内网渗透如何打开突破口 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/454/2021_2022__E5_86_85_E7_BD_91_E6_B8_97_E9_c98_454857.htm 内网渗透的思想是源于特洛伊木马的思想---堡垒最容易从内部攻破，一个大型的网站，一个大型的公司，一个大型的目标，在外肉，管理员总会千方百计的加强防范和修补漏洞，常规的方法进去几乎是不可能。 内网渗透的突破口是我们如何得到一个内网的个人机或是内网的服务器，我个人的经验有三种，一是从外网分站渗透到内网，二是发木马信得到内网机器，三是利用取得信任得到内网机器。 一、从外网分站渗透到内网 通常一个大的站点都有很多分站，有很多我们未知的分站或是未知的站点目录，越大的站点展现在我们面前的机会就越多，可以利用传统手法得到一个分站的服务器权限，比如注入，猜解，溢出等。得到分站服务器的情况下有两种思想：一是通过分站渗到主站或是其它分站，需要它们分配有一个内网并没划分vlan的情况，这时可以通过取得密码或是内网嗅探等方式取得更多的分站。二是通过分站服务器的分析，诱使管理员中马，比如在分站服务器取得管理员的密码，收集分站上的邮箱信息，查看分站服务器的ftp信息，收集管理员常用的工具，或是管理员有可能下载回去的文件(通常是管理员传输工具的tools文件里)或是管理员保存在站点目录的工具。 二、发木马信取得内网机器 这应该算是一种社会工程学与漏洞的结合，比如0day，也就是word或是pdf或是ie0day发挥作用的地方。很多人拿到ie0day是直接用于挂马，其实ie0day发信的价值更高，如何欺骗管理员点击你发的邮件里的url链接也是一

种艺术。也可以想想，涉及到他网站的问题，他产品的问题，这样的东西管理员总会点击的，要考虑到管理员点击后会百分之百的中这是一个技术性问题。常规的木马信发送过程中，chm的木马用得更多，因为不被杀，命中率可达百分之百，然后就要考虑到管理员会打开么?即使是客服机器中马也一样的非常有用。比如我在一次木马信的发送中，使用的附件是打包的chm，信的内网是：“ 使用你们的xx后，我觉得相当不错，不过在使用过程中发现一些bug，不知道是我的机器问题还是你们这方面没有考虑到，具体信息我以图文形式保存在附件中。 ”当然要找到目标的邮件地址，这个在网站上或是google中很容易找到的。 三、利用取得信任得到内网机器 网站管理员或是客服，都会有email或是msn或是QQ，或是现实中的人，我们可以慢慢的套近乎，抓住他的弱点，或是心理，比如他喜欢的东西，慢慢跟他聊天，降低他的心理防线，在成熟的时候发送url，或是打包的软件里捆绑木马，也不是不可以的。具体的涉及到社会工程学方面，主要看自己怎么去发挥。 内网渗透-----如何打开突破口，这只是平时的一些经验总结，没有具体的步骤，只有一种思想，黑站已经不是一种单纯的玩注入的时代。过段时间将再写《内网渗透-----基本手法》，仅仅做技术上的探讨与分享。 