SAP ® Cybersecurity Virtual Internship Program
Vulnerability Assessment Report (Capstone Project)

Created by: Joseph Martinez

Date: June 16th, 2022

LinkedIn: https://www.linkedin.com/in/ofcljm/

Version 1.0

Confidentiality Statement

This document is the exclusive property of ***Joseph Martinez*** (*https://www.linkedin.com/in/ofcljm/*). This document contains non-confidential simulated results to display how a real vulnerability assessment is conducted. Duplication, redistribution, or use, in whole or in part, in any form, shall be permitted to share for public use and project showcase.

Joseph Martinez may share this document with auditors under public disclosure to demonstrate Vulnerability Assessment compliance.

Disclaimer

A Vulnerability Assessment is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
CRITICAL	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
HIGH	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Scope

Assessment	Details
Internal Vulnerability Scan	10.10.1.1/24

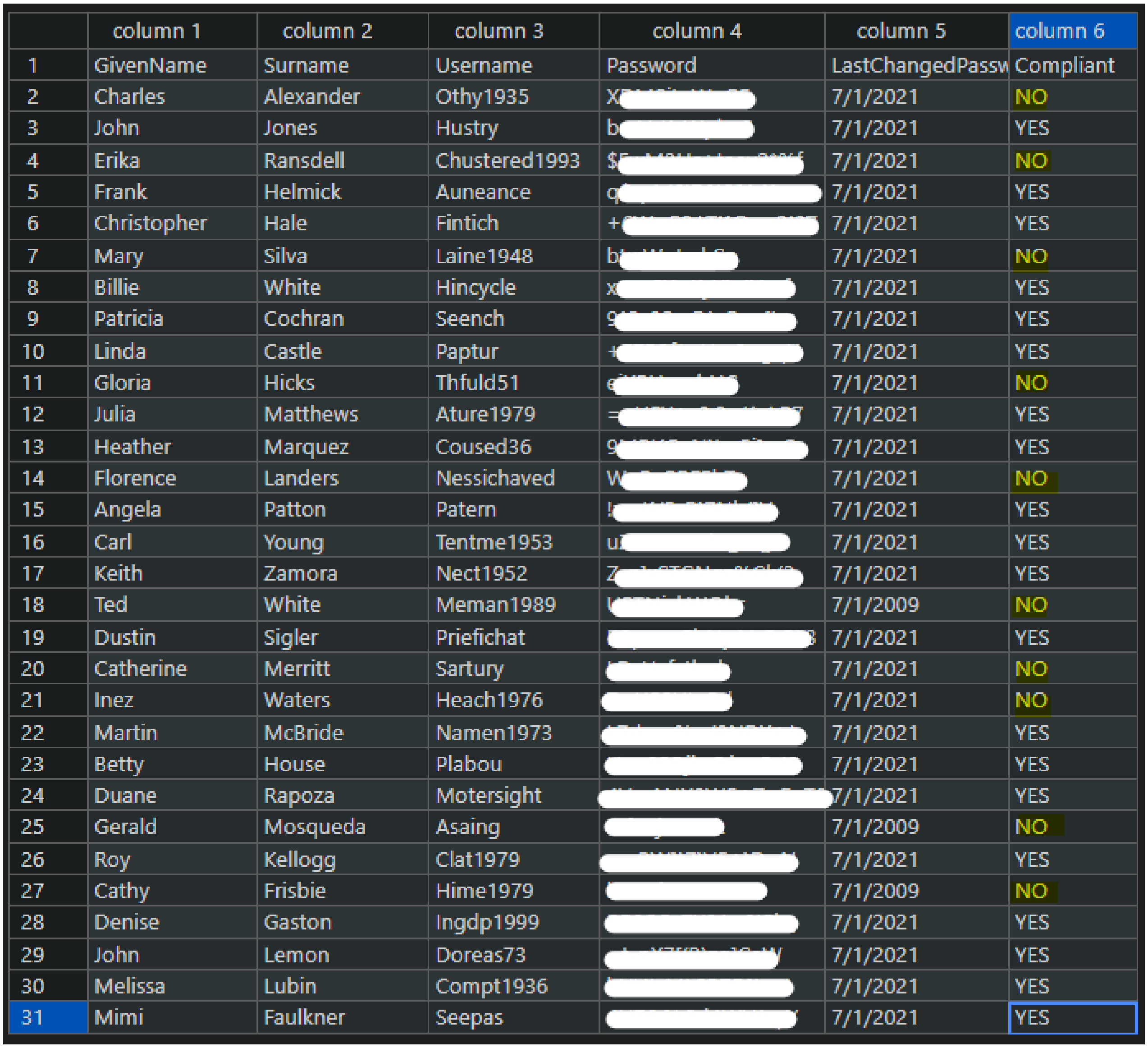
Scope Exclusions

Per client request, Joseph Martinez did **NOT** perform any Denial of Service attacks during testing.

Executive Summary

The purpose of this vulnerability scan is to gather data on Windows and Linux Operating systems, as well as user accounts in the **"ClientDomains"** domain in the 10.10.1.1/24 subnet. Of the hosts identified, ***30 user accounts and 30 systems*** were found to be active and were scanned.

Scan Results



	column 1	column 2	column 3	column 4	column 5	column 6
1	GivenName	Surname	Username	Password	LastChangedPassw	Compliant
2	Charles	Alexander	Othy1935	[redacted]	7/1/2021	NO
3	John	Jones	Hustry	[redacted]	7/1/2021	YES
4	Erika	Ransdell	Chustered1993	[redacted]	7/1/2021	NO
5	Frank	Helmick	Auneance	[redacted]	7/1/2021	YES
6	Christopher	Hale	Fintich	[redacted]	7/1/2021	YES
7	Mary	Silva	Laine1948	[redacted]	7/1/2021	NO
8	Billie	White	Hincycle	[redacted]	7/1/2021	YES
9	Patricia	Cochran	Seench	[redacted]	7/1/2021	YES
10	Linda	Castle	Paptur	[redacted]	7/1/2021	YES
11	Gloria	Hicks	Thfuld51	[redacted]	7/1/2021	NO
12	Julia	Matthews	Ature1979	[redacted]	7/1/2021	YES
13	Heather	Marquez	Coused36	[redacted]	7/1/2021	YES
14	Florence	Landers	Nessichaved	[redacted]	7/1/2021	NO
15	Angela	Patton	Patern	[redacted]	7/1/2021	YES
16	Carl	Young	Tentme1953	[redacted]	7/1/2021	YES
17	Keith	Zamora	Nect1952	[redacted]	7/1/2021	YES
18	Ted	White	Meman1989	[redacted]	7/1/2009	NO
19	Dustin	Sigler	Priefichat	[redacted]	7/1/2021	YES
20	Catherine	Merritt	Sartury	[redacted]	7/1/2021	NO
21	Inez	Waters	Heach1976	[redacted]	7/1/2021	NO
22	Martin	McBride	Namen1973	[redacted]	7/1/2021	YES
23	Betty	House	Plabou	[redacted]	7/1/2021	YES
24	Duane	Rapoza	Motersight	[redacted]	7/1/2021	YES
25	Gerald	Mosqueda	Asaing	[redacted]	7/1/2009	NO
26	Roy	Kellogg	Clat1979	[redacted]	7/1/2021	YES
27	Cathy	Frisbie	Hime1979	[redacted]	7/1/2009	NO
28	Denise	Gaston	Ingdp1999	[redacted]	7/1/2021	YES
29	John	Lemon	Doreas73	[redacted]	7/1/2021	YES
30	Melissa	Lubin	Compt1936	[redacted]	7/1/2021	YES
31	Mimi	Faulkner	Seepas	[redacted]	7/1/2021	YES

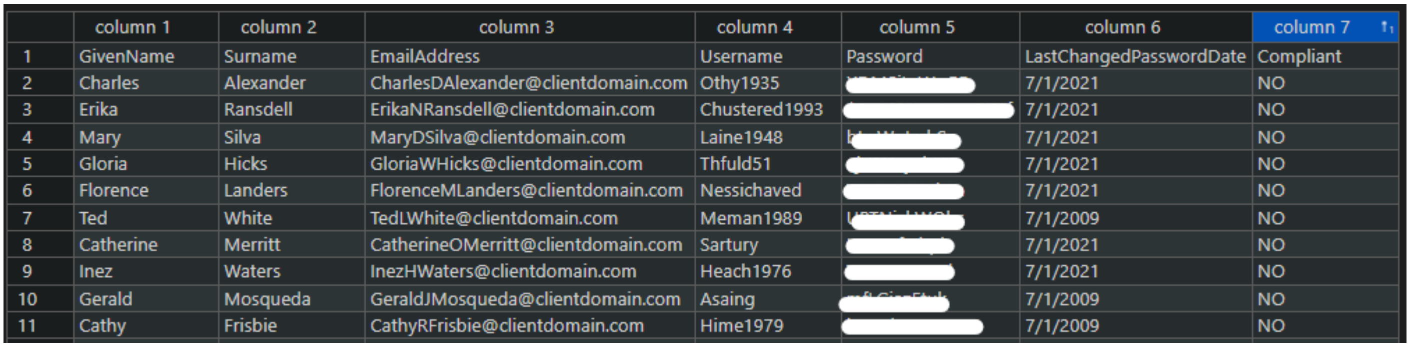
Vulnerability Assessment Findings

Weak Active Directory Password Policy - User Account login (High)

Description:	Based on our findings, we have determined that 10 / 30 (33%) user accounts do NOT follow **NIST 800-63b Password Guidelines and Best Practices** and are vulnerable to potential brute force attacks due to the lack of complexity.
Impact:	HIGH (7.5)
System:	10.10.1.1
References:	● https://pages.nist800-63-3/sp800-63b.html ● https://csrc.nist.gov/publications/detail/sp/800-63b/final

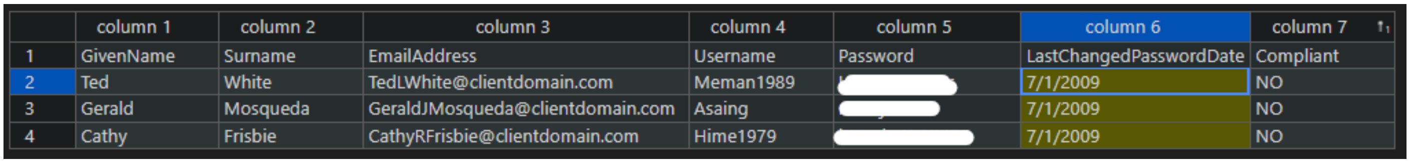
Proof of Concept (PoC):

Gathered historical breached data found in credentials dumps. The data amounted to 30 total account credentials with 10 of them **NOT** following Password Policy compliance standards. (**Note**: A full list of compromised accounts can be found in “SAP_VulAssessmentReport.csv”).



	column 1	column 2	column 3	column 4	column 5	column 6	column 7
1	GivenName	Surname	EmailAddress	Username	Password	LastChangedPasswordDate	Compliant
2	Charles	Alexander	CharlesDAlexander@clientdomain.com	Othy1935	[redacted]	7/1/2021	NO
3	Erika	Ransdell	ErikaNRansdell@clientdomain.com	Chustered1993	[redacted]	7/1/2021	NO
4	Mary	Silva	MaryDSilva@clientdomain.com	Laine1948	[redacted]	7/1/2021	NO
5	Gloria	Hicks	GloriaWHicks@clientdomain.com	Thfuld51	[redacted]	7/1/2021	NO
6	Florence	Landers	FlorenceMLanders@clientdomain.com	Nessichaved	[redacted]	7/1/2021	NO
7	Ted	White	TedLWhite@clientdomain.com	Meman1989	[redacted]	7/1/2009	NO
8	Catherine	Merritt	CatherineOMerritt@clientdomain.com	Sartury	[redacted]	7/1/2021	NO
9	Inez	Waters	InezHWaters@clientdomain.com	Heach1976	[redacted]	7/1/2021	NO
10	Gerald	Mosqueda	GeraldJMosqueda@clientdomain.com	Asaing	[redacted]	7/1/2009	NO
11	Cathy	Frisbie	CathyRFrisbie@clientdomain.com	Hime1979	[redacted]	7/1/2009	NO

Furthermore we have found that 3 user accounts have **NOT** been updated / changed since the year of 2009, this will put the following accounts in risk of **Credential Stuffing** (Credential stuffing takes advantage of accounts that never had their passwords changed after an account break-in):



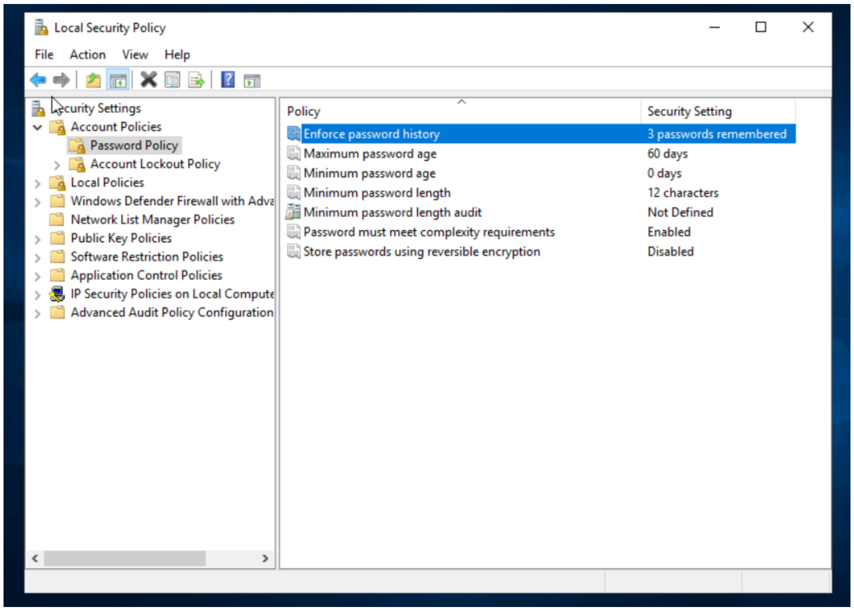
	column 1	column 2	column 3	column 4	column 5	column 6	column 7
1	GivenName	Surname	EmailAddress	Username	Password	LastChangedPasswordDate	Compliant
2	Ted	White	TedLWhite@clientdomain.com	Meman1989	[redacted]	7/1/2009	NO
3	Gerald	Mosqueda	GeraldJMosqueda@clientdomain.com	Asaing	[redacted]	7/1/2009	NO
4	Cathy	Frisbie	CathyRFrisbie@clientdomain.com	Hime1979	[redacted]	7/1/2009	NO

Remediation

<table>
<tr><td><b>Who</b>:</td><td>IT Team</td></tr>
<tr><td><b>Vector</b>:</td><td>Remote</td></tr>
<tr><td><b>Action</b>:</td><td>
<b>Item 1</b>: Permitted successful login via a Brute Force Attack, signifying a weak password policy. It is recommended that the following password policy is used, per the Center for Internet Security (CIS):

- 14 characters or longer.
- Maximum Password Age of 60 Days.
- Enforce Password History of a maximum of 3.
- Use different passwords for each account accessed.
- Do not use common words and proper names in passwords, regardless of language.

<b>Screenshot</b>:


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	3 passwords remembered
Maximum password age	60 days
Minimum password age	0 days
Minimum password length	12 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled
</td></tr>
</table>

Additional Reports and Scans (Informational)

Joseph Martinez provides all clients with all report information gathered during testing. This includes vulnerability scans and detailed findings documents. For more information, please see the following documents:

- SAP_VulAssessmentReport.csv
- SAP_Vulnerability_Assessment_Report(Capstone Project).pdf