CWL
CyberWarFare Labs

Certified Offensive OSINT Operator (CO3)

I. Introduction to Offensive OSINT

Build a strong foundation in offensive reconnaissance and intelligence gathering.

1.1 OSINT fundamentals and offensive use cases

1.2 The OSINT lifecycle and reconnaissance stages

1.3 Types of OSINT (GEOINT, WEBINT, SOCMINT, HUMINT, CODEINT)

1.4 Offensive reconnaissance methodology

II. OPSEC for Offensive OSINT

Build resilient operational infrastructure for anonymous reconnaissance.

2.1 Threat modeling for offensive operations

2.2 Anonymous browsing (TOR, VPNs, proxies, browser OPSEC)

2.3 Browser fingerprinting and anti-detection techniques

2.4 Sock puppets and persona development

2.5 Operational domains, DNS, and email infrastructure

2.6 Cloud-based execution environments (server-based & serverless)

III. Company Profiling

Transform publicly available information into actionable organizational intelligence.

3.1 Initial target discovery and search engine dorking

3.2 Company profiling and organizational analysis

3.3 Public documents, disclosures, and online presence

3.4 Asset discovery and subsidiary mapping

3.5 Naming convention and email pattern analysis

IV. Attack Surface Discovery & Analysis

Identify and analyze an organization's externally observable attack surface.

4.1 Domain and infrastructure discovery

4.2 Cloud infrastructure reconnaissance

4.3 Internet-wide exposure analysis

4.4 Technology and service fingerprinting

4.5 Web application analysis

4.6 Source code repository analysis

4.7 Credential and exposure discovery

V. People & Social Profiling

Collect intelligence on people, roles, and organizational structure.

5.1 Company presence across public platforms

5.2 Social media intelligence (SOCMINT)

5.3 Linked intelligence and messaging platform discovery

5.4 Employee discovery and role identification

VI. Real-World Case Studies

Study how advanced threat actors leverage OSINT during intrusion operations.

6.1 Target prioritization methodology

6.2 Lazarus Group crypto developer campaign

6.3 Volt Typhoon critical infrastructure compromise

6.4 Peach Sandstorm critical infrastructure attacks

6.5 Uber Breach (2022)

VII. Automating OSINT Workflows

Build AI-assisted reconnaissance pipelines using modern automation platforms.

7.1 LLM-assisted reconnaissance and prompt engineering

7.2 AI-driven intelligence analysis

7.3 Automated reconnaissance using Maltego

7.4 Workflow automation using n8n

7.5 Domain intelligence automation

7.6 Email OSINT automation

7.7 Web application analysis automation

CWL
CyberWarFare Labs

THANK YOU

Cyberwarfare.live