Password Audit

PENTEST REPORT

Executed by Cerberus Security

SUNDAY, DECEMBER 10, 2023

MODIFICATIONS HISTORY

Version	Date	Author	Description
0.1	12/10/2023	Daniel Scheidt	Initial Version
0.2	12/10/2023	Daniel Scheidt	Technical Details
1.0	12/10/2023	Daniel Scheidt	Finalization

TABLE OF CONTENTS

General Information

Scope

Testcompany has mandated us to perform security tests on the following scope:

- mcafeelab.local

Organization

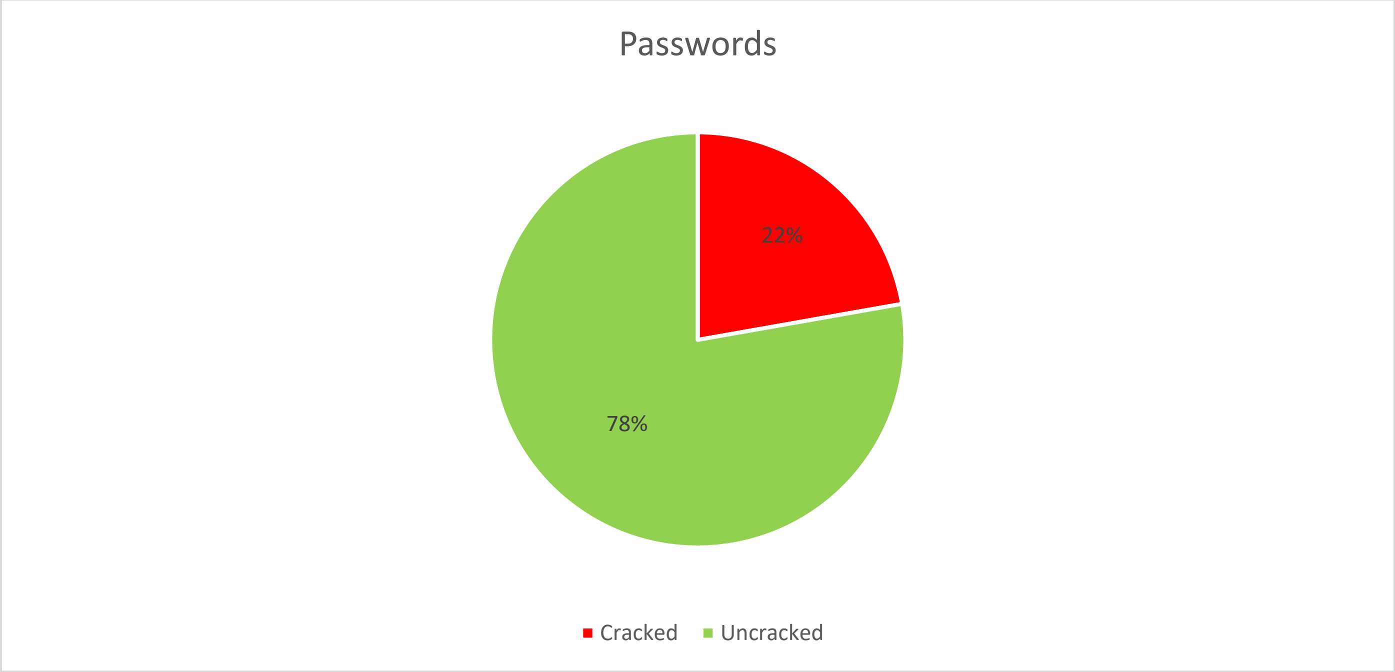
The testing activities were performed between 12/09/2023 and 12/10/2023.

Executive Summary

Cerberus Security was tasked with conducting a password audit for the domain *mcafeelab.local*. The testing activities were performed between 12/09/2023 and 12/09/2023.

The goal is the get an overview of the overall security posture regarding possibly weak passwords.
Conclusions can be drawn if all accounts follow the password rules in place.
This also allows to detect blind spots that might occur if certain conditions are met, so that rules do not apply to certain accounts.

The tests include checks for well known passwords, as well as combinations with certain rules and brute-force attacks against the hashed passwords values.

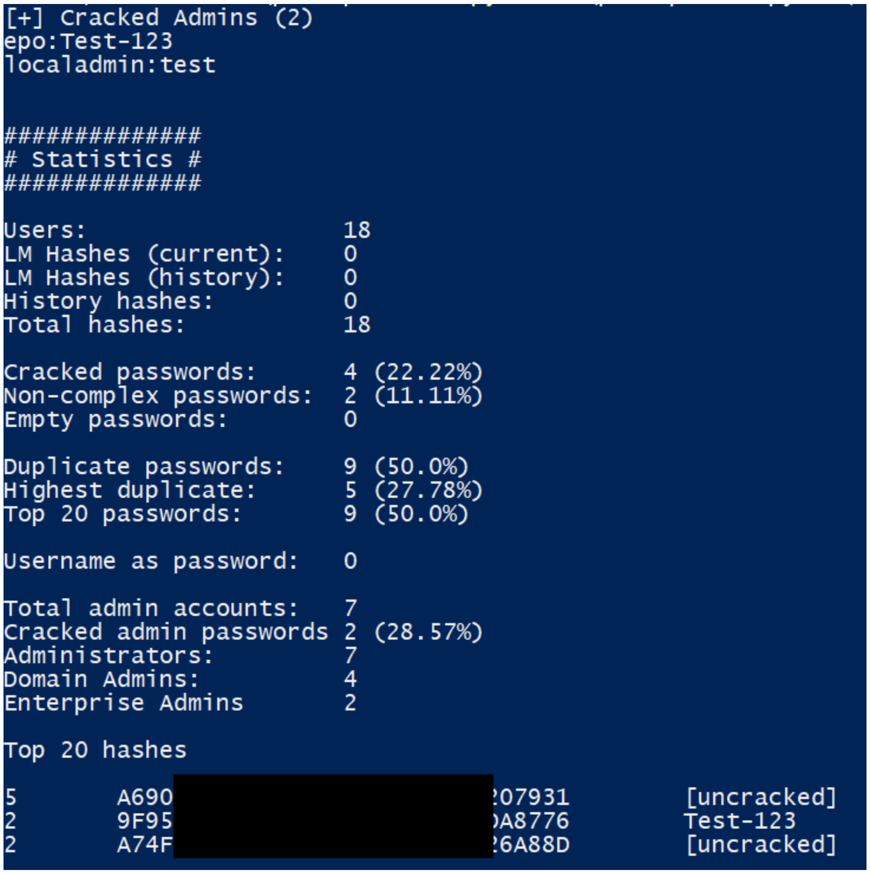


DETAILS

Out of 18 hashes that were obtained from the *ntds.dit* database, it was possible to retrieve the clear text credentials from 4 of them.
Out of those 4 there were two administrative accounts with weak passwords which should urgently be checked:

Epo:Test-123
localadmin:test

The following overview shows the overall outcome of the password analysis.



```
[+] Cracked Admins (2)
epo:Test-123
localadmin:test


##############
# Statistics #
##############

Users:                   18
LM Hashes (current):     0
LM Hashes (history):     0
History hashes:          0
Total hashes:            18

Cracked passwords:       4 (22.22%)
Non-complex passwords:   2 (11.11%)
Empty passwords:         0

Duplicate passwords:     9 (50.0%)
Highest duplicate:       5 (27.78%)
Top 20 passwords:        9 (50.0%)

Username as password:    0

Total admin accounts:    7
Cracked admin passwords  2 (28.57%)
Administrators:          7
Domain Admins:           4
Enterprise Admins        2

Top 20 hashes

5       A690[redacted]07931        [uncracked]
2       9F95          A8776        Test-123
2       A74F          6A88D        [uncracked]
```

FIGURE 1: PASSWORD AUDIT STATISTICS

The following passwords were calculated to their cleartext value from the hashes:

Password123!
Summer20024
Test-123
test