AWS IAM PrivEsc

Attacks & Defenses

Today’s Session

- Introductions
- What are privilege escalations?
- Why it matters
- Real-world attacks that involve PrivEscs in AWS
- Demo attack
- Demo defense
- About CodeShield & Cybr
- Q&A

About Us

AWS IAM PrivEsc Attacks & Defenses

Christophe Limpalair
Founder & Trainer
at Cybr

Manuel Benz
CTO and Co-Founder of
CodeShield

About Manuel Benz

- Founder and CTO of CodeShield
- ☁️ 5+ years of AWS experience
- 🔬 Research background in SAST/DAST
- 🥁 Drummer and house owner
- ✈ I live next to Frankfurt, Germany

Manuel Benz
linkedin.com/in/manuel-benz/

About Christophe Limpalair

- 📽️ Founder and Trainer at Cybr
- 👨‍💻 8+ years of AWS experience
- ⏮️ Background primarily in web dev and AWS cloud
- 🥾 I live in Colorado and love hiking & skiing

Cybr.com/discord

Christophe Limpalair
https://linkedin.com/in/christophelimpalair

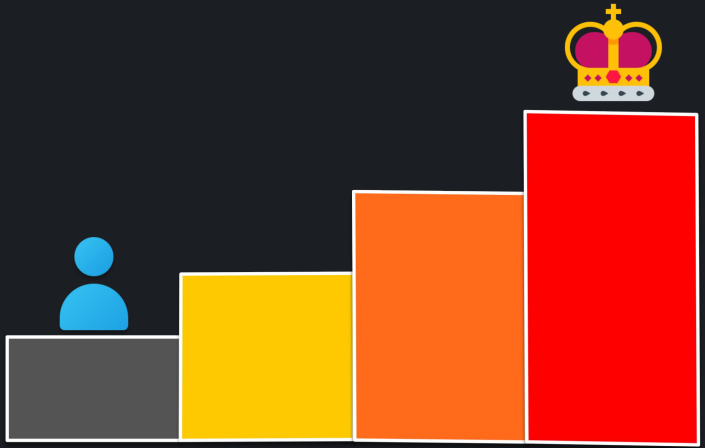
@ChristopheLimp
https://twitter.com/christophelimp

code_shield
CYBR

What are Privilege Escalations?

In simple terms:

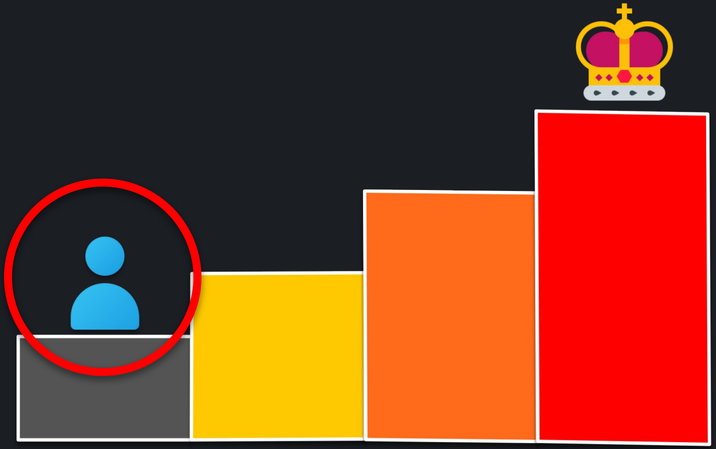
An attacker going from lower to higher privileges



What are Privilege Escalations?

In terms of AWS PrivEscs:

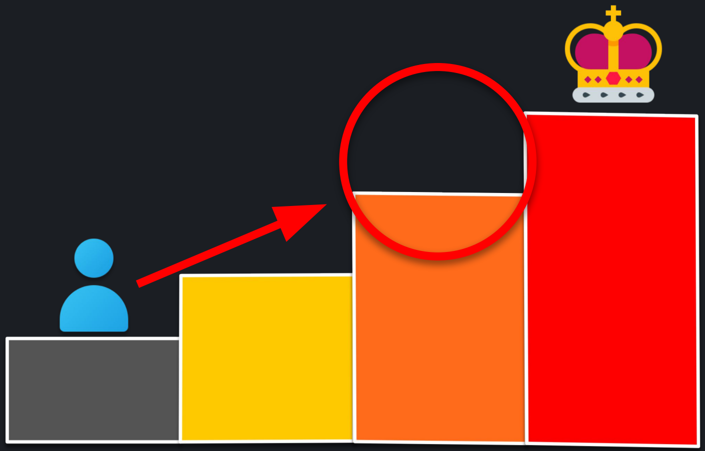
An attacker found a way in through a user, role, or resource, but their access is limited



What are Privilege Escalations?

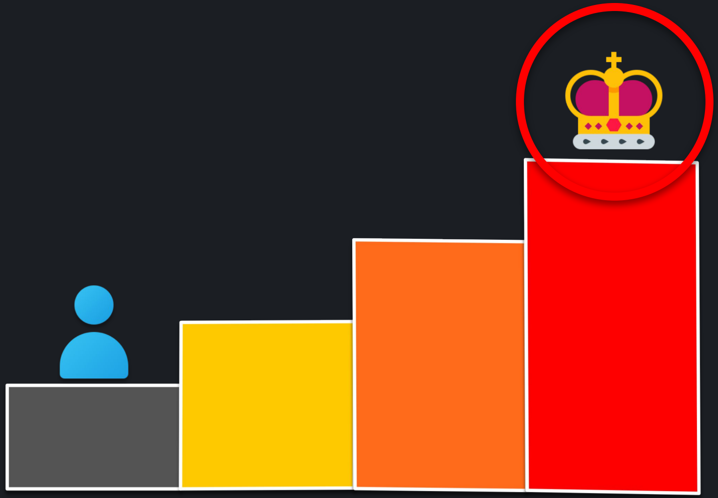
In terms of AWS PrivEscs:

They will want to look for a privilege escalation path to elevate their permissions



What are Privilege Escalations?

Ideally, they would grant themselves admin rights…but realistically that's often not needed…



What are Privilege Escalations?

Even without admin rights, they could:

- Launch big EC2 instances for crypto mining ($$$)
- Exfiltrate sensitive data *<- What we'll demo today*
- Access secret values from Secrets Manager
- Etc…

What are Privilege Escalations?

In fact, Manuel brought a real-world example of impact…

Hacker Puts Hosting Service Code Spaces Out of Business

> *“Within 12 hours, Code Spaces went from a viable business to devastation. The company reported that all of its svn repositories—backups and snapshots—were deleted. All EBS volumes containing database files were also deleted. A few old svn nodes and one git node were left untouched, the company said.”*
>
> *Code Spaces hack 2014*
>
> *https://threatpost.com/hacker-puts-hosting-service-code-spaces-out-of-business/106761/*

Code Spaces Hack 2014 Walkthrough (12h)

1. DDoS against website as distraction

Code Spaces Hack 2014 Walkthrough (12h)

1. DDoS against website as distraction
2. Attackers gained access to EC2 control panel with stolen credentials

Code Spaces Hack 2014 Walkthrough (12h)

1. DDoS against website as distraction
2. Attackers gained access to EC2 control panel with stolen credentials
3. Attackers gained persistence in the account with a privilege escalation towards Admin access (*iam:CreateUser, iam:AttachUserPolicy, iam:CreateAccessKey*)

Code Spaces Hack 2014 Walkthrough (12h)

1. DDoS against website as distraction
2. Attackers gained access to EC2 control panel with stolen credentials
3. Attackers gained persistence in the account with a privilege escalation towards Admin access (*iam:CreateUser, iam:AttachUserPolicy, iam:CreateAccessKey*)
4. Attackers raised extortion demands against Code Spaces

Code Spaces Hack 2014 Walkthrough (12h)

1. DDoS against website as distraction
2. Attackers gained access to EC2 control panel with stolen credentials
3. Attackers gained persistence in the account with a privilege escalation towards Admin access (*iam:CreateUser, iam:AttachUserPolicy, iam:CreateAccessKey*)
4. Attackers raised extortion demands against Code Spaces
5. Code Spaces changed keys for EC2

Code Spaces Hack 2014 Walkthrough (12h)

1. DDoS against website as distraction
2. Attackers gained access to EC2 control panel with stolen credentials
3. Attackers gained persistence in the account with a privilege escalation towards Admin access (*iam:CreateUser, iam:AttachUserPolicy, iam:CreateAccessKey*)
4. Attackers raised extortion demands against Code Spaces
5. Code Spaces changed keys for EC2
6. Attackers deleted all business data and backups

Common Priv. Esc. Vulnerabilities seen in the Wild

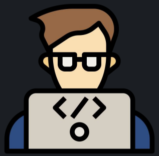
Entities able to gain admin access

- Third-party providers
  - Security/Monitoring Tools
  - AWS Service Catalog

Common Priv. Esc. Vulnerabilities seen in the Wild

Entities able to gain admin access

- Third-party providers
  - Security/Monitoring Tools
  - AWS Service Catalog



- Developers
  - By accident
  - Leaked/Phished Credentials
  - Insider/prior-employee

Common Priv. Esc. Vulnerabilities seen in the Wild

Entities able to gain admin access

- Third-party providers
  - Security/Monitoring Tools
  - AWS Service Catalog
- Developers
  - By accident
  - Leaked/Phished Credentials
  - Insider/prior-employee
- CI Runner
  - Developers
  - Malicious/Vulnerable 3rd-party libraries

IAM PrivEsc Attack Demo

iam:CreateLoginProfile

IAM PrivEsc Defense Demo

About CodeShield.io

- Scan your AWS account for privilege escalation in under 30 minutes
- Gain an overview of all permissions and connectivity of your cloud assets
- Get your first audit including discussion of results for free!
- Learn how to protect against IAM privilege escalation in AWS

Trusted by

DB Systel GmbH · syracom business efficiency engineering · handly · HANKO · northmill bank · TEMPEST Protegendo negócios no mundo digital. · zoph.io

Schedule a Demo

or drop me an email @ manuel.codehield.io

🔒 About Cybr.com

Learn AWS cloud security hands-on

Access training Courses, 🧪 Hands-On Labs,
and Ebooks on AWS Cloud Security

RED TEAM FREE
Intro to AWS IAM Enumeration

RED TEAM FREE
Intro to Secrets Manager Enumeration

RED TEAM FREE
Intro to S3 Enumeration

FOUNDATIONAL FREE
Getting started with the AWS CLI

BLUE TEAM
Configure Security Groups (SGs) and NACLs

BLUE TEAM
Create a VPC with public and private subnets

BLUE TEAM
Deploy AWS WAF ACL for Application Load Balancer

RED TEAM
S3 Data Exfiltration via EC2 IMDSv1

Resource Links

- Lab used in the demo:
  - https://cybr.com/courses/iam-privilege-escalation-labs/lessons/lab-ctf-iamcreateloginprofile-privesc/
- Cybr’s Hands-On Labs:
  - https://cybr.com/hands-on-labs
- CodeShield.io:
  - https://codeshield.io

Thank you for attending!

Any questions?

Christophe Limpalair
https://linkedin.com/in/christophelimpalair

Manuel Benz
https://linkedin.com/in/manuel-benz/

LIVE

Upcoming webinars
https://cybr.com/webinars