

**计算机学院实验报告册**

2023 至 2024 学年 第 一 学期

**课 程**  网络安全技术

**专 业** 信息安全

**班 级** 信安211

**学 号** 211346020

**姓 名** 彭明尧

**指导教师** 葛兴

**实 验 室** S408

计算机学院制

二〇二二年

实 验 须 知

1．进入实验室，应保持安静和整洁。

2．课前应认真预习本次实验内容及有关仪器设备介绍，基本了解实验基本原理，明确实验要求。

3．认真听取指导教师对仪器及设备的构造、基本原理、实验要求、注意事项等的讲解。

4．爱护仪器设备，细心操作，注意安全。实验中如发生意外或异常现象，应立即向指导教师报告。

5．实验结束后，应将所用的仪器及设备恢复为初始状态，收拾好桌凳，做好清洁工作。

6．实验报告是处理实验结果的总结资料，是考核学生实验成绩的主要依据之一，必须认真独立完成。课后一周内送交指导教师批阅，实验成绩按百分制计。

7．学生应规范填写实验报告，由实验指导教师给出填写样本。

8．本实验册应妥善保管，课程实验结束后应交回实验室。

|  |  |  |  |
| --- | --- | --- | --- |
| **实验题目** | Linux标识和鉴别实验 | |  |
| **实验目的** | 掌握用户账户安全设置方法;掌握账户锁定策略、账户注销策略的设置方法 | | |
| **说明及要求** | 主流配置计算机一台,安装 Ubuntu14.04。 | | |
| **实验内容**  1.清除多余账户  账户是黑客入侵系统的突破口,系统的账户越多,黑客们得到合法用户权限的可能性一般也就越大。我们需要定期查看账户、口令文件,与系统管理员确认后删除一些不必要的账户,删除用户的命令为 userdel,利用该命令删除 sync,news uucp、games 等账户,这些账户为系统默认创建但很少使用的账户。  2.清除多余的组  同样,应该删除系统安装时默认创建但很少使用的组账号,如 admdip 等以减少系统受攻击的风险,删除组用命令 groupdel。  3.锁定账户登录  如果某些账户一段时间内不用,为了防止被恶意用户利用,可以锁定这些账户以禁止其登录,在需要时可以解锁。锁定账户的命令为 passwd -1<用户名>;解锁账户的命令为passwd -u<用户名>,可以用 passwd-S 查看用户状态。  4.禁用root 之外的超级用户执行命令:#cat /etc/passwd检查账户文件中的用户 ID,若用户 ID=0,则表示该用户拥有超级用户权限,禁用除root 之外的超级用户。  5.保护root 账户的安全策略  由于 root 账户具有最高权限,一旦被攻击者获取 root 权限,将对系统造成巨大的危害，用户需要具备以下对 root 账户的保护意识  (1)除非必要，避免以超级用户登录;  (2)严格限制root 只能在某一终端登录,远程用户可以使用/bin/su-l来成为 root;(3)不要随意把 root shell 留在终端;  (4)若某人确实需要以 root 来运行命令，则考虑使用 sudo 命令临时以 root 身份来运行命令;  (5)不要把当前目录(“./”)和普通用户的 bin 目录放在 root 账户的环境变量 PATH中;(6)不以 root 运行其他用户或来源不明的程序。  6.用户口令策略的设置为了防范字典攻击和暴力破解,用户应该设置强口令,为了强制用户设置安全口令.Linux系统提供了类似 Windows 的密码策略,在配置文件/etc/login,defs 中进行设置，如图所示，口令策略涉及如下参数:  (1) PASS MAX DAYS 99999  (2) PASS MIN DAYS O  (3) PASS MIN LEN 5  (4) PASS WARN AGE 7  ##密码设置最长有效期(默认值);  ##密码设置最短有效期;  ##设置密码最小长度;  ## 提前多少天警告用户密码即将过期。  e33cdfefa642e437b33b701905d3ebd  7.修改自动注销账号时间  在 Linux系统中 root 账户具有最高特权,如果系统管理员在离开系统之前忘记注销root 账户,将会带来很大的安全隐患,安全起见,应该让系统自动注销用户。通过修改账户中 TIMOUT 参数,可以实现此功能,编辑你的 profile 文件/etc/profile 后加人下面这行:  export TIMEOUT =300  300 表示300 秒,也就是表示5分钟,如图所示。这样,如果系统中登录的用户在 5 分钟内都没有动作,那么系统会自动注销这个账户。  1f3a1ef4f0e74c7df298d3ccdb4badb  8.设置账户登录失败锁定次数、锁定时间  在 Ubuntu 14.04 中账户登录失败锁定的次数也是在配置文件/etc/login.defs 中设置,如图所示,但是如果系统启用 PAM 登录机制的话,相应的锁定策略由 PAM 机制设置。  而在 Redhat 等版本的 Linux 中,可以编辑文件/etc/pam,d/system-auth,设置 authrequired pam\_tally.so 为需要的策略:  auth required pam tally. so onerr = fail deny = 6 unlock time = 300  设置密码连续错误 6 次锁定账户，且锁定时间为 300 秒。  984ca7774ad3555e9c2a01af334afe4 | | | |
| **年 月 日** | | | |
| **实验小结**  **（心得体会）** | |  | |
| **成绩及评语** | |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **实验题目** | Linux 访问控制实验 | |  |
| **实验目的** | 掌握自主访问控制的概念;掌握文件和目录自主访问控制的设置。 | | |
| **说明及要求** | 主流配置计算机,安装 Ubuntu14.04。 | | |
| **实验内容**  1。利用 Linux自主访问控制机制实现用户授权   1. 以 root 创建用户 linda 和 lucy,并分别为两个用户设置密码,如图所示   ba8b8294fce0b6a97f8b3fa089b2ecc   1. 用户 linda 用 touch 命令创建文件 helloworld,查看 helloworld 的文件权限，测试用户 lucy 能否写,可以看到文件写入失败,请求被拒绝,如图所示。   476965c1b0e52aaee272e88d9eb1b8c   1. 用户 linda 用 chmod 命令修改文件 helloworld 的权限，使得 lucy 能写文件,如图所示。   c07adbff019bea5ab1b8f78953b170c  3.目录文件的访问权限控制  (1)用户 linda在/tmp 目录下创建目录/tmp/data,查看目录权限,可以看到用户ucy对于目录/tmp/data 拥有读和执行的权限。在新建目录下用 touch helloworld 创建文件,切换当前用户为 lucy,由于拥有对 data 目录的读权限,因而可以利用 Is 列出目录tmp/data 的内容。由于具有对 data 目录的执行权限,因而利用 cd 进入目录,但由于不具有对目录的写权限,所以不能在该目录下创建文件 worldhello,如图所示。  54462062eea67d753cd319a4341e984   1. 用户 linda 修改用户对目录/tmp/data 的权限,依次去掉其他用户对目录的读权限和执行权限,验证 luy 是否能执行 ls 和 cd 操作,由此可见对于目录的读权限对应的是列出目录下内容的权限,目录的执行权限是进入目录的权限,如图所示。   0ac3fb3205b8f1baf135bef3fb0673e  (3)用户 linda 修改用户对目录/tmp/data 的权限,使其他用户具有对目录的读写和执行权限，并验证，如图所示。  8b8d26ff3e5bf8e0e942e799cbb2079 | | | |
| **年 月 日** | | | |
| **实验小结**  **（心得体会）** | |  | |
| **成绩及评语** | |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **实验题目** | Linux特殊权限实验 | |  |
| **实验目的** | 掌握 Linux中SUIDSGIDSticky 3种特殊权限的含义和配置方法 | | |
| **说明及要求** | 主流配置计算机一台，安装 Ubuntu14.04 | | |
| **实验内容**  1.SUID特殊权限  1)查找系统中所有设置了 SUID 权限位的可执行文件Linux中有一类具有特殊权限的可执行文件,当执行该类文件时会使普通用户的权限得到提升,给系统带来很大的安全隐患,这样的特殊权限是通过给可执行文件设置SUID位(有时简称s位)来实现的。  find path-perm 用于根据文件权限在指定路径下查找文件,有 3种形式(1) find path -perm mode;  (2) find path -perm -mode;  (3) find path -perm +mode。  其中find path-permmode 表示严格匹配也即文件权限必须跟mode完全一致才能匹配成功;find path -perm-mode表示文件权限包含 mode 权限的文件都能匹配成功;ind path-perm +mode表示文件权限被 mode权限包含的文件都能匹配成功。在5.12节中介绍过用户的普通权限可以表示成3 位十进制数值型,分别表示属主司组用户和其他用户的权限,而对于特殊权限 SUID、SGID、Sticky,也可以表示成十进制直,其中4 表示SUID2表示 SGID1代表Sticky 权限值,这里我们查找的是设置了SUID位的所有程序,可以通过用find /-perm -4000命令找到所有具有s位权限的文件2)关闭/usr/bin/gpasswd的s 位权限利用 chmod命令可以关闭可执行文件的 s 位权限。  2Sticky 特殊权限  如果多个用户对同一目录具有写权限,则一个用户可以删除另一个用户创建的文件.给系统带来安全隐患。如果在目录上设置 Sticky 特殊权限,则可以防止一个用户删除另一个用户创建的文件,而只有文件或目录的属主可以删除该文件。   1. root 用户创建目录/tmp/bookstore,查看目录权限,可以看到在默认情况下目录对非同组的其他用户只有读和执行的权限,因而其他用户无法在该目录下新建文件或子目录,通过指令“chmod 777”修改新建目录的权限,使得所有用户都具有所有权限。以linda 用户的身份登录系统,进入/tmp/bookstore 目录后创建文件 helloworld,切换 lucy用户,可以看到 lucy 可以删除 linda 创建的文件,存在安全隐患,如图所示。   d400a886f0ef7467b277aa1a61f29b0   1. root 用户利用 chmod 1777 命令或 chmod o+s 命令设置/tmp/bookstore目录的Sticky 权限,用户linda 再次在该目录下创建 helloworld 文件,可以发现lucy 无法删除该文件,如图所示。   b76b014bba9779147c2035cb184934d | | | |
| **年 月 日** | | | |
| **实验小结**  **（心得体会）** | |  | |
| **成绩及评语** | |  | |