Caywood Security

Security Assessment Findings Report

Barnaby Consulting Services

Business Confidential

Date: 4/30/2024

Project: 730-53

CONTENTS

Table of Contents **1**
Confidentiality Statement **2**
Disclaimer **2**
Contact Information **2**
Assessment Overview **3**
Assessment Components **3**
External Penetration Testing **3**
Finding Severity Rating **4**
Scope **5**
Scope Exclusions 5
Client Allowances 5
Executive Summary **6**
Attack Summary 6
Security Strengths **7**
SIEM Alerts of Vulnerability Scans 7
Security Weaknesses **8**
Missing Multi-Factor Authentication 8
Weak Password Policy 8
Unrestricted Login Attempts 8
Vulnerabilities By Impact **9**
External Penetration Test Findings 9
Insufficient Lookout Policy – Outlook Web App (Critical) 9
Additional Reports and Scans (Informational) 10

PREFACE

Confidentiality Statement

This penetration test report and all associated documentation are confidential and intended solely for the use of the client, Barnaby Consulting Services, and authorized personnel of Caywood Security. Any unauthorized review, use, disclosure, or distribution of this information is prohibited. This report contains sensitive information regarding the security vulnerabilities of the systems tested and must be handled with the utmost care to prevent unauthorized access or disclosure.

Disclaimer

This penetration test report is based on the results of testing conducted by Caywood Security and is provided to Barnaby Consulting Services for informational purposes only. The findings, conclusions, and recommendations contained in this report are based on the conditions as they existed at the time of testing and may not be applicable or accurate in the future. Caywood Security makes no warranties, express or implied, regarding the accuracy, completeness, or usefulness of the information contained herein. Caywood Security assumes no liability for any damages or losses arising from the use of or reliance on this report.

Contact Information

Name	Title	Contact Information
Barnaby Consulting Services		
Barnaby Buckworth	CEO	bbuckworth@bcs.com
Bobby Buckworth	CTO	bobbyb@bcs.com
Caywood Security		
John Doe	CEO	johndoe@caywoodsec.com
Barrett Caywood	CTO	bcay@caywoodsec.com

OVERVIEW

Assessment Overview

The assessment conducted by Caywood Security for Barnaby Consulting Services aimed to evaluate the company's information security posture. The assessment included a comprehensive review of the organization's network, systems, and applications to identify potential vulnerabilities and assess the effectiveness of existing security controls. The primary goal of the assessment was to provide Barnaby Consulting Services with actionable recommendations to enhance its security posture and mitigate potential risks.

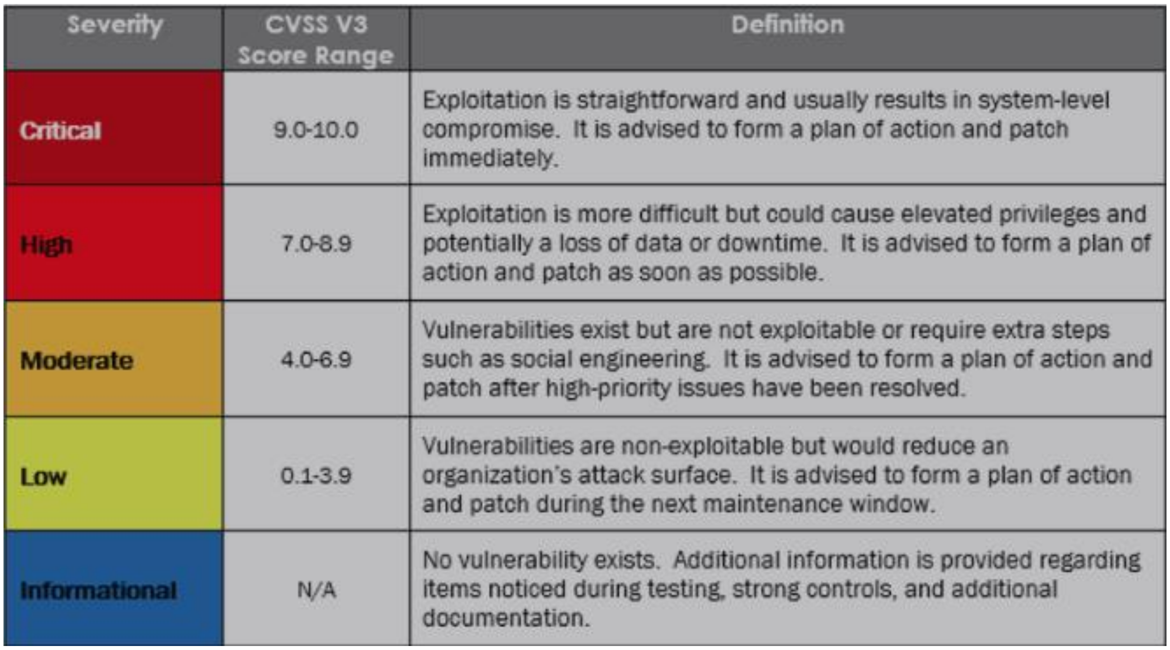
Assessment Components

External Penetration Test

The external penetration test focused on evaluating the security of Barnaby Consulting Services' external-facing network infrastructure and web applications. The assessment followed methodologies outlined in NIST SP 800-115 and the OWASP Testing Guide, employing a combination of automated tools and manual testing techniques. The assessment included reconnaissance activities to gather information about the organization's external network infrastructure, vulnerability scanning to identify known vulnerabilities and misconfigurations, exploitation of vulnerabilities to assess their impact, and post-exploitation assessments to identify additional security weaknesses. The assessment was conducted over a period of two weeks and aimed to provide actionable recommendations to enhance Barnaby Consulting Services' security posture.

SEVERITY RATING

Finding Severity Ratings



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.

The severity ratings are assigned based on the impact and exploitability of each finding. The ratings are intended to help prioritize remediation efforts and address the most critical security issues first.

SCOPE

Assessment	Details
External Penetration Test	192.168.0.0/24 192.168.1.0/24 192.168.2.0/24

Scope Exclusions

The assessment does not include testing of physical security controls, such as security guards, surveillance systems, or access control mechanisms at Barnaby Consulting Services' physical locations.

Client Allowances

During the assessment, Barnaby Consulting Services allowed Caywood Security access to its external-facing network infrastructure, including IP addresses, domain names, and web applications, for testing purposes. Barnaby Consulting Services also provided access to selected systems for vulnerability scanning and penetration testing activities. Additionally, Barnaby Consulting Services shared relevant information about its network infrastructure, systems, and applications to assist in the assessment process. The assessment was conducted in a testing environment isolated from the production environment to prevent any impact on operational systems. Barnaby Consulting Services designated a point of contact for communication during the assessment. These allowances were essential for conducting a thorough assessment of Barnaby Consulting Services' information security posture.

SUMMARY

Executive Summary

The attack on Barnaby Consulting Services (BCS) began with a phishing email impersonating a trusted source, leading to an employee clicking a malicious link or attachment. This action resulted in the theft of employee credentials, which the attacker used to access BCS's financial accounts or internal systems containing sensitive data. The potential impact includes financial loss, exposure of financial data, and reputational damage. To prevent such attacks, BCS should implement security awareness training, email filtering, and multi-factor authentication (MFA). Regular security audits and testing can help identify and address vulnerabilities. The summary uses color coordination to highlight key points and is designed to be concise and accessible to non-cybersecurity executives.

Attack Summary

Step	Action	Recommendation
1	Initial Compromise	Sends a phishing email to a BCS employee, impersonating a trusted source (e.g., bank, vendor, colleague). The email may contain a malicious link or attachment.
2	User Interaction	The unsuspecting employee clicks on the link or opens the attachment, which could download malware or redirect them to a fake login page designed to steal credentials.
3	Credential Theft	If the employee enters their login credentials on the fake page, the attacker captures this information.
4	Financial Data Access	Using the stolen credentials, the attacker attempts to access BCS's financial accounts or internal systems containing sensitive financial data.
5	Potential Impact	
	* Financial Loss	Attacker steals funds directly from BCS accounts.
	* Data Breach	Client or employee financial data may be exposed.
	* Reputational Damage	A security breach can damage BCS's reputation.

SECURITY

Security Strengths

Barnaby Consulting Services demonstrates several security strengths, including:

- ❖ Employee Training: BCS provides security awareness training for its employees, which can help them recognize and respond to phishing attempts and other cyber threats.

- ❖ Email Filtering: BCS has implemented email filtering measures to detect and block malicious emails, reducing the likelihood of successful phishing attacks.

- ❖ Security Policies: BCS has established security policies and procedures, providing a framework for managing security risks and ensuring compliance with relevant regulations.

Security Weaknesses

BCS also has several security weaknesses that need to be addressed:

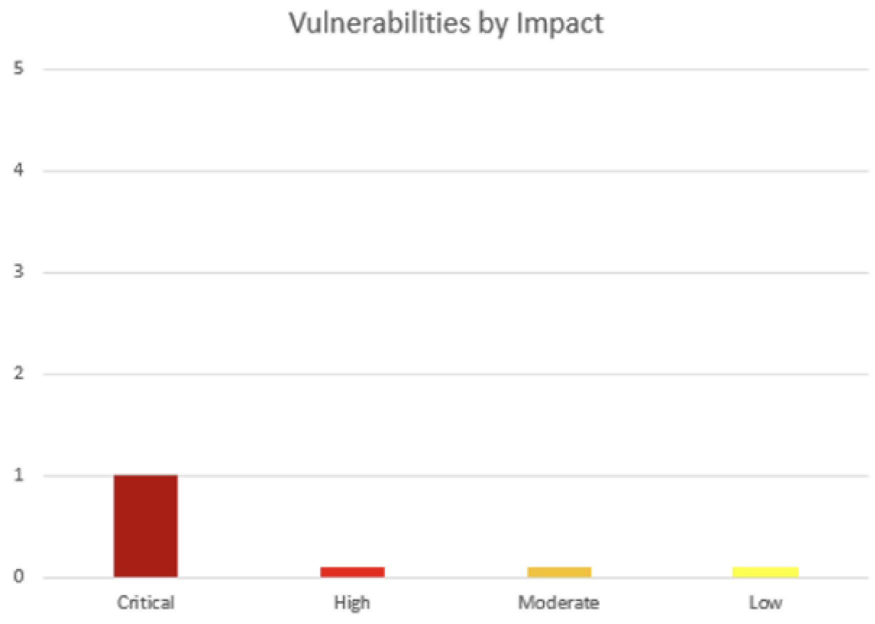
- ❖ Missing Multi-Factor Authentication (MFA): BCS does not have MFA implemented, which could have mitigated the impact of the phishing attack by requiring an additional form of authentication.

- ❖ Limited Security Monitoring: BCS's security monitoring capabilities are limited, making it difficult to detect and respond to security incidents in a timely manner.

- ❖ Insufficient Employee Awareness: While BCS provides security awareness training, there is still room for improvement in ensuring that employees are vigilant against phishing attempts and other cyber threats.

VULNERABILITIES

The following chart illustrates the vulnerabilities found by impact:



FINDINGS

External Penetration Test Findings

Insufficient Lockout Policy for Outlook:

Description:	The Outlook login interface does not enforce a lockout policy after a certain number of failed login attempts. This lack of lockout policy makes it easier for an attacker to conduct brute-force attacks to guess valid credentials
Impact:	CRITICAL
System:	192.168.1.32
Recommendation:	Implement a lockout policy for Outlook that locks out an account after a specified number of failed login attempts, helping to mitigate the risk of brute-force attacks

Exploitation Proof of Concept:

An attacker could use the breached credentials listed above to attempt to log in to Outlook accounts. Without a lockout policy in place, the attacker could repeatedly attempt different username and password combinations until a valid login is achieved, potentially gaining unauthorized access to sensitive information.

List of Breached User Credentials:

Username	Password
jill@bcs.com	$up3r$3cur3P@$$w0rd
phill@bcs.com	Phill123
steve@bcs.com	$hrek777

REMEDIATION

To address the insufficient lockout policy for Outlook and mitigate the risk of unauthorized access due to brute-force attacks, the following actions are recommended:

Who:	IT Team
Vector:	Remote/On-Site
Action:	1. **Implement Lockout Policy:** Configure Outlook to enforce a lockout policy that automatically locks out an account after a specified number of failed login attempts. 2. **Set Threshold for Failed Attempts:** Define the threshold for failed login attempts that trigger the lockout mechanism. A common recommendation is to lock out the account after three to five consecutive failed attempts. 3. **Lockout Duration:** Determine the duration of the lockout period, during which the account remains inaccessible. This period should provide sufficient time for legitimate users to reset their passwords while deterring attackers from further attempts. 4. **Notify Users:** Inform all Outlook users about the implementation of the lockout policy and the consequences of multiple failed login attempts. Encourage users to report any suspicious login attempts or unusual activity immediately. 5. **Monitor and Review:** Regularly monitor and review the effectiveness of the lockout policy to ensure it adequately addresses the risk of brute-force attacks. Adjust the threshold and lockout duration, if necessary, based on observed patterns of login attempts.

By implementing these remediation measures, Barnaby Consulting Services can enhance the security of Outlook accounts and reduce the risk of unauthorized access due to brute-force attacks.

CONCLUSION

The external penetration test conducted by Caywood Security for Barnaby Consulting Services has provided valuable insights into the organization's information security posture. The assessment identified several vulnerabilities, including the insufficient lockout policy for Outlook, which could have serious implications if exploited by malicious actors.

While Barnaby Consulting Services demonstrates security strengths, such as employee training and regular security audits, there are areas for improvement, including the implementation of a lockout policy for Outlook and the enhancement of security controls.

To mitigate the risks identified during the assessment, Barnaby Consulting Services should prioritize the implementation of the recommended remediation actions. These actions include implementing a lockout policy for Outlook, enhancing employee awareness, and training, and improving security controls to prevent unauthorized access and data breaches.

By addressing these vulnerabilities and implementing the recommended remediation actions, Barnaby Consulting Services can enhance its overall security posture and better protect its systems and data from cyber threats. Ongoing security assessments and proactive security measures are essential to maintain a strong security posture in the ever-evolving threat landscape.