# CYBERSECURITY ASSESSMENT REPORT

## Comprehensive Threat Simulation & Vulnerability Analysis

Performed by IRIS - Intrusion Risk Identification System

**Client Organization:** DR Maritime Assets
**Target Environment:** 138.248.175.103
**Assessment Date:** December 16, 2025
**Report Generated:** November 28, 2026 at 12:28 PM
**Assessment Type:** Comprehensive APT Simulation
**Scan ID:** 55

**CONFIDENTIAL SECURITY ASSESSMENT**

This document contains sensitive security information about the assessed environment. It should be treated as confidential and distributed only to authorised personnel.

# EXECUTIVE SUMMARY

This report presents the results of a comprehensive cybersecurity assessment performed on 138.248.175.103 for DR Maritime Assets. The assessment utilised advanced penetration testing methodologies and tools to identify potential security vulnerabilities.

### *Key Findings Summary*

| Metric | Count | Risk Level |
|---|---|---|
| Hosts Discovered | 1 | Info |
| Open Ports Found | 2 | Low-Medium |
| Services Identified | 0 | Info |
| Network Vulnerabilities | 0 | High |
| SMB Vulnerabilities | 0 | Critical |
| Web Vulnerabilities | 0 | Medium-High |
| Weak Credentials Found | 0 | Critical |

**OVERALL RISK LEVEL: MINIMAL**

# DETAILED TECHNICAL FINDINGS

### *Network Discovery Results*

Masscan discovered 1 responsive host(s)
Host 138.248.175.103: 2 open ports - 1194/tcp, 1723/tcp

### *Service Enumeration Results*

Host: 138.248.175.103 - OS: FreeBSD 11.2-RELEASE
Open ports found: 2

### *Network Vulnerabilities Detected*

No critical network vulnerabilities detected

### *Web Application Analysis*

### *SMB/NetBIOS Analysis Results*

### *Credential Security Assessment*

# SECURITY RECOMMENDATIONS

### *1. [LOW] Maintain security posture*

Category: General Security
Continue regular security assessments and monitoring. Implement security best practices.