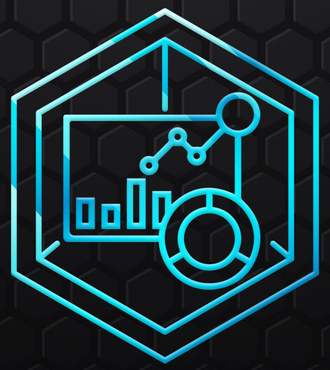
CWL
CyberWarFare Labs

Cyber Defense Analyst [CCDA]



@CyberWarFare Labs

Certified Cyber Defense Analyst [CCDA] Architecture

- FIM
- Endpoint Monitoring
- Network Monitoring
- SIEM

- Phishing Alert
- Web Targetted Alert
- Network Targetted Alert
- Host Targetted Alert

Cyber Defense Team

CWL
CyberWarFare Labs

I. INTRODUCTION TO CYBER DEFENCE

II. PHISHING THREATS INVESTIGATION AND ANALYSIS

2.1 General overview of Phishing attack

2.2 Common types of the phishing attack

2.3 Phishing Investigation techniques

2.4 Header Analysis

2.5 URL Analysis

2.6 Suspicious file download

2.7 Malicious macros investigation

2.8 Incident Response Mind map

CYBER RANGE CHALLENGES

Email Header Analysis

Credential Phishing Investigation

Suspicious Attachment Phishing Investigation

Suspicious Macros Phishing Investigation

CWL
CyberWarFare Labs

III. WEB-BASED INTRUSIONS: INVESTIGATIVE STRATEGIES AND ANALYSIS

CYBER RANGE CHALLENGES

Subdomain Enumeration

Admin Page access detected

SQL-Map activity detected

Vulnerability Enumeration activity detected

File Inclusion activity detected

Command Injection activity detected

CWL
CyberWarFare Labs

IV. UNVEILING NETWORK INTRUSIONS: METHODS AND ANALYTICAL APPROACHES

4.1 General overview of Network based attack

4.2 Common types of the Network based attacks

4.3 Working of Network Defence

4.4 Incident response Mind-Map

4.5 Network Scan activity investigation

4.6 Log4J investigation

4.7 Bind Shell investigation

CYBER RANGE CHALLENGES

NMAP Detection

DOS investigation

Suspected Data exfiltration detected

Netcat activity detected

Service brute forcing

CWL
CyberWarFare Labs

V. DECODING HOST-BASED INTRUSIONS: TECHNIQUES AND ANALYTICAL METHODS

5.1 General overview of Host based attack

5.2 Common types of the Host based attacks

5.3 Host attack Investigation

5.4 Working of EDR & XDR

5.5 Incident response Mind-Map

CYBER RANGE CHALLENGES

Suspicious File activity detected

Suspected .SH file detected

Suspicious Scheduled task detected

Suspicious Linpeas activity detected

Multiple Remote Failed Login Detected

Suspicious PowerShell activity detected

CWL
CyberWarFare Labs

CYBER RANGE CHALLENGES

Password File Modification Detected

File modification activity Detected

CWL
CyberWarFare Labs

Thank You

Cyberwarfare.live