WiFi Security Deep Analysis Report

Network: 5a:72:46:d6:d0:33

Analysis ID:	4e8557cf-fe79-4719-80b7-03a7af6629dd
Generated:	2025-08-17 03:14:55 UTC
Security Score:	83.0/100
Threat Level:	NO_RISK
AI Models Used:	7

Security Score: 83.0/100

Executive Summary

The WiFi network '5a:72:46:d6:d0:33' demonstrates strong security posture with a score of 83.0/100. This assessment utilized 7 specialized AI models with an ensemble confidence of 0.0%. High-priority security issues were identified (1 high severity).

Metric	Value	Status
Security Score	83.0/100	Excellent
Threat Level	NO_RISK	Secure
AI Confidence	0.0%	Low
Vulnerabilities	2	Few
Recommendations	0	None

Network Details

Basic Information

Property	Value
SSID	5a:72:46:d6:d0:33
BSSID	Unknown
Signal Strength	-30 dBm
Frequency	2437 MHz
Channel	6
Encryption	Unknown
Authentication	Unknown

Security Configuration

Security Feature	Status
Encryption Type	Unknown
Cipher Suite	Unknown
WPA3 Support	No
PMF Enabled	No
WPS Enabled	No
Security Score	10/100

AI Analysis Results

Ensemble Prediction

The ensemble AI model predicts: ERROR with 0.0% confidence. Risk score: 0.0/10

Model consensus: Weak (33.3% agreement) with 3 models participating.

Confidence Metrics

Metric	Value
Ensemble Confidence	0.0%
Model Agreement	3333.3%
Data Quality	60.0%

Individual Model Predictions

Model Name	Prediction	Confidence	Risk Score	Model Type
Cnn Final	CREDENTIAL_COMPROMISE	98.8%	15.8	TENSORFLOW
Lstm Main	ERROR	0.0%	0.0	TENSORFLOW
Lstm Production	ERROR	0.0%	0.0	TENSORFLOW
Gnn	ERROR	0.0%	0.0	TENSORFLOW
Cnn Lstm Hybrid	ERROR	0.0%	0.0	TENSORFLOW
Random Forest	0	43.0%	0.9	SKLEARN
Gradient Boosting	3	53.9%	4.3	SKLEARN

Model Descriptions

Cnn Final: CNN Final - Pattern recognition in network traffic and security features

Lstm Main: LSTM Main - Temporal behavior analysis and sequence prediction

Lstm Production: LSTM Production - Optimized temporal analysis for real-time threats

Gnn: Graph Neural Network - Network topology and relationship analysis

Cnn Lstm Hybrid: CNN-LSTM Hybrid - Combined spatial-temporal analysis

Random Forest: Random Forest - Tree-based ensemble classifier

Gradient Boosting: Gradient Boosting - Sequential boosting classifier

Risk Assessment

Overall Security Score: 83.0/100 (Strong security posture) Threat Level: NO_RISK

Risk Breakdown

Risk Category	Score	Level
Encryption Risk	0.0/100	Minimal
Topology Risk	10.0/100	Minimal
Traffic Risk	5.0/100	Minimal
Configuration Risk	20.0/100	Low
AI Risk Assessment	0.0/10	Minimal

Identified Vulnerabilities

High Severity Vulnerabilities

CREDENTIAL_COMPROMISE (Source: AI Model: cnn_final) CREDENTIAL_COMPROMISE detected by cnn_final with 98.8% confidence Confidence: 98.8%

Medium Severity Vulnerabilities

3 (Source: AI Model: gradient_boosting) 3 detected by gradient_boosting with 53.9% confidence Confidence: 53.9%

Security Recommendations

No specific recommendations were generated.

Compliance Status

Overall Compliance Status: Compliant Compliance Score: 90/100

Standards Compliance

Standard	Status
PCI DSS	Compliant
NIST	Compliant
ISO27001	Compliant

Technical Appendix

Analysis Metadata

Property	Value
Models Used	cnn_final, lstm_main, lstm_production, gnn, cnn_lstm_hybrid, random_forest
Analysis Depth	comprehensive
Data Sources	network_scan, traffic_analysis, topology_mapping, ai_models
Analysis Duration	0.0 seconds

Data Collection Summary

Traffic Analysis: 1250 packets captured over 30 seconds. Dominant protocol: HTTP (45.2%)

Disclaimer

This report is generated by automated AI analysis and should be used as a security assessment tool. Results should be validated by security professionals. The analysis is based on network data collected at the time of the scan and may not reflect current network status.