YOUR CI/CD IS MY CI/CD:

A TABLETOP DISCUSSION ON THE ATTACK SURFACE OF THE PIPELINE

Defcon416
Geoff Heymann *Security Compass*

INTRODUCTION

- ```
  [speaker@dc416]$ whoami
  geoff.heymann
  ```
- ```
  [speaker@dc416]$ groups
  seneca.college ifs hackfest
  security.compass
  senior.security.consultant
  ```
- ```
  [speaker@dc416]$ certutil -d sql:$HOME/.pki/nss
  Certificate Nickname
  OSCP
  OSCE
  AWS Solutions Architect Associate
  AWS Certified Security
  ```
  ```

SHAMELESS PLUG

```
[speaker@dc416]$ grep -r "hiring" ./securitycompass/status.txt
 Yes we are
```

Speaker notes

For more information head to https://securitycompass.com/careers/

OVERVIEW

- State of application security
- Brief description of DevOps
- Perspective of interested parties
- Various tabletop case studies around attacking the pipeline

STATE OF APPLICATION SECURITY

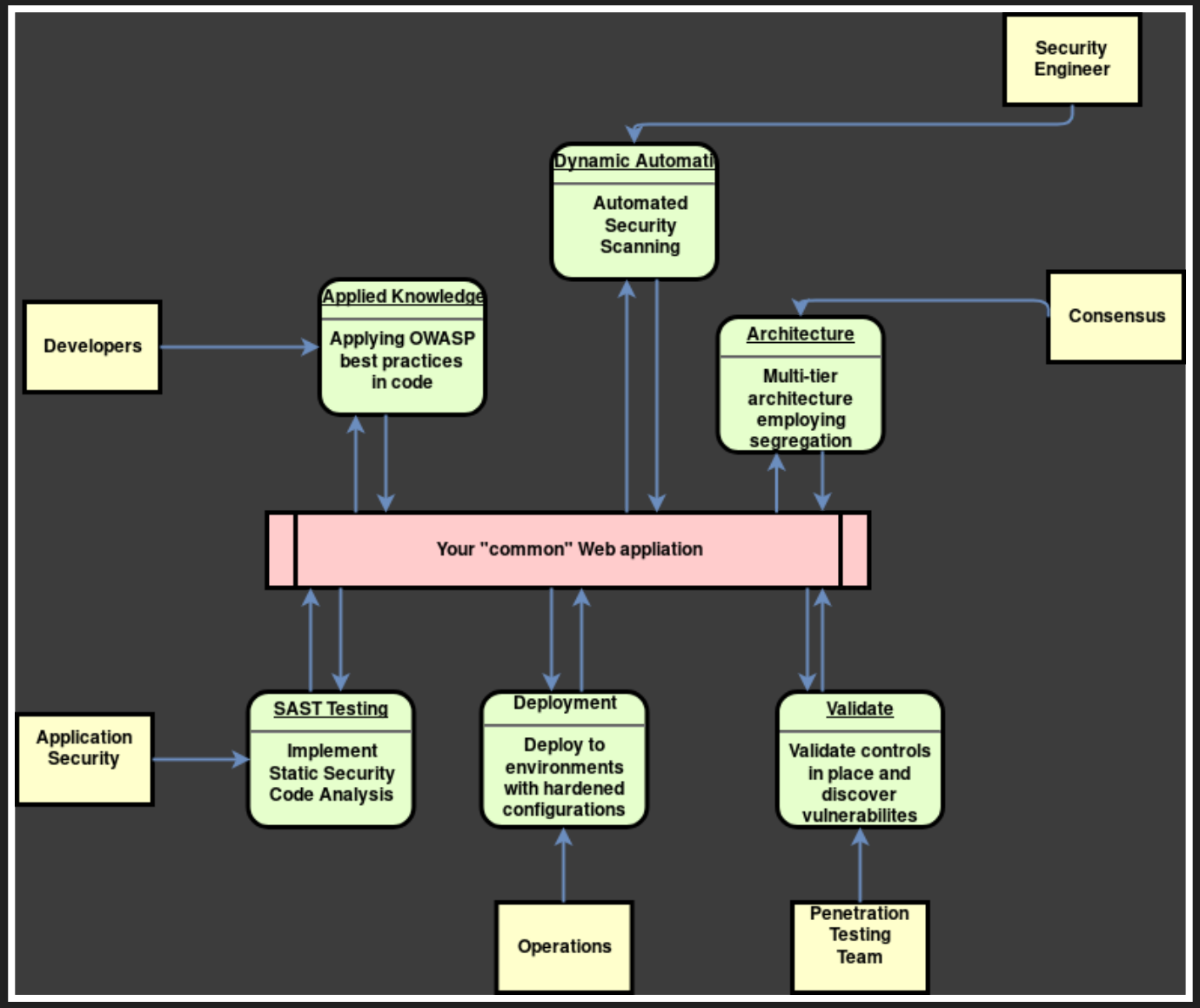
- Newer applications have the potential to be better
- It's harder to find traditional bugs i.e. buffer overflows and command injection
- the overall baseline of a secure application is increasing
- Thanks DevSecOps ! But really...

- SSDLC
- Popular Frameworks/Stacks
- Published Security Standards
- Conferences
- Meetups
- Bug Bounties
- Security Programs
- Security Champions
- Threat Modelling
- Training
- Penetration Tests
- **Automation**
- Security Organizations

- Popular Media
- **Gamification of Security**

- **Adoption in school**
- **Previous experiences**
- **Customer and client interest**
- Regulatory Bodies
- Speed in patching
- Twitter
- Shared Responsibility
- and more...

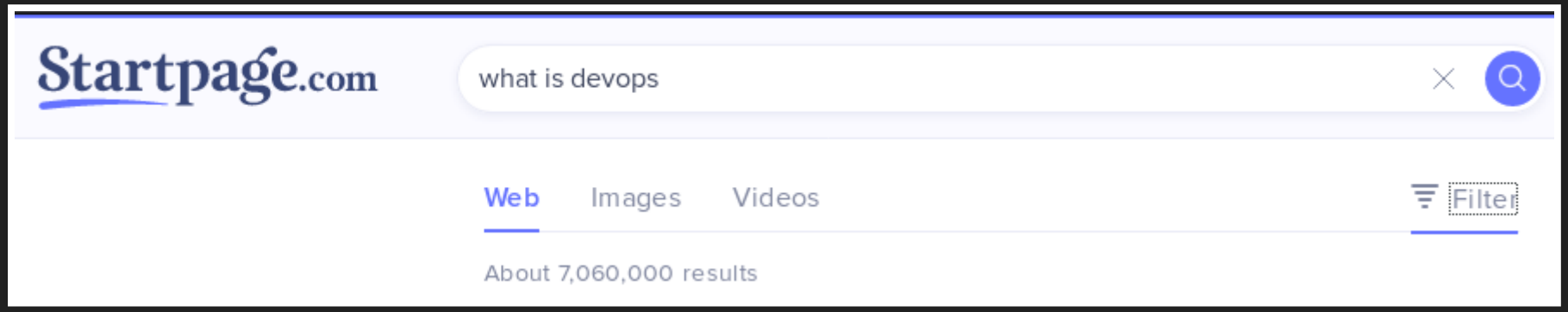
Controls an attacker might be up against with an application



Speaker notes

This would be a small snippet of the controls and considerations that may go into designing, building and deploying a secure application

DEVOPS ?!

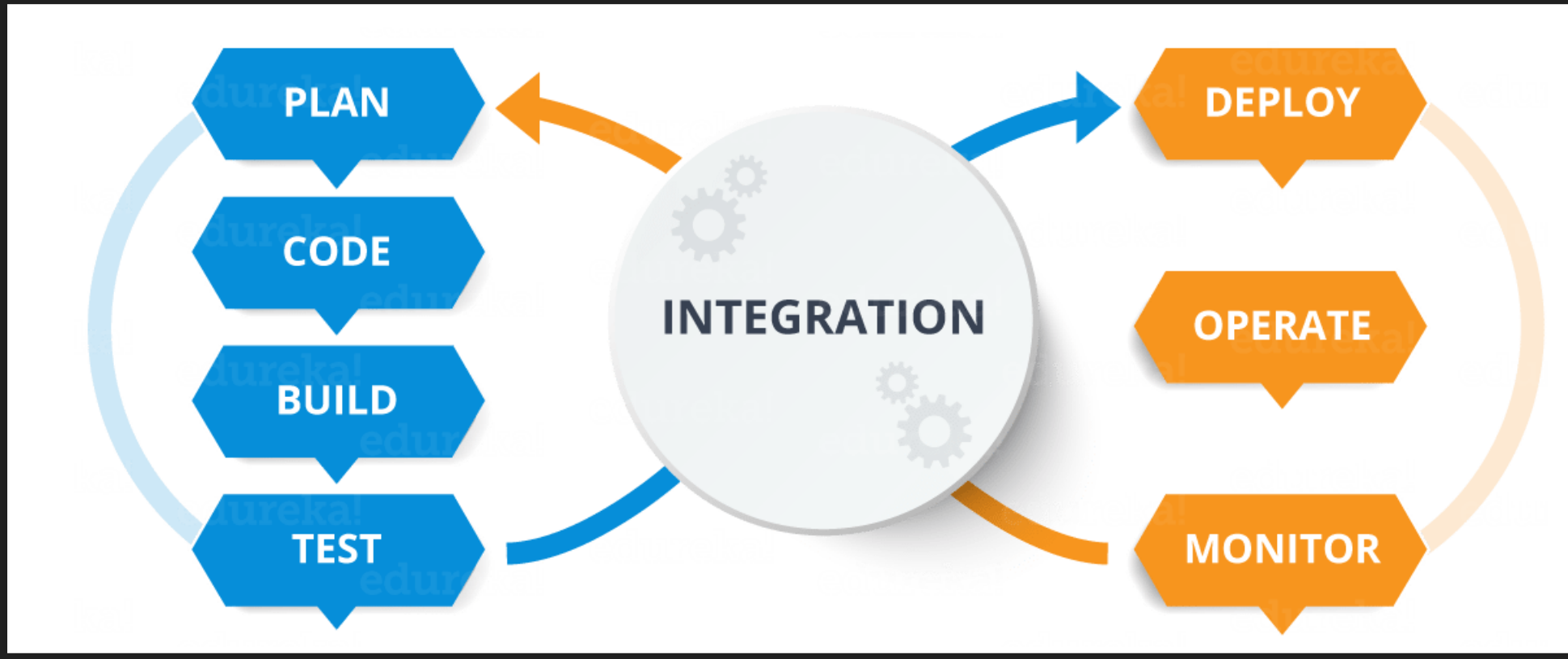


"DevOps is the process of continuously improving software products through rapid release cycles, global automation of integration and delivery pipelines, and close collaboration between teams" - **Julien Vehent**

Speaker notes

A notable talk conducted by him on security test integration in a DevOps pipeline https://www.youtube.com/watch?v=1Nlbf7XXn7s

HOLISTIC PERSPECTIVES



Edureka image on the elements of a devops pipeline

PERSPECTIVES: RED TEAM

- Abuse of transitive trust
- Are these orchestration systems configured with privilege action in mind?
- Logging?
- Limited exposure?
- Bi-directional trust?
- Can any element or application in the pipeline be used for as a foothold for greater objectives?

PERSPECTIVES: BLUE TEAM

- Are logs being maintained?
- Do first responders have visibility in the environment
- Is non-repudiation and integrity being maintained in the environment

PERSPECTIVES: OPS

- Does that data remain confidential?
- Does the environment reflect security standards
- Does it work?

CASE STUDY 1: THE NEW GITHUB

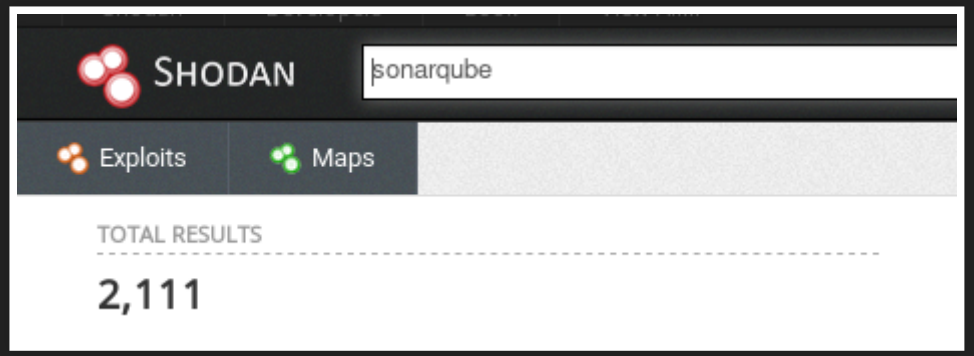
- Early cases of credentials being stored on Github
- Some Teams have done better:
  - Private Repositories
  - Access Controls
  - Not pushing configuration files to a central repository
  - Locking down their Source Code repository

CASE STUDY 1: ENTER SONARQUBE

SonarQube is a continuous inspection of code quality to perform automatic reviews with static analysis of code to detect bugs, code smells, and security vulnerabilities

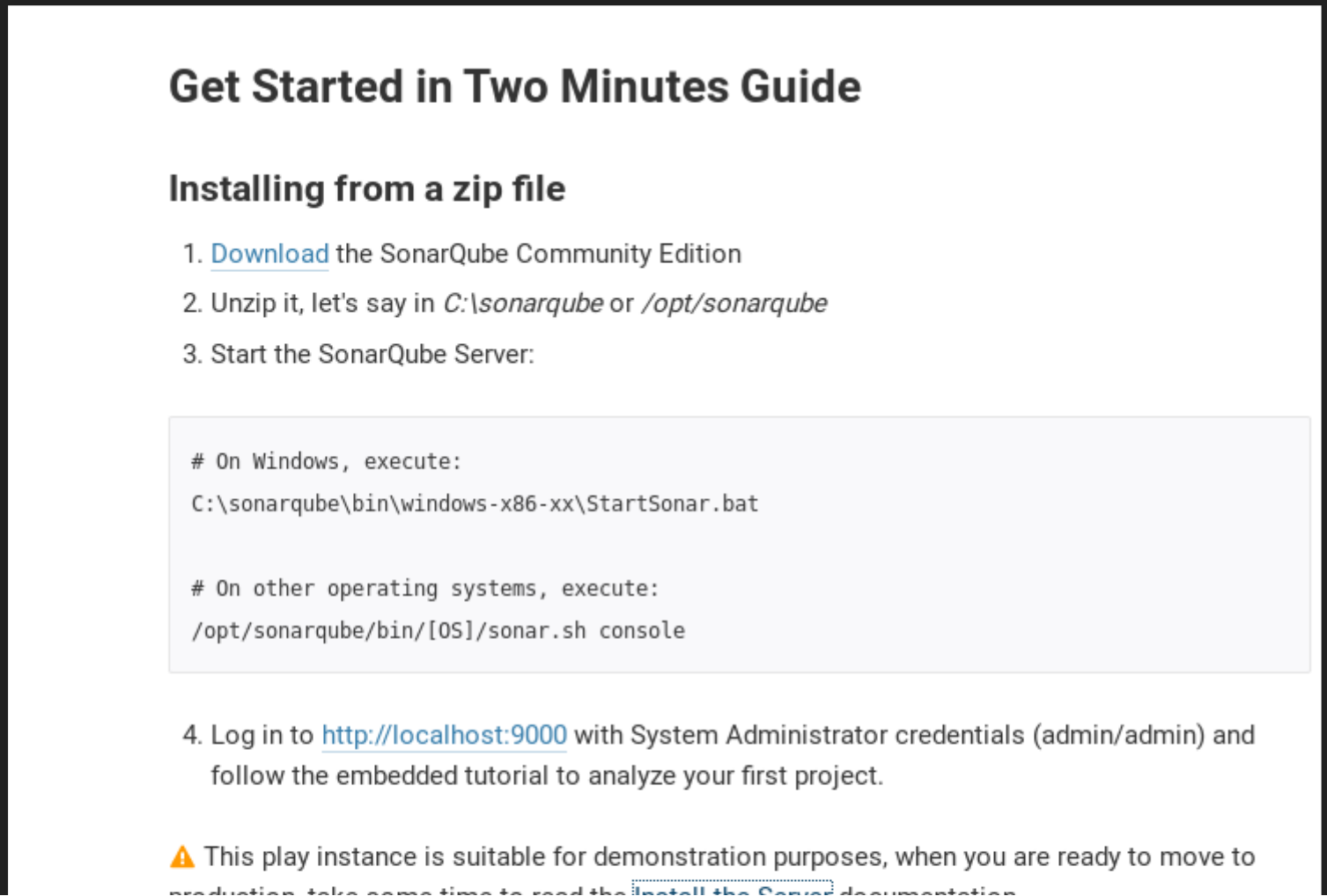
CASE STUDY 1: SONARQUBE STATS

- Usually listens on port ~9000
- If you queried Shodan you may get more than 2000 instances



CASE STUDY 1: SO WHAT'S THE ISSUE

- Same issue that plagues alot of tooling. The option for default credentials



Get Started in Two Minutes Guide

Installing from a zip file

1. Download the SonarQube Community Edition
2. Unzip it, let's say in *C:\sonarqube* or */opt/sonarqube*
3. Start the SonarQube Server:

```
# On Windows, execute:
C:\sonarqube\bin\windows-x86-xx\StartSonar.bat

# On other operating systems, execute:
/opt/sonarqube/bin/[OS]/sonar.sh console
```

4. Log in to http://localhost:9000 with System Administrator credentials (admin/admin) and follow the embedded tutorial to analyze your first project.

⚠ This play instance is suitable for demonstration purposes, when you are ready to move to

production, take some time to read the Install the Server documentation.

Using Docker

A Docker image of the Community Edition is available on Docker Hub, see usage and configuration examples there.

⚠ This instance is suitable for demonstration or testing purposes only.

Speaker notes

Ensure that authorization and authentication aligns with the current organizational policies

CASE STUDY 1: YOUR ACTIONABLE POC

```
def main():
    username='admin'
    password='admin' #testing default creds
    target_list = read_file('final_list.txt')
    for x in target_list:
        try:
            url = 'http://'+x
            test_connection(url)
        except Exception as e:
            print('Most likely needs to be https')
            print(e)
            url = 'https://'+x
        print(url)
        projects = list_projects(url,username,password,proxies
        print(projects)
```

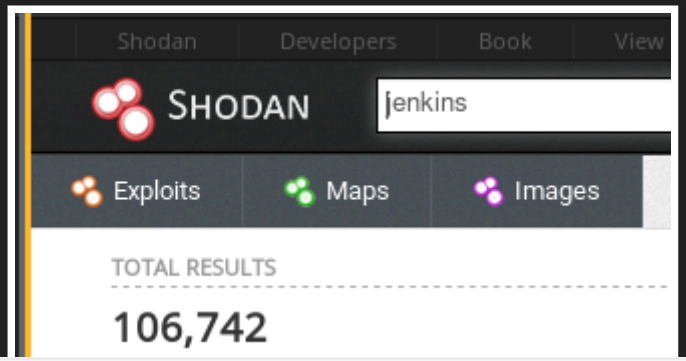
CASE STUDY 2: JENKINS

Popular CI/CD tool

10. Which CI server do you use?

As most developers would expect, Jenkins wins the CI server race with a whopping 57% market share. It's closest competitor is "none" at 21% of the vote, which almost matches the rest of the competition combined (at 22%). The remaining CI servers have less than 5% of the market share each, with Hudson, the elderly relative of Jenkins, struggling on at 2%. It's worth mentioning VSTS, Microsoft VSTS (Visual Studio Team Server), which is not usually thought of in the Java/JVM space, clocks in at 2%.

Most developers, we believe, expect that nearly all sites today use continuous integration. So, it's startling to see that 1 in 5 applications do none at all. Even personal projects today use CI (such as Travis CI and CircleCI), which are made available on public project-hosting sites such as Bitbucket and GitHub. If you're one of the 21% who don't use CI on your projects, we'd love to hear why.



Speaker notes

Statistics obtained from Synk https://snyk.io/blog/jvm-ecosystem-report-2018-tools/

CASE STUDY 2: JENKINS IS THE COOL KID

- Currently has 256 vulnerabilities disclosed
- This is where patch management needs to be addressed for tooling as critical as this
- What compromising a Jenkins server may provide:
  - Temporary Credentials to deployment environments
  - The opportunity to backdoor an application
  - The opportunity for privilege escalation

CASE STUDY 2: ACTIONABLE ATTACK VECTOR - KNOWN VULNERABILITIES

- Vulnerability research on this is pretty viable
  - Open Source
  - Proven track record
  - Central to a successful pipeline

CASE STUDY 2: VULNERABILITY RESEARCH CONTINUED

- One researcher has produced some recent vulnerabilities **Orange Tsai**
- CVE-2018-1999002 - Arbitrary file read vulnerability
- CVE-2018-1999046 - Unauthorized users could access agent logs
- CVE-2018-1000861 - Code execution through crafted URLs

Speaker notes

Link to the research being done by DEVCORE
https://devco.re/blog/2019/01/16/hacking-Jenkins-part1-play-with-dynamic-routing-en/

CASE STUDY 3: SOME THINGS YOU JUST DON'T NOTICE

- Companies often leverage their CSP (Cloud Service Provider to manage their docker registries)
- Traditionally you would need to protect your docker login credentials and no one would be the wiser....
- Different case in cloud environments

CASE STUDY 3: ACTIONABLE POC

```
aws ecr get-login --region us-east-1 --profile Read_C
sudo docker login -u AWS -p eyJwYXls..
sudo docker pull 65371xxxx.dkr.ecr.us-east-1.amazonaws.com/pro
```

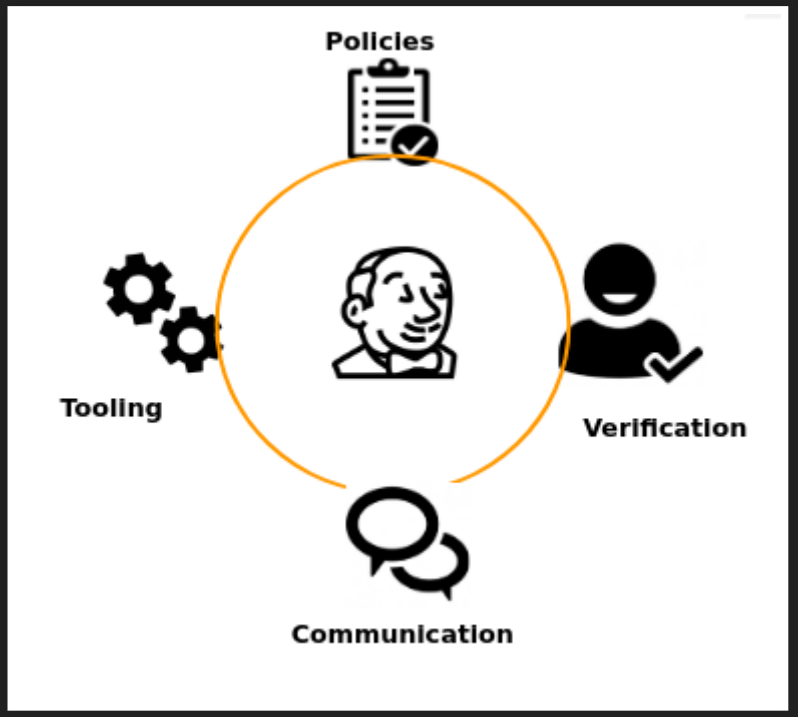
- If you get your hands on the image name you have a really good chance to interact with their deployment image.
- Good practice is `flaws2.cloud`

Speaker notes

When dealing with managing your registry consider the following:

- Ensure that the repository policy is limited to required users i.e. modifying the principals that have access to the registry.
- https://docs.aws.amazon.com/AmazonECR/latest/userguide/set-repository-policy.html

SUMMARY



- Misconfigurations - Will always be an issue
- Vulnerabilities - Will always be an issue
- Your Pipeline will grow in complexity

Speaker notes

Maintain an updated discussion around securing the pipeline

Q&A