

- Filename: intro-to-aws-pentesting-4-4-1-cloud-breach-s3.md
- Show Name: Intro to AWS Pentesting
- Topic Name: CloudGoat
- Episode Name: Cloud Breach S3

Cloud Breach S3

Objectives:

- Utilize aws pentesting tools, tactics, and procedures to solve the CloudGoat 'Cloud Breach S3' challenge
- Employ Pacu for enumeration
- Exploit reverse proxy server to gain access to EC2 Meta-Data Service for SSRF

-
- We're given just an IP
 - `nslookup 111.222.333.444`
 - Looks like an EC2 instance
 - If we don't have anything other than an IP where do we begin?
 - Let's scan it with nmap
 - Port 80 open
 - Run script/version scan on port 80
 - We definitely have a web server
 - OK, so we have a web server. What do we do now?
 - Let's check it out
 - No landing page
 - Check robots.txt
 - Message: proxy through EC2 Metadata Service
 - We've seen this before, but how to we work with the Metadata service here?
 - Verbose message
 - Let's use Burp Suite
 - Yay, we found keys
 - New Keys, new profile, what now?
 - Let's use Pacu
 - Attempt to enumerate
 - IAM
 - EC2
 - S3
 - Looks like we can view buckets
 - Is that Credit Card Data?
 - We call that a data breach
 - This will definitely make the findings page of your pentest report