



RED TEAM INFRASTRUCTURE ON THE FLY WITH REDINFRACRAFT

About CyberWarfare Labs

CW Labs is a global Infosec company specializing in practical cybersecurity learning. They provide on-demand educational services. The company has 3 primary divisions :

- 1. Learning Management System (LMS) Platform**
- 2. CWL CyberSecurity Playground (CCSP) Platform**
- 3. Infinity Learning Platform**



INFINITE LEARNING EXPERIENCE

About Speaker:

Parth Agrawal
(Cloud Security Researcher @CWL)

Is a cloud security enthusiast with a keen interest in the intricacies of cloud services offered by AWS, Azure, and GCP. Possessing a comprehensive understanding of these platforms, they are particularly drawn to exploring Red Team methodologies. Interested in Red Team methodologies, focusing on vulnerability testing and detection across external attack surfaces.

Table of Contents

- **What exactly is RedInfraCraft?**
- **Why should you use it?**
- **How does it work in practice?**
- **what are its real-world use cases?**

RedInfraCraft – Automating Red Team Infrastructure

- An open-source tool to automate the deployment of red team infrastructure.
- Supports tools like Mythic C2, PwnDrop, redirectors, and phishing setups.
- Built using Terraform and integrates with cloud platforms (multi-cloud support).
- Focused on speed, stealth, and ease of use.
- Designed by red teamers, for red teamers.

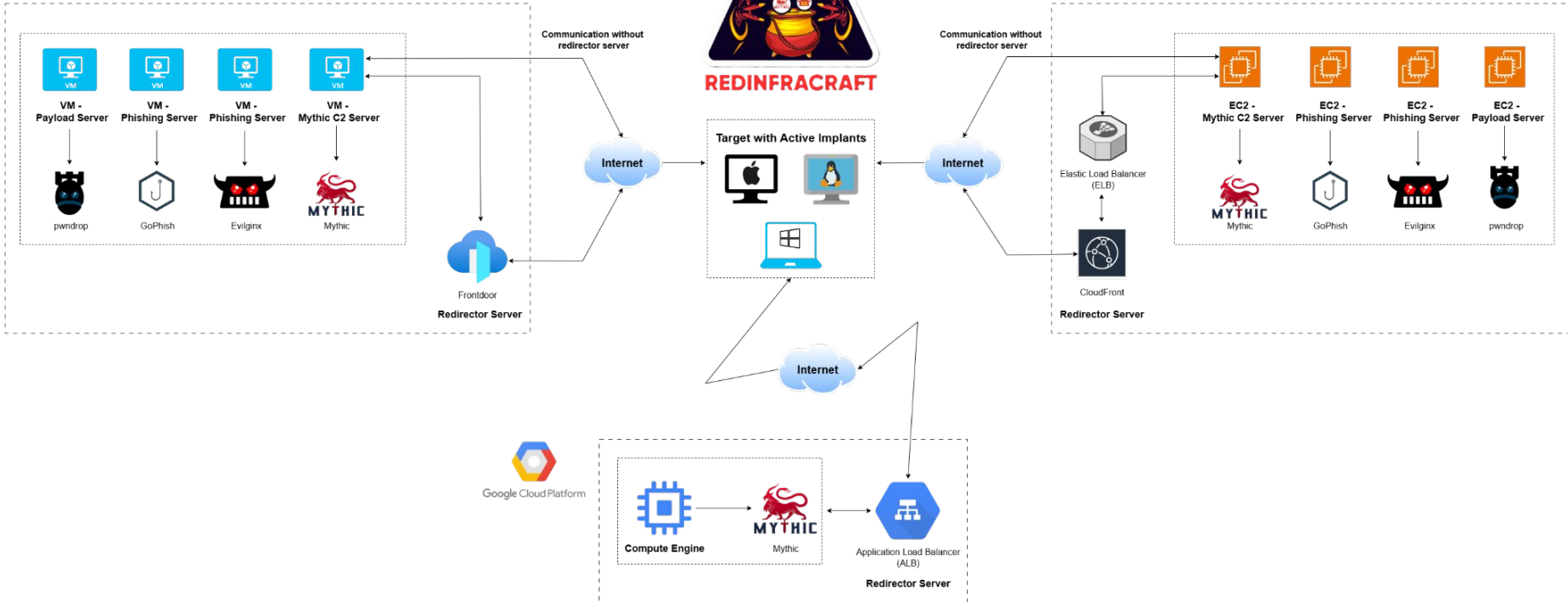
 Infrastructure as Code meets offensive security operations.




REDINFRACRAFT

Microsoft
Azure

aws



Why RedInfraCraft Stands Out

- Saves hours of manual setup time for each engagement.
 - Reduces human error in complex deployments.
 - Ensures repeatable, scalable, and stealthy infrastructure setups.
 - Seamlessly integrates TLS, redirectors, and domain fronting.
 - Great for solo red teamers and large adversary simulation teams alike.
-  Focus more on your ops, less on the infrastructure.

From Zero to C2 in Minutes

- Uses modular Terraform scripts to provision infra on AWS, Azure & GCP.
- Customizable tfvars files let you tailor deployments (region, domain, Credentials, etc.).
- One command to deploy, and one command to destroy.
- Supports Mythic C2, phishing payload hosts, and more.

 Hands-free, script-driven deployment for red team missions.

Where RedInfraCraft Makes an Impact

- Client red team engagements: Deploy C2 & redirectors in minutes.
- Time-boxed operations: Fast infra for short internal drills or competitions.
- Payload testing labs: Quickly spin up environments to test delivery and evasion.
- Training environments: Perfect for red team labs or student simulations.
- Secure cleanup: Teardown infra instantly to prevent post-engagement footprint.

 Operational speed and stealth in real-world scenarios.



Thank You

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings
please contact

support@cyberwarfare.live

To know more about our offerings, please visit: **<https://cyberwarfare.live>**