IT 系统多功能批量密码修改工具①

吕荣峰, 唐 军, 余 虹

(中国联合网络通信有限公司 重庆市分公司, 重庆 400042)

摘 要: IT 系统多功能批量密码修改工具利用 bat、vbs 和 scurecrt script 语言, 结合相关操作系统命令实现对主流 linux、unix 操作系统和网络设备密码的自动批量修改, 解决了 IT 系统密码修改及验证耗时、耗力和耗神的问题, 为保证 IT 系统各种帐号密码的长度和密码修改的频度, 提升 IT 系统的安全度提供了一个良好的工具. 测试和实际应用表明, 该工具的综合效率是普通手动修改密码的 10 倍以上, 且具有很高的可靠性.

关键词: IT 系统; 多功能; 批量; 密码修改; 工具

Multi-Function Batch Password-Changing Tool for IT System

LV Rong-Feng, TANG Jun, YU Hong

(Chongqing Branch, China United Network Communications Co. Ltd, Chongqing 400042, China)

Abstract: The multi-function batch password-changing tool for IT system uses BAT, VBS, scurecrt script and combination with command of operating system and network devices. It realizes function of automatically batch changing password of mainstream Linux, UNIX operating system and network device. It solves the difficulty that changing password of IT system is very hard, tedious and time-consuming. It provides a good tools to ensure the frequency changing IT system password and the password length so as to enhance the security of IT system. The test and practical application indicate that the comprehensive efficiency of the tool is more than 10 times of manually changing and verifying password, and it has high reliability.

Key words: IT system; muti-function; batch; password-changing; tool

网络黑客通过 Metasploit 等工具对 IT 系统构成越来越大的威胁[1]. 随着计算设备性能不断提高, 彩虹表解密算法日益发展[2], 密码安全作为计算机安全重要组成部分, 也面临着严重威胁[3]. 一般而言, 安全的密码必须要有一定的长度和复杂度[4,5]; 按照 IT 系统安全基线要求, 在符合密码复杂度条件下, 普通帐号密码长度要在 8 位以上, 超级帐号密码在 12 位以上, 并进行定期修改[6]. 但 IT 系统具有系统大、设备多和帐号多等特点, 密码修改是一件既枯燥又非常耗时费神的工作. 在CNKI 数据库和 Elsevier SDOL 数据库中, 作者没有发现可以解决 IT 系统密码修改劳动强度高和时间长的文章和方法. 因此为减少密码修改的时间, 减轻 IT 系统密码修改的劳动强度, 开发一种可以自动、安全、可靠的 IT 系统自动批量密码修改工具, 缩短密码修改时间和减轻密码修改的劳动强度, 从而达到提升保证 IT 系统密码修改频度, 提高系统安全的目的, 显得非常必要. 由于采用命令行对 linux 和 Unix 操作系统[7], 华为类和 cisco 类网络设备进行密码修改时, 都会根据不同情况返回相关的信息; 这就可以利用这些信息, 编写工具使其与 IT 设备进行自动交互, 从而能够实现密码自动批量化修改目的.

1 IT系统多功能批量密码修改工具设计概要

IT 系统多功能批量密码修改工具(以下也简称“工具”)设计思想是, 在安全的内网维护网络, 以 windows 操作系统和 securecrt7.0 为运行环境, 使用 bat、vbs 和 securecrt script 语言编写代码, 实现通过读取指定的密码修改配置文件、自动进行参数分解、设备登录、帐

① 收稿时间:2014-04-23;收到修改稿时间:2014-06-06

号切换、并模拟多种操作系统和网络设备密码修改过程完成密码修改和相关帐号新密码的验证; 达到取消手工输入, 使工具通过 securecrt 和进行密码修改设备的自动化交互处理, 完成相关帐号密码修改和新密码的验证等相关工作, 使密码修改和验证的时间仅取决于设备的反应时间和数据在网络上的传输时间, 从而大大减少密码修改时间和降低密码修改劳动强度的目的.

为保证工具的可靠性, 工具在密码修改前完成所有密码修改设备自动登录、获取超级权限并保持会话链接, 从而在密码修改失败时, 进行补救; 同时, 工具记录整个密码修改过程中各个设备帐号密码修改的各种情况, 以便于复核和检查; 在密码修改全部完成后, 工具能自动完成所有设备登录和使用超级帐号密码切换到超级帐号界面并保持会话链接, 以对相关设备登录帐号和超级帐号密码进行再一次确认.

需要说明的是: 为保证密码安全, 在密码修改完成后, 应立即彻底删除相关日志文件,加密并安全地保存相关配置文件或删除配置文件重要信息.

2 工具的实现方法和流程

工具利用 securecrt 对 suse 类、solaris、redhat、aix 类等主流操作系统和 F5、华为类、cisco 类主流网络设备进行密码自动批量修改, 对 linux、unix 操作系统提供 ssh2 登录方式, 对 aix 操作系统也提供 telnet 登录方式, 为网络设备提供 telnet、ssh1 和 ssh2 三种登录方式.

2.1 工具主要流程

工具主要有以下模块: 自动登录和会话保持模块, 密码修改配置文件读取模块, 批量密码修改模块, 登录帐号和超级帐号密码验证模块.

工具在初始化后进入自动登录和会话保持模块, 该模块在读取密码修改配置文件登录部分参数并分解后, 执行 bat 命令来完成调用自动登录工具在新的 securecrt 窗口完成所有修改密码设备的自动登录, 并获取超级帐号权限, 执行相关指令进行会话保持, 保证密码修改失败时, 能及时补救.

设备自动登录完成后并获得确认后, 和用户交互进行修改密码状态设置; 用户选择不可控状态, 状态标志位设为 0, 设备的登录和帐号密码的修改均由工具自动完成, 只在出现设备不能登录、帐号不存在, 相关帐号密码不正确等异常情况下, 才需要用户介入. 用户选择可控状态, 设备标志位设为 1, 在设备登录期间, 工具将操作系统类型或网络设备类型、IP 地址、ssh 登录时的端口号、登录帐号、登录帐号密码、超级帐号密码(aix 不获取超级帐号)等数据参数显示在 securecrt 窗口界面上; 密码修改期间, 在每一个帐号进行密码修改前, 会提示密码修改帐号和相应的新旧密码信息, 并由用户决定是否继续密码修改.

在完成密码修改状态设置后, 进入密码修改配置文件读取模块, 自动读取指定的密码修改配置文件并完成参数分解.

在完成参数分解后, 进入批量密码修改模块, 进行设备登陆、帐号切换和密码修改. 在此期间, 工具获取各种设备登录、密码修改、网络设备配置文件保存等情况的关键词、从而判断当前设备是否正常登录和当前密码是否修改成功并采取相应的措施, 并在登录失败时, 提示用户重新输入帐号和密码、并将相关获取的帐号和密码参数显示在界面上, 方便用户检查和修改; 密码修改期间在出现异常情况时(如帐号名或旧密码错误、密码修改不成功、和工具未设置的情况等), 进行异常情况处理, 工具将根据情况进行人机交互, 密码修改者根据提示, 手动输入帐号、密码、相关命令, 再由工具保存后发送到当前设备并完成后续的诸如的登录、帐号切换、密码修改和配置文件保存等工作.

在完成一个设备所有帐号的密码修改后, 工具自动完成设定帐号的新密码验证, 获取用户 id.

在完成所有设备密码修改后, 工具的密码登录帐号和超级帐号验证模块将根据登录帐号和超级帐号密码是否修改, 自动使用新密码或原密码进行登录、获取超级帐号权限并发送相关命令进行会话保持, 以进一步验证登录帐号和超级帐号密码是否正确; 在密码修改过程中, 工具记录各个设备帐号密码修改的各种情况, 并将相关情况复制到一个统一的文件, 以便于密码修改失败时进行比对和检查. 工具的基本流程图如图 1.

2.2 密码修改配置文件样式

密码修改配置文件参数用逗号隔开, 并按照规定的位置排列, 内容包括: 操作系统名称或网络设备操作系统类型号、登录的 IP 地址、ssh 登录时的端口号、登录帐号, 登录帐号密码、超级帐号密码、登录方式(telnet、ssh1、ssh2)、修改密码的帐号、相应帐号的新密码, 行连接符(用“_”表示, 表示本行相关数据为上一行参数的延续), 当前设备参数数据结束符(用“&_”

表示); 此外, aix 操作系统还有修改帐号的旧密码, 华为类网络设备有密码修改方式、cisco 防火墙 telnet 方式有 password 密码. 如果配置文件相邻设备的相同位置参数相同, 可以使用“-”表示, 以简化配置文件, 并减少编辑和检查文件时间.

工具在读取配置文件时, 使用正则表达式自动过滤首字母为“#”的注释行, 空白行和密码修改数据的空白参数; 并过滤各个参数左右两边的空格.

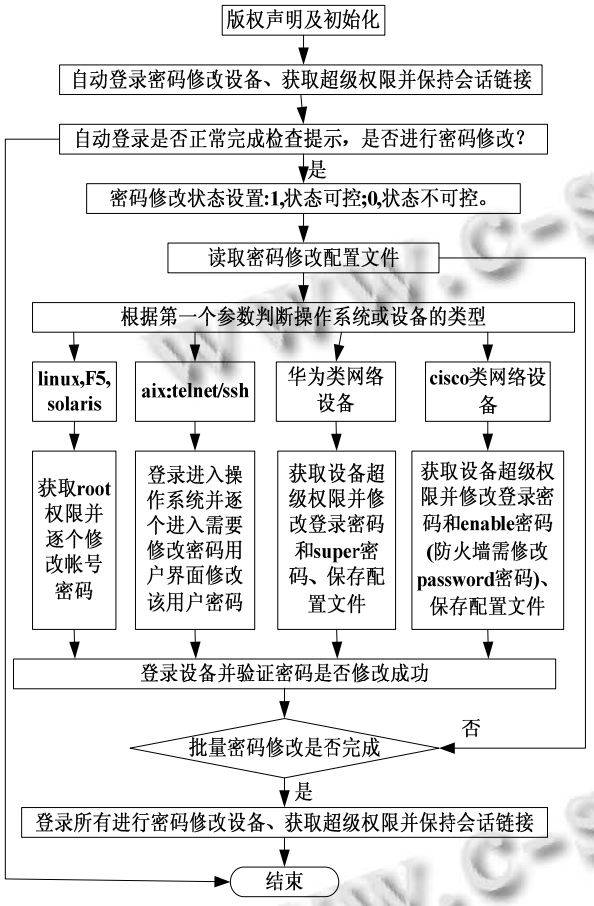

图 1 IT 系统多功能自动批量密码修改工具基本流程图

2.3 aix 操作系统密码修改流程

aix 操作系统由于在 root 帐号修改其它帐号的密码后, 在帐号下一次成功登录后, 会要求该帐号立即修改密码; 故有效修改帐号密码的方式是: 在相应帐号权限 shell 下修改其密码[8]. 而 aix 操作系统除 root 帐号外, 所有其它帐号在修改密码时, 都需进行以前的密码验证. 故 aix 操作系统密码修改相对比较复杂, 该节以 aix 操作系统为例简要说明操作系统和网络设备的密码修改流程.

一个 aix 操作系统设备密码修改基本流程为: 数据读取和处理、设备登录、shell 英语语言环境设置, 密码修改可控状态设置、帐号是否为 root 帐号判定、帐号切换、密码修改、设备所有修改密码帐号的新密码验证.

当前设备密码修改完成后, 重新登录设备, 进行当前设备所有帐号新密码的验证, 并获取帐号 ID; 相关基本流程图如图 2, 对单个 aix5.3 操作系统采用 ssh2 登录后进行密码修改状况如图 3, 帐号新密码验证如图 4.

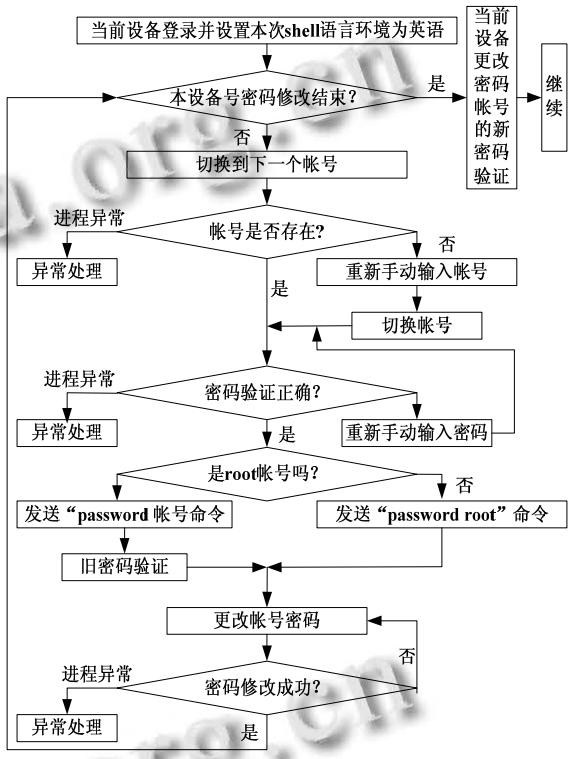

图 2 aix 操作系统密码修改流程图

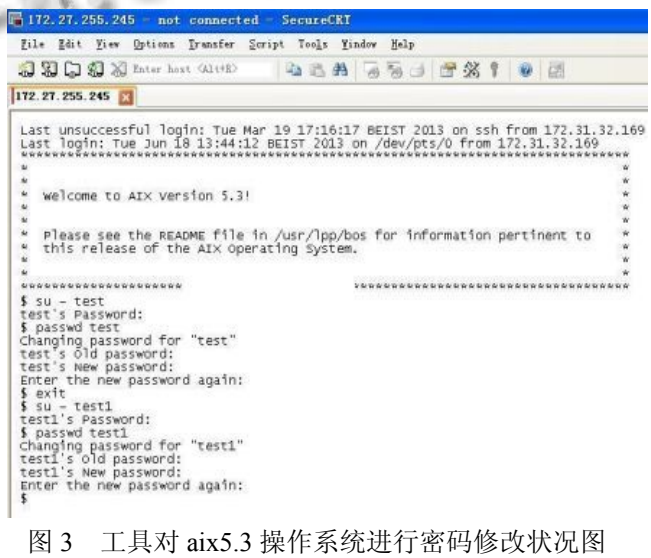

图 3 工具对 aix5.3 操作系统进行密码修改状况图

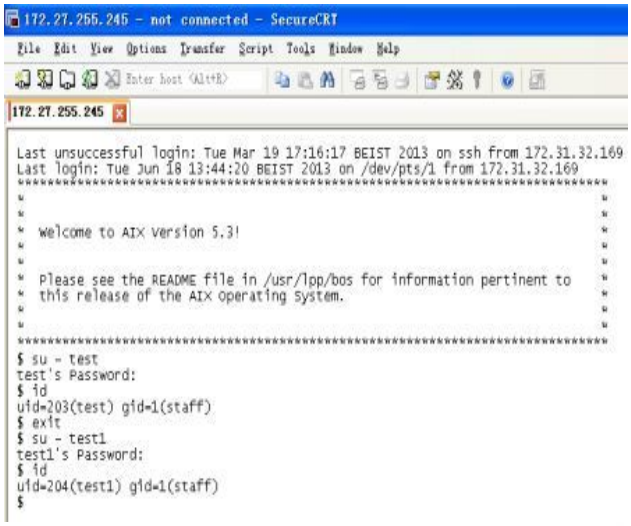

图 4　工具在 aix.3 操作系统帐号新密码验证状况图

其它操作系统和负载均衡器 F5 与 aix 操作系统密码修改方法相似. 只是其它系统采用 root 权限修改密码, 各个操作系统关键词也不一样, 故个别地方的处理有些差别.

网络类设备密码修改方法与操作系统密码修改方法类似; 华为类网络设备根据密码修改是否需要进入 aaa 视图和保存配置文件方式不同分为 aaa、S85 和 S35 方式; aaa 方式为采用 aaa 方式进行登录帐号密码修改的防火墙、路由器和交换机, S85 方式针对类似于 S8500 交换机密码修改和配置文件保存方式的交换机, S35 方式针对类似于 S3500 交换机密码修改和配置文件保存方式的交换机. cisco 类网络设备采用命令行方式进行密码修改[9], 其防火墙 ios 6.3 以下版本可以修改登录密码, 也可以不修改登录帐号密码, 但 enable 密码必须进行修改.

3　工具实现的功能和效果

工具能够根据密码修改配置文件提供的数据, 自动批量完成 suse 类、redhat 类、solaris、aix 操作系统、华为类、cisco 类网络设备和负载均衡器 F5 给定帐号的密码修改及密码验证功能, 并能对异常情况进行相关处理; 密码修改期间进行全程日志记录, 并将整个密码修改过程写入指定文件中, 方便密码修改失败时进行检查和比对. 正常情况下的密码修改过程, 不需要进行手工干预, 从而在大大减少了密码修改时间的同时也极大地减轻了密码修改的劳动强度. 表 1 为一次工具和手工修改密码在测试条件下和一次实际 IT 系统利用工具和手工进行密码修改所用时间的比较表:

表 1　工具效率表

对比场景[1]	手工修改及验证密码时间[2]	工具修改及验证密码时间[3]	工具修改密码时配置文件编辑时间[4]	效率比[5]
工具测试[6]	8 分 22 秒	4 秒	27 秒	6.2
实际 IT 系统[7]	171 分 15 秒	1 分 25 秒	8 分 12 秒	15.4

注 1. 在测试过程中, 设置相关异常情况进行测试, 对一次帐号或旧密码错误的异常处理, 采用复制粘贴正确的帐号或密码的方法处理时间在 5 秒左右; 而对一次密码修改不成功, 根据采用手动输入命令, 再负载粘贴复制帐号或密码的方法, 处理时间在 20 秒内; 对工具未设置的状况, 点击 “忽略”按钮(情况正常), 处理时间在 2 秒左右, 点击继续“继续”按钮, 根据提示手动输入命令及相关操作, 处理时间在 20 秒内; 如果点击“放弃”按钮, 重新检查和修正配置文件, 然后重新执行剩余操作, 处理时间在在 2 分钟以内. 但在工具所有编码及调测修正后的正常测试和实际使用过程中, 在密码修改配置文件正确和系统运行正常情况下, 工具没有产生过异常处理情况.

注 2. 手工进行设备登录和密码及验证, 密码修改时, 事先先写好密码, 采用需要时进行复制和粘贴密码.

注 3. 工具采用不可控状态进行密码修改, 采用可控状态时, 设备登录和密码修改时将显示相关参数(由用户进行相关检查, 用户确定后自动完成相关登录和密码修改流程, 用户此时可以选择中断密码修改进程), 每次时间在 4 秒以下.

注 4. 配置文件为上次密码保存的密码修改配置文件, 经解密后复制并修改后, 进行 2 到 3 次检查的时间.

注 5. 效率比= 手工修改及验证密码时间/(配置文件编辑时间+工具修改和密码验证时间).

注 6. 工具测试条件为 2 台 aix 操作系统设备; 每台 2 个帐号: test, test1, 密码为 18 位.

注 7. 实际系统条件为 13 台主机; 包括登录帐号、业务帐号和 root 帐号共 79 个帐号; 2 台 F5 负载均衡器

4 个帐号; 2 台华为交换机, 2 台华为防火墙, 共 8 个帐号; 密码长度均大于 15 位.

对工具的几十次测试和几十次实际应用也表明, 正常情况下, 工具对一个帐号密码修改及验证(包括帐号自动切换)时间小于 0.5 秒, 密码修改和验证过程的效率是手动修改和验证 15 位长度以上密码的 60 倍以上, 而且密码越长, 效率越高; 由于工具需要建立密码修改配置文件及有的 IT 系统帐号的密码长度可能小于 16 位和网络设备配置文件的保存等因素, 工具的综合效率是手工修改密码的 10 倍以上.

4 结语

IT 系统多功能自动批量密码修改工具采用 bat、vbs 和 scurecrt script 语言, 利用相关操作系统及网络设备命令成功实现了对 suse 类、solaris、redhat 类、aix 等操作系统、负载均衡器 F5、华为类网络设备和 cisco 类网络设备密码的自动修改. 在测试和实际的应用中, 工具的综合效率是手工进行密码修改的 10 倍以上; 同时在工具进行密码修改过程中, 一般不需要手工介入或手工介入过程简单、时间短, 因而极大地减轻了密码修改的劳动强度; 工具在实际应用中体现了很好的实用价值. 工具采用的帐号新密码验证和密码修改全程的日志留存机制, 以及所有设备在密码修改前, 在另外一个窗口登录和获取超级用户权限并进行会话保持, 使得密码修改万一失败, 可以及时补救, 从而保证了密码修改的高可靠性. 这在通信系统 IP 化、IT 化大背景下, 为安全和自动化运维[10]提供一个良好的工具.

参考文献:

1 严俊龙.基于框架自动化渗透测试研究.信息网络安全,2013,(2):69–72.
2 王小鉴,廖晓峰,黄宏宇.基于归约函数数量裁减的彩虹表技术改进.计算机工程,2013,(7):162–166,170.
3 Sean Convery 著,田果,刘丹宁译.网络安全体系结构.北京:人民邮电出版社,2013:665–667.
4 李匀.网络渗透测试—保护网络安全技术、工具和过程.北京:电子工业出版社,2007:274.
5 雷静,张博,郑宝昆.linux 操作系统密码安全问题解析.计算机光盘与应用,2012,(18):160,162.
6 郝永清.堡垒主机搭建全攻略与流行黑客攻击技术深度分析.北京:科学出版社,2010,(1):210–227.
7 张勤,鲜学丰.Linux 从初学到精通.,北京:电子工业出版社,2011:150.
8 文平.AIX UNIX 系统管理、维护与高可用集群建设.北京:机械工业出版社,2011:109.
9 刘晓辉.网络设备规划、配置与管理大全(cisco).北京:电子工业出版社,2012:110–122.
10 梁春丽.IT 运维管理自动化是关键.金融科技时代,2012,(2):39–43.