Course Outline

MOC 40551 A Microsoft Security Workshop: Enterprise Security Fundamentals

Course Summary

Description

This 1-day Instructor-led security workshop provides insight into security practices to improve the security posture of an organization. The workshop examines the concept of Red team – Blue team security professionals, where one group of security pros--the red team--attacks some part or parts of a company's security infrastructure, and an opposing group--the blue team--defends against the attack. Both teams work to strengthen a company's defenses. Since the goal of the two teams is to help the business attain a higher level of security, the security industry is calling this function, the Purple team.

This workshop is part of a larger series of Workshops offered by Microsoft on the practice of Security. While it is not required that you have completed any of the other courses in the Security Workshop series before taking this workshop, it is highly recommended that you start with this workshop in the series, Microsoft Security Workshop: Enterprise Security Fundamentals.

Objectives

After taking this course, students will be able to:

- Describe the current cybersecurity landscape
- Describe the assume compromise philosophy
- Identify factors that contribute to the cost of a breach
- Distinguish between responsibilities of red teams and blue teams
- Identify typical objectives of cyber attackers
- Describe a kill chain carried out by read teams
- Describe the role, goals, and kill chain activities of the blue team in red team exercises
- Describe the ways limiting how an attacker can compromise unprivileged accounts.
- Describe the methods used to restrict lateral movement.
- Describe how telemetry monitoring is used to detect attacks.
- Explain the concept of Confidentiality, Integrity, and Availability (CIA) triad.
- Describe the primary activities that should be included in organization preparations
- Identify the main principles of developing and maintaining policies.

Topics

- Understanding the cyber-security landscape
- Red Team: Penetration, Lateral Movement, Escalation, and Exfiltration
- Blue Team Detection, Investigation, Response, and Mitigation
- Organizational Preparations

Audience

This 1-day workshop is intended for IT Professionals that require a deeper understanding of Windows Security that wish to increase their knowledge level. This course also provides background in cyber-security prior to taking the other security courses in this track.

Prerequisites

In addition to their professional experience, students who take this training should already have the following technical knowledge: The current cyber-security ecosystem, analysis of hacks on computers and networks and Basic Risk Management

Duration

One day

Course Outline

MOC 40551 A Microsoft Security Workshop: Enterprise Security Fundamentals

Course Outline

I. Understanding the cyber-security landscape

In this module, you will learn about the current cybersecurity landscape and learn how adopting the assume compromise philosophy, you can you restrict an attacker's ability to move laterally between information systems and to restrict their ability to escalate privileges within those systems. The current cyber-security landscape is vast and likely impossible for any one individual to comprehend in its entirety. There are, however, several aspects of that landscape to which those interested in the fundamentals of enterprise security should pay attention.

A. Current Cyber-security Landscape
B. Assume Compromise Philosophy

II. Red Team: Penetration, Lateral Movement, Escalation, and Exfiltration

Red team versus blue team exercises involve the simulation of an attack against an organization's information system. The red team simulates and, in some cases, performs proof of concept steps taken in the attack against the organization's IT systems. The blue team simulates the response to that attack. This adversarial approach not only allows for the identification of security vulnerabilities in the way that the organization's IT systems are configured, but also allows members of the organization's information systems staff to learn how to detect and respond to attacks. In this module you will learn the Practice Red team versus Blue team approach to detecting and responding to security threats.

A. Red Team versus Blue Team Exercises
B. The Attackers Objective
C. Red Team Kill Chain

.

III. Blue Team Detection, Investigation, Response, and Mitigation

In this module you will learn about the Blue Team roles and goals in the attack exercises. You will learn the structure of an attack against an objective (Kill Chain) and the ways limiting how an attacker can compromise unprivileged accounts. You will also learn the methods used to restrict lateral movement that prevent attackers from using a compromised system to attack other systems and how telemetry monitoring is used to detect attacks.

A. The Blue Team
B. Blue Team Kill Chain
C. Restricting Privilege Escalation
D. Restrict Lateral Movement
E. Attack Detection

IV. Organizational Preparations

There are several ongoing preparations that an organization can take to improve their overall approach to information security. In this module, we will take a closer look at some of them. You will learn about a conceptual model for thinking about the security of information and how to approach information security and to prepare properly including ensuring your organization has a deliberate approach to information security.

A. CIA Triad
B. Organizational Preparations
C. Developing and Maintain Policies

Lab : Designing a Blue Team strategy