Modern Red Team Infra Development

28th Feb 2023 Webinar

About CyberWarFare Labs :

CyberWarFare Labs is an Ed-Tech Cyber Security

Focused Platform which is totally engrossed in solving

the problem of Cybersecurity by providing candidates

real-time hands-on manner Cyber Range Labs solutions.

We provide Practical Labs [Simulation of critical

infrastructure] like Healthcare, Nuclear Facility etc.

Our Offering On Courses :

- CWL CERTIFIED CYBER SECURITY ANALYST — C3SA — CYBER SECURITY ESSENTIALS
  - INTRODUCTION TO CYBER SECURITY
  - WEB APPLICATION EXPLOITATION
  - OPERATING SYSTEM EXPLOITATION
  - CLOUD PENETRATION TESTING
  - SECURITY OPERATIONS
- Windows Internals For Red Team [Beginner Edition] — CYBER SECURITY ESSENTIALS
  - Introduction to Windows Internals
  - Start Debugging in Kernel Land
  - Explore the codes in Kernel Land
  - Learn Various Kernel Data Structures
- CERTIFIED RED TEAM SPECIALIST COURSE — CYBER SECURITY ESSENTIALS
  - ADVERSARY SIMULATION LAB
  - CERTIFIED RED TEAM SPECIALIST
  - MITRE ATTACK FRAMEWORKS
  - 1 UNIQUE ATTACK PATH MANUALS
- CERTIFIED RED TEAM ANALYST COURSE — CYBER SECURITY ESSENTIALS
  - 150+ PAGES PDF
  - CERTIFIED RED TEAM ANALYST CERTIFICATE
  - RED TEAM LAB SETUP IN LOCAL ENVIRONMENT
- CERTIFIED AWS CLOUD RED TEAM SPECIALIST COURSE — CYBER SECURITY ESSENTIALS
  - 150+ PAGES PDF
  - 20+ HD HD VIDEOS
  - RED TEAMING IN AWS CLOUD ENVIRONMENT
  - CERTIFIED AWS CLOUD RED TEAM SPECIALIST CERTIFICATE
- CERTIFIED PURPLE TEAM ANALYST COURSE — CYBER SECURITY ESSENTIALS
  - RED & BLUE TEAM OPERATIONS
  - CERTIFIED PURPLE TEAM ANALYST CERTIFICATE
  - DEDICATED PURPLE TEAM TRAINING DASHBOARD
- CERTIFIED ENTERPRISE SECURITY CONTROLS ATTACK SPECIALIST — CYBER SECURITY ESSENTIALS

Our Offering On Trainings :

- HYBRID MULTI CLOUD RED TEAM
- GCP CLOUD RED TEAMING
- STEALTH OPERATIONS
- RED & BLUE JOINT OPERAION
- AZURE CLOUD RED TEAMING
- AWS CLOUD RED TEAMING

Our Offering On Mini-Course :

- ATTACK & DETECT ADVANCE PROCESS INJECTION TECHNIQUES
  - MINI-COURSE

About Speakers :

Yash Bharadwaj

Co-Founder & Technical architect at CyberWarFare Labs

With over 4.5 Years of Experience as Technologist. Highly attentive towards finding, learning and discovering new TTP's used during offensive engagements. His area of interest includes building Red / Blue team infrastructure, evading AVs & EDRs, Pwning Active Directory infrastructure, stealth enterprise networks & Multi cloud attacks. Previously he has delivered hands-on red / blue / purple team trainings / talks / workshops at Nullcon, X33fCon, NorthSec, BSIDES Chapters, OWASP, CISO Platform, YASCON. You can reach out to him on Twitter @flopyash.

- Modern Red Team Infrastructure Components

  - **Command & Control Server**

  - Payload Server

  - **Redirector Server**

  - Phishing Server

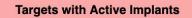 - VPNs & Proxies

  - Collaboration Tools like Slack, Discord etc

Redirection Methods

- ### Cloud Based Redirection (SSL)

  - AWS CloudFront

    - Content Delivery Network Service Offered by AWS

    - Provide secure content delivery of AWS Services like Application Load Balancers etc

    - Web Application Firewall (WAF) & Geo-Restriction can be applied on distribution

    - Secure Domain "*.cloudfront.net* " & Redirection Capability

1. AWS Infrastructure

DEMO : AWS CloudFront

- OPSEC Safe Setup

- Pointers:
  - Default Headers / Banners
  - SSL Certificates
  - Network Firewall
  - Traffic Redirection
  - Infra Network Routing
  - Geo-Fencing
    - Victim IP Range
    - Selective Headers
    - Secret Cookies

Thank You for providing your precious time!

If you like the content, please feel free to shout out & tag us at social media platforms.

For any technical questions / doubts related to the content please email us at *support@cyberwarfare.live*

For Professional Red / Purple Team Labs & Technical Training Services kindly email at *info@cyberwarfare.live*