马士兵教育

定制未来，成就更好的你

马士兵教育

花名：万里

曾就职于奇安信集团，担任高级渗透测试工程师，从事网络安全工作7年，参与四届全国HW行动、北京冬奥重保等活动，担任CISP-PTE、CISP-IRE出题及监考，为CNCERT、SRC平台等提交数百漏洞。专注研究前沿网络安全技术，具有丰富的实战经验。擅长技术：Web渗透、内网渗透、代码审计、Kali、安全工具开发等。

中华人民共和国网络安全法

第二十七条

任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

课程内容仅用于以防御为目的的教学演示
请勿用于其他用途，否则后果自负

1、《中华人民共和国刑法》的相关规定：

第二百八十五条规定，非法侵入计算机信息系统罪;非法获取计算机信息系统数据、非法控制计算机信息系统罪;提供侵入、非法控制计算机信息系统程序、工具罪是指，违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金;情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

*

第一条

非法获取计算机信息系统数据或者非法控制计算机信息系统，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节严重”：

（一）获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上的；

（二）获取第（一）项以外的身份认证信息五百组以上的；

（三）非法控制计算机信息系统二十台以上的；

（四）违法所得五千元以上或者造成经济损失一万元以上的；

（五）其他情节严重的情形。

实施前款规定行为，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节特别严重”：

（一）数量或者数额达到前款第（一）项至第（四）项规定标准五倍以上的；

（二）其他情节特别严重的情形。

明知是他人非法控制的计算机信息系统，而对该计算机信息系统的控制权加以利用的，依照前两款的规定定罪处罚。

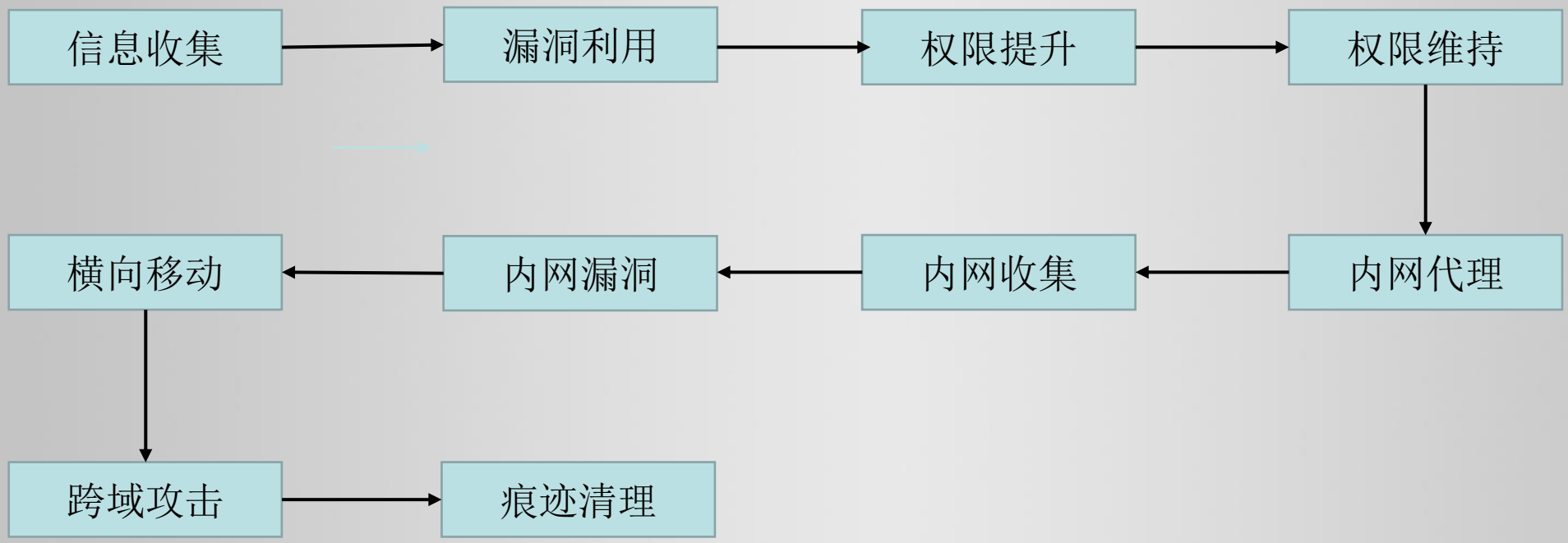
*

目录

课程安排

请查看课程安排表

渗透流程



网络安全大事件

八方网域
bafangwy.com







2010	2012	2013	2014	2015	2016	2017	2018	2019
震网	Flame	棱镜门	心脏出血	铁道部	美国断网	wannacry	华住	

世界上的hacker都属于什么

1. APT组织
2. 犯罪团伙
3. 职业白帽
4. 搞黑/灰产的
5. 个人爱好

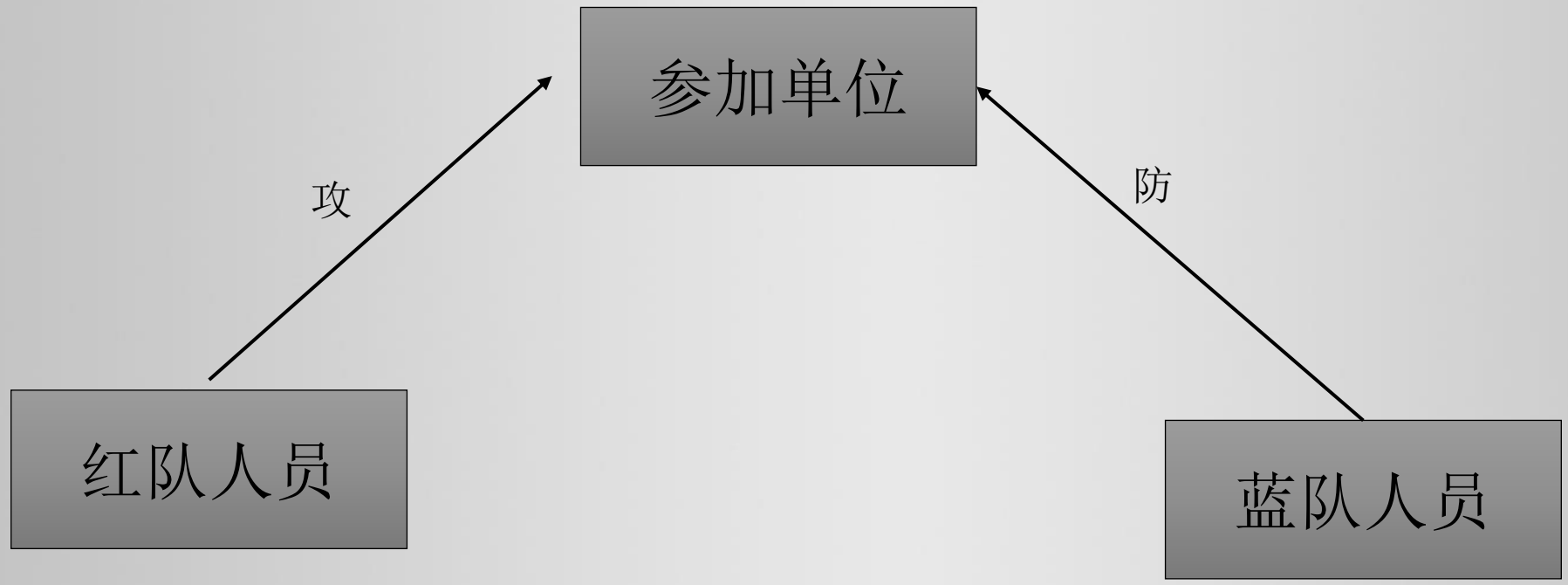
什么是HW行动

2016年，公安部会同民航局、国家电网组织开展了 “护网2016”网络安全攻防演习活动。同年，《网络安全法》颁布，出台网络安全演练相关规定：者应“制定网络安全事件应急预案，并定期进行演练”。自此“护网行动”进入人们视野关键信息基础设施的运营，成为网络安全建设重要的一环。

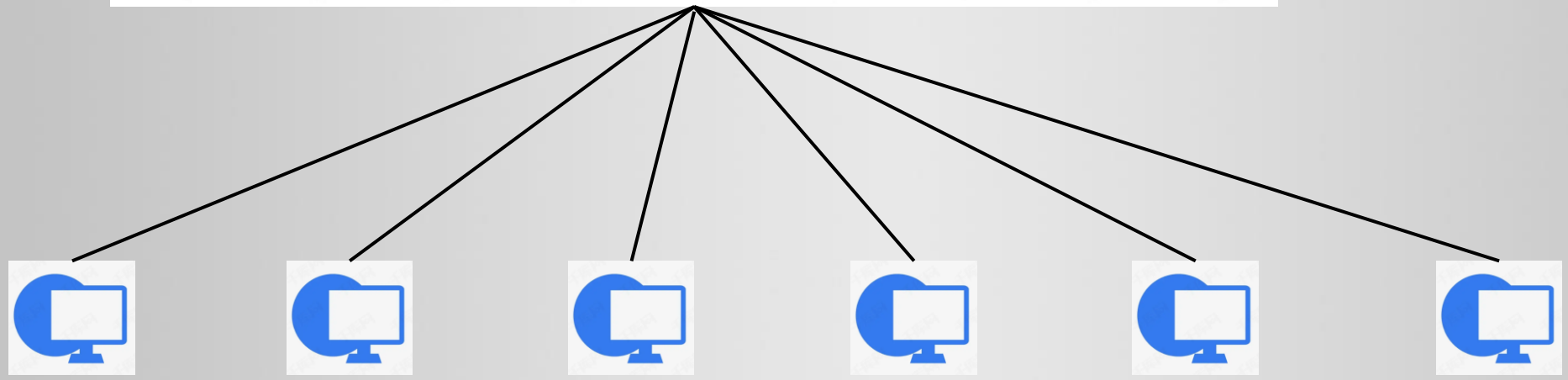
网传的HW指的就是护网，从2020年起，就被广大师傅们传成HVV。护网是当前国家、重要机关单位和企业组织用来检验网络安全防御能力的重要手段之一，是当下检验对关键信息系统基础设施网络安全保护工作的重要组成部分。

护网攻防演练这个概念是从2016年开始有的，在国家相关网络安全监管机构的推动下，网络安全演习工作日益得到重视，从而分出红队和蓝队，由红队担任攻击方、蓝队担任防守方，通过一定规则限制下进行实战网络攻防演练，即红蓝对抗。

什么是HW行动



什么是HW行动



为什么蓝队HW需要大量的人

运营商:中国电信、中国移动、中国联通
金融：农业银行、中信银行、中国银行、工商银行、建设银行、交通银行。。。。。
能源：中国华电集团公司、中煤能源公司
电力：华能、华电、国电、国电投和大唐
民航：国航、东方、南航、海南航空
共计百多家单位

HW能给自己带来什么利益

获得一笔很不错的收益
获得一笔很不错的收益
获得一笔很不错的收益

*

HW能给自己带来什么利益

蓝队：1000/天-6000/天

红队：5000/天-15000/天

按照一次HW15天计算，大概工资在2.25万至22.5万，按照二八定律，最高收入和最低收入是比较少的，基本日薪2000是比较多的，15天应该在4.5W左右，还有可能提前驻场，可能在30天左右。先去先得

HW能给自己带来什么利益

福利待遇

1、为每位参与2022护网行动的人员提供一份商业安全保险；

2、住宿（实报实销）

3、高铁机票交通费（实报实销）

4、核酸检测费（实报实销）

5、每位通过客户最终面试并签订协议书的同学先期支付住宿、交通费、核酸检测费以及一定数量的Hw费用

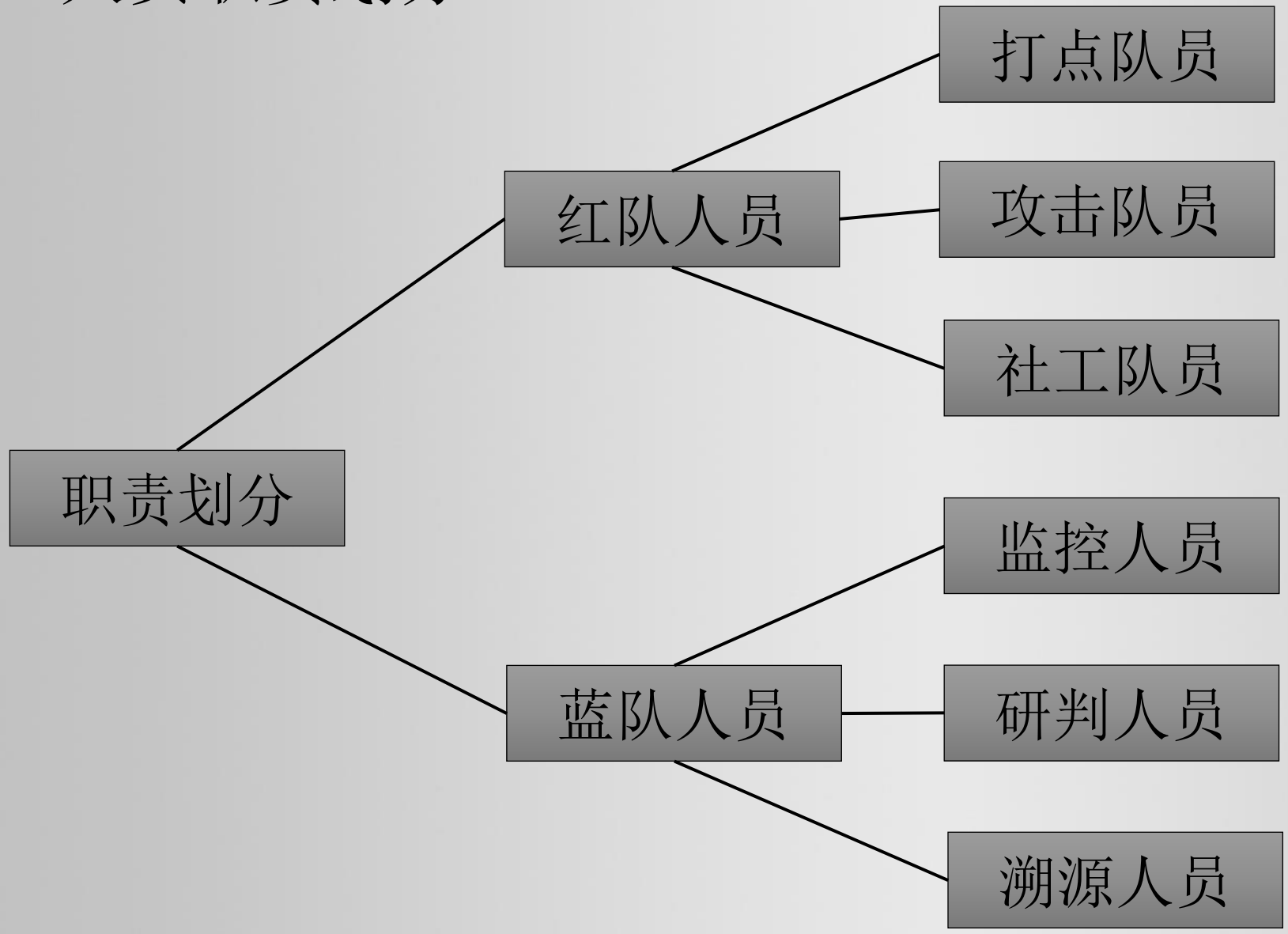
6、每位Hw行动的防守人员日薪：1000/天—20000/天，每天按照8小时算，如果工作了12h就按照1.5天算

HW能给自己带来什么利益

2、为自己的简历添加色彩，积累实际工作经验，可以帮助找到工作

3、结交朋友和大佬

HW人员职责划分



还有其他人员如、实验室、民间大佬等等

还有其他人员如、网络维护应急响应等等，一般是内部人员

HW需要具备的技能

红队人员

- 外围打点能力
- 代码审计能力
- 漏洞挖掘能力
- 木马免杀能力
- 漏洞分析能力
- 内网渗透能力
- 权限提升能力
- 横向移动能力
- 权限维持能力
- 域渗透能力
- 钓鱼远控能力
- 跨域渗透能力

*

HW需要具备的技能

蓝队人员

- 设备使用能力
- 设备监控能力
- 研判分析能力
- 攻击辨别能力
- 流量分析能力
- 入侵排查能力
- 日志分析能力
- 溯源分析能力
- 人肉搜索能力
- 逆向分析能力

网络安全都有哪些职业

八方网域
bafangwy.com

安全运维工程师

Java代码审计工程师

溯源、情报分析师

安卓逆向工程师

等保测评工程师

PHP代码审计工程师

黑产研究工程师

逆向分析工程师

安全服务工程师

安全工具开发师

渗透测试工程师

安全研究工程师

网络安全讲师

红队攻防工程师

*

网络安全企业


奇安信
QI-ANXIN


NSFOCUS
绿盟科技


Venus
启明星辰
领航信息安全


HUAWEI


安恒信息
DAS-security 安全中国


天融信
TOPSEC


SANGFOR
深信服科技


360政企安全


亚信安全