培训服务合同

合同编号:【　　】

甲方:【广东省通信产业服务有限公司广州分公司】
地址:【广州市天河区华景路1号办公楼（部位：8层B）】
法定代表人/负责人:【肖楚邈】

乙方:【广州中睿信息技术有限公司　】
地址:【广州市天河区翰景路1号1801房自编A、B、C房】
法定代表人/负责人:【鹿传明】

经友好平等协商，甲乙双方对培训事宜达成如下一致协议并共同遵照执行。

第一条 培训服务内容

1.1 培训目标:[为让学员了解最新的网络技术与网络安全形式,加深其对网络安全的理解,从本质上提高学员的网络安全知识水平]。

1.2 乙方负责下述培训服务工作:

（1）提供培训课程，包括但不限于聘用培训讲师、组织培训内容、教材、版权;

服务详细内容及对应价格见附件四。

1.3 乙方为本次培训提供设备为:/

1.4 乙方为本次培训提供的场地为:/

第二条 培训要求

2.1 培训地点为【东莞市】。

2.2 培训时间为【3】天，即自2023年9月23日至2023年12月31日内根据甲方需求开展课程，每期每课程授课3天，共1期，每天授课时间不少于【6】学时。

2.3 培训讲师为【张海杰】，具体培训内容及讲师介绍见附件二、附件

三。

2.4 未经甲方事先书面同意,乙方不得将服务事项全部或部分转交他人完成。乙方如需将部分工作交由第三人办理的，应事先征得甲方书面同意，并就该第三人的工作向甲方承担全部责任。

第三条 甲方权利与义务

3.1 甲方应与乙方共同协商培训内容、方式、效果及时间安排，并提前【15】天以上通知乙方；如有变动应提前【5】天以上通知乙方。

3.2 甲方应与乙方共同对培训内容（或对培训课程的总体规划）进行商讨、评估、跟踪和总结。

3.3 甲方有权利对乙方提交的教员资料及培训方案进行审核和确认。

3.4 甲方应向乙方提供培训需要的相关信息。

3.5 在培训实施期间，甲方应协助乙方对参培学员进行管理。

3.6 甲方指派【黄小莹】担任项目联络人，负责传达、下达甲方的指令及服务需求。

3.7 甲方应按时足额向乙方支付培训费用。

3.8 【/】。

第四条 乙方权利与义务

4.1 乙方须遵守甲方培训工作的相关规定和要求，并尽其所能确保培训质量和培训效果并接受甲方的服务质量考核。

4.2 乙方须提前 7 天以上向甲方提供培训课程大纲和学员教材的电子版等资料用于课前审核。

4.3 乙方指派【俞小芸】担任项目经理，负责会议现场联络、综合协调各项资源落实甲方的指令及服务需求、解决甲方现场问题；项目经理应与甲方代表进行及时、充分的沟通，推进培训服务工作；服从甲方的现场调度、安排，确保培训顺利进行；

4.4 乙方在从事甲方安排的培训任务过程中，须遵守国家法律法规和政策、甲方的相关制度与要求；履行职业操守，尊重甲方与受训学员。严禁乙方人员在课堂上谈论、发表、传播违背国家法律法规和政策，违背职业道德，损害甲方和受训学员利益和情感的言论，否则引起的一切后果由乙方自行承担并赔偿由此导致甲方的全部损失。

4.5 乙方应保证对其自带课程版权的完整拥有或已得到使用授权；如

在课程执行过程中与第三方产生版权纠纷，一切后果由乙方自行承担，由此导致的甲方损失乙方应予以全额赔付（包括甲方由此支出的律师费、诉讼费等合理费用）。

4.6 乙方应协助甲方进行培训调研，配合甲方进行培训效果评估和培训的后期跟踪服务。

4.7 培训时间确定后，非经甲方同意乙方不得擅自更改授课时间。

4.8 未经甲方书面允许，乙方不得向学员收取任何费用。

4.9 培训期间，乙方人员及乙方转交第三方完成的工作人员所引起的工伤、侵权、被侵权等所有责任，与甲方无关，由乙方负责处理并承担费用。

/

第五条 费用及支付

5.1 乙方就培训服务获得的报酬总额：人民币[27000]元，大写[人民币贰万柒仟元整]，包括：

（1）乙方提供的培训课程报酬。

（2）乙方为履行本合同第一条所述服务及培训相关的其他全部成本、费用。

（3）与本合同相关的所应缴纳的所有税费。

除另有约定外，甲方无需就本项目向乙方支付上述费用之外的其他任何费用。

5.2 支付方式和进度

（1）首付款

在本合同签订并生效，且收到乙方开具的相应金额的、符合国家规定的发票后[/]日内，甲方将本项目报酬总额的[/]%（即人民币[/]）支付给乙方。

（2）考核付款

乙方完成本合同约定的全部服务内容、达到甲方设定的第 1.1 款所述培训目标并经甲方考核且收到乙方开具的等额合规发票后 15 日内，甲方按照考核结果将考核款支付给乙方。

5.2.1 甲方在支付任何一期合同款前，有权要求乙方按付款数额向甲方开具符合国家法律法规和标准的增值税专用发票。乙方承诺其开具发票的形式与内容均合法、有效、完整、准确。若乙方不开具或开具发票不合格的，甲方有权不予付款直至乙方开具合格发票之日。乙方的各项合同义务仍应按合同约定履行。

5.2.2 乙方应在具备开票条件且接到甲方开票指令后开具发票，并应在开具发票之日起 10 个工作日内将增值税专用发票送达至甲方，每逾期一日，乙方应按逾期送达发票金额的万分之三支付违约金。甲方签收发票的日期为发票的送达日期。如乙方提供的增值税专用发票不符合法律法规要求或本合同约定，或不能通过税务认证的，甲方有权拒收或于发现问题后退回，乙方应及时更换，如因此导致逾期送达增值税专用发票的，乙方应当按照前述约定承担逾期送达的违约责任；若造成甲方无法抵扣的，乙方还应赔偿甲方由此遭受的损失，金额相当于逾期送达发票可抵扣金额。

5.2.3 由于乙方未足额缴纳应缴税款和开具发票不真实、不合格而引起的一切责任（包括商业责任和法律责任）和损失，由乙方承担，甲方有权对每张违规发票扣减 3000 元作为违约金。

5.2.4 如乙方主管税务机关未将其属于营改增范围的业务纳入增值税应税范围，乙方应承诺其业务被主管税务机关纳入增值税应税范围后向甲方提供增值税专用发票。

5.2.5 若乙方涉及免税事项应提供主管税务机关认定的相关证明材料。

5.2.6 双方银行账户信息和纳税人信息如下：

甲方：

户名：[广东省通信产业服务有限公司广州分公司]

账号：[7443900182600101320]

开户行：[中信银行广州花园支行]

统一社会信用代码：[91440101558395814K]

地址：[广州市天河区华景路 1 号南方通信大厦 8 楼]

电话：[020-38638000]

乙方：

户名：[广州中睿信息技术有限公司]

账号：[3602845009100024921]

开户行：[中国工商银行广州创展支行]

统一社会信用代码：[91440106661844913F]

地址：[广州市天河区翰景路1号1801房自编A、B、C房]

电话：[020-38931912]

5.3 培训结束之日起【7】 个工作日内，甲方向乙方出具《培训评估表》，甲方按照以下考核结果向乙方支付考核款：

（1）【90（含本数）】分以上，甲方全额付培训费；

（2）【80（含本数）--89】分，甲方付【“考核总分/100分”的比例】培训费；

【/】分，甲方付【/】培训费；

【80】分（不含本数）以下，甲方付【/】培训费或有权要求乙方无偿重新授课。

5.4 若根据本合同约定乙方应当支付违约金和/或承担赔偿责任，则甲方有权从上述任何一笔付款中直接扣除相应金额

第六条 知识产权、商业秘密及相关

（一）知识产权

6.1 对乙方提供的课程讲义、教学案例、电子板书等资料（下称培训资料），乙方保证拥有知识产权或合法使用权；甲方有权利用乙方提供的培训资料在甲方、甲方子公司或分公司内部进行再培训或进一步加工利用组织培训材料。

6.2 甲方有权对培训过程进行录音录像并且在甲方、甲方子公司或分公司内部利用录音录像资料进行再培训或组织员工集体学习。

6.3 乙方保证依本合同为甲方提供的服务及服务成果符合国家相关法律、法规和规章规定，不存在任何权利瑕疵。如果有人提出法律或行政程序(合称“侵权指控”)，声称甲方违反了国家相关法律、法规和规章规定或侵犯了其知识产权、其他人身及财产权利的，乙方应当负责解决，返还甲方已支付款项及按照同期中国人民银行贷款利率计付利息，并赔偿甲方就此所承担的一切损失和费用，包括但不限于上述侵权指控中所产生的诉讼费用、合理的律师费用、调查费用、罚金、和解金额或生效法律文书中规定的赔偿金额。

（二）商业秘密

6.4 乙方在为甲方实施培训过程中所获得的甲方提供的相关企业内部管理制度流程、经营信息、营销方式与策略、客户投诉案例、企业案例、客户名单等资料信息为甲方商业秘密。

6.5 乙方在甲方实施培训过程中所获得的甲方培训计划、培训课程内容、培训资源、学员名单等资料信息为甲方商业秘密。

6.6 本合同约定的甲方向乙方支付的培训费用等条款内容为甲方的商业秘密。

6.7 以上所述商业秘密，乙方应作为商业秘密予以保护，除本协议授权实施的行为外，不得将保密资料部分地或全部地对外披露。接受方可仅为本协议的目的向其确有知悉必要的雇员披露对方提供的保密资料，但同时须指示其雇员遵守本章规定的保密及不披露义务。接受方仅得为履行本协议之目的对保密资料进行复制。接受方应当在本协议终止或解除后时将保密资料原件全部返还披露方，并销毁所有复制件。接受方应当妥善保管保密资料，并对保密资料在接受方期间发生的被盗、泄露或其他有损保密资料保密性的事件承担全部责任，因此造成披露方损失的，接受方应负责赔偿。

6.8 如乙方违反本协议关于保密的约定，应赔偿因此而给甲方造成的一切损失。

6.9 本保密条款自保密资料提供或披露之日起至协议终止或解除后【10】年内有效

第七条 违约责任

7.1 任何一方未履行或未完全履行本合同项下的义务，均构成违约。违约方应赔偿因违约给对方造成的一切损失。

7.2 乙方未能按本合同约定按期并保质保量提供本项目下任一项服务的，每违反一项，乙方须向甲方支付该项目报酬总额15%的违约金；违约金不足以弥补损失的，乙方据实赔偿。

7.3 如乙方的违反导致甲方培训目标无法实现，甲方有权解除本合同，乙方应向甲方支付本合同总额的30%违约金，退还甲方已支付款项及按照同期中国人民银行贷款利率计付利息，并赔偿甲方的损失。

7.4 乙方违反本合同约定，提供服务不符合甲方要求的，由乙方负责根据甲方要求更正和修改，因此造成的所有损失和费用的增加由乙方负责。

如甲方提出更正或修改要求后7日内，乙方仍未满足甲方要求，则甲方有权终止本合同并不再支付本项目报酬；同时，乙方应退还甲方已支付款项及按照同期中国人民银行贷款利率计付利息，并赔偿甲方的相应损失。

第八条 法律适用和争议解决

8.1 本合同适用中华人民共和国法律。

8.2 所有因本合同有关的任何争议将通过双方友好协商解决。如果双方不能通过友好协商解决争议，则任何一方均可将该争议提交北海国际仲裁院，按照申请仲裁时该会的仲裁规则进行仲裁。仲裁语言为中文。仲裁裁决是终局的，对双方均有约束力。仲裁费用由败诉方承担。

8.3 仲裁进行过程中，双方将继续履行本合同未涉仲裁的其它部分。

第九条 合同生效及其他

9.1 本合同自双方签字盖章之日起生效。 合同有效期内发生地震、台风等不可抗力或讲师生病等意外事件，遭受事故方在提供有效证明文件并及时通知对方后可以终止合同或签订补充协议变更培训日期。

9.2 本合同一式[肆]份，甲乙双方各执[贰]份，具有同等法律效力。

9.3 如果本合同的任何条款在任何时候变成不合法、无效或不可强制执行而不从根本上影响本合同的效力时，本合同的其它条款不受影响。

9.4 本合同各条标题仅为提示之用，应以条文内容确定各方的权利义务。

9.5 未得到对方的书面许可，一方均不得以广告或在公共场合使用或摹仿对方的商业名称、商标、图案、服务标志、符号、代码、型号或缩写，任何一方均不得声称对对方的商业名称、商标、图案、服务标志、符号、代码、型号或缩写拥有所有权。

9.6 本合同的任何内容不应被视为或解释为双方之间具有合资、合伙、代理关系。

9.7 本合同替代此前双方所有关于本合同事项的口头或书面的纪要、备忘录、合同和协议。

9.8 甲乙双方因执行本合同或与本合同有关的一切的通知都必须按照本合同中的地址，以书面信函、传真、电子邮箱或双方约定的通讯方式进行。使用信函通知的应采用挂号信或者具有良好信誉的特快专递送达。如

使用传真或类似的通讯方式，通知日期即为通讯发出日期，如使用挂号信件或特快专递，通知日期即为邮件寄出日期并以邮戳为准。如使用电子邮件方式，电子邮件到达接受方指定电子邮箱的时间为通知送达时间。如果因接受方原因（包括但不限于接受方拒收书面信函、接受方传真机关闭或故障、接受方电子邮箱地址不存在或者邮箱已满或者设置拒收等）导致通知发送失败，视为通知已经送达（发送方侧载明的书面信函寄出时间或者传真发送时间或者电子邮件发送时间视为通知送达时间）。仲裁法律文书适用于本条款约定。

如致甲方：

联系人：【毕文哲】　　电子邮箱：【biwzh@iter.cn】

电话：【020-83888072】　　传真：【/】

地址：【广州市天河区华景路 1 号办公楼（部位：8 层 B）】

邮政编码：【510000】

如致乙方：

联系人：【俞小芸】　　电子邮箱：【/】

电话：【15800025515】　　传真：【/】

地址：【广州市天河区翰景路 1 号 18 楼】

邮政编码：【510000】

9.9 附件为本合同不可分割的部分。若附件与合同正文有任何不一致，以合同正文为准。

本合同附件为：附件一：培训评估表

附件二：讲师介绍

附件三：课程大纲

附件四：报价明细

补充附页

经友好协商，对本合同条款补充、修改如下，本补充附页为合同正文的一部分，与合同正文冲突时，以本补充附页为准：

本次培训根据实际培训进度进行费用结算。

甲方：广东省通信产业服务有限公司广州分公司

法定代表人
或授权代表（签字）：

2023年9月18日

乙方：广州中睿信息技术有限公司

法定代表人
或授权代表（签字）：

2023年9月18日

附件一：培训评估表

被考核单位：	合同名称及编号：
项目名称：	□ 完成 □未完成
考核评价单位：	考核评价时间：

考核评价内容	分值	评分标准	得分
项目准备	10	按项目要求做好培训讲义、会场布置等准备工作，且质量符合要求。准备工作不符合要求，每一项扣5分。未做准备工作不得分。	
疫情防控	5	确保服务人员为甲方提供服务时不存在已确诊、疑似感染新型冠状病毒、按要求需隔离或有发热症状的员工的情况，在服务期间佩戴口罩、注意卫生，并配合做好疫情防控工作。	
师资保障	15	按合同要求配备优秀师资。违反合同约定擅自更换师资，每出现一次扣5分，扣完为止。	
跟班管理	10	按合同约定指派专人(班主任或助教)负责跟班、学员考勤、教学服务等全程跟班管理，否则不得分。指派工作人员不足，扣10分，扣完为止。	
效果测评	25	按项目要求组织对外聘师资教学效果进行测评且综合满意度在90%以上。未组织测评或综合满意度低于90%不得分。	
服务质量	10	项目实施期间，及时沟通、协助处理教学中的问题。每出现一次有效投诉，扣5分，扣完为止。	
保密管理	10	按合同要求履行保密管理责任，违反合同约定的，每发现一次至少扣5分，影响严重的不得分。	
讲台纪律	10	严格遵守讲台纪律，自觉与党中央的理论、路线、方针政策保持高度一致，严守政治纪律。	
改进措施	5	未及时沟通、反映或处理项目实施中的问题且给教学造成影响的，每发现一次扣5分。影响严重的不得分。	
考核评价得分			

备注：
1. 考核总分≥90分，全额付培训费
2. 90＞考核总分≥80分，“考核总分/100分”的比例支付培训培训费
3. 考核总分＜80分，不予支付培训费或有权要求乙方无偿重新授课

考核方（盖章）：	被考核方（盖章）：

张海杰



技术栈

1. 具备 CTF-Web 经验，星盟安全团队 Web 负责人，星盟安全团队 SRC 组负责人，具备护网经验；
2. 熟悉常见漏洞原理和利用，包括 SQL 注入，XSS，SSRF，文件上传等 OWASP TOP 10 安全漏洞；
3. 熟悉渗透测试技术和各种主流测试工具的使用，例如 Metasploit、Cobalt Strike、Sqlmap、Burp Suite、Xray、AWVS 等；
4. 熟悉网络空间搜索引擎，比如 FOFA、鹰图、shadan 等；
5. 熟悉常见提权方法 ，比如 SUID 提权、EXP 提权、数据库提权、DLL 劫持提权、ByPassUAC 等提权；
6. 熟悉简单 PHP 代码审计能力、掌握 python 语言，能够独立编写 poc 和简易自动化脚本、二开 sqlmap 和 dirsearch 等脚本，有自己的武器库；
7. 了解常见网络安全设备，例如天眼、绿盟 waf、玄武盾、明御 APT、IDS/IPS、堡垒机、默安蜜罐等；
8. 了解 Linux 和 Windows 应急响应和溯源反制手段；
9. 了解 MySQL、SQL server、Redis 数据库常规操作；

荣誉奖项与证书

1. 2022 第二十四届中国机器人及人工智能大赛全国赛 **全国三等奖**
2. 2022 广东省粤盾红队第九名
3. 2023 B01lers CTF 国际赛 **全世界第 12**
4. 2023 NKCTF 网络安全大赛**全国第四**
5. 2023 **中国国际数博会之** 大数据及网络安全精英对抗赛 全国线下赛总排名前 30 **奖金 1w**(人民日报)
6. 2023 信息安全与对抗技术竞赛全国个人赛与擂台赛双赛道**全国一等奖**
7. 2023 第四届 "闽盾杯" (黑盾杯) 初赛**全国第二**，线下**全国第五** 二等奖 (省公安、省政府主办)
8. 2023 第七届粤港澳大湾区 IT 应用系统开发大赛全国赛 **全国铜奖**
9. 2023 江门市攻防演练 邑盾 红队 **全市总排名第二**
10. 2023 "羊城杯" 网络安全大赛 全国三等奖
11. 2023 全国智能网联汽车"天融信杯"信息安全攻防赛线下全国总决赛优胜奖
12. 2023 中国电信"巅峰极客"网络安全技能挑战赛 线上赛**全国第四** 线下赛全国第 9
13. 2023 第二届 "陇剑杯" 网络安全大赛 **总决赛**全国第 11 **奖金 1w**

证书

1. CNVD 原创漏洞证书 CNVD-YCGN-202304039653 北京某公司固件产品 **网络设备-高危 无条件命令执行**
2. CNVD 原创漏洞证书 CNVD-YCGN-202304018212 厦门某科技公司 **网络设备-高危漏洞 无条件命令执行**
3. CNVD 原创漏洞证书 CNVD-YCGN-202304018313 厦门某科技公司 网络设备-中危漏洞 有条件**命令执行**
4. CNVD 原创漏洞编号 CNVD-2023-41446 江苏某科技公司 中危漏洞 设备存在逻辑绕过权限
5. CNVD-2023-54452 事件性漏洞 中国电信小程序存在逻辑漏洞 中危漏洞
6. CNNVD 漏洞证书 CNNVD-2023-84828004 北京某公司 **设备高危漏洞 无条件命令执行**
7. CNNVD 漏洞 CNNVD-2023-45321926 某知名 CMS 高危漏洞 SQL 注入
8. CVE-2023-37119 某知名公司产品设备 **高危漏洞 无条件命令执行**
9. CVE-2023-39132 织梦 CMS(DedeCMS) **高危漏洞 代码审计后台代码执行**

10. **某市公安局(授权书)打击黑色产业感谢信**
11. **某县公安局(授权书)打击黑色产业感谢信**
12. **某县公安局(授权书)打击黑色产业感谢信**
13. 上海交通大学漏洞报告证书(**Getshell**)
14. 广西中医药大学漏洞报告证书(**Getshell**)
15. 2023 江西省萍乡市”燎原杯” 网络安全大赛出题感谢证书
16. 2023 第三届陕西省大学生网络安全技能大赛出题感谢证书

项目经历

2022.07 **第二十四届中国机器人及人工智能大赛全国赛**

项目内容: 全自动核酸机器人 通过全自动化核酸采样实现在采集样本和移送的过程中对于被采样人体都是稳定牢靠且无伤害的，本人用 C++语言实现了 UR10E 机械臂上的 D435i 双目视觉相机中视觉的矩阵转换以及视觉的识别定位这一开发模块

项目成果: 组装成功后可以实现对人体鼻子的识别，并且通过力反馈来进行数据的连接和控制，最终可以完成整套全自动化核酸采样的流程，成功在本次第二十四届中国机器人及人工智能大赛全国赛荣获**全国三等奖**

2022.07 **江门市护网邑盾红队**

项目内容: 对江门市直的某些组织系统和江门市直的公司下的产品进行信息收集 尝试通过红队测试手段进行渗透

项目成果: 通过信息收集整理好重点资产并且逐一排查，配合团队找到江门市物业某系统存在 sql 注入漏洞成功 getshell 进入内网，通过 psexec、PTT、PTH 等横向移动手段成功拿下域控权限，最终成功拿下某公司近 10 台服务器权限

2022.08 **国家某委员会护网蓝队中级**

项目内容: 按照任务对网站进行全局监控，基线排查，通过厂商的安全设备明御 APT 预警平台进行对红队人员的非法入侵进行过滤和溯源，完成敏感日志文件等的巡逻工作，最后生成护网总结报告提交厂商

项目成果: 通过开发 python 的简易脚本和规则进行对恶意 ip 进行拦截和封禁，护网期间没有失分，防守无出现被入侵现象，完善保护了甲方资产，最后成果是没有出现安全问题，封禁异常 IP 达 800+且成功溯源两名红队选手

2022.08 **广东省护网粤盾红队**

项目内容: 对广东省授权系统进行信息收集 尝试通过红队测试手段进行渗透

项目成果: 通过团队信息收集整理资产 个人测试到广东省农民工某平台存在弱口令以及后台存在接口未授权，泄露 5w+左右用户敏感信息包括姓名，电话，身份证等;

2022.11 **江门市邑安科技授权渗透项目**

项目内容: 对授权的公司下的某产品渗透测试

项目成果: 最终在所有目标内找到 58 个漏洞，包括 XSS、SQL 注入、文件上传、SSRF、逻辑漏洞等，高危漏洞 24 个，敏感信息总共泄露 5w+

2023.02 **第七届粤港澳大湾区 IT 应用系统开发大赛全国赛**

项目内容: 基于 IOT 的多频电力监控系统是一款是将 GPS、GSM 和计算机、网络、电力检测等现代技术集于一体

课程介绍

课程名称	网络安全攻防渗透技术	
课程描述	信息技术的创新日新月异，数字化、网络化、智能化深入发展，在推动经济社会发展、促进国家治理体系和治理能力现代化、满足人民日益增长的美好生活需要方面发挥着越来越重要的作用。随着信息技术的发展和信息化建设的高速推进，为信息安全产业的发展带来了前所未有的机遇，同时也产生了各种各样的信息安全问题。网络空间逐渐被视为继陆、海、空、天之后的“第五空间”，成为国际社会关注的焦点和热点。2017 年《网络安全法》颁布实施，标志着我国对于信息安全的重视达到一个全新的高度。长期以来，我国在网络安全政策、产业、技术等方面取得较大进展的同时，各类网络攻击、信息泄密、网络谣言等网络安全事件频发，安全攻防问题愈演愈烈！ 本次安全攻防培训，通过针对性的技术技能学习，结合大量的实战练习，全方位掌握信息安全攻防相关知识及技能，培养学员在网络安全方面的关键技能和职业素养，最终达到提升企业员工网络安全技能的目的。	
课程收益	1. 与时俱进——我们了解最新的网络技术与网络安全形式，我们了解企业和个人常发生或容易忽略的安全问题，我们能提供覆盖更为广泛的内容； 2. 形象生动——突破传统教科书似的教学方式，穿插响应的图片、动画、视频来吸引学员的注意力，加深其对网络安全的理解，并给其留下深刻的印象； 3. 注重效果——对于相关主题我们会结合实际案例来引发学员的兴趣与思考，再联系最佳实践或企业相关要求，从本质上提高学员的网络安全知识水平。	
授课说明	课程形式：	课堂讲授、讲义解析、情景模拟、实战互动演练、模拟考试

	课程时间：	3 天
时间安排	课程内容	
第 1 天	• 主机渗透测试技术 • 渗透测试技术基础 ➢ 渗透测试基本概念及流程介绍 ➢ 渗透测试环境部署 ➢ 渗透测试常用工具讲解 ➢ 信息收集技术 ➢ 主机探测及端口扫描 ➢ 漏洞扫描（扫描框架、工具、脚本） • 渗透测试进阶技术 ➢ MSF 渗透测试框架的使用 ➢ 常见系统漏洞利用（MS17-010：永恒之蓝、CVE-2019-0708、CVE-2020-0796：永恒之黑、CVE-2021-44228：Apache Log4j） ➢ 后渗透（权限提升、后门植入、隐藏账号、痕迹清除） • 实践一：某商城靶场漏洞利用获取管理员权限 • 实践二：Apache Log4j 漏洞利用	
第 2 天	• Web 渗透测试技术 • Web 渗透技术基础 ➢ Web 渗透测试概述 ➢ 2021 OWASP TOP 10 安全威胁介绍	

	➢ 基于 wvs 的网站漏洞扫描与分析 ➢ 主流漏洞讲解（SQL 注入、XSS、CSRF、SSRF、文件上传、文件包含、中间件漏洞、逻辑漏洞、越权漏洞） ● Web 渗透进阶技术 ➢ SQL 注入漏洞实践 ➢ 命令执行漏洞实践 ➢ XSS 漏洞实践 ➢ 文件上传漏洞实践 ➢ 文件包含漏洞实践 ● 实践一：构造 XSS 代码获取用户 cookie 信息 ● 实践二：利用文件上传及文件包含漏洞 getshell
第 3 天	● 安全攻防实战 ● 攻击靶场实战 ➢ 攻击靶场部署 ➢ Web 网站扫描、敏感信息收集 ➢ 某 CMS 网站渗透实战 ➢ 某人才系统网站渗透实战 ● 漏洞防护技巧 ➢ 安全防护工具介绍 ➢ 主流防护技巧讲解 ➢ 操作系统配置加固（账户与权限配置、进程与服务加固、组策略和注册表、日志分析）

	➢ 主机漏洞加固（MS17-010、CVE-2019-0708、CVE-2020-0796、CVE-2021-44228） ➢ Web 漏洞加固（SQL 注入、XSS、CSRF、SSRF、文件上传、文件包含等） ➢ 第三方工具防护应用 ● 实践一：DiscuzX3 网站漏洞利用获取管理权限
	总结、回顾、答疑

附件四：报价明细

序号	项目报价内容	服务内容	单位	数量	单价（含增值税）	增值税率	合价增值税款	合价价款（不含增值税）	合价价税合计	备注
1	网络安全攻防技术培训课程讲师课酬	要求授课师资具备本科或以上学历，授课评价高，至少拥有五年或以上网络安全工作经验，对网络攻防、web 技术、漏洞防护等有培训授课、实践带教经验。	元/天	3	9000	6%	1,528.30	25,471.70	27,000.00	
合计（小写）							1,528.30	25,471.70	27,000.00	
汇总总价（大写）					人民币贰万柒仟元整					