CTF-Crypto必备自动解密神器-Ciphey

原创

OceanSec 于 2021-10-27 21:17:26 发布

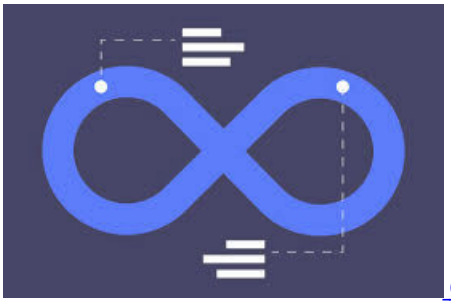
分类专栏： # CTF # Other 文章标签： ci

本文链接：https://blog.csdn.net/q20010619/article/details/121002378

CTF 同时被 2 个专栏收录

66 篇文章 29 订阅

订阅专栏



Other

32 篇文章 2 订阅

订阅专栏

Ciphey-自动解码神器

> Github地址：https://github.com/Ciphey/Ciphey
> 建议给作者点星✔

使用自然语言处理和人工智能以及一些常识的全自动解密/解码/破解工具

特性

- **支持 30+的加密方法** 例如编码（二进制，base64）和常规加密（例如 Caesar 密码，重复密钥 XOR 等）**有关完整列表，请单击此处**
- **具有增强搜索功能的定制人工智能（AuSearch）可以回答"使用了哪种加密技术?"** 解密时间不到 3 秒
- **定制的自然语言处理系统** Ciphey 可以确定某些东西是否是纯文本。无论该纯文本是 JSON，CTF 标志还是英语 Ciphey，都可以在几毫秒内获得它
- **多国语言支持** 目前，仅有德语和英语（带有 AU，UK，CAN，USA 变体）
- **支持加密和哈希** 诸如 CyberChef Magic 之类的替代品则没有。
- **C++ 核心** 这会使整个过程变得非常快

Ciphey安装方法

Python	Docker (Universal)	MacPorts (macOS)	Homebrew (macOS/Linux)
			
`python3 -m pip install ciphey --upgrade`	`docker run -it --rm remnux/ciphey`	`sudo port install ciphey`	`brew install ciphey`

要安装 Ciphey，您需要 2 个核心内容：

1. Python3.7或以上
2. Pip（在 Python 3 上）

检查 Python 是否已经安装。运行这两个命令：

```
python -c "import sys; print(sys.version)"
```

或

```
python3 -c "import sys; print(sys.version)"
```

Linux命令安装

在 Linux 上运行以下命令：

```
python3 -m pip install -U ciphey
```

Windows Python 默认安装 32 位。Ciphey 仅支持 64 位。确保您使用的是 64 位 Python

```
建议用linux，如果Linux安装过程中，报错
ERROR: Cannot uninstall 'PyYAML'. It is a distutils installed project and thus we cannot accurately determine wh
ich files belong to it which would lead to only a partial uninstall.
可以通过执行以下命令来解决
sudo -H pip3 install --ignore-installed PyYAML
```

ciphey命令参数

```
ciphey --help
用法: ciphey [选项] [TEXT_STDIN]

  Ciphey - 自动解密工具

  文档地址: https://github.com/Ciphey/Ciphey/wiki

  Discord (这里支持，我们大部分时间都在线):
  https://discord.ciphey.online/

  GitHub: https://github.com/ciphey/ciphey

 cipher是一种使用智能人工智能的自动解密工具
和自然语言处理。输入加密文本，获取解密文本


例如:
 基本用法: ciphey -t "aGVsbG8gbXkgbmFtZSBpcyBiZWU="

选项:
  -t, --text TEXT             您想要解密的密文。
  -q, --quiet                 减少冗长的显示,直接给结果
  -g, --greppable             只输出答案(对于grep很有用)
  -v, --verbose
  -C, --checker TEXT          使用给定的检查器
  -c, --config TEXT           使用给定的配置文件。默认为
                              appdirs.user_config_dir('ciphey',
                              'ciphey')/'config.yml'

  -w, --wordlist TEXT         使用给定的密码字典
  -p, --param TEXT            将参数传递给语言检查器
  -l, --list-params BOOLEAN   列出所选模块的参数
  --searcher TEXT             选择要使用的搜索算法
  -b, --bytes                 强制密码使用二进制模式作为输入
  --default-dist TEXT         设置默认的字符/字节分布
  -m, --module PATH           从给定路径添加模块
  -A, --appdirs               输出密码到想要的文件位置

  -f, --file FILENAME
  --help                      显示此帮助消息并退出。
```

以一道题为例：

将flag经过base32->base58->base64加密

```
root@kali:~/桌面# ciphey -t "I44EOOLCIFUDQ5KLME======"
Possible plaintext: 'ZA?R' (y/N): n
Possible plaintext: 'flag' (y/N): y

 Formats used:
    base32
    utf8
    base58_bitcoin
    base64
    utf8Plaintext: "flag"
```

```
ciphey -t "I44EOOLCIFUDQ5KLME======"
```

运行，会自动运算，如果不是想要的结果可以输入 n，继续运算，直至正确结果

附录

支持解密列表

> ## 支持破解的密码列表
>
> ### 基本加密
>
> - Caesar Cipher-凯撒密码
> - ROT47（使用 ROT47 字母高达 ROT94）
> - ASCII 移位（高达 ROT127，带有完整的 ASCII 字母表）
> - Vigenère Cipher-维吉尼亚密码
> - Affine Cipher-仿射密码
> - Binary Substitution Cipher-二进制替换密码 (XY-Cipher)
> - Baconian Cipher -培根密码（两种变体）
> - Soundex
> - Transposition Cipher-转置密码
> - Pig Latin-猪拉丁语
>
> ### 现代密码学
>
> - Repeating-key XOR-重复键异或
> - Single XOR-单异或
>
> ### 编码
>
> 为什么你有很多解码器？
>
> - Base2（二进制）
> - Base8（八进制）
> - Base10（十进制）
> - Base16（十六进制）
> - Base32
> - Base58 比特币
> - Base58 Flickr（发布候选阶段）
> - Base58 Ripple
> - Base62
> - Base64
> - Base64 URL（发布候选阶段）
> - Base69
> - Base85
> - Z85（发布候选阶段）
> - ASCII Base85
> - Base91
> - Base65536（发布候选阶段）
> - ASCII
> - Reversed text-反转文字

- Morse Code-摩尔斯电码
- DNA codons-DNA 密码子（释放候选阶段）
- Atbash
- Standard Galactic Alphabet-标准银河字母表（又名 Minecraft Enchanting Language）
- Leetspeak
- Baudot ITA2
- URL encoding-网址编码
- SMS Multi-tap
- DMTF（发布候选阶段）
- A1Z26（发布候选阶段）
- Prisoner's Tap Code-囚犯的窃听代码
- UUencode
- Braille-盲文（1 级）

深奥的语言 (EsoLang)

- Brainfuck-脑残

压缩方法

- GZip

哈希值

注意：由于我们无法控制的外部服务的一些错误，哈希现在被关闭。
Ciphey 支持 272 个哈希。

MD5

SHA-1

SHA-256

SHA-384
深奥的语言 (EsoLang)

Brainfuck-脑残

压缩方法

- GZip

哈希值

注意：由于我们无法控制的外部服务的一些错误，哈希现在被关闭。
Ciphey 支持 272 个哈希。

- MD5
- SHA-1
- SHA-256
- SHA-384
- SHA-512

关注博主,学习更多安全知识