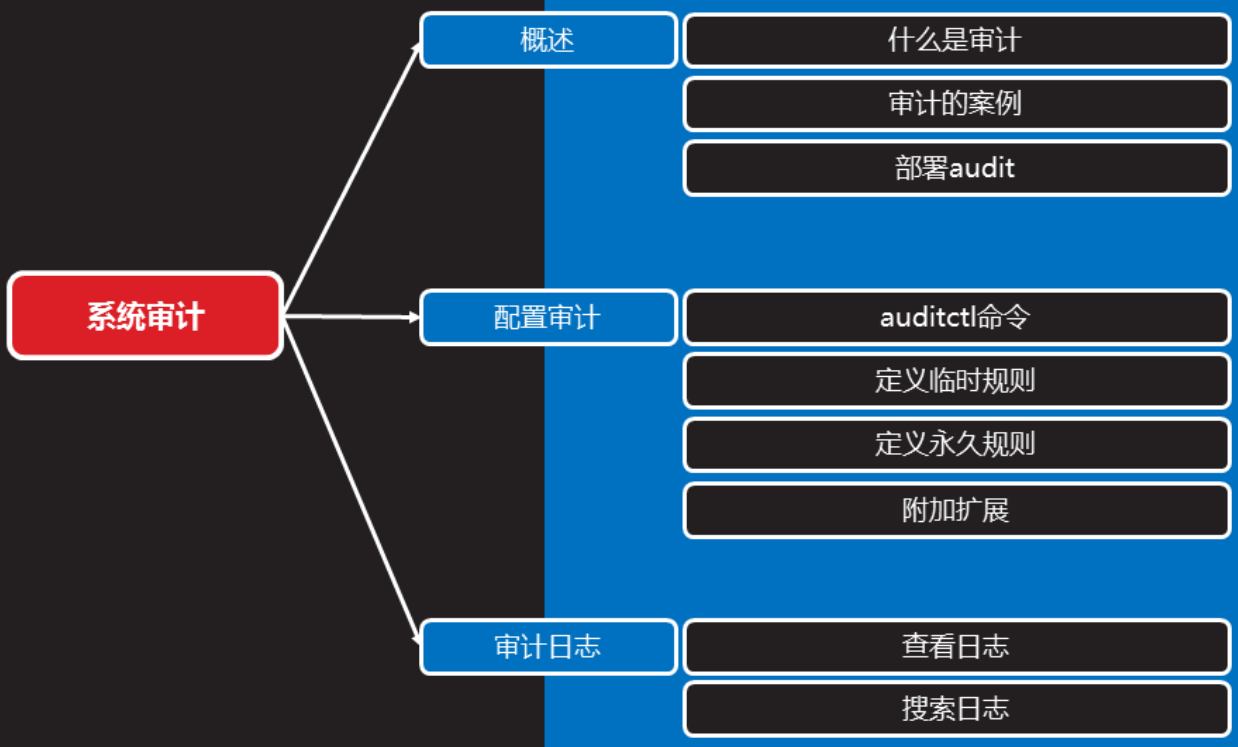
SECURITY DAY03

内容

上午	09:00 ~ 09:30	作业讲解和回顾
	09:30 ~ 10:20	系统审计
	10:30 ~ 11:20	
	11:30 ~ 12:00	服务安全
下午	14:00 ~ 14:50	
	15:00 ~ 15:50	Linux安全之打补丁
	16:10 ~ 17:00	
	17:10 ~ 18:00	总结和答疑

系统审计



概述

什么是审计

知识讲解

- 基于事先配置的规则生成日志，记录可能发生在系统上的事件
- 审计不会为系统提供额外的安全保护，但她会发现并记录违反安全策略的人及其对应的行为
- 审计能够记录的日志内容：
  - 日期与事件、事件结果
  - 触发事件的用户
  - 所有认证机制的使用都可以被记录，如ssh等
  - 对关键数据文件的修改行为等

审计的案例

Tedu.cn 达内教育

知识讲解

- 监控文件访问
- 监控系统调用
- 记录用户运行的命令
- 审计可以监控网络访问行为
- ausearch工具，可以根据条件过滤审计日志
- aureport工具，可以生成审计报告

auditctl命令

Tedu.cn 达内教育

- auditctl命令控制审计系统并设置规则决定哪些行为会被记录日志

知识讲解

```
[root@svr7 ~]# auditctl  -s          //查询状态
[root@svr7 ~]# auditctl  -l          //查看规则
[root@svr7 ~]# auditctl  -D          //删除所有规则
```

定义永久规则

Tedu.cn 达内教育

知识讲解

- 定义永久规则
- 写入配置文件/etc/audit/rules.d/audit.rules

```
[root@svr7 ~]# vim  /etc/audit/rules.d/audit.rules
-w /etc/passwd -p wa -k passwd_changes
-w /usr/sbin/fdisk -p x -k partition_disks
```

附加扩展

Tedu.cn 达内教育

知识讲解

- 扩展知识
  - 系统提供的参考模板

```
[root@svr7 ~]# ls  /usr/share/doc/audit-版本号/rules/
```


Tedu.cn
达内教育
审计日志

搜索日志

Tedu.cn 达内教育

知识讲解

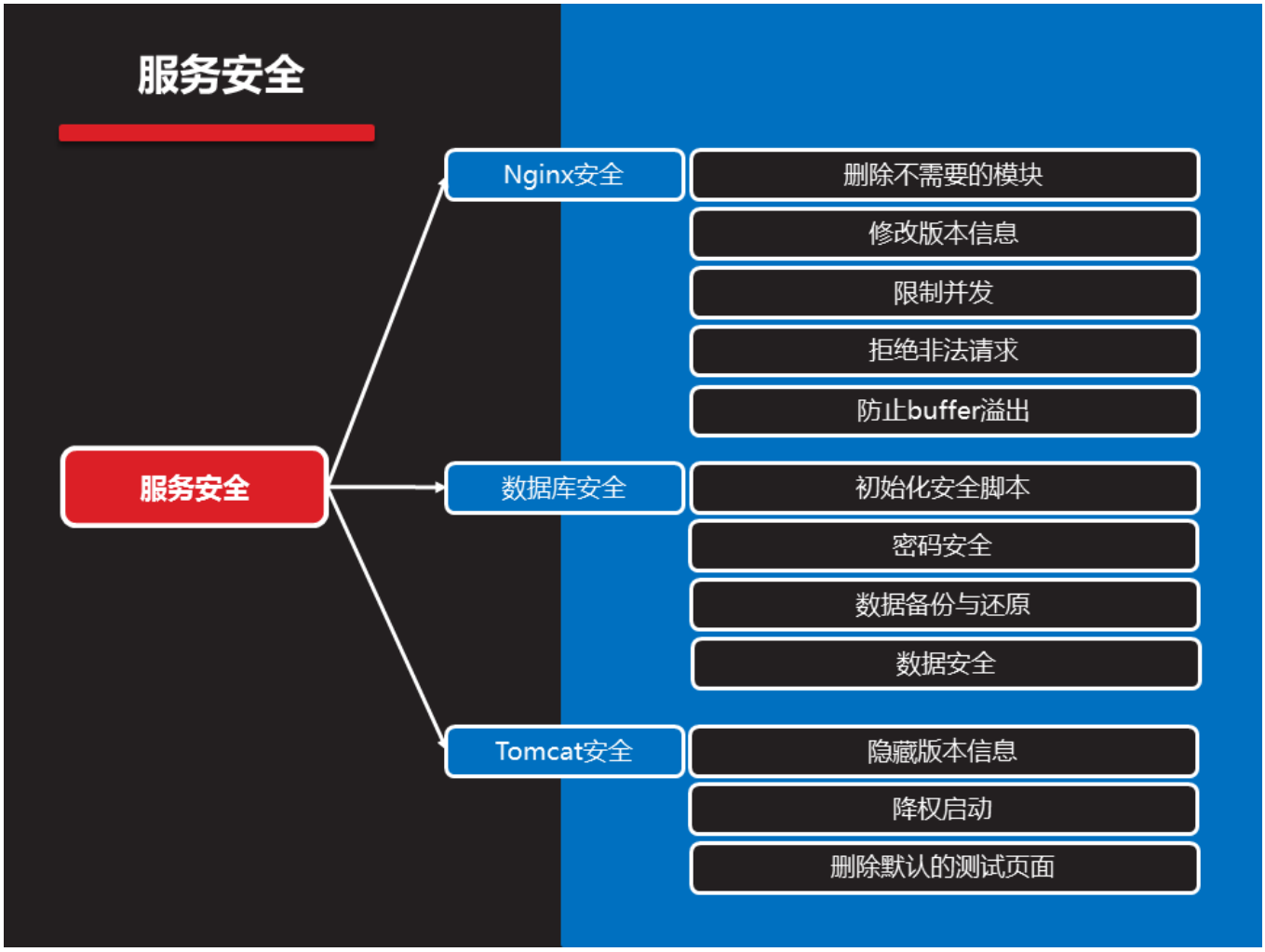
- 系统提供的ausearch命令可以方便的搜索特定日志
  - 默认该程序会搜索/var/log/audit/audit.log
  - ausearch options -if file_name可以指定文件名

```
[roo@svr7 ~]# ausearch -k sshd_config -i
//根据key搜索日志，-i为交互式操作
```

案例1：部署audit监控文件

Tedu.cn 达内教育

1. 使用audit监控/etc/ssh/sshd_config
2. 当该文件发生任何变化即记录日志


服务安全
服务安全
Nginx安全
删除不需要的模块
修改版本信息
限制并发
拒绝非法请求
防止buffer溢出
数据库安全
初始化安全脚本
密码安全
数据备份与还原
数据安全
Tomcat安全
隐藏版本信息
降权启动
删除默认的测试页面


Tedu.cn
达内教育
Nginx安全

删除不需要的模块

Tedu.cn 达内教育

知识讲解

- Nginx是模块化设计
  - 需要的模块使用--with加载模块
  - 不需要的模块使用--without禁用模块
- 最小化安装永远的对的！！！

```
[roo@svr7 nginx-1.12]# ./configure \
>--without-http_autoindex_module \
>--without-http_ssi_module
[roo@svr7 nginx-1.12]# make
[roo@svr7 nginx-1.12]# make install
```

限制并发

Tedu.cn 达内教育

知识讲解

- ngx_http_limit_req_module为默认模块
  - 该模块可以降低DDos攻击风险

```
[roo@svr7 ~]# vim /usr/local/nginx/conf/nginx.conf
http{
limit_req_zone $binary_remote_addr zone=one:10m rate=1r/s;
        server {
                listen 80;
                server_name localhost;
                limit_req zone=one burst=5;
        }
}
```

限制并发（续1）

知识讲解

- 下面配置的功能为：
  - 语法：limit_req_zone key zone=name:size rate=rate;
  - 将客户端IP信息存储名称为one的共享内存，空间为10M
  - 1M可以存储8千个IP的信息，10M存8万个主机状态
  - 每秒中仅接受1个请求，多余的放入漏斗
  - 漏斗超过5个则报错

```
limit_req_zone $binary_remote_addr  zone=one:10m rate=1r/s;
limit_req zone=one burst=5;
```

```
[roo@client ~]# ab -c 100 -n 100  http://192.168.4.5/
```

拒绝非法请求

知识讲解

- 常见HTTP请求方法
  - HTTP定义了很多方法，实际应用中一般仅需要get和post

请求方法	功能描述
GET	**请求指定的页面信息，并返回实体主体**
HEAD	类似于get请求，只不过返回的响应中没有具体的内容，用于获取报头
POST	**向指定资源提交数据进行处理请求（例如提交表单或者上传文件）**
DELETE	请求服务器删除指定的页面
PUT	向服务器特定位置上传资料
…	其他

防止buffer溢出

- 防止客户端请求数据溢出
- 有效降低机器Dos攻击风险

知识讲解

```
[roo@svr7 ~]# vim /usr/local/nginx/conf/nginx.conf
http{
        client_body_buffer_size  1K;
        client_header_buffer_size 1k;
        client_max_body_size 16k;
        large_client_header_buffers 4 4k;
 ... ...
}
```

数据库安全

密码安全（续1）

知识讲解

- 问题是历史记录会出卖你!
- binlog日志里有明文密码（5.6版本后修复了）

```
[roo@svr7 ~]# cat .bash_history
mysqladmin -uroot -pxxx password 'redhat'
[roo@svr7 ~]# cat .mysql_history
set password for root@'localhost'=password('redhat');
select user,host,password from mysql.user;
flush privileges;
```

- 解决：
  - 管理好自己的历史，不使用明文登录，选择合适的版本
  - 日志，行为审计
  - 防火墙从TCP层设置ACL（禁止外网接触数据库）

数据备份与还原

知识讲解

- 备份

```
[roo@svr7 ~]# mysqldump -uroot -predhat mydb table > table.sql
[roo@svr7 ~]# mysqldump -uroot -predhat mydb > mydb.sql
[roo@svr7 ~]# mysqldump -uroot -predhat --all-databases > all.sql
```

- 还原

```
[roo@svr7 ~]# mysql -uroot -predhat mydb  < table.sql     //还原表
[roo@svr7 ~]# mysql -uroot -predhat mydb  < mydb.sql    //还原数据库
[roo@svr7 ~]# mysql -uroot -predhat < all.sql                 //还原所有
```

数据安全

Tedu.cn 达内教育

知识讲解

- 创建可以远程登录的账户

```
[roo@svr7 ~]# mysql -uroot -predhat
MariaDB [(none)]> grant all on *.* to tom@'%' identified by '123';
```

- 使用tcpdump抓包

```
[roo@svr7 ~]# tcpdump -w log -i eth0 src or dst port 3306
```

- 客户端远程登录数据库，查看抓包数据

```
[roo@client ~]# mysql -utom -p123 -h 192.168.4.5
MariaDB [(none)]> select * from mysql.user;
[roo@svr7 ~]# tcpdump -A -r log
```

- 解决：使用SSL或SSH加密数据传输

隐藏版本信息

Tedu.cn 达内教育

知识讲解

- 修改tomcat主配置文件，隐藏版本信息

```
[roo@svr7 tomcat]# yum -y install java-1.8.0-openjdk-devel
[roo@svr7 tomcat]# cd lib/ ;  jar -xf catalina.jar
[roo@svr7 tomcat]# vim org/apache/catalina/util/ServerInfo.properties //修改内容
[roo@svr7 tomcat]# vim /usr/local/tomcat/conf/server.xml
<Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"  redirectPort="8443" server="jacob" />
```

- 测试

```
[roo@svr7 ~]# curl -I http://192.168.2.100:8080/xx       //头部信息
[roo@svr7 ~]# curl -I http://192.168.2.100:8080          //头部信息
[roo@svr7 ~]# curl http://192.168.2.100:8080/xx          //报错页面
```

降权启动

Tedu.cn 达内教育

知识讲解

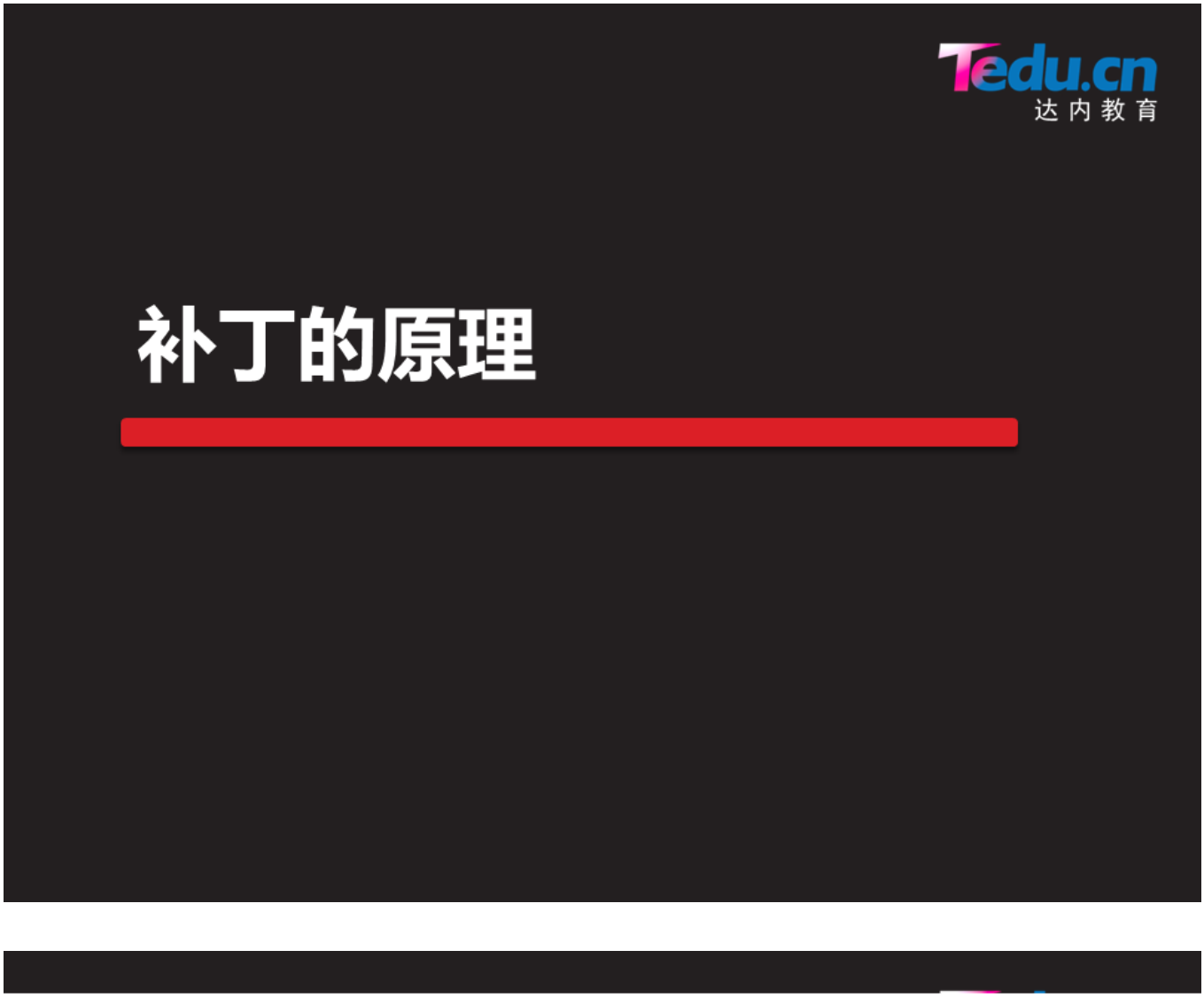
- 使用非root启动tomcat服务

```
[roo@svr7 ~]# useradd tomcat
[roo@svr7 ~]# chown -R tomcat:tomcat /usr/local/tomcat/
[roo@svr7 ~]# su -c /usr/local/tomcat/bin/startup.sh tomcat
```

- 开机启动

```
[roo@svr7 ~]# chmod +x /etc/rc.local
[roo@svr7 ~]# vim /etc/rc.local                  //添加如下内容
 su -c /usr/local/tomcat/bin/startup.sh tomcat
```


Tedu.cn
达内教育
删除默认的测试页面
[roo@svr7 ~]# rm -rf /usr/local/tomcat/webapps/*
知识讲解


Tedu.cn
达内教育
补丁的原理