

Exercise 1: Performing Passive Reconnaissance

In this exercise, you will perform passive reconnaissance to gather information about the target organization, ACME Corp. Passive reconnaissance is difficult to detect because the information listed is often public. You will review the organization's website to find information that you can weaponize in later exercises.

Review the Target Organization Website

You will gather information from the target's website that you can use in an attack.

To gather information about the target

1. On the bastion host, open a new Google Chrome tab.
2. Enter the following URL:

`https://www.fakeacmecorp.lab`



Make sure that you type the URL correctly.

3. Review the information on the web page.

Because the bastion host has internet access, you are using a fake URL with a .lab domain to access a locally hosted web page. A host DNS record is configured to resolve the URL to its own IP address. This prevents you from accessing a legitimate website.



In addition to the target's website, you can also find information about employees by looking at their career profiles (for example, on LinkedIn), and personal social media pages (for example, on Facebook, Instagram, and so on). In this exercise, you will review the corporate website only.

4. Complete the following table so you have useful information that you can use for spear phishing:

Information	Details
Email addresses	
Names	
Interests	
Downloadable file	
Physical address	
Phone number	



Even though the users' email addresses are not included on the web page, if you have the email domain and usernames, you can increase your success rate with email enumeration, which is the process of discovering valid email addresses. You will perform email enumeration in a later exercise.

Find a Vulnerability to Attack

In the previous task, you should have identified a downloadable intake form. This is a plausible attack vector because you have a target inbox and you know what the target is expecting to receive.

You will download that intake form and see if vulnerable software created it.

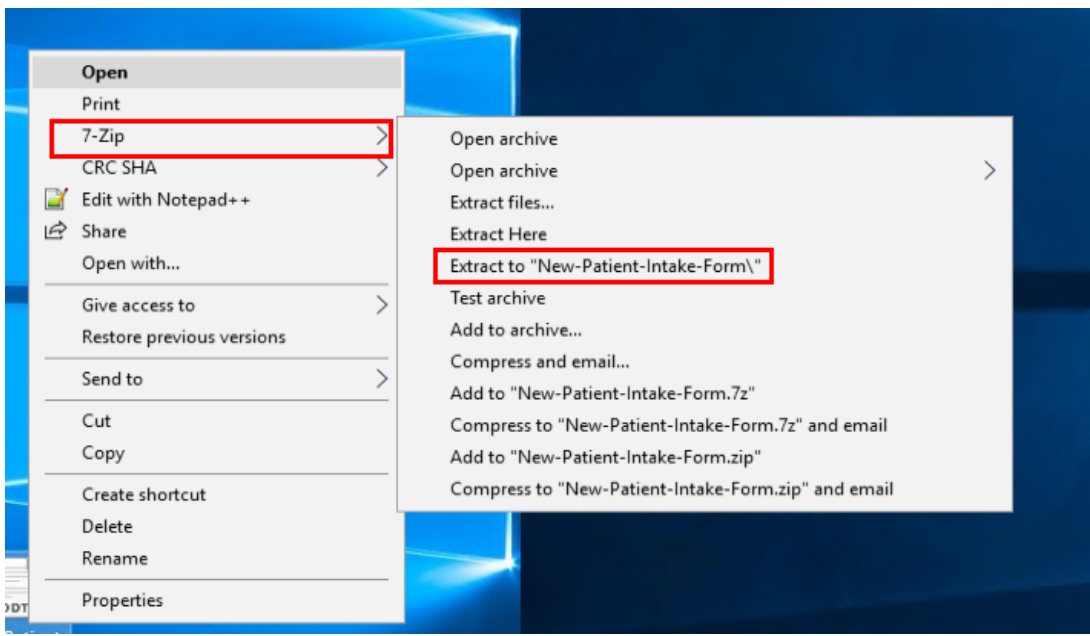
To download the intake form and view its metadata

1. At the bottom of the page, click **intake form** to download the file.

ACME Corp.
1234 Fictional Ave, Suite 100
Fake City, XY 98765
P: (123) 456-7890

For business inquiries: admin@acmecorp.com
For internship opportunities: student@acmecorp.com
For new patients, please download and fill out the **intake form** and send it to admin@acmecorp.com

2. Save the file to the desktop.
3. On the desktop, right-click the New-Patient-Intake-Form.odt file.
4. Click **7-Zip** > **Extract to "New-Patient-Intake-Form\"**.




5. Double-click the extracted folder to open it.
6. In the folder, right-click meta.xml.

Name	Date modified	Type	Size
Configurations2	2024-07-11 6:13 PM	File folder	
META-INF	2024-07-11 6:13 PM	File folder	
Thumbnails	2024-07-11 6:13 PM	File folder	
content.xml	2024-07-10 7:32 PM	XML Document	11 KB
manifest.rdf	2024-07-10 7:32 PM	RDF File	1 KB
meta.xml	2024-07-10 7:32 PM	XML Document	1 KB
mimetype	2024-07-10 7:32 PM	File	1 KB
settings.xml	2024-07-10 7:32 PM	XML Document	11 KB
styles.xml	2024-07-10 7:32 PM	XML Document	12 KB

7. Click **Edit with Notepad++**.
8. Click **View > Word Wrap**.
9. Review the metadata of the XML file.

You are particularly interested in the LibreOffice version that was used to create the file.

```
<?xml version="1.0" encoding="UTF-8"?>
<office:document-meta xmlns:office="urn:oasis:names:tc:opendocument:xmlns:office:1.0" xmlns:xlink=
"http://www.w3.org/1999/xlink" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:meta=
"urn:oasis:names:tc:opendocument:xmlns:meta:1.0" xmlns:ooo="http://openoffice.org/2004/office" xmlns:grddl=
"http://www.w3.org/2003/g/data-view#" office:version="1.2">
  <office:meta>
    <meta:creation-date>2024-07-10T12:26:36.843000000</meta:creation-date>
    <meta:editing-duration>PT6M16S</meta:editing-duration>
    <meta:editing-cycles>1</meta:editing-cycles>
    <meta:document-statistic meta:table-count="1"
meta:image-count="0" meta:object-count="0" meta:page-count="1" meta:paragraph-count="7" meta:word-count="18"
meta:character-count="103" meta:non-whitespace-character-count="92"/>
    <meta:generator>LibreOffice/6.1.2.1$Windows_X86_64
LibreOffice_project/65905a128db06ba48db947242809d14d3f9a93fe</meta:generator>
  </office:meta>
</office:document-meta>
```

 Many office file types are essentially archive files that bundle together components such as text, images, styles, fonts, and metadata. This includes Microsoft Office files and OpenDocument files.

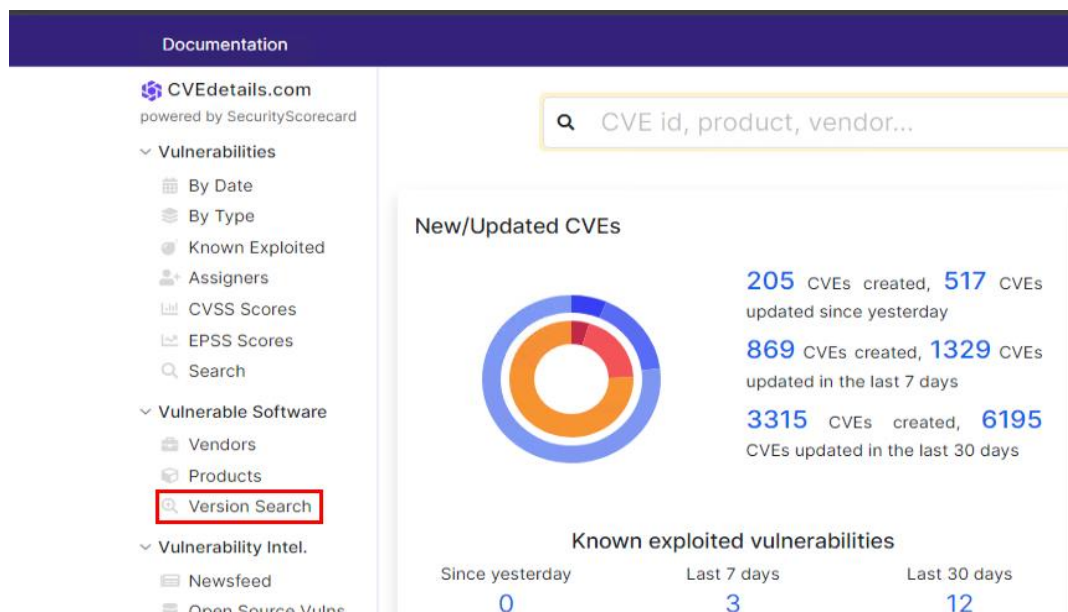
This is why you can use 7-Zip to extract different files from the .odt extension.

To confirm vulnerabilities of the software

1. In Chrome, open a new tab.
2. In the bookmarks bar, click **SOC Analyst > CVEdetails**.

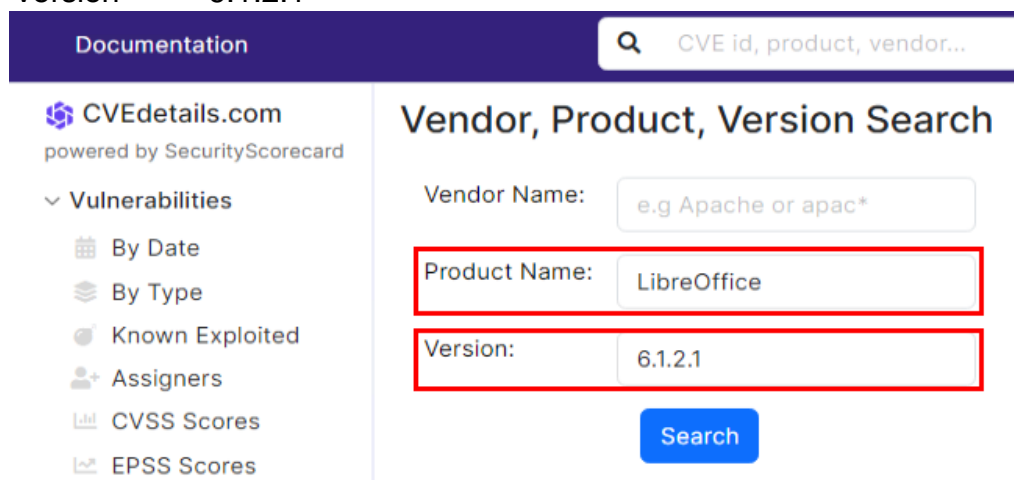
The CVEdetails.com website should load.

3. In the menu on the left, expand **Vulnerable Software**, and then click **Version Search**.



4. Configure the following settings to set the search parameters:

Field	Value
Vendor Name	Leave this field empty.
Product Name	LibreOffice
Version	6.1.2.1



5. Click **Search**.
6. Review the list of vulnerabilities.
7. Click the **CVE-2018-16858** entry.

CVE-2018-16858

Public exploit

It was found that libreoffice before versions 6.0.7 and 6.1.3 was vulnerable to a directory traversal attack which could be used to execute arbitrary macros bundled with a document. An attacker could craft a document, which when opened by LibreOffice, would execute a Python method from a script in any arbitrary file system location, specified relative to the LibreOffice install location.

Source: Red Hat, Inc.

Max CVSS

9.8

EPSS Score

96.33%

Published

2019-03-25

Updated

2019-08-06

8. Review the vulnerability details.

Vulnerability Details : CVE-2018-16858

Public exploit exists!

It was found that libreoffice before versions 6.0.7 and 6.1.3 was vulnerable to a directory traversal attack which could be used to execute arbitrary macros bundled with a document. An attacker could craft a document, which when opened by LibreOffice, would execute a Python method from a script in any arbitrary file system location, specified relative to the LibreOffice install location.

Published 2019-03-25 18:29:00 Updated 2019-08-06 17:15:29 Source Red Hat, Inc.

View at NVD, CVE.org

Vulnerability category: Directory traversal

EPSS FAQ

Exploit prediction scoring system (EPSS) score for CVE-2018-16858

96.33%

Probability of exploitation activity in the next 30 days

EPSS Score History

~ 100 %

Percentile, the proportion of vulnerabilities that are scored at or less

Metasploit modules for CVE-2018-16858

LibreOffice Macro Code Execution

Disclosure Date: 2018-10-18 First seen: 2020-04-26

exploit/multi/fileformat/libreoffice_macro_exec

LibreOffice comes bundled with sample macros written in Python and allows the ability to bind program events to them. A macro can be tied to a program event by including the script that contains the macro and the function name to be executed. Additionally, a director

More information

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source	First Seen
7.5	HIGH	AV:N/AC:L/Au:N/C:P/I:P/A:P	10.0	6.4	NIST	
9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	3.9	5.9	NIST	
7.8	HIGH	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	1.8	5.9	Red Hat, Inc.	

9. Complete the following table:

Question	Answer
What does the exploit do?	
Which versions are affected?	
Is the LibreOffice version from the ODT file vulnerable?	You can scroll to the bottom of the page to see the affected versions.
	Make a note that there is a Metasploit module for this vulnerability.
	So far, you have only confirmed that the intake form is running an old version of LibreOffice. However, this does not mean the software in production is unpatched. Regardless, this is important information that you can use to potentially exploit the organization.

LAB-CHALLENGE > Performing Passive Reconnaissance