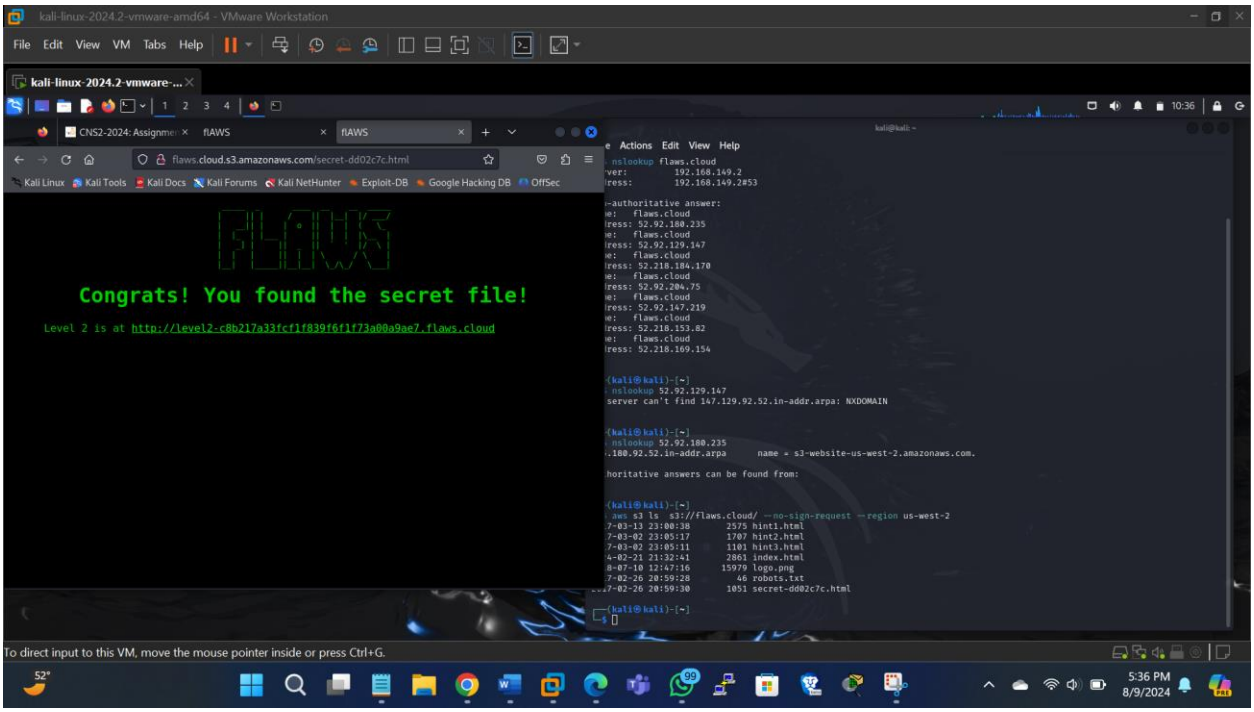
Objectives:

1. Improve your understanding of AWS security best practices, including permissions management, data protection, and resource monitoring.
2. Learn how to implement security measures to protect AWS resources from potential attacks.
3. Learn about typical security flaws in AWS environments and how they can be exploited.
4. Gain practical skills by working through real-world scenarios that illustrate how attackers might breach cloud environments.

Level 1: S3 Bucket Enumeration

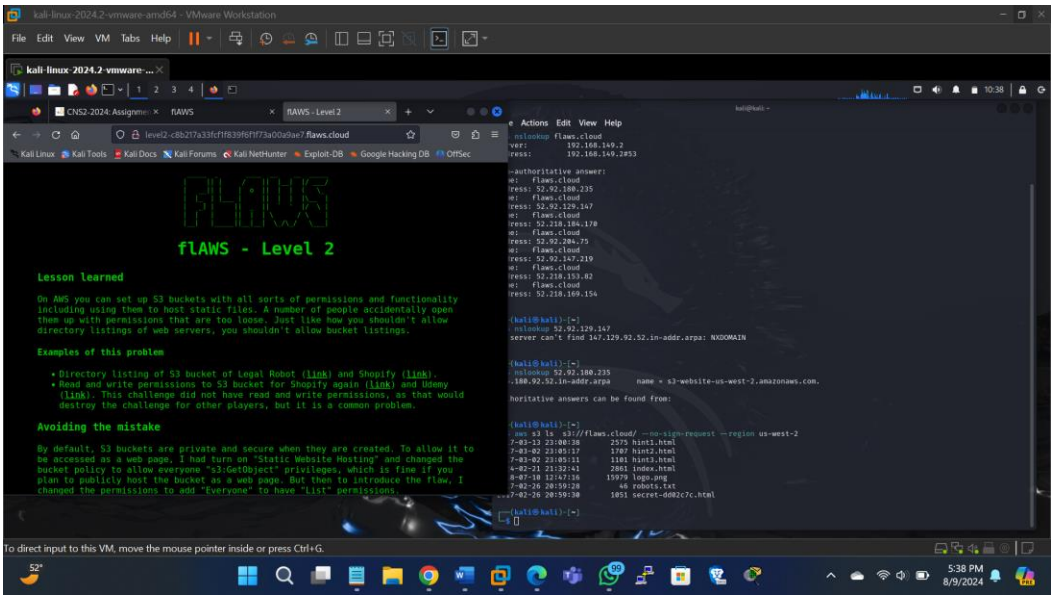
Here we will find a public bucket by searching fir potential bucket names.


WEEK 9 AWS KMS
Introduction
Level 1 (s3 bucket)
Do dns lookup on flaws.clou
dig flaws.cloud
nslookup flaws.cloud
kali-linux-2024.2-vmware-amd64 - VMware Workstation
nslookup 54.231.184.255
** server can't find 255.184.231.54.in-addr.arpa: NXDOMAIN
nslookup flaws.cloud
Server: 192.168.149.2
Address: 192.168.149.2#53
Non-authoritative answer:
Name: flaws.cloud
Address: 52.92.180.235
Address: 52.92.129.147
Address: 52.218.184.170
Address: 52.92.204.75
Address: 52.92.147.219
Address: 52.218.153.82
Address: 52.218.169.154
nslookup 52.92.129.147
** server can't find 147.129.92.52.in-addr.arpa: NXDOMAIN
nslookup 52.92.180.235
235.180.92.52.in-addr.arpa name = s3-website-us-west-2.amazonaws.com.
Authoritative answers can be found from:
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


kali-linux-2024.2-vmware-amd64 - VMware Workstation
Congrats! You found the secret file!
Level 2 is at http://level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud
aws s3 ls s3://flaws.cloud/ --no-sign-request --region us-west-2
2017-03-13 23:00:38 2575 hint1.html
2017-03-02 23:05:17 1707 hint2.html
2017-03-02 23:05:11 1101 hint3.html
2020-05-21 21:32:41 2861 index.html
2018-07-10 12:47:16 15979 logo.png
2017-02-26 20:59:28 46 robots.txt
2017-02-26 20:59:30 1051 secret-dd02c7c.html
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

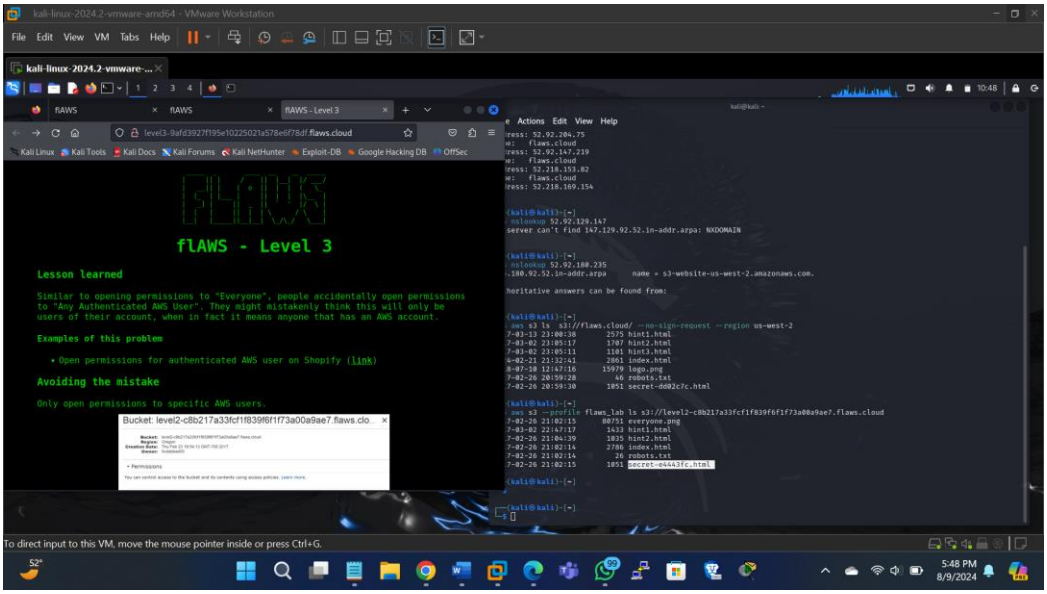
Level 2: S3 Bucket Permissions

In the second step will focus on S3 bucket permissions where we will identify a bucket with correct permissions and use them to access or modify its content.

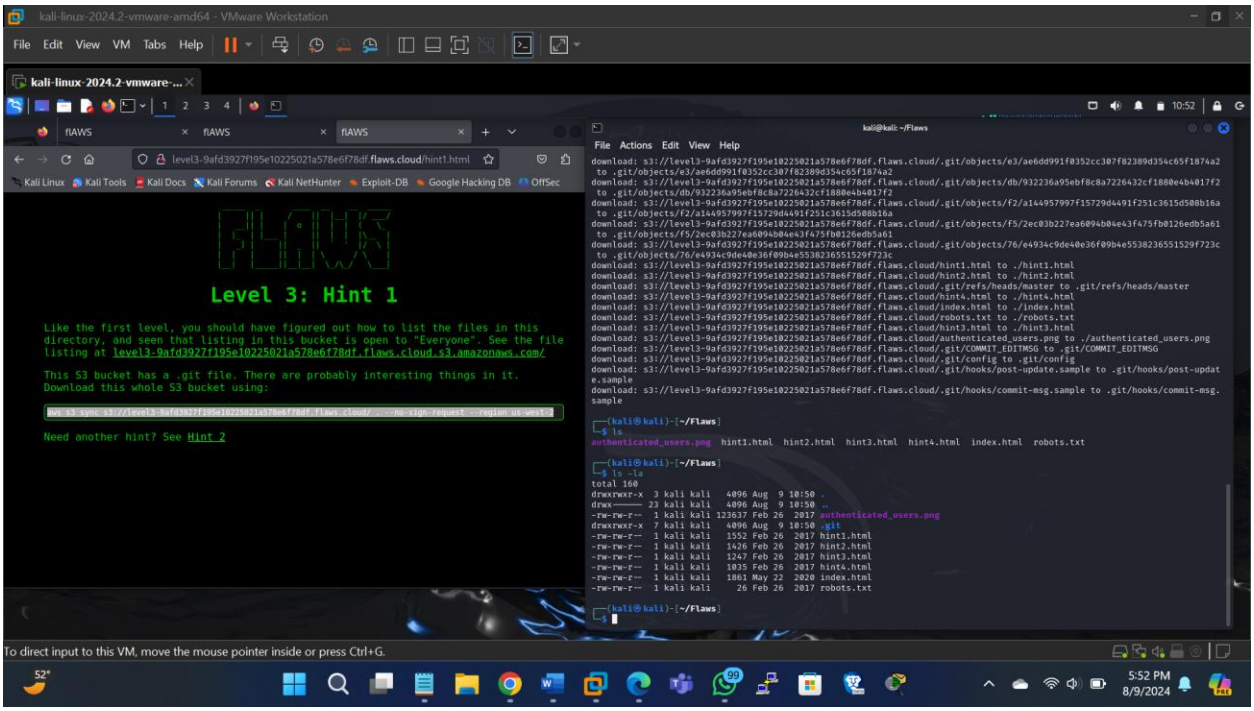


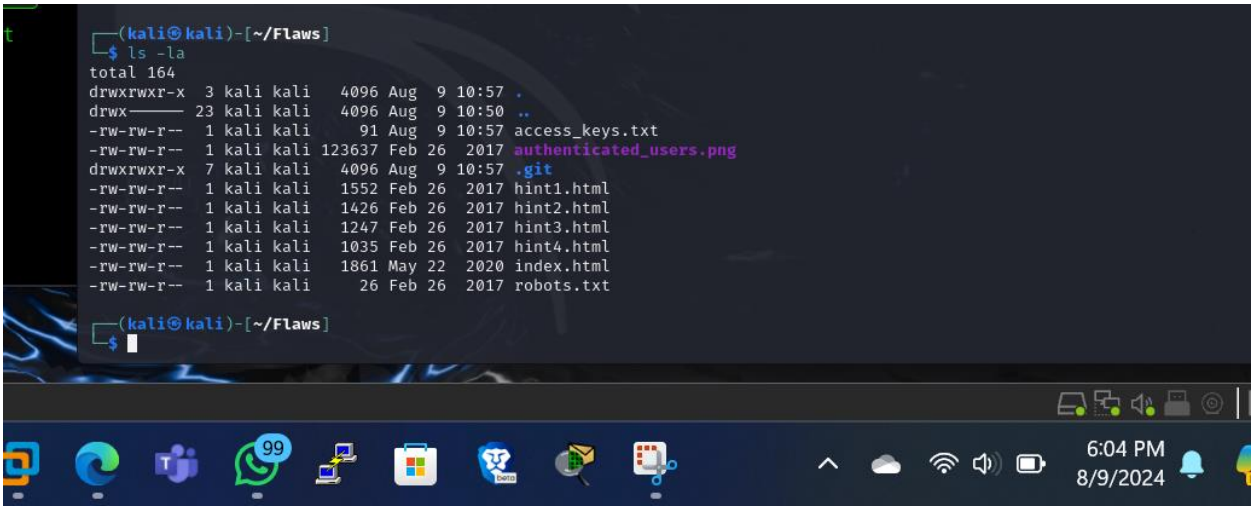
Level 3: IAM Policy Misconfigurations

In this section I will explore (IAM) policies, discovering how excessive permissions can lead to privilege escalation and unauthorized access to resources.



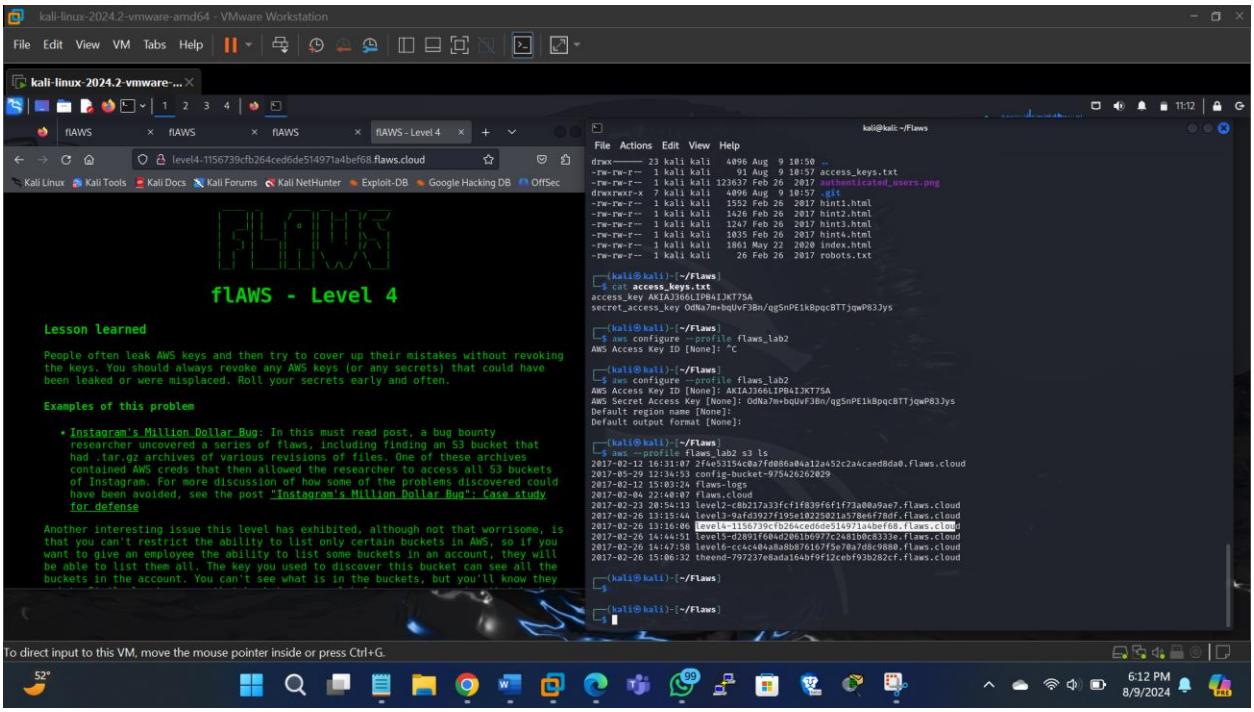
To see what was deleted

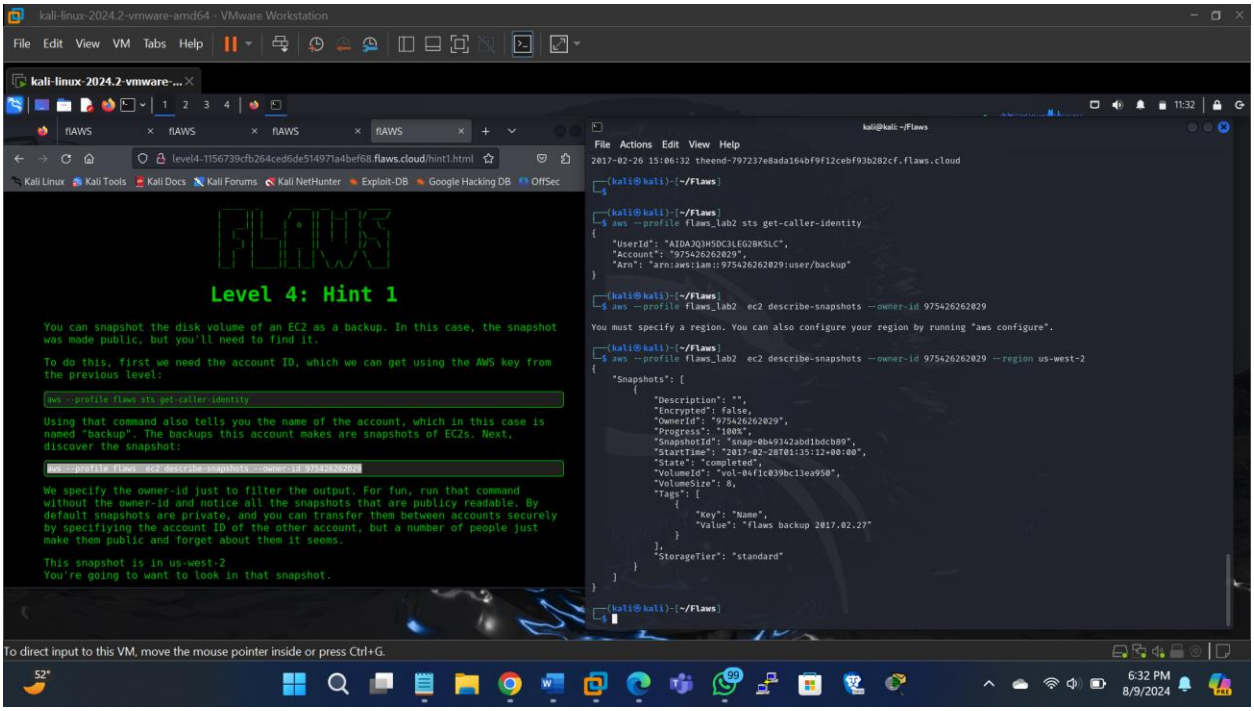

kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Level 3: Hint 1
Like the first level, you should have figured out how to list the files in this directory, and seen that listing in this bucket is open to "Everyone". See the file listing at level3-9afd3927f195e10225021a578e6f78df.flaws.cloud.s3.amazonaws.com/
This S3 bucket has a .git file. There are probably interesting things in it. Download this whole S3 bucket using:
aws s3 sync s3://level3-9afd3927f195e10225021a578e6f78df.flaws.cloud/ . --no-sign-request --region us-west-2
Need another hint? See Hint 2
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


(kali㉿kali)-[~/Flaws]
$ ls -la
total 164
drwxrwxr-x 3 kali kali 4096 Aug 9 10:57 .
drwx------ 23 kali kali 4096 Aug 9 10:50 ..
-rw-rw-r-- 1 kali kali 91 Aug 9 10:57 access_keys.txt
-rw-rw-r-- 1 kali kali 123637 Feb 26 2017 authenticated_users.png
drwxrwxr-x 7 kali kali 4096 Aug 9 10:57 .git
-rw-rw-r-- 1 kali kali 1552 Feb 26 2017 hint1.html
-rw-rw-r-- 1 kali kali 1426 Feb 26 2017 hint2.html
-rw-rw-r-- 1 kali kali 1247 Feb 26 2017 hint3.html
-rw-rw-r-- 1 kali kali 1035 Feb 26 2017 hint4.html
-rw-rw-r-- 1 kali kali 1861 May 22 2020 index.html
-rw-rw-r-- 1 kali kali 26 Feb 26 2017 robots.txt
(kali㉿kali)-[~/Flaws]
$
6:04 PM
8/9/2024

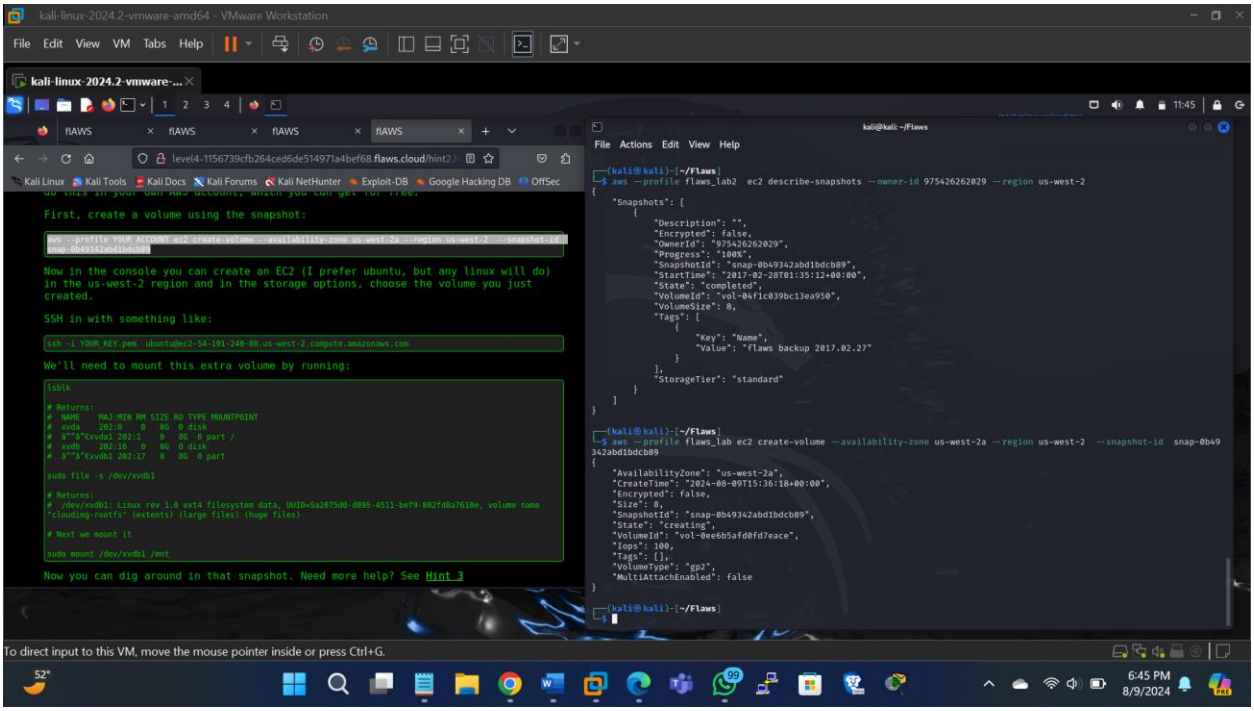
Level 4: IAM Role Misuse

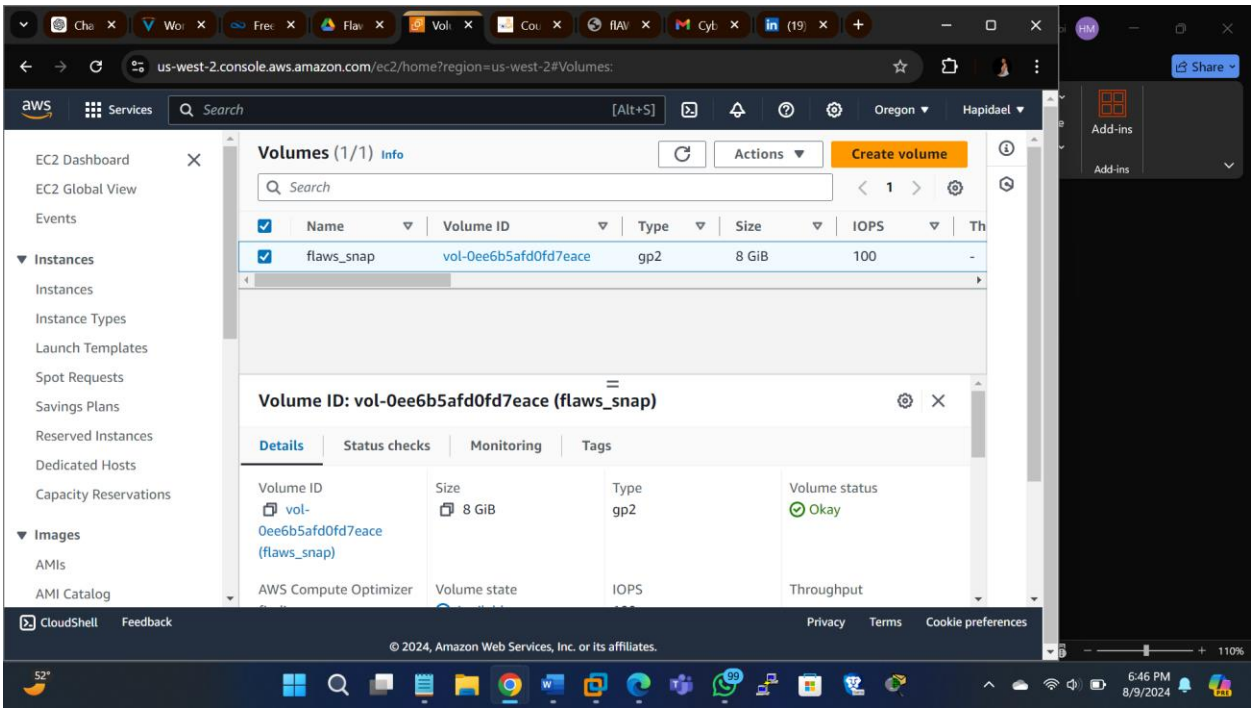
This level demonstrates how misconfigured IAM roles can be exploited by attackers to gain unauthorized access, showing the importance of role-specific permissions and the principle of least privilege.



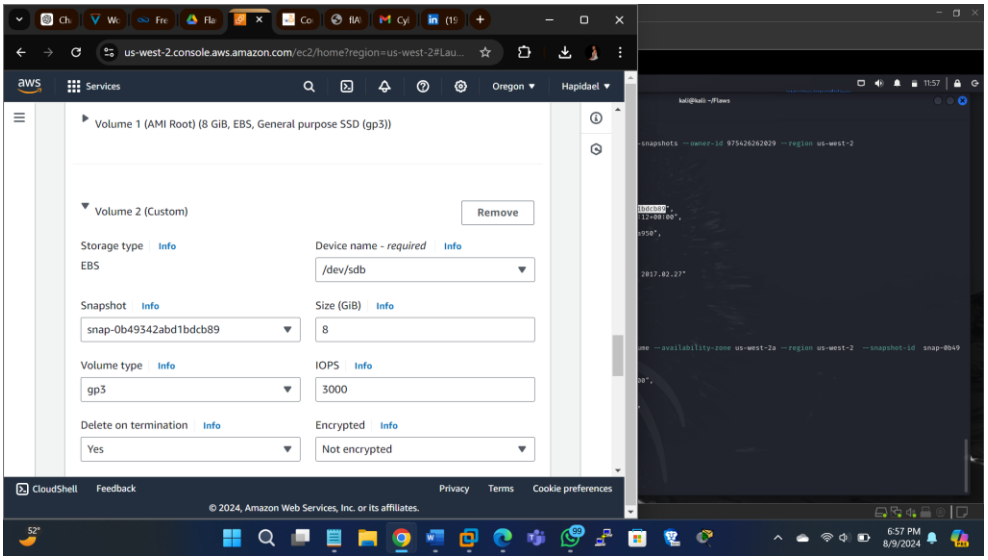


Volume creation

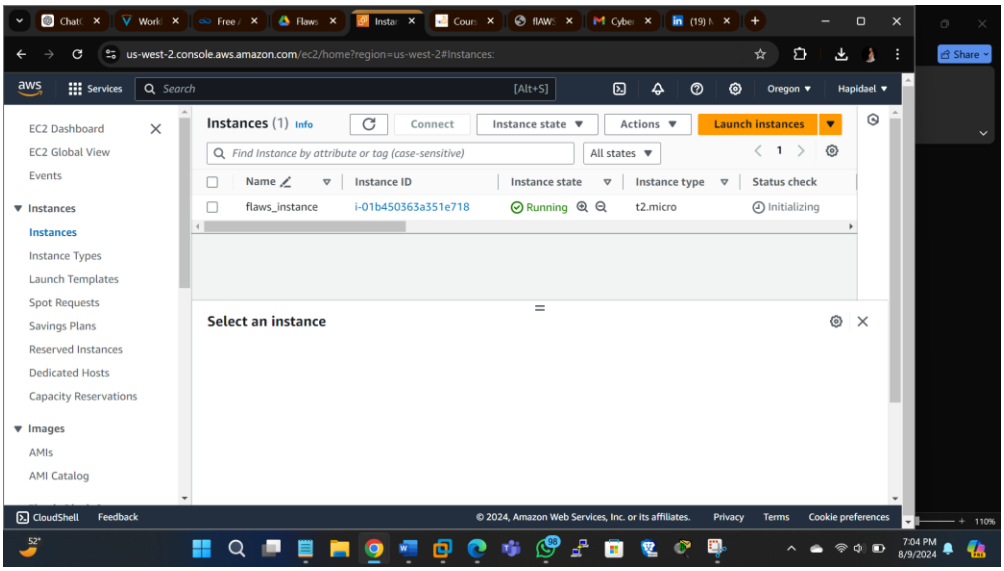




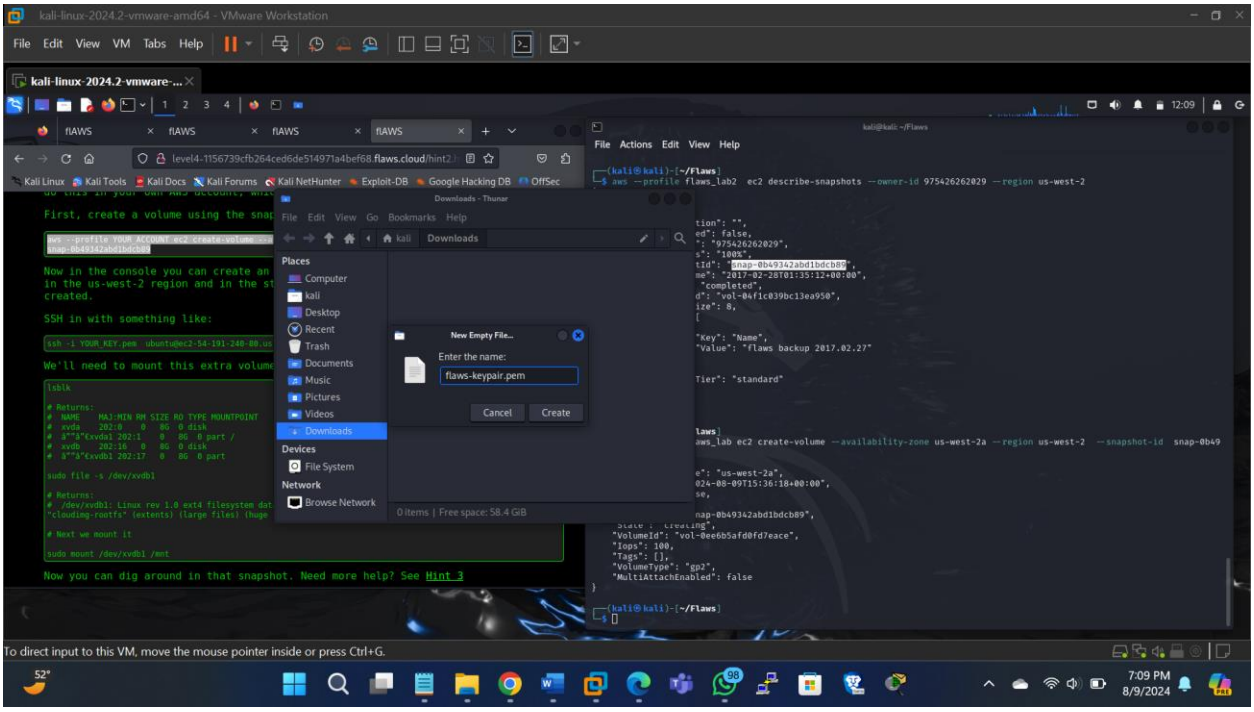
Storage (volume) Launching Instance

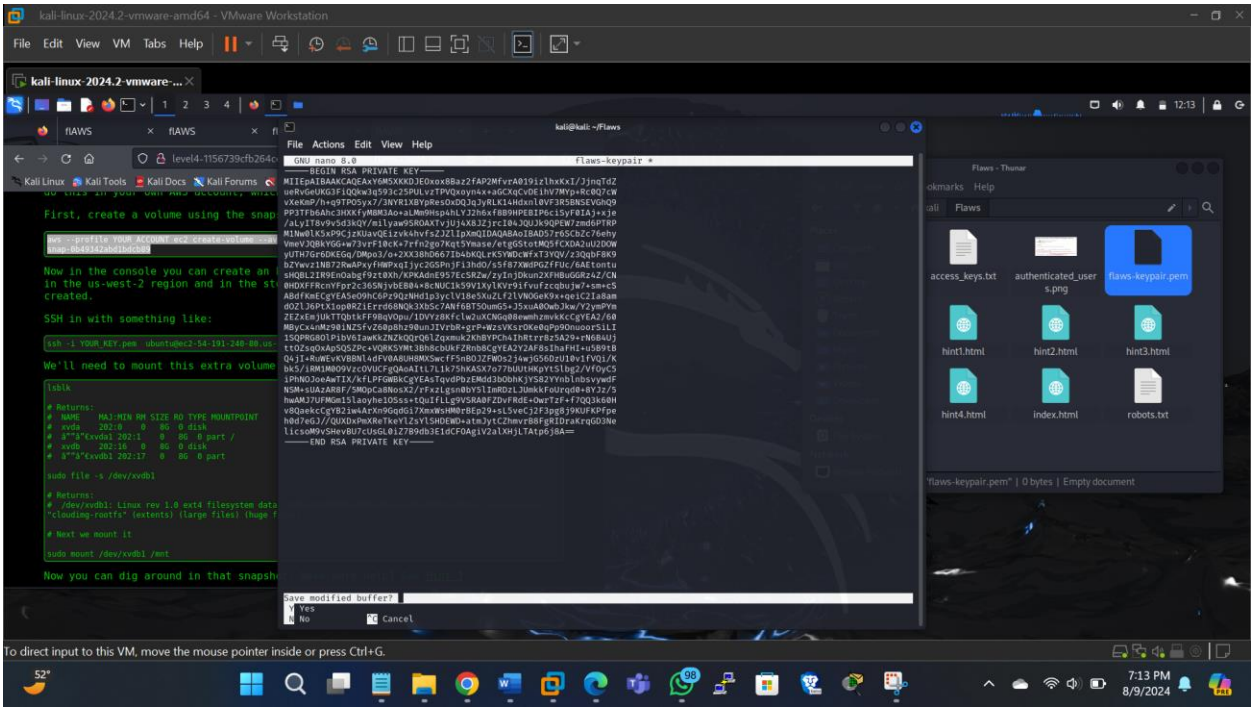


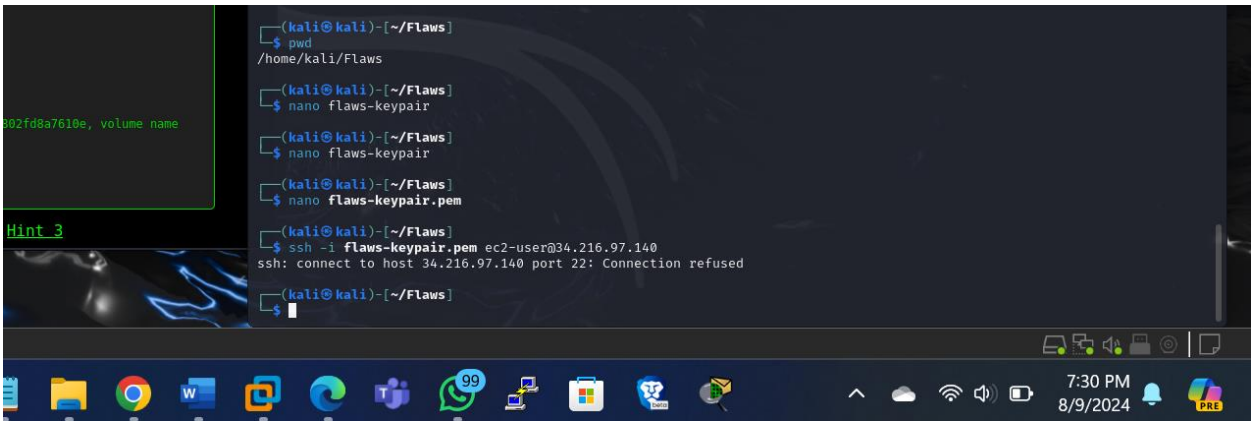
Instance launched

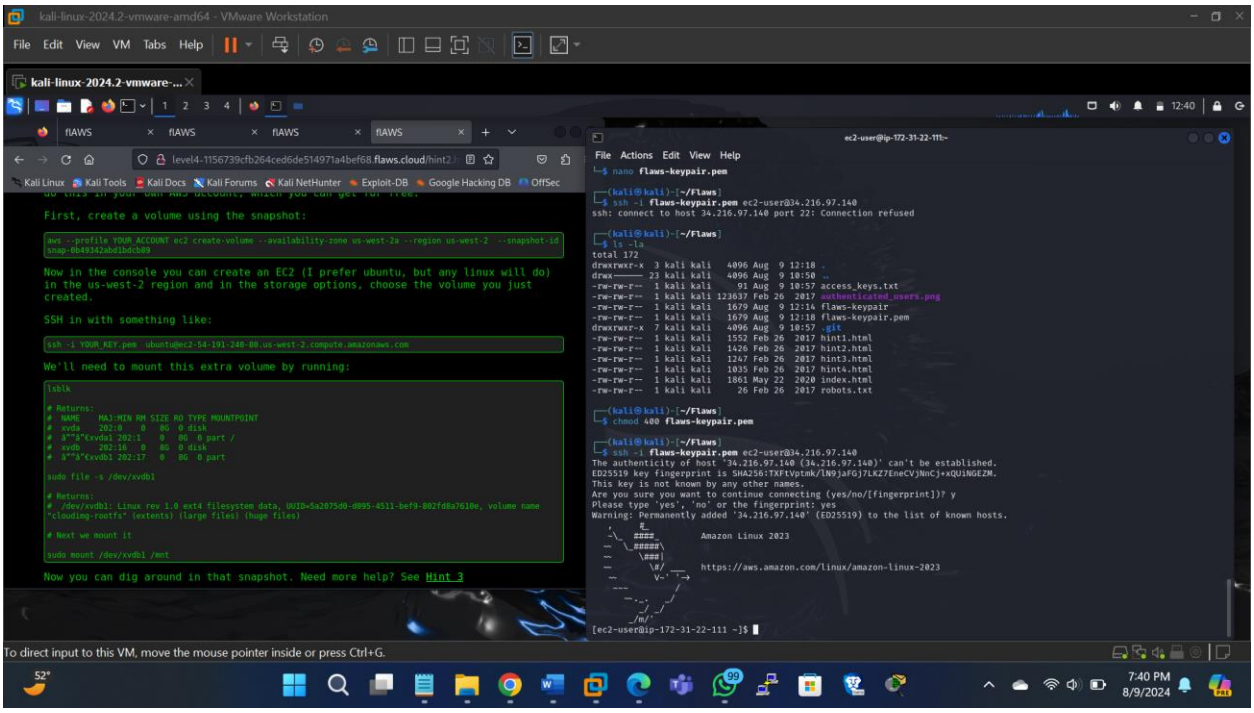


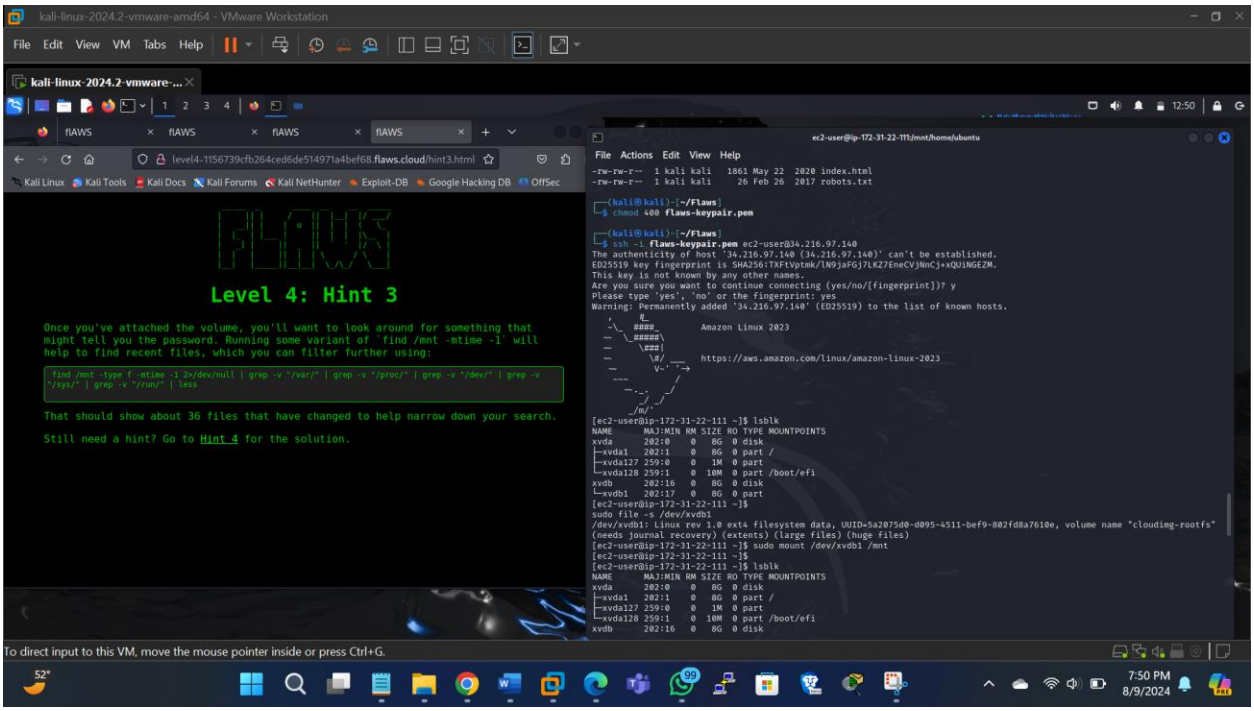
Saving the downloaded file in windows to kali machine

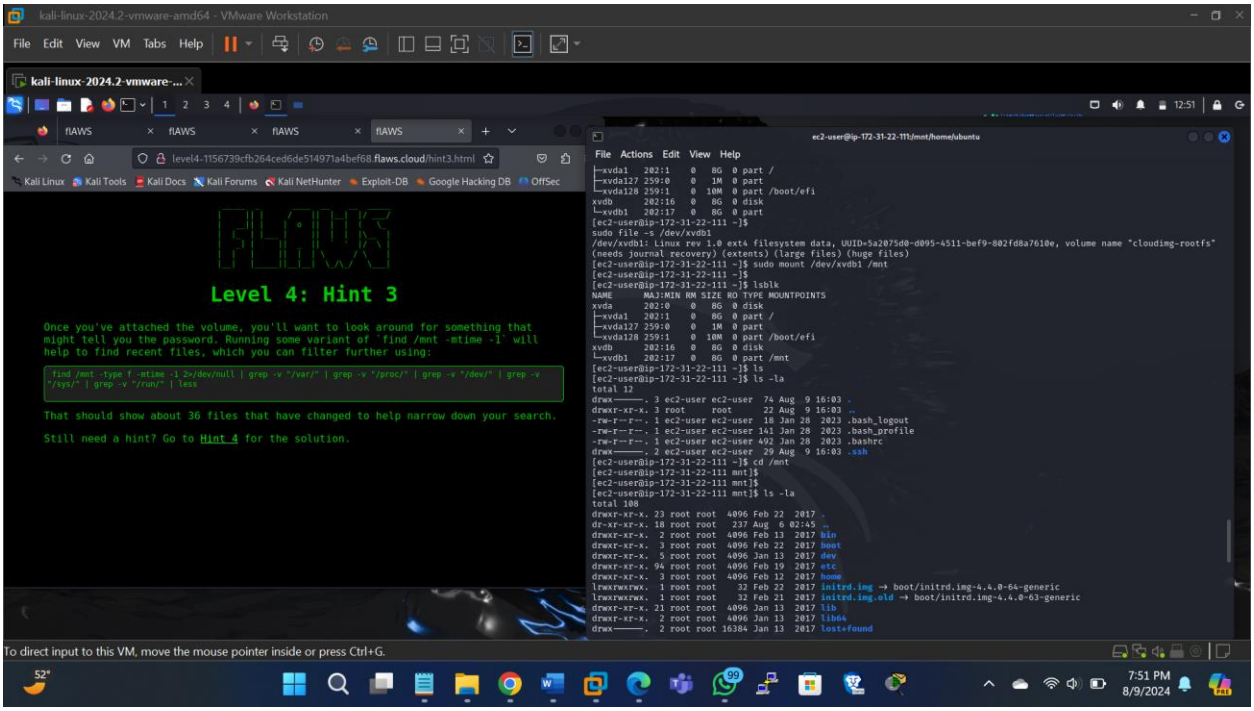





802fd8a7610e, volume name
Hint 3
(kali㉿kali)-[~/Flaws]
$ pwd
/home/kali/Flaws
(kali㉿kali)-[~/Flaws]
$ nano flaws-keypair
(kali㉿kali)-[~/Flaws]
$ nano flaws-keypair
(kali㉿kali)-[~/Flaws]
$ nano flaws-keypair.pem
(kali㉿kali)-[~/Flaws]
$ ssh -i flaws-keypair.pem ec2-user@34.216.97.140
ssh: connect to host 34.216.97.140 port 22: Connection refused
(kali㉿kali)-[~/Flaws]
$
7:30 PM
8/9/2024

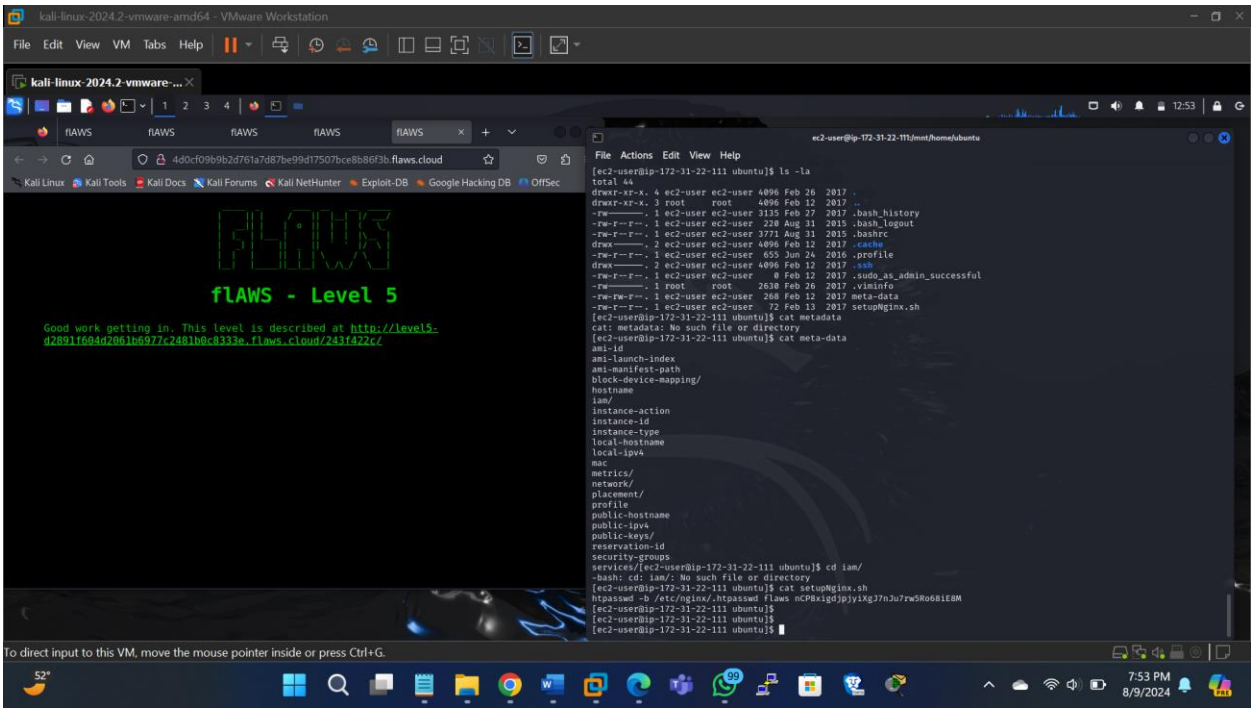

kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2024.2-vmware-...
fIAWS
level4-1156739cfb264ced6de514971a4bef68.flaws.cloud/hint2
First, create a volume using the snapshot:
Now in the console you can create an EC2 (I prefer ubuntu, but any linux will do) in the us-west-2 region and in the storage options, choose the volume you just created.
SSH in with something like:
We'll need to mount this extra volume by running:
Now you can dig around in that snapshot. Need more help? See Hint 3
ec2-user@ip-172-31-22-111:~
File Actions Edit View Help
nano flaws-keypair.pem
ssh -i flaws-keypair.pem ec2-user@34.216.97.140
ssh: connect to host 34.216.97.140 port 22: Connection refused
ls -la
total 172
drwxrwxr-x 3 kali kali 4096 Aug 9 12:18 .
drwx------ 23 kali kali 4096 Aug 9 10:50 ..
-rw-rw-r-- 1 kali kali 91 Aug 9 10:57 access_keys.txt
-rw-rw-r-- 1 kali kali 123637 Feb 26 2017 authenticated_users.png
-rw-rw-r-- 1 kali kali 1679 Aug 9 12:14 flaws-keypair
-rw-rw-r-- 1 kali kali 1679 Aug 9 12:18 flaws-keypair.pem
drwxrwxr-x 7 kali kali 4096 Aug 9 10:57 .git
-rw-rw-r-- 1 kali kali 1552 Feb 26 2017 hint1.html
-rw-rw-r-- 1 kali kali 1426 Feb 26 2017 hint2.html
-rw-rw-r-- 1 kali kali 1247 Feb 26 2017 hint3.html
-rw-rw-r-- 1 kali kali 1035 Feb 26 2017 hint4.html
-rw-rw-r-- 1 kali kali 1861 May 22 2020 index.html
-rw-rw-r-- 1 kali kali 26 Feb 26 2017 robots.txt
chmod 400 flaws-keypair.pem
ssh -i flaws-keypair.pem ec2-user@34.216.97.140
The authenticity of host '34.216.97.140 (34.216.97.140)' can't be established.
ED25519 key fingerprint is SHA256:TXFtVptmk/lN9JaFGj7LKZ7EneCVjNnCj+xQUiNGEZM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '34.216.97.140' (ED25519) to the list of known hosts.
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-172-31-22-111 ~]$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
7:40 PM
8/9/2024

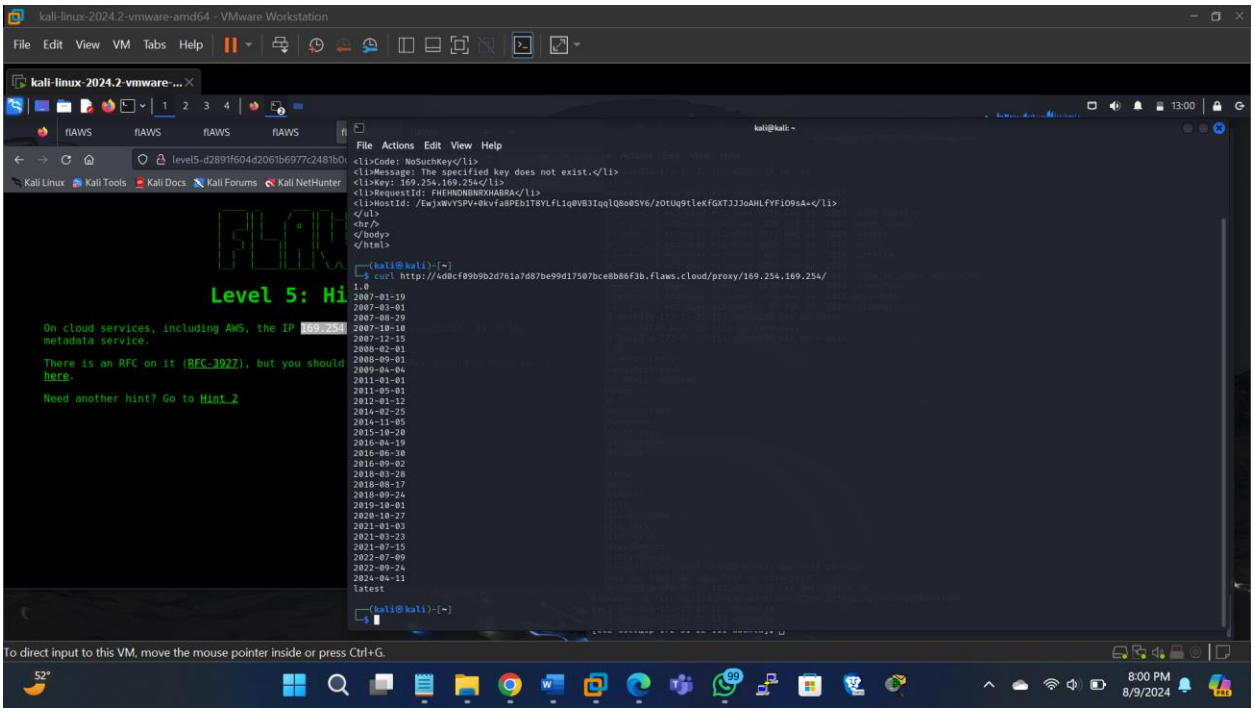

kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Level 4: Hint 3
Once you've attached the volume, you'll want to look around for something that might tell you the password. Running some variant of `find /mnt -mtime -1` will help to find recent files, which you can filter further using:
find /mnt -type f -mtime -1 2>/dev/null | grep -v "/var/" | grep -v "/proc/" | grep -v "/dev/" | grep -v "/sys/" | grep -v "/run/" | less
That should show about 36 files that have changed to help narrow down your search.
Still need a hint? Go to Hint 4 for the solution.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
7:50 PM
8/9/2024

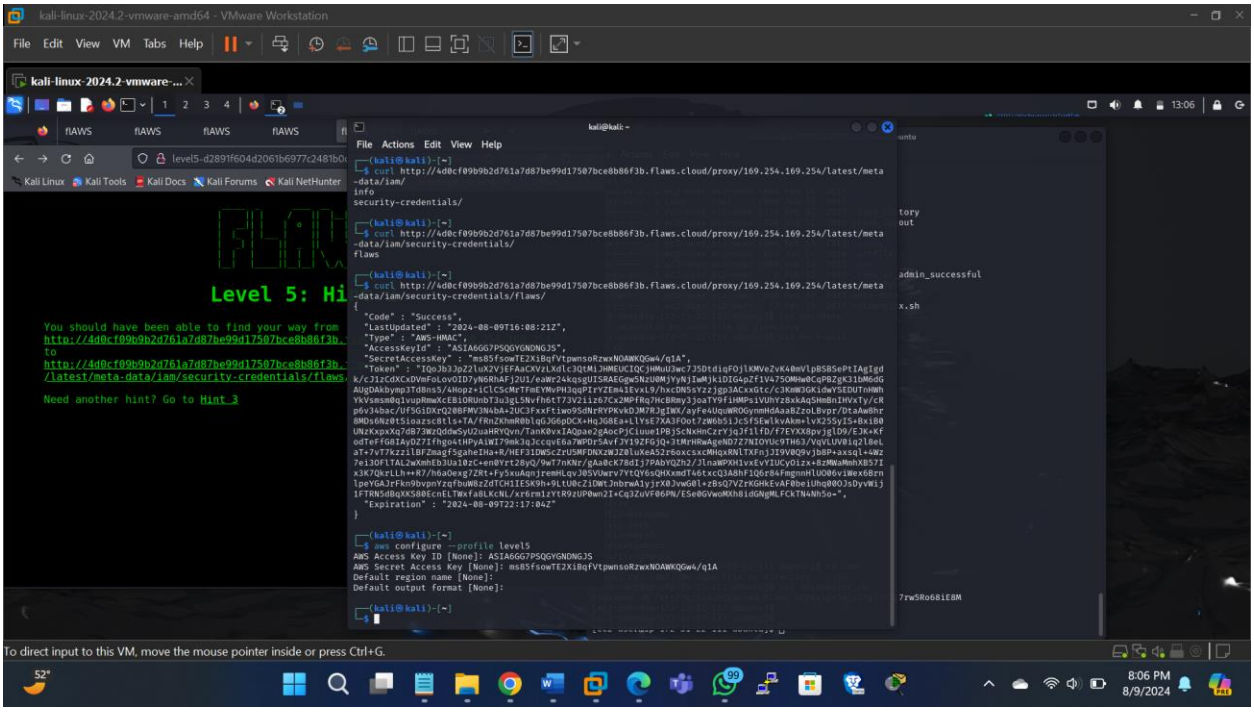

kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Level 4: Hint 3
Once you've attached the volume, you'll want to look around for something that might tell you the password. Running some variant of `find /mnt -mtime -1` will help to find recent files, which you can filter further using:
find /mnt -type f -mtime -1 2>/dev/null | grep -v "/var/" | grep -v "/proc/" | grep -v "/dev/" | grep -v "/sys/" | grep -v "/run/" | less
That should show about 36 files that have changed to help narrow down your search.
Still need a hint? Go to Hint 4 for the solution.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
7:51 PM
8/9/2024

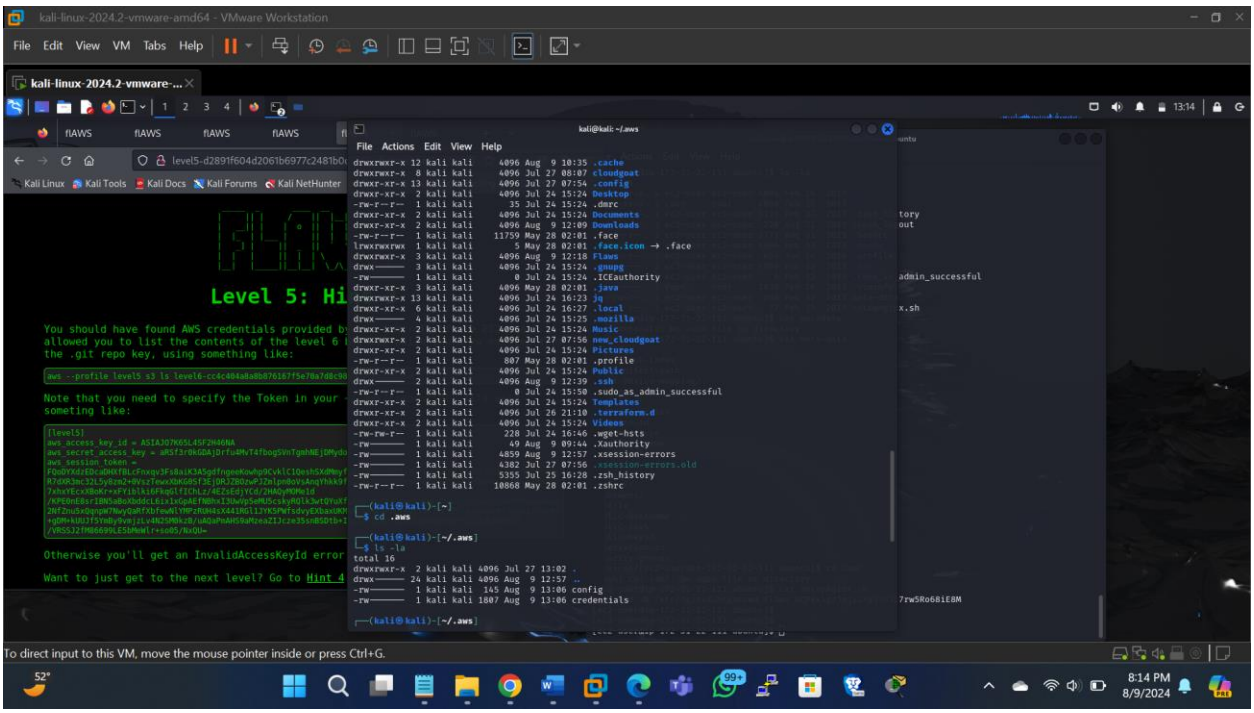
And on to level 5

Here examine an insecurely configured Lambda function, learning how such vulnerabilities can be exploited to gain access to sensitive data or escalate privileges within an AWS environment

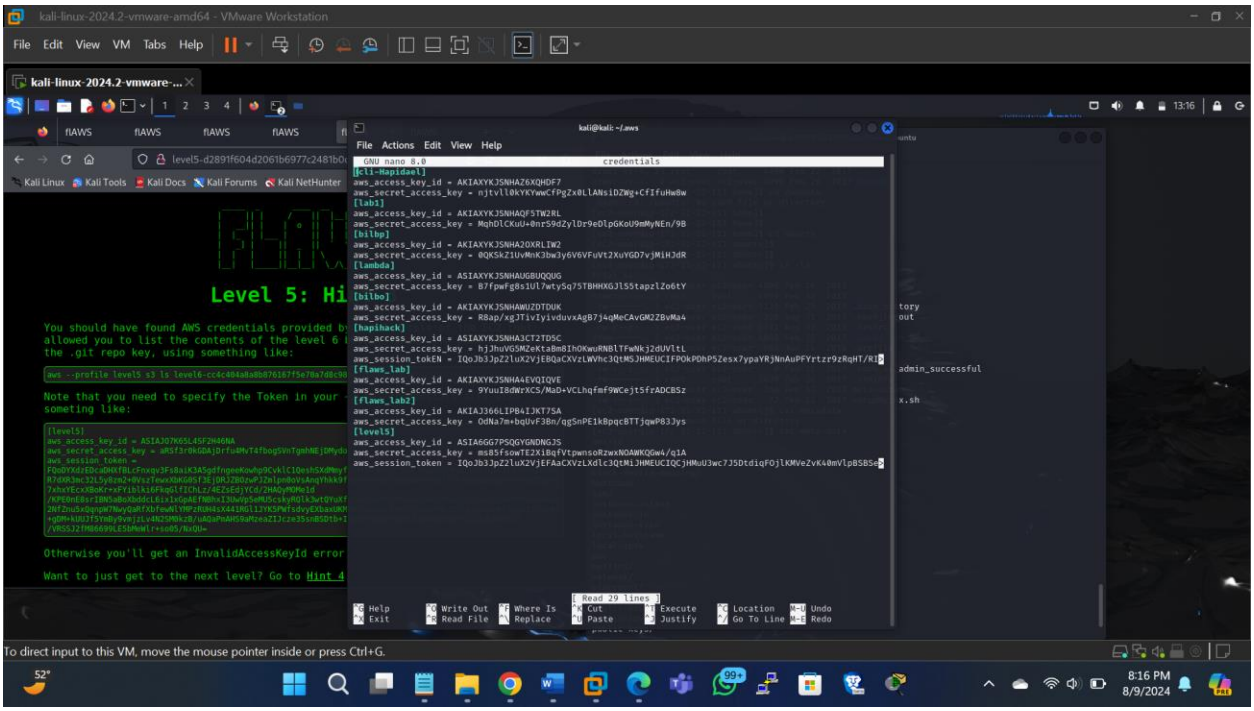








In the above I'll nano the credentials file to include the session token we obtained from the flaws directory in the level5 directory



Conclusion

The Flaws.cloud lab provides a practical and engaging way to learn about AWS security by simulating real-world vulnerabilities and attack scenarios. By completing each level, participants not only gain a deeper understanding of common cloud security issues but also learn how to implement best practices to protect against these vulnerabilities. The lab serves as a valuable resource for anyone looking to improve their cloud security skills, whether **they are beginners or experienced professionals. Through this hands-on approach, participants are better equipped to identify and mitigate security risks in their own cloud environments, making the Flaws.cloud lab an essential tool for anyone involved in cloud security.**