



渗透测试工程师技术实战课

暴力破解



● 暴力破解

- 身份认证方法
- 证明你是声称你是的那个人
 - 你知道什么（账号密码、pin）
 - 你有什么（令牌、token、key、证书、密保、手机
 - 你是谁（指纹、视网膜、虹膜、掌纹、声纹、面部识别）
 - 以上方法结合适用（多因素身份认证）
- 基于互联网的身份验证以账号密码为主要形式



● 暴力破解

● 思路

- 目标系统实施了强安全措施
- 安装了所有补丁
- 无任何已知漏洞
- 无应用层漏洞
- 攻击面最小化

● 社会工程学

● 获取目标系统用户身份

- 非授权用户不守信，认证用户可以访问守信资源
- 已有用户账号权限受限，需要提权
- 不会触发系统报警



赛博梦工厂

Cyber Works

暴力破解

- 暴力破解漏洞的产生来自于服务器并没有对输入参数的内容，输入参数次数进行限制。导致攻击者可以通过暴力的手段进行破解所需要的信息，如用户名、密码、验证码等。暴力破解需要一个庞大的字典，4位数字的验证码，暴力破解的范围就是0000~9999，暴力破解的关键在于字典的大小

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the payload type. The number of payload sets depends on the payload type. The number of payload sets depends on the payload type. The number of payload sets depends on the payload type.

Payload set: 1 Payload count: 10,000
Payload type: Brute forcer Request count: 0

Payload Options [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations of the specified character set.

Character set: 0123456789
Min length: 4
Max length: 4

您的密码将被破解

25纳秒



● 暴力破解

- 人工猜解
- 基于字典暴力破解（主流）
- 键盘字符爆破
- 字典
 - 保存有用户名和密码的文本文件
 - `crunch <min-len> <max-len> [<charset string>] [options]`
 - `<charset sting>`默认是小写字符
 - `crunch 6 6 0123456789 -o START -d 2 -b 1mb / -c 100`
 - `-b`按大小分割字典文件(kb/kib、mb/mib、gb/gib)
 - `-c`每个字典行数
 - `-d`同一字符连贯出现数量(aa/aaa)



● 暴力破解

- 字符集

- `crunch 4 4 -f /usr/share/crunch/charset.lst lalpha-sv -o 1.txt`

- -t 命令如下:

- -t @,%^, 指定模式, @,%^分别代表意义如下:

- @ 插入小写字母
 - , 插入大写字母
 - % 插入数字
 - ^ 插入特殊符号



● 暴力破解

- `cewl www.baidu.com -m 3 -d 3 -e -c -v -w a.txt`
 - -m: 最小长度, 默认最小长度为3
 - -d: 爬行深度, 默认2
 - -c: 显示发现的每个单词的数量
 - -v: verbose
- 字典变形
 - 基于cewl的结果进行密码变型
 - 末尾增加数字串
 - 字母大小写变化
 - 字母与字符互相转换
 - 字母与数字互相转换
 - P@\$w0rd



● 暴力破解

- Windows密码破解
 - `hydra -l administrator -P pass.lst smb://1.1.1.1/admin$`
 - `hydra -l administrator -P pass.lst rdp://1.1.1.1 -t 1`
- Linux密码破解
- - `hydra -l root -P pass.lst ssh://1.1.1.1 -vV`
- 其他服务密码破解
- - `hydra -L user.lst -P pass.lst ftp://1.1.1.1 -s 2121 -e nsr -o p.txt -t 64`
- 图形化界面
- - `xhydra`
- web表单破解
 - Burpsuite
 - pkAV



● 暴力破解-防御

- 账户锁定
- 返回信息
- 适当的延时
- IP策略锁定
- 验证码



The image features a central figure of a person wearing a black hoodie, with their right hand resting on the hood. The background is a vibrant blue digital landscape. On the right side, a glowing globe is visible, surrounded by intricate network patterns of lines and nodes. The overall aesthetic is high-tech and futuristic, with various icons like padlocks and arrows scattered throughout the scene.

谢谢观赏