PenDonn

Penetration Testing Report

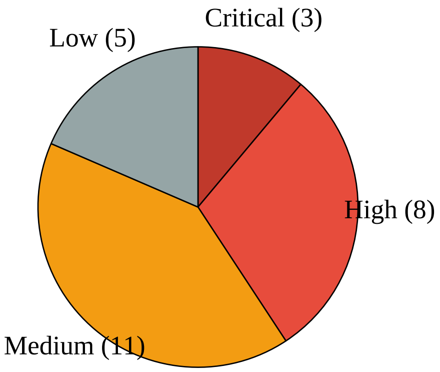
Report Date:	December 24, 2025
Generated By:	PenDonn Automated System
Report Type:	Comprehensive Security Assessment

LEGAL DISCLAIMER: This report contains sensitive security information and should be handled with care. Unauthorized access to computer networks is illegal. This testing was authorized and performed for security assessment purposes only.

Executive Summary

This report presents the findings from an automated penetration test conducted using PenDonn. The assessment identified **15** wireless networks, captured **8** handshakes, and cracked **3** passwords.

Metric	Count
Networks Discovered	15
Handshakes Captured	8
Passwords Cracked	3
Network Scans	5
Critical Vulnerabilities	3
High Vulnerabilities	8
Medium Vulnerabilities	11
Low Vulnerabilities	5



Discovered Networks

SSID	BSSID	Channel	Encryption	Signal
HomeWiFi_5G	AA:BB:CC:DD:EE:01	36	WPA2	-45
NETGEAR84	AA:BB:CC:DD:EE:02	6	WPA2	-52
TP-Link_Guest	AA:BB:CC:DD:EE:03	11	Open	-68
Office_WiFi	AA:BB:CC:DD:EE:04	1	WPA3	-55
SmartHome_IoT	AA:BB:CC:DD:EE:05	6	WPA2	-62
Basement_AP	AA:BB:CC:DD:EE:06	11	WPA2	-75
Guest_Network	AA:BB:CC:DD:EE:07	1	Open	-58
SecureNet_5G	AA:BB:CC:DD:EE:08	149	WPA2	-48

Captured Handshakes

SSID	BSSID	Captured	Status
HomeWiFi_5G	AA:BB:CC:DD:EE:01	2025-12-24T18:28:44	Cracked
NETGEAR84	AA:BB:CC:DD:EE:02	2025-12-24T18:45:44	Cracked
Office_WiFi	AA:BB:CC:DD:EE:04	2025-12-24T19:01:44	Pending
SmartHome_IoT	AA:BB:CC:DD:EE:05	2025-12-24T19:18:44	Cracked
Basement_AP	AA:BB:CC:DD:EE:06	2025-12-24T19:35:44	Pending
SecureNet_5G	AA:BB:CC:DD:EE:08	2025-12-24T19:58:44	Pending

Cracked Passwords

HomeWiFi_5G: Summer2024! (Cracked: 2025-12-24T19:58:44)

NETGEAR84: password123 (Cracked: 2025-12-24T19:31:44)

SmartHome_IoT: admin1234 (Cracked: 2025-12-24T20:45:44)

Network Scans

Scan #1 - HomeWiFi_5G (2025-12-24T19:53:44)

Hosts found: 12

Scan #2 - NETGEAR84 (2025-12-24T20:08:44)

Hosts found: 8

Scan #3 - Office_WiFi (2025-12-24T20:25:44)

Hosts found: 25

Scan #4 - SmartHome_IoT (2025-12-24T20:41:44)

Hosts found: 6

Scan #5 - Guest_Network (2025-12-24T20:58:44)

Hosts found: 3

Vulnerabilities

CRITICAL Severity (3)

- **192.168.1.1** (HTTP) - Default Credentials: Router accessible with default credentials: admin/admin
- **192.168.1.105** (SMB) - VPN Credentials Found: VPN configuration file found on SMB share: company-vpn.ovpn
- **192.168.1.254** (SNMP) - Information Disclosure: SNMP accessible with community string "public"

HIGH Severity (8)

- **192.168.1.50** (FTP) - Anonymous Access: FTP server allows anonymous access with read/write permissions
- **192.168.1.1** (UPnP) - Exposed UPnP: UPnP service exposed - port forwarding possible
- **192.168.1.105** (SMB) - SSH Keys Found: Private SSH keys found on SMB share: id_rsa, id_ed25519
- **192.168.1.200** (HTTP) - Weak Credentials: IP Camera accessible with credentials: admin/12345
- **192.168.1.15** (DNS) - Open Recursion: DNS server allows recursive queries (amplification risk)
- **192.168.1.25** (SSH) - Weak Configuration: SSH server allows password authentication
- **192.168.1.88** (HTTP) - Directory Listing: Web server has directory listing enabled
- **AA:BB:CC:11:22:33** (bluetooth) - Bluetooth Injection Risk: Bluetooth keyboard vulnerable to injection attacks

MEDIUM Severity (11)

- **192.168.1.100** (HTTP) - Missing Headers: Web application missing security headers (X-Frame-Options, CSP)
- **192.168.1.150** (SMB) - Null Session: SMB server allows null session enumeration
- **192.168.1.20** (HTTP) - Outdated Software: Web server running outdated Apache 2.4.25
- **192.168.1.30** (SSH) - Outdated Software: SSH server running OpenSSH 7.4 (multiple CVEs)
- **192.168.1.55** (HTTP) - Information Disclosure: Server banner reveals exact version information
- **AA:BB:CC:44:55:66** (bluetooth) - Insecure Bluetooth Service: Device exposes OBEX File Transfer service
- **192.168.1.75** (SNMP) - Weak Community String: SNMP accessible with community string "private"

- **192.168.1.90** (HTTP) - HTTP Methods: Web server allows potentially dangerous HTTP methods
- **192.168.1.110** (SMB) - Password Files: Password-related files found on SMB share
- **192.168.1.125** (DNS) - Zone Transfer: DNS server allows zone transfer (AXFR)
- **192.168.1.135** (FTP) - Weak Credentials: FTP accessible with credentials: ftp/ftp

LOW Severity (5)

- **192.168.1.10** (HTTP) - SSL/TLS Issues: Web server supports TLS 1.0/1.1 (deprecated)
- **192.168.1.45** (SSH) - Banner Information: SSH banner reveals OS and version information
- **AA:BB:CC:77:88:99** (bluetooth) - Information Disclosure: Bluetooth device "John's iPhone" discoverable
- **192.168.1.65** (HTTP) - Cookie Settings: Cookies missing Secure and HttpOnly flags
- **192.168.1.80** (Web) - Clickjacking: Application vulnerable to clickjacking attacks

Security Recommendations

- Use WPA3 encryption for all WiFi networks where supported
- Implement strong, unique passwords (minimum 16 characters)
- Disable WPS (WiFi Protected Setup) on all access points
- Enable network segmentation to isolate critical systems
- Regularly update firmware on all network devices
- Implement MAC address filtering as an additional security layer
- Use a firewall and intrusion detection system
- Disable unnecessary services and close unused ports
- Implement regular security audits and penetration testing
- Enable logging and monitoring for suspicious activity

End of Report - Generated by PenDonn