**个人简历**

##### 1.基本信息

**基本信息** --突出自己的优势

姓名：x x x 性别： 男 出生日期：1988.1 团体成员：中共党员

毕业院校：广东工业大学 学历：硕士 专业：计算机应用 英语：CET-6

联系电话: 134xxxx8419 E-Mail： mazhiguo@163.com

##### 2.求职意向

**求职意向**  --与即将面试的岗位要完全一致

网络安全工程师/安全服务工程师/渗透测试工程师 –-三选一

##### 3.专业技能

**专业技能**  --随时调整，根据企业招聘的岗位要求酌情修改

1. 熟悉OSI模型、TCP/IP网络协议和HTTP、HTTPS、SMTP、FTP等应用协议
2. 熟悉Windows和linux操作系统和常用应用软件，能够进行日志分析和系统维护
3. 熟悉常用网络安全设备（如防火墙、堡垒机、态势感知、zabbix集群、IDS、IPS、WAF、防病毒网关等）的部署、策略配置和日常管理方法
4. 熟悉掌握网络安全法，等级保护2.0、风险评估等政策法规，熟悉等级保护定级备案和测评
5. 熟练掌握OWASP TOP 10 中常见的Web安全漏洞、业务逻辑漏洞原理、危害、利用方式及其修复方法
6. 熟悉渗透测试的流程、思路和方法，熟练使用常见的渗透测试工具，如Nmap、SQLMap、Burpsuite、Metasploit 、OpenVAS、AWVS、蚁剑、御剑等
7. 熟悉windows、linux系统、web容器安全以及数据库等安全基线检测和安全加固
8. 熟练编写各种安全文档，项目提交的资料等
9. 了解代码审计的步骤、工具和方法；有一定的代码编写能力，例如php、python

##### 4.工作经历

**工作经历** --注意时间要对应，岗位要相关，一个公司最好两年以上 【7】

**xxxx．xx~今 北京xxx网络科技有限公司 安全服务工程师**

**工作职责：** --根据自己掌握的知识酌情增加

1. 参与安全服务项目内部评估，并给出交付意见；

2. 项目的进度跟踪，项目的报告审查、交付；

3. 项目成果总结、统计分析和技术汇报；

4. 参与渗透测试、安全加固、应急响应、重要保障等安全服务工作；

5 跟进客户现场相关安全服务需求，并能及时响应；

6. 完成客户的安全运营相关服务，如安全风险评估、渗透测试、安全加固、漏洞扫描、基线检查、应急响应等相关内容，撰写相关安全服务项目报告；

**xxxx.xx~至今 XXXX信息科技有限公司 安全技术工程师**

**工作职责：** --根据自己掌握的知识酌情增加

1、负责XXXX网络安全设备的安装实施，售前沟通，方案制定，售后培训2、已售各种类型设备的定期巡检3、安全服务项目，如漏洞扫描，弱口令，配置核查等服务项目4、重保期间安全防护服务5、各类软件或监控项目部署实施培训6、参与大型网络等保建设集成项目，作为总包商，协调各分包商和客户资源共同完成项目**xxxx.xx~ xxxx.xx XXXXX信息科技有限公司 网络安全工程师工作职责：** --根据自己掌握的知识酌情增加

1. 负责XXXX项目的安全产品的运维和运营工作 2. 配置和维护SaaS化的安全产品（堡垒机、防火墙，云web应用防火墙、终端检测与响应系统、数据库审计、日志审计等14款安全产品）3. 解决客户在日常使用中遇到的问题**xxxx.xx~xxxx.xx 华安信息技术有限公司 安全运维工程师工作职责：** --根据自己掌握的知识酌情增加

1. 负责甲方重要网络设备的维护，包括核心交换机、边界防火墙等 2. 负责甲方网络安全的维护及安全事件的处理，拒绝服务攻击、黑客入侵等安全事故3. 针对甲方网络安全或风险问题，给出合理性建议，并完成修复与加固4. 日常例行检查；提供安全巡检报告5. 配合甲方技术人员对安全及网络设施等设备进行维护及优化**xxxx.xx~xxxx.xx 上海网域网络科技有限公司** IDC运维工程师**工作职责：** --根据自己掌握的知识酌情增加

1．负责德邦快递独立机房三百多台服务器的日常巡检2．及时发现故障统计报告通知客户，收到客户允许和客服工单后处理3．散户机房服务器设备，监控流量，防范DDOS攻击上报运营商封IP处理4．新旧设备上下架，准备环境，故障服务器更换硬件，提供客户要求的测试机器5．及时响应客户需求，提供增值服务**xxxx.xx~xxxx.xx 华际深圳电子系统有限公司 网络运维工程师工作职责：**--根据自己掌握的知识酌情增加1．负责公司与客户网络设备维护及管理2．负责对网络产品运营过程中的突发故障进行排查与处理3．负责网络架构搭建与配置4．负责网络设备的资源调配和系统安全，数据备份**xxxx.xx~xxxx.xx 广州双环网络科技有限公司 网络运维工程师工作职责：**--根据自己掌握的知识酌情增加1．负责公司计算机及自动化办公设备的维护及管理2．负责网络设备的资源调配和系统安全，数据备份3．负责对网络设备，服务器设备，操作系统运行状况进行监控4．负责对网络产品运营过程中的突发故障进行处理5．负责服务器的实施部署与搭建等等

##### 5.项目经验

**项目名称1：**XXXX教育集团数据安全解决方案

**项目时间**：xxxx年6月~xxxx年8月

**项目描述：**近期某教育集团下中心学员收到退费短信，告诉学员可以申请退款，但是需要先交纳X元的管理费。而且除学生外，公司的员工也收到了这样的短信。甚至，新学员信息刚录入2小时，学员就收到了诈骗短信。针对数据泄露的情况，我们初步分析这些数据泄露的原因可能来自于企业的各种Web应用管理系统。随后，针对公司的多个域名进行渗透测试，通过渗透测试发现了严重漏洞1个，高危漏洞3个，中危漏洞5个，并在漏洞测试过程中发现了黑客攻击的方式和痕迹。并且有针对性的采取了相应的安全加固方案，分别对主机和web应用进行安全加固，部署飞连办公终端安全系统，防止员工将敏感数据外传。同时，使用安恒数据库透明加密系统对数据加密。

**项目职责：**1.对xxx教育集团多个域名进行渗透测试

 2.对xxx教育集团制定并实施安全加固方案

**项目成果**：xxx教育集团数据安全方案实施后，新的学员和员工没有收到类似的诈骗信息，公司的数据信息得到了保障。

**项目名称2：**xxx财政局攻防演练

**项目时间**：xxxx年3月~xxxx年4月

**项目描述：**为深入贯彻落实习近平总书记关于网络强国的重要思想，按照做好两会、中国共产党第二十次全国代表大会（简称中共二十大）网络安全保障工作的相关工作部署，结合xxx财政局工作实际，根据主管单位通知本单位已被选中为本次攻防演习参演单位，要求上报在线业务系统做为攻击靶标，由国家组织的攻击队进行不破坏性的攻击行为，本单位做为防守方，演练真实环境下的防守与应急能力。

**项目职责：**

1.目标系统梳理和安全基线检测

2.使用OpenVAS对系统进行漏洞扫描，生成漏洞扫描报告

3.针对目标网站开展渗透测试，编写渗透测试报告

4.根据漏洞扫描结果和渗透测试报告进行安全加固化

5.通过流量分析发现攻击行为、初步确认攻击IP和行为，提交综合研判组分析、研判，撰写防守成果，通知应急处置组通过防火墙\CDN封禁攻击IP，应用处置组修复漏洞

**项目成果**：安全基线/配置检查报告、漏洞扫描报告、渗透测试报告、防守成果报告

**项目收获:**熟悉了护网的工作流程、安全基线检测检测工具的使用、漏洞扫描工具的使用、渗透测试的工作流程以及护网活动中蓝方的工作流程及工具的使用

**项目名称3：**国家公安部重点网络保护攻防演练两次(蓝队） **项目时间：**2019年6月~2020年10月**项目地点：**上海烟草集团、兴业银行上海支行、上海资信

**项目描述：**公安部通知指定客户单位定点接受攻防演练，我司提供设备和人工技术保障，以高分通过演练**项目职责：**

1、梳理客户单位网络资产，关闭一些老旧服务器对外通道2、对高危区域增加网络流量分析记录设备，人员驻场，及时响应处理疑似攻击行为等3、对内部网络进行全方位扫描探测，以规避明显的弱口令行为，关闭仍存在的高危端口4、接受国家烟草总局和人民银行总行的统一指挥，情报共享，严格控制互联网出口5、银行单位采用知道创宇云防平台，对各处网络节点进行监控，响应总行指挥统一调配，及时封堵阻截可疑IP5、以设备在前为主，人工响应在后的模式应对此次演练硬件设备：借给客户两台IPS、日志审计TSOC-SA大数据版、WAF、默安幻阵、绿盟IDS、奇安信天眼**项目结果：**2019年烟草集团、兴业银行两单位均以高分通过此次重保攻防演练，2020年上海资信未丢分，未被通报批评；但重保最后一天的下午15:00左右，红队通过内蒙古、新疆某地区银行，渗透进入金融行业内网，导致人行总行损失部分。 **项目名称4：**上海路政局ETC并网接入项目 **项目时间：**2019.11~2019.12**项目地点：**江桥ETC路网中心，省高速公路联网中心

**项目描述：**李克强总理在吉林作出指示，截止2020年，全国收费站ETC取代人工收费，我司作为总咨询公司入驻项目，需完成并网要求，并符合国家三级等保检查项。

**项目过程：**一个路段中心，130余收费站，1000余门架系统，数千人协同工作。根据会议调配，我参与项目负责江桥收费站、朱桥收费站的物理检查，与网络安全核查，一台业务用防火墙VPN模块接入，同时数百台设备进行漏洞扫描，基线安全检查。

硬件设备：项目总工包含1300余台天融信设备，每个路段包含固有设备，IDS、堡垒机、防火墙\*2**项目结果：**我司圆满完成此项目中的工作，获得客户褒奖，并出具感谢信**项目名称5：**闵行区卫计委等保建设集成项目 **项目时间：**2019.10~2019.12**项目地点：**闵行急救中心硬件设备：深信服设备---终端安全响应平台EDR，安全感知系统-探针，AF-1000-FA40核心防火墙，数据中心防火墙备机AF8.0.7R2。华为USG6570边界防火墙。H3C ：F1010出口防火墙+VPN模块，上网行为管理+准入控制ACG1000-AK230-L，日志审计CSAP-SA-AK640-L，数据库审计D2010-G**项目描述：** 为应对等保2.0，客户单位决定采购部分网络和安全设备，对内部网络进行升级改造，我司作为总包商进驻现场**项目过程：**基于客户对网络和业务的需求，重新设计了一份网络架构方案，根据此拓扑，统一调配各家厂商的实施工程师，有计划的实施各个设备，逐一上线测试，并满足等保2.0检查要求。配合上海测评中心的测评师进场测评。**项目结果：** 测评分数达到客户预期。**项目名称6：**上海公共研发服务平台三级等保集成建设项目（科委子公司） **项目时间：**2020.7 ~2020.8**项目地点：**钦州路100号**硬件设备：**华为NFW\*2，启明星辰日志审计\*1、堡垒机\*1、WAF\*1、数据库审计\*1、IDS\*1、深信服商密VPN\*1**项目描述：**客户单位的新上线的公共研发服务云平台要通过三级等保测评**项目过程：**从商务阶段结束之后，正式进驻现场，协调资源，各网络与安全厂商同心协作，按照三级等保的要求进行技术实施；我主要负责启明星辰设备的实施。项目结果： 等保测评已经结束，高分通过。证明还在走流程没有正式下来。**项目名称7：**上海仁恒置地集团终端安全建设项目 **项目时间：**2019.9~2019.11**项目地点**：丁香路，浦东仁恒置地总部**硬件设备：**奇安信天擎360终端安全管理系统（软件）**项目描述：**为保障集团内部终端信息安全，采购360天擎取代之前的国外开源软件 **项目过程：**以上海集团总部为总控制中心，全国16家分公司作为子控节点，购买5000终端资源，采用级联部署的方式远程实施，历时半月余，全部实施结束。 **项目结果：**除招投标、方案制定阶段外，全部实施过程，包括售后培训，由我一人完成，得到了客户信息部经理的高度赞扬，并给我司致一感谢邮件。**项目名称8：**上海疾病预防与控制中心安全运维项目 **项目时间**：2019.8~2019.10**项目地点**：中山西路1800号疾控中心硬件设备：zabbix软件集群监控部署**项目描述：**客户单位购买长期运维服务，由我司一人长期驻场运维，我担任项目经理，因客户性质特殊，此监控方案为附赠。**项目过程：**每周二次项目例会，参与配置变更研讨，需求分析，运维计划。并部署一整套zabbix的监控方案，监控上海市各分支机构网络节点，网络和安全设备、服务器资源。并为其实现邮件、微信告警功能。制定运维计划方案，确认工作界面，巡检工作范围等。**项目结果：**持续合作中。 此开源方案成功部署应用，为客户单位节约了大量预算，深得客户好评，2021年合同已经续签，客户对于我司的安全运维工作高度肯定。

**项目名称9**：2019国家护网-南网供电局蓝方

**参演单位：**防守方：电网公司，中国南方电网省公司，地洲供电局，县供电局及供电局个下属单位；攻击方：公安部，中国移动，各大安全厂商，渗透测试专家**项目简介：**一是增强对网络安全的认知，二是加强组织领导，各专业协同作战。三是强调边界防护，杜绝跨区互联。四是防护重点突出，保障重要系统。五是做好主动防御及监测预警，严格落实网络安全管控要求。确保内网边界不失守、等保三级及以上系统不被控、敏感数据不泄露。本次国家级的网络攻防演习是对公司网络安全防护水平的重大考验，前期各专业、各单位已经开展了大量相关的工作，行百里半九十，牢守公司网络安全防御底线，在本次网络安全大考中向国家交出满意答卷。

项目职责：

1.目标系统梳理和安全基线检测

2.使用OpenVAS对系统进行漏洞扫描，生成漏洞扫描报告

3.针对目标网站开展渗透测试，编写渗透测试报告

4.根据漏洞扫描结果和渗透测试报告进行安全加固化

5.通过流量分析发现攻击行为、初步确认攻击IP和行为，提交综合研判组分析、研判，撰写防守成果，通知应急处置组通过防火墙\CDN封禁攻击IP，应用处置组修复漏洞

**项目名称10：**地州供电局信息安全加固 **项目周期：**1年

**项目简介：**为了保障南网的网络安全，按照南网基线合规库标准进行基线合规检查和加固。对供电局内部30服务器，20个中间件，20个数据库，230台网络设备，2000台终端进行脆弱性扫描，向客户提供整体的安全整改方案，建立在业务优先的原则上最大限度的加强内网整体安全，做到1：系统的安全，2.动态的安全，无边界的安全，4，非传统的安全，保证内部信息的保密性，完整性，可用性。**项目流程：**对所有资产进行南网基线合规库标准进行加固，漏洞扫描并加固，高危端口封堵，IPS入侵防御系统检测，防火墙策略编写，应急方案编写。应急演练。准入系统编写策略。对下级单位开展信息安全督查。检查各下属单位对周局通报的漏洞整改情况。对检测到的危险立马进行处理，保证内部网络的安全和数据安全。落实3分技术，7分管理的安全管控原则。对二级系统进行自评估，对应完成在运二级系统的加固工作，三级系统到公安局备案。

**国家护网具体技术实施：--不用写到简历中，面试过程中的描述**

针对已停止原厂服务的在运老旧系统制定演习期间运行方式。对废弃、无主系统和设备进行下线处理。通过自检查表，统计排查各单位的互联网应用，完善互联网应用台账。采用技术手段对暴露在互联网上的设备、应用、数据库等网络资产进行排查评估，关闭不必要的主机、应用和服务。通过暴露面分析工具，对主域进行子域名发现，子域名发现通过主域名暴力破解、google hack、及全球实时DNS数据检索等检测，发现暴露互联网的子域名，对子域名进行Web指纹发现，发现是否存在风险的中间件或脚本框架，对域名进行WEB漏洞扫描。，清查托管在外的生产、开发及测试系统，对相关系统立即停运下线并清除数据。全面梳理清查各类网络边界，绘制网络拓扑图。对网络边界安全防护设备进行查漏补缺。清理边界无效过期或者过于宽泛的策略，封堵危险端，策略要求：1）根据业务需要将访问策略细化至IP和端口,访问策略应与系统运行方式一致； 2）策略中不允许出现any to any； 3）策略中不允许出现命中率为0的策略； 4）策略以置顶黑名单形式双向封堵高危端口和服务； 5）策略中不允许出现过宽地址段，如B类地址段； 6）对NAT后的I区地址实行严格的白名单访问控制；2、应封堵以下高危端口：TCP：135、139、445、3389；UDP：137、1383、操作系统、数据库、中间件的登录端口，应仅面向运维堡垒机及所需IP地址，不得向地址段开放弱口令检查：1、弱口令检测工具的检测字典：需要结合南方电网内部常使用密码或初始密码生成规则，及全国前100活跃密码。2、弱口令自检表：需注明是否存在弱口令、默认口令、通用口令等内容，发放到各事业部根据要求及自查表完成自查；3、4A平台登录方式：需检测是否已实现仅允许通过证书登录的双因子身份认证登录方式。按照公司信息安全合规库要求强制设置用户在7天内更改1次口令，对不符合要求用户进行锁定处理。网络拓扑排查：1、对网络拓扑图的合理性进行排查，确保不存在直接渗透内网核心系统的拓扑路径；在各边界部署安全设备，对安全设备的策略进行梳理、强化防护策略。建立有效的防护策略：1、防火墙有防扫描功能，需检测是否开启防扫描功能；2、需检测WAF是否对全网开启高级拦截策略，如过滤单引号，对multipartform-data请求，需要开启全规则过滤，封堵IP等，防止攻击方通过特珠手法绕过WAF进行入侵攻击。3、需检测IPS是否开启全规则拦截过滤，对规则有效性进行测试，防止攻击方通过特珠手法绕过WAF进行入侵攻击。形成网络安全布防图：对内网网络拓扑进行安全分析，检测是否存在互联网直接渗透内网核心系统的拓扑路径。梳理清查各类边界，梳理边界防护设备设施的访问控制策略，加强边界安全及收紧防护设备的访问控制策略。加强“社工”防御：编写网络安全意识培训PPT，以安全意识案例为主。对全员开展开安全意识教育。着重对易受“社工”突破的人员，如1000号客服，开展一次强化安全意识培训，补充完善网络安全责任书条款，组织全员签订网络安全责任书。加强基层人员安全意识教育，做好重点防护：做好主机精准防护，做好数据库精细管控，做好终端全面管控，做好泛终端全面管控，部署公安专业防护设备。

**项目名称11：达内TMOOC直播平台监控系统项目简介：**针对TMOOC直播平台的30多台服务器主机部署zabbix监控平台，集中监控Web服务可用性、数据库系统可用性，以及各服务器主机的CPU/内存/磁盘使用率/网卡流量等指标。**责任描述**：1.负责zabbix监控服务端的安装部署2.负责zabbix-agent的安装部署3.负责各被控主机的添加、监控项/触发器、邮件告警项目的设置4.负责监控图形制作、聚合图形及监控报告制作

##### 6.教育经历

--培训经历可以不写

##### 7.个人评价

--体现学习能力、抗压能力、团队合作精神