PASSWORD SECURITY AUDIT REPORT

Evaluator: Bighiu Rares

Student UAIC

Scope: Internal Password Strength Audit

Date: November 28, 2025

Objective

The objective of this audit is to evaluate password strength within the target infrastructure and identify weak credentials that can be exploited by attackers through offline cracking techniques.

Methodology

The following cracking techniques and tools were used during the password audit:

- **Dictionary Attack** (rockyou.txt dataset)
- **Hybrid Combinator Attack** (name + year patterns)
- **Mask Attack** for predictable structures (`?l?l?l?l?l?l?d?d`)

Tools Used:

- John the Ripper (6 sha512crypt hashing)
- Hashcat (demonstration on MD5 / NTLM)
- GNU/Linux CLI utilities for hash extraction and cleanup

Results

Total passwords tested	47
Compromised successfully	20
Compromise rate	42.55%
Time required	Under 15 minutes

Examples of Compromised Passwords

The following examples illustrate weak patterns commonly found in enterprise environments:

- `iloveyou`
- `andrei2005`
- `parola123`

Risk Impact

Weak credentials may enable:

- Unauthorized lateral movement
- Privilege escalation to administrative accounts
- Credential reuse attacks across internal or external systems
- Full compromise from a single initial weak account

Recommendations

The following corrective security measures are recommended:

- Mandatory **Multi-Factor Authentication (MFA)**
- Enforce minimum **12+ character password policy**
- Disallow predictable patterns (name + birth year)
- Implement **password managers**
- Conduct periodic automated credential audits
- User security awareness training

Management Summary

The audit demonstrates that **42.55%** of evaluated passwords were cracked using standard offline password-cracking techniques. Immediate remediation is recommended to prevent credential-based attacks.

Prepared by:
Bighiu Rares
Student UAIC