



# Certified Modern Red Team Infra Developer [CRT-ID]



@CyberWarFare Labs

# MODULE DIVISION

# Introduction

- i. Red Team & Models**
- ii. Modern Red Team Infrastructure**
- iii. Red Team Infra Components**
  - C2 Server**
  - Redirectors**
  - Payload Server**
  - Phishing Server**

# Command Control Server

- i. Introduction**
- ii. C2 Pools & Selection**
- iii. Mythic Installation**
- iv. Operator Roles**
- v. C2 Profiles**
- vi. OPSEC Safe Setup**

# Redirector

## i. Cloud Based Setup (SSL)

**AWS CloudFront**

**Azure FrontDoor CDN**

## ii. On-Premise Setup (SSL)

**NGINX**

- **Manual Setup**
- **Automated Setup**

**Custom Rules Creation**

- **Directory Based Rule**
- **User Agent & IP Based Rule**

# Payload Server

## i. Open-Source Setup

PwnDrop

## ii. Custom Setup

NGINX : Facade Files

# Phishing Server

- i. Evilginx
- ii. GoPhish
- iii. Multi-Factor Authentication Bypass

# Red Team Case Study

## **i. Full-Fledged Initial Access Operations**

- Infrastructure Overview
- Resource Development
- Successful Completion





# Thank You

Cyberwarfare.live

