02_系统安全实验报告

《信息安全综合实践》实验报告

系统安全

一、实验目的

1. 了解操作系统的用户认证、安全审计等安全机制；
2. 熟悉linux系统及其基本操作命令；
3. 了解linux用户管理和安全策略设置方法；
4. 了解一些基本的攻击工具、攻击方法。

二、实验内容

序	内容	实验结果
1)	Windows用户口令破解	- [ ] 失败 - [√] 成功
2)	linux用户管理	- [ ] 失败 - [√] 成功
3)	linux用户口令策略设置（选做）	- [ ] 未做 - [ ] 失败 - [√] 成功
4)	Apparmor访问控制策略	- [ ] 失败 - [√] 成功
5)	Linux日志查看（选做）	- [] 未做 - [ ] 失败 - [√] 成功

三、分析和思考（90分）

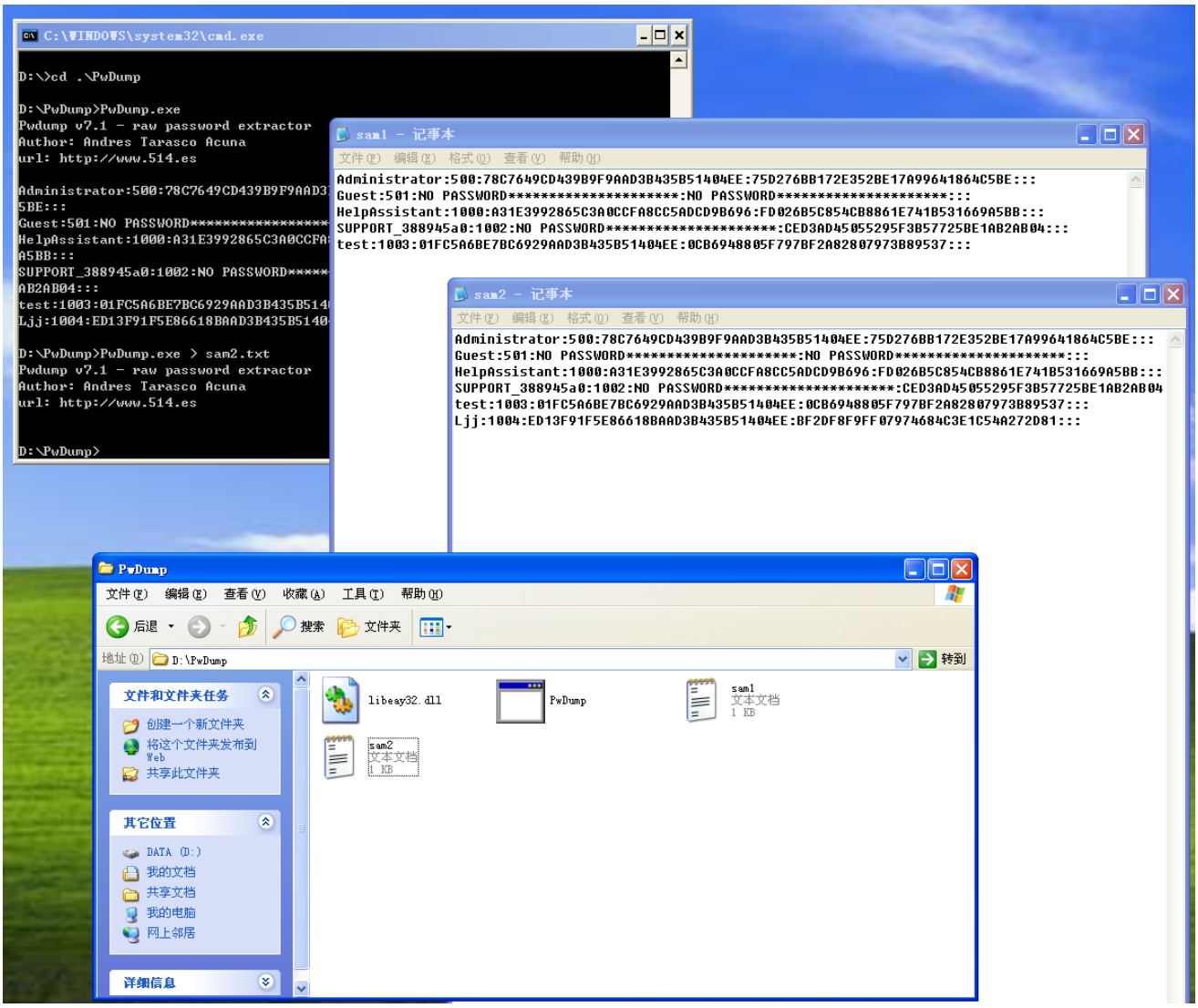
1. 在口令破解实验中请结合自己所做的操作（如增加或修改用户口令），比较操作前后所获得SAM文件信息的不同之处，说明每条记录的各字段的含义（截图不超过4张），并总结SAM文件的安全特性。（15分）

本次试验中我增加了用户Ljj，此用户的密码为Ljj
以下为使用mimikatz工具获取的sam文件内容：


mimikatz 2.1 x86 (oe.eo)
.#####. mimikatz 2.1 (x86) built on Sep 10 2016 23:10:12
.## ^ ##. "A La Vie, A L'Amour"
/ \ ## /* * *
\ / ## Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com)
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' with 20 modules * * */
mimikatz # lsadump::sam /sam:SAM /system:SYSTEM
Domain : MK-C24134628432
SysKey : bec2c5bf1c2a871ff9fc8e0687255c21
Local SID : S-1-5-21-1085031214-1078145449-725345543
SAMKey : 59b01701d4e3d21a4384de2e689b6166
RID : 000001f4 (500)
User : Administrator
LM : 78c7649cd439b9f9aad3b435b51404ee
NTLM : 75d276bb172e352be17a99641864c5be
RID : 000001f5 (501)
User : Guest
LM :
NTLM :
RID : 000003e8 (1000)
User : HelpAssistant
LM : a31e3992865c3a0ccfa8cc5adcd9b696
NTLM : fd026b5c854cb8861e741b531669a5bb
RID : 000003ea (1002)
User : SUPPORT_388945a0
LM :
NTLM : ced3ad45055295f3b57725be1ab2ab04
RID : 000003eb (1003)
User : test
LM : 01fc5a6be7bc6929aad3b435b51404ee
NTLM : 0cb6948805f797bf2a82807973b89537
mimikatz # lsadump::sam /sam:SAM /system:SYSTEM
Domain : MK-C24134628432
SysKey : bec2c5bf1c2a871ff9fc8e0687255c21
Local SID : S-1-5-21-1085031214-1078145449-725345543
SAMKey : 59b01701d4e3d21a4384de2e689b6166
RID : 000001f4 (500)
User : Administrator
LM : 78c7649cd439b9f9aad3b435b51404ee
NTLM : 75d276bb172e352be17a99641864c5be
RID : 000001f5 (501)
User : Guest
LM :
NTLM :
RID : 000003e8 (1000)
User : HelpAssistant
LM : a31e3992865c3a0ccfa8cc5adcd9b696
NTLM : fd026b5c854cb8861e741b531669a5bb
RID : 000003ea (1002)
User : SUPPORT_388945a0
LM :
NTLM : ced3ad45055295f3b57725be1ab2ab04
RID : 000003eb (1003)
User : test
LM : 01fc5a6be7bc6929aad3b435b51404ee
NTLM : 0cb6948805f797bf2a82807973b89537
RID : 000003ec (1004)
User : Ljj
LM : ed13f91f5e86618baad3b435b51404ee
NTLM : bf2df8f9ff07974684c3e1c54a272d81
mimikatz #

通过对比我们发现：
增加新用户后，sam文件中新增了一组数据。其中RID代表用户的编号；User代表用户名；LM和NTLM分别代表使用LM和NTLM加密方式生成的哈希值。

以下为使用PwDump工具获取的sam文件内容：



通过对比我们发现：
增加新用户后sam文件中多了一行数据，各条信息以冒号分割；各组信息以三个连续冒号分割。结构可以表示成：username:RID:LM-Hash:NT-Hash
第一条信息代表用户名；第二条信息是RID；第三条信息是经过LM加密算法生成的hash值；第四条信息是NTLM加密算法生成的hash值。

我们可以总结sam文件的安全特性：

- 在系统运行期间， SAM文件被system账号锁定，即使是administrator账号也无法对其进行删除或拷贝等操作，需要特殊工具通过特殊方式才可以获取。
- SAM文件中的密码信息并非是使用明文形式保存，而是保存着两种不同加密算法得到的hash值。
- 在运行lsass.exe时内存中会出现以明文形式存储的密码，易导致密码泄露；同时可以从repair目录攫取备份的SAM。

2. 根据SAM口令破解的情况，给出设置安全性较高的用户口令的原则或建议。（20分）

设置用户口令的建议：

- 不同用户应当采用不同的口令，避免使用相同的口令。
- 口令与用户名之间应当没有语义或者逻辑上的联系。
- 口令长度应当足够长，并且包含但不限于数字、字母、符号，同时避免字母或者数字是连续的，防止枚举攻击。
- 口令应当不涉及使用者的身份信息，比如生日以及身份证号等。

3. 查看mysql的apparmor配置文件内容，说明文件结构和各部分含义。并对比工作模式更改前后的变化。（25分）

mysql的apparmo配置文件内容：

```
test@ubuntu1804:~$ cd /etc/apparmor.d
test@ubuntu1804:/etc/apparmor.d$ cat usr.sbin.mysqld
# vim:syntax=apparmor
# Last Modified: Tue Feb 09 15:28:30 2016
#include <tunables/global>

/usr/sbin/mysqld {
  #include <abstractions/base>
  #include <abstractions/nameservice>
  #include <abstractions/user-tmp>
  #include <abstractions/mysql>
  #include <abstractions/winbind>

# Allow system resource access
  /proc/*/status r,
  /sys/devices/system/cpu/ r,
  /sys/devices/system/node/ r,
  /sys/devices/system/node/** r,
  capability sys_resource,
  capability dac_override,
  capability dac_read_search,
  capability setuid,
  capability setgid,

# Allow network access
  network tcp,

  /etc/hosts.allow r,
  /etc/hosts.deny r,

# Allow config access
  /etc/mysql/** r,

# Allow pid, socket, socket lock file access
  /var/run/mysqld/mysqld.pid rw,
  /var/run/mysqld/mysqld.sock rw,
  /var/run/mysqld/mysqld.sock.lock rw,
  /run/mysqld/mysqld.pid rw,
  /run/mysqld/mysqld.sock rw,
  /run/mysqld/mysqld.sock.lock rw,

# Allow systemd notify messages
  /{,var/}run/systemd/notify w,

# Allow execution of server binary
  /usr/sbin/mysqld mr,
  /usr/sbin/mysqld-debug mr,

# Allow plugin access
  /usr/lib/mysql/plugin/ r,
  /usr/lib/mysql/plugin/*.so* mr,
```

```
# Allow error msg and charset access
  /usr/share/mysql/ r,
  /usr/share/mysql/** r,

# Allow data dir access
  /var/lib/mysql/ r,
  /var/lib/mysql/** rwk,

# Allow data files dir access
  /var/lib/mysql-files/ r,
  /var/lib/mysql-files/** rwk,

# Allow keyring dir access
  /var/lib/mysql-keyring/ r,
  /var/lib/mysql-keyring/** rwk,

# Allow log file access
  /var/log/mysql.err rw,
  /var/log/mysql.log rw,
  /var/log/mysql/ r,
  /var/log/mysql/** rw,

# Allow read access to OpenSSL config
  /etc/ssl/openssl.cnf r,
  # Site-specific additions and overrides. See local/README for details.
  #include <local/usr.sbin.mysqld>
}
test@ubuntu1804:/etc/apparmor.d$
```

从配置文件可以看到apparmor对mysqld进程的访问控制粒度非常细，包括所有类型的文件、网络、系统资源等，这样大大提高了安全性。配置文件中包含以下内容：

- include语句：Include 语句是可提取其他 apparmor 配置文件的组件以简化配置文件的指令。Include 文件会检索程序的访问权限。通过使用 include，可以向程序赋予访问其它程序也需要的目录路径和文件的权限。使用 include 可减小配置文件的大小。
- 网络访问控制：network tcp，说明支持的协议为tcp协议。
- 功能项：capability一次后接功能名称，用以授权功能。
- 配置文件名称：通过指定程序可执行文件的完整路径来将配置文件关联到相应程序。

complain模式下：

```
test@ubuntu1804:/etc/apparmor.d$ sudo aa-complain /usr/sbin/mysqld
Setting /usr/sbin/mysqld to complain mode.
test@ubuntu1804:/etc/apparmor.d$ sudo apparmor_status
apparmor module is loaded.
38 profiles are loaded.
35 profiles are in enforce mode.
   /sbin/dhclient
   /snap/core/4486/usr/lib/snapd/snap-confine
   /snap/core/4486/usr/lib/snapd/snap-confine//mount-namespace-capture-helper
   /usr/bin/evince
   /usr/bin/evince-previewer
   /usr/bin/evince-previewer//sanitized_helper
   /usr/bin/evince-thumbnailer
   /usr/bin/evince//sanitized_helper
   /usr/bin/man
   /usr/lib/NetworkManager/nm-dhcp-client.action
   /usr/lib/NetworkManager/nm-dhcp-helper
   /usr/lib/connman/scripts/dhclient-script
   /usr/lib/cups/backend/cups-pdf
   /usr/lib/snapd/snap-confine
   /usr/lib/snapd/snap-confine//mount-namespace-capture-helper
   /usr/sbin/cups-browsed
   /usr/sbin/cupsd
   /usr/sbin/cupsd//third_party
   /usr/sbin/ippusbxd
   /usr/sbin/tcpdump
   libreoffice-senddoc
   libreoffice-soffice//gpg
   libreoffice-xpdfimport
   man_filter
   man_groff
   snap-update-ns.core
   snap-update-ns.gnome-calculator
   snap-update-ns.gnome-characters
   snap-update-ns.gnome-logs
   snap-update-ns.gnome-system-monitor
   snap.core.hook.configure
   snap.gnome-calculator.gnome-calculator
   snap.gnome-characters.gnome-characters
   snap.gnome-logs.gnome-logs
   snap.gnome-system-monitor.gnome-system-monitor
3 profiles are in complain mode.
   /usr/sbin/mysqld
   libreoffice-oopslash
   libreoffice-soffice
4 processes have profiles defined.
3 processes are in enforce mode.
   /sbin/dhclient (3147)
   /usr/sbin/cups-browsed (2761)
   /usr/sbin/cupsd (2760)
1 processes are in complain mode.
   /usr/sbin/mysqld (955)
0 processes are unconfined but have a profile defined.
```

enforce模式下：

```
test@ubuntu1804:/etc/apparmor.d$ sudo aa-enforce /usr/sbin/mysqld
Setting /usr/sbin/mysqld to enforce mode.
test@ubuntu1804:/etc/apparmor.d$ sudo apparmor_status
apparmor module is loaded.
38 profiles are loaded.
36 profiles are in enforce mode.
   /sbin/dhclient
   /snap/core/4486/usr/lib/snapd/snap-confine
   /snap/core/4486/usr/lib/snapd/snap-confine//mount-namespace-capture-helper
   /usr/bin/evince
   /usr/bin/evince-previewer
   /usr/bin/evince-previewer//sanitized_helper
   /usr/bin/evince-thumbnailer
   /usr/bin/evince//sanitized_helper
   /usr/bin/man
   /usr/lib/NetworkManager/nm-dhcp-client.action
   /usr/lib/NetworkManager/nm-dhcp-helper
   /usr/lib/connman/scripts/dhclient-script
   /usr/lib/cups/backend/cups-pdf
   /usr/lib/snapd/snap-confine
   /usr/lib/snapd/snap-confine//mount-namespace-capture-helper
   /usr/sbin/cups-browsed
   /usr/sbin/cupsd
   /usr/sbin/cupsd//third_party
   /usr/sbin/ippusbxd
   /usr/sbin/mysqld
   /usr/sbin/tcpdump
   libreoffice-senddoc
   libreoffice-soffice//gpg
   libreoffice-xpdfimport
   man_filter
   man_groff
   snap-update-ns.core
   snap-update-ns.gnome-calculator
   snap-update-ns.gnome-characters
   snap-update-ns.gnome-logs
   snap-update-ns.gnome-system-monitor
   snap.core.hook.configure
   snap.gnome-calculator.gnome-calculator
   snap.gnome-characters.gnome-characters
   snap.gnome-logs.gnome-logs
   snap.gnome-system-monitor.gnome-system-monitor
2 profiles are in complain mode.
   libreoffice-oopslash
   libreoffice-soffice
4 processes have profiles defined.
4 processes are in enforce mode.
   /sbin/dhclient (3147)
   /usr/sbin/cups-browsed (2761)
   /usr/sbin/cupsd (2760)
   /usr/sbin/mysqld (955)
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
test@ubuntu1804:/etc/apparmor.d$
```

通过对比，
开启complain模式后，mysqld的profile和process被从enforce模式中转换到了complain模式，其余的Profiles 和 Processes状态未发生变化。

4. 思考Windows的两种安全认证协议NTLM和Kerberos，总结分析各自的优点、缺点及其可能存在的至少 1 种攻击方式。（30分）

NTLM：
优点：

- 兼容性好：相比于Kerberos，NTLM可以在非Active Directory域成员或者Windows 2000以下版本的Windows计算机上使用，应用场景更加广泛。
- 简单易用：相比Kerberos协议，NTLM协议的配置和管理比较简单，适用于小型和中型组织。
- 适用于多平台：NTLM协议不仅仅适用于Windows操作系统，还适用于其他操作系统和应用程序。

缺点：

- 算法安全性低：NTLM使用的哈希算法已被证实安全性较差，易被破解。
- 不支持跨域认证：NTLM协议不支持跨域认证，这意味着在多域环境下，用户需要为每个域分别进行认证。

可能存在的攻击方式：
（1）针对NTLM v1 hash的枚举攻击
（2）针对Net-NTLM的重放攻击
（3）中间人攻击

Kerberos：
优点：

- 安全性较高：认证过程复杂，无需通过网络发送密码或将密码缓存在本地用户的硬盘上，安全性较高。
- 支持跨域认证：Kerberos支持跨域认证，这使得在多域环境下进行认证变得更加容易。
- 可扩展性好：Kerberos协议支持使用多种加密算法，可以根据需要进行扩展。

缺点：

- 兼容性差：服务和客户端都必须在Windows系统的Windows 2000或更高版本上运行并且必须在Active Directory下才可以使用，否则身份验证将失败，应用范围较窄。
- 成本较高：Kerberos需要在网络中部署Key Distribution Center (KDC)来管理票据，需要更多的网络资源和管理成本。

可能存在的攻击方式：

- Kerberos票据重放攻击：此认证协议下，拥有票据很重要。Ticket一旦生成，在生存时间内可以被Client多次使用来申请同一个Server的服务，这就可能存在票据窃取的攻击方式。
- 中间人攻击：攻击者可以通过欺骗用户向自己发出身份验证请求，然后冒充用户向服务器发出身份验证请求，获取用户的票据并访问受保护的资源。

四、实验总结（收获和心得）（5分）

通过这次实验我对操作系统的访问控制的理解更加深入，对Windows和Linux所采用的访问控制策略以及协议有了更加深入的理解。

撰写报告时，通过查阅课外资料，我对NTLM以及Kerberos协议的了解相比于其它概念更加深刻，对各自的认证流程有了比较清晰的认识。在此基础上我对比分析了二者在安全性、兼容性以及经济上的优劣，也看到了各自因为其特性而存在的特殊安全漏洞以及一些共性导致可能存在的相同攻击方式，比如中间人攻击。
总而言之，本次实验的操作过程以及整理实验报告的过程让我学会了很多，我开始入门信息安全专业，我对此感到十分开心十分期待。

五、尚存问题或疑问、建议（5分）

尚存疑问：

- 使用LM或者是NTLM加密方式时，内存中会保存以明文形式保存的密码，有没有额外的加密方式使得内存中的数据也能得到保护？
- 可以从repair目录中攫取备份的SAM文件，为何不对备份文件进行锁定？
- Kerberos认证过程中如果网络不稳定甚至是链接断掉该如何处理？