内网渗透

万里

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。

*

课程介绍

- 内网介绍
- 域环境搭建
- 工作组信息收集
- 域内信息收集
- 内网扫描
- NTML和LM哈希
- 密码抓取
- 横向移动