内网代理

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

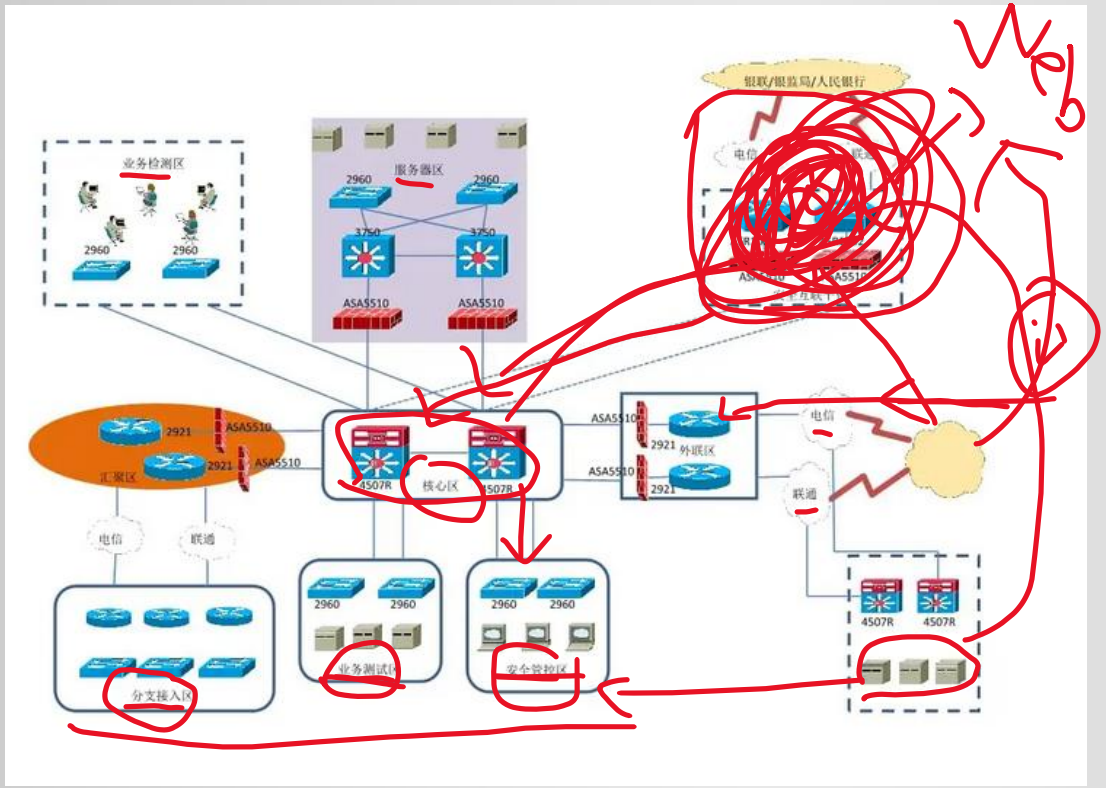
- 内网代理介绍
- 端口转发和端口映射
- 反弹shell的方法
- 客户端代理的使用
- 隐藏隧道的搭建

内网代理在攻防中的地位

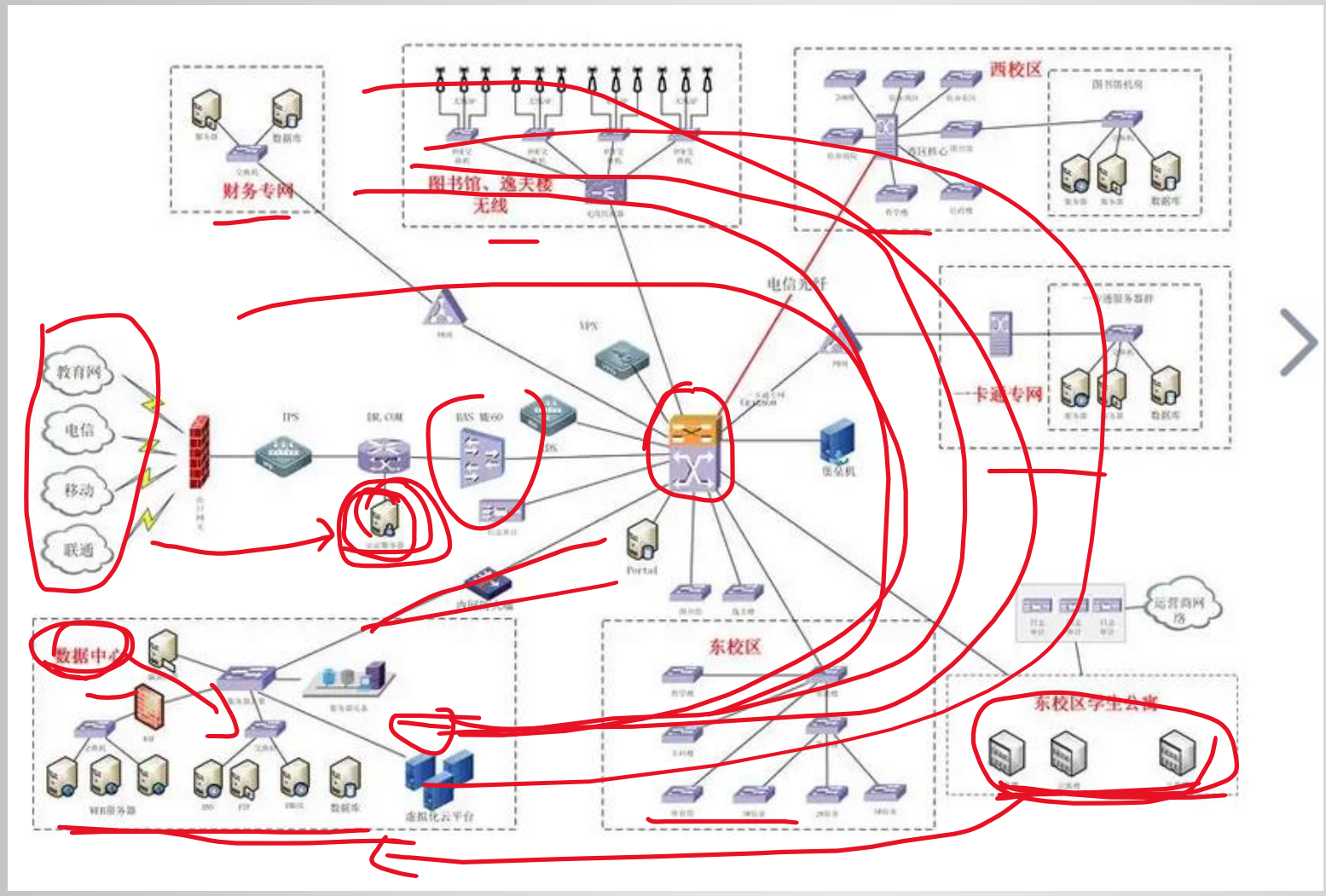
内网代理在攻防中的地位

攻击者通过边界主机进入内网，往往会利用它当跳板进行横向渗透，但现在的内部网络大多部署了很多安全设各，网络结构错综复杂，对于某些系统的访问会受到各种阻挠，这就需要借助代理去突破这些限制，因此面对不同的网络环境对于代理的选择及使用显得格外重要

内网代理在攻防中的作用



内网代理在攻防中的作用



概念介绍

端口转发和端口映射

端口转发,有时被称为做隧道,是安全壳(SSH)为网络安全通信使用的一种方法简单来说,端口转发就是将一个端口收到的流量转发到另一个端口。

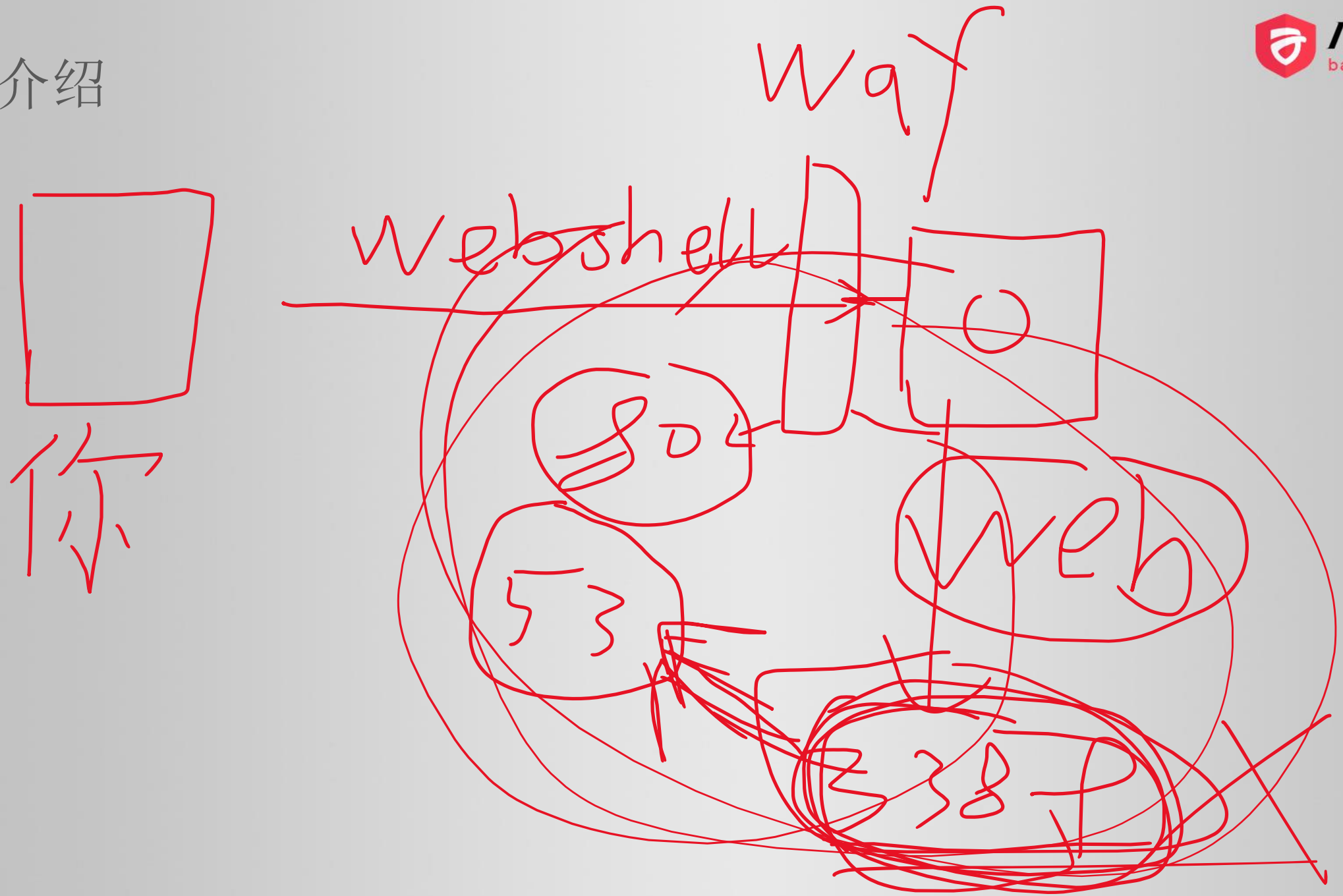
端口映射是 NAT的一种,功能是把在公网的地址转成私有地址。简单来说,端口映射就是将一个端口映射到另一个端口供其他人使用

Http代理和Socks代理

Http代理用的是Http协议，工作在应用层，主要是用来代理浏览器访问网页。

Socks代理用的是Socks协议，工作在会话层，主要用来传递数据包。socks代理又分为Socks4和Sock5，Socks4只支持TCP，而Socks5支持TCP和UDP。

概念介绍



概念介绍

反弹shell介绍

反弹shell（reverse shell），就是控制端监听在某TCP/UDP端口，被控端发起请求到该端口，并将其命令行的输入输出转到控制端。reverse shell与telnet，ssh等标准shell对应，本质上是网络概念的客户端与服务端的角色反转。

正向代理和反向代理

正向是从攻击者电脑主动访问目标机器，例如通过主动访问目标建立Shell是正向Shell。

反向是从目标机器主动连接攻击者电脑，例如通过在目标机器执行操作访问攻击者电脑建立的Shell是反向Shell

端口转发和映射

LCX是一款端口转发工具，分为Windows版和Linux版，Linux版本为PortMap。LCX有端口映射和端口转发两大功能，例如当目标的3389端口只对内开放而不对外开放时，可以使用端口映射将3389端口映射到目标的其他端口使用；当目标处于内网或目标配置的策略只允许访问固定某一端口时，可以通过端口转发突破限制。

反弹shell

Netcat反弹

Powercat反弹

Python反弹

Bash反弹

客户端代理的使用

Proxifier工具
ProxyChains 工具

隐藏隧道的搭建

ReGeorg
EarthWorm
FRP
Nsp
……