Course Outline

Module 1: 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.

Lessons

- Current Cyber-security Landscape
- Assume Compromise Philosophy

After completing this module, 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.

Module 2: 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.

Lessons

- Red Team versus Blue Team Exercises
- The Attackers Objective
- Red Team Kill Chain

After completing this module, students will be able to:

- Distinguish between responsibilities of red teams and blue teams.
- Identify typical objectives of cyber attackers.
- Describe a kill chain carried out by red teams.

Module 3: 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.

Lessons

- The Blue Team
- Blue Team Kill Chain
- Restricting Privilege Escalation
- Restrict Lateral Movement
- Attack Detection

After completing this module, students will be able to:

- Describe the Blue Team rRole, and Ggoals, and kill chain activities of the blue team in the red team exercises.
- Describe the structure of an attack against an objective (Kill Chain).
- 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.

Module 4: 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.

Lessons

- CIA Triad
- Organizational Preparations
- Developing and Maintain Policies

Lab : Designing a Blue Team strategy

After completing this module, students will be able to:

- 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.

After completing this lab, students will be able to:

1. Design a high-level approach to mitigating threats
2. Recommend tools and methodology facilitating tracking down origins of cyberattacks
3. Provide high level steps of a recovery effort
4. Recommend methods of preventing cyberattacks
5. Describe regulatory challenges that result from malware exploits