CYBERSECURITY ASSESSMENT REPORT

Comprehensive Threat Simulation & Vulnerability Analysis

Performed by IRIS - Intrusion Risk Identification System

Client Organization: tester4
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: 53

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 tester4. 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	19	Low-Medium
Services Identified	12	Info
Network Vulnerabilities	8	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: 19 open ports - 135/tcp, 139/tcp, 445/tcp, 3389/tcp, 5040/tcp, 5357/tcp, 5985/tcp, 7680/tcp, 35621/tcp, 35623/tcp, 47001/tcp, 49664/tcp, 49665/tcp, 49666/tcp, 49668/tcp, 49669/tcp, 49676/tcp, 49677/tcp, 64925/tcp

Service Enumeration Results

Host: 192.168.1.97 - OS: FreeBSD 11.2-RELEASE
Open ports found: 19
Port 135/tcp: msrpc service
Port 135/tcp: msrpc Service
Port 139/tcp: netbios-ssn Service
Port 139/tcp: netbios-ssn service
Port 445/tcp: microsoft-ds? Service
Port 445/tcp: microsoft-ds? service
Port 3389/tcp: ms-wbt-server service
Port 3389/tcp: ms-wbt-server Service
Port 5040/tcp: unknown service
Port 5357/tcp: http service
Port 5357/tcp: http Service
Port 5985/tcp: http service
Port 5985/tcp: http Service
Port 7680/tcp: pando-pub? service
Port 35621/tcp: unknown service
Port 35623/tcp: unknown service
Port 47001/tcp: http service
Port 49664/tcp: msrpc service
Port 49665/tcp: msrpc service
Port 49666/tcp: msrpc service
Port 49668/tcp: msrpc service
Port 49669/tcp: msrpc service
Port 49676/tcp: msrpc service
Port 49677/tcp: msrpc service
Port 64925/tcp: msrpc service

Network Vulnerabilities Detected

[CRITICAL] CVE: CVE-2024-6387...
[CRITICAL] CVE: CVE-2024-6387...
[CRITICAL] CVE: CVE-2024-6387...
[CRITICAL] CVE: CVE-2024-6387...
[CRITICAL] CVE: CVE-2024-6387...
[CRITICAL] CVE: CVE-2024-6387...
[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 8 network vulnerability(ies). Apply security patches and harden network services.