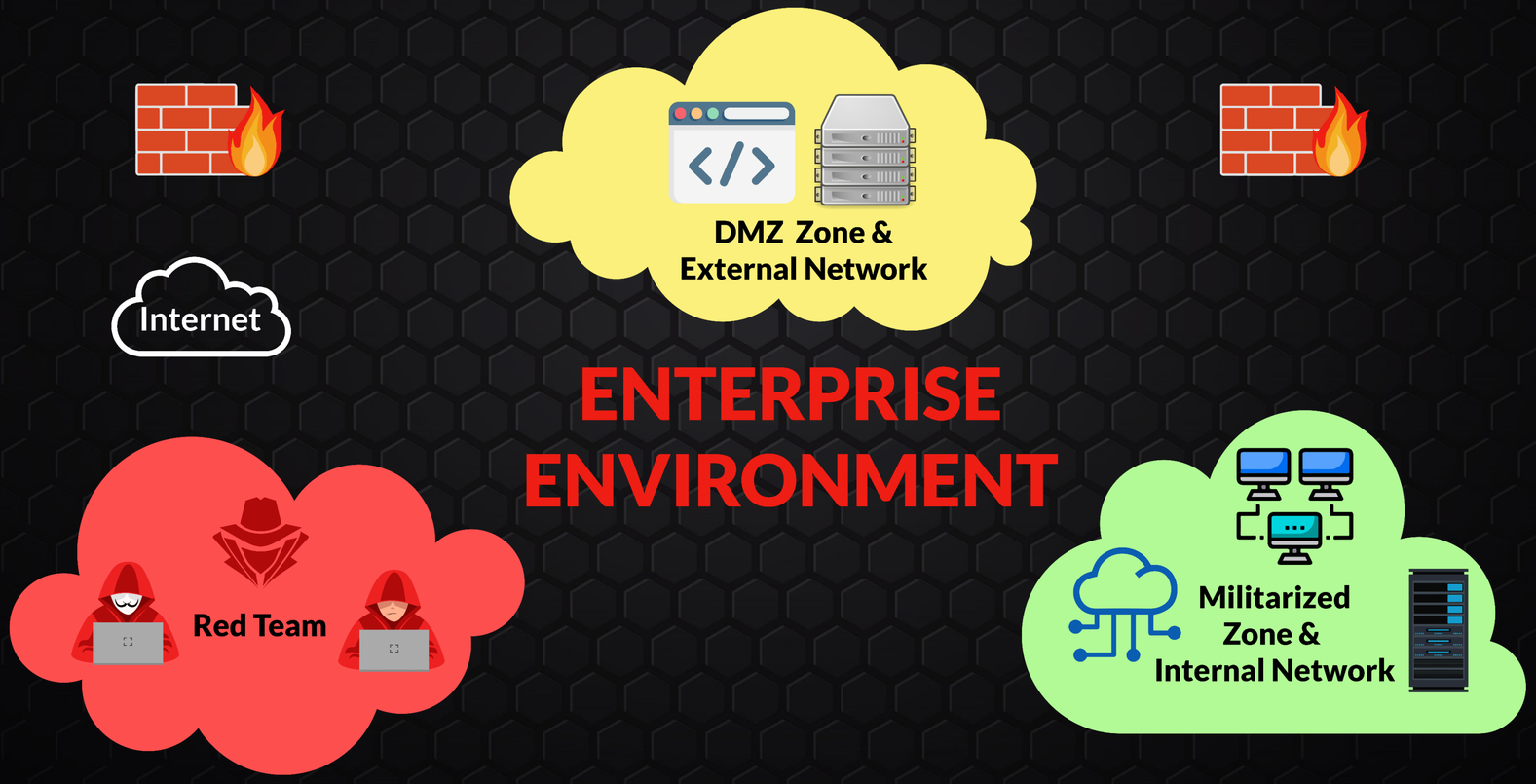
CWL
CyberWarFare Labs

Certified Red Team Analyst (CRTA)

@CyberWarFare Labs

Certified Red Team Analyst Architeture



CWL
CyberWarFare Labs

Introduction To Red Team Analyst

CWL
CyberWarFare Labs

Module 1

Introduction to Red Teaming

1.1 What is Red Teaming ?

1.2 Red Team Attack Lifecycle (Phases)

1.3 Red Team Infrastructure (Nomenclature)

1.4 Enterprise Environment Overview

1.5 Technologies Exploitation in Red Teaming

- 1.5.1 Web Technology
- 1.5.2 Network Technology
- 1.5.3 Cloud Technology
- 1.5.4 Physical Red Teaming 1.5.5 Wireless

Module 2
Red Team Lab Setup

2.1 Virtual Environment Setup and Configuration

2.2 Setting up Attacker Machine

2.3 External Red Team Lab Setup

- 2.3.1 Lab setup overview
- 2.3.2 Setting up Virtual Machines
  - A. Metasploitable Installation
  - B. Employee Machine Installation

2.4 Internal Red Team Lab Setup

2.4.1 Internal Lab setup overview

2.4.2 Active Directory Lab Setup

- A. Domain Controller
- B. Domain Joined Machine – Employee Machine Setup
- C. Domain Joined Machine – Application Server Setup

CWL
CyberWarFare Labs

Module 3

Red Teaming in External Environment

- 3.1 External Infrastructure Overview
- 3.2 Externally exposed service exploitation
  - 3.2.1 Information Gathering
  - 3.2.2 Scanning & Enumeration
  - 3.2.3 Vulnerability Assessment
  - 3.2.4 Exploitation
    - A.Web based
    - B. Network based
  - 3.2.5 Post-Exploitation
    - A.Web based
    - B. Network based

CWL
CyberWarFare Labs

Module 4

Red Teaming in Internal Environment

4.1 Internal Infrastructure Overview

4.2 Infrastructure Enumeration

- 4.2.1 Internal Network Enumeration
- 4.2.2 Active Directory Environment
- 4.3 Active Directory Phases Exploitation

CWL
CyberWarFare Labs

Module 5
Case Study

5.1 Accessing the Lab 5.2 Lab Architecture

5.3 Mapping the Lab with MITRE ATT&CK Framework

5.4 External & Internal Red Teaming

5.5 Utilizing LOLBAS for stealth persistence & Data Exfiltration

5.6 Preparing for Examination

CWL
CyberWarFare Labs

Thank You

Cyberwarfare.live