祥解HONEYPOT(蜜罐)引诱技术计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/643/2021_2022__E7_A5_A5_E8_A7_A3HONE_c98_643695.htm HONEYPOT（蜜罐）技术 什么是蜜罐 蜜罐（Honeypot）是一种在互联网上运行的计算机系统。它是专门为吸引并诱骗那些试图非法闯 入他人计算机系统的人（如电脑黑客）而设计的，蜜 罐系统是一个包含漏洞的诱骗系统，它通过模拟 一个或多个易受攻击的主机，给攻击者提供一个 容易攻击的目标。由于蜜罐并没有向外界提供真 正有价值的服务，因此所有对蜜罐尝试都被视为 可疑的。蜜罐的另一个用途是拖延攻击者对真正 目标的攻击，让攻击者在蜜罐上浪费时间。简单 点一说：蜜罐就是诱捕攻击者的一个陷阱。 一、初接触HoneyPot Defnet HoneyPot就是一款非常有名的蜜罐软件，它能够虚拟出各种常见的系统漏洞，从而等着黑客们上钩。 首先该软件。由于这是一款绿色软件，将下载后的文件直接解压即可运行。软件运行后，可以看到其界面还是比较简单的，其中左侧主要区域就是记录黑客攻击时的信息，而右侧则是相应的配置按钮。下面我们就对其进行必要的配置，使其成为一个完美的诱捕陷阱。 二、开启虚拟漏洞 单击软件主界面上的“ HoneyPot ”按钮打开程序配置窗口，首先在窗口左侧是常见的Web、FTP等伪装服务。例如我们要伪装成一台Web服务器，那么就可以在C盘根目录下创建一个wwwrood文件夹，然后在里面新建一个index.htm文件，同时还可以复制一个普通的文本文件放置到该目录下，以便用于伪装FTP服务器。 做好准备工作之后，我们就可以分别选中“ Web Server ”选项，同时在“ Port ”

中输入“ 80 ”即虚拟80端口，同时在“ Directory ”中填入“ C:wwwroot ”目录；同理可以选中“ FTP Server ”虚拟FTP服务器，如果选中“ Full Access ”即指该虚拟FTP开放所有权限。 除了伪装常见的服务之外，我们还可以伪装本地磁盘。选中右下角的“ Telnet Server ”，然后单击“ Advanced ”按钮，在打开的窗口中分别设置驱动器盘符“ Drive ”、卷标“ Volume ”、可用空间“ Free Space in bytes ”等详细信息，以使虚拟的系统更加真实可靠。全国计算机等级考试网，加入收藏 设置好这些信息之后，返回软件主界面，单击“ Monitore ”按钮，这样程序即开始工作。 当黑客开始扫描我们的计算机时，他发现的所有漏洞都是由蜜罐提供的虚拟漏洞，而这一切黑客并不知情，或许还在为自己的成功侵入而暗自高兴呢，其实此时我们完全可以从主界面上看到黑客们所进行的一举一洞了。 三、远程查看数据 由于蜜罐一般都是布置在服务器上，作为管理员不可能随时都坐在服务器前。对此，我们可以使用邮件来接收蜜罐的诱捕记录。 单击主界面上的“ Options ”按钮，然后选中“ Send logs by e-mail ”项，并在“ Your e-mail ”处填写接收的邮件地址，在“ Server ”处填写邮件服务器地址，同时在“ For ”处填写发送地址，最后在“ Authentication required ”处填写邮箱的用户名和密码，这样保存设置之后程序即可按照预定的设置将黑客们攻击而留下的日志发送到指定信箱了。 布置好了蜜罐，我们就可以对黑客们的入侵采集下证据，而且保证了计算机的安全。如果你饱受黑客攻击，那么赶紧布置一个“ 甜蜜的罐子 ”来诱捕黑客吧。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com