

# 网络安全

重构课程体系 迭代教学品质

V3.0课程简章重磅上线

亮点一：  
红蓝对抗复现

亮点二：  
全新等级保护2.0解析

亮点三：  
真实企业项目实战

亮点四：  
靶机实战CTF大赛解析

每1名学员都能成为企业注册白帽子安全工程师

01

品牌介绍

# 千锋教育




有情怀、有良心、有品质的IT职业教育机构

千锋教育专注IT职业教育，高薪聘请名师面授，携手一线企业联合研发教学课程，为18000余家合作企业输送优质人才，目前已在全国各大城市开设20余个大中型教学基地，推出“**免费试学两周，满意后再报名**”体验教学，成功打造IT教育全产业链人才服务平台。

千锋年培养优质人才20000余人，全国同期在校学员8000余人，合作院校超600所，为高校举办实训5000余次，组织实施各类讲座4万余场，合作企业超18000家，累计向互联网输出免费教学视频152套，年播放量逾6000万次。每年有数百万名学员受益于千锋教育组织的技术研讨会、技术培训课、网络公开课及免费教学视频。



## [不同城市 同样面授]

-  全国各校区讲师统一管理，招聘标准一致
-  课程大纲全范围内定期升级更新
-  关心学员学习质量

## [一地学习 全国就业]

 就业体系  
覆盖全国

 超18000家  
合作企业定期招聘

 合作名企定向输出  
学员就业随心选择

02

# 市场 分析

# 网络安全市场分析

## 什么是网络安全

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。具有保密性、完整性、可用性、可控性、可审查性的特性。

## 生活中涉及到的网络安全

"白帽子"安全工程师守卫网络世界黑白界线

### 国泰航空940万用户隐私数据泄露

公司及全资子公司港龙航空有限公司乘客资料被窃取，包含有940万乘客的姓名、生日、电话、地址、身份证及护照号等敏感信息。还有403张信用卡账号，27张无安全码信用卡账号被窃取。

### 手机短信验证码存漏洞

手机有时无缘无故地收到短信验证码，但是本人并未进行任何操作，而且支付宝或银行卡的钱却被转走。

这是一种新型伪基站诈骗。犯罪分子可实时获取用户手机短信内容，利用各大知名银行、网站、移动支付App存在的基础漏洞和缺陷，实现信息窃取、资金盗刷和网络诈骗等。

### 思科高危漏洞攻击国内多家机构

思科高危漏洞 CVE-2018-0171在清明小长假期间被黑客利用发动攻击，国内多家机构中招，配置文件被清空，安全设备形同虚设。此漏洞影响底层网络设备，且漏洞 PoC 已公开，很有可能构成重大威胁。

### 浙江省1000万学籍数据在暗网被售卖

浙江省1000万条学籍数据在网上售卖，学籍数据覆盖了浙江的大部分市区，被泄露的信息包含了学生姓名、身份证、学籍号、户籍位置、监护人、监护人号码、居住地址等。除了文字数据，售卖的学籍数据里还提供有照片链接，在100G左右。

### “微信支付”勒索病毒 100000台电脑被感

一种新型勒索病毒入侵电脑运行后，会加密用户文件，但不收取比特币，而是要求受害者扫描弹出的微信二维码支付110元赎金，获得解密钥匙，这也是国内首次出现要求微信支付赎金的勒索病毒。利用自制病毒木马入侵用户计算机，非法获取淘宝、支付宝、百度网盘、邮箱等各类用户账号、密码数据约5万余条，全网已有超过10万台计算机被感染。

### 摄像头漏洞暴露数百万摄像内容

多个厂商/型号的摄像头被披露出多个漏洞，通过ZoomEye搜索引擎能得到200万的设备暴露在公网上，但是通过枚举Cloud ID，能访问到约900万设备。存在着硬编码凭证和远程代码执行漏洞，如果这些设备被用来传播僵尸网络，将会给网络空间造成巨大的危害。

## 网络安全的市场前景

21世纪是信息化时代，IT技术瞬息万变，安全是唯一不变的主题。网络恶意攻击强度、频率、规模和影响在不断升级，网络安全越来越被重视。网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，自2014年以来，国家就高度重视网络安全问题，提出：没有网络安全就没有国家安全，没有信息化就没有现代化。但是由于我国网络安全起步较晚，所以网络安全工程师十分紧缺，网络安全人才缺口到2020年预计将达到200万，同时人才需求呈爆炸式增长。

## 国家政策扶持：网络安全已上升为国家战略

2003年

中办、国办印发《国家信息化领导小组关于加强信息安全保障工作的意见》

2005年

国家信息化领导小组印发《国家信息安全战略报告》

2012年

国务院印发《关于大力推进信息化发展和切实保障信息安全的若干意见》

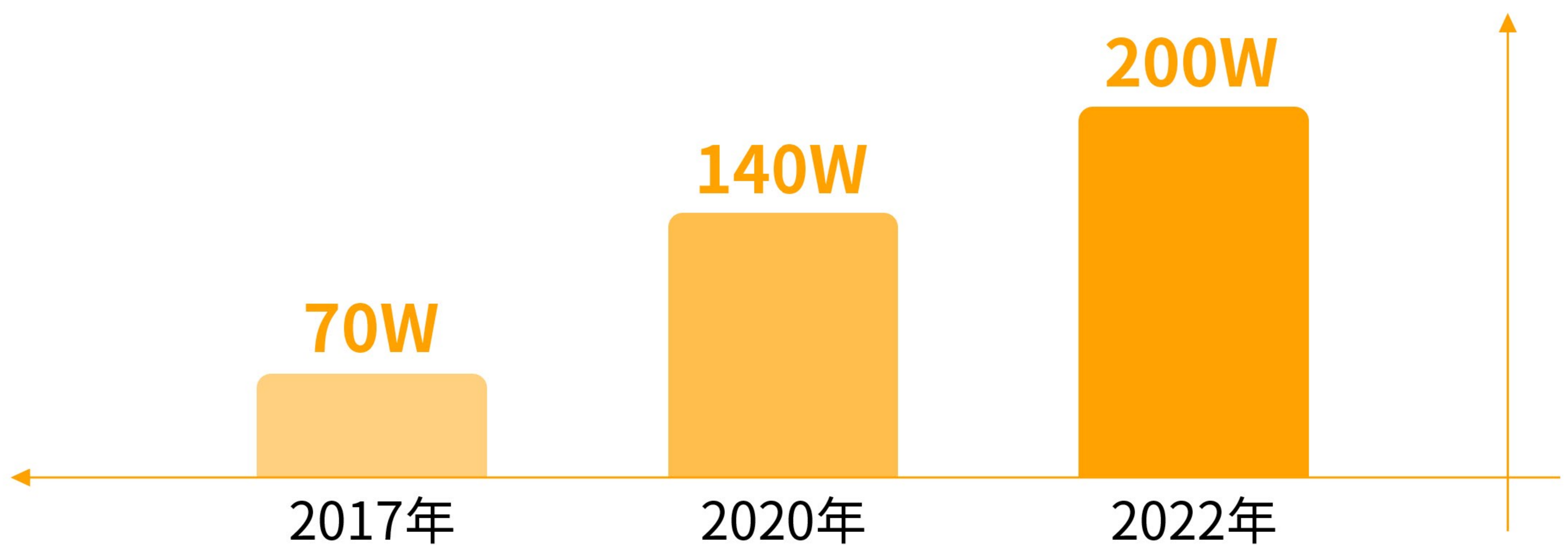
2014-2016年

出台《中华人民共和国网络安全法》《国家网络空间安全战略》

## 人才需求现状：网络安全人才需求量巨大，未来更大

2017年我国网络安全人才缺口超70万，国内3000所高校仅120所开设相关专业，年培养1万-2万人，加上10-20家社会机构，全国每年相关人才输送量约为3万，距离70万缺口差距达95%。

此外，2022年网络安全人才需求量直线增长，预计达200万！



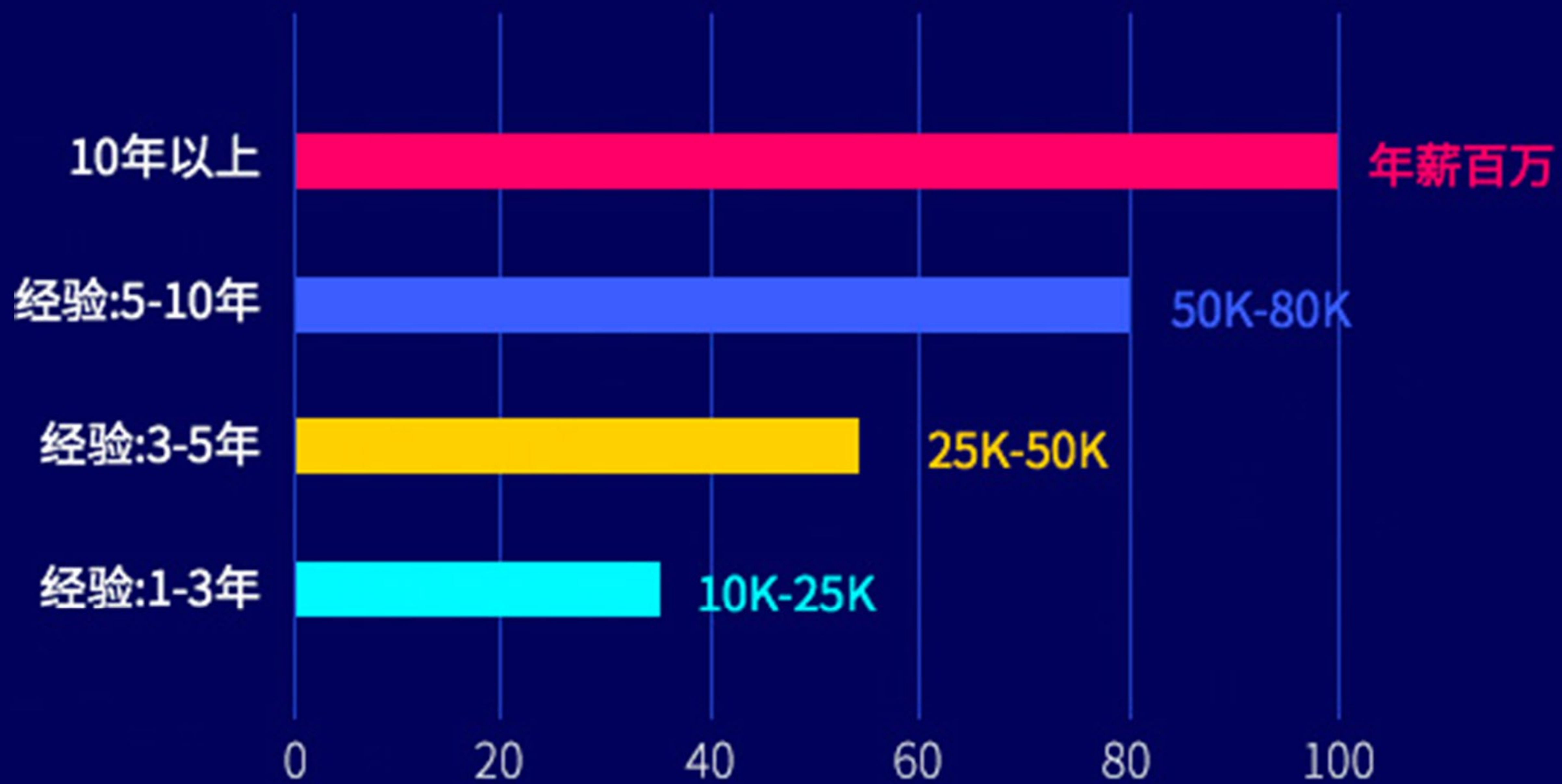
## 行业薪资分布：网络安全薪资高，且门槛低

因为行业人才输送与人才缺口的比例问题，网络安全对从业者经验要求偏低，且多数对从业者学历不设限。



## 薪资竞争分析：起步薪资高，经验与薪资成正比

越来越多的行业从业者上升到一定阶段便再难进步，很容易被新人取代，但网络安全与其他行业的可取代性不同，网络安全工程师将在未来几十年都处于紧缺状态，并且，对于防御黑客攻击，除了极少数人靠天分，经验才是保证网络安全的第一法则。



## 职业发展方向：网络安全工程师岗位众多，方向灵活

网络安全专业入职岗位非常宽泛，包括：安全运维工程师、渗透测试工程师、安全售前工程师、Web安全工程师、安全服务工程师、安全咨询工程师、产品实施工程师等。

网络安全工程师

大数据安全工程师

渗透测试工程师

云密码安全工程师

电信系统安全工程师

信息安全工程师

高级安全专家

服务器安全工程师

系统安全工程师



## 职业入职领域：多维度发展，就业口径宽广

目前互联网、通信、新能源、房地产、金融证券、电子技术等行业迫切需要网络安全人才，因为网络安全的重要性，每一行业同时又催生出不同的需求方向，从业者完全可以根据自己的喜好自主择业。



信息安全  
设备厂商



互联网  
安全公司



安全  
服务公司



系统  
集成商



国企

— 以上数据来源于搜狐平台报道与职友集统计 —

03

# 课程 解读

# 千锋网络安全课程解读

## 课程概述

千锋网络安全，秉承以就业为导向、以实用技能为核心，产品设计以企业岗位需求为基础。所有案例均来自于知名企业的真实攻防项目，由业内权威技术专家提供，确保与企业真实需求无缝对接，将企业的真实需求先整理为技能体系，围绕技能，展开并梳理与之相关的理论，形成知识体系。根据知识体系中不同技术方向之间的关联性和难易程度，调整先后顺序，并组织为课程内容。

以“学会学习”为学习目标，在一、二阶段，将正确的在校学习方法融入到教学方法中，学员潜移默化地养成习惯，三阶段，将正确的在职自学方法融入到案例课和翻转课堂，使学员学习专业技能的同时，掌握了在职业发展中必不可少的自学能力。

## 课程版本

3.0版千锋网络安全大纲，按企业实际需求全新调整了每一天的课程设计及知识点，加入更多新的特性及技能，加入红蓝对抗、全新等级保护2.0解析、靶机实战CTF大赛解析等亮点内容。

## 培养目标

培养学员学习黑客发展史、术语、简单工具的使用，踩点、网络协议、远控、简单的攻击思路、以及未来网络安全发展趋势等知识。

输出

储备安全技能的关键理论点，使学员能够达到在工作中发现并分析常见的攻击手段，提高安全意识，具备管理和维护以及使用简单的工具对企业的信息安全做出基本评测，初步形成企业信息安全知识架构。

从深度和广度加深知识点，并配合平台上大量的攻防场景来融合理论知识，通过学习信息探测、工具(kali)、漏洞扫描、注入、解析、绕过、文件包含、XSS跨站漏洞、提权、旁注攻击、爆破、CSRF等。

输出

锻炼学员的动手能力。面向技术提升，以“攻”的基础环境为主，“以攻促防”，为实现企业级高端应用、系统、信息安全，铺垫必备的技能 and 知识体系。具备一定的分析和解决常见问题的能力。

# 课程升级内容

## 1. 等级保护2.0（windows、网络设备、服务器部分）

网络安全等级保护是国家网络安全保障的基本制度、基本策略、基本方法。开展网络安全等级保护工作是保护信息化发展、维护网络安全的根本保障，是网络安全保障工作中国家意志的体现。对网络安全就业有加分项。

## 2. 红蓝对抗复现

在军事领域，演习是专指军队进行大规模的实兵演习，演习中通常分为红军、蓝军，演习多以红军守、蓝军进攻为主。类似于军事领域的红蓝军对抗，网络安全中，红蓝军对抗则是一方扮演黑客（蓝军），一方扮演防御者（红军）。在国外的话，进行渗透攻击的团队经常称做红队，在国内称为蓝队实际上应该还是比较准确的叫法。

安全是一个整体，正如木桶定律，最短的木板是评估木桶品质的标准，安全最薄弱环节也是决定系统好坏的关键。而网络红蓝军对抗的目的就是用来评估企业安全性，有助于找出企业安全中最脆弱的环节，提升企业安全能力的建设。

## 3. CTF大赛解析与靶机实战

CTF是一种流行的信息安全竞赛形式，其英文名可直译为“夺得Flag”，也可意译为“夺旗赛”。其大致流程是，参赛团队之间通过进行攻防对抗、程序分析等形式，率先从主办方给出的比赛环境中得到一串具有一定格式的字符串或其他内容，并将其提交给主办方，从而夺得分数。为了方便称呼，我们把这样的内容称之为“Flag”。

## 4. 网络空间AWD对抗

AWD赛制是一种网络安全竞赛的赛制。AWD赛制由安全竞赛专家及行业专家凭借十多年实战经验，将真实网络安全防护设备设施加入抽象的网络环境中，模拟政府、企业、院校等单位的典型网络结构和配置，开展的一种人人对抗的竞赛方式，考验参赛者攻防兼备的能力。其主要特点为：强调实战性、实时性、对抗性，综合考量竞赛队的渗透能力和防护能力。

## 5. 安全众测项目实战

与合作企业启明联合做安全项目，云众可信、众测实战项目，学习到一定程度后，即可成为企业注册白帽子，可参与真实的企业渗透、安服、风评等众测项目。

## 6. 承接合作企业真实项目

千锋有多家安全企业合作，学员在学习期间，可以边学习，边做真实的项目，增加真实实战经验。

# 适学人群

大学专科及以上学历

有踏实的学习态度  
强烈学习欲望

抗压能力强

立志在网络安全方向  
深入研究群体

对安全技术敏感

想步入信息安全行业从业者

## 课程优势



### 01.课程研发

由千锋教育主导，奇虎360、启明星辰等企业联合研发教学课程，根据企业岗位定制，由用人单位评估，经多家企业联合研发。



### 02.靶场设备

依托真实企业项目场景，采用真实的企业漏洞还原环境搭建，以真实的企业平台与设备实操攻防对抗，学习与工作相融，学员可无障碍迈入职场。



### 03.实战平台

启明星辰、云众可信、众测实战项目，学习到一定程度后，即可成为企业注册白帽子，可参与真实的企业渗透、安服、风评等众测项目。



### 04.师资团队

业界高水平的白帽极客战队全程授课，项目驱动教学，让学员在学习期间有能力胜任安服、渗透等项目。



### 05.企业级的项目案例

适应企业需求，拓宽职业发展空间。丰富的安全项目与CTF对抗赛、及靶机实战，全面增加学员的真实项目实战经验。



### 06.先进的教学模式

覆盖面广、实用性强，打造“一专多能”的复合型人才，技术课融入学习方法和职业素质。

# 千锋网络安全竞品对比

## 技术点差异化

技术点	千锋网络安全	其他机构一	其他机构二
IP地址详解	✓	✓	✓
进制转换	✓	✓	✓
DOS命令	✓	✓	✓
批处理	✓	✗	✓
用户和组管理	✓	✓	✓
服务器远程管理	✓	✓	✓
破解系统密码	✓	✓	✗
NTFS	✓	✓	✓
IIS-WEB	✓	✓	✓
IIS-FTP	✓	✓	✓
DNS	✓	✓	✓
DHCP	✓	✓	✓
AD域	✓	✗	✓
PKI	✓	✓	✓
445传播木马	✓	✗	✗
windows安全基线	✓	✓	✓
TCP/IP	✓	✓	✓
OSI	✓	✓	✓
抓包分析	✓	✓	✓
交换机工作原理	✓	✓	✓
路由器工作原理	✓	✓	✓
路由	✓	✓	✓

技术点	千锋网络安全	其他机构一	其他机构二
VLAN	✓	✓	✓
VTP	✓	✗	✓
ICMP	✓	✓	✓
DHCP中继	✓	✗	✓
三层交换技术	✓	✓	✓
VPN	✓	✓	✓
网络架构分析	✓	✗	✓
ACL	✓	✓	✓
NAT	✓	✓	✓
动态路由	✓	✗	✓
TCP分析	✓	✓	✓
UDP分析	✓	✓	✓
防火墙	✓	✓	✓
IDS/IPS	✓	✗	✓
Linux基本命令	✓	✓	✓
Linux命令与编辑器与软件安装	✓	✓	✓
Linux账户安全	✓	✓	✓
日志审计系统	✓	✓	✓
LAMP安全配置（一）	✓	✓	✓
LNMP安全配置（二）	✓	✓	✓
防火墙技术与应用	✓	✓	✗
shell脚本与自动化	✓	✓	✗



技术点	千锋网络安全	其他机构一	其他机构二
阶段综合项目三与测试	✓	✓	✗
模拟人机交互	✓	✗	✗
程序实现文件拷贝	✓	✗	✗
建立随机密码生成器	✓	✗	✗
linux用户密码破解	✓	✗	✗
凯撒密码加密程序	✓	✗	✗
内网主机存活检测程序	✓	✗	✗
文件的增量备份程序	✓	✗	✗
程序的高级应用	✓	✗	✗
网页信息爬取	✓	✓	✗
后门程序编写与远程控制	✓	✗	✗
HTTP 协议	✓	✓	✓
BurpSuite	✓	✓	✓
渗透测试神器 - hackerbar 使用	✓	✓	✓
HTML	✓	✓	✓
PHP	✓	✓	✓
MYSQL	✓	✓	✓
JS	✓	✓	✓
渗透测试方法论	✓	✓	✗
法律法规与道德	✓	✓	✗
渗透测试武器库	✓	✓	✗
信息收集	✓	✓	✗

技术点	千锋网络安全	其他机构一	其他机构二
Nmap	✓	✓	✓
Openvas	✓	✓	✓
AWVS	✓	✓	✗
御剑	✓	✓	✗
nikto	✓	✓	✗
同源策略	✓	✗	✗
CORS	✓	✓	✗
AJAX 技术	✓	✗	✗
XSS	✓	✓	✓
CSRF	✓	✓	✓
SQL注入	✓	✓	✓
sqlmap	✓	✓	✓
代码与命令注入	✓	✓	✓
文件上传漏洞	✓	✓	✓
文件包含漏洞	✓	✓	✓
任意文件读取漏洞	✓	✓	✓
业务逻辑漏洞	✓	✓	✗
请求伪造漏洞	✓	✓	✓
服务器提权与隧道技术	✓	✓	✗
Metasploit 渗透平台	✓	✓	✗
定制EXP之python 实现	✓	✓	✗
反序列化漏洞	✓	✓	✗

# 千锋网络安全竞品对比

## 项目差异化

### - 千锋网络安全 -

项目均来自多家国内顶级安全公司的真实项目，包括360、启明星辰等企业大咖的指导，项目更注重内网渗透、web渗透、等级保护的实战能力，实现真实项目+靶机相结合学习，就业前学生就可以参与精心提炼的真实项目，丰富项目经验，强化学员竞争能力！

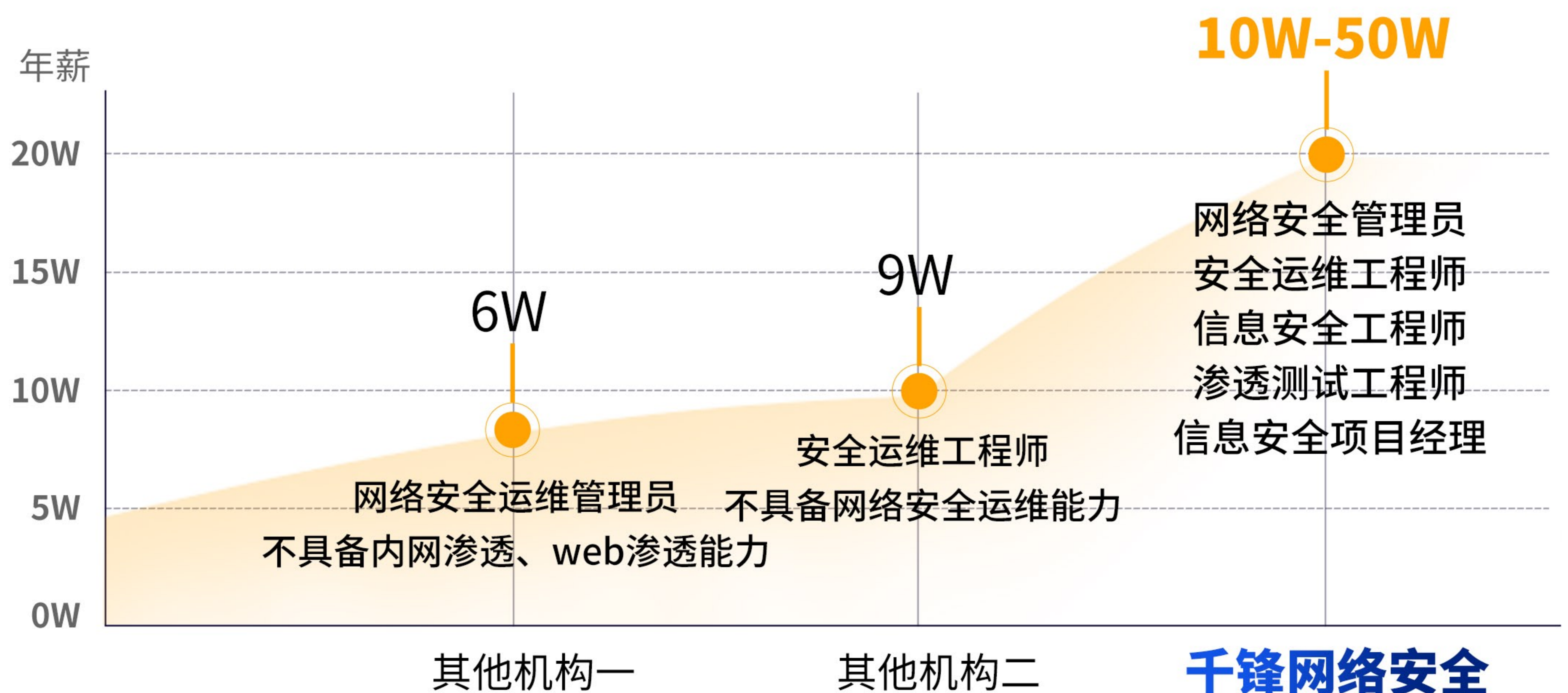
### - 其他机构 -

项目只有部分企业项目，大部分没有真实项目，而是只有自己搭建的靶机环境，这样缺少了真实项目案例的经验和实战能力。学员对真实项目的流程和关键点缺少认知，面试时将无法说出真实项目的流程、感受、以及项目的侧重点，大大降低面试成功率。

## 职业路径

千锋网络安全就业领域宽广，可入职领域多维发展，包括信息安全设备厂商、互联网安全公司、安全服务公司、系统集成商、国企。

千锋网络安全学员入职岗位非常宽泛，包括：安全运维工程师、渗透测试工程师、安全售前工程师、Web安全工程师、安全服务工程师、安全咨询工程师、产品实施工程师等。



# 千锋网络安全课程体系

V3.0碾压式课程迭代：四个阶段深度赋能，知名企业的真实攻防项目，就业力更突出！



## 第一阶段

数通安全  
【共5周】

### 学完本阶段可胜任岗位：

网络安全管理员、系统安全管理员、终端安全管理员、驻场监控管理员

### 就业月薪范围：

4000-6000

课程目录	课程内容
windows服务安全与评估	<ul style="list-style-type: none"> <li>安全概述</li> <li>虚拟化架构与系统部署</li> <li>IP地址详解</li> <li>进制转换</li> <li>DOS基本命令与批处理</li> <li>用户与组管理</li> <li>服务器远程管理</li> <li>破解windows系统密码</li> <li>NTFS安全权限</li> <li>文件共享服务器</li> <li>DNS部署与安全</li> <li>DHCP部署与安全</li> <li>WEB服务部署</li> <li>FTP服务部署</li> <li>域与活动目录</li> <li>域的部署与管理</li> <li>组策略高级应用</li> <li>PKI技术与应用</li> </ul>
以太网交换与路由技术	<ul style="list-style-type: none"> <li>OSI与TCP/IP协议簇</li> <li>通过抓包分析TCP/IP协议架构</li> <li>交换机工作原理与配置</li> <li>IP分析与静态路由</li> <li>ARP协议与中间人攻击</li> <li>ICMP协议分析</li> <li>虚拟局域网VLAN</li> <li>VTP</li> <li>单臂路由</li> <li>DHCP服务与DHCP中继</li> </ul>
高级网络技术与安全评估	<ul style="list-style-type: none"> <li>三层交换技术</li> <li>网络架构规划与阶段性综合实验</li> <li>TCP与UDP协议分析</li> <li>访问控制策略ACL</li> <li>NAT技术</li> <li>RIP动态路由协议</li> <li>IPsecVPN原理与配置</li> <li>Cisco基础网络设备安全配置基线</li> </ul>
安全设备防护与综合项目	<ul style="list-style-type: none"> <li>防火墙原理及部署</li> <li>HA热备份与负载均衡</li> <li>入侵检测系统IDS</li> <li>等级保护2.0 网络设备部分</li> </ul>



## 第二阶段

服务安全  
【共2周】

### 学完本阶段可胜任岗位：

安全运维工程师、服务安全管理员、安全测试工程师

### 就业月薪范围：

6000-10000

### 课程目录

Linux安全运维

### 课程内容

Linux操作系统介绍与安装与目录结构分析  
linux系统的基本操作与软件安装  
Linux系统下用户以及权限管理  
网络配置与日志服务器建立应急思路  
建立php主页解析以及主页的访问控制  
Nginx服务都建立以及tomcat负载均衡  
iptables包过滤与网络地址转换  
实用型脚本案例  
等级保护2.0 服务器部分



## 第三阶段

代码审计  
【共4周】

### 学完本阶段可胜任岗位：

信息安全工程师、网络安全工程师、风控安全工程师

### 就业月薪范围：

8000-15000

### 课程目录

Python安全应用

### 课程内容

python特点	元祖特性
python运行方法	字典相关函数
导入tab模块	条件和循环、迭代
while循环语法结构	文件相关模块
for循环 range、xrange函数	检测和处理异常
列表解析	触发异常
语句语法	函数
变量赋值	变量作用域
标识符	函数式编程
字符串操作符和内建函数	内部函数
列表操作符、作用域列表的函数	生成器

课程目录	课程内容	
Python安全应用	模块 类 方法 组合 继承	Re模块-正则、核心函数 urllib与urllib2模块 C/S架构与套接字 socket函数应用
前端代码安全	标记语法 元素 元素嵌套 属性和值 CSS与HTML之间的关系 内联方式 内部样式表、外部样式表 语法结构与浏览器 变量的声明与使用 运算符 常量 数据类型转换 转换函数 运算符和表达式 短路逻辑	三目运算 函数的定义 变量的作用域 函数的作用域 流程控制 if结构 switch结构 break while循环 for循环 循环流程控制 创建与使用数组 JS数组3个不限制 遍历数组
数据库安全	sqlserver简介 sqlserver特性 sqlserver漏洞与版本 access简介 oracle简介	oracle特性 oracle漏洞与版本 mysql简介 mysql特性 mysql漏洞与版本

课程目录	课程内容		
<p>后台代码安全</p>	<table border="0"> <tr> <td>                     PHP变量                      语法结构                      数据类型                      常量"                      数据类型转换                      运算符与表达式                      函数                      可变变量、外部变量、环境变量                      资源类型"                      if结构                      switch结构                      while循环                      for循环                      循环流程控制                      遍历数组"                      数组函数                 </td> <td>                     字符串函数                      正则函数                      文件处理函数                      数学函数                      时间函数                      URL处理函数"                      mysqli函数库                      暴力破解漏洞审计                      命令执行漏洞审计                      CSRF漏洞审计                      文件包含漏洞审计                      文件上传漏洞审计"                      sql注入漏洞审计                      XSS注入漏洞审计                      ZVulDrill平台实战                      seay使用"                 </td> </tr> </table>	PHP变量 语法结构 数据类型 常量" 数据类型转换 运算符与表达式 函数 可变变量、外部变量、环境变量 资源类型" if结构 switch结构 while循环 for循环 循环流程控制 遍历数组" 数组函数	字符串函数 正则函数 文件处理函数 数学函数 时间函数 URL处理函数" mysqli函数库 暴力破解漏洞审计 命令执行漏洞审计 CSRF漏洞审计 文件包含漏洞审计 文件上传漏洞审计" sql注入漏洞审计 XSS注入漏洞审计 ZVulDrill平台实战 seay使用"
PHP变量 语法结构 数据类型 常量" 数据类型转换 运算符与表达式 函数 可变变量、外部变量、环境变量 资源类型" if结构 switch结构 while循环 for循环 循环流程控制 遍历数组" 数组函数	字符串函数 正则函数 文件处理函数 数学函数 时间函数 URL处理函数" mysqli函数库 暴力破解漏洞审计 命令执行漏洞审计 CSRF漏洞审计 文件包含漏洞审计 文件上传漏洞审计" sql注入漏洞审计 XSS注入漏洞审计 ZVulDrill平台实战 seay使用"		



## 第四阶段

Web渗透  
【共5周】

### 学完本阶段可胜任岗位：

网络安全工程师、Web安全工程师、  
信息安全项目经理、信息安全项目设计师

### 就业月薪范围：

8000-25000

课程目录	课程内容		
<p>渗透测试导论</p>	<table border="0"> <tr> <td>                     渗透测试方法论                      法律法规与道德                      Web 工作机制                 </td> <td>                     HTTP 协议                      Cookie 与session                      同源策略                 </td> </tr> </table>	渗透测试方法论 法律法规与道德 Web 工作机制	HTTP 协议 Cookie 与session 同源策略
渗透测试方法论 法律法规与道德 Web 工作机制	HTTP 协议 Cookie 与session 同源策略		
<p>情报收集</p>	<table border="0"> <tr> <td>                     DNS                      DNS 解析                      IP 查询                      主机测探与端口扫描                 </td> <td>                     网络漏洞扫描                      Web 漏洞扫描                      其他工具                 </td> </tr> </table>	DNS DNS 解析 IP 查询 主机测探与端口扫描	网络漏洞扫描 Web 漏洞扫描 其他工具
DNS DNS 解析 IP 查询 主机测探与端口扫描	网络漏洞扫描 Web 漏洞扫描 其他工具		
<p>口令破解</p>	<table border="0"> <tr> <td>                     口令安全威胁                      破解方式                      windows 口令破解                 </td> <td>                     linux 口令破解                      网络服务口令破解                      在线密码查询网站                 </td> </tr> </table>	口令安全威胁 破解方式 windows 口令破解	linux 口令破解 网络服务口令破解 在线密码查询网站
口令安全威胁 破解方式 windows 口令破解	linux 口令破解 网络服务口令破解 在线密码查询网站		

课程目录	课程内容	
<p>常见得漏洞攻防</p>	<p>SQL 注入基础 四大基本手法 其他注入手法 SQLmap 的使用 XSS 漏洞概述 XSS 的分类 XSS的构造 XSS 的变形 Shellcode 的调用 XSS 通关挑战 实战：Session 劫持 PHP 代码执行 OS 命令执行 文件上传漏洞原理概述 WebShell 概述 文件上传漏洞的危害 PUT 方法上传文件</p>	<p>.htaccess 攻击 图片木马的制作 upload-labs 上传挑战 Web容器解析漏洞 开源编辑器上传漏洞 开源CMS 上传漏洞 PHP 中的文件包含语句 文件包含示例 漏洞原理及特点 Null 字符问题 文件包含漏洞的利用 业务安全概述 业务安全测试流程 业务数据安全 密码找回安全 CSRF SSRF</p>
<p>提权与后渗透</p>	<p>Metasploit Framework 前言 urllib2 SQL 注入POC 到EXP 定制EXP 案例：Oracle Weblogic CVE2017-10271 RCE 案例：JBoss AS 6.X 反序列化</p>	<p>服务器提权技术 隧道技术 缓冲区溢出原理</p>
<p>项目实战</p>	<p>红蓝对抗 靶机实战 网络空间攻防对抗</p>	<p>等级保护规范 安全众测项目实战 承接企业项目</p>



# 千锋网络安全项目展示

13大主流项目，全部数据分析及机器学习类型，包含图片处理、推荐系统、地震预测、音视频合成、新闻分类、人脸识别等。更有千锋拥有独特资源，与UI，H5联合项目演练。

## 项目一：黑客大曝光

### 项目介绍

主要了解学习目前国内外网络安全的现状，常见的隐私泄露手段、以及黑客进行暗网交易的内幕。

### 技术点

web渗透、ARP攻击、DNS欺骗等。

### 【安全事件分析】

2016年8月21日，徐玉玉因被诈骗电话骗走上大学费用9900元，伤心欲绝，郁结于心，最终导致心脏骤停，虽经医院全力抢救，但仍不幸离世。



### 【大量微信聊天记录被劫持】



## 项目二：黄焖鸡引发的血案

### 项目介绍

针对目前各种卡片的漏洞，包括银行卡、饭卡、门禁卡，黑客可以利用卡片读取、复制、还原等技术来获取卡片的隐私信息。

### 技术点

卡片机、进制等。

#### 【卡片并不安全需小心】

定位设备伪装成手机充电器、充电宝，在手机充电的时候，利用设备中sim卡的定位功能进行设备定位并进行数据回传，从而获取使用户的地理位置、私密信息。



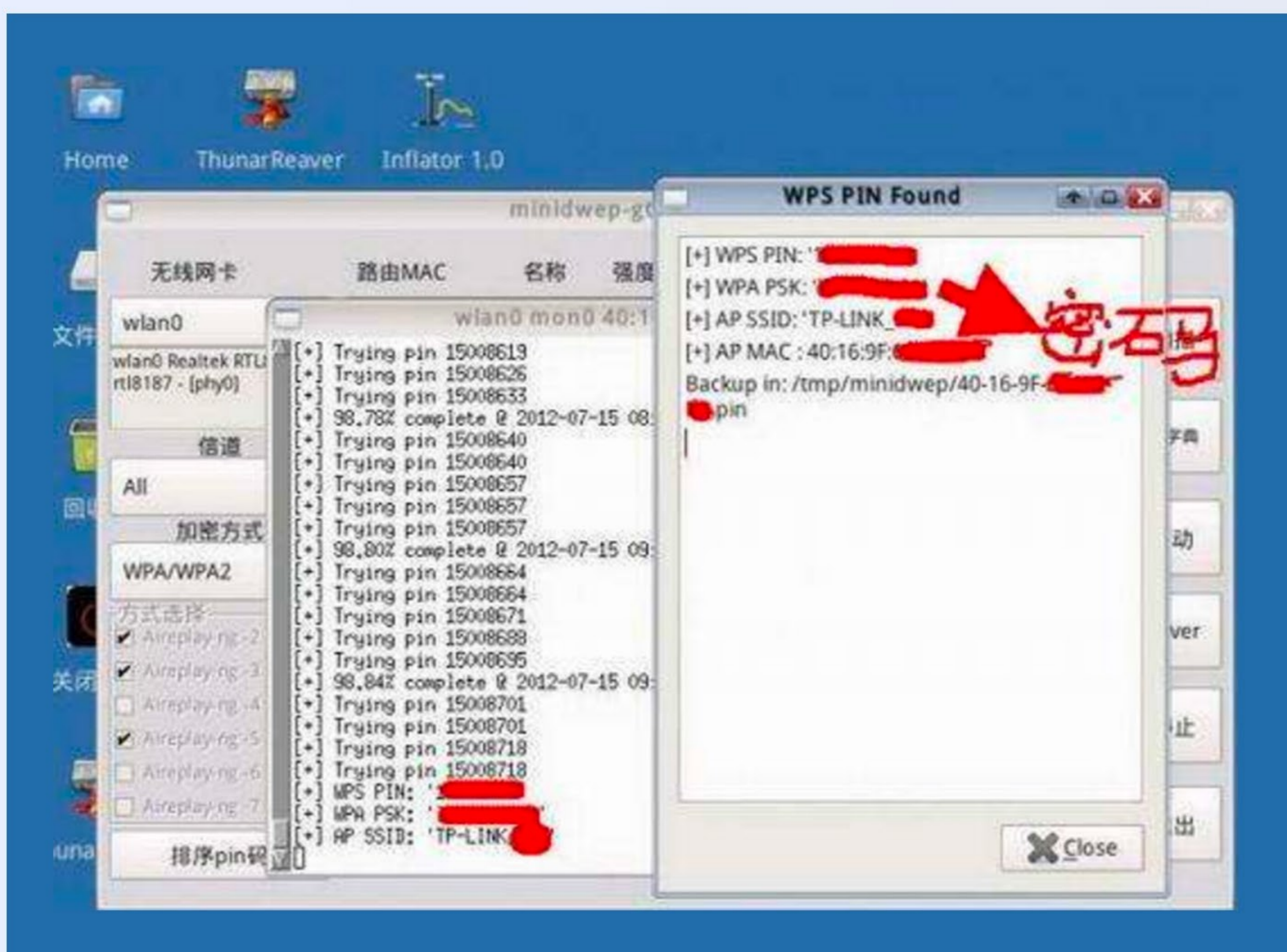
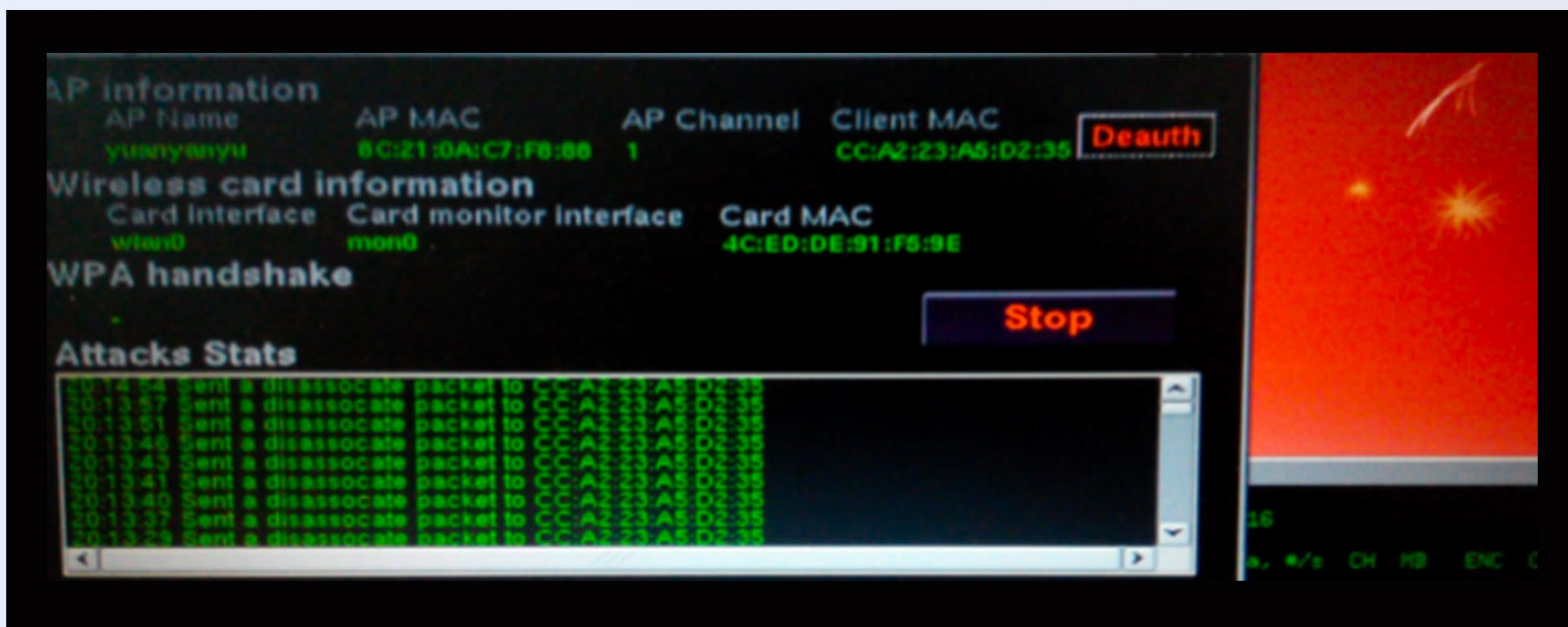
## 项目三：我就蹭蹭

### 项目介绍

针对目前wifi覆盖区域越来越大，黑客可以利用相关技术手段来破解wifi的登录密码达到入侵的目的。

### 技术点

kali平台，扫描，暴力破解，抓包等。



## 项目四：哇！病毒

### 项目介绍

计算机病毒（Computer Virus）是编制者在计算机程序中插入的破坏计算机功能或者数据的代码，能影响计算机使用，本项目用朋友间恶搞的形式来讲解最简单的病毒制作与防御。

### 技术点

VB编程语言，虚拟化技术，windows shell命令等。



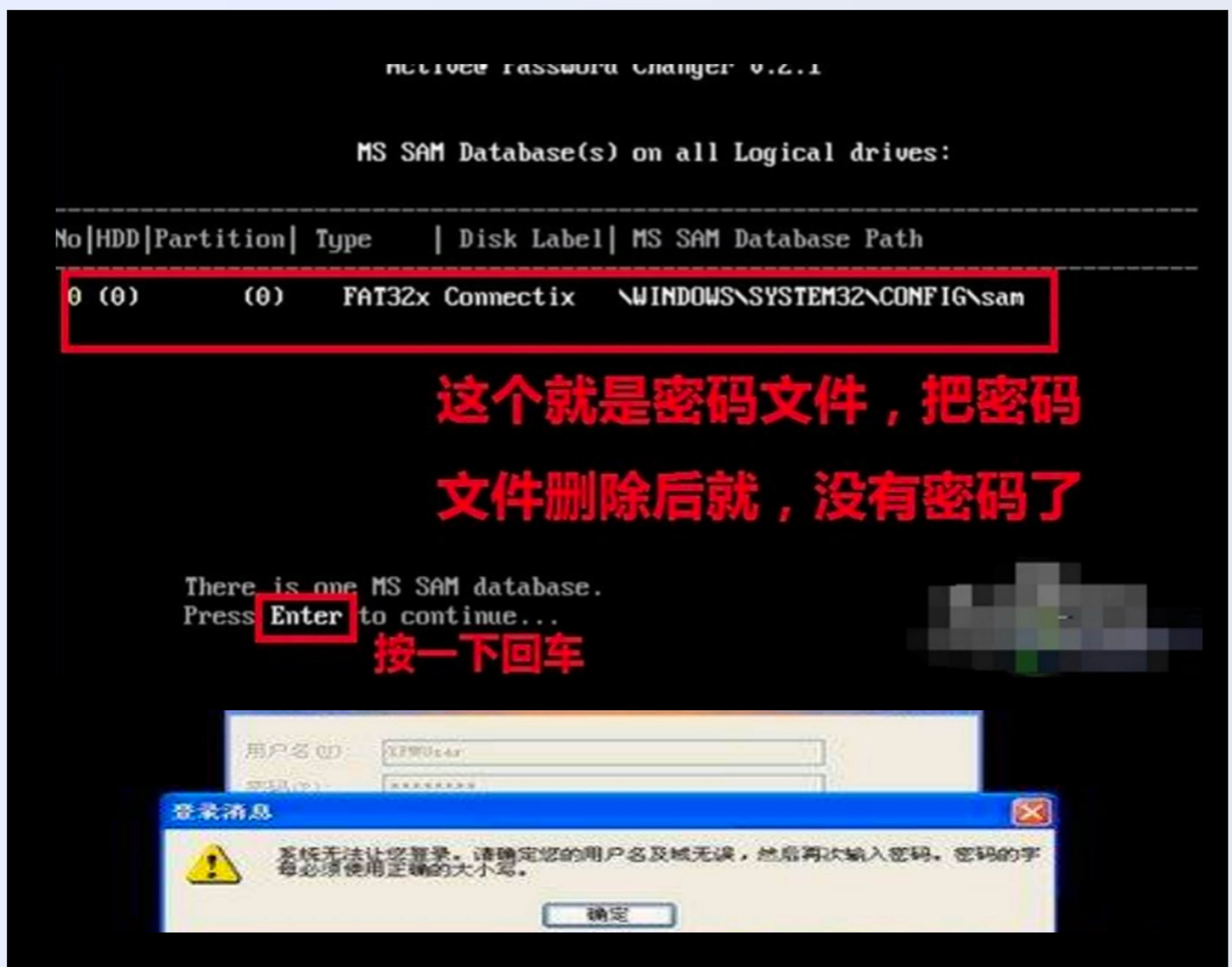
## 项目五：有密码了不起啊

### 项目介绍

利用kali下的九头蛇hydra工具进行各种协议的暴力破解，破解相关网络协议FTP、telnet、HTTP、ssh等。

### 技术点

kali、相关网络服务、hydra等。



```
nccivet Password Changer 0.2.1

MS SAM Database(s) on all Logical drives:

-----
No|HDD|Partition| Type      | Disk Label| MS SAM Database Path
-----
0 (0)      (0)      FAT32x Connectix  \\WINDOWS\\SYSTEM32\\CONFIG\\sam
-----
```

**这个就是密码文件，把密码文件删除后就，没有密码了**

There is one MS SAM database.  
Press **Enter** to continue...  
**按一下回车**

用户名 (U): xzfuser  
密码 (P): \*\*\*\*\*

**登录消息**

系统无法让您登录。请确定您的用户名及域无误，然后再次输入密码。密码的字母必须使用正确的大小写。

确定

## 项目六：傀儡与肉鸡的故事

### 项目介绍

常见木马的封装攻击与防御。木马病毒源自古希腊特洛伊战争中著名的“木马计”而得名，顾名思义就是一种伪装潜伏的网络病毒，等待时机成熟就出来害人。本项目主要通过经典的木马攻击还原场景，来学习木马的制作，入侵以及防御手段。

### 技术点

windows服务、shell命令、相关工具等。



## 项目七：外面是世界好可怕

### 项目介绍

针对用户已经泄露的信息，黑客可以在暗网、社工库中查询，并通过部分隐私信息来获取其他的隐私信息。

### 技术点

暗网、社工库、深网等。



12月11日 09:57 来自 iPhone 7  
关于有媒体报道京东数据安全问题声明

复制链接 分享到微博 分享到微信

[京东泄露12g的最新相关信息](#)

[京东12G用户数据泄露事故手尾长 凤凰科技](#)

在刚过去的周末,有媒体报道称,最近黑市上流通着多达12G疑似京东的

## 项目八：钓鱼去咯

### 项目介绍

姜太公钓鱼，愿者上钩！钓鱼者运用社会工程学知识诱骗受害者，以在未授权情况下获取对方的姓名、年龄、邮箱账号、甚至是银行卡密码等私人信息。所以说“防人之心不可无”这句话并非没有道理，凡事不要害人但是总要留个心眼否则最终受伤的就是自己。本项目将带领大家剖析钓鱼攻击案例。

### 技术点

ARP欺骗与攻击、DNS劫持、webserver搭建、html、PHP、ettercap等。





## 项目九：永恒之蓝

### 项目介绍

利用经典的勒索病毒肆虐全球的永恒之蓝漏洞，用虚拟场景来还原漏洞场景，分析黑客的攻击手段，来达到更加有效的防御措施。

### 技术点

kali、metasploit、metapreter、windows服务、防火墙等。

## Microsoft 安全公告 MS17-010 - 严重

### Microsoft Windows SMB 服务器安全更新 (4013389)

发布日期：2017年3月14日

版本：1.0

### 执行摘要

此安全更新程序修复了 Microsoft Windows 中的多个漏洞。如果攻击者向 Windows SMBv1 服务器发送特殊设计的消息，那么其中最严重的漏洞可能允许远程执行代码。

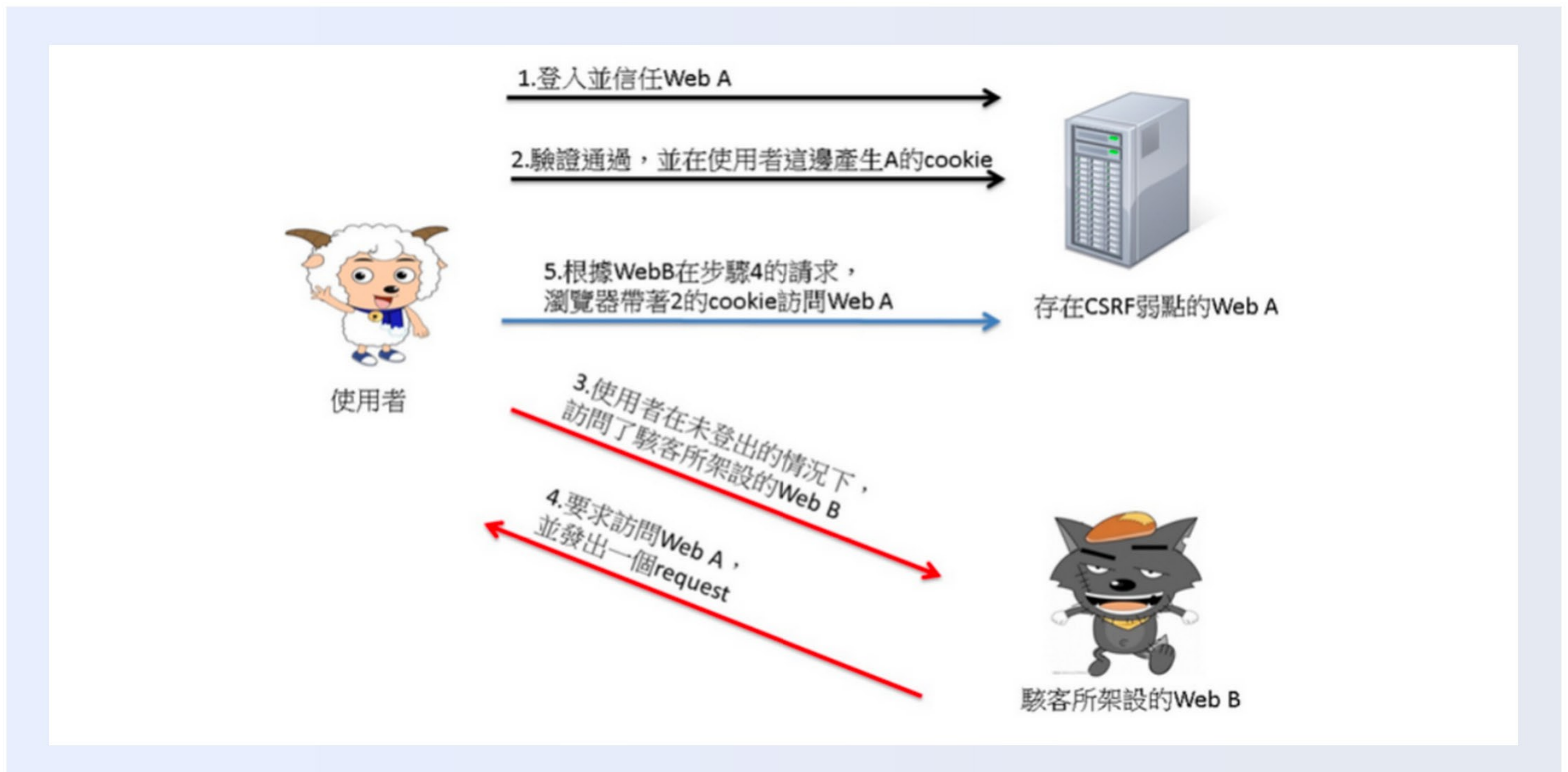
## 项目十：XSS与CSRF

### 项目介绍

利用虚拟平台搭建相关互联网生产业务环境，还原网络攻击经典的跨站脚本攻击，与跨站请求伪造攻击。

### 技术点

kali、各种攻击工具、kali平台、虚拟化平台、数据库等。



## 项目十一：sql注入攻击

### 项目介绍

还原经典的全球十大漏洞之一，通过本项目熟练掌握sql注入攻击的原理、危害、漏洞挖掘技巧、防御等，使之能够独立在互联网平台挖掘sql注入漏洞。

### 技术点

数据库、后端语言、kali平台、python自动化工具等。



## 项目十二：文件上传与包含漏洞

### 项目介绍

该项目利用虚拟化平台还原经典的十大漏洞之一的文件上传漏洞，通过该项目使之能够达到掌握黑客是如何利用网络来上传木马与病毒的手段。

### 技术点

中国菜刀、中国蚁剑、kali、御剑、后端语言等。



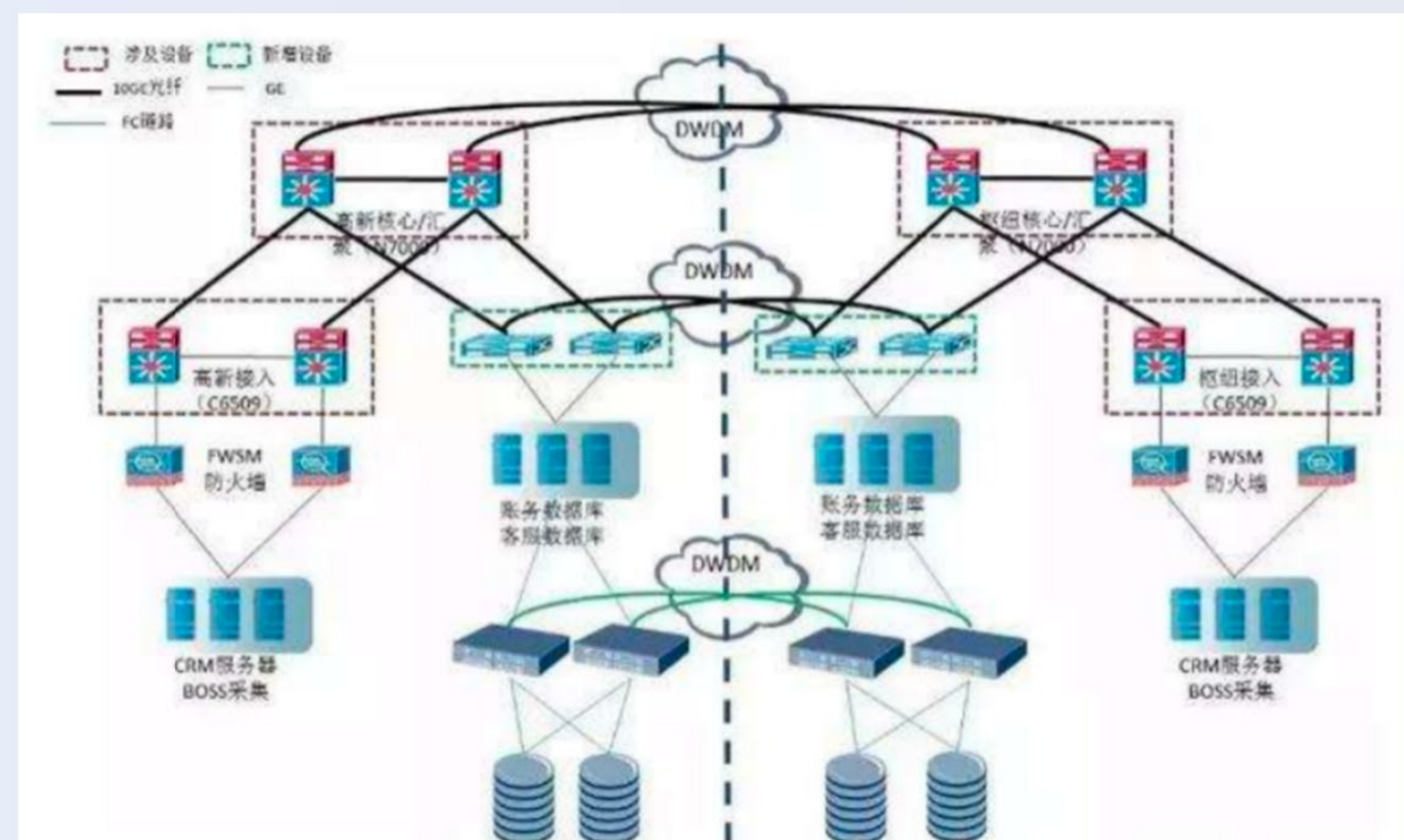
## 项目十三：按需求规划企业级网络架构

### 项目介绍

真实的千万级网络部署项目还原，从项目需求开始一直到项目交付，使之能够达到理解网络基础建设从零到上线的全部过程，为后期的网络安全运维打下坚实基础。

### 技术点

各种网络设备、网络协议、各种数通命令等。

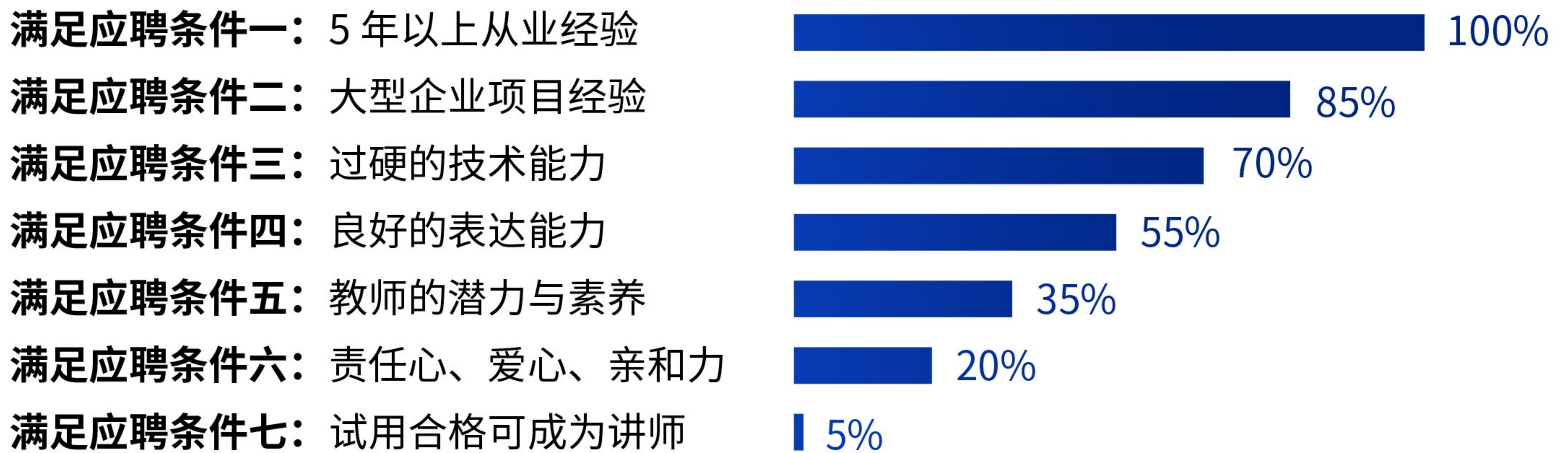


04

# 师资 体系

# 干锋网络安全师资体系

## 严选师资：对讲师严苛就是对学员负责



## 教学管理：教学研究、教学管理、品质管控、就业保障4个方面优化教学过程



### 教学研究

- 大量资源投入教研
- 百名企业顾问共建课程



### 教学管理

- 100%高品质全程面授
- 300余位实战强师
- QFTS教辅系统



### 品质管控

- 全国教学过程监管
- 超996严格式品质保障



### 就业保障

- 职业规划师全程指导
- 18000家合作企业推荐就业

千锋讲师：教研院统一选拔业内教学精英，全线提高课程竞争力

## 深林 | 千锋网络安全金牌讲师

**授课阶段：**一、二阶段

**授课内容：**Windows服务安全、Windows安全评估、网络安全、交换与路由技术、高级网络技术、安全设备防护、Linux安全运维、阶段综合项目。

**授课总时长：**8周

**名师介绍：**具有近10年IT和信息安全领域从业经验，具有丰富的项目实施经验。

曾任Cisco金牌厂家项目经理，某国资金融企业安全顾问，启明星辰云众可信技术中心特聘安全专家。

对网络安全架构、基线安全评估、防火墙技术、入侵检测防御、渗透测试、VPN、无线技术、Linux安全运维等技术有深入研究。

**技术栈：**Windows服务安全、网络安全架构、Linux安全运维、渗透测试、安全评估与加固。

**授课特点：**条理清晰，深入浅出，注重理论和实践。



已授课学员人数

**5000+**

带班薪资

**12000+**

学员测试评分

**99.61**

**学员评价：**备课充足，条理清晰，细致到位，堪称大神。

## ajest | 千锋网络安全金牌讲师

**授课阶段：**三、四阶段

**授课内容：**Python、HTML、JS、mysql、PHP、渗透测试导论、Web渗透。

**授课总时长：**9周



**名师介绍：**毕业于天津理工大学信息安全专业。中国计算机学会会员、国家注册信息安全专员CISP，启明星辰云众可信技术中心特聘信息安全专家，某安全实验室研究员兼高级Web安全顾问，白帽子战队Dnsec队长。

擅长代码审计、渗透测试与漏洞挖掘等技术、系统安全基线、渗透测试与应急响应等技术。

**技术栈：**渗透测试、Python、黑/白盒测试、基线安全评估、内网渗透、web渗透测试、安全设备防护。

**项目经验：**网络安全架构、web渗透测试项目、安全评估与加固、内网渗透测试。

**授课特点：**幽默风趣、课堂气氛融洽，互动性强。

已授课学员人数  
**5000+**

带班薪资  
**15000+**

学员测试评分  
**99.70**

**学员评价：**技术能力强、备课充足、讲解细致。

05

# 就业保障



# 千锋网络安全就业保障

## 后续技术支持：一次学习，终身IT技能提高服务

- 1 毕业后提供网络安全、云计算、Python人工智能三大学科全套资源（视频+文档）
- 2 毕业后提供每月2-4次企业大牛技术提升课
- 3 毕业后提供专职老师技术支持
- 4 毕业后提供企业大咖录制的技术实战扩展课

## 宽广就业渠道：开创优质人才输出新模式

-  **招聘平台**  
整合企业招聘资源，搭建互联网行业优质人才输送平台，18000余家合作企业对千锋学员打开职场通道。
-  **上门招聘**  
企业定期上门招聘，在毕业班进行人才选拔，表现优秀即可直接录用。
-  **就业共享**  
全国 18 城 22 个教学中心可共享就业资源，方便学员自由选择工作地点，同城异地，就业畅通无阻。
-  **人才定制**  
与企业签订人才培养协议，按需求定制培养人才，学员毕业即可直接入职名企。
-  **企业内推**  
就业老师以企业人脉为渠道，将学员简历直接推送到 HR 手中，学员可快速面试入职。



# 千锋网络安全就业战报

## 千锋网络安全学员就业画像

推荐就业率

**40.4%**

就业薪资冠军

**¥18000**

平均就业薪资

**¥8330**

本科学历占比

**70.1%**

## 学员就业战报（部分）：和优秀的人一起学习，你会是另一种状态

姓名	学历	专业	薪资	入职单位
杨同学	专科	软件技术	15000	北京**科平
高同学	专科	软件技术	12000	3**团
王同学	专科	汽车工程系	12000	网**云
金同学	专科	物联网	10000	北京**信安
丁同学	专科	信息工程系	9000	启**辰
陈同学	专科	计算机系	8000	北京科德**限公司
赵同学	专科	计算机	8000	3**
谢同学	专科	计算机	8000	北京**环创
王同学	硕士+	其它	18000	保密
郑同学	高中	信息工程学院	10000	弘**行
张同学	本科	通信工程学院	16000	保密

06

合作企业

# 千锋网络安全合作伙伴

**教研合作：**从企业顾问教学到课程协同研发，千锋教育与众多企业展开深入合作教研领域持续共建，从未间断。



**人才合作：**联合企业共同探索并形成，上门招聘、订单培养、名企双选、企业直推等多元化人才合作新模式。



**战略合作：**与企业达成授权认证、共建基地、资源共享等多层次合作，全方位提升学员软实力，软硬兼具保持长足竞争力。



## 与启明星辰达成深度合作：联合研发教学课程，根据企业岗位定制课程

由千锋教育主导，启明星辰等企业联合研发教学课程，根据企业岗位定制，由用人单位评估，经多家企业联合研发。提供企业级实战平台，云众可信、众测实战项目，学习到一定程度后，即可成为企业注册白帽子，可参与真实的企业渗透、安服、风评等众测项目。



千锋学员很有特色，经过多轮面试我们发现每个学员都有自己独特的项目，并且能够详细说出技术要点，与其他培训机构学员完全不同，作为招聘者，很喜欢这种现象。



与千锋是长期合作伙伴，学员整体质量不错，能够满足我们的岗位需求，是一个值得信赖的培训机构。



千锋学员技能不错、实战能力很强，可以满足我们中高端人才需求，相信入职之后能够快速上手。



千锋能从实际工作入手，通过实践演练的方式，来巩固和提升学员基础知识的掌握程度，通过模拟线上业务场景，提高学员知识的运用、理解能力以及技能的提升。



经过面试不难发现，学员在千锋真的能够学到东西，具有过硬的开发本领，并且信心十足，可以说正是企业目前急需的IT人才。



虽是第一次，但我对千锋学员的整体质量很满意，我们招聘的多为高级开发工程师，一般培训机构无法满足，千锋确实符合我们的需求。