实验 - 使用黑客工具加密和解密数据

目标

第 1 部分：创建和加密文件

第 2 部分：恢复加密的 zip 文件密码

1. 背景/场景

如果同学们在一家大型公司工作，而该公司制定了关于可移动媒体的公司政策，会出现什么情况？具体地说，该政策规定只能将加密的 zip 文档复制到便携式 USB 闪存驱动器。

在此情景中，首席财务官 (CFO) 在外地出差，他慌慌张张地联系同学们并提出了紧急的求助请求。在外地出差时，他试图解压 USB 驱动器上某加密 zip 文件中的重要文档。但是，提供的用于打开 zip 文件的密码无效。CFO 联系同学们，想看看同学们是否能帮他做点什么。

**注**：所提供的情景很简单，仅用作示例。

可能有一些工具可用于恢复丢失的密码。如果网络安全分析师可以从 CFO 那里获得相关信息（例如密码的长度，以及密码可能是什么），则在这类情况下，尤其有可能可以使用工具恢复密码。在试图恢复密码时，了解相关信息会有很大的帮助。

密码恢复实用工具和程序的例子包括 hashcat、John the Ripper、Lophtcrack 等。在我们的情景中，我们将使用 **fcrackzip**，它是一种简单的 Linux 实用程序，用于恢复加密的 zip 文件的密码。

请注意，网络犯罪分子也可以使用这些工具来发现未知密码。虽然他们无法访问某些相关信息，但随着时间的推移，他们可能会发现密码以打开加密的 zip 文件。所需的时间长短取决于密码强度和密码长度。密码越长且越复杂（（混合使用不同类型的字符），就越安全。

在本实验中，同学们将：

* 创建和加密示例文本文件。
* 解密加密的 zip 文件。

**注：**本实验仅用于教学目的。这里介绍的方法不得用于保护真正敏感的数据。

1. 所需资源

* CyberOps Workstation 虚拟机
* 互联网接入

1. 创建和加密文件

在本部分中，同学们需要创建几个文本文件，在下一步中将其用于创建加密的 zip 文件。

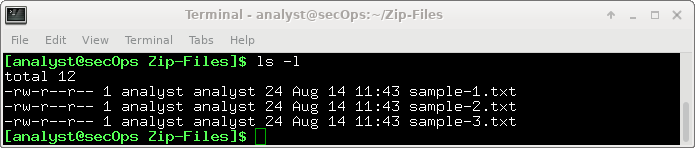
* 1. 创建文本文件。
     1. 启动 CyberOps Workstation 虚拟机。
     2. 打开终端窗口。验证同学们是否处于 analyst 主目录中。否则，请在终端提示符后输入 **cd ~**。
     3. 使用 **mkdir Zip-Files** 命令创建一个名为 Zip-Files 的新文件夹。
     4. 使用 **cd Zip-Files** 命令移动到该目录中。
     5. 输入以下命令以创建名为 **sample-1.txt** 的文本文件。

[analyst@secOps Zip-Files]$ **echo This a sample text file > sample-1.txt**

[analyst@secOps Zip-Files]$ **echo This a sample text file > sample-2.txt**

[analyst@secOps Zip-Files]$ **echo This a sample text file > sample-3.txt**

* + 1. 使用 **ls** 命令验证文件是否已创建。



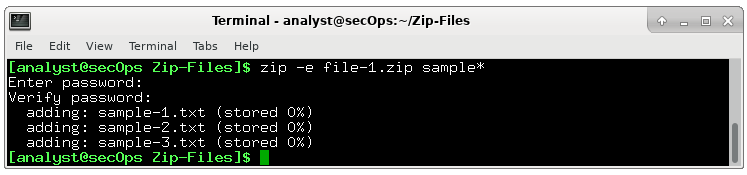
* 1. 压缩并加密文本文件。

接下来，我们将使用不同的密码长度创建几个加密的 zip 压缩文件。为此，我们将使用 **zip** 实用程序对这三个文本文件进行加密。

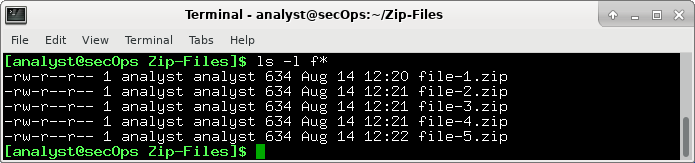
* + 1. 使用以下命令创建一个名为 **file-1.zip** 的加密 zip 文件，其中包含三个文本文件：

[analyst@secOps Zip-Files]$ **zip –e file-1.zip sample\***

* + 1. 当系统提示输入密码时，输入同学们所选择的单字符密码。在本例中，输入了字母 **B**。在系统提示验证时输入相同的字母。

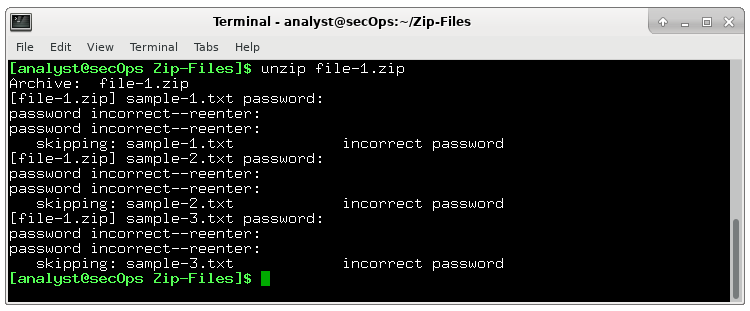


* + 1. 重复此过程，以创建以下 4 个其他文件
* 使用同学们所选择的由 2 个字符组成的密码创建 **file-2.zip**。在我们的示例中，使用的是 **R2**。
* 使用同学们所选择的由 3 个字符组成的密码创建 **file-3.zip**。在我们的示例中，使用的是 **0B1**。
* 使用同学们所选择的由 4 个字符组成的密码创建 **file-4.zip**。在我们的示例中，使用的是 **Y0Da**。
* 使用同学们所选择的由 5 个字符组成的密码 **file-5.zip**。在我们的示例中，使用的是 **C-3P0**。
  + 1. 验证是否使用 **ls** 命令创建了所有压缩文件。



* + 1. 尝试使用不正确的密码打开 zip 文件，如下所示。

[analyst@secOps Zip-Files]$ **unzip file-1.zip**

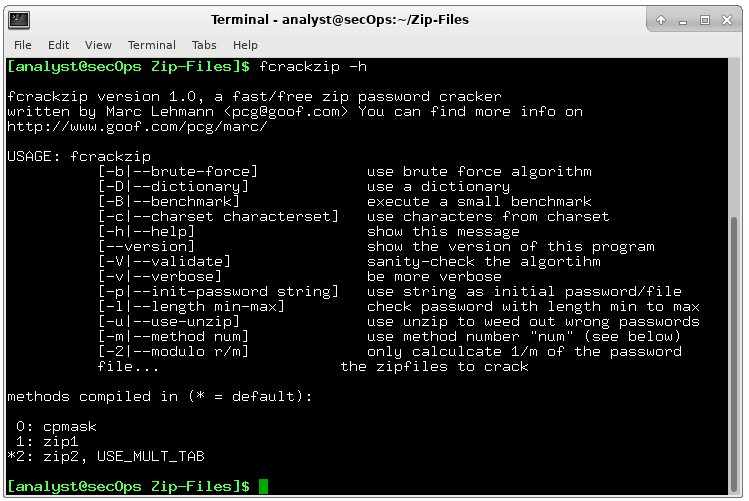


1. 恢复加密的 zip 文件密码

在本部分中，同学们需要使用 **fcrackzip** 实用程序从加密的 zip 文件恢复丢失的密码。Fcrackzip 会搜索所提供的每个 zip 文件是否包含加密文件，并尝试用暴力破解方法猜测密码。

之所以使用不同密码长度创建 zip 文件，是为了查看密码长度是否会影响发现密码所需的时间。

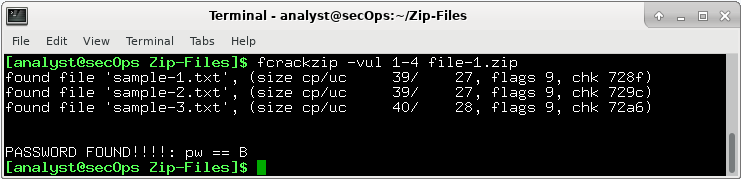
* 1. Fcrackzip 简介
     1. 在终端窗口中，输入 **fcrackzip –h** 命令以查看相关的命令选项。



在我们的示例中，将使用 **–v**、**-u** 和 **-l** 命令选项。-l 选项之所以列在最后，是因为它指定了可能的密码长度。随意试验其他选项。

* 1. 使用 fcrackzip 恢复密码
     1. 现在，尝试恢复 **file-1.zip** 文件的密码。回想一下，加密文件使用的是单字符密码。因此，请使用以下 **fcrackzip** 命令：

[analyst@secOps Zip-Files]$ **fcrackzip -vul 1-4 file-1.zip**



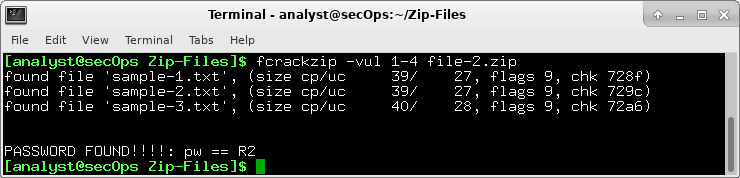
**注：**密码长度可能已设置为少于 1–4 个字符。

发现密码需要多长时间？

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. 现在，尝试恢复 **file-2.zip** 文件的密码。回想一下，加密文件使用的是由 2 个字符组成的密码。因此，请使用以下 **fcrackzip** 命令：

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-4 file-2.zip**

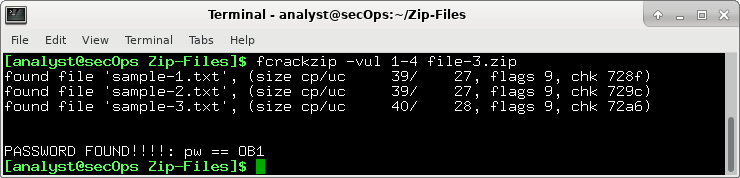


发现密码需要多长时间？

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. 重复该程序并恢复 **file-3.zip** 文件的密码。回想一下，加密文件使用的是由 3 个字符组成的密码。现在来看看发现由 3 个字母组成的密码需要多长时间。使用以下 **fcrackzip** 命令：

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-4 file-3.zip**

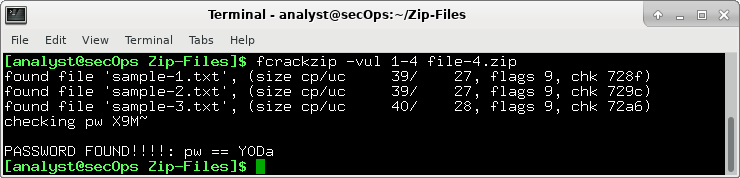


发现密码需要多长时间？

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. 破解由 4 个字符组成的密码需要多长时间？重复该程序并恢复 **file-4.zip** 文件的密码。现在来看看使用以下 **fcrackzip** 命令发现密码需要多长时间：

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-4 file-4.zip**

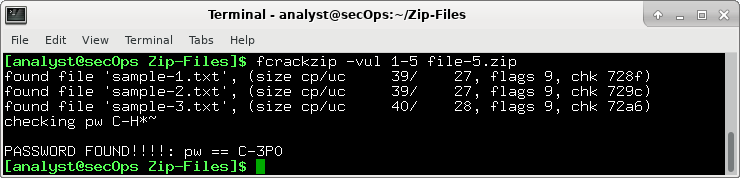


发现密码需要多长时间？

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. 破解由 5 个字符组成的密码需要多长时间？重复该程序并恢复 **file-5.zip** 文件的密码。密码长度为 5 个字符，因此我们需要将 **-l** 命令选项设为 **1-5**。现在来看看使用以下 **fcrackzip** 命令发现密码需要多长时间：

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-5 file-5.zip**



发现密码需要多长时间？

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. 使用 fcrackzip 恢复由 6 个字符组成的密码

密码越长，发现密码所需的时间似乎越长，因此也越安全。但是，由 6 个字符组成的密码无法阻止网络犯罪分子。

同学们认为 fcrackzip 发现由 6 个字符组成的密码需要多长时间？

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

要回答这个问题，请使用同学们所选择的由 6 个字符组成的密码创建一个名为 **file-6.zip** 的文件。在我们的示例中，使用的是 **JarJar**。

[analyst@secOps Zip-Files]$ **zip –e file-6.zip sample\***

* + 1. 重复该程序，使用以下 **fcrackzip** 命令恢复 **file-6.zip** 文件的密码：

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-6 file-6.zip**

Fcrackzip 发现密码需要多长时间？

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

显而易见的是，密码越长越安全，因为密码越长，发现密码所需的时间也越长。

为确保密码的安全，同学们建议的密码长度是多少？

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_