Beauvais Security Consulting, Inc.

Penetration Testing Report
Demo Company

Business Confidential

Preparer: Berline BEAUVAIS
Date: March 17th, 2023
Cohort: 8/8/2022

Confidentiality Statement, Disclaimer, and Contact Information

This document is the exclusive property of Demo Company (DC) and Beauvais Security Consulting (BSC). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires both the consent of Demo Company and Beauvais Security Consulting.

Table of contents

Document Control

Issue Control			

Owner Details	Title	Contact Information	
John Smith	VP Information Security (CISO)	Office:(555)-555-5555 Email:john.smith@demo.com	

Revision History			
Issue	Date	Author	Comments
	3/18/2023	Berline BEAUVAIS	

Executive Summary

Beauvais Security Consulting was contracted by Demo Company to conduct a penetration test from May 20th, 2019 to May 29th 2019 in order to determine its exposure to a targeted attack. By leveraging a series of attacks. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted against Demo Company. With the goals of:

- Identifying if a remote attacker could penetrate Demo Company's defenses
- Determining the impact of a security breach on:
    - Confidentiality of the company's private data
    - Internal infrastructure and availability of Demo Company's information systems

Test Scope

Demo Company engaged our service to evaluate the security posture of its infrastructure compared to current industry best practices, that included an external penetration test.

The following external accessible IP addresses were within the scope of this engagement:

Target IP Addresses
192.168.0.0/24
192.168.1.0/24

Scope exclusion, Denial of Service attack during testing.

Results

Beauvais Security Consulting Inc, found critical level vulnerabilities that allowed full internal network access to the Demo Company headquarters office.

Finding Severity Ratings

The severity is rate based on the CVSS v3.1 which attempts to assign severity scores to vulnerabilities. The scores are calculated on a formula that depends on several metrics that approximate ease and impact of an exploit. Scores range from 0 to 10, with 10 being the most severe.

Severity	CVSs.v3 Score Range

Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

The table below includes the scope of the test performed, as well as the overall results of penetration testing these environments.

Environment Tester	**Testing Results based on CVSs.v3 Score Range**
Missing Multi-Factor Authentication	8.0
Weak Password Policy	8.9
Unrestricted Logon Attempts.	9.5

Recommendations

It is highly recommended that Demo Company address vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.
The following recommendations provide direction on improving the overall security posture of Demo Company's networks and business-critical applications:

Step	Action	Recommendation
1	Obtained historical breached account credentials to leverage against all company login pages	Discourage employees from using work e-mails and usernames as login credentials to other services unless necessary
2	Attempted a "credential stuffing" attack to obtain from a data breach and login information against Outlook Web Access (OWA), the web-based used by the employees of Demo Company to access their mailboxes from the internet. This attack was unsuccessful . However, OWA provided username enumeration, which allowed our company to gather a list of valid usernames to leverage in further attacks.	Synchronize valid and invalid account messages
3	Performed a "Password spraying" attack where the list of usernames to login on the Outlook Web Access (OWA) using the usernames discovered in step 2. Our Company used the password of Summer2018! (Season +year +special character) against a valid accounts and gained access into the OWA application	Outlook Web Access (OWA) permitted authenticated with valid credentials. Beauvais Consulting recommends Demo Company implement Multi-Factor Authentication (MFA) which is an authentication method that requires the user to provide two or more verification factors to gain access to their email on all external services. We recommend restricting login attempts against their service. To avoid unlimited login.

4	Leverage valid credentials to log into VPN	Implement Multi-Factor Authentication (MFA) on all external services.

Assessment Overview and Assessment Components

Overview

The test was performed in accordance with the recommendations outlined in *NIST SP 800-115 Technical Guide to Information Security Testing and Assessment*[1], which provide practical recommendations for designing, implementing, and maintaining technical information security test and examination processes and procedures. Moreover, we used *OSWAP Testing Guide (V4)* and customized testing frameworks[2]. With all tests and actions being conducted under controlled conditions.
Beauvais Security Consulting, emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. To gather intelligence, our staff attempts to gather sensitive information about Demo Company through open-source intelligence (OSINT), including employee information , historical breached passwords, and more that can be leveraged against external systems to gain internal network access.

Network Penetration Testing Results

Security Strengths

SIEM alerts of vulnerability scans.

During the test, the Demo Company team alerted Beauvais Consulting of detected vulnerability scanning against their systems. The team was successfully able to identify our engineering 's attacker IP address within minutes of scanning and was capable of blacklisting our team from further scanning actions.

[1] https://csrc.nist.gov/publications/detail/sp/800-115/final
[2] https://owasp.org/www-project-top-ten/#

Security Weaknesses

Missing Multi-Factor Authentication

Our Engineering team leveraged multiple attacks against Demo Company login forms using valid credentials harvested through open-source intelligence.

Weak Password Policy

Beauvais Consulting successfully performed password guessing attacks against Demo Company login forms, providing internal network access. A predictable password format for Summer2018! (Season + year + special character) was attempted and successful .

Unrestricted Logon Attempts.

During the assessment, Beauvais Consulting performed multiple brute-force attacks against login forms found on the external network. For all logins, unlimited attempts were allowed, which permitted an eventual successful login on the Outlook Web Access application.

Vulnerability by impact

Based on the CVSS v1 Score rating when exploitation is straightforward and usually results in system-level compromise. It i

External Penetration Test Findings

Result Classification	**Insufficient Lockout Policy- Outlook Web App (Critical)**	**CVSS Score Rating**
Description:	Demo Company unlimited logon attempts against their Outlook Web App (OWA) services. This configuration allowed brute force and password guessing attacks	
Impact:	Critical	9.5
System:	192.168.0.5	
References:	Access Unsuccessful Logon Attempts |Automatic account Lock	

Conclusion

Demo Company suffered a series of control failures, which led to a complete compromise of critical company assets. These failures would have had a dramatic effect on Demo Company operations if a malicious party had exploited them. Current policies concerning password reuse and deployed access controls are not adequate to mitigate the impact of the discovered vulnerabilities.

The specific goals of the penetration test were stated as:

- Identifying if a remote attacker could penetrate Demo Company's defenses
- Determining the impact of a security breach on:
    - Confidentiality of the company's private data
    - Internal infrastructure and availability of Demo Company's information systems.

These goals of the penetration test were met. A targeted attack against Demo Company can result in a complete compromise of organizational assets. Beauvais Security Consulting have found critical level vulnerabilities that allowed full internal network access to the Demo Company headquarters office. The vulnerabilities were rated according to the CVSS V3.1 one of the three vulnerabilities is rated as critical and two other ones as high. We recommend that Demo Company discourage employees from using work emails and usernames as login credentials to other services unless necessary. Likewise, to synchronize valid and invalid account messages. Finally, we recommend restricting login attempts against their service. To avoid unlimited login.