Cyberwarfare Labs

Advanced Threat Emulation & Detection

1 Day Training Format

Abstract :

As adversarial attacks against enterprises continue to rise, the need for effective detection and investigation strategies has become critical for organizations. This training program is designed to equip participants with in-depth knowledge and practical experience, enabling them to effectively understand and counter various attack vectors that target **clouds and hosts.** Additionally, the program covers sophisticated evasion techniques employed by Advanced Persistent Threat (APT) groups, which are often the most challenging to detect.

By the end of the training, attendees will have developed a robust set of skills that allow for proactive threat identification, thereby strengthening their organization's overall security posture.

Red Team Highlights

- **Simulate Attacks Across Various Environments:**
    - **On-Premises & Cloud**

Blue Team Highlights

- **Hands-on Investigations**
- **Understand Offensive Operations**
- **Enhance Real-Time Investigation Skills**

Format : On-Site

Trainers : Manish Gupta & Yash Bharadwaj

Table of Content

iii. Applocker Bypass

d. Implant disguise tips
    i. RTLO technique
    ii. Extension / Extension spoofing

Pre-Requisites :

- Kali / Parrot VM in VMWare workstation Pro / VirtualBox (NAT mode) internet access
- An Open Mind :)

NOTE : Team will share specific setup requirements 10 days before the training

Deliverable :

- Comprehensive 150+ Page PDF
- 7 Days of Lab Access
- Lab command reference
- Cloud / On-Premise investigation & detection rules

Attendees Takeaway :

- Premium training materials + lab access (during training)
- Direct technical support over discord channel
- Investigative Mind Maps
- Detective mindset to tackle complex on-premise attacks

Trainer Infra Requirements :

- 2 Big Screens with projector
- Standard Table with 2 chairs
- Power Extension
- Whiteboard & Marker
- Separate Trainer Wi-Fi & 2 Mic

BIO

Manish Gupta is Director of CyberWarFare Labs having 8.5+ years of expertise in offensive Information Security. His Research interest includes Real World Cyber Attack Simulation and Advanced persistent Threat (APT). Previously he has delivered hands-on red / blue / purple team training / talks / workshops at Blackhat USA, DEFCON, Nullcon, BSIDES Chapters, X33fcon, NorthSec & other corporate training etc. You can reach out to him on Twitter @cyberwarfarelab

Yash Bharadwaj, Technical director at CyberWarFare Labs, With a sharp focus on building and optimizing Red and Blue team infrastructures, evading advanced security controls, and exploiting complex systems. His expertise extends to conducting and delivering hands-on Red, Blue, and Purple team trainings, talks, workshops, and research presentations at some of the most prestigious conferences in the industry, including Black Hat (Asia, USA), Nullcon, X33fCon, NorthSec, BSIDES chapters, OWASP, CISO Platform, YASCON, and more. You can reach out to him on Twitter @flopyash