2016年全国职业院校信息技术技能大赛
网络信息安全赛项规程

一、赛项信息

赛项名称：网络信息安全

赛项组别：中职组

赛项归属产业：信息技术产业

二、竞赛目的

本赛项面向信息技术大类的中职学生，能够规范学生的上网行为，培养学生各种上网行为的法律意识。赛项主要考察中职生网络安全方面的专业基础知识及相关的操作技能，使学生能适应网络技术发展对网络与网站管理人才的技能要求，特别是安全方面的需求，提高信息技术大类学生的就业能力，同时也让学生懂得对自己的上网行为负责任。

三、竞赛内容

本项目为中职生技能竞赛。结合教学要求和企业对技能的需要，重点考查学生网络安全、访问控制、安全认证配置、网络行为监控、网站安全防范等方面技能。主要涉及的知识和技能点如下：

本竞赛分为知识测试和技能实操二个竞赛部分，成绩比例是知识测试占20%，技能实操占80%；比赛时间共180分钟。

第一部分：知识测试

比赛时限：15分钟。

比赛技能：主要考查选手对网络信息安全知识的理解、判别和灵活运用程度，考查选手上网行为的规范和网络安全的职业素养。比赛

形式：在计算机上测试，由系统自动评改，完成共计 50 个题目的测试任务。考试题型为是非题、单选题及多选题，其中是非题共 40 分、每题 2 分，单选题共 40 分、每题 2 分，多选题共 20 分、每题 2 分

第二部分：技能实操

比赛时限：165 分钟。

比赛技能：重点考核内容分四个模块：网络搭建、应用系统与服务安全、上网行为管理、网站安全防范。

模块一 网络搭建 （实操的 20%）

网络基础知识:按照拓扑图结构,完成网络环境的设计与搭建(不用制作双绞线),并根据设计出的各台设备接口地址,连通内部网络。

以太局域网、无线局域网安全管理。

网络设备安全防范。

模块二 应用系统与服务安全（实操的 25%）

虚拟机安装系统，操作系统安全、数据库安全、应用服务安全保护等。

账号以及组织架构，能根据用户的角色，对文件、系统组件、系统工具、应用软件的访问控制权进行分配。使得不同角色的用户对不同的资源具有指定的操作权限。

证书认证防护，安装证书服务，根据需要颁发证书。提供给其他模块使用。配置系统认证服务的组件，设置终端用户接入认证服务。

VPN 服务，通过 VPN 接入内部网络。

Windows 系统，系统自带防火墙、进程与服务等安全。

Linux 系统，IPtables 防火墙及 SELinux 的配置，相关 Linux 服务安全等。

无线接入安全，作为无线客户端接入。

模块三 上网行为管理（实操的30%）

利用安全网关实现，流量管理，按用户分配带宽，应用控制，设定内部网络允许（或禁止）使用的网络应用。

内容审计，将通过WebMail或邮件客户端外发的信息记录，并执行相应的操作。网页过滤，能针对内网用户访问网站以及网页地址、内容进行分析,过滤非法网站和含有非法词汇的数据通信。行为分析，记录用户访问互联网应用或服务时所通信的内容。

模块四 网站安全防范（实操的25%）

安装PHP+MySQL，使用ZAP扫描工具，扫描基本的漏洞，并导出报告；在虚拟机成功发布作品，能通过工位IP访问；检测注入漏洞，通过注入获取非法操作权限；功能缺陷，授权管理；信息泄露，非法参数而导致信息泄露；防范脚本攻击；部署安全，数据库日常管理，文件权限；密码复杂度低、运行不必要服务、防火墙配置不当、不充分的日志记录、宽松的文件目录访问控制等。

四、竞赛方式

本赛项为**团体赛**，每支参赛队由2名同校在籍学生（其中队长1名）和不超过2名指导教师组成。参赛选手须为2016年度在籍中等职业学校（职业高中、普通中专、技工学校、成人中专）学生；五年制高职一至三年级（含三年级）学生可参加比赛，参赛选手年龄须不超过21周岁（即1995年7月1日及以后出生）。

五、竞赛流程

（一）比赛时间

比赛流程：先在计算机上进行理论考核，每队2人各做1套理论题，由计算机自动随机出题，自动计时和自动计算成绩（以2人的平

均分作为该队的理论成绩)；然后再进行技能实操比赛。

（二）比赛流程安排参考如下：

日程安排	
07:00-07:10	裁判进入裁判室
07:10-07:50	选手抽签并入场
07:50-08:00	参赛代表队就位并领取比赛任务
08:00-11:00	比赛时间（先做 15 分钟理论，再进行实操）
11:00-11:10	参赛代表队离场
12:00-18:00	裁判评分

六、竞赛试题

网络信息安全样题：

网络信息安全理论题部份（20%）

比赛时间：15 分钟

说明：理论题由计算机随机抽题，选手在计算机上独立完成并提交，考试时间由计算机计时（统一开始，时间一到自动结束），成绩也是计算机自动统计。

（一）单选题（共 20 题，每题 2 分）

1.在 NT 中，允许你使用只有个别用户和经过认证的恢复代理能够解密的密钥对保存在磁盘上的文件进行加密的系统是（ ）

A、EDS

B、EFS

C、ESS

D、SLL

2. _____，不得利用计算机信息系统从事危害国家利益、集体利

益和公民合法利益的活动，不得危害计算机信息系统的安全。（　）

A、除计算机专业技术人员外的任何人

B、除从事国家安全工作人员外的任何人

C、除未满 18 周岁未成年人外的任何人

D、任何组织或者个人

3.下面____验证方法是把用户帐号密码以明文形式传输的（ ）

A、基本验证

B、Windows 域服务器的简要验证

C、集成 Windows 验证

D、以上都不是

4.当选择无限制文件大小的方式作为日志记录的方式时，日志中不会包含（　）

A、日期

B、用户

C、类型

D、事件

5.包过滤防火墙利用_____对数据包实施有选择的通过，实现控制流出和流入网络的数据（ ）

A、地址

B、端口

C、协议类型

D、源地址、目标地址、端口号等

6.在_____情况下，防火墙会不起作用（ ）

A、内部网用户通过防火墙访问 Internet

B、内部网用户通过Modem拨号访问Internet

C、外部用户向内部用户发E-mail

D、外部用户通过防火墙访问Web 服务器

7.防火墙从防范方式和技术实现的角度可分为有_____（ ）

A、包过滤型防火墙和应用网关防火墙

B、包过滤防火墙和基于状态防火墙

C、代理服务型防火墙和状态监视型防火墙

D、包过滤防火墙、代理服务型防火墙和状态监视型防火墙

8.如何设置防火墙规则来防止极小数据段式攻击（Tiny Fragment Attacks)（ ）

A、丢弃协议类型为TCP，IP Fragment Offset等于1的数据包

B、丢弃协议类型为UDP，IP Fragment Offset等于1的数据包

C、丢弃协议类型为TCP，IP Fragment Offset等于0的数据包

D、丢弃协议类型为UDP，IP Fragment Offset等于0的数据包

9.防火墙采用_____方法对UDP数据进行包过滤，防火墙记住流出的UDP数据包,当一个UDP数据包要进入防火墙时，防火墙会判断它是否和流出的UDP数据包相匹配，如果匹配则允许进入，否则阻塞该数据包（ ）

A、动态数据包过滤

B、静态数据包过滤

C、状态数据包过滤

D、规则数据包过滤

10.丢弃所有来自路由器外部端口的使用内部源地址的数据包的方法是用来挫败（ ）

A、源路由攻击（Source Routing Attacks）

B、源 IP 地址欺骗式攻击(Source IP Address Spoofing Attacks)

C、Ping of Death

11.能防范 WEB 攻击的技术是（ ）

A、防火墙

B、IDS

C、隐患扫描

D、防病毒

12.入侵检测技术起源于___技术（ ）

A、网络管理

B、安全审计

C、防火墙

D、数据库

13.IDS 系统中____部件是存放各种中间和最终数据的地方（ ）

A、事件产生器

B、事件分析器

C、响应单元

D、事件数据库

14.下列____说法是错误的（ ）

A、将文件改为只读方式就不会感染病毒

B、病毒不会感染写保护的磁盘

C、磁盘文件损坏并不都是病毒所为

D、反病毒软件也不能随时随地防护所有病毒

15.关于包过滤防火墙说法错误的是（　　）。

A、包过滤防火墙通常根据数据包源地址、目的地址、端口号和协议类型等标志设置访问控制列表实施对数据包的过滤

B、包过滤防火墙可以有效防止利用应用程序漏洞进行的攻击

C、包过滤防火墙可以有效防止利用应用程序漏洞进行的攻击

D、由于要求逻辑的一致性、封堵端口的有效性和规则集的正确性，给过滤规则的制定和配置带来了复杂性，一般操作人员难以胜任管理，容易出现错误

16.关于应用代理网关防火墙说法正确的是（　　）。

A、基于软件的应用代理网关工作在 OSI 网络参考模型的网络层上，它采用应用协议代理服务的工作方式实施安全策略

B、一种服务需要一种代理模块，扩展服务较难

C、和包过滤防火墙相比，应用代理网关防火墙的处理速度更快

D、不支持对用户身份进行高级认证机制。一般只能依据包头信息，因此很容易受到“地址欺骗型”攻击

17.网站运行安全保障措施是（　）

A、网站服务器和其他计算机之间设置防火墙，做好安全策略，拒绝外来的恶意程序攻击，保障网站正常运行。

B、打开网站系统中的服务功能及相关端口。

C、交互式栏目不要有 IP 地址等识别确认功能。

D、不要留存访问日志。

18.某客户购买了一台安全网关（审计）设备，用来做上网行为的控制和审计，另外客户希望安全网关（审计）设备能替代内网的 DHCP 服务器，我们推荐安全网关（审计）采用什么部署模式？（ ）

A、路由模式

B、网桥模式

C、旁路模式

D、路由和网桥模式均可

19.客户内网安全网关（审计）的 IP 地址是 172.16.100.252，下列关于访问安全网关（审计）的方式，说法错误的是：（ ）

A、可以用 https://172.16.100.252 登录安全网关（审计）控制台

B、可以用 http://172.16.100.252:85 登录安全网关（审计）的内置数据中心

C、可以用 http://172.16.100.252 登录安全网关（审计）的认证页面

D、可以用 http://172.16.100.252:810 登录安全网关（审计）的外置数据中心

20.安全网关(审计)路由模式部署，下列哪些配置是正确的（ ）

A、选择“路由模式”，配置 LAN 口和 WAN1 口的 IP 地址，LAN 和 WAN1 口 IP 可以任意配置，也可以设置在同一个网段

B、选择“路由模式”，LAN 口和 DMZ 口的 IP 可以在同一网段，LAN 口和 WAN1 口不能在同一网段

C、选择“路由模式”，LAN，DMZ 和 WAN1 口 IP 均可以选择自动获得

D、选择“路由模式”，必须为 LAN 口和 WAN1 口分别配置两个不同网段的 IP 地址

（二）判断题（共 20 题，每题 2 分）

1.防火墙是设置在内部网络与外部网络（如互联网）之间，实施

访问控制策略的一个或一组系统。( )

2.组成自适应代理网关防火墙的基本要素有两个：自适应代理服务器（Adaptive Proxy Server）与动态包过滤器（Dynamic Packet Filter)。( )

3.软件防火墙就是指个人防火墙。( )

4.网络地址端口转换（NAPT）把内部地址映射到外部网络的一个IP地址的不同端口上。( )

5.防火墙提供的透明工作模式，是指防火墙工作在数据链路层，类似于一个网桥。因此，不需要用户对网络的拓扑做出任何调整就可以把防火墙接入网络。( )

6.针对入侵者采取措施是主动响应中最好的响应措施。( )

7.在早期大多数的入侵检测系统中，入侵响应都属于被动响应。( )

8.性能“瓶颈”是当前入侵防御系统面临的一个挑战。( )

9.漏报率，是指系统把把正常行为作为入侵攻击而进行报警的概率。( )

10.与入侵检测系统不同，入侵防御系统采用在线（inline）方式运行。( )

11.蜜罐技术是一种被动响应措施。( )

12.企业应考虑综合使用基于网络的入侵检测系统和基于主机的入侵检测系统来保护企业网络。在进行分阶段部署时，首先部署基于网络的入侵检测系统，因为它通常最容易安装和维护，接下来部署基于主机的入侵检测系统来保护至关重要的服务器。( )

13.入侵检测系统可以弥补企业安全防御系统中的安全缺陷和漏

洞。( )

14.使用误用检测技术的入侵检测系统很难检测到新的攻击行为和原有攻击行为的变种。( )

15.网桥模式部署，必须将安全网关（审计）设备的 LAN 口连接内网三层交换机，WAN 口连接防火墙。( )

16.按照国家有关规定，网站将保存 3 月内系统运行日志和用户使用日志记录。( )

17.入侵检测技术是用于检测任何损害或企图损害系统的机密性、完整性或可用性等行为的一种网络安全技术。( )

18.主动响应和被动响应是相互对立的，不能同时采用。( )

19.异常入侵检测的前提条件是入侵性活动集作为异常活动集的子集，而理想状况是异常活动集与入侵性活动集相等。( )

20.QQ 是与朋友联机聊天的好工具，不必担心病毒。( )

（三）多选题（共 10 题，每题 2 分）

1.安全帐户管理(SAM)数据库可以由以下____用户复制

A、Administrator 帐户

B、Administrator 组中的所有成员

C、备份操作员

D、服务器操作员

2.服务器操作员关于帐户的管理，下列做法正确的有___

A、审计你系统上的帐号，建立一个使用者列表

B、制定管理制度，规范增加帐号的操作，及时移走不再使用的帐号

C、经常检查确认有没有增加新的帐号，不使用的帐号是否已被

删除

D、对所有的帐号运行口令破解工具，以寻找弱口令或没有口令的帐号

3.通过日志分析，我们可以得到_____

A、系统崩溃的原因

B、黑客攻击的踪迹

C、系统的运转状况

D、系统服务的运转是否正常

4.防火墙的目的有以下_____方面

A、限制他人进入内部网络

B、过滤掉不安全的服务和非法用户

C、防止入侵者接近你的防御设施

D、限定人们访问特殊站点

E、为监视局域网安全提供方便

5.入侵检测系统的常用的响应方法包括____

A、发警报

B、写日志文件

C、联动防火墙

D、切断电源

6.下列那些可以作为 IDS 信息收集的对象_____

A、系统和网络日志文件

B、目录和文件中的不期望的改变

C、程序执行中的不期望行为

D、物理形式的入侵信息

7.某公司需求如下：公司普通员工上网需要限制下载以及监控发帖和邮件内容，所以普通员工修改电脑 IP 后不允许上网。公司领导可以在公司任何电脑上网，并且领导上网的时候不受到任何监控。以下关于通过安全网关（审计）设备实现客户需求的说法，错误的是_____

A、无法实现该需求

B、需要启用准入功能才能实现该客户需求

C、普通员工采用绑定 IP/MAC 的认证方式，领导使用防监控 KEY 的认证方式

D、普通员工采用用户名密码和 MAC 地址绑定的认证方式，领导使用防监控 KEY 的认证方式

8.行为监测法的特点包括：_____

A、可发现未知病毒

B、误报警

C、不能识别病毒名称

D、能对付隐蔽型病毒

9.受染文件存在服务器有以下_____原因

A、受染文件直接由工作站拷贝至服务器

B、由服务器自己的可移动媒介复制到硬盘上

C、一个带有受染文件的备份被恢复至系统

D、病毒由服务器的通讯端口传入系统

10.在网络中都需要在____平台上部署防病毒软件

A、客户端

B、邮件服务器

C、其他服务器

D、网关

网络信息安全实操题部份（80%）

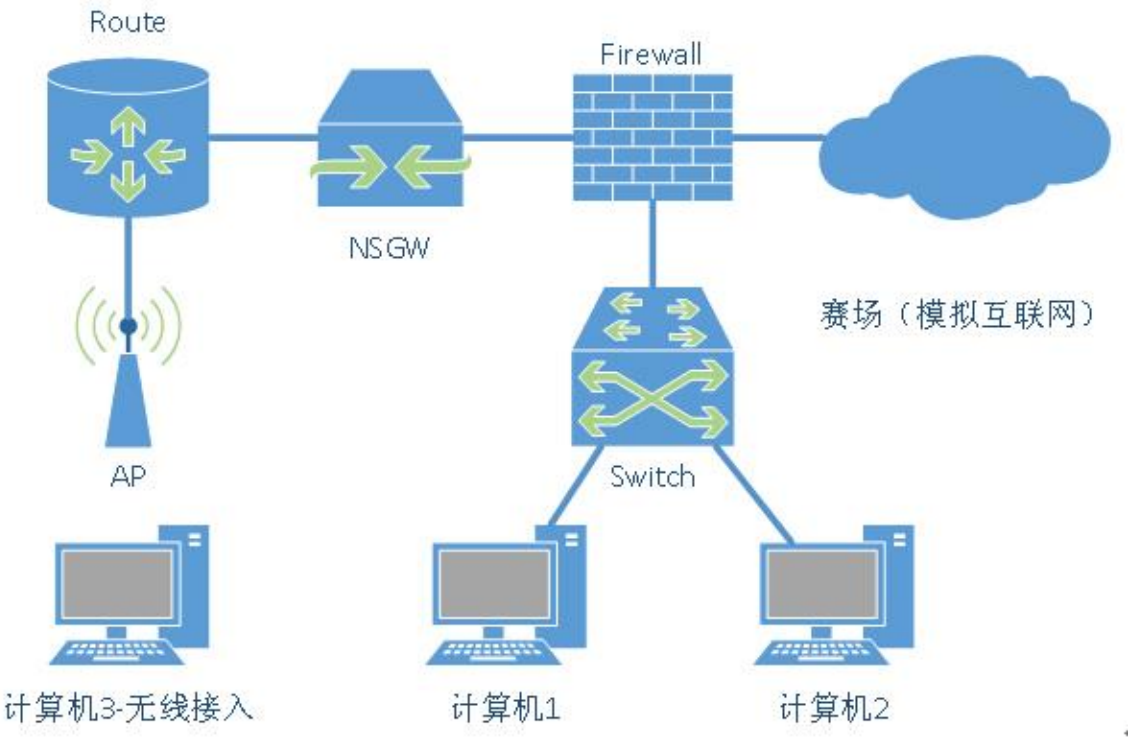
比赛时间：165 分钟

浪都信息服务集团为了建立一个更安全的办公网络环境，准备通过建设一个项目实现对网络进行升级改造。项目主要内容如下。

（一）网络搭建与网络环境安全（25%）

交换机与路由器设置完成后，将配置内容导出。

按照拓扑结构图，连接小组内部网络。（20 分）



根据地址规划表配置各设备名称，接口地址，使得网络连通。（20 分）

设备	设备接口	接口地址	备注

Route	第一个以太口	172.16.10.1/24	上联行为安全网关
	第二个以太口	192.168.1.254/24	下联无线接入点
Firewall	第二个以太口	67.58.203.X/24	模拟互联网
	第三个以太口	172.16.3.2/30	下联三层交换机
	第四个以太口	172.16.10.254/24	下联行为安全网关
Switch	以太口 24	172.16.3.1/30	上联防火墙
NSGW	以太口 1	172.16.10.253/24	下联路由器
	以太口 2		上联防火墙
AP	以太口	192.168.1.1/24	上联路由器

办公室内部创建 OSPF 实例 1，区域 0。保证办公室内部全网连通。【将防火墙设置 OSPF 的界面截屏保存为 FW4】（35 分）

防火墙将第四个以太口接口归入 Trust 区域。将第二个以太口归入 Untrust 区域。将第三个以太口归入 DMZ 区域。【将防火墙接口地址设置与区域划分结果界面截屏保存为 FW5-Y，其中 Y 表示序号，如第一张截屏命名为 FW5-1，第二张命名为 FW5-2。下同】（30 分）

防火墙第二个以太口作为办公室的互联网出口，办公室内部计算机以 NAT 方式访问互联网。（35 分）

将 Switch 的 1-20 端口划分到 VLAN10，地址范围 172.16.1.1-254，网关接口地址 172.16.1.254。（30 分）

办公室内部使用无线网路构建办公环境。AP 以胖模式工作。无线网络设计一个 VLAN，使用 192.168.100.0/24 网段。SSID 为 LDOfficeX（X 为工位号，下同）。使用 WPA 加密，密码 LDOffice2014。为接入无线网络的计算机自动分配地址。【将无线 AP 以太口配置界面截屏保存命名为 WF3-1；将设置 SSID 界面截屏保存为 WF3-2；将设置

加密方式的界面截屏保存为 WF3-3；将 DHCP 设置的界面截屏保存为 3-4】（50 分）

将 67.58.203.X 的 80 端口、MySQL 数据库访问端口，远程桌面端口影射到 172.16.1.4/24 的对应端口。其余另有额外的映射规则请根据题目后续内容进行设定。【将防火墙端口影射设置界面截屏保存为 FW7-Y】（30 分）

（二）应用系统与服务安全（25%）

虚拟机系统的配置截屏保存在对应的实体主机桌面的文件夹“服务安全”中。

在计算机 1 的 VirtualBox 添加以下虚拟机。

计算机名：DCSERVER；安装 WindowsServer2008R2；设定 IP 为 172.16.1.1/24；网关 172.16.1.254；DNS 172.16.1.1 。【将 DCSERVER 的控制面板-属性界面截屏保存为 S1-1】（10 分）

在计算机 2 的 VirtualBox 中添加如下虚拟机。

计算机名：VPNSERVER；安装 WindowsServer2008R2；IP 172.16.1.3/24；网关 172.16.1.254；DNS 172.16.1.1 【将 VPNSERVER 的控制面板-属性界面截屏保存为 S2-1】（10 分）

计算机名：WEBSERVER；安装 WindowsServer2008R2；IP 172.16.1.4/24；网关 172.16.1.254；DNS 172.16.1.1 。【将 WEBSERVER 的控制面板-属性界面截屏保存为 S2-2】（10 分）

将计算机 3 利用无线网路接入办公室环境，自动获取 IP。（15 分）

将 DCServer 升级为域控制器，域名 LDGroupX.com。【升级域完成后的系统属性-计算机名称界面截屏保存为 S4-1】（15 分）

集团的员工结构如下表所示。请根据区域划分组织单元，根据职

位划分工作组，创建集团的域用户结构。（45 分）

区域 / 职位	Zongbu	Ouzhou	Meiguo
Jingli	Zbjl	Ozjl	Mgjl
Zhuguan	Zbag1	Ozzg1	Mgzg1
	Zbag2	Ozzg2	Mgzg2
Zhiyuan	Zgzy1	Ozzy1	Mgzy1
	Zgzy2	Ozzy2	Mgzy2
	Zgzy3	Ozzy3	Mgzy3

【将显示 Jingli 组的成员列表界面截屏保存为 S5-1。将显示 Zhuguan 组的成员列表界面截屏保存为 S2-2。将显示 Zhiyuan 组的成员列表界面截屏保存为 S5-3。】

在 Zhiyuan 的用户禁止访问控制面板，并在开始菜单删除“图片”和“音乐”。【将控制面板管理的设置截屏保存为 S6-1。将开始菜单管理的设置界面截屏保存为 S6-2。】（40 分）

将 VPNServer 加入 LDGroupX.com 域作为域成员。配置 VPN 服务，允许 jingli 组的用户在互联网通过 VPN 拨号 67.58.203.X 登录进入集团总部的网络。通过 VPN 拨入的计算机静态分配 IP 范围 172.16.1.100-150。身份验证方式使用 MS-CHAPv2。注意需要将 VPN 的通信端口 1723 影射到 VPNServer 对应端口。【将 VPNServer 加入域后的系统属性-计算机截屏保存为 A4-1。将 VPN 地址分配设置界面截屏保存为 A4-2。将身份验证方式设置界面截屏保存为 A4-3。将设置

支持 VPN 拨入的用户组界面截屏保存为 A4-4】（70 分）

WEBServer 开启系统防火墙，添加规则启动数据库服务端口，Web 服务端口、远程桌面端口的访问许可。【将数据库相关规则属性的常规选项页截屏保存为 A5-1；将数据库相关规则属性的协议与端口选项页截屏保存为 A5-2；将 Web 服务相关规则属性的常规选项页截屏保存为 A5-3；将远程桌面相关规则属性的常规选项页截屏保存为 A5-4。】（35 分）

（三）上网行为管理（30%）

相关截屏文件保存在计算机 2 桌面的文件夹“上网行为管理”中。

以太口 1 与以太口 2 组合成为网桥，网关地址为防火墙对应接口地址。【将网口组合的设置界面截屏保存为 SG1-1；将网桥网关设置界面截屏保存为 SG1-2】（10 分）

办公室租用 ISP 带宽为下行 8MB，上行 1M。设置线路带宽利用率为 75%或以下表示空闲。启动线路繁忙保护，线路带宽使用率为 90%表示繁忙。【将带宽设置的界面截屏保存为 SG2-1；将线路利用率设置界面截屏保存为 SG2-2】（20 分）

全天禁止办公室用户访问视频网站。【将相关系列的设置界面截屏保存为 SG3-Y。其中 Y 表示序号，如第一张截屏命名为 SG3-1，第二张命名为 SG3-2。下同】（30 分）

禁止办公室用户在 9 点-17 点使用 p2p 软件。【将相关系列的设置界面截屏保存为 SG4-Y。】（30 分）

屏蔽网页正文内容有敏感词“战争”的网站。【将相关系列的设置界面截屏保存为 SG7-Y。】（30 分）

审计所有办公室用户在 WebBBS 发布的内容，WebMail 邮件内容

和附件内容。【将相关系列的设置界面截屏保存为 SG8-Y。】（40 分）

对于办公室用户外发的含有关键字“图纸”的电子邮件进行延迟审计。延时审计时间 25 分钟，超时不外发。【将相关系列的设置界面截屏保存为 SG9-Y。】（40 分）

模拟互联网中，有一个 BBS 站点，地址 bbs.nsexample.net，登录账号和密码均为 UserX。登录 BBS，在“信息安全讨论”栏目中发一张帖，标题“X 组选手报到”，内容为“X 组选手访问 BBS”。【将发帖操作完成的界面截屏保存为 SG10-1】（30 分）

模拟互联网中,有一台 WebMail 服务器地址 mail.nsexample.net，登录账号和密码均为 UserX。请登录邮箱，并向管理员 admin 发送一封邮件，主题:“X 小组测试邮件”，内容:“X 小组向大会报到”。【将已发邮件内容的界面截屏保存为 SG11-1】（30 分）

登录邮箱，向管理员发送一封邮件，主题为“最新设计”，内容为“新产品设计图纸”。【将已发邮件内容的界面截屏保存为 SG12-1】（30 分）

导出审计系统从比赛开始 2 小时 45 分钟内的流量统计信息、审计日志总体情况。【流量统计信息导出的文件命名为 SG13-1，审计日志总体信息导出的文件命名为 SG13-2】（20 分）

（四）网站安全（25%）

注意：不得改变原有系统的功能、站点结构和网页的命名。

NSWeb.rar 是一个具有若干安全漏洞的不完善的内容发布系统，请按照题目要求尽量找出漏洞并有效修复。修复完成后在 WebServer 中搭建环境，发布成品。（20 分）

用户登录验证功能有注入漏洞，可能导致非法绕过登录验证，请

修复漏洞。（50 分）

新闻管理模块存在 XSS 脚本攻击漏洞，请修复避免让非法用户利用脚本进行攻击。（50 分）

信息系统在用户密码存放上存在敏感信息泄露的威胁，请修复该漏洞的威胁。（50 分）

新闻管理模块存在功能级访问控制缺失漏洞。应该只有管理员才能进入改模块进行新闻管理。请修复该漏洞。（50 分）

发布作品时注意完善网站的默认路径、管理员账号及密码。（30 分）

若评委无法通过 http://67.58.203.X 访问你的成品，网站安全项目整体不作评分。

七、竞赛规则

（一）竞赛工位通过抽签决定，竞赛期间参赛选手不得离开竞赛工位。

（二）参赛选手不得自带软件、移动存储、辅助工具、移动通信工具及其他电子和纸界文档资料等进入竞赛现场，否则取消比赛成绩。

（三）参赛队自行决定选手分工、工作程序和时间安排。

（四）参赛队在赛前 10 分钟进入竞赛工位并领取竞赛任务，竞赛正式开始后方可进行相关操作。竞赛时间到，参赛选手必须停止操作。

（五）竞赛过程中，选手须严格遵守操作规程，确保人身及设备安全，并接受裁判员的监督和警示。若因选手因素造成设备故障或损坏，无法继续竞赛，裁判长有权决定终止该队竞赛；若因非选手个人因素造成设备故障，由裁判长视具体情况做出裁决。

（六）竞赛过程中，选手如果有问题，请即时举手反映，否则影响成绩自己负责。

（七）竞赛结束（或提前完成）后，参赛队要确认已成功提交所有竞赛资料，且参赛队队长签字确认，参赛队在确认前不得离场。

八、竞赛环境

(1)供评委使用环境要求：

两台服务器（双核 2.5GHz 以上，8G 内存），2-3 台裁判用机（与参赛选手设备硬件功能相同的计算机），一台打印机，二台 24 口三层交换机（恢复原厂设定）作为赛场交换机。

赛场应用服务器安装 Windows Server 2008 系统。安装 Virtual Box 虚拟机软件，Office 2010 系列，搜狗输入法。

赛场理论考试服务器安装 Windows Server 2003 系统，安装好 Office 软件，搜狗输入法，谷歌浏览器。裁判用机安装软件与选手用机一致。

(2)选手工位：

三台计算机,其中 2 台配备无线网卡。三台计算机软件配置一致：安装 win7 系统,安装 Virtual Box、Office 2010 套件、Dreamweaver、Apache、MySQL。将竞赛指定的全部软件的安装包保存在磁盘中。承办单位应提供 3%的备用设备。

2.赛位设置

选手工位间隔：每组选手工位前后距离为 4.5 米，左右距离为 2.5 米，保持工位间有足够的操作空间和通道。

3.单位赛位大小

每单位赛位长为 1.8 米、宽为 0.8 米、高为 1.8 米。

4.安全防范措施

电源需接地保护，每组设单独漏电保护开关。

九、技术规范

网络信息安全主要有以下国家标准，参赛代表队在实施竞赛项目中要求遵循如下规范：

（一）GB/T 22081-2008 《信息技术 信息安全管理实用规则》。

（二）GB/T 20010-2005《信息安全技术 包过滤防火墙评估准则》。

（三）GB/T 20270-2006《信息安全技术 网络基础安全技术要求》。

（四）GB/T 20272-2006《信息安全技术 操作系统安全技术要求》。

（五）GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》。

（六）GB/T 28454-2012 《信息技术 入侵检测系统的选择、部署和操作》

（七）GB/T 25068.1-2012 《信息技术 IT 网络安全 第 1 部分：网络安全管理》。

（八）GB/T 25068.2-2012 《信息技术 IT 网络安全 第 2 部分：网络安全体系结构》

（九）GB/T 25068.3-2010 《信息技术 IT 网络安全 第 3 部分：使用安全网关的网间通信安全保护》

（十）GB/T 25068.4-2010 《信息技术 IT 网络安全 第 4 部分：远程接入的安全保护》

（十一）GB/T 25068.5-2010 《信息技术 IT 网络安全 第 5 部分：使用虚拟专用网的跨网通信安全保护》

（十二）GB/T 22080-2008 《信息技术 信息安全管理体系要求》

（十三）《中华人民共和国计算机信息系统安全保护条例》（国务院令第 147 号）。

（十四）《中华人民共和国计算机信息网络国际联网安全保护管理办法》（公安部令第 33 号）。

十、技术平台

本项目比赛使用通用联网的计算机硬件、网络设备与软件系统作为比赛器材，具体要求如下：

（一）竞赛硬件技术平台

1 台路由器：利用路由器实现骨干网络的互联。

1 台三层交换机：构建本地核心网络。

1 台无线 AP：构建无线网络。

1 台电源适配器：向无线 AP 供电。

1 台防火墙：对安全的威胁进行防护，构建安全等级防护网络。

1 台安全网关：安全配置及防范。

1 台 38U 的网络机架（含 PDU 电源 1 个，标准网线若干条）：安装网络设备。

3 台计算机（参考参数：CPU 双核，内存>=4GB，硬盘>=320GB，其中至少有 2 台配备无线网卡）。

(1)网络信息安全项目的网络设备参考型号如下表：

序号	设备名称	设备型号	每队数量
1	路由器	RG-RSR20-14E	1 台
2	三层交换机	RG-S3760E-24	1 台
3	防火墙	RG-WALL1600-S3100	1 台
4	无线 AP	RG-AP3220	1 个
5	电源适配器	RG-E-120	1 台
6	安全网关	广东唯康 VSG-350A	1 台
7	网络机架	广东唯康 VGZSJ-3A	1 台
8	计算机（有 2 台含无线网卡）	CPU 双核，内存>=4GB，硬盘>=320GB。	3 台

（2）竞赛使用的软件环境

序号	品牌	型号	技术参数	参考价格
1	微软	Windows XP 专业版 (中文版)	试用版	——
2	微软	Windows 7 专业版(中文版)	试用版	——
3	Oracle	Oracle VM VirtualBox 4.3	免费版	——
4	Rar	RAR 4.0 (中文版)	免费版	——
5	微软	Microsoft Office 2010(中文版)	试用版	——
6	微软	Microsoft Visio 2010(中文版)	试用版	——
7	微软	Windows 2003 Server R2(中文版)	试用版	——
8	微软	Windows Server 2008 R2(中文版)	试用版	——
9	Redhat	CentOS 6.5	免费	——
10	ASF	Apache 2.2	免费	——
11	PHP	PHP 5.3	免费	——
12	Oracle	Mysql 5.5	免费	——
13	Notepad++	Notepad++ 6.0 或以上	免费	——
14	Adobe	Dreamweaver CS6 中文版	试用版	——
15	微软	超级终端压缩包（从 XP 提取）	免费	——
16	微软	Microsoft Visual C++ 2008SP1 Redistributable Package (x86)	免费	——
17	OWASP	Zed attack proxy 2.3（网站应用程序漏洞扫描工具）	免费	——
18	Oracle	JRE 1.7	免费	——
19	腾讯	Foxmail 7	免费	——
20	唯康	VTE-1A 网络信息安全考试系统	广东唯康提供	

其中：VTE-1A 网络信息安全考试系统是广东唯康教育科技股份有限公司提供的计算机在线考试系统，它具有随机抽题组成试卷和在线测试，自动计时和自动评改并统计成绩等功能。

十一、成绩评定

本赛项评分细则：本项目的技能实操基本是客观分，选手完成就

得分，没有完成或操作错误就不得分。理论部分机考评分，即由计算机即时自动评改。

技能实操题评分方法：本赛项成立裁判组，负责共同评改某一技能模块，分模块计分，然后按权重比计算得出总分。

本项目评分标准：理论分占 20%，技能实操分占 80%；

理论考核的评分方法：

理论题建立约 500 题以上的题目库并公开，竞赛时在该理论题库随机抽出是非题 20 题，单选题 20 题，多选题 10 题作为考试题；理论考试采用计算机在线答卷，由计算机自动改卷。

实操考核的评分方法：评分表中的每个评分点的得分，**只能是“零分”或该项所示分值的 “满分”**；也就是说，选手完成每个评分点项就得分，没有完成或操作错误就得零分。

如果总分相同，则实操分高的选手名次排在前面。

项目	名称	分值	权重
模块一	网络搭建与网络环境安全部分	200 分	20%
模块二	应用系统与服务安全	250 分	25%
模块三	上网行为管理	300 分	30%
模块四	网站安全	250 分	25%

十二、奖项设定

赛项设团体一、二、三等奖。以实际参赛总队数为基数，团体一、二、三等奖获奖比例分别为 10%、20%、30%（小数点后四舍五入）。获奖选手由大赛组委会颁发证书。

大赛组委会为奖得奖项团队的指导教师颁发“优秀指导教师证书”。

十三、赛项安全

（一）场地及消防设施：竞赛现场为教学机房，须符合消防安全要求。

（二）赛场电源必须接地，且配有漏电开关。

（三）疏散通道与紧急出口：疏散通道宽度应符合相关要求，通道交汇处需布置引导人员，现场需设置紧急疏散门并设置指引设备。

（四）采光与通风：赛场需保证空气流通、照明需符合教室采光规范。

（五）参赛人员安全与保健：竞赛现场需布置休息室、医务室，配备医生及急救药品。

（六）赛前组织专人对比赛现场进行考察，保证安全防范、赛场布置、赛场内的器材、设备等符合国家有关安全规定。

（七）赛场周围设立警戒线，防止无关人员进入，避免发生意外事件。

十四、申诉与仲裁

本赛项在比赛过程中若出现有失公正或有关人员违规等现象，代表队领队可在比赛结束后 2 小时之内向仲裁组提出书面申诉。大赛采取两级仲裁机制。赛项承办校设**仲裁工作组**，大赛组委会设**仲裁委员会**。赛项承办校仲裁工作组在接到申诉后的 2 小时内组织复议，并及时反馈复议结果。申诉方对复议结果仍有异议，可由各领队向大赛仲裁委员会提出申诉。大赛仲裁委员会的仲裁结果为最终结果。

十五、竞赛观摩

媒体观众可以在不打扰选手竞赛的要求下，沿现场指定观摩通道有组织地参观竞赛现场，了解网络信息安全技术及职业教育教学成果。

在赛场外布置开放式展区，对网络信息安全进行科普宣传，将网络信息安全技术应用在人们生活中的应用或者未来生活的应用对公众进行展现。

十六、竞赛视频

为保证公平、公正、公开，竞赛过程将全程录像，包括赛项的比赛过程、开闭幕式等，并制作优秀选手采访、优秀指导教师采访、裁判专家点评和企业人士采访视频资料，突出赛项的技能重点与优势特色。为宣传、仲裁、资源转化提供全面的信息资料。视频资料亦作为竞赛成果提交组委会，作为竞赛历史材料供后续赛项提高进行参考，选手竞赛过程可作为教学资料进行资源转换，促进相关专业教学发展。

十七、竞赛须知

1.参赛队须知

（1）参赛队名称：统一使用规定的学校代表队名称，不接受跨市、跨校组队报名。

（2）参赛队组成：每个参赛队由 2 名选手组成，其中队长 1 名，选手须为 2016 年同校在籍学生，性别和年级不限。

（3）指导教师：每个参赛队可配指导教师 2 名，指导教师经报名并通过资格审查后确定。

（4）每个参赛队可配领队 1 名，负责竞赛的协调工作。

（5）参赛选手在报名获得确认后，原则上不再更换。如在筹备过程中，选手因故不能参赛，参赛学校主管部门需出具书面说明并按相关参赛选手资格补充人员并接受审核。竞赛开始后，参赛队不得更换参赛选手，允许队员缺席比赛。

（6）参赛队不得携带任何设备、工具（包括通讯工具和存储设备等）、技术资料。竞赛过程中所需的设备、工具、技术资料全部由赛项承办校统一提供。

（7）参赛队在竞赛开始前一天，由赛项承办校统一安排抽取竞赛工位号，并由参赛队长对抽签结果签字确认。

（8）各参赛队应在竞赛开始前一天规定的时间段进入赛场熟悉环境，入场后，赛场工作人员与参赛选手共同确认操作条件及设备状况，设备、材料、工具清点后，由参赛队长签字认可。

（9）为防止参赛路途及竞赛过程意外的发生，建议参赛队领队、带队老师及参数选手等建议购买意外伤害保险。

2.指导教师须知

（1）各个参赛队的指导教师及领队不得进入比赛现场指导。

（2）指导教师不得在赛场外喧哗，影响赛场纪律。

（3）对比赛过程及结果有疑议者，应及时通过领队向仲裁长提出书面反映。

3.参赛选手须知

（1）参赛选手应严格遵守赛场规章、操作规程，保证人身及设备安全，接受裁判员的监督和警示，文明竞赛。

（2）参赛选手凭大赛组委会颁发的参赛凭证和有效身份证件（身份证、学生证）参加竞赛及相关活动，在赛场内操作期间应当始终佩带参赛凭证以备检查。

（3）参赛选手按规定时间进入竞赛场地，对现场条件进行确认并签字，按统一指令开始竞赛，在收到开赛信号前不得启动操作。各参赛队自行决定分工、工作程序和时间安排，在指定工位上完成竞赛项目。

（4）选手比赛时间内连续工作，食品、饮水等由赛场统一提供。选手休息、饮食及如厕时间均计算在比赛时间内。

（5）竞赛期间，选手不得提前离开赛场。如特殊原因（如身体不适等）无法继续参赛的，需举手请示裁判，经裁判同意后方可离开赛场。选手离开赛场后不得在场外逗留，也不得再返回赛场。

（6）竞赛结束时间到后，选手不得再进行任何与竞赛有关的操作。参赛队若提前结束比赛，应向裁判员举手示意，裁判员记录比赛完成时间。

（7）参赛选手须按照竞赛要求及规定提交竞赛结果及相关文件，禁止在竞赛成果上做任何与竞赛无关的标记，如单位名称、参赛者姓名等，否则视为作弊。

（8）参赛选手须严格遵守操作规程，确保人身及设备安全。竞赛期间，若因选手个人原因出现安全事件或设备故障不能进行竞赛的，由裁判组裁定其竞赛结束，保留竞赛资格，累计其有效竞赛成绩；非选手个人原因出现的设备故障，由裁判组做出裁决，可视具体情况给选手补足排除故障耗费时间。

（9）参赛选手须严格遵守赛场规章制度、服从裁判，文明竞赛。有作弊行为的，参赛队该项成绩为 0 分；如有不服从裁判、扰乱赛场秩序等不文明行为，按照相关规定扣减分数，情节严重的取消比赛资格和成绩。

（10）为培养技能型人才的工作风格，在参赛期间，选手应当注意保持工作环境及设备摆放，符合企业生产“5S”（即整理、整顿、清扫、清洁和素养）的原则，如果过于脏乱，裁判员有权酌情扣分。

4. 工作人员须知

（1）赛场工作人员由赛项承办校统一聘用并进行工作分工。

（2）服从大赛组委会的领导，遵守职业道德，坚持原则，按章办事，以高度负责的精神、严肃认真的态度和严谨细致的作风做好工作，为赛场提供有序的服务。

（3）必须佩带工作人员证件，仪表整洁，语言举止文明礼貌。

（4）熟悉《竞赛规程》，认真执行竞赛规则，严格按照工作程序和有关规定办事。

（5）坚守岗位，不迟到，不早退，不擅离职守。

（6）赛场工作人员要积极维护好赛场秩序，以利于参赛选手正常发挥水平。

（7）赛场工作人员在比赛中不回答选手提出的任何有关比赛技术问题，如遇争议问题，需上报执委会。

（8）违反规定，给竞赛带来恶劣影响或造成严重损失的，将给予必要的处理。

十八、教学资源转化建设方案

“以赛促教、以赛促改、以赛促学”是全国职业院校技能大

赛的重要目的。将竞赛内容成功转化为可教学化的资源无疑是实现这一目的的重要保障。为此，拟制定如下教学资源转化方案：

（一）网络与信息安全专业教学资源包

中等职业网络与信息安全专业教学资源包系统地梳理了网络与信息安全专业的培养目标、岗位需求、课程体系、核心知识点及竞赛考核内容与评分要点，并结合网络信息安全发展趋势对未来的竞赛内容设置进行预测。

（二）网络信息安全赛项案例集

将各省赛及国赛的竞赛内容进行分析汇总，形成行业应用案例，从而使赛题中的行业应用成为日常教学内容的载体。

（三）网络与信息安全专业系列教材

依托大赛，开发一套融入大赛思想的，体现“新设备、新技术、新标准”的实用型系列教材。2014 年组织中职一线教师、企业专家和大学教授编写了一套信息安全系列教材《网络信息安全教程》和《上网行为管理与网站安全防范》，并已在 2014 年 8 由广东海燕出版社正式出版；在 2015 年全国职业院校大赛的基础上结合赛项专家组和参赛指导老师的意见，于 2015 年 8 月经过修订第二版发行。