ZOMBIECOP

ROCHESTON { HACKING }

WORKSHOP

Red Team / Blue Team Hacking EDR Engagements Workshop

Train your team for a Cybersecurity incident

RED TEAM /BLUE TEAM

REALISTIC ENTERPRISE NETWORK ATTACK SIMULATION.

Rocheston Red Team / Blue Team Hacking and EDR Engagements Workshop with Realistic Enterprise Network Attack Simulation.

This is a complete hands-on realistic cybersecurity workshop. The exercises and labs are highly technical. Students will walk away with troves of knowledge and skills delivered by the most powerful cybersecurity hacking platform: Rocheston CyberLabs. You will need to bring your own laptop to access the labs in the cloud.

Students will also receive Workshop Completion Excellence certificate and you can use them for your CPE (Continuing education) points.

What you will learn?

- Endpoint Security
- Configuration Assessment
- Extended Detection and Response
- File Integrity Monitoring
- Threat Intelligence
- Threat Hunting
- Threat Modeling and DevSecOps
- Cybersecurity Hygiene with RCF (Rocheston Cybersecurity Framework)
- Vulnerability Detection
- Security Operations
- SOC2 Dashboards
- Log Data Analysis
- Malware Detection
- Audit and Compliance
- Cloud Security
- Posture Management
- Workload Protection
- Container Security
- MITRE Attack Framework
- Implementing PCI-DSS and HIPAA Standards
- Implementing GDPR Standards
- Implementing CIS Standards
- Implementing NIST 800-53 Standards
- Auditing commands run by a user
- Amazon AWS infrastructure monitoring
- Detecting a brute-force attack
- Monitoring Docker
- File integrity monitoring
- Blocking a malicious actor
- Detecting unauthorized processes
- Osquery integration
- Network IDS integration
- Detecting a Shellshock attack
- Detecting an SQL Injection attack
- Slack integration
- Detecting suspicious binaries
- Detecting and removing malware using VirusTotal integration
- Vulnerability Detector
- Detecting malware using Yara integration
- Ransomware attacks
- Defacing websites
- Dark Web onion sites
- Phishing attacks
- Incident Response

HIGHLY TECHNICAL WORKSHOP

This 3 hour workshop is highly technical. You will need the skills of RCCE Cybersecurity Engineer to understand the concepts and to practice the labs.

WHY?

01

Experience a simulated cyber incident and build muscle memory. Feel the adrenaline rush of an intense, immersive, gamified experience with your entire cross-functional team.

02

Respond to real-world cyberattack scenarios, in a fusion team environment based on a security operation center. See the potential consequences of a deficit of incident response and crisis management planning and practice.

03

Understand how your solutions and teams work together. Engage with multiple tools and work as a team to investigate a cyber issue.

Train for a full-business crisis response. Collaborate with your cyber analysts, legal, PR, and executive teams during a simulated incident.

Experience the most cutting-edge security technologies and how they are applied to modern investigations. Understand how hacker tools work and how attackers compromise victims.

4

The most realistic enterprise cybersecurity attack in action.

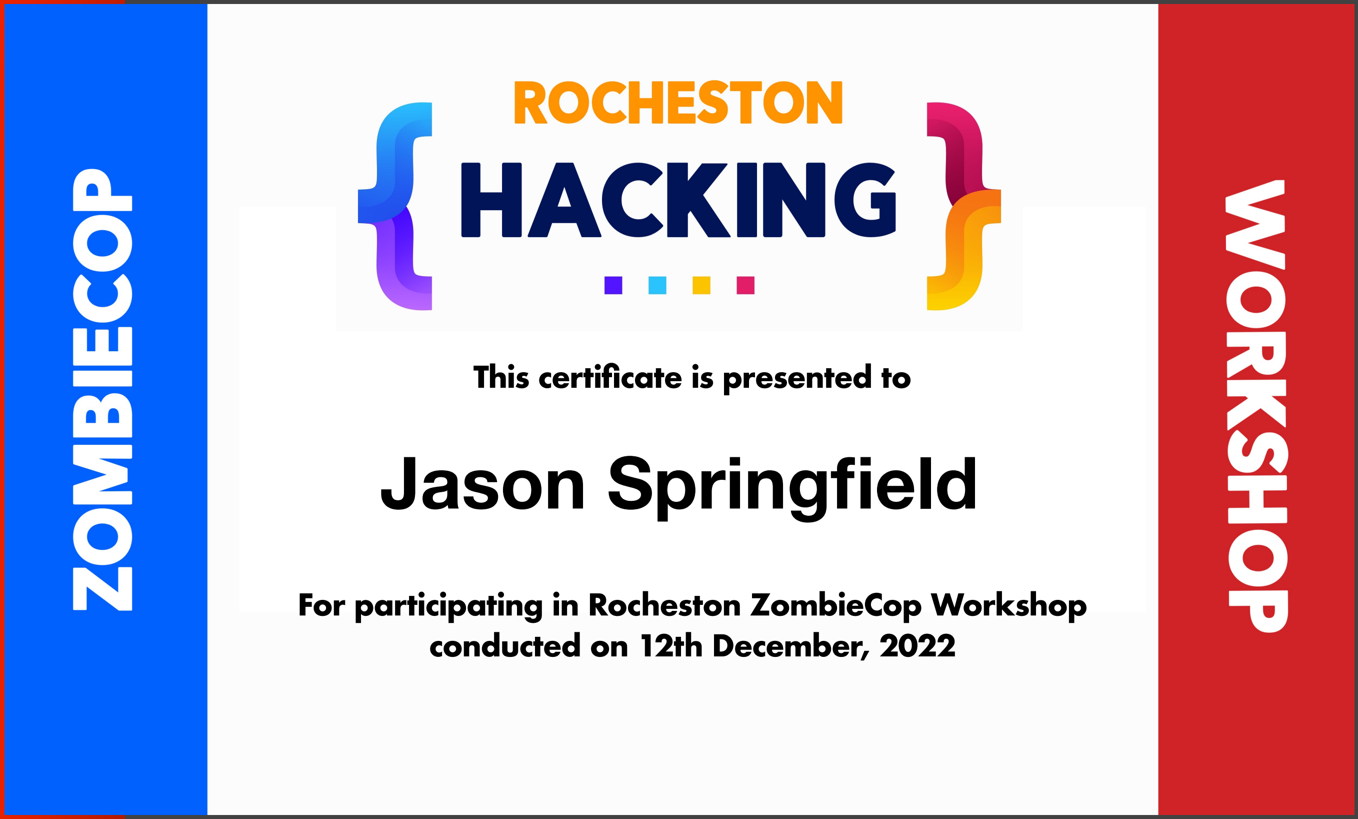
ROCHESTON RCCE
CYBER THREAT MAP
LOCAL TIME
16:45:43
RCCE
ANAB
CYBERSECURITY ENGINEER
Rochester Certified Cybersecurity Engineer
ZOMBIECOP
ROCHESTON
HACKING
Propagate the Attacks To Other Servers
Around the World At ZombieCop
files have been encrypted
LEFT 59:59:59

Participate in engaging lab exercises. Cutting edge technologies delivered in a most powerful cybersecurity platform: Rocheston CyberLabs.

5

You will be hacking a fictious video game company called: ZombieCop.Run

Here is their website:
https://zombiecop.run



ZOMBIECOP

ROCHESTON

HACKING

This certificate is presented to

Jason Springfield

For participating in Rocheston ZombieCop Workshop
conducted on 12th December, 2022

WORKSHOP

You will receive workshop certificate after the event.

Contact Us

Rocheston

https://www.rocheston.com

Book your session today. Contact Rocheston for a demo.