浅谈蜜罐技术及其应用

蜜罐技术是信息安全保障的研究热点与核心技术。本文介绍了目前国际上先进的网络安全策略一蜜罐技术及其运作方法，并对近年来蜜罐技术的研究进展进行了综述评论。同时也探讨一种全新的网络安全策略一蜜网。

1 引言

随着计算机网络技术的发展，网络在世界经济发展中的地位已十分重要。然而在网络技术日益发展的同时“黑客”们对网络的攻击从未停止过。我们目前的主要防范策略就是构建防火墙。通过防火墙来阻止攻击，保障网络的正常运行。

2 蜜罐技术

一般情况下，防火墙确实起到了一定的保护作用，但是细想一下，这样却不近常理，“黑客”们在不断的攻击，我们的网络总是处于被动的防守之中。既不知道自己已被攻击，也不知道谁在攻击。岂有久攻不破之理。虽然网络安全技术在不断的发展，“黑客”们攻击方法也在不断翻新，在每次的攻击中“黑客”们并没有受到任何约束和伤害，一次失败回头再来。而且在这众多“黑客”对个别营运商的局面下，我们是否太被动了，稍有不周就遭恶运。

而蜜罐好比是情报收集系统。蜜罐好像是故意让人攻击的目标，引诱黑客前来攻击。所以攻击者入侵后，你就可以知道他是如何得逞的，随时了解针对服务器发动的最新的攻击和漏洞。还交可以通过窃听黑客之间的联系，收集黑客所用的种种工具，并且掌握他们的社网络。

蜜罐 Honeypot 以及蜜罐延伸技术，当前十分流行，它已不是一种新的技术，

可以说是一大进步的安全策略。它使我们知道正在被攻击和攻击者，以使“黑客”们有所收敛而不敢肆无忌惮。蜜罐的引入，类似于为网络构建了一道防火沟，使攻击者掉入沟中，装入蜜罐以至于失去攻击力，然后再来个瓮中捉鳖。关于蜜罐，目前还没有一个完整的定义。读者可以参阅 ClifStoil 所著“Cuckoo’ s"Egg''，和 BillCheswick 所著“AnEvwitllBeId”。在此我们把蜜罐定义为“一种被用来侦探，攻击或者缓冲的安全资源”。当今处于商业运作的蜜罐技术方案主要是两种：商品型和研究型。商品型主要就是通过使黑客攻击蜜罐从而减轻网络的危险。研究型主要就是通过蜜罐来获得攻击者的信息，加以研究。实现知己知彼，既了解黑客们的动机，又发现我们所面临的危险，从而更好地加以防范。无论是商品型还是研究型蜜罐，他们的主要目的是被用来探测、攻击和潜在的开发利用。

实际上蜜罐就是一种工具，怎样使用该工具由你决定，并取决于你打算做什么。它是一个仿效系统或应用程序系统，它建立了一个监狱系统。它的主要目的就是诱人攻击。

3 蜜罐技术的分类和比较

目前蜜罐技术的应用比较广泛，主要用于攻击的检测、捕获、分析、取证、预警以及网络安全的教学等方面。下面从蜜罐和蜜网两个方面分类比较，剖析现有系统的最新研究进展及其特征。

根据系统的功能，蜜罐可以分为产品型和研究型两类。1)产品型蜜罐主要是用于攻击检测、预警防御和取证，为一个组织的网络提供安全保护。它一般采用虚拟的操作系统和应用程序来构建系统，部署在一个部门的内部网络环境。这类蜜罐系统的代表有 SymantecDecoyServer、SmokeDetector、Honeyd、Specter、ManTraq 等。随着研究的深入，产品型蜜罐出现了针对特定攻击的应用，比如检

测内部攻击的 Honeytoken，检测缓冲区溢出攻击的 TaintCheck，检测对无线网络攻击的 802．11Honeypot，检测恶意网站对浏览器攻击的 Honeyclient 检测 DOS 攻击，检测恶意代码攻击的 HoneyStat，检测垃圾邮件攻击的 HoneySpam，检测 Web 应用攻击的 HoneyWeb“等。

研究型蜜罐主要是用于研究攻击的特征和发展趋势，以帮助安全组织研究系统所面临的威胁，以便更好地抵抗这些威胁。它一般采用真实的操作系统和应用程序来构建系统，部署在网络系统中各个网段上。例如，Kreibich 提出了一种从 Honeypot 捕获的数据中自动提取攻击特征的 LCS(1ongest-com—mon—subsVing)算法，该算法比较简单，但是提取的攻击特征质量较差。UoitaThakar 首先采用可视化、统计分析等方法辅助人工筛选出可疑数据，然后基于 LCS 算法从选出的数据中自动提取攻击特征。该方法提高了攻击特征提取的质量，但是还需要人工参与。产品型蜜罐部署简单，引入风险低，容易维护，但是捕获的攻击信息少。研究型蜜罐可以捕获大量的攻击信息，但是部署复杂，维护代价大。根据系统允许与黑客交互活动的级别，蜜罐可分为低交互蜜罐与高交互蜜罐。低交互蜜罐允许蜜罐与黑客交互活动次数少，通常采用虚拟的操作系统和应用程序来构建系统。多数产品型蜜罐属于低交互蜜罐。高交互蜜罐一般不限制黑客与蜜罐交互的活动，通常采用真实的操作系统和应用程序来构建系统。研究型蜜罐一般属于高交互蜜罐，也有部分产品型蜜罐属于高交互蜜罐，如 ManTrap。低交互蜜罐与黑客交互次数少，引入的风险较小，但是容易被攻击者识别，捕获的攻击信息少。高交互蜜罐捕获的攻击信息较多，容易捕获到新的攻击工具，但是部署复杂，难以维护，引入了较高的安全风险。

还可以根据服务实现方式分类。为了欺骗攻击者，蜜罐需要提供与真实的主

机相似的操作系统和服务。根据服务实现方式将蜜罐系统分为真实蜜罐和虚拟蜜罐。真实蜜罐是由真实的主机、操作系统和应用程序构建的。主要用于获取攻击行为。虚拟蜜罐是由虚拟的操作系统和应用程序构建的，黑客的行为只能局限在模拟的级别。主要用于攻击的检测、预警防御等。较具代表性的系统如 DTK、Honeyd 等开源工具和 KFSensor、 ManTrap 等一系列的商业产品。虚拟蜜罐又可以分为手写脚本的蜜罐和学习服务的蜜罐。手写脚本的蜜罐是手工编写脚本，模拟一个真实的系统。学习服务的蜜罐是通过机器学习由系统编写脚本，模拟一个真实的系统。学习服务的蜜罐是实现动态蜜罐 n 的一个关键的技术，但是实现难度较大。真实蜜罐交互程度高，无蜜罐指纹，捕获的攻击信息量大，适合作研究，但是高交互引入了较高的安全风险。虚拟蜜罐部署比较方便，引入风险较低，适合作为商业产品，但是收集攻击数据少，易被黑客识别。

根据服务提供方式将蜜罐分为服务端蜜罐和客户端蜜罐。服务端蜜罐是运行服务端的软件，等待攻击者来入侵。目前大部分蜜罐是服务端蜜罐。客户端蜜罐是运行客户端的软件，模拟普通的互联网客户端访问恶意网站或间谍软件，如 Honeyclient。服务端蜜罐通过诱骗攻击者攻击来了解服务器端的安全威胁，但是难以发现针对客户端的安全威胁。客户端蜜罐通过模拟客户端访问恶意网站或间谍软件来发现浏览器的漏洞，主动了解互联网上针对客户端的安全威胁，但是难以发现针对服务端的安全威胁。

4 蜜罐技术的问题和发展趋势

近年来蜜罐技术在安全领域的应用越来越广泛。但是，蜜罐技术的应用仍受到很多问题的困扰，我们认为蜜罐技术现阶段面临的主要挑战其主要特征是：

①模拟服务交互程度低，容易被识别；

②系统架构部署和维护还比较复杂，难以有效控制风险，不能满足大规模网络环境的需要；

③数据表示和存储不统一；

④分析攻击信息的工具的功能较为有限；

⑤触犯法律问题。

下面主要论述解决这些关键问题可能采取的方法。

(1)增强系统智能性，动态自适应网络变化。由于采用真实的系统环境实现蜜罐系统，其部署代价大，管理维护困难，而采用虚拟的系统环境实现蜜罐系统，其交互程度低，因此，为了实时地与受保护的目标网络环境保持一致，防止入侵者识别，捕获尽可能多的攻击信息，需要提高模拟服务的质量，增强系统智能性，感知和学习目标网络环境，动态自适应网络变化，自动地进行系统配置。

(2)采用分布式蜜罐部署技术，简化部属复杂性。目前在大规模网络环境部署蜜罐系统，其代价和风险仍然较大，管理与维护比较困难，因此需要构建一个开放的分布式蜜罐体系结构，包括层次化、支持分布式处理、统～资源管理、统一用户界面接口、可配置算法服务和工作流、良好的可扩展能力等，构成一个有效的大规模网络安全风险态势感知模型，确保其它业务对攻击数据资源的需求与共享，提高网络整体的安全防护水平。

(3)统一数据格式，融合多源信息。多源信息融合是大规模网络环境中安全风险态势感知和攻击分析与趋势预测的重要环节之一。它使得一方面可以及时利用局部获得的采集信息来分析攻击、预测潜在的安全隐患，另一方面又能通过局部信息的汇集与融合对攻击和整体的安全状况进行分析预测并反过来对攻击和局部的安全隐患形成更准确的判断。因而需要用统一的标准来表示和存储从各个

子网中采集的攻击信息，并对多源信息进行精化处理与数据挖掘，根据信息的特性选择最优化的融合算法，以提高融合分析的快速性与准确性。

(4)自动分析和提取攻击特征。虽然蜜罐采集的攻击数据少而精，但是仍需要专家投入较多的精力和时间，很多有价值的信息要通过专家的手工分析才能得到的，难以满足实际的需要。因此，可以借鉴其它领域中处理数据信息的一些成熟的理论、方法和技术，对蜜罐系统捕获的数据从网络数据流、系统日志、攻击工具、入侵场景等多个层次进行分析，利用可视化、统计分析、机器学习和数据挖掘等方法研究攻击特征，自动识别攻击的工具、策略、动机，提取未知攻击的特征，分析攻击趋势。

(5)与各种安全技术整合，构建优势互补的网络安全体系。蜜罐系统只能检测和捕获那些和它进行交互的攻击行为，不能直接防护有漏洞的信息系统，而且其部署会给网络引入一定的安全风险。蜜罐系统与防火墙、入侵检测等其它安全系统协作和联动，有利于提高阻止、检测和响应攻击的能力，弥补单一的安全技术和产品的不足，也是网络安全纵深防御的一个发展趋势。

(6)计算机取证和法律问题。蜜罐系统捕获的信息都是与入侵者有关，信息量小，能够迅速找到犯罪证据，因此可以用于计算机取证。蜜罐是一种防御系统，只要不对部署的蜜罐进行宣传，就不会触犯到法律。但是如果蜜罐被黑客用来攻击第三方网络而造成破坏，就会被受害方提出诉讼，因此当黑客利用蜜罐向第三方网络发起攻击时，需要采取强有力的控制措施来避免此风险。

5.蜜罐的配置模式

①诱骗服务（**deceptionservice**）

诱骗服务是指在特定的 IP 服务端口帧听并像应用服务程序那样对各种网络

请求进行应答的应用程序。DTK 就是这样的一个服务性产品。DTK 吸引攻击者的诡计就是可执行性，但是它与攻击者进行交互的方式是模仿那些具有可攻击弱点的系统进行的，所以可以产生的应答非常有限。在这个过程中对所有的行为进行记录，同时提供较为合理的应答，并给闯入系统的攻击者带来系统并不安全的错觉。例如，当我们将诱骗服务配置为 FTP 服务的模式。当攻击者连接到 TCP/21 端口的时候，就会收到一个由蜜罐发出的 FTP 的标识。如果攻击者认为诱骗服务就是他要攻击的 FTP，他就会采用攻击 FTP 服务的方式进入系统。这样，系统管理员便可以记录攻击的细节。

②弱化系统（**weakenedsystem**）

只要在外部因特网上有一台计算机运行没有打上补丁的微软 Windows 或者 RedHatLinux 即行。这样的特点是攻击者更加容易进入系统，系统可以收集有效的攻击数据。因为黑客可能会设陷阱，以获取计算机的日志和审查功能，需要运行其他额外记录系统，实现对日志记录的异地存储和备份。它的缺点是“高维护低收益”。因为，获取已知的攻击行为是毫无意义的。

③强化系统（**hardenedsystem**）

强化系统同弱化系统一样，提供一个真实的环境。不过此时的系统已经武装成看似足够安全的。当攻击者闯入时，蜜罐就开始收集信息，它能在最短的时间内收集最多有效数据。用这种蜜罐需要系统管理员具有更高的专业技术。如果攻击者具有更高的技术，那么，他很可能取代管理员对系统的控制，从而对其它系统进行攻击。

④用户模式服务器（**usermodeserver**）

用户模式服务器实际上是一个用户进程，它运行在主机上，并且模拟成一个真实的服务器。在真实主机中，每个应用程序都当作一个具有独立 IP 地址的操

作系统和服务的特定是实例。而用户模式服务器这样一个进程就嵌套在主机操作系统的应用程序空间中，当 INTERNET 用户向用户模式服务器的 IP 地址发送请求，主机将接受请求并且转发到用户模式服务器上。（我们用这样一个图形来表示一下他们之间的关系）：这种模式的成功与否取决于攻击者的进入程度和受骗程度。它的优点体现在系统管理员对用户主机有绝对的控制权。即使蜜罐被攻陷，由于用户模式服务器是一个用户进程，那么 Administrator 只要关闭该进程就可以了。另外就是可以将 FIREWALL,IDS 集中于同一台服务器上。当然，其局限性是不适用于所有的操作系统。

6.蜜罐的信息收集

当我们察觉到攻击者已经进入蜜罐的时候，接下来的任务就是数据的收集了。数据收集是设置蜜罐的另一项技术挑战。蜜罐监控者只要记录下进出系统的每个数据包，就能够对黑客的所作所为一清二楚。蜜罐本身上面的日志文件也是很好的数据来源。但日志文件很容易被攻击者删除，所以通常的办法就是让蜜罐向在同一网络上但防御机制较完善的远程系统日志服务器发送日志备份。（务必同时监控日志服务器。如果攻击者用新手法闯入了服务器，那么蜜罐无疑会证明其价值。）

近年来，由于黑帽子群体越来越多地使用加密技术，数据收集任务的难度大大增强。如今，他们接受了众多计算机安全专业人士的建议，改而采用 SSH 等密码协议，确保网络监控对自己的通讯无能为力。蜜网对付密码的计算就是修改目标计算机的操作系统，以便所有敲入的字符、传输的文件及其它信息都记录到另一个监控系统的日志里面。因为攻击者可能会发现这类日志，蜜网计划采用了一种隐蔽技术。譬如说，把敲入字符隐藏到 NetBIOS 广播数据包里面。

7.蜜罐的实际例子

下面我们以 Redhatlinux9.0 为平台，做一个简单的蜜罐陷阱的配置。

我们知道，黑客一旦获得 root 口令，就会以 root 身份登录，这一登录过程就是黑客入侵的必经之路。其二，黑客也可能先以普通用户身份登录，然后用 su 命令转换成 root 身份，这又是一条必经之路。

我们讨论如何在以下情况下设置陷阱：

(1)当黑客以 root 身份登录时；

(2)当黑客用 su 命令转换成 root 身份时；

(3)当黑客以 root 身份成功登录后一段时间内；

第一种情况的陷阱设置

一般情况下，只要用户输入的用户名和口令正确，就能顺利进入系统。如果我们在进入系统时设置了陷阱，并使黑客对此防不胜防，就会大大提高入侵的难度系数。例如，当黑客已获取正确的 root 口令，并以 root 身份登录时，我们在此设置一个迷魂阵，提示它，你输入的口令错误，并让它重输用户名和口令。而其实，这些提示都是虚假的，只要在某处输入一个密码就可通过。黑客因此就掉入这个陷阱，不断地输入 root 用户名和口令，却不断地得到口令错误的提示，从而使它怀疑所获口令的正确性，放弃入侵的企图。

给超级用户也就是 root 用户设置陷阱，并不会给系统带来太多的麻烦，因为，拥有 root 口令的人数不会太多，为了系统的安全，稍微增加一点复杂性也是值得的。这种陷阱的设置时很方便的，我们只要在 root 用户的.profile 中加一段程序就可以了。我们完全可以在这段程序中触发其他入侵检测与预警控制程序。陷阱程序如下：

```
#root.profile

Clear

Echo “Youhadinputanerrorpassword,pleaseinputagain!”

Echo

Echo –n “Login:”

Readp

If(“$p”=“123456”)then

Clear

Else

Exit
```

第二种情况的陷阱设置

在很多情况下，黑客会通过 su 命令转换成 root 身份，因此，必须在此设置陷阱。当黑客使用 su 命令，并输入正确的 root 口令时，也应该报错，以此来迷惑它，使它误认为口令错误，从而放弃入侵企图。这种陷阱的设置也很简单，你可以在系统的/etc/profile 文件中设置一个 alias，把 su 命令重新定义成转到普通用户的情况就可以了，例如 aliassu=” suuser1”。这样，当使用 su 时，系统判断的是 user1 的口令，而不是 root 的口令，当然不能匹配。即使输入 suroot 也是错误的，也就是说，从此屏蔽了转向 root 用户的可能性。

第三种情况的陷阱设置

如果前两种设置都失效了，黑客已经成功登录，就必须启用登录成功的陷阱。一旦 root 用户登录，就可以启动一个计时器，正常的 root 登录就能停止计时，而非法入侵者因不知道何处有计时器，就无法停止计时，等到一个规定的时间到，

就意味着有黑客入侵,需要触发必要的控制程序,如关机处理等,以免造成损害,等待系统管理员进行善后处理。陷阱程序如下:

```
#.testfile

times=0

while[$times－le30]do

sleep1

times=$[times+1]

done

halt/*30 秒时间到，触发入侵检测与预警控制*/

将该程序放入 root.bashrc 中后台执行：

#root.bashrc

….

Sh.testfile&
```

该程序不能用 Ctrl-C 终止，系统管理员可用 jobs 命令检查到，然后用 kill%n 将它停止。

从上述三种陷阱的设置，我们可以看到一个一般的规律：改变正常的运行状态，设置虚假信息，使入侵者落入陷阱，从而触发入侵检测与预警控制程序。

8 蜜网的作用

蜜网的作用主要表现在它的使用价值和研究价值两个方面。我们在进行传统的防护墙开发时，对于谁在攻击、何时被攻击、采用什么方法和手段进行攻击、攻击的目的是什么，这些都是未知数。进行所有可能的全方位的防护?就如同用

百万大军来抵御一个盗贼。

产品型蜜网可以说是一个真实运行网的拷贝，它完全模拟的仿真，不易被黑客发现。当有入侵发生时及时了解和获得黑客们的信息，实现知己知彼，变被动地受攻击为主动地出击，实现重点防范。其中可以有系统的自动行为，也可有人工参与措施。既实现了有效的防护，又节约了成本。通过跟踪及时准确地记录黑客的攻击信息，获得入侵的犯罪证据。蜜网的引入解决了网络安全中的两大难题。首先，能使我们及时认识到网络安全中的隐患。有了蜜网，就可以将黑客们的时间和精力都耗在对蜜网的攻击上。每次成功攻击都不会影响我们的网络，同时为我们找出了网络安全漏洞以便补漏。可以说是一件变害为宝的好事。其次，解决了证据收集难的问题。在网上客户信息数据交流量十分庞大，要在这茫茫数据海洋中找出黑客信息，并区分其危险等级从而加以防范，确实不是件容易事。然而在蜜网中，都是些黑客或者说有些是误入歧途者，信息量不大，通过跟踪与检测能从中找到不被污染的证据。蜜网的引入解决了网络中的安全与速度的矛盾，给我们带来了效率的提高和使用的方便。蜜网的研究价值并不是进行防御，而是按部就班地记录“黑帽子团体”的攻击过程，记录他们所使用的工具。通过分析就可以找到目前我们还未知的缺陷以及黑客技术的发展。同时也考验我们的阻止、发现和反应是否达到要求。从而改进我们的系统。一般来说研究型蜜网并没有商业化，它通常用于大学、军事、政府安全机构和研究部门等。

9 结语

本文剖析了蜜罐技术的相关概念、分类及其应用，比较了各类系统的优缺点，总结了蜜罐技术近年来的研究进展，研究了蜜罐的工作方法，重点讨论了近期所面临的一些主要问题及最新成果，并对将来的一些研究工作进行了展望。蜜罐技

术是一种应用欺骗思想的主动防御技术。在攻击检测、分析、特征提取、追踪、取证和预警防御等方面已经取得了比较显著的研究成果，展现了广泛的应用前景，是现有安全机制的有力补充。但随着相关应用的发展及需求的不断提升，仍有很多值得研究的问题。随着机器学习、数据挖掘和相关领域理论和技术研究的深入，针对不同实际应用，特别是系统动态自适应、分布式蜜罐体系结构、多源信息融合、攻击特征自动提取及计算机取证等问题，将成为蜜罐技术相关研究和应用的重点和主要突破的方向。