CYBERSECURITY ASSESSMENT REPORT

Comprehensive Threat Simulation & Vulnerability Analysis

Performed by IRIS - Intrusion Risk Identification System

Client Organization: tester3
Target Environment: 192.168.1.97
Assessment Date: August 19, 2025
Report Generated: November 28, 2026 at 12:28 PM
Assessment Type: Comprehensive APT Simulation
Scan ID: 52

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 192.168.1.97 for tester3. 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	8	Low-Medium
Services Identified	0	Info
Network Vulnerabilities	2	High
SMB Vulnerabilities	2	Critical
Web Vulnerabilities	0	Medium-High
Weak Credentials Found	0	Critical

OVERALL RISK LEVEL: CRITICAL

DETAILED TECHNICAL FINDINGS

Network Discovery Results

Masscan discovered 1 responsive host(s)
Host 192.168.1.97: 8 open ports - 139/tcp, 445/tcp, 3389/tcp, 5040/tcp, 5985/tcp, 7680/tcp, 35621/tcp, 35623/tcp

Service Enumeration Results

Host: 192.168.1.97 - OS: FreeBSD 11.2-RELEASE
Open ports found: 8

Network Vulnerabilities Detected

[CRITICAL] CVE: CVE-2024-6387...
[CRITICAL] CVE: CVE-2024-6387...

Web Application Analysis

SMB/NetBIOS Analysis Results

Credential Security Assessment

SECURITY RECOMMENDATIONS

1. [HIGH] Remediate network vulnerabilities

Category: Network Security
Found 2 network vulnerability(ies). Apply security patches and harden network services.