信息网络安全培训的总结（精选4篇）

篇1：信息网络安全培训的总结

安徽省20XX年高职教师计算机网络信息安全“双师宿州”培训在安徽职业技术学院举行，时间为7月21月30日。本次培训班教师都是来自行业或专业的资深专家，有着丰富的网络安全与攻防经验，帮助许多学校和企业进行了网络安全与病毒防范等相关工作的培训与指导，本人知识和技能经过培训学习获得了很大进步。

一、 完备的实训条件和培训计划让我受益匪浅。

首先，我要对安徽职业技术学院信息工程系的老师们冒着酷暑辛勤付出表示衷心感谢。特别是班主任董武对我们的无微不至的关怀，给我们宾至如归的感觉，让我们能够安心学习，没有任何后顾之忧。信息工程系的老师们，不但精心组织了资深专家教学，还给我们提供了条件完备的网络信息安全实训实验条件，所提供的国家示范性高职院校建设项月成果教材《网络安全与病毒防护》和《路由与交换技术》，为我们的学习提供了珍贵资料，让我们的实训更有针对性。

二、 在这十天的培训中，按照软件项目流程安排了丰富的学习内容。

既有专业教师的高屋建令瓦的讲授，也有来自企业的专家传经送宝；既有理论的深度广度，乂有实战的惊心动魄，既有教学的经验总结，乂有全国大赛的精彩分析，很我深有受益。本次培训学习内容包含五个方面：

1、 XX老师和XX老师结合国家示范性高职院校建设给我们就“专业建设”进行了言简意赅的分析说明。

2、 来自H3C的企业专家结合实际，给我们就“网络架构与路由配置”进行了详细介绍；另外，我们还专门考察了新华学院信息工程学院网络实验中心，有效的对所学知识进行了实地验证，加深理解。

3、 戴洁老师和孙武老师重点围绕《网络安全与病毒防护》课程的教学与实训等环节，结合实训室模拟教学系统，进行了深入浅出的讲授，就信息安全体系结构和主机系统加固、网络攻击与防御、病毒防御、密码学与认证技术和数据备份与灾难恢复分四个专题进行理论研讨和实训操作。戴洁老师所提供的实验实训案例，有效地化解了我们对知识重点和难点的掌握难度。

4、 唐笑林老师和李京文老师重点指导和演示了“网络攻防实战”，既有针对个人计算机及Web的入侵，乂有服务器提取权限的实战。通过实际的进攻，让我获得了丰富的实战经验，对所获得技能技巧有了更深刻的理解。

5、来自神州数码的王岳老师结合20XX年的全国高职学生信息安全大赛真题，对“入网检测技术”和大赛中所需要注意的技巧做了深入浅出的说明，并应学员的要求提供了大赛所需的实用工具软件。

三、本次学习我个人认为还是比较有价值的，开阔了视野，掌握了技能，也增进了对省内兄弟院校的了解。

通过系统的学习，本人收获很大：

1、 了解了更多的教学模式，加强了对网络信息安全课程教学改革的信心。

2、 提高了信息安全意识，更深刻的理解了信息安全威胁，掌握了相应的攻防技术，以及指导学生大赛需要注意的技巧和技能。

3、加深对常用安全检测工具的使用技巧技能的应用理解，获得了更多网络安全防护的工具软件。

本次培训学习也为我们提供了一次很好的交流平台。

在学习之余，我与其他院校的老师讨论了信息安全专业的教学以及本专业的发展规划和学生将来的就业情况，大家交流了自己学校的专业发展和教学方法、教学改革，教科研课题申报技巧等，还结识了不少新朋友，通过交流、沟通，交换意见，大家取长补短，相互学习，共同进步，所以说这。

篇2：信息网络安全培训的总结

20XX年11月8日，内蒙古电力信息通信中心举办了一期信息网络安全培训班，此次培训地点设在内蒙古电力培训中心，历时5天，至20XX年11月12日上午结束。在培训期间，我们学习了常用网络设备的实际操作，信息网络新技术在当今网络系统中的应用知识，以及生产系统和网络监控系统方面的内容。

通过学习我加深了对以往知识的理解，同时也了解了当今网络方面的新技术应用，还向受课老师请教了日常工作中遇到的疑难问题，感到受益菲浅。同时也看到了各单位同事们积极向上的学习劲头，深感自己存在的差距。紧张的学习过去了，现将学习的内容做了整理如下：

第一天交换机、路由器介绍

1、IOS是交换机及路由器的操作系统，通过tftp方式可以备份旧的IOS、删除旧的IOS、下载新的IOS、启动新的IOS；

2、交换机分类，基于layer2base，基于IPbase，基于IPSERVICES，基于ENTER

PRISESERVICES，可以实现基于二层网络和三层网络的数据流。

3、路由器IOS的更新，路由器的用途等。

4、路由器的查看命令，了解路由的基本配置方法。

第二天交换机、路由器配置

1、交换机的使用命令，配置名称、IP地址、启用接口模式、设置密码；

2、交换机间互连，配置trunk，启用vtp，查看日志基本信息；

3、建立vlan，配置IP地址，划分端口；

4、路由器的使用命令，设置密码，配置IP地址，开启路由。

第三天访问控制列表(ACL)配置、监控系统学习

1、使用交换机和路由器建立网络连接；

2、建立访问控制列表(ACL)，进行安全的网络配置；

3、监控系统介绍；

4、建立监控系统的网络拓扑；

5、使用监控系统进行网络管理。

第四天防火墙介绍、防火墙配置

1、登录ISG1000防火墙，使用netscreen用户名及密码登录系统具有系统管理员的相关权限；

2、进行防火墙的基本系统配置，可以通过图形化的访问介面进行相关配置，如系统升级、更新密码、权限配置；

3、端口、区域、虚拟路由的概念；

4、理解防火墙的区域概念、安全策略、VPN等概念。

第五天防火墙配置、生产系统介绍

1、trust区域、untrust区域、DMZ区域的关系trust区域用于连接内网系统的安全区域、untrust区域用于连接外网的不安全区域、DMZ区域用于接入服务器的安全区域；

2、在trust区域、untrust区域、DMZ区域之间进行网络策略配置；

3、安全策略的组成：源地址、目的地址、所使用的服务及端口号、对数据采取的行动、附加行动；

4、创建服务对象，配置策略的优先级，实现安全的网络的防护；

5、生产系统中所看到的各类管理界面的用途，一个工单流程中所经历的所有界面，常见问题的处理方法等。

篇3：信息网络安全培训的总结

随着信息技术的飞速发展和网络应用的不断普及，政府及企事业单位已经建立了良好的安全防范意识,拥有了抵御网络安全威胁的基本能力和硬件设施。但受利益驱使，针对数据、信息、身份等窃取为主的入侵攻击、机密信息泄露现象时有发生，网络管理和安全管理人员急需要了解渗透与防御技术的内幕知识，加强应急响应体系的科学构建，掌握丢失数据的恢复方法，全面提高信息安全防范的实用操作技能。因而，对于我们网络管理员而言，网络安全是我们必须掌握一门技术。所以能参加这次计算机培训，我感到很荣幸，故而倍加珍惜这次学习的机会。

本次培训主要任务是网络安全的技术特点和应用，以及系统安全漏洞引发的攻击分析和硬盘数据恢复，本次培训采用理论与实践相结合的培训方式，对我加深理论知识的理解非常有帮助。现将学习内容和心得总结如下：

1、网络扫描与风险评估

通过学习了网络扫描与风险评估技术，我掌握了OS扫描、端口扫描、漏洞扫描的相关知识，并可以熟练的操作XSCAN、NESSUS、NMAP等各类网络漏洞扫描器，从而通过这些扫描器可以有效的了解我院网络风险的各类故障，并可及时防范网络攻击故障。

2、网络嗅探技术及网络监控管理

网络嗅探技术是在应用层进行的分析底层网络数据的技术，通过利用数据包分析软件（Sniffer）截获网络数据包并进行分析。通过对网络嗅探技术的了解，明白了sniffer数据包分析软件可以听网络中的密码，观察网络运行情况，并进行网络故障排查，及时发现网络内外部攻击情况。

3、网络安全现状需求分析

通过学习网络安全现状需求分析，明确网络安全的作用；网络安全的趋势分析，明确未来网络安全的主要发展方向。学习了sniffer软件安装和使用，包括FTP明文抓包、http明文抓包、telnet明文抓包等网络攻击保护，明白了DOS攻击和DDOS攻击原理，并知道了如何对该网络攻击的防范。以及了解了目前网络中常见的网络钓鱼技术，懂得了如何识别常见网络钓鱼的手段，并分清真假网站。

4、硬盘数据恢复

通过学习硬盘数据恢复明白了数据恢复就是由硬件缺陷导致不可访问或不可获得、或由于误操作等各种原因导致丢失的数据还原成正常数据。通过这次学习了解了数据灾难的几种分类以及磁盘分区结构分析，并熟练掌握了常用的数据恢复软件DiskGenius和winhex等工具。

5、网络攻击模拟实践

根据网络攻击的基本过程，利用攻击软件完成网络扫描与网络监听、网络入侵、网络后门与网络隐身实现。理解了网络踩点、网络扫描和网络监听技术、社会工程学攻击、物理攻击、暴力攻击、漏洞攻击、缓冲区溢出攻击、网络后门的概念，掌握了使用Windows2000无密码登陆的方法登陆远程主机、用DOS命令进行IPC$入侵、IPC$入侵留后门的方法、IPC$入侵的防护知识、计算机木马特点及其危害性、信息隐藏技术等。

6、入侵检测系统与应用

入侵检测系统是防火墙的合理补充，防火墙之后的第二到安全阀门，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力提供了信息安全基础结构的完整性。从计算机网络系统中的若干关键点收集信息，并分析这些信息，在发现入侵行为与迹象后及时作出响应，包括切断网络连接、记录事件和报警等。并对网络进行监测，提供对外部攻击和误操作的实时保护。

总之通过这次安全培训，使我进一步加强了网络安全方面意识，业务知识与技术水平也有了一定程度的提高。因为有了培训老师的精彩视频与细致讲解，我学到了很多在书本上学不到的业务知识与技能，使我对网络安全有了整体的认识，对网络安全体系有了更深刻的理解，并顺利的通过了资格考试。

在此感谢辛勤工作的老师们，也感谢内蒙古农牧业科学院的各位领导，是你们为我提供了一个这么好的平台，谢谢！

篇4：信息网络安全培训的总结

网络安全是当代社会中非常重要的一个话题。为了提高员工对网络安全的认知和能力，我们进行了一次网络安全培训。以下是对此次培训的总结。

培训内容

我们的网络安全培训主要涵盖了以下几个方面：

1.网络威胁和攻击类型：我们学习了各种常见的网络威胁和攻击类型，包括病毒、恶意软件、网络钓鱼等。了解这些攻击类型有助于我们更好地识别和应对潜在的威胁。

2.密码和身份验证：我们学习了创建强密码的技巧，以及如何使用多因素身份验证来提高账户的安全性。这些措施可以有效地保护个人和公司的重要信息。

3.社交工程和网络钓鱼：我们了解到社交工程和网络钓鱼是网络攻击中常见的手段。通过学习如何辨别和避免这些欺诈行为，我们可以更好地保护自己和公司的利益。

4.安全浏览和电子邮件：我们学习了如何安全地使用网络浏览器和电子邮件客户端，以避免恶意软件和网络攻击。通过合理的浏览和邮件使用习惯，我们可以降低受到攻击的风险。

培训成果

通过此次网络安全培训，我们获得了许多知识和技能。以下是培训的几个成果：

1.提高了网络安全意识：我们了解到网络威胁的严重性，懂得如何保护个人和公司的信息安全。

2.学会了识别和应对威胁：我们学习了一些常见的威胁指示标志，可以在遇到潜在威胁时快速采取适当的措施。

3.了解了安全最佳实践：我们学习了如何创建强密码、使用多因素身份验证和安全地浏览互联网等最佳实践，可以帮助我们保持网络安全。

4.增强了团队合作能力：此次培训促使我们进行了团队合作和讨论，加强了我们之间的协作和交流能力。

后续行动

为了巩固培训成果并保持网络安全，我们计划采取以下行动：

1.定期更新密码：我们将定期更改密码，并确保密码具有足够的复杂性和安全性。

2.加强网络防护：我们会增强网络防火墙和安全软件的配置，并定期进行漏洞扫描和安全检查。

3.继续培训和宣传：我们将定期进行网络安全培训，并通过内部宣传活动提高员工的网络安全意识。

结论

此次网络安全培训对我们提高网络安全意识和能力非常有益。通过学习网络

威胁和攻击类型，以及掌握安全最佳实践，我们可以更加安全地使用互联网和电子设备。希望我们能够持续关注网络安全问题，并将所学知识应用于实际工作中。