Company Name

Security Assessment Finding Report

September 7, 2020

Contents

1 Confidentiality Statement

This document is the exclusive property of Company Name (CN) and Sudneo Security (SSec). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both CN and SSec.

SSec may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

2 Disclaimer

A penetration test 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.
Time-limited engagements do not allow for a full evaluation of all security controls. SSec prioritized the assessment to identify the weakest security controls an attacker would exploit. SSec recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

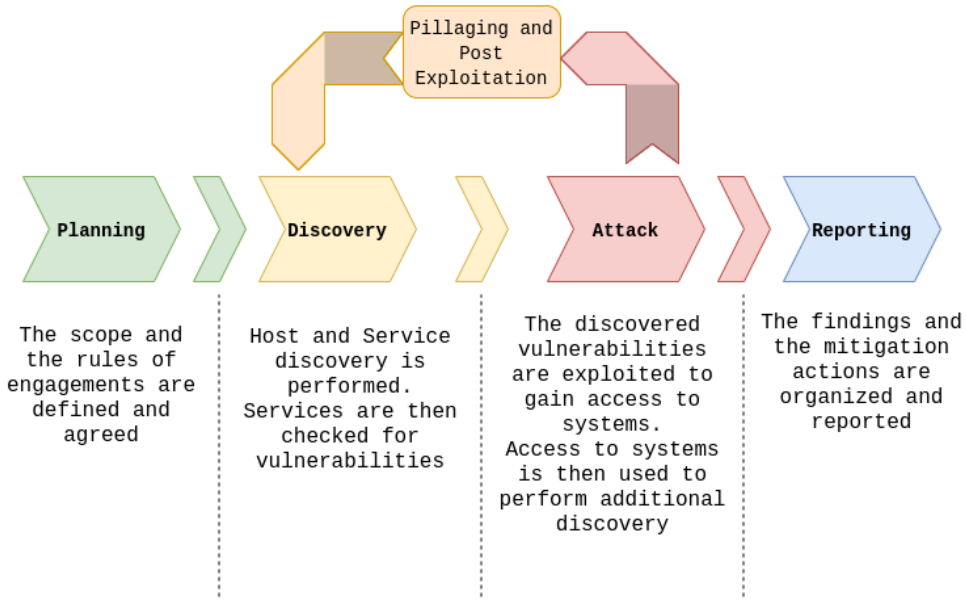
3 Contact Information

Name	Title	Contact Information
Company Name		
John Doe	CTO	Phone: 123456789 Email: john@company.com
Sudneo Security		
Sudneo	Pentester	Phone: 123456789 Email: sudneo@sudneo.me

4 Assessment Overview

From May 20th, 2019 to May 29th, 2019, SSec engaged CN to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test. All testing performed is based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks. Phases of penetration testing activities include the following:

- Planning Customer goals are gathered and rules of engagement obtained.
- Discovery Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



5 Assessment Components

External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A SSecengineer attempts to gather sensitive information 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. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

6 Findings Severity Classification

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

Table 1: Summary of the findings severity classification used.

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 organizations 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.

7 Scope

The overview of the scope of the engagement is described in Table 2.
Full details can be attached in Appendix.

Table 2: Scope of the engagement

Assessment	Details
External Penetration Test	10.10.100.0/24 10.100.10.0/24

7.1 Scope Exclusion

Per client request, SSec did not perform any Denial of Service attacks during testing.

7.2 Client Allowances

did not provide any allowances to assist the testing.

8 Executive Summary

SSec evaluated CNs external security posture through an external network penetration test from May 20th, 2019 to May 29th, 2019. By leveraging a series of attacks, SSec found critical level vulnerabilities that allowed full internal network access to the CN headquarter office. It is highly recommended that CN address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

8.1 Attack Summary

The following table describes how SSec gained internal network access, step by step.

Step	Action	Recommendation
1	Perform port scan on CN's infrastructure	Disable or protect ports which don't need to be public.

8.2 Security Strengths

SIEM alerts of vulnerability scan During the assessment, the CN security team alerted SSec engineers of detected vulnerability scanning against their systems. The team was successfully able to identify the SSec engineers attacker IP address within minutes of scanning and was capable of blacklisting SSec from further scanning actions.

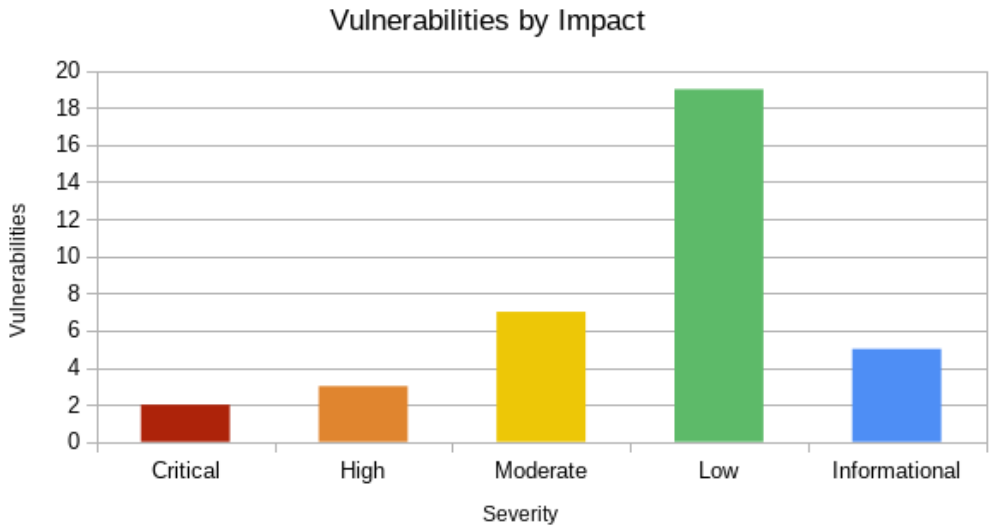
8.3 Security Weaknesses

Missing Password Policy SSec successfully performed password attacks using lists of common passwords. Several systems of CN were compromised using this method. Enabling a password policy that requires a minimum password complexity could protect the organization from similar attacks.

9 Vulnerabilities by Impact

Figure 1 illustrates the vulnerabilities found by impact.

Figure 1: Vulnerabilities by Impact



10 External Penetration Test Findings

10.1 Insufficient Lockout Policy - Outlook Web App (Critical)

Description:	CN allowed unlimited logon attempts against their Outlook Web App (OWA) services. This configuration allowed brute force and password guessing attacks in which SSec used to gain access to CNs internal network.
Impact:	Critical
System:	10.100.0.1
References:	• NIST SP800-53r4 AC-17 - Remote Access • NIST SP800-53r4 AC-7(1) - Unsuccessful Logon Attempts; Automatic Account Lock

10.1.1 Exploitation Proof of Concept

SSec gathered historical breached data found in credentials dumps. The data amounted to 868 total account credentials (Note: A full list of compromised accounts can be found in Demo Company-867-19 Full Findings.xslx.).

SSec used the gathered credentials to perform a credential stuffing attack against the OWA login page. Credential stuffing attacks take previously known credentials and attempt to use them on login forms to gain access to company resources. SSec was unsuccessful in the attack but was able to gather additional sensitive information from the OWA server in the form of username enumeration.

10.1.2 Remediation

Who:	IT Team
Vector:	Remote
Actions:	
1	VPN and OWA login with valid credentials did not require Multi-Factor Authentication (MFA). SSec recommends CN implement and enforce MFA across all external-facing login services.

2	OWA permitted unlimited login attempts. SSec recommends CN restrict logon attempts against their service.
3	CN permitted a successful login via a password spraying attack, signifying a weak password policy. SSec recommends the following password policy, per the Center for Internet Security (CIS): • 14 characters or longer • Use different passwords for each account accessed • Do not use words and proper names in passwords, regardless of language
4	OWA permitted user enumeration.SSec recommends CN synchronize valid and invalid account messages. Additionally, SSec recommends that CN : • Train employees on how to create a proper password • Check employee credentials against known breached passwords • Discourage employees from using work emails and usernames as login credentials to other services unless absolutely necessary

10.2 Unprotected Backup File (Low)

Description:	The file backup.zip is left unprotected on a server
Impact:	Low
System:	10.100.0.10
References:	• Owasp - Page on files permissions

10.2.1 Exploitation Proof of Concept

To find the file SSec accessed the machine 10.100.0.10 and verified the following:

```
file /var/backups/backups.zip
```

10.2.2 Remediation

Who:	Operations
Vector:	Local
Actions:	
1	Delete the file or restrict its permissions

10.3 Exposed service (Moderate)

Description:	Some server's port is open and unprotected
Impact:	Moderate
System:	10.100.0.11
References:	N/A

10.3.1 Exploitation Proof of Concept

All it takes is a Curl request:

```
curl -XPOST https://10.100.0.11/gimmefile.php -d 'file=test.txt'
```

10.3.2 Remediation

Who:	IT team
Vector:	Remote
Actions:	
1	Close the port if not public

10.4 Bad Server Name (Informational)

Description:	Some server names are hard to memorize
Impact:	Informational
System:	hjwowjsmc.example.org
References:	N/A

10.4.1 Exploitation Proof of Concept

```
hostname
```

10.4.2 Remediation

Who:	IT Team
Vector:	Local
Actions:	
1	Rename the server

10.5 SQL Injection in Backoffice (High)

Description:	The Backoffice site has multiple SQL Injections
Impact:	High
System:	backoffice.example.org
References:	• Nist Reference - Nist Input validation

10.5.1 Exploitation Proof of Concept

SSec managed to exploit several vulnerabilities

```
curl https://backoffice.example.org?id=1' OR '1'='1'#
```

10.5.2 Remediation

Who:	Development Team
Vector:	Remote
Actions:	
1	Implement Input validation for the id parameter
2	parameter

10.6 Exposed Site with default Credentials (Critical)

Description:	The site admin.example.org is exposed and allows access with default credentials
Impact:	Critical
System:	admin.example.org
References:	• NIST SP XXX - Nist on default credentials

10.6.1 Exploitation Proof of Concept

SSec was able to access the site simply by going to url

```
curl -XPOST "admin.example.org/login.php" -d 'username=admin&password=admin'
```

10.6.2 Remediation

Who:	Administration Team
Vector:	Remote
Actions:	
1	Change default credentials on administration site

11 Additional Reports and Scans (Informational)

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

- Demo Company-867-19 Full Findings.xslx
- Demo Company-867-19 Vulnerability Scan Summary.xslx
- Demo Company-867-19 Vulnerability Scan by Host.pdf