BISHOPFOX



MORE KEYS THAN THE JANITOR

HACKING EXPOSED AWS EBS VOLUMES

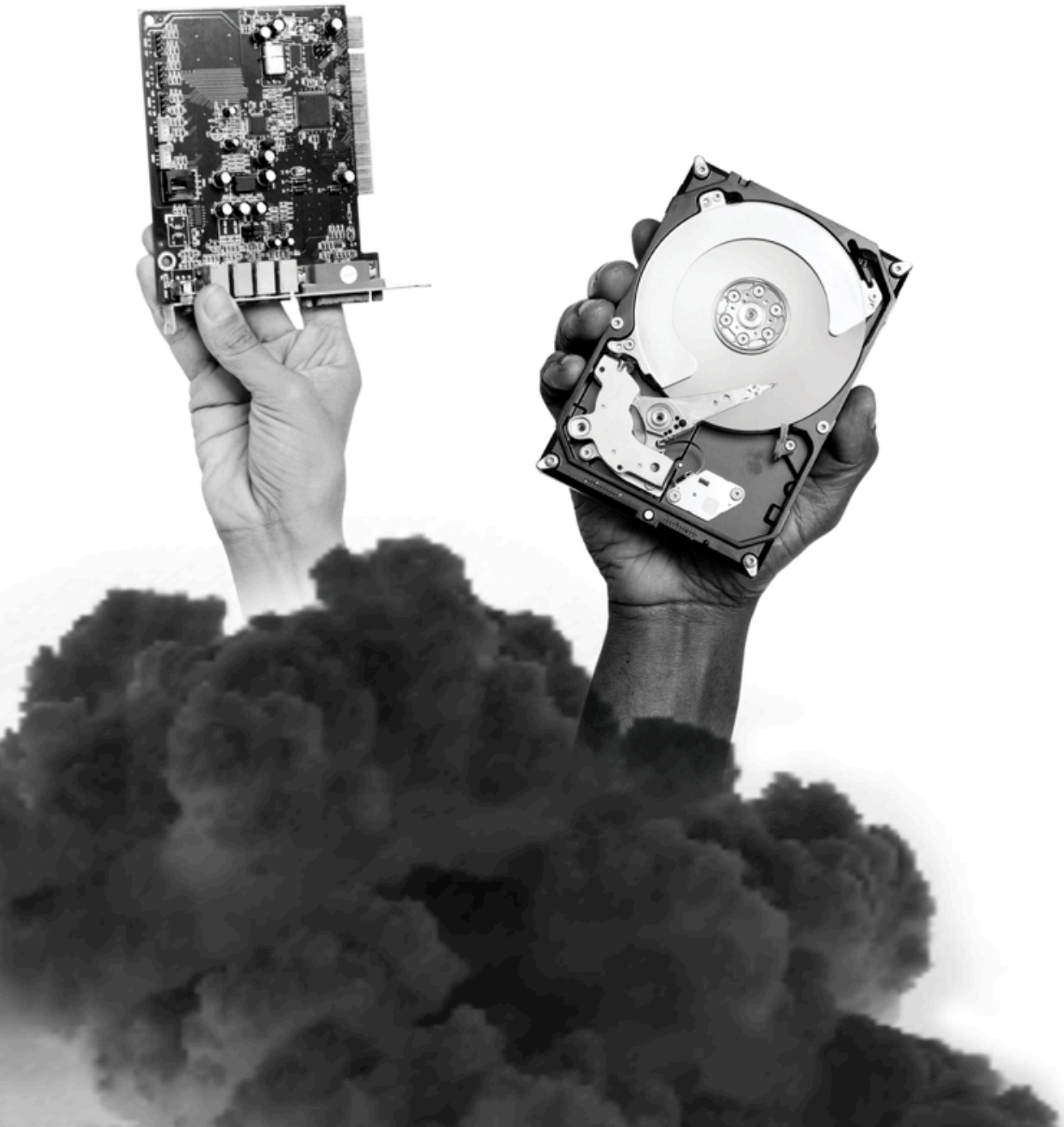
BY BEN MORRIS



Disclaimer

(Hello FBI)

- No post-exploitation was performed.
- Everything sensitive discussed in this talk was gathered from the EBS volumes themselves, which are publicly available.
- Metadata stored has been anonymized. I don't want your secrets, and I delete them after marking them as valid or expired.
- I'm releasing the tool in two weeks to give companies a chance to pull up their pants.



WHAT IS AWS EBS?

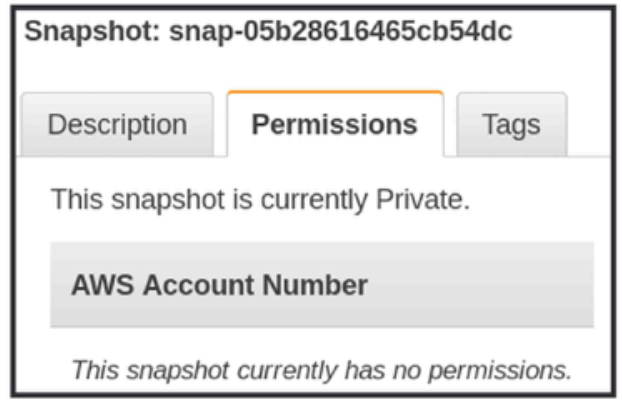
- Virtual hard disks in the cloud
- Usually private

amazon web services EBS | https://aws.amazon.com/ebs/

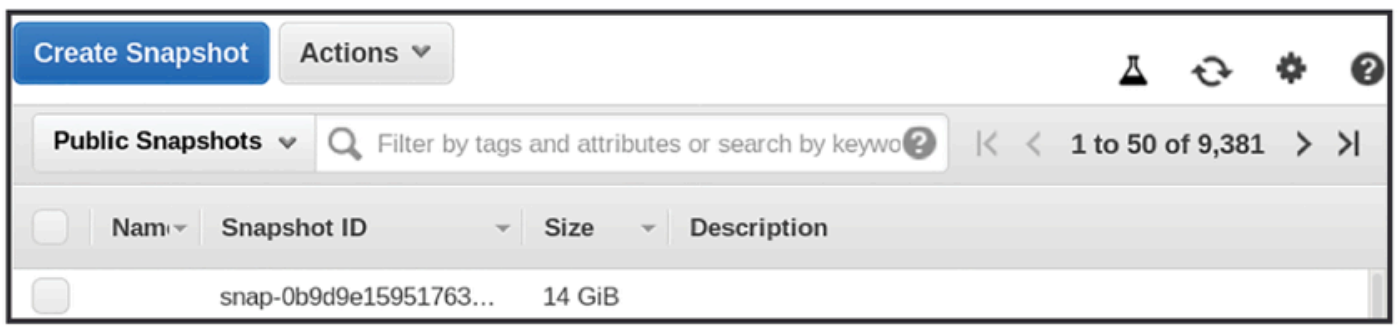


WHAT COULD POSSIBLY GO WRONG?

HOW CAN THIS HAPPEN?



AWS dashboard has a Permissions tab

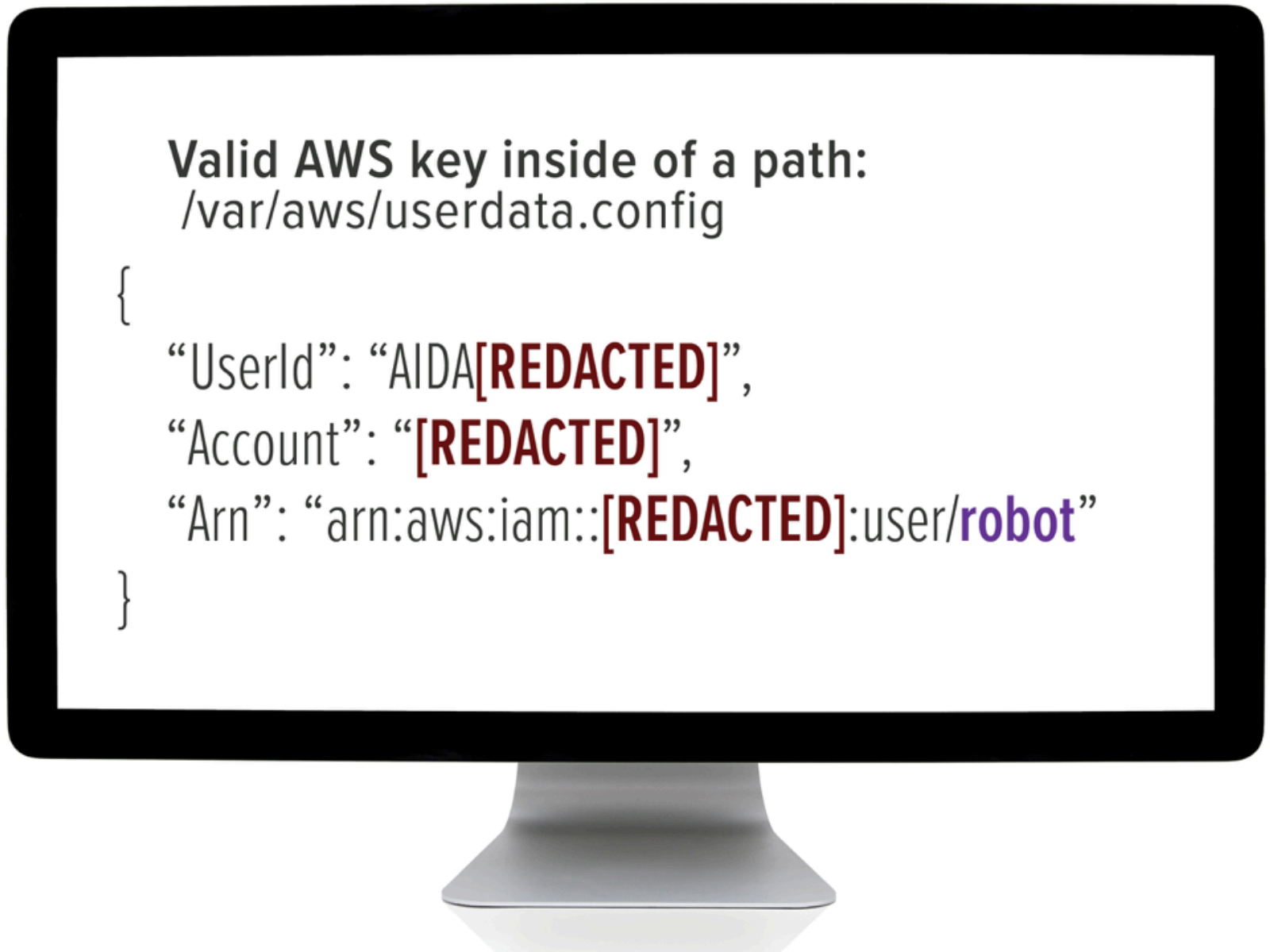


Once a volume's here, it's compromised

LOOT!



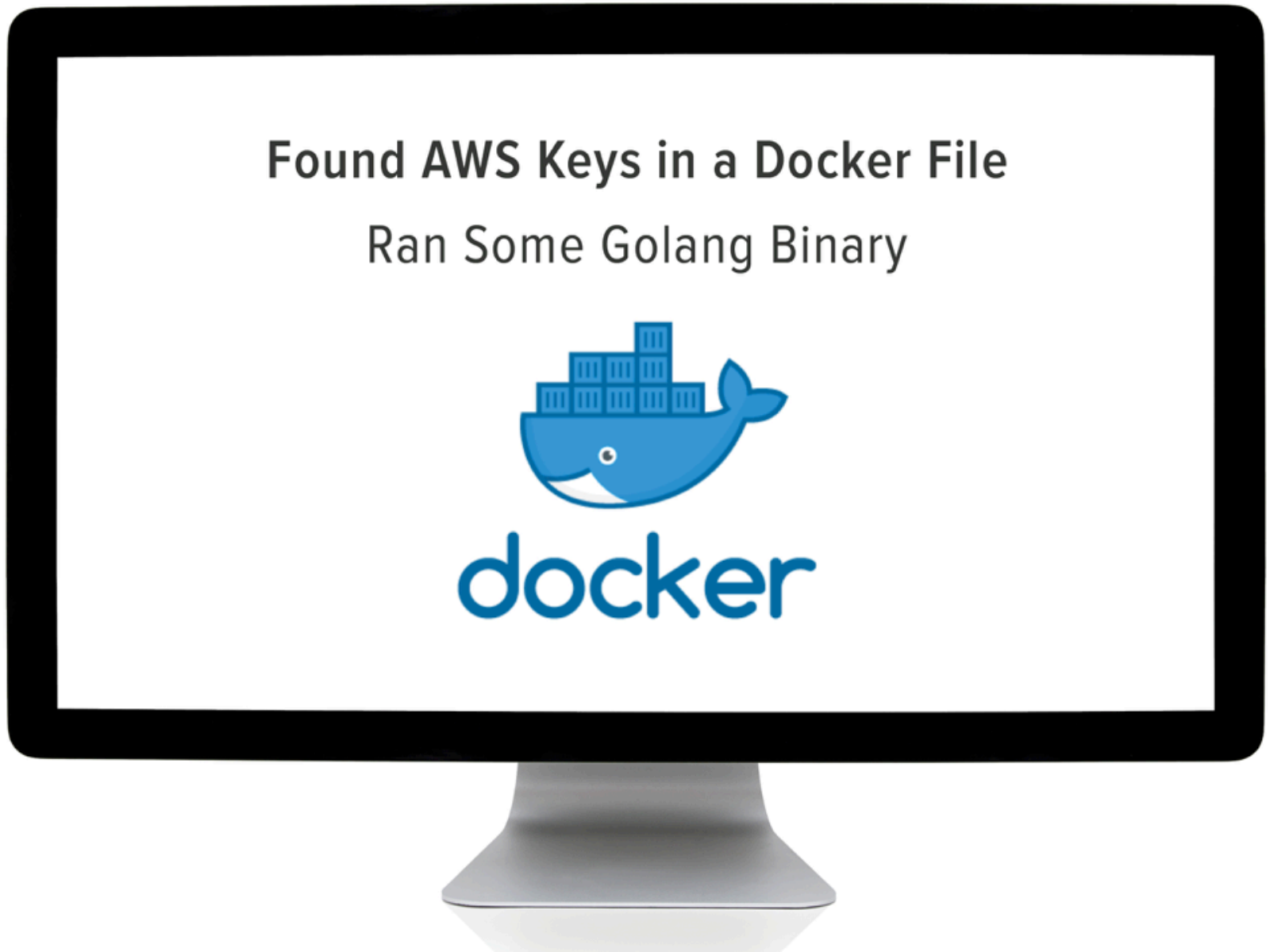
DISK A - I AM ROBOT



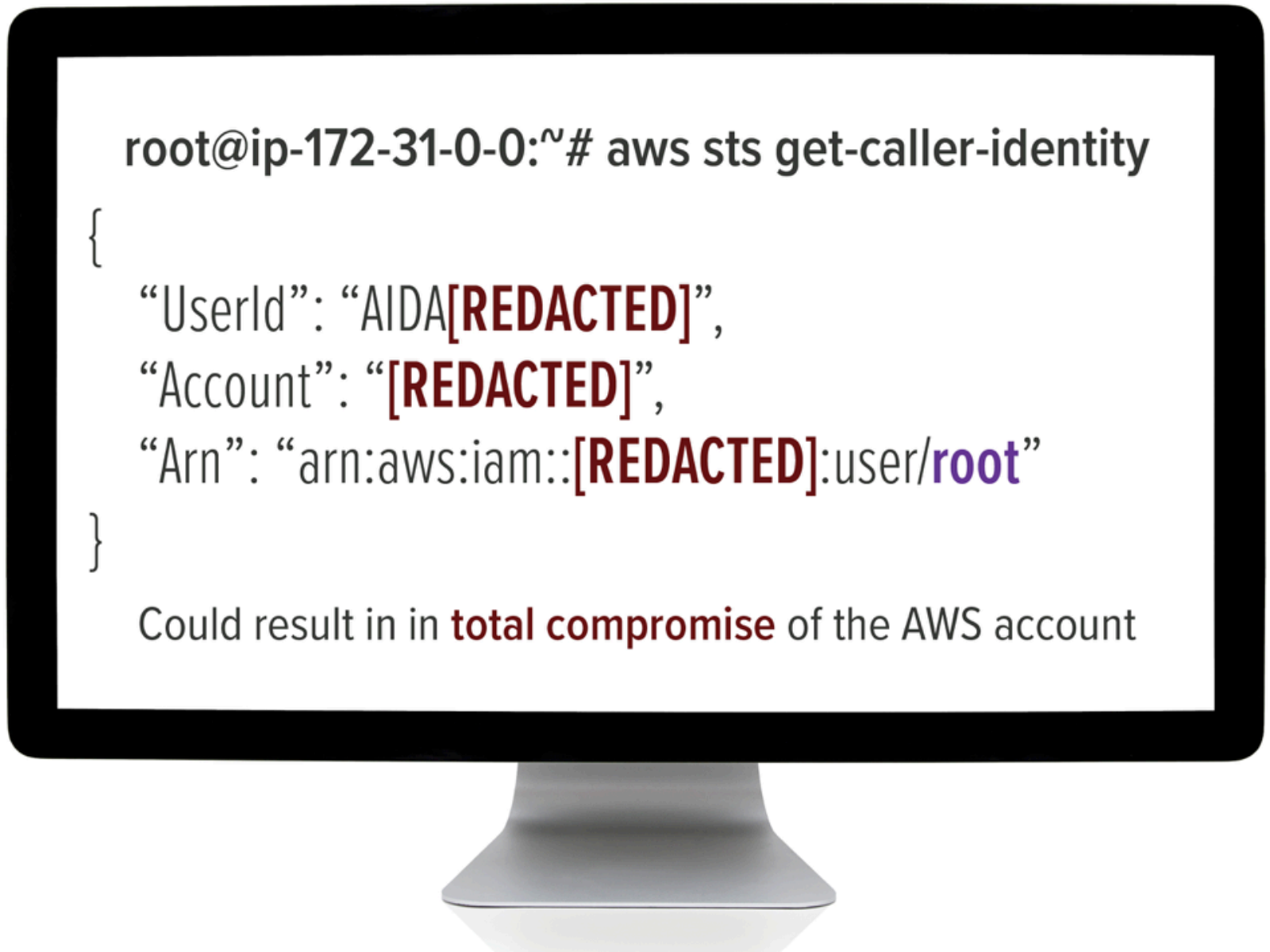
DISK A - I AM ROBOT



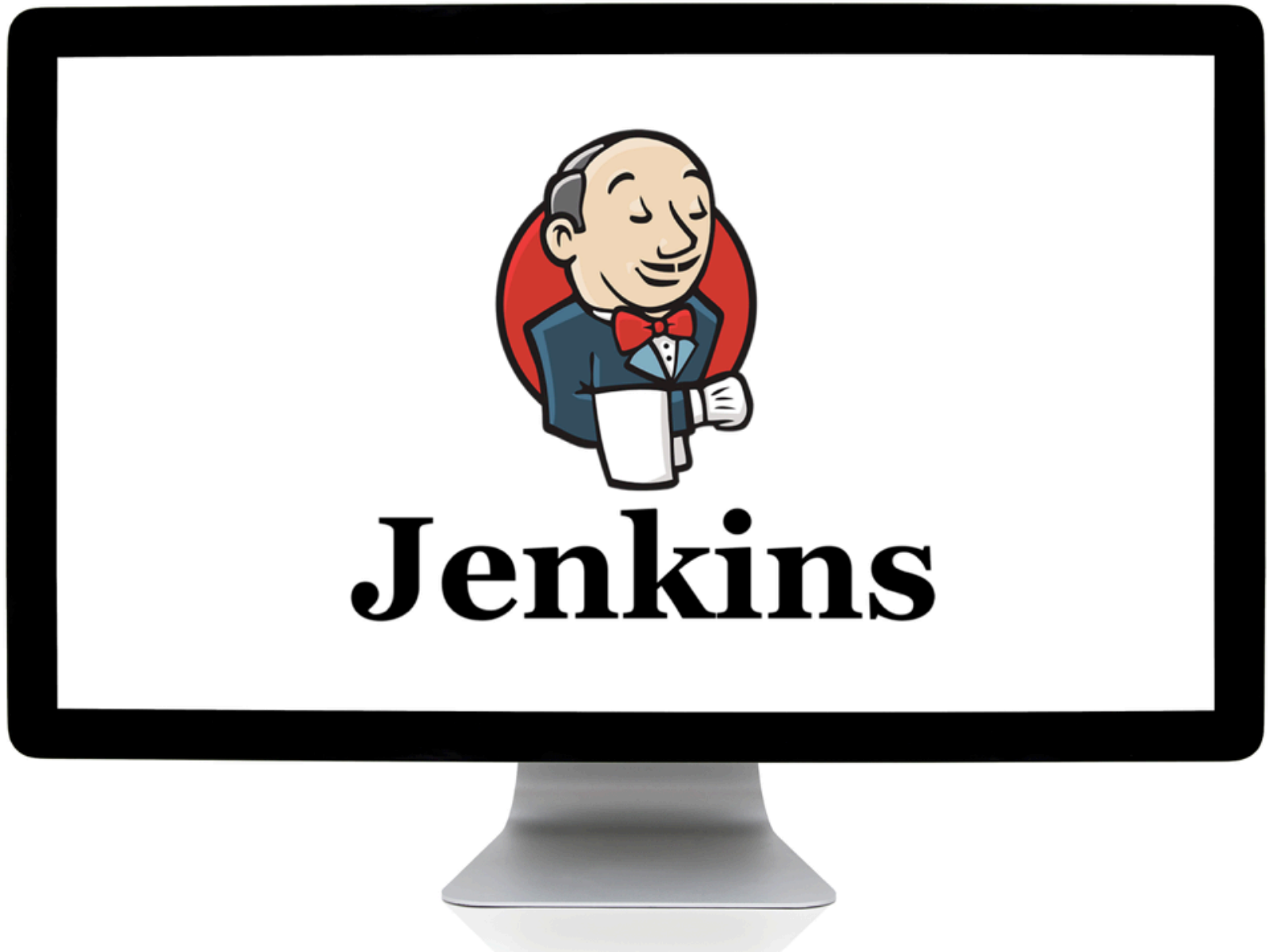
DISK B - w00t w00t



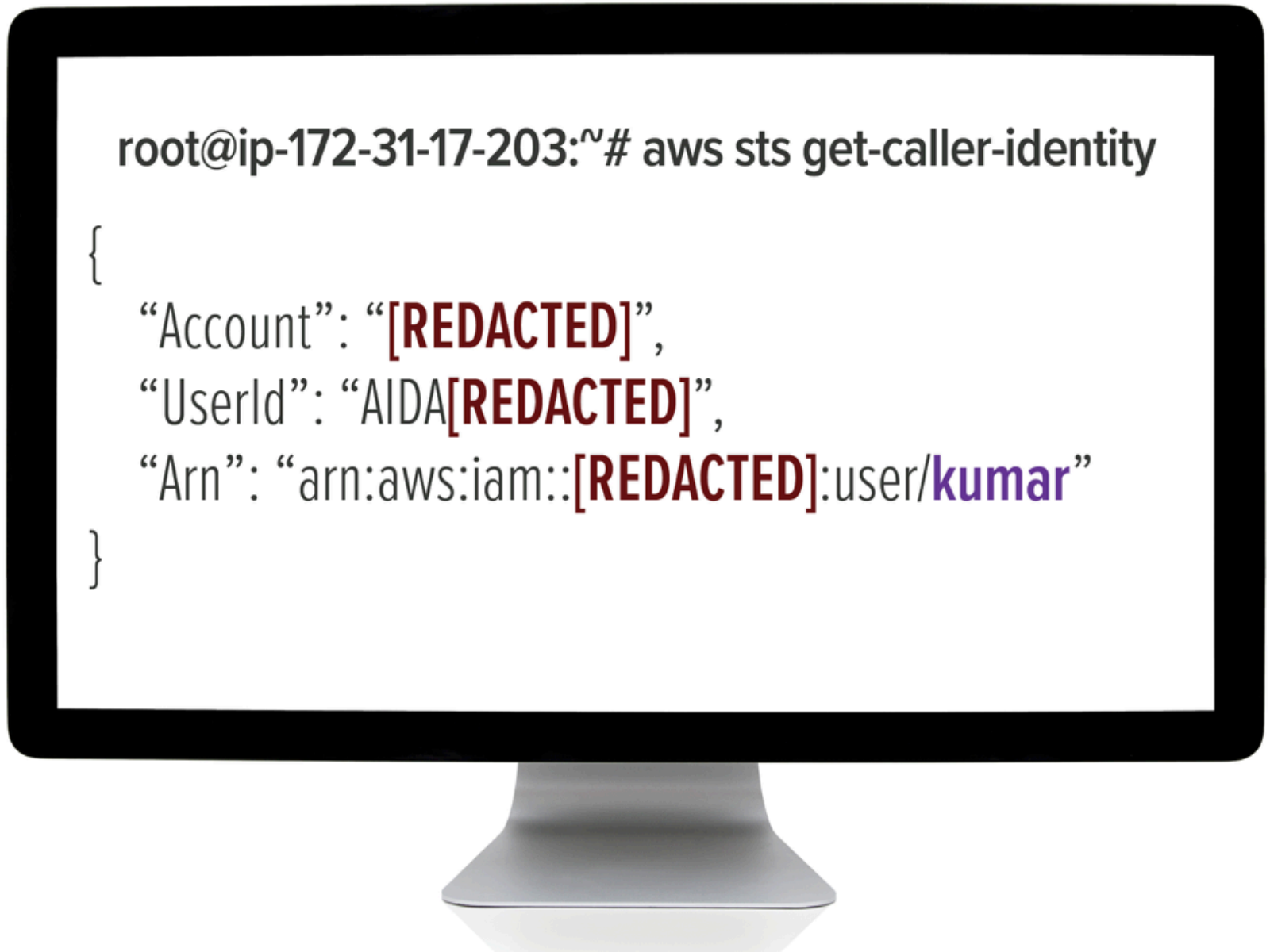
DISK B - w00t w00t



DISK C - HAROLD & BOTNET GO TO WHITE CASTLE



DISK C - HAROLD & BOTNET GO TO WHITE CASTLE



DISK C - HAROLD & BOTNET GO TO WHITE CASTLE



WALL OF SHEEP

- **Leaked Source Code:**
  - Government contractors
  - Large tech companies
- **SSH Private Keys**
  - Major businesses
  - IoT companies



- **PII (Emails and Passwords)**
  - SQL files containing tens of thousands of records, including email and hashed passwords
- **Wordpress Installations**
  - Password hashes, API tokens, etc.
- **VPN Creds**
  - OpenVPN connection files
- **AWS Keys, Google OAuth Tokens, Email Passwords**
  - Something called “SurveillanceApp”

HOW DID I FIND ALL THIS?

JUNK IN THE TRUNK

Exploitation process is simple on the surface

01: Pick an exposed snapshot

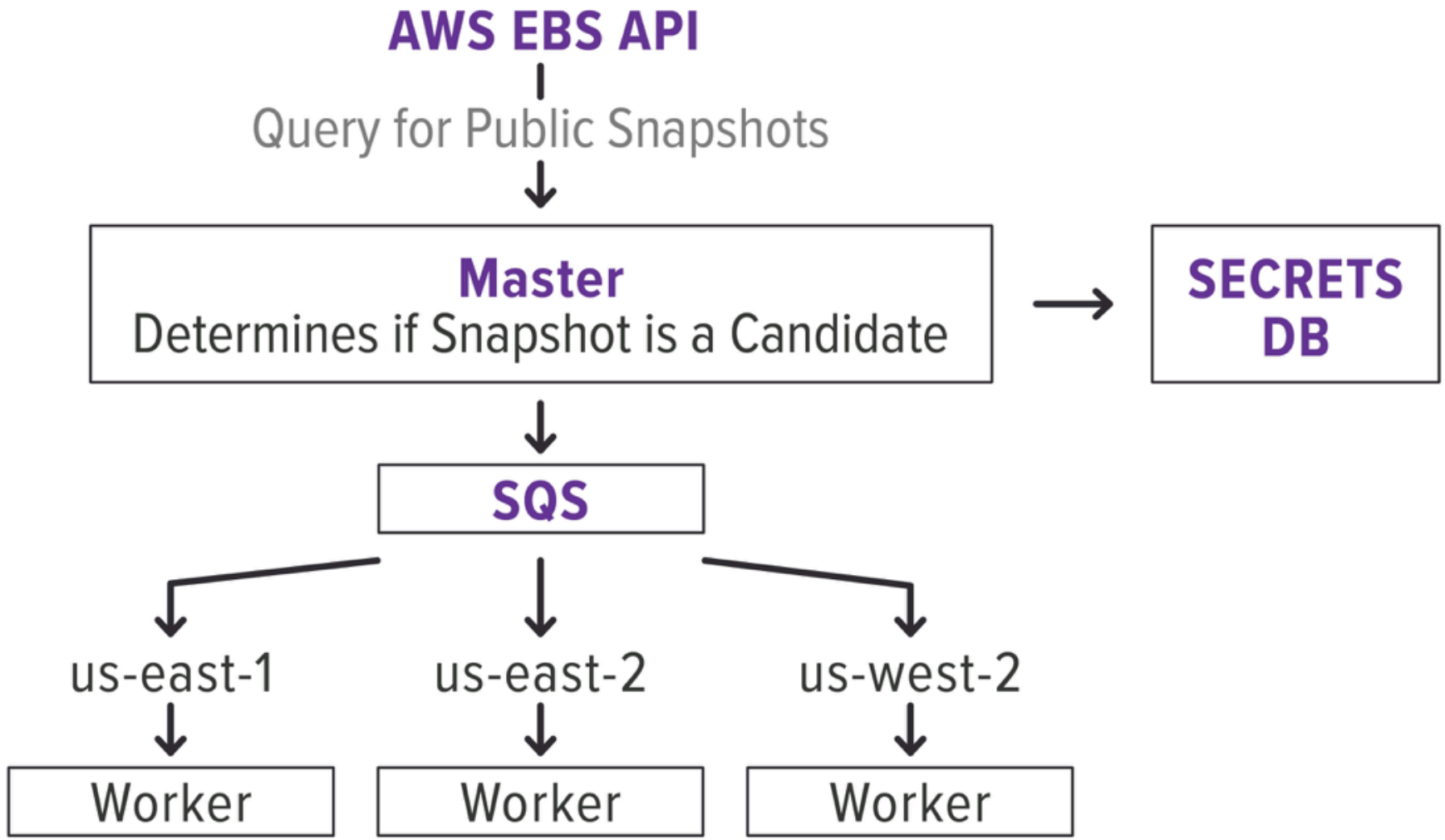
02: Attach the volume to your EC2 instance

03: Search the disk for secrets

...but there's just way too much data!



ARCHITECTURE



01
Pick an exposed snapshot

WHAT TO READ?



02

Attach the volume to your EC2 instance

THE “AWS BUTTERFLY EFFECT”



Tons of Hidden Failure Points

Metadata URL Failure

Mounting Disks

Filesystem Issues

03
Search the disk for secrets

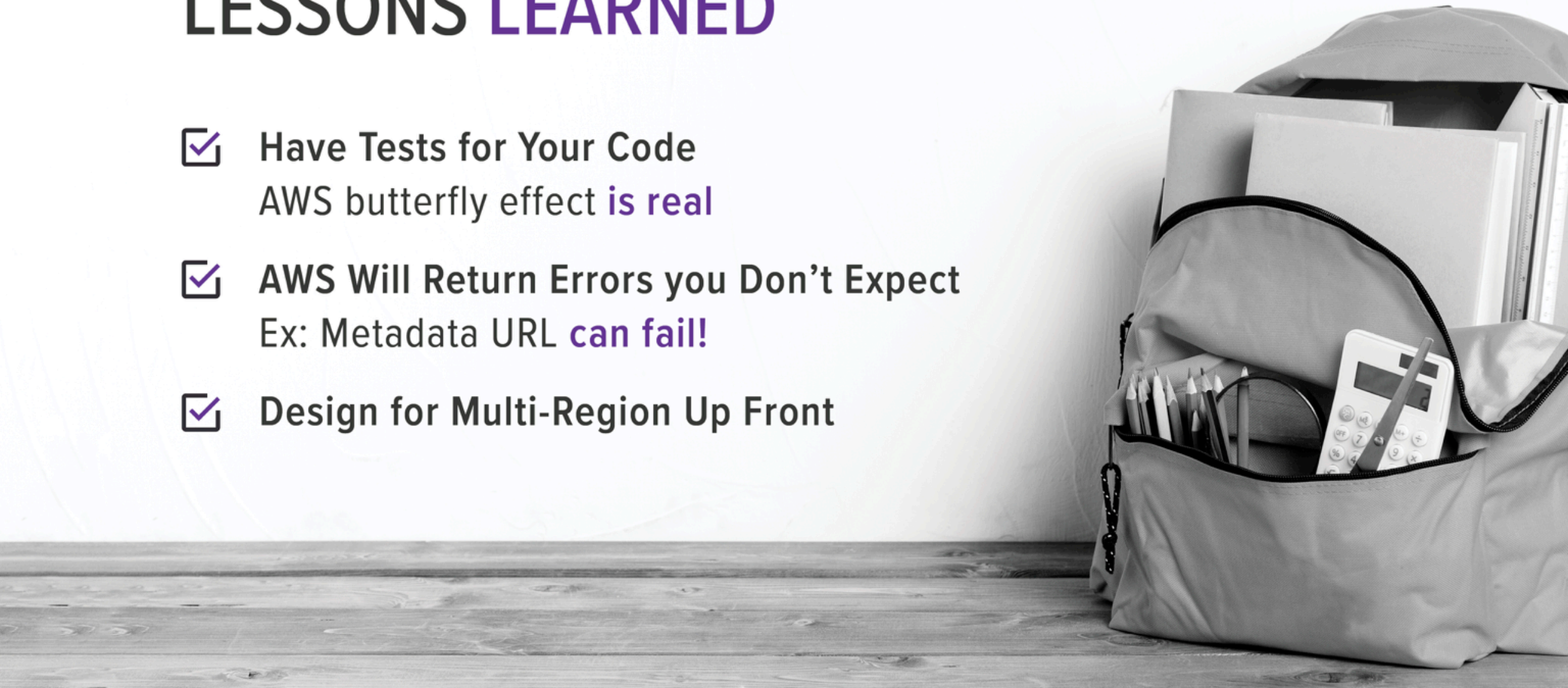
DLP DIGGITY



https://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/

LESSONS LEARNED

- **Have Tests for Your Code**
  AWS butterfly effect **is real**
- **AWS Will Return Errors you Don't Expect**
  Ex: Metadata URL **can fail!**
- **Design for Multi-Region Up Front**





REMEDIATION

EXPOSED DISK DISCOVERED

- If you find a disk that is:
  - **Unencrypted**
  - **Public**
  - Contains **sensitive information**
    01. Take down the snapshot
    02. Rotate any creds on it
    03. Investigate how you got here

Check your AWS environment:
https://github.com/bishopfox/dufflebag
"Coming Soon...in two weeks"



MORE LOOT

- **Passwords**
  - My favorite: nug!L0v3r
- **Captured the Flag**
  - root@ip-172-31-0-0:~# cat /mnt/snap-0489716372dc4b8c3/1/home/ec2-user/**.flag_here**
  - flag::**NSSCloudHackLabFLAG53::6a55505df2550fb680b1e0b23df42293fd099cf9ac5d7ae94ef0b938**
- **Bitcoin Miners**
  - wallet.dat
- **SSH Private Keys**
  - Lots of Windows disks





CONCLUSIONS

- **50 CONFIRMED EXPOSURES**
  Manually validated in one AWS region
- **~750-1,250 TOTAL EXPOSURES**
  Estimated across all AWS regions
- **WIDE-RANGING INDUSTRIES IMPACTED**
  Government contractors, software, healthcare, etc.

TOTAL COST:
$300 + R&D Time



THANK YOU!

SPECIAL THANKS TO

Dan Petro, Jake Miller, Cici Tran

Zach Glick at Amazon for the
great responsible disclosure process

(Hi Mom, Hi Dad, Hi Nick)

