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...
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
  - AWS Tutorial: Lambda Accessing RDS in VPC
    - [https://docs.aws.amazon.com/lambda/latest/dg/vpc.html](https://docs.aws.amazon.com/lambda/latest/dg/vpc.html)
Pilfer Credentials ~ Read Only Access

D:\Users\tradichel\.aws>notepad .credentials

```
[default]
aws_access_key_id = AKIAJRWIVY7NJ6UYCKEQ
aws_secret_access_key = KSF2LhoTeRetZrnDMummAq/WhYgxW0kXXN0a8
```
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...
Examine Selected Database Subnets

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

All traffic allowed ~ Sweet.
What Traffic Do DB Security Groups Allow?

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
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...
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
```

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
```

```
D:\Users\tradichel\.aws>aws lambda list-functions --query Functions[?VpcConfig.SecurityGroupIds==["sg-93aadef8"]].FunctionName --output table --color off

<table>
<thead>
<tr>
<th>ListFunctions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateTableAddRecordsAndRead</td>
</tr>
</tbody>
</table>
```
aws lambda get-function --function-name CreateTableAddRecordsAndRead --query Code.Location

Gives us URL to code location in S3...
Hmm, what’s in this file?
About that rds_config file...

Oops. Database credentials.

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.
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!!

IAM Master - Initial Roles

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
Actions allow users to manage their account – BUT NOT PERMISSIONS

Sid: AllowUserstoManageOwnAccount
Effect: Allow
Action:
- "iam:ChangePassword"
- "iam:CreateAccessKey"
- "iam:CreateLoginProfile"
- "iam:DeleteAccessKey"
- "iam:DeleteLoginProfile"
- "iam:GetLoginProfile"
- "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}"

Resource only allows them to perform on their username – can’t modify anyone else
IAM ~ User Roles

- **Sid: AllowUserstoListOnlyTheirMFA**
  - **Effect:** Allow
  - **Action:**
    - "iam:ListVirtualMFADevices"
    - "iam:ListMFADevices"
  - **Resource:**
    - "arn:aws:iam::*:mfa/*"
    - "arn:aws:iam::*:user/${aws:username}"

- **Sid: AllowUsertoManageTheirMFA**
  - **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: AllowUserstoDeactiveTheirMFAWhenUsingMFA**
  - **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

MFA Required to assume role with temp creds

User ➔ IAM ➔ MFA ➔ Role 1 ➔ MFA ➔ Role 2 ➔ MFA ➔ User
IAM Master

Failure due to default policy not having permissions

Temporary credential request & setting at environmental variable

Commands work!
CloudTrail

Monitor all API Actions

Feed data to events

Respond
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

Calls AWS SSM
Monitoring

- AWS GuardDuty
- VPC Flow Logs
- CloudTrail
- Config
- Log shipping
- Secure log backups
- Automate Remediation
<table>
<thead>
<tr>
<th>Finding</th>
<th>Last seen</th>
<th>Account ID</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unprotected port on EC2 Instance... is being probe...</td>
<td>2018-03-22 16:27:54 (10 minutes ago)</td>
<td>1111</td>
<td>2343</td>
</tr>
<tr>
<td>Unprotected port on EC2 Instance... is being probe...</td>
<td>2018-03-22 16:26:26 (12 minutes ago)</td>
<td>2222</td>
<td>1675</td>
</tr>
<tr>
<td>Unprotected port on EC2 Instance... is being probe...</td>
<td>2018-03-22 16:25:33 (13 minutes ago)</td>
<td>3333</td>
<td>2496</td>
</tr>
<tr>
<td>Unprotected port on EC2 Instance... is being probe...</td>
<td>2018-03-22 16:13:39 (25 minutes ago)</td>
<td>4444</td>
<td>1737</td>
</tr>
<tr>
<td>Unprotected port on EC2 Instance... is being probe...</td>
<td>2018-03-22 16:04:30 (34 minutes ago)</td>
<td>5555</td>
<td>1764</td>
</tr>
<tr>
<td>Unprotected port on EC2 Instance... is being probe...</td>
<td>2018-03-22 15:50:33 (1 hour ago)</td>
<td>6666</td>
<td>2729</td>
</tr>
<tr>
<td>Unprotected port on EC2 Instance... is being probe...</td>
<td>2018-03-22 15:38:54 (1 hour ago)</td>
<td>7777</td>
<td>2643</td>
</tr>
<tr>
<td>Unprotected port on EC2 Instance... is being probe...</td>
<td>2018-03-22 07:18:49 (8 hours ago)</td>
<td>8888</td>
<td>43</td>
</tr>
<tr>
<td>222.03.66.103 is performing SSH brute force attacks against...</td>
<td>2018-03-22 07:03:19 (10 hours ago)</td>
<td>9999</td>
<td>1</td>
</tr>
<tr>
<td>Unprotected port on EC2 Instance... is being probe...</td>
<td>2018-03-22 01:26:01 (15 hours ago)</td>
<td></td>
<td>17</td>
</tr>
<tr>
<td>Unprotected port on EC2 Instance... is being probe...</td>
<td>2018-03-21 23:58:32 (17 hours ago)</td>
<td></td>
<td>27</td>
</tr>
<tr>
<td>Tor Exit node is communicating with EC2 instance...</td>
<td>2018-03-22 22:21:14 (18 hours ago)</td>
<td></td>
<td>19</td>
</tr>
<tr>
<td>222.161.209.43 is performing SSH brute force attacks against...</td>
<td>2018-03-21 19:54:57 (21 hours ago)</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>221.132.31.23 is performing SSH brute force attacks against...</td>
<td>2018-03-21 18:34:04 (24 hours ago)</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>117.78.42.53 is performing SSH brute force attacks against...</td>
<td>2018-03-20 22:56:23 (2 days ago)</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>217.160.107.156 is performing SSH brute force attacks against...</td>
<td>2018-03-18 16:39:03 (4 days ago)</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>
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 allow 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
THANK YOU!

Teri Radichel
CEO
2nd Sight Lab
@teriradichel

Kolby Allen
DevOps Engineer
Zipwhip
@kolbyallen