TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Attack and Defense in AWS: Chaining vulnerabilities to go beyond the OWASP 10

Date of the training: **March 16-17, 2020** in Heidelberg, Germany

Book now using the voucher code: TR20_HMTS and save an additional 5% of the current valid rate of any package!

Overview

This is an intense, hands-on, scenario-driven training on attack and defense in AWS. In this training students will learn to enumerate, exploit and pivot inside AWS. Students will also learn to detect and defend against these attacks. This training is designed to cover real world attacks where we delve deep into chaining vulnerabilities that go beyond the basics.

In this tools and techniques based training, we will cover real world attacks mimicking breaches from world over and scenarios based on our numerous penetration testing engagements which will teach the students how attackers use common footholds to get inside your cloud infra and then use the access that they have to move laterally between privileges and horizontally between services within AWS.

The training will essentially teach you how you can go beyond the OWASP Top 10 by chaining weaknesses discovered within the scope of the targets and use that to move between the attack and the data planes.

The training will also show, as an addendum to the attacks, the potential defenses that can be applied, using multiple features and services, some of which are already part of AWS. As an attacker or defender, if you have ever asked any of the following questions, this training is for you:

- Is there a process to attacking the cloud or do we go after the services as and when they are discovered?
- Is SSRF the only vulnerability to access the metadata service on EC2?
- How do I use stolen AWS secret keys to attack further?
- How do I hide cover my tracks in AWS environment?
- If I can't see a service due to security group, can I still attack it?
- How do I create better wordlists to discover and exploit S3 buckets that have uncommon names?
- Can I impersonate other users within AWS?
- Is there a way to extract secrets from AWS Lambda?
- How do I prevent credential compromise in AWS?
- How can I be sure there is no attacker already within my cloud infrastructure?
- How do I enumerate and move between accounts that are part of AWS organizations?

Highlights of the training

- Real world attacks and exploitation from popular breaches and our pentesting engagements;
- Multiple unconventional ways of gaining shells and achieving AWS account compromise;
- Chaining of vulnerabilities across services and type, going beyond the OWASP Top 10 to access the data planes;
- Hands-on and lab driven, with complete automation of the setting up of attacker tools and target labs;
- OSINT techniques to find security issues at Internet scale;
- Complete documentation and lab manuals for the scenarios covered;
- Guidance around mitigation around the attacks;
- A fun CTF to end the training that requires some out of the box thinking;

Prerequisites

- Familiarity with AWS web console;
- Familiarity with Security Testing basics and tools like Nmap, Burp Suite / OWASP ZAP;
- Comfortable using command line tools to login to servers, install packages, executing scripts and applications;
- Basics of HTTP, JavaScript;
- Basics of Networking concepts enough to understand Cloud Architecture;
- (Optional) Ideally you should have started VMs in AWS, configured S3 buckets and have an idea of IAM.

Requirements

- A laptop with a modern OS Windows 10/OSX/Linux;
- At least 8 GB RAM and 40 GB free disk space;
- Updated browsers such as Chrome, Firefox;
- Ability to connect to a wireless / wired network;
- A working AWS account activated for payments (the EC2 service should be accessible).

About the Trainers

Bharath is a Security Engineer with Appsecco. He has a strong passion for information security and building solutions that solve real world problems. Bharath is an active member and contributor at various security and developer communities including null open security community and Python Malaysia User Group. His core interest lies in Application security, Infrastructure security, Cloud Security, Reconnaissance and Protocol security. Bharath holds multiple CVEs, the latest include - CVE-2018-15635, CVE-2018-15636, CVE2018-15638, CVE-2018-15639 and CVE-2018-15641.

Riyaz Walikar currently heads the Offensive Security Team at Appsecco and is responsible for the assessment and delivery of Web and Mobile Application Security Testing engagements. He is an OSCP certified Web Application Pentester, Security evangelist and researcher. He has been active in the security community for the better part of the last 10 years. He has been actively involved with the Bangalore OWASP and null chapter for the last 7 years and is one of the OWASP and null Bangalore chapter leads. He has also been a speaker and trainer at several security conferences including OWASP AppsecUSA 2012, BlackHat Abu Dhabi 2012, Las Vegas 2015, EU 2015, Nullcon, DefCon Las Vegas 2016 and c0c0n.

Booking

Recommended online booking of trainings through:
https://troopers.de/tickets/

Voucher code: TR20_HMTS
Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code until seats have run out.

Contact

Need assistance? Don't hesitate to call us. We are fluent in English and German. +49 151 16228365 or info@troopers.de

Booking is also possible offline through your trusted partner:

HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany
+49 6022 508200 / info@hmtrainingsolutions.com
+49 6022 5089999 / www.hmtrainingsolutions.com