Google Developer Groups

HOW TO DO REPORTING

Google Developer Groups

SYLVIA FEBRIANTI

Cybersecurity Core Team (Curriculum)

Teknologi Informasi 2022

Meet The

Instructor

Google Developer Groups

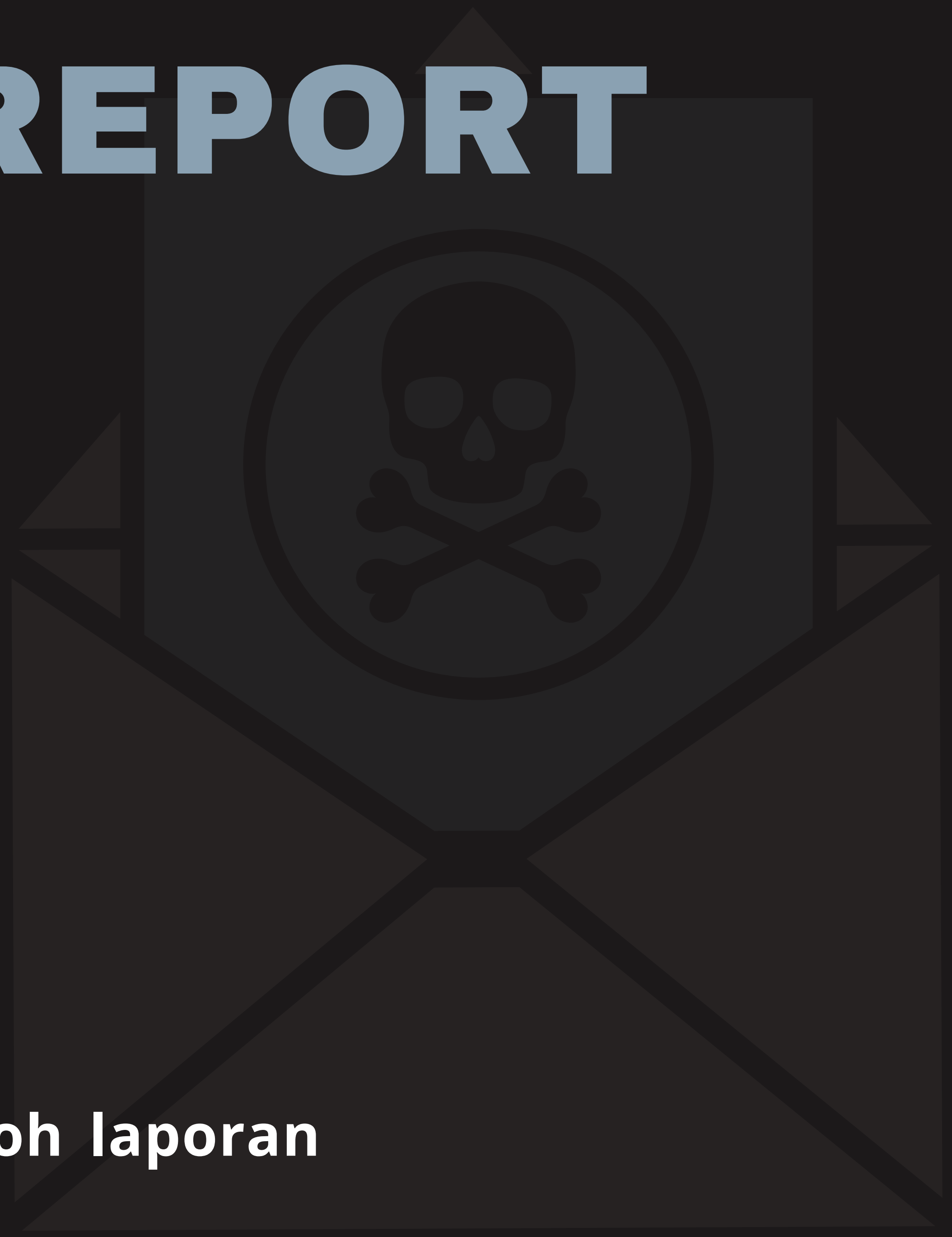
OVERVIEW

Laporan penetration testing berisi vulnerability yang ditemukan, dengan bukti (proof of concept) dari setiap tahapan pengujian.

MENGAPA REPORTING PENTING?

- Mengkomunikasikan temuan teknis ke bahasa non-teknis
- Membantu klien memahami risiko keamanan
- Mendukung prioritas perbaikan keamanan

YANG WAJIB ADA DI REPORT

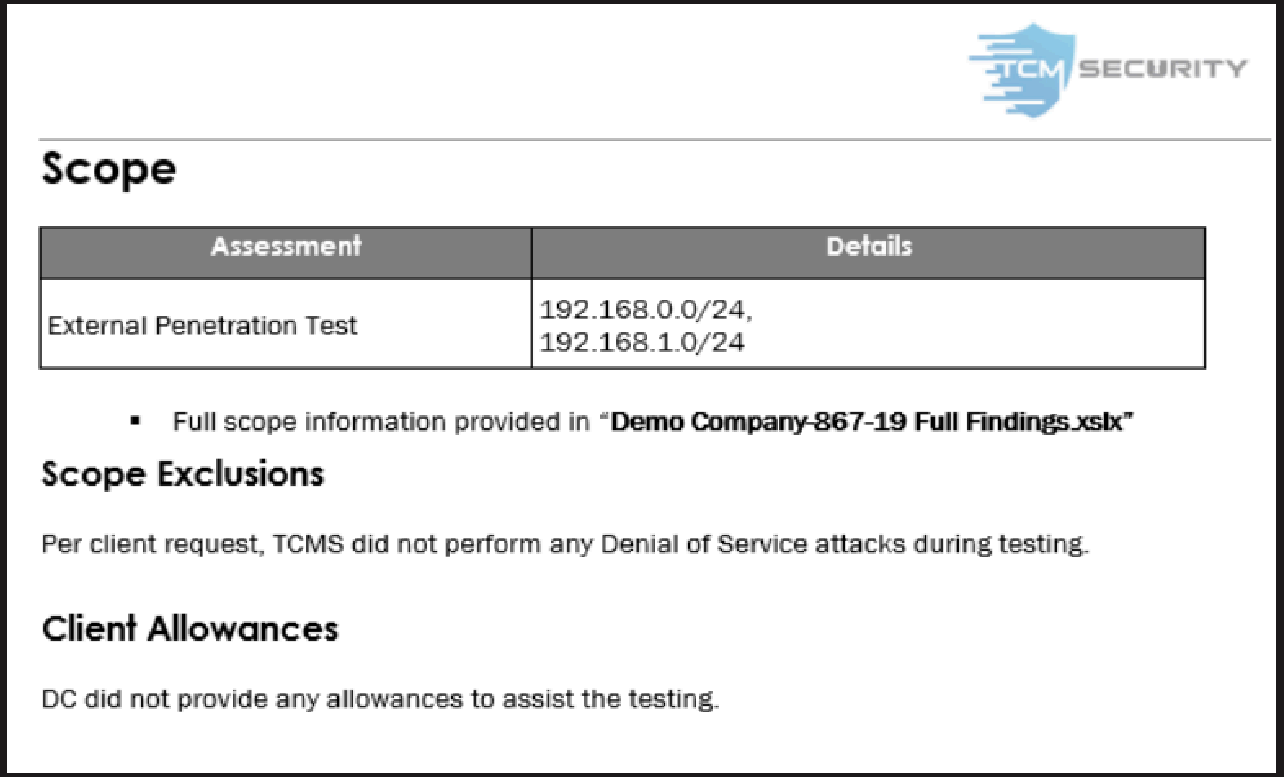


- Description
- Step to Reproduce
- Url Affected/Endpoint
- Impact
- Mitigation/Remediation/Recommendation
- Proof of Concept (Video/Images)

FORMAT???

Tidak ada suatu acuan format yang wajib diikuti. Berikut contoh laporan pentest yang baik memiliki beberapa komponen berikut:

ENGAGEMENT SUMMARY



TCM SECURITY

Scope

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

- Full scope information provided in "**Demo Company-867-19 Full Findings.xslx**"

Scope Exclusions

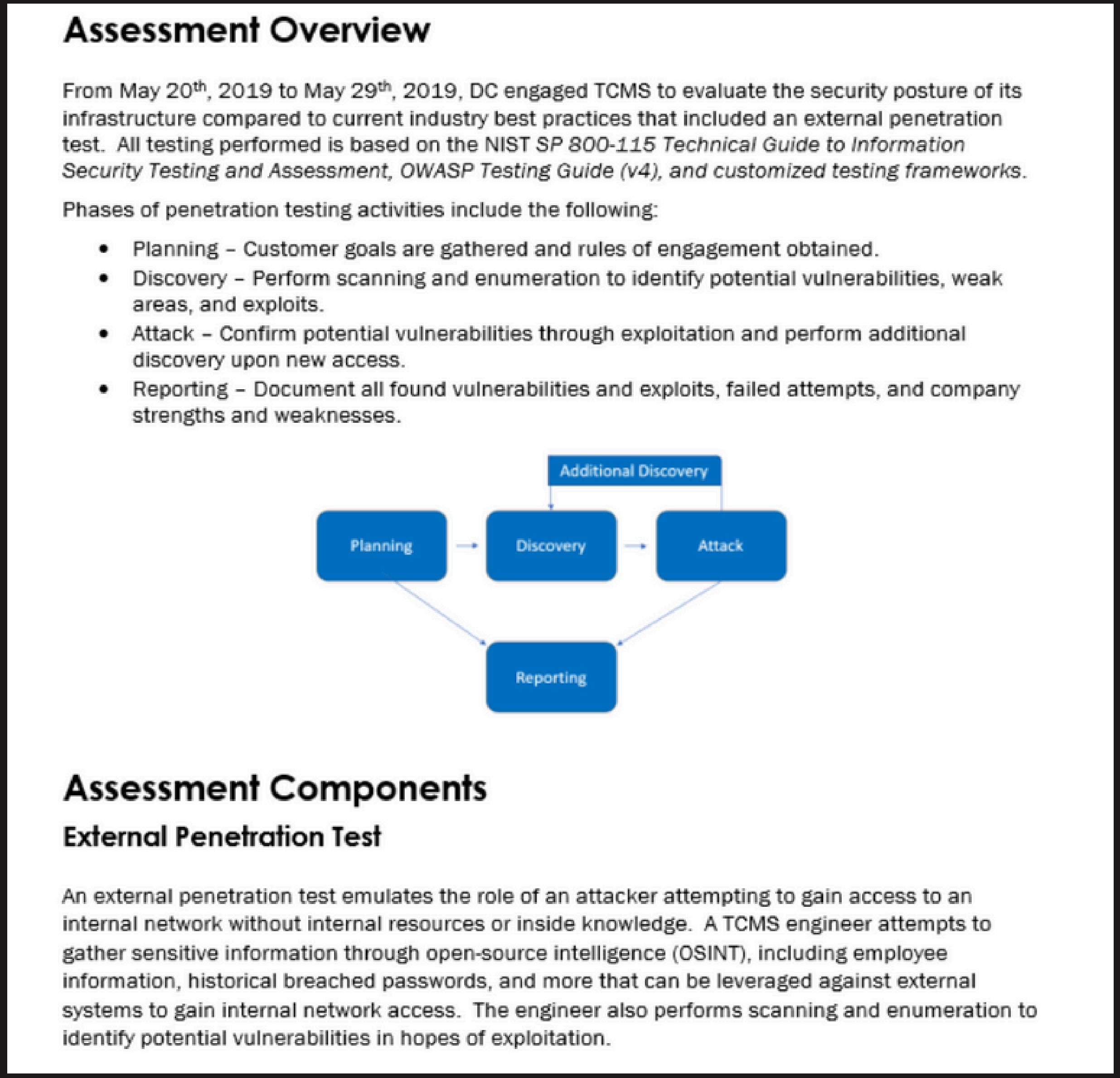
Per client request, TCMS did not perform any Denial of Service attacks during testing.

Client Allowances

DC did not provide any allowances to assist the testing.

Mencakup:

- **Scope (IP, sistem, aplikasi, larangan)**
- **Jadwal testing (tanggal, waktu, resource)**
- **Standar pengujian (PTES, OWASP)**



Assessment Overview

From May 20th, 2019 to May 29th, 2019, DC engaged TCMS 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:

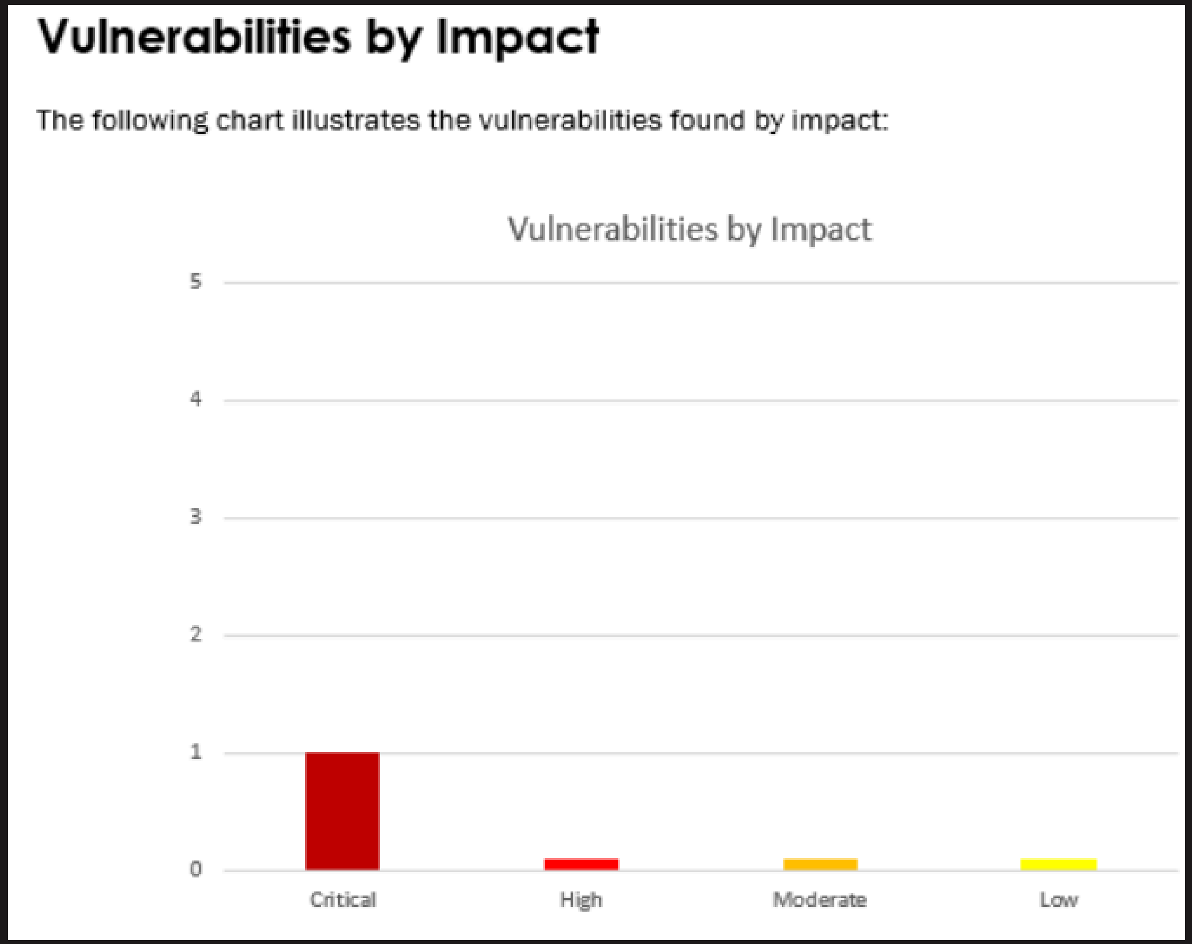
- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.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

Assessment Components

External Penetration Test

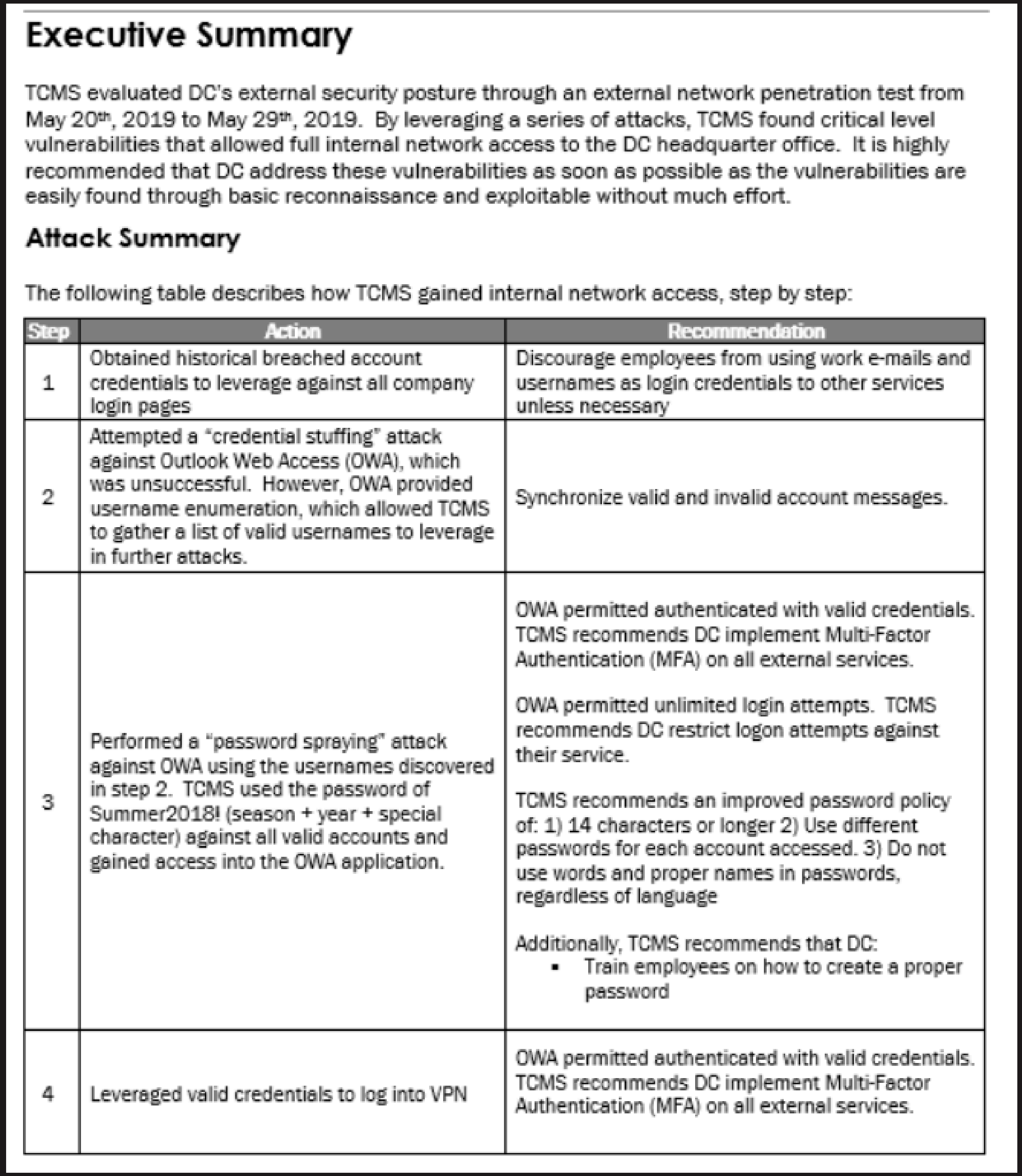
An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A TCMS engineer attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical 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.

EXECUTIVE SUMMARY



Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:



Executive Summary

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

Attack Summary

The following table describes how TCMS gained internal network access, step by step:

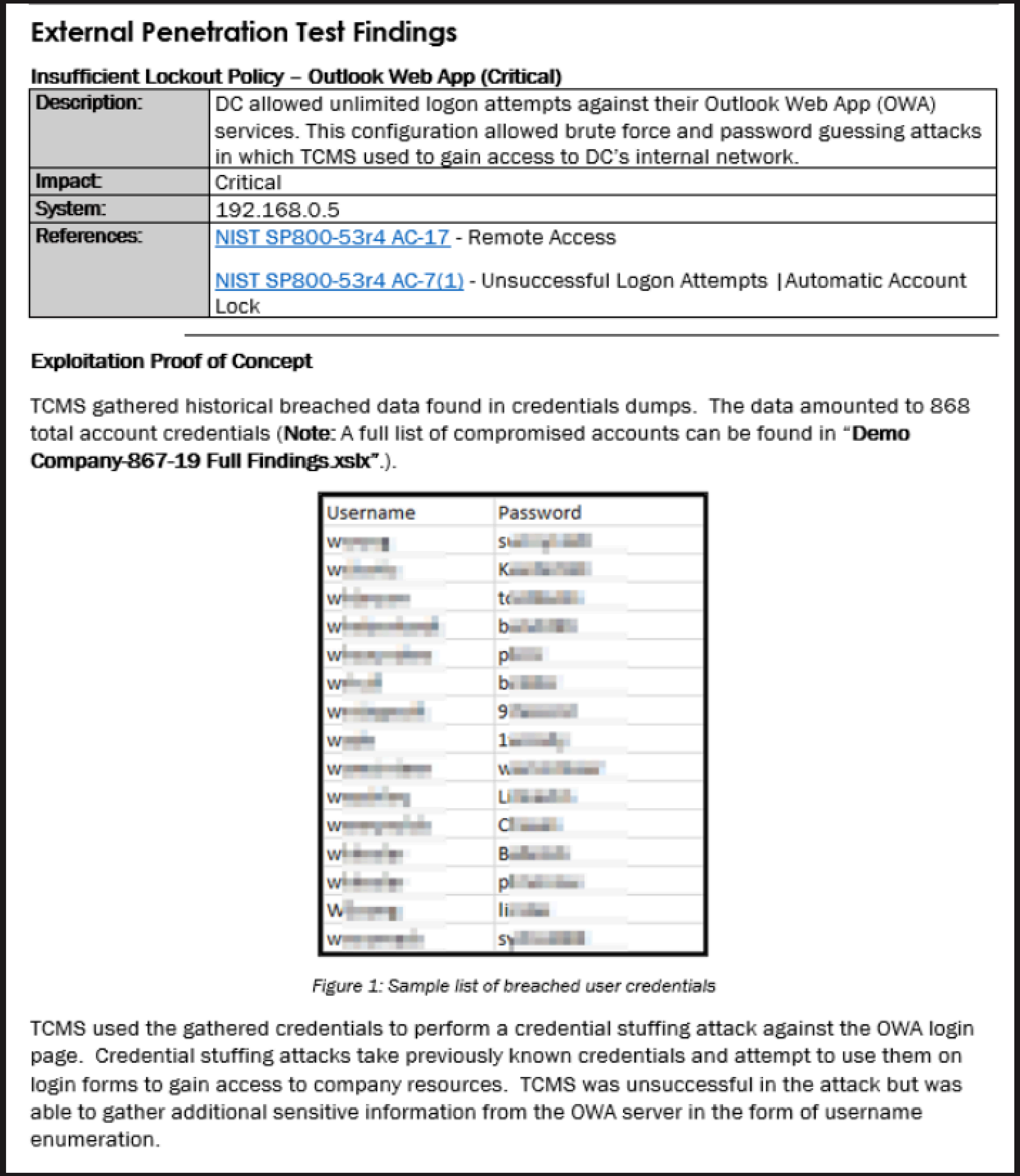
Step	Action	Recommendation
1	Obtained historical breached account credentials to leverage against all company login pages	Discourage employees from using work e-mails and usernames as login credentials to other services unless necessary
2	Attempted a "credential stuffing" attack against Outlook Web Access (OWA), which was unsuccessful. However, OWA provided username enumeration, which allowed TCMS to gather a list of valid usernames to leverage in further attacks.	Synchronize valid and invalid account messages.
3	Performed a "password spraying" attack against OWA using the usernames discovered in step 2. TCMS used the password of Summer2018! (season + year + special character) against all valid accounts and gained access into the OWA application.	OWA permitted authenticated with valid credentials. TCMS recommends DC implement Multi-Factor Authentication (MFA) on all external services. OWA permitted unlimited login attempts. TCMS recommends DC restrict logon attempts against their service. TCMS recommends an improved password policy of: 1) 14 characters or longer 2) Use different passwords for each account accessed. 3) Do not use words and proper names in passwords, regardless of language Additionally, TCMS recommends that DC: ▪ Train employees on how to create a proper password
4	Leveraged valid credentials to log into VPN	OWA permitted authenticated with valid credentials. TCMS recommends DC implement Multi-Factor Authentication (MFA) on all external services.

Google Developer Groups

KEY FINDINGS/ TECHNICAL FINDINGS

Bagian utama untuk tim teknis Mencakup setiap vulnerability dengan detail:

- Nama vulnerability
- Resource yang terpengaruh
- Impact
- Proof of Concept (POC)
- Risk assessment
- Recommendation



External Penetration Test Findings

Insufficient Lockout Policy – Outlook Web App (Critical)

Description:	DC allowed unlimited logon attempts against their Outlook Web App (OWA) services. This configuration allowed brute force and password guessing attacks in which TCMS used to gain access to DC's internal network.
Impact:	Critical
System:	192.168.0.5
References:	NIST SP800-53r4 AC-17 - Remote Access NIST SP800-53r4 AC-7(1) - Unsuccessful Logon Attempts | Automatic Account Lock

Exploitation Proof of Concept

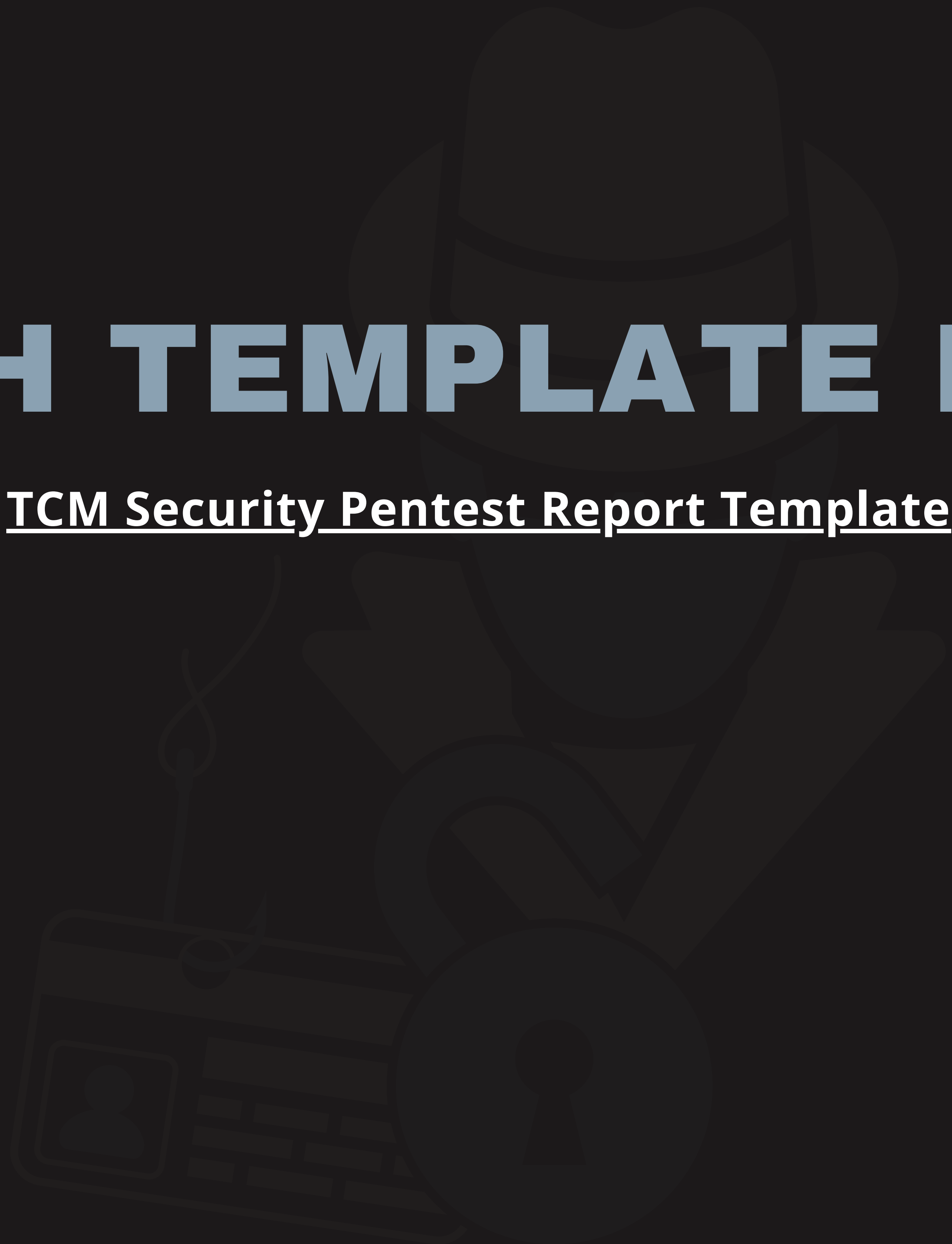
TCMS gathered historical breached data found in credentials dumps. The data amounted to 868 total account credentials (**Note:** A full list of compromised accounts can be found in "**Demo Company-867-19 Full Findings.xslx**".).

Username	Password
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Figure 1: Sample list of breached user credentials

TCMS 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. TCMS was unsuccessful in the attack but was able to gather additional sensitive information from the OWA server in the form of username enumeration.

Google Developer Groups



CONTOH TEMPLATE REPORT

TCM Security Pentest Report Template

LIST GOOGLE DORK BUG HUNTING INSTANSI & SWASTA

- site:csirt.*.go.id
- site:soc.*.go.id
- site:diskominfo.*.go.id
- intext: bug bounty site:co.id
- intext:responsible disclosure site:co.id

Google Developer Groups

THANK YOU