RSA Conference 2019

BETTER.

LEARNING LABS

Fine-tuning Your Cyber Defense Technologies with the ATT&CK Framework

LAB1-R10

Lane Thames,
Tripwire, Inc.

Table of Contents

INTRODUCTION ... 3

Thanks for attending! ... 3

LAB SUMMARY ... 3

Key Takeaways ... 3

Lessons Learned ... 4

Contact Details ... 5

Reading and References ... 5

Introduction

Thanks for attending!

It was a pleasure meeting and working with you at RSA Conference 2019. I am honored that you chose to spend some of your valuable time attending my Learning Lab, *Fine-tuning Your Cyber Defense Technologies with the ATT&CK Framework*. The goal of this learning lab was for us to learn about the ATT&CK framework together, using hands-on exercises along with active group-based discussions. The objectives for this learning lab were to introduce lab attendees to the MITRE ATT&CK framework, to introduce how we can use the framework to fine-tune our cybersecurity technologies, and to discover how modern deception-based technologies can shift the defender's odds for the better and how deception can be coupled with the ATT&CK framework.

Lab Summary

Key Takeaways

Core Aspects of ATT&CK

We learned that, according to David Bianco's Pyramid of Pain, we can make things much harder for cyber adversaries if we can implement security measures that target the adversary's Tactics, Techniques, and Procedures (TTPs). The ATT&CK framework helps us with achieving this. ATT&CK, developed by MITRE, is a curated knowledge base and framework. The name is an acronym for Adversarial Tactics, Techniques, and Common Knowledge, and it provides knowledge describing behaviors, actions, and processes that a cyber adversary might utilize once initial access has been gained within an organization's network. ATT&CK is focused on tactics and techniques that are employed by adversaries during the Exploit, Control, Execute, and Maintain phases of the so-called Cyber Killchain.

Use Cases

Common use cases for the ATT&CK framework include:

- Threat Intelligence
    - Threat hunting and capturing indicators of compromise (IoC)
- Internal security training

- Gap Analysis
    - Discovering areas in the organization where security controls, countermeasures, defenses, etc. are lacking with respect to the tactics and techniques defined in ATT&CK
- Adversary Emulation
- Red-Blue (Purple Teaming)
- High-fidelity detection

These use cases can be utilized to fine-tune your cyber defenses. This can be achieved numerous ways. One very important use case is gap analysis with respect to ATT&CK in terms of your organization's people, processes, and technologies. For example, we saw that the Tactic "Initial Access" is very important, and it is really your first line of defense. Many techniques used for initial access are based on phishing. As such, it is very important to have good security awareness and training programs used, consistently, in your organization. We also learned how gap analysis can be used to discover what types of security technologies you might need to add or modify for your organization. For example, if you have file integrity monitoring in place, there are numerous ATT&CK techniques that can be detected. We also saw that other frameworks such as the CIS Critical Security Controls can be coupled with ATT&CK for a specialized gap analysis.

Deception

Numerous advancements in technologies such as cloud computing, containers, and virtualization have provided new avenues for implementing and deploying deception technologies. One such deception technology is based on the classical honeypot/honeynet. Nowadays, we can create large scale collections of honeypots at minimum cost, and creating large scale honeypots allows us to induce significant confusion on attackers, which increases their costs and amount of time required to achieve their goals. There are several ATT&CK tactics that can be coupled with deception technology, including the Discovery, Lateral Movement, and Collection tactics.

Lessons Learned

We discussed a few key lessons that we should start adopting with respect to how we approach and manage the cybersecurity of our organizations.

1: We have to understand that cyber-attacks are inevitable and we should "embrace system compromise". This means that we should operate in a fashion where we focus on systems and processes that enable us to recover quickly and with minimum damage when a successful cyber-attack occurs, instead of creating policies that induce complacency and compliance based on “heads will roll if we get attacked” attitudes.

2: We need to change our traditional ways of thinking. We need to defend “graphs of assets” instead of “lists of assets”, we need to “manage adversaries” instead of “manage incidents”, and we need to “think about increasing attacker requirements” instead of “thinking about stopping attacks”.

Contact Details

You can contact we at twitter, LinkedIn, or email:
https://twitter.com/Lane_Thames
https://www.linkedin.com/in/lanethames
lthames@tripwire.com

Reading and References

https://attack.mitre.org/

https://mitre.github.io/attack-navigator/enterprise/

http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

https://en.wikipedia.org/wiki/Deception_technology

https://github.com/jlthames2/thddt

https://github.com/jlthames2/ddt