Comprehensive Penetration Test Report

Target System: 192.168.1.100
Generated: 2025-07-13 16:23:32
Total Test Sessions: 8
Latest Session Duration: 0
Total Commands Executed: 8

■ Executive Summary

This comprehensive analysis combines data from **8 penetration test sessions** against the target system. The assessment revealed critical database services and potential security exposures requiring immediate attention.

■ Critical Findings

- **MongoDB Database Exposed** on non-standard port
- **Service Authentication Status Unknown**
- **Potential Unauthorized Access Risk**

■ Technical Analysis

Open Ports Discovered

- **Port 8080/tcp:** http
- **Port 27018/tcp:** mongod?

Service Details

MongoDB Database Server (Port 27018)

Analysis Results:
- Service responds to HTTP requests with message about native driver port
- Multiple security scripts attempted (brute force, database enumeration)
- Authentication mechanism requires further investigation
- Service responds to HTTP requests with message about native driver port
- Multiple security scripts attempted (brute force, database enumeration)
- Authentication mechanism requires further investigation

Security Assessment

Attempted Security Tests

8. 8. Command #8
Timestamp: 2025-07-11 16:00:22.999101

Command: nmap -sV -p 27018 --script mongodb-* 127.0.0.1

Identified Issues

1. **Database Service Exposure**: MongoDB accessible on localhost
2. **Unknown Authentication State**: Security scripts failed to complete
3. **Service Fingerprinting**: Unusual port configuration (27018 instead of 27017)

Failed Security Tests

- |_mongodb-brute: ERROR: Script execution failed (use -d to debug)
- |_mongodb-databases: ERROR: Script execution failed (use -d to debug)
- |_mongodb-info: ERROR: Script execution failed (use -d to debug)
- |_mongodb-brute: ERROR: Script execution failed (use -d to debug)
- |_mongodb-databases: ERROR: Script execution failed (use -d to debug)

■ Detailed Command Progression

The AI orchestrator executed the following analysis sequence:

1. Command #1
Timestamp: 2025-07-13 15:27:32.681184
Command: nmap -sS -p- -oN nmap_initial_scan 192.168.1.100
2. Command #2
Timestamp: 2025-07-13 15:27:44.580954
Command: nmap -Pn -sT -vv -oN nmap_initial_tcp_scan 192.168.1.100
3. Command #3
Timestamp: 2025-07-11 16:23:01.146688
Command: nmap -sV -p 8080,27018 -oN nmap_service_scan 127.0.0.1
4. Command #4
Timestamp: 2025-07-11 16:23:54.375677
Command: gobuster dir -u http://127.0.0.1:8080 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 10
5. Command #5
Timestamp: 2025-07-11 16:23:58.359528
Command: gobuster dir -u http://127.0.0.1:8080 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
6. Command #6
Timestamp: 2025-07-11 16:24:01.437395
Command: gobuster dir -u http://127.0.0.1:8080 -w /usr/share/wordlists/dirb/common.txt
7. Command #7
Timestamp: 2025-07-11 16:24:05.248555
Command: nmap -sV -p 8080,27018 -oN nmap_service_scan 127.0.0.1
8. Command #8
Timestamp: 2025-07-11 16:00:22.999101
Command: nmap -sV -p 27018 --script mongodb-* 127.0.0.1

■ Risk Assessment

High Risk

- **MongoDB Database**: Potentially accessible database service
- **Unknown Authentication**: Unable to determine if authentication is enabled

Medium Risk

- **Non-standard Port**: Service running on port 27018 instead of default 27017
- **Service Fingerprinting**: Database service detectable through port scanning

Remediation Required

- **Authentication Verification**: Confirm MongoDB authentication is enabled
- **Access Control**: Implement proper network access restrictions
- **Configuration Review**: Audit MongoDB configuration for security hardening
- **Monitoring**: Implement database access logging and monitoring

■ Test Statistics

- **Total Commands Executed:** 8
- **Session Duration:** 0
- **Files Generated:** 29
- **Services Identified:** 2
- **Security Scripts Attempted:** 1

■ Conclusion

The penetration test successfully identified a MongoDB database service running on the target system. While security scripts were unable to complete their analysis (suggesting possible authentication), the service remains a critical asset requiring security review and hardening.

Priority Actions:
1. Verify MongoDB authentication configuration
2. Review database access logs
3. Implement network segmentation if not already present
4. Consider moving to standard port (27017) if appropriate

Report generated by AI-Powered Cybersecurity Operations Orchestrator