

20200703信息安全实训

笔记本： 我的第一个笔记本

创建时间： 2020/7/3 9:01

更新时间： 2020/7/3 16:40

作者： 820410740@qq.com

暴力破解

暴力破解原理

暴力破解是用户使用自定义字典文件中的内容与验证程序交互，从而在枚举过程中得到正确数据。

案例：

- 1、破解用户名、密码
- 2、破解验证码 - 之前四位数的手机验证码在未进行任何防护措施，导致被枚举出来。

由此得暴力破解的基础

- 1、应用程序或服务器未进行限制
- 2、具有内容涵盖全面的字典文件

暴力破解的方式

根据破解的验证内容是否处于服务状态将暴力破解分为以下两类：

- 1、在线破解
- 2、离线破解

无论是在线还是离线是否可以破解成功都取决于字典文件内容的强大。同时破解速度的瓶颈在于本地机器与服务器性能、带宽等因素。

hash-identifer

cmd5

cupp

泰阿

cupp介绍与安装

Cupp是一个跨平台的，用Python编写，用来针对个人情况制作密码字典。它的功能很简单，但有非常强大的结果。

安装步骤：

```
git clone https://github.com/Mebus/cupp.git
cd cupp
ls
./cupp.py
```

需要使用Python3来运行cupp

cupp使用基础

下面给出cupp的参数帮助信息。

- h 显示帮助信息
- i 以交互的方式制作用户密码字典文件
- w 使用此选项配置现有字典
- l 从仓库下载大型字典文件
- a 直接从Alecto DB解析默认用户名和密码。
- v 显示版主信息

```
root@kali:~/Desktop/cupp# python3 cupp.py -h
usage: cupp.py [-h] [-i | -w FILENAME | -l | -a | -v] [-q]

Common User Passwords Profiler

optional arguments:
  -h, --help            show this help message and exit
  -i, --interactive     Interactive questions for user password profiling
  -w FILENAME           Use this option to improve existing dictionary, or WyD.pl
                        output to make some pwnsauce
  -l                    Download huge wordlists from repository
  -a                    Parse default usernames and passwords directly from
                        Alecto DB. Project Alecto uses purified databases of
                        Phenoelit and CIRT which were merged and enhanced
  -v, --version         Show the version of this program.
  -q, --quiet           Quiet mode (don't print banner)
root@kali:~/Desktop/cupp#
```

pydictor介绍与安装

- Pydictor是新手和专业人士都能欣赏的工具之一。它是一个字典构建工具，在处理密码强度测试时，它是一个非常好的工具。该工具提供了大量的特性，可以用来为几乎任何测试情况创建完美的字典。

安装步骤：

```
git clone https://github.com/LandGrey/pydictor.git
cd pydictor
python pydictor.py
```

参考文档：https://github.com/LandGrey/pydictor/blob/master/README_CN.md

HTTP Basic认证

HTTP Basic认证介绍

基本认证 basic authentication ← HTTP1.0提出的认证方法

基本认证步骤:

1. 客户端访问一个受http基本认证保护的资源。
2. 服务器返回401状态, 要求客户端提供用户名和密码进行认证。
401 Unauthorized
WWW-Authenticate: Basic realm="WallyWorld"
3. 客户端将输入的用户名密码用Base64进行编码后, 采用非加密的明文方式传送给服务器。
Authorization: Basic xxxxxxxxxx.
4. 如果认证成功, 则返回相应的资源。如果认证失败, 则仍返回401状态, 要求重新进行认证。

htpasswd.exe

```
4      AddHandler fcgid-script .php
5      FcgidWrapper "D:/phpstudy_pro/Extensions/php/
6  <Directory "D:/phpstudy_pro/WWW">
7      Options FollowSymLinks ExecCGI
8      AllowOverride authconfig
9      Order allow,deny
10     Allow from all
11     AuthName "do you want to go in?"
12     AuthType basic
13     AuthUserFile "E:\\basic_auth.txt"
14     Require valid-user
15     DirectoryIndex index.php index.html
16 </Directory>
17 ErrorDocument 400 /error/400.html
18 ErrorDocument 402 /error/402.html
```