Zero to Hero for Cyber Personnel(OT)

Certification Plan

CYBERGYM

EXPECT THE UNEXPECTED

Zero to Hero for Cyber Personnel(OT)

DESCRIPTION

In today's connected world, many organizations need to operate under the constant possibility of cyber threats: Industrial espionage, Cybercrime, Hacktivism.

In order to be ready to promptly react to a cyber attack, investigate and mitigate it, and prevent similar attacks in the future – an organization needs to have in-house a competent, skilled Red Team personnel, available on-premise and on demand.

The "Cyber Red Team" training program provides its trainees with all the required tools, skills and theoretical knowledge, to become a successful Cyber Red Team member, guarding the organization and its critical assets.

TARGET AUDIENCE

- Basic knowledge with security systems
- Basic knowledge with system servers and workstations
- Familiar with network protocols
- Basic knowledge with python development
- Familiar with malware forensics methodology and technique
- Basic knowledge with website architecture

OUTCOMES

- Understanding the tools and methodology of cyber defense
- General knowledge and tools in the field of Cyber Security, attacks and malware types
- Mastering the theory and practice of Cyber Attack planning, development and life cycle management

CERTIFICATE TRAININGS

1

Defender POV

Main Goals:

During this session the trainees will get the feeling of the defender side in cyber security incident. By getting familiar with the defender side, the trainees will have a better understanding of their challenge as a red team.

Outcome:

N/A

2

Cyber Security Concepts & Methodology

Main Goals:

The training presents its participants with the solid theoretical basis required in order to learn and understand the key threats, attacks, and dangers in the cyber world, and to understand the methods and concepts of both protecting and - on the other hand, attacking, the critical data assets of the organization.

Outcome:

N/A

3

Security Monitoring & Management

Main Goals:

Getting familiar with the common tools, concepts, and methods used for monitoring and managing Cyber Security infrastructure, and learning the skills essential for effectively understand the picture and flow of a Cyber Security Incident unfolding in the organization's network.

Outcome:

The trainee will learn an implement hands-on the most important and common network monitoring tools and techniques.

4 Principles of Vulnerabilities Assessment and PENTEST

Main Goals:

The Vulnerabilities Assessment and PENTEST training allows its participants to develop understanding of the principles, methodologies, and tools of Ethical Hacking and Penetration Testing.

The trainees will get familiar with the relevant key concepts, such as exploit, vulnerability, information gathering and others.

The training combines comprehensive theoretical sessions, along with actual, hands-on experience in the controlled environment of the Cyber Arena.

Outcome:

- Able to expertly manage and investigate ongoing, complex cyberattacks and their consequences in organizations of all sizes
- Ability to execute well-designed procedures during an actual cyberattacks

5 Vulnerabilities Assessment and PENTEST – Advanced Topics

Main Goals:

Advanced penetration testing training, focusing on attacking the business logic of web applications, and techniques for bypassing filters and security systems.

Outcome:

N/A

6 PENTEST Planning & Reporting

Main Goals:

During this session the trainees will learn to plan the phases of penetration testing process (including performing scoping), and get familiar with the required parts and components of a comprehensive PENTEST report.

Outcome:

N/A

7

Cyber Attack Development Life-cycle

Main Goals:

During this session the trainees will learn how to build their own set of penetration testing tools and attacks, which will allow them to be unique and evade detection by security systems.

Outcome:

N/A

8

Advanced Persistent Threat (APT): Methodology & Development

Main Goals:

An Advanced Persistent Threat (APT) is a targeted cyber attack in which an intruder gains access to a network and remains undetected for an extended period of time. The attackers use the APT methodology and lifecycle in order to build the complete attack flow, defining its stages and targets.

The APT training provides the future Red Team specialist with a critical insight on the attack planning and execution process, understanding of which is important for developing the ability to correctly plan and execute a pen-test attack or vulnerability assessment process.

Outcome:

N/A

9 Mobile Platforms Attacks–Unique Aspects & Tools

Main Goals:

A unique training experience providing the participants with specific tools and methods, required for performing penetration testing and vulnerability assessment in the mobile environment.

The training guides the participants through all the steps and components of a mobile platform attack, such as application mapping and architecture, mobile pen-testing tools, file and binary analysis, etc.

Outcome:

N/A

10 OT-Centric Attacks – Unique Aspects & Practices

Main Goals:

During this session, the trainees will learn the unique aspects of performing Penetration testing on SCADA systems and experience a simulated cyber-attack and vulnerability assessment of computer-based supervisory control systems.

Outcome:

N/A

11

“Capture the Flag” Challenge: Graduation Training & Workshop

Main Goals:

“Capture The Flag” is a computer security/hacking competition which generally requires from its participants to implement all the tools learned during the course, in order to successfully investigate and break into a test system, and reach the attack goals defined by the trainers (capture the flags). During the activity the trainees will be split into groups, competing with each other in an activity both enjoyable and educating.

Capture The Flag is the ultimate challenge for the Red Team training program participants, allowing them to implement all the knowledge and techniques acquired during the training process in the real-life-like environment of the Cyber Arena.

Outcome:

Ability to execute well-designed procedures during an actual cyberattacks