RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: CSV-R12

RED TEAM VS. BLUE TEAM ON AWS

Teri Radichel

CEO
2nd Sight Lab
@teriradichel

Kolby Allen

DevOps Engineer
Zipwhip
@kolbyallen

Attacker vs. Defender

Cloud Admin…Duh Duh Duh.

Would Be A Boring Talk…

GAME OVER

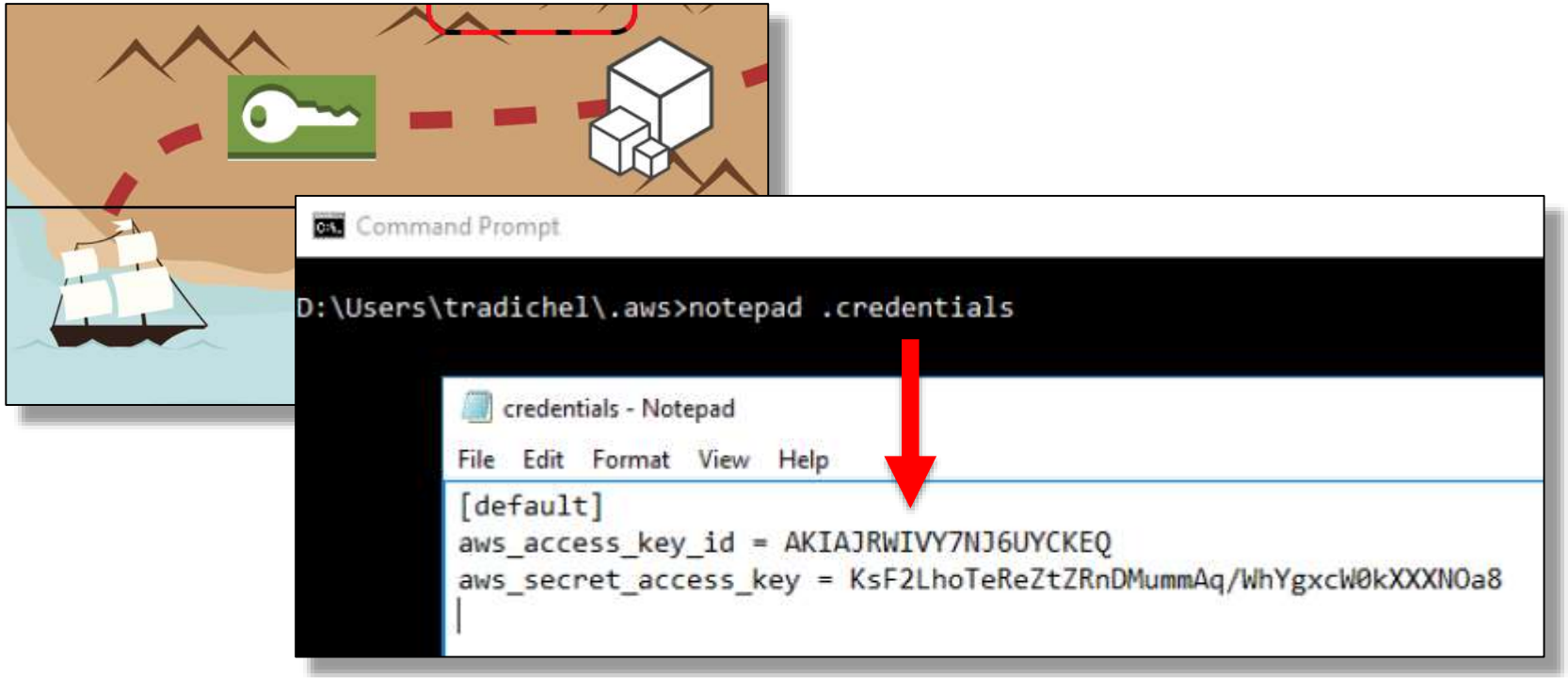
Instead…

Let's search for buried treasure!

Some background

- Initial Setup
  - Vanilla Account
    - Single Admin User
    - Base VPC & defaults
  - AWS Tutorial: Elastic Beanstalk with WordPress
    - https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/php-hawordpress-tutorial.html
  - AWS Tutorial: Lambda Accessing RDS in VPC
    - https://docs.aws.amazon.com/lambda/latest/dg/vpc.html

Pilfer Credentials ~ Read Only Access



Look for RDS Databases

aws rds describe-db-instances --filter --query DBInstances[].[DBInstanceIdentifier,MasterUsername,DBSubnetGroup.VpcId,Endpoint.Address] --output=table --color off

supersecretdb?! That sounds like a good target…

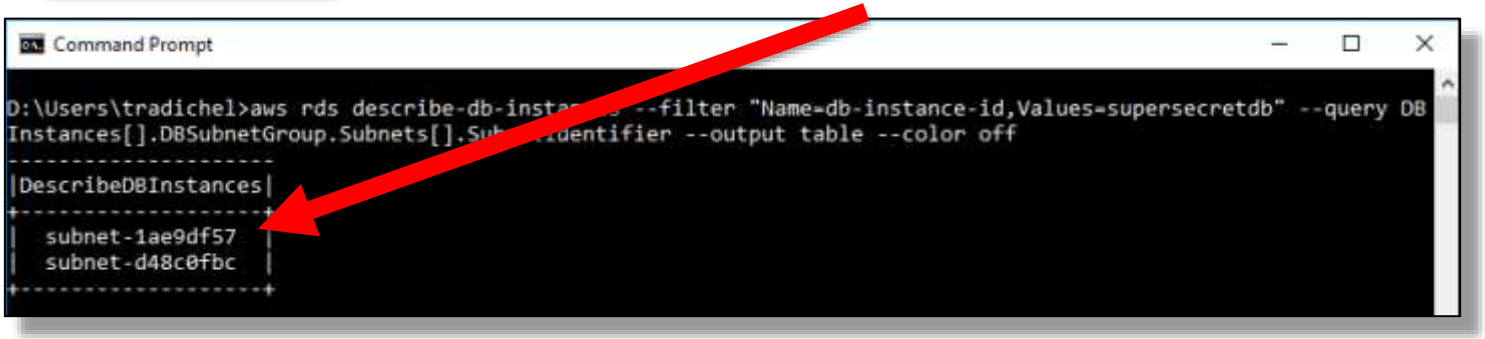
Command Prompt

```
D:\Users\tradichel>aws rds describe-db-instances --filter --query DBInstances[].[DBInstanceIdentifier,MasterUsername,DBSubnetGroup.VpcId,Endpoint.Address] --output=table --color off
-----------------------------------------------------------------------------------------------------------------------
|                                                   DescribeDBInstances                                                |
+-----------------+----------------+--------------+-------------------------------------------------------------+
|  aa1fe08ildto0z5|  wordpresstest |  vpc-96c34cfe|  aa1fe08ildto0z5.c15fcy9momq1.us-east-2.rds.amazonaws.com   |
|  supersecretdb  |  kolbyadmin    |  vpc-96c34cfe|  supersecretdb.c15fcy9momq1.us-east-2.rds.amazonaws.com     |
+-----------------+----------------+--------------+-------------------------------------------------------------+
```

Examine Selected Database Subnets

aws rds describe-db-instances --filter "Name=db-instance-id,Values=supersecretdb" --query DBInstances[].DBSubnetGroup.Subnets[].SubnetIdentifier --output table --color off

Hmm… let's check out: subnet-1ae9df57



What Traffic Do NACLs Allow?

aws ec2 describe-network-acls --filter "Name=association.subnet-id,Values=subnet-1ae9df57" --query NetworkAcls[].Entries --output table --color off

All traffic allowed ~ Sweet.

Command Prompt

```
D:\Users\tradichel>aws ec2 describe-network-acls --filter "Name=association.subnet-id,Values=subnet-1ae9df57" --query Ne
tworkAcls[].Entries --output table --color off
-----------------------------------------------------------------
|                      DescribeNetworkAcls                      |
+-----------+---------+-----------+-------------+--------------+
| CidrBlock | Egress  | Protocol  | RuleAction  | RuleNumber   |
+-----------+---------+-----------+-------------+--------------+
|  0.0.0.0/0|  True   |  -1       |  allow      |  100         |
|  0.0.0.0/0|  True   |  -1       |  deny       |  32767       |
|  0.0.0.0/0|  False  |  -1       |  allow      |  100         |
|  0.0.0.0/0|  False  |  -1       |  deny       |  32767       |
+-----------+---------+-----------+-------------+--------------+
```

What Traffic Do DB Security Groups Allow?

Command Prompt

```
-----------------------------------------------------------------------------------
|                            DescribeSecurityGroups                               |
+---------------------------------------------------------------------------------+
||                                SecurityGroups                                 ||
|+-------------+-------------------------------------------------------------------+|
||  Description|  Created from the RDS Management Console: 2018/03/22 05:26:10    ||
||  GroupId    |  sg-217f3e4a                                                      ||
||  GroupName  |  rds-launch-wizard-1                                              ||
||  OwnerId    |  310610724838                                                     ||
||  VpcId      |  vpc-96c34cfe                                                     ||
|+-------------+-------------------------------------------------------------------+|
|||                              IpPermissions                                  |||
||+-----------------------------------------------+---------------------------+||
|||  FromPort                                     |  3306                     |||
|||  IpProtocol                                   |  tcp                      |||
|||  ToPort                                       |  3306                     |||
||+-----------------------------------------------+---------------------------+||
||||                               IpRanges                                    ||||
|||+---------------------------+-------------------------------------------------+|||
||||  CidrIp                   |  172.31.0.0/16                                  ||||
|||+---------------------------+-------------------------------------------------+|||
|||                            IpPermissionsEgress                              |||
||+-----------------------------------------------+---------------------------+||
|||  IpProtocol                                   |  -1                       |||
||+-----------------------------------------------+---------------------------+||
||||                               IpRanges                                    ||||
|||+-----------------------------+-----------------------------------------------+|||
||||  CidrIp                     |  0.0.0.0/0                                    ||||
|||+-----------------------------+-----------------------------------------------+|||
```

aws ec2 describe-security-groups --filter "Name=group-id,Values=sg-217f3e4a" --output table --color off

Port 3306

172.31.0.0/16

Find VPC With Access to Database

aws ec2 describe-vpcs --filter "Name=cidrBlock,Values=172.31.0.0/16" --query Vpcs[].VpcId --output table --color off

vpc-96c34cfe is assigned to CIDR 172.31.0.0/16

Command Prompt

```
D:\Users\radichel>aws ec2 describe-vpcs --filter "Name=cidrBlock,Values=172.31.0.0/16" --query Vpcs[].VpcId --output ta
ble --color off
-----------------
|  DescribeVpcs  |
+----------------+
|  vpc-96c34cfe  |
+----------------+
```

VPC Security Groups ~ 3306 Egress

aws ec2 describe-security-groups --filter "Name=egress.ip-permission.to-port,Values=3306 Name=vpc-id,Values=vpc-96c34cfe" --output table --color off

None…hmm…

Command Prompt

```
D:\Users\tradichel\.aws>aws ec2 describe-security-groups --filter "Name=egress.ip-permission.to-port,Values=3306 Name=vp
c-id,Values=vpc-96c34cfe" --output table --color off
------------------------
|DescribeSecurityGroups|
+----------------------+
```

Security Groups ~ No Outbound Restrictions

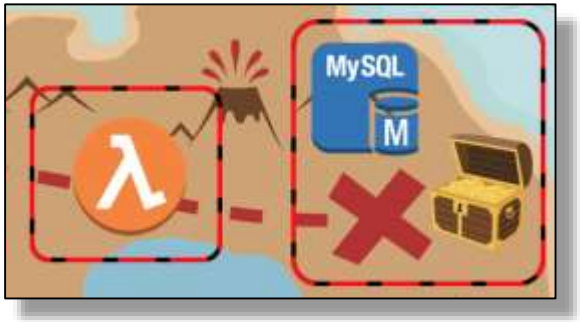
aws ec2 describe-security-groups --filter "Name=egress.ip-permission.cidr,Values='0.0.0.0/0',Name=vpc-id,Values=vpc-96c34cfe" --output table --color off --query SecurityGroups[].GroupId

Command Prompt

```
D:\Users\tradichel\.aws>aws ec2 describe-security-groups --filter "Name=egress.ip-permission.cidr,Values='0.0.0.0/0',Nam
e=vpc-id,Values=vpc-96c34cfe" --output table --color off --query SecurityGroups[].GroupId
------------------------
|DescribeSecurityGroups|
+----------------------+
|  sg-217f3e4a         |
|  sg-3984c552         |
|  sg-8db2c2e6         |
|  sg-91b5c5fa         |
|  sg-93aadef8         |
|  sg-a0b9c9cb         |
|  sg-a9bbcbc2         |
|  sg-b1bacada         |
|  sg-b97b3ad2         |
+----------------------+
```

Cool. Wide Open Outbound.
Let's see what's using these.

Check Lambda Functions



aws lambda list-functions --query Functions[?VpcConfig.SecurityGroupIds==[`sg-93aadef8`]].FunctionName --output table --color off

Command Prompt

```
D:\Users\tradichel\.aws>aws lambda list-functions --query Functions[?VpcConfig.SecurityGroupIds==[`sg-93aadef8`]].Functi
onName --output table --color off
----------------------------------------
|              ListFunctions           |
+--------------------------------------+
|  CreateTableAddRecordsAndRead        |
+--------------------------------------+
```

Query Lambda Code Location

aws lambda get-function --function-name CreateTableAddRecordsAndRead --query Code.Location

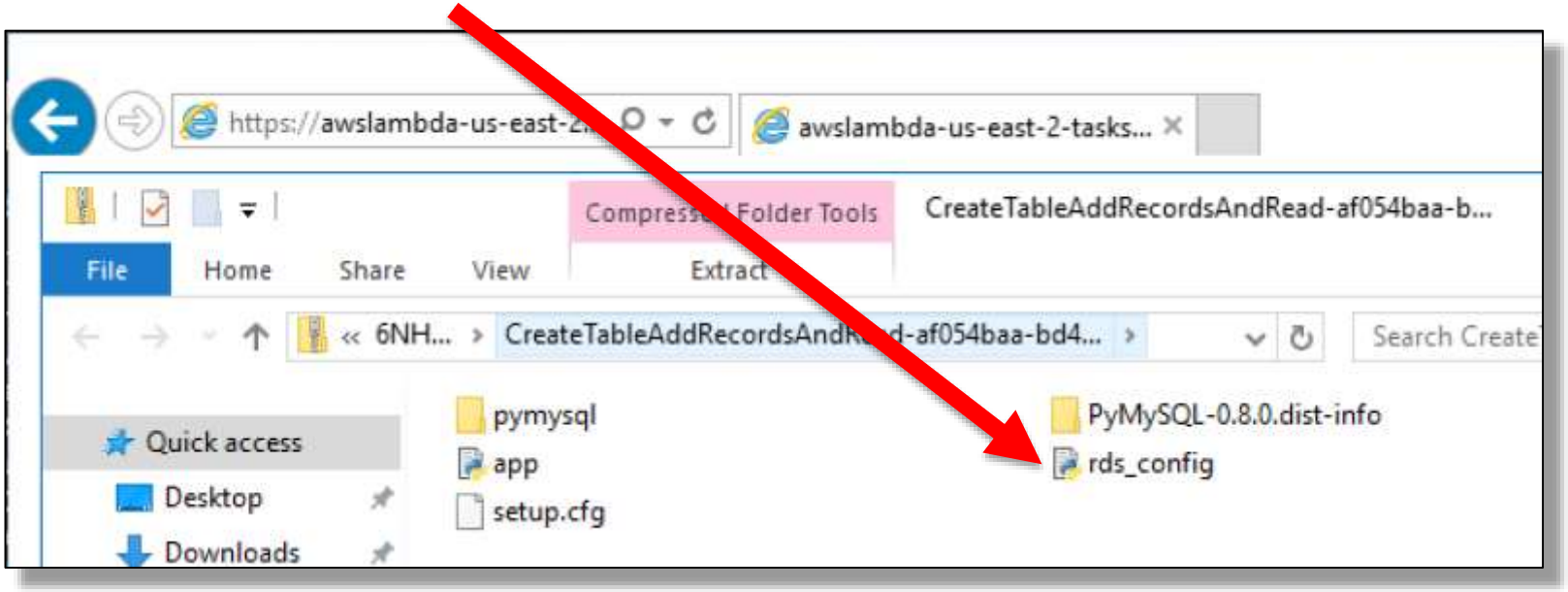
Gives us URL to code location in S3…

Command Prompt

```
D:\Users\tradichel\.aws>aws lambda get-function --function-name CreateTableAddRecordsAndRead --query Code.Location
"https://awslambda-us-east-2-tasks.s3.us-east-2.amazonaws.com/snapshots/310610724838/CreateTableAddRecordsAndRead-af054b
aa-bd47-414d-bd56-54ed119cd6f8?versionId=jBCcttupPkmmceMPTJn_c3RgrsJnGn6r&X-Amz-Security-Token=FQoDYXdzECQaDPOQBfxx1bL3a
fb5mSK3A%2BqmipS5sGqJzxXZwQg1w9DRVrt2bY9GbgxT9D73PydpgXo4GR6uaQjdHRQmxnU%2F27fDQ9KvTjVLKoGPEGoayleVkzgZpPVVevo4OvO4gZ3S5
C8exKeqLFUi5NPSfjuOLID%2BdZJxvE60qoB2XWWs1gM8wuyZgNP26Yb4pdHqObXVxXxbnigZwo0GOmlrVIvQWZH%2FgymxPQN22DG%2F1sY%2FeUA3mhKOE
UqgEzor0iMMMa3vkZFV2bdrWjcSutTt5XtFFmKSNwWAdnO%2Bslj28jp9Sca50D3o58o%2F%2FLpRq8gvP82WxmbzYjnX9yVGwMqjfxQyK%2FDt%2BUiY3J4
VM%2B4B6PF4oXEA0Mkxjhh6SXBqZS8ma2hAmkQUI%2FCSHb21EWbbzS9MYEVLrDvDQBzyhqvWx%2FlR%2B1jZ7TaD3BdO8WWEo8JxR8i%2BDuRCjq2yTkLBL
WCULUzr6ybChufIfRHSTNdl5ikMdEwXRO4CWQuSi1i61QHVYQKhhDMEmeOEFsLAkCMk0ACmf9adrG0Iz5W5L2PWBxQ7DLjcQ3Nu3xpyFxMETVvNuU1%2BrMn
1YTCgvQnQiKwOpbvzgbi%2BLypFjvwo%2F9vR1QU%3D&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20180323T043812Z&X-Amz-SignedHea
ders=host&X-Amz-Expires=600&X-Amz-Credential=ASIAI6UZQFNPGFJYM4XA%2F20180323%2Fus-east-2%2Fs3%2Faws4_request&X-Amz-Signa
ture=a322f24da64b08be598484198eb75da5b761c3f629e909503d4b03c213aa4ba5"
```

Go To URL…Check out the code

Hmm, what's in this file?



About that rds_config file…

Oops. Database credentials.

rds_config - Notepad

File Edit Format View Help

```
db_username = "lambdauser"db_password = "@ccess!1"db_name = "supersecretdb"
```

Look for Instances That Can Exfil

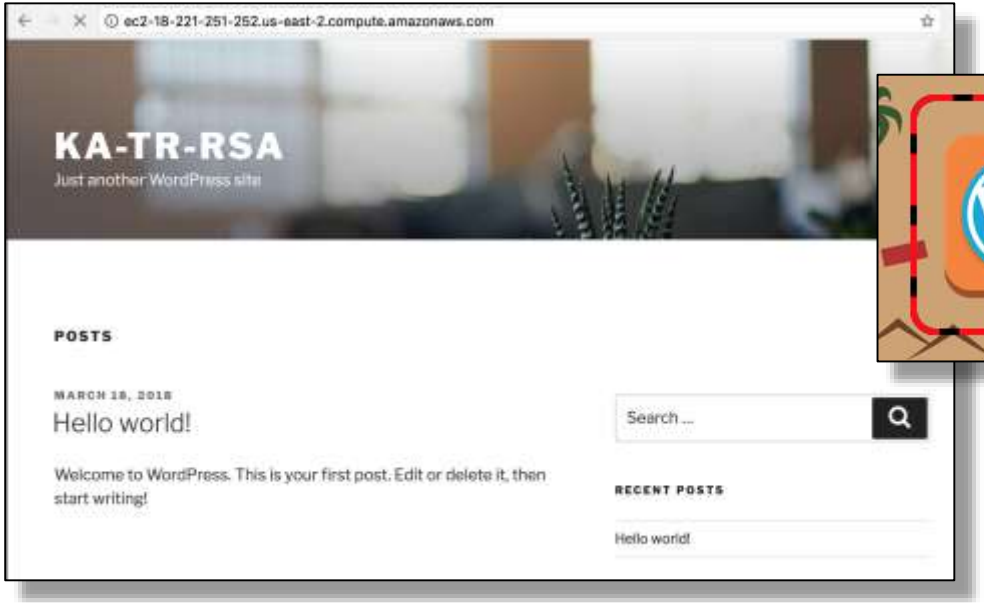
aws ec2 describe-instances --output text --query Reservations[].Instances[].NetworkInterfaces[]. Association.[PublicIp,PublicDnsName]

Check the domains in a browser to find web sites.

Command Prompt

```
D:\Users\tradichel\.aws>aws ec2 describe-instances --output text --query Reservations[].Instances[].NetworkInterfaces[].
Association.[PublicIp,PublicDnsName]
18.188.35.35     ec2-18-188-35-35.us-east-2.compute.amazonaws.com
18.221.251.252   ec2-18-221-251-252.us-east-2.compute.amazonaws.com
```

Exploit Web Site and Exfil



Scan Site. Exploit Vulnerability.
Upload code to connect to DB.
Publish to public web site.

IAM Best Practices

- Roles
- Least Privilege
- Segregation of Duties
- IAM Top 10

Protecting Credentials

- User training ~ Phishing and handling of credentials
- Password policies and rotation
- MFA!!
- Require frequent re-auth – especially to sensitive apps
- Prevent deployment of code with embedded credentials
  https://github.com/awslabs/git-secrets

IAM Configuration

WOW THAT IS A LOT OF YAML!!

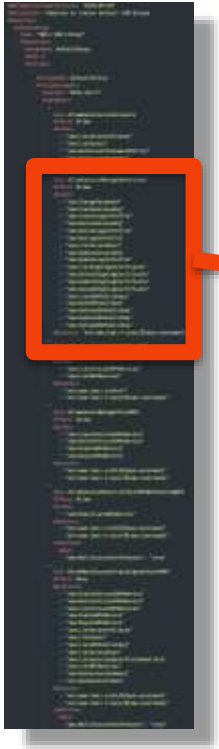
https://github.com/allenk1/2018rsapresentation/blob/master/Default-IAM-Profile.yaml

IAM Master - Initial Roles

```yaml
Sid: AllowUserstoListAccounts
Effect: Allow
Action:
- "iam:ListAccountAliases"
- "iam:ListUsers"
- "iam:GetAccountPasswordPolicy"
- "iam:GetAccountSummary"
Resource: "*"
```

- Allows users to view enough information to get into IAM
- Can get the PW Policy ←IMPORTANT so it can apply
- List Users – needed in order to find themselves

IAM Master - Initial Roles



```
Sid: AllowUserstoManageOwnAccount
Effect: Allow
Action:
- "iam:ChangePassword"
- "iam:CreateAccessKey"
- "iam:CreateLoginProfile"
- "iam:DeleteAccessKey"
- "iam:DeleteLoginProfile"
- "iam:GetLoginProfile"
- "iam:ListAccessKeys"
- "iam:UpdateAccessKey"
- "iam:UpdateLoginProfile"
- "iam:ListSigningCertificates"
- "iam:DeleteSigningCertificate"
- "iam:UpdateSigningCertificate"
- "iam:UploadSigningCertificate"
- "iam:ListSSHPublicKeys"
- "iam:GetSSHPublicKey"
- "iam:DeleteSSHPublicKey"
- "iam:UpdateSSHPublicKey"
- "iam:UploadSSHPublicKey"
Resource: "arn:aws:iam::*:user/${aws:username}"
```

Actions allow users to manage their account – BUT NOT PERMISSIONS

Resource only allows them to perform on their username – can't modify anyone else

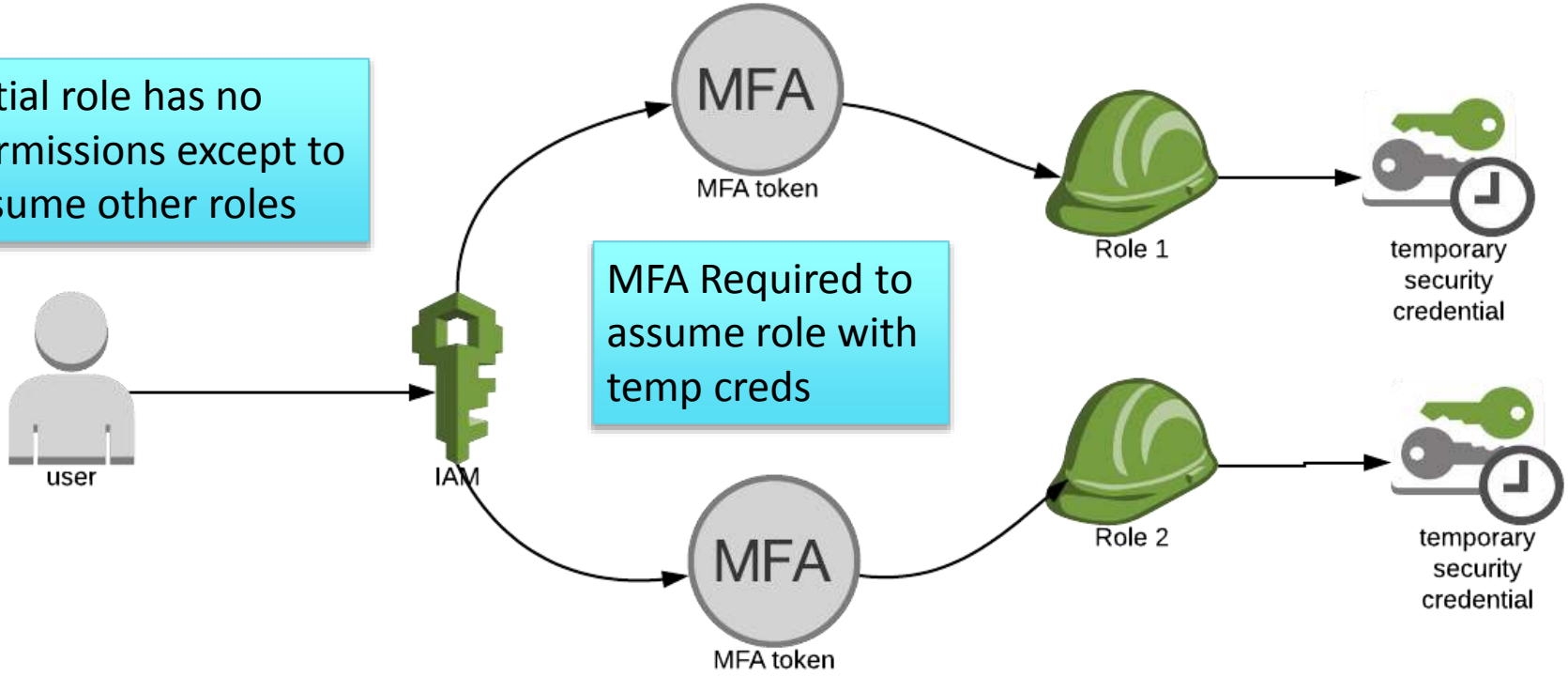
IAM ~ User Roles

```
Sid: AllowUserstoListOnlyThierMFA
Effect: Allow
Action:
- "iam:ListVirtualMFADevices"
- "iam:ListMFADevices"
Resource:
- "arn:aws:iam::*:mfa/*"
- "arn:aws:iam::*:user/${aws:username}"
-
Sid: AllowUsertoManageThierMFA
Effect: Allow
Action:
- "iam:CreateVirtualMFADevice"
- "iam:DeleteVirtualMFADevice"
- "iam:EnableMFADevice"
- "iam:ResyncMFADevice"
Resource:
- "arn:aws:iam::*:mfa/${aws:username}"
- "arn:aws:iam::*:user/${aws:username}"
-
Sid: AllowUserstoDeactiveTheirMFAWhenUseingMFA
Effect: Allow
Action:
- "iam:DeactivateMFADevice"
Resource:
- "arn:aws:iam::*:mfa/${aws:username}"
- "arn:aws:iam::*:user/${aws:username}"
Condition:
Bool:
"aws:MultiFactorAuthPresent": "true"
```

- Allows users to manage this MFA
- Must login with MFA to remove device

IAM ~ Assumed Roles

Initial role has no permissions except to assume other roles



IAM Master


```
1. – (fish)
➜  aws rds describe-db-instances --query DBInstances[].DBInstanceIdentifier --output=text --region us-east-2

An error occurred (AccessDenied) when calling the DescribeDBInstances operation: User: arn:aws:iam::310610724838:user/secu
re-readonly is not authorized to perform: rds:DescribeDBInstances
1 ➜  aws sts assume-role --role-arn "arn:aws:iam::310610724838:role/Secure-ReadOnly-Role" --role-session-name "rsa" --
serial-number "arn:aws:iam::310610724838:mfa/secure-readonly" --token-code "695733"
{
    "Credentials": {
        "AccessKeyId": "[redacted]",
        "SecretAccessKey": "[redacted]"
        "SessionToken": "[redacted]
[redacted]
        "Expiration": "2018-03-23T01:51:21Z"
    },
    "AssumedRoleUser": {
        "AssumedRoleId": "[redacted]",
        "Arn": "arn:aws:sts::310610724838:assumed-role/Secure-ReadOnly-Role/rsa"
    }
}
➜  export AWS_ACCESS_KEY_ID=[redacted]; export AWS_SECRET_ACCESS_KEY=[redacted]
 export AWS_SESSION_TOKEN=[redacted]
[redacted]
➜  aws rds describe-db-instances --query DBInstances[].DBInstanceIdentifier --output=text --region us-east-2
aaife0illdto025 supersecretdb
➜  ⬚                                                                                    (docker-for-desktop)
– (fish)
```

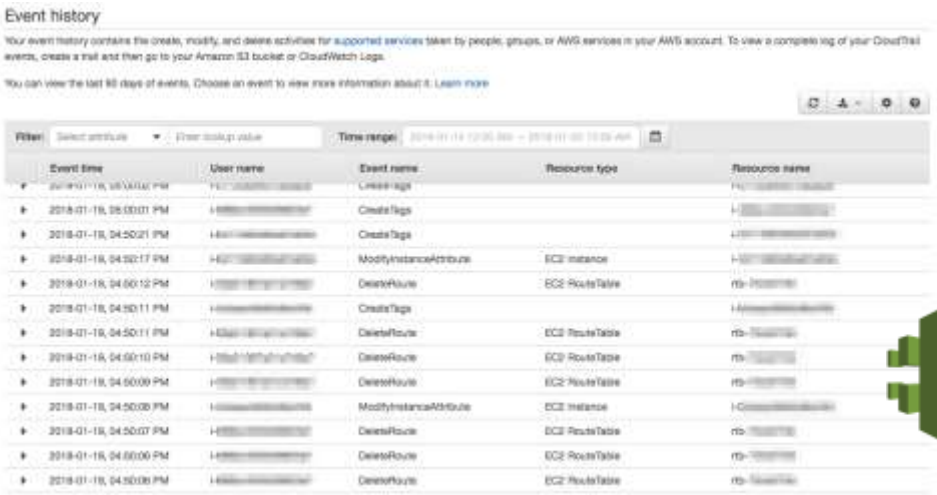
MFA!

Failure due to default policy not having permissions

Temporary credential request & setting at environmental variable

Commands work!

CloudTrail



Feed data to events

Respond

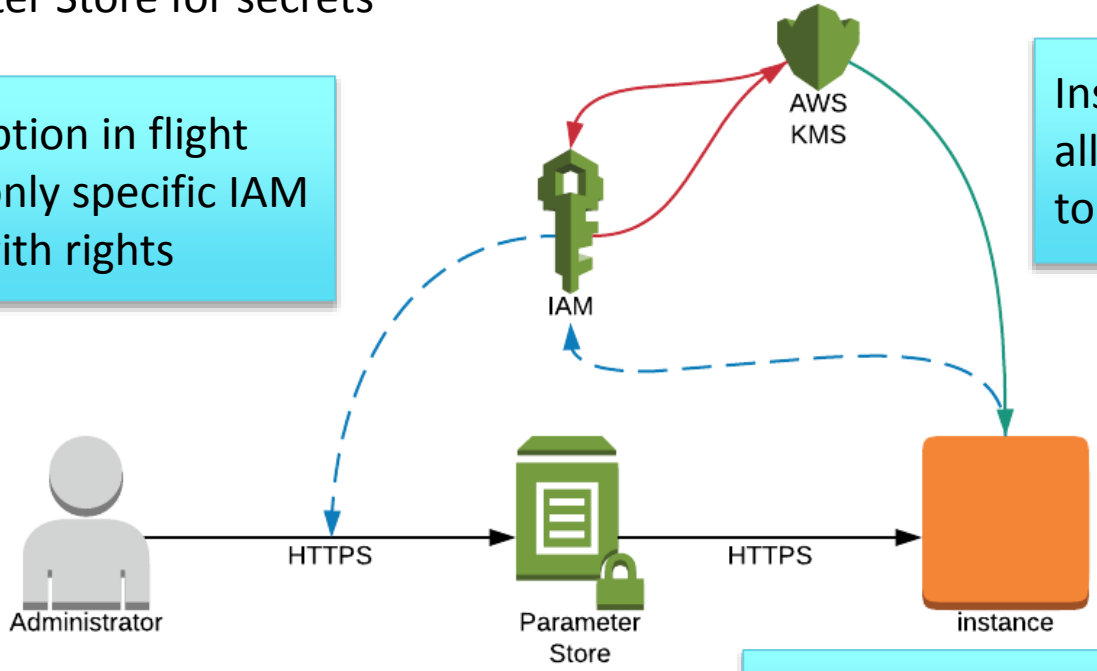
Monitor all API Actions

Scan and Secure

EC2 Parameter Store for secrets

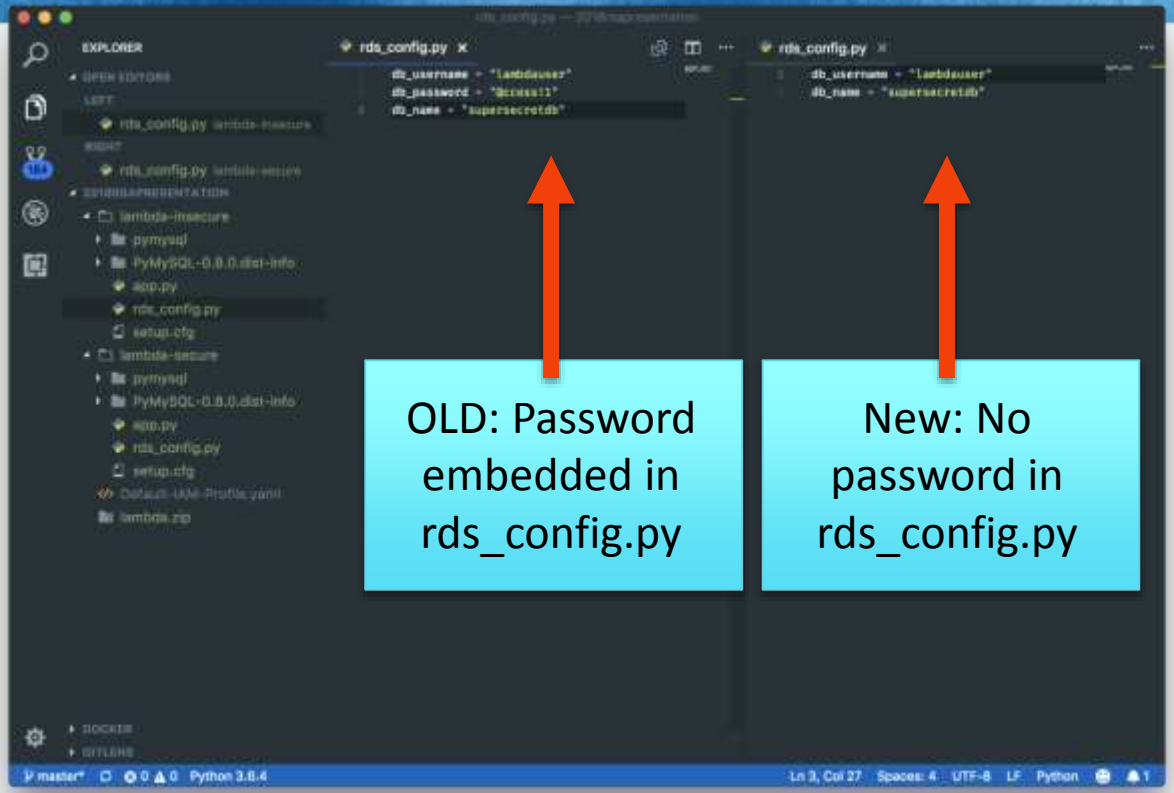
Encryption in flight with only specific IAM role with rights

Instance IAM Role allows rights to use key to decrypt



Instance retrieves encrypted value

EC2 Parameter Store



OLD: Password embedded in rds_config.py

New: No password in rds_config.py

EC2 Parameter Store

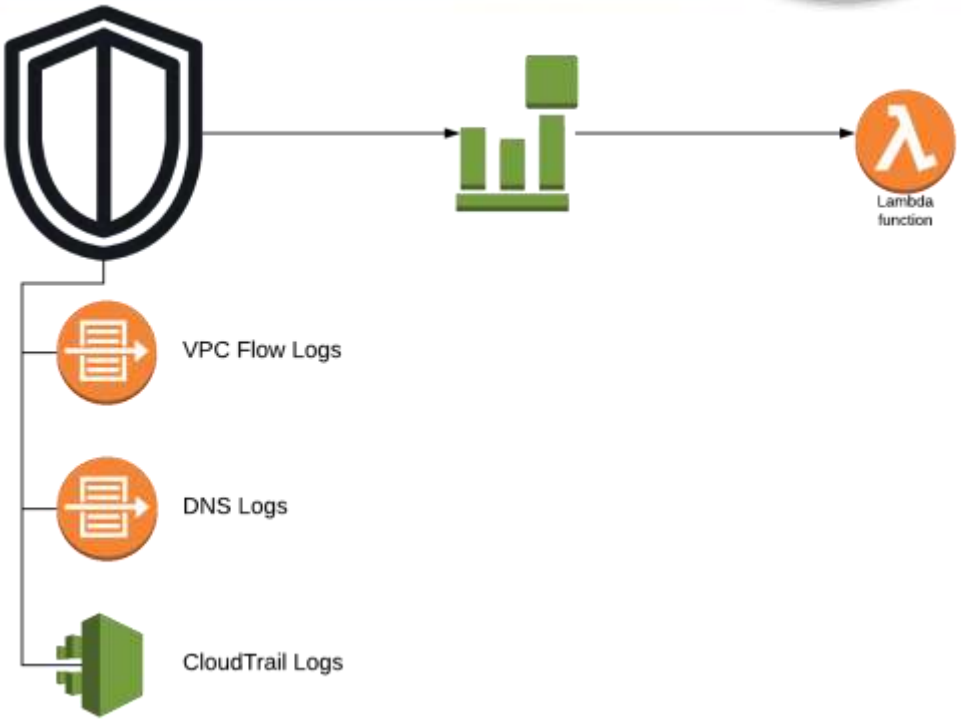
#RSAC

Calls AWS SSM

```
client = boto3.client('ssm')
response = client.get_parameters(Names=['mysql.password'], WithDecryption=True)
password = response["Parameters"][0]["Value"]
```

Monitoring

- AWS GuardDuty
- VPC Flow Logs
- CloudTrail
- Config
- Log shipping
- Secure log backups
- Automate Remediation



aws Services Resource Groups

GuardDuty

Findings
- Current
- Archived

Settings
- General
- Lists
- Accounts

Usage
- Details

Partners

New feature: GuardDuty added new findings

GuardDuty added nine new finding types for unusual API usage by an IAM user in your account Learn more

Current findings

Showing 57 of 57 55 2 0

Actions

Saved filters: No saved filters

Include and exclude filter options are available on certain finding attributes in the details

Finding	Last seen	Account ID	Count
Unprotected port on EC2 instance is being pro...	2018-03-22 16:27:54 (10 minutes ago)		2343
Unprotected port on EC2 instance is being pro...	2018-03-22 16:26:25 (12 minutes ago)		1675
Unprotected port on EC2 instance is being pro...	2018-03-22 16:25:33 (13 minutes ago)		2496
Unprotected port on EC2 instance is being probed.	2018-03-22 16:13:39 (25 minutes ago)		1757
Unprotected port on EC2 instance is being probed.	2018-03-22 16:04:30 (34 minutes ago)		1764
Unprotected port on EC2 instance is being pr...	2018-03-22 15:50:33 (an hour ago)		2729
Unprotected port on EC2 instance is being probed.	2018-03-22 15:38:54 (an hour ago)		2643
Unprotected port on EC2 instance is being pro...	2018-03-22 07:18:49 (9 hours ago)		43
222.93.96.163 is performing SSH brute force attacks against i-bcfcbb...	2018-03-22 07:03:19 (10 hours ago)		1
Unprotected port on EC2 instance is being pr...	2018-03-22 01:28:01 (15 hours ago)		17
Unprotected port on EC2 instance is being pro...	2018-03-21 23:58:32 (17 hours ago)		27
Tor Exit node is communicating with EC2 instance	2018-03-21 22:21:14 (18 hours ago)		19
222.161.209.43 is performing SSH brute force attacks against	2018-03-21 19:54:07 (21 hours ago)		1
221.132.31.23 is performing SSH brute force attacks against	2018-03-21 18:34:04 (a day ago)		4
117.78.42.53 is performing SSH brute force attacks against	2018-03-20 22:56:23 (2 days ago)		3
217.160.107.156 is performing SSH brute force attacks against	2018-03-18 16:39:03 (4 days ago)		1

Feedback English (US)

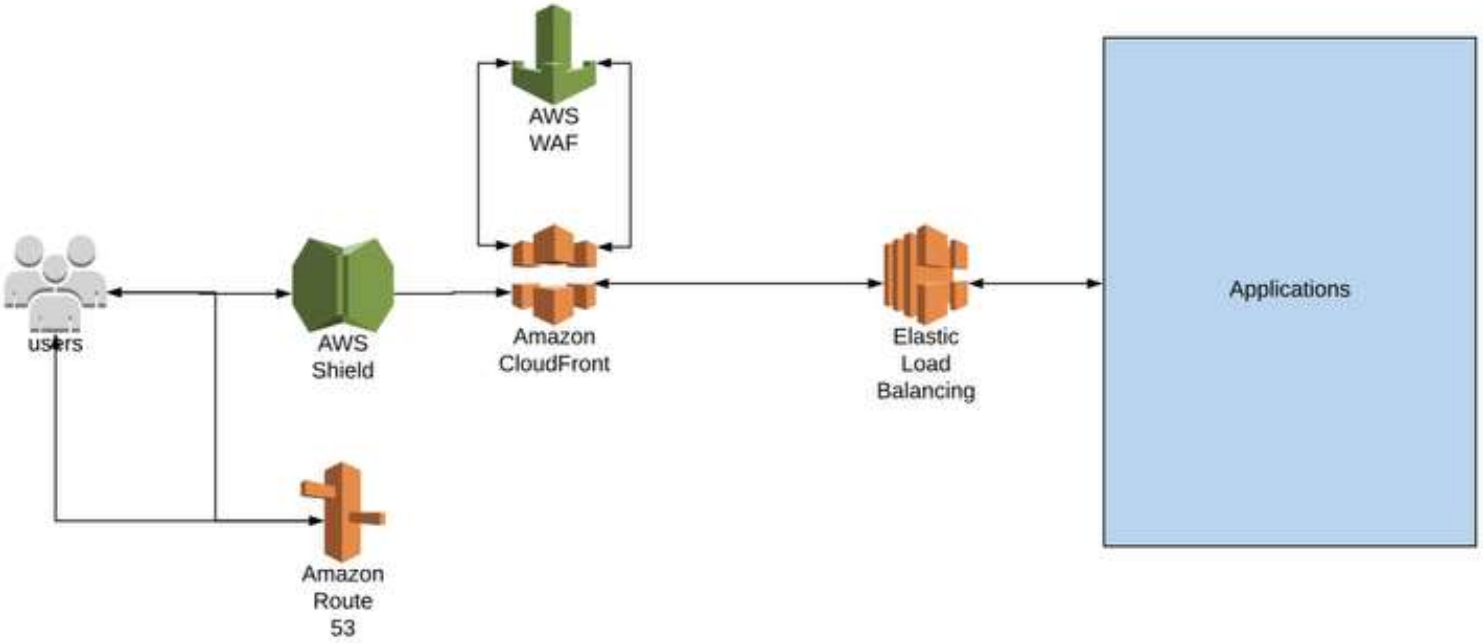
 Privacy Policy Terms of Use

#RSAC

zipwhip 2ND SIGHT LAB

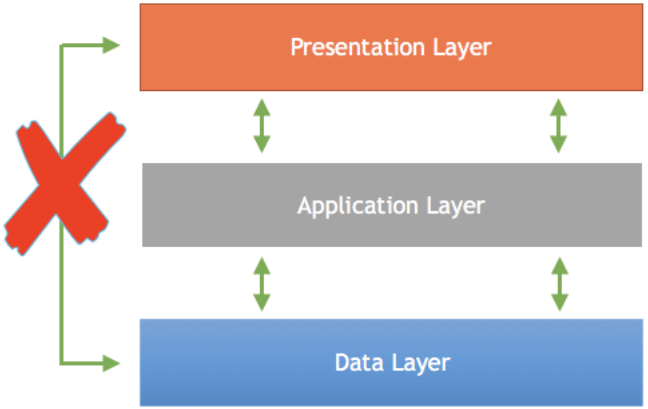
RSAConference2018

WAF Security



Network Architecture

- Presentation Layer
- Application Layer
- Data Layer

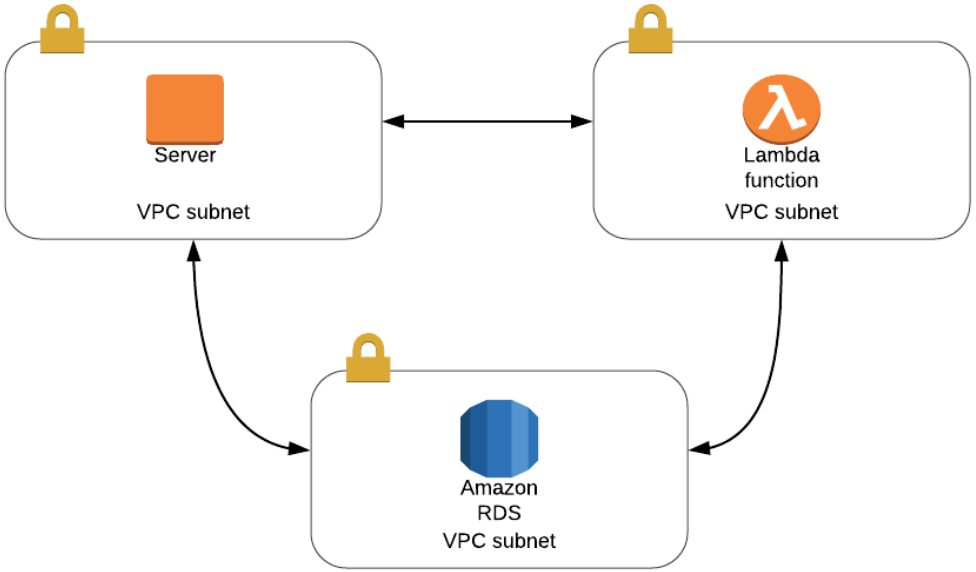


- Limited NACL & Security Groups between subnets
- Limit all outbound traffic

Network Architecture

BAD NETWORK

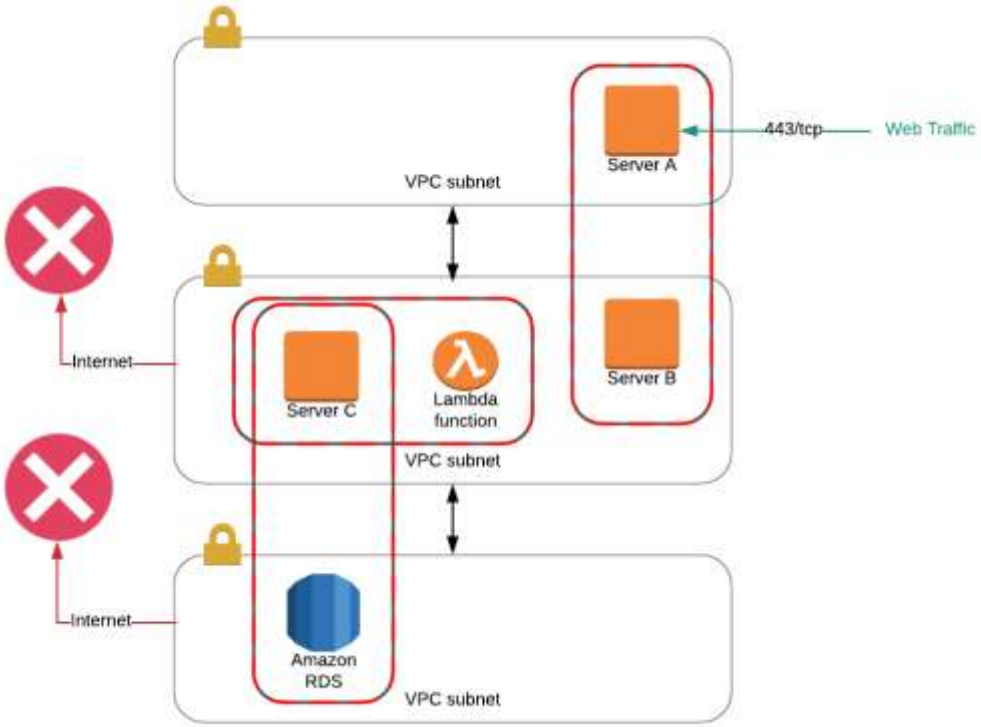
- NACLs are wide open
- Wide open inbound rules on security groups
- Security groups all everything to talk to internet



Network Architecture

BETTER NETWORK

- NACLs limit access between subnets
- Security Groups limiting access to specific servers
- Blocking internet where not needed



Conclusion

- Red Team:
  - Attackers can use the same tools used by DevOps teams.
  - Cloud APIs provide a means for mapping out an entire account.
  - Read only access can be powerful.

- Blue Team:
  - Restrict access
  - Automated deployment
  - Architect networks to minimize open ports and pivoting
  - Protect secrets - don't embed in code!
  - Monitor everything

RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: CSV-R12

THANK YOU!

Teri Radichel

CEO
2nd Sight Lab
@teriradichel

Kolby Allen

DevOps Engineer
Zipwhip
@kolbyallen