Vulnerability/Risk Assessment Lab

1 Overview

For this lab, you will be assessing the vulnerabilities in the current state vs. upgrading your network's Microsoft Office or Adobe Acrobat Reader installations. You only have the staffing for one project at a time, so you will need to use the techniques described in the OWASP model, as well as the provided data below, to rate the risk to your business in two scenarios, for each upgrade option, and make and explain your recommendation.

The two threat scenarios are as follows:

1) An advanced adversary with limited staff surgically targets your business for the purpose of stealing sensitive intellectual property which could be sold off to a competitor for a profit to the adversary, and would eliminate your firm's competitive edge.

2) Opportunistic attacker steals and might encrypt (for ransom) some Personally Identifiable Information (PII) for your end-users, including social media access, personal banking, etc. The attacker stands to profit from this, but the value of the information to your business is negligible

2 Assignment

You must calculate the risk ratings (critical/high/medium/low/note) for each upgrade/no-upgrade option.

You are only able to upgrade one software package with the project, **so you don't need to perform all permutations**.

You need to make a **recommendation**, **for each of the two threat adversary scenarios**, as to which one of the packages should be upgraded and which version it should be upgraded to (for a tie-breaker, favor the newer version of the software).

Use the OWASP Risk Rating Methodology, these Slides, and the content discussed in class. However, we will be making one **simplification** to the description, and that is that **all impact factors will contribute to a single impact metric, rather than the separate "technical" and "business" impacts** that are discussed in the external link.

You've contracted a consulting firm to provide base impact & likelihood values for these two scenarios.

Scenario 1 **Likelihood**	**Scenario 1** **Impact**	**Scenario 2** **Likelihood**	**Scenario 2** **Impact**
• **Skill**: 9 • **Motive**: 9 • **Opportunity**: 4 • **Size**: 3 • **Discovery**: 9 • **Awareness**: 6	• **Confidentiality**: 9 • **Integrity**: 2 • **Availability**: 3 • **Financial damage**: 6	• **Skill**: 7 • **Motive**: 9 • **Opportunity**: 7 • **Size**: 6 • **Discovery**: 9 • **Awareness**: 6	• **Confidentiality**: 6 • **Integrity**: 3 • **Availability**: 1 • **Financial damage**: 3

The present state is as follows:
All systems have installed the following software versions

- Microsoft Office XP
- Adobe Acrobat Reader 8

In addition to the impact constants above, there is also an **impact factor** for **Upgrading**, as that requires staff, and must include risk to compatibility and user experience that results in efficiency loss as well. The costs to upgrade from the current state to newer versions is below, and the cost to not upgrade is **0**:

- Microsoft Office 2003: 1
- Microsoft Office 2007: 5
- Microsoft Office 2010: 6

- Adobe Reader 9.3: 5
- Adobe Reader 9.4: 5
- Adobe Reader 10: 8
- Adobe Reader 11: 9

Each version of software comes with its own vulnerabilities which contribute as a **likelihood factor**. As a heuristic, your firm team will be assessing the vulnerability of each package based upon a set of metasploit modules available. It will be assumed that any vulnerability in a version of the software also exists in all earlier versions as well.

From analyzing the module set, we identified that the following file format vulnerabilities are to be considered for the Adobe Acrobat package:

Exploit	Rank	Acrobat 8	Acrobat 9.0-9.3	Acrobat 9.4-9.9	Acrobat 10	Acrobat 11
adobe_collectemailinfo	Good	X				
adobe_cooltype_sing	Great	X	X			
adobe_flashplayer_button	Normal	X	X	X		
adobe_flashplayer_newfunction	Normal	X	X			
adobe_flatdecode_predictor02	Good	X	X			
adobe_geticon	Good	X	X			
adobe_jbig2decode	Good	X	X			
adobe_libtiff	Good	X	X			
adobe_media_newplayer	Good	X	X			
adobe_pdf_embedded_exe_nojs	Excellent	X	X			
adobe_pdf_embedded_exe	Excellent	X	X			
adobe_reader_u3d	Average	X	X	X	X	
adobe_toolbutton	Normal	X	X	X	X	X

adobe_u3d_meshdecl	Good	X	X			
adobe_utilprintf	Good	X				

And from analyzing the module set, we identified that the following file format vulnerabilities are to be considered for the Microsoft Office software suite:

Exploit	Rank	Office XP	Office 2003	Office 2007	Office 2010
ms09_067_excel_featheader	Good	X	X	X	
ms10_004_textbytesatom	Good	X	X		
ms10_038_excel_obj_bof	Normal	X			
ms10_087_rtf_pfragments_bof	Great	X	X	X	X
ms11_021_xlb_bof	Normal	X	X	X	
ms12_005	Excellent	X	X	X	X
ms12_027_mscomctl_bof	Average	X	X	X	X
ms14_017_rtf	Normal	X	X	X	X
mswin_tiff_overflow	Average	X	X	X	X
visio_dxf_bof	Good	X			

Metasploit uses a ranking system to identify the probability with which exploits will succeed. Since exploits are typically operating in a variable state environment, some exploits will periodically crash the program prior to establishing desired access, while others may always succeed. This also informs likelihood, and we will use the following rank values for the likelihood of each exploit, to convert from Metasploit's concept to ours:

Manual = 0 | Low = 1 | Average = 3 | Normal = 5 | Good = 6 | Great = 7 | Excellent = 9

You'll want to determine this **likelihood measurement** of each version of the software packages. Where the vulnerability is not exploitable under a particular version of the software, use the **Manual = 0** rank to measure likelihood. All exploits should be weighed equally when calculating their contribution to the

overall "exploitability" / "ease" likelihood factor. In actuality, their ranking is what impacts their weighting. In other words, you will want to average together the supported exploits as well as the non-functional ones (as zeros) to establish the measurement for this exploitability factor on a per software basis.

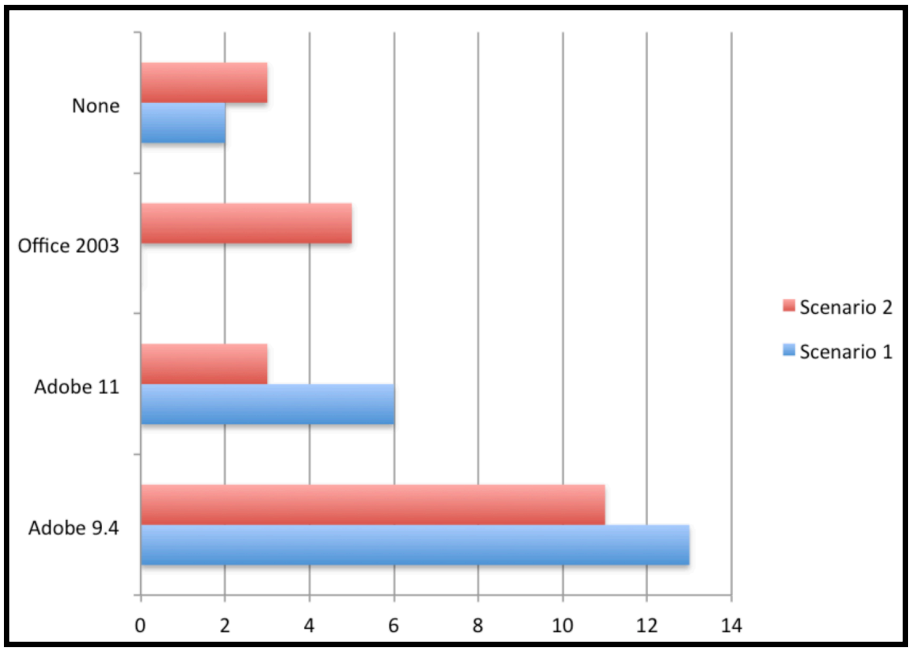

Figure 1:Aggregate Results

3 Hints

Be sure to tie the adversary to the options of not upgrading, upgrading Microsoft and upgrading Adobe. Just one example: the risk associated with an adversary with a high skill level exploiting a severe vulnerability is going to be much higher than the risk associated with a low skill adversary.

Also, note that there is a cost associated with an upgrade (the cost includes many factors). But remember, we want to assign numbers to everything. We also need to justify calculations according to those numbers.

4 Handin

Write a report and submit it via Canvas on or before the specified due date. If you write any supporting programs or spreadsheets, include those as part of the pdf. **Any and all supporting code/notes/documentation will assist in**

grading if your conclusions/results differ from a typical solution.

5 Credit

Dr. John Franco.