DevSecOps Bootcamp

BUILDING RUGGED SOFTWARE

YEAR ONE / WEEK ONE / LESSON TWO

Anatomy of an attack

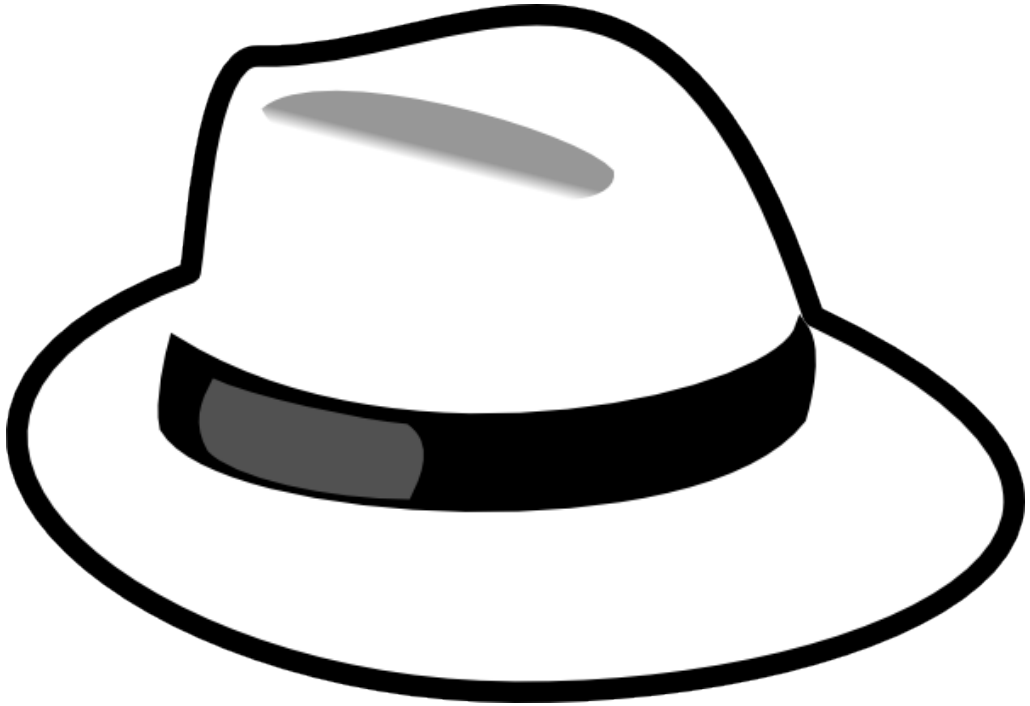
- Understanding the motivations of an attacker
- Getting in the mind state of an attacker

Motivations of an attacker

- Recreational
- Monetary
- Fraud
- Data
- Computing power
- Political

Getting into the mind state of an attacker

- How would they attack us?
- Why would they attack us?
- What do we have that is valuable to an attacker?



Attack Map Introduction

- An attack map is a graphical representation of the attack surface of an application and or environment
- Helps Intuit get ahead of attackers by understanding our attack surface
- Helps the Red Team to quickly verify vulnerability remediation and mitigations
- Allows PD Teams to understand their weaknesses, areas of attack and address the most important weaknesses quickly/efficiently
- Enables PD Teams to design their applications to be resilient to attacks

Attack Map Creation

- Create a graphical representation of your application including all communication flows and technologies being used
- Gather a list of potential vulnerabilities and areas of attack. Think about Confidentiality, Integrity and Availability for each connection/interaction within the application
- Map the attacks/vulnerabilities to the graphical representation
- Create a key that allows for mapping attack descriptions to the graphical attack map
- Include this document as an ATTACKS.md file in your repository

Example Attack Map Key

IHP Threats

1. Denial of Service of application
2. Malicious insider access to physical app server host
3. Malicious outsider access to physical app server host
4. Some AWS access keys logged
5. Some Key Encryption Keys and AWS access keys logged
6. All Key Encryption Keys compromised from Hardware Security Module
7. Untrusted employee departure

Mixed Threats

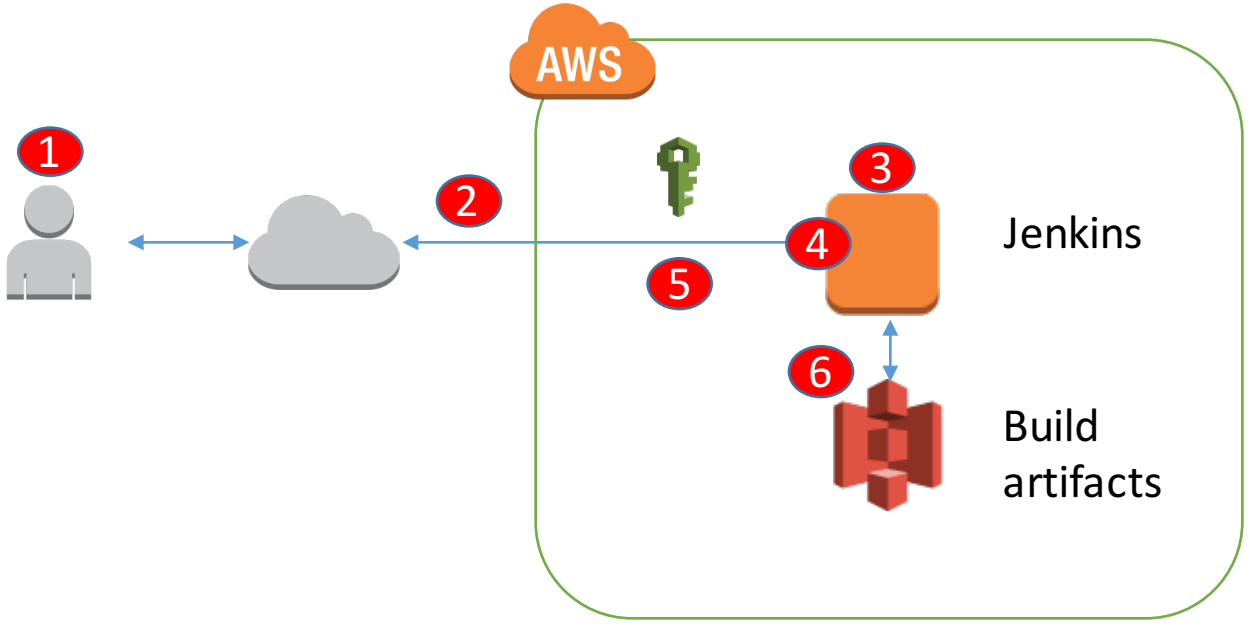
21. Trusted operator departure

AWS Threats

8. Denial of Service
9. AWS IAM (app) user has more than one AWS API access key
10. EC2 host compromised
11. IAM account and bucket policy error
12. Malicious modification or delete of objects
13. Many Key Encryption Keys compromised during key rotation
14. Unexpected AWS IAM role on account
15. Access to physical media
16. Compromise of root
17. S3 object retrieved from a non-Intuit IP address
18. Unexpected AWS IAM user on account
19. Untrusted employee departure
20. AWS encryption keys compromised

Lab 2 - Attack Maps

1.
2.
3.
4.
5.
6.
7.



Intel High Way

Crawl, Walk, Run

- **Crawl** - Identifying security design constraints and controls that need to be built into the software to reduce successful attack

- **Walk** - Prioritize and build security into for issues found later in the software lifecycle

- **Run** - Build automation into script deployment to detect issues, unit testing, security testing , black box testing