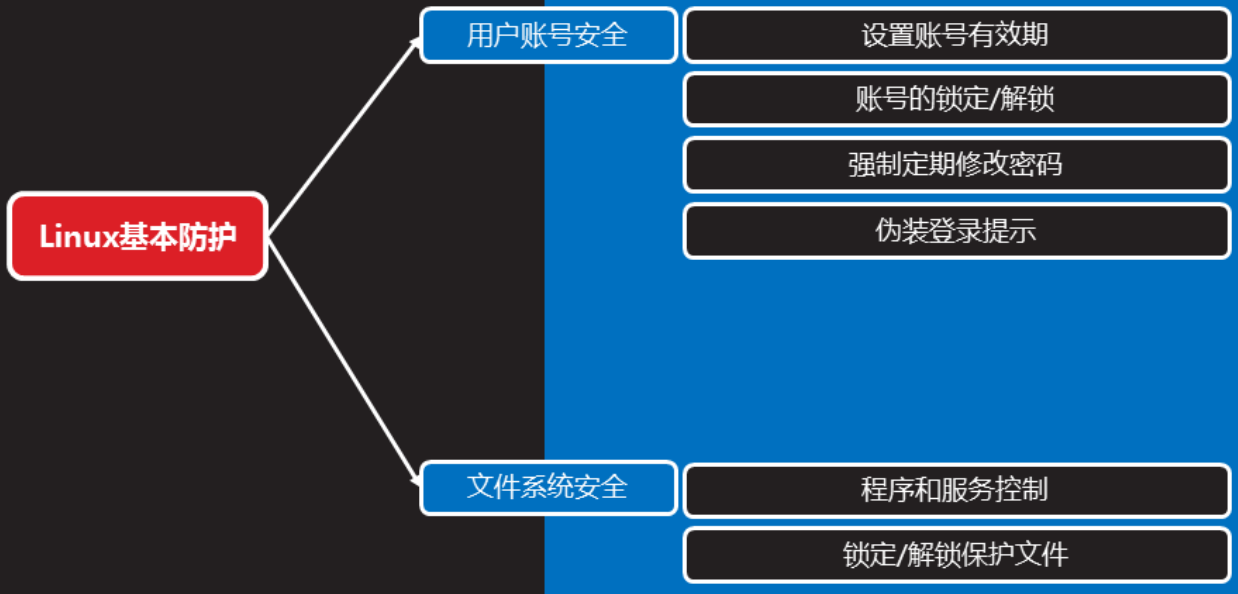
SECURITY DAY01

内容

上午	09:00 ~ 09:30	Linux基本防护
	09:30 ~ 10:20	
	10:30 ~ 11:20	用户切换与提权
	11:30 ~ 12:00	
下午	14:00 ~ 14:50	SSH访问控制
	15:00 ~ 15:50	SELinux安全防护
	16:10 ~ 17:00	
	17:10 ~ 18:00	总结和答疑

Linux基本防护



用户账号安全

设置账号有效期

知识讲解

- 使用chage工具
  - -d 0，强制修改密码
  - -E yyyy-mm-dd，指定失效日期（-1取消）

```
[root@svr7 ~]# chage  -E  2017-12-31  zengye
[root@svr7 ~]# chage  -l  zengye
.. ..
Password inactive                       : never
Account expires                         : Dec 31, 2017
.. ..
```

伪装登录提示

知识讲解

- 配置文件/etc/issue、 /etc/issue.net
  - 分别适用于本地、远程登录
  - 默认会提示内核、系统等版本信息

```
Windows Server 2012 Enterprise R2
NT 6.2 Hybrid
svr1 login: root
Password:
Last login: Mon Jul 29 11:24:12 on tty1
[root@svr1 ~]#
```

文件系统安全

程序和服务控制

Tedu.cn 达内教育

- 禁用非必要的系统服务
  - 使用systemctl、chkconfig工具

知识讲解

案例1：Linux基本防护措施

Tedu.cn 达内教育

课堂练习

1. 使用户zhangsan在2017-12-31日失效
2. 临时锁定用户lisi的账户，验证效果后解除锁定
3. 锁定文件/etc/resolv.conf、/etc/hosts，以防止其内容被无意中修改
4. 修改tty终端提示，使得登录前看到的第一行文本为“Windows Server 2012 Enterprise R2”，第二行文本为“NT 6.2 Hybrid”


Tedu.cn
达内教育
su切换用户身份


Tedu.cn

su切换的基本用法

Tedu.cn 达内教育

知识讲解

- Substitute User，换人
  - 快速切换为指定的其他用户
  - 普通用户执行时，需验证目标用户的口令
  - root执行时，无需验证口令
- 命令格式
  - 用法1：su [-] [目标用户]
  - 用法2：su [-] -c "命令" [目标用户]

su操作示例（续1）

Tedu.cn 达内教育

知识讲解

- root以指定的普通用户身份执行任务
  - 以用户tom的身份创建目录
  - 以用户tom的身份执行管理员操作会出错

```
[root@svr7 ~]# su - tom  -c "mkdir /home/tom/test "

[root@svr7 ~]# su - nb -c "systemctl restart sshd"
Error creating textual authentication agent
```

分析su切换的使用情况

- 安全日志/var/log/secure
  - 记录su验证、Shell开启与关闭

知识讲解

```
[root@svr7 ~]# tail  /var/log/secure
.. ..
Jul 29 15:11:05 svr7 su: pam_unix(su-l:session): session opened
for user root by zengye(uid=500)
Jul 29 15:11:09 svr7 su: pam_unix(su-l:session): session closed for
user root
```

su切换登入成功

su会话断开成功

sudo提升执行权限

sudo提权的基本用法

Tedu.cn 达内教育

知识讲解

- Super or another Do，超级执行
  - 管理员预先为用户设置执行许可
  - 被授权用户有权执行授权的命令，验证自己的口令
- 命令格式
  - 用法1：sudo 特权命令
  - 用法2：sudo [-u 目标用户] 特权命令

配置sudo授权

Tedu.cn 达内教育

知识讲解

- 修改方法
  - 推荐：visudo
  - 其他：vim /etc/sudoers
- 授权记录格式
  - 用户 主机列表=命令列表

```
[root@svr7 ~]# grep ^root /etc/sudoers
root            ALL=(ALL)       ALL
```

可以是 %组名

目标身份，省略时表示root

配置sudo授权（续2）

Tedu.cn 达内教育

知识讲解

- 示例2
  - wheel组的用户无需验证可执行所有命令

```
[root@svr7 ~]# visudo
.. ..
%wheel        ALL=(ALL)       NOPASSWD: ALL
```

分析sudo提权的使用情况

Tedu.cn 达内教育

知识讲解

- 修改全局配置，启用日志
  - Defaults logfile="/var/log/sudo"

```
[root@svr7 ~]# tail  /var/log/sudo
.. ..
Jul 29 16:10:26 : mike : TTY=pts/0 ; PWD=/home/mike ; USER=root ;
   COMMAND=/bin/mkdir /opt/mydata
Jul 29 16:11:02 : mike : TTY=pts/0 ; PWD=/home/mike ; USER=root ;
   COMMAND=/bin/cp /etc/shadow /opt/mydata/
```

sudo别名设置

知识讲解

- 主要用途
  - 提高可重用性、易读性
  - 简化配置、使记录更有条理

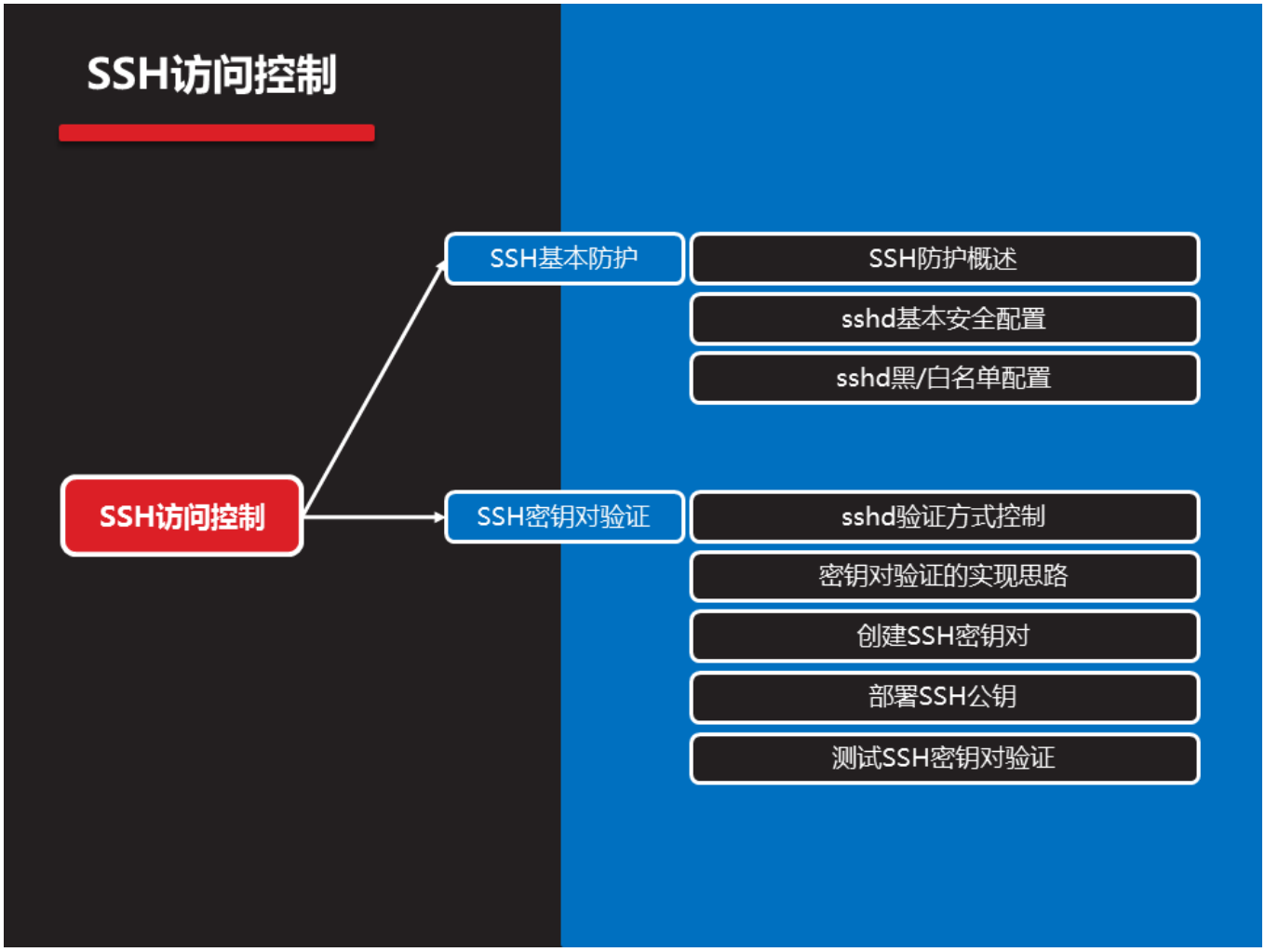
```
[root@svr7 ~]# visudo
.. ..
User_Alias  OPERATORS=jerry,tom,tsengyia
Host_Alias  MAILSERVERS=mail,smtp,pop,svr7
Cmnd_Alias  SOFTMGR=/bin/rpm,/usr/bin/yum
OPERATORS   MAILSERVERS=SOFTMGR
```

别名的名称必须全大写

案例2：使用sudo分配管理权限

课堂练习

1.使用su命令临时切换账户身份，并执行命令
2.允许softadm管理系统服务的权限
3.允许用户useradm管理本地账号（root除外）
4.允许wheel组成员以特权执行/usr/bin/下的命令
5.启用sudo日志以便跟踪


SSH访问控制
SSH访问控制
SSH基本防护
SSH防护概述
sshd基本安全配置
sshd黑/白名单配置
SSH密钥对验证
sshd验证方式控制
密钥对验证的实现思路
创建SSH密钥对
部署SSH公钥
测试SSH密钥对验证


Tedu.cn
达内教育
SSH基本防护

SSH防护概述

Tedu.cn 达内教育

知识讲解

- 存在的安全隐患
  - 密码嗅探、键盘记录
  - 暴力枚举账号、猜解密码
- 常见的防护措施
  - 用户限制、黑白名单
  - 更改验证方式（密码-->密钥对）
  - 防火墙.. ..

sshd黑/白名单配置

Tedu.cn 达内教育

知识讲解

- 配置文件 /etc/ssh/sshd_config
  - DenyUsers USER1 USER2 ...
  - AllowUsers USER1@HOST USER2 ...
  - DenyGroups GROUP1 GROUP2 ...
  - AllowGroups GROUP1 GROUP2 ...

Tedu.cn 达内教育

SSH密钥对验证

sshd验证方式控制

知识讲解

- 口令验证
  - 检查登录用户的口令是否一致
- 密钥验证
  - 检查客户端私钥与服务器上的公钥是否匹配

```
PasswordAuthentication   yes
.. ..
PubkeyAuthentication   yes
AuthorizedKeysFile   .ssh/authorized_keys
```

公钥库：存放授权客户机的公钥文本

密钥对验证的实现思路

知识讲解

客户机的用户 **mike**

① 创建密钥对
私钥文件：id_rsa
公钥文件：id_rsa.pub

② 上传公钥 id_rsa.pub

服务器的用户 **john**

③ 导入公钥信息
公钥库：.ssh/authorized_keys

创建SSH密钥对

Tedu.cn 达内教育

知识讲解

- 使用工具 ssh-keygen
  - 可以手动指定加密算法（ -t rsa 或 -t dsa ）
  - 若不指定，默认采用RSA加密

```
[mike@svr7 ~]$ ssh-keygen
Enter passphrase (empty for no passphrase):          //设置私钥口令为空
Enter same passphrase again:
.. ..
[mike@svr7 ~]$ ls  -Al  /home/mike/.ssh/
-rw-------.  1  mike  mike  1743 7月  31 15:32  id_rsa          //私钥文件
-rw-r--r--.  1  mike  mike   391 7月  31 15:32  id_rsa.pub      //公钥文件
```

部署SSH公钥

Tedu.cn 达内教育

知识讲解

- 方法一，通过 ssh-copy-id 自动部署
  - 好处： ② ③ 一步到位
  - 局限性：要求SSH口令认证可用
- 方法二，通过FTP等方式上传、手动添加
  - 好处：灵活、适用范围广
  - 局限性：操作繁琐、易出错

```
[mike@svr7 ~]$ ssh-copy-id  john@192.168.4.7
john@192.168.4.7's password:
Now try .. ..  check in:
    .ssh/authorized_keys
.. ..
```

案例3：提高SSH服务安全

Tedu.cn 达内教育

课堂练习

1. 基本安全策略（禁止root、禁止空口令）
2. 为SSH访问配置“仅允许”策略
3. 分别实现密钥验证登入、免密码登入
4. 禁用密码验证