弱口令扫描实施标准

2019护网专项培训

NSFOCUS

CONTENTS

目 录

01

怎么定制口令字典库

1. 字典库定制原理
2. 字典库定制流程与操作
3. 字典库优化与维护

2.1

字典库定制原理

a. 为什么需要定制字典库

b. 字典库形式

c. 字典库包含要素

d. “合格”字典库的判断

字典库定制原理 – 为什么需要定制字典库

字典库大小

- 评估资产有弱口令却检查不出来

字典库太大

- 评估时间过长，无法结束，耽误评估进度及业务、运维工作
- 字典库还没遍历完任务就超时了

字典库定制原理 – 字典库形式

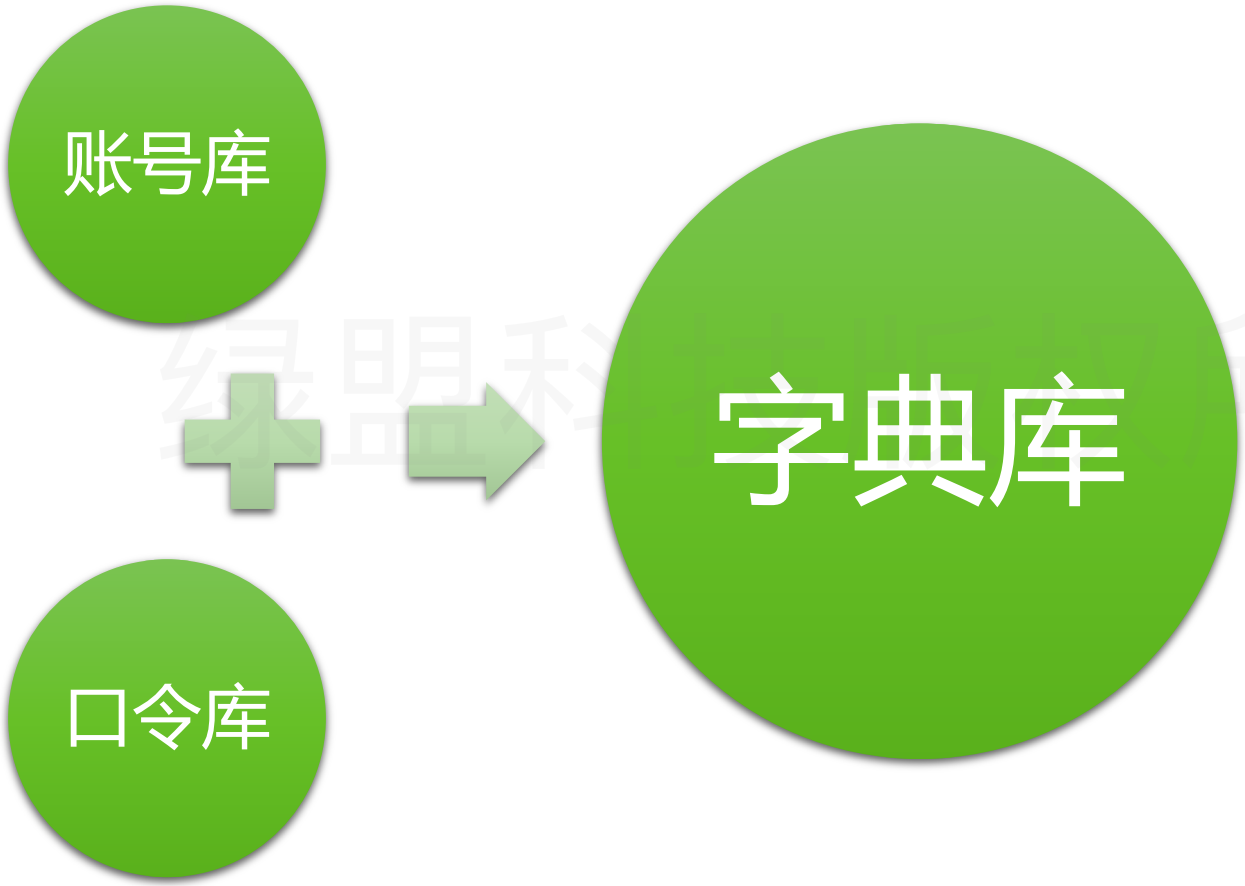
标准模式

- 账号：口令，账号与口令一对一
- 如user1:psw1，user2:psw2……

混合模式

- 分别制定账号库和口令库，账号与口令一对多
- 扫描时遍历账号库中账号，分别与口令库中所有口令对应
- 如user1:psw1，user1:psw2，user1:psw3……
- user2:psw1，user2:psw2，user2:psw3……

字典库定制原理 – 字典库包含要素



字典库定制原理 – “合格”字典库的判断

效率

- 时间不宜过长，需控制在超时时间内能遍历完所有字典库，或任务时间不影响业务、运维工作的开展

合格的字典库应在效率和完整性中取得平衡，护网期间，时间允许的情况下可尽量保证完整性

完整性

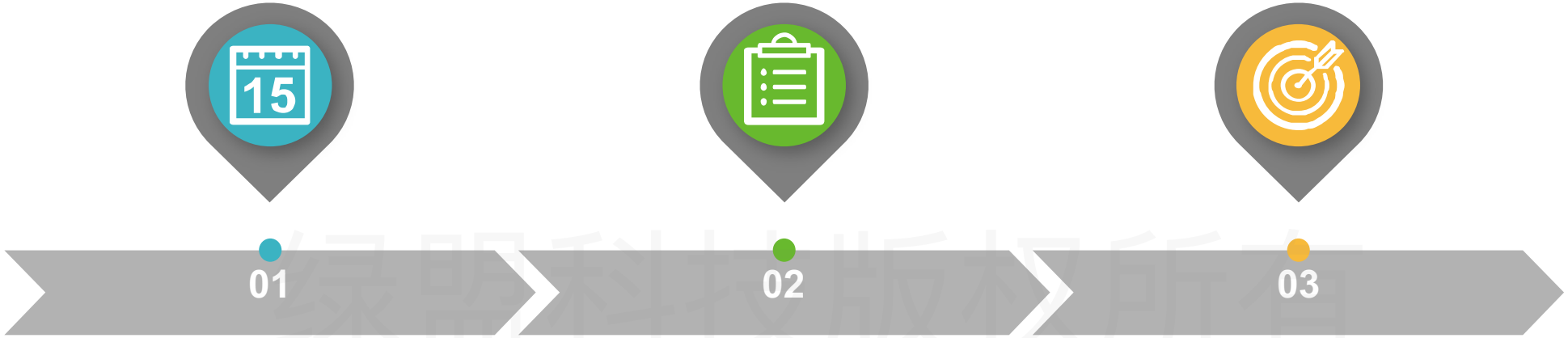
- 字典库应尽量覆盖通用弱口令、几率较高的热门弱口令、评估目标组织常用弱口令、目标系统应用默认弱口令等，尽可能发现目标环境中存在的各类脆弱口令

1.3

字典库定制流程与操作

a. 定制流程概述
b. 字典库形式选择
c. 字典库收集
d. 字典库输出

字典库定制流程与操作 – 定制流程概述



收集

- 收集各类通用弱口令
- 针对评估环境收集特定弱口令

形式选择

- 账号与口令一对一形式
- 账号与口令一对多形式

输出

- 输出适用特定评估环境的字典库

字典库定制流程与操作 – 字典库收集

通用弱口令

- 弱口令扫描工具内置的通用弱口令字典库
- 近期公布的常见弱口令报告或弱口令排名，如《2018年度密码报告》

评估模式下的特定弱口令

- 评估组织业务及运维人员常用弱口令
- 评估目标系统组件、应用的默认账号口令
- 评估目标同类业务系统的常用弱口令
- 评估目标所属行业中的常用弱口令
- 评估目标代维厂商的常用弱口令

字典库定制流程与操作 – 字典库形式选择

账号与口令一对一	账号与口令一对多
• 对应关系较明确，扫描时间短 • 适用于相同口令不多的环境	• 需遍历账号库和口令库，扫描时间长 • 适用于不同账号较多相同口令的环境

字典库定制流程与操作 – 字典库输出

账号与口令一对一

```
空:public
anonymous:anon@ymous.tw
ftp:nsfocus
anonymous:anonymous
ftp:ftp
anonymous:nsfocus
sudouser:sudouser
sudoroot:sudoroot
gxcmcc:gxcmcc
patrol:patrol
sudouser:sudouser
patrol:patrol
sudoroot:sudoroot
test:test
siteview:siteview
simsp:simsp
nftrans:nftrans
nftrans:nftrans
sudouser:sudouser
patrol:patrol
sudoroot:sudoroot
patrol:patrol
simsp:simsp
```

账号与口令一对多

```
abrt
acct
acct1
acct2
acctrt
adm
admin
admin_bonc
admin_ykc143
admincuijia
administrato
administrator
adminoa_52
adminroot
adminstrator
adminweb
ais
aix
ajaxterm
```

```
%null%
%username%
%username%123
%username%1234
sa
123
1234
12345
123456
1234567
12345678
654321
54321
111
1314521
1314520
000000
00000000
11111111
88888888
```

2.1

字典库优化与维护

a. 字典库使用测试

b. 实际场景中使用的调整

c. 字典库迭代维护

字典库优化与维护 – 字典库使用测试

测试环境

- 由于字典库为顺序遍历，可设置测试环境存在字典库部分弱口令的同时，将字典库最后一组弱口令设置，以验证字典库是否能正常遍历完整，**测试字典遍历时间。**

测试目标

- 在适当的评估时间内，能够正常遍历完整所有账号口令组合，并发现设置好的弱口令组合。

字典库优化与维护 – 实际场景中使用的调整

根据当次扫描对象（系统/部门）、时间限制，需要对当次扫描的字典库进行调整。

字典拆分

- 默认口令字典库
- 多个特定字典库（分批扫描以缩短单任务时间）

形式变化

- 由于实际场景的调整，不同账号的重复弱口令情况增加，可适当调整为账号与口令一对多的形式进行检查
- 当次扫描的环境单一，涉及的人员、应用较少，可能的口令组合较少，可筛选调整为账号与口令一对一的形式

CONTENTS 目 录

02

怎么做 弱口令扫描

1. 扫描前计划准备
2. 按计划实施扫描
3. 扫描后收尾总结

NSFOCUS

弱口令扫描概述 – 弱口令存在的场景

协议

- RDP、SSH、Telnet、FTP等

应用

- 各类操作系统、数据库、Web应用系统等

设备

- 服务器主机、路由器、交换机、网络打印机等

弱口令扫描概述 – 常见弱口令扫描产品

- 绿盟科技远程安全评估系统 – 口令猜测模块
- Hscan
- John the ripper
- 其他各类工具

弱口令扫描 – 工作流程

计划准备 → 扫描实施 → 收尾确认 → 报告分析

- 沟通及技术交流
- 确认目标及口令策略
- 工具及环境准备
- 扫描方案确认及获取授权

- 扫描方式、策略及字典库确认
- 扫描换季及网络配置
- 扫描目标的口令策略配置
- 扫描任务下发

- 异常任务排查
- 导出报告
- 收尾工作

2.1

扫描前计划准备

a. 沟通及技术交流
b. 确认目标及口令策略
c. 工具及环境准备
d. 扫描方案确认及获取授权
e. 常见问题及风险规避

扫描前计划准备 – 沟通及技术交流

01

技术、原理沟通

- 沟通扫描原理
- 确定扫描范围
- **不一定能发现所有“弱”口令**
- **应与基线配置、双因素认证等手段互补以保障可能的弱口令造成的影响**

02

客观风险的提示与告知

- 如占用部分带宽
- 会产生大量登录日志
- **口令猜测策略有锁定风险**
- **正在使用的账号有可能受影响**

03

沟通弱口令扫描的必要条件

- 如网络环境
- 接入点
- 配合人员
- 口令策略配置等

04

沟通交付的成果

- 如扫描报告的要求等

扫描前计划准备 – 确认目标及口令策略

明确扫描范围，收集目标系统资产信息

IP地址、承载的应用、开放的服务端口等

收集安全防护产品配备情况

当前已使用的防火墙、安全产品及使用情况，策略情况等，
以方便确认是否存在阻断口令猜测的情况

确认口令配置策略

哪些协议或应用已配置多次猜测锁定策略。

其他信息

业务系统的重要程度、业务繁忙时期等（重要资产夜间扫描），
是否可以长时间挂扫。

NSFOCUS

扫描前计划准备 – 工具及环境准备

扫描设备准备

- 确定弱口令扫描工具
- 证书有效、设备/工具正常使用
- **导入使用本次扫描的字典库**

目标网络接入环境准备

- 确定网络接入的方式和位置，以及电源的接入情况
- 提供弱口令扫描目标网段的空闲IP地址、网络掩码、网关等配置信息；
- **收集接入网络安全防护产品部署情况、口令锁定策略配置情况；**

扫描时间、地点和人员

- 扫描时间（夜间、下班时间、业务不繁忙期以及其他时间）
- 是否可长时间挂扫
- 进入机房流程等
- 机房配合人员、业务系统配合人员等

扫描前计划准备 – 扫描方案确认及获取授权

- **确定扫描方案，护网期间建议与护网方案结合，提前完成沟通准备**
- **在弱口令扫描实施之前，制定单项扫描计划，通过邮件与安全接口人及系统负责人确认扫描时间，并获取相关的授权或审批**
  - 建议通过邮件或者线上申请相关操作流程，避免口头、电话沟通；
  - **若涉及收集密码文件的，还需进行文件收集申请。**

扫描前计划准备 – 常见问题及风险规避

资产收集

- 基础资产表：资产属性一般包括：所属于系统、IP地址、承载业务、映射前地址、映射后地址、浮动IP、所属部门、责任人、联系方式、已安装的应用、开放的服务端口、是否配置账号锁定策略等。
- 信息资产，禁止未授权分发，外泄。

扫描申请与授权

- 禁止对他人的资产或非授权的服务、应用、IP进行扫描操作
- **禁止在非计划时间内，不告知客户进行任何扫描操作**

2.2

按计划实施扫描

a. 扫描方式、策略及字典库确认

b. 扫描环境、网络配置

c. 扫描目标的口令策略配置

d. 扫描任务下发

e. 常见扫描工具操作

按计划实施扫描 – 扫描方式、策略及字典库确认

扫描方式及策略

- 本次扫描为使用字典库进行远程暴力猜解扫描，或为对密码文件进行破解扫描；
- 本次扫描需设定的扫描超时时间（**参考字典库前期测试遍历时间**）。

字典库

- 根据本次评估范围的资产，导入适当字典库作为本次扫描使用，可按系统或部门选用。
- 字典库可包括通用弱口令字典库及针对评估环境的特定弱口令字典库。

按计划实施扫描 –扫描环境及网络配置

扫描环境

- 扫描其间，维护人员全程配合观察业务系统运行状态；
- 涉及机房操作的，针对网线插拔、开关机柜等操作，由配合人员完成；
- 遵守客户场地要求：如机房严谨吸烟、吃东西、需要穿戴鞋套等要求；
- **佩戴通行证，**不要出入非授权场所。

网络配置

- 扫描器接入前需确认扫描口IP地址配置，避免发生IP地址冲突问题；
- 如网络不通，需要进行扫描设备故障排查、和网络环境故障排查（配合人员负责网络故障的排查）。

按计划实施扫描 – 扫描目标的口令策略配置

口令策略确认及配置

- 与管理员确认哪些应用或协议中，已开启了多次猜测失败则锁定的配置，在资产表中标记
- 确认标记中的目标资产是否可以进行弱口令扫描
- 在扫描器将口令锁定策略临时关闭

按计划实施扫描 – 扫描任务下发

扫描任务下发

- 任务开始前，可通过扫1-2个地址，进行网络承载、路由通路等测试；
- 每个扫描任务IP地址不宜太多，建议分批扫描（防止设备卡死、扫描中断等意外情况）；
- 扫描的资产应以业务系统为单位，当无法确认业务系统时，应以部门单位进行扫描，方便历史数据统计分析；切勿一个扫描任务涵盖多个部门的资产。
- **同一个扫描任务中，需确认是否所以资产可进行同类协议的弱口令扫描，如不同则需分开任务进行。**
- 扫描任务命名时明确部门、系统等关键信息，例如【部门名称+系统名称+任务类型+其他】，能够有效的区分不同的扫描任务 。
- 扫描其间，配合人员需要全程关注业务运行情况，观察是否出现异常；
- 在扫描其间一旦出现系统瘫痪、宕机等情况，根据提前准备的应急预案，立即配合进行处置和恢复。并根据现场情况决定业务恢复后是否还继续进行扫描任务。

按计划实施扫描 – 常见扫描工具操作

操作演示

- RSAS – 口令猜测模块
- Hscan
- John the ripper

2.3

扫描后收尾确认

a. 异常任务排查

b. 导出报告实操

c. 收尾工作

扫描后收尾确认 – 异常任务排查

异常现象

- 扫描任务失败
- 扫描资产减少
- 扫描进度长期停滞

发生原因

- 网络不可达或网络波动
- 有安全防护设备或配置安全策略
- 扫描超时时间设置过长

处置措施

- 排查网路环境故障
- 确认目标资产防护情况
- 重新配置扫描任务

扫描后收尾确认 – 导出报告实操

报告导出

- RSAS – 口令猜测模块
- Hscan
- John the ripper

结果验证

- 抽查结果报告中发现的弱口令，进行远程访问、登录验证

扫描后收尾确认 – 收尾工作

扫描收尾工作

- 配合人员对系统运行状态、业务运行状态进行确认，如有异常按照应急措施进行处置；
- 扫描人员关闭扫描器，断开网线；
- 恢复评估前取消的口令锁定策略，确认启用生效；
- 经确认无误后扫描人员离场。

FAQ

谢谢！

NSFOCUS