考试科目2： 网络信息安全工程与综合应用实践　（下午大题）

概述：

根据教程例题可知重点应该在 **网站安全配置** 、**网络安全设备部署与使用** 上

根据大纲可知重点在 **网站安全配置** 和 **云安全**上

加起来就是：

网站安全配置

网络安全设备部署与使用

云安全

1. 网络安全风险评估与需求分析

1.1 风险评估

.....教程中不知道对应内容在哪

1.2 网络安全数据收集与分析

syslog日志数据

日志分析

.....

2. 网络安全常用方案设计

.....可能不是重点吧

3. 网络安全设备部署与使用　　重点

3.1　防火墙部署与使用　　**对应第8章**

3.2　IDS/IPS部署与使用

3.3 网闸部署与使用 第11章220页有相关内容

3.4 VPN部署与使用 对应第9章

3.5 漏洞扫描部署与使用

多看看防火墙配置真题

4. 网络信息系统安全配置与管理 重点

4.1 操作系统安全配置与管理

- Windows系统安全配置与管理
- Linux系统安全配置与管理

4.2 数据库系统安全配置与管理 对应第20章

- Oracle
- mssql
- mysql
- 国产数据库

4.3 网络系统安全配置与管理 重中之中 在22章

- apche
- iis

4.4 网络设备安全配置与管理 在第21章 命令得背背了

- 路由器
- 交换机

5. 网络安全需求分析与安全保护工程 对应第22章

5.1

网络安全概念

网络安全分析

网络安全需求

5.2 Apache 重点

大纲：

- apache 安装与配置
- apache 安全分析
- apache安全机制及配置
  - 文件权限设置
  - 认证和授权
  - 日志配置和读取
  - IP地址和域名访问控制
- apahce 安全漏洞处理办法

内容：

apache安全分析

1. 非授权访问
2. 网页篡改
3. 数据泄露
4. 恶意代码
5. 网站假冒
6. 拒绝服务
7. 网站后台管理威胁

- IP地址和域名访问控制

修改access.conf ，实现域名和ip地址的访问控制。

首先把deny from all设为初始指令，再使用allow from指令打开访问权限。

```
order deny, allow
deny from all
allow from pair 192.168.x.0/255.255.255.0
```

- 认证和授权

例如对某目录进行访问控制

第一步，修改配置文件httpd.conf

```
<Directory "/var/www/html">
    Options Indexes FollowSymLinks MultiViews
    AllowOverride AuthConfig
    Order allow,deny
    Allow from all
</Directory>
```

第二步，在该目录下建立.htaccess,内容如下

```
AuthName “private”        # 描述，随便写
AuthType Basic
AuthUserFile /usr/local/apache/conf/passwd
Require valid-user        # 所有合法用户
```

第三步，用apache提供的htpasswd命令创建用户

```
# /usr/local/apache/bin/htpasswd -c /usr/local/apache/conf/passwd testuser
```

apahce 安全漏洞处理办法

1.及时安装补丁

2.启用.htaccess文件保护网页

> .htaccess文件是apache的配置文件，功能包括设置网页密码、设置发生错误时出现的文件、改变首页的文件名（如:index.html）、禁止读取文件名、重新导向文件、加上mime类别、禁止列目录

> 下的文件等。

3. 为Apache服务软件设置专门的用户和组

按 特权最小原则分，不要用系统预定义的账号，例如nobody用户和组

4. 隐藏Apache软件的版本号

修改httpd.conf,设置

```
ServerSignature Off
ServerTokens Prod
```

重启apache

5. Apache目录访问安全性增强

三步

（1）禁止使用目录索引文件（即没有index.html的情况会列出目录）

修改配置文件httpd.conf

```
Options -Indexes FollowSymLinks
```

（2）禁止默认方法

```
Order Deny,Allow
Allow from All
```

（3）禁止用户重载

```
AllowOverride None
```

- **日志配置和读取**

  xxxxx

名词记录：

当 AllowOverride 设置为 None 时， .htaccess 文件将被完全忽略。

当此指令设置为 All 时，所有具有 “.htaccess” 作用域的指令都允许出现在 .htaccess 文件中。

AuthConfig

允许使用与认证授权相关的指令(AuthDBMGroupFile, AuthDBMUserFile, AuthGroupFile, AuthName, AuthType, AuthUserFile, Require,等)。

5.3 IIS

大纲

- IIS 安装与配置
- IIS 安全分析
- IIS安全机制及配置
    - 文件权限设置
    - 认证和授权
    - 日志配置和读取
    - IP地址和域名访问控制
- IIS 安全漏洞处理办法

内容：

- IIS 安装与配置

- IIS 安全分析

  IIS典型的安全威胁如下：

    - 非授权访问
    - 网络蠕虫
    - 网页篡改
    - 拒绝服务
    - IIS软件漏洞

> 与apache安全分析比较
> 1.非授权访问

2. 网页篡改
3. 数据泄露
4. 恶意代码
5. 网站假冒
6. 拒绝服务
7. 网站后台管理威胁

- IIS安全机制及配置
    - 文件权限设置
    - 认证和授权

        iis支持多重认证

        1. 匿名认证
        2. 基本验证
        3. 证书认证
        4. 数字签名认证
        5. IIS证书认证
        6. windows认证

    - 日志配置和读取

        ...

    - IP地址和域名访问控制

        IIS具有以下访问控制措施：

        1. 请求过滤
        2. URL授权控制
        3. IP地址限制
        4. 文件授权

        IIS访问控制流程：

        1. IP 地址限制　验证IP　验证访问者ip是否受限
        2. 用户认证 验证用户身份，验证账户是否非法
        3. WEB权限验证　　验证iis中的web权限是否允许
        4. NTFS权限验证　　即文件夹或web文件的ntfs权限

通过上述访问控制措施则允许访问其请求的资源

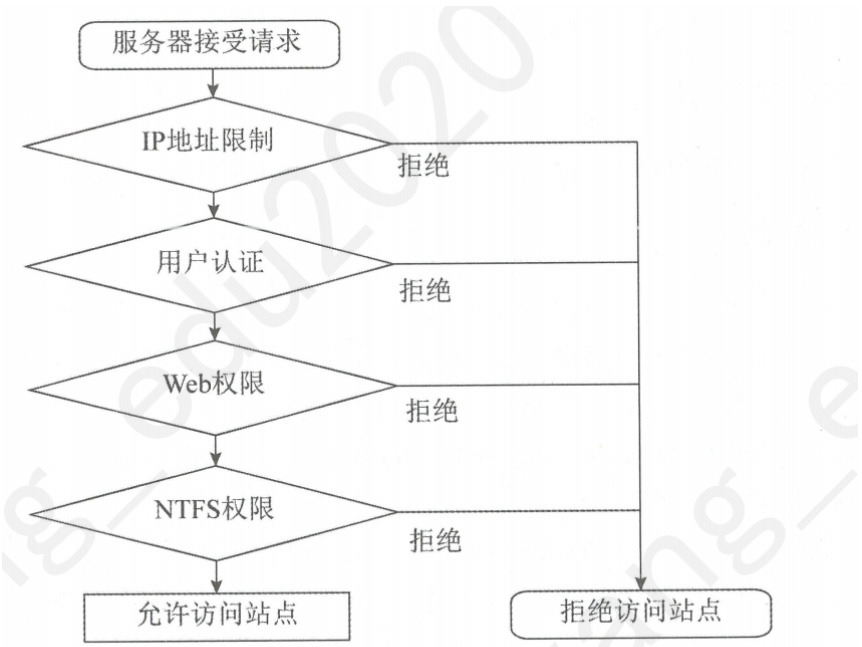

图 22-6　IIS 访问控制流程示意图

参教程485

- IIS 安全漏洞处理办法

  1.及时安装IIS补丁

  2.启用动态ip限制

  3.启用URLscan ： 可以限制特点的请求

  4.启用IIS Web应用防火墙

  5.启用SSL服务

6. 云计算安全需求分析与安全保护工程 (第23章)

6.1.1 云计算安全威胁　背一下

- 云计算用户安全威胁
- 云计算平台安全威胁
- 虚拟机安全威胁
- 云平台运维安全威胁

6.1.2 云计算安全需求　　背一下

- 云操作系统安全
- 云服务安全合规
- 多租户安全隔离
- 数据托管
- 隐私保护

6.2.1

云计算保护对象安全等级划分 就还是等保“用系安结访”那五个

云计算保护对象安全保护方法

6.2.2 云计算安全防护

表 23-2　云计算平台技术措施等级保护要求

保护对象类型	安 全 措 施 内 容
物理和环境安全	物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护
网络和通信安全	网络架构、通信传输、边界防护、访问控制、入侵防范、恶意代码防范、安全审计、集中管控
设备和计算安全	身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、资源控制、镜像和快照保护
应用和数据安全	身份鉴别、访问控制、安全审计、软件容错、资源控制、接口安全、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护

6.2.4 云计算安全运维

云计算安全运维安全措施

1. 云计算安全风险评估机制

2.云计算内部安全防护机制

3.云计算网络安全监测机制

4.云计算应急响应机制

5.云计算容灾备份机制

7.工控安全需求分析与安全保护工程

7.1

概念及组成：

工业控制系统简称**工控系统-ICS**

工控系统通常分为**离散制造类**和**过程控制类**两大类，**控制系统**包括

SCADA系统、

分布式控制系统DCS、

过程控制系统PCS、

可编程逻辑控制器PLC、

远程终端RTU、

数控机床及数控系统等。

SCADA系统 - 数据采集与监视控制系统。

工业控制系统安全威胁

1.自然灾害及环境

2.内部安全威胁

3.设备功能安全故障

4.恶意代码 （PLC Worm）

5.网络攻击

工业控制系统安全隐患

1.工控协议安全

2.工控系统 技术产品安全漏洞

3.工控系统 基础软件安全漏洞

4.工控系统 基础软件算法安全漏洞

5.工控系统 设备估计漏洞

6.工控系统 设备硬件漏洞

7.工控系统 开放接入漏洞

8.工控系统 供应链安全

7.2 工控系统安全保护机制与技术

物理及环境安全防护

视频监控

工业主机加固

安全分区与边界防护

安全分区

工控防火墙

工业控制安全隔离与信息交换系统

身份认证与访问控制

多因素认证

最小特权

避免使用默认口令或者弱口令

远程访问安全

禁用高风险服务

安全加固

虚拟专用网络

安全审计

工控系统安全加固

安全配置策略

身份认证增强

强制访问控制

程序白名单控制

工控安全审计

安全审计设备部署

审计数据备份

审计数据分析与利用

恶意代码防范 （如震网病毒、火焰病毒）

防病毒软件测试及部署运行

防病毒和恶意软件入侵管理机制

重大工控安全漏洞信息获取及补丁升级

7.2.8 工控数据安全

- 工业数据安全保护措施

安全隔离

访问控制

加密传输与存储

定期备份

- 测试数据保护措施

测试数据保护类型

签订保密协议

回收测试数据

7.2.9 工控安全检测与应急响应

- 工控网络安全监测设备安装和使用
- 工控安全事件应急响应预案制定、演练

7.2.10 工控安全管理

- 资产管理
- 冗余配置
- 安全软件选择与管理
- 配置和补丁管理
- 供应链管理
- 落实责任

7.2.11

8.移动应用安全需求分析与安全保护工程

Android系统安全机制 （考纲跟教程不太符）

1.应用程序签名机制
2.权限声明机制
3.沙箱隔离机制
4.网络通信传输加密
5.内核安全机制

IOS系统安全机制 （考纲跟教程不太符）

1.安全启动链
2.沙箱机制
3.数据的加密与保护机制
4.地址空间布局随机化
5.代码签名机制
6.网络传输加密

移动应用APP安全风险

1.逆向工程风险
2.篡改风险
3.数据窃取风险

APP安全加固

防逆向、防调试、防篡改

数据防泄露、数据传输保护

APP安全检测

身份认证机制检测

访问控制机制检测

服务器鉴权

APP安全漏洞检测

防SQL

防钓鱼

9. 大数据安全需求分析与安全保护工程

9.1

大数据概念与特点：

一般来说，大数据是指非传统的数据处理攻击的数据集，**具有海量的数据规模、快速的数据流转、多样的数据类型和价值密度低等特征。**

大数据安全问题：

1."数据集"安全边界日渐模糊，安全保护难度提升

2.敏感数据泄露风险增大

3.数据失真与大数据污染

4.业务连续性与拒绝服务

5.个人数据分布平台广泛，保护难度大

6.数据交易风险

7.大数据滥用

大数据安全需求：

- 数据安全基本要求

  机密性、完整性、可用性、**真实性、实时性、可追溯性**

- 大数据安全合规

- 大数据跨境安全
- 大数据隐私保护
- 大数据处理平台安全
- 大数据业务安全
- 大数据安全运营

9.2

大数据自身安全保护技术

- 数据源认证
- 数据溯源
- 数据用户标识和鉴别
- 数据资源访问控制

大数据平台安全保护技术

- 大数据平台边界安全
- ~网络通信安全
- ~用户身份认证与权限管理
- ~计算安全
- 平台应急灾备
- 大数据审计与监控

大数据隐私安全保护技术

- 数据身份匿名
- 数据差分隐私
- 数据脱敏
- 数据加密
- 数据访问控制

考试科目2：网络信息安全工程与综合应用实践

试题一(10分)

某公司网站应用架构采用 LAMP模式，其操作系统为Linux，Web服务器采用Apache HTP，数据库是MySQL，应用编程则为PHP，试解决网站应用中的安全问题。

(1)已知管理员使用Telnet和HTTP远程管理网站服务器，而国家信息安全等级安全保护要求为：(5分)

·当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。

·应为操作系统和数据库的不同用户分配不同的用户名，确保用户名具有唯一性。

请问：采取什么安全措施可以符合等级保护要求?如何获取网站操作系统和数据库的用户信息?

(1)解答：

①

1.通过iptables防火墙关闭23端口

```
iptables -A INPUT -p tcp --dport 23
iptables save
```

2.通过

-cmd防火墙关闭23端口

```
firewall-cmd --zone=public --remove-port=23/tcp --permanent
firewall-cmd --reload
```

参考：基线

https://blog.csdn.net/u011635437/article/details/109105024

②

操作系统用户名

cat /etc/passwd

数据库用户名

select user from mysql.user;

(2)网站安全策略要求网站的默认服务端口改成**8081**，远程计算机的IP地址192.68.02，若要其可以访问网站服务器/www/admin资源。如何配置Apache相关文件以符合安全策略要求?(5分)

(2)解答：

修改 httpd.conf

① 参数修改： Listen 8081

②

```
<Directory "/www/admin">
    Order Deny,Allow //允许指定字段访问，禁止其他所有字段
    Deny from all
 Allow from 1192.168.0.2
</Directory>

```

试题二(25 分)

(1)公司为了防止生产网受到外部的网络安全威胁，安全策略要求生产网和外部网之间部署安全隔离装置，隔离强度达到接近物理隔离。

请问：X最有可能代表的安全设备是什么?简要描述该设备的工作原理。(6分)

（1） X是网闸

工作原理：

> 网闸利用GAP技术，使两个或者两个以上的网络在不连通的情况下，
> 实现他们之间的安全数据交换和东西。

其技术原理是使用一个具有控制功能的开关　读写存储安全设备，通过开关的设置来连接或切断两个独立主机系统的数据交换。

(2)公司拟购买云计算服务，并租用虚拟主机，请列举云计算的服务安全风险类型。(5分)

- 云计算用户安全威胁
- 云计算平台安全威胁
- 虚拟机安全威胁
- 云平台运维安全威胁

(3)公司的防火墙是否能有效地保护虚拟主机安全?为什么?(4分)

不能，租用的虚拟主机在云端，威胁者可以直接发起攻击请求，不经过防火墙

(4)高级持续威胁(简称APT)常常利用电子邮件，开展有针对性的目标攻击，威胁者A发送带有恶意Word附件的电子邮件到公司邮件服务器，等待邮件接收者执行电子邮件附件，触发恶意程序运行，从而渗透到甲公司内部网络，

请给出威胁者A的攻击流量经过的网络设备。针对APT，可以部署什么安全设备来自动检测?该设备的主要技术方法是什么?(10分)

解答：

威胁者　互联网->

路由器 防火墙2　交换机4　网站邮件服务->

防火墙1交换机2 王五计算机（访问邮件服务，打开了恶意邮件）

可以部署 APT检测系统（部署在核心交换机处）

技术方法：（这里也是，因为是按点得分的，所以多写点）

恶意代码检测技术：静态检测，动态调试

恶意代码阻断能力：网络阻断、主机阻断、应用阻断　　及时阻断。

其他：

第8章是重中之重 尤其是8.4防火墙防御体系结构类型

httpd.conf

```
<Directory "你要限制访问的目录">
    Order Deny,Allow//允许指定字段访问，禁止其他所有字段
    Deny from all
 Allow From 192.168.0.0/24 //允许指定字段的访问
 Allow From 127.0.0.1
 Allow From 59.37.x.x/28
 //----如果是以下，即为限制从192.168.0 和 127.0.1这两个字段内的用户访问，别的用户可以
 Allow From all
 Deny From 192.168.0
  Deny From 127.0.0.1
</Directory>



<Files "你要限制访问的文件名">
    Order Deny,Allow
 //允许指定字段访问，禁止其他所有字段
    Deny from all
 Allow From 192.168.0.0/24 //允许指定字段的访问
 Allow From 127.0.0.1
 Allow From 59.37.x.x/28
 //----如果是以下，即为限制从192.168.0 和 127.0.1这两个字段内的用户访问，别的用户可以
 Allow From all
 Deny From 192.168.0
 Deny From 127.0.0.1
```

```
26 </Files>
```

其他：

linux目录解析

/etc/passwd shadow group 各个字段含义

/etc/passwd 权限64 rw- r-- r--

/etc/group 权限644 rw- r-- r--

/etc/shadow 权限640 r-- --- --

认为不重要的不写或者直接删掉好了，反正也背不过来

Linux有7种运行模式 init 0-6

0 关机

1 单用户模式

2 多用户模式

3 切换到命令行模式 服务一般处于这种模式

4 未被使用的模式

5 切换到桌面模式

6 重启