APP100-M1-1-Assignment 1-Penetration Test Report

Start Assignment

Due No Due Date **Points** 10 **Submitting** a text entry box or a file upload
File Types doc, docx, and pdf

Exercise Objective(s)

By the end of this lab, the student should be able to:

EO1: Describe the need for a pen testing report

EO2: Create a penetration testing report outline

Abstract

Penetration Testing is a valuable process for organizations, either through internal testing or by hiring an external third party that specializes in PenTesting Techniques. In either case, an essential outcome of the activity is the final report.

This lab will focus on creating a template for a Penetration Testing Report, which will be utilized in the final project for this course.

System Requirements & Configuration

System Requirements

Physical or virtualized Windows, Linux, or Mac desktop.

Network Requirements

Internet access from a lab machine to the internet.

Software Requirements

Word processing software.

Procedure – Detailed Lab Steps

Procedure - Detailed Lab Steps

Setup

A fictitious company will need to be created for the report. Remember, this is part of the overall portfolio of projects and will demonstrate the ability to write, analyze, and present information to potential clients (hiring companies).

Think of an appropriate company name and logo. A simple name, like <lastname> Consulting, Inc. or something similar, can be used. A logo can be as simple as initials in a fancy box. Creativity in this portion of the lab is not being judged, but do keep the names and logos professional.

Lab Execution

The objective of this lab is to design a penetration testing report based on the building blocks described in the lecture. The deliverable for this lab will be used as the basis of an actual penetration testing report at the end of this course. Each component that makes a report useful, readable, and detailed will be discussed, and a sample report with screenshots is included, along with guidance on the subject matter. Although creativity is not being judged, feel free to flex creative muscles, as the deliverable is essentially a PDF.

Base Lab

There are several components to a penetration testing report:

- Executive summary
- Scope
- Methodology
- Risk rankings
- Findings
- Evidence
- Recommendations
- Steps to reproduce
- Conclusion

Here are some samples:

- **https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf (https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf)**
- **https://tbgsecurity.com/wordpress/wp-content/uploads/2016/11/Sample-Penetration-Test-Report.pdf (https://tbgsecurity.com/wordpress/wp-content/uploads/2016/11/Sample-Penetration-Test-Report.pdf)**
- **https://static1.squarespace.com/static/589316f3cd0f68e6bd715655/t/5d7ce2ed69433d1**

(https://static1.squarespace.com/static/589316f3cd0f68e6bd715655/t/5d7ce2ed69433d1c3e3f702

- **(https://static1.squarespace.com/static/589316f3cd0f68e6bd715655/t/5d7ce2ed69433d1c3e3f702**

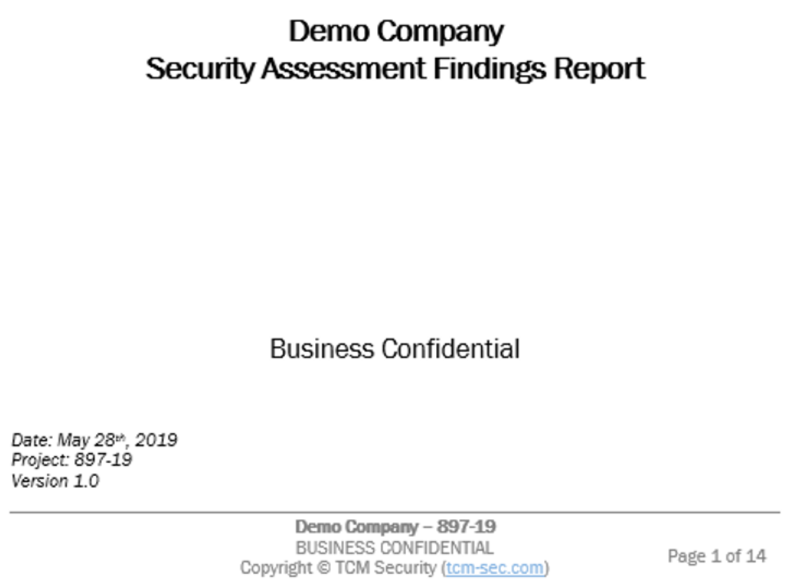
http://youtube.com/watch?v=EOoBAq6z4Zk (http://youtube.com/watch?v=EOoBAq6z4Zk) in conjunction with:

- **https://github.com/hmaverickadams/TCM-Security-Sample-Pentest-Report/blob/master/Demo%20Company%20-%20Security%20Assessment%20Findings%20Report.docx (https://github.com/hmaverickadams/TCM-Security-Sample-Pentest-Report/blob/master/Demo%20Company%20-%20Security%20Assessment%20Findings%20Report.docx)**

The remainder of this lab will critique a report.

Cover Page

TCM SECURITY



Demo Company
Security Assessment Findings Report

Business Confidential

Date: May 28th, 2019
Project: 897-19
Version 1.0

Demo Company – 897-19
BUSINESS CONFIDENTIAL
Copyright © TCM Security (tcm-sec.com)

Page 1 of 14

The cover page should include:

- Company name and logo
- Date the report was created
- Name of the company that was tested
- Including a confidential label is also important as proper documentation labels are industry standard.

Table of Contents

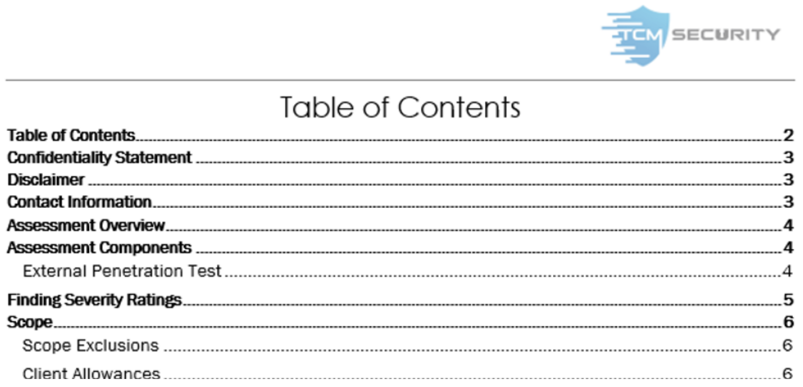
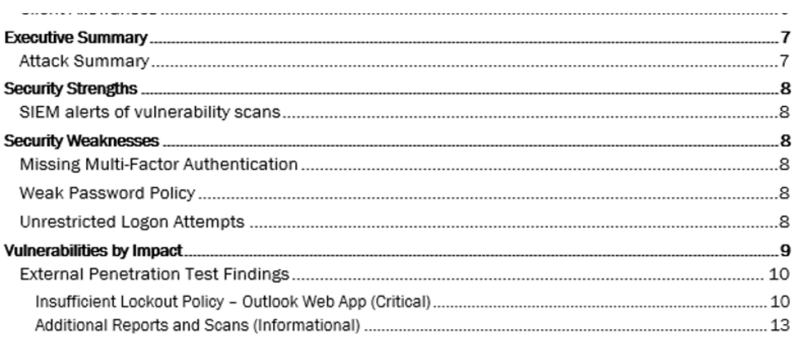
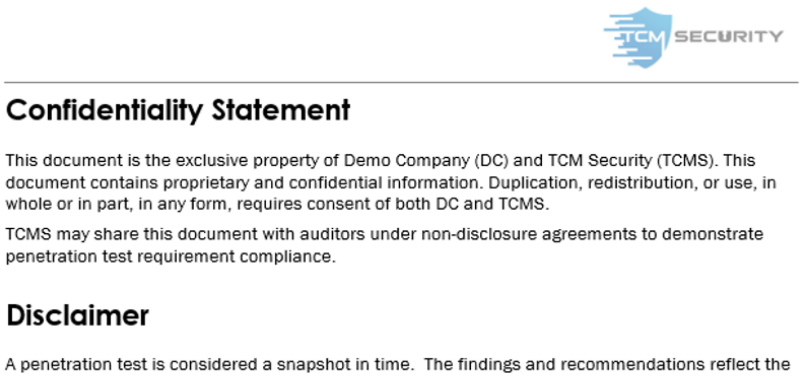


Table of Contents



Spend some time with a word processor learning how to use the built-in function to create custom headers that will then be automatically populated with the appropriate page numbers. Bold letters and subheaders are optional. Try to keep the entire report in **one** single font with varying font sizes for specific sections/headers.

Confidentiality Statement, Disclaimer, and Contact Information



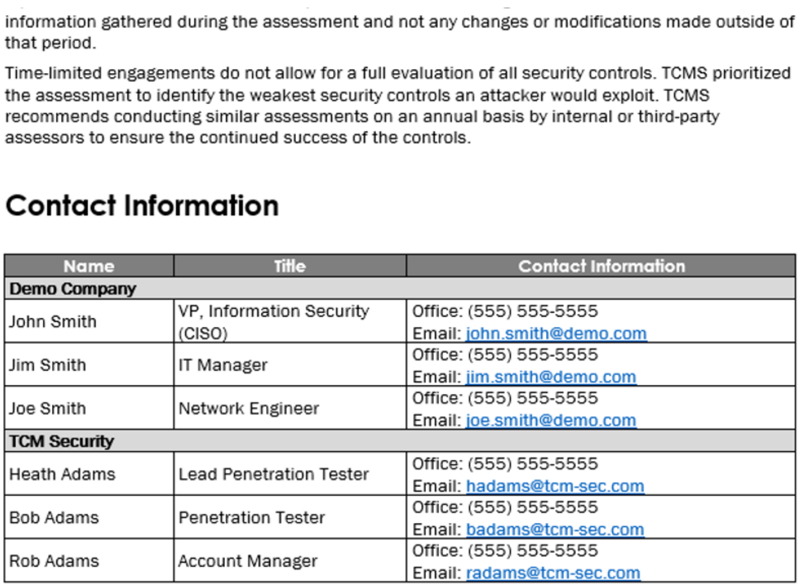
Confidentiality Statement

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

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

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.

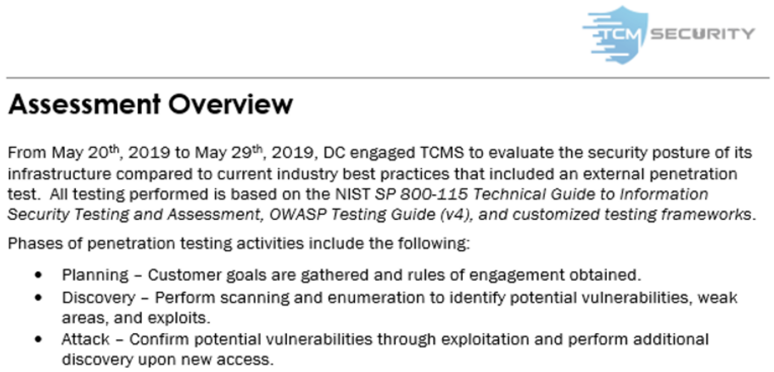
Time-limited engagements do not allow for a full evaluation of all security controls. TCMS prioritized the assessment to identify the weakest security controls an attacker would exploit. TCMS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the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

Contact Information

Name	Title	Contact Information
Demo Company		
John Smith	VP, Information Security (CISO)	Office: (555) 555-5555 Email: john.smith@demo.com
Jim Smith	IT Manager	Office: (555) 555-5555 Email: jim.smith@demo.com
Joe Smith	Network Engineer	Office: (555) 555-5555 Email: joe.smith@demo.com
TCM Security		
Heath Adams	Lead Penetration Tester	Office: (555) 555-5555 Email: hadams@tcm-sec.com
Bob Adams	Penetration Tester	Office: (555) 555-5555 Email: badams@tcm-sec.com
Rob Adams	Account Manager	Office: (555) 555-5555 Email: radams@tcm-sec.com

Notice that there is a specific section for the confidentiality statement. Not every sample will have this. The disclaimer is a nice touch; while it is not necessary, the statement makes it clear that not every vulnerability was certified to have been found during testing. Contact information is commonly found on these reports and is good practice. Also, note that the logo is on each page.

Assessment Overview and Assessment Components



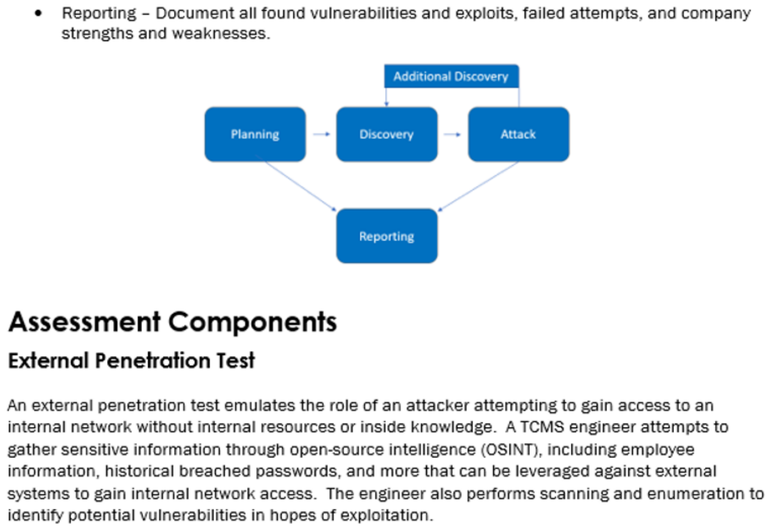
TCM SECURITY

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.

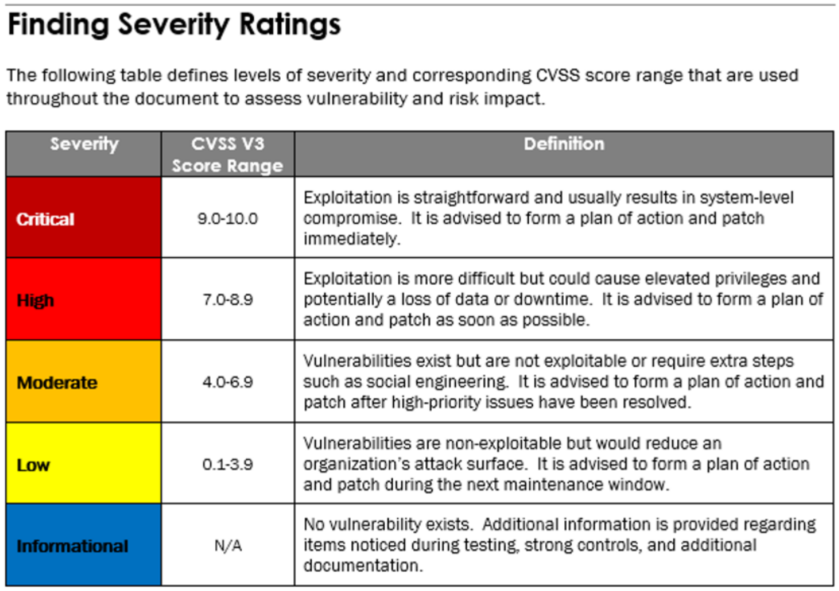
Assessment Components

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.

This section explains when the testing was done. The template mentions NIST SP 800-115 and the OWASP testing guide but without any real detail. This may not be sufficient and is rather lacking, as is the single, basic graphic. Consider adding more details about the methodology that will be employed.

Finding Severity Ratings



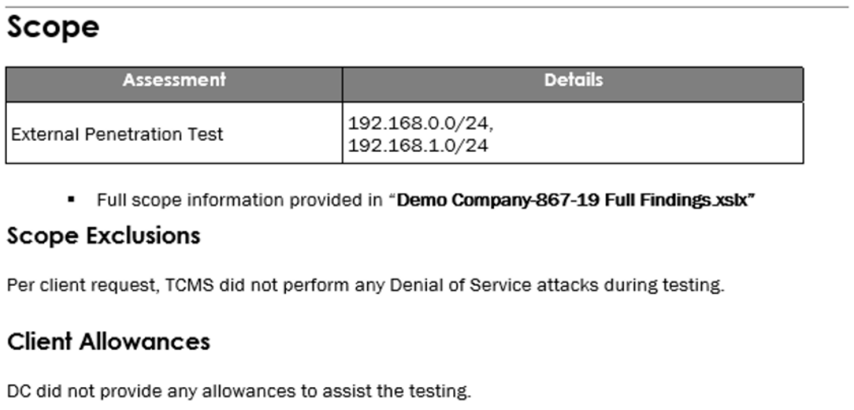
Finding Severity Ratings

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.

CVSS V3.1 is now industry standard, as are the ranges for the severities since CVSS already outlines these and the definitions. Take note that CVSS categorizes **Medium** instead of **Moderate**. Determine whether the colors are appropriate given the different severities. Research how to calculate the CVSS score for a finding.

Scope



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

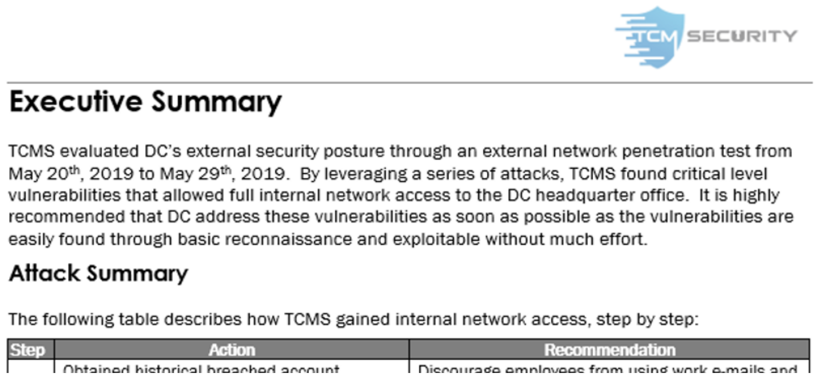
Per client request, TCMS did not perform any Denial of Service attacks during testing.

Client Allowances

DC did not provide any allowances to assist the testing.

The scope is not very exciting. It's a sample report, but even so, the "External" assets are private IP space, and who is DC (Demo Company)? Was social engineering involved? What were the rules of engagement? More details would make this section more robust.

Executive Summary



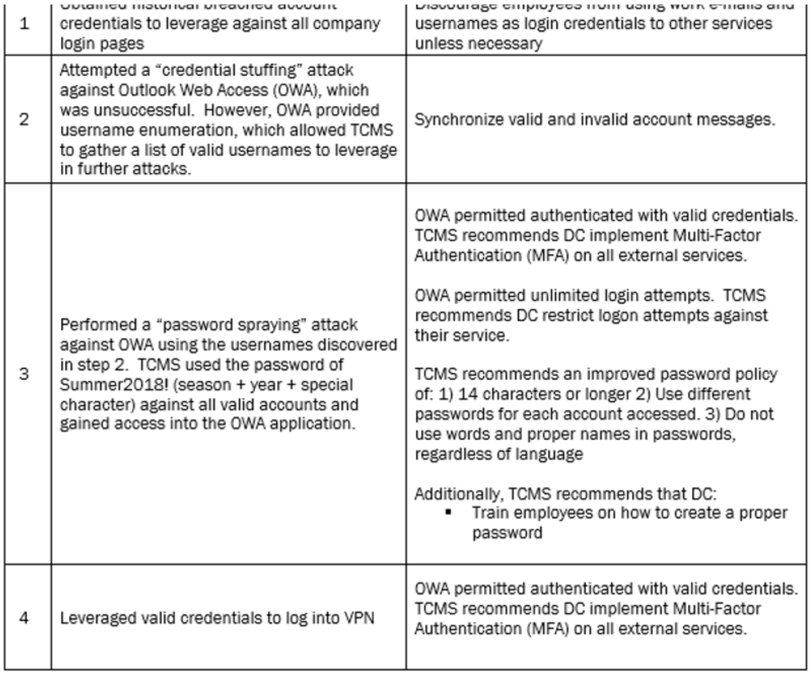
Executive Summary

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:

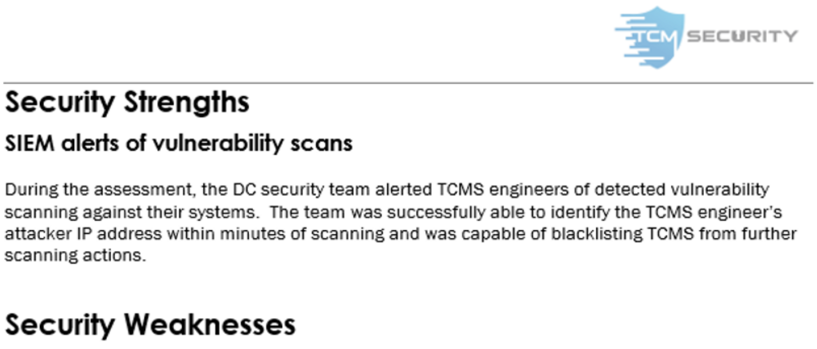
Step	Action	Recommendation
	Obtained historical breached account	Discourage employees from using work e-mails and



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.

The executive summary is on page 7. An executive does not want to have to go SEVEN pages into a document to get to the point. Even on page 7, this is not really “to the point”. One would have to have an understanding of cybersecurity to actually make full sense of this. Many executives don’t know what password spraying, OWA, nor MFA are. The executive section should be much more to the point. Notice that the color coordination from the CVSS severity ranking section is lacking in this summary as well. It may sound weird or funny, but there is value in making things visually appealing and to the point. If it is not possible to show executives nice graphs, there should at least be some color to this summary.

Security Strengths and Security Weaknesses



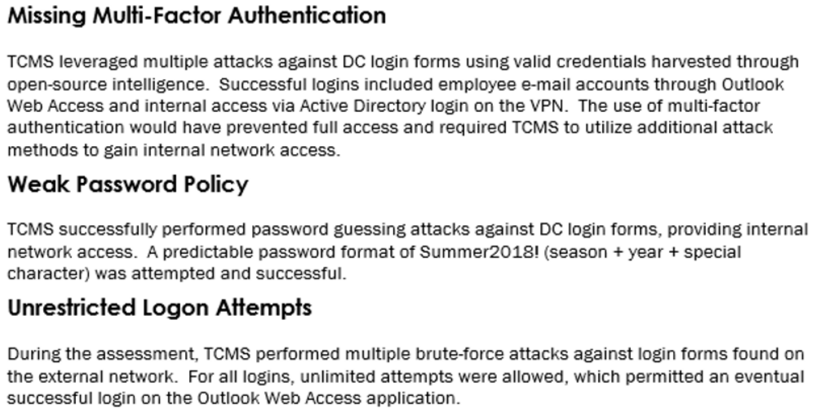
TCM SECURITY

Security Strengths

SIEM alerts of vulnerability scans

During the assessment, the DC security team alerted TCMS engineers of detected vulnerability scanning against their systems. The team was successfully able to identify the TCMS engineer’s attacker IP address within minutes of scanning and was capable of blacklisting TCMS from further scanning actions.

Security Weaknesses



Missing Multi-Factor Authentication

TCMS leveraged multiple attacks against DC login forms using valid credentials harvested through open-source intelligence. Successful logins included employee e-mail accounts through Outlook Web Access and internal access via Active Directory login on the VPN. The use of multi-factor authentication would have prevented full access and required TCMS to utilize additional attack methods to gain internal network access.

Weak Password Policy

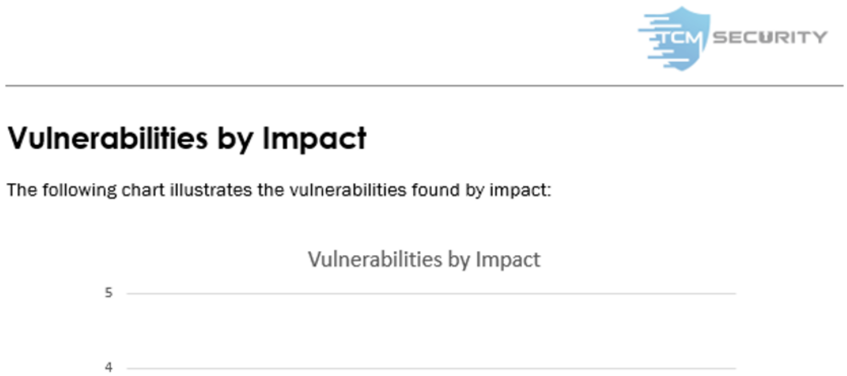
TCMS successfully performed password guessing attacks against DC login forms, providing internal network access. A predictable password format of Summer2018! (season + year + special character) was attempted and successful.

Unrestricted Logon Attempts

During the assessment, TCMS 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.

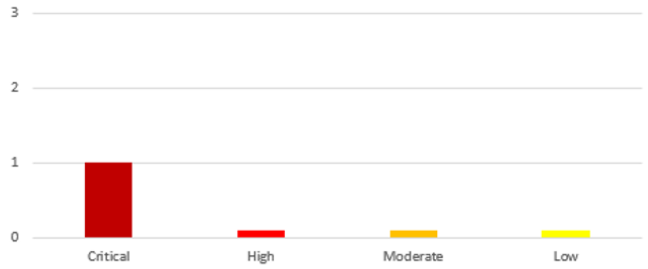
Giving credit where credit is due is certainly a common theme among companies. The report does not need to focus entirely on the negative aspects of the company or the identified/exploited vulnerabilities. If the company is doing some things right, then there is a time and a place to make sure to highlight those things. Also, generalizing the higher-level root causes of multiple issues, such as missing MFA, can help focus attention on a problem area.

Vulnerabilities by Impact



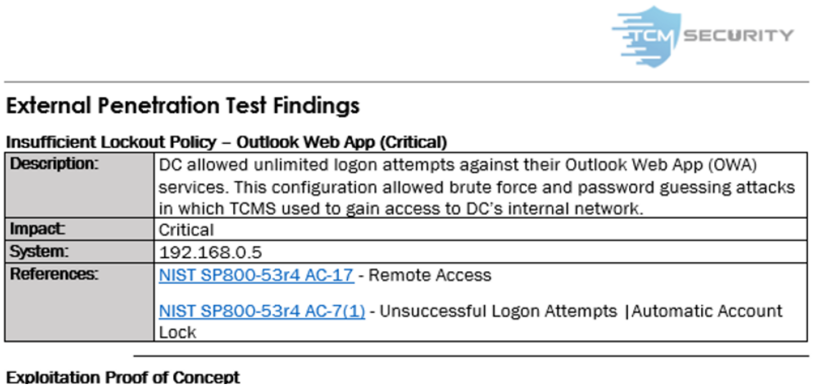
Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:



The first chart and the first actual instance of color in this report occur on page 9 of the report. Look at the graph: not too exciting. Is it even necessary?

External Penetration Test Findings

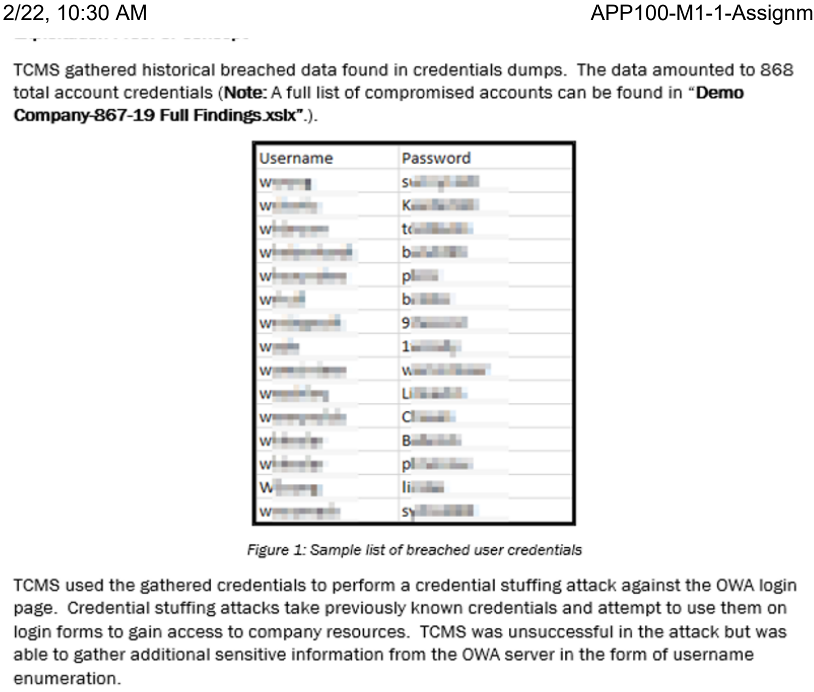


External Penetration Test Findings

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**".).

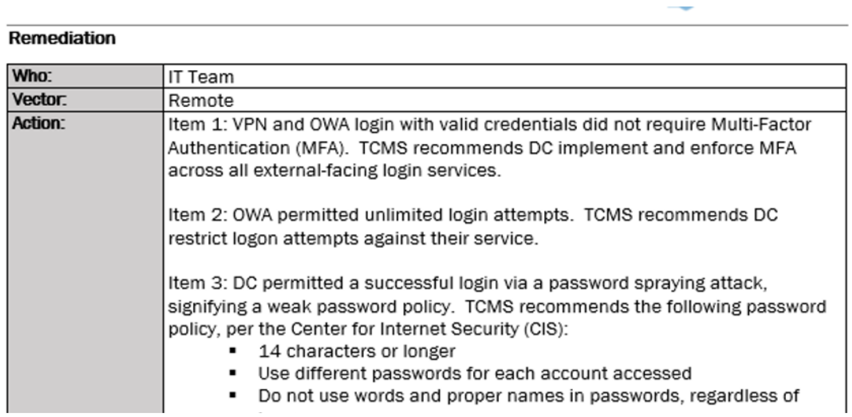
Username	Password
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]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

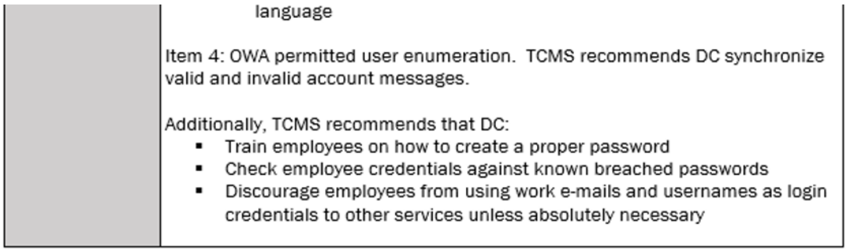
Here is the "meat" of the report. Once again, some colors would be nice. If this is critical, a bright red banner would quickly help denote that. The description is ok; the impact is "Critical," but what is the CVSS score? There should be a number associated with the CVSS score, as earlier in the report, CVSS was described as the mechanism used to rate the risk for findings. Not including the score AND how it was calculated invites a "conversation" about the risk of this finding; the best way to combat this is to be in a defensible position backed by quantitative data. Keep this in mind. This template report may not have findings, as this is essentially an outline. Regardless, keep this in mind for future reports.

Remediation of Penetration Test Findings



Remediation

Who:	IT Team
Vector:	Remote
Action:	Item 1: VPN and OWA login with valid credentials did not require Multi-Factor Authentication (MFA). TCMS recommends DC implement and enforce MFA across all external-facing login services. Item 2: OWA permitted unlimited login attempts. TCMS recommends DC restrict logon attempts against their service. Item 3: DC permitted a successful login via a password spraying attack, signifying a weak password policy. TCMS 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

Item 4: OWA permitted user enumeration. TCMS recommends DC synchronize valid and invalid account messages.

Additionally, TCMS recommends that DC:

- Train employees on how to create a proper password
- Check employee credentials against known breached passwords
- Discourage employees from using work e-mails and usernames as login credentials to other services unless absolutely necessary

If a penetration test is performed internally for a company, then MAYBE part of the action steps can be suggesting what team is responsible for remediations, but outside of that situation, it should probably be avoided, unless explicitly requested. Try to come up with more specific advice on how to fix the issues; knowing how to attack and defend is paramount as a professional penetration tester. Also, consider what tools were used to help with this attack. If they were internally developed, will they be shared?

That's pretty much it for the sample report. Did this report hit the main topics?

- Executive summary
- Scope
- Methodology
- Risk rankings
- Findings
- Evidence
- Recommendations
- Steps to reproduce
- Conclusion

There is some work to be done. Review all the linked sample reports and take the report to the next level. Please submit a template (not all information needs to be populated) of your own report as a PDF.

As APP100 progresses, actual target networks, applications, and the like will be dealt with. As these items occur, update this report with "real" information on findings and complete it as a deliverable.

To be clear, this report is a work in progress and will be built upon as this course continues.

Submission: Submit a word document or pdf copy of the Penetration Test Report Template.

Advanced Lab

Calculating CVSS scores can be a bit challenging. Spend some time developing an understanding of how CVSS scores are calculated. Make sure to consider the context and compensating controls in each situation.

compensating controls in each situation.

Writeup

Criteria	Ratings					Pts
Depth of Writing Student was able to express appropriate levels of knowledge in the allotted assignment	**5 pts** **Exceeds Expectations** Student expressed a deep understanding, going beyond the basic Learning Objectives	**3 pts** **Meets Expectations** Student express an appropriate level of understanding to meet the learning objectives	**0 pts** **No Marks**			5 pts
All sections completed	**5 pts** **Exceeds Expectations** All sections completed fully, with some indication the student went beyond the lab	**4 pts** **Meets Expectations** All sections completed	**3 pts** **Minimum Expectations Met** Some work performed on all sections	**2 pts** **Partial Completion** Some sections not attempted or quality of work was lower than expected	**0 pts** **No Marks**	5 pts
						Total Points: 10

Have specific feedback?

Tell us here! (https://flatironschoolforms.formstack.com/forms/canvas_feedback?CourseID=6144&LessonID=205847&LessonType=assignments&CanvasUserID=10700&Course=None)